D-Link DGS-1510 シリーズ

Gigabit Layer 2+ Stackable Smart Pro Switch

ユーザマニュアル

D-Link
Building Networks for People

安全にお使いいただくために

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

安全上のご注意　必ずお守りください

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

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

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

⚠危険

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

⃠ 禁止 **ぬれた手でさわらない**
感電の原因となります。

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

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

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

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

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

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

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

⚠警告

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

⚠警告

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

⚠注意

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

電波障害自主規制について

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

ご使用上の注意

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

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

静電気障害を防止するために

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

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

2. 静電気に敏感な部品を運ぶ場合、最初に必ず静電気対策を行ってください。

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

電源の異常

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

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

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

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

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

目次

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

はじめに 13

本マニュアルの対象者 15
表記規則について 15
製品名 / 品番一覧 15

第 1 章　本製品のご利用にあたって 16

スイッチ概要 16
SFP について 16
前面パネル 17
Reset（リセットボタン） 17
LED 表示 18
背面パネル 20
側面パネル 21
スマートファンについて 22

第 2 章　スイッチの設置 23

パッケージの内容 23
ネットワーク接続前の準備 23
ゴム足の取り付け（19 インチラックに設置しない場合） 23
19 インチラックへの取り付け 24
SFP スロットの設置 25
電源抜け防止クリップの装着 25
電源の投入 27
電源の異常 27

第 3 章　スイッチの接続 28

エンドノードと接続する 28
ハブまたはスイッチと接続する 28
バックボーンまたはサーバと接続する 29

第 4 章　スイッチ管理について 30

Web GUI による管理 30
SNMP による管理 30
CLI による管理 30
コンソールポートの接続 31
端末をコンソールポートに接続する 31
ユーザアカウント / パスワードの設定 32
IP アドレスの設定 32
SNMP 設定 33
トラップ 33
MIB 33

第 5 章　Web ベースのスイッチ管理 34

Web ベースの管理について 34
Web マネージャへのログイン 34
Smart Wizard 設定 36
Web モードの選択（Smart Wizard） 36
IP アドレスの設定（Smart Wizard） 37
ユーザアカウントの設定（Smart Wizard） 38
SNMP の設定（Smart Wizard） 39
Web ベースのユーザインタフェース 40
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） 40
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） 41
Web マネージャのメニュー構成 42

第 6 章　System（システム設定）　44

Device Information（デバイス情報）....45
System Information Settings（システム情報）....46
Peripheral Settings（環境設定）....46
Port Configuration（ポート設定）....47
Port Settings（ポート設定）....47
Port Status（ポートステータス）....48
Port GBIC（ポート GBIC 情報）....48
Port Auto Negotiation（ポートオートネゴシエーション）....48
Error Disabled Settings（エラーディセーブル設定）....49
Jumbo Frame（ジャンボフレーム設定）....50
Interface Description（インタフェース概要）....50
PoE（PoE の管理）（DGS-1510-28P/28XMP）....51
PoE System（PoE システム設定）....51
PoE Status（PoE ステータス）....52
PoE Configuration（PoE ポート設定）....52
PD Alive（PD アライブ）....53
PoE Statistics（PoE 統計）....54
PoE Measurement（PoE 測定）....54
PoE LLDP Classification（PoE LLDP 分類表示）....55
System Log（システムログ）....56
System Log Settings（システムログ設定）....56
System Log Discriminator Settings（システムログディスクリミネーター設定）....57
System Log Server Settings（システムログサーバの設定）....58
System Log（システムログ）....58
System Attack Log（システムアタックログ）....58
Time and SNTP（時間設定・SNTP 設定）....59
Clock Settings（時間設定）....59
Time Zone Settings（タイムゾーン設定）....59
SNTP Settings（SNTP 設定）....61
Time Range（タイムレンジ設定）....62

第 7 章　Management（スイッチの管理）　63

User Accounts Settings（ユーザアカウント設定）....64
Password Encryption（パスワード暗号化）....65
Login Method（ログイン方法）....66
SNMP（SNMP 設定）....67
トラップ....67
MIB....68
SNMP Global Settings（SNMP グローバル設定）....68
SNMP Linkchange Traps Settings（SNMP リンクチェンジトラップ設定）....69
SNMP View Table Settings（SNMP ビューテーブル）....69
SNMP Community Table Settings（SNMP コミュニティテーブル設定）....70
SNMP Group Table Settings（SNMP グループテーブル設定）....71
SNMP Engine ID Local Settings（SNMP エンジンローカル ID 設定）....71
SNMP User Table Settings（SNMP ユーザテーブル設定）....72
SNMP Host Table Settings（SNMP ホストテーブル設定）....73
RMON（RMON 設定）....74
RMON Global Settings（RMON グローバル設定）....74
RMON Statistics Settings（RMON 統計情報）....74
RMON History Settings（RMON ヒストリ設定）....75
RMON Alarm Settings（RMON アラーム設定）....76
RMON Event Settings（RMON イベント設定）....77
Telnet / Web Settings（Telnet /Web 設定）....78
Session Timeout（セッションタイムアウト）....79
DHCP（DHCP 設定）....79
Service DHCP（DHCP サービス）....79
DHCP Class Settings（DHCP クラスサービス設定）....80
DHCP Server（DHCP サーバ）....81
DHCPv6 Server（DHCPv6 サーバ設定）....87
DHCP Relay（DHCP リレー）....90
DHCPv6 Relay（DHCPv6 リレー）....95
DHCP Auto Configuration（DHCP 自動設定）....96

DNS（ドメインネームシステム）.....97
DNS Global Settings（DNS グローバル設定）.....97
DNS Name Server Settings（DNS ネームサーバ設定）.....98
DNS Host Settings（DNS ホスト名設定）.....98
NTP（ネットワークタイムプロトコル）.....99
NTP Global Settings（NTP グローバル設定）.....99
NTP Server Settings（NTP サーバ設定）.....99
NTP Peer Settings（NTP ピア設定）.....100
NTP Access Group Settings（NTP アクセスグループ設定）.....101
NTP Key Settings（NTP 鍵設定）.....102
NTP Interface Settings（NTP インタフェース設定）.....102
NTP Associations（NTP アソシエーション）.....103
NTP Status（NTP ステータス）.....104
IP Source Interface（IP ソースインタフェース）.....104
File System（ファイルシステム）.....105
Physical Stacking（物理スタッキング）.....107
シングル IP マネジメント（SIM）設定 110
シングル IP マネジメント（SIM）の概要.....110
シングル IP マネジメント（SIM）のルールと動作.....110
バージョン 1.61 へのアップグレード.....111
Single IP Settings（シングル IP 設定）.....112
Topology（トポロジ）.....113
ツールヒント 115
Firmware Upgrade（ファームウェア更新）.....117
Configuration File Backup/ Restore（コンフィグレーションファイルの更新）.....117
Upload Log File（ログファイルのアップロード）.....117
D-Link Discovery Protocol（D-Link ディスカバリプロトコル）.....118

第 8 章　L2 Features（レイヤ 2 機能の設定）　119

FDB（FDB 設定）.....120
Static FDB（スタティック FDB 設定）.....120
MAC Address Table Settings（MAC アドレステーブル設定）.....121
MAC Address Table（MAC アドレステーブル）.....122
MAC Notification（MAC 通知設定）.....123
VLAN（VLAN 設定）.....124
VLAN Configuration Wizard（ VLAN 設定ウィザード）.....124
802.1Q VLAN Settings（802.1Q VLAN 設定）.....125
VLAN Interface（VLAN インタフェース設定）.....125
802.1v Protocol VLAN（802.1v プロトコル VLAN）.....128
GVRP（GVRP 設定）.....129
Asymmetric VLAN（Asymmetric VLAN 設定）.....131
MAC VLAN（MAC VLAN 設定）.....132
L2VLAN Interface Description（L2 VLAN インタフェース概要）.....132
Auto Surveillance VLAN（自動サーベイランス VLAN）.....133
Voice VLAN（音声 VLAN）.....137
STP（スパニングツリーの設定）.....139
802.1Q-2005 MSTP.....139
802.1D-2004 Rapid Spanning Tree.....139
ポートの状態遷移.....139
STP Global Settings（STP グローバル設定）.....140
STP Port Settings（STP ポートの設定）.....141
MST Configuration Identification（MST の設定）.....142
STP Instance（STP インタンス設定）.....143
MSTP Port Information（MSTP ポート情報）.....143
ERPS (G.8032)（イーサネットリングプロテクション設定）.....144
ERPS 144
ERPS Profile（ERPS プロファイル）.....146
Loopback Detection（ループバック検知設定）.....148
Link Aggregation（リンクアグリゲーション）.....149
ポートトランクグループについて 149
L2 Multicast Control（L2 マルチキャストコントロール）.....152
IGMP Snooping（IGMP スヌーピング）.....152
MLD Snooping Settings（MLD スヌーピング）.....157
Multicast Filtering（マルチキャストフィルタリング）.....162

LLDP（LLDP 設定）.....163
LLDP Global Settings（LLDP グローバル設定）.....163
LLDP Port Settings（LLDP ポート設定）.....164
LLDP Management Address List（LLDP 管理アドレスリスト）.....165
LLDP-MED Port Settings（LLDP-MED ポート設定）.....167
LLDP Statistics Information（LLDP 統計情報）.....168
LLDP Local Port Information（LLDP ローカルポート情報）.....168
LLDP Neighbor Port Information（LLDP ネイバポート情報）.....170

第 9 章　L3 Features（レイヤ 3 機能）　171

ARP（ARP 設定）.....171
ARP Aging Time（ARP エージングタイム設定）.....171
Static ARP（スタティック ARP 設定）.....172
Proxy ARP（プロキシ ARP 設定）.....172
ARP Table（ARP テーブル）.....173
Gratuitous ARP（Gratuitous ARP 設定）.....173
UDP Helper（UDP ヘルパー）.....174
IP Forward Protocol（IP 転送プロトコル）.....174
IP Helper Address（IP ヘルパーアドレス）.....174
IPv4 Interface（IPv4 インタフェース）.....175
IPv4 Static/Default Route（IPv4 スタティック / デフォルトルート）.....176
IPv4 Route Table（IPv4 ルートテーブル）.....177
IPv6 Interface（IPv6 インタフェース）.....177
IPv6 Neighbor（IPv6 Neighbor 設定）.....179
IPv6 Static/Default Route（IPv6 スタティック / デフォルトルート）.....180
IPv6 Route Table（IPv6 ルートテーブル）.....180
IPMC（IPMC 設定）.....181
IP Multicast Global Settings（IP マルチキャストグローバル設定）.....181
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）.....181

第 10 章　QoS（QoS 機能の設定）　182

Basic Settings（基本設定）.....182
Port Default CoS（ポートデフォルト CoS 設定）.....182
Port Scheduler Method（ポートスケジューラーメソッド設定）.....183
Queue Settings（QoS 設定）.....184
CoS to Queue Mapping（CoS キューマッピング設定）.....184
Port Rate Limiting（ポートレート制限設定）.....185
Queue Rate Limiting（キューレート制限設定）.....186
Advanced Settings（アドバンス設定）.....187
DSCP Mutation Map（DSCP 変更マップ設定）.....187
Port Trust State and Mutation Binding（ポートトラスト設定）.....187
DSCP CoS Mapping（DSCP CoS マップ設定）.....188
CoS Color Mapping（CoS カラーマップ設定）.....188
DSCP Color Mapping（DSCP カラーマップ設定）.....189
Class Map（クラスマップ設定）.....189
Aggregate Policer（アグリゲートポリサー設定）.....190
Policy Map（ポリシーマップ設定）.....192
Policy Binding（ポリシーバインディング設定）.....195

第 11 章　ACL（ACL 機能の設定）　196

ACL Configuration Wizard（ACL 設定ウィザード）.....196
ACL Configuration Wizard（ACL 設定ウィザードの開始）.....196
パケットタイプ選択（ACL 設定ウィザード）.....197
プロトコル設定（ACL 設定ウィザード）.....197
ポート設定（ACL 設定ウィザード）.....221
ACL Access List（ACL アクセスリスト）.....222
Standard IP ACL（通常 IP ACL）.....222
Extended IP ACL（拡張 IP ACL）.....225
Standard IPv6 ACL（通常 IPv6 ACL）.....232
Extended IPv6 ACL（拡張 IPv6 ACL）.....235
Extended MAC ACL（拡張 MAC ACL）.....241
Extended Expert ACL（拡張詳細 ACL）.....244
ACL Interface Access Group（ACL インタフェースアクセスグループ）.....252
ACL VLAN Access Map（ACL VLAN アクセスマップ）.....252
Match Access-List（合致するアクセスリスト設定）.....253
ACL VLAN Filter（ACL VLAN フィルタ設定）.....253

第 12 章　Security（セキュリティ機能の設定）　254

Port Security（ポートセキュリティ）....255
Port Security Global Settings（ポートセキュリティグローバル設定）....255
Port Security Port Settings（ポートセキュリティポート設定）....256
Port Security Address Entries（ポートセキュリティアドレスエントリ設定）....257
802.1X（802.1X 認証設定）....258
802.1X Global Settings（802.1X グローバル設定）....262
802.1X Port Settings（802.1X ポート設定）....262
Authentication Session Information（オーセンティケーションセッションの状態）....263
Authenticator Statistics（オーセンティケータ統計情報）....263
Authenticator Session Statistics（オーセンティケータセッション統計情報）....264
Authenticator Diagnostics（オーセンティケータ診断）....264
AAA（AAA 設定）....265
AAA Global Settings（AAA グローバル設定）....265
Application Authentication Settings（アプリケーションの認証設定）....265
Application Accounting Settings（アプリケーションアカウント設定）....266
Authentication Settings（認証設定）....266
Accounting Settings（アカウンティング設定）....268
Server RADIUS Dynamic Author Settings（サーバ RADIUS Dynamic Author 設定）....268
RADIUS（RADIUS 設定）....269
RADIUS Global Settings（RADIUS グローバル設定）....269
RADIUS Server Settings（RADIUS サーバの設定）....270
RADIUS Group Server Settings（RADIUS グループサーバの設定）....271
RADIUS Statistic（RADIUS 統計情報）....272
TACACS+（TACACS+ 設定）....273
TACACS+ Global Settings（TACACS+ グローバル設定）....273
TACACS+ Server Settings（TACACS+ サーバの設定）....273
TACACS+ Group Server Settings（TACACS+ グループサーバの設定）....274
TACACS+ Statistic（TACACS+ 統計情報）....274
IMPB（IP-MAC-Port Binding / IP-MAC- ポートバインディング）....275
IPv4....275
IPv6....285
DHCP Server Screening（DHCP サーバスクリーニング設定）....289
DHCP Server Screening Global Settings（DHCP サーバスクリーニンググローバル設定）....289
DHCP Server Screening Port Settings（DHCP サーバスクリーニングポート設定）....290
ARP Spoofing Prevention（ARP スプーフィング防止設定）....291
BPDU Attack Protection（BPDU アタック防止設定）....292
MAC Authentication（MAC 認証）....293
Web-based Access Control（Web 認証）....294
Web Authentication（Web 認証設定）....296
WAC Port Settings（Web 認証ポート設定）....296
WAC Customize Page（WAC カスタマイズページ設定）....297
Japanese Web-based Access Control（JWAC 設定）....298
JWAC Global Settings（JWAC グローバル設定）....298
JWAC Port Settings（JWAC ポート設定）....299
JWAC Customize Page Language（JWAC カスタムページ言語設定）....300
JWAC Customize Page（JWAC 画面のカスタマイズ）....300
Network Access Authentication（ネットワークアクセス認証）....302
Guest VLAN（ゲスト VLAN 設定）....302
Network Access Authentication Global Settings（ネットワークアクセス認証グローバル設定）....302
Network Access Authentication Port Settings（ネットワークアクセス認証ポート設定）....303
Network Access Authentication Sessions Information（ネットワークアクセス認証セッション情報）....304
Safeguard Engine（セーフガードエンジン）....305
Safeguard Engine Settings（セーフガードエンジン設定）....306
CPU Protect Counters（CPU プロテクトカウンタ）....306
CPU Protect Sub-Interface（CPU プロテクトサブインタフェース）....307
CPU Protect Type（CPU プロテクトタイプ）....307
Trusted Host（トラストホスト）....308
Traffic Segmentation Settings（トラフィックセグメンテーション設定）....308
Storm Control Settings（ストームコントロール設定）....309
DoS Attack Prevention Settings（DoS 攻撃防止設定）....311
SSH（Secure Shell の設定）....312
SSH Global Settings（SSH グローバル設定）....312
Host Key（Host Key 設定）....313
SSH Server Connection（SSH サーバ接続）....313
SSH User Settings（SSH ユーザ設定）....314

SSL（Secure Socket Layer）.....315
SSL Global Settings（SSL グローバル設定）.....316
Crypto PKI Trustpoint（暗号 PKI トラストポイント）.....317
SSL Service Policy（SSL サービスポリシー）.....317
Network Protocol Port Protection Settings（ネットワークプロトコルポート保護設定）.....318

第 13 章　OAM（Operations, Administration, Maintenance：運用・管理・保守）　319

Cable Diagnostics（ケーブル診断機能）.....319
DDM（DDM 設定）.....320
DDM Settings（DDM 設定）.....320
DDM Temperature Threshold Settings（DDM 温度しきい値設定）.....320
DDM Voltage Threshold Settings（DDM 電圧しきい値設定）.....321
DDM Bias Current Threshold Settings（DDM バイアス電流しきい値設定）.....321
DDM TX Power Threshold Settings（DDM 送信電力しきい値設定）.....322
DDM RX Power Threshold Settings（DDM 受信電力しきい値設定）.....322
DDM Status Table（DDM ステータステーブル）.....323

第 14 章　Monitoring（スイッチのモニタリング）　324

Utilization（利用分析）.....324
Port Utilization（ポート使用率）.....324
Statistics（統計情報）.....325
Port（ポート統計情報）.....325
Port Counters（ポートカウンタ）.....326
Counters（カウンタ）.....327
Mirror Settings（ミラー設定）.....329
sFlow（sFlow 設定）.....330
sFlow Agent Information（sFlow エージェント情報）.....330
sFlow Receiver Settings（sFlow レシーバ設定）.....331
sFlow Sampler Settings（sFlow サンプラ設定）.....331
sFlow Poller Settings（sFlow ポーラ設定）.....332
Device Environment（機器環境確認）.....332

第 15 章　Green（省電力テクノロジー）　333

Power Saving（省電力）.....333
EEE（Energy Efficient Ethernet/ 省電力イーサネット）.....334

第 16 章　Toolbar（ツールバー）　335

Save（保存）.....335
Save Configuration（コンフィグレーションの保存）.....335
Tools（ツール）.....336
Firmware Upgrade & Backup（ファームウェアアップグレード＆バックアップ）.....336
Configuration Restore & Backup（コンフィグレーションリストア＆バックアップ）.....338
Log Backup（ログファイルのバックアップ）.....340
Ping.....341
Trace Route（トレースルート）.....343
Language Management（言語管理）.....344
Reset（リセット）.....344
Reboot System（システム再起動）.....345
Wizard（ウィザード）.....346
Online Help（オンラインヘルプ）.....346
D-Link Support Site（D-Link サポート Web サイト（英語））.....346
User Guide（ユーザガイド（英語版））.....346
Surveillance Mode（サーベイランスモードへの変更）.....346
Logout（ログアウト）.....346

第 17 章　サーベイランスモード　347

Overview（サーベイランスモード概要）.....348
Surveillance Topology（サーベイランストポロジ）.....348
Device Information（デバイス情報）.....351
Port Information（ポート情報）.....352
IP-Camera Information（IP-Camera 情報）.....354
NVR Information（NVR 情報）.....355
PoE Information（PoE 情報）（PoE モデルのみ）.....356
PoE Scheduling（PoE スケジューリング）（PoE モデルのみ）.....357
Management（管理）.....358
File System（ファイルシステム）.....358

Time（時刻設定）.....359
Clock Settings（時刻設定）.....359
SNTP Settings（SNTP 設定）.....359
Surveillance Settings（サーベイランス設定）.....360
Surveillance Log（サーベイランスログ）.....361
Health Diagnostic（正常性診断）.....362
Toolbar（ツールバー）（サーベイランスモード）.....363
Wizard（ウィザード）.....363
Toos（ツール）.....364
Save（保存）.....367
Help（ヘルプ画面）.....367
Online Help（オンラインヘルプ）.....368
Standard Mode（スタンダードモード）.....368
Logout（ログアウト）.....368
【付録 A】ログエントリ 369
【付録 B】トラップログ 381
【付録 C】RADIUS 属性の割り当て指定 388
【付録 D】IETF RADIUS 属性のサポート 391
【付録 E】ERPS 情報 392
【付録 F】ケーブルとコネクタ 393
【付録 G】ケーブル長 393
【付録 H】用語解説 394
【付録 I】機能設定例 396
対象機器について.....396
Traffic Segmentation（トラフィックセグメンテーション）.....396
VLAN.....397
Link Aggregation（リンクアグリゲーション）.....399
Access List（アクセスリスト）.....400
Loopback Detection（LBD）（ループ検知）.....401

はじめに

DGS-1510 シリーズユーザマニュアルは、本スイッチのインストールおよび操作方法を例題と共に記述しています。

- 第 1 章 本製品のご利用にあたって
  - 本スイッチの概要と前面、背面、側面の各パネル、LED 表示について説明します。
- 第 2 章 スイッチの設置
  - システムの基本的な設置方法および電源接続の方法について紹介します。
- 第 3 章 スイッチの接続
  - スイッチをご使用のイーサネットに接続する方法を説明します。
- 第 4 章 スイッチ管理について
  - パスワード設定、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。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 6 章 System（システム設定）
  - デバイス情報の確認、環境設定、ポートの設定、ユーザアカウントの設定、システムログの設定と管理、システム時刻の設定について説明します。
- 第 7 章 Management（スイッチの管理）
  - ユーザアカウント設定、パスワード暗号化、ログイン方法、SNMP 設定、RMON 設定、Telnet/Web 設定、DHCP 設定、DNS 設定、ファイルシステム、スタック、ファームウェア / コンフィグレーション更新設定などについて説明します。
- 第 8 章 L2 Features（レイヤ 2 機能の設定）
  - FDB 設定、VLAN 設定、スパニングツリーの設定、ループバック検知設定、リンクアグリゲーション、L2 マルチキャストコントロール、LLDP 設定など L2 機能について説明します。
- 第 9 章 L3 Features（レイヤ 3 機能）
  - 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、TACACS 設定、IMPB、DHCP サーバスクリーニング設定、ARP スプーフィング防止設定、BPDU アタック防止設定、ネットワークアクセス認証、セーフガードエンジン、トラストホスト、トラフィックセグメンテーション、ストームコントロール、DoS 攻撃防止設定、SSH、SSL、MAC アドレス /WAC/JWAC 認証などのセキュリティの設定について解説します。
- 第 13 章 OAM（Operations, Administration, Maintenance：運用・管理・保守）
  - ケーブル診断機能、DDM 設定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（グリーンテクノロジー）
  - 本スイッチの省電力、EEE について設定、表示します。
- 第 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」「Surveillance 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。
- 第 16 章 Surveillance Mode（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 ログエントリ
  - システムに表示される可能性のある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
  - 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
  - DGS-1510 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: ベンダー固有属性）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 ERPS 情報
  - ハードウェア / ソフトウェアベースの ERPS について説明します。
- 付録 F ケーブルとコネクタ
  - スイッチに使用されるケーブルとコネクタ形状について説明します。
- 付録 G ケーブル長
  - スイッチに使用されるケーブル長の最大値について説明します。
- 付録 H 用語解説
  - 本マニュアルに使用される用語の定義を示します。
- 付録 I 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
DGS-1510-20	A1	DGS-1510-20
DGS-1510-28P	A1	DGS-1510-28P
DGS-1510-28X	A1	DGS-1510-28X
DGS-1510-52X	A2	DGS-1510-52X/A2
DGS-1510-52X	A3	DGS-1510-52X/A3
DGS-1510-28XMP	A1	DGS-1510-28XMP/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
- 前面パネル
- LED 表示
- 背面パネル
- 側面パネル

DGS-1510 シリーズは、既存のスマートスイッチの機能に加え、スタティックルーティングなどのマネージドスイッチのパフォーマンスと信頼性を提供するギガビット L2 ＋スタッカブルスマート Pro スイッチです。10/100/1000BASE-T ポートを 16/24/48 ポート、そしてアップリンク可能な SFP スロットと 10G に対応した SFP+ スロットをそれぞれ 2 つずつ（28X/52X/28XMP は SFP+ スロットを 4 つずつ）搭載、SNMP、Web GUI、CLI などを使用した効率的な管理が可能です。MAC アドレス認証、WEB 認証、Compound 認証、IEEE 802.1X 認証、ARP スプーフィング防止、アクセスコントロールリスト（ACL）機能などにより快適で信頼性の高いネットワーク環境を提供します。さらに、IEEE802.3az に準拠した EEE や、スケジューリングにより LED 消灯やポートシャットダウンなどを行うことができる D-Link Green 省電力機能に対応し、環境への配慮や運用コストの削減をお客様に提供します。また、DGS-1510-28P/28XMP は IEEE 802.3af/at 準拠の PoE 給電機能もサポートしています。

本マニュアルでは、DGS-1510-20、DGS-1510-28P、DGS-1510-28X、DGS-1510-28XMP、および DGS-1510-52X を含む D-Link DGS-1510 シリーズの設置、管理および設定の方法について記述しています。本シリーズは機能設定やハードウェア構成は一部機能を除き同じであるため、本マニュアルの情報をすべての種類にほぼ適用できます。Web による管理画面例は、上に記載したいずれかの機種のものですが、一部機能、ポート数を除き設定内容はほぼ同じです。

スイッチ概要

DGS-1510 シリーズは以下の製品で構成されるギガビット L2 Web スマートスイッチです。

- DGS-1510-20 : 10BASE-T/100BASE-TX/1000BASE-T x 16 ポート、SFP x 2 スロット、10G SFP+ x 2 スロット搭載
- DGS-1510-28P : 10BASE-T/100BASE-TX/1000BASE-T（PoE）x 24 ポート、SFP x 2 スロット、10G SFP+ x 2 スロット搭載
- DGS-1510-28X : 10BASE-T/100BASE-TX/1000BASE-T x 24 ポート、10G SFP+ x 4 スロット搭載
- DGS-1510-52X : 10BASE-T/100BASE-TX/1000BASE-T x 48 ポート、10G SFP+ x 4 スロット搭載
- DGS-1510-28XMP : 10BASE-T/100BASE-TX/1000BASE-T x 24 ポート（PoE）、10G SFP+ x 4 スロット搭載

注意　DGS-1510 シリーズのすべての機種について、区別する必要がある場合を除き、本マニュアル上では単に“スイッチ”あるいは“DGS-1510”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 1000BASE-T ポートと SFP（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、以下のオプションモジュールと共に使用が可能です。

DGS-1510 シリーズスイッチ対応オプションモジュール

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

※ SFP+ スロットでのみ使用可能です。

前面パネル

スイッチの前面パネルには、電源、コンソール、Fan、PoE（28P/28XMP）、スタック ID および各ポートの Link/Act を示す各ポート（SFP スロットを含む）用の LED が配置されています。

DGS-1510-20

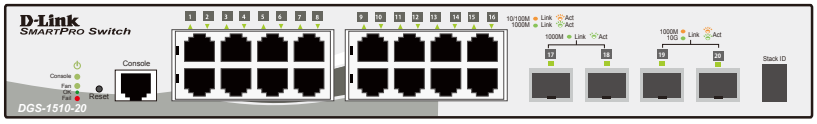


図 1-1　DGS-1510-20 の前面パネル

DGS-1510-28P

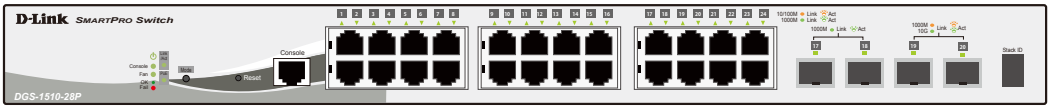


図 1-2　DGS-1510-28P の前面パネル

DGS-1510-28X

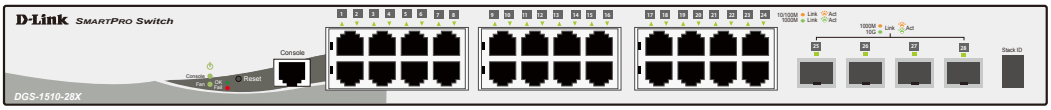


図 1-3　DGS-1510-28X の前面パネル

DGS-1510-52X

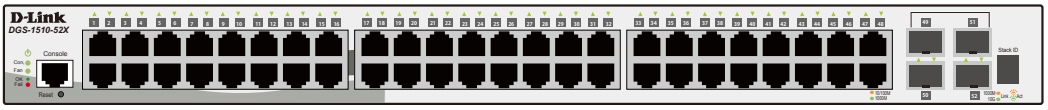


図 1-4　DGS-1510-52X の前面パネル

DGS-1510-28XMP



図 1-5　DGS-1510-28XMP の前面パネル

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。

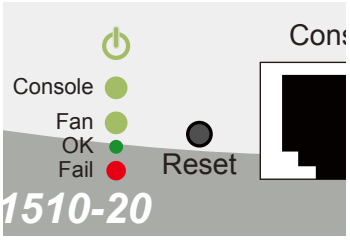


図 1-6　リセットボタン（DGS-1510-20）

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。その際、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。その際、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

スイッチは、Power、Console、ファン、スタック ID、PoE（28P/28XMP）、およびギガビットポートを含む各ポートについての LED をサポートしています。

DGS-1510-20

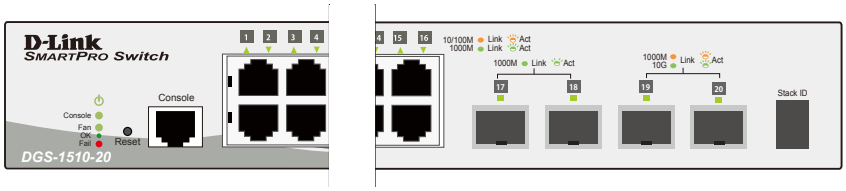


図 1-7　DGS-1510-20 の LED 配置図

DGS-1510-28P

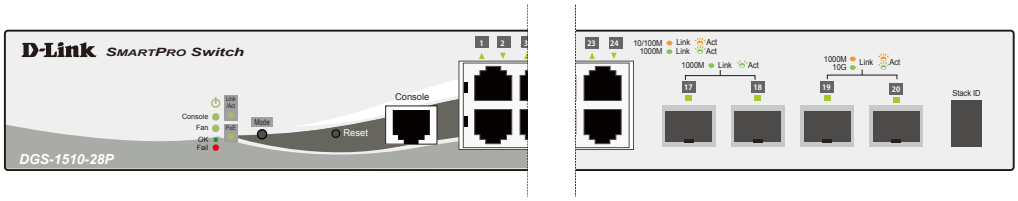


図 1-8　DGS-1510-28P の LED 配置図

DGS-1510-28X



図 1-9　DGS-1510-28X の LED 配置図

DGS-1510-52X

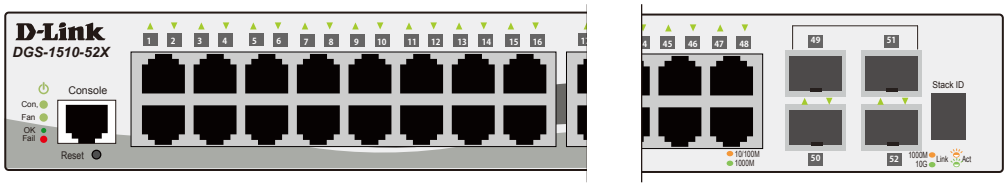


図 1-10　DGS-1510-52X の LED 配置図

DGS-1510-28XMP

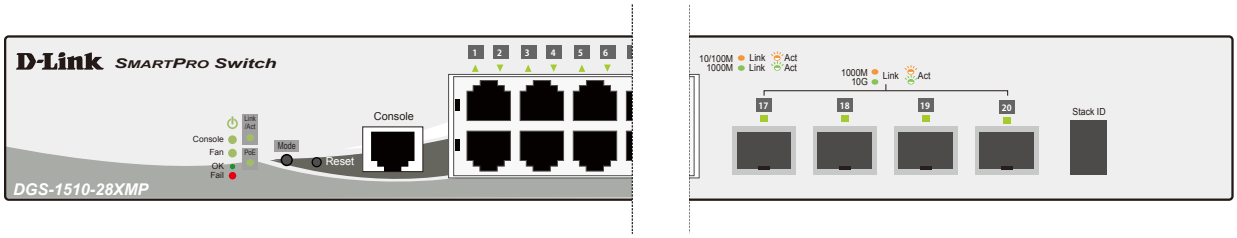


図 1-11　DGS-1510-28XMP の LED 配置図

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。

LED	色	状態	内容
Fan	緑	点灯	診断が終了しファンは正常に動作しています。
	赤	点灯	ファンのいずれかが故障しています。
Stack ID	緑	番号点灯	スタック番号（1-6）が表示されます。 スタック番号（ボックス ID）はユーザ（スタティックモード）またはシステム（自動モード）によりアサインされます。プライマリマスタに指定されると、スタック番号の LED 表示は複数の意味を表示します。まずプライマリマスタを意味する「H」が表示され、その後ボックス ID の数字が表示されます。以後交互に表示されることになります。
		「H」表示	デバイスはスタッキング内マスタとして動作しています。
		「h」表示	デバイスはスタッキング内バックアップマスタとして動作しています。
		「G」表示	セーフガードエンジン機能が「exhausted」モードになっています。
		「E」表示	システムセルフテストでエラーが検出されました。
GE ポート LED			
Link/Act/Speed	緑	点灯	1000Mbps でリンクが確立しています。
		点滅	1000Mbps でデータを送受信しています。
	橙	点灯	10/100Mbps でリンクが確立しています。
		点滅	10/100Mbps でデータを送受信しています。
	ー	消灯	リンクが確立していません。
PoE Mode （DGS-1510-28P/28XMP）	緑	点灯	接続中の PoE 受電機器に給電中です。
	橙	点灯	PoE ポートにエラーが発生しました。
	ー	消灯	給電をしていません。
SFP スロット LED			
Link/ACT	緑	点灯	1000Mbps でリンクが確立しています。
		点滅	1000Mbps でデータを送受信しています。
	ー	消灯	リンクが確立していません。
SFP+ スロット LED			
Link/ACT	緑	点灯	10Gbps でリンクが確立しています。
		点滅	10Gbps でデータを送受信しています。
	橙	点灯	1000Mbps でリンクが確立しています。
		点滅	1000Mbps でデータを送受信しています。
	ー	消灯	リンクが確立していません。

背面パネル

DGS-1510-20

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

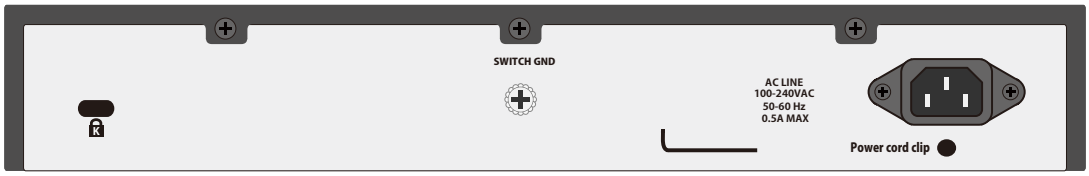


図 1-12　DGS-1510-20 の背面パネル

DGS-1510-28X

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

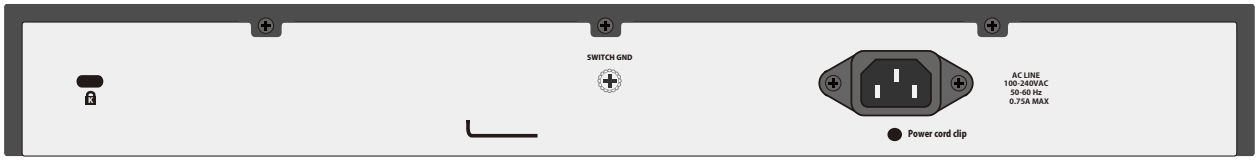


図 1-13　DGS-1510-28X の背面パネル

DGS-1510-52X

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

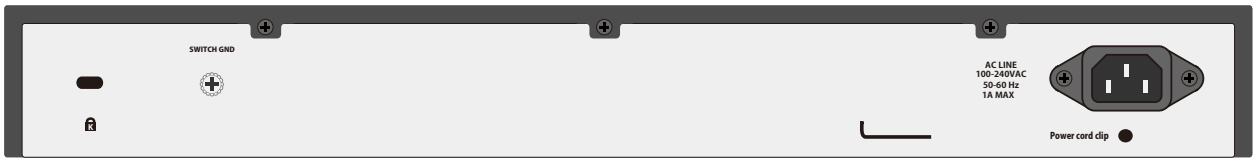


図 1-14　DGS-1510-52X の背面パネル

DGS-1510-28P

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

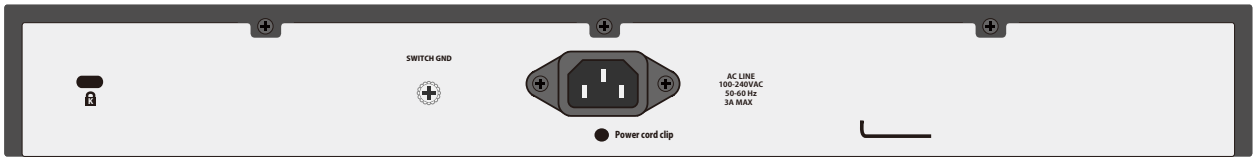


図 1-15　DGS-1510-28P の背面パネル

DGS-1510-28XMP

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

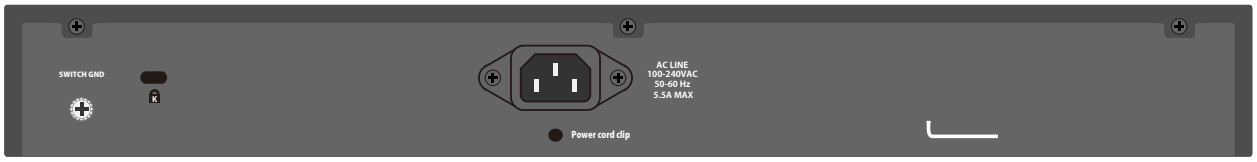


図 1-16　DGS-1510-28XMP の背面パネル

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

側面パネル

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

DGS-1510-20

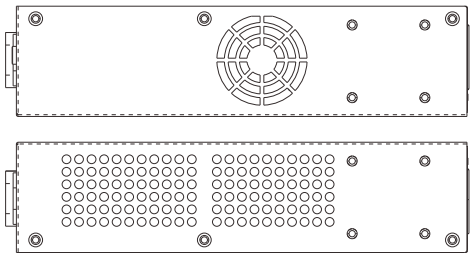


図 1-17　DGS-1510-20 の側面パネル

DGS-1510-28X

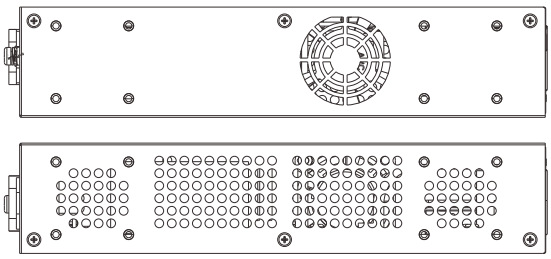


図 1-18　DGS-1510-28X の側面パネル

DGS-1510-28P

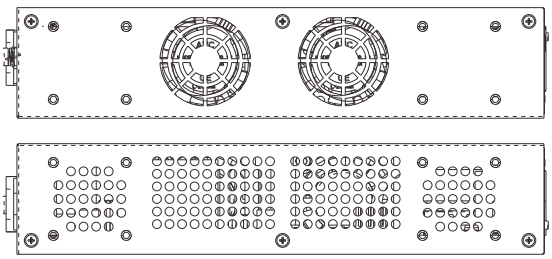


図 1-19　DGS-1510-28P の側面パネル

DGS-1510-28XMP

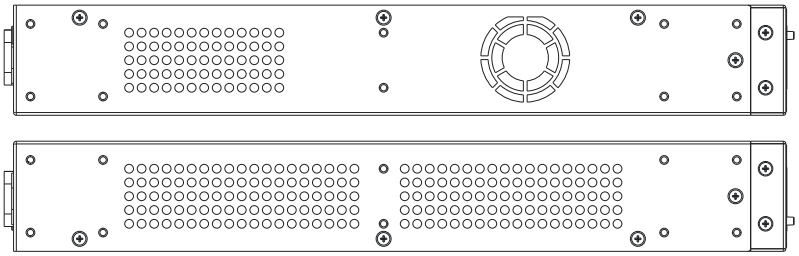


図 1-20　DGS-1510-28XMP の側面パネル

DGS-1510-52X

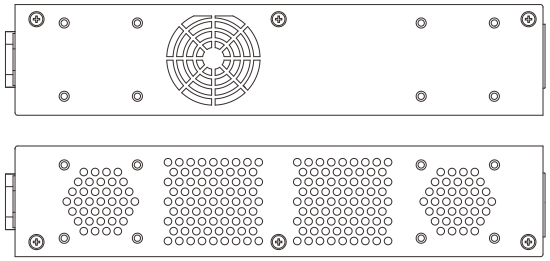


図 1-21　DGS-1510-52X の側面パネル

スマートファンについて

DGS-1510 シリーズスイッチはハードウェアに内蔵されたセンサによってスイッチ内部の温度を検出し、自動的にファンのスピードを調整する「スマートファン」を搭載しています。スピードには「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。

DGS-1510-20
内部温度が 48℃以上になった場合、ファンは「高スピード回転」に移行します。
内部温度が 43 度以下になった場合、ファンは「低スピード回転」に移行します。

DGS-1510-28P
内部温度が 36℃以上になった場合、ファンは「高スピード回転」に移行します。
内部温度が 31℃以下になった場合、ファンは「低スピード回転」に移行します。

DGS-1510-28X
内部温度が 48℃以上になった場合、ファンは「高スピード回転」に移行します。
内部温度が 43℃以下になった場合、ファンは「低スピード回転」に移行します。

DGS-1510-52X
内部温度が 34.7℃以上になった場合、ファンは「中スピード回転」に移行します。
内部温度が 44.7℃以上になった場合、ファンは「高スピード回転」に移行します。
内部温度が 39.7℃以下になった場合、ファンは「中スピード回転」に移行します。
内部温度が 29.7℃以下になった場合、ファンは「低スピード回転」に移行します。

DGS-1510-28XMP
内部温度が 36℃以上になった場合、ファンは「高スピード回転」に移行します。
内部温度が 31℃以下になった場合、ファンは「低スピード回転」に移行します。

第 2 章　スイッチの設置

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

パッケージの内容

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

- 本体　x　1
- 電源ケーブル　x　1
- 19 インチラックマウントキット 1 式
- ゴム足（貼り付けタイプ）　x　4
- RJ-45/RS-232C コンソールケーブル　x　1
- 電源抜け防止クリップ　x　1
- クイックインストールガイド
- CD-ROM　x　1
- PL シート　x　1
- シリアルラベル　x　1

ネットワーク接続前の準備

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

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

ゴム足の取り付け（19 インチラックに設置しない場合）

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

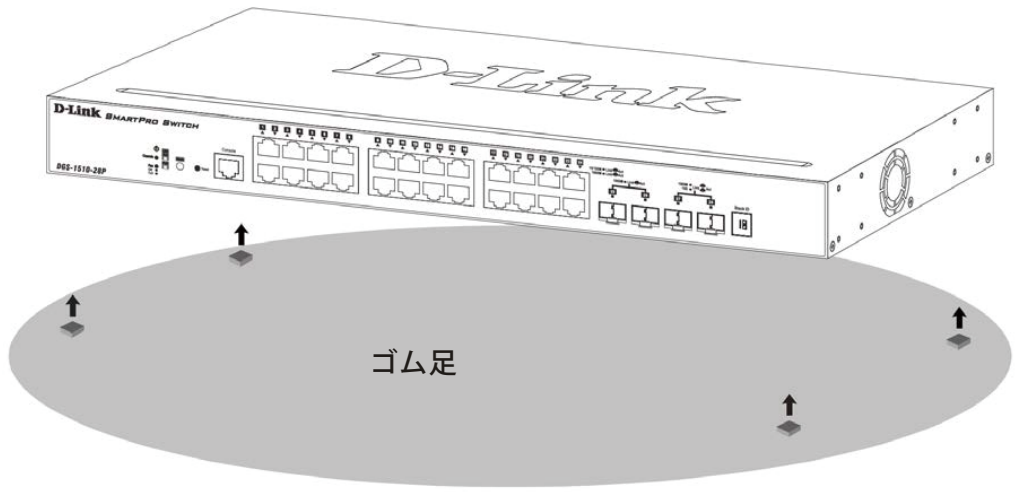


図 2-1　　机や棚の上に設置する場合の準備（DGS-1510-28P）

19 インチラックへの取り付け

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

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

以下の手順に従って本スイッチを標準の 19 インチラックに設置します。

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

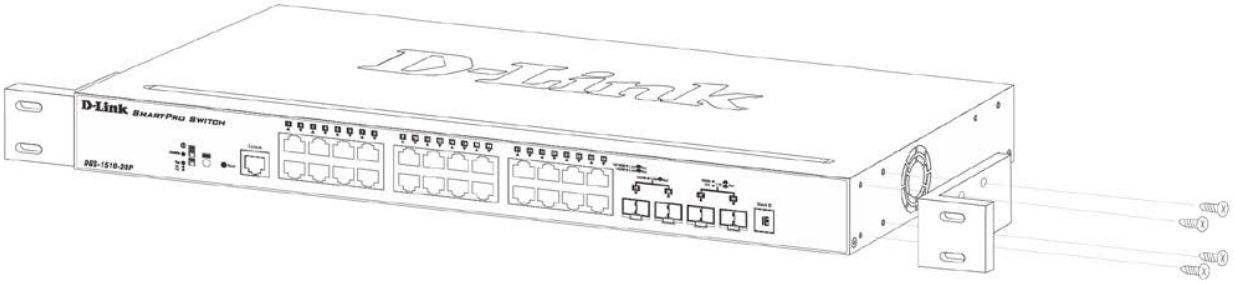


図 2-2　ブラケットの取り付け

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

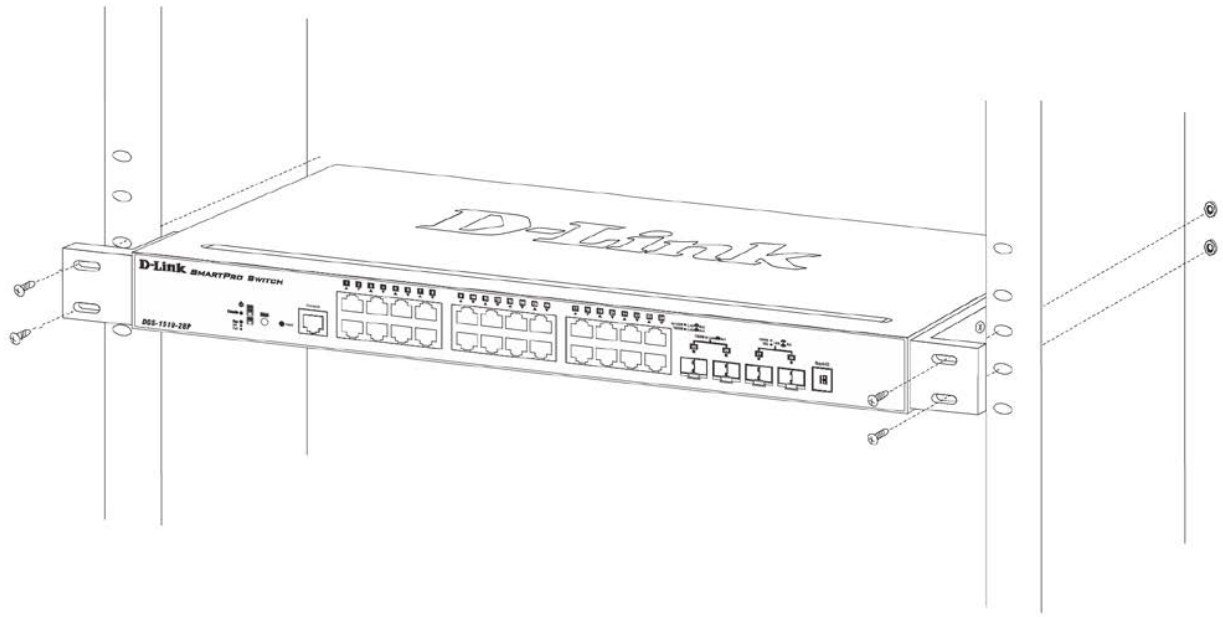


図 2-3　19 インチラックへの設置

SFP スロットの設置

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

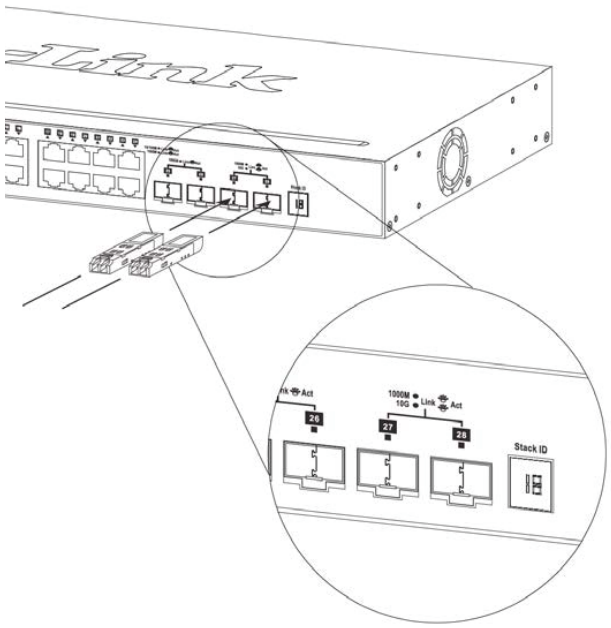


図 2-4　SFP ポートにモジュールを挿入

電源抜け防止クリップの装着

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

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

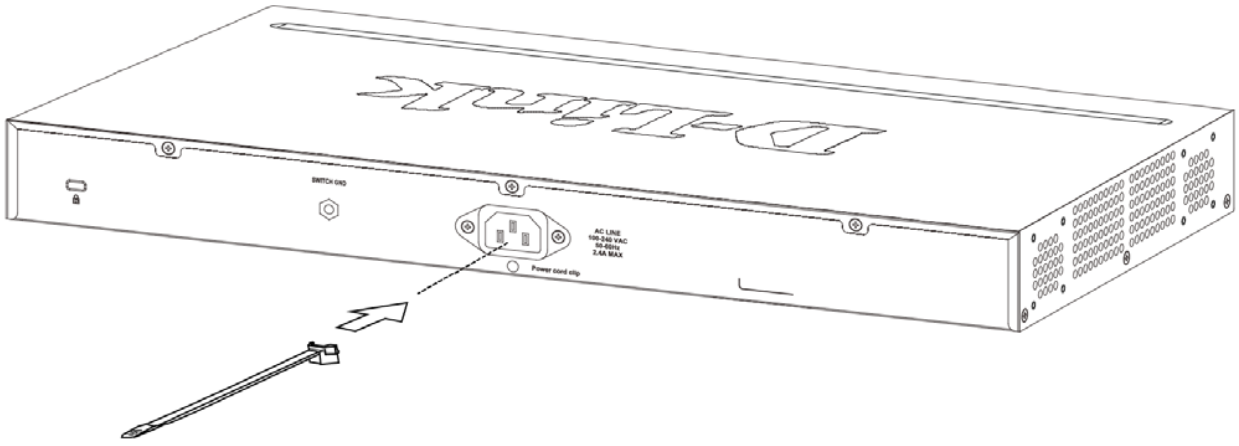


図 2-5　　タイラップの挿し込み

2. AC 電源コードをスイッチの電源プラグに挿し込みます。

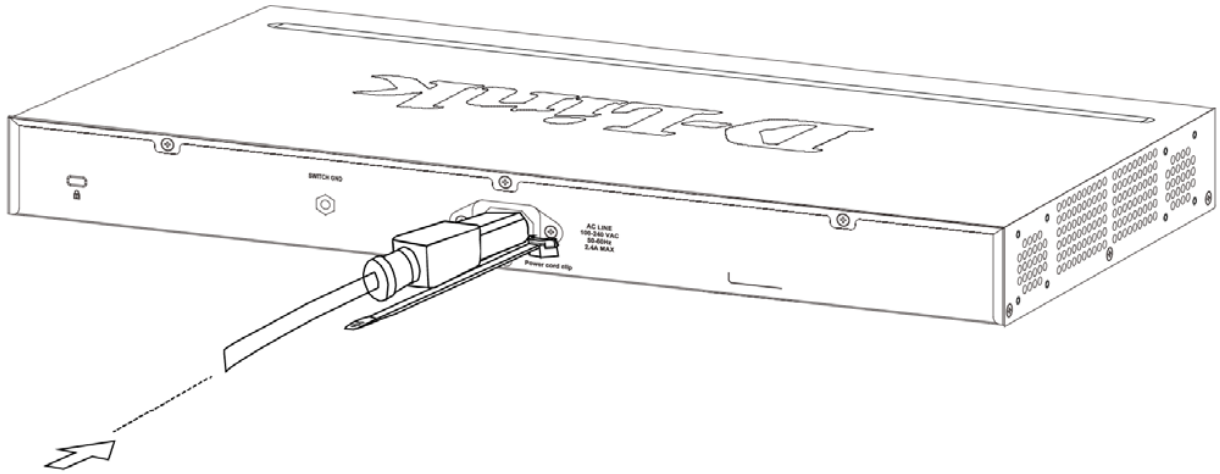


図 2-6　電源コード挿し込み

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

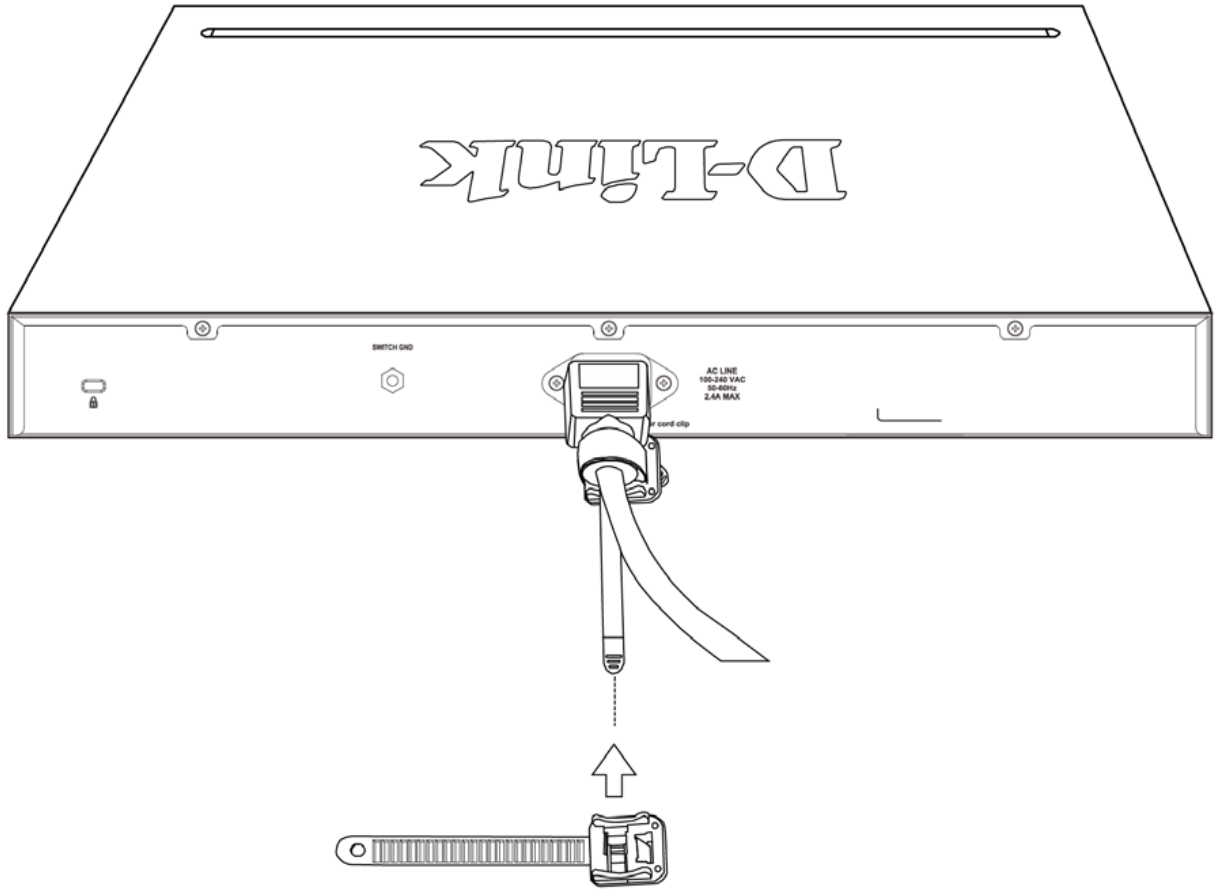


図 2-7　リテイナー（固定具）のスライド

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

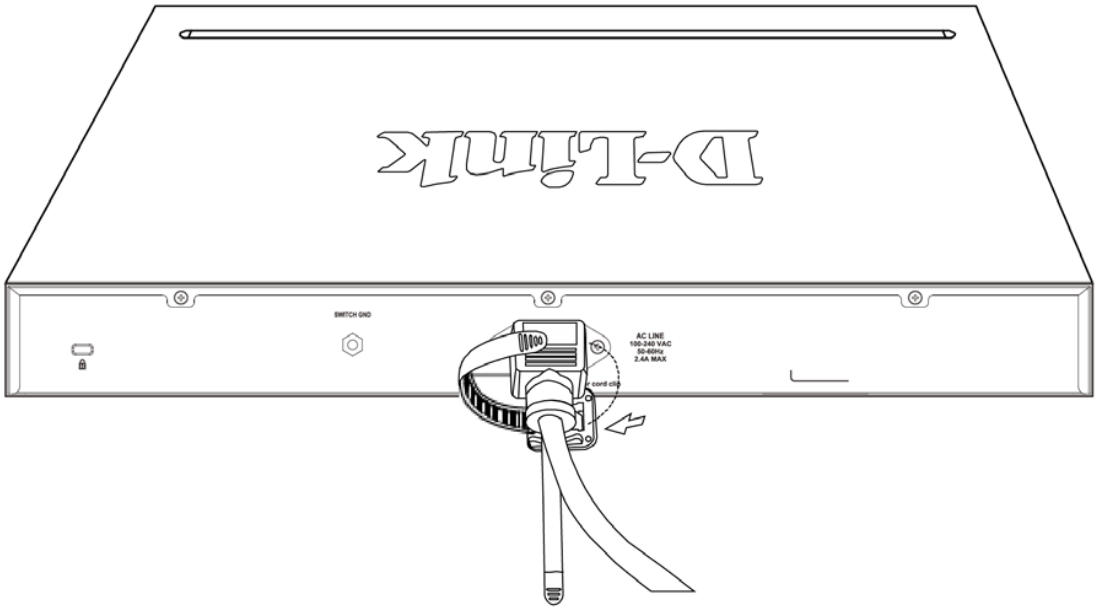


図 2-8　リテイナーの巻き付け、固定

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

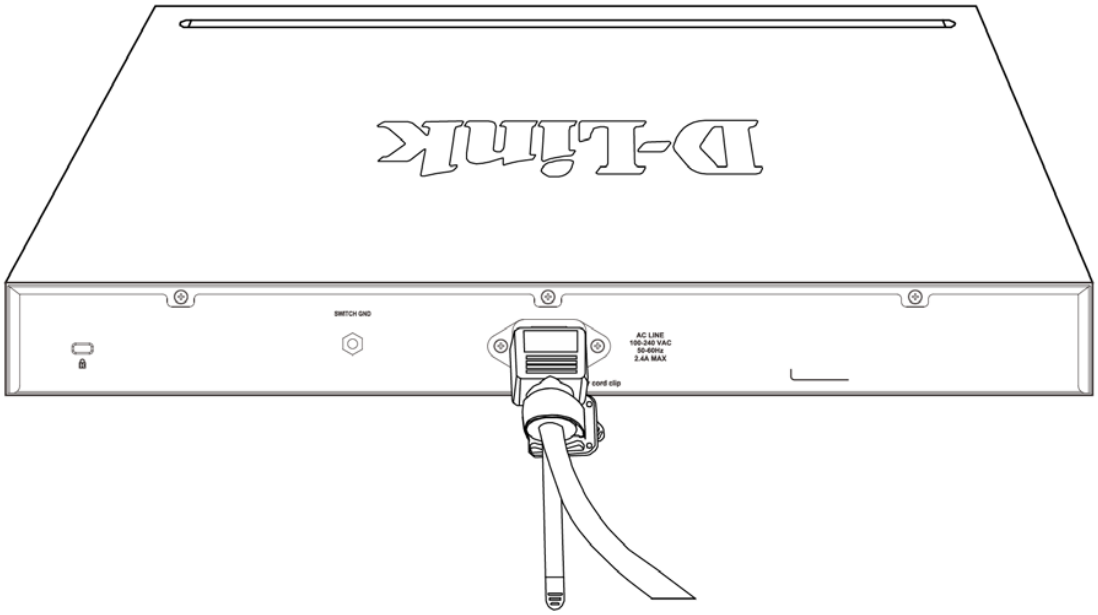


図 2-9　電源抜け防止クリップの固定確認

電源の投入

1. 電源ケーブルを本スイッチの電源コネクタに接続します。電源ケーブルのプラグを電源コンセントに接続します。

2. 本スイッチに電源が供給されると、Power LED が緑色に点灯します。

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。

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

第 3 章　スイッチの接続

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

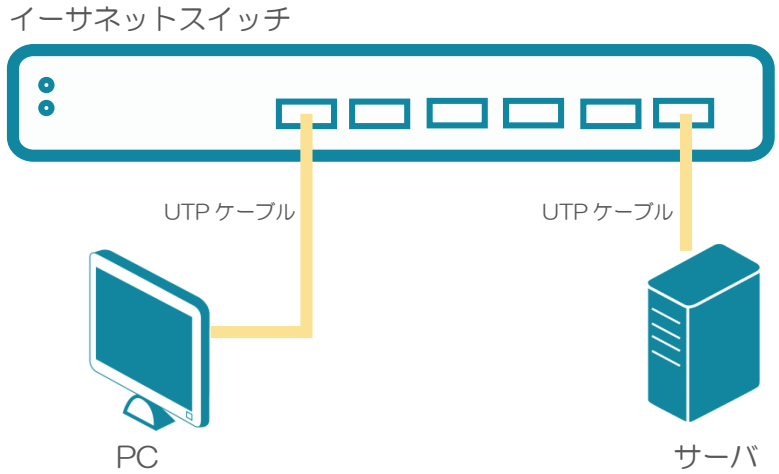


図 3-1　エンドノードと接続したスイッチ

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

ハブまたはスイッチと接続する

使用するケーブルによって以下のように接続します。

- カテゴリ 3 以上の UTP ケーブル：10BASE-T ハブまたはスイッチと接続する。
- カテゴリ 5 以上の UTP ケーブル：100BASE-TX ハブまたはスイッチと接続する。
- エンハンスドカテゴリ 5 以上の UTP ケーブル：1000BASE-T スイッチと接続する。

ケーブル仕様については「【付録 F】ケーブルとコネクタ」（393 ページ）を参照してください。

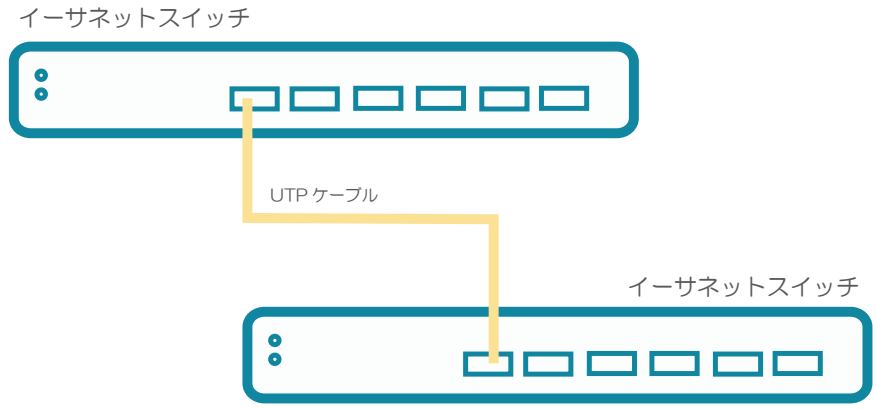


図 3-2　ストレート、クロスケーブルでハブまたはスイッチと接続する

バックボーンまたはサーバと接続する

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

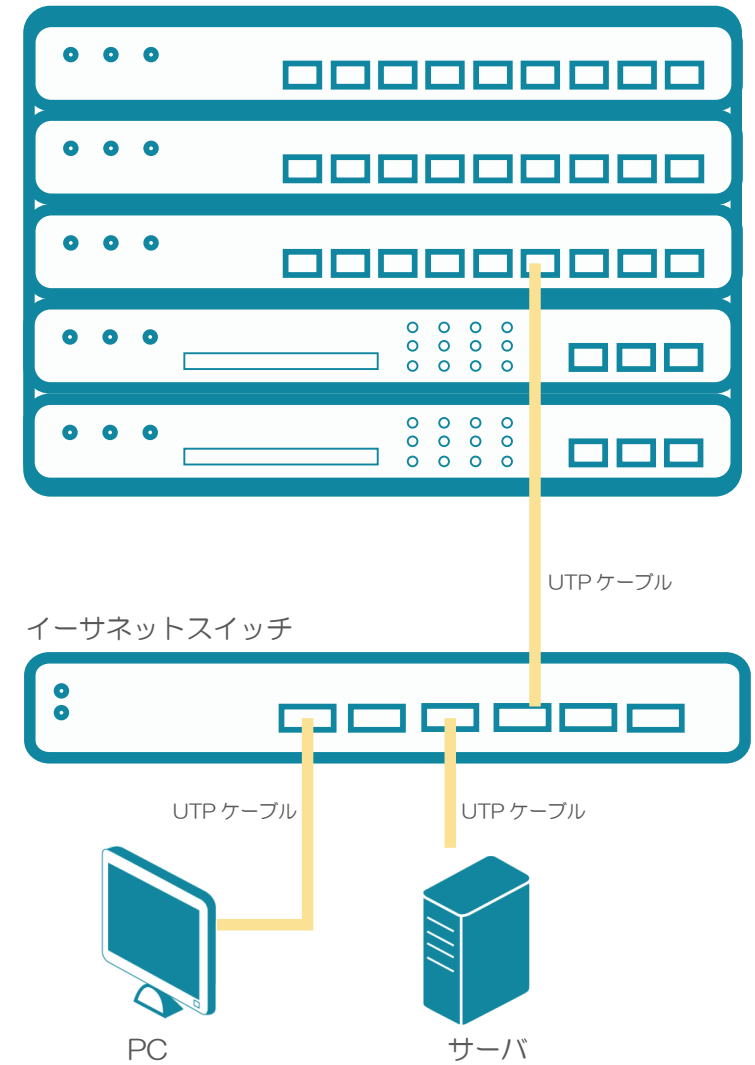


図 3-3　サーバ、PC、スイッチスタックとのアップリンク接続図

第 4 章　スイッチ管理について

- 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
- SNMP 設定

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 9 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 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」

ログインとログアウト

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

注意　パスワードの大文字と小文字は区別されます。

4. コマンドを入力し、必要な設定を行います。

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

ユーザアカウント / パスワードの設定

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

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

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

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

注意 パスワードの大文字と小文字は区別されます。
ユーザ名とパスワードは 15 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-configuration start-up-configuration」コマンドを使用して実行中の設定ファイルをスタート時の設定ファイルとしてコピーする必要があります。詳しくは「DGS-1510_CLI マニュアル」を参照ください。

IP アドレスの設定

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

- IP アドレスの初期値：10.90.90.90/8

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

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

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 v1.0、v2c、および v3.0 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。

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。

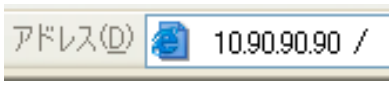


図 5-1　URL の入力

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

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

4. スマートウィザード画面が表示されます。

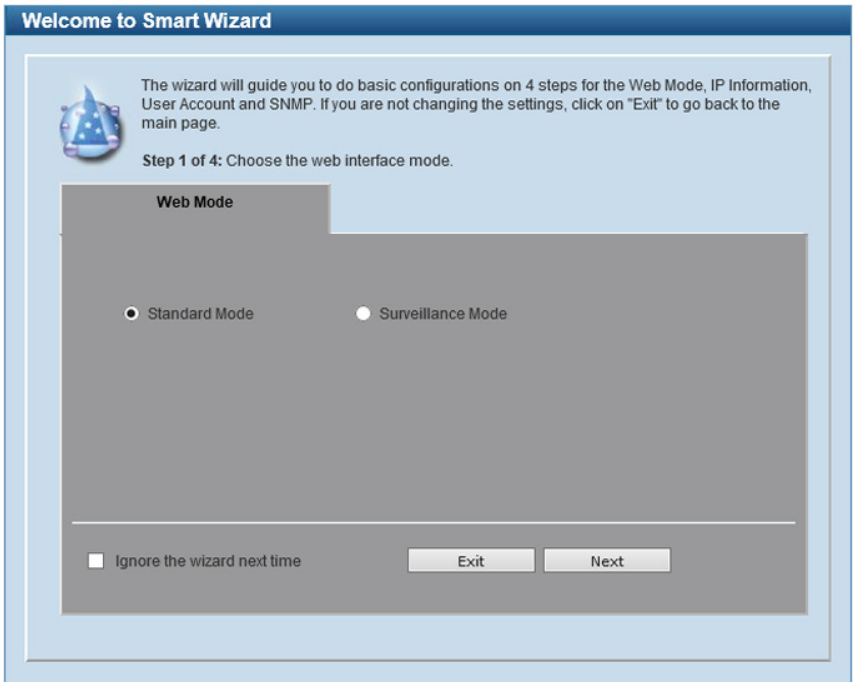


図 5-3　Smart Wizard 画面

ウィザード画面では、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。

注意　Smart Wizard では、IPv4 アドレスのみ設定可能です。

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

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

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 UI 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「Standard Mode（スタンダードモード）」と「Surveillance Mode（サーベイランスモード）」から選択します。

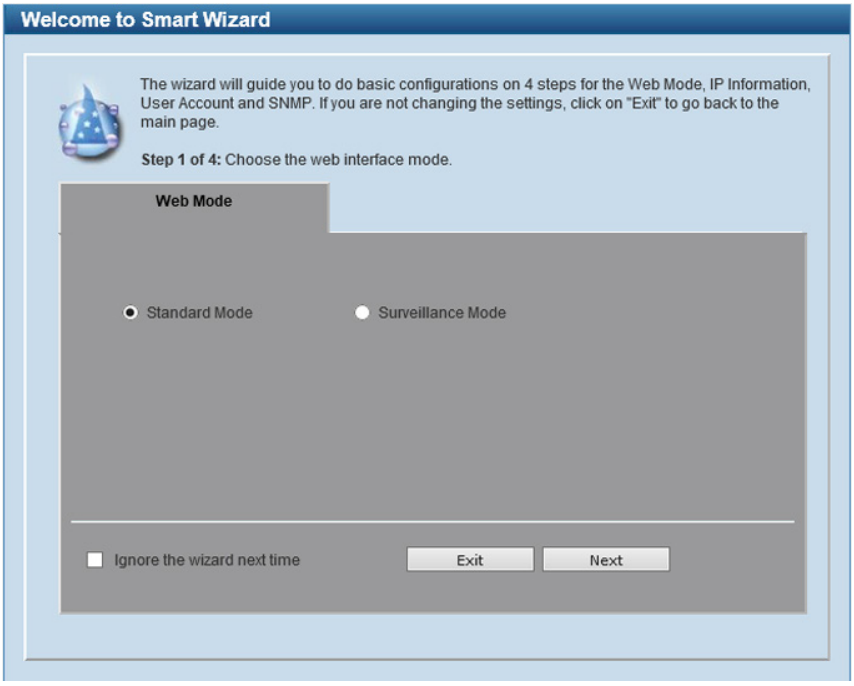


図 5-4　Web モード選択

1. 「Standard Mode（スタンダードモード）」と「Surveillance Mode（サーベイランスモード）」のいずれかをクリックします。
2. 「Next」をクリックします。

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

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

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

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

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 WebUI 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。

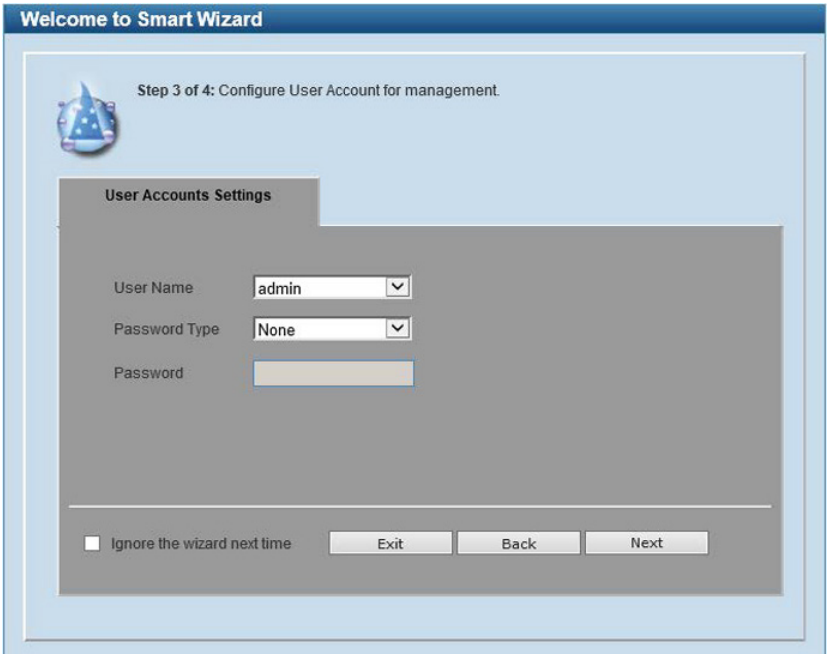


図 5-6　ユーザアカウント設定画面

以下の項目が表示されます。

項目	説明
User Name	ユーザアカウントに使用するユーザ名を入力します。
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。「暗号化フォーマット」へ暗号化することができないことを意味します。 • Encrypted-SHA1 -「SHA-1」でパスワードを指定します。「SHA-1」方式の暗号化パスワードになります。 • Encrypted-MD5 -「MD5」でパスワードを指定します。「MD5」方式の暗号化パスワードになります。
Password	パスワードの種類で「Plain Text」「Encrypted」をした場合本項目は指定可能になります。ユーザアカウントのパスワードを入力します。

ユーザアカウント設定手順

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

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

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 UI へ戻る場合は、「Exit」ボタンをクリックします。
前のページへ戻る場合は、「Back」ボタンをクリックします。

Web ベースのユーザインタフェース

Web ユーザインタフェースではスイッチの設定、管理画面にアクセスし、パフォーマンス状況やシステム状態をグラフィック表示で参照できます。

ユーザインタフェース内の各エリア（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。

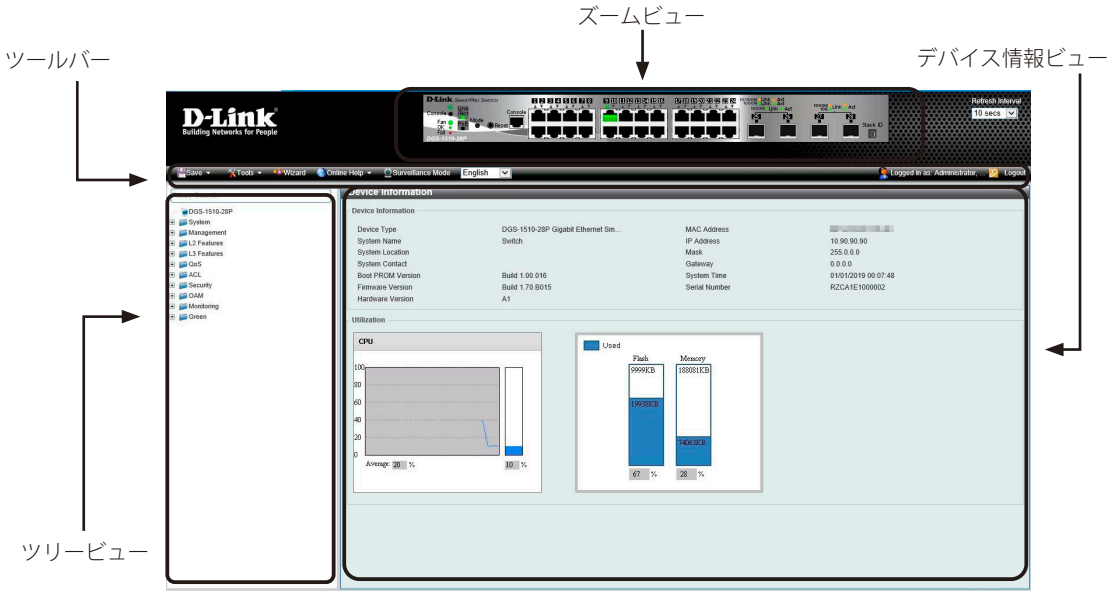


図 5-8　Device Information 画面

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

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

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

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の Web ベースインタフェースの初期画面では以下の情報を参照することができます。

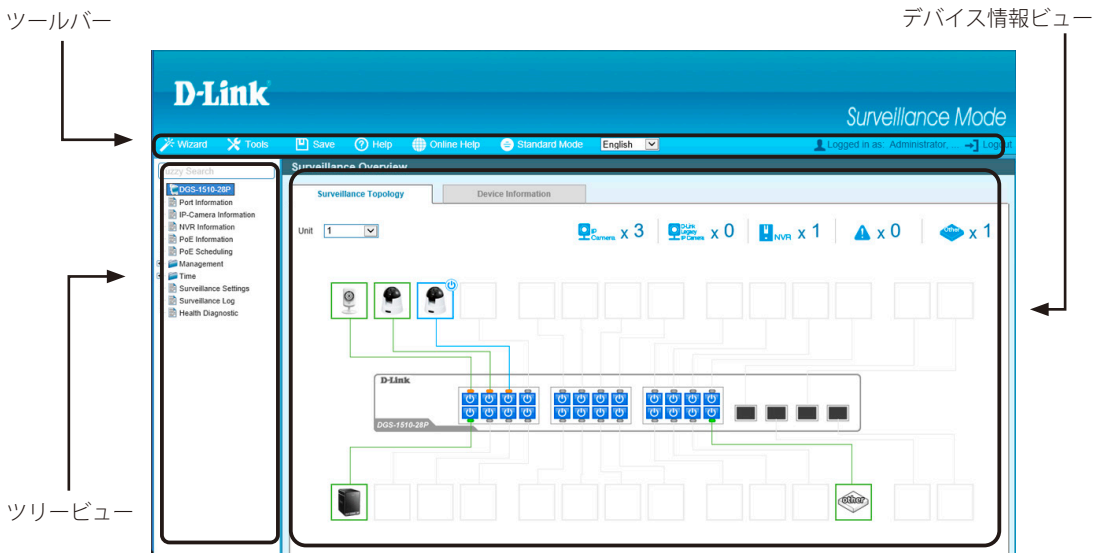


図 5-9　サーベイランスモード初期画面

次の表ではサーベイランスモード初期画面の主要な 3 つの領域について説明します。

ビュー	説明
ツールバー （メニュー情報ビュー）	「Save」、「Tools」メニューや、「Wizard」、「Help」「Online Help」、「Logout」ボタンを提供します。また、言語情報や IP 情報、ログインユーザ名も表示します。「Standard Mode」をクリックするとスタンダードモードへ移行します。
ツリービュー	システムの機能、設定オプションごとに分類して表示します。 表示されているフォルダか画面を選択します。フォルダアイコンを開くことにより、ハイパーリンクメニューボタンやさらにその下のサブフォルダを表示することができます。
デバイス情報ビュー	ツリービューで選択した項目が表示されます。デバイス情報ビューはスイッチの情報、テーブル、設定について表示します。

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。
	PoE	PoE システムの設定を行います。（DGS-1510-28P/28XMP）
	System Log	スイッチのシステムログ設定を行います。
	Time and SNTP	スイッチの時間設定を行います。
	Time Range	スイッチのタイムレンジを設定します。
Management	User Accounts Settings	ユーザアカウントの作成と設定を行います。有効なユーザアカウントを表示可能です。
	Password Encryption	パスワードの暗号を設定ファイルに保存します。
	Login Method	各管理インタフェースでのログイン方法について表示、設定します。
	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 サーバ /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。
	DNS	スイッチの DNS サービスについて設定します。
	NTP	スイッチが持つ時計の時刻を同期するための通信プロトコルの設定を行います。
	IP Source Interface	IP ソースインタフェースを設定します。
	File System	フラッシュファイルシステムを設定します。
	Physical Stacking	物理スタッキングの設定を行います。
	Virtual Stacking	D-Link シングル IP マネジメントと仮想スタッキングの設定、表示を行います。
	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。
	ERPS (G.8032)	イーサネットリングプロテクション設定を行います。
	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。
	UDP Helper	UDP Helper の設定、編集を行います。
	IPv4 Interface	IPv4 アドレスのインタフェースの設定を行います。
	IPv4 Static/Default Route	IPv4 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 Interface	IPv6 アドレスのインタフェースの設定を行います。
	IPv6 Neighbor	IPv6 ネイバの設定を行います。
	IPv6 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。
	IPMC	IPMC の設定を行います。
QoS	Basic Settings	QoS、CoS キューマッピングなどの設定を行います。
	Advanced Settings	DSCP/CoS のマップ設定などを行います。

メイン メニュー	サブメニュー	説明
ACL	ACL Configuration Wizard	ウィザードを使用してアクセスプロファイルとルールを作成します。
	ACL Access List	ACL アクセスリストの設定をします。
	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。
	ACL VLAN Access Map	ACL VLAN アクセスマップの設定を行います。
	ACL VLAN Filter	ACL VLAN フィルタの設定を行います。
Security	Port Security	ポートセキュリティの設定を行います。
	802.1X	802.1X 認証設定を行います。
	AAA	AAA の設定を行います。
	RADIUS	RADIUS の設定を行います。
	TACACS+	TACACS+ 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。
	BPDU Attack Protection	BPDU アタック防止設定を行います。
	MAC Authentication	MAC 認証の設定を行います。
	Web-based Access Control	Web 認証（WAC）の設定を行います。
	Japanese Web-based Access Control	JWAC 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。
OAM	Cable Diagnostics	ケーブル診断を行います。
	DDM	DDM の設定を行います。
Monitoring	Utilization	CPU 使用率、ポートの帯域使用率を表示します。
	Statistics	パケット統計情報とエラー統計情報を表示します。
	Mirror Settings	ポートミラーリングの設定を行います。
	sFlow	sFlow を設定し、スイッチやルータを経由するネットワークトラフィックをモニタします。
	Device Environment	機器環境の設定、表示を行います。
Green	Power Saving	機器の省電力設定を行います。
	EEE	Energy Efficient Ethernet/ 省電力イーサネットの設定を行います。
Toolbar	Save	コンフィグレーションの保存などを行います。
	Tools	ファームウエアアップグレードやバックアップ、コンフィグレーションのリストア、バックアップなどを行います。
	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	ログアウトします。

第 6 章　System（システム設定）

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

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

サブメニュー	説明
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。（「製品名」をクリック）
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。
PoE（PoE の管理）	PoE システムの設定を行います。
System Log（システムログ構成）	スイッチのログを保存する方法、Syslog サーバの設定を行います。
Time and SNTP（時刻と 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）	アクセスプロファイル機能を実行する期間を決定します。

Device Information（デバイス情報）

ログイン時に自動的に表示されるスイッチの主な機能の設定内容です。他の画面から「Device Information」画面に戻るためには、「製品名」をクリックします。「Device Information」画面にはデバイスの一般的な情報として設定する項目があります。これには、システム名、場所、接続、システム MAC アドレス、システム稼働時間、IP アドレス、ファームウェア、ブート、およびハードウェアのバージョン情報などが含まれます。

ツリービューの製品名（例 : DGS-1510-28P）をクリックし、以下の画面を表示します。

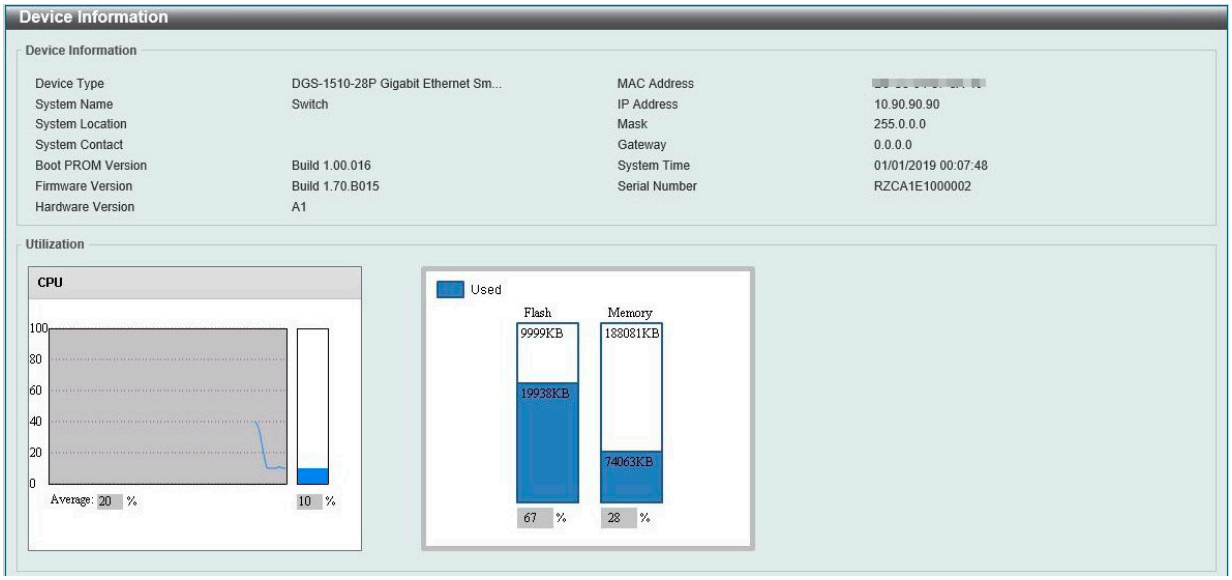


図 6-1　Device Information 画面

「Device Information」画面には以下の項目があります。

項目	説明
Device Information	
Device Type	工場にて定義した機種名と型式を表示します。
System Name	ユーザが定義したシステム名を表示します。
System Location	システムが現在動作している場所を表示します。（半角英数字 255 文字以内）
System Contact	担当者名を表示します。（半角英数字 255 文字以内）
Boot PROM Version	デバイスのブート /PROM バージョンを表示します。
Firmware Version	デバイスのファームウェアバージョンを表示します。
Hardware Version	デバイスのハードウェアバージョンを表示します。
MAC Address	デバイスに割り当てられた MAC アドレスを表示します。
IP Address	デバイスに割り当てられた IP アドレスを表示します。
Mask	デバイスに割り当てられたサブネットマスクを表示します。
Gateway	デバイスに割り当てられたデフォルトゲートウェイを表示します。
System Time	システムの日付を表示します。日 / 月 / 年で表示します。
Serial Number	デバイスのシリアル番号を表示します。

System Information Settings（システム情報）

システム情報を提供します。

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

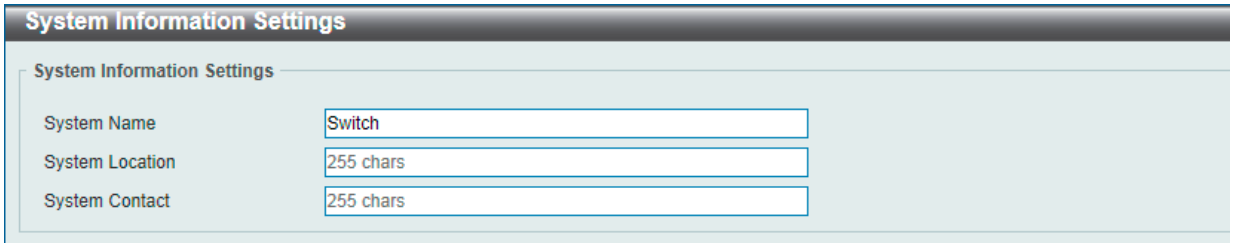


図 6-2　System Information Settings 画面

画面には以下の項目があります。

項目	説明
System Name	ユーザが定義するシステム名を設定します。
System Location	システムが現在動作している場所を定義します。（半角英数字 255 文字以内）
System Contact	担当者名を表示します。（半角英数字 255 文字以内）

「Apply」ボタンをクリックすると設定が更新されます。

注意　System Name の頭文字を数字にすることはできません。

Peripheral Settings（環境設定）

システムの警告温度や環境トラップの設定を行います。

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

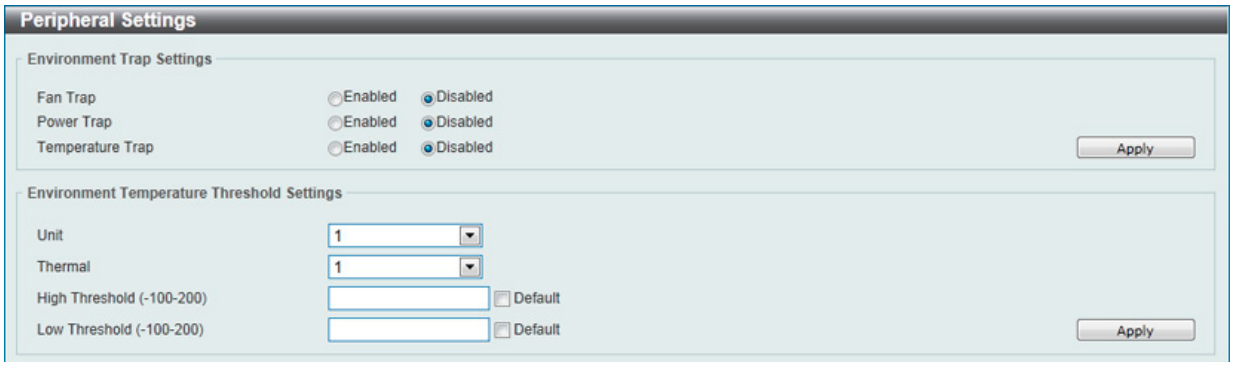


図 6-3　Peripheral Settings 画面

画面には以下の項目があります。

項目	説明
Environment Trap Settings	
Fan Trap	プルダウンメニューを使用して、ファン警告設定のトラップを有効 / 無効に設定します。
Power Trap	プルダウンメニューを使用して、電源警告設定のトラップを有効 / 無効に設定します。
Temperature Trap	プルダウンメニューを使用して、温度警告設定のトラップを有効 / 無効に設定します。
Environment Temperture Threshold Settings	
Unit	本設定を適用するユニットを選択します。
Thermal	温度センサ ID を選択します。
High Threshold	高温警告しきい値を指定します。-100℃から 200℃の間で指定できます。「Default」をチェックすると初期値に戻ります。
Low Threshold	低温警告しきい値を指定します。-100℃から 200℃の間で指定できます。「Default」をチェックすると初期値に戻ります。

「Apply」ボタンをクリックすると設定が更新されます。

Port Configuration（ポート設定）

各ポートの設定を行います。

Port Settings（ポート設定）

デバイスのポートの詳細説明を設定します。

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

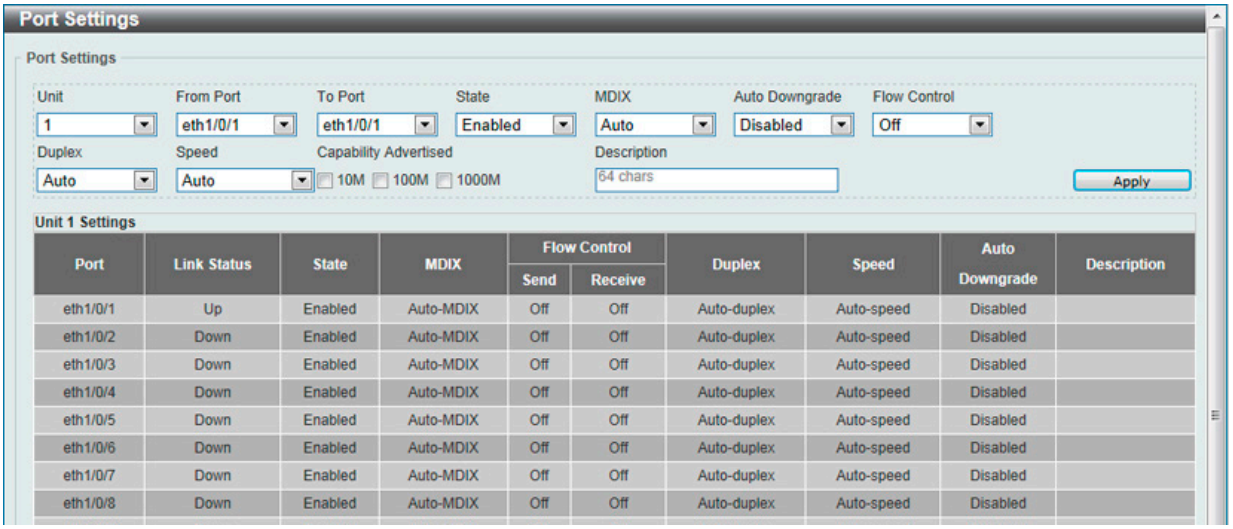


図 6-4　Port Settings 画面

画面には以下の項目があります。

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を設定します。
State	物理ポートの有効 / 無効を指定します。 • Enabled - 選択した物理ポートを有効にします。 • Disabled - 選択した物理ポートを無効にします。
MDIX	MDIX オプションを「Auto」「Normal」「Cross」から選択します。 • Auto - 適したケーブリングタイプを自動的に選択します。 • Normal - このオプションを選択すると、ポートは MDIX になります。PC の NIC に接続する際にはストレートケーブル、別のスイッチに接続する際にはクロスケーブルを使用します。 • Cross - このオプションを選択すると、ポートは MDI になります。別のスイッチ（MDIX モードのスイッチ）と接続する際にはストレートケーブルを使用します。
Auto Downgrade	リンクが有効なスピードを確立できなかった場合、アドバタイズされたスピードでの自動的なダウングレードを有効 / 無効にします。
Flow Control	Full-Duplex では 802.3x フローコントロールを、Half-Duplex ではバックプレッシャーによる制御を自動で行います。「Enabled」（フロー制御あり）または「Disabled」（フロー制御なし）を選択します。「Auto」は自動的にいずれかを使用します。
Duplex	全二重 / 半二重モードの選択を行います。「Auto」「Half」「Full」から選択します。
Speed	「Speed」欄でポートの速度を選択します。ここでは指定したポートを指定した速度のみで接続するように手動で設定します。「Auto」を指定すると、接続相手の状況に合わせて、最適な通信を行うよう自動的に判別します。 オプションには「Auto」「10M」「100M」「1000M」「1000M Master」「1000M Slave」、および「10G」があります。「Auto」以外のオプションのポート設定は固定となります。 スイッチは 2 つのタイプ（「1000M Master」および「1000M Slave」）のギガビット接続設定ができます。 マスタ設定 (1000M Master) によりポートはデュプレックス、速度および物理レイヤタイプに関連する情報を通知します。さらに接続している物理レイヤ間におけるマスタとスレーブを決定します。この関係は物理レイヤ間の連携のタイミングをコントロールするために必要です。タイミングのコントロールには、ローカルソースによってマスタの物理層に設定されます。スレーブ設定 (1000M Slave) はループタイミングを使用します。マスタから受信したデータストリームによりタイミングを合わせます。一方の接続に「1000M Master」を設定すると、他方の接続は「1000M Slave」とする必要があります。その他の設定では両ポートのリンクダウンを引き起こします。
Capability Advertised	上記「Speed」が「Auto」に設定されている場合、オートネゴシエーションの間、本機能は有効になります。
Description	関連のポートについて 64 文字以内に概要を指定します。

「Apply」ボタンをクリックすると設定が更新されます。

Port Status（ポートステータス）

ポートの状態、設定について表示します。

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

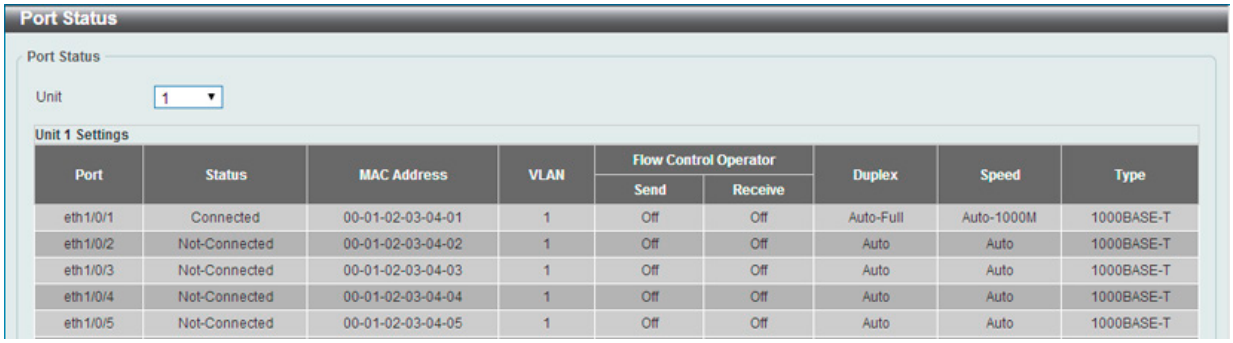


図 6-5　Port Status 画面

以下の項目を使用して設定します。

項目	説明
Unit	表示するユニットを選択します。

Port GBIC（ポート GBIC 情報）

スイッチの各物理ポートの GBIC 情報について表示します。

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

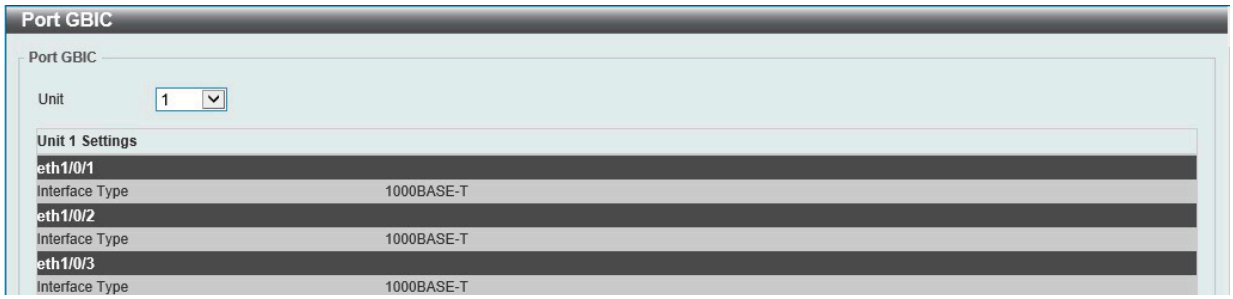


図 6-6　Port GBIC 画面

以下の項目を使用して設定します。

項目	説明
Unit	表示するユニットを選択します。

Port Auto Negotiation（ポートオートネゴシエーション）

ポートオートネゴシエーションの状態、設定について表示します。

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

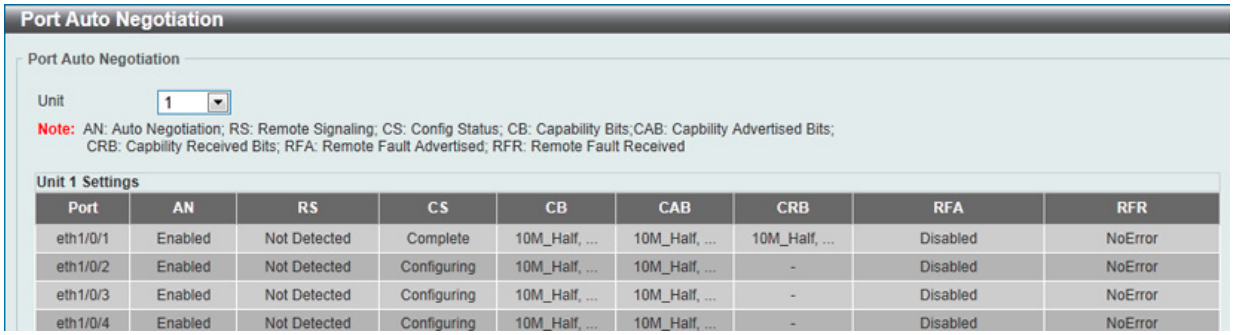


図 6-7　Port Auto Negotiation 画面

以下の項目を使用して設定します。

項目	説明
Unit	表示するユニットを選択します。

Error Disabled Settings（エラーディセーブル設定）

エラーディセーブル発生時の SNMP 通知送信について設定します。

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

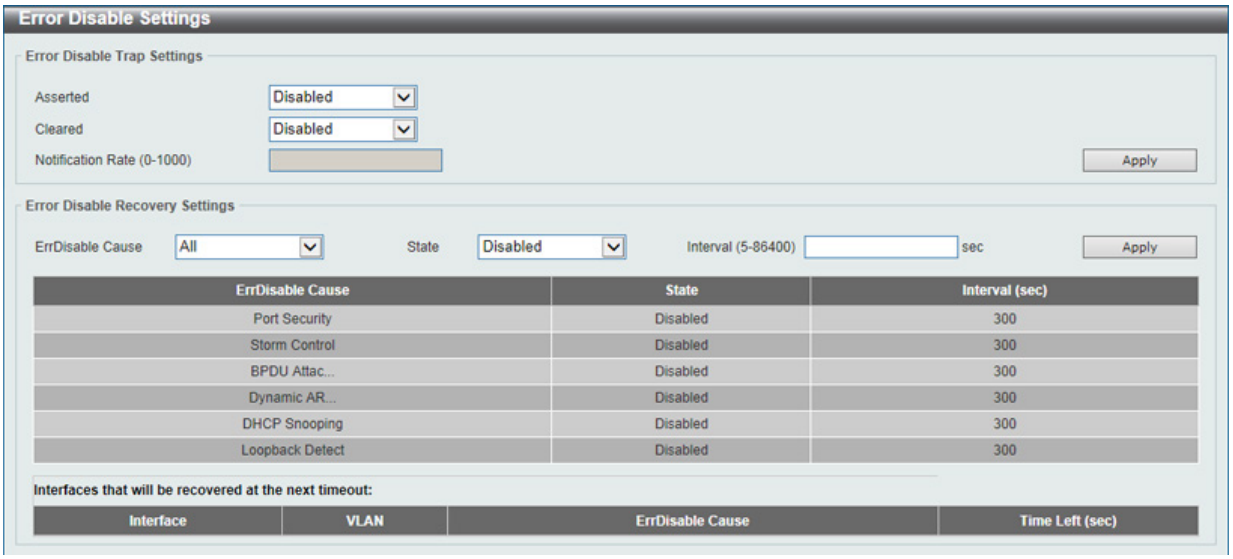


図 6-8　Error Disabled Settings 画面

画面には以下の項目があります。

Error Disable Trap Settings（エラーディセーブルトラップ設定）

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

「Apply」ボタンをクリックすると設定が更新されます。

Error Disable Recovery Settings（エラーディセーブルリカバリ設定）

項目	説明
ErrDisable Cause	エラーディセーブルの原因を次から選択します。 「ALL」「Port Security」「Storm Control」「BPDU Attack Protection」「Dynamic ARP Inspection」「DHCP Snooping」「Loopback Detect」
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	ポートリカバリ実行の間隔時間を 5 から 86400（秒）で指定します。

「Apply」ボタンをクリックすると設定が更新されます。

Jumbo Frame（ジャンボフレーム設定）

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

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

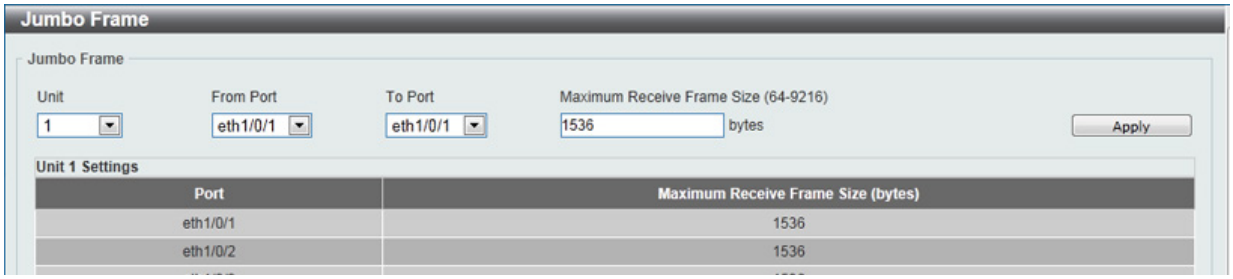


図 6-9　Jumbo Frame 画面

画面には以下の項目があります。

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

「Apply」ボタンをクリックすると設定が更新されます。

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。

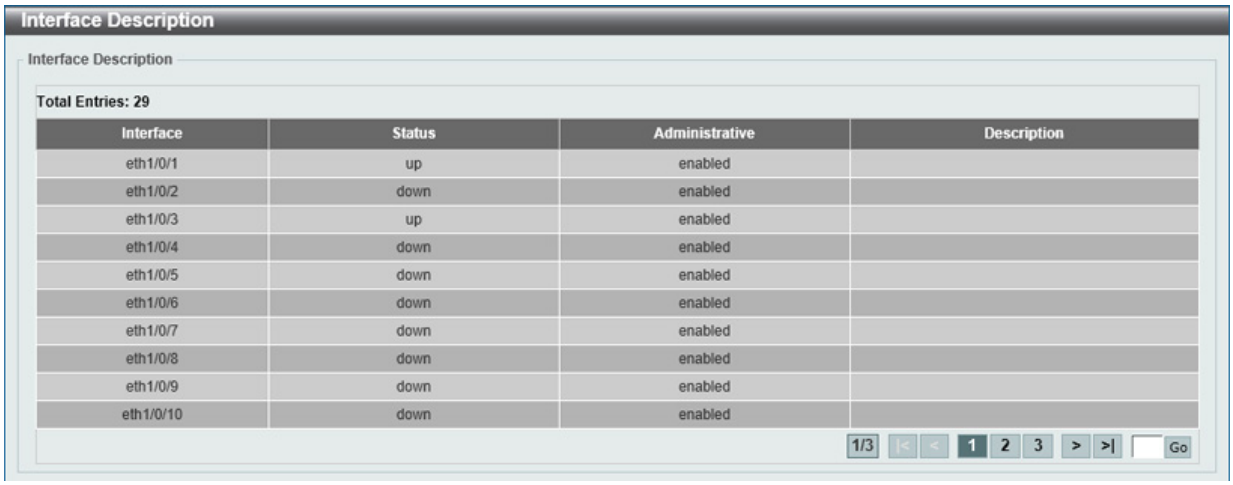


図 6-10　Interface Description 画面

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

PoE（PoE の管理）（DGS-1510-28P/28XMP）

DGS-1510-28P と 28XMP は IEEE の 802.3af と IEEE802.3at 規格の PoE 機能をサポートしています。すべてのポートは 30W まで PoE をサポートしています。ポート 1-24 はカテゴリ 5 以上の UTP イーサネットケーブル経由で PoE 受電機器に約 48VDC 電力を供給できます。本スイッチは PSE pinout Alternative A に準拠しており、電力はピン 1、2、3、および 6 を通じて供給されます。
本スイッチでは次の PoE 機能を使用することができます。

- Auto-discovery 機能は PD(受電機器) に自動的に電力を供給します。
- Auto-disable 機能は次の 2 つの条件が揃うと動作します。消費電力がシステム電源のリミットを超えている場合と各ポートの消費電力リミットを超えている場合です。
- Active circuit 防止機能は電力の不足が生じた場合、自動的にポートを無効にする機能です。他のポートは有効性は変わりません。

802.3af/at 準拠の受電機器の最大受信電力一覧：

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

PSE の最大電力一覧：

クラス	給電機器の最大出力電力
0	16.2W
1	4.2W
2	7.4W
3	16.2W
4	31.6W

PoE System（PoE システム設定）

デバイスの PoE 情報を参照および変更します。

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

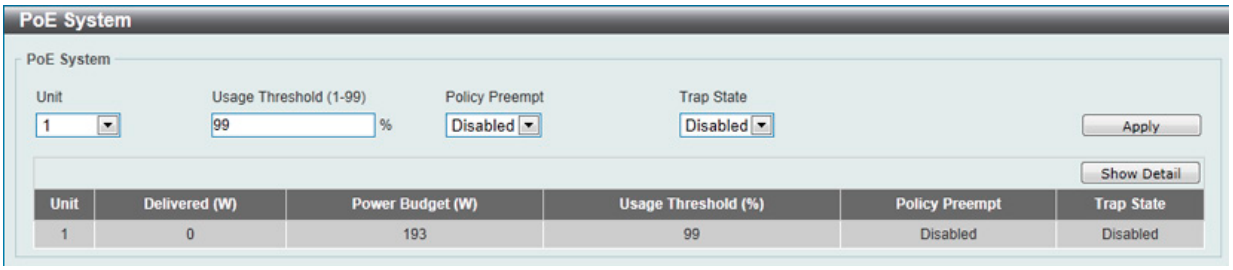


図 6-11　PoE System 画面

画面には以下の項目があります。

項目	説明
Unit	ユニット番号を設定します。全てのユニットを選択する場合は「All」にチェックします。
Usage Threshold	ログの記録や通常の通知送信を実行するしきい値を指定します。1 から 99（%）で指定できます。
Policy Preempt	給電不足のデバイスが発生した場合の給電ポリシーの一時的回避を有効 / 無効に指定します。 有効にすると、電力供給不足となった低優先値のデバイスに、高優先値のデバイスを差し置いて、緊急回避的に給電する機能です。無効だといかなる場合においても給電ポリシーどおりに給電をします。
Trap State	PoE の通知送信について有効 / 無効を指定します。

「Apply」ボタンをクリックすると設定が更新されます。
「Show Detail」ボタンをクリックすると以下の画面が表示されます。



図 6-12　PoE System（Show Detail）画面

PoE Status（PoE ステータス）

各ポートの PoE ステータスの表示と概要の設定を行います。

PoE ポートステータスは次の項目で表示されます。

- Disabled：無効
- Searching：検出中（リモート PD が非接続）
- Requesting：リクエスト中（リモート PD が接続されていますが電源が供給されていません。）
- Delivering：供給中（リモート PD が接続されており電源が供給されています。）
- Faulty：不具合発生（電力信号が消失、PD 短絡、オーバーロード、給電拒否、高温遮断、起動失敗など）

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

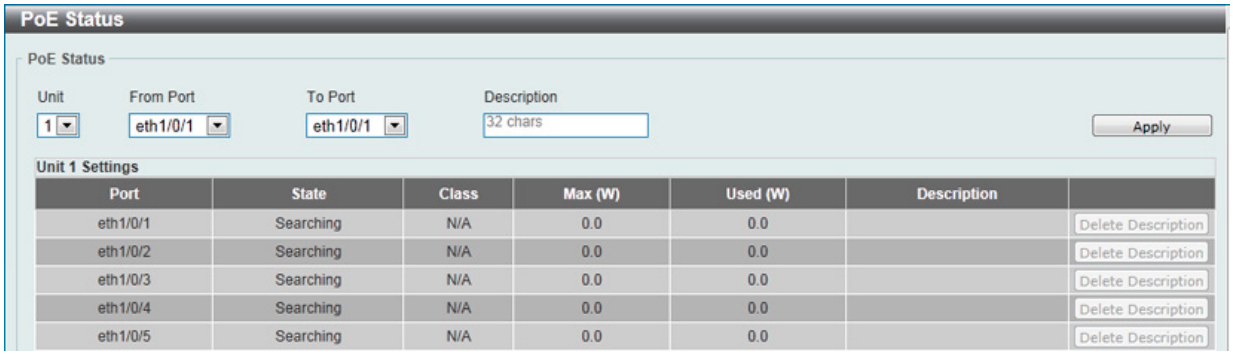


図 6-13　PoE Status 画面

画面には以下の項目があります。

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を設定します。
Description	PoE インタフェースに接続中の PD の概要について入力します。32 文字以内で指定できます。

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

PoE Configuration（PoE ポート設定）

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

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

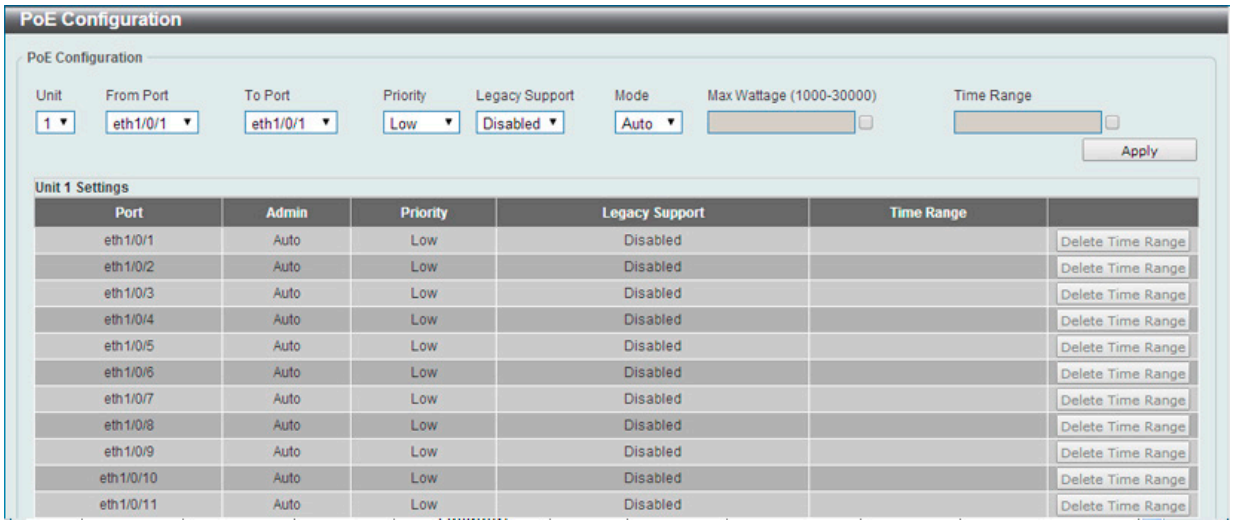


図 6-14　PoE Configuration 画面

画面には以下の項目があります。

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を設定します。

項目	説明
Priority	プルダウンメニューを使ってポートの優先度（Critical、High、Low）を指定します。 ポート優先度はシステムがどのポートに優先的に電力供給を行うかを設定します。優先度には 3 段階あり「Critical」「High」「Low」で設定できます。
Legacy Support	レガシー PD へのサポートの有効 / 無効を指定します。
Mode	PoE ポートの電力管理モードを選択します。「Auto」か「Never」から指定できます。
Max Wattage	上記「Mode」で「Auto」を選択した場合、本オプションが表示されます。 チェックボックスにチェックを入れ、自動検出 PD へ供給する最大電力数（W）を指定します。 数値を指定しない場合は PD のクラスは供給可能な最大の電力で指定されます。「1000 mW」から「30000 mW」までで指定可能です。
Time Range	上記「Mode」で「Auto」を選択した場合、本オプションが表示されます。 ポートの PoE 機能を有効にする時間設定を行います。名称と時間を指定します。ポートは設定した時間内のみ給電を行います。

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

PD Alive（PD アライブ）

PoE ポートに接続した PD についての PD アライブ機能について説明します。PD の状態について「Ping」を使用して確認します。PD が動作していない場合、リセット、通知などを行います。

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

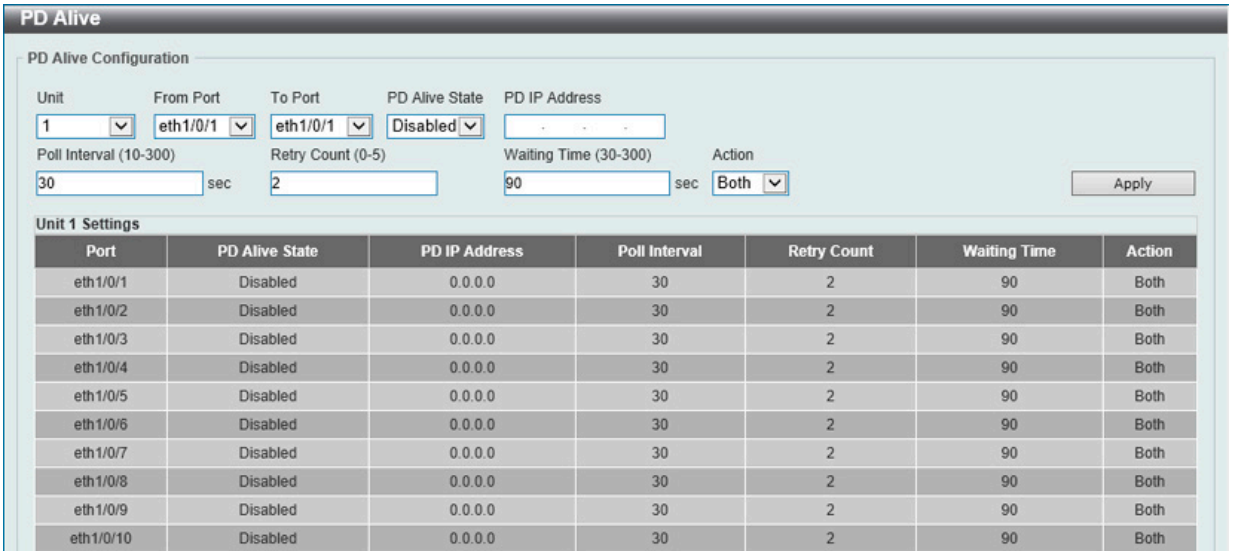


図 6-15　PD Alive 画面

画面には以下の項目があります。

項目	説明
Unit	本設定を適用するユニットを選択します。
From Port/To Port	本設定を適用するポート範囲を設定します。
PD Alive State	指定ポートの PD アライブの有効 / 無効を指定します。
PD IP Address	PD の IP アドレスを指定します。
Poll Interval	ポールインターバルを指定します。システムから PD に「Ping」を送信する間隔を指定します。10-300（秒）になります。
Retry Count	リトライカウントを指定します。PD に無反応の場合に再度「Ping」を送信する回数を指定します。0 から 5 になります。
Waiting Time	待機時間を指定します。リセット後にシステムから PD に「Ping」を送信するまでの待機時間を指定します。30-300（秒）になります。
Action	動作を指定します。「Reset」「Notify」「Both」から指定します。 • Reset - PoE ポートをリセットします。（PoE ポートのオフ / オン） • Notify - 管理者へログとトラップを送信します。 • Both - PoE ポートをリセット（PoE ポートのオフ / オン）し、管理者へログとトラップを送信します。

「Apply」ボタンをクリックすると設定が更新されます。

注意　Time Range を PD Alive と併用した場合、PD Alive は機能しません。

PoE Statistics（PoE 統計）

PoE の統計情報を表示します。

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

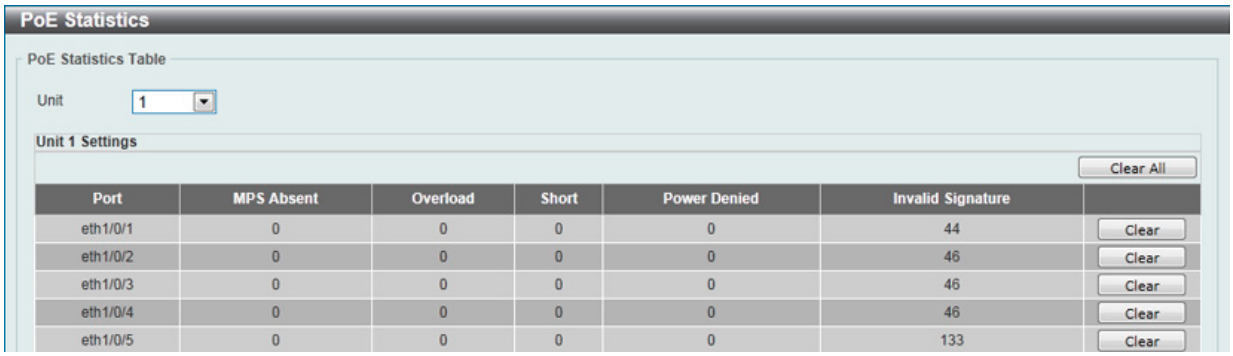


図 6-16　PoE Statistics 画面

画面には以下の項目があります。

項目	説明
Unit	本設定を適用するユニットを選択します。
MPS Absent	PD（受電機器）からの MPS（PD 検出信号）が喪失すると、値が増加します。
Overload	最大供給電力を超えた電力需要が発生した場合、本項目の値が増加します。
Short	PD で短絡が発生している場合、本項目の値が増加します。
Power Denied	システムによる給電が拒否されている場合、本項目の値が増加します。
Invalid Signature	無効な PD シグネチャが検出されると、本項目の値が増加します。

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

PoE Measurement（PoE 測定）

PoE の測定情報を表示します。

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

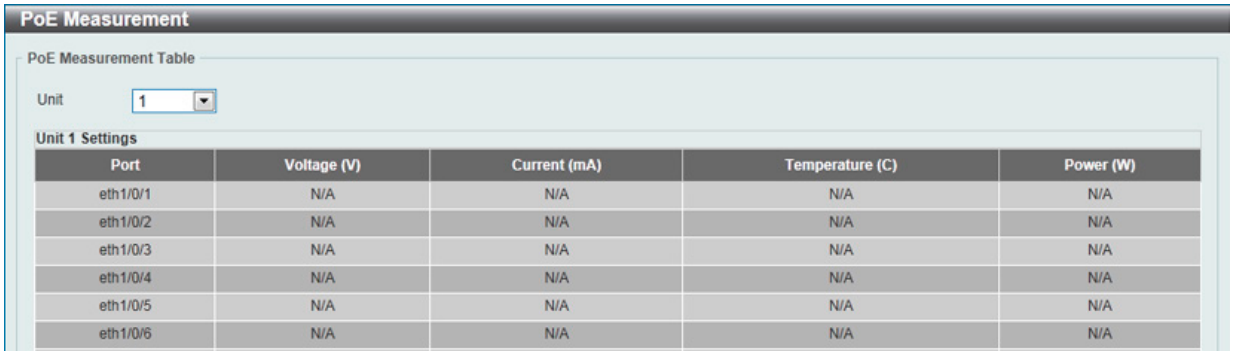


図 6-17　PoE Measurement 画面

画面には以下の項目があります。

項目	説明
Unit	本設定を適用するユニットを選択します。

PoE LLDP Classification（PoE LLDP 分類表示）

PoE の LLDP 分類情報を表示します。

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

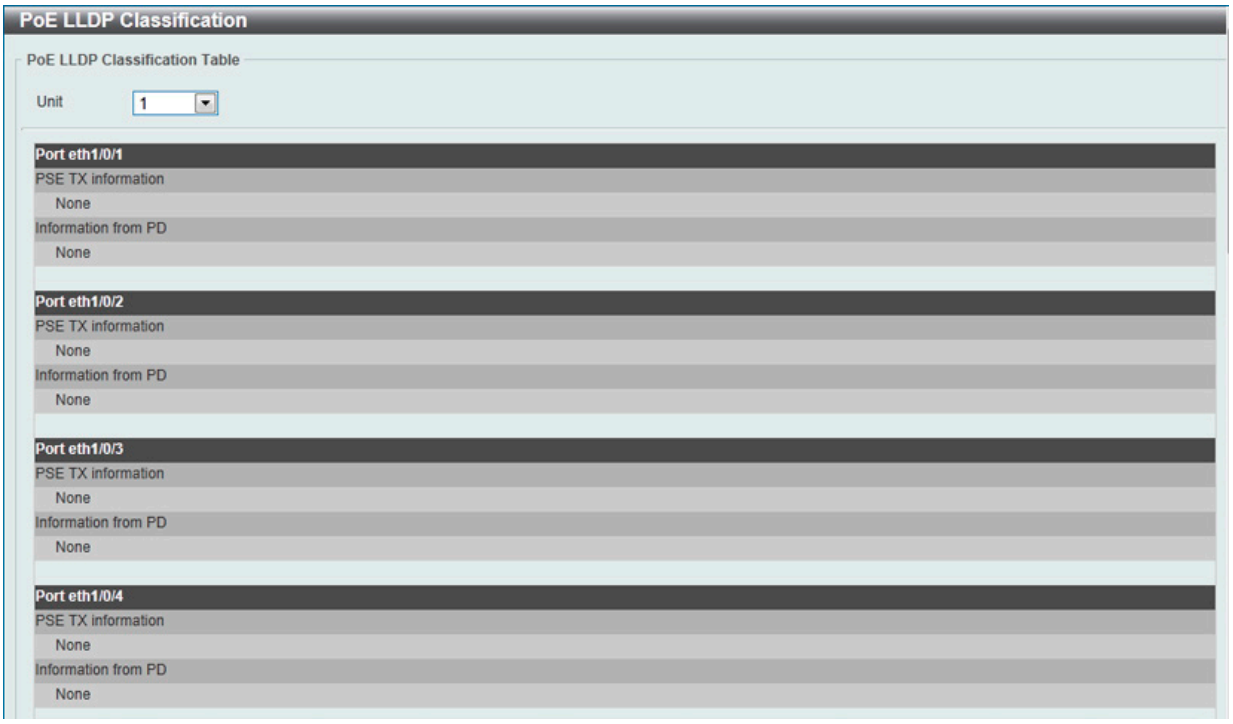


図 6-18　PoE LLDP Classification 画面

画面には以下の項目があります。

項目	説明
Unit	本設定を適用するユニットを選択します。

System Log（システムログ）

System Log Settings（システムログ設定）

スイッチのシステムログ設定を行います。

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

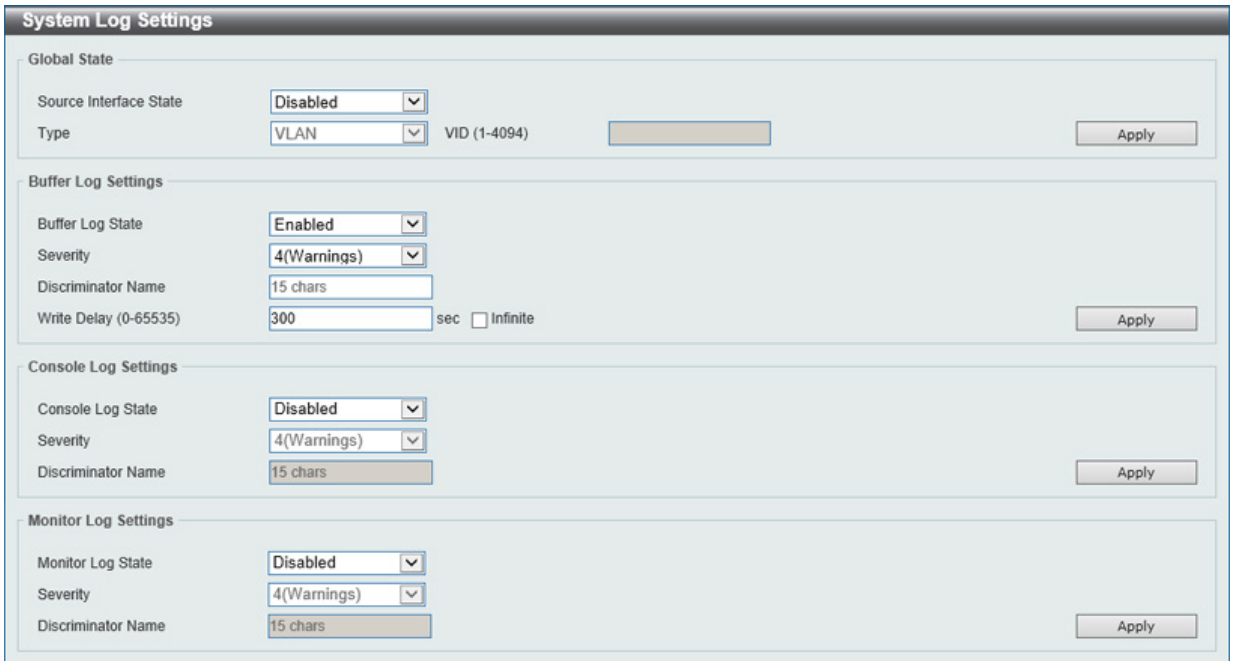


図 6-19　System Log Settings 画面

System Log Settings 画面には次の項目があります。

Global State（グローバルステート）

項目	説明
Source Interface State	送信元インタフェースをグローバルに有効 / 無効に指定します。
Type	インタフェースの種類を選択します。ここでは「VLAN」を選択できます。
VID	「VLAN ID」を指定します。1 から 4094 の間で指定できます。

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

Buffer Log Settings（バッファログ設定）

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

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

Console Log Settings（コンソールログ設定）

項目	説明
Console Log State	コンソールログのグローバルステートを有効 / 無効にします。
Severity	ログされる情報のレベルをプルダウンメニューから選択します。「0：Emergencies」（緊急）、「1：Alerts」（警告）、「2：Critical」（重大）、「3：Errors」（エラー）、「4：Warnings」（警告）、「5：Notifications」（通知）、「6：Informational」（情報）、「7：Debugging」（デバッグ）から選択します。
Discriminator Name	ディスクリミネーターの名前を入力します。15 字以内に指定できます。

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

Monitor Log Settings（モニタログ設定）

項目	説明
Monitor Log State	モニタログのグローバルステートを有効 / 無効にします。
Severity	ログされる情報のレベルをプルダウンメニューから選択します。「0：Emergencies」（緊急）、「1：Alerts」（警告）、「2：Critical」（重大）、「3：Errors」（エラー）、「4：Warnings」（警告）、「5：Notifications」（通知）、「6：Informational」（情報）、「7：Debugging」（デバッグ）から選択します。
Discriminator Name	ディスクリミネーターの名前を入力します。15 字以内に指定できます。

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

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

システムログディスクリミネーターの設定、設定内容の表示を行います。
System > System Log > System Log Discriminator Settings の順にクリックし、以下の画面を表示します。

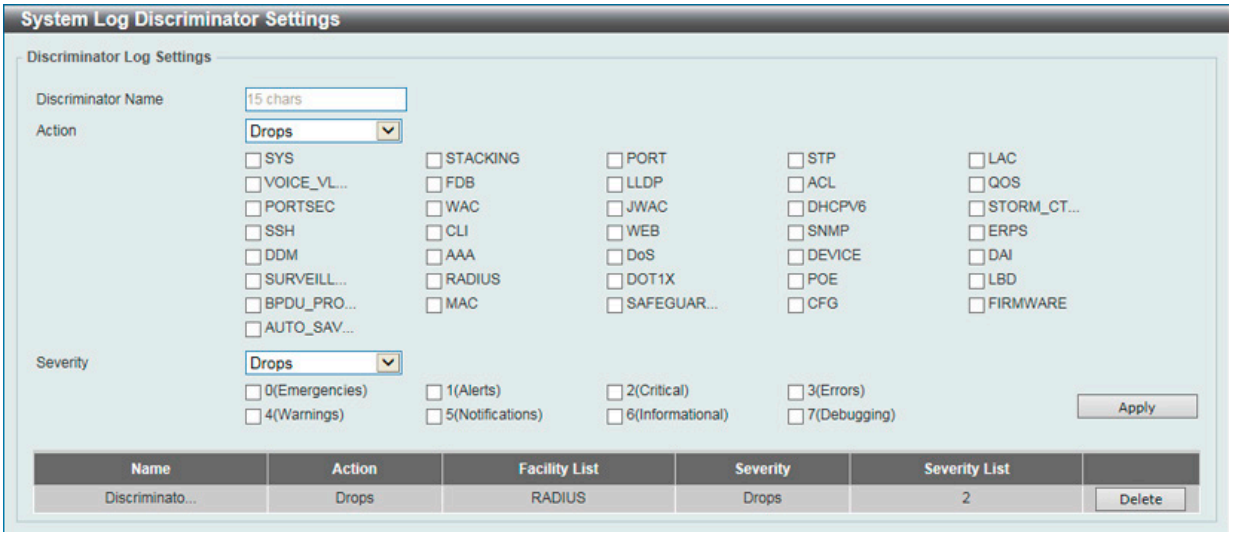


図 6-20　System Log Discriminator Settings 画面

本画面には次の項目があります。

項目	説明
Discriminator Name	ディスクリミネーターの名前を入力します。15 字以内に指定できます。
Action	ディスクリミネーターのログに関して実行する動作と動作対象となる機能にチェックを入れます。 動作は「Drops」（破棄）、「Includes」（内包）から選択します。
Severity	ディスクリミネーターのログに関して実行する動作と動作対象となるログの Severity（重要度）にチェックを入れます。 動作は「Drops」（破棄）、「Includes」（内包）から選択します。重要度は「0：Emergencies」（緊急）、「1：Alerts」（警告）、「2：Critical」（重大）、「3：Errors」（エラー）、「4：Warnings」（警告）、「5：Notifications」（通知）、「6：Informational」（情報）、「7：Debugging」（デバッグ）から選択します。

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

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

システムログはイベントの記録と管理、エラーと情報のメッセージをレポートします。イベントメッセージは、すべてのエラーレポートに Syslog プロトコルの推奨する固有のフォーマットを使用します。例えば、Syslog とローカルデバイスのレポートメッセージはその重要度や、メッセージを生成するアプリケーションを識別するためのメッセージ識別名を含みます。メッセージは緊急度かその関連する事項に基づいてフィルタされます。
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 6-21　System Log Server 画面

本画面には次の項目があります。

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

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

System Log（システムログ）

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。

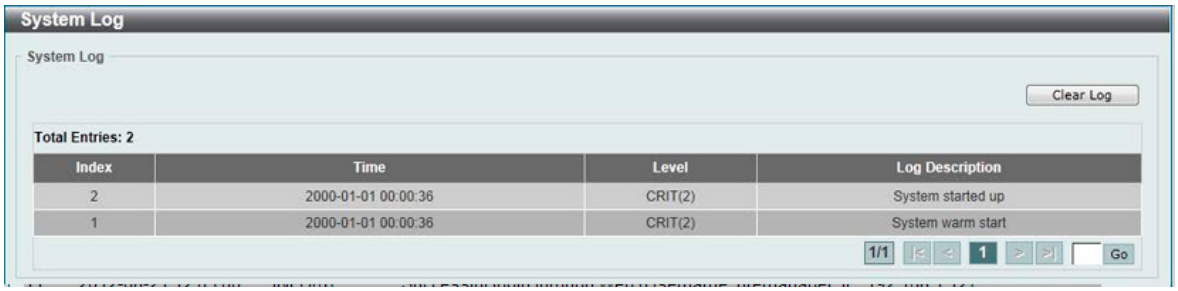


図 6-22　System Log 画面

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

System Attack Log（システムアタックログ）

攻撃を受けたシステムログの閲覧 / 消去を行います。
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 6-23　System Attack Log 画面

画面には以下の項目があります。

項目	説明
Unit	本設定を適用するユニットを選択します。

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

Time and SNTP（時間設定・SNTP 設定）

SNTP（Simple Network Time Protocol）は、インターネットを介してコンピュータのクロックを同期するためのプロトコルです。NTP サーバにアクセスし、システムの時間を調整します。

注意　本シリーズは RTC を持っていないため、再起動すると設定した時間は消去されます。

Clock Settings（時間設定）

スイッチの時間設定を行います。

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

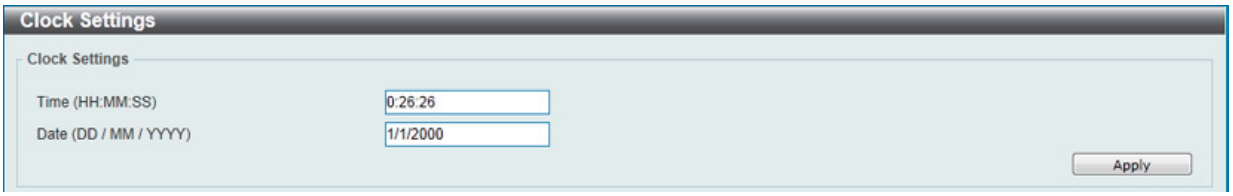


図 6-24　Clock Settings 画面

画面には以下の項目があります。

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

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

Time Zone Settings（タイムゾーン設定）

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

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

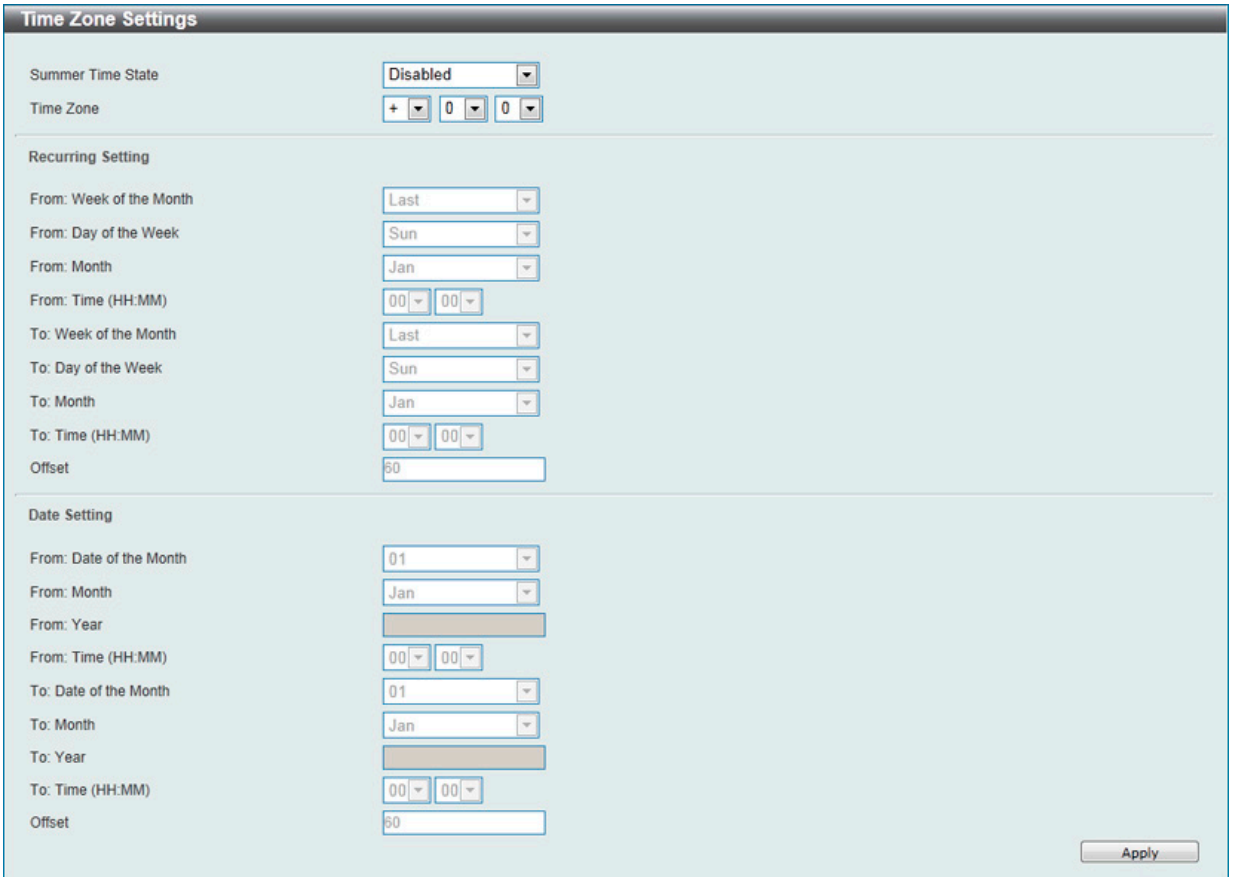


図 6-25　Time Zone Settings 画面

以下に、画面の各項目を示します。

項目	説明
Summer Time State	デバイスに設定するサマータイムの種類を設定します。 • Disabled - サマータイムを無効にします。（初期値） • Recurring Setting - サマータイムを周期的に有効にします。このオプションでは開始と終了のタイミングを指定月の指定週で設定する必要があります。 • Date Setting - サマータイムを日付指定で有効にします。このオプションでは開始と終了の日付を設定する必要があります。
Time Zone	UTC からのタイムゾーンを選択します。
Recurring Setting	
Recurring Setting モードを使用すると、サマータイムの設定を指定した期間で自動的に調整できるようになります。例えば、サマータイムを 4 月の第 2 週の土曜日から、10 月の最終週の日曜日までと指定することができます。	
From: Week Of The Month	月の第何週から DST が始まるかを設定します。
From: Day Of the Week	サマータイムが開始する曜日を指定します。Sun、Mon、Tue、Web、Tues、Fri、Sat
From: Month	サマータイムが開始する月を指定します。Jan、Feb、Mar、Apr、May、Jun、Jul、Aug、Sep、Oct、Nov、Dec
From: Time (HH:MM)	サマータイムが開始する時間を指定します。
To: Week Of The Month	月の第何週でサマータイムが終わるかを設定します。
To: Day Of the Week	サマータイムが終了する曜日を指定します。
To: Month	サマータイムが終了する月を指定します。
To: Time (HH:MM)	サマータイムが終了する時間を指定します。
Offset	サマータイムに追加する時間を指定します。初期値は 60（分）です。オフセットの範囲は「30」「60」「90」「120」を入力できます。
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	サマータイムが始まる月日を指定します。
From: Month	サマータイムが開始する月を指定します。
From: Year	サマータイムが開始する年を指定します。
From: Time In HH MM	サマータイムが開始する時間を指定します。
To: Date of the Month	サマータイムが終了する月日を指定します。
To: Month	サマータイムが終了する月を指定します。
To: Year	サマータイムが終了する年を指定します。
To: Time In HH MM	サマータイムが終了する時間を指定します。
Offset	サマータイムに追加する時間を指定します。初期値は 60（分）です。 オフセットの範囲は「30」「60」「90」「120」から指定できます。

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

SNTP Settings（SNTP 設定）

スイッチに SNTP での時刻同期の設定を行います。

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。

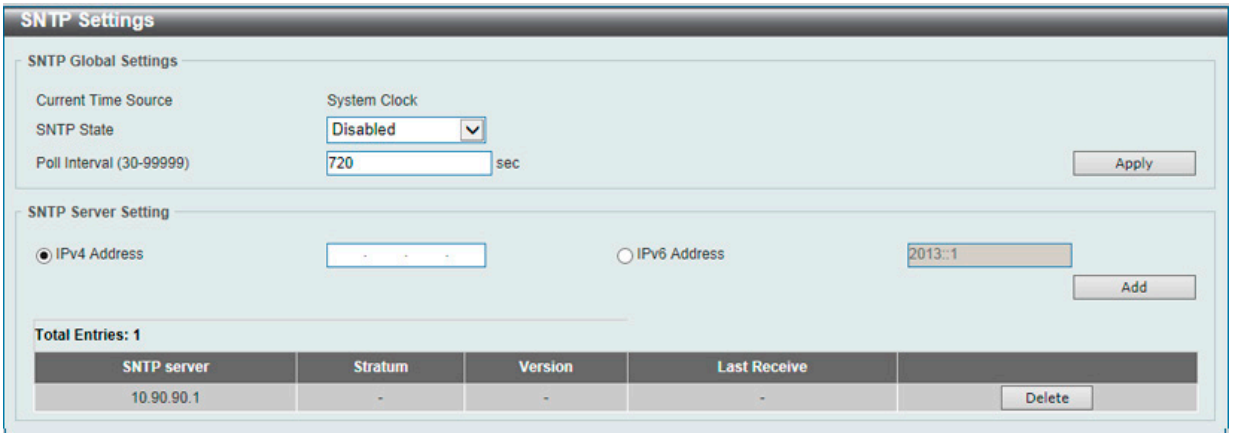


図 6-26　SNTP Settings 画面

以下の項目を使用して設定、表示を行います。

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

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

Time Range（タイムレンジ設定）

スイッチのタイムレンジを設定します。

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

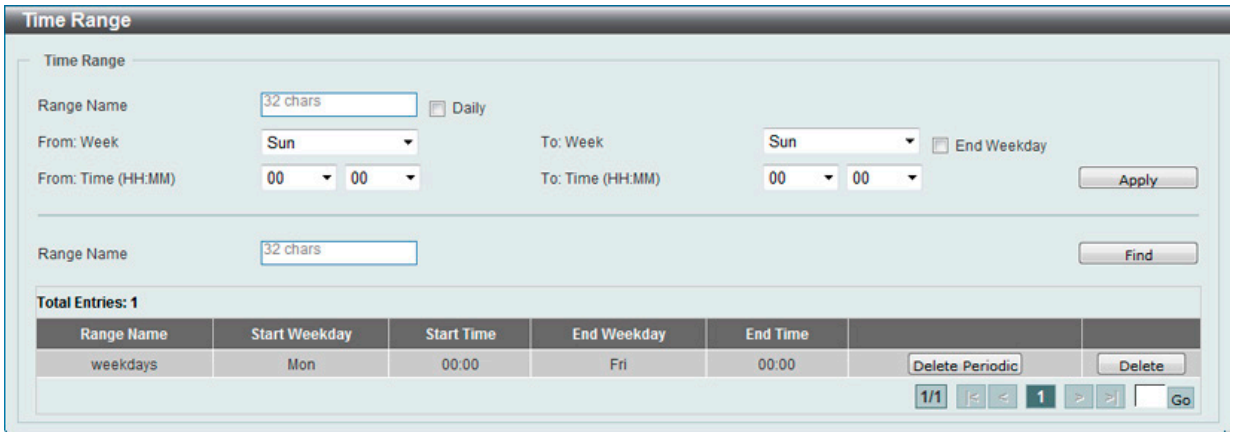


図 6-27　Time Range 画面

以下の項目を設定することができます。

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

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

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

第 7 章　Management（スイッチの管理）

本章でスイッチの管理を行います。

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

サブメニュー	説明
User Accounts Settings （ユーザアカウント設定）	ユーザアカウントの作成と設定を行います。有効なユーザアカウントを表示可能です。
Password Encryption （パスワード暗号化）	設定ファイル内のパスワードの暗号化に関する設定をします。
Login Method（ログイン方法）	各管理インタフェースでのログイン方法について表示、設定します。
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 Settings （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 サーバ /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）	DHCP 自動設定機能の設定を行います。
DNS（ドメインネームシステム）	DNS の設定を行います。
NTP（ネットワークタイムプロトコル）	スイッチが持つ時計の時刻を同期するための通信プロトコルの設定を行います。
IP Source Interface （IP ソースインタフェース）	IP ソースインタフェースを設定します。
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。
Physical Stacking（物理スタッキング）	物理スタックの設定を行います。
Virtual Stacking （仮想スタック / シングル IP マネジメント設定）	仮想スタック /D-Link シングル IP マネジメントの設定を行います。
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設定を行います。有効なユーザアカウントを表示可能です。

注意　初期値ではユーザアカウントとして「admin」（パスワード：admin / 権限レベル：15）が設定されています。

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

- Basic User（基本ユーザ）- 権限レベル 1。ユーザアカウントの中でも一番低い優先値になります。このアカウントの目的は基本的なシステムのチェックになります。
- Operator（オペレータ）- 権限レベル 12。システム設定の変更や確認が可能です。SNMP アカウントやユーザアカウントなどのセキュリティ関連情報への権限はありません。
- Administrator - 権限レベル 15。システム情報を含むすべての設定に関する閲覧、変更の権限があります。

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

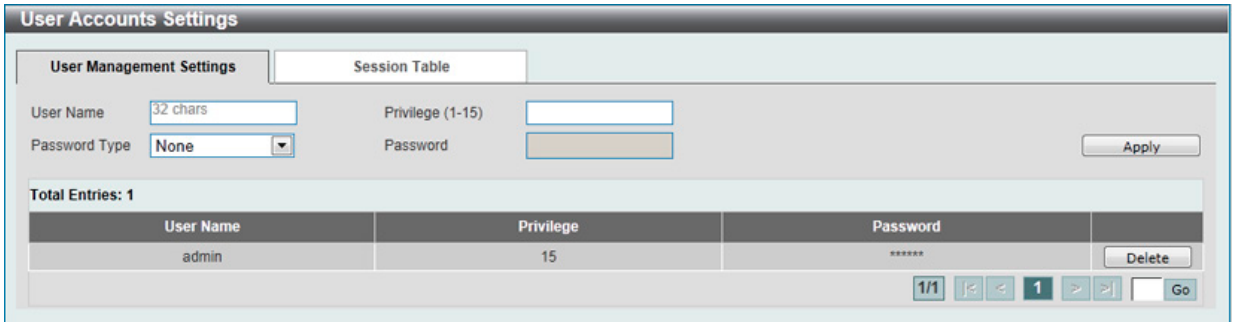


図 7-1　User Accounts Settings - User Management Settings 画面

画面には次の項目があります。

項目	説明
User Name	ユーザ名を定義します。（半角英数字 32 文字以内）
Privilege	アカウントの権限レベルを指定します。1 から 15 までで設定可能です。
Password Type	アカウントで使用する暗号化の方法を「None」「Plain Text」「Encrypted-SHA1」「Encrypted-MD5」から選択します。 • 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。「暗号化フォーマット」へ暗号化することができないことを意味します。 • Encrypted-SHA1 -「SHA-1」でパスワードを指定します。「SHA-1」方式の暗号化パスワードになります。 • Encrypted-MD5 -「MD5」でパスワードを指定します。「MD5」方式の暗号化パスワードになります。 「Password Encryption」については「パスワード暗号化」を参照ください。
Password	アカウントで使用するパスワードを入力します。

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

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

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

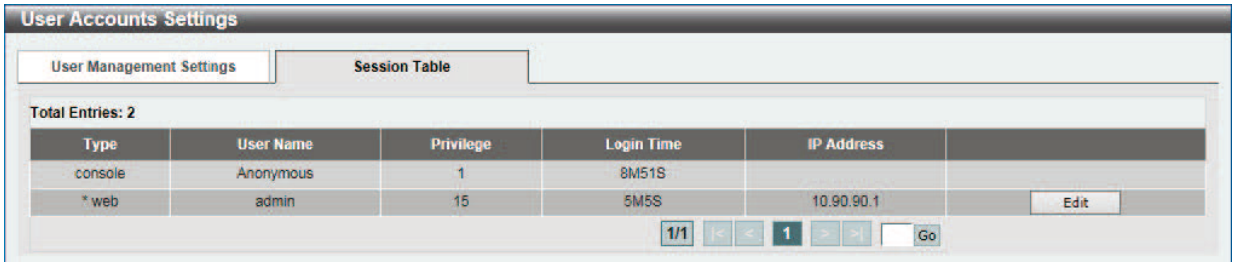


図 7-2　User Accounts Settings - Session Table 画面

「Edit」ボタンをクリックすると、ユーザ権限を設定することができます。

「Edit」ボタンをクリックするとユーザ権限の設定画面が表示されます。



図 7-3　User Priviledge 画面

画面には次の項目があります。

項目	説明
Action	ユーザレベルのセキュリティ設定の有効 / 無効を設定します。
Privilege	ユーザ権限レベル（1-15）を指定します。
Password	アカウントで使用するパスワードを 32 文字以内で入力します。

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Back」ボタンをクリクして、前のページに戻ります。

Password Encryption（パスワード暗号化）

設定ファイル内のパスワードの暗号化に関する設定をします。

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

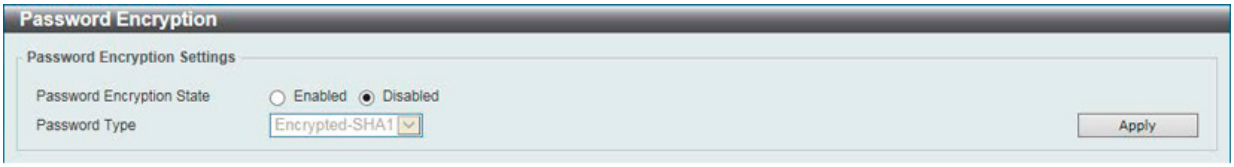


図 7-4　Password Encryption 画面

画面には次の項目があります。

項目	説明
Password Encryption State	設定ファイルに保存されるパスワードの暗号化の有効 / 無効を設定します。
Password Type	暗号化の方法を「Encrypted-SHA1」「Encrypted-MD5」から選択します。 • Encrypted-SHA1 -「SHA-1」でパスワードを指定します。「SHA-1」方式の暗号化パスワードになります。 • Encrypted-MD5 -「MD5」でパスワードを指定します。「MD5」方式の暗号化パスワードになります。

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

Login Method（ログイン方法）

各管理インタフェースでのログイン方法について表示、設定します。

注意　「Login Method」は「AAA」（Authentication、Authorization、and Accounting）が無効の時にのみ設定可能です。

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

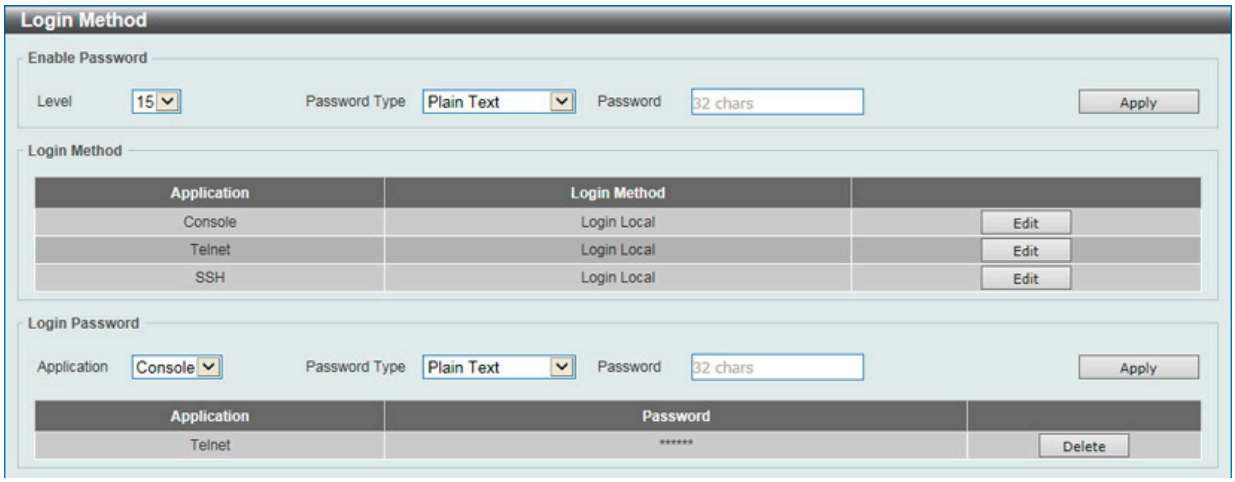


図 7-5　Login Method 画面

画面には次の項目があります。

項目	説明
Enable Password	
Level	パスワードのレベル（1-15）を指定します。
Password Type	パスワード暗号化の方法を「Plain Text」「Encrypted-SHA1」「Encrypted-MD5」から選択します。 • Plain Text - プレーンテキストでパスワードを指定します。「暗号化フォーマット」へ暗号化することができないことを意味します。 • Encrypted-SHA1 -「SHA-1」でパスワードを指定します。「SHA-1」方式の暗号化パスワードになります。 • Encrypted-MD5 -「MD5」でパスワードを指定します。「MD5」方式の暗号化パスワードになります。
Password	パスワードを指定します。
Login Method	
Login Method	Login Method は Authentication、Authorization、Accounting（AAA）が無効な場合にのみ利用可能です。 各項目の「Edit」をクリックし、各項目におけるログイン方法を指定します。「No Login」「Login」「Login Local」から指定できます。「No Login」を指定すると当該項目へのアクセスにおいてログイン認証が不要になります。「Login」を指定すると当該項目へのアクセスにおいて「パスワード」が必要になります。「Login Local」を指定すると当該項目へのアクセスにおいて「ユーザ名」「パスワード」が必要になります。
Login Password	
Application	設定するアプリケーションを選択します。「Console」「Telnet」「SSH」から選択できます。
Password Type	暗号化の方法を「Plain Text」「Encrypted-SHA1」「Encrypted-MD5」から選択します。
Password	選択したアプリケーションで使用するパスワードを入力します。 指定のアプリケーションのログイン方法が「Login」に設定されている時のパスワードになります。

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

エントリの削除

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

SNMP（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 v1.0、v2c、および v3.0 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 の順にメニューをクリックし、以下の画面を表示します。

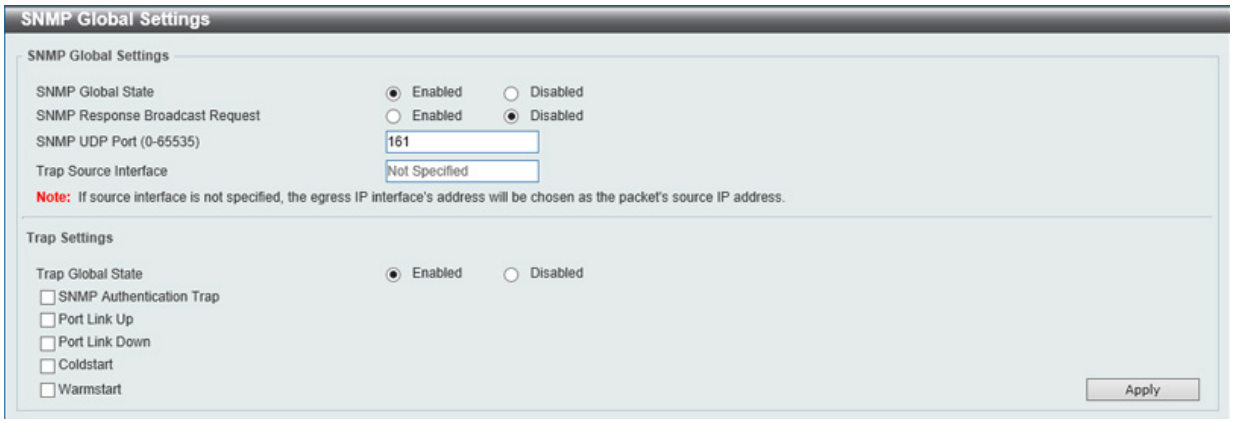


図 7-6　SNMP Global Settings 画面

以下の項目が使用されます。

項目	説明
SNMP Global Settings	
SNMP Global State	「SNMP」機能の有効 / 無効を選択します。
SNMP Response Broadcast Request	「SNMP GetRequest」パケットのブロードキャストに対応するサーバを有効 / 無効に指定します。
SNMP UDP Port	SNMP UDP ポート番号を指定します。
Trap Source Interface	SNMP トラップパケットを送信する送信元アドレスとしての IP アドレスのインタフェースを入力します。
Trap Settings	
Trap Global State	「SNMP」トラップを有効 / 無効にします。
SNMP Authentication Trap	SNMP 認証失敗の通知送信の設定を行います。認証失敗トラップは、機器が正しく認証されていない SNMP メッセージを受信した時に実行されます。認証方法は使用している SNMP のバージョンによります。SNMPv1 または SNMPv2c の場合、不正なコミュニティ文字列によってパケットが構成されている時に認証に失敗します。SNMPv3 の場合は、間違った SHA/MD5 キーによってパケットが構成されている時に認証に失敗します。
Port Link Up	ポートリンクアップ通知送信の設定を行います。リンクアップトラップは機器がリンクアップを認識すると実行します。
Port Link Down	ポートリンクダウン通知送信の設定を行います。リンクダウントラップは機器がリンクダウンを認識すると実行します。
Coldstart	「Coldstart Traps」を有効 / 無効にします。
Warmstart	「Warmstart Traps」を有効 / 無効にします。

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

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

スイッチの SNMP リンクチェンジトラップを有効または無効にします。

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

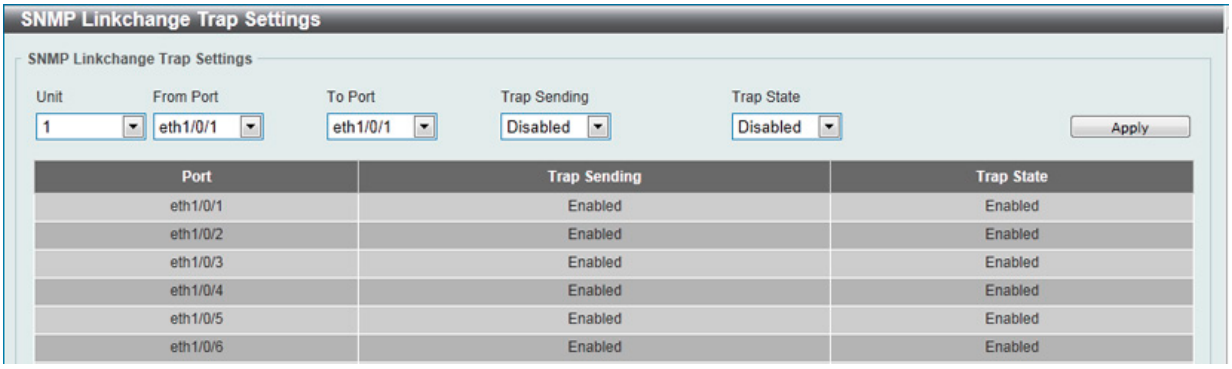


図 7-7　SNMP Linkchange Traps Settings 画面

以下の項目が使用されます。

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

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

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

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

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

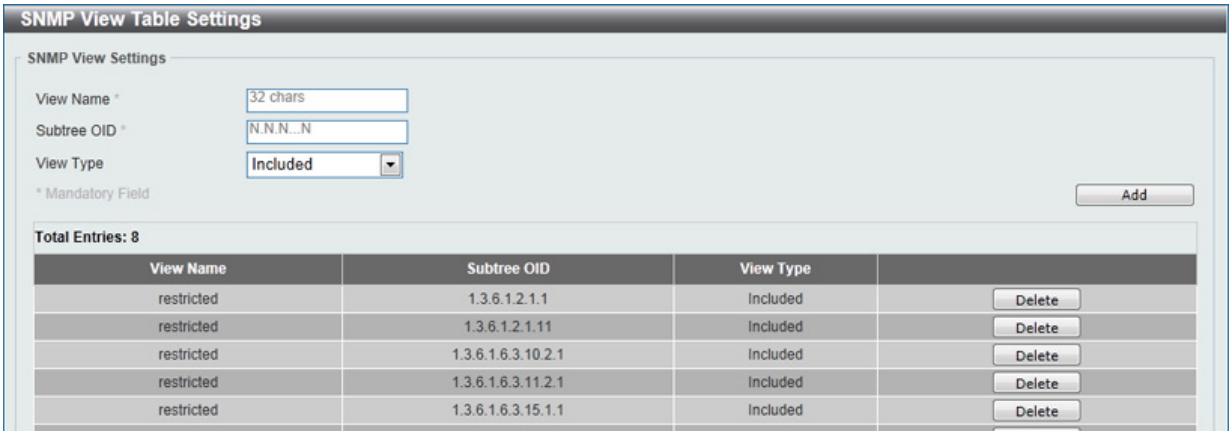


図 7-8　SNMP View Table 画面

エントリの削除

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

エントリの作成

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

以下の項目が使用されます。

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

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

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

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

コミュニティエントリを設定するためには、**Management> SNMP > SNMP Community Table Settings** の順にクリックし、以下の画面を表示します。

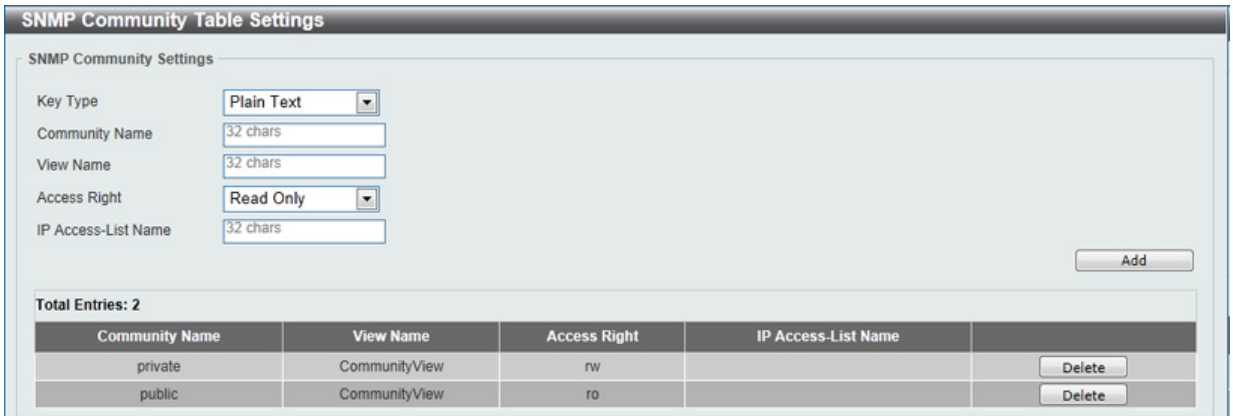


図 7-9　SNMP Community Table Settings 画面

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

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

エントリの作成

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

エントリの削除

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

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

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

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

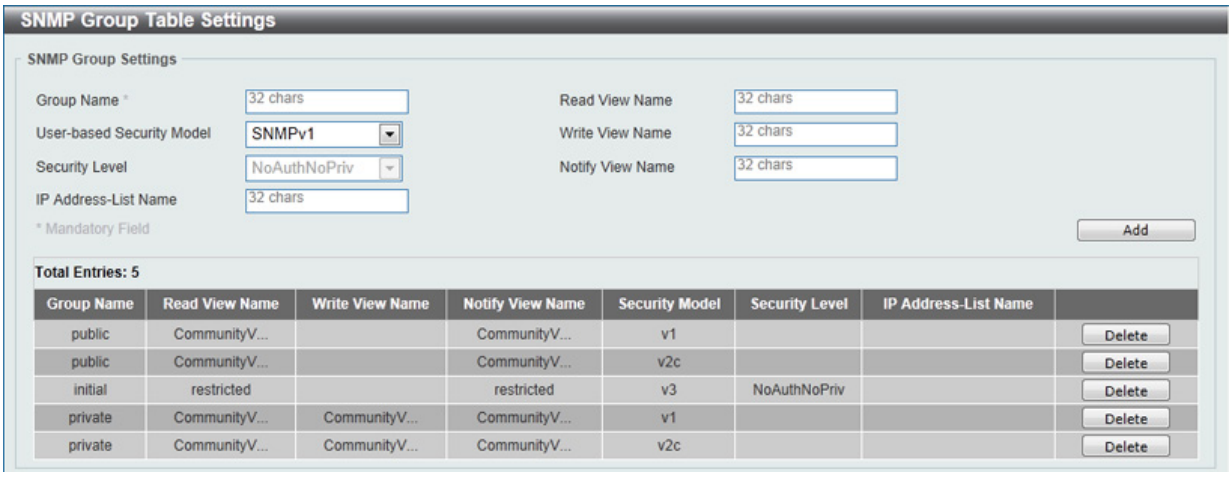


図 7-10　SNMP Group Table 画面

「SNMP Group Table」画面のエントリの削除
エントリの行の「Delete」ボタンをクリックします。

「SNMP Group Table」画面への新規エントリの追加
上記画面に情報を入力し、「Add」ボタンをクリックします。

以下の項目が使用されます。

項目	説明
Group Name	32 文字までの半角英数字を入力します。SNMP ユーザのグループの識別に使用します。
User-based Security Model	• SNMPv1 - SNMP バージョン 1 が使用されます。 • SNMPv2c - SNMP バージョン 2c が使用されます。SNMP バージョン 2 は集中型、分散型どちらのネットワーク管理にも対応します。SNMP バージョン 1 と比較して SMI（Structure of Management Information）およびセキュリティ機能において強化されています。 • SNMPv3 - SNMP バージョン 3 が使用されます。ネットワーク上で認証とパケットの暗号化を併用することにより、デバイスへの安全なアクセスを提供します。
Security Level	セキュリティレベル設定は SNMP バージョン 3 にのみ適用されます。 • NoAuthNoPriv - スイッチとリモート SNMP マネージャ間のパケットは認証も暗号化もされません。 • AuthNoPriv - スイッチとリモート SNMP マネージャ間のパケットは認証あり、暗号化なしになります。 • AuthPriv - スイッチとリモート SNMP マネージャ間のパケットは認証あり、暗号化ありになります。
IP Access-List Name	グループに関連付ける標準 IP アクセスリスト（ACL) を入力します。
Read View Name	グループユーザがアクセス可能な読み取りビュー名を入力します。
Write View Name	グループユーザがアクセス可能な書き込みビュー名を入力します。
Notify View Name	グループユーザがアクセス可能な書き込みビュー名を入力します。 Notify View はトラップパケットを介してステータスをグループユーザにレポートすることができるオブジェクトです。

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

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

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

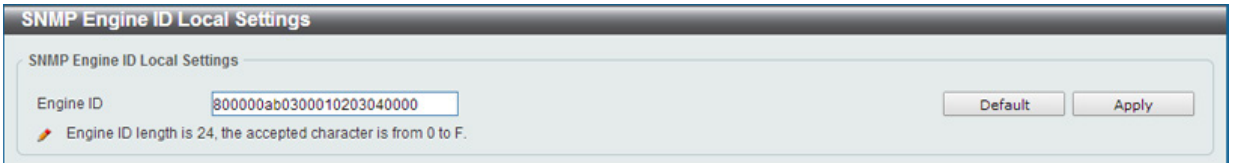


図 7-11　SNMP Engine ID 画面

エンジン ID を変更するためには、新しいエンジン ID（最大 24 文字）を入力し、「Apply」ボタンをクリックします。
「Default」をクリックするとエンジン ID は初期値に戻ります。

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

スイッチに現在設定されているすべての SNMP ユーザが表示されます。

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

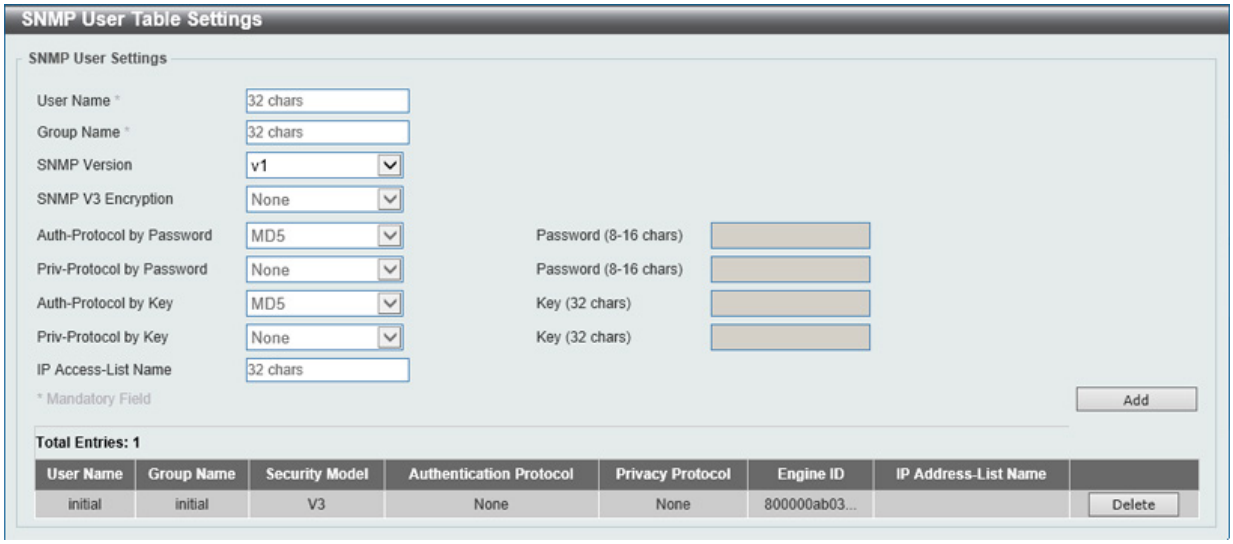


図 7-12　SNMP User Table 画面

エントリの削除

エントリの行の「Delete」ボタンをクリックします。

エントリの新規登録

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

上記画面中の項目を以下に示します。

項目	説明
User Name	32 文字までの半角英数字。SNMP ユーザを識別します。
Group Name	作成した SNMP グループが SNMP メッセージを要求するために使用される名前です。
SNMP Version	• v1 - SNMP バージョン 1 が使用されます。 • v2c - SNMP バージョン 2 が使用されます。 • v3 - SNMP バージョン 3 が使用されます。
SNMP V3 Encryption	SNMP v3 の暗号化の設定を行います。本項目は「SNMP Version」で「v3」を選択した場合に有効になります。 • None - 暗号化は行いません。 • Key - キー（鍵）による暗号化を行います。 • Password - パスワードによる暗号化を行います。
Auth-Protocol	本項目は「SNMP Version」で「v3」を選択され、「SNMP V3 Encryption」で「Password」または「Key」を選択した場合に有効になります。本項目を選択後、「Password」/「Key」にパスワードを入力します。 • MD5 - HMAC-MD5-96 認証レベルが使用されます。 • SHA - HMAC-SHA 認証プロトコルが使用されます。
Priv-Protocol	本項目は「SNMP Version」で「v3」を選択され、「SNMP V3 Encryption」で「Password」または「Key」を選択した場合に有効になります。 • None - 認証プロトコルは使用されません。 • 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。本項目を選択後、「Password」/「Key」を入力する必要があります。
IP Access-List Name	アクセスするための標準 IP アクセスリスト（ACL）の名前を入力します。

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

SNMP トラップの送信先を登録します。

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

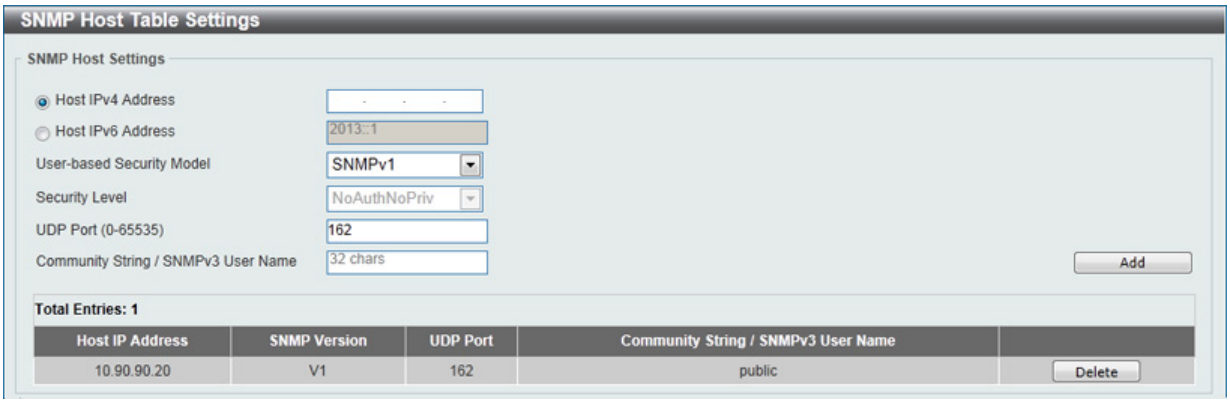


図 7-13　SNMP Host Table 画面

エントリの新規登録

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

以下の項目を設定します。

項目	説明
Host IPv4 Address	スイッチの SNMP ホストとなるリモート管理ステーション（トラップの送信先）の IPv4 アドレスを入力します。
Host IPv6 Address	スイッチの SNMP ホストとなるリモート管理ステーション（トラップの送信先）の IPv6 アドレスを入力します。
User-based Security Model	• SNMPv1 : SNMP バージョン 1 が使用されます。 • SNMPv2c : SNMP バージョン 2c が使用されます。 • SNMPv3 : SNMP バージョン 3 が使用されます。
Security Level	「User-based Security Model」で「SNMPv3」を指定した場合、次のオプションを選択します。 • NoAuthNoPriv - リモート SNMP マネージャーとスイッチ間において認証 / パケット暗号化が適用されません。 • AuthNoPriv - リモート SNMP マネージャーとスイッチ間において認証が必要ですが、パケット暗号化は適用されません。 • AuthPriv - リモート SNMP マネージャーとスイッチ間において認証 / パケット暗号化は適用されます。
UDP Port	UDP ポート番号を入力します。UDP ポート番号の初期トラップは 162 です。UDP ポート範囲は 0 から 65535 です。いくつかのポート番号は他のプロトコルと衝突する可能性があります。
Community String/ SNMPv3 User Name	コミュニティ名または SNMP V3 ユーザ名を入力します。

エントリの登録を行う場合

1. 設定項目を入力します。
2. 「Add」をクリックします。

エントリの削除

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

RMON（RMON 設定）

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

RMON Global Settings（RMON グローバル設定）

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

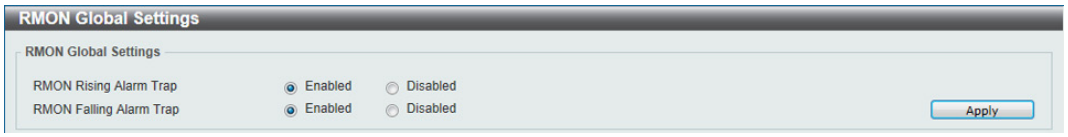


図 7-14　RMON Global Settings 画面

以下の項目が使用されます。

項目	説明
RMON Rising Alarm Trap	「RMON」における上昇しきい値警告トラップを有効にします。しきい値の設定は「RMON Alarm Settings（RMON アラーム設定）」で行います。
RMON Falling Alarm Trap	「RMON」における下降しきい値警告トラップを有効にします。しきい値の設定は「RMON Alarm Settings（RMON アラーム設定）」で行います。

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

RMON Statistics Settings（RMON 統計情報）

RMON 統計情報を表示、設定します。

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

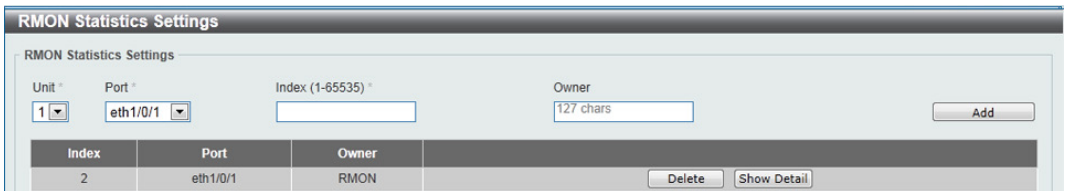


図 7-15　RMON Statistics Settings 画面

以下の項目が使用されます。

項目	説明
Unit	設定するユニットを選択します。
Port	RMON 情報を取得したポートを指定します。
Index (1 - 65535)	RMON イーサネット統計情報エントリの番号を指定します。
Owner	オーナ名（文字列）を 127 字までで指定します。

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

統計情報の登録を行う場合
設定項目を入力し「Add」をクリックします。

統計情報の削除を行う場合
「Delete」をクリックします。

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

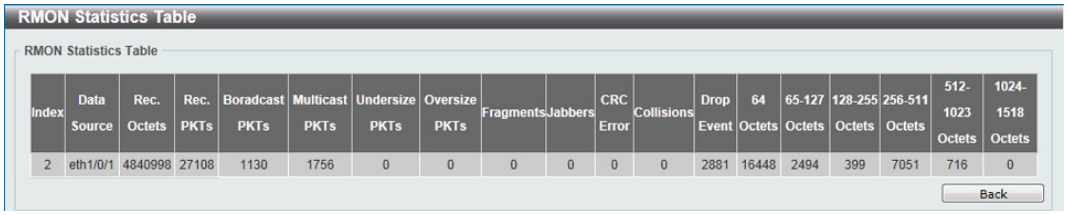


図 7-16　RMON Statistics Settings - Show Detail 画面

「Back」をクリックすると前ページへ移動します。

RMON History Settings（RMON ヒストリ設定）

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

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

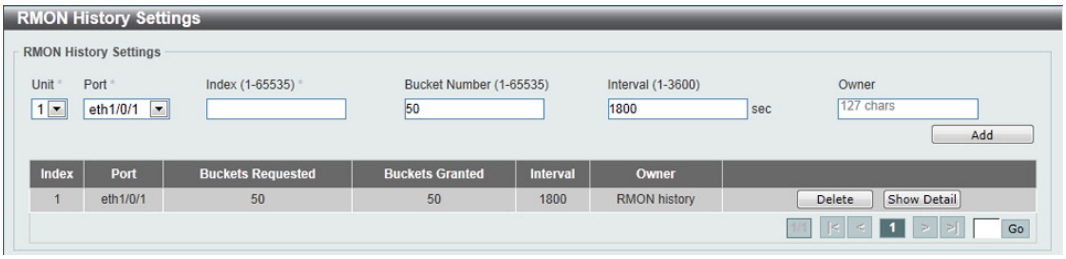


図 7-17　RMON History Settings 画面

以下の項目が使用されます。

項目	説明
Unit	設定するユニットを選択します。
Port	RMON ヒストリを取得するポートを指定します。
Index (1 - 65535)	インデックス番号を指定します。(1-65535)
Bucket Number	統計の RMON 取得履歴グループに指定するバケット数（1-65535）を指定します。初期値は 50 です。
Interval (1-3600)	ポーリング間隔（秒）を設定します。 初期値：1800 (秒) 入力可能範囲：1-3600 (秒)
Owner	オーナーの文字列を入力します。127 文字まで入力可能です。

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

履歴情報の登録を行う場合

1. 設定項目を入力します。
2. 「Add」をクリックします。

履歴情報の削除を行う場合

「Delete」をクリックします。

指定ポートの履歴情報を表示する場合

「Show Detail」をクリックします。以下の画面が表示されます。

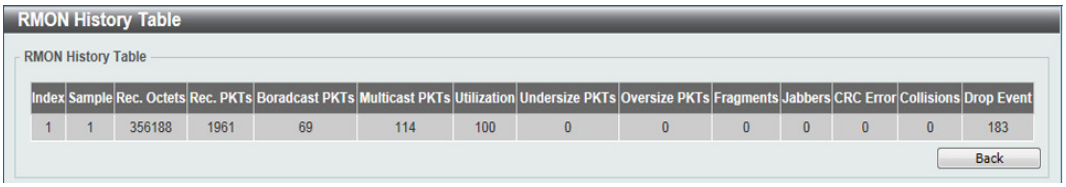


図 7-18　RMON History Settings - Show Detail 画面

「Back」をクリックすると前ページへ移動します。

RMON Alarm Settings（RMON アラーム設定）

インタフェースをモニタする設定を行います。

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

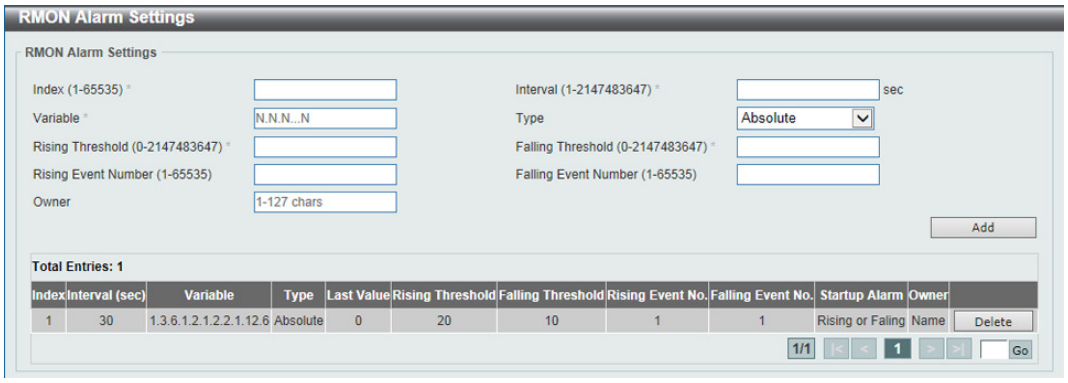


図 7-19　RMON Alarm Settings 画面

以下の項目が使用されます。

項目	説明
Index (1-65535)	アラームインデックスを入力します。（1-65535）
Interval	変数のサンプリングと閾値を確認する間隔を秒で指定します。1 から 2147483647（秒）の間で指定可能です。
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	モニタリングタイプを Absolute と Delta から選択します。 • Absolute - MIB 値をしきい値としてアクションを作動する方式です。 • Delta - MIB 値の差分（変動率）をしきい値としてアクションを作動する方式です。
Rising Threshold	上昇しきい値を設定します。0 から 2147483647（秒）の間で指定可能です。
Falling Threshold	下降しきい値を設定します。0 から 2147483647（秒）の間で指定可能です。
Rising Event Number (1-65535)	上昇しきい値を超えたときに始動するイベントエントリのインデックスを入力します。 1 から 65535 から指定します。指定しない場合、上昇しきい値を超えてもアクションをとりません。
Falling Event Number (1-65535)	下降しきい値を下回ったときに始動するイベントのインデックスを入力します。 1 から 65535 から指定します。指定しない場合は、下降しきい値を下回ってもアクションをとりません。
Owner	オーナーの文字列を入力します。127 文字まで入力可能です。

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

エントリの登録を行う場合

1. 設定項目を入力します。
2. 「Add」をクリックします。

エントリの削除を行う場合

「Delete」をクリックします。

RMON Event Settings（RMON イベント設定）

RMON イベントに関する設定と参照を行います。

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

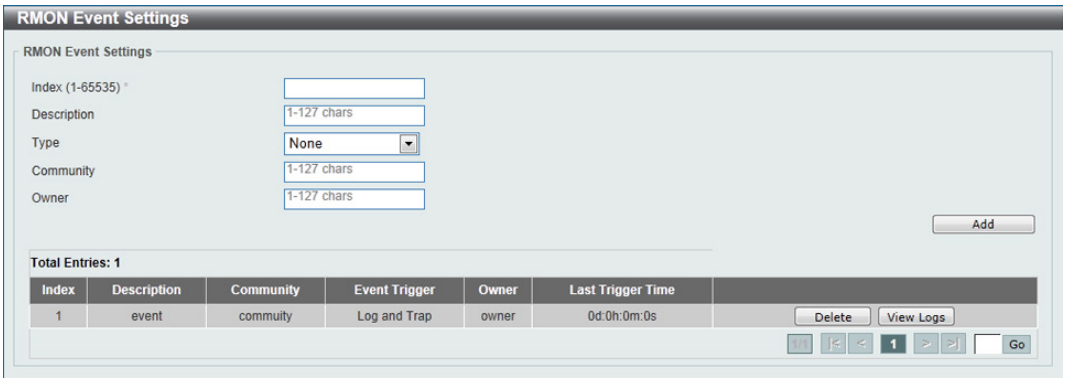


図 7-20　RMON Event Settings 画面

以下の項目が使用されます。

項目	説明
Index (1-65535)	イベントを指定します。
Description	RMON イベントエントリの説明を入力します。最大 127 文字までです。
Type	RMON イベントエントリタイプを選択します。 • None - イベントが発生しなかったことを示します。 • Log - イベントがログエントリであることを示します。 • Trap - イベントがトラップであることを示します。 • Log and Trap - イベントがログエントリとトラップの両方であることを示します。
Community	イベントが所属するコミュニティを指定します。127 文字まで入力可能です。
Owner	オーナーの文字列を入力します。127 文字まで入力可能です。

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

エントリの登録を行う場合

1. 設定項目を入力します。
2. 「Add」をクリックします。

エントリの削除を行う場合

「Delete」をクリックします。

指定エントリのログ情報を表示する場合

「View Logs」をクリックします。以下の画面が表示されます。



図 7-21　Event Logs Table 画面

「Back」をクリックすると前ページへ移動します。

Telnet / Web Settings（Telnet /Web 設定）

スイッチに Telnet 設定と Web 設定をします。

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

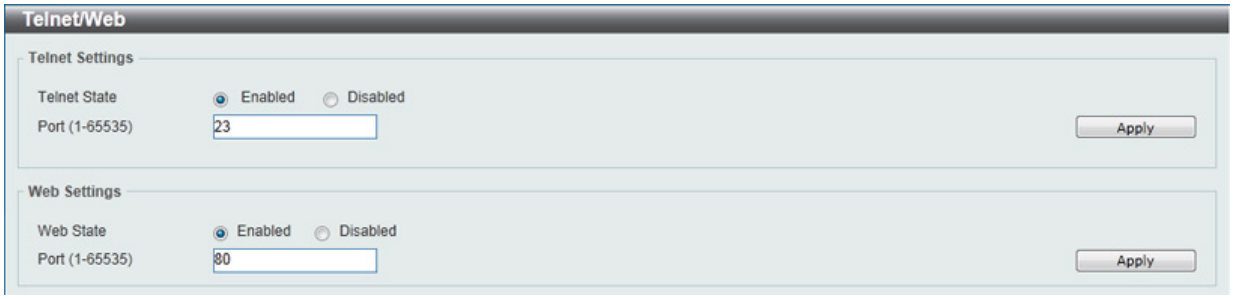


図 7-22　Telnet/Web Settings 画面

以下の項目が使用されます。

Telnet 設定

項目	説明
Telnet State	Telnet 設定は初期値で「Enabled」（有効）です。Telnet 経由のシステム設定を許可しない場合は、「Disabled」（無効）を選択します。
Port (1-65535)	スイッチの Telnet マネジメントに使用される TCP ポート番号（1-65535）。Telnet プロトコルに通常使用される TCP ポートは 23 です。

Web 設定

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

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

Session Timeout（セッションタイムアウト）

セッションタイムアウトの設定、表示を行います。他のスイッチの Telnet インタフェースへの Console/Telnet/SSH 接続（CLI 経由）には「Outgoing Session Timeout（外部セッションタイムアウト）」の値を使用します。

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

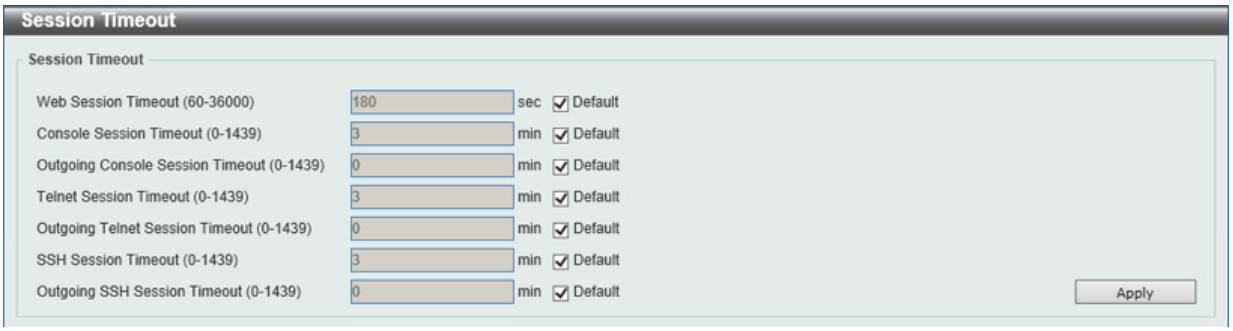


図 7-23　Session Timeout 画面

以下の項目が使用されます。

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

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

DHCP（DHCP 設定）

Service DHCP（DHCP サービス）

スイッチの DHCP サービスについて設定します。

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

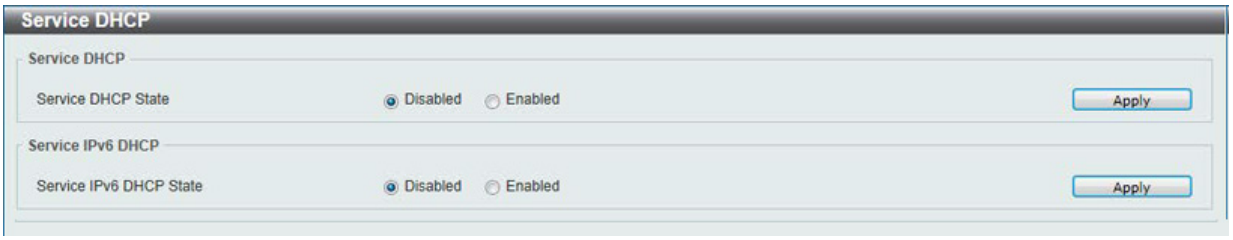


図 7-24　Service DHCP 画面

以下の項目が使用されます。

項目	説明
Service DHCP State	DHCP サーバ及びリレーサービスを有効 / 無効に設定します。
Service IPv6 DHCP State	IPv6 DHCP サーバ及びリレーサービスを有効 / 無効に設定します。

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

DHCP Class Settings（DHCP クラスサービス設定）

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

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



図 7-25　DHCP Class Settings 画面

以下の項目が使用されます。

項目	説明
DHCP Class State	
DHCP Use Class State	DHCP クラス機能を有効 / 無効に設定します。
SNTP Server Settings	
Class Name	DHCP クラス名を 32 文字までで指定します。

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

エントリの削除を行う場合
「Delete」をクリックします。

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



図 7-26　DHCP Class Option Settings 画面

以下の項目が使用されます。

項目	説明
Option	DHCP オプション番号を指定します。1-255 までで指定可能です。
Hex	指定した DHCP オプションの 16 進数方式を入力します。「*」にチェックを入れると残りのオプションのビットはマッチされません。
Bitmask	16 進数ビットマスクを入力します。マスクされたビット方式はマッチします。指定されない場合、16 進数で入力されたすべてのビットがチェックされます。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Back」をクリックすると前ページへ移動します。

エントリの削除を行う場合
「Delete」をクリックします。

DHCP Server（DHCP サーバ）

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

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

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

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

DHCP Server Global Settings（DHCP サーバグローバル設定）

DHCP サーバのグローバルパラメータを設定します。

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

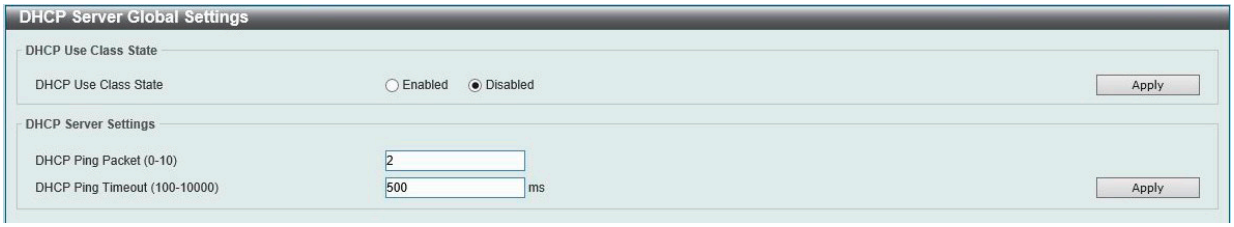


図 7-27　DHCP Server Global Settings 画面

以下の項目が表示されます。

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

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

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

DHCP サーバプールの追加および削除を行います。

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



図 7-28　DHCP Server Pool Settings 画面

以下の項目が表示されます。

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

「Apply」ボタンをクリックして、設定内容に基づくエントリを追加します。
作成されたプールは、「Edit Class」「Edit Option」「Configure」ボタンをクリックして、設定を編集することができます。
「Delete」ボタンをクリックして、指定エントリを削除します。

テーブル情報が複数ページ存在する場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

エントリの編集（クラス割り当て）

「Edit Class」ボタンをクリックすると、以下の画面が表示されます。



図 7-29　DHCP Server Pool Class Settings（Edit Class）画面

以下の項目が表示されます。

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

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Delete by Name」をクリックすると、名前に基づいて DHCP クラス割り当てを削除します。
「Delete by Address」をクリックすると、アドレスに基づいて DHCP クラス割り当てを削除します。

「Back」をボタンをクリックすると前のページに戻ります。

エントリの編集（DHCP オプション設定）

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



図 7-30　DHCP Server Pool Option Settings（Edit Option）画面

以下の項目が表示されます。

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

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Delete」ボタンをクリックして、エントリを削除します。

「Back」をボタンをクリックすると前のページに戻ります。

エントリの編集（サーバプール設定）

「Configure」ボタンをクリックすると、以下の画面が表示されます。

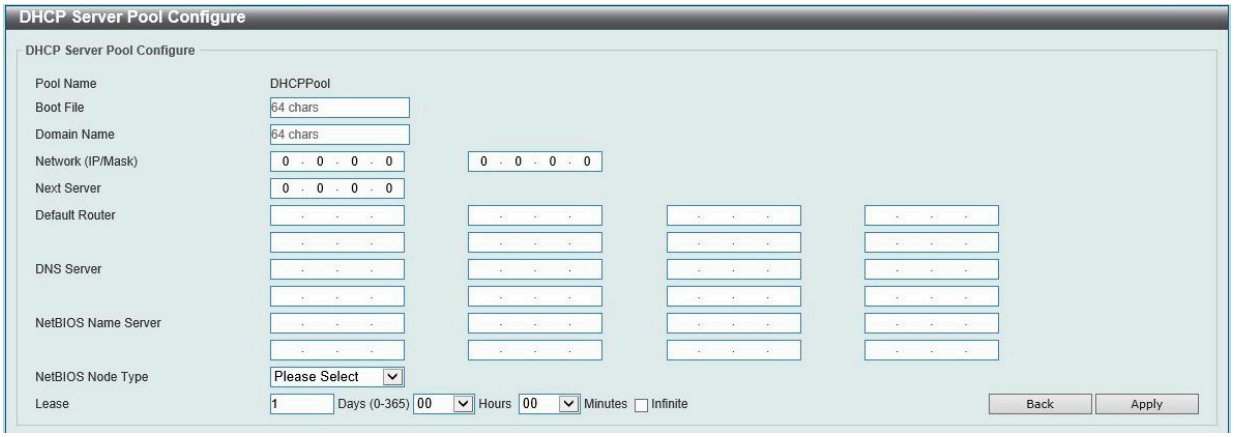


図 7-31　DHCP Server Pool Settings (Configure) 画面

以下の項目が表示されます。

項目	説明
Pool Name	編集する DHCP プール名が表示されます。
Boot File	ブートイメージのファイル名を指定します。（64 文字以内）
Domain Name	DHCP クライアントのドメイン名を入力します。（64 文字以内）
Network (IP/Mask)	プールのネットワークアドレスと対応するネットマスクを入力します。
Next Server	ネクストサーバの IP アドレスを指定します。本サーバに格納されているブートイメージファイルが DHCP クライアントによって検索されます。一般的に TFTP サーバが使用されます。ネクストサーバの IP アドレスはひとつのみ指定できます。
Default Router	DHCP クライアントのデフォルトルータの IP アドレスを入力します。ここでは最大 8 つの IP アドレスを指定できます。本ルータの IP アドレスはクライアントのサブネットと同じサブネットである必要があります。ルータは優先度の高い順に並んでいます。デフォルトルータが既に設定済みの場合、後から設定されたデフォルトルータはデフォルトインタフェースリストに追加されます。

項目	説明
DNS Server	DHCP クライアントが使用する DNS サーバの IP アドレスを入力します。ここでは最大 8 つの IP アドレスを指定できます。DNS サーバは優先度の高い順に並んでいます。DNS サーバが既に設定済みの場合、後から設定された DNS サーバは DNS サーバリストに追加されます。
NetBIOS Name Server	DHCP クライアントが使用する WINS サーバの IP アドレスを指定します。最大 8 つの IP アドレスを指定できます。サーバは優先度の高い順に並んでいます。ネームサーバが既に設定済みの場合、後から設定されたネームサーバはデフォルトインテフェースリストに追加されます。
NetBIOS Node Type	マイクロソフト DHCP クライアントの NetBIOS ノードタイプを指定します。このオプションでは、NetBIOS において登録および名前解決に使用する方法を選択します。 • 「Broadcast」- システムはブロードキャストを使用します。 • 「Peer to Peer」（p-node）- ネームサーバ（WINS）に対して Peer to Peer による名前クエリのみを使用します。 • 「Mixed」（m-node）- まずブロードキャストを使用し、その後ネームサーバへの問い合わせます。 • 「Hybrid」（h-node）- まずネームサーバへの問い合せを行い、その後ブロードキャストを使用します。 「Hybrid」を使用することを推奨します。
Lease	アドレスプールから割り当てるアドレスのリース期間を指定します。 • 「Days」- リースする日数（0-365） • 「Hours」- リースする時間（時） • 「Minutes」- リースする時間（分） • 「Infinite」- リース期間が無制限

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Back」をボタンをクリックすると前のページに戻ります。

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

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

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



図 7-32　DHCP Server Exclude Address 画面

以下の項目が表示されます。

項目	説明
Begin Address	除外する IP アドレス範囲の開始 IP アドレスを指定します。
End Address	除外する IP アドレス範囲の終了 IP アドレスを指定します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Delete」ボタンをクリックして、指定エントリを削除します。

DHCP Server Manual Binding（DHCP サーバマニュアルバインディング）

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

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



図 7-33　DHCP Server Manual Binding 画面

以下の項目が表示されます。

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

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Delete」ボタンをクリックして、指定エントリを削除します。

「Back」をボタンをクリックすると前のページに戻ります。

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

DHCP サーバダイナミックバインディングエントリの表示と削除を行います。

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

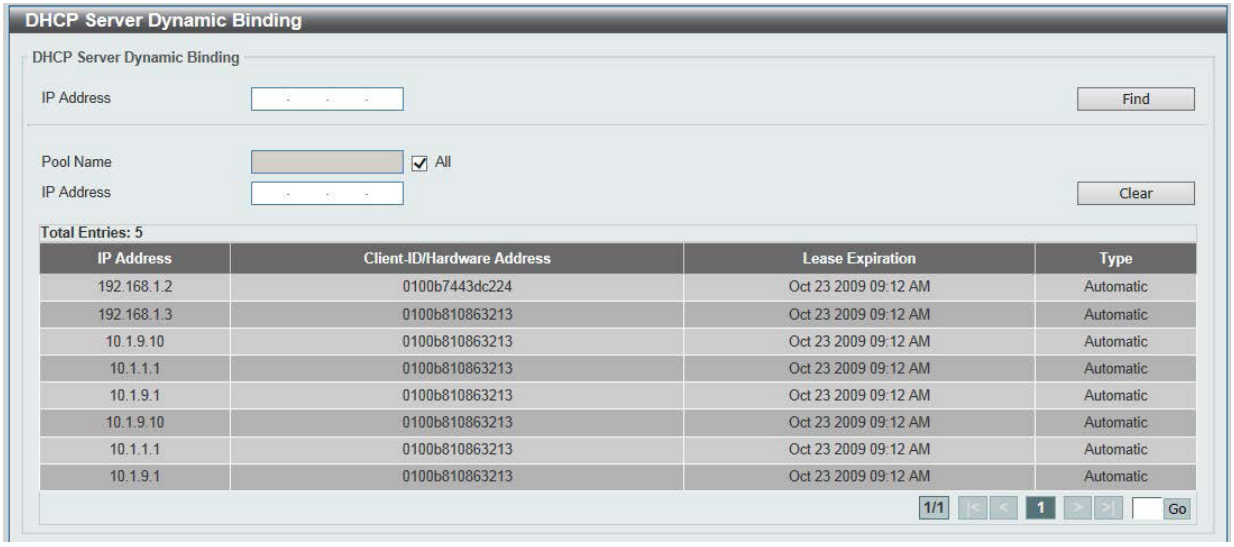


図 7-34　DHCP Server Dynamic Binding 画面

以下の項目が表示されます。

項目	説明
IP Address	バインディングエントリの IP アドレスを指定します。
Pool Name	ダイナミックにバインドされている DHCP エントリのプール名を指定します。「All」オプションにチェックを入れると、全てのプールのバインディングエントリを削除します。

「Find」ボタンをクリックして、指定条件に基づくエントリを検索 / 表示します。
「Clear」ボタンをクリックして、指定条件に基づくエントリを削除します。

DHCP Server IP Conflict（DHCP サーバ IP コンフリクト）

DHCP サーバデータベースの DHCP コンフリクトエントリを表示、クリアします。

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

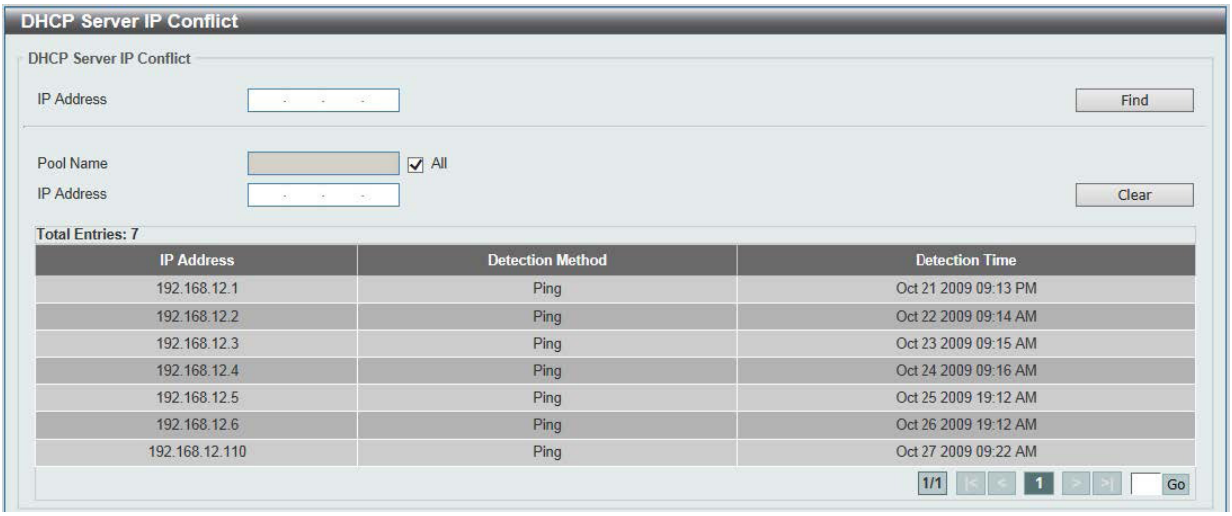


図 7-35　DHCP Server IP Conflict 画面

以下の項目が表示されます。

項目	説明
IP Address	コンフリクトエントリの IPv4 アドレスを入力します。
Pool Name	DHCP エントリのプール名を指定します。「All」オプションにチェックを入れると、全てのプールのコンフリクトエントリを削除します。

「Find」ボタンをクリックして、指定条件に基づくエントリを検索 / 表示します。
「Clear」ボタンをクリックして、指定条件に基づくエントリを削除します。

DHCP Server Statistic（DHCP サーバ統計）

DHCP サーバの統計情報を表示します。

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

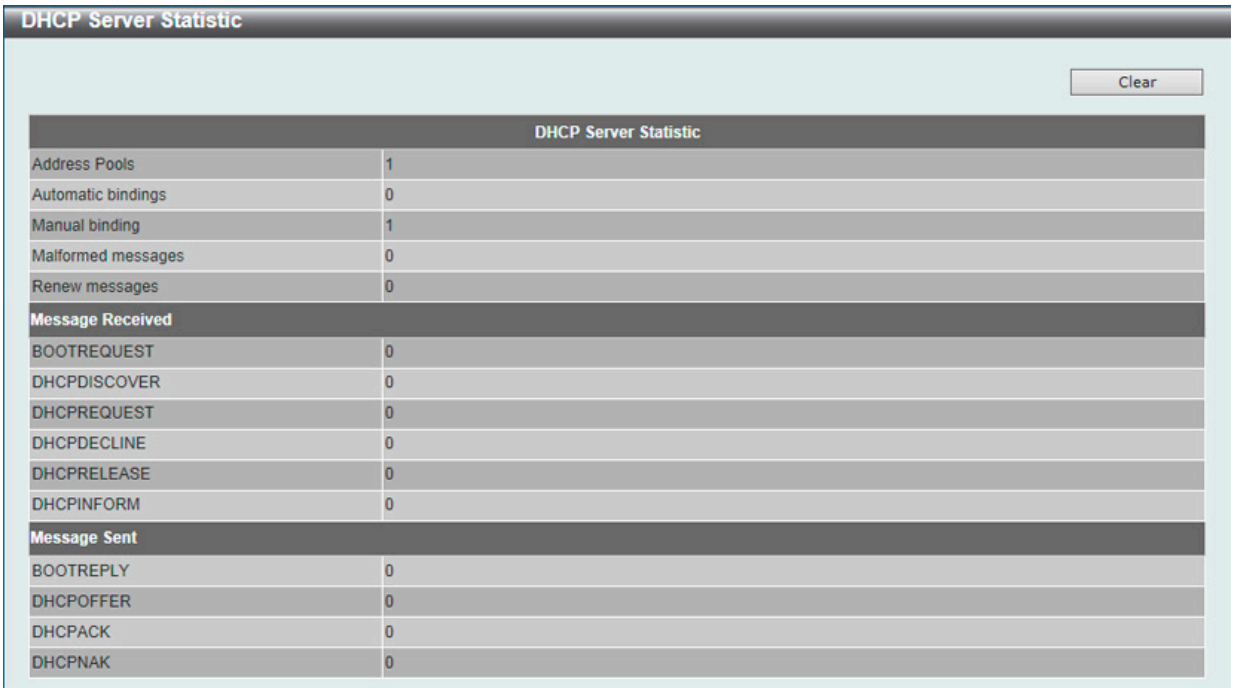


図 7-36　DHCP Server Statistic 画面

「Clear」ボタンをクリックして、エントリを削除します。

DHCPv6 Server（DHCPv6 サーバ設定）

Management > DHCP > DHCPv6 Server

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

DHCPv6 プールの作成および設定を行います。

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

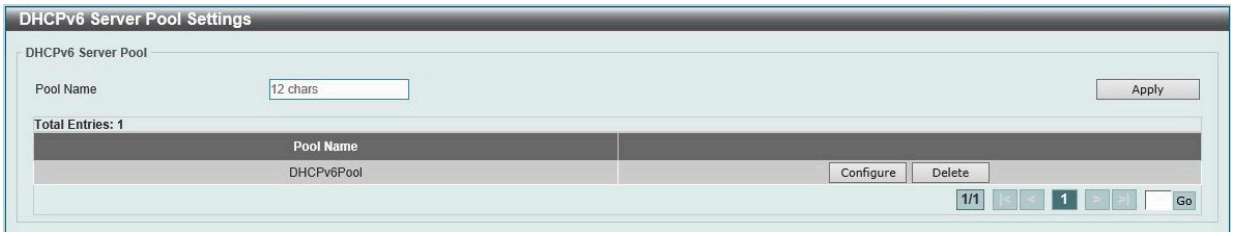


図 7-37　DHCPv6 Server Pool Settings 画面

以下の項目が表示されます。

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

「Apply」ボタンをクリックして、入力した情報に基づいて新しいエントリを追加します。
「Delete」ボタンをクリックして、エントリを削除します。

テーブル情報が複数ページ存在する場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

エントリの編集

「Configure」ボタンをクリックすると、以下の画面が表示されます。

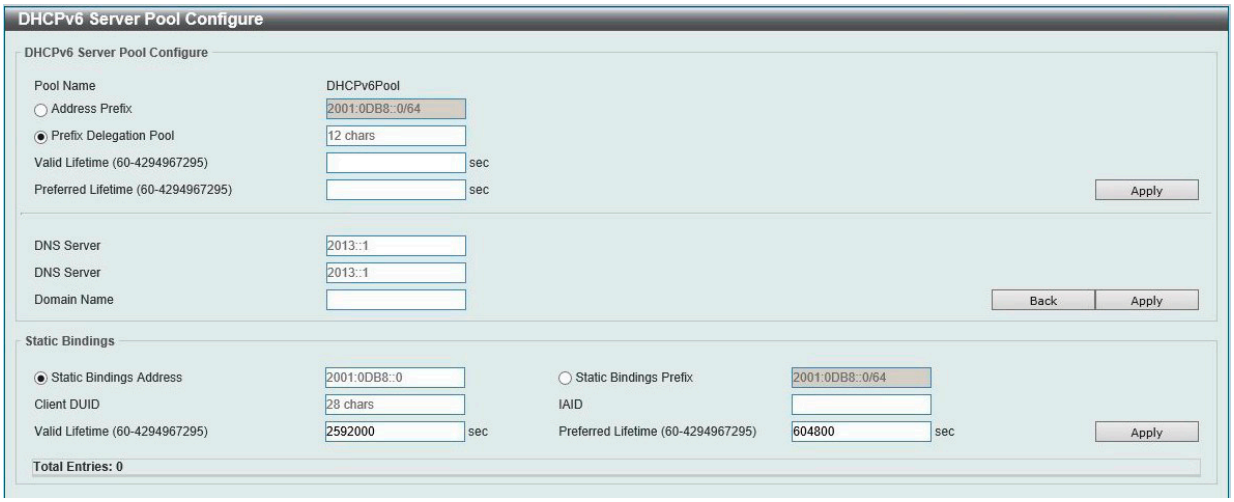


図 7-38　DHCPv6 Server Pool Settings (Configure) 画面

以下の項目が表示されます。

項目	説明
DHCPv6 Server Pool Configure	
Address Prefix	DHCPv6 サーバプール IPv6 ネットワークアドレスとプレフィクス長を入力します。（例：2015::0/64）
Prefix Delegation Pool	DHCPv6 サーバプールプレフィクス委任名を 12 字以内で入力します。
Valid Lifetime	IPv6 アドレスが有効な状態を維持する時間を入力します。「Preferred Lifetime 」よりも大きい値である必要があります。 • 設定可能範囲：60-4294967295(秒)
Preferred Lifetime	IPv6 アドレスが preferred-lifetime（推奨有効期限）状態を維持する時間を入力します。 • 設定可能範囲：60-4294967295（秒）
DNS Server	DHCPv6 クライアントに割り当てる DNS サーバの IPv6 アドレスを入力します。
Domain Name	DHCPv6 クライアントに割り当てるドメイン名を指定します。
Static Bindings	
Static Bindings Address	指定クライアントに割り当てるスタティックバインディング IPv6 アドレスを入力します。
Static Bindings Prefix	スタティックバインディング IPv6 ネットワークアドレスとプレフィクスを入力します。

項目	説明
Client DUID	デバイスの DUID を入力します。（28 文字以内）
IAID	「Identity Association Identifier」(IAID/IA 識別子) を入力します。これは、クライアントに割り当てられる一時的ではないアドレス（IANA）の集合体を識別します。
Valid Lifetime	IPv6 アドレスが有効な状態を維持する時間を入力します。 • 設定可能範囲：60-4294967295（秒） • 初期値：2592000（秒）（30 日）
Preferred Lifetime	IPv6 アドレスが preferred-lifetime（推奨有効期限）状態を維持する時間を入力します。 • 設定可能範囲：60-4294967295（秒） • 初期値：604800（秒）（7 日）

設定を変更する際は、必ず該当セクションの「Apply」ボタンをクリックし、設定内容を適用してください。
「Back」をクリックすると前のページに戻ります。

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

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

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



図 7-39　DHCPv6 Server Excluded Address 画面

以下の項目が表示されます。

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

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Delete」ボタンをクリックして、エントリを削除します。

DHCPv6 Server Binding（DHCPv6 サーババインディング）

DHCPv6 バインディング情報を参照、削除します。

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

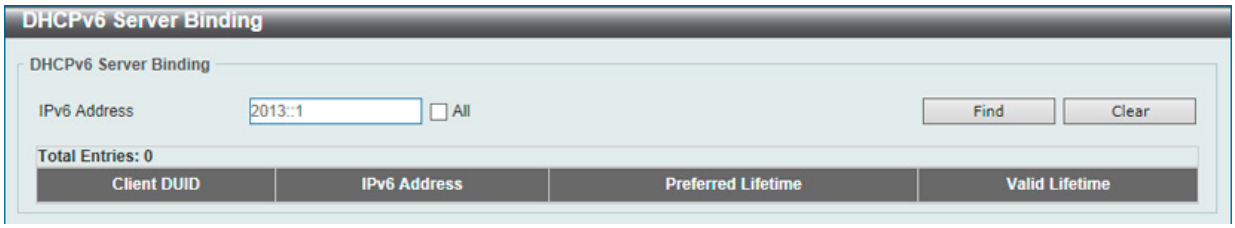


図 7-40　DHCPv6 Server Binding 画面

以下の項目が表示されます。

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

「Find」ボタンをクリックして、指定条件に基づくエントリを検索 / 表示します。
「Clear」ボタンをクリックして、指定条件に基づくエントリを削除します。

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

インタフェースごとに DHCPv6 サーバ状態を表示および設定します。

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

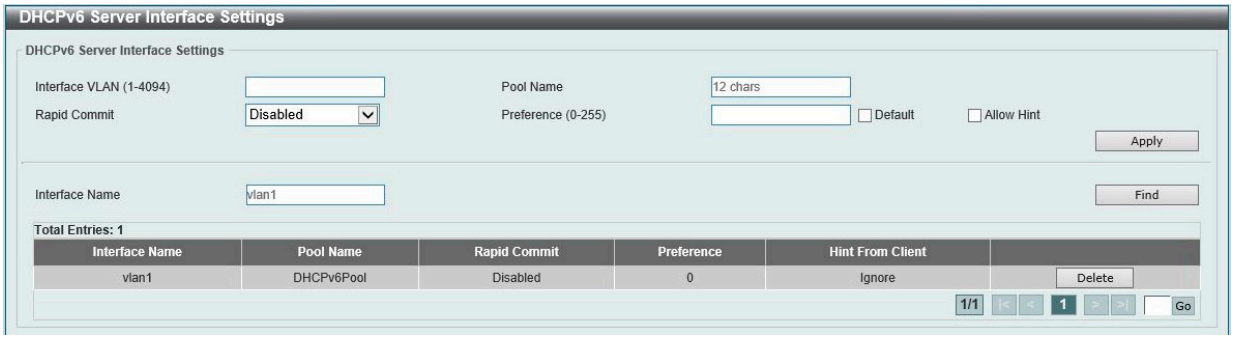


図 7-41　DHCPv6 Server Interface Settings 画面

以下の項目が表示されます。

項目	説明
Interface VLAN	インタフェース VLAN を指定します。 • 設定可能範囲：1-4094
Pool Name	DHCPv6 サーバプール名を入力します。（12 文字以内）
Rapid Commit	2 メッセージ交換を有効 / 無効に設定します。 • 初期値：「Disabled」（無効）
Preference	Preference 値を指定します。「Allow Hint」を選択するとヒントが表示されます。
Interface Name	インタフェース名を入力します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Find」ボタンをクリックして、指定条件に基づくエントリを検索 / 表示します。
「Delete」ボタンをクリックして、エントリを削除します。

テーブル情報が複数ページ存在する場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

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

DHCPv6 サーバ状態を表示します。

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

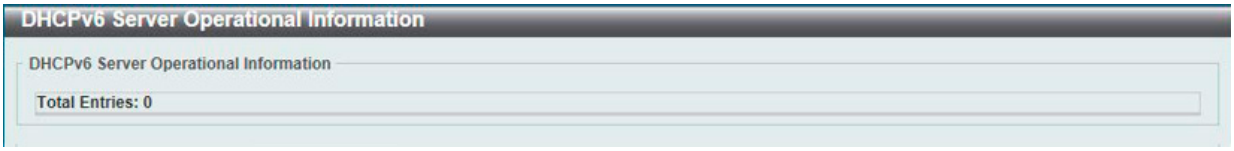


図 7-42　DHCPv6 Server Operational Information 画面

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。

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

DHCP リレーグローバル機能を有効にします。

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

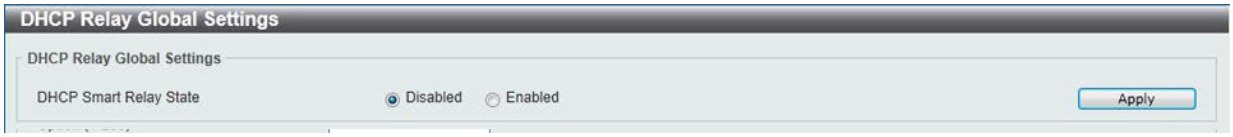


図 7-43　DHCP Relay Global Settings 画面

以下の項目が使用されます。

項目	説明
DHCP Smart Relay State	「Enabled」または「Disabled」を選択し、スイッチ上で DHCP スマートリレーを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Disabled」です。

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

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

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

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

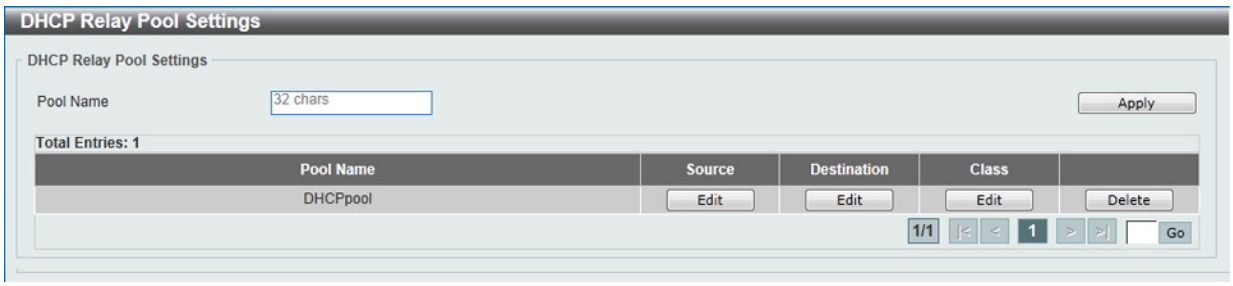


図 7-44　DHCP Relay Pool Settings 画面

以下の項目が使用されます。

項目	説明
Pool Name	32 文字以内でプール名を指定します。

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

エントリの削除を行う場合
「Delete」をクリックします。

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。

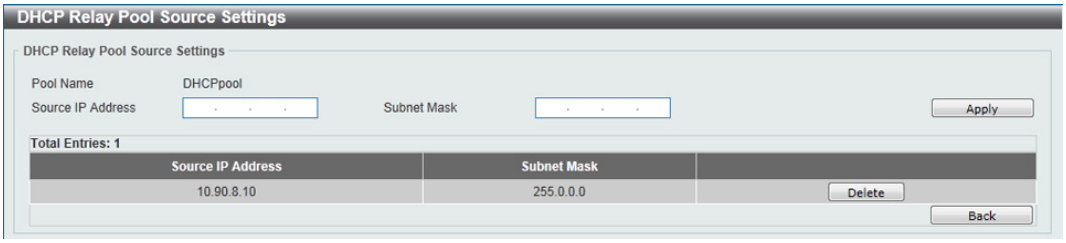


図 7-45　DHCP Relay Pool Source Settings 画面

以下の項目が使用されます。

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

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
エントリの削除を行う際は「Delete」をクリックします。
「Back」をクリックすると前の画面へ戻ります。

「Destination」の編集を行う場合

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

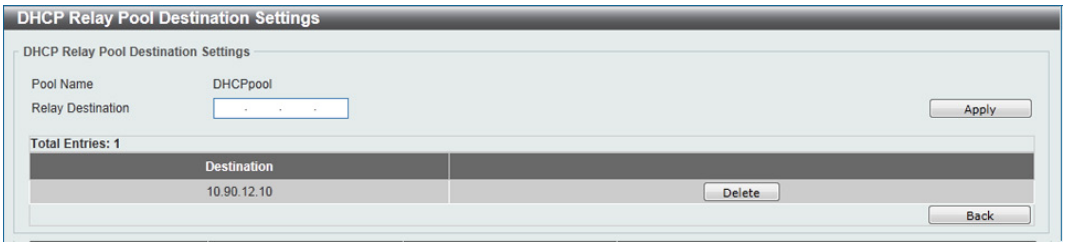


図 7-46　DHCP Relay Pool Destination Settings 画面

以下の項目が使用されます。

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

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
エントリの削除を行う際は「Delete」をクリックします。
「Back」をクリックすると前の画面へ戻ります。

「Class」の編集を行う場合

「Class」下の「Edit」をクリックします。以下の画面が表示されます。

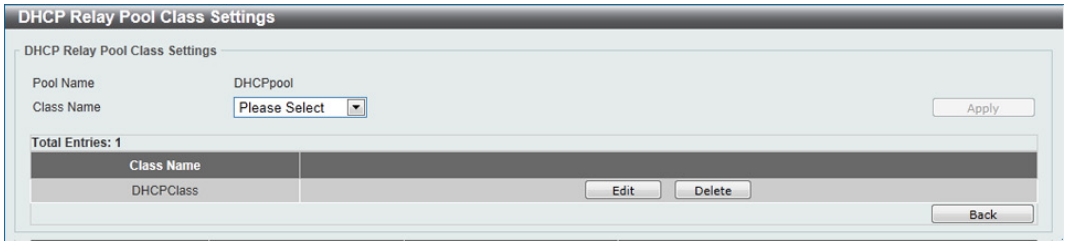


図 7-47　DHCP Relay Pool Class Settings 画面

以下の項目が使用されます。

項目	説明
Class Name	DHCP クラス名を選択します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
エントリの削除を行う際は「Delete」をクリックします。
「Back」をクリックすると前の画面へ戻ります。

クラス名の横の「Edit」をクリックすると以下の画面が表示されます。

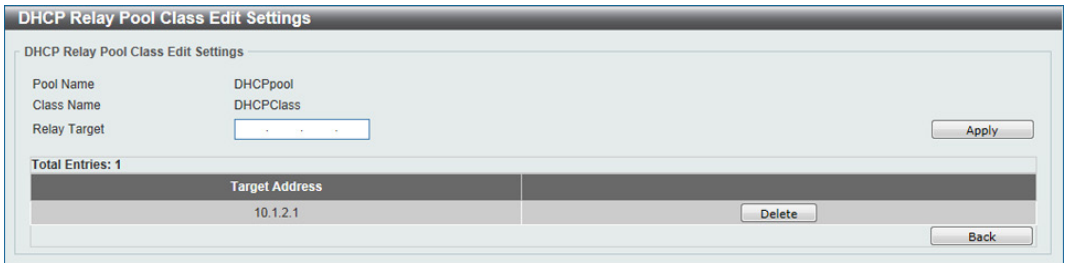


図 7-48　DHCP Relay Pool Class Settings 画面

以下の項目が使用されます。

項目	説明
Relay Target	DHCP クラスで設定したオプションの方式とマッチするパケットをリレーする DHCP リレーターゲットを入力します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
エントリの削除を行う際は「Delete」をクリックします。
「Back」をクリックすると前の画面へ戻ります。

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

DHCP リレー情報の表示、設定を行います。

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

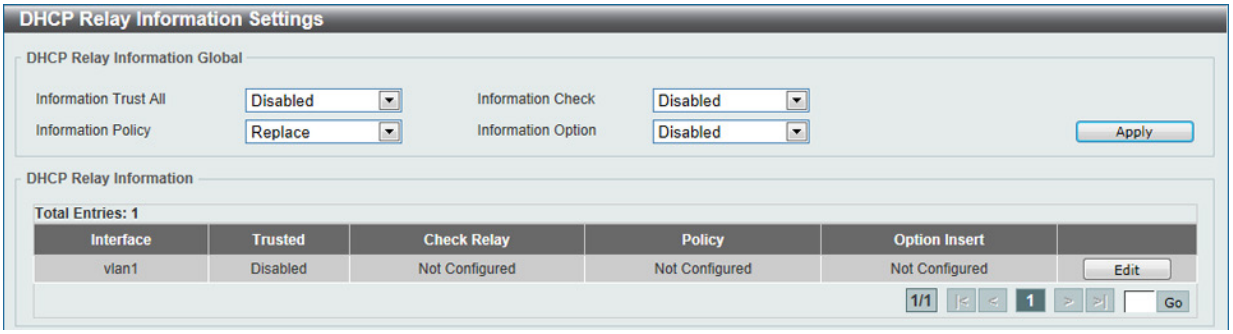


図 7-49　DHCP Relay Information Settings 画面

以下の項目が使用されます。

項目	説明
Information Trust All	DHCP リレーエージェントがすべてのインタフェースの IP DHCP リレー情報を信頼するようにするかを有効化 / 無効化します。
Information Check	DHCP リレーエージェントが受信した DHCP リプライパケットのリレーエージェント情報オプションを検証して削除するかを有効化 / 無効化します。
Information Policy	DHCP リレーエージェントの Option82 再転送ポリシーを「Keep」「Drop」「Replace」から選択します。初期値は「Replace」です。 • Keep - リレーオプションを保持している DHCP リクエストパケットをそのまま保持し、直接 DHCP サーバにリレーします。 • Drop - リレーオプションを保持しているパケットを破棄します。 • Replace - リレーオプションを保持している DHCP リクエストパケットに新しいオプションを入れ替えます。
Information Option	DHCP リクエストパケットのリレーの間にリレーエージェント情報（Option82）を挿入を有効 / 無効に設定します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Edit」をクリックして対応するインタフェースの編集を行うことができます。
設定エントリページが複数ページある場合、ページ番号を指定して「Go」をクリックすると当該のページへ移動します。

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

DHCP 情報フォーマットの表示、設定を行います。

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

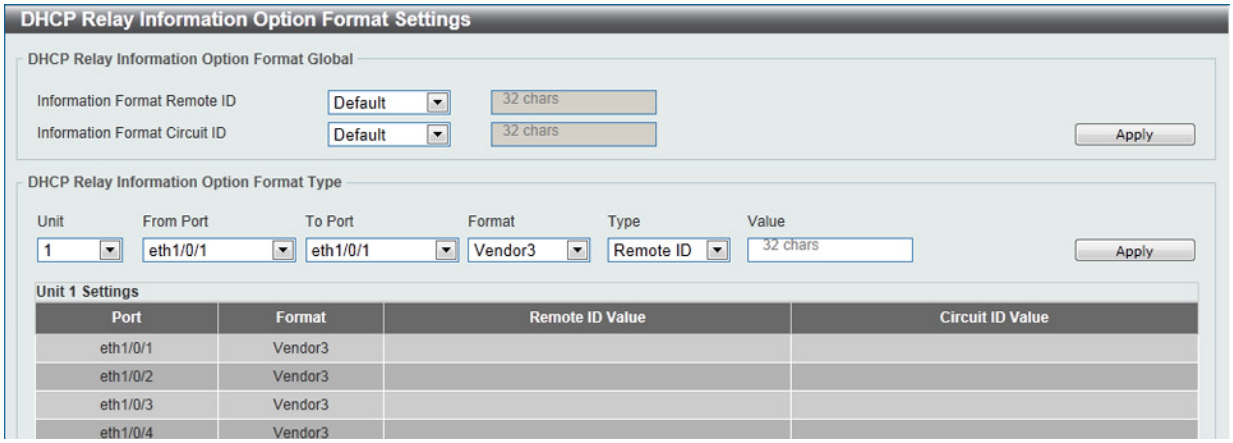


図 7-50　DHCP Relay Information Option Format Settings 画面

以下の項目が使用されます。

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。 • 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。 • Expert UDF - Expert UDF リモート ID を使用します。本オプションを指定した場合、スタンドアロンのユニットフォーマットを選択します。
Information Format Circuit ID	「DHCP information circuit ID」のサブオプションを選択します。 • Default - 初期値のサーキット ID を使用します。 • User Define - ユーザ定義のサーキット ID を使用します。32 文字以内。 • Vendor1 - サーキット ID 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。 • Expert UDF - Expert UDF サーキット ID を使用します。本オプションを指定した場合、スタンドアロンのユニットフォーマットを選択します。
DHCP Relay Information Option Format Type	
Unit	設定するユニットを選択します。
From Port / To Port	ポートの始点 / 終点を設定します。
Format	「DHCP information circuit ID」のフォーマットを選択します。「Vendor3」または「Expert UDF」を選択できます。
Type	「DHCP information circuit ID」の種類を選択します。「Remote ID」「Circuit ID」を選択できます。
Value	ベンダ定義の文字列を入力します。

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

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

VLAN、またはグループ VLAN のローカルリレー設定を行います。

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

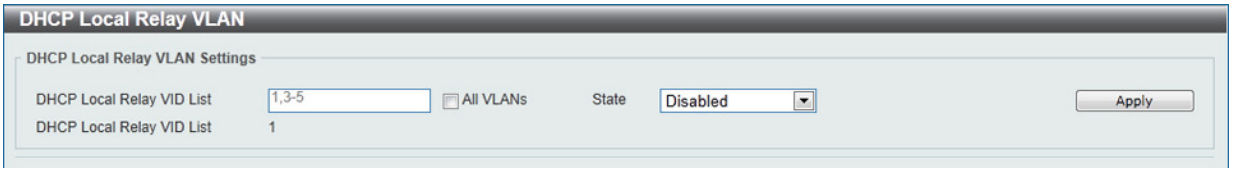


図 7-51　DHCP Local Relay VLAN 画面

以下の項目が使用されます。

項目	説明
DHCP Local Relay VID List	DHCP ローカルリレーを適用する VLAN ID を入力します。「All VLANs」にチェックを入れるとすべての VLAN を選択します。
State	指定の VLAN の DHCP ローカルリレーを有効 / 無効に設定します。

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

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 リレーリモート ID を設定します。

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

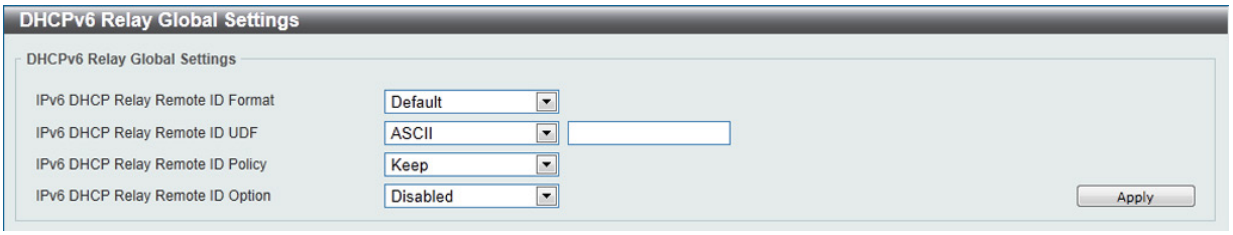


図 7-52　DHCPv6 Relay Global Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
IPv6 DHCP Relay Remote ID Format	リモート ID のサブタイプを指定します。 「Default」「CID With User Define」「User Define」から選択します。
IPv6 DHCP Relay Remote ID UDF	リモート ID のユーザ定義項目 (UDF) の入力形式 を選択します。「None」「ASCII」「Hex」から選択します。 • ASCII -「ASCII」文字列で入力します。最大 128 文字まで入力可能です。 • HEX - 16 進数文字列で入力します。最大 256 文字まで入力可能です。
IPv6 DHCP Relay Remote ID Policy	DHCPv6 リレーエージェントのオプション 37 フォワーディングポリシーを選択します。 • Drop - DHCP クライアントから受信したパケット内に既にオプション 37 リレー情報があった場合はそのパケットを削除します。 • Keep - DHCP クライアントから受信したパケット内の既存のオプション 37 リレー情報を保持したまま、DHCPv6 サーバへリレーします。
IPv6 DHCP Relay Remote ID Option	DHCP IPv6 リクエストパケットのリレーの間にリレーエージェントリモート ID オプション 37 を挿入を有効 / 無効に設定します。

「Apply」ボタンをクリックし、設定を適用します。

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

DHCPv6 リレーインタフェース設定の表示と設定を行います。

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

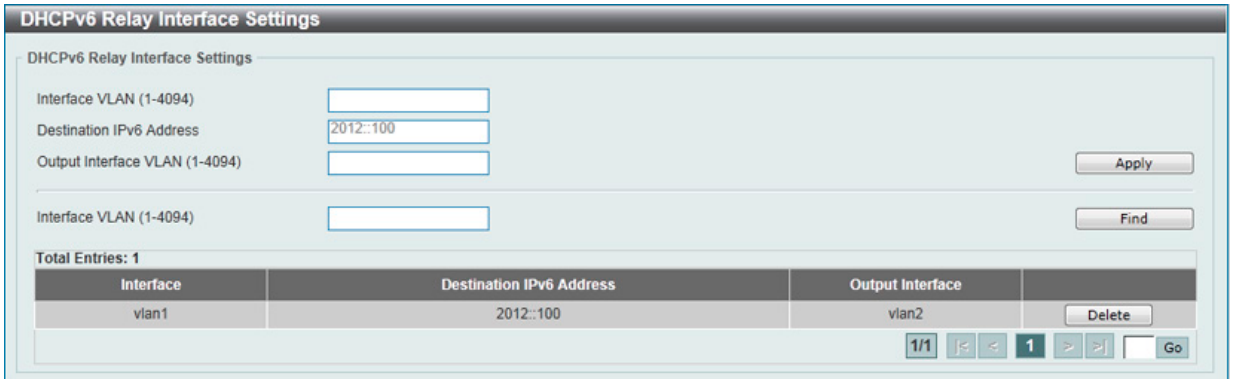


図 7-53　DHCPv6 Relay Interface Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
Interface VLAN	DHCPv6 リレーの VLAN を 1 から 4094 の間で指定します。
Destination IPv6 Address	DHCPv6 リレーの宛先アドレスを入力します。
Output Interface VLAN	リレー先への出力インタフェース VLAN を入力します。

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

DHCP Auto Configuration（DHCP 自動設定）

DHCP 自動設定機能の設定を行います。

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

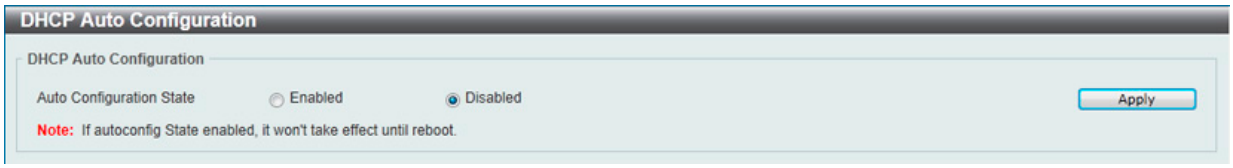


図 7-54　DHCP Auto Configuration 画面

以下の項目を使用して設定、表示を行います。

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

「Apply」ボタンをクリックし、設定を適用します。

DNS（ドメインネームシステム）

コンピュータのユーザは外部と接続するコンピュータの名前として、テキスト形式のものを使用する方が使い勝手が良いといえます。コンピュータ自身には 32 ビットの IP アドレスが必要です。このため、ネットワークデバイスのテキスト形式の名前（ドメイン名）とそれに対応する IP アドレスのデータベースがどこかに保持される必要があります。

DNS（Domain Name System）は、そのようなドメイン名と IP アドレスの関連付けをインターネット経由で行い、イントラネットでもこれが使用されるようになってきました。異なるサブネットを通して通信する DNS サーバの間には、中継を行うために DNS リレー機能が必要になります。DNS サーバは IP アドレスにより識別します。

ドメイン名とアドレスのマッピング

ドメイン名とアドレスの関連付けはネームサーバというプログラムにより行われます。クライアントプログラムはネームリゾルバと呼ばれます。ネームリゾルバは、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。

DNS サーバ群は、ドメイン名に対応した階層構造になっています。1 台のサーバは通常 1 つのネットワークにドメイン名を持ち、これが上位に位置するルート DNS サーバ（通常 ISP が管理）に接続を行います。

ドメイン名の解決

ドメイン名の解決はその都度ネームサーバに問い合わせる場合と、DNS にまとめて解決を求める場合があります。クライアントは、ドメイン名、必要な応答の種類、およびクエリを受信したサーバが名前の解決をできない場合に、DNS によってすべてのドメイン名の解決を行うか、または次の DNS サーバのアドレスのみを返せばよいのかを指定したコードを含むクエリを作成します。

DNS サーバがクエリを受信すると、その名前がサブドメイン中に存在するかどうかをチェックします。存在していればサーバは名前を解決し、クエリへの応答としてクライアントに返します。自分で解決できない場合は、クライアントが要求する方法の名前解決を実行します。 1 つは再帰的解決と呼ばれる方法で、サーバは名前の解決が完了するまで、他の DNS サーバと連絡を取り合います。もう 1 つは反復的解決と呼ばれる方法で、DNS サーバが自分で解決できない場合は、クライアントが連絡すべき次の DNS サーバのアドレスのみを返します。

各 DNS クライアントは、最低 1 台の DNS サーバに連絡可能で、各 DNS サーバは最低 1 台のルートサーバに連絡する手段を持たなければなりません。

ドメインネームサービスを行うデバイスのアドレスは、DHCP または BOOTP サーバから得る場合と、初期設定時に手動で OS に設定する場合があります。

DNS Global Settings（DNS グローバル設定）

DNS のグローバル設定を行います。

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

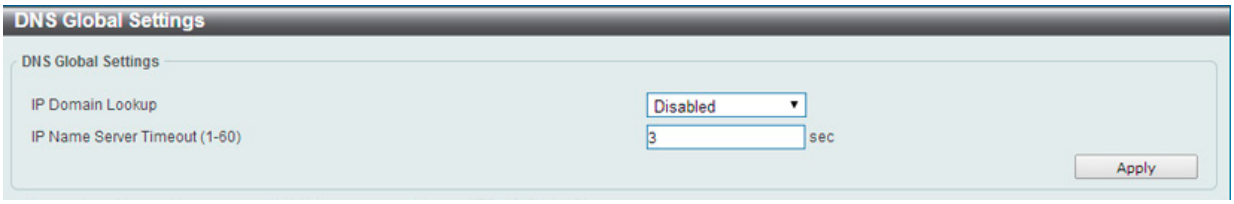


図 7-55　DNS Global Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
IP Domain Lookup	ドメイン名の解決について DNS の実行を有効 / 無効にします。
IP Name Server Timeout	指定ドメイン名サーバからの応答に対する最大待機時間を指定します。1 から 60（秒）で指定できます。

「Apply」ボタンをクリックし、設定を適用します。

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

スイッチにドメインネームサーバの IP アドレスを設定します。

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

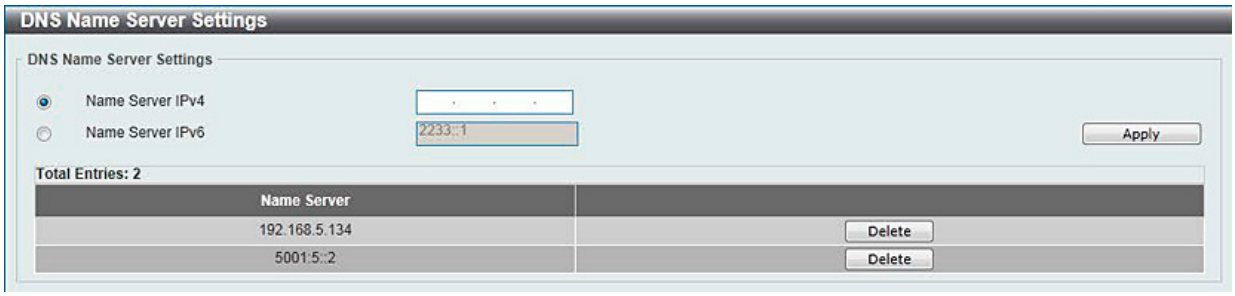


図 7-56　DNS Name Server Settings 画面

以下の項目を使用して設定、表示を行います。

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

「Apply」ボタンをクリックし、設定を適用します。

エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。

DNS Host Settings（DNS ホスト名設定）

ホストテーブル内に、ホスト名と IP アドレスのスタティックマッピングエントリを設定します。

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



図 7-57　DNS Host Settings 画面

以下の項目を使用して設定、表示を行います。

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

「Apply」ボタンをクリックし、設定を適用します。

エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。

NTP（ネットワークタイムプロトコル）

スイッチの時刻を同期するための通信プロトコルの設定を行います。

NTP Global Settings（NTP グローバル設定）

NTP のグローバル設定を行います。

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

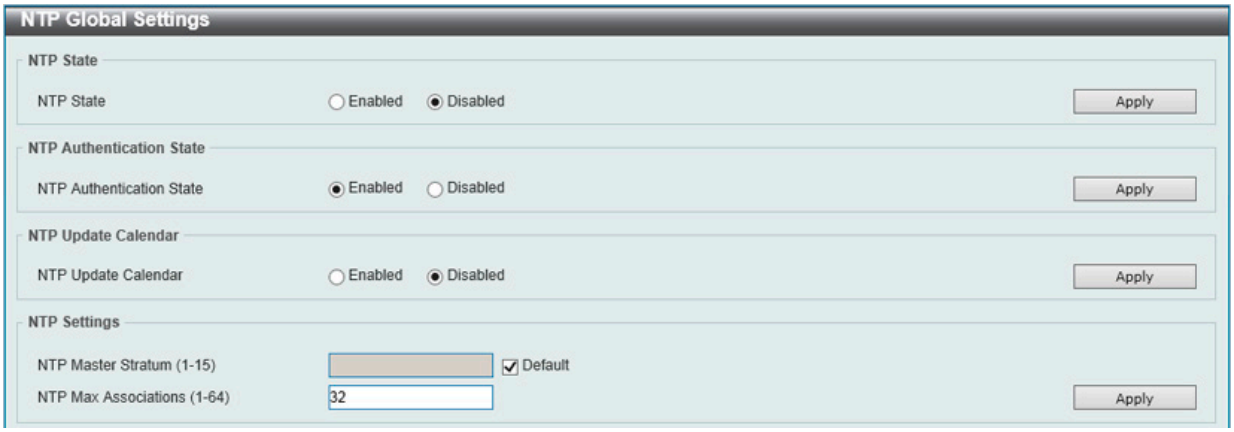


図 7-58　NTP Global Settings 画面

以下の項目を使用して設定、表示を行います。

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

「Apply」ボタンをクリックし、設定を適用します。

NTP Server Settings（NTP サーバ設定）

NTP サーバの設定を行います。

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

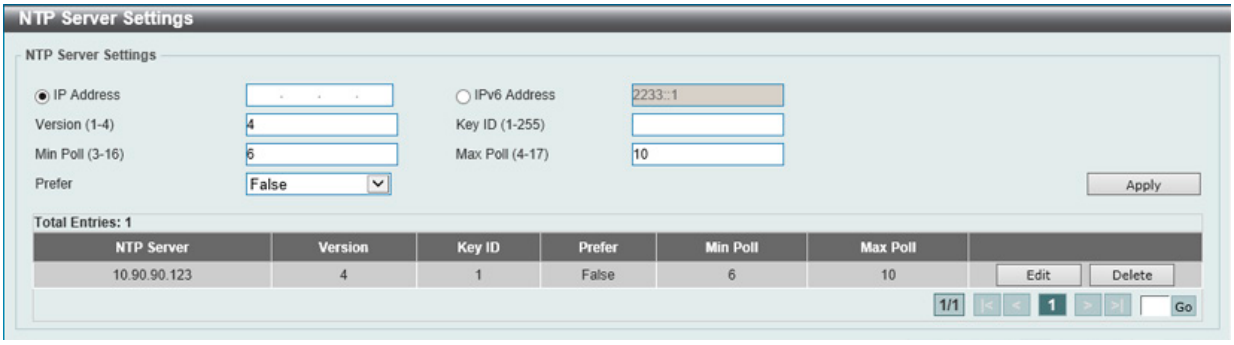


図 7-59　NTP Server Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
IP Address	NTP サーバの IPv4 アドレスを指定します。
IPv6 Address	NTP サーバの IPv6 アドレスを指定します。
Version	NTP サーバのバージョンを指定します。1 から 4 までで指定します。
Key ID	認証キー ID を指定します。1 から 255 まで指定します。
Min Poll	NTP メッセージ送信の最小ポーリング間隔を指定します。3 から 16（秒）で指定します。
Max Poll	NTP メッセージ送信の最大ポーリング間隔を指定します。4 から 17（秒）で指定します。
Prefer	対象のサーバを優先するか否かを選択します。True または False から指定します。

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

NTP Peer Settings（NTP ピア設定）

NTP のピア設定を行います。

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

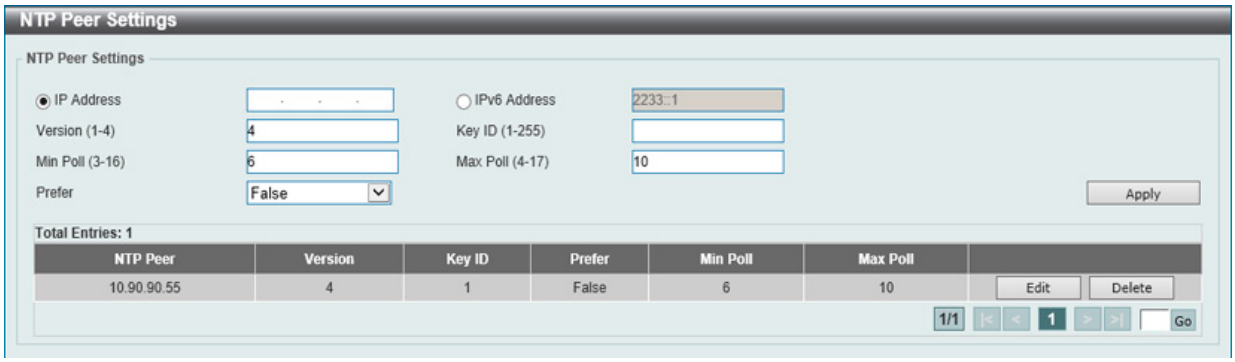


図 7-60　NTP Peer Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
IP Address	NTP ピアの IPv4 アドレスを指定します。
IPv6 Address	NTP ピアの IPv6 アドレスを指定します。
Version	NTP ピアのバージョンを指定します。1 から 4 までで指定します。
Key ID	認証キー ID を指定します。1 から 255 まで指定します。
Min Poll	最小ポーリング間隔を指定します。3 から 16（秒）で指定します。
Max Poll	最大ポーリング間隔を指定します。4 から 17（秒）で指定します。
Prefer	対象のピアを優先するか否かを選択します。「True」または「False」から指定します。

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

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

NTP のアクセスグループ設定を行います。

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

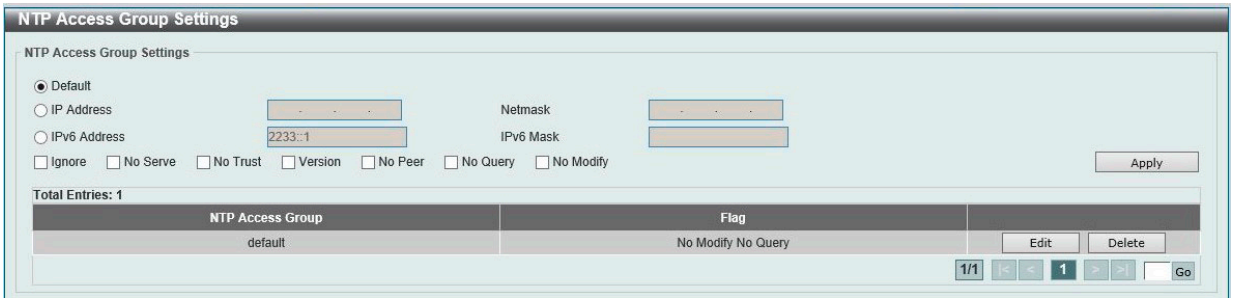


図 7-61　NTP Access Group Settings 画面

以下の項目を使用して設定、表示を行います。

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

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

NTP Key Settings（NTP 鍵設定）

NTP の鍵設定を行います。

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

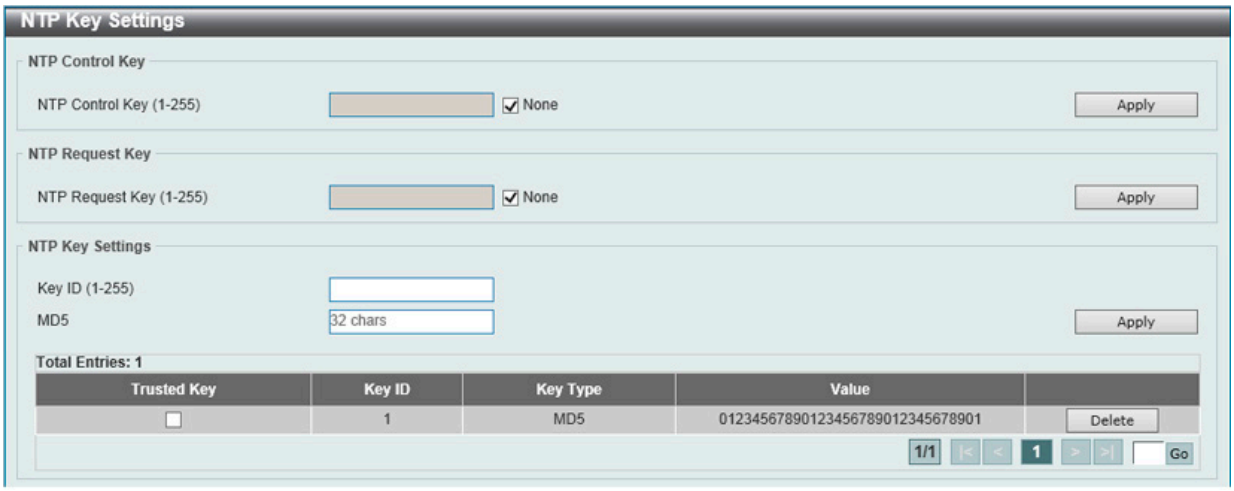


図 7-62　NTP Key Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
NTP Control Key	NTP コントロールキー（制御鍵）を 1 から 255 で指定します。「None」を選択すると NTP コントロールキーは使用しません。
NTP Request Key	NTP リクエストキー（要求鍵）を 1 から 255 で指定します。「None」を選択すると NTP リクエストキーは使用しません。
Key ID	NTP キー ID（鍵番号）を 1 から 255 で指定します。
MD5	MD5 NTP キー（鍵番号）を指定します。32 文字まで指定可能です。

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

NTP Interface Settings（NTP インタフェース設定）

NTP のインタフェース設定を行います。

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



図 7-63　NTP Interface Settings 画面

以下の項目を使用して設定、表示を行います。

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

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

NTP Associations（NTP アソシエーション）

NTP アソシエーションを表示します。

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

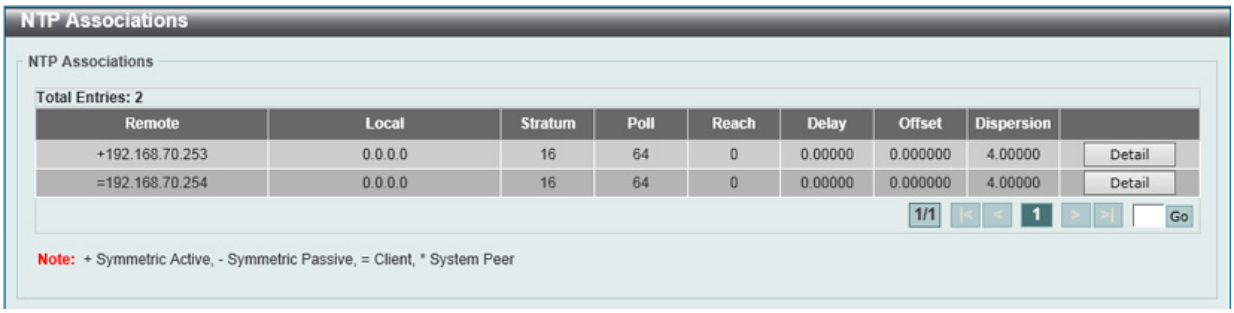


図 7-64　NTP Assosiations 画面

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

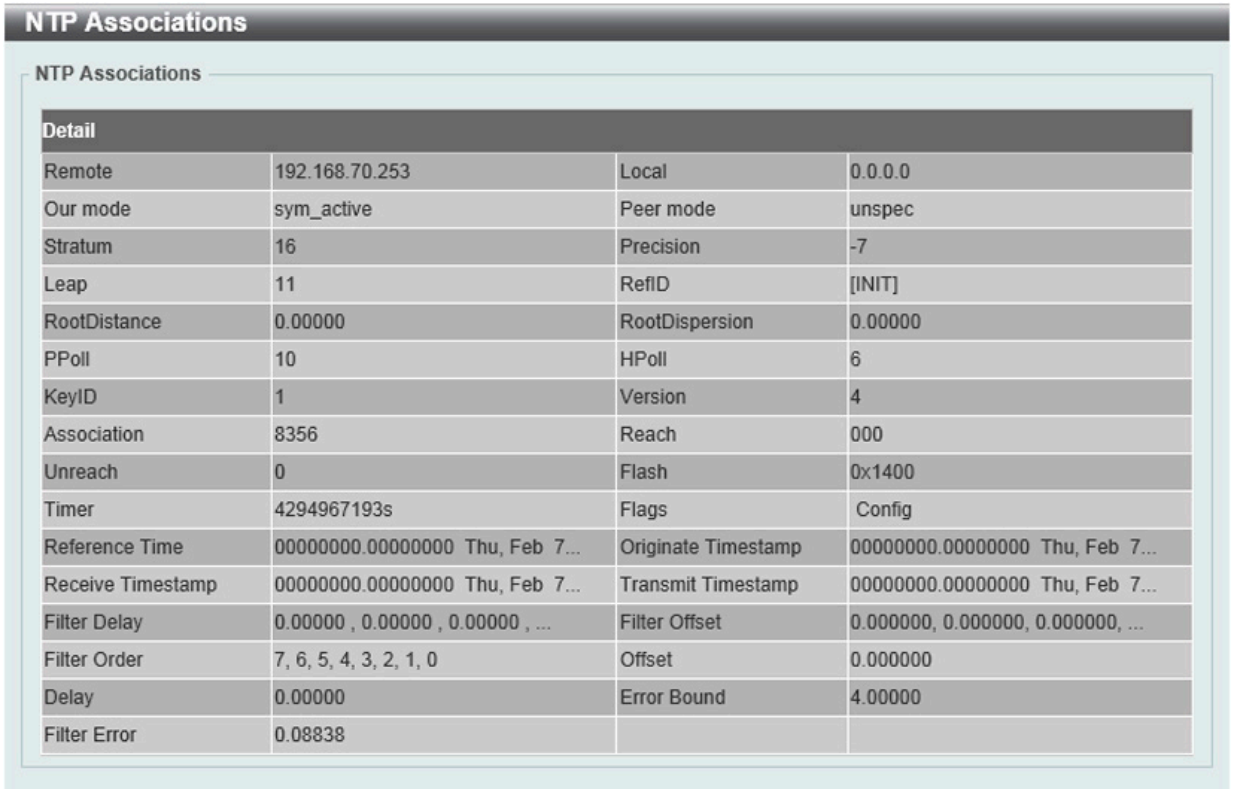


図 7-65　NTP Assosiations - Detail 画面

NTP Status（NTP ステータス）

NTP ステータスを表示します。

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

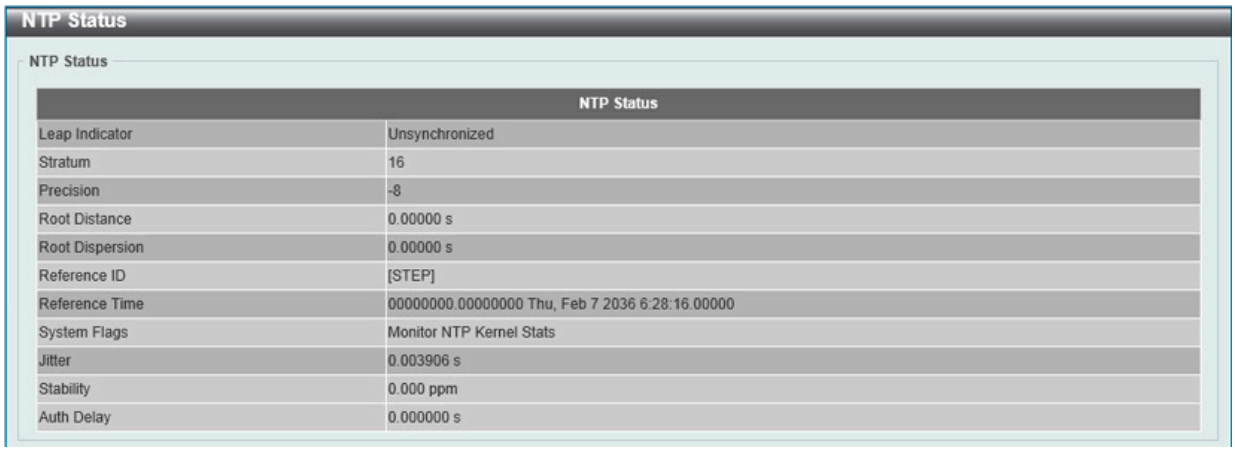


図 7-66　NTP Status 画面

IP Source Interface（IP ソースインタフェース）

IP ソースインタフェースを設定します。

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

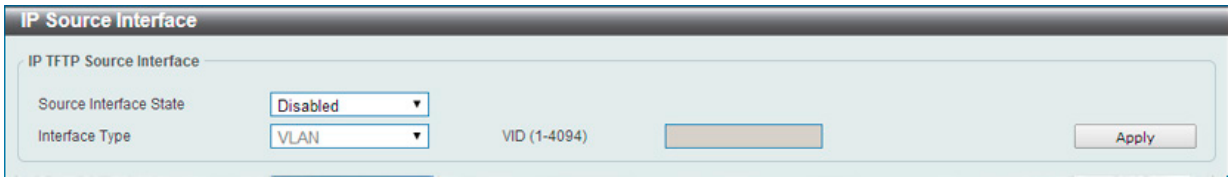


図 7-67　IP Source Interface 画面

以下の項目を使用して設定、表示を行います。

項目	説明
Source Interface State	ソースインタフェースをグローバルに有効 / 無効にします。
Interface Type	インタフェースの種類を選択します。「VLAN」のみ指定可能です。
VID (1-4094)	VLAN ID を指定します。1 から 4094 まで指定可能です。

「Apply」ボタンをクリックし、設定を適用します。

File System（ファイルシステム）

フラッシュファイルシステムを使用する理由

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

本スイッチに採用されているフラッシュファイルシステム

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

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

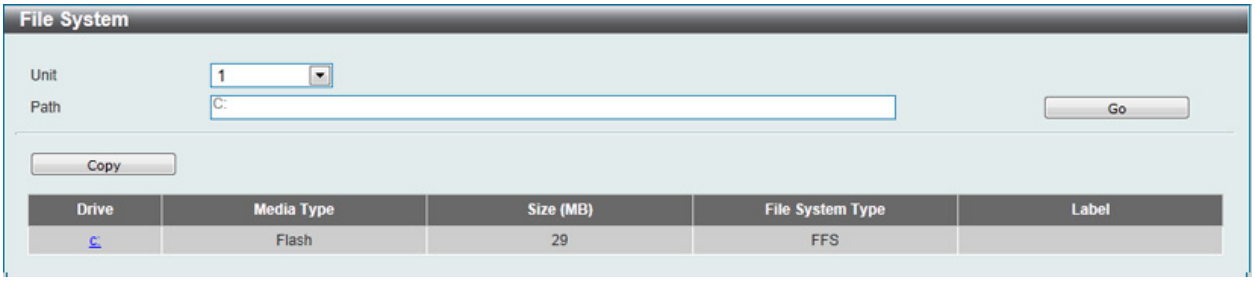


図 7-68　File System 画面

以下の項目を使用して設定、表示を行います。

項目	説明
Unit	設定するユニットを選択します。
Path	パスの文字列を入力します。

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

「C:」リンクをクリックした後、次の画面が表示されます。

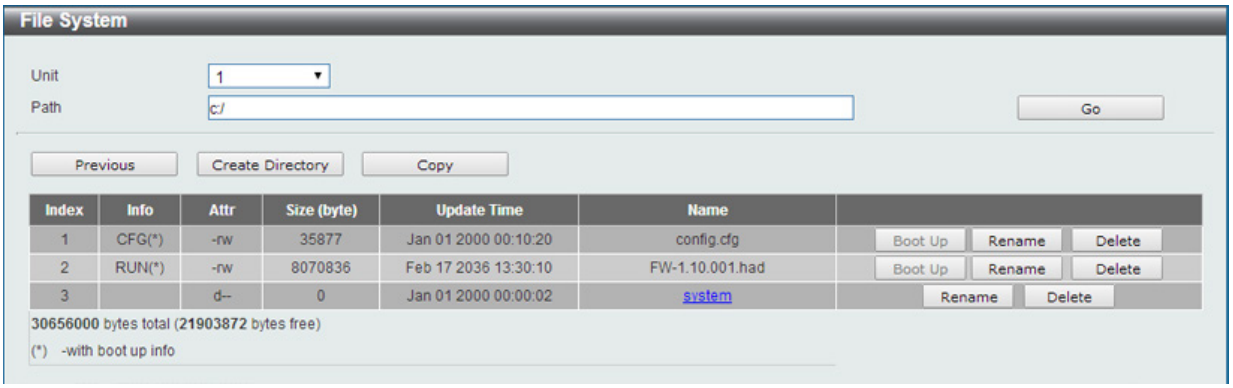


図 7-69　Flash File System Setting – Search for Drive 画面

以下の項目を使用して設定、表示を行います。

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

ファイルのコピー

1. 「Copy」ボタンをクリックすると、以下の画面が表示されます。

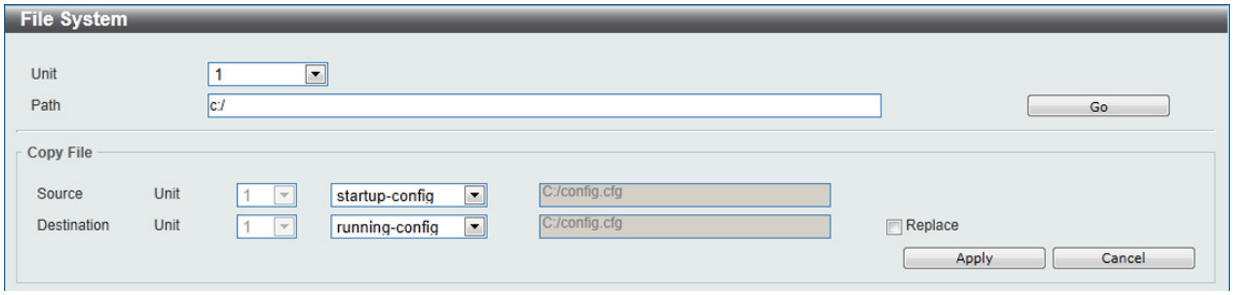


図 7-70　Flash File System Settings 画面 - Copy

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

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

Physical Stacking（物理スタッキング）

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

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

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

以下は、SFP+ モジュールに接続された光ファイバケーブル、または SFP+ ダイレクトアタッチケーブルを使用した「Duplex Chain」構成での物理スタック図です。

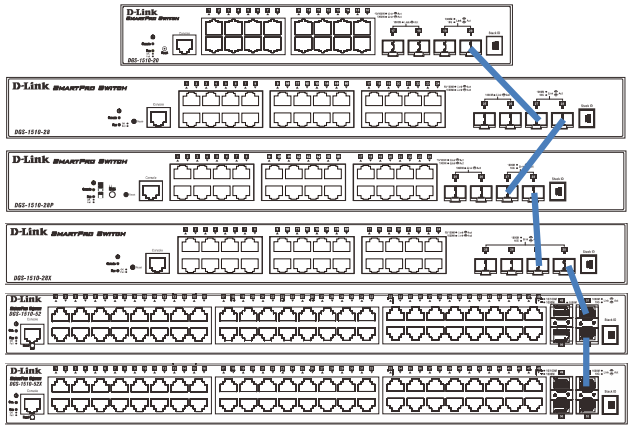


図 7-71　Duplex Chain でスタックされているスイッチ前面

以下は、SFP+ モジュールに接続された光ファイバケーブル、または SFP+ ダイレクトアタッチケーブルを使用した「Duplex Ring」構成での物理スタック図です。

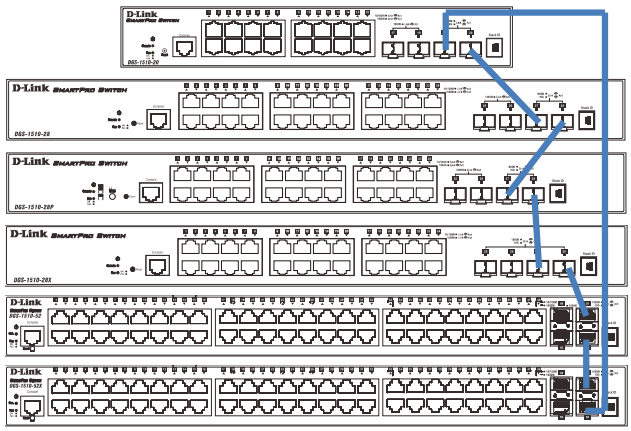


図 7-72　Duplex Ring でスタックされているスイッチ画面

スタック内のスイッチ役割

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

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

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

- スレーブ
  スレーブスイッチは、プライマリマスタまたはバックアップマスタではないスイッチスタックの残りのスイッチです。プライマリマスタおよびバックアップマスタが故障、またはスタックから取り外される場合に、それらの機能を引き継ぎます。スレーブスイッチは、マスタに要求された操作を実行して、スタックとスタックトポロジにある近接スイッチの状態をモニタします。さらに、バックアップマスタがプライマリマスタになるとバックアップマスタのコマンドに従います。スレーブスイッチは、バックアップマスタがプライマリマスタに移行する場合や、バックアップマスタが故障、またはスイッチから取り外される場合に、セルフチェックを行い、自身がバックアップマスタになるかどうかを決定します。プライマリマスタとバックアップマスタの両方が故障、またはスイッチから取り外される場合、プライマリマスタになるかどうかを決定します。これらの役割はプライオリティによって決定され、プライオリティが同じである場合は、最も値の小さい MAC アドレスによって決定されます。

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

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

これらの処理が完了すると、スイッチスタックは通常の操作モードに入ります。

スタックスイッチのスワップ

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

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

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

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

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

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

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

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

デバイスのスタック機能を有効にし、設定します。

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

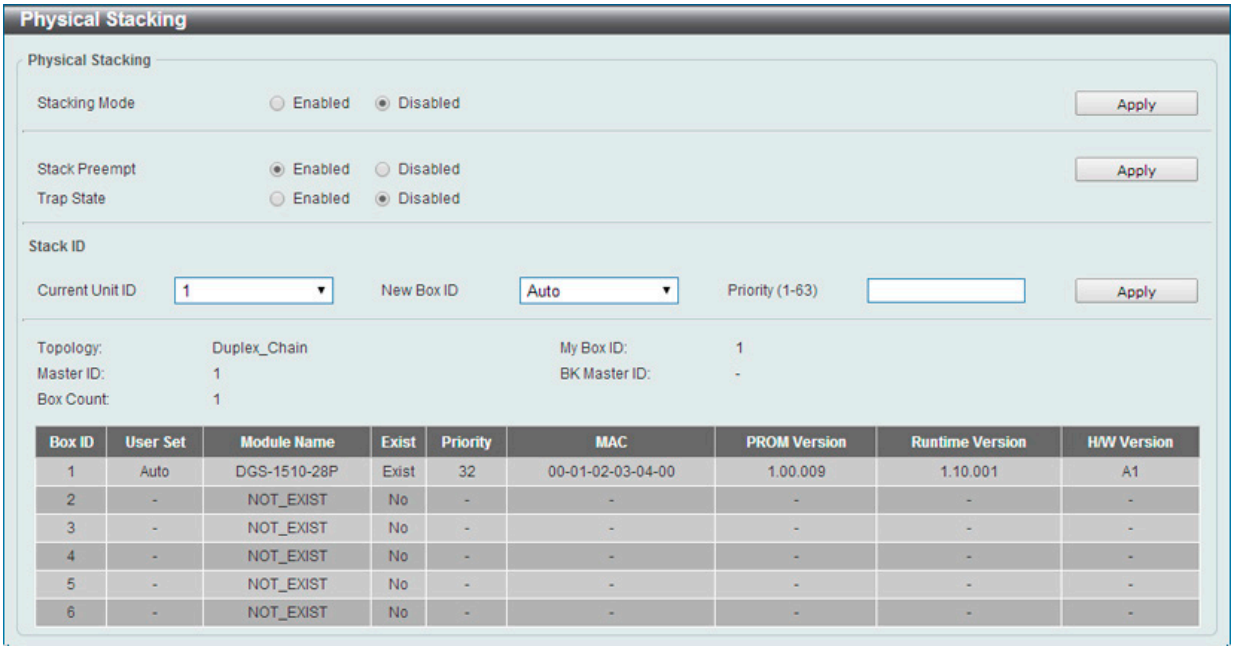


図 7-73　Physical Stacking 画面

設定および表示する項目は以下の通りです。

項目	説明
Stacking Mode	スタックを有効化 / 無効化します。初期値では「Disabled」(無効) になっています。
Stack Preempt	優先度の高いユニットが後から追加された場合の、マスタの役割の変更を有効 / 無効にします。
Trap State	スタック関連のトラップの送信を有効 / 無効にします。
Current Unit ID	スタックにおけるスイッチの現在のボックス番号を選択します。
New Box ID	「Current Unit ID」で選択したスタック内のスイッチに新しくボックス番号 (1-6) を指定します。「Auto」はスイッチスタック内のスイッチに自動的にボックス番号を割り当てます。
Priority (1-63)	スイッチの優先度番号を表示します。低い値ほど高いプライオリティを示します。スタック内で最も低い優先度番号を持つボックス（スイッチ）が、プライマリマスタです。プライマリマスタスイッチは、スイッチスタックにおけるアプリケーションを設定するために使用されます。

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

シングル IP マネジメント（SIM）設定

シングル IP マネジメント（SIM）の設定を行います。

シングル IP マネジメント（SIM）の概要

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

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

シングル IP マネジメント（SIM）のルールと動作

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

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

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

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

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

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

これらの役割には、さらに以下のルールが適用されます。

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

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

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

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

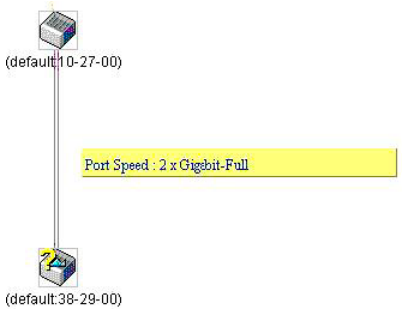
バージョン 1.61 へのアップグレード

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

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

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

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



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

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

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

Single IP Settings（シングル IP 設定）

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

1. Web インタフェースを使用してスイッチの SIM を有効にするためには **Management > Virtual Stacking (SIM) > Single IP Settings** の順にメニューをクリックし、以下の画面を表示します。

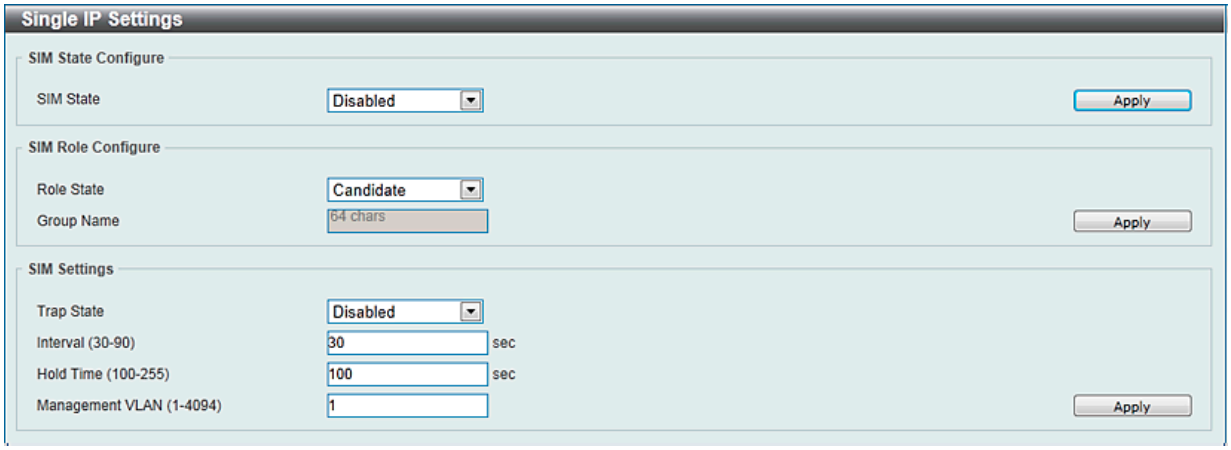


図 7-74　Single IP Settings 画面（CaS 無効状態）

2. プルダウンメニューを使用して、「SIM State」を「Enabled」（有効）、「Role State」を「Commander」に変更し、次に「Group Name」欄を指定します。
3. 「Apply」ボタンをクリックして、設定を有効にします。

以下の項目が使用できます。

項目	説明
SIM State	プルダウンメニューから「Enabled」（有効）または「Disabled」（無効）を選択します。「Disabled」を選択すると、スイッチのすべての SIM 機能が無効になります。初期値は「Disabled」です。
Role State	プルダウンメニューからスイッチの SIM での役割を選択します。以下の 2 つから選択できます。 • Candidate - Candidate Switch（CaS）は SIM グループメンバではありませんが、Commander スイッチに接続しています。本スイッチの SIM 機能の初期設定です。 • Commander - Commander Switch（CS）。ユーザは CS に他のスイッチを参加させて SIM グループを作成します。このオプションを選択すると、本スイッチは SIM 機能対象のスイッチとして設定されます。
Group Name	SIM グループ名を入力します。
Trap State	プルダウンメニューからトラップ送信の有効 / 無効を指定します。
Interval (30-90)	スイッチが Discovery パケットを送信する Discovery プロトコル送信間隔（秒）を設定します。CS スイッチに情報が送られてくると、接続する他のスイッチ（MS、CaS）の情報が CS に組み込まれます。値は 30-90（秒）の間から指定します。初期値は 30（秒）です。
Hold Time (100-255)	他のスイッチが「Discovery Interval」の間隔で送信してきた情報をスイッチが保持する時間（秒）を指定します。値は 100-255（秒）の間から指定します。初期値は 100（秒）です。
Management VLAN	IP マネジメントメッセージ VLAN ID を入力します。

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

スイッチを CS として登録すると、「Single IP Management」フォルダには 4 つのリンクが追加され、Web を使用した SIM 設定が続けられるようになります。追加されるリンクは「Topology」、「Firmware Upgrade」、「Configuration Backup/Restore」、「Upload Log File」です。

Topology（トポロジ）

「Topology」画面は、SIM グループ内のスイッチの設定および管理に使用されます。本画面は表示のためには、ご使用のコンピュータの設定で JavaScript が有効になっている必要があります。

Management > Virtual Stacking (SIM) > Topology の順にメニューをクリックします。サーバ上で Java Runtime Environment が起動し、以下の「Topology」画面が表示されます。

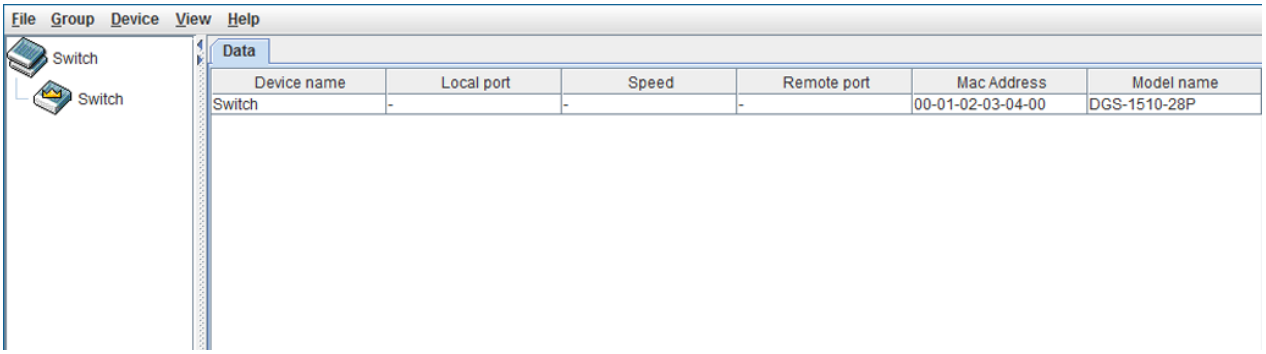


図 7-75　トポロジ画面

トポロジ画面の「Data」タブには以下の情報が表示されます。

項目	説明
Device name	ユーザが設定した SIM グループ内のスイッチのデバイス名を表示します。デバイス名がない場合は、default が与えられ、識別のために MAC アドレスの終わり 6 桁が付加されます。
Local port	MS または CaS が接続している CS 上の物理ポート数を表示します。CS の場合は何も表示されません。
Speed	CS と MS、または CaS 間の接続速度を表示します。CS の場合は何も表示されません。
Remote port	CS が接続している MS または CaS 上の物理ポート数を表示します。CS の場合は何も表示されません。
Mac Address	対応するスイッチの MAC アドレスを表示します。
Model name	対応するスイッチのモデル名を表示します。

メニューバー

トポロジ画面には、デバイスの設定に使用するメニューバーが配置されています。



図 7-76　トポロジメニューバー

メニューバーには以下の 5 つのメニューが存在します。

「File」メニュー

- Print Topology – トポロジマップを印刷します。
- Preference – ポーリング間隔など表示プロパティを設定します。



図 7-77　Preference ダイアログボックス

画面には以下の情報が表示されます。

項目	説明
Interval	SIM トポロジ画面の更新間隔を指定します。10 ～ 300 の範囲で指定可能です。
Show All	トポロジ上の全ての SIM デバイスを表示します。
Show Member Only	トポロジ上の SIM メンバデバイスを表示します。

「Apply」ボタンをクリックし、設定を適用します。
「Cancel」ボタンをクリックし、設定を適用せずに画面を閉じます。

「Group」メニュー

- Add to Group – リストから Candidate スイッチ（CaS）を選択し、本項目をクリックしてグループに CaS を追加します。このオプションを選択すると、以下のパスワード入力画面が表示され、CaS を SIM グループに追加するための認証を行います。パスワードを入力して「Apply」ボタンをクリックするか、「Cancel」ボタンをクリックして画面を閉じます。

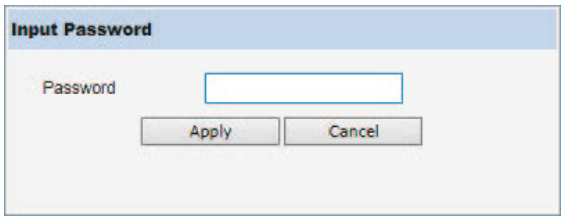


図 7-78　Input password ダイアログボックス

- Remove from Group – MS をグループから削除します。

「Device」メニュー

- Configure – 指定したデバイスの Web マネージャを開きます。

「View」メニュー

- Refresh – ビューを最新の状態に更新します。
- Topology – トポロジビューを表示します。

トポロジビューは定期的に（初期値：20 秒）更新されます。

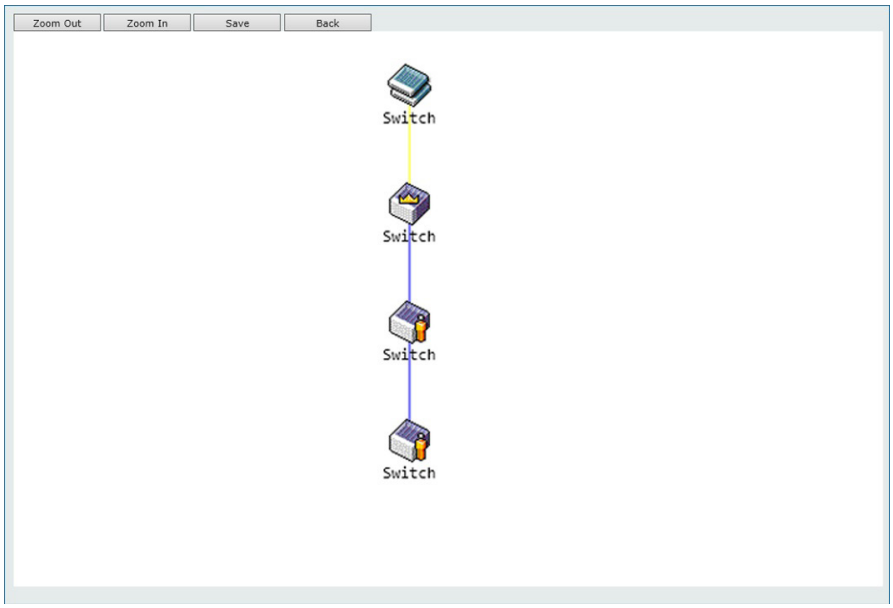


図 7-79　Topology 画面

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

本画面は、SIM グループ内のデバイスが他のグループやデバイスとどのように接続しているかを表示します。本画面で表示されるアイコンは以下の通りです。

アイコン	説明
	グループ
	レイヤ 2 Commander スイッチ
	レイヤ 3 Commander スイッチ

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

ツールヒント

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

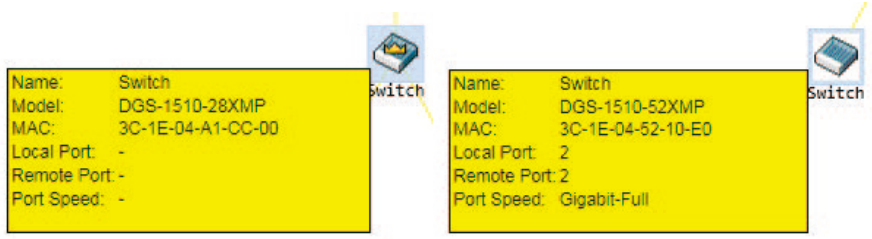


図 7-80　ツールヒントを利用したデバイス情報の表示

2 つのデバイスの間のライン上でマウスポインタを静止させると、以下の図のようにデバイス間の接続速度を表示します。

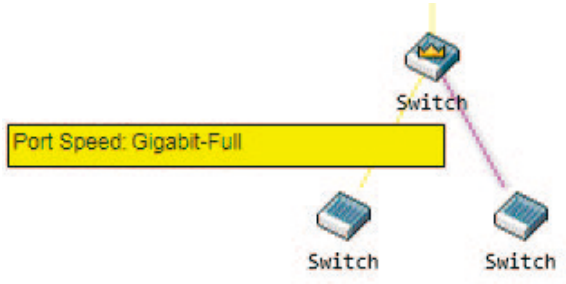


図 7-81　ツールヒントを利用したポート速度の表示

右クリックメニュー

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

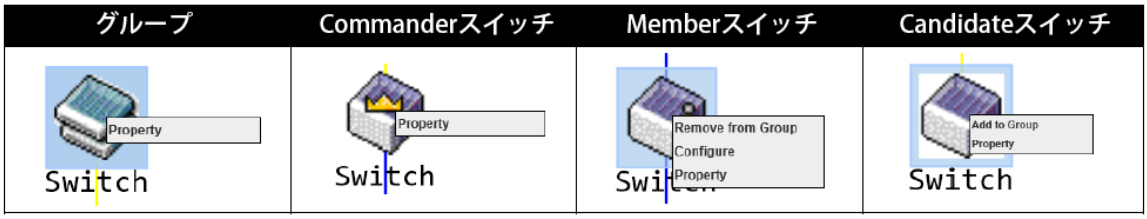


図 7-82　各アイコン上での右クリック

以下のオプションが表示されます。

項目	説明
Property	ポップアップ画面が開き、グループ情報が表示されます。
Configure	選択デバイスの Web UI へ接続します。（Member スイッチのみ）
Add to Group	選択した Candidate スイッチを SIM グループへ追加します。（Candidate スイッチのみ） SIM グループへ追加する場合、パスワードが要求されます。
Remove from Group	選択した Member スイッチを SIM グループから削除します。（Member スイッチのみ）



図 7-83　Property 画面

画面には以下の情報が表示されます。

項目	説明
Device Name	ユーザが設定した SIM グループ内のスイッチのデバイス名を表示します。デバイス名がない場合は、「default」が与えられ、識別のために MAC アドレスの終わり 6 桁が付加されます。
Module Name	右クリックされたスイッチのモジュール名を表示します。
Mac Address	対応するスイッチの MAC アドレスを表示します。
Remote Port No	CS が接続している MS または CaS の物理ポートの番号を表示します。CS の場合は何も表示されません。
Local Port No	MS または CaS が接続している CS の物理ポートの番号を表示します。CS の場合は何も表示されません。
Port Speed	CS と MS/CaS 間の接続スピードを表示します。

「Help」メニュー

- About – 現在の SIM バージョンなどの SIM 情報を表示します。



図 7-84　SIM 情報

Firmware Upgrade（ファームウェア更新）

本画面は、CS から MS へのファームウェアの更新を行う場合に使用します。

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

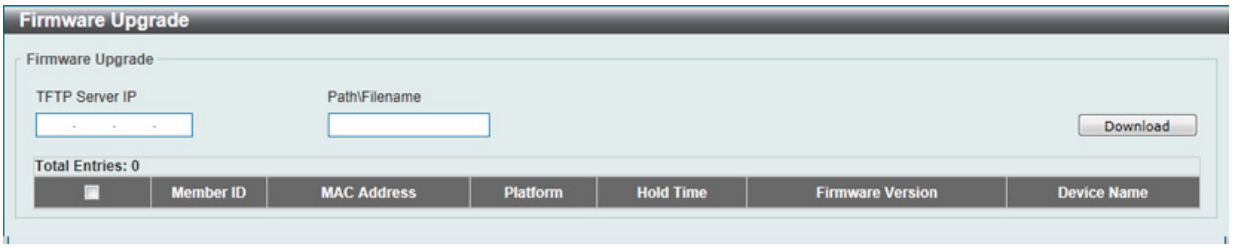


図 7-85　Firmware Upgrade 画面

設定には以下の項目を使用します。

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

「Download」ボタンをクリックすると、ファイル転送が開始されます。

Configuration File Backup/ Restore（コンフィグレーションファイルの更新）

本画面は、TFTP サーバを使用して CS から MS へのコンフィグレーションファイルの更新を行う際に使用します。

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

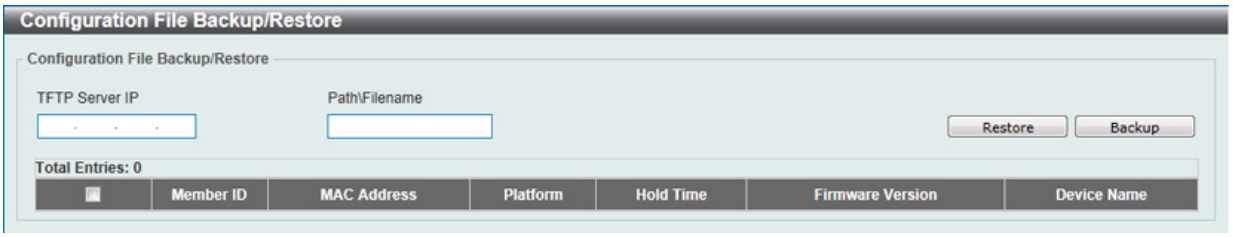


図 7-86　Configuration File Backup/Restore 画面

設定には以下の項目を使用します。

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

「Restore」ボタンをクリックすると、メンバスイッチに TFTP サーバからの設定をアップデートします。
「Backup」ボタンをクリックすると、TFTP サーバに設定をバックアップします。

Upload Log File（ログファイルのアップロード）

以下の画面は、SIM メンバスイッチから指定した PC へログファイルのアップロードを行う際に使用します。

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

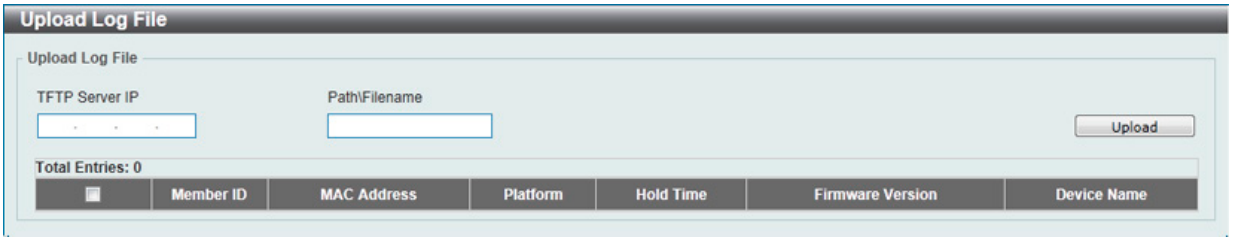


図 7-87　Upload Log File 画面

設定には以下の項目を使用します。

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

「Upload」ボタンをクリックすると、ファイル転送が開始されます。

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

D-Link ディスカバリプロトコル（DDP）の表示、設定を行います。

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

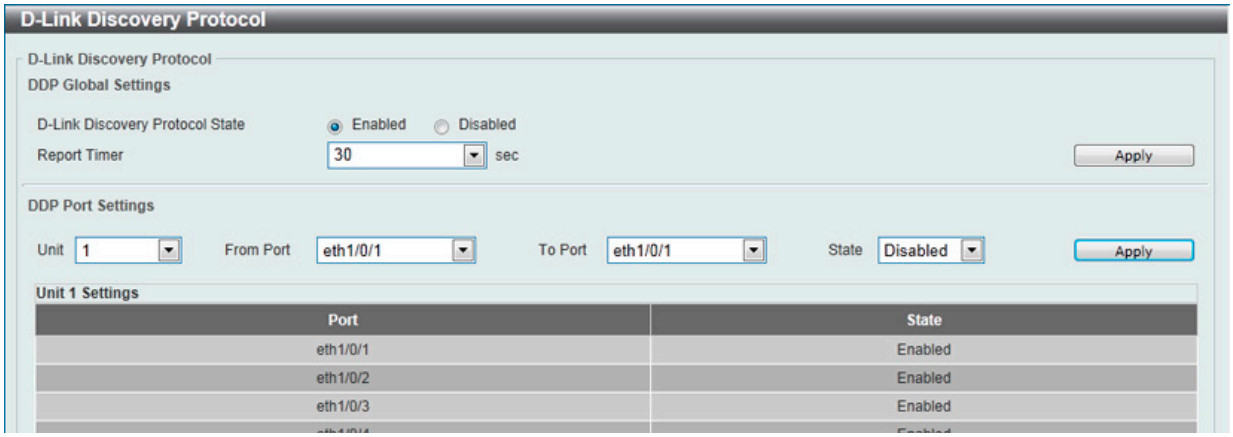


図 7-88　D-Link Discovery Protocol 画面

設定には以下の項目を使用します。

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

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

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）	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 設定）	VLAN 表示、設定を行います。
STP（スパニングツリーの設定）	スパニングツリーの設定を行います。
ERPS (G.8032) （イーサネットリングプロテクション設定）	イーサネットリングプロテクション設定を行います。
Loopback Detection （ループバック検知設定）	ループバック検知設定を行います。
Link Aggregation （リンクアグリゲーション）	複数のポートを結合して 1 つの広帯域のデータパイプラインとして利用します。
L2 Multicast Control （L2 マルチキャストコントロール）	L2 マルチキャストコントロールの設定を行います。
LLDP（LLDP 設定）	LLDP（Link Layer Discovery Protocol）の設定を行います。

FDB（FDB 設定）

Static FDB（スタティック FDB 設定）

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

スタティックユニキャスト転送の設定を行います。

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

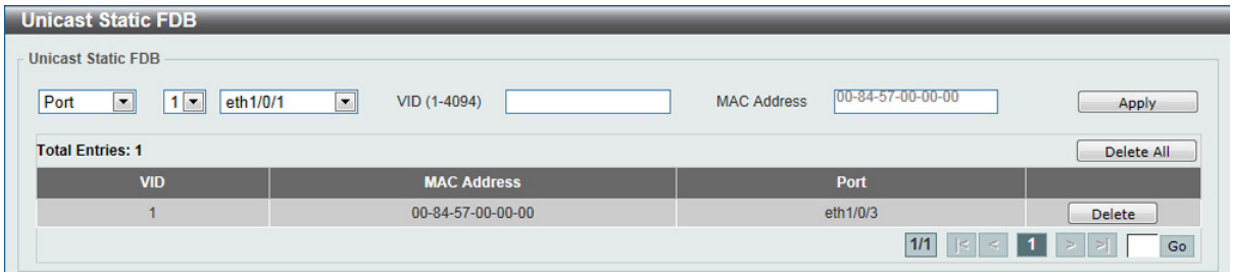


図 8-1　Unicast Static FDB 設定

画面には以下の項目があります。

項目	説明
Port/Drop	上記で入力した MAC アドレスの存在する、ポート番号の選択を行います。このオプションは同時にユニキャストスタティック FDB からの MAC アドレスを破棄するのに使用されます。ポート番号を項目に入力します。ユニット番号の初期値は 1 です。入力形式は次の通りです。 「ユニット番号 : ポート番号」（例 : 1:5） 「ポート番号」（例 : 5）
Unit Number	設定するユニットを選択します。
Port Number	設定するポートを選択します。
VID	ユニキャスト MAC アドレスのある VLAN ID を入力します。
MAC Address	パケットを静的に転送する MAC アドレスを入力します。これはユニキャスト MAC アドレスです。

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

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

マルチキャストスタティック FDB の設定を行います。

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

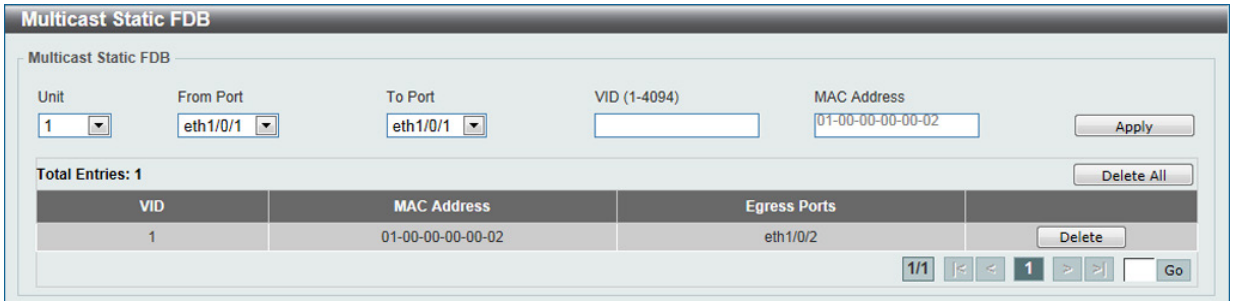


図 8-2　Multicast Static FDB 設定

画面には以下の項目があります。

項目	説明
Unit	設定するユニットを指定します。
From Port / To Port	ポートの始点 / 終点を設定します。
VID	対象の MAC アドレスが属する VLAN の VLAN ID です。
MAC Address	マルチキャストパケットのスタティック送信先 MAC アドレスを入力します。形式は 01-XX-XX-XX-XX-XX です。

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

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

MAC アドレステーブルのグローバル設定を行います。

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

Global Settings（グローバル設定タブ）



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

以下の項目を使用して設定を行います。

項目	説明
Aging Time (10-1000000)	MAC アドレステーブルのエージングタイムを入力します（10-1000000 秒）。0 を入力すると MAC アドレスエージングは無効化されます。初期値は 300 秒です。
Aging Destination Hit	Aging Destination Hit を有効にすると宛先 MAC アドレスのトリガによる更新が行われ、MAC アドレスエントリのヒットビットがパケットの送信先 MAC アドレスと VLAN に基づいて更新されます。宛先 MAC アドレスのトリガ更新機能は、MAC アドレスエントリのヒットビット更新の頻度が増えると、MAC アドレスエントリのエージングの期限でトラフィックのフラッディングを削減します。

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

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

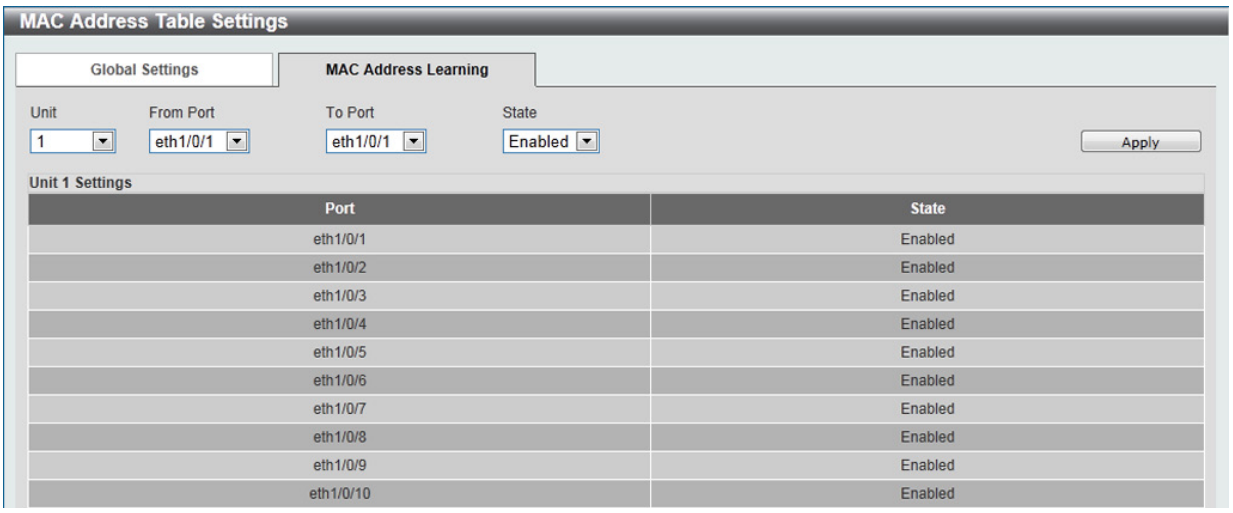


図 8-4　MAC Address Table Settings (MAC Address Learning) 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Unit	設定するユニットを指定します。
From Port / To Port	ポートの始点 / 終点を設定します。
State	指定したポートでの MAC アドレス学習機能を有効 / 無効にします。

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

MAC Address Table（MAC アドレステーブル）

MAC アドレステーブル内のエントリリストの表示を行います。

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



図 8-5　MAC Address Table 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Port	MAC アドレスと関連付けられるユニットとポートを選択します。
VLAN ID	表示する VLAN ID を入力します。
MAC Address	表示する MAC アドレスを入力します。

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

エントリの検索

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

ダイナミックエントリの削除

「Clear Dynamic by Port」ボタンをクリックして、対象のポートで学習されたダイナミック MAC アドレスを削除します。
「Clear Dynamic by VLAN」ボタンをクリックして、対象の VLAN で学習されたダイナミック MAC アドレスを削除します。
「Clear Dynamic by MAC」ボタンをクリックして、入力されたダイナミック MAC アドレスを削除します。

エントリの表示

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

全エントリの削除

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

MAC Notification（MAC 通知設定）

MAC Notification（通知）の表示、設定を行います。

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

MAC 通知を行うためには、**L2 Features > FDB > MAC Notification** の順にメニューをクリックし、以下の画面を表示します。

MAC Notification Settings タブ

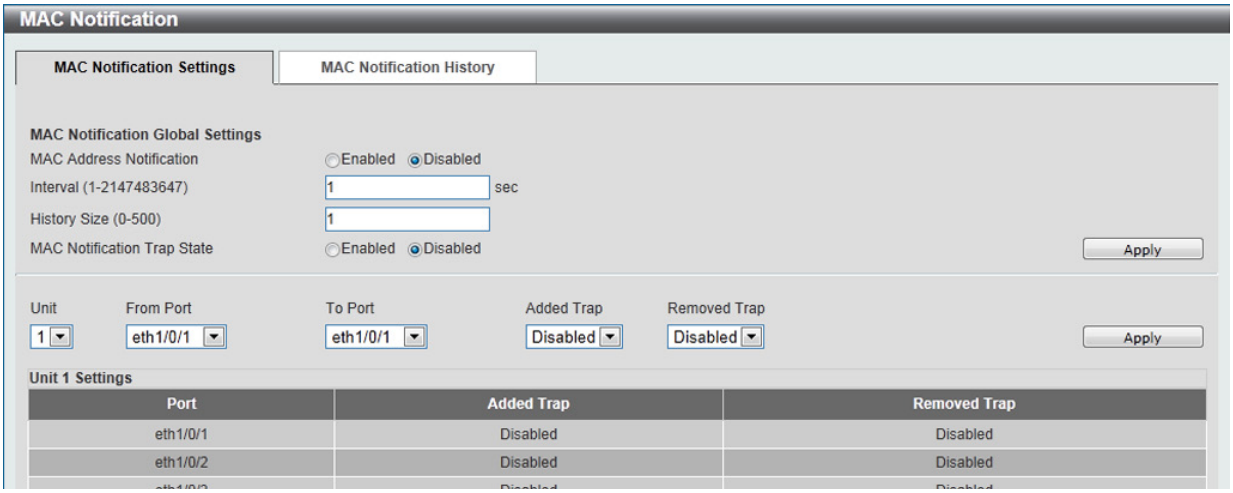


図 8-6　MAC Notification Settings 画面

以下の項目を使用して設定を行います。

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

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

MAC Notification History タブ

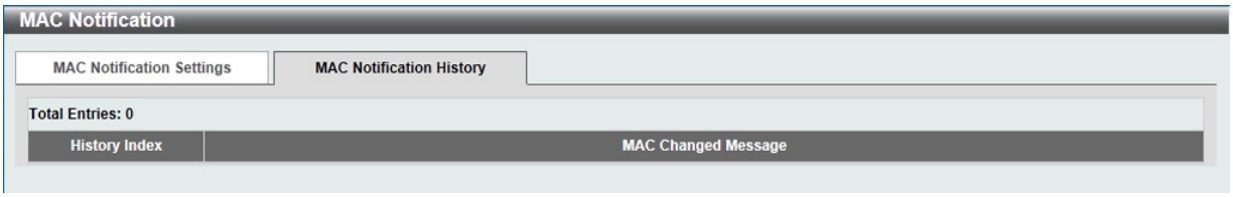


図 8-7　MAC Notification History 画面

MAC 通知メッセージの履歴が表示されます。

VLAN（VLAN 設定）

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 8-8　VLAN Configuration Wizard 画面

以下の項目が含まれます。

項目	内容
Create VLAN	新しく VLAN を作成する場合に選択します。VID を 1-4094 の間で入力します。 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。設定する VID を入力します。

「Next」ボタンをクリックし、以下の画面で設定を行います。

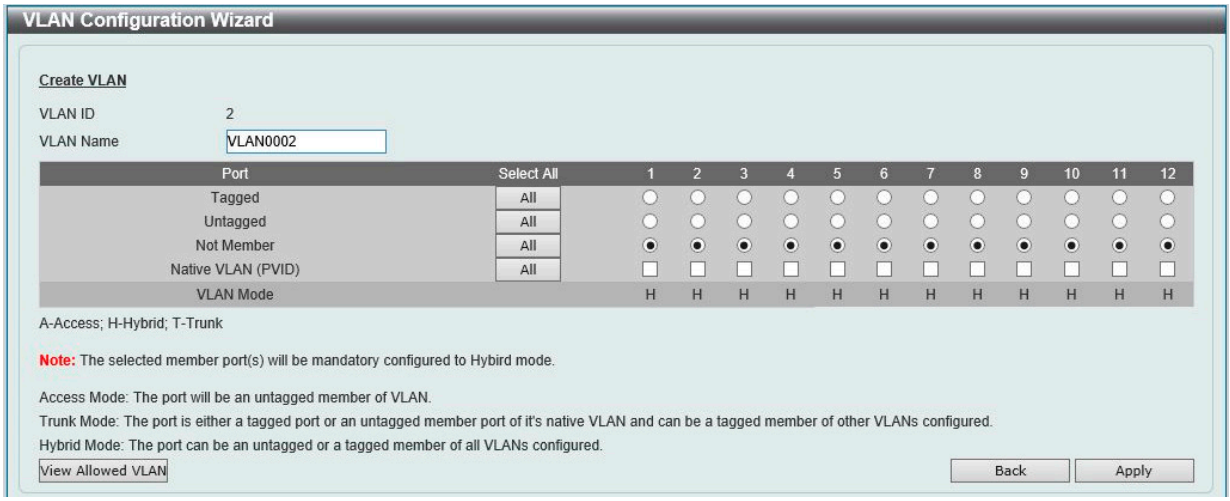


図 8-9　VLAN Configuration Wizard 画面

以下の項目が含まれます。

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」ボタンをクリックすると、すべてのポートが選択されます。
	VLAN Mode 各ポートの VLAN モードが表示されます。 アルファベットの表示は以下のモードを表します。 • A：Access モード ポートは VLAN のタグなしメンバになります。 • H：Hybrid モード ポートは設定されているすべての VLAN のタグなしまたはタグ付きメンバにすることができます。 • T：Trunk モード ポートはネイティブ VLAN のタグ付きポートまたはタグなしメンバポートのいずれかであり、設定されている他の VLAN のタグ付きメンバにすることができます。

項目	内容
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。

「Next」ボタンをクリックし、次へ進みます。

802.1Q VLAN Settings（802.1Q VLAN 設定）

VLAN 表示、設定を行います。

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



図 8-10　802.1Q VLAN 画面

以下の項目が含まれます。

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

「Apply」ボタンをクリックし、設定を適用します。

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

エントリの削除
対象のエントリの行の「Delete」ボタンをクリックします。

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

VLAN の編集
該当エントリの横で「Edit」ボタンをクリックします。

VLAN Interface（VLAN インタフェース設定）

VLAN インタフェースの設定を行います。

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

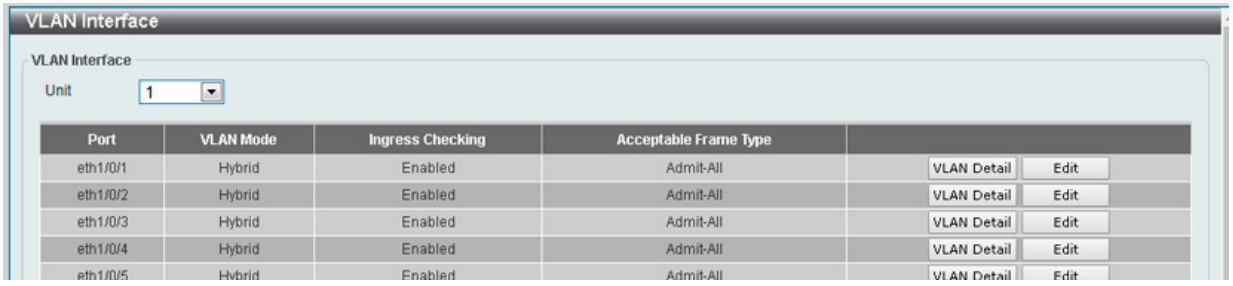


図 8-11　VLAN Interface 画面

項目	説明
Unit	設定、表示するユニットを指定します。

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

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

VLAN Deteil（VLAN 詳細情報の表示）

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

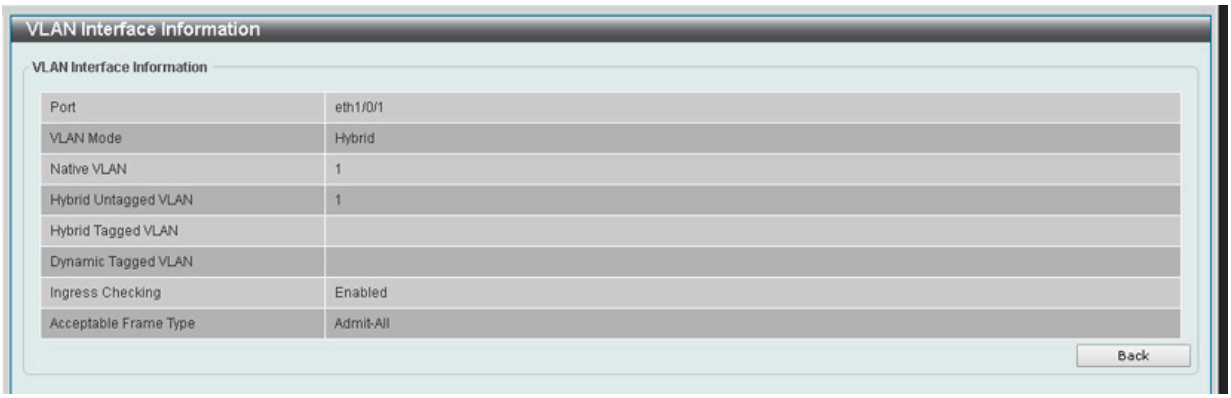


図 8-12　VLAN Interface Information 画面

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

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

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

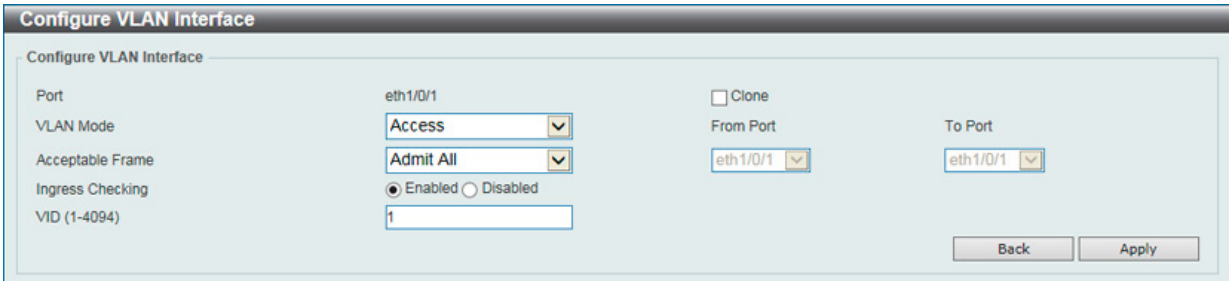


図 8-13　Configure VLAN Interface - Access 画面

画面には次の項目があります。

項目	説明
VLAN Mode	VLAN モードを「Access」「Hybrid」「Trunk」から選択します。
Acceptable Frame	許可するフレームの種類を「Tagged Only」「Untagged Only」「Admit All」から選択します。
Ingress Checking	イングレスチェック機能を有効 / 無効に指定します。
VID	設定する「VLAN ID」を指定します。1 から 4094 で指定可能です。
Clone	チェックすると指定ポートに設定を適用します。
From Port / To Port	ポート範囲を指定します。

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

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

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

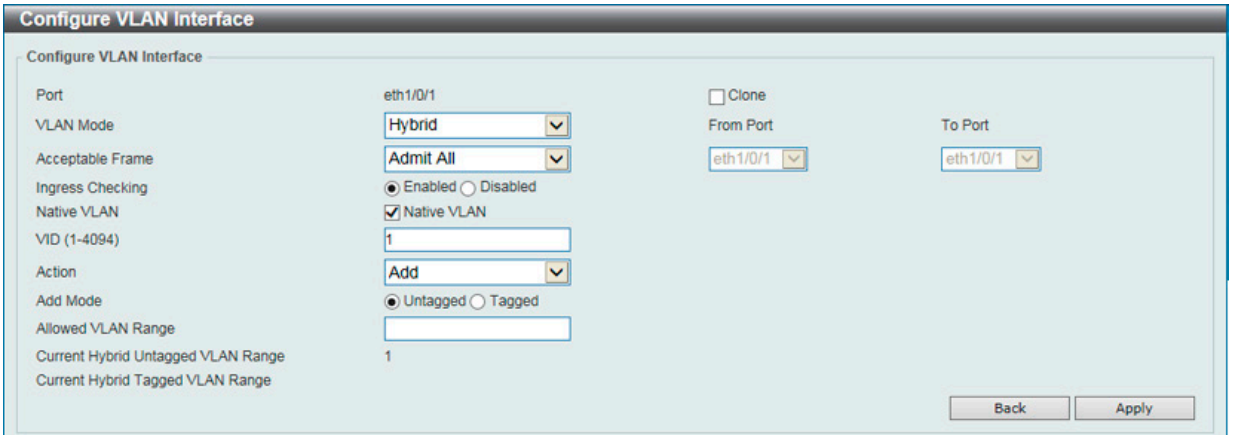


図 8-14　Configure VLAN Interface - Hybrid 画面

画面には次の項目があります。

項目	説明
VLAN Mode	VLAN モードを「Access」「Hybrid」「Trunk」から選択します。
Acceptable Frame	許可するフレームの種類を「Tagged Only」「Untagged Only」「Admit All」から選択します。
Ingress Checking	イングレスチェック機能を有効 / 無効に指定します。
Native VLAN	「Native VLAN」を有効にします。
VID	「Native VLAN」を有効にした後、「Native VLAN」に設定する「VLAN ID」を指定します。1 から 4094 で指定可能です。
Action	実行する動作を「Add」「Remove」「Tagged」「Untagged」から選択します。
Add Mode	「Add Mode」のパラメータに「Untagged」または「Tagged」を追加します。
Allowed VLAN Range	許可した VLAN 範囲情報を指定します。
Clone	チェックすると指定ポートに設定を適用します。
From Port / To Port	ポート範囲を指定します。

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

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

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

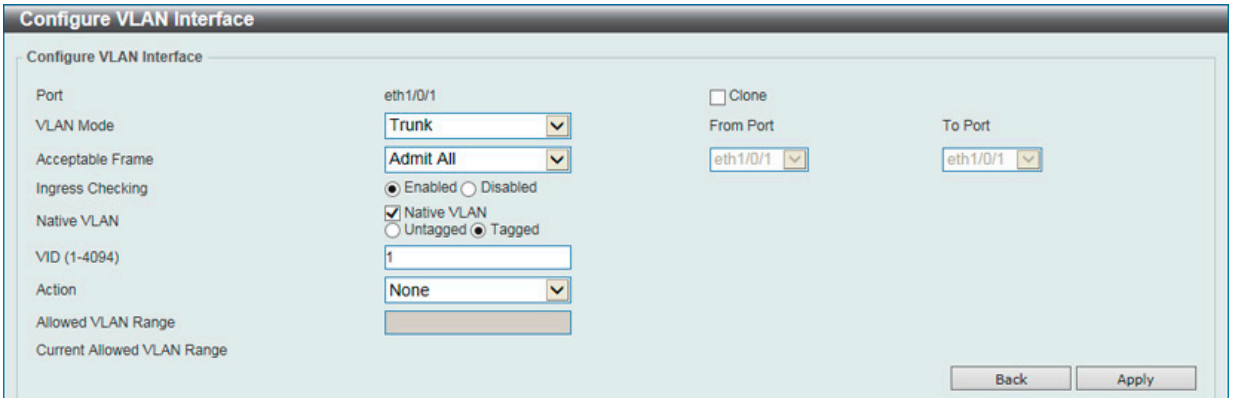


図 8-15　Configure VLAN Interface - Trunk 画面

画面には次の項目があります。

項目	説明
VLAN Mode	VLAN モードを「Access」「Hybrid」「Trunk」から選択します。
Acceptable Frame	許可するフレームの種類を「Tagged Only」「Untagged Only」「Admit All」から選択します。
Ingress Checking	Trunk を VLAN Mode として選択すると使用可能になります。イングレスチェック機能を有効 / 無効に指定します。
Native VLAN	「Native VLAN」を有効にします。また「Native VLAN」が「Untagged」または「Tagged」フレームをサポートしている場合に選択します。

項目	説明
VID	「Native VLAN」を有効にした後、「Native VLAN」に設定する「VLAN ID」を指定します。1 から 4094 で指定可能です。
Action	実行する動作を「None」「All」「Add」「Remove」「Except」「Replace」から選択します。
Allowed VLAN Range	許可した VLAN 範囲情報を指定します。
Clone	チェックすると指定ポートに設定を適用します。
From Port / To Port	ポート範囲を指定します。

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

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

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

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

本項目では、プロトコル VLAN プロファイルの作成、設定、管理を行います。

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

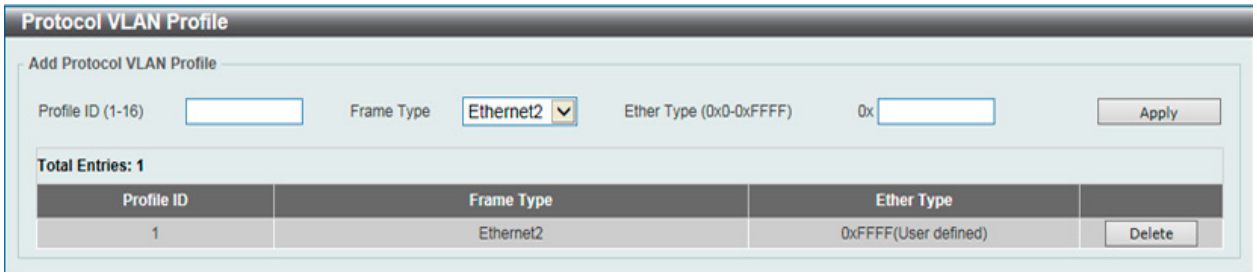


図 8-16　Protocol VLAN Profile 画面

以下の項目を使用して、設定します。

項目	説明
Profile ID	802.1v プロトコル VLAN プロファイル ID 番号を 1-16 の範囲から指定します。
Frame Type	フレームタイプを選択します。「Ethernet 2」「LLC」「SNAP」から選択します。
Ether Type	イーサネットタイプを指定します。プロトコル値は入力形式は 16 進数方式です。

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

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

プロトコル VLAN プロファイルインタフェースの設定を行います。

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

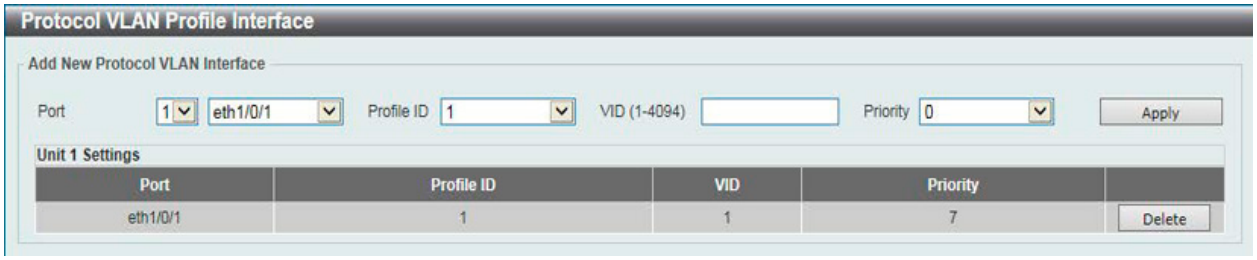


図 8-17　Protocol VLAN Profile Interface 画面

以下の項目を使用して、設定します。

項目	説明
Port	設定するユニット ID とポート番号を指定します。
Profile ID	プロトコルグループの ID を選択します。
VID (1-4094)	プロトコル VLAN の VLAN ID を入力します。
Priority	プロトコル VLAN のプライオリティを選択します。

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

GVRP（GVRP 設定）

GARP VLAN Registration Protocol（GVRP）グローバル設定を表示、設定します。

GVRP Global（GVRP グローバル設定）

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

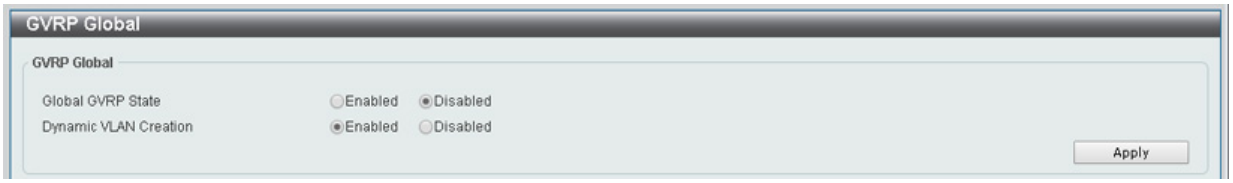


図 8-18　GVRP Global 画面

画面には次の項目があります。

項目	説明
Global GVRP State	GVRP を有効にするかを設定します。 • Enabled - GVRP を有効にします。 • Disabled - GVRP を無効にします。（初期値）
Dynamic VLAN Creation	ダイナミック VLAN 作成機能を有効 / 無効にします。

「Apply」ボタンをクリックし、設定を適用します。

GVRP Port（GVRP のポート設定）

GVRP のポート設定を行います。

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

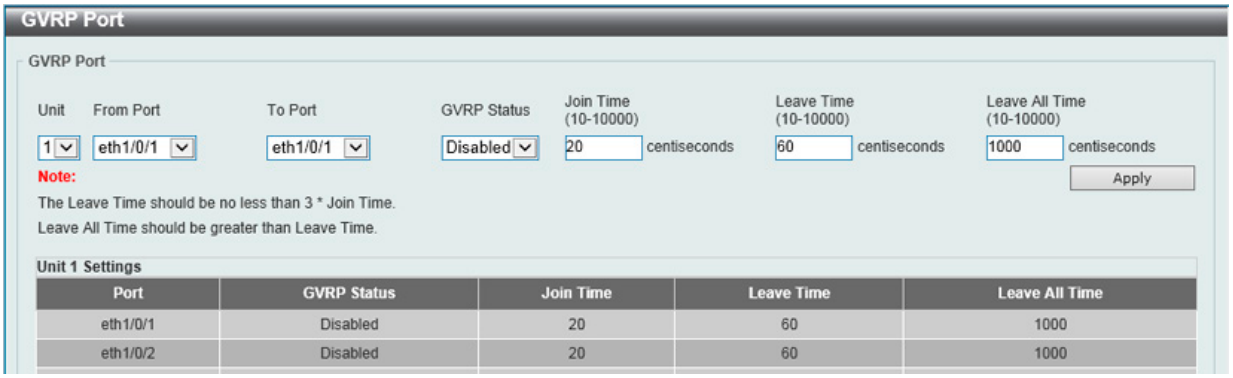


図 8-19　GVRP Port 画面

画面には以下の項目があります。

項目	説明
Unit	設定するユニットを指定します。
From Port / To Port	ポートの始点 / 終点を設定します。
GVRP Status	GVRP が各ポートで有効かどうかを設定します。有効にするとポートが自動的に VLAN のメンバになります。 • Enabled - 選択したポートで GVRP を有効にします。 • Disabled - 選択したポートで GVRP を無効にします。（初期値）
Join Time（10-10000）	Join 時間を設定します。10-10000（センチ秒）で指定します。初期値は 20（センチ秒）です。
Leave Time（10-10000）	Leave 時間を設定します。10-10000（センチ秒）で指定します。初期値は 60（センチ秒）です。
Leave All Time（10-10000）	Leave All 時間を設定します。10-10000（センチ秒）で指定します。初期値は 1000（センチ秒）です。

「Apply」ボタンをクリックし、設定を適用します。

GVRP Advertise VLAN（GVRP Advertise VLAN 設定）

GVRP advertised VLAN の設定、表示を行います。

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

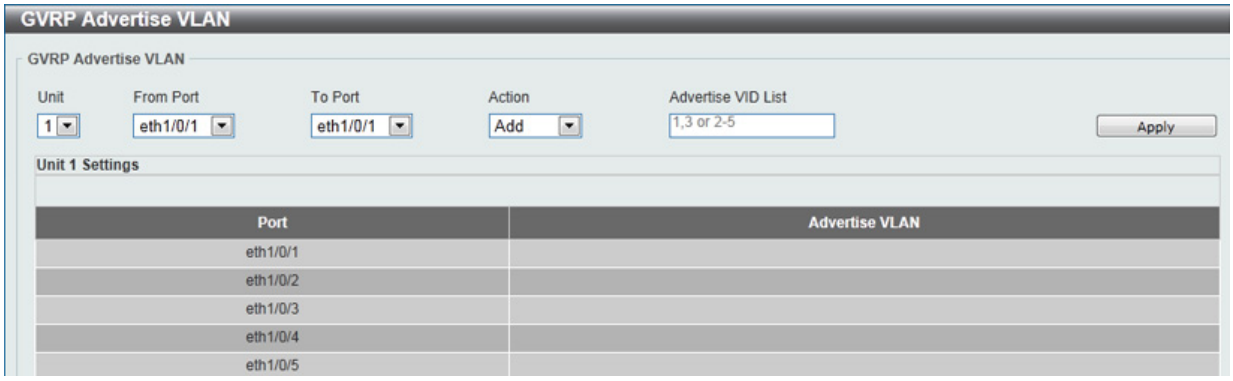


図 8-20　GVRP Advertise VLAN 画面

画面には次の項目があります。

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

「Apply」ボタンをクリックし、設定を適用します。

GVRP Forbidden VLAN（GVRP Forbidden VLAN 設定）

GVRP Forbidden VLAN の設定、表示を行います。

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

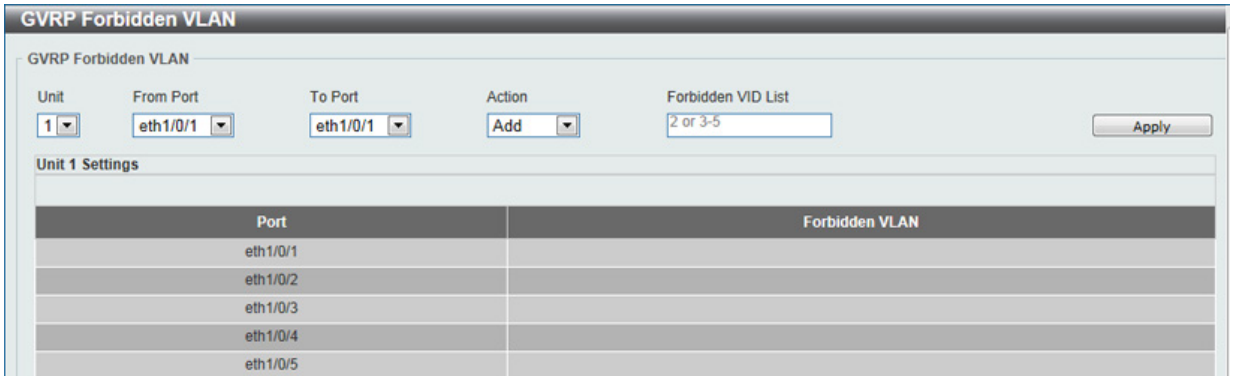


図 8-21　GVRP Forbidden VLAN 画面

画面には次の項目があります。

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

「Apply」ボタンをクリックし、設定を適用します。

GVRP Statistics Table（GVRP 統計テーブル）

GVRP の統計情報を表示します。

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

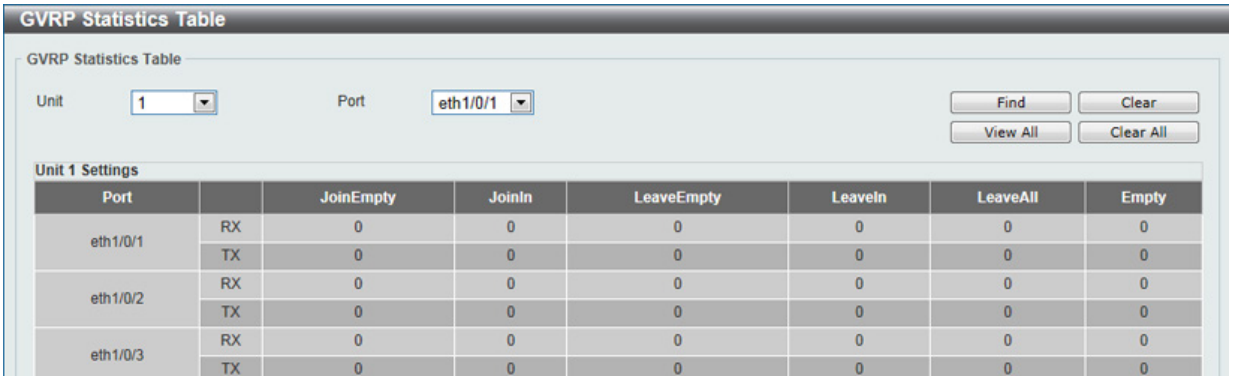


図 8-22　GVRP Statistics Table 画面

画面には次の項目があります。

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

エントリの検索
「Find」ボタンをクリックして、エントリを検索します。

エントリの削除
「Clear」ボタンをクリックして、指定したポートの情報をクリアします。

全エントリの表示
「View All 」ボタンをクリックして、すべての GVRP 統計情報を表示します。

全表示エントリの削除
「Clear All 」ボタンをクリックして、このテーブル内のすべての情報を削除します。

Asymmetric VLAN（Asymmetric VLAN 設定）

Asymmetric VLAN の設定を行います。

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

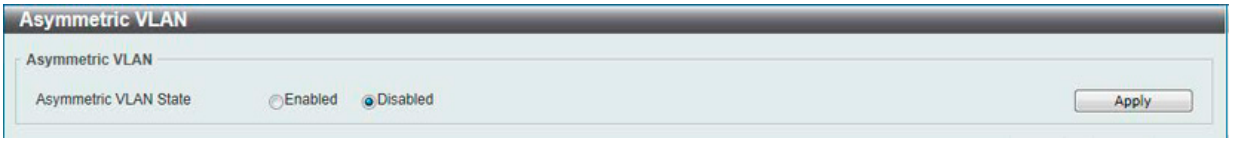


図 8-23　Asymmetric VLAN 画面

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

「Apply」ボタンをクリックし、設定を適用します。

MAC VLAN（MAC VLAN 設定）

MAC ベース VLAN を設定します。

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

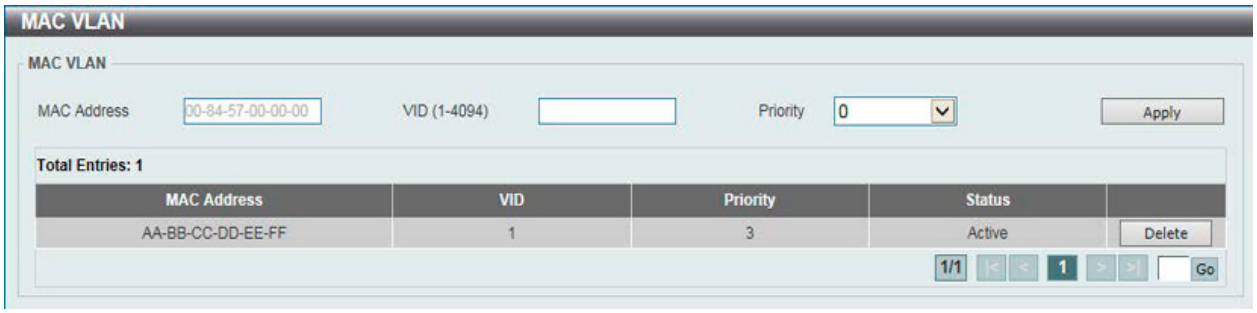


図 8-24　MAC VLAN 画面

以下の項目を使用して設定します。

項目	説明
MAC Address	MAC アドレスを入力します。
VID	MAC ベース VLAN の VLAN ID を入力します。
Priority	MAC ベース VLAN のプライオリティを選択します。

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

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

L2 VLAN インタフェースの概要を設定、表示します。

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

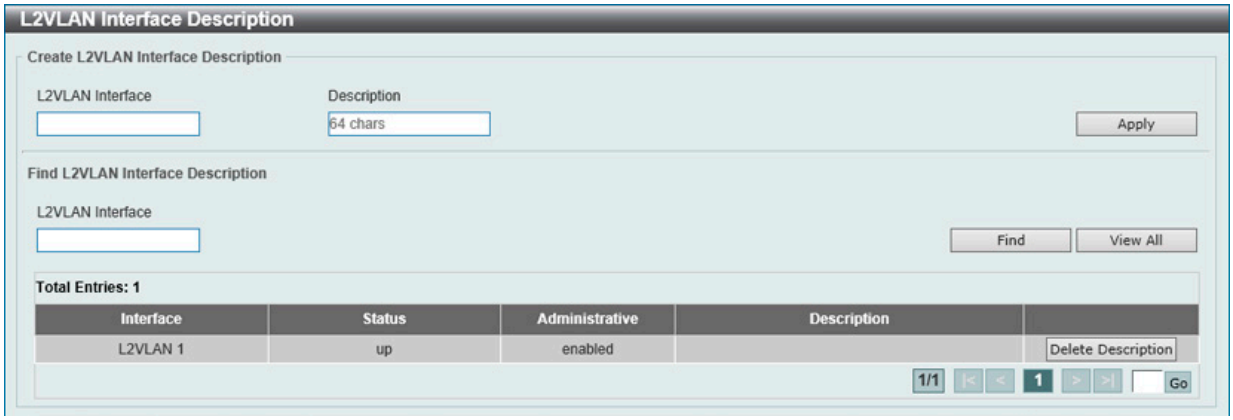


図 8-25　L2VLAN Interface Description 画面

「Create L2VLAN Interface Description 画面には次の項目があります。

項目	説明
Create L2VLAN Interface Description（L2 VLAN 概要作成）	
L2VLAN Interface	レイヤ 2 VLAN インタフェースの ID を指定します。
Description	レイヤ 2 VLAN インタフェースの概要を指定します。
Find L2VLAN Interface Description（L2 VLAN 概要検索）	
L2VLAN Interface	設定、表示するレイヤ 2 VLAN インタフェースを検出します。

「Apply」ボタンをクリックし、設定を適用します。
「Find」ボタンをクリックし、入力内容に基づくエントリを検出します。
「View All」ボタンをクリックし、すべてのエントリを表示します。
「Delete Description」ボタンをクリックし、指定エントリの概要を削除します。
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、指定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。

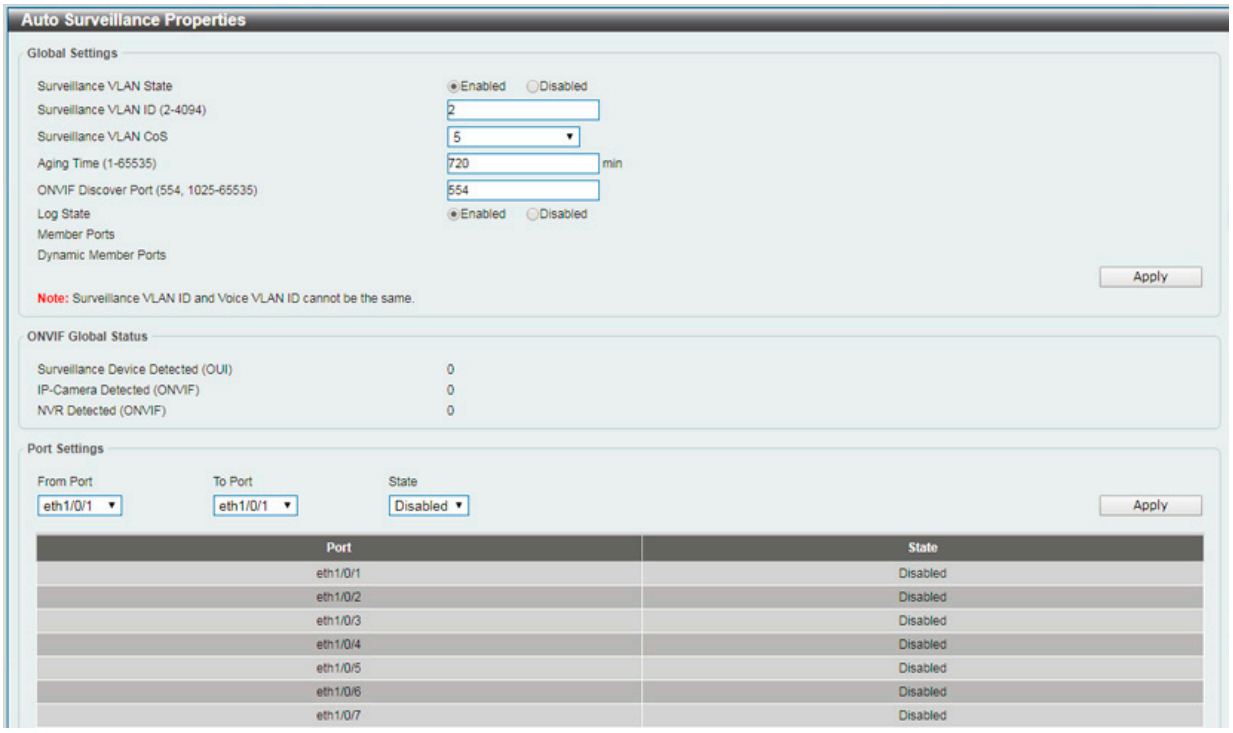


図 8-26　Auto Surveillance Properties 画面

画面には次の項目があります。

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。2 から 4094 で指定できます。
Surveillance VLAN CoS	サーベイランス VLAN の優先値を指定します。0 から 7 で指定できます。
Aging Time	エージングタイム（1-65535 分）。 初期値は 720（分）です。 エージングタイムは、ポートがオートサーベイランス VLAN メンバである場合にサーベイランス VLAN からポートを削除するために使用されます。最後のサーベイランスデバイスが、トラフィックの送信を止めて、このサーベイランスデバイスの MAC アドレスがエージングタイムに到達すると、サーベイランス VLAN エージングタイマが開始されます。 ポートはサーベイランス VLAN のエージングタイム経過後にサーベイランス VLAN から削除されます。 サーベイランストラフィックがエージングタイム内に再開すると、エージングタイマは停止し、リセットされます。
ONVIF Discover Port	「TCP/UDP」ポート番号を指定します。範囲は「554」または「1025 から 65535」です。RSTP ストリームスヌーピングのポート番号になります。ONVIF IP カメラと ONVIF NVR が「WS-Discovery」を使用し他のデバイスを検出します。IP カメラが検出されるとスイッチは IP カメラと NVR 間のスヌーピング RSTP/HTTP/HTTPS パケットによってさらに NVR を検出します。これらのパケットは TCP/UDP ポートと RTSP ポート番号が同等でないとスヌーピングされません。
Port Settings	
Unit	設定を適用するユニットを指定します。
From Port / To Port	ポート範囲を指定します。
State	ポートの状態を有効または無効にします。

「Apply」ボタンをクリックし、設定を適用します。

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

ユーザ定義のサーベイランスデバイスの OUI を設定します。

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

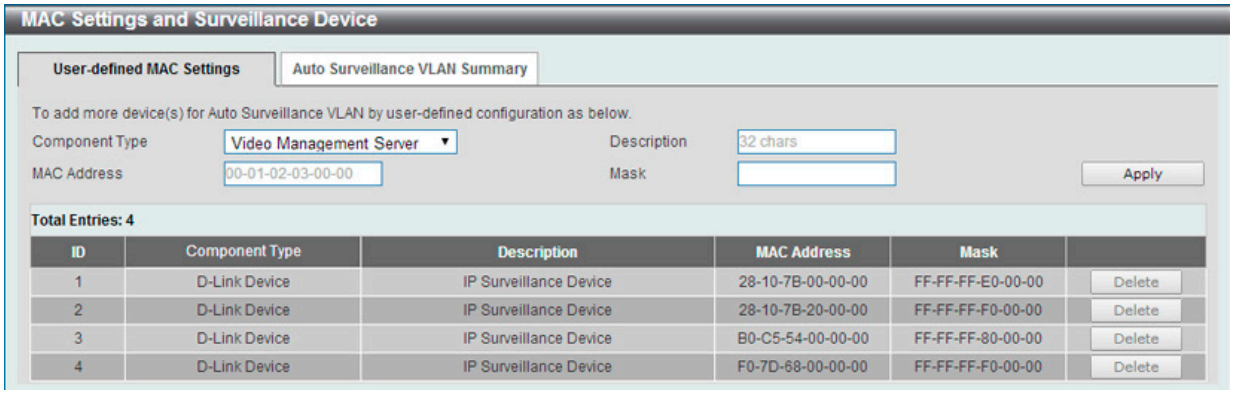


図 8-27　User -defined MAC Settings 画面

以下の項目を使用して設定します。

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

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

エントリの削除

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

自動サーベイランス VLAN サマリの表示

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

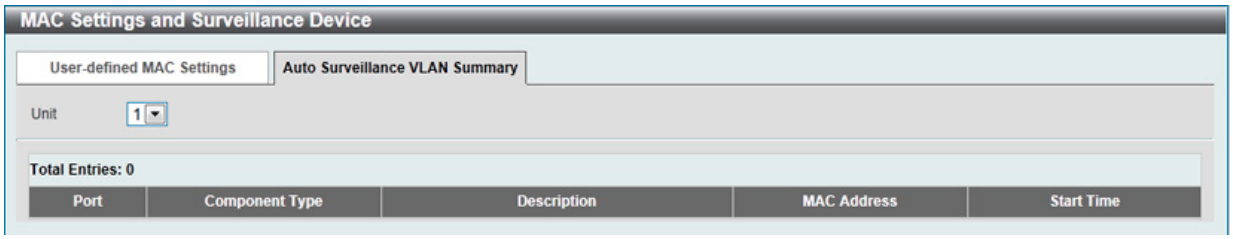


図 8-28　Auto Surveillance VLAN Summary 画面

以下の項目が表示されます。

項目	説明
Unit	表示するユニットを選択します。

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

IP カメラ情報ページでは ONVIF を通して検出されたデバイスについて表示します。ここでは ONVIF 対応機器について表示されます。

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。

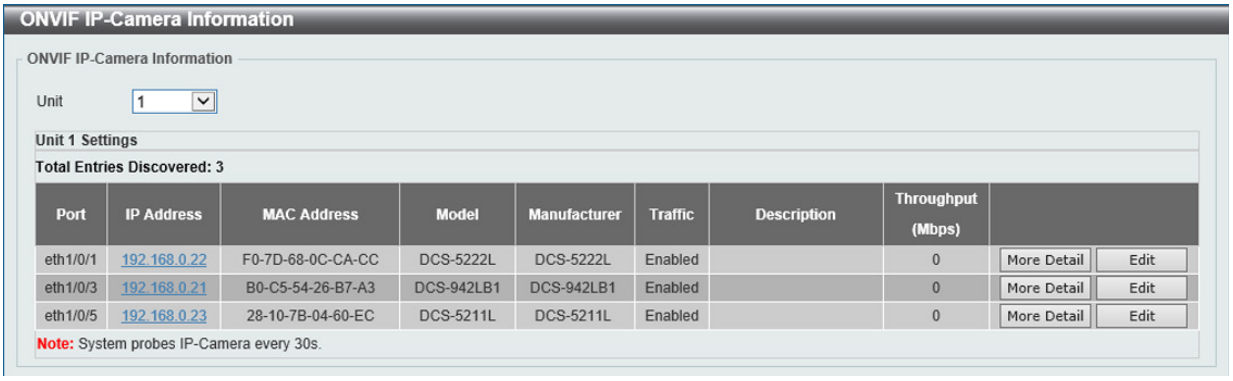


図 8-29　ONVIF IP-Camera Information 画面

「Unit」をクリックして表示するユニットを指定します。
「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 カメラのステートと説明を設定できます。



図 8-30　ONVIF IP-Camera Information_Edit 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
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。

設定を変更する場合は、「Apply」ボタンをクリックし、設定内容を適用してください。
「Back」ボタンをクリックし、前画面にもどります。

「More Detail」をクリックするとより詳細な情報が表示されます。

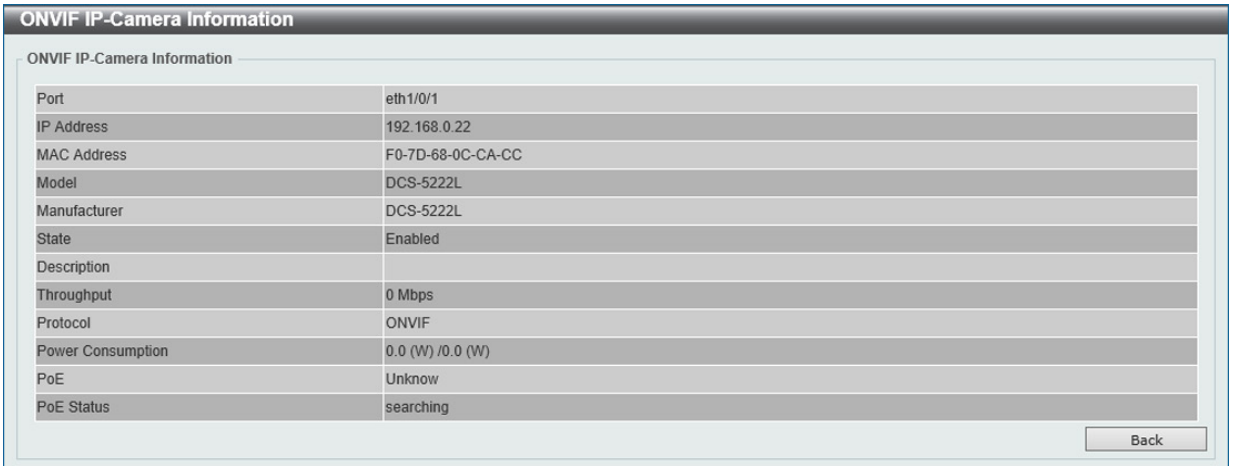


図 8-31　ONVIF IP-Camera Information_More Detail 画面

ONVIF NVR Information（ONVIF NVR 情報）

ONVIF VLAN で検出された NVR 機器のリストを表示します。

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。

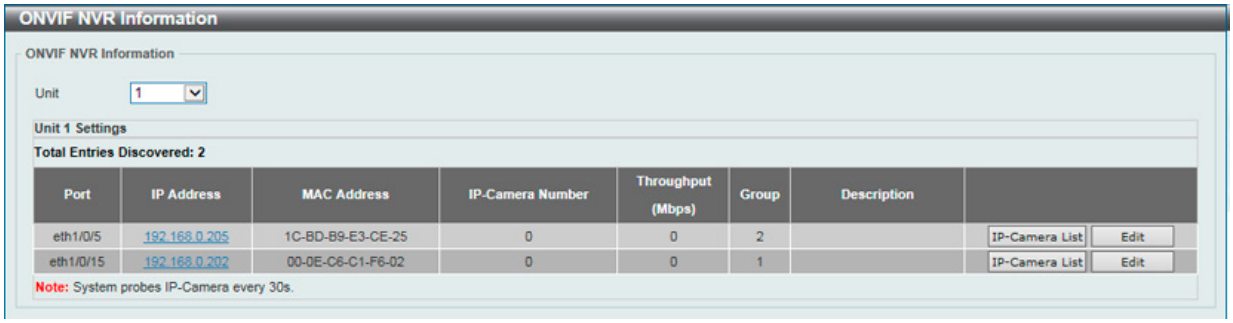


図 8-32　ONVIF NVR Information 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Unit	クリックして表示するユニットを指定します。

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 8-33　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」ボタンをクリックし、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。

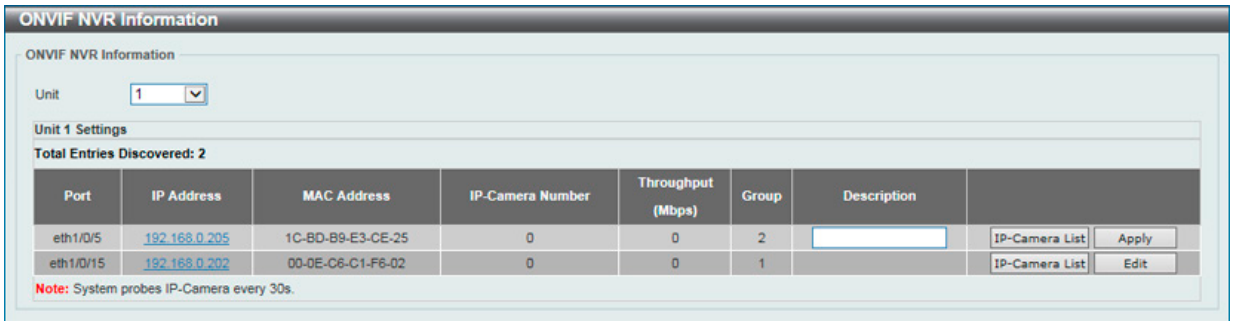


図 8-34　ONVIF NVR Information_Edit 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Description	NVR の概要を入力します。

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

Voice VLAN（音声 VLAN）

Voice VLAN は IP 電話からの音声トラフィックを送信する上で使用される VLAN です。IP 電話の音声品質が劣化するなどの理由から音声トラフィックの QoS を通常のトラフィックより優先的に送信されるように設定します。
スイッチは、受信したパケットの送信元 MAC アドレスをチェックすることにより、音声パケットであるかどうかを判断します。送信元 MAC アドレスが、設定された OUI アドレスであった場合、パケットは音声パケットとして判別され、音声 VLAN で送信されます。

Voice VLAN Global（音声 VLAN グローバル設定）

音声 VLAN をグローバルに有効 / 無効にします。

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

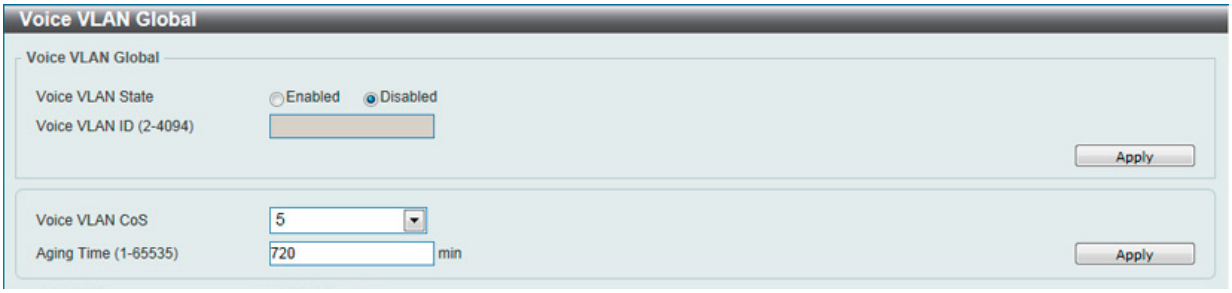


図 8-35　Voice VLAN Global 画面

以下の項目を使用して、設定します。

項目	説明
Voice VLAN State	プルダウンメニューを使用して、本機能を「Enabled」（有効）/「Disabled」（無効）にします。
Voice VID (2-4094)	選択をして音声 VLAN の VLAN ID を入力します。
Voice VLAN CoS	プルダウンメニューを使用して音声 VLAN の優先度を設定します。音声 VLAN 優先度はデータトラフィック中の音声トラフィックの QoS を判別する上で使用されます。範囲は 0-7 の間で設定できます。初期値は 5 です。
Aging Time (1-65535)	音声 VLAN のエージングタイムを入力します（1-65535 分）。エージングタイムは、ポートが音声 VLAN メンバである場合、音声 VLAN からポートを削除するために使用されます。最後の音声デバイスが送信を停止し、この音声デバイスの MAC アドレスが期限切れになると音声 VLAN のエージングタイマが開始されます。音声 VLAN エージングタイマの満了後、ポートは音声 VLAN から削除されます。エージングタイム中に音声トラフィックが再開すると、エージングタイマはリセットされます。

「Apply」ボタンをクリックし、設定を適用します。

Voice VLAN Port（音声 VLAN ポート設定）

音声 VLAN のポート設定を行います。

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

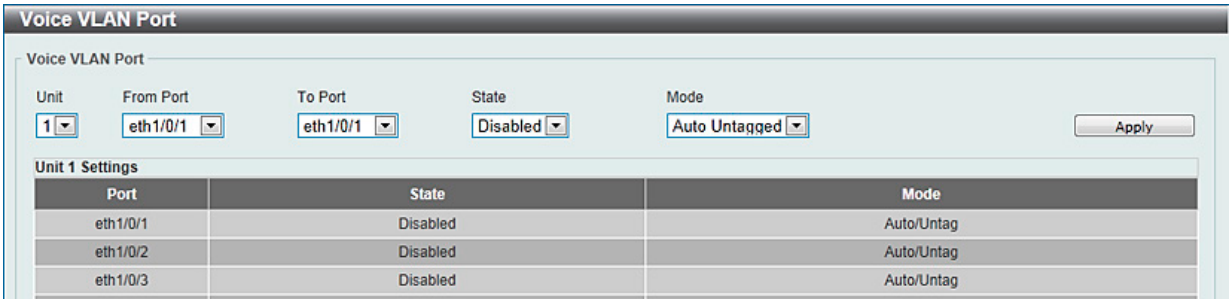


図 8-36　Voice VLAN Port 画面

以下の項目を使用して、設定します。

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

「Apply」ボタンをクリックし、設定を適用します。

Voice VLAN OUI（音声 VLAN OUI 設定）

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

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

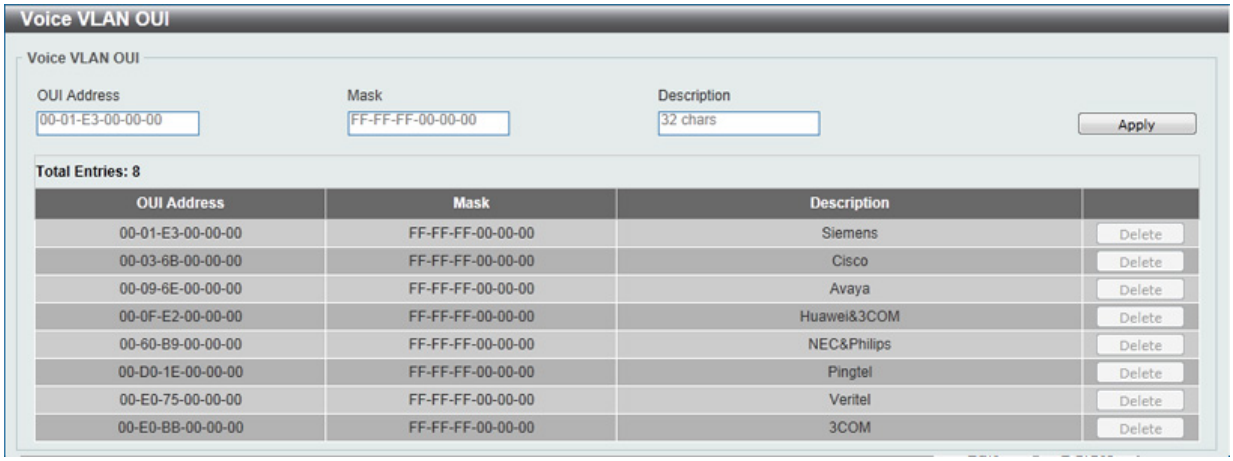


図 8-37　Voice VLAN OUI 画面

以下の項目を使用して、設定します。

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

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

Voice VLAN Device（音声 VLAN 機器）

各スイッチポートに接続中の音声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 8-38　Voice VLAN Device 画面

以下の項目が表示されます。

項目	説明
Unit	表示するユニットを選択します。

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

スイッチに接続された音声 VLAN LLDP-MED デバイスを表示します。

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

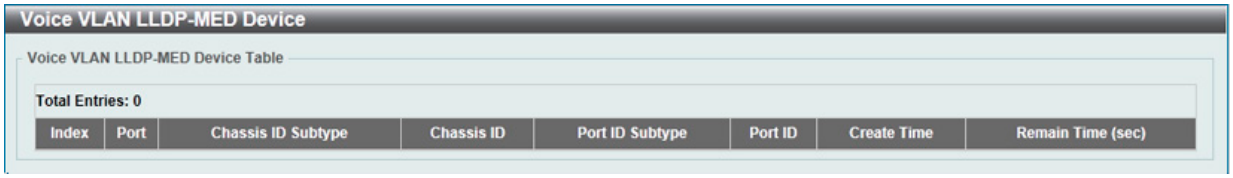


図 8-39　Voice VLAN LLDP-MED Device 画面

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（802.1D-1998 STP、802.1D-2004 Rapid STP、および 802.1Q-2005 MSTP）をサポートしています。ネットワーキング管理者間では 802.1D-1998 STP が最も一般的なプロトコルとして認識されていると思います。しかし、D-Link のマネジメントスイッチにも 802.1D-2004 RSTP と 802.1Q-2005 MSTP は導入されており、それらの技術について、以下に簡単に紹介します。また、802.1D-1998 STP、802.1D-2004 Rapid STP、802.1Q-2005 MSTP それぞれの設定方法についても、本章中に記述します。

802.1Q-2005 MSTP

MSTP（Multiple Spanning Tree Protocol）は IEEE 委員会により定義された標準規格で、複数の VLAN を 1 つのスパニングツリーインスタンスにマッピングし、ネットワーク中に複数の経路を提供します。また、ロードバランシングを可能にし、1 つのインスタンスに障害が発生した場合でも、広い範囲で影響を与えないようにすることができます。障害発生時には障害が発生したインスタンスに代わって新しいトポロジを素早く収束します。これら VLAN 用のフレームは、これらの 3 つのスパニングツリープロトコル（STP、RSTP、MSTP）のいずれかを使用して、素早く適切に相互接続されたブリッジを通して処理されます。

このプロトコルは BPDU パケットもまたタグ付けし、受信するデバイスはスパニングツリーのインスタンスやリージョン、それらに関連する VLAN を区別することも可能です。MSTI ID（MST インスタンス ID）はこれらのインスタンスをクラス分けします。MSTP 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決定し、1 つのスパニングツリーを構成する 1 つの仮想ブリッジとして表示されます。そのため、異なる VLAN に割り当てられたフレームは、定義した VLAN や各スパニングツリー内の管理エラーに関係なく、フレームの単純で完全な処理を続けながら、ネットワーク上の管理用に構築されたリージョン中の異なるデータ経路を通ります。

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

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

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

1. スイッチに MSTP 設定を行います。（「STP Bridge Global Settings」画面の「STP Version」で設定）
2. MSTP インスタンスに適切なスパニングツリープライオリティを設定します。（「MSTI Config 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

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

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

ポートの状態遷移

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

トポロジの計算については 3 つのすべてのプロトコルにおいて同様に行われます。各セグメントにはルートブリッジへの 1 つのパスがあります。すべてのブリッジは BPDU パケットをリッスンします。しかし、BPDU パケットは、さらに Hello パケット送信ごと送信されます。
BPDU パケットは、受信されないことがあっても送信されます。そのため、ブリッジ間のリンクはリンクの状態に反応します。結果として、この違いがリンク断の素早い検出とトポロジの調整に繋がるのです。802.1D-1998 の欠点は隣接するブリッジからの即時のフィードバックがないことです。

ポート状態の比較

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

RSTP では、タイマの設定への依存をやめ、フォワーディング状態への急速な遷移が可能になりました。RSTP 準拠のブリッジは他の RSTP に準拠するブリッジリンクからのフィードバックに反応するようになりました。ポートは、フォワーディング状態の遷移の間トポロジが安定するまで待つ必要がなくなりました。この急速な遷移を実現するために、RSTP プロトコルでは以下の 2 つの新しい変数（Edge Port と P2P Port）が使用されます。

Edge Port

エッジポートは、ループを作成できないセグメントに直接接続しているポートに指定するものです。例えば、1 台のワークステーションに接続しているポートがこれに該当します。エッジポートとして指定されたポートは、直接 forwarding に遷移し、listening および learning の段階は飛ばしてしまいます。エッジポートは BPDU パケットを受け取った時点で、通常のスパニングツリーポートに変わります。

P2P Port

P2P ポートでも急速な遷移が可能になっています。P2P ポートは他のブリッジとの接続に使用されます。RSTP と MSTP では、全二重モードで動作しているすべてのポートは、特に設定を変えられていない限り、P2P ポートと見なされます。

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

RSTP や MSTP はレガシー機器と相互運用が可能で、必要に応じて BPDU パケットを 802.1D-1998 形式に自動的に変換することができます。しかし、802.1D-1998 STP を使用しているセグメントでは、MSTP や RSTP の利点である迅速な遷移やトポロジ変更の検出を享受することはできません。それらのプロトコルは、セグメント上でレガシー機器が RSTP や MSTP を使用するためにアップデートを行う場合などの、マイグレーションに使用する変数を用意しています。

2 つのレベルで動作するスパニングツリープロトコル

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

STP Global Settings（STP グローバル設定）

STP をグローバルに設定します。

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

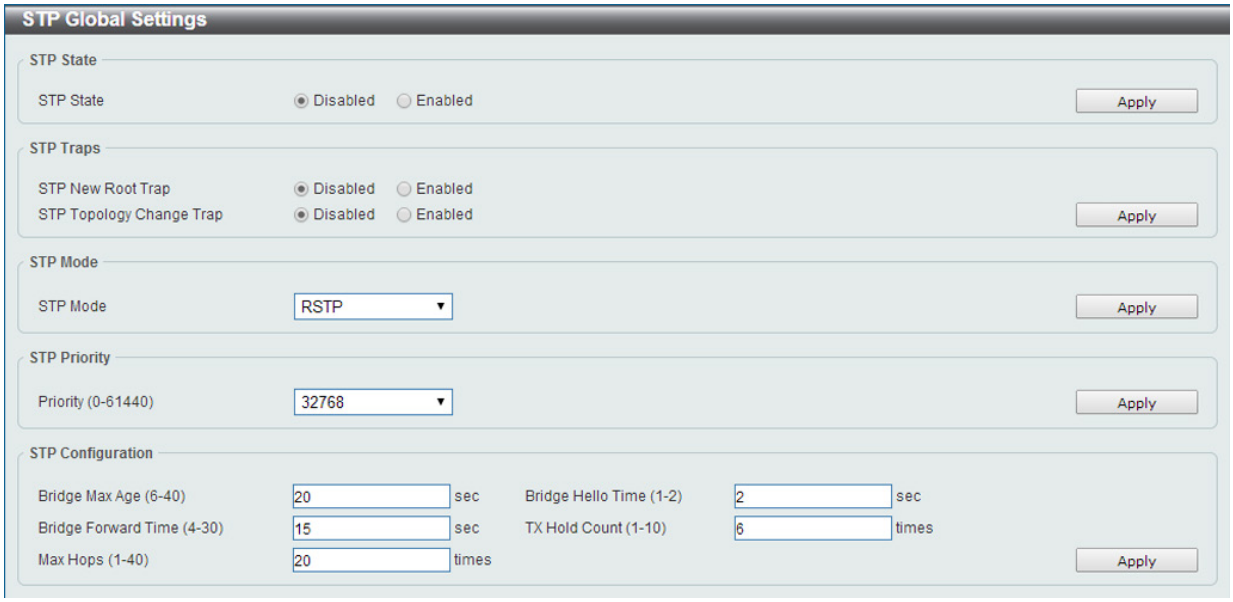


図 8-40　STP Global Settings 画面

設定には以下の項目が使用されます。

項目	説明
STP State	
STP State	STP をグローバルに「Enabled」（有効）/「Disabled」（無効）にします。
STP Trap	
STP New Root Trap	新しいルートトラップ送信の有効 / 無効を設定します。
STP Topology Change Trap	トポロジ変更トラップ送信の有効 / 無効を設定します。
STP Mode	
STP Mode	スイッチで使用する STP のバージョンをプルダウンメニューから選択します。 • STP - スイッチ上で STP がグローバルに使用されます。 • RSTP - スイッチ上で RSTP がグローバルに使用されます。 • MSTP - スイッチ上で MSTP がグローバルに使用されます。

項目	説明
STP Priority	
Priority	STP 優先値を指定します。0 から 61440 までで指定可能です。初期値は 32768 です。値が低いほうがプライオリティが高くなります。
STP Configuration	
Bridge Max Age (6-40)	本項目は、古い情報がネットワーク内の冗長パスをずっと循環し、新しい有効な情報の伝播を妨げるのを防ぐために設定します。ルートブリッジによりセットされるこの値は、スイッチと他の Bridged LAN（ブリッジで相互接続された LAN）内のデバイスが持っているスパニングツリー設定値が矛盾していないかを確認するための値です。本値が経過した時にルートブリッジからの BPDU パケットが受信されていなければ、スイッチは自分で BPDU パケットを送信し、ルートブリッジになる許可を得ようとします。この時点でスイッチのブリッジ識別番号が一番小さければ、スイッチはルートブリッジになります。6-40（秒）の範囲から値を指定します。初期値では 20（秒）が指定されています。
Bridge Hello Time (1-2)	STP モードとして、RSTP/STP を選択するとこのパラメータが利用可能になります。ブリッジの Hello タイム値を入力します。この値は 1-2 秒である必要があります。初期値は 2 秒です。これは、ルートブリッジが実際にルートブリッジであることを他のすべてのスイッチに伝達するために、ルートブリッジによって送信される BPDU パケット 2 回分の送信の間隔です。MSTP の場合、Hello タイムはポートごとに設定する必要があります。
Bridge Forward Time (4-30)	ブリッジ転送時間の値を入力します。この値は 4-30 秒である必要があります。初期値は 15 秒です。スイッチ上のどのポートも、ブロッキングステートからフォワーディングステートに移行する間、この時間の間リスニングステート状態になります。
Tx Hold Count (1-10)	Hello パケットの最大送信回数を指定します。1-10 の範囲から指定します。初期値は 6 です。
Max Hops (6-40)	許可するホップの最大数を入力します。この値は 6-40 である必要があります。初期値は 20 です。この値はスイッチから送信された BPDU パケットが破棄されるまでに可能なスパニングツリー上域内のデバイス間のホップ数を設定します。ホップカウントの各スイッチは、値がゼロになるまでホップカウントを 1 つずつ減算します。スイッチが BPDU パケットを破棄すると、ポートに保持されている情報はエージアウトされます。

「Apply」ボタンをクリックし、設定を適用します。

STP Port Settings（STP ポートの設定）

STP をポートごとに設定します。

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

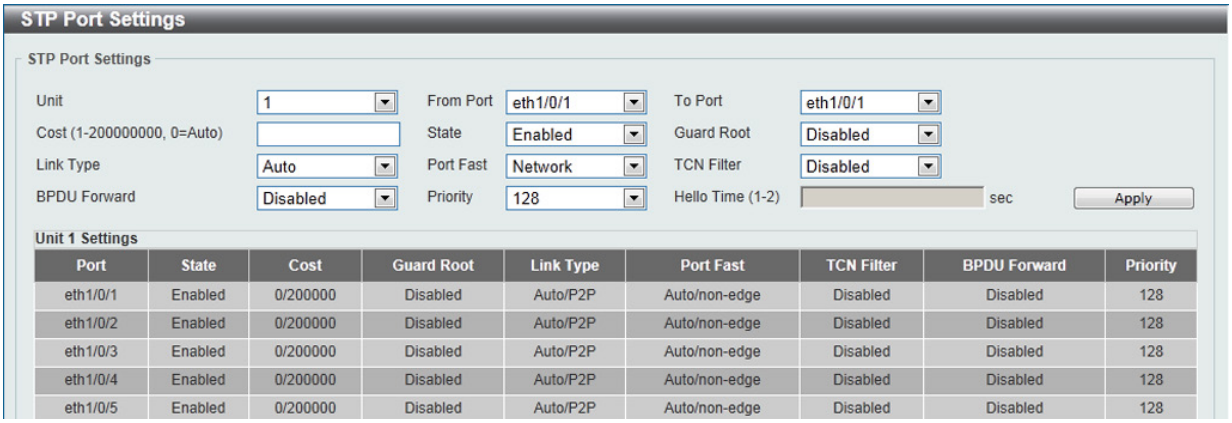


図 8-41　STP Port Setting 画面

本画面には以下の項目があります。

項目	説明
Unit	設定するユニットを選択します。
From Port	連続するポートグループの最初の番号を設定します。
To Port	連続するポートグループの最後の番号を設定します。
Cost (1-200000000, 0=Auto)	指定ポートへのパケット転送をするための適切なコストを表すメトリックを指定します。ポートのコストは自動か、メトリックの値で設定します。初期値は 0（Auto）です。 • 0（Auto）- 選択ポートに可能な最良のパケット転送速度を自動的に設定します。 ポートコストの初期値 :100Mbps ポート = 200000、Gigabit ポート = 20000。 • 値 1-200000000 - 外部転送のコストとして 1 から 200000000 までの値を設定します。数字が低いほど転送に使用されます。
State	ポートでの STP の「Enabled」（有効）/「Disabled」（無効）を設定します。初期値は「Enabled」です。
Guard Root	Guard Root の「Enabled」（有効）/「Disabled」（無効）を設定します。
Link Type	リンクの種類を設定します。初期値は「Auto」です。 • P2P - P2P ポートとしてリンクを共有します。P2P ポートは全二重でなくてはならないという制限があります。 • Shared - 半二重ポートとして認識されます。 • Auto - 自動で設定します。

項目	説明
Port Fast	ポートファストオプションを指定します。 「Network」「Disabled」「Edge」から選択します。「Network」モードでは、ポートは 3 秒だけ非ポートファスト状態に残ります。ポートは BPDU が受信されず、フォワーディングステートに変更されない場合、ポートファスト状態に変更します。のちに BPDU を受信すると非ポートファストへ戻ります。「Disable」モードではポートは常に非ポートファスト状態です。フォワーディングステートに変更するまで転送時間遅延の間、常に待ちます。「Edge」モードではポートは転送時間遅延の間待たずに、直接 STP フォワーディングステートに変更されます。インタフェースが「BPDU」を受信すると非ポートファストへ移行します。初期値では「Network」になります。
TCN Filter	TCN（Topology Change Notification）フィルタを有効 / 無効に設定します。 ポートの TCN フィルタリングを有効にすると、域内のアドレスフラッシングを発生させるネットワークのコア域への外部ブリッジを ISP により防ぐために有効です。 こういったブリッジは管理者のコントロール下で構築されることはないためです。ポートが TCN フィルタモードに設定されると、ポートが受信した TC イベントは無視されます。初期値は無効です。
BPDU Forward	BPDU パケットの転送を「Enabled」（有効）または「Disabled」（無効）にします。 有効にすると受信した STP BPDU はすべての VLAN メンバポートにタグなしフォームで転送されます。初期値は無効です。
Priority	優先値を指定します。0 から 240 で指定可能です。初期値は 128 です。値が小さいほど、優先値は高くなります。
Hello Time	ハロータイムの値を指定します。1 から 2（秒）の間で指定可能です。 この値は、指定されたポートが各構成メッセージの定期的な送信の間に待機する間隔を指定します。

「Apply」ボタンをクリックし、設定を適用します。

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。ユーザはその項目を変更できますが、MSTI ID の変更や削除は行うことができません。

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

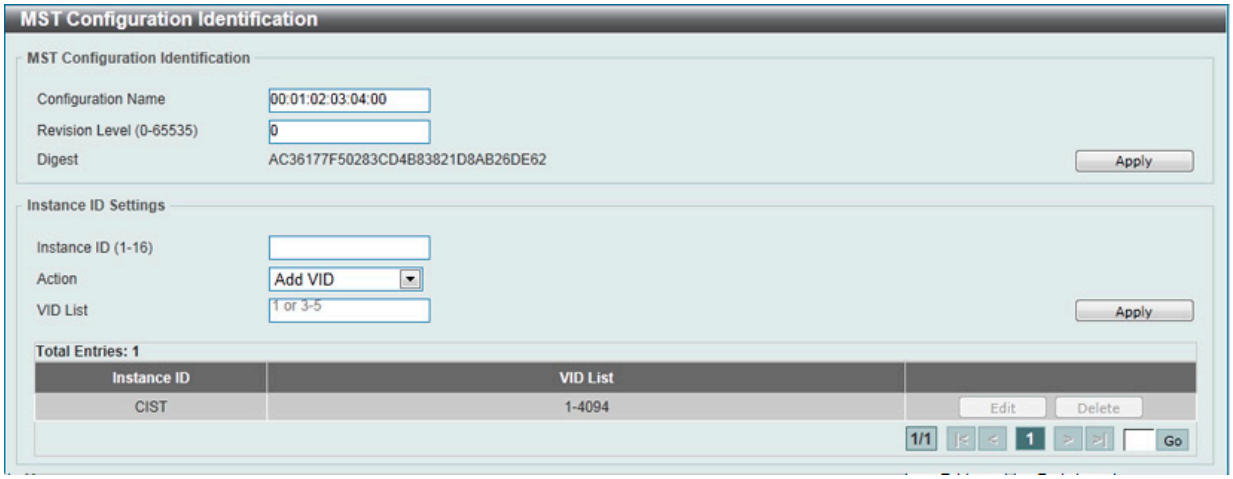


図 8-42　MST Configuration Identification 画面

上記画面には以下の項目が含まれます。

項目	説明
Configuration Name	各 MSTI（Multiple Spanning Tree Instance）を識別するためにスイッチに名前を設定します。 名前が設定されていない場合、MSTP が動作しているデバイスの MAC アドレスが表示されます。
Revision Level	スイッチ上に設定された MST リージョンの値 (0-65535) を設定します。初期値は 0 です。「Configuration Name」とともに MSTP リージョンの識別に使用されます。
Instance ID	1-16 の番号を入力し、スイッチに Instance ID を設定します。
Action	MSTI に行う変更を選択します。 • Add VID - VID List 項目に指定された VID を MSTI ID に追加します。 • Remove VID - VID List 項目に指定された VID を MSTI ID から削除します。
VID List	VLAN の VID の範囲を指定します。

「Apply」ボタンをクリックし、設定を適用します。

エントリの編集

1. 編集するエントリ横の「Edit」ボタンをクリックします。
2. 現在の設定が表示されます。設定変更後、「Apply」ボタンをクリックします。

エントリの削除

削除するエントリ横の「Delete」ボタンをクリックします。

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。

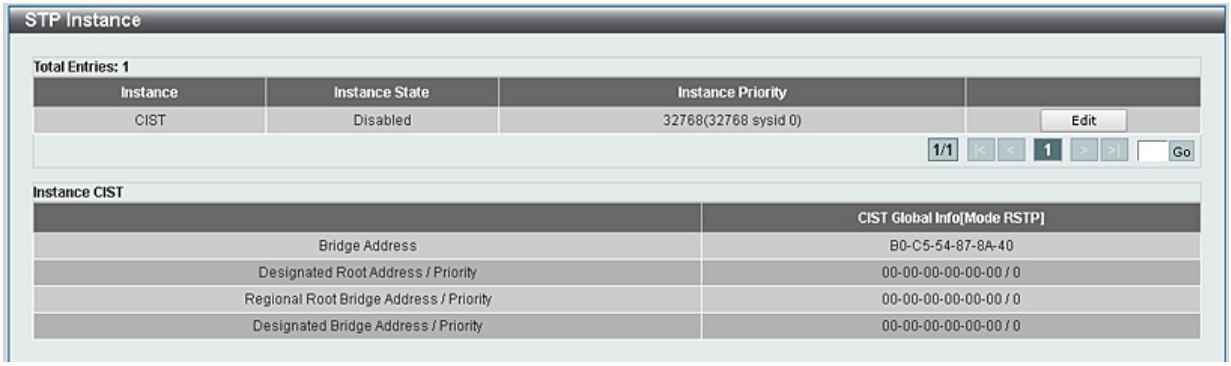


図 8-43　STP Instance 画面

エントリの編集

編集するエントリ横の「Edit」ボタンをクリックし、エントリの編集を行います。

MSTP Port Information（MSTP ポート情報）

現在の MSTP ポート情報の表示、およびポート構成の更新を行います。

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。

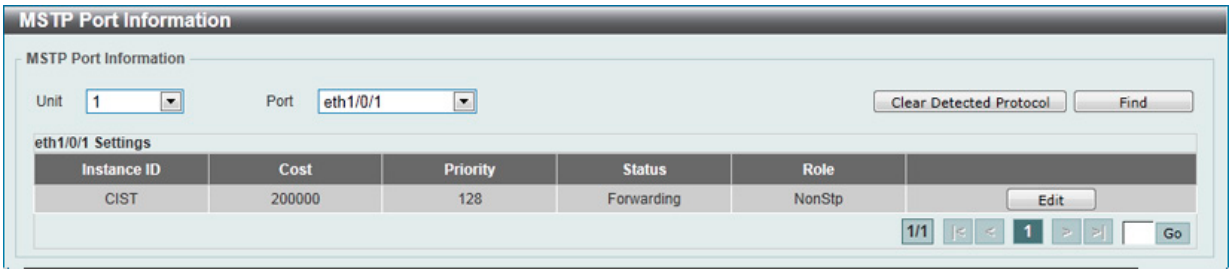


図 8-44　MSTP Port Information 画面

本画面には以下の情報があります。

項目	説明
Unit	設定するユニットを選択します。
Port	プルダウンメニューを使用して、ポートを選択します。

「Apply」ボタンをクリックし、新しい設定を適用します。

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

指定ポートの MSTP 設定の参照

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

指定ポートの MSTI インスタンス設定の編集

1. 特定の MSTI インスタンス設定を編集する場合は、編集する MSTI の「Edit」ボタンをクリックします。
2. 現在の設定を編集し「Apply」ボタンをクリックします。

ERPS (G.8032)（イーサネットリングプロテクション設定）

ERPS（Ethernet Ring Protection Switching）はイーサネットリング保護スイッチングの業界標準 (ITU-T G.8032) です。これは、イーサネットリングネットワークに対して十分に考慮されたイーサネット操作、管理、およびメンテナンス機能と簡単な APS（automatic protection switching）プロトコルを統合することによって実行されます。ERPS はリングトポロジ内のイーサネットトラフィックに sub-50ms 保護を提供します。

注意　ポート毎の詳細については「【付録 E】ERPS 情報」をご確認ください。

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

ERPS

スイッチの ERPS 機能を有効にします。

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



図 8-45　ERPS 画面

上記画面には以下の項目が含まれます。

項目	説明
Ring Name	ERPS インスタンス名を入力します。32 文字まで指定可能です。

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

Ring の編集

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

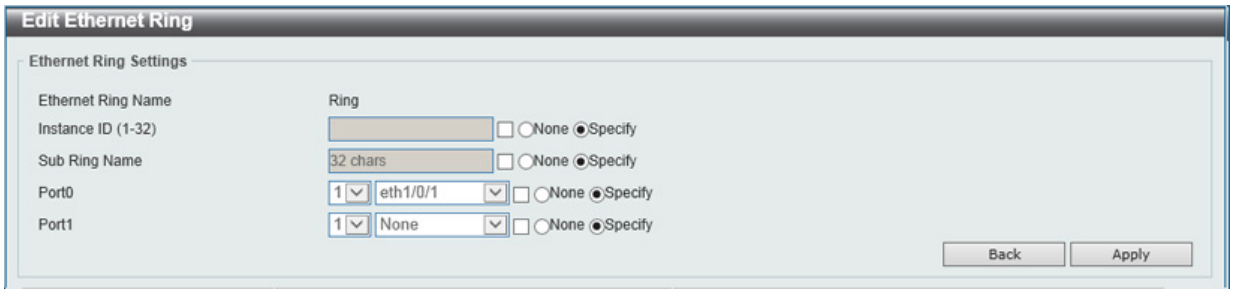


図 8-46　ERPS 画面 - Edit

設定対象となる項目は以下の通りです。

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

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

Instance の編集

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

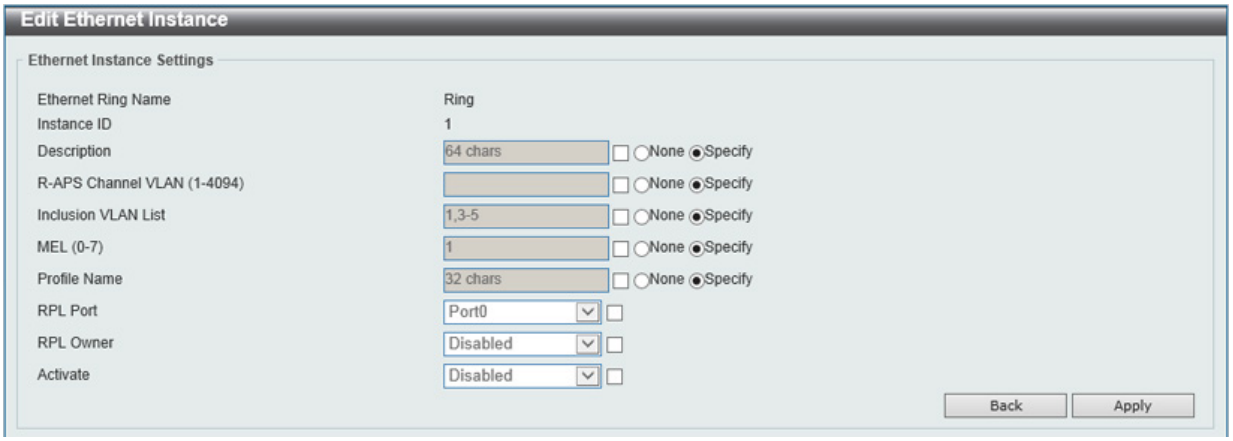


図 8-47　ERPS 画面 - Instance

設定対象となる項目は以下の通りです。

項目	説明
Description	チェックを入れ「ERP インスタンス」の概要を指定します。64 文字まで指定可能です。 「Specify」にチェックを入れパラメータを指定します。「None」にチェックを入れるとパラメータの値は初期値になります。
R-APS Channel VLAN	チェックを入れ「ERP インスタンス」の「R-APS Channel VLAN ID」を指定します。サブインスタンスの「APS channel VLAN」はサブリングの仮想チャネルでもあります。1 から 4094 までの間で指定可能です。 「Specify」にチェックを入れパラメータを指定します。「None」にチェックを入れるとパラメータの値は初期値になります。
Inclusion VLAN List	チェックを入れインスタンスに含まれる VLAN リストを指定します。 「-」を使用すると範囲として指定され、「,」を使用すると個別に複数の VLAN を指定します（例：「VLAN1 から 5」は「1-5」、「VLAN1 と 3 と 5」は「1,3,5」）。指定された VLAN は ERP のメカニズムで保護されます。 「Specify」にチェックを入れパラメータを指定します。「None」にチェックを入れるとパラメータの値は初期値になります。
MEL	チェックを入れ ERP インスタンスの「MEL」を指定します。0 から 7 までの間で指定可能です。 同じ ERP インスタンスに参加するすべてのリングノードの MEL 値は同一である必要があります。 「Specify」にチェックを入れパラメータを指定します。「None」にチェックを入れるとパラメータの値は初期値になります。
Profile Name	チェックを入れ ERP インスタンスに関連する「G.8032」のプロファイルを指定します。複数の ERP インスタンスを同じ G.8032 プロファイルに関連付けることも可能です。同じプロファイルに関連付けられたインスタンスは VLAN の同じセットを保護するか、もしくはあるインスタンスに保護される VLAN は、別のインスタンスに保護されている LAN のサブセットです。32 文字まで指定可能です。「Specify」にチェックを入れパラメータを指定します。「None」にチェックを入れるとパラメータの値は初期値になります。
RPL Port	チェックを入れ RPL ポートオプションを選択します。オプションは「Port0」「Port1」から指定します。 選択されたオプションは RPL ポートとして設定されます。
RPL Owner	チェックを入れノードが RPL オーナかネイバかを選択します。「Enable/Disable」から選択し、「Enable」の場合、RPL は「オーナ」として設定されます。
Activate	チェックを入れ ERP インスタンスをアクティブにするか選択します。「Enable/Disable」から選択し、「Enable」の場合、ERP インスタンスはアクティブになります。

「Back」をクリックすると設定は破棄され前画面に戻ります。

「Apply」をクリックして設定を適用します。

Status の表示

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

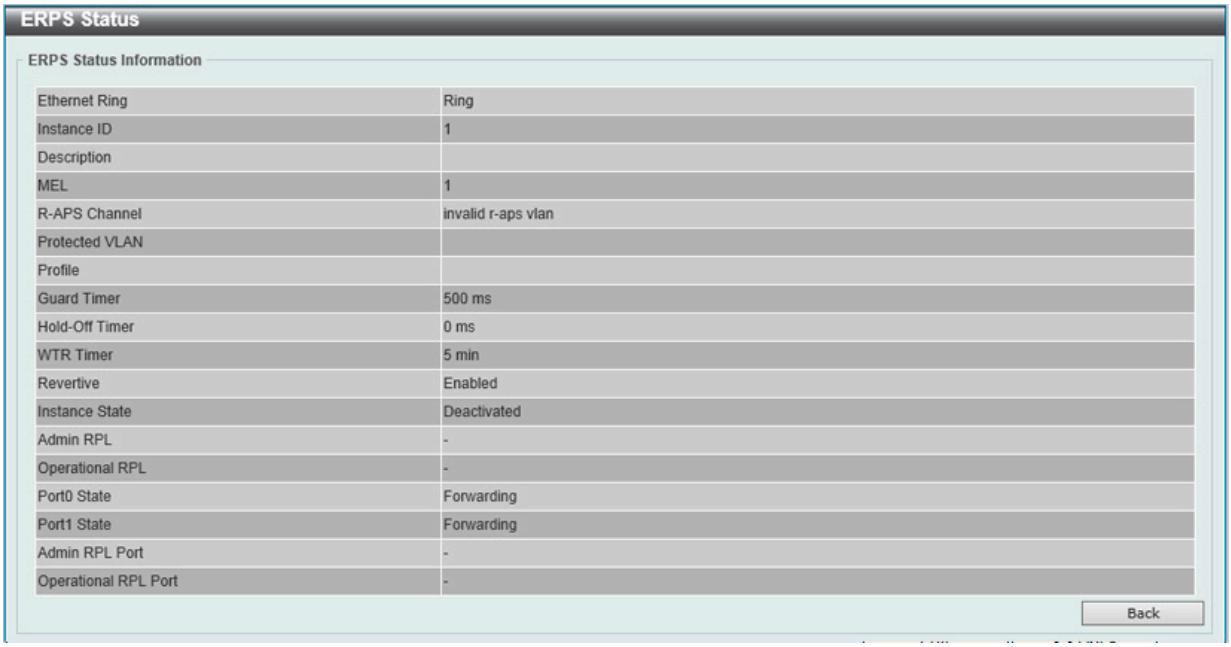


図 8-48　ERPS Staus 画面

「Back」をクリックすると前画面に戻ります。

ERPS Profile（ERPS プロファイル）

ERPS プロファイル設定を行います。

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

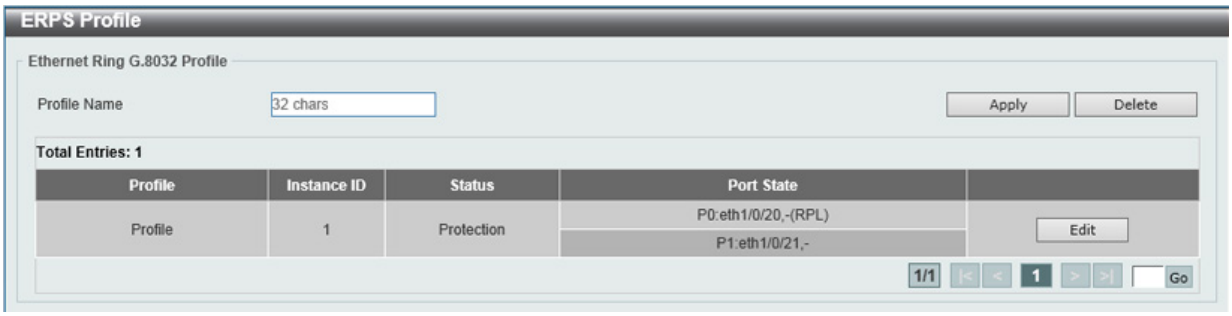


図 8-49　ERPS Profile 画面

設定対象となる項目は以下の通りです。

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

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

「G.8032」プロファイルの編集

「Edit 」ボタンをクリックすると、以下の設定画面が表示されます。

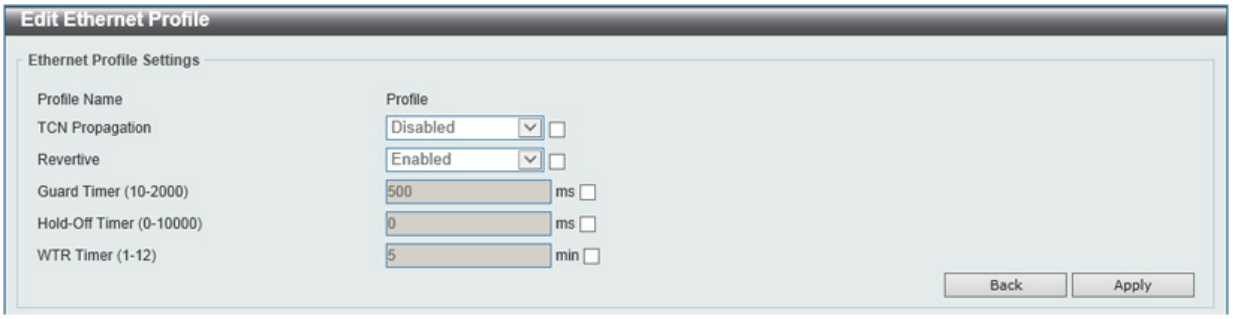


図 8-50　「G.8032」プロファイル画面 - Edit

設定対象となる項目は以下の通りです。

項目	説明
TCN Propagation	チェックを入れ「TCN Propagation」の設定を行います。「Enable/Disable」から選択します。 本機能はサブ ERP インスタンスからメジャーインスタンスへのトポロジ変更の通知の伝播を有効にします。
Revertive	チェックを入れ「Revertive」の設定を行います。「Enable/Disable」から選択します。本機能は運用系トランスポートエンティティに戻すために使用されます。例えば RPL がブロックされた場合などです。
Guard Timer	チェックを入れ Guard Timer の設定を行います。10 から 2000（ミリ秒）の間で指定可能です。初期値は 500（ミリ秒）です。
Hold-Off Timer	チェックを入れ Hold-Off Timer の設定を行います。0 から 10000（ミリ秒）の間で指定可能です。初期値は 0（ミリ秒）です。
WTR Timer	チェックを入れ WTR Timer の設定を行います。1 から 12（分）の間で指定可能です。初期値は 5（分）です。

「Back」をクリックすると設定は破棄され前画面に戻ります。

「Apply」をクリックして設定を適用します。

Loopback Detection（ループバック検知設定）

ループバック検知機能は、特定のポートによって生成されるループを検出するために使用されます。
本機能は、CTP（Configuration Testing Protocol）パケットがスイッチにループバックすると、スイッチのポートを一時的にシャットダウンします。スイッチが CTP パケットをポートまたは VLAN から受信したことを検知すると、ネットワークにループが発生していると認識します。スイッチは、自動的にポートまたは VLAN をブロックして管理者にアラートを送信します。ループバック検知機能は、一度に複数のポートの範囲に設定できます。ドロップダウンメニューを使用して本機能を有効 / 無効にすることができます。

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

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

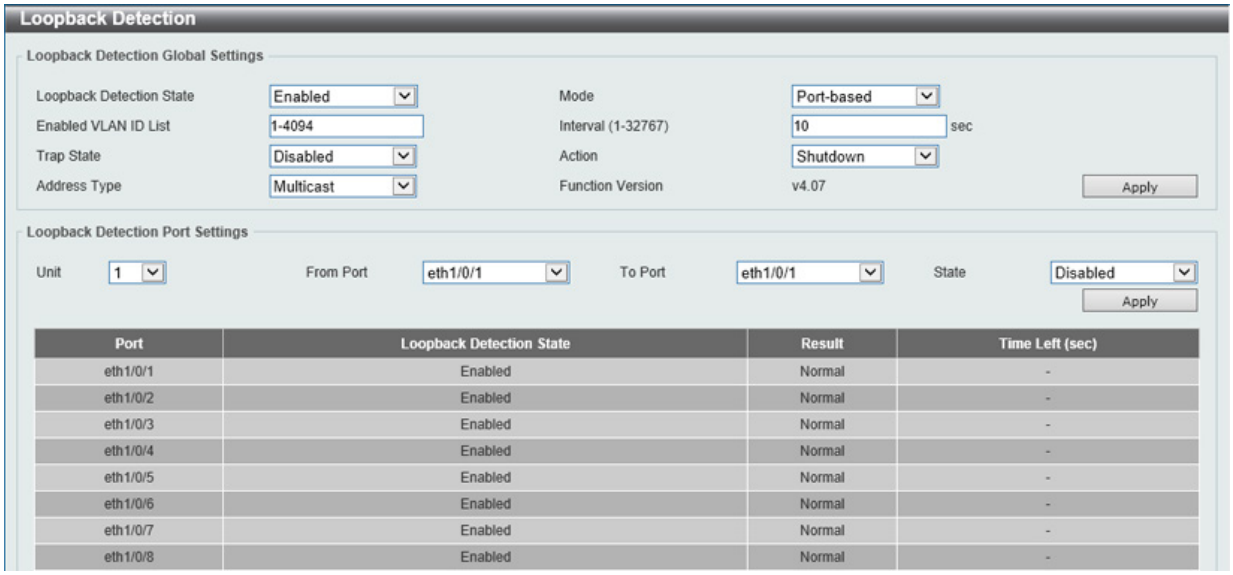


図 8-51　Loopback Detection Settings 画面

項目	説明
Loopback Detection State	ループバック検知機能を「Enabled」（有効）または「Disabled」（無効）にします。初期値は「Disabled」です。
Mode	プルダウンメニューで「Port Based」または「VLAN Based」を選択します。
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 (1-32767)	ループバックイベント検知のための CTP(Configuration Test Protocol) パケット送信間隔（1-32767 秒）です。 初期値は 10 秒です。
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	実行する動作を指定します。 • Shutdown - ループが検知された時に、ポートベースモードはポートをシャットダウン（無効化）します。VLAN モードでは特定の VLAN でトラフィックはブロックされます。 • None - ループが検知された時でも、ポートはシャットダウンされません（ポートベースモード）。VLAN でもトラフィックはブロックされません（VLAN モード）。ログとトラップメッセージのみが送信されます。
Address Type	アドレスタイプを指定します。ループバック検知のための LDB パケットの宛先アドレスタイプです。 • Multicast - マルチキャスト LBD パケットが送信されます。宛先アドレスは「CF-00-00-00-00-00」です。 • Broadcast - ブロードキャスト LBD パケットが送信されます。宛先アドレスは「FF-FF-FF-FF-FF-FF」です。
Unit	設定するユニットを指定します。
From Port	プルダウンメニューで開始ポートを選択します。
To Port	プルダウンメニューで終了ポートを選択します。
State	「Enabled」（有効）または「Disabled」（無効）を指定します。

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

注意 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。

Link Aggregation（リンクアグリゲーション）

ポートトランクグループについて

ポートトランクグループは、複数のポートを結合して 1 つの広帯域のデータパイプラインとして利用する機能です。トランクグループは最大 32 個まで作成可能であり、各グループには最大 8 個までの物理ポートを割り当てることができます。

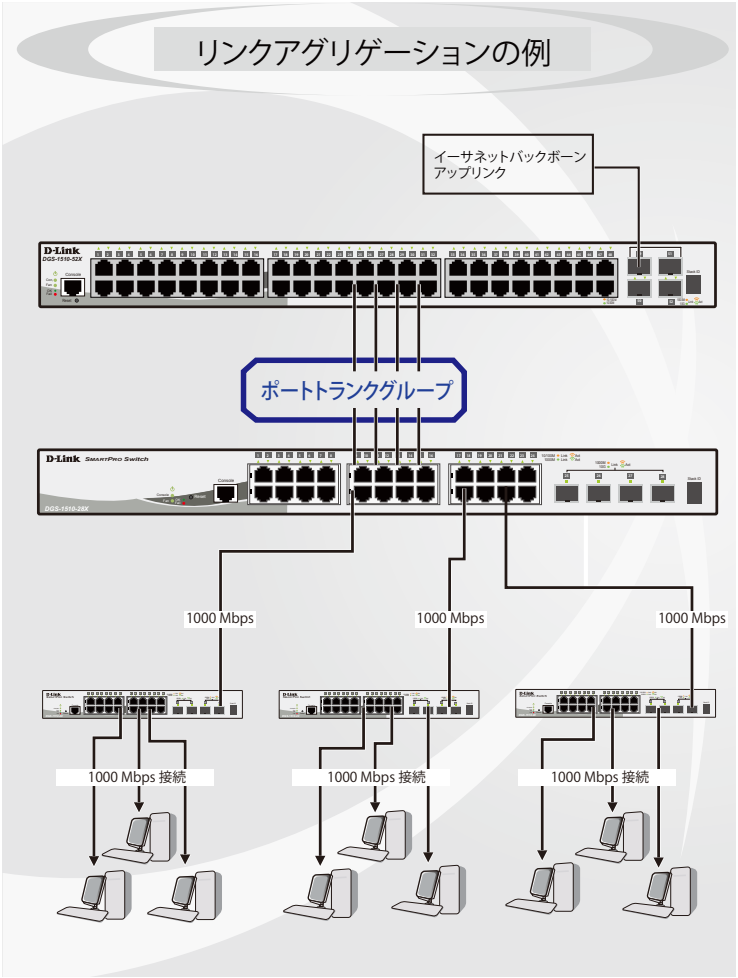


図 8-52　ポートトランクグループの例

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、最大 8 個のリンク（ポート）から構成される最大 32 個のリンクアグリゲーショングループの構築が可能です。各ポートは 1 つのリンクアグリゲーショングループにのみ所属することができます。

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

グループ内のポート間では自動的にロードバランスが行われ、グループ内でのリンク断が発生した場合、ネットワークトラフィックはグループ内の他のリンクに振り分けられます。

スパニングツリープロトコル（STP）は、スイッチレベルにおいて、リンクアグリゲーショングループを 1 つのリンクとして扱います。ポートレベルでは、STP はマスタポートのパラメータを使用してポートコストを計算し、リンクアグリゲーショングループの状態を決定します。スイッチに冗長化された 2 つのリンクアグリゲーショングループが設定されている場合、STP において片方のグループはブロックされます（冗長リンクを持つポートがブロックされるケースと同様）。

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

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

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

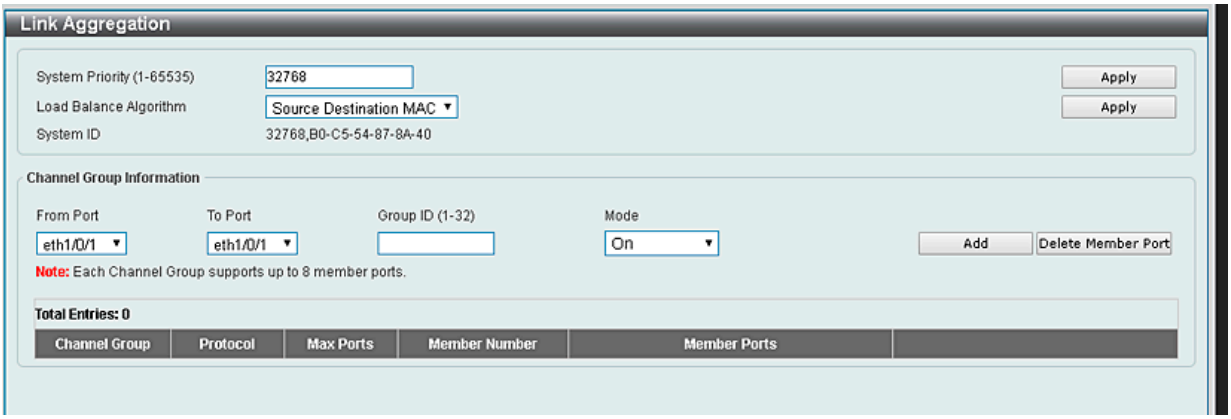


図 8-53　Link Aggregation 画面

本画面には次の項目があります。

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

指定のエントリを削除するためには、削除するグループの「Delete Channel」ボタンをクリックします。
指定のメンバポートを削除するためには、削除するグループの「Delete Member Port」ボタンをクリックします。
チャネルについてのより詳細な情報の確認には「Channel Detail」をクリックします。

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

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

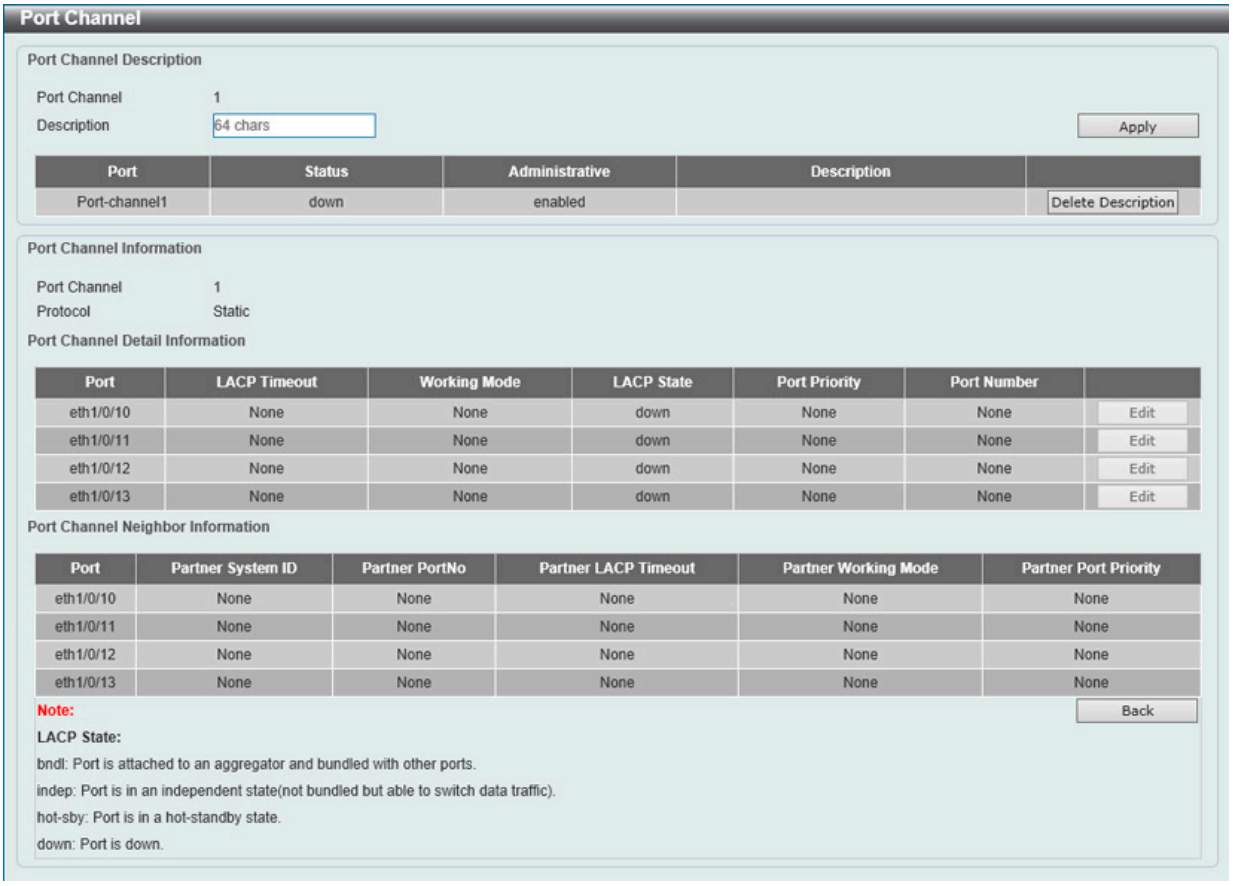


図 8-54　Port Channel 画面

「Description」で該当ポートチャンネルの概要（64 文字以内）を指定できます。
設定を変更する際は、必ず「Apply」ボタンをクリックし設定内容を適用してください。
「Delete Description」で該当ポートチャンネルの概要（64 文字以内）を削除できます。
編集するグループの「Edit」ボタンをクリックします。
「Back」ボタンをクリックし前の画面に戻ります。

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

IGMP Snooping（IGMP スヌーピング）

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

IGMP Snooping Settings（IGMP スヌーピング設定）

IGMP Snooping 設定を有効または無効にします。

IGMP Snooping 機能を利用するためには、まず、画面上部の IGMP の「Global Settings」セクションでスイッチ全体に機能を有効にします。「Edit」ボタンをクリックして、各 VLAN の設定を編集することができます。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対するポートを開閉できるようになります。スイッチは IGMP メッセージをモニタして、マルチキャストパケットを要求しているホストがもう存在していないと判断すると、マルチキャストパケットの送信を停止します。

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

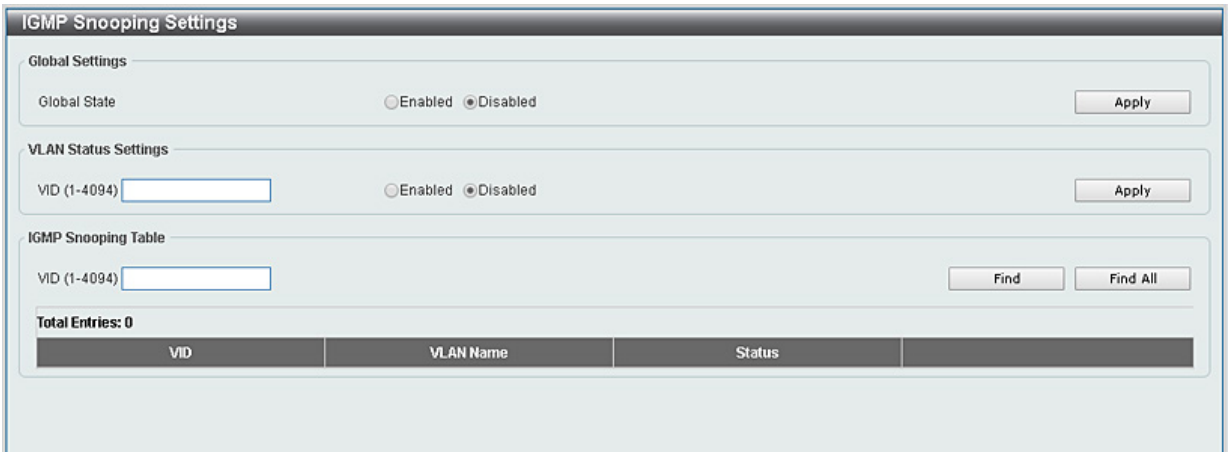


図 8-55　IGMP Snooping Settings 画面

画面には以下の項目があります。

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

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

IGMP Snooping VLAN の詳細情報表示

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

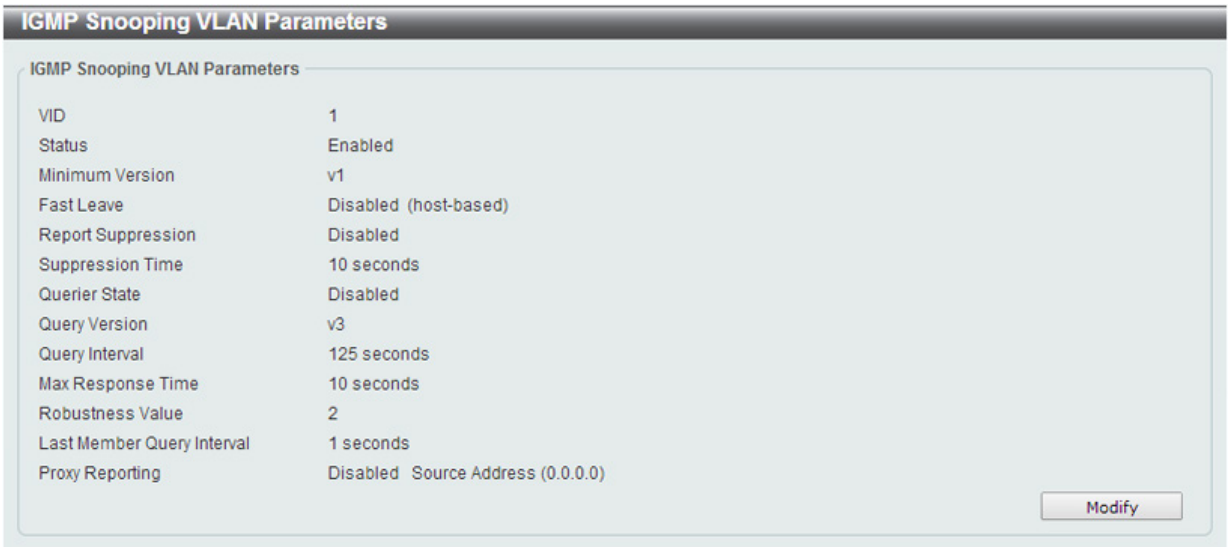


図 8-56　IGMP Snooping VLAN Parameters 画面

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

IGMP Snooping 機能の詳細設定

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

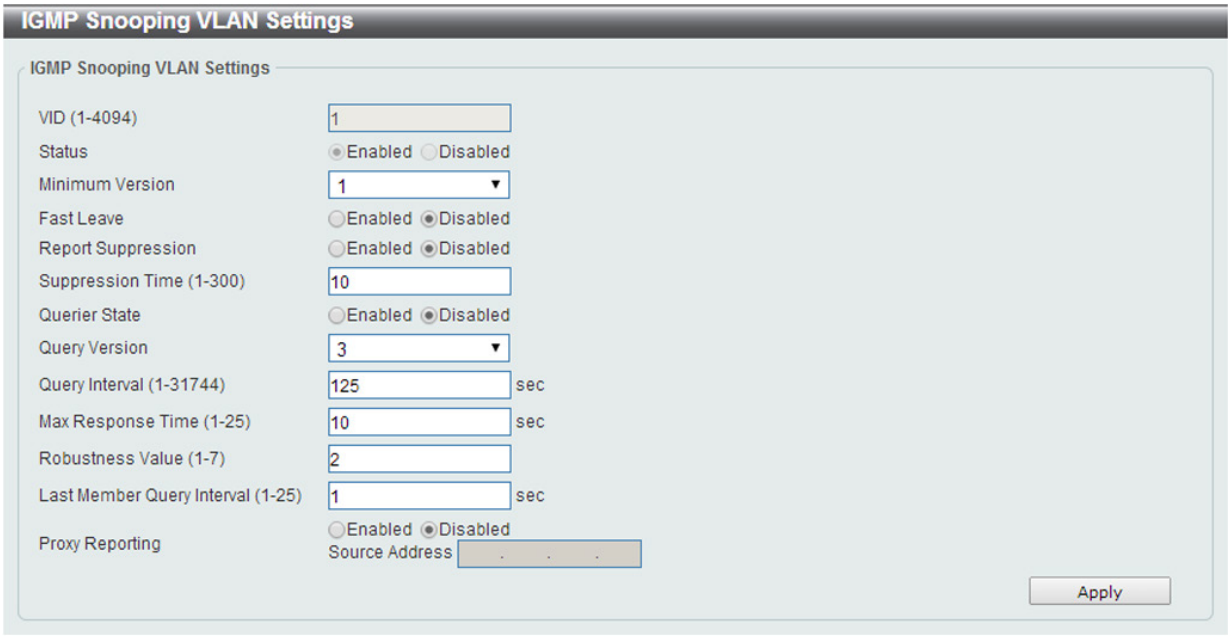


図 8-57 IGMP Snooping VLAN Settings 画面

以下の項目が表示、または設定変更に使用できます。

項目	説明
VID	IGMP Snooping 設定を変更する VLAN を識別する VLAN ID を表示します。
State	指定した VLAN の IGMP Snooping 機能の状況（有効 / 無効）について表示します。
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。
Fast Leave	「Enabled」（有効）にすると、Fast Leave 機能が有効になります。この機能が有効になると、スイッチが IGMP Leave Report パケットを受信する時、マルチキャストグループのメンバは（Last Member Query Time の失効を待たずに）直ちにグループから脱退します。初期値は「Disabled」（無効）です。
Report Suppression	特定の VLAN への IGMP スヌーピングレポートの抑制を「Enabled」（有効）/「Disabled」（無効）にします。 レポート抑制機能は「IGMPv1」「IGMPv2」トラフィックでのみ機能します。 レポート抑制機能が有効になっている場合、スイッチはホストから送信された重複レポートを抑制し、抑制時間が終了するまで、同じグループレポートまたは離脱メッセージの抑止が継続します。同じグループへのレポートもしくは離脱メッセージは、1 つのレポートもしくは離脱メッセージだけが転送されます。残りのレポートと離脱メッセージは抑制されます。

項目	説明
Suppression Time	重複 IGMP レポートもしくは離脱メッセージの抑制時間を設定します。1 から 300（秒）で設定可能です。
Querier State	クエリアを有効 / 無効にします。
Query Version	IGMP スヌーピングクエリアにより送信される General クエリパケットのバージョンを選択します。「1」「2」「3」から選択可能です。
Query Interval	IGMP スヌーピングクエリアが、IGMP General クエリメッセージを定期的に送信する間隔を入力します。1-31744 の範囲から指定します。初期値は 125 です。
Max Response Time (1-25)	IGMP 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秒で入力します。1-25 の範囲から指定します。初期値は 10（秒）です。
Robustness Value (1-7)	IGMP スヌーピングで使用されるロバストネス変数。初期値は 2 です。
Last Member Query Interval (1-25)	IGMP スヌーピングクエリアが、IGMP グループ独自もしくは送信元グループ独自のクエリメッセージを送信する間隔を入力します。初期値は 1 です。
Proxy Reporting	プルダウンメニューを使用して、本機能を「Enabled」（有効）/「Disabled」（無効）にします。
Source Address	プロキシレポーティングの送信元 IP アドレスを指定します。

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

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

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

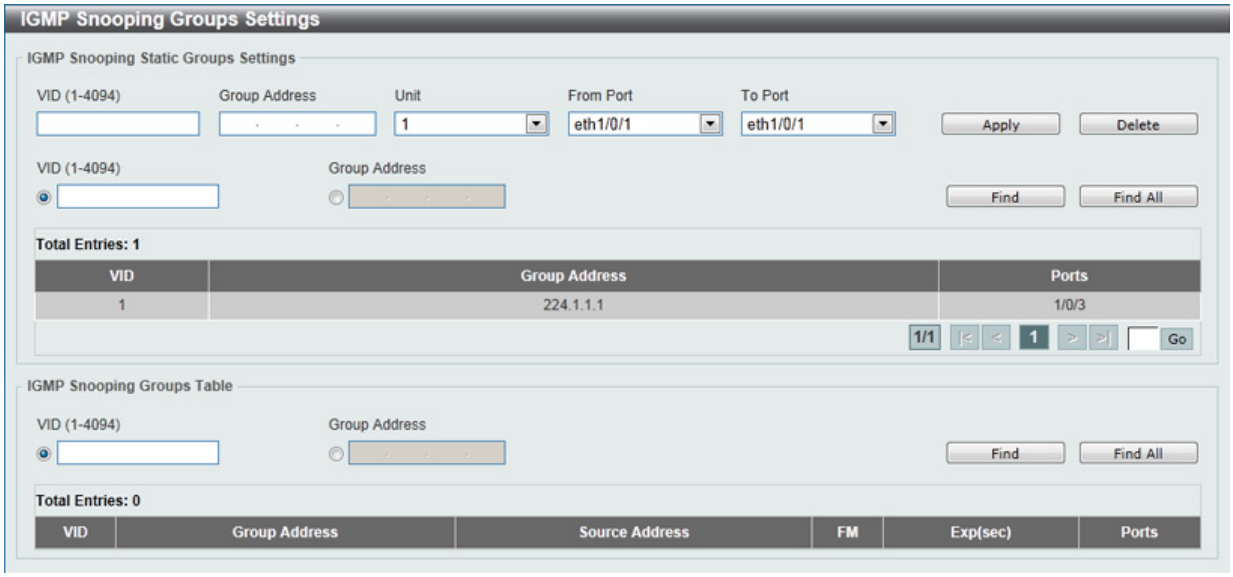


図 8-58　IGMP Snooping Group Settings 画面

以下の項目を使用して、設定します。

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

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

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

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

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

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

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

指定インタフェースをマルチキャストルータポートもしくはマルチキャストルータポートにならないように設定します。

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

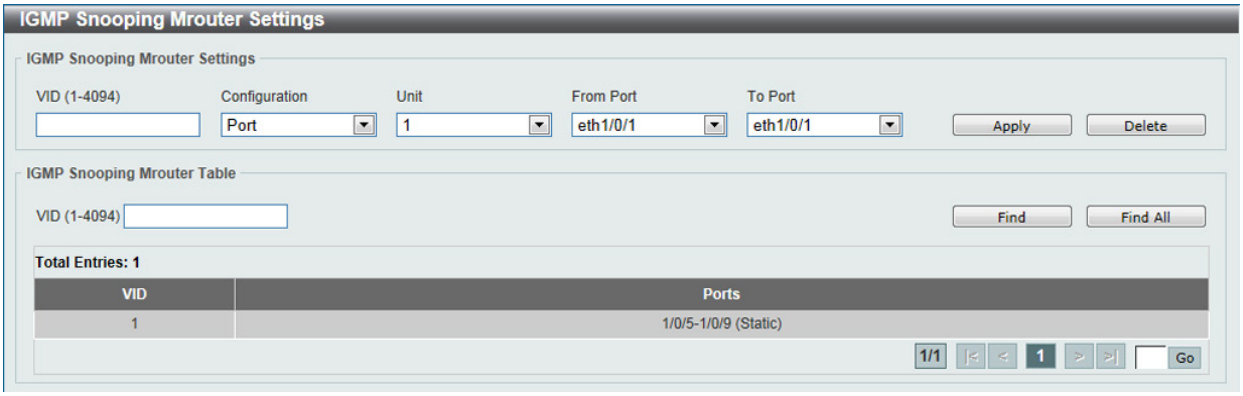


図 8-59　IGMP Snooping Mrouter Settings 画面

画面には以下の項目があります。

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

項目	説明
IGMP Snooping Mrouter Settings	
VID	VLAN ID を入力します。
Configuration	ポートの設定を行います。「Port」「Forbidden Port」から選択します。 • Port - 指定したポートをスタティックマルチキャストルータポートにする場合に選択します。 • Forbidden Router Port - 指定したポートがマルチキャストルータポートにならないようにする場合に選択します。
Unit	設定するユニットを選択します。
From Port / To Port	設定するポートの範囲を設定します。

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

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

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

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

IGMP Snooping Statistics Settings（IGMP Snooping 統計設定）

現在の IGMP Snooping の統計情報を表示します。

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

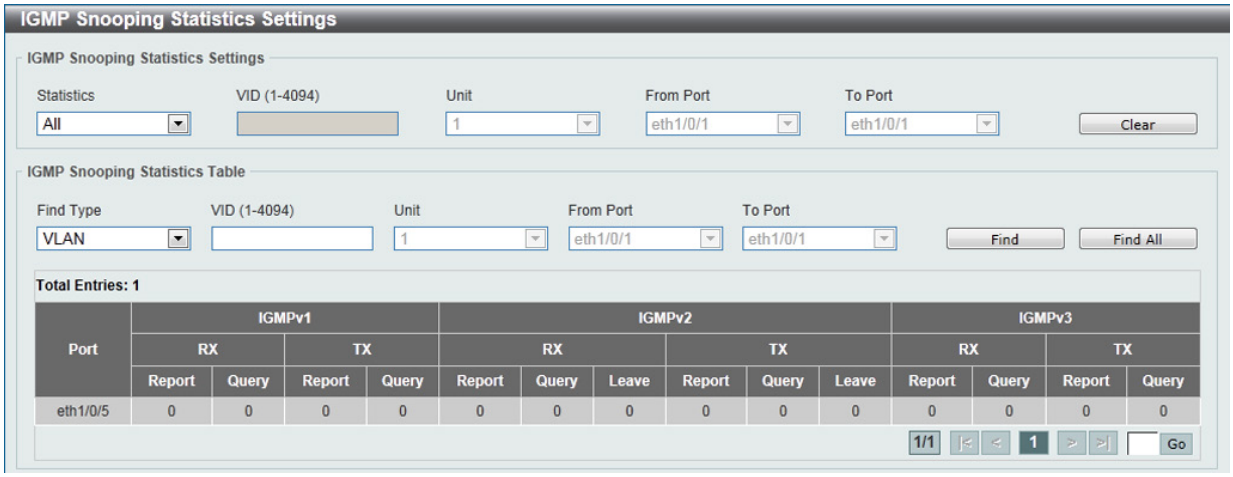


図 8-60　IGMP Snooping Statistics Settings 画面

以下の項目が表示されます。

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

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

「Clear」をクリックすると表示された統計情報がクリアされます。

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

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

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

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

MLD Snooping Settings（MLD スヌーピング）

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

MLD コントロールメッセージ

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

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

MLD Snooping Settings（MLD スヌーピング設定）

MLD Snooping 設定を有効または無効にします。

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

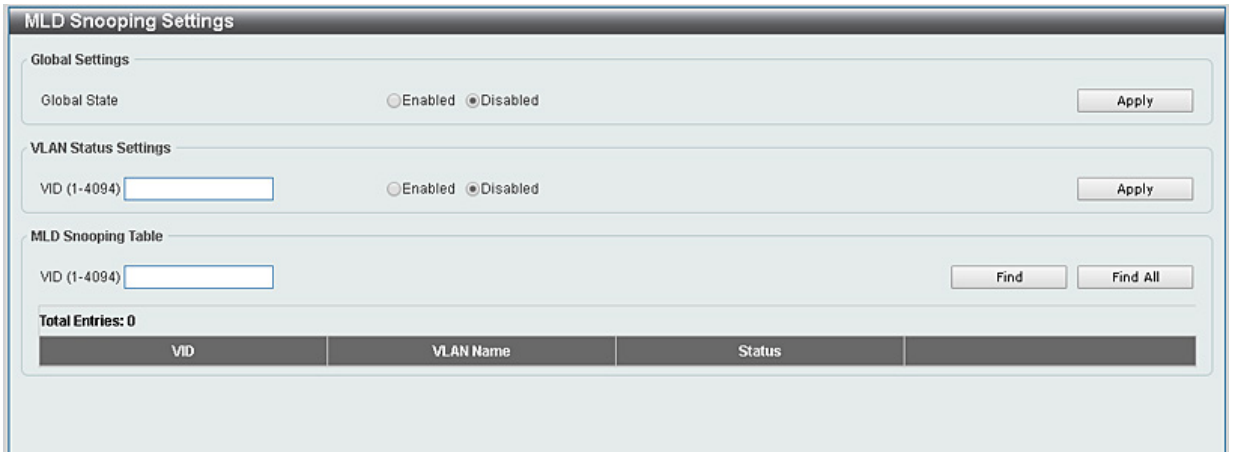


図 8-61　MLD Snooping Settings 画面

画面には以下の項目があります。

項目	説明
Global Setting	
Global State	MLD Snooping の有効 / 無効を設定します。 • Enabled - デバイスで MLD Snooping を有効にします。 • Disabled - デバイスで MLD Snooping を無効に設定します。（初期値）

項目	説明
VLAN Status Settings	
VID	VLAN 上の MLD Snooping を有効 / 無効にし、VLAN を識別する VLAN ID を指定します。 • Enabled - VLAN 上での MLD スヌーピングを有効にします。 • Disabled - VLAN での MLD スヌーピングを無効にします。（初期値）
MLD Snooping Table	
VID	MLD Snooping Table 上の VLAN を表示させるための VLAN ID を指定します。

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

MLD Snooping VLAN の詳細情報表示

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

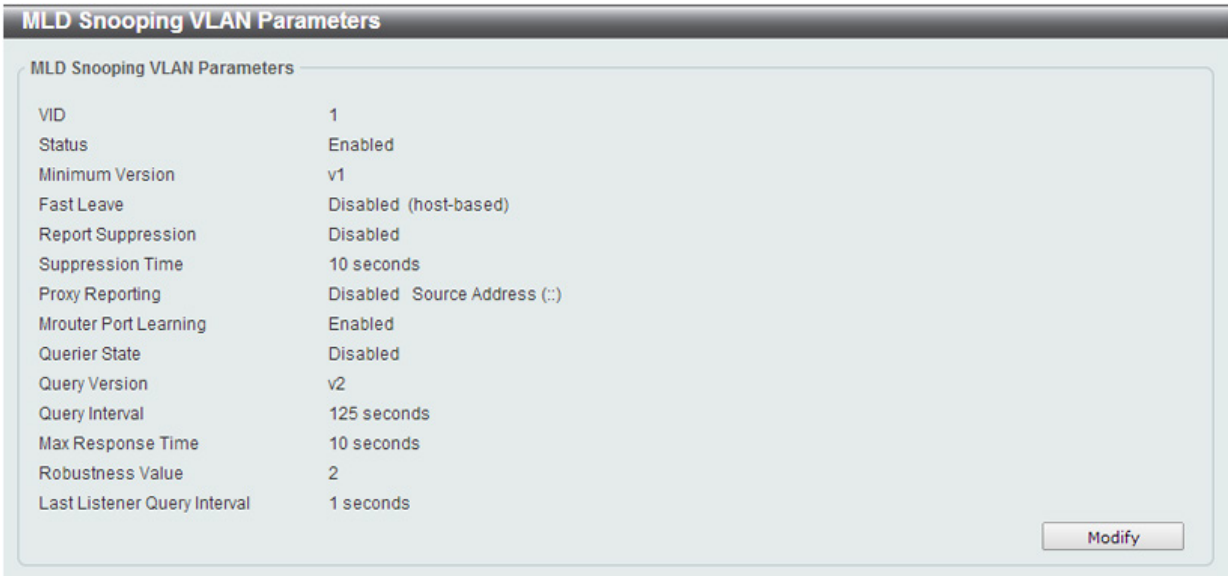


図 8-62　MLD Snooping VLAN Parameters 画面

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

MLD Snooping 機能の詳細設定

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

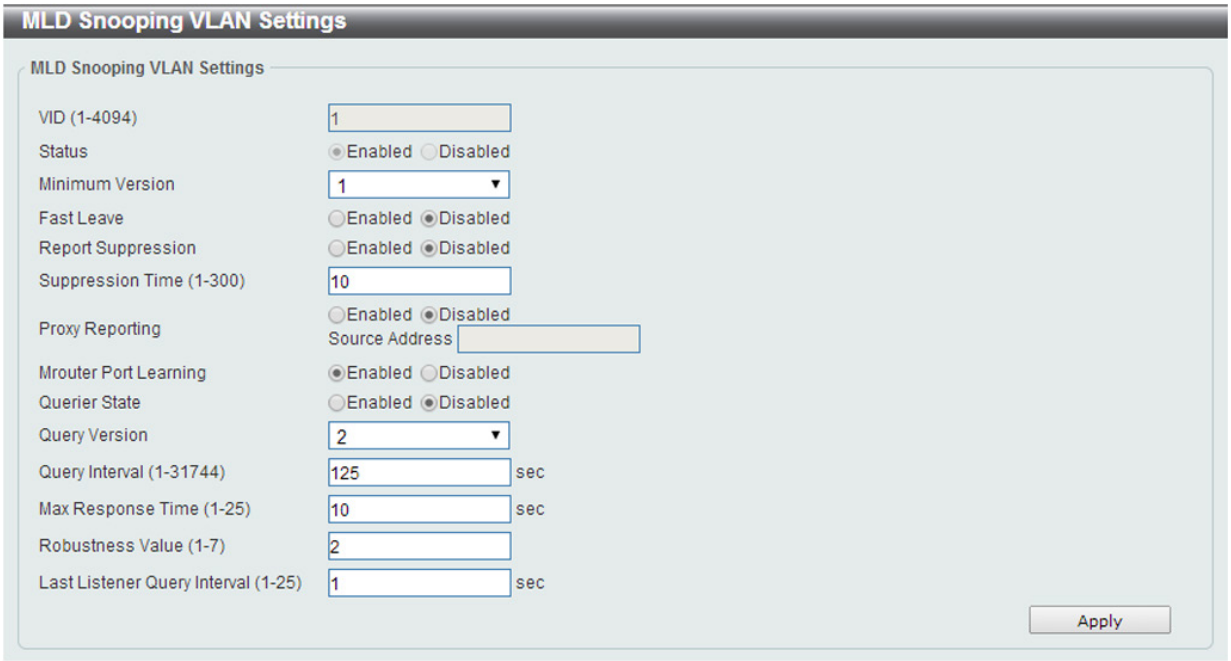


図 8-63 MLD Snooping VLAN Settings 画面

以下の項目が表示、または設定変更に使用できます。

項目	説明
VID	MLD Snooping 設定を変更する VLAN を識別する VLAN ID を表示します。
Status	指定した VLAN の MLD Snooping 機能の状況（有効 / 無効）について表示します。
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。
Fast Leave	「Enabled」（有効）にすると、Fast Leave 機能が有効になります。この機能が有効になると、スイッチが MLD Leave Report パケットを受信する時、マルチキャストグループのメンバは（Last Member Query Time の失効を待たずに）直ちにグループから脱退します。初期値は「Disabled」（無効）です。
Report Suppression	特定の VLAN への MLD スヌーピングレポートの抑制を「Enabled」（有効）/「Disabled」（無効）にします。 レポート抑制機能は「MLDv1」「MLDv2」トラフィックでのみ機能します。 レポート抑制機能が有効になっている場合、スイッチはホストから送信された重複レポートを抑制し、抑制時間が終了するまで、同じグループレポートまたは離脱メッセージの抑止が継続します。同じグループへのレポートもしくは離脱メッセージは、1 つのレポートもしくは離脱メッセージだけが転送されます。残りのレポートと離脱メッセージは抑制されます。
Suppression Time	重複 MLD レポートもしくは離脱メッセージの抑制時間を設定します。1 から 300（秒）で設定可能です。
Proxy Reporting	プルダウンメニューを使用して、本機能を「Enabled」（有効）/「Disabled」（無効）にします。
Source Address	プロキシレポーティングの送信元 IP アドレスを指定します。
Mrouter Port Learning	マルチキャストルータポートラーニングを有効 / 無効にします。
Querier State	クエリアを有効 / 無効にします。
Query Version	MLD スヌーピングクエリアにより送信される General クエリパケットのバージョンを選択します。「1」「2」から選択可能です。
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定期的に送信する間隔を入力します。1-31744 の範囲から指定します。初期値は 125 です。
Max Response Time (1-25)	MLD 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秒で入力します。1-25 の範囲から指定します。初期値は 10（秒）です。
Robustness Value (1-7)	MLD スヌーピングで使用されるロバストネス変数。初期値は 2 です。
Last Listener Query Interval	MLD スヌーピングクエリアが、MLD グループ独自もしくは送信元グループ独自のクエリメッセージを送信する間隔を入力します。初期値は 1 です。

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

MLD Snooping Group 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設定と表示および MLD スヌーピンググループの表示に使用されます。

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

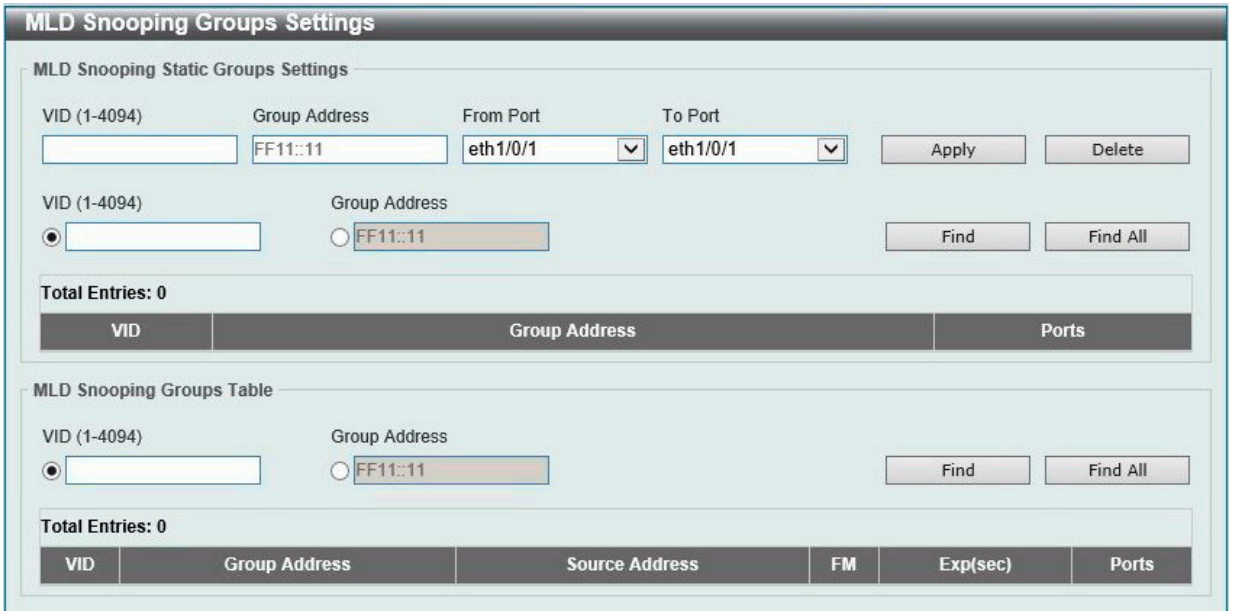


図 8-64　MLD Snooping Group Settings 画面

以下の項目を使用して、設定します。

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

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

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

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

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

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

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

本項目では指定インタフェースをルータポートとして、もしくはスイッチの VLAN インタフェースの IPv6 マルチキャストルータポートになるのを禁止する設定を行います。

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

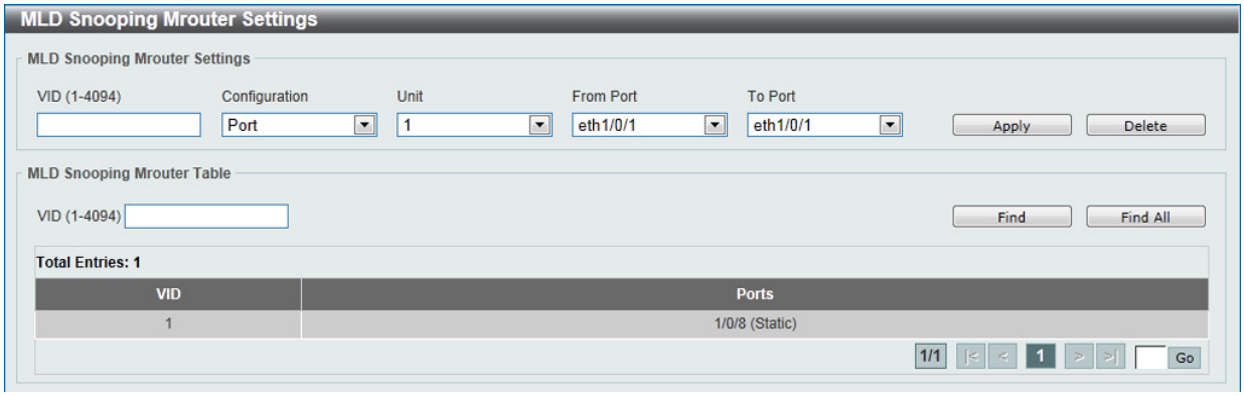


図 8-65　MLD Snooping Mrouter Settings 画面

画面には以下の項目があります。

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

項目	説明
MLD Snooping Mrouter Settings	
VID	VLAN ID を入力します。
Configuration	ポートの設定を行います。「Port」「Forbidden Port」「Learn pimv6」から選択します。 • Port - 指定したポートをスタティックマルチキャストルータポートにする場合に選択します。 • Forbidden Router Port - 指定したポートがマルチキャストルータポートにならないようにする場合に選択します。 • Learn pimv6 - マルチキャストルータポートの自動取得を有効にします。
Unit	設定するユニットを選択します。
From Port / To Port	設定するポートの範囲を設定します。

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

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

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

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

MLD Snooping Statistics Settings（MLD Snooping 統計設定）

現在の MLD Snooping の統計情報を表示します。

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

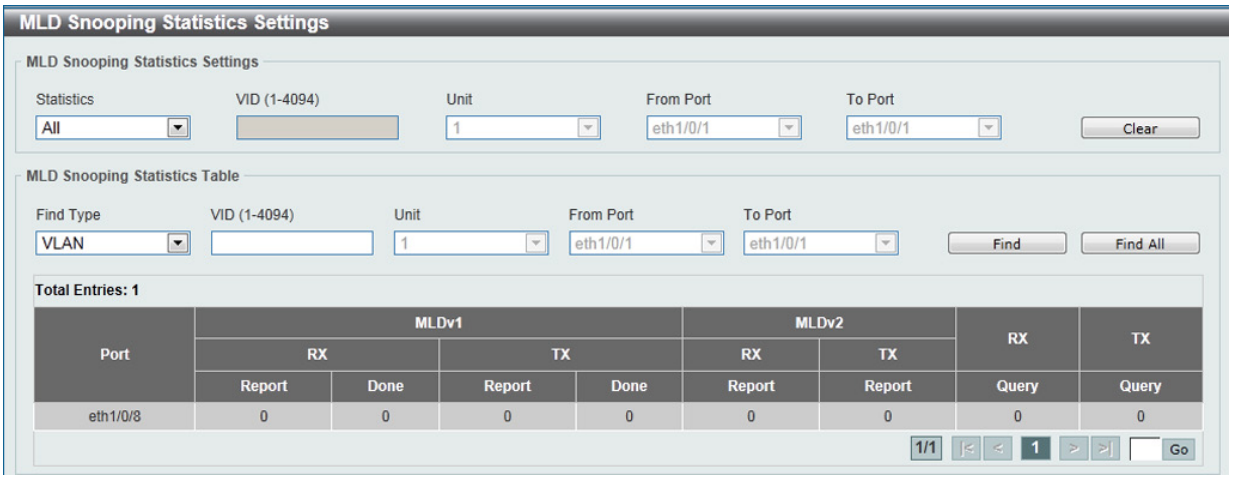


図 8-66　MLD Snooping Statistics Settings 画面

以下の項目が表示されます。

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

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

「Clear」をクリックすると表示された統計情報がクリアされます。

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

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

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

Multicast Filtering（マルチキャストフィルタリング）

本項目では L2 マルチキャストフィルタリングを表示、設定します。

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

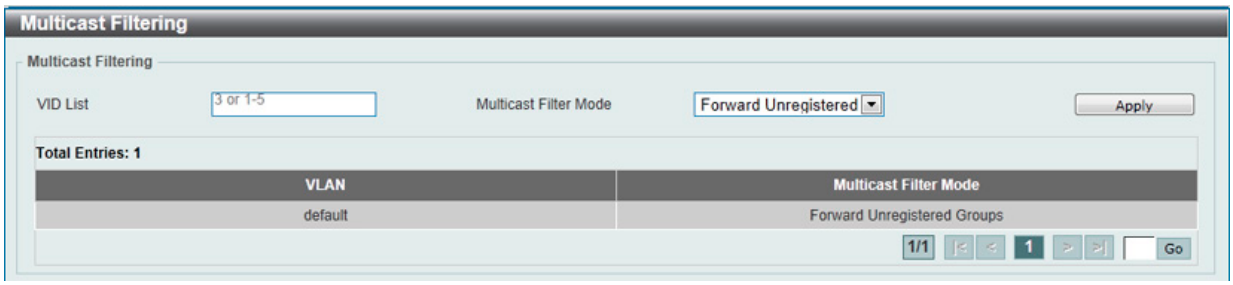


図 8-67　Multicast Filtering 画面

以下の項目を使用して、設定します。

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

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

LLDP（LLDP 設定）

LLDP（Link Layer Discovery Protocol）は、IEEE 802 ネットワークに接続しているステーションから同じ IEEE 802 ネットワークに接続している他のステーションに通知を出します。本プロトコルによって送信される情報は、受信先によって標準の管理情報ベース（MIB）に格納されるので、SNMP（Simple Network Management Protocol）などの管理プロトコル使ったネットワーク管理システム（NMS）からその情報にアクセスできるようになります。

LLDP Global Settings（LLDP グローバル設定）

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

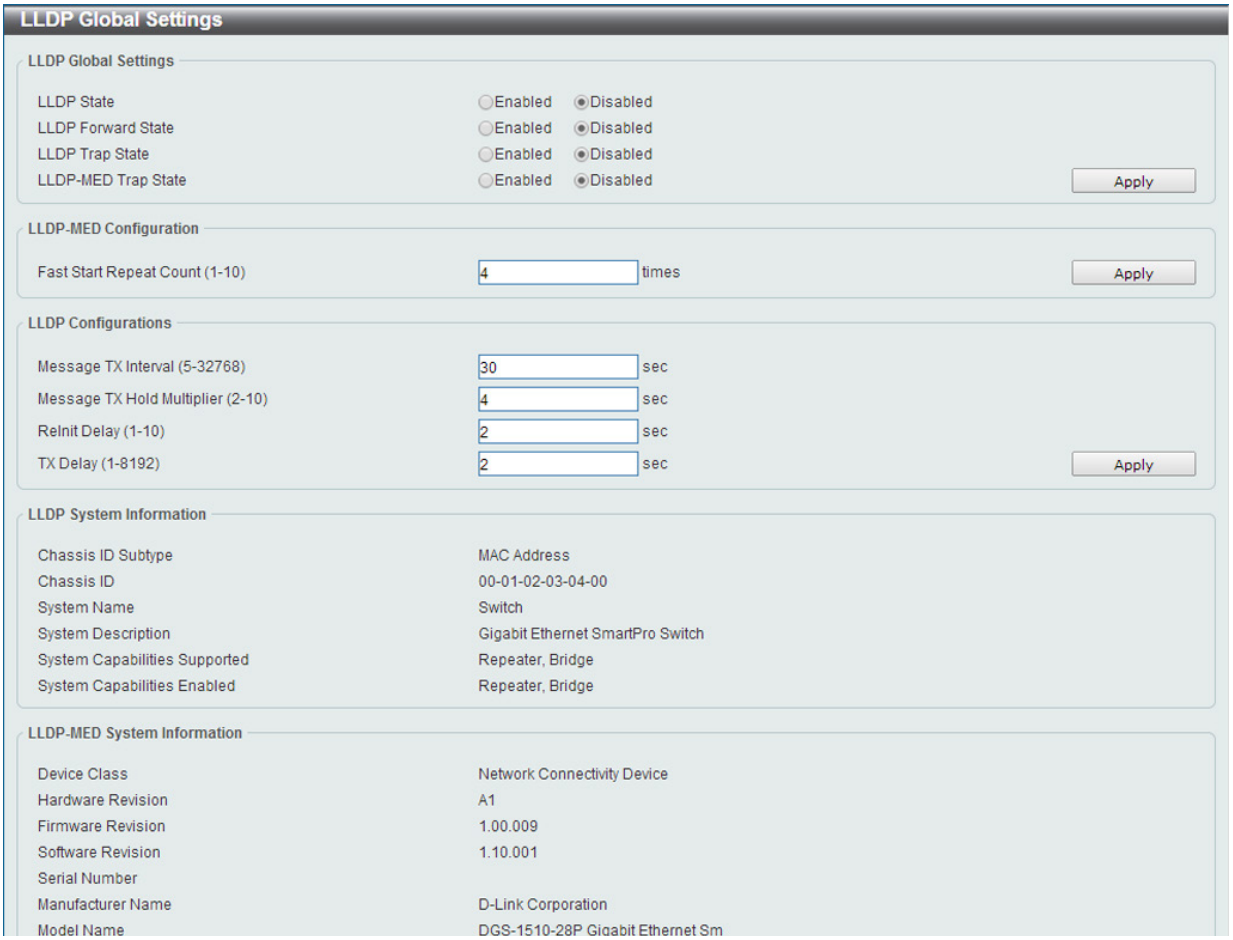


図 8-68　LLDP Global Settings 画面

以下の項目を設定できます。

項目	説明
LLDP State	スイッチにおける LLDP 機能を「Enabled」（有効）または「Disabled」（無効）にします。
LLDP Forward State	同じ IEEE 802 ネットワークに割り当てられた他のステーションに通知するために LLDP 機能のメッセージ転送を「Enabled」（有効）または「Disabled」（無効）にします。 「LLDP」が 無効で「LLDP Forward Sate」が有効の場合、受信した「LLDPDU」パケットは転送されます。
LLDP Trap State	LLDP Trap を有効 / 無効に指定します。
LLDP-MED Trap State	LLDP-MED Trap を有効 / 無効に指定します。
Fast Start Repeat Count	「LLDP-MED」ファストスタートリピートカウント値を指定します。1 から 10 の間で指定できます。
Message TX Interval (5-32768)	各物理インタフェース上での LLDP アドバタイズの連続送信間隔を入力します。5-32768（秒）の範囲で値を入力します。
Message TX Hold Multiplier (2-10)	LLDPDU の TTL 値を計算するために使用された LLDPDUs 送信間隔の乗数を入力します。2-10 から値を入力します。
Relnit Delay (1-10)	インタフェース上の LLDP 初期化の遅延値を入力します。1-10（秒）から値を入力します。
TX Delay (1-8192)	連続する LLDPDU をインタフェースに送信するための遅延値を入力します。有効な値は 1-8192 秒で、送信間隔タイマの 4 分の 1 を超えてはいけません。

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

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。

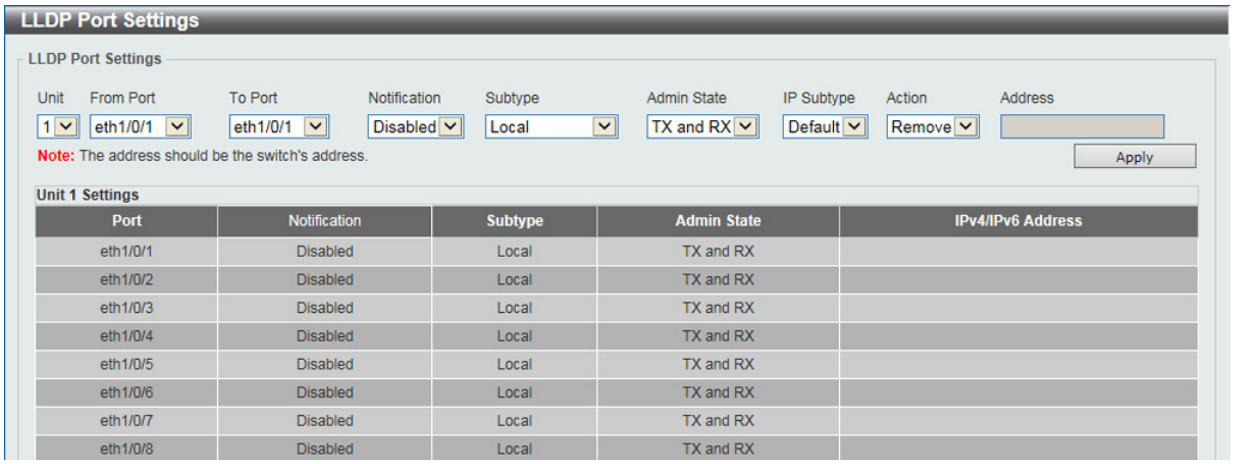


図 8-69　LLDP Port Settings 画面

以下の項目を設定できます。

項目	説明
Unit	設定するユニットを指定します。
From Port/To Port	プルダウンメニューを使用して設定するポート範囲を指定します。
Notification	プルダウンメニューを使用して LLDP 通知を「Enabled」（有効）または「Disabled」（無効）にします。
Subtype	プルダウンメニューを使用して LLDP TLV(s) のサブタイプを選択します。「MAC Address」「Local」から選択可能です。
Admin State	ローカル LLDP エージェントを選択し、ポート上で LLDP フレームを送受信できるようにします。: Tx（送信のみ）、Rx（受信のみ）、Tx And Rx（送受信）または「Disabled」（無効）。 • TX - ローカル LLDP エージェントは LLDP フレーム送信のみします。 • RX - ローカル LLDP エージェントは LLDP フレーム受信のみします。 • TX and RX - ローカル LLDP エージェントは LLDP フレームの送受信をします。（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しません。
IP Subtype	プルダウンメニューを使用して送信する IP アドレスの種類を選択します。「Default」「IPv4」「IPv6」から指定します。
Action	設定内容を指定ポート / ポート範囲に「Add（追加）/Remove（削除）」します。
Address	送信される IP アドレスを入力します。

「Apply」ボタンをクリックし、変更を有効にします。

注意　ここで入力される IPv4 もしくは IPv6 アドレスは既存の LLDP 管理 IP アドレスである必要があります。

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

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



図 8-70　LLDP Management Address List 画面

以下の項目を設定できます。

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

「Find」ボタンをクリックし、LLDP 管理情報を検索します。

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

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

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

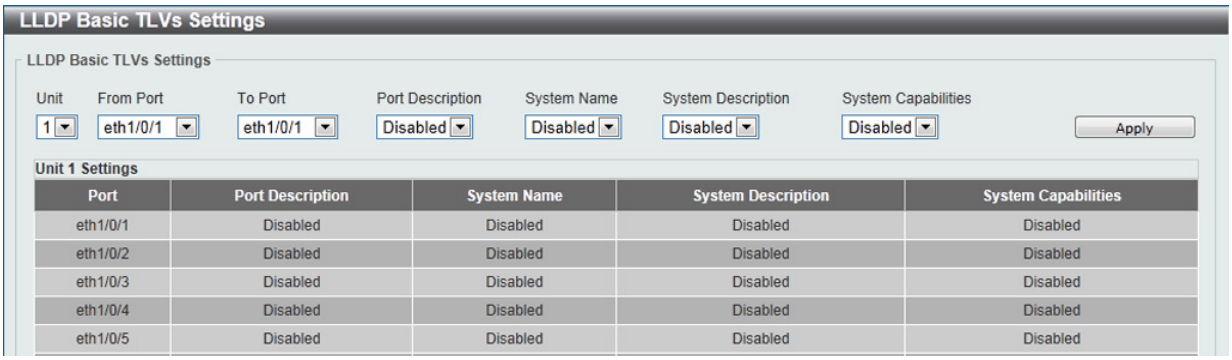


図 8-71　LLDP Basic TLVs Settings 画面

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

以下の項目を設定できます。

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

「Apply」ボタンをクリックし、変更を有効にします。

LLDP Dot1 TLVs Settings（LLDP Dot1 TLV 設定）

LLDP Dot1 TLV は、IEEE 802.1 によって組織的に定義されている TLV で、送信 LLDP アドバタイズメントから一つ以上の IEEE 802.1 規定のポート VLAN ID の TLV データタイプを除外するようにポートやポートグループを設定する時に使用します。

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

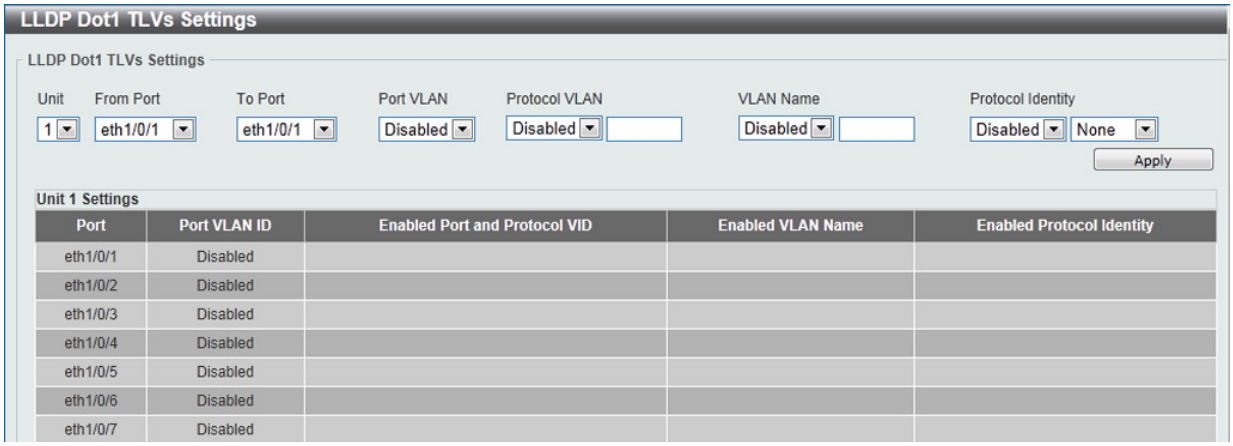


図 8-72　LLDP Dot1 TLVs Settings 画面

以下の項目が使用できます。

項目	説明
Unit	設定するユニットを指定します。
From Port/To Port	設定するポート範囲を指定します。
Port VLAN	ポート VLAN ID TLV の通知を「Enabled」（有効）/「Disabled」（無効）にします。 「ポート VLAN ID TLV」はオプションの固定長 TLV で、VLAN ブリッジポートがタグなしフレームまたは、優先タグ付きフレームに関連づけられるポートの VLAN 識別子（PVID) をアドバタイズできるようにします。
Protocol VLAN	ポートおよびプロトコル VLAN ID（PPVID）TLV の通知を有効または無効にします右の欄に VLAN ID を入力します。
VLAN Name	VLAN 名 TLV の通知を有効または無効にします。右の欄に VLAN ID を入力します。
Protocol Identity	プロトコル識別子の通知を「Enabled」（有効）/「Disabled」（無効）にします。 次に対象とするプロトコルを None、EAPOL、LACP、GVRP、STP または All から選択します。

「Apply」ボタンをクリックし、変更を有効にします。

LLDP Dot3 TLVs Settings（LLDP Dot3 TLV 設定）

個別のポートやポートグループが送信する LLDP アドバタイズメントから IEEE 802.3 規定の特定の TLV データタイプを除外するように設定します。

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

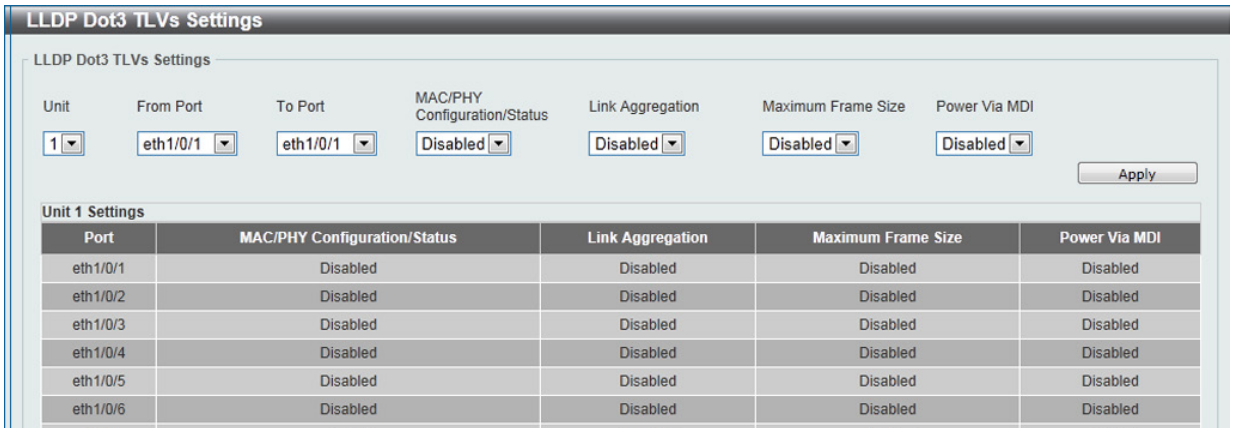


図 8-73　LLDP Dot3 TLVs Settings 画面

以下の項目を設定できます。

項目	説明
Unit	設定するユニットを指定します。
From Port/To Port	設定するポート範囲を指定します。

項目	説明
MAC/PHY Configuration/Status	MAC/PHY 設定 / ステータス TLV の送信を有効 / 無効にします。MAC/PHY 設定 / ステータス TLV は、(1) 送信側 IEEE802.3 LAN ノードのデュプレックスおよびビットレート機能、（2）送信側 IEEE802.3 LAN ノードの現在のデュプレックスおよびビットレート設定 を識別するオプションの TLV です。
Link Aggregation	スイッチのリンクアグリゲーション TLV 送信を「Enabled」（有効）/「Disabled」（無効）にします。 リンクアグリゲーション TLV は次の情報を含みます。「リンクのアグリゲートの可 / 不可」「アグリゲーション状態の有無」「アグリゲートされたポートチャネル ID」です。ポートがアグリゲートされていない場合、ID は「0」です。
Maximum Frame Size	最大フレームサイズ TLV の通知を「Enabled」（有効）/「Disabled」（無効）にします。 最大フレームサイズ TLV は MAC/PHY を含んだ最大フレームサイズを意味します。
Power Via MDI	Power via MDI TLV の通知を有効 / 無効にします。 3 つの IEEE802.3PMD 項目（10BASE-T、100BASE-TX、1000BASE-T）へ非電力供給システムリンク越しでの電力供給を許可します。Power Via MDI TLV を使用すると、送信する IEEE802.3 LAN ノードの MDI 電力サポート機能をアドバタイズし、検出することができます。

「Apply」ボタンをクリックし、変更を有効にします。

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

LLDP-MED TLV の送信を有効または無効にします。

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

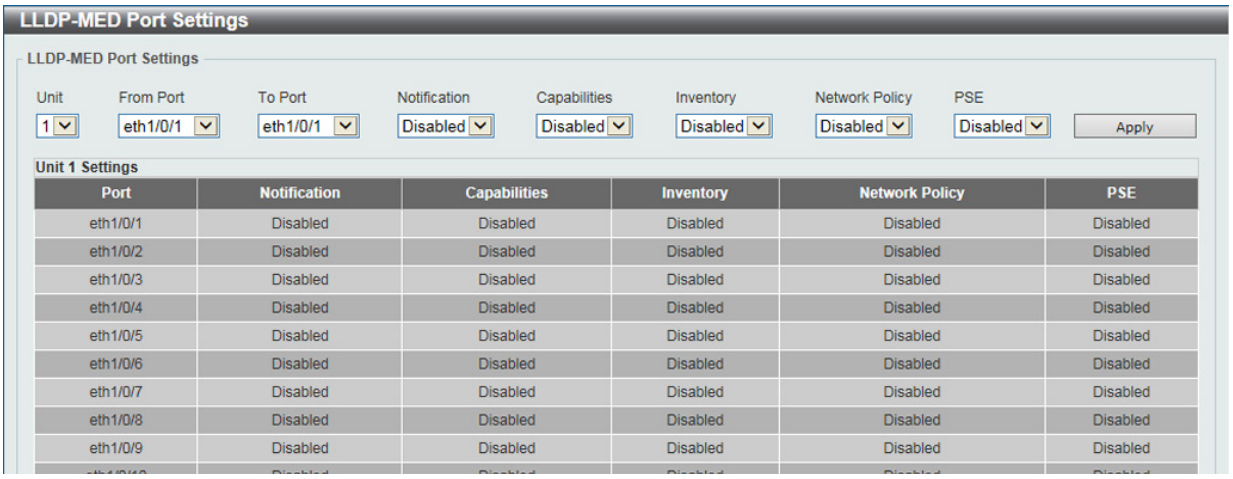


図 8-74　LLDP-MED Port Settings 画面

以下の項目が使用できます。

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	設定するポート範囲を指定します。
Notification	「LLDP-MED」通知の送信を有効 / 無効にします。
Capabilities	「LLDP-MED capabilities TLV」の送信を有効 / 無効にします。
Network Policy	「LDP-MED network policy TLV」の送信を有効 / 無効にします。
PSE	MDI TLV を経由する拡張電力「LLDP-MED」の送信を有効または無効にします。ローカル機器が PD 機器である場合有効です。
Inventory	「LLDP-MED inventory management TLV」の送信を有効 / 無効にします。

「Apply」ボタンをクリックして変更を適用します。

LLDP Statistics Information（LLDP 統計情報）

スイッチにおける LLDP 統計情報と各ポートの設定を参照できます。

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

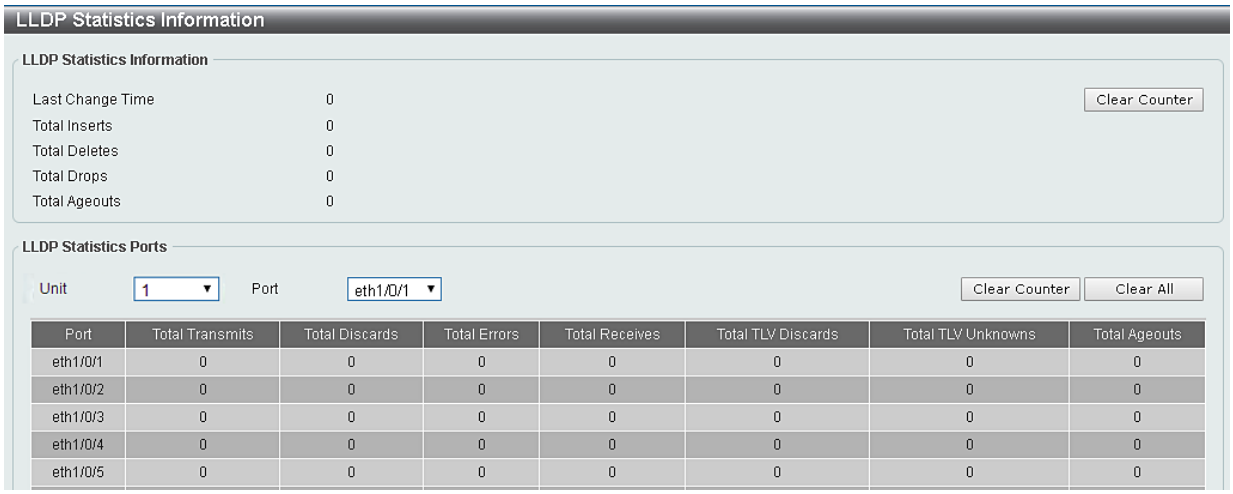


図 8-75　LLDP Statistics Information 画面

以下の項目が使用できます。

項目	説明
Unit	表示するユニットを選択します。
Port	表示するポートを指定します。

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

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

以下のローカルポートの要約テーブルにポートベースの情報を表示します。

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

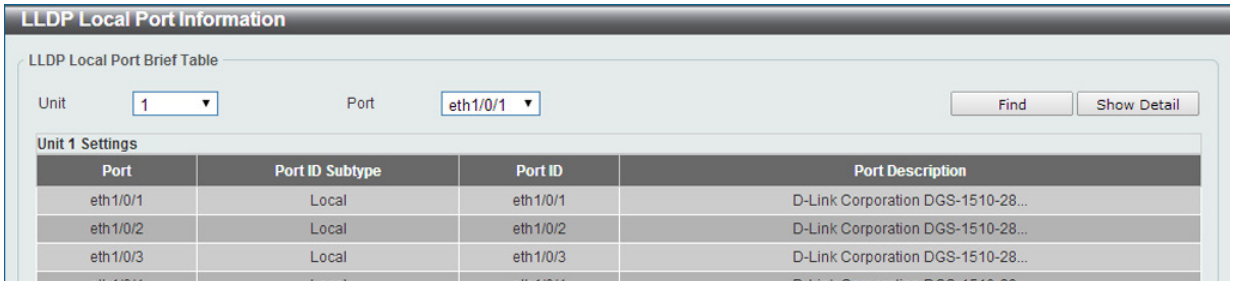


図 8-76　LLDP Local Port Information 画面

以下の項目が使用できます。

項目	説明
Unit	表示するユニットを選択します。
Port	表示するポートを指定します。

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

各パラメータの詳細の参照

「Show Detail」リンクをクリックし、以下の画面を表示します。

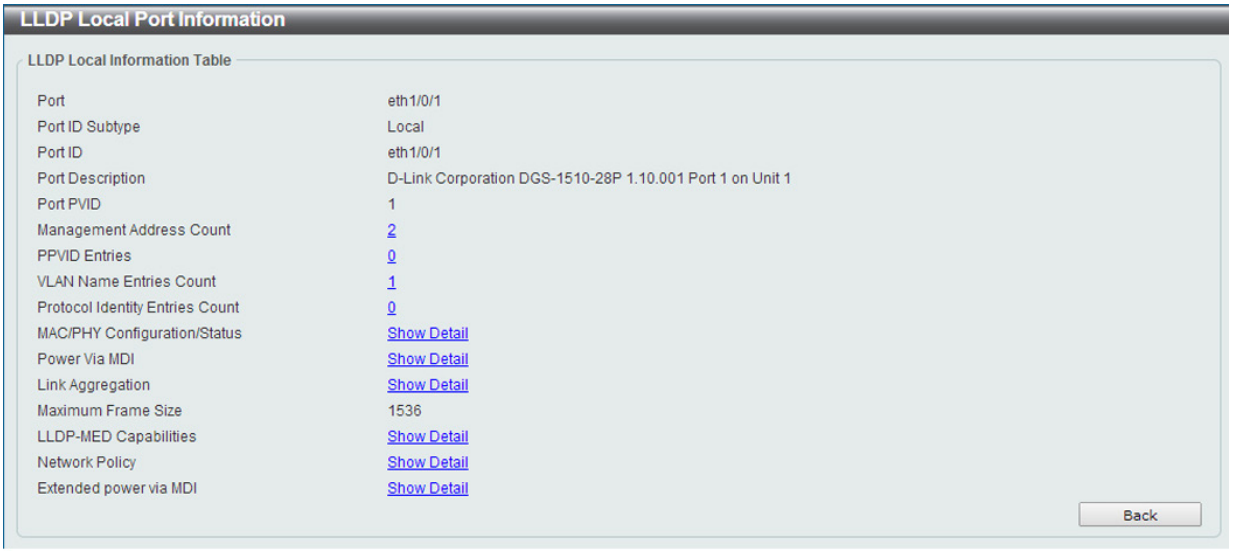


図 8-77　LLDP Local Port Information（Show Detail）画面

「MAC/PHY Configuration/Status」情報の参照

「Show Detail」リンクをクリックし、以下の画面を表示します。



図 8-78　LLDP Local Port Information - MAC/PHY Configuration/Status 画面

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

Neighbor から学習した情報を表示します。

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。

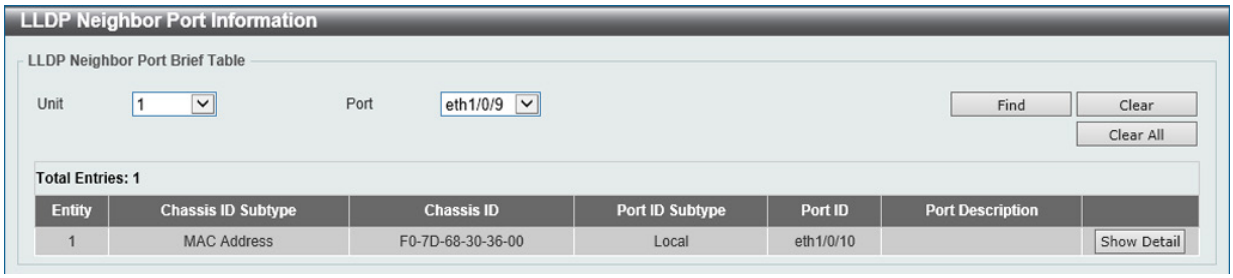


図 8-79　LLDP Neighbor Port Information 画面

以下の項目が使用できます。

項目	説明
Unit	表示するユニットを選択します。
Port	表示するポートを指定します。

ポートを選択し、「Find」ボタンをクリックします。情報が画面下半分に表示されます。
「Clear」をクリックしてポート情報をクリアします。
「Clear All」ボタンをクリックして、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 8-80　LLDP Neighbor Port Information - Show Detail 画面

「Back」をクリックすると前画面に戻ります。

各項目の「Show Detail」をクリックすることで、さらに詳細を確認することが可能です。

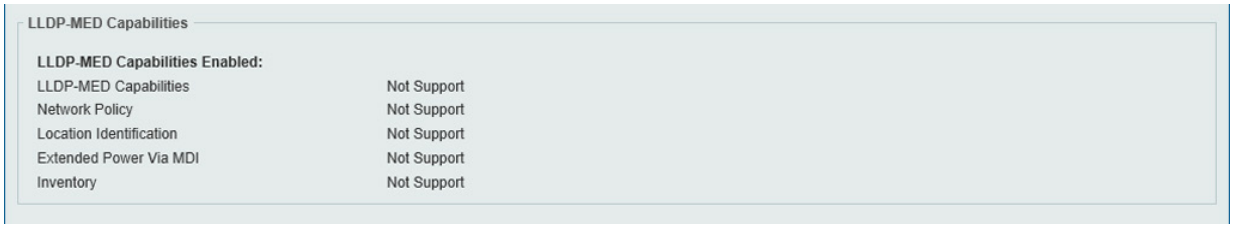


図 8-81　LLDP Neighbor Port Information - Show Detail（例 : LLDP-MED Capabilities）画面

「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）

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。
UDP Helper（UDP ヘルパー）	UDP ヘルパーの設定、編集を行います。
IPv4 Interface（IPv4 インタフェース）	IPv4 アドレスのインタフェースの設定を行います。
IPv4 Static/Default Route（IPv4 スタティック / デフォルトルート）	IPv4 アドレスのスタティック / 初期ルートの設定を行います。
IPv4 Route Table（IPv4 ルートテーブル）	IPv4 のルートテーブルの設定を行います。
IPv6 Interface（IPv6 インタフェース）	IPv6 アドレスのインタフェースの設定を行います。
IPv6 Neighbor（IPv6 Neighbor 設定）	IPv6 ネイバの設定を行います。
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。
IPMC(IPMC 設定)	IPMC 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。

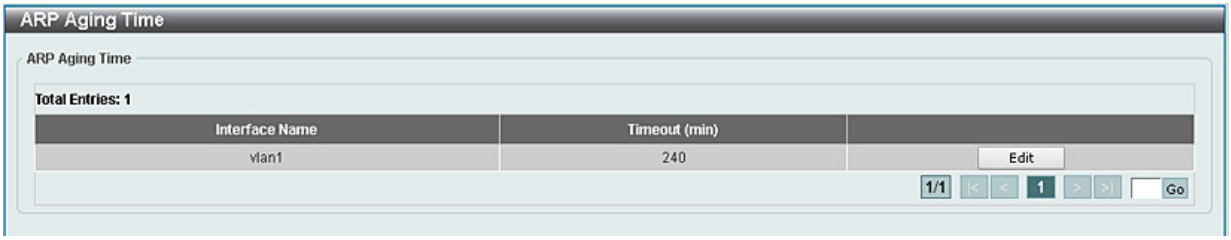


図 9-1　ARP Aging Time 画面

設定には以下の項目を使用します。

項目	説明
Timeout	ARP テーブルエントリのリクエストから、エントリを保持する時間（分）設定します。この時間が経過すると、エントリはテーブルから削除されます。初期値は 20 分です。

ARP エージングタイムの編集

1. 編集するエントリの「Edit」ボタンをクリックします。
2. 「Timeout」を設定します。
3. 「Apply」ボタンをクリックします。

Static ARP（スタティック ARP 設定）

スタティック ARP エントリを設定します。

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

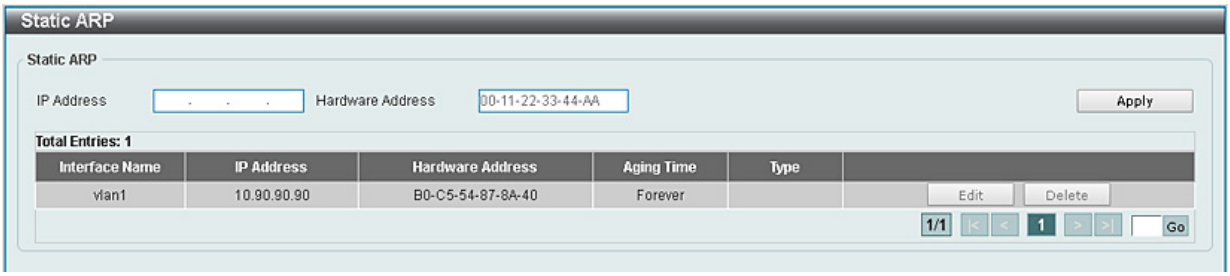


図 9-2　Static ARP 画面

以下の項目を使用します。

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。

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

Static ARP のエントリの編集

1. 編集するエントリの「Edit」ボタンをクリックします。
2. 「MAC Address」を編集します。
3. 「Apply」ボタンをクリックします。

Static ARP のエントリの削除

1. 削除するエントリの「Delete」ボタンをクリックします。

Proxy ARP（プロキシ ARP 設定）

プロキシ ARP 機能は、スイッチが元の ARP のレスポンダとして IP や MAC アドレスを偽装して、別のデバイス宛の ARP リクエストに応答します。従って、スタティックのルーティングやデフォルトゲートウェイを設定せずに、目的の宛先にパケットをルーティングすることが可能です。ホスト（通常レイヤ 3 スイッチ）は別のデバイス宛のパケットに応答します。

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

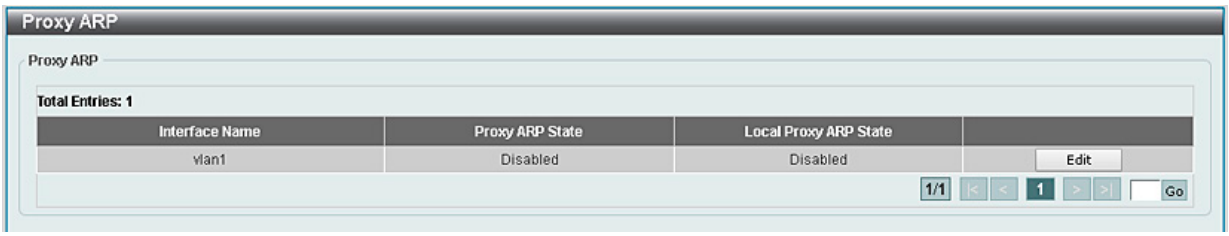


図 9-3　Proxy ARP 画面

以下の項目を使用します。

項目	説明
Proxy ARP State	プロキシ ARP を有効 / 無効にします。
Local Proxy ARP State	ローカルプロキシ ARP を有効 / 無効にします。 ローカルプロキシ ARP 機能は送信元 IP と宛先 IP が同じインタフェースの場合、スイッチがプロキシ ARP に返答します。

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

エントリの編集

1. 編集するエントリの「Edit」ボタンをクリックします。
2. 指定エントリを編集して、IP インタフェースのプロキシ ARP の状態を選択します。
3. 「Apply」ボタンをクリックします。

初期値では「Proxy ARP」「Local Proxy ARP State」の両方とも無効になります。

ARP Table（ARP テーブル）

現在のスイッチの 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。

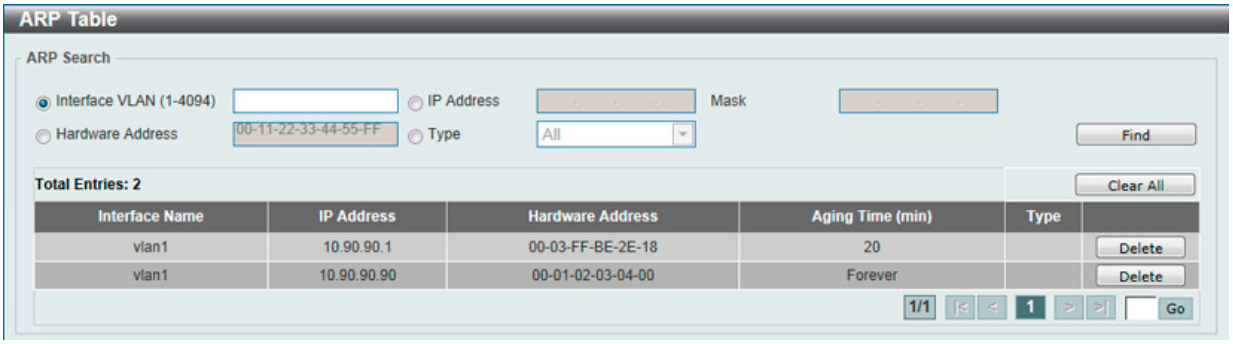


図 9-4　ARP Table 画面

設定には以下の項目を使用します。

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。1 から 4094 で指定できます。
IP Address	表示する IP アドレスを入力します。
Mask	上記 IP アドレスのマスクを指定します。
Hardware Address	表示する MAC アドレスを入力します。
Type	表示する ARP の種類を指定します。「All」「Dynamic」から指定できます。

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

Gratuitous ARP（Gratuitous ARP 設定）

本項目では Gratuitous ARP の設定 / 表示を行います。Gratuitous ARP リクエストパケットは、宛先 / 送信元 IP アドレスが両方、送信デバイスの IP アドレスに設定されていて、宛先 MAC アドレスはブロードキャストアドレスの ARP リクエストパケットです。通常、デバイスは他のホストによって重複している IP アドレス、またはインタフェースに接続したホストの ARP キャッシュエントリの先行読み込みか再設定を行うために Gratuitous ARP リクエストパケットを使用します。

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。

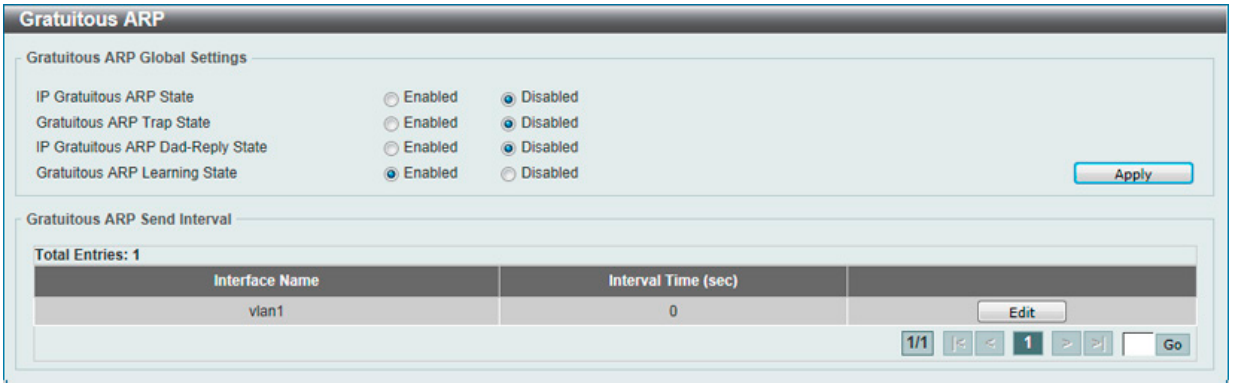


図 9-5　Gratuitous ARP 画面

設定には以下の項目を使用します。

項目	説明
IP Gratuitous ARP State	Gratuitous ARP パケットの送信を有効 / 無効にします。
Gratuitous ARP Trap State	Gratuitous ARP トラップ を有効 / 無効にします。
IP Gratuitous ARP Dad-Reply State	IP gratuitous ARP Dad-reply を有効 / 無効にします。
Gratuitous ARP Learning State	受信した Gratuitous ARP パケットに基づいて、ARP エントリの更新を有効または無効にします。通常、システムの IP アドレスに対応する MAC アドレスを要求する ARP 応答パケットまたは通常の ARP 要求パケットのみを学習します。このオプションは、受信した Gratuitous ARP パケットに基づく ARP キャッシュの ARP エントリの学習を有効 / 無効します。GratuitousARP は、パケットが照会している IP と同一の送信元 IP アドレスにより送信されます。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Edit」をクリックして指定エントリを再編集します。

UDP Helper（UDP ヘルパー）

L3 Features > UDP Helper

IP Forward Protocol（IP 転送プロトコル）

本項目ではポートの IP ヘルパー転送を設定、表示します。

L3 Features > UDP Helper > IP Forward Protocol の順にメニューをクリックし、以下の画面を表示します。

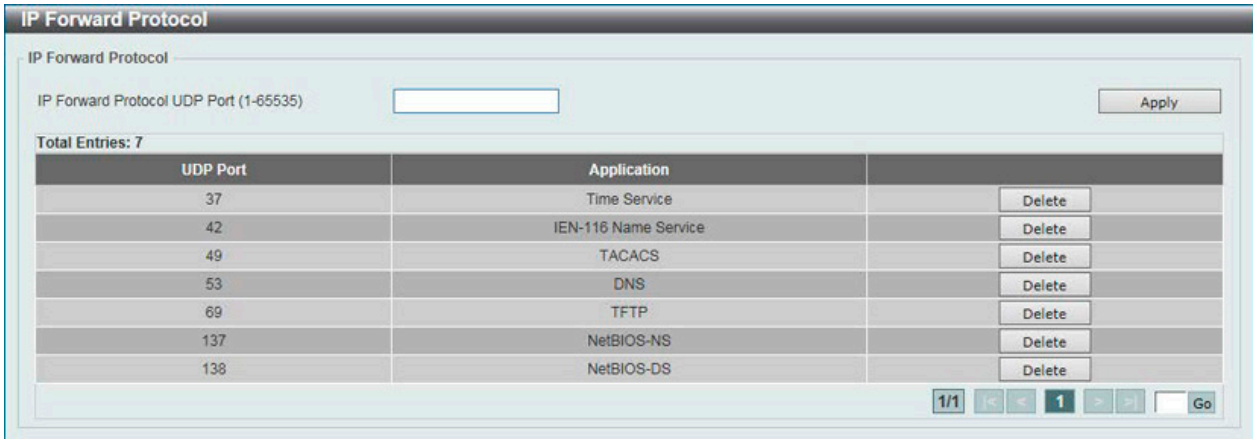


図 9-6　IP Forward Protocol 画面

以下の項目が表示、または設定変更に使用できます。

項目	説明
IP Forward Protocol UDP Port	転送する UDP サービスの宛先ポート（1-65535）を指定します。

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

IP Helper Address（IP ヘルパーアドレス）

本項目では VLAN の IP ヘルパー転送を設定、表示します。

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

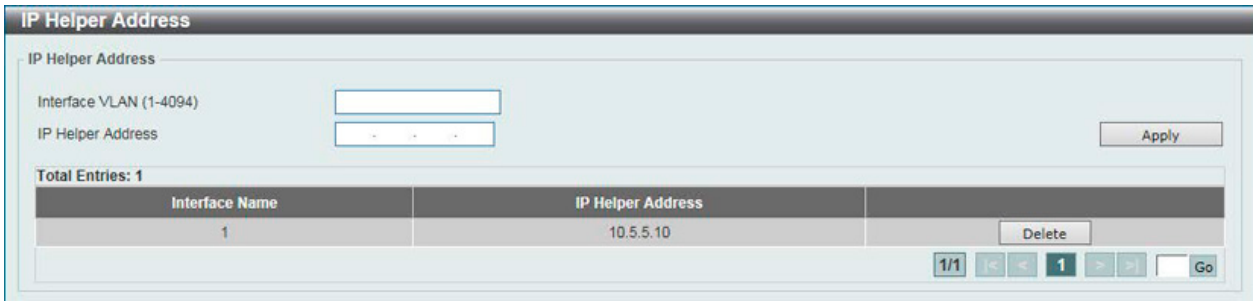


図 9-7　IP Helper Address 画面

以下の項目が表示、または設定変更に使用できます。

項目	説明
Interface VLAN	VLAN インタフェース ID（1-4094）を指定します。
IP Helper Address	指定 VLAN の IP ヘルパーのアドレスを指定します。

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

IPv4 Interface（IPv4 インタフェース）

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

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

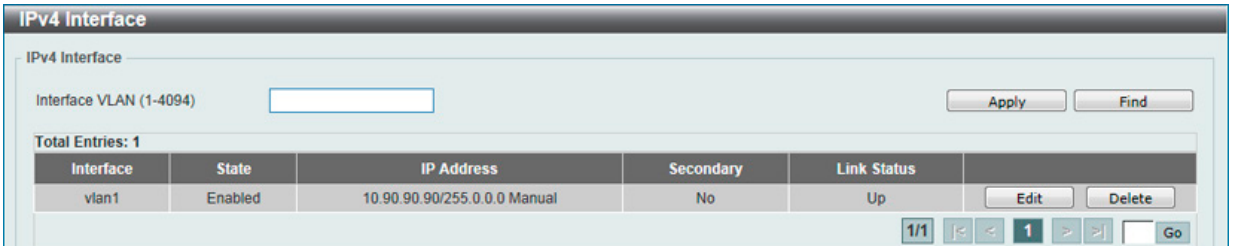


図 9-8　IPv4 Interface 画面

スイッチの現在の IP インタフェース設定が表示されます。

項目	説明
Interface VLAN	設定、表示するインタフェースの VLAN ID を入力します。1 から 4094 までで入力可能です。

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

IPv4 インタフェースの編集（IPv4 Interface Settings）
指定エントリの「Edit」ボタンをクリックして以下の画面を表示します。

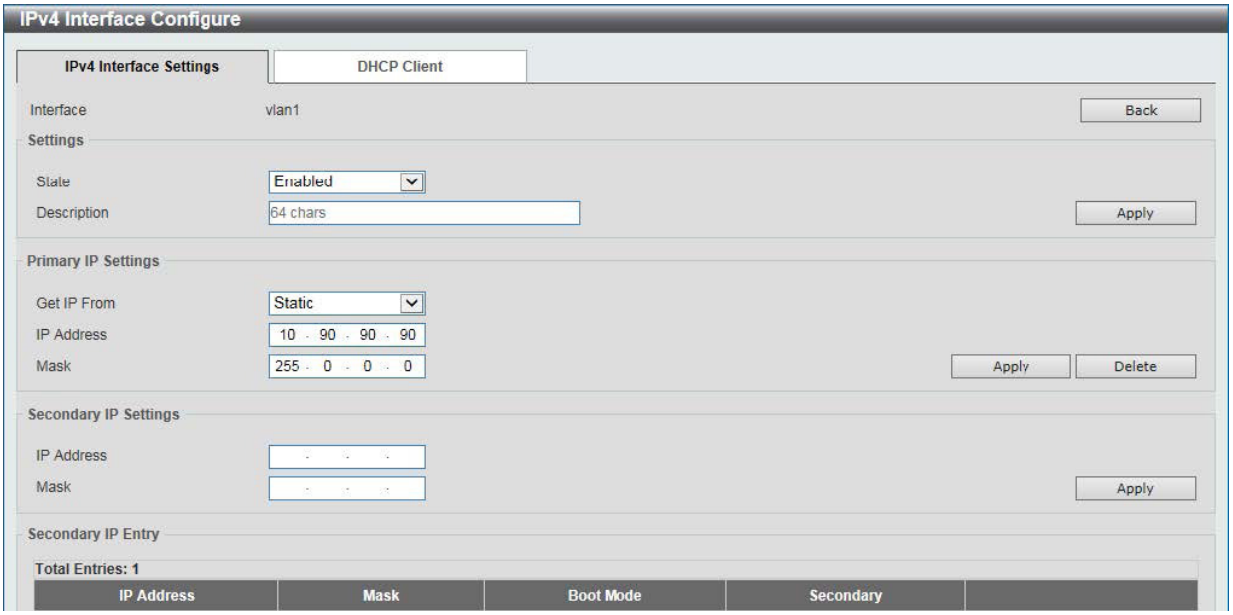


図 9-9　IPv4 Interface Configure 画面

「Back」をクリックすると前画面へ戻ります。

以下の項目を使用して設定を行います。

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。
Description	該当 IPv4 インタフェースの概要（64 文字以内）を指定します。
Primary IP Settings	
Get IP From	IPv4 アドレスの取得方法について「Static」（手動設定）、「DHCP」（DHCP サーバから自動割り当て）から指定します。
IP Address	IPv4 インタフェースに割り当てる IPv4 アドレスを入力します。
Mask	IPv4 インタフェースに割り当てるサブネットマスクを入力します。
Secondary IP Settings	
IP Address	セカンダリ IP アドレスに割り当てる IPv4 アドレスを入力します。
Mask	セカンダリ IP アドレスに割り当てるサブネットマスクを入力します。

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

IPv4 インタフェースの編集（DHCP Client）

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

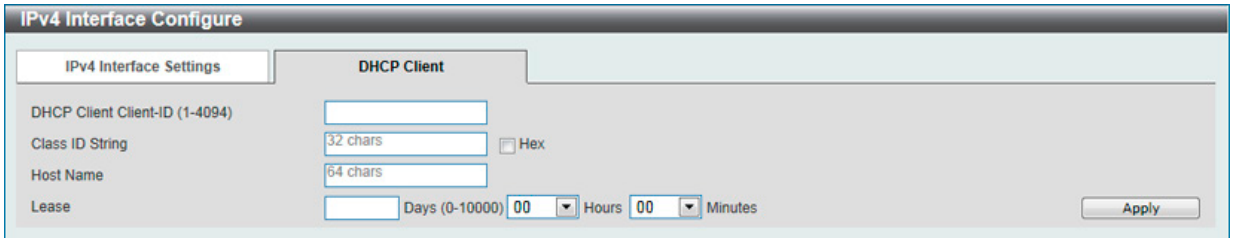


図 9-10　DHCP Client 画面

画面には以下の項目が表示されます。

項目	説明
DHCP Client Client-ID	VLAN インタフェースを入力します。この 16 進数 MAC アドレスはディスカバメッセージを送信するクライアント ID として使用されます。
Class ID String	最大 32 文字を使用してベンダクラス識別名を入力します。「Hex」にチェックを入れると 16 進数方式になります。
Host Name	ホスト名（64 字以内）を入力します。ホスト名の最初の文字はアルファベットで始まるようにします。最後の文字はアルファベットまたは数字で終わるようにします。その他はアルファベット、数字、ハイフン（-）が使用できます。
Lease	DHCP サーバから割り振られる IP アドレスのリース時間を指定します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
入力 / 指定した変更を破棄し前のページに戻る場合は「<<Back」をクリックします。

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

本スイッチは IPv4 アドレシングのためにスタティックルーティング機能をサポートしています。IPv4 でのスタティックルートを 64 エントリまで作成することができます。IPv4 スタティックルートにおいて、スタティックルートが設定されるとすぐに、スイッチはユーザにより設定されたネクストホップルータへ ARP リクエストパケットを送信します。ARP の応答をネクストホップからスイッチが取得すると、ルートは有効になりますが、ARP エントリが既に存在している場合には、ARP リクエストは送信されません。

スイッチはフローティングスタティックルートもサポートしています。これは、異なるネクストホップに対して代替スタティックルートを作成することができることを意味しています。このセカンダリネクストホップデバイスルートは、プライマリスタティックルートがダウンした場合にバックアップスタティックルートとして動作します。プライマリルートが失われると、バックアップルートのステータスがアクティブになります。

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

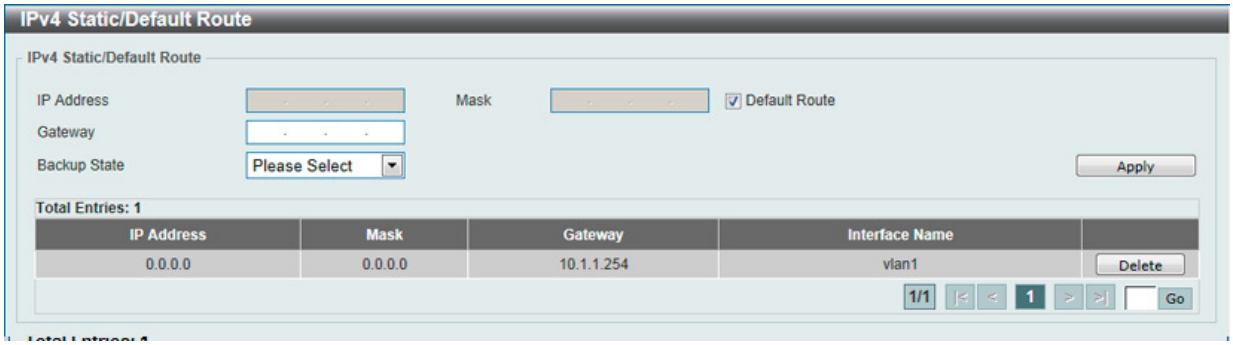


図 9-11　IPv4 Static/Default Route 画面

画面には以下の項目が表示されます。

項目	説明
IP Address	スタティック / デフォルトルートの IP アドレス。 「Default Route」にチェックを入れるとデフォルトルートを設定することができます。
Mask	上記 IP アドレスのネットマスク
Gateway	上記 IP ルートのゲートウェイアドレス
Backup State	IP ルートに設定されたバックアップ状態を表示します。「Primary」または「Backup」が表示されます。 「Primary」を選択すると宛先へプライマリルートを使用します。 「Backup」を選択すると宛先へバックアップルートを使用します。

「Apply」ボタンをクリックし、設定を有効にします。

エントリの削除

対象のエントリの行の「Delete」ボタンをクリックします。

IPv4 Route Table（IPv4 ルートテーブル）

IP ルーティングテーブルを確認します。

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



図 9-12　IPv4 Route Table 画面

画面には以下の項目が表示されます。

項目	説明
IP Address	ラジオボタンで選択し、表示する IPv4 アドレスを入力します。
Network Address	ラジオボタンで選択し、表示する IPv4 宛先アドレスを入力します。 最初の空欄にはネットワークプリフィクスを入力し、二つ目には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するにはこのオプションを選択します。
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	アクティブなルーティングエントリのサマリを表示します。

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

IPv6 Interface（IPv6 インタフェース）

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

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

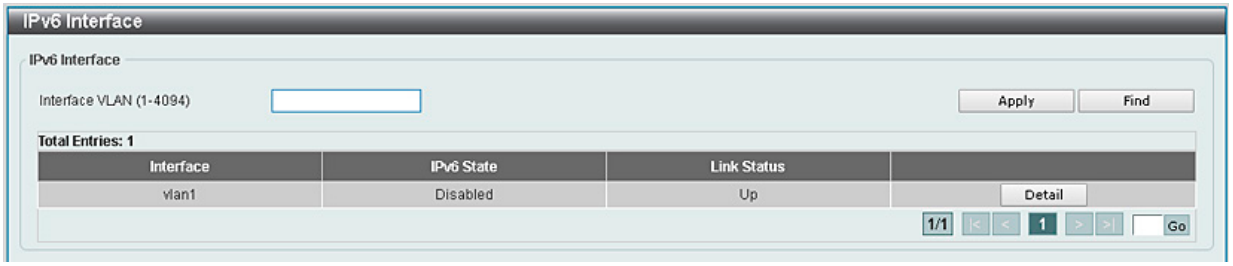


図 9-13　IPv6 Interface 画面

スイッチの現在の IP インタフェース設定が表示されます。

項目	説明
Interface VLAN	IPv6 エントリに関連付ける VLAN インタフェース ID を入力します。1 から 4094 までで入力可能です。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
「Detail」ボタンをクリックして ,IPv6 インタフェースエントリの詳細設定を行います。

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

指定エントリの「Detail」ボタンをクリックして以下の画面を表示します。

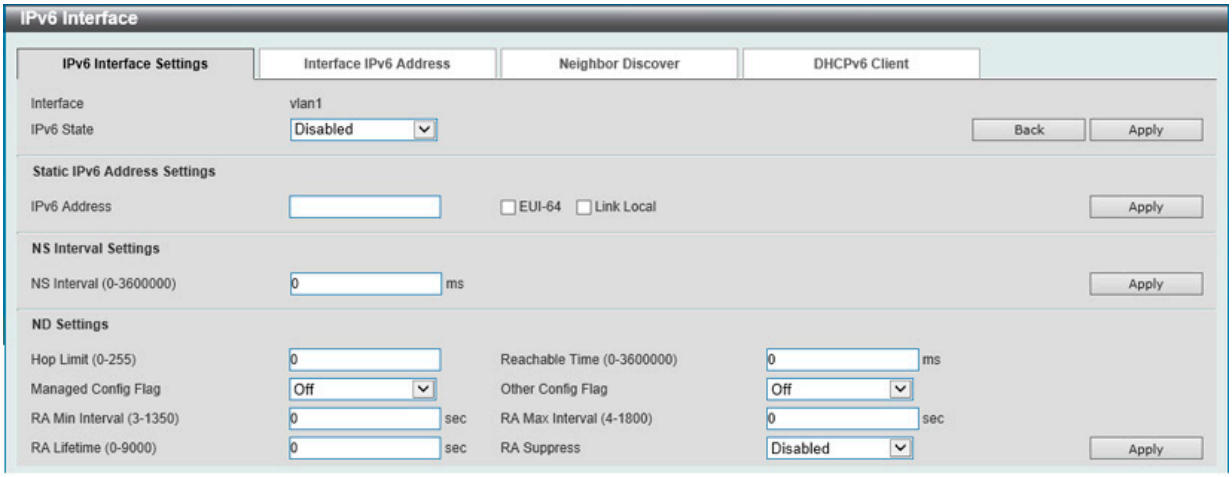


図 9-14　IPv6 Interface - Detail, IPv6 Interface Settings 画面

以下の項目を使用して設定を行います。

項目	説明
IPv6 State	該当エントリの IPv6 インタフェースをグローバルに有効 / 無効にします。
IPv6 Address	IPv6 インタフェースに割り当てる IPv6 アドレスを入力します。 • 「EUI-64」- EUI-64 インタフェース ID を使用してインタフェースの IPv6 アドレスを設定します。 • 「Link Local」- IPv6 インタフェースにリンクローカルアドレスを使用します。
NS Interval	NS Interval を 0 から 3600000 ミリ秒で設定します。
Hop Limit	「IPv6 Hop Limit」の値を入力します。RA メッセージ内で通知されるホップリミットを設定します。システムで生成された IPv6 パケットは内部ホップリミットとしてこの値を使用します。このインタフェースで初期値を使用する場合「0」に設定してください。0-255 の範囲で指定可能です。
Reachable Time	ND プロトコルにおける到達時間を指定します。この値はインタフェースのルータに使用され、RA メッセージ内においても通知されます。「0」に指定すると、ルータは 30 秒を使用し、RA メッセージ内で 0 秒（未指定）を通知します。到達時間は IPv6 ノードによる近隣ノードの到達可能性の見極めに使用されます。「0-3600000」（ミリ秒）の範囲内で 1000（ミリ秒）単位で指定可能です。
Managed Config Flag	「Managed Config Flag」の「On/Off」を指定します。通知された RA メッセージの「Managed Config Flag」を有効 / 無効に指定します。近隣ホストは有効なフラグの RA を受領し、ホストは IPv6 アドレス取得のためにステートフル設定プロトコルを使用する必要があります。
Other Config Flag	他の設定フラグの「On/Off」を指定します。通知された RA メッセージの「Other Config Flag」を有効 / 無効に指定します。本機能が有効の場合、ルータは、接続されたホストに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構成情報を取得するように指示します。
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。「3-1350」（秒）から指定します。最大値の 75%未満である必要があります。
RA Max Interval	RA メッセージの再送信間隔の最大値を指定します。「4-1800」（秒）から指定します。
RA Lifetime	RA ライフタイムを指定します。「0-9000」（秒）になります。RA のライフタイム値は、RA を受信したホストが、RA の送信元ルータをデフォルトルータとして使用できる時間を通知します。
RA Suppress	インタフェースの RA メッセージ送信の有効 / 無効を指定します。初期値では VLAN インタフェースで有効、トンネルインタフェースでは無効です。

「Apply」ボタンをクリックし、設定を有効にします。入力 / 指定した変更を破棄し前のページに戻る場合は「<<Back」をクリックします。

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

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



図 9-15　Interface IPv6 Address 画面

エントリの削除

対象のエントリの「Delete」ボタンをクリックします。

IPv6 インタフェースの編集（Neighbor Discover）

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



図 9-16　Neighbor Discover 画面

IPv6 インタフェースの編集（DHCPv6 Client）

「DHCPv6 Client」タブをクリックして以下の画面を表示します。



図 9-17　DHCPv6 Client 画面

画面には以下の項目が表示されます。

項目	説明
Client State	DHCPv6 クライアントを有効 / 無効に指定します。「Rapid Commit」にチェックを入れると、プレフィックス委任のメッセージ交換を実行します。

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

「Restart」をクリックするとインタフェースの DHCPv6 クライアントはリスタートします。

IPv6 Neighbor（IPv6 Neighbor 設定）

IPv6 Neighbor の設定を行います。

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。

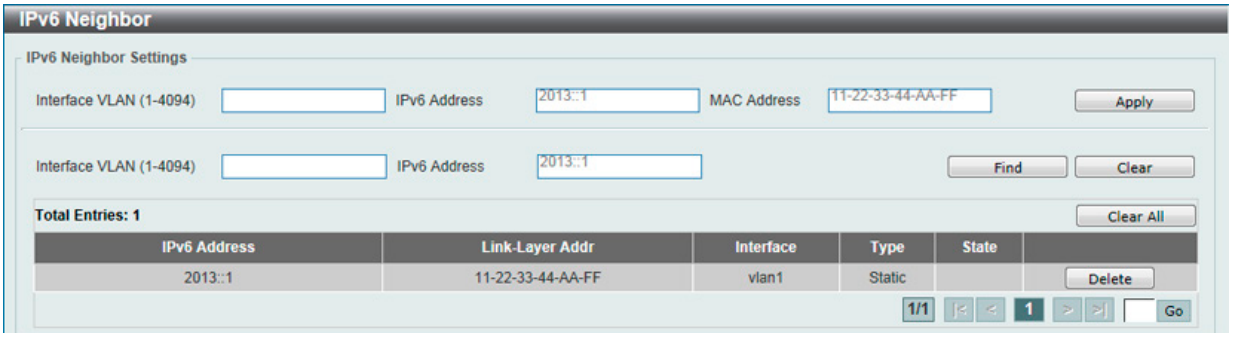


図 9-18　IPv6 Neighbor 画面

「IPv6 Neighbor」画面には次の項目があります。

項目	説明
Interface VLAN	IPv6 Neighbor のインタフェース VLAN を指定します。
IPv6 Address	IPv6 Neighbor の 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、設定内容を適用します。

「Find」をクリックして、入力内容を基にエントリを検索します。

「Clear」をクリックして、指定エントリの情報をクリアします。

「Clear All」をクリックして、テーブルのすべての情報をクリアします。

「Delete」をクリックして、指定のエントリを削除します。

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、指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）

本スイッチは IPv6 アドレシングのためにスタティックルーティング機能をサポートしています。
L3 Features > IPv6 Static/Default Route の順にメニューをクリックし、以下の画面を表示します。



図 9-19　IPv6 Static/Default Route 画面

画面には以下の項目が表示されます。

項目	説明
IPv6 Address/Prefix Length	ルートの 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 VLAN	このルートに関連付けられるインタフェースの VLAN ID を入力します。
Next Hop IPv6 Address	ネクストホップ IPv6 アドレスを入力します。
Backup State	スイッチの IPv6 ネットワーク接続のために本インタフェースの役割が「Primary」か「Backup」であるかを選択します。 「Primary」を選択すると宛先へのプライマリルートとして設定されます。 「Backup」を選択すると宛先へのバックアップルートとして設定されます。

「Apply」ボタンをクリックし、設定を有効にします。

IPv6 Route Table（IPv6 ルートテーブル）

現在の IPv6 ルーティングテーブルを表示します。

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



図 9-20　IPv6 Route Table 画面

画面には以下の項目が表示されます。

項目	説明
IPv6 Address	ラジオボタンを選択し、表示する IPv6 アドレスを入力します。
IPv6 Address/Prefix Length	ラジオボタンを選択し、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全 IPv6 ルートを表示します。
Interface VLAN	ラジオボタンを選択し、表示するインタフェースＶＬＡＮを入力します。
Connected	ラジオボタンを選択し、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	チェックボックスにチェックを入れると、チップに記録されたルートのみ表示されます。
Summary	チェックボックスにチェックを入れると、アクティブなルーティングエントリのサマリを表示します。

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
「Apply」ボタンをクリックし、設定を有効にします。

IPMC（IPMC 設定）

IP Multicast (IPMC) の設定を行う場合は **L3 Features > IPMC** から設定を行います。

IP Multicast Global Settings（IP マルチキャストグローバル設定）

IP Multicast Global Settings（IP マルチキャストグローバル設定）の表示、グローバル設定を行います。

L3 Features > IPMC > IP Multicast 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。

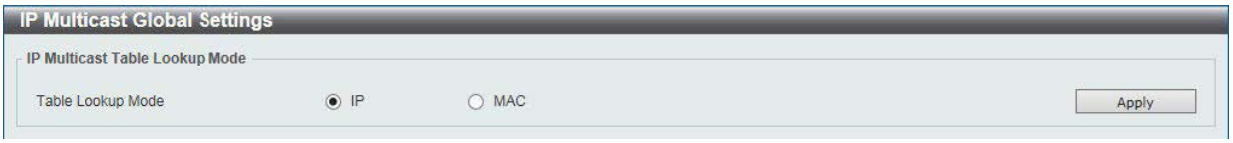


図 9-21　IP Multicast Global Settings 画面

画面には以下の項目が表示されます。

項目	説明
Table Lookup Mode	IP マルチキャストフォワーディングルックアップモードを指定します。 • IP - マルチキャストフォワーディングルックアップを IP アドレス基準で行います。 • MAC - マルチキャストフォワーディングルックアップを MAC アドレス基準で行います。

「Apply」をクリックし、設定内容を適用します。

IP Multicast Forwarding Cache（IP マルチキャストフォワーディングキャッシュ）

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

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



図 9-22　IP Multicast Forwarding Cache 画面

画面には以下の項目が表示されます。

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

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

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、CoS キューマッピングなどの設定を行います。
Advanced Settings（アドバンス設定）	DSCP/CoS のマップ設定などを行います。

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。

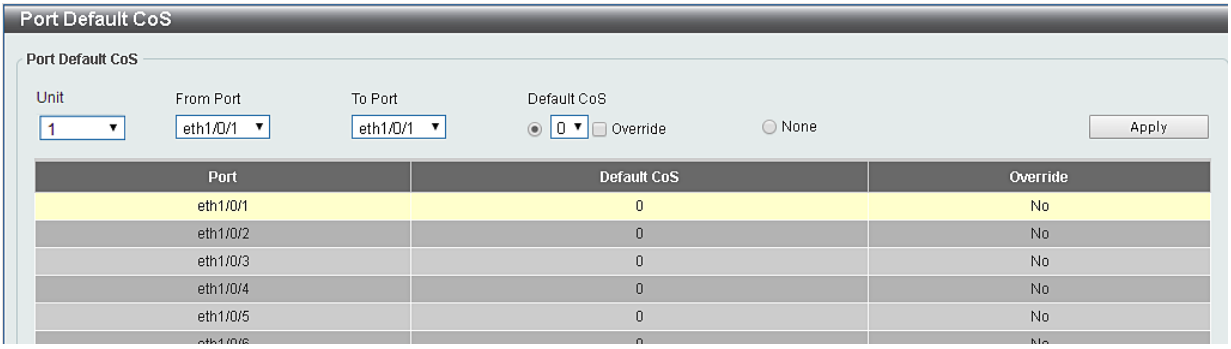


図 10-1　Port Default CoS 画面

本画面には以下の項目があります。

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

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

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

ポートスケジューラーメソッドを設定します。

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

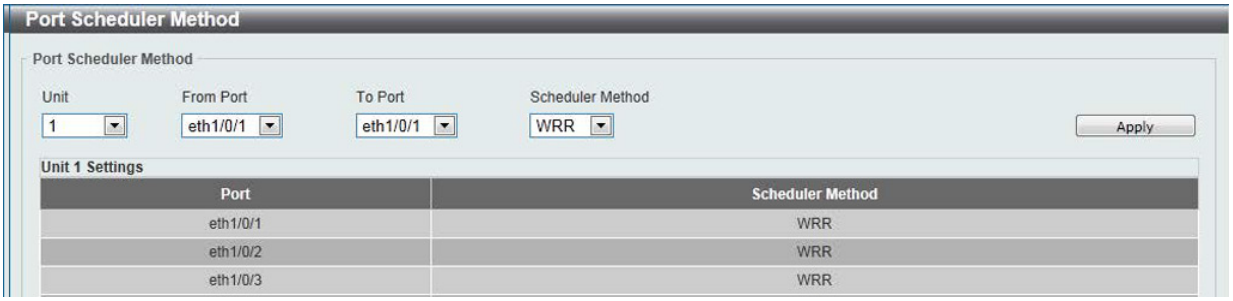


図 10-2　Port Scheduler Method 画面

本画面には以下の項目があります。

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	設定するポート / ポート範囲を入力します。
Scheduler Method	指定ポートに対するスケジューリングの方法を設定します。 「Strict Priority」(SP)、「Round-Robin」(RR)、「Weighted Round-Robin」(WRR)、「Weighted Deficit Round-Robin」(WDRR) から指定できます。初期値ではアウトプットキュースケジューリングアルゴリズムは「WRR」です。「WDRR」は送信キューに蓄積したバックログクレジットのセットを供給することで作動します。 はじめに各キューはクレジットカウンタを量の値として設定します。CoS キューからのパケットが送信される度に、パケットのサイズはクレジットカウンタから差し引かれ、サービスの権利は次の低い CoS キューに移行されます。 クレジットカウンタが 0 以下になると、クレジットが補完されるまでキューは停止します。すべての CoS キューが 0 に到達するとクレジットカウンタは補完されます。すべてのパケットはクレジットカウンタが 0 かそれ以下の場合、実行され最後のパケットも全て送信されます。こうなった場合、クレジットは補完されます。クレジットが補完されるといくつかのクレジットは各 QoS キュークレジットカウンタに追加されます。各 CoS キューのクォンタムは、ユーザ設定に基づいて異なる場合があります。SP モードでの CoS キューの設定はより優先値の高い CoS キューがストリクトプライオリティーモードで設定されている必要があります。優先値の高い CoS キューからパケットが送信されると、関連した重みづけ（Weight）が 1 差し引かれ、次の低い CoS キューがのパケットが実行されます。CoS キューの重みづけ（Weight）がゼロになると、補完されるまでキューは実行されません。すべての CoS キューの重みづけ（Weight）が 0 に到達すると同時にその重みづけ（Weight）は補完されます。

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

Queue Settings（QoS 設定）

キューを設定、表示します。

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

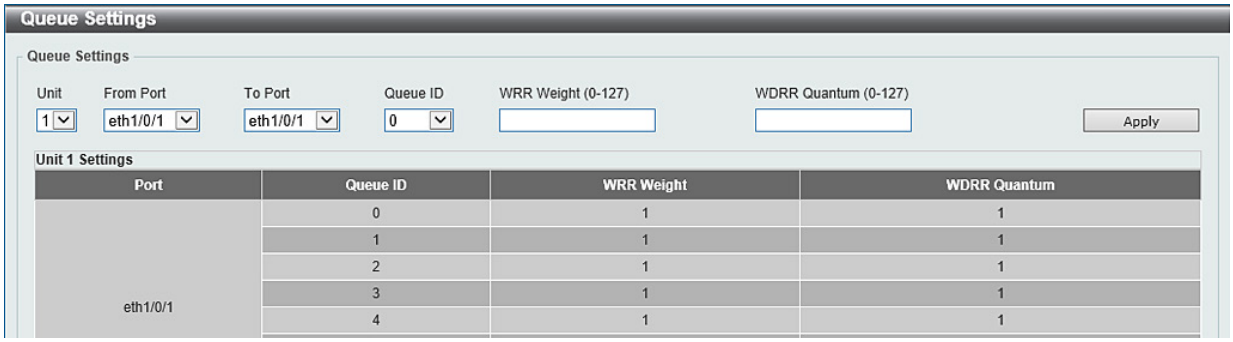


図 10-3　Queue Settings 画面

本画面には以下の項目があります。

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

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

CoS to Queue Mapping（CoS キューマッピング設定）

CoS-to-Queue マッピングの表示、設定を行います。

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

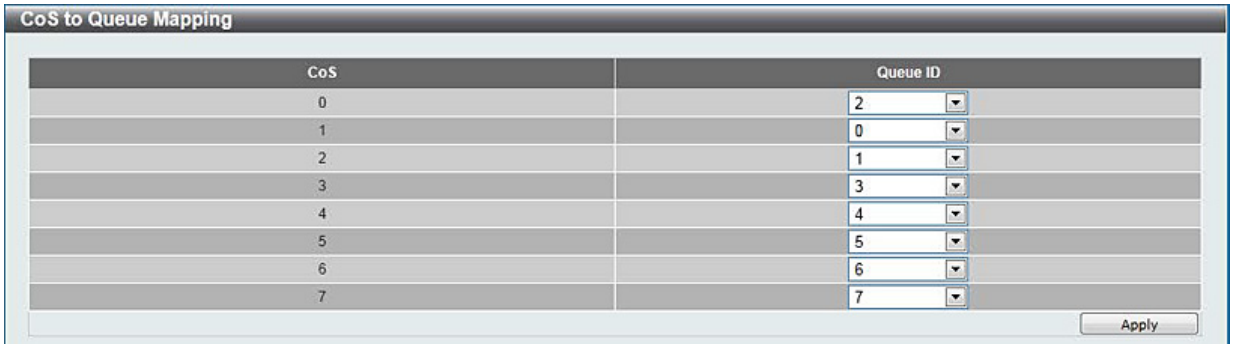


図 10-4　CoS to Queue Mapping 画面

本画面には以下の項目があります。

項目	説明
Queue ID	対応する CoS 値に対応するキュー ID を選択します。「0」（クラス 0）は最も低い優先度のキューで、「7」（クラス 7）が最も高くなります。

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

Port Rate Limiting（ポートレート制限設定）

ポートレート制限の設定を行います。

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

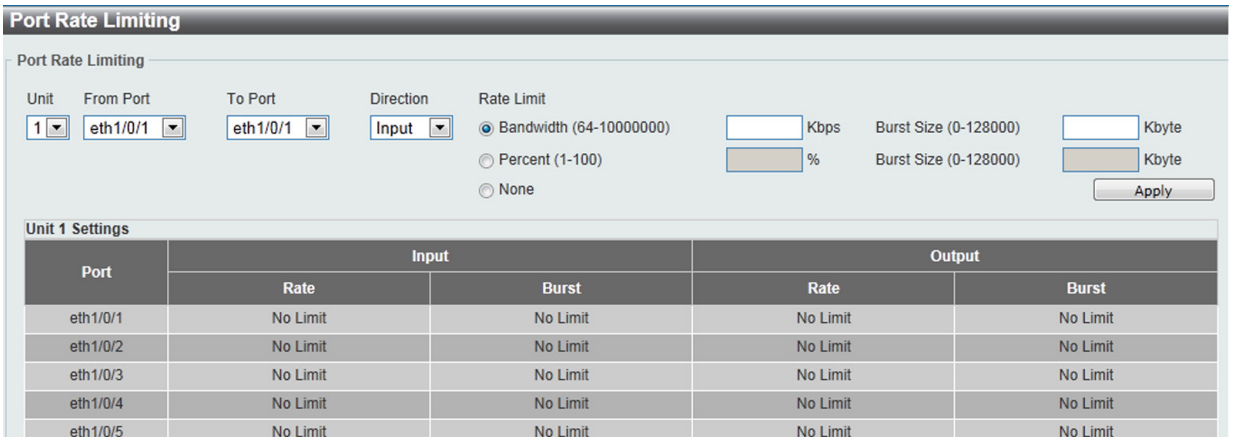


図 10-5　Port Rate Limiting 画面

以下の項目を設定または表示できます。

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

「Apply」ボタンをクリックして行った変更を適用します。

Queue Rate Limiting（キューレート制限設定）

キューレートの制限設定をします。

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

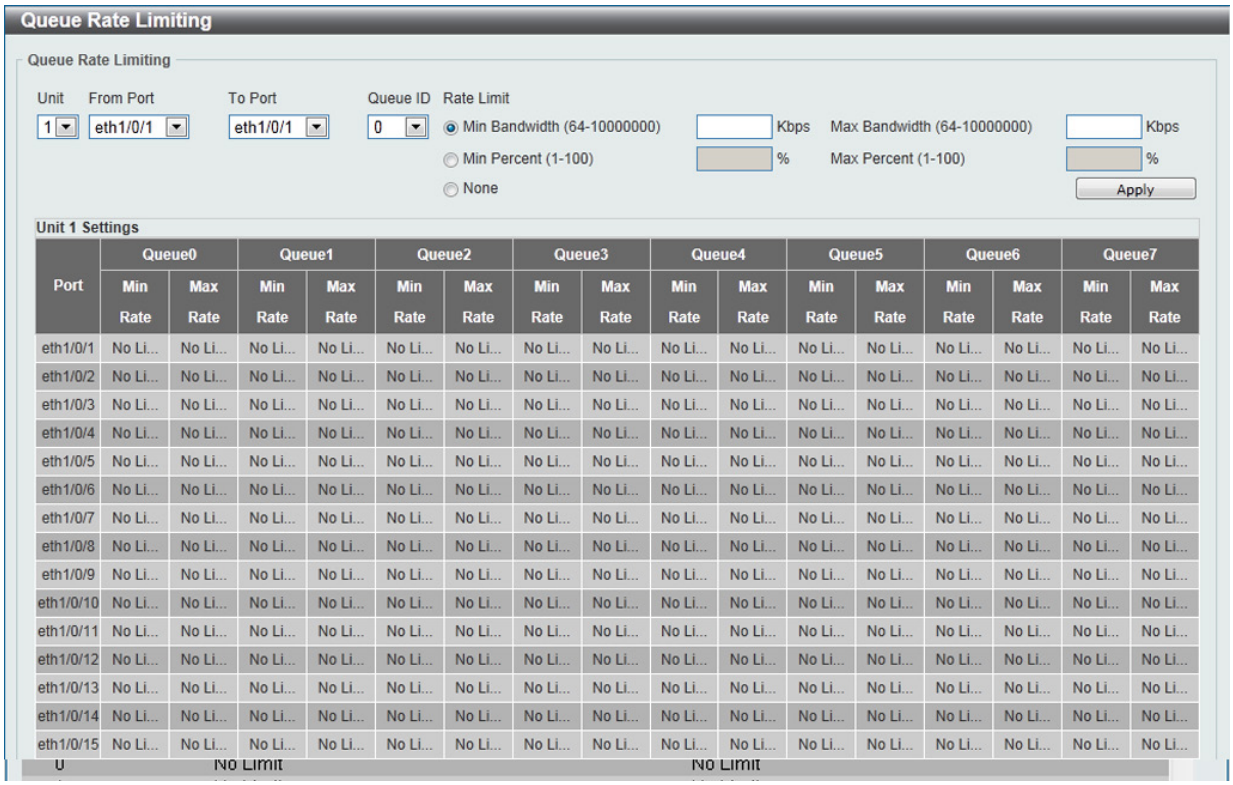


図 10-6　Queue Rate Limiting 画面

以下の項目を設定または表示できます。

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	この設定に使用するポート範囲を選択します。
Queue ID	キュー ID を指定します。「0」（クラス 0）は最も低い優先度のキューで、「7」（クラス 7）が最も高くなります。
Rate Limit	キューレート制限の設定を行います。 「Min Bandwidth」を選択し、最小帯域幅を入力欄に入力します。この値は 64 から 10000000 Kbps で指定できます。 また「Max Bandwidth」で最大帯域幅も入力可能です。この値は 64 から 10000000 Kbps で指定できます。粒度は 64 です。 最小帯域が指定されるとこのキューから送信されるパケットは保証されます。最大値の帯域値が指定されると、その帯域が有効であっても、このキューからの送信パケットは最大の帯域幅を超えることができません。 最小帯域幅を設定する場合、設定された最小帯域幅が保証されるように、設定された最小帯域幅の合計はインターフェイス帯域幅の 75%未満にする必要があります。 最も高い Strict 優先キューは最小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が条件を満たしていれば、このキューのトラフィックが最初に処理されるためにです。 このコマンドの設定は物理ポートにのみ設定可能でポートチャネルには不可能です。それは一つの CoS の最小保証帯域は物理ポート間では使用不可能だからです。 「Min Percent」では最小帯域パーセントを入力欄に入力します。この値は 1 から 100%で指定できます。最大値（Max Percent）も 1 から 100%で指定できます。

「Apply」ボタンをクリックして行った変更を適用します。

注意　キュー帯域幅制御の最小グラニュラリティは 64Kbps です。システムは自動的に 64 倍の数に調整します。

Advanced Settings（アドバンス設定）

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。インタフェースにパケットが受信すると DSCP 変更マップに基づき受信 DSCP は QoS 動作の前に他の DSCP に変更される可能性があります。DSCP 変更は違う DSCP タスクの統合にとても有効です。DSCP-CoS マップと DSCP-color マップはパケット本来の DSCP に基づいて動作します。すべての後続の動作は変更 DSCP に基づいています。

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

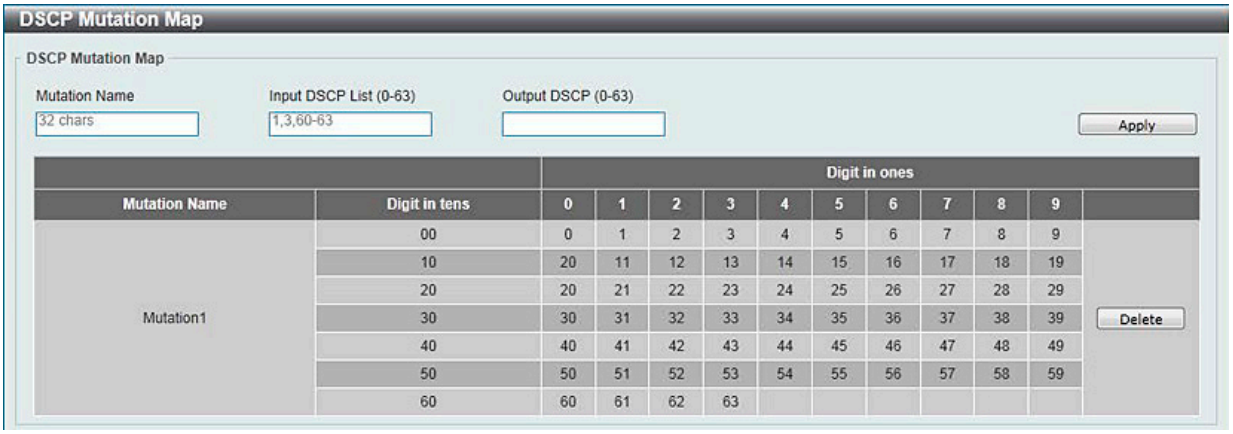


図 10-7　DSCP Mutation Map 画面

本画面には次の項目があります。

項目	説明
Mutation Name	DSCP 変更マップ名を指定します。32 文字以内で指定可能です。
Input DSCP List	インプットされる DSCP リスト値を入力します。0 から 63 で指定可能です。
Output DSCP	アウトプットされる DSCP 値を入力します。0 から 63 で指定可能です。

「Apply」ボタンをクリックし、各項目の変更を適用します。

Port Trust State and Mutation Binding（ポートトラスト設定）

本スイッチにおけるポートトラスト設定と表示を行います。

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

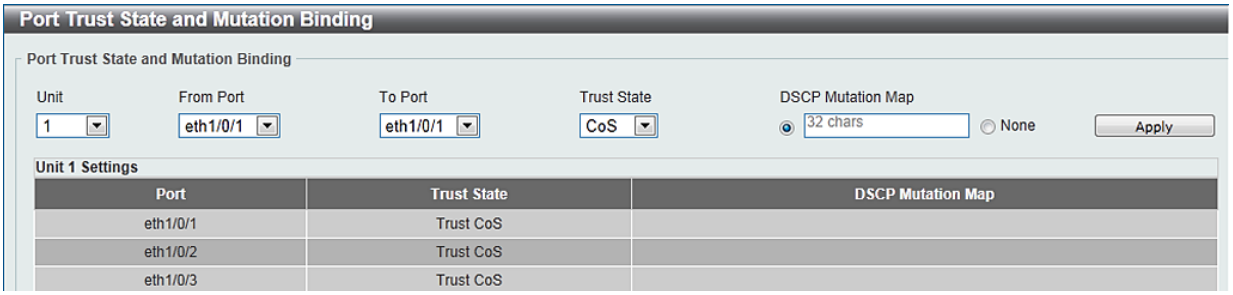


図 10-8　Port Trust State and Mutation Binding 画面

以下の項目を設定または表示できます。

項目	説明
Unit	設定するユニット名を選択します。
From Port / To Port	設定するポート / ポート範囲を入力します。
Trust State	ポートトラストの設定をします。「CoS」「DSCP」から選択可能です。
DSCP Mutation Map	DSCP 変更マップ名を入力します。32 文字以内で設定可能です。 「None」を選択するとポートに DSCP 変更マップを指定しません。

「Apply」ボタンをクリックして行った変更を適用します。

DSCP CoS Mapping（DSCP CoS マップ設定）

本スイッチにおける DSCP CoS マップの設定と表示を行います。

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

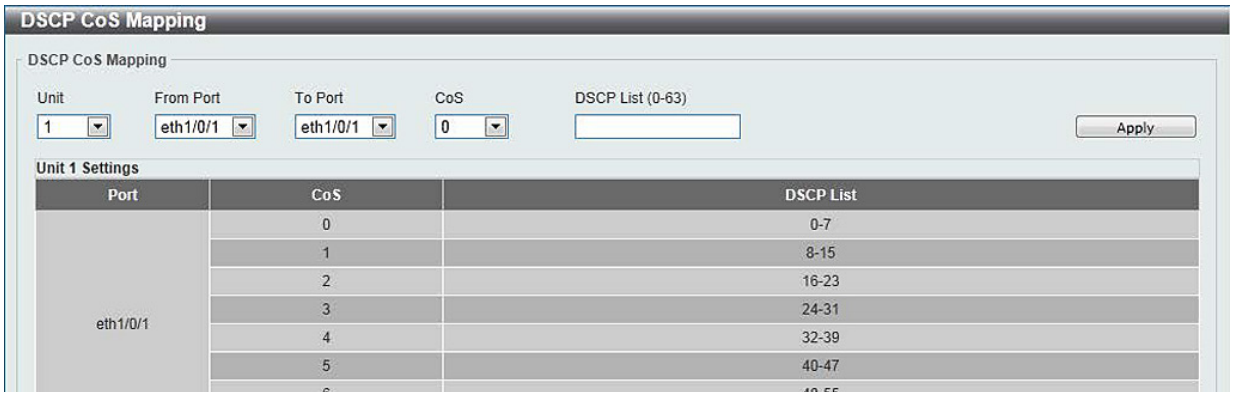


図 10-9　DSCP CoS Mapping 画面

本画面には以下の項目があります。

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

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

CoS Color Mapping（CoS カラーマップ設定）

本スイッチにおける CoS カラーマップの設定と表示を行います。

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

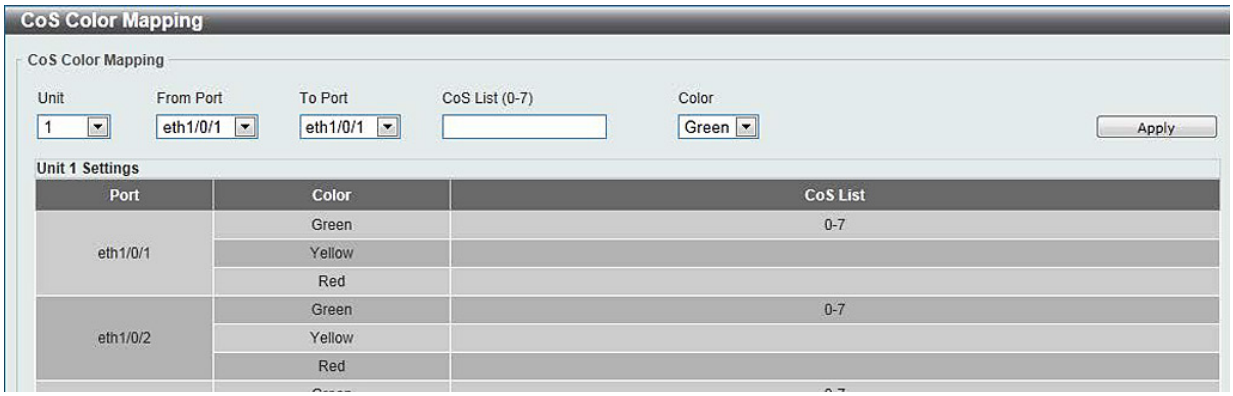


図 10-10　CoS Color Mapping 画面

本画面には以下の項目があります。

項目	説明
Unit	設定するユニットを指定します。
From Port/To Port	設定の対象となるポートを指定します。
CoS List	カラーマップされる CoS の値を指定します。0 から 7 の間で指定可能です。
Color	マップされるカラーを指定します。「Green」「Yellow」「Red」から指定可能です。

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

DSCP Color Mapping（DSCP カラーマップ設定）

本スイッチにおける DSCP カラーマップの設定と表示を行います。

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



図 10-11　DSCP Color Mapping 画面

本画面には以下の項目があります。

項目	説明
Unit	設定するユニットを指定します。
From Port/To Port	設定の対象となるポートを指定します。
DSCP List	カラーマップされる DSCP の値を指定します。0 から 63 の間で指定可能です。
Color	マップされるカラーを指定します。「Green」「Yellow」「Red」から指定可能です。

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

Class Map（クラスマップ設定）

本スイッチにおけるクラスマップの設定と表示を行います。

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



図 10-12　Class Map 画面

本画面には以下の項目があります。

項目	説明
Class Map Name	クラスマップ名を指定します。32 文字まで指定可能です。
Multiple Match Criteria	複数の一致基準オプションを指定します。「Match All」「Match Any」から選択可能です。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Match」ボタンをクリックし、指定のエントリを設定します。
「Delete」ボタンをクリックし、指定のエントリを削除します。

「Match」ボタンをクリックすると下記の画面が表示されます。

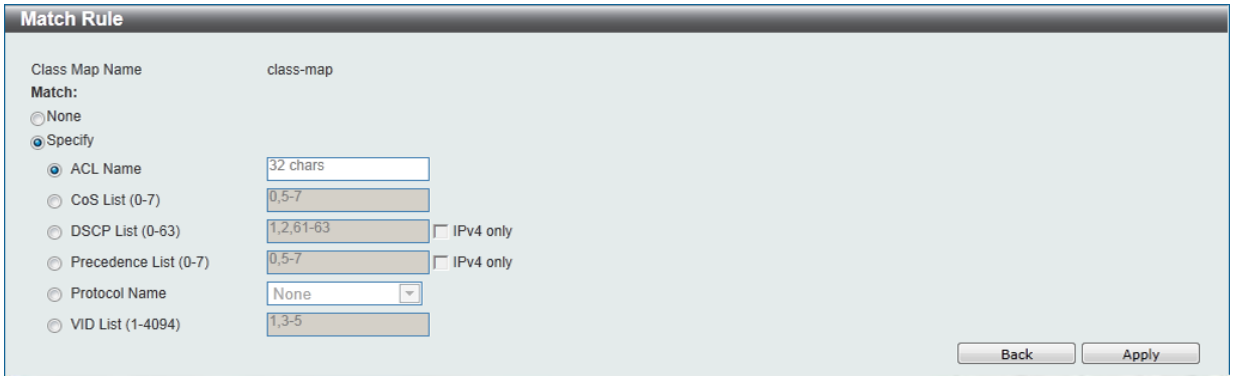


図 10-13　Match Rule 画面

本画面には以下の項目があります。

項目	説明
None	このクラスマップと何もマッチさせない場合に選択します。
Specify	このクラスマップと下記のオプションのどれかをマッチさせる場合に選択します。
ACL Name	クラスマップとマッチさせるアクセスリスト名を指定します。32 文字まで指定できます。
CoS List	クラスマップとマッチさせる CoS リスト名を指定します。0 から 7 まで指定できます。
DSCP List	クラスマップとマッチさせる DSCP リスト名を指定します。0 から 63 まで指定できます。 「IPv4 only」にチェックを入れると IPv4 パケットのみとマッチします。チェックを入れないと IPv4/v6 どちらのパケットともマッチします。
Precedence List	クラスマップとマッチさせる優先リスト名を指定します。0 から 7 まで指定できます。 「IPv4 only」にチェックを入れると IPv4 パケットのみとマッチします。チェックを入れないと IPv4/v6 どちらのパケットともマッチします。IPv6 パケットの場合、IPv6 ヘッダのトラフィッククラスにある 3 つの重要なビットになります。
Protocol Name	クラスマップとマッチさせるプロトコル名を指定します。「None」「ARP」「BGP」「DHCP」「DNS」「EGP」「FTP」「IPv4」「IPv6」「NetBIOS」「NFS」「NTP」「OSPF」「PPPOE」「RIP」「RTSP」「SSH」「Telnet」「TFTP」から選択可能です。
VID List	クラスマップとマッチさせる VLAN リストを指定します。1 から 4094 まで指定できます。

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

Aggregate Policer（アグリゲートポリサー設定）

本スイッチにおけるアグリゲートポリサーの設定と表示を行います。

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

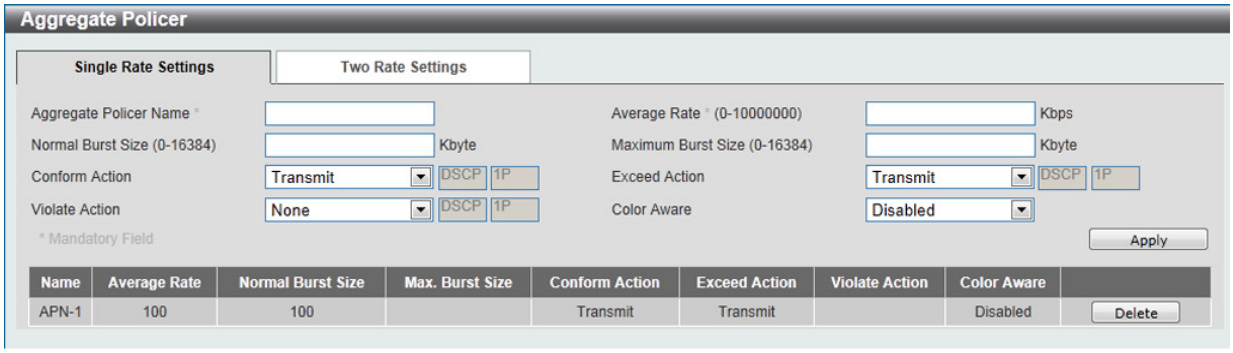


図 10-14　Aggregate Policer 画面

本画面には以下の項目があります。

項目	説明
Aggregate Policer Name	アグリゲートポリサー名を入力します。
Average Rate	平均レート値を入力します。0 から 10000000 kbps まで指定可能です。
Normal Burst Size	ノーマルバーストサイズを入力します。0 から 16384 Kbytes まで指定可能です。
Maximum Burst Size	最大バーストサイズを入力します。0 から 16384 Kbytes まで指定可能です。

項目	説明
Confirm Action	ここでは緑色パケットに行う操作を指定します。 アクションをここで指定しない場合、初期アクションは「Transmit」になります。 オプションは「Drop」「Set-DSCP-Transmit」「Set-1P-Transmit」「Transmit」「Set-DSCP-1P」から選択します。 • 「Drop」- パケットを破棄します。 • 「Set-DSCP-Transmit」- IP differentiated services code points（DSCP）を設定して、新しい DSCP 値設定でパケットを送信します。 • 「Set-1P-Transmit」- パケット CoS 値を設定して、新しい CoS 値で送信します。 • 「Set-DSCP-1P」- IP DSCP と 1P transmit の値を入力します。 • 「Transmit」- パケットはそのまま送信されます。
Exceed Action	レート制限を超えたパケットに行う操作を指定します。 アクションをここで指定しない場合、初期アクションは「Drop」になります。 オプションは「Drop」「Set-DSCP-Transmit」「Set-1P-Transmit」「Transmit」「Set-DSCP-1P」から選択します。 • 「Drop」- パケットを破棄します。 • 「Set-DSCP-Transmit」- IP differentiated services code points（DSCP）を設定して、新しい DSCP 値設定でパケットを送信します。 • 「Set-1P-Transmit」- パケット CoS 値を設定して、新しい CoS 値で送信します。 • 「Set-DSCP-1P」- IP DSCP と 1P transmit の値を入力します。 • 「Transmit」- パケットはそのまま送信されます。
Violate Action	ノーマル、そしてシングルレートの最大バーストサイズを超えたパケットに行う操作を指定します。 「CIR」や「PIR」を順守しないパケットの動作を指定します。シングルレートのポリサーの場合、本項目で指定がされないと、シングルレート 2 色ポリサーを作成します。 2 レートポリサーの場合、本項目で指定されないと初期設定は Exceed Action と同等になります。オプションは「None」「Drop」「Set-DSCP-Transmit」「Set-1P-Transmit」「Transmit」「Set-DSCP-1P」から選択します。 • 「Drop」- パケットを破棄します。 • 「Set-DSCP-Transmit」- IP differentiated services code points（DSCP）を設定して、新しい DSCP 値設定でパケットを送信します。 • 「Set-1P-Transmit」- パケット CoS 値を設定して、新しい CoS 値で送信します。 • 「Set-DSCP-1P」- IP DSCP と 1P transmit の値を入力します。 • 「Transmit」- パケットはそのまま送信されます。
Color Aware	「Color Aware」を有効/無効に指定します。「Color Aware」が指定されないとポリサーはブラインドモードで動作します。有効の場合はポリサーは Color Aware モードで動作します。

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

「Two Rate Setting」タブをクリックすると次のページが表示されます。

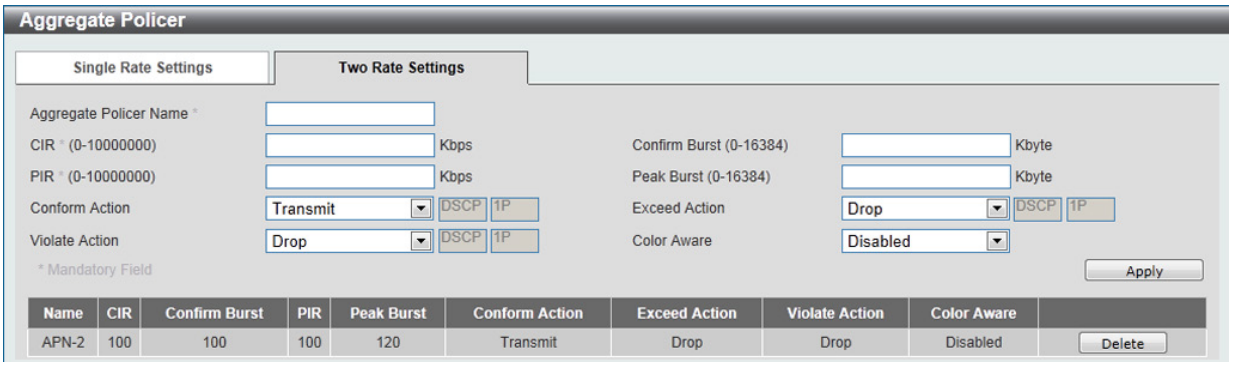


図 10-15　Two Rate Setting 画面

本画面には以下の項目があります。

項目	説明
Aggregate Policer Name	アグリゲートポリサー名を入力します。
CIR	CIR 値を入力します。0 から 10000000 kbps まで指定可能です。 コミットされたパケットは 2 レートメータリングにおける最初のトークンバケットになります。
Confirm Burst	バーストサイズを入力します。0 から 16384 Kbytes まで指定可能です。 Confirm Burst は kbps における最初のトークンバケットのバーストサイズになります。
PIR	PIR 値を入力します。0 から 10000000 kbps まで指定可能です。 PIR は 2 レートメータリングにおける二つ目のトークンバケットになります。
Peak Burst	ピークバーストサイズを入力します。0 から 16384 Kbytes まで指定可能です。 ピークバーストサイズは kbps における二つ目のトークンバケットのバーストサイズになります。

項目	説明
Confirm Action	ここでは緑色パケットに行う操作を指定します。 アクションをここで指定しない場合、初期アクションは「Transmit」になります。 オプションは「Drop」「Set-DSCP-Transmit」「Set-1P-Transmit」「Transmit」「Set-DSCP-1P」から選択します。 • 「Drop」- パケットを破棄します。 • 「Set-DSCP-Transmit」- IP differentiated services code points（DSCP）を設定して、新しい DSCP 値設定でパケットを送信します。 • 「Set-1P-Transmit」- パケット CoS 値を設定して、新しい CoS 値で送信します。 • 「Set-DSCP-1P」- IP DSCP と 1P transmit の値を入力します。 • 「Transmit」- パケットはそのまま送信されます。
Exceed Action	レート制限を超えたパケットに行う操作を指定します。 アクションをここで指定しない場合、初期アクションは「Drop」になります。 オプションは「Drop」「Set-DSCP-Transmit」「Set-1P-Transmit」「Transmit」「Set-DSCP-1P」から選択します。 • 「Drop」- パケットを破棄します。 • 「Set-DSCP-Transmit」- IP differentiated services code points（DSCP）を設定して、新しい DSCP 値設定でパケットを送信します。 • 「Set-1P-Transmit」- パケット CoS 値を設定して、新しい CoS 値で送信します。 • 「Set-DSCP-1P」- IP DSCP と 1P transmit の値を入力します。 • 「Transmit」- パケットはそのまま送信されます。
Violate Action	ノーマル、そしてシングルレートの最大バーストサイズを超えたパケットに行う操作を指定します。 「CIR」や「PIR」を順守しないパケットの動作を指定します。シングルレートのポリサーの場合、本項目で指定がされないと、シングルレート 2 色ポリサーを作成します。 2 レートポリサーの場合、本項目で指定されないと初期設定は Exceed Action と同等になります。オプションは「Drop」「Set-DSCP-Transmit」「Set-1P-Transmit」「Transmit」「Set-DSCP-1P」から選択します。 • 「Drop」- パケットを破棄します。 • 「Set-DSCP-Transmit」- IP differentiated services code points（DSCP）を設定して、新しい DSCP 値設定でパケットを送信します。 • 「Set-1P-Transmit」- パケット CoS 値を設定して、新しい CoS 値で送信します。 • 「Set-DSCP-1P」- IP DSCP と 1P transmit の値を入力します。 • 「Transmit」- パケットはそのまま送信されます。
Color Aware	「Color Aware」を有効 / 無効に指定します。「Color Aware」が指定されないとポリサーはブラインドモードで動作します。有効の場合はポリサーは Color Aware モードで動作します。

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

Policy Map（ポリシーマップ設定）

本スイッチにおけるポリシーマップの設定と表示を行います。

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

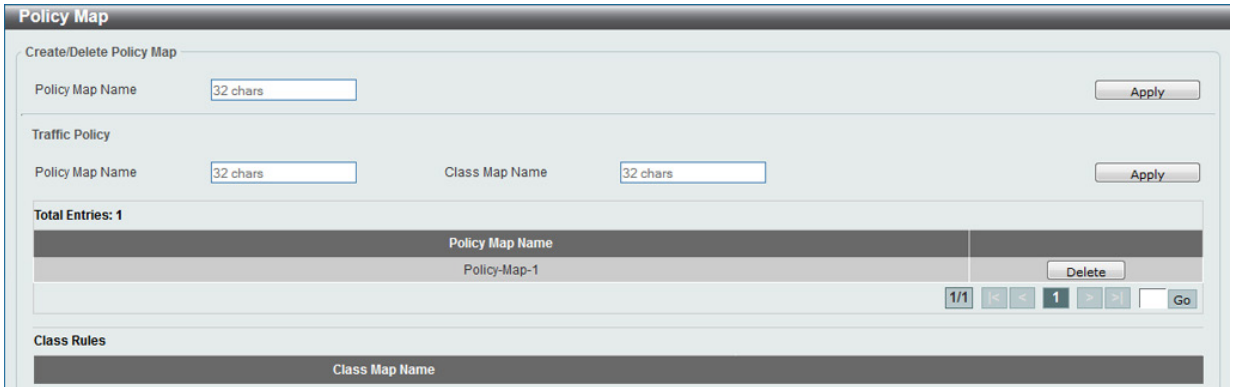


図 10-16　Policy Map 画面

本画面の「Create/Delete Policy Map」には以下の項目があります。

項目	説明
Policy Map Name	ポリシーマップ名を指定します。32 文字まで指定可能です。

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

本画面の「Traffic Policy」には以下の項目があります。

項目	説明
Policy Map Name	ポリシーマップ名を指定します。32 文字まで指定可能です。
Class Map Name	クラスマップ名を指定します。32 文字まで指定可能です。

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

「Delete」ボタンをクリックし、指定のエントリを削除します。
指定のポリシーマップルールを表示するにはテーブルのポリシーマップをクリックします。

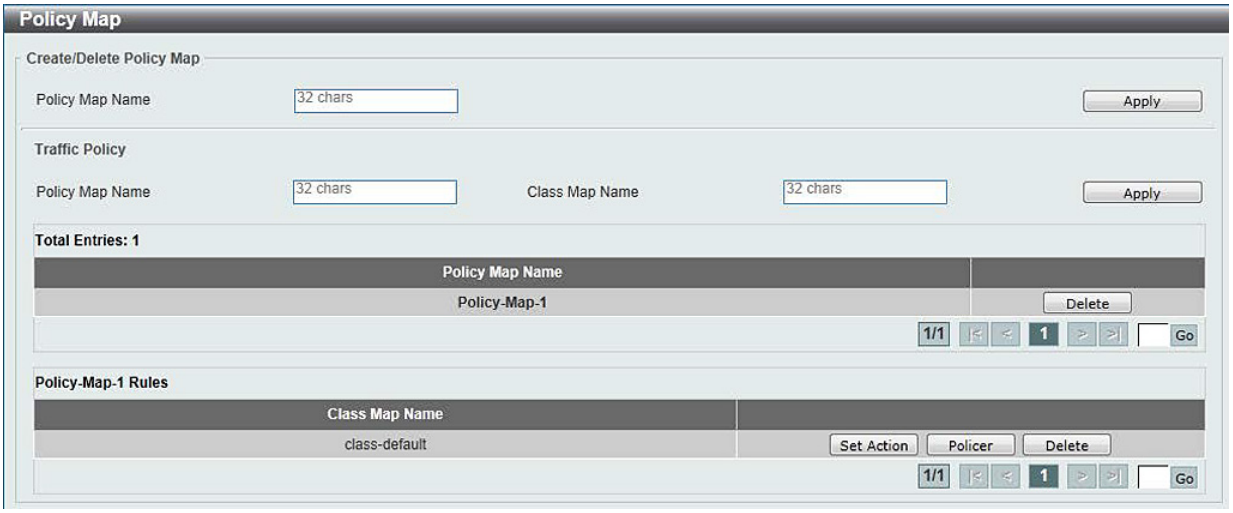


図 10-17　Policy Map (View Rules) 画面

「Policer」ボタンをクリックし、指定のポリシーマップのポリサーアクション設定をします。
「Delete」ボタンをクリックし、指定のエントリを削除します。

「Set Action」ボタンをクリックし、指定のポリシーマップの設定をします。以下の画面が表示されます。

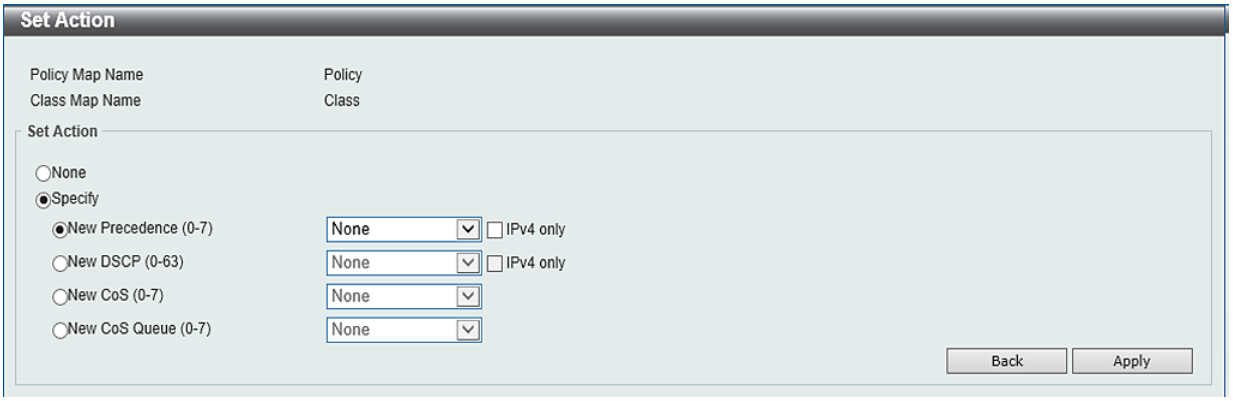


図 10-18　Set Action 画面

本画面には以下の項目があります。

項目	説明
None	このマップと何もマッチさせない場合に選択します。
Specify	このマップとオプションのどれかをマッチさせる場合に選択します。
New Precedence	パケットの優先値を指定します。0 から 7 まで指定できます。 「IPv4 only」にチェックを入れると IPv4 パケット優先になります。CoS キュー選択には影響ありません。
New DSCP	パケットの新しい DSCP 名を指定します。0 から 63 まで指定できます。 「IPv4 only」にチェックを入れると IPv4 パケット優先になります。CoS キュー選択には影響ありません。
New CoS	パケットの新しい CoS 値を指定します。0 から 7 まで指定できます。CoS キュー選択には影響ありません。
New CoS Queue	パケットの新しい CoS キューを指定します。0 から 7 まで指定できます。CoS キュー選択を上書きします。

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

「Policer」ボタンをクリックすると以下の画面が表示されます。

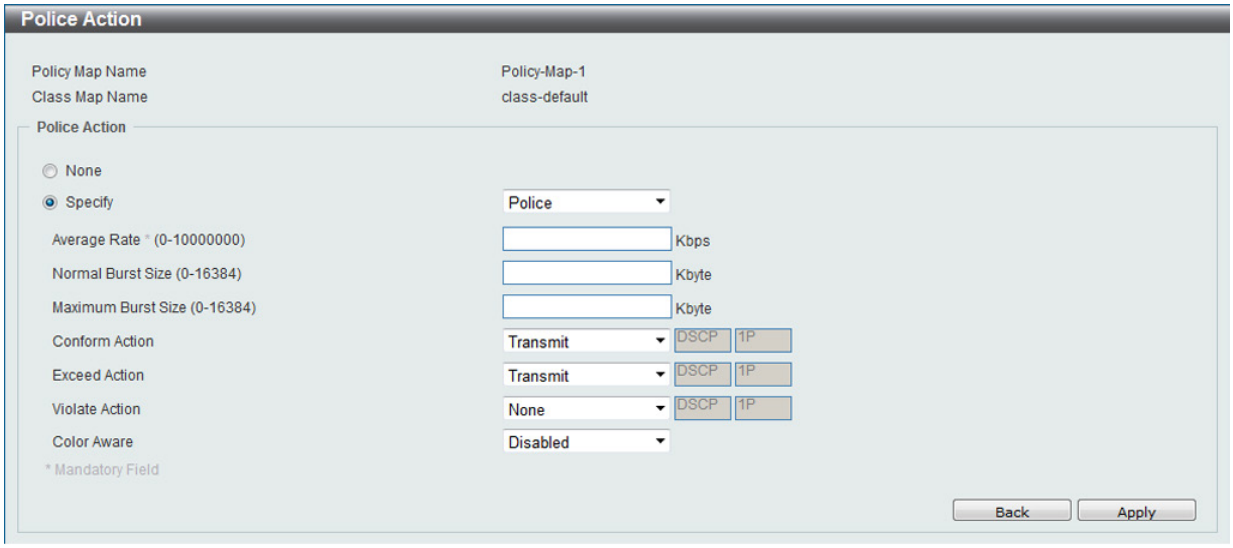


図 10-19　Policer 画面

本画面には以下の項目があります。

項目	説明
None	このマップと何もマッチさせない場合に選択します。
Specify	このマップとオプションのどれかをマッチさせる場合に選択します。
Average Rate	アベレージレート値を入力します。
Normal Burst Size	ノーマルバーストサイズを入力します。
Maximum Burst Size	最大バーストサイズを入力します。
Confirm Action	ここでは緑色パケットに行う操作を指定します。 オプションは「Drop」「Set-DSCP-Transmit」「Set-1P-Transmit」「Transmit」「Set-DSCP-1P」から選択します。
Exceed Action	ここでは黄色パケットに行う操作を指定します。 オプションは「Drop」「Set-DSCP-Transmit」「Set-1P-Transmit」「Transmit」「Set-DSCP-1P」から選択します。
Violate Action	ここでは赤色パケットに行う操作を指定します。 オプションは「Drop」「Set-DSCP-Transmit」「Set-1P-Transmit」「Transmit」「Set-DSCP-1P」から選択します。
Color Aware	「Color Aware」を有効 / 無効に指定します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
前画面に戻る場合は「Back」をクリックします。

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。

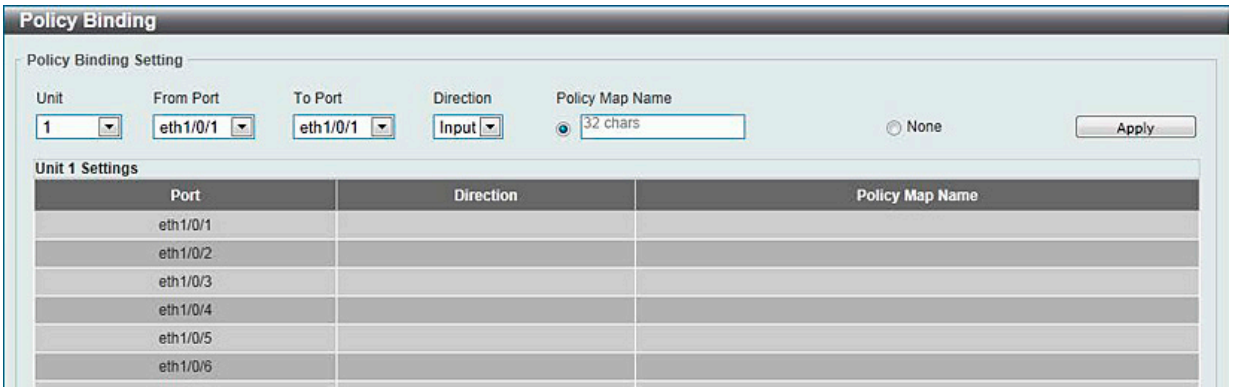


図 10-20　Policy Binding 画面

本画面には以下の項目があります。

項目	説明
Unit	設定するユニットを指定します。
From Port/To Port	設定の対象となるポートを指定します。
Direction	方向を指定します。「Input」が選択可能です。「Input」は指定のイングレストラフィックのことです。
Policy Map Name	ポリシーマップ名を指定します。32 文字まで指定可能です。「None」を選択すると本エントリにポリシーマップは関連付けられません。

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

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 VLAN Access Map（ACL VLAN アクセスマップ）	ACL VLAN アクセスマップの設定を行います。
ACL VLAN Filter（ACL VLAN フィルタ設定）	ACL VLAN フィルタの設定を行います。

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。

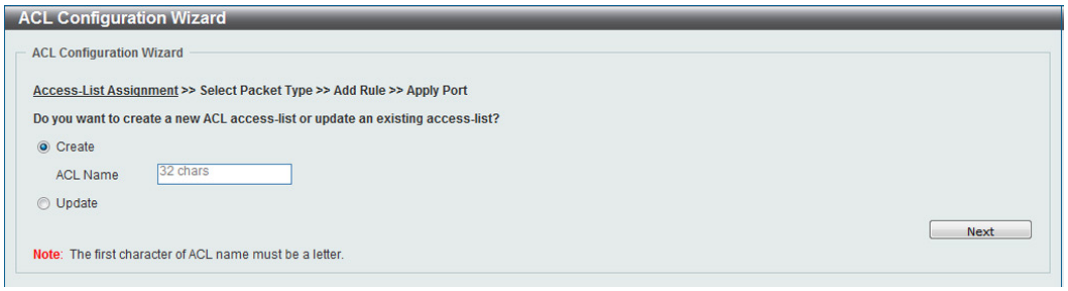


図 11-1　ACL Configuration Wizard 画面（Create）

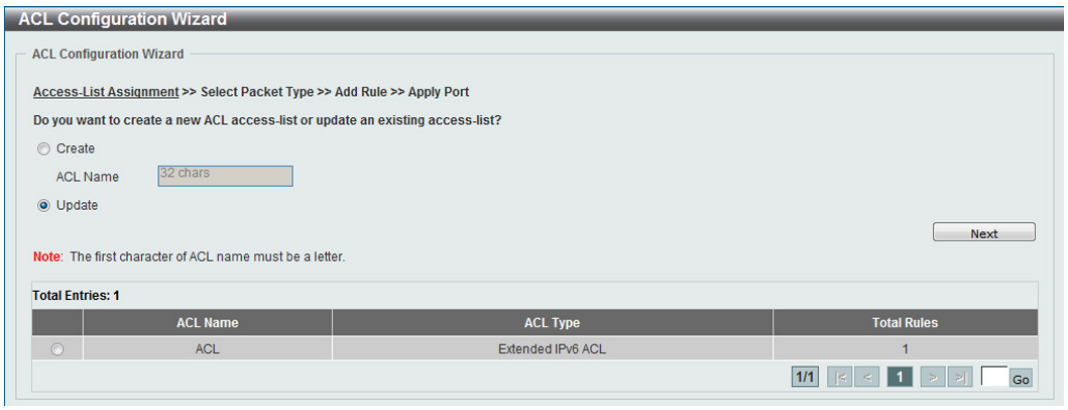


図 11-2　ACL Configuration Wizard 画面（Update）

本画面には以下の項目があります。

項目	説明
Create	最大 32 文字までで ACL 名を入力します。
Update	既存の ACL アクセスリストを表示し、エントリを再設定する場合に選択します。

「Next」をクリックし、パケットタイプの選択を行います。
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、指定のページへ移動します。

パケットタイプ選択（ACL 設定ウィザード）

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

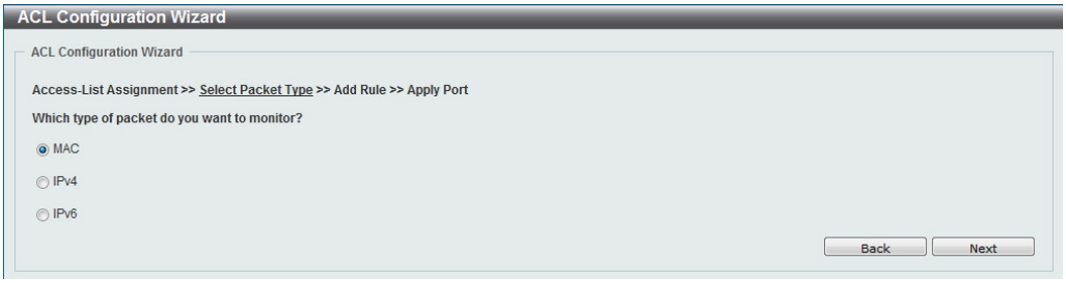


図 11-3　ACL Configuration Wizard (Select Packet Type) 画面

本画面には以下の項目があります。

項目	説明
MAC	MAC ACL を選択します。
IPv4	IPv4 ACL を選択します。
IPv6	IPv6 ACL を選択します。

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

プロトコル設定（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 エントリにおけるプロトコルの設定を行います。

MAC ACL Rule の設定

MAC ACL Rule を設定します。「MAC」を選択し「Next」をクリックし、表示された以下の画面の設定を行います。

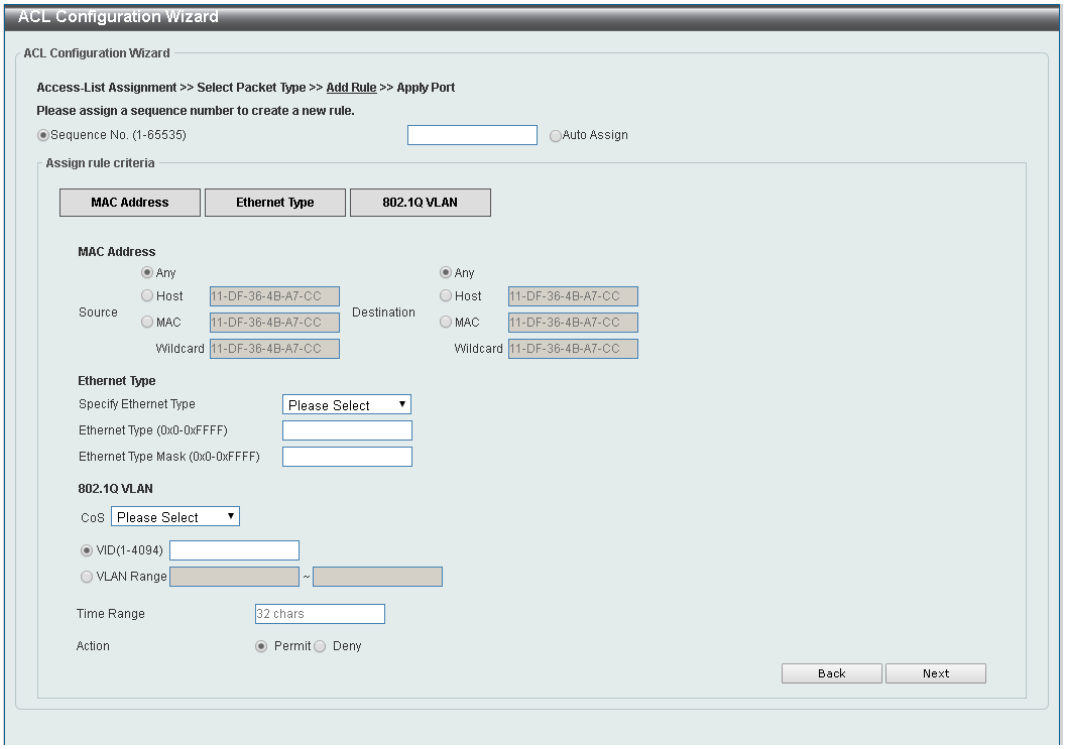


図 11-4　ACL Configuration Wizard - MAC ACL Rule 画面

画面に表示される項目

項目	説明
シーケンス番号の指定	
Sequence No. (1-65535)	シーケンス番号を指定します。「1」から「65535」の間で指定できます。
Auto Assign	新規ルール用のシーケンス番号を自動でアサインします。

項目	説明
Assign Rule Criteria:（MAC アドレスの設定）	
Source	送信元の MAC アドレスを指定します。「Any」「Host」「MAC」から指定します。 「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの MAC アドレスを入力します。 「MAC」を選択すると「Wildcard」オプションが選択可能になり送信元 MAC アドレスとワイルドカードを入力することができます。
Destination	宛先の MAC アドレスを指定します。「Any」「Host」「MAC」から指定します。 「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。 「Host」を選択すると宛先ホストの MAC アドレスを入力します。 「MAC」を選択すると「Wildcard」オプションが選択可能になり宛先 MAC アドレスとワイルドカードを入力することができます。
Specify Ethernet Type	イーサネットタイプを選択します。「aarp」「appletalk」「decent-iv」「etype-6000」「etype-8042」「lat」「lavc-sca」「mop-console」「mop-dump」「vines-echo」「vines-ip」「xns-idp」「arp」から選択します。
Ethernet Type	イーサネットタイプの 16 進数値を指定します。0x0 から 0xFFFF の間で指定できます。「Specify Ethernet Type」で指定したイーサネットタイプに基づき適切な値が入力されます。
Ethernet Type Mask	イーサネットタイプマスクの 16 進数値を指定します。0x0 から 0xFFFF の間で指定できます。「Specify Ethernet Type」で指定したイーサネットタイプに基づき適切な値が入力されます。
CoS	CoS の値を入力します。0 から 7 の間で入力できます。
VID	ACL ルールに関連する VLAN ID を入力します。1 から 4094 の間で入力可能です。
VLAN Range	ACL ルールに関連する VLAN 範囲を入力します。
Time Range	ACL ルールに関するタイムレンジ名を指定します。
Action	ルール動作に関する設定を行います。「Permit」または「Deny」から指定できます。

「Next」をクリックします。
「Back」をクリックすると前画面に戻ります。

IPv4 ACL Rule の設定

IPv4 ACL Rule を設定します。「IPv4」を選択し「Next」をクリックし、表示された以下の画面の設定を行います。

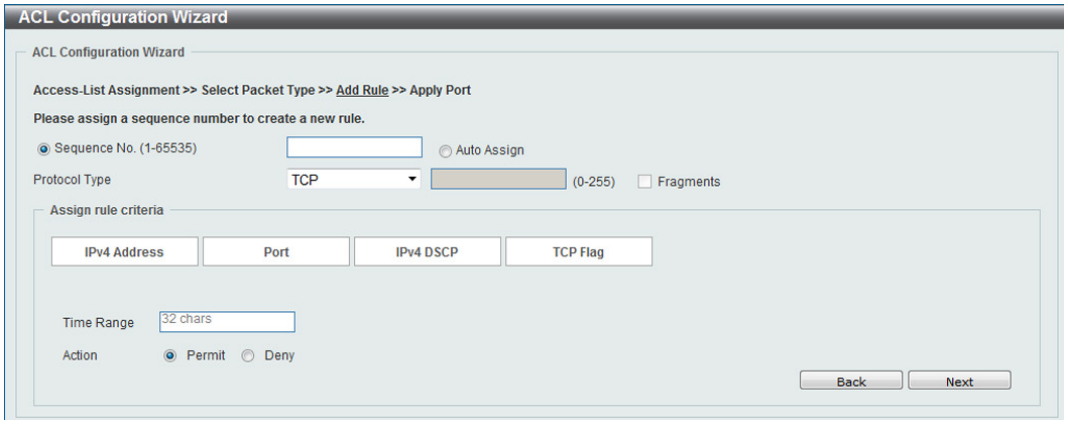


図 11-5　ACL Configuration Wizard -IPv4 画面

画面に表示される項目

項目	説明
Sequence No. (1-65535)	シーケンス番号を指定します。「1」から「65535」の間で指定できます。
Auto Assign	新規ルール用のシーケンス番号を自動でアサインします。
Protocol Type	プロトコルの種類を選択します。「TCP」「UDP」「ICMP」「EIGRP」「ESP」「GRE」「IGMP」「OSPF」「PIM」「VRRP」「IP-in-IP」「PCP」「Protocol ID」「None」から選択します。 選択したプロトコルの種類によってはプロトコルに関連する数値（ID 等）を右の欄に入力する必要があります。その際、欄の右にある制限値（0-255 等）に注意して入力してください。

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

「TCP」選択時に表示される項目（IPv4 ACL Rule / Protocol Type）

「Protocol Type」で TCP 選択時に表示される項目です。

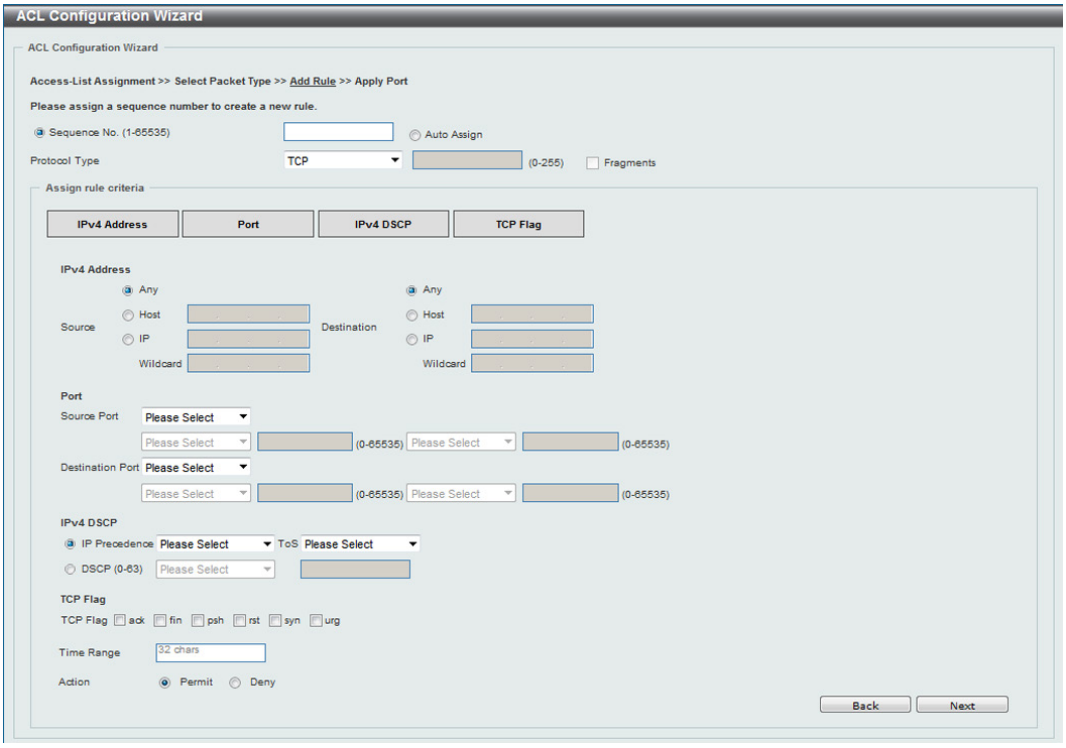


図 11-6　ACL Configuration Wizard (Add Rule for IPv4 ACL) TCP 画面

項目	説明
Source	送信元のアドレスを指定します。「Any」「Host」「IP」から指定します。 「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IP アドレスを入力します。 「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い送信元 IP アドレス群を入力します。ビット値 1 に対応するビットは無視され、ビット値 0 に対応するビットが認識されます。
Destination	宛先のアドレスを指定します。「Any」「Host」「IP」から指定します。 「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IP アドレスを入力します。 「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い宛先 IP アドレス群を入力します。ビット値 1 に対応するビットは無視され、ビット値 0 に対応するビットが認識されます。
Source Port	送信元ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選択した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択すると選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポートが使用されます。「Range」を選択すると指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。
Destination Port	宛先ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選択した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択すると選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポートが使用されます。「Range」を選択すると指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。
IP Precedence	IP 優先値を指定します。「0 (routine)」「1 (priority)」「2, (immediate)」「3 (flash)」「4 (flash-override)」「5 (critical)」「6 (internet)」「7 (network)」から指定できます。
ToS	IP 優先値を選択後、使用する「Type-of-Service」(ToS) の値を指定します。「0 (normal)」「1 (min-monetary-cost)」「2 (max-reliability)」「3, 4(max-throughput)」「5, 6, 7, 8 (min-delay)」「9」「10」「11」「12」「13」「14」「15」から指定できます。
DSCP	使用する DSCP 値を入力します。0 から 63 で入力できます。
TCP Flag	TCP フラグを本ルールに含める場合、該当のフラグにチェックを入れます。「ack」「fin」「psh」「rst」「syn」「urg」から指定できます。
Time Range	ACL ルールに関するタイムレンジ名を指定します。
Action	ルール動作に関する設定を行います。「Permit」または「Deny」から指定できます。

「Next」をクリックします。

「Back」をクリックすると前画面に戻ります。

「UDP」選択時に表示される項目（IPv4 ACL Rule / Protocol Type）

「Protocol Type」で UDP 選択時に表示される項目です。

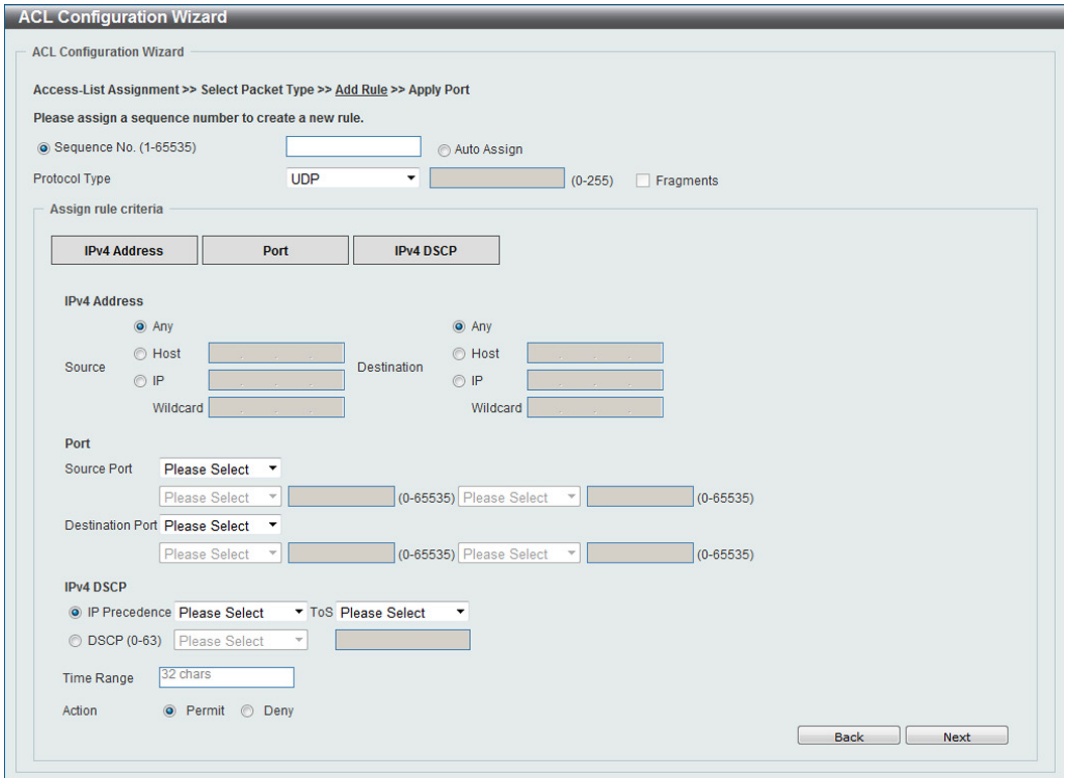


図 11-7　ACL Configuration Wizard (Add Rule for IPv4 ACL) UDP 画面

項目	説明
Source	送信元のアドレスを指定します。「Any」「Host」「IP」から指定します。 「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IP アドレスを入力します。 「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い送信元 IP アドレス群を入力します。ビット値 1 に対応するビットは無視され、ビット値 0 に対応するビットが認識されます。
Destination	宛先のアドレスを指定します。「Any」「Host」「IP」から指定します。 「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IP アドレスを入力します。 「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い宛先 IP アドレス群を入力します。ビット値 1 に対応するビットは無視され、ビット値 0 に対応するビットが認識されます。
Source Port	送信元ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選択した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択すると選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポートが使用されます。「Range」を選択すると指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。
Destination Port	宛先ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選択した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択すると選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポートが使用されます。「Range」を選択すると指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。
IP Precedence	IP 優先値を指定します。「0 (routine)」「1 (priority)」「2, (immediate)」「3 (flash)」「4 (flash-override)」「5 (critical)」「6 (internet)」「7 (network)」から指定できます。
ToS	IP 優先値を選択後、使用する「Type-of-Service」(ToS) の値を指定します。「0 (normal)」「1 (min-monetary-cost)」「2 (max-reliability)」「3, 4(max-throughput)」「5, 6, 7, 8 (min-delay)」「9」「10」「11」「12」「13」「14」「15」から指定できます。
DSCP	使用する DSCP 値を入力します。0 から 63 で入力できます。
Time Range	ACL ルールに関するタイムレンジ名を指定します。
Action	ルール動作に関する設定を行います。「Permit」または「Deny」から指定できます。

「Next」をクリックします。

「Back」をクリックすると前画面に戻ります。

「ICMP」選択時に表示される項目（IPv4 ACL Rule / Protocol Type）

「Protocol Type」で ICMP 選択時に表示される項目です。

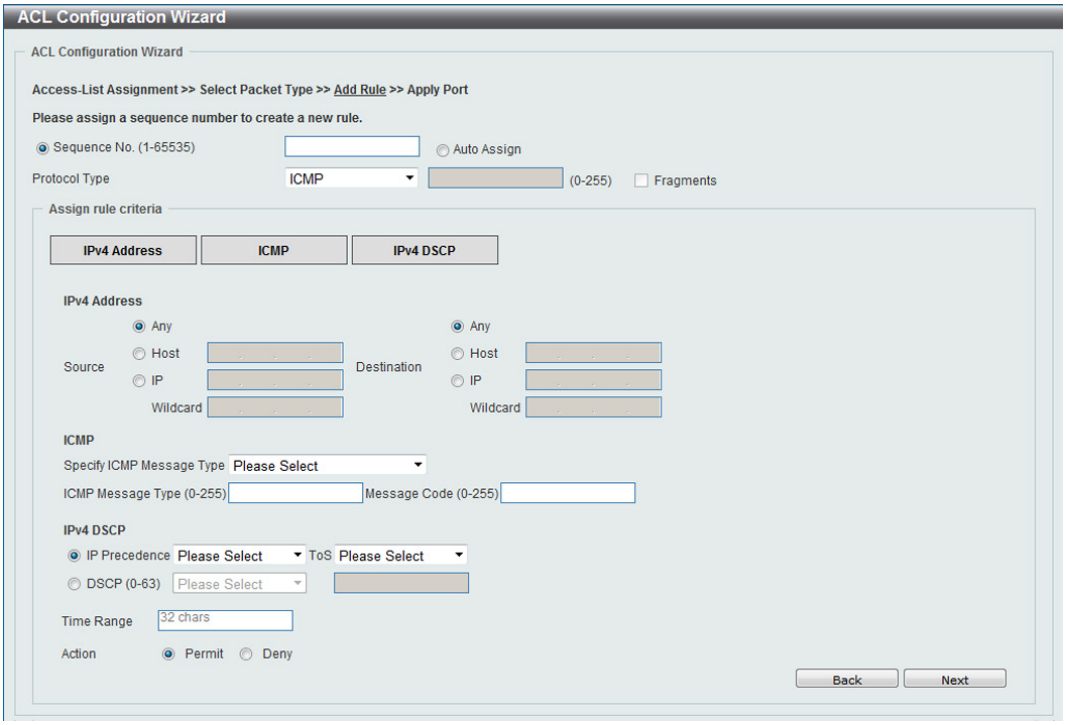


図 11-8　ACL Configuration Wizard (Add Rule for IPv4 ACL) ICMP 画面

項目	説明
Source	送信元のアドレスを指定します。「Any」「Host」「IP」から指定します。 「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IP アドレスを入力します。 「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い送信元 IP アドレス群を入力します。ビット値 1 に対応するビットは無視され、ビット値 0 に対応するビットが認識されます。
Destination	宛先のアドレスを指定します。「Any」「Host」「IP」から指定します。 「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IP アドレスを入力します。 「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い宛先 IP アドレス群を入力します。ビット値 1 に対応するビットは無視され、ビット値 0 に対応するビットが認識されます。
Specify ICMP Message Type	使用する ICMP メッセージの種類を選択します。
ICMP Message Type	ICMP メッセージタイプが選択されていない場合は、使用される ICMP メッセージタイプの数値を入力します。 ICMP メッセージタイプが選択されると、この数値が自動的に入力されます。
Message Code	ICMP メッセージタイプが選択されていない場合、使用されるメッセージコード数値を入力します。 ICMP メッセージタイプが選択されると、この数値が自動的に入力されます。
IP Precedence	IP 優先値を指定します。「0 (routine)」「1 (priority)」「2, (immediate)」「3 (flash)」「4 (flash-override)」「5 (critical)」「6 (internet)」「7 (network)」から指定できます。
ToS	IP 優先値を選択後、使用する「Type-of-Service」(ToS) の値を指定します。「0 (normal)」「1 (min-monetary-cost)」「2 (max-reliability)」「3, 4(max-throughput)」「5, 6, 7, 8 (min-delay)」「9」「10」「11」「12」「13」「14」「15」から指定できます。
DSCP	使用する DSCP 値を入力します。0 から 63 で入力できます。
Time Range	ACL ルールに関するタイムレンジ名を指定します。
Action	ルール動作に関する設定を行います。「Permit」または「Deny」から指定できます。

「Next」をクリックします。

「Back」をクリックすると前画面に戻ります。

「EIGRP」選択時に表示される項目（IPv4 ACL Rule / Protocol Type）

「Protocol Type」で EIGRP 選択時に表示される項目です。

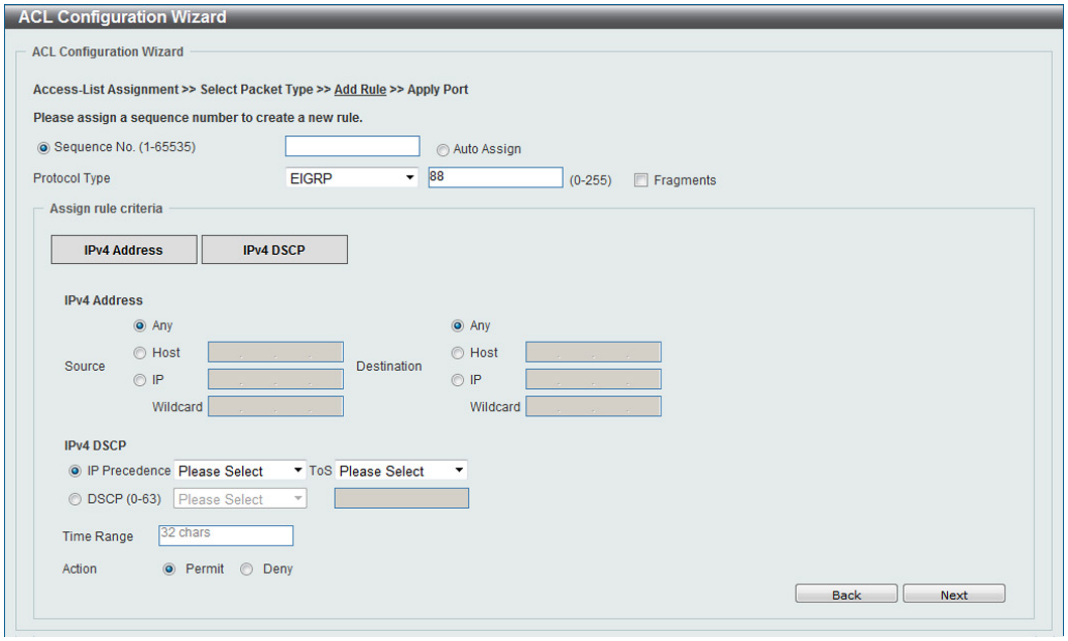


図 11-9　ACL Configuration Wizard (Add Rule for IPv4 ACL) EIGRP 画面

項目	説明
Fragments	パケットフラグメントフィルタリングを使用する場合、選択します。
Source	送信元のアドレスを指定します。「Any」「Host」「IP」から指定します。 「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IP アドレスを入力します。 「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い送信元 IP アドレス群を入力します。ビット値 1 に対応するビットは無視され、ビット値 0 に対応するビットが認識されます。
Destination	宛先のアドレスを指定します。「Any」「Host」「IP」から指定します。 「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IP アドレスを入力します。 「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い宛先 IP アドレス群を入力します。ビット値 1 に対応するビットは無視され、ビット値 0 に対応するビットが認識されます。
IP Precedence	IP 優先値を指定します。「0 (routine)」「1 (priority)」「2, (immediate)」「3 (flash)」「4 (flash-override)」「5 (critical)」「6 (internet)」「7 (network)」から指定できます。
ToS	IP 優先値を選択後、使用する「Type-of-Service」(ToS) の値を指定します。「0 (normal)」「1 (min-monetary-cost)」「2 (max-reliability)」「3, 4(max-throughput)」「5, 6, 7, 8 (min-delay)」「9」「10」「11」「12」「13」「14」「15」から指定できます。
DSCP	使用する DSCP 値を入力します。0 から 63 で入力できます。
Time Range	ACL ルールに関するタイムレンジ名を指定します。
Action	ルール動作に関する設定を行います。「Permit」または「Deny」から指定できます。

「Next」をクリックします。
「Back」をクリックすると前画面に戻ります。

「ESP」選択時に表示される項目（IPv4 ACL Rule / Protocol Type）

「Protocol Type」で ESP 選択時に表示される項目です。

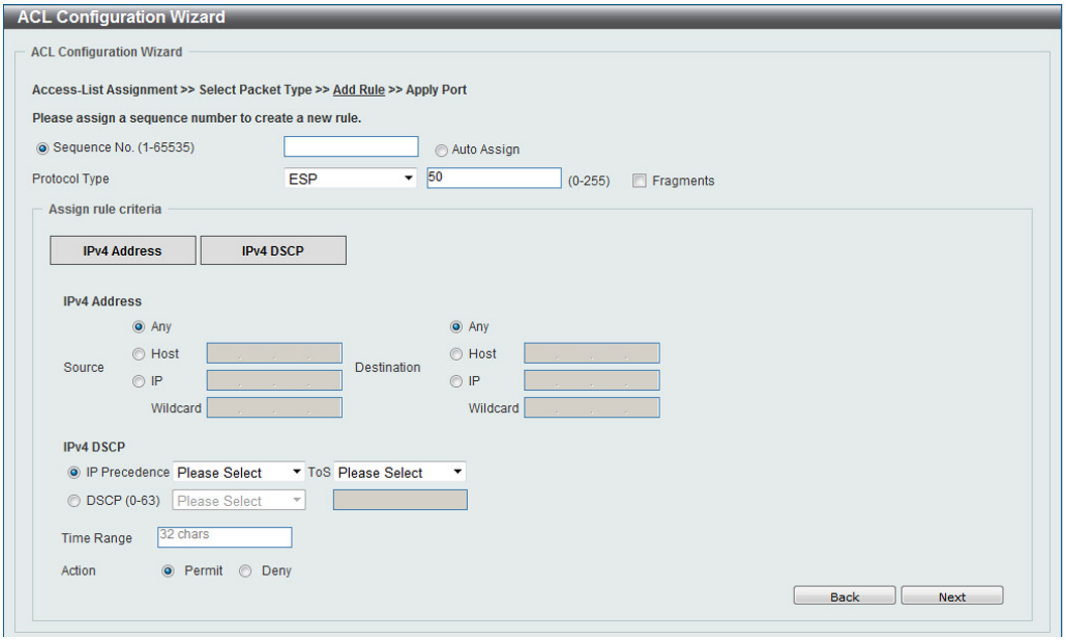


図 11-10　ACL Configuration Wizard (Add Rule for IPv4 ACL) ESP 画面

項目	説明
Fragments	パケットフラグメントフィルタリングを使用する場合、選択します。
Source	送信元のアドレスを指定します。「Any」「Host」「IP」から指定します。 「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IP アドレスを入力します。 「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い送信元 IP アドレス群を入力します。ビット値 1 に対応するビットは無視され、ビット値 0 に対応するビットが認識されます。
Destination	宛先のアドレスを指定します。「Any」「Host」「IP」から指定します。 「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IP アドレスを入力します。 「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い宛先 IP アドレス群を入力します。ビット値 1 に対応するビットは無視され、ビット値 0 に対応するビットが認識されます。
IP Precedence	IP 優先値を指定します。「0 (routine)」「1 (priority)」「2, (immediate)」「3 (flash)」「4 (flash-override)」「5 (critical)」「6 (internet)」「7 (network)」から指定できます。
ToS	IP 優先値を選択後、使用する「Type-of-Service」(ToS) の値を指定します。「0 (normal)」「1 (min-monetary-cost)」「2 (max-reliability)」「3, 4(max-throughput)」「5, 6, 7, 8 (min-delay)」「9」「10」「11」「12」「13」「14」「15」から指定できます。
DSCP	使用する DSCP 値を入力します。0 から 63 で入力できます。
Time Range	ACL ルールに関するタイムレンジ名を指定します。
Action	ルール動作に関する設定を行います。「Permit」または「Deny」から指定できます。

「Next」をクリックします。

「Back」をクリックすると前画面に戻ります。

「GRE」選択時に表示される項目（IPv4 ACL Rule / Protocol Type）

「Protocol Type」で GRE 選択時に表示される項目です。

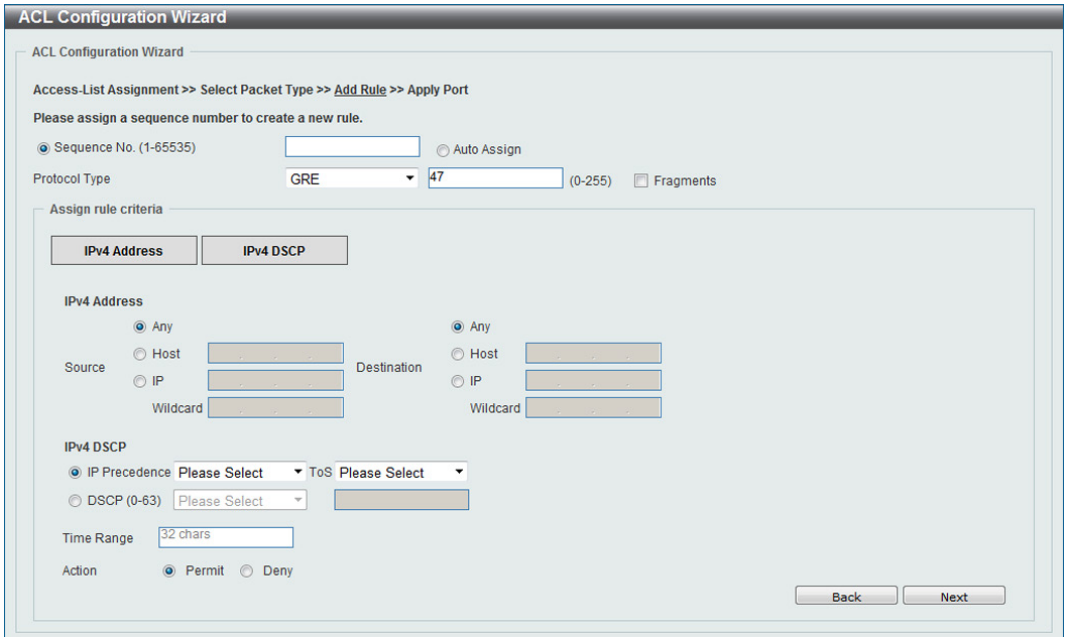


図 11-11　ACL Configuration Wizard (Add Rule for IPv4 ACL) GRE 画面

項目	説明
Fragments	パケットフラグメントフィルタリングを使用する場合、選択します。
Source	送信元のアドレスを指定します。「Any」「Host」「IP」から指定します。 「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IP アドレスを入力します。 「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い送信元 IP アドレス群を入力します。ビット値 1 に対応するビットは無視され、ビット値 0 に対応するビットが認識されます。
Destination	宛先のアドレスを指定します。「Any」「Host」「IP」から指定します。 「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IP アドレスを入力します。 「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い宛先 IP アドレス群を入力します。ビット値 1 に対応するビットは無視され、ビット値 0 に対応するビットが認識されます。
IP Precedence	IP 優先値を指定します。「0 (routine)」「1 (priority)」「2, (immediate)」「3 (flash)」「4 (flash-override)」「5 (critical)」「6 (internet)」「7 (network)」から指定できます。
ToS	IP 優先値を選択後、使用する「Type-of-Service」(ToS) の値を指定します。「0 (normal)」「1 (min-monetary-cost)」「2 (max-reliability)」「3, 4(max-throughput)」「5, 6, 7, 8 (min-delay)」「9」「10」「11」「12」「13」「14」「15」から指定できます。
DSCP	使用する DSCP 値を入力します。0 から 63 で入力できます。
Time Range	ACL ルールに関するタイムレンジ名を指定します。
Action	ルール動作に関する設定を行います。「Permit」または「Deny」から指定できます。

「Next」をクリックします。
「Back」をクリックすると前画面に戻ります。

「IGMP」選択時に表示される項目（IPv4 ACL Rule / Protocol Type）

「Protocol Type」で IGMP 選択時に表示される項目です。

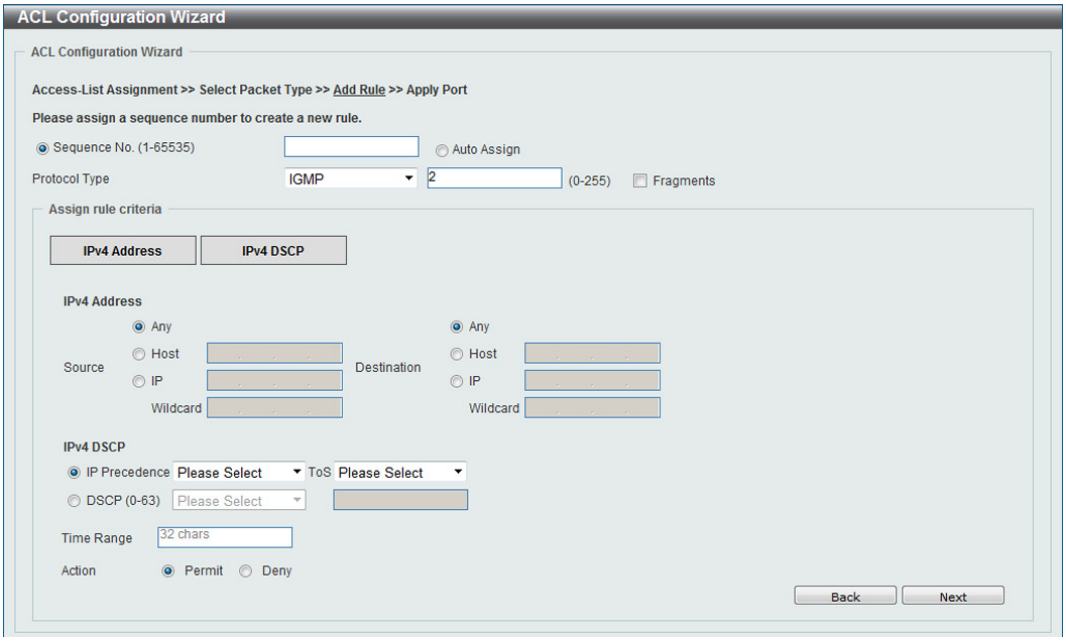


図 11-12　ACL Configuration Wizard (Add Rule for IPv4 ACL) IGMP 画面

項目	説明
Fragments	パケットフラグメントフィルタリングを使用する場合、選択します。
Source	送信元のアドレスを指定します。「Any」「Host」「IP」から指定します。 「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IP アドレスを入力します。 「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い送信元 IP アドレス群を入力します。ビット値 1 に対応するビットは無視され、ビット値 0 に対応するビットが認識されます。
Destination	宛先のアドレスを指定します。「Any」「Host」「IP」から指定します。 「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IP アドレスを入力します。 「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い宛先 IP アドレス群を入力します。ビット値 1 に対応するビットは無視され、ビット値 0 に対応するビットが認識されます。
IP Precedence	IP 優先値を指定します。「0 (routine)」「1 (priority)」「2, (immediate)」「3 (flash)」「4 (flash-override)」「5 (critical)」「6 (internet)」「7 (network)」から指定できます。
ToS	IP 優先値を選択後、使用する「Type-of-Service」(ToS) の値を指定します。「0 (normal)」「1 (min-monetary-cost)」「2 (max-reliability)」「3, 4(max-throughput)」「5, 6, 7, 8 (min-delay)」「9」「10」「11」「12」「13」「14」「15」から指定できます。
DSCP	使用する DSCP 値を入力します。0 から 63 で入力できます。
Time Range	ACL ルールに関するタイムレンジ名を指定します。
Action	ルール動作に関する設定を行います。「Permit」または「Deny」から指定できます。

「Next」をクリックします。

「Back」をクリックすると前画面に戻ります。

「OSPF」選択時に表示される項目（IPv4 ACL Rule / Protocol Type）

「Protocol Type」で OSPF 選択時に表示される項目です。

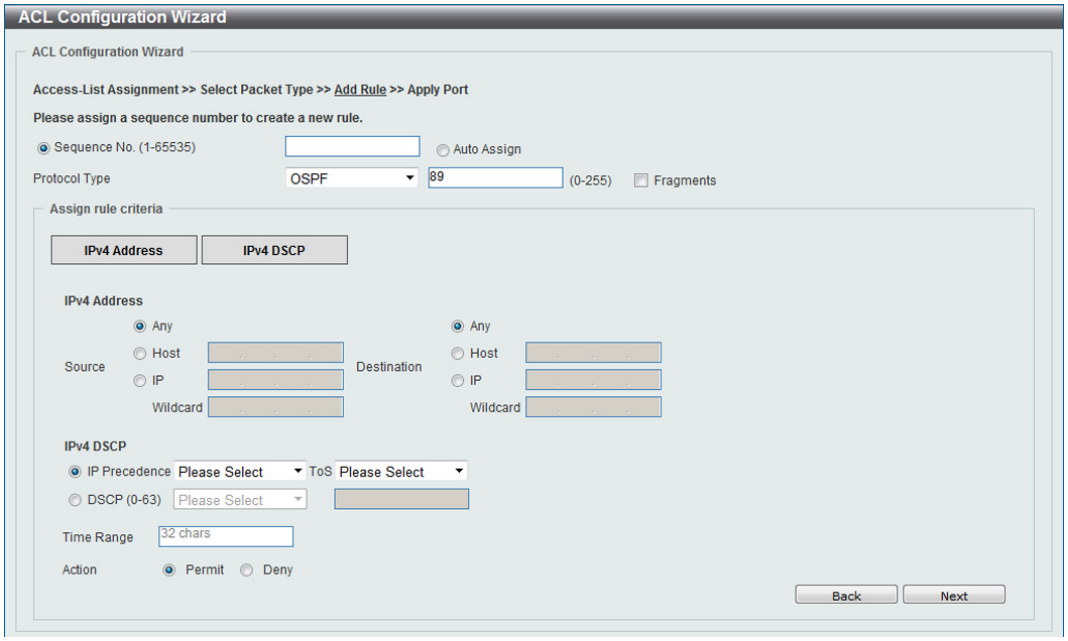


図 11-13　ACL Configuration Wizard (Add Rule for IPv4 ACL) OSPF 画面

項目	説明
Fragments	パケットフラグメントフィルタリングを使用する場合、選択します。
Source	送信元のアドレスを指定します。「Any」「Host」「IP」から指定します。 「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IP アドレスを入力します。 「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い送信元 IP アドレス群を入力します。ビット値 1 に対応するビットは無視され、ビット値 0 に対応するビットが認識されます。
Destination	宛先のアドレスを指定します。「Any」「Host」「IP」から指定します。 「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IP アドレスを入力します。 「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い宛先 IP アドレス群を入力します。ビット値 1 に対応するビットは無視され、ビット値 0 に対応するビットが認識されます。
IP Precedence	IP 優先値を指定します。「0 (routine)」「1 (priority)」「2, (immediate)」「3 (flash)」「4 (flash-override)」「5 (critical)」「6 (internet)」「7 (network)」から指定できます。
ToS	IP 優先値を選択後、使用する「Type-of-Service」(ToS) の値を指定します。「0 (normal)」「1 (min-monetary-cost)」「2 (max-reliability)」「3, 4(max-throughput)」「5, 6, 7, 8 (min-delay)」「9」「10」「11」「12」「13」「14」「15」から指定できます。
DSCP	使用する DSCP 値を入力します。0 から 63 で入力できます。
Time Range	ACL ルールに関するタイムレンジ名を指定します。
Action	ルール動作に関する設定を行います。「Permit」または「Deny」から指定できます。

「Next」をクリックします。

「Back」をクリックすると前画面に戻ります。

「PIM」選択時に表示される項目（IPv4 ACL Rule / Protocol Type）

「Protocol Type」で PIM 選択時に表示される項目です。

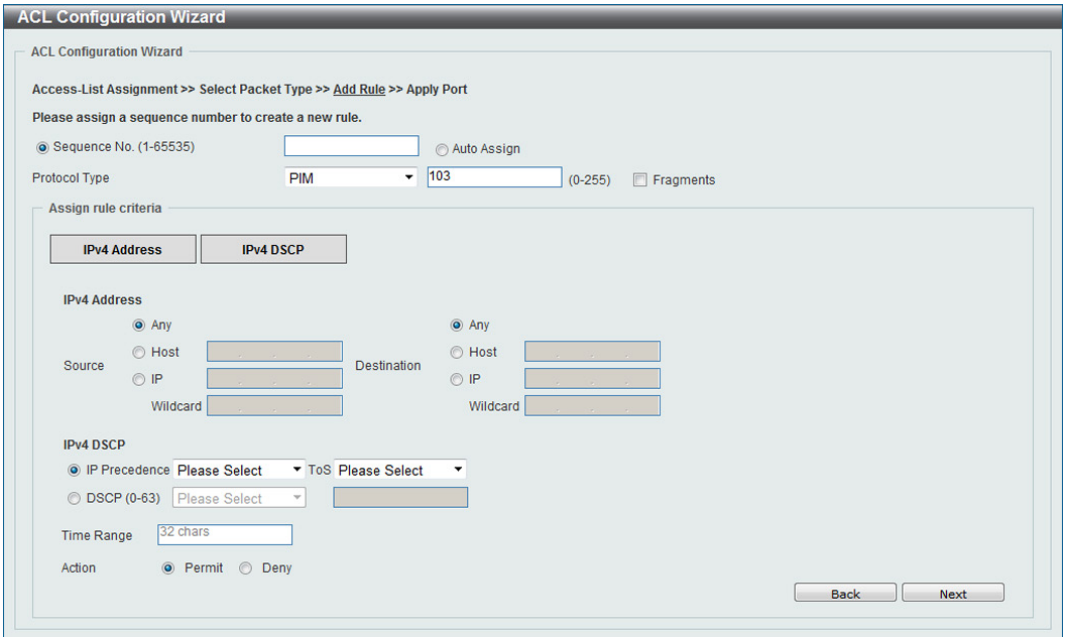


図 11-14　ACL Configuration Wizard (Add Rule for IPv4 ACL) PIM 画面

項目	説明
Fragments	パケットフラグメントフィルタリングを使用する場合、選択します。
Source	送信元のアドレスを指定します。「Any」「Host」「IP」から指定します。 「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IP アドレスを入力します。 「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い送信元 IP アドレス群を入力します。ビット値 1 に対応するビットは無視され、ビット値 0 に対応するビットが認識されます。
Destination	宛先のアドレスを指定します。「Any」「Host」「IP」から指定します。 「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IP アドレスを入力します。 「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い宛先 IP アドレス群を入力します。ビット値 1 に対応するビットは無視され、ビット値 0 に対応するビットが認識されます。
IP Precedence	IP 優先値を指定します。「0 (routine)」「1 (priority)」「2, (immediate)」「3 (flash)」「4 (flash-override)」「5 (critical)」「6 (internet)」「7 (network)」から指定できます。
ToS	IP 優先値を選択後、使用する「Type-of-Service」(ToS) の値を指定します。「0 (normal)」「1 (min-monetary-cost)」「2 (max-reliability)」「3, 4(max-throughput)」「5, 6, 7, 8 (min-delay)」「9」「10」「11」「12」「13」「14」「15」から指定できます。
DSCP	使用する DSCP 値を入力します。0 から 63 で入力できます。
Time Range	ACL ルールに関するタイムレンジ名を指定します。
Action	ルール動作に関する設定を行います。「Permit」または「Deny」から指定できます。

「Next」をクリックします。

「Back」をクリックすると前画面に戻ります。

「VRRP」選択時に表示される項目（IPv4 ACL Rule / Protocol Type）

「Protocol Type」で VRRP 選択時に表示される項目です。

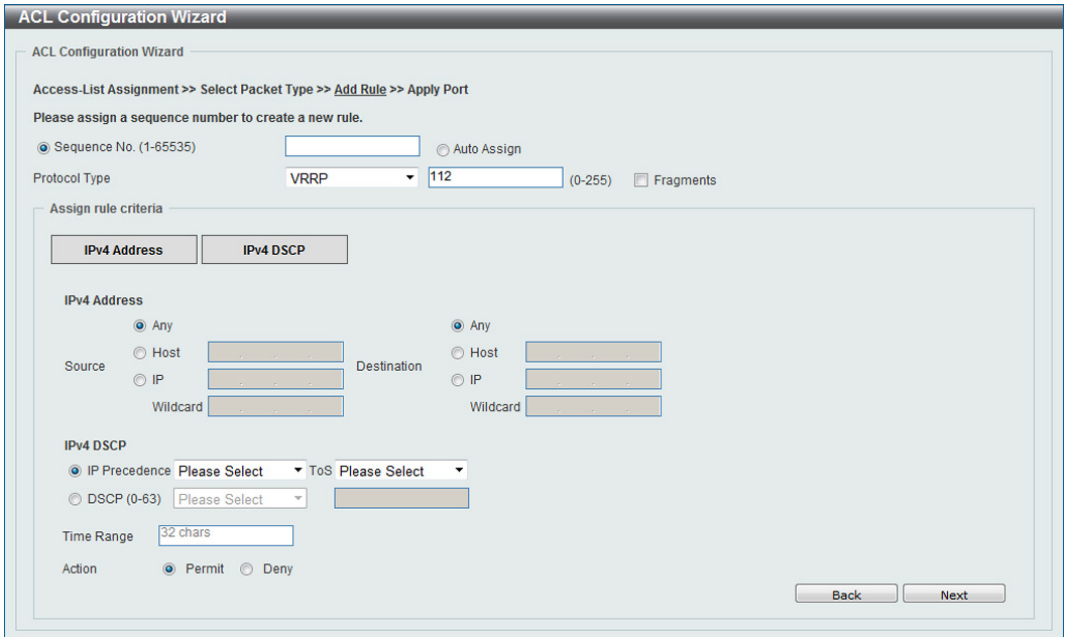


図 11-15　ACL Configuration Wizard (Add Rule for IPv4 ACL) VRRP 画面

項目	説明
Fragments	パケットフラグメントフィルタリングを使用する場合、選択します。
Source	送信元のアドレスを指定します。「Any」「Host」「IP」から指定します。 「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IP アドレスを入力します。 「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い送信元 IP アドレス群を入力します。ビット値 1 に対応するビットは無視され、ビット値 0 に対応するビットが認識されます。
Destination	宛先のアドレスを指定します。「Any」「Host」「IP」から指定します。 「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IP アドレスを入力します。 「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い宛先 IP アドレス群を入力します。ビット値 1 に対応するビットは無視され、ビット値 0 に対応するビットが認識されます。
IP Precedence	IP 優先値を指定します。「0 (routine)」「1 (priority)」「2, (immediate)」「3 (flash)」「4 (flash-override)」「5 (critical)」「6 (internet)」「7 (network)」から指定できます。
ToS	IP 優先値を選択後、使用する「Type-of-Service」(ToS) の値を指定します。「0 (normal)」「1 (min-monetary-cost)」「2 (max-reliability)」「3, 4(max-throughput)」「5, 6, 7, 8 (min-delay)」「9」「10」「11」「12」「13」「14」「15」から指定できます。
DSCP	使用する DSCP 値を入力します。0 から 63 で入力できます。
Time Range	ACL ルールに関するタイムレンジ名を指定します。
Action	ルール動作に関する設定を行います。「Permit」または「Deny」から指定できます。

「Next」をクリックします。

「Back」をクリックすると前画面に戻ります。

「IP-in-IP」選択時に表示される項目（IPv4 ACL Rule / Protocol Type）

「Protocol Type」で IP-in-IP 選択時に表示される項目です。

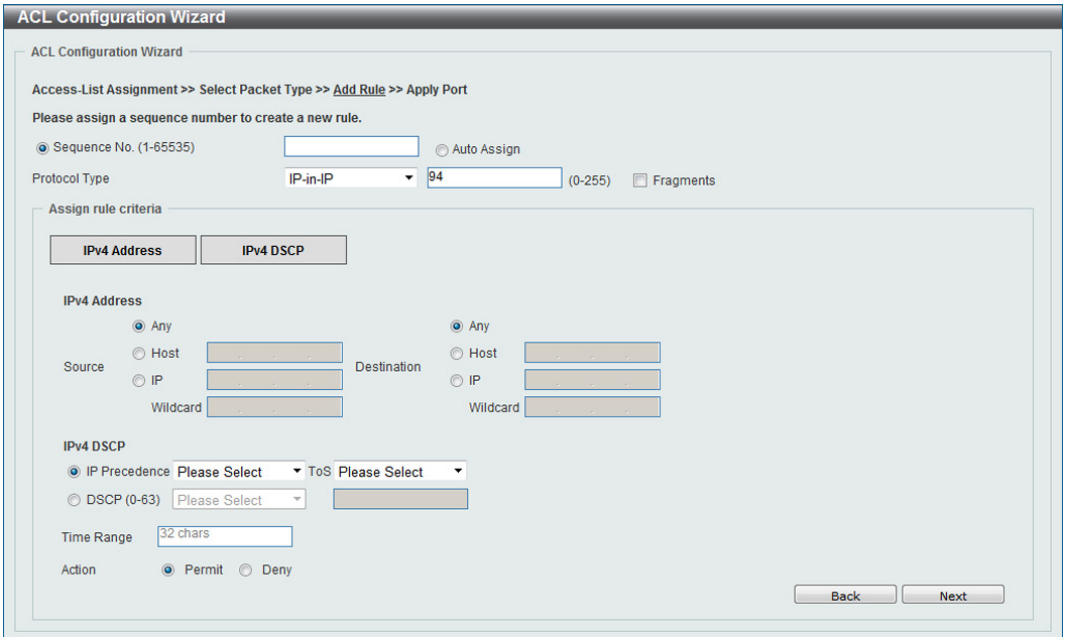


図 11-16　ACL Configuration Wizard (Add Rule for IPv4 ACL) IP-in-IP 画面

項目	説明
Fragments	パケットフラグメントフィルタリングを使用する場合、選択します。
Source	送信元のアドレスを指定します。「Any」「Host」「IP」から指定します。 「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IP アドレスを入力します。 「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い送信元 IP アドレス群を入力します。ビット値 1 に対応するビットは無視され、ビット値 0 に対応するビットが認識されます。
Destination	宛先のアドレスを指定します。「Any」「Host」「IP」から指定します。 「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IP アドレスを入力します。 「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い宛先 IP アドレス群を入力します。ビット値 1 に対応するビットは無視され、ビット値 0 に対応するビットが認識されます。
IP Precedence	IP 優先値を指定します。「0 (routine)」「1 (priority)」「2, (immediate)」「3 (flash)」「4 (flash-override)」「5 (critical)」「6 (internet)」「7 (network)」から指定できます。
ToS	IP 優先値を選択後、使用する「Type-of-Service」(ToS) の値を指定します。「0 (normal)」「1 (min-monetary-cost)」「2 (max-reliability)」「3, 4(max-throughput)」「5, 6, 7, 8 (min-delay)」「9」「10」「11」「12」「13」「14」「15」から指定できます。
DSCP	使用する DSCP 値を入力します。0 から 63 で入力できます。
Time Range	ACL ルールに関するタイムレンジ名を指定します。
Action	ルール動作に関する設定を行います。「Permit」または「Deny」から指定できます。

「Next」をクリックします。

「Back」をクリックすると前画面に戻ります。

「PCP」選択時に表示される項目（IPv4 ACL Rule / Protocol Type）

「Protocol Type」で PCP 選択時に表示される項目です。

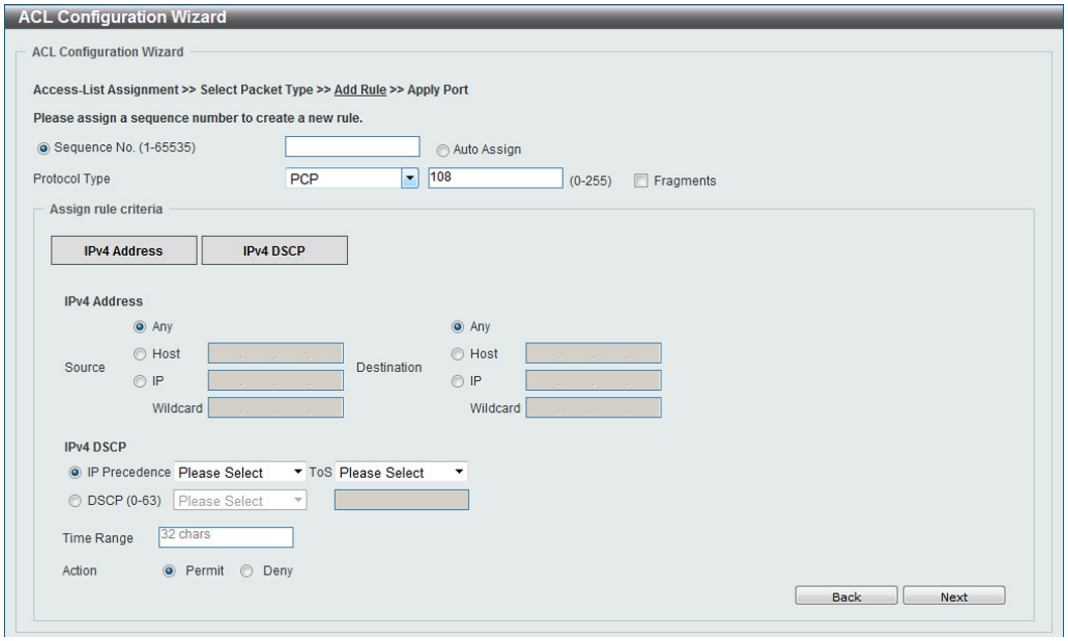


図 11-17　ACL Configuration Wizard (Add Rule for IPv4 ACL) PCP 画面

項目	説明
Fragments	パケットフラグメントフィルタリングを使用する場合、選択します。
Source	送信元のアドレスを指定します。「Any」「Host」「IP」から指定します。 「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IP アドレスを入力します。 「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い送信元 IP アドレス群を入力します。ビット値 1 に対応するビットは無視され、ビット値 0 に対応するビットが認識されます。
Destination	宛先のアドレスを指定します。「Any」「Host」「IP」から指定します。 「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IP アドレスを入力します。 「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い宛先 IP アドレス群を入力します。ビット値 1 に対応するビットは無視され、ビット値 0 に対応するビットが認識されます。
IP Precedence	IP 優先値を指定します。「0 (routine)」「1 (priority)」「2, (immediate)」「3 (flash)」「4 (flash-override)」「5 (critical)」「6 (internet)」「7 (network)」から指定できます。
ToS	IP 優先値を選択後、使用する「Type-of-Service」(ToS) の値を指定します。「0 (normal)」「1 (min-monetary-cost)」「2 (max-reliability)」「3, 4(max-throughput)」「5, 6, 7, 8 (min-delay)」「9」「10」「11」「12」「13」「14」「15」から指定できます。
DSCP	使用する DSCP 値を入力します。0 から 63 で入力できます。
Time Range	ACL ルールに関するタイムレンジ名を指定します。
Action	ルール動作に関する設定を行います。「Permit」または「Deny」から指定できます。

「Next」をクリックします。
「Back」をクリックすると前画面に戻ります。

「Protocol ID」選択時に表示される項目（IPv4 ACL Rule / Protocol Type）

「Protocol Type」で Protocol ID 選択時に表示される項目です。

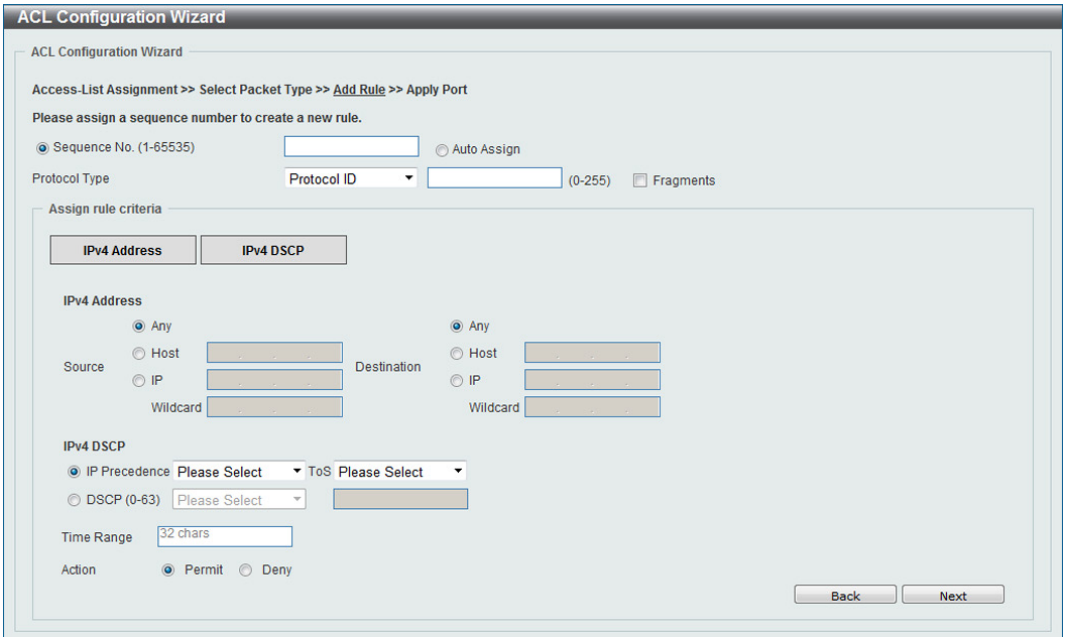


図 11-18　ACL Configuration Wizard (Add Rule for IPv4 ACL) Protocol ID 画面

項目	説明
Protocol	プロトコル ID（0-255）を指定します。
Fragments	パケットフラグメントフィルタリングを使用する場合、選択します。
Source	送信元のアドレスを指定します。「Any」「Host」「IP」から指定します。 「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IP アドレスを入力します。 「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い送信元 IP アドレス群を入力します。ビット値 1 に対応するビットは無視され、ビット値 0 に対応するビットが認識されます。
Destination	宛先のアドレスを指定します。「Any」「Host」「IP」から指定します。 「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IP アドレスを入力します。 「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い宛先 IP アドレス群を入力します。ビット値 1 に対応するビットは無視され、ビット値 0 に対応するビットが認識されます。
IP Precedence	IP 優先値を指定します。「0 (routine)」「1 (priority)」「2, (immediate)」「3 (flash)」「4 (flash-override)」「5 (critical)」「6 (internet)」「7 (network)」から指定できます。
ToS	IP 優先値を選択後、使用する「Type-of-Service」(ToS) の値を指定します。「0 (normal)」「1 (min-monetary-cost)」「2 (max-reliability)」「3, 4(max-throughput)」「5, 6, 7, 8 (min-delay)」「9」「10」「11」「12」「13」「14」「15」から指定できます。
DSCP	使用する DSCP 値を入力します。0 から 63 で入力できます。
Time Range	ACL ルールに関するタイムレンジ名を指定します。
Action	ルール動作に関する設定を行います。「Permit」または「Deny」から指定できます。

「Next」をクリックします。
「Back」をクリックすると前画面に戻ります。

「None」選択時に表示される項目（IPv4 ACL Rule / Protocol Type）

「Protocol Type」で None 選択時に表示される項目です。

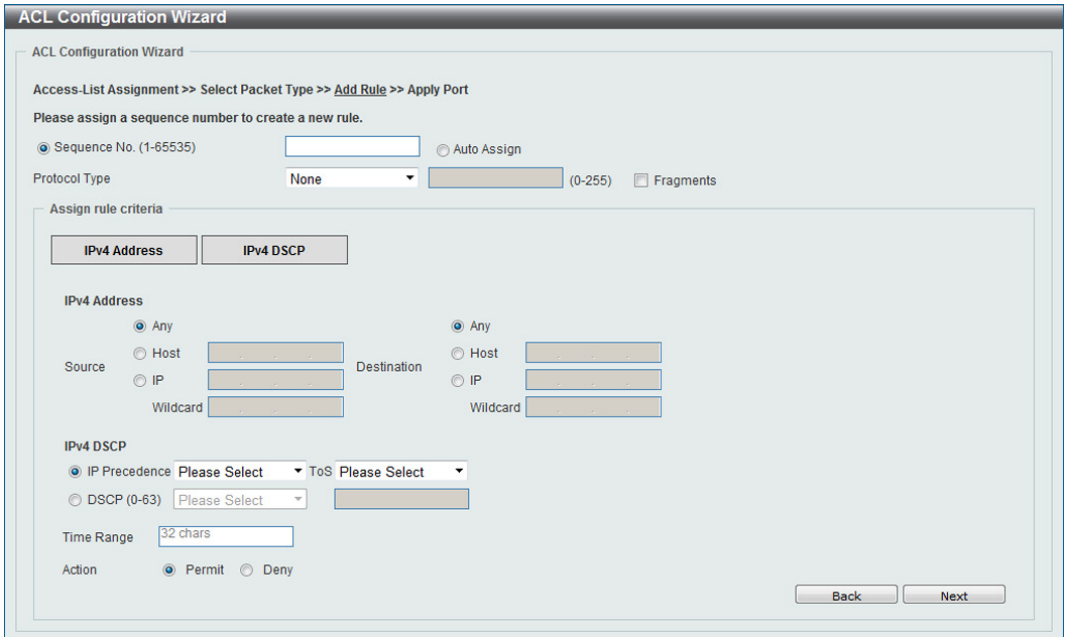


図 11-19　ACL Configuration Wizard (Add Rule for IPv4 ACL) None 画面

項目	説明
Fragments	パケットフラグメントフィルタリングを使用する場合、選択します。
Source	送信元のアドレスを指定します。「Any」「Host」「IP」から指定します。 「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IP アドレスを入力します。 「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い送信元 IP アドレス群を入力します。ビット値 1 に対応するビットは無視され、ビット値 0 に対応するビットが認識されます。
Destination	宛先のアドレスを指定します。「Any」「Host」「IP」から指定します。 「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IP アドレスを入力します。 「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い宛先 IP アドレス群を入力します。ビット値 1 に対応するビットは無視され、ビット値 0 に対応するビットが認識されます。
IP Precedence	IP 優先値を指定します。「0 (routine)」「1 (priority)」「2, (immediate)」「3 (flash)」「4 (flash-override)」「5 (critical)」「6 (internet)」「7 (network)」から指定できます。
ToS	IP 優先値を選択後、使用する「Type-of-Service」(ToS) の値を指定します。「0 (normal)」「1 (min-monetary-cost)」「2 (max-reliability)」「3, 4(max-throughput)」「5, 6, 7, 8 (min-delay)」「9」「10」「11」「12」「13」「14」「15」から指定できます。
DSCP	使用する DSCP 値を入力します。0 から 63 で入力できます。
Time Range	ACL ルールに関するタイムレンジ名を指定します。
Action	ルール動作に関する設定を行います。「Permit」または「Deny」から指定できます。

「Next」をクリックします。
「Back」をクリックすると前画面に戻ります。

IPv6 ACL Rule の設定

IPv6 ACL Rule を設定します。「IPv6」を選択し「Next」をクリックし、表示された以下の画面の設定を行います。

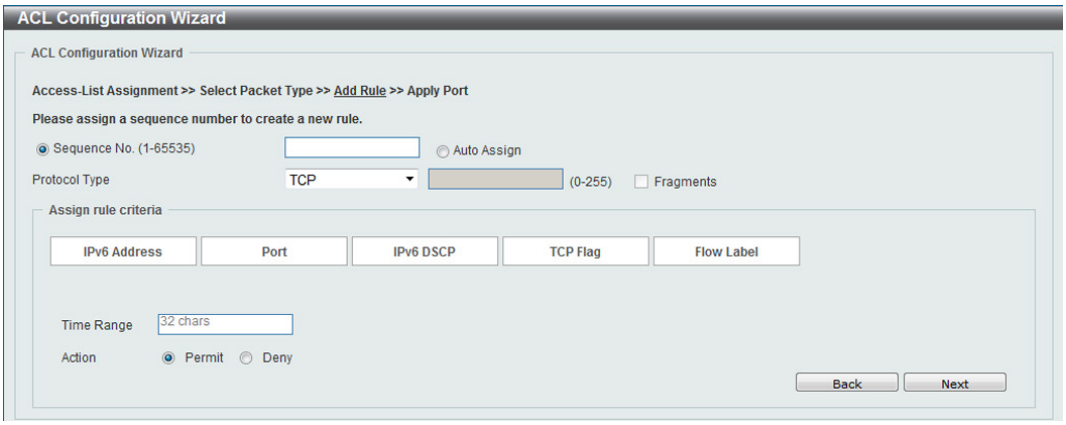


図 11-20　ACL Configuration Wizard -IPv6 画面

画面に表示される項目

項目	説明
Sequence No. (1-65535):	シーケンス番号を指定します。「1」から「65535」の間で指定できます。
Auto Assign:	新規ルール用のシーケンス番号を自動でアサインします。
Protocol Type	プロトコルの種類を選択します。「TCP」「UDP」「ICMP」「Protocol ID」「ESP」「PCP」「SCTP」「None」から選択します。選択したプロトコルの種類によってはプロトコルに関連する数値（ID 等）を右の欄に入力する必要があります。その際、欄の右にある制限値（0-255 等）に注意して入力してください。

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

「TCP」選択時に表示される項目（IPv6 ACL Rule / Protocol Type）

「Protocol Type」で TCP 選択時に表示される項目です。

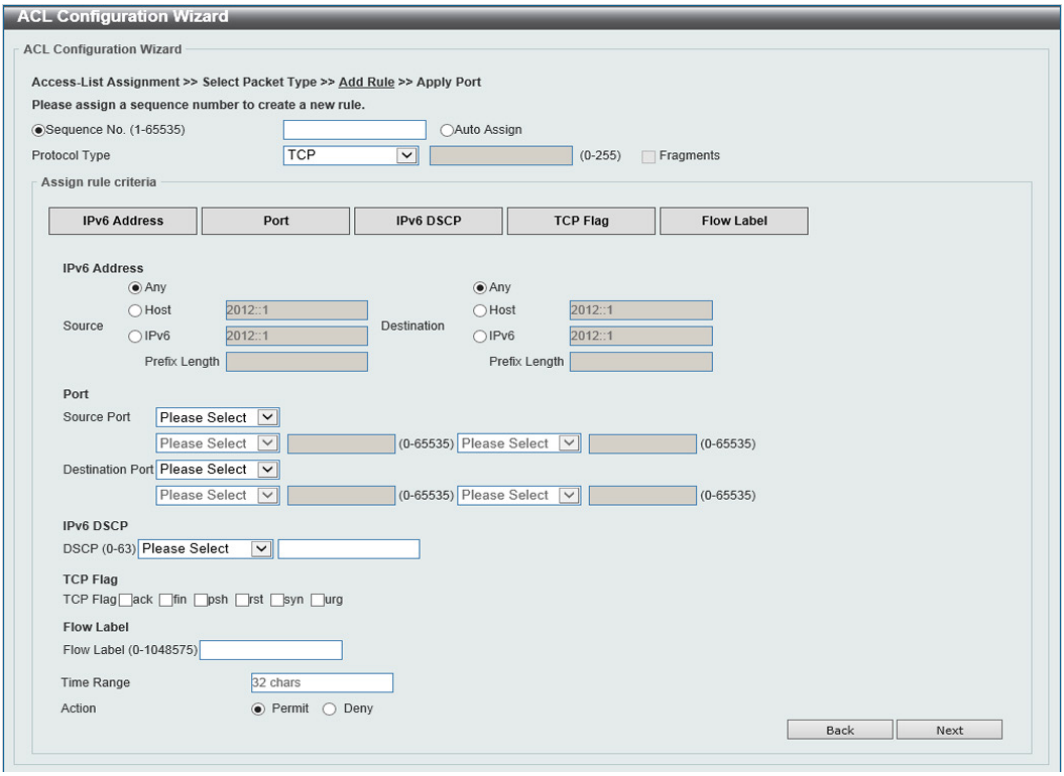


図 11-21　ACL Configuration Wizard (Add Rule for IPv6 ACL) TCP 画面

項目	説明
Source	送信元のアドレスを指定します。「Any」「Host」「IPv6」から指定します。 「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IPv6 アドレスを入力します。 「IPv6」を選択すると「Prefix Length」が指定可能になり、送信元 IPv6 アドレスと Prefix Length を入力します。
Destination	宛先のアドレスを指定します。「Any」「Host」「IPv6」から指定します。 「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IPv6 アドレスを入力します。 「IPv6」を選択すると「Prefix Length」が指定可能になり、宛先 IPv6 アドレスと Prefix Length を入力します。
Source Port	送信元ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選択した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択すると選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポートが使用されます。「Range」を選択すると指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。
Destination Port	宛先ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選択した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択すると選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポートが使用されます。「Range」を選択すると指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。
DSCP	使用する DSCP 値を入力します。0 から 63 で入力できます。
TCP Flag	TCP フラグを本ルールに含める場合、該当のフラグにチェックを入れます。「ack」「fin」「psh」「rst」「syn」「urg」から指定できます。
Flow Label	フローラベルの値を入力します。0 から 1048575 まで指定可能です。
Time Range	ACL ルールに関するタイムレンジ名を指定します。
Action	ルール動作に関する設定を行います。「Permit」または「Deny」から指定できます。

「Next」をクリックします。ポート設定（ACL 設定ウィザード）に進みます。
「Back」をクリックすると前画面に戻ります。

「UDP」選択時に表示される項目（IPv6 ACL Rule / Protocol Type）

「Protocol Type」で UDP 選択時に表示される項目です。

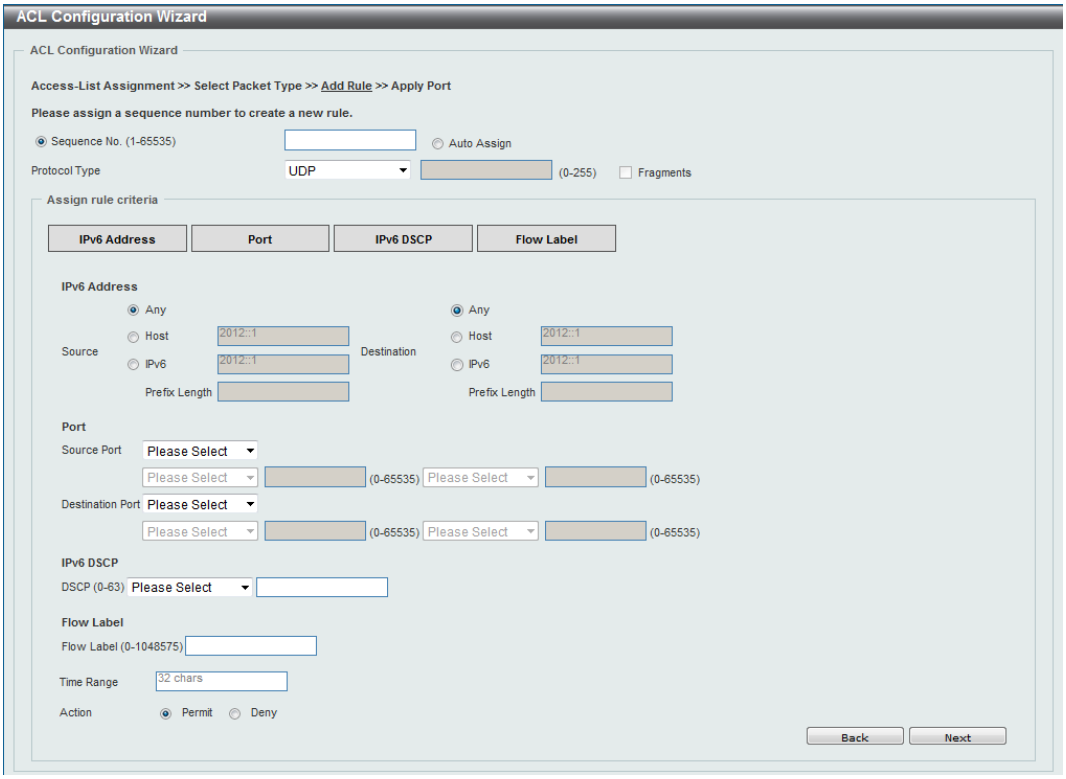


図 11-22　ACL Configuration Wizard (Add Rule for IPv6 ACL) UDP 画面

項目	説明
Source	送信元のアドレスを指定します。「Any」「Host」「IPv6」から指定します。 「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IPv6 アドレスを入力します。 「IPv6」を選択すると「Prefix Length」が指定可能になり、送信元 IPv6 アドレスと Prefix Length を入力します。
Destination	宛先のアドレスを指定します。「Any」「Host」「IPv6」から指定します。 「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IPv6 アドレスを入力します。 「IPv6」を選択すると「Prefix Length」が指定可能になり、宛先 IPv6 アドレスと Prefix Length を入力します。
Source Port	送信元ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選択した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択すると選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポートが使用されます。「Range」を選択すると指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。
Destination Port	宛先ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選択した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択すると選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポートが使用されます。「Range」を選択すると指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。
DSCP	使用する DSCP 値を入力します。0 から 63 で入力できます。
Flow Label	フローラベルの値を入力します。0 から 1048575 まで指定可能です。
Time Range	ACL ルールに関するタイムレンジ名を指定します。
Action	ルール動作に関する設定を行います。「Permit」または「Deny」から指定できます。

「Next」をクリックします。ポート設定（ACL 設定ウィザード）に進みます。
「Back」をクリックすると前画面に戻ります。

「ICMP」選択時に表示される項目（IPv6 ACL Rule / Protocol Type）

「Protocol Type」で ICMP 選択時に表示される項目です。

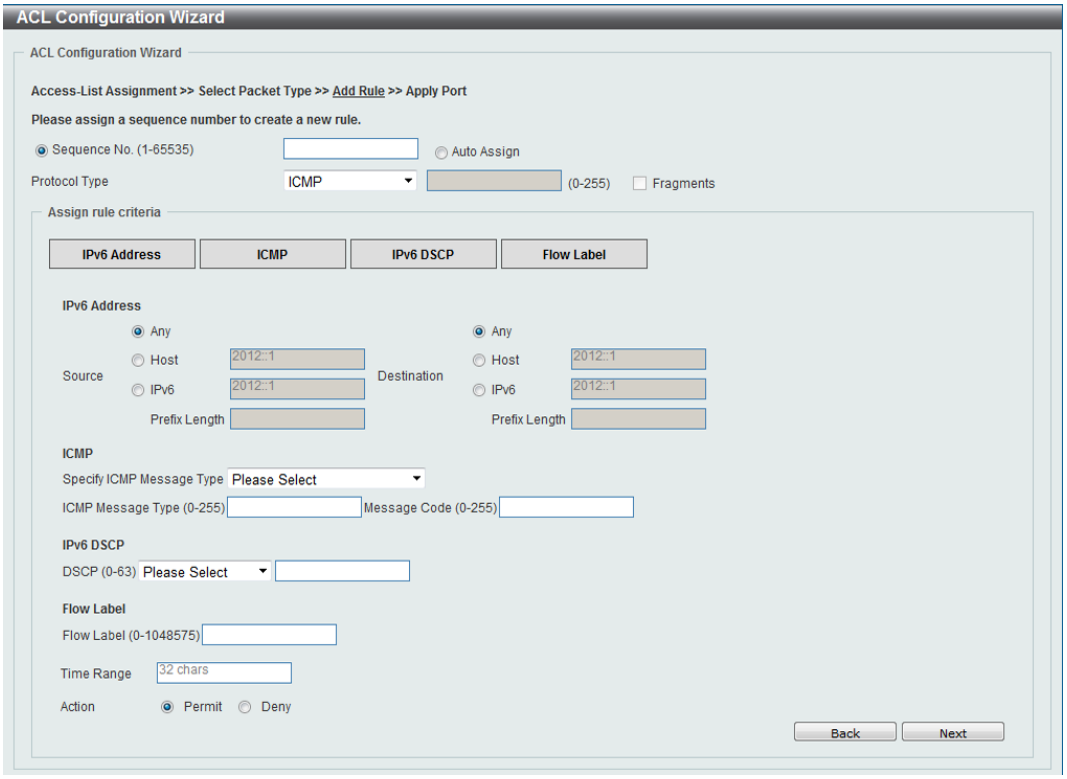


図 11-23　ACL Configuration Wizard (Add Rule for IPv6 ACL) ICMP 画面

項目	説明
Source	送信元のアドレスを指定します。「Any」「Host」「IPv6」から指定します。 「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IPv6 アドレスを入力します。 「IPv6」を選択すると「Prefix Length」が指定可能になり、送信元 IPv6 アドレスと Prefix Length を入力します。
Destination	宛先のアドレスを指定します。「Any」「Host」「IPv6」から指定します。 「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IPv6 アドレスを入力します。 「IPv6」を選択すると「Prefix Length」が指定可能になり、宛先 IPv6 アドレスと Prefix Length を入力します。
Specify ICMP Message Type	使用する ICMP メッセージの種類を指定します。自動的に ICMP メッセージ種類の数値とメッセージコードは指定されます。
ICMP Message Type	ICMP メッセージを指定しない場合、手動で ICMP メッセージ種類の数値を指定します。
Message Code	ICMP メッセージを指定しない場合、手動でメッセージコードを指定します。
DSCP	使用する DSCP 値を入力します。0 から 63 で入力できます。
Flow Label	フローラベルの値を入力します。0 から 1048575 まで指定可能です。
Time Range	ACL ルールに関するタイムレンジ名を指定します。
Action	ルール動作に関する設定を行います。「Permit」または「Deny」から指定できます。

「Next」をクリックします。ポート設定（ACL 設定ウィザード）に進みます。
「Back」をクリックすると前画面に戻ります。

「Protocol ID」選択時に表示される項目（IPv6 ACL Rule / Protocol Type）

「Protocol Type」で Protocol ID 選択時に表示される項目です。

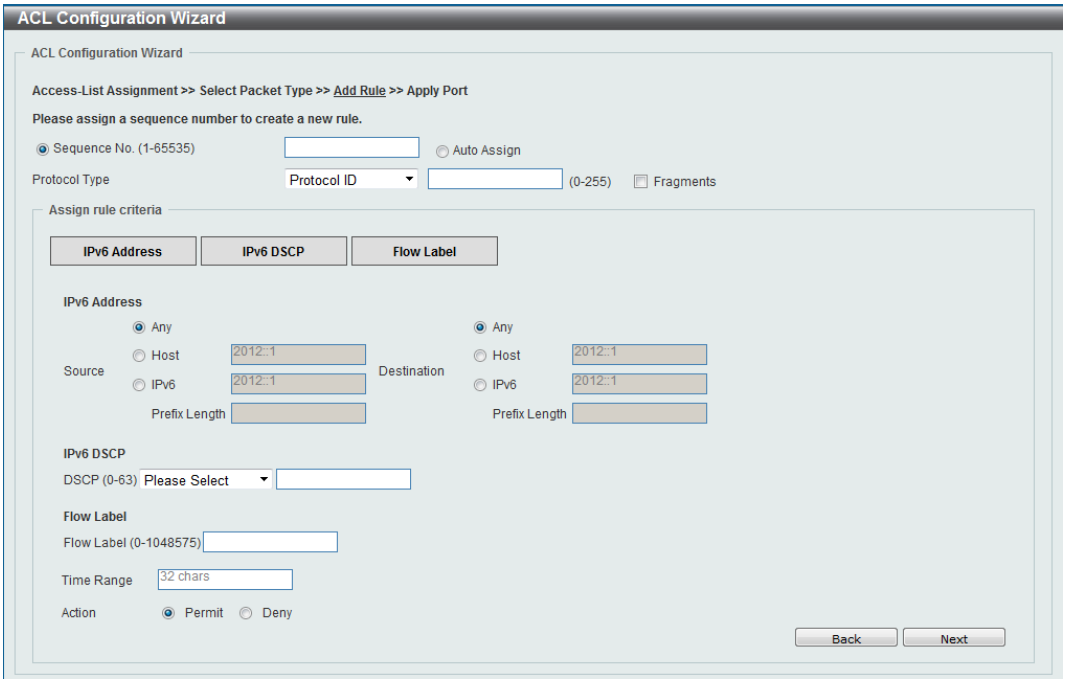


図 11-24　ACL Configuration Wizard (Add Rule for IPv6 ACL) Protocol ID 画面

項目	説明
Protocol	プロトコル ID（0-255）を指定します。
Fragments	パケットフラグメントフィルタリングを使用する場合、選択します。
Source	送信元のアドレスを指定します。「Any」「Host」「IPv6」から指定します。 「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IPv6 アドレスを入力します。 「IPv6」を選択すると「Prefix Length」が指定可能になり、送信元 IPv6 アドレスと Prefix Length を入力します。
Destination	宛先のアドレスを指定します。「Any」「Host」「IPv6」から指定します。 「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IPv6 アドレスを入力します。 「IPv6」を選択すると「Prefix Length」が指定可能になり、宛先 IPv6 アドレスと Prefix Length を入力します。
DSCP	使用する DSCP 値を入力します。0 から 63 で入力できます。
Flow Label	フローラベルの値を入力します。0 から 1048575 まで指定可能です。
Time Range	ACL ルールに関するタイムレンジ名を指定します。
Action	ルール動作に関する設定を行います。「Permit」または「Deny」から指定できます。

「Next」をクリックします。ポート設定（ACL 設定ウィザード）に進みます。
「Back」をクリックすると前画面に戻ります。

「ESP」選択時に表示される項目（IPv6 ACL Rule / Protocol Type）

「Protocol Type」で ESP 選択時に表示される項目です。

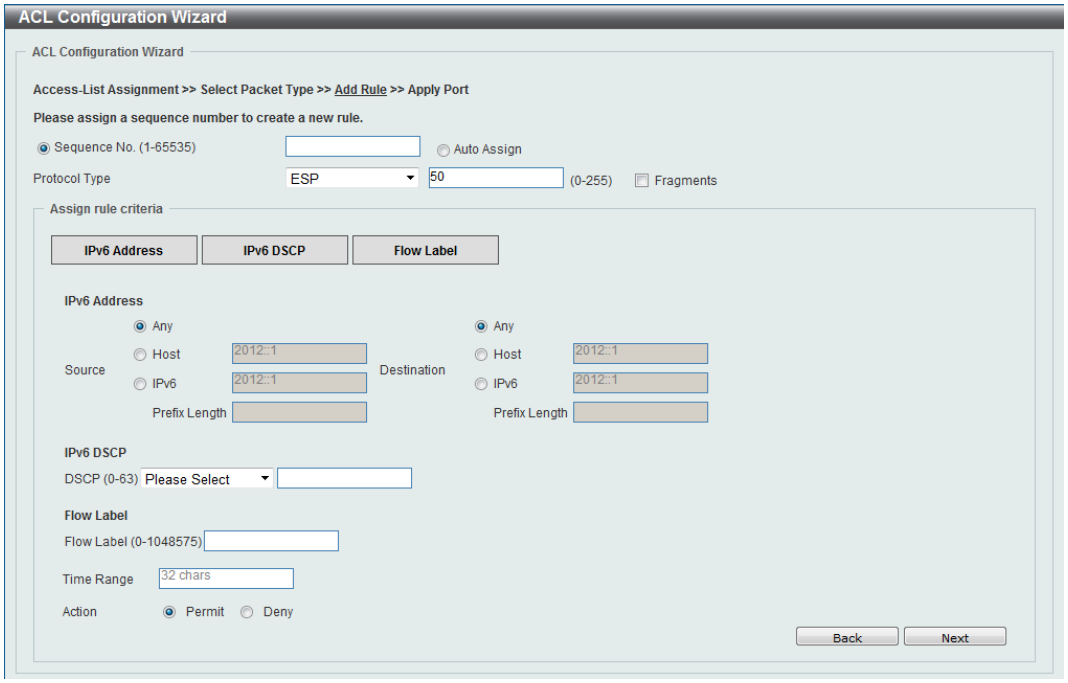


図 11-25　ACL Configuration Wizard (Add Rule for IPv6 ACL) ESP 画面

項目	説明
Fragments	パケットフラグメントフィルタリングを使用する場合、選択します。
Source	送信元のアドレスを指定します。「Any」「Host」「IPv6」から指定します。 「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IPv6 アドレスを入力します。 「IPv6」を選択すると「Prefix Length」が指定可能になり、送信元 IPv6 アドレスと Prefix Length を入力します。
Destination	宛先のアドレスを指定します。「Any」「Host」「IPv6」から指定します。 「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IPv6 アドレスを入力します。 「IPv6」を選択すると「Prefix Length」が指定可能になり、宛先 IPv6 アドレスと Prefix Length を入力します。
DSCP	使用する DSCP 値を入力します。0 から 63 で入力できます。
Flow Label	フローラベルの値を入力します。0 から 1048575 まで指定可能です。
Time Range	ACL ルールに関するタイムレンジ名を指定します。
Action	ルール動作に関する設定を行います。「Permit」または「Deny」から指定できます。

「Next」をクリックします。ポート設定（ACL 設定ウィザード）に進みます。
「Back」をクリックすると前画面に戻ります。

「PCP」選択時に表示される項目（IPv6 ACL Rule / Protocol Type）

「Protocol Type」で PCP 選択時に表示される項目です。

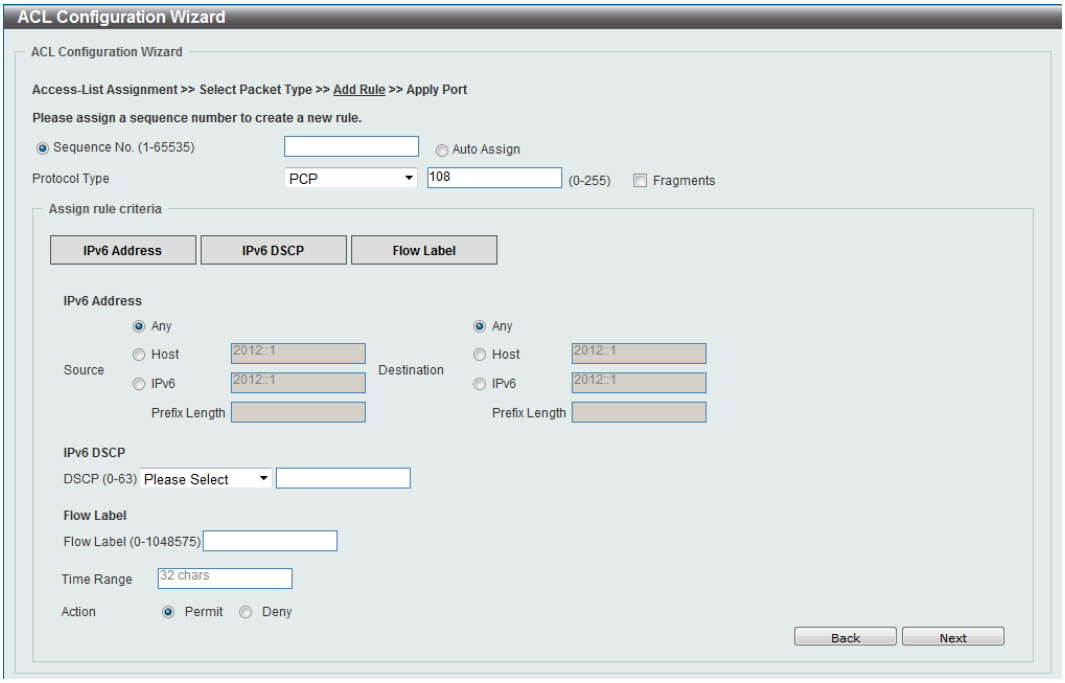


図 11-26　ACL Configuration Wizard (Add Rule for IPv6 ACL) PCP 画面

項目	説明
Fragments	パケットフラグメントフィルタリングを使用する場合、選択します。
Source	送信元のアドレスを指定します。「Any」「Host」「IPv6」から指定します。 「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IPv6 アドレスを入力します。 「IPv6」を選択すると「Prefix Length」が指定可能になり、送信元 IPv6 アドレスと Prefix Length を入力します。
Destination	宛先のアドレスを指定します。「Any」「Host」「IPv6」から指定します。 「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IPv6 アドレスを入力します。 「IPv6」を選択すると「Prefix Length」が指定可能になり、宛先 IPv6 アドレスと Prefix Length を入力します。
DSCP	使用する DSCP 値を入力します。0 から 63 で入力できます。
Flow Label	フローラベルの値を入力します。0 から 1048575 まで指定可能です。
Time Range	ACL ルールに関するタイムレンジ名を指定します。
Action	ルール動作に関する設定を行います。「Permit」または「Deny」から指定できます。

「Next」をクリックします。ポート設定（ACL 設定ウィザード）に進みます。
「Back」をクリックすると前画面に戻ります。

「SCTP」選択時に表示される項目（IPv6 ACL Rule / Protocol Type）

「Protocol Type」で SCTP 選択時に表示される項目です。

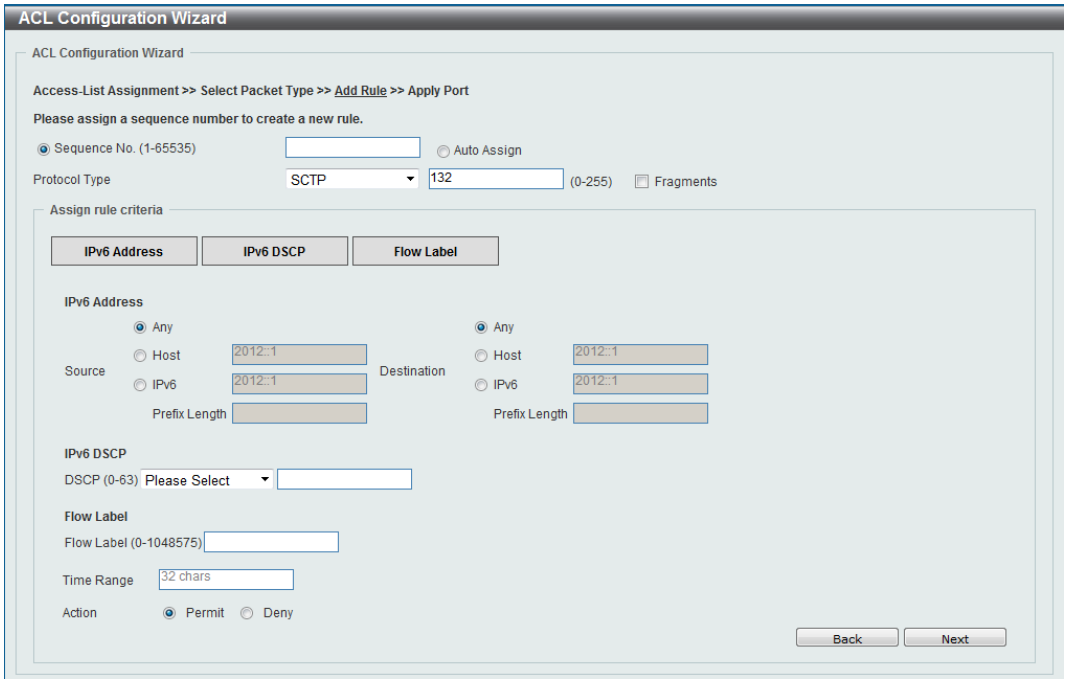


図 11-27　ACL Configuration Wizard (Add Rule for IPv6 ACL) SCTP 画面

項目	説明
Fragments	パケットフラグメントフィルタリングを使用する場合、選択します。
Source	送信元のアドレスを指定します。「Any」「Host」「IPv6」から指定します。 「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IPv6 アドレスを入力します。 「IPv6」を選択すると「Prefix Length」が指定可能になり、送信元 IPv6 アドレスと Prefix Length を入力します。
Destination	宛先のアドレスを指定します。「Any」「Host」「IPv6」から指定します。 「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IPv6 アドレスを入力します。 「IPv6」を選択すると「Prefix Length」が指定可能になり、宛先 IPv6 アドレスと Prefix Length を入力します。
DSCP	使用する DSCP 値を入力します。0 から 63 で入力できます。
Flow Label	フローラベルの値を入力します。0 から 1048575 まで指定可能です。
Time Range	ACL ルールに関するタイムレンジ名を指定します。
Action	ルール動作に関する設定を行います。「Permit」または「Deny」から指定できます。

「Next」をクリックします。ポート設定（ACL 設定ウィザード）に進みます。
「Back」をクリックすると前画面に戻ります。

「None」選択時に表示される項目（IPv6 ACL Rule / Protocol Type）

「Protocol Type」で None 選択時に表示される項目です。

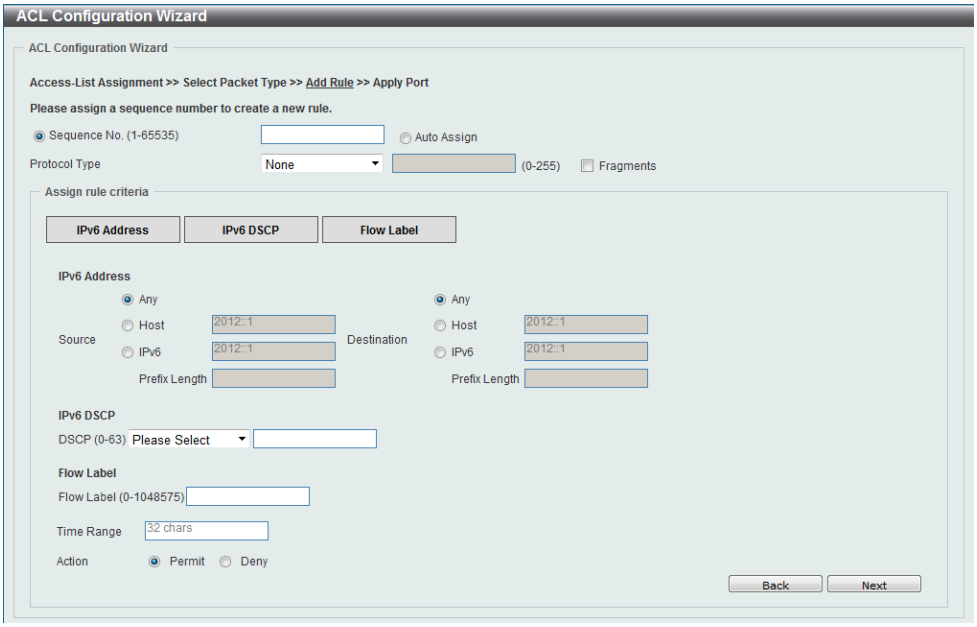


図 11-28　ACL Configuration Wizard (Add Rule for IPv6 ACL) None 画面

項目	説明
Fragments	パケットフラグメントフィルタリングを使用する場合、選択します。
Source	送信元のアドレスを指定します。「Any」「Host」「IPv6」から指定します。 「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IPv6 アドレスを入力します。 「IPv6」を選択すると「Prefix Length」が指定可能になり、送信元 IPv6 アドレスと Prefix Length を入力します。
Destination	宛先のアドレスを指定します。「Any」「Host」「IPv6」から指定します。 「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IPv6 アドレスを入力します。 「IPv6」を選択すると「Prefix Length」が指定可能になり、宛先 IPv6 アドレスと Prefix Length を入力します。
DSCP	使用する DSCP 値を入力します。0 から 63 で入力できます。
Flow Label	フローラベルの値を入力します。0 から 1048575 まで指定可能です。
Time Range	ACL ルールに関するタイムレンジ名を指定します。
Action	ルール動作に関する設定を行います。「Permit」または「Deny」から指定できます。

「Next」をクリックします。ポート設定（ACL 設定ウィザード）に進みます。
「Back」をクリックすると前画面に戻ります。

ポート設定（ACL 設定ウィザード）

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

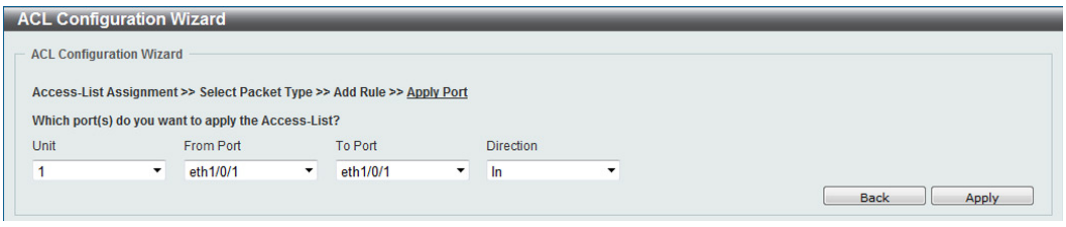


図 11-29　ACL Configuration Wizard (Apply Port) 画面

画面に表示される項目

項目	説明
Unit	設定するユニットを指定します。
From Port/To Port	設定の対象となるポート範囲を指定します。
Direction	方向を指定します。「In」が選択可能です。

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

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。

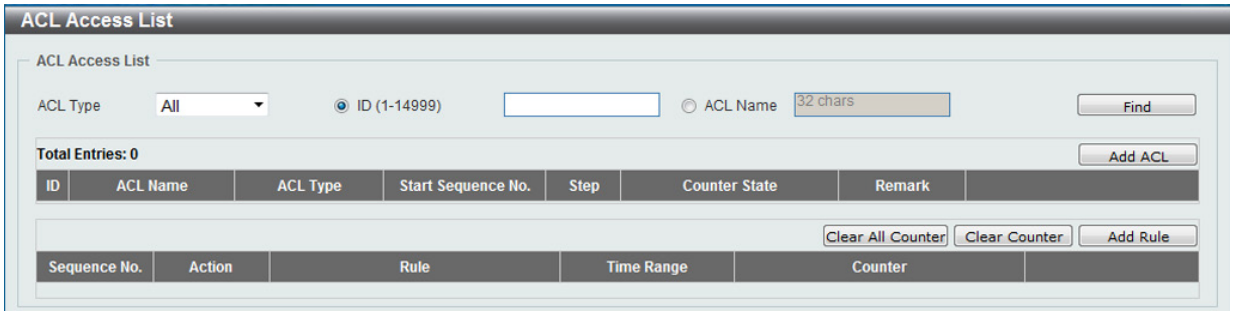


図 11-30　ACL Access List 画面

画面に表示される項目

項目	説明
ACL Type	ACL プロファイルの種類を選択します。「All」「IP ACL」「IPv6 ACL」「MAC ACL」「Expert ACL」から選択します。
ID	ACL ID を入力します。1 から 14999 の範囲で入力できます。
ACL Name	ACL 名を入力します。32 文字まで指定できます。

「Find」ボタンをクリックし、入力した情報を元に特定のエントリを指定します。
「Clear All Counter」ボタンをクリックし、表示されたすべてのカウンタ情報を消去します。
「Clear Counter」ボタンをクリックし、表示された指定ルールのカウンタ情報を消去します。
「Add Rule」ボタンをクリックし、ACL ルールを作成します。
「Add ACL」ボタンをクリックし、新しい ACL プロファイルを作成します。

Standard IP ACL（通常 IP ACL）

Standard IP ACL の作成（Add ACL）

「Add ACL」をクリックし新しい ACL プロファイルを作成します。以下の画面が表示されます。

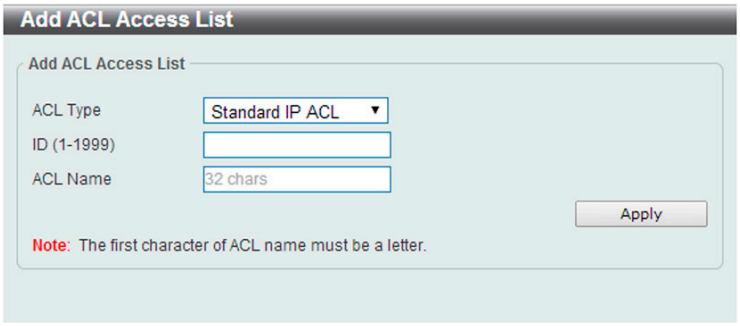


図 11-31　Standard IP ACL (Add ACL Access List) 画面

画面に表示される項目

項目	説明
ACL Type	ACL プロファイルの種類を選択します。「Standard IP ACL」「Extended IP ACL」「Standard IPv6 ACL」「Extended IPv6 ACL」「Extended MAC ACL」「Extended Expert ACL」から選択します。
ID	ACL ID を入力します。1 から 1999 の範囲で入力できます。
ACL Name	ACL 名を入力します。32 文字まで指定できます。

「Apply」ボタンをクリックして、設定を適用します。

ACL プロファイルを作成すると、「ACL Profile Table」に新しく作成した ACL プロファイルが以下の様に表示されます。

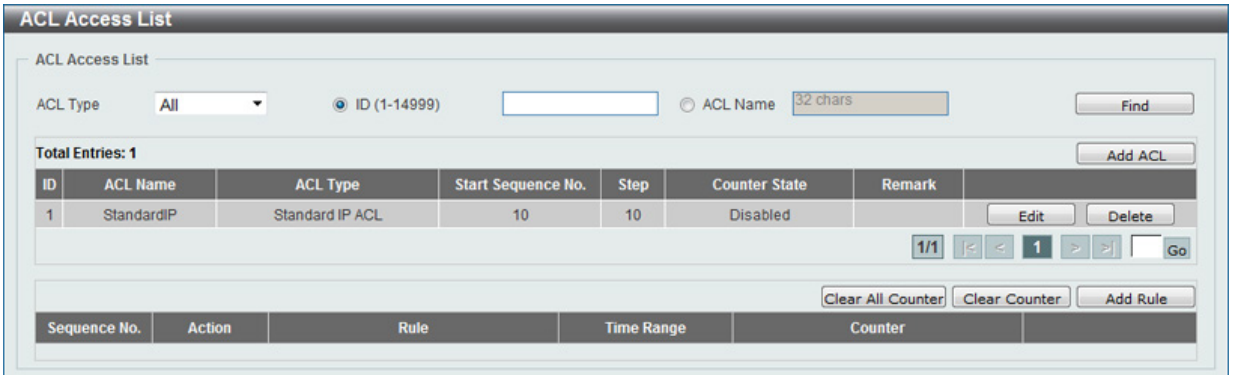


図 11-32　Standard IP ACL (Main) 画面

「Edit」をクリックし、指定 ACL プロファイルの編集を行います。
「Delete」ボタンをクリックし、指定 ACL プロファイルの削除を行います。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

ACL プロファイルにルールを追加する場合、ACL プロファイルを選択後「Add Rule」ボタンをクリックします。

ACL ルールの追加（Add Rule）（Standard IP ACL）

「Add Rule」をクリックし新しい ACL ルールを追加します。
ACL プロファイルを選択後「Add Rule」ボタンをクリックすると、以下の画面が表示され新しい ACL ルールを設定できます。

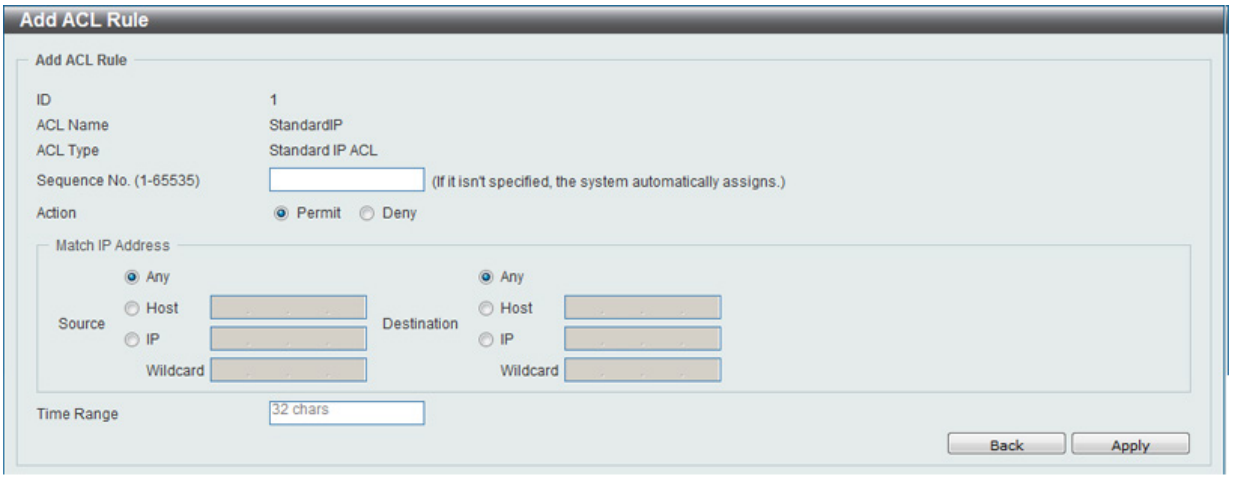


図 11-33　Standard IP ACL (Add Rule) 画面

画面に表示される項目

項目	説明
Sequence No. (1-65535):	シーケンス番号を指定します。「1」から「65535」の間で指定できます。値が指定されないと自動的に番号が割り振られます。
Action	ルール動作に関する設定を行います。「Permit」または「Deny」から指定できます。
Source	送信元のアドレスを指定します。「Any」「Host」「IP」から指定します。 「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IP アドレスを入力します。 「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い送信元 IP アドレス群を入力します。ビットは 1 の値が無視され、0 が認識されます。
Destination	宛先のアドレスを指定します。「Any」「Host」「IP」から指定します。 「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IP アドレスを入力します。 「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い宛先 IP アドレス群を入力します。ビットは 1 の値が無視され、0 が認識されます。
Time Range	ACL ルールに関するタイムレンジ名を指定します。

「Back」ボタンをクリックして、変更を破棄し前の画面に戻ります。
「Apply」ボタンをクリックして、設定を適用します。

ACL ルールの編集（Edit）（Standard IP ACL）

「Counter State」オプションの有効化やプロファイルへの「Remark」の入力など ACL ルールの編集を行う場合、「ACL Profile Table」で該当するプロファイル横の「Edit」ボタンをクリックします。以下の画面が表示されます。

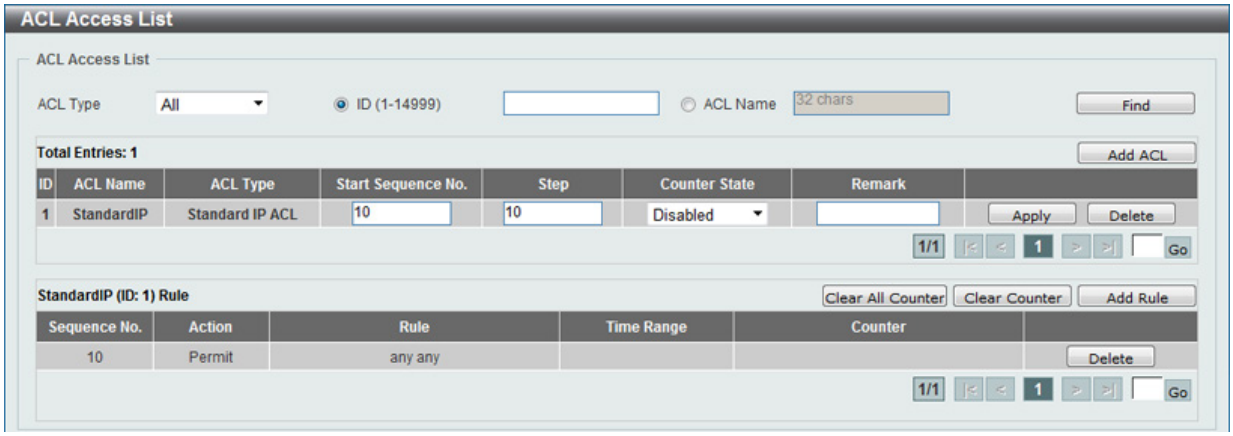


図 11-34　Standard IP ACL (Edit ACL) 画面

画面に表示される項目

項目	説明
Start Sequence No.	シーケンス番号の開始番号を指定します。
Step	シーケンス番号の増加番号を指定します。
Counter State	カウンタ機能の有効 / 無効を指定します。
Remark	指定プロファイルと関連するリマークを入力します。

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

特定の ACL プロファイルに関連する ACL ルール表示するには「ACL Profile Table」で該当の ACL プロファイルを選択します。ACL ルールが表示されます。

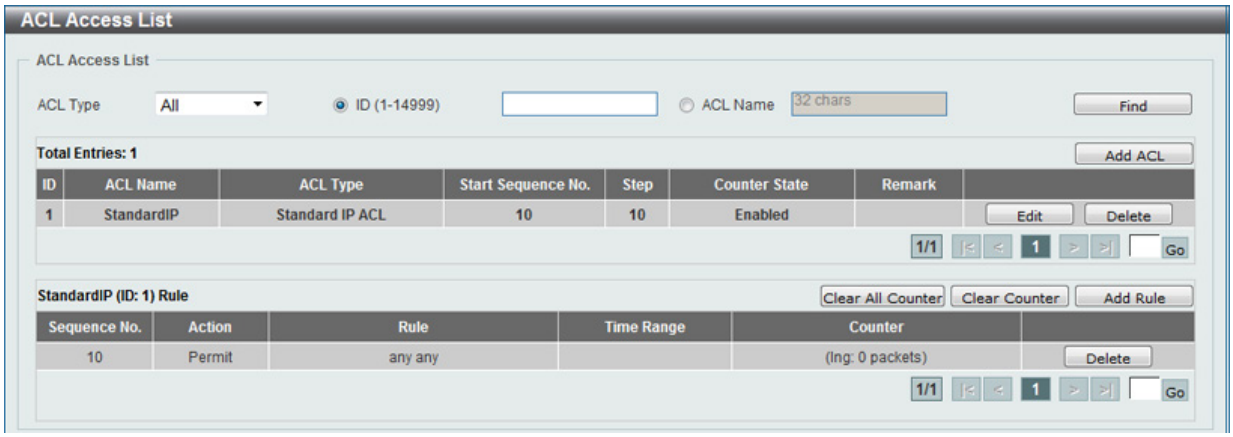


図 11-35　Standard IP ACL (Rule Display) 画面

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

Extended IP ACL（拡張 IP ACL）

Extended IP ACL の作成（Add ACL）

「Add ACL」をクリックし新しい ACL プロファイルを作成します。以下の画面が表示されます。

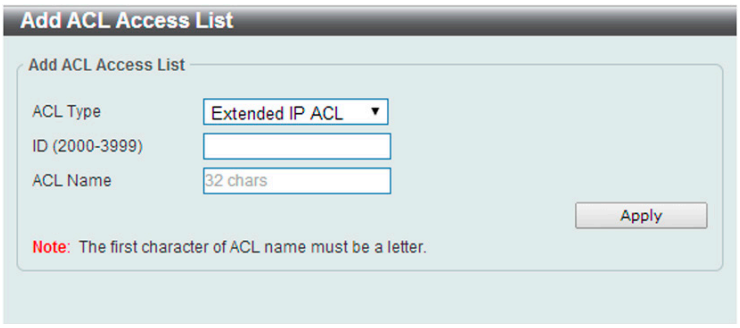


図 11-36　Extended IP ACL (Add ACL Access List) 画面

画面に表示される項目

項目	説明
ACL Type	ACL プロファイルの種類を選択します。「Standard IP ACL」「Extended IP ACL」「Standard IPv6 ACL」「Extended IPv6 ACL」「Extended MAC ACL」「Extended Expert ACL」から選択します。
ID	ACL ID を入力します。2000 から 3999 の範囲で入力できます。
ACL Name	ACL 名を入力します。32 文字まで指定できます。

「Apply」ボタンをクリックして、設定を適用します。

ACL プロファイルを作成すると、「ACL Profile Table」に新しく作成した ACL プロファイルが以下の様に表示されます。

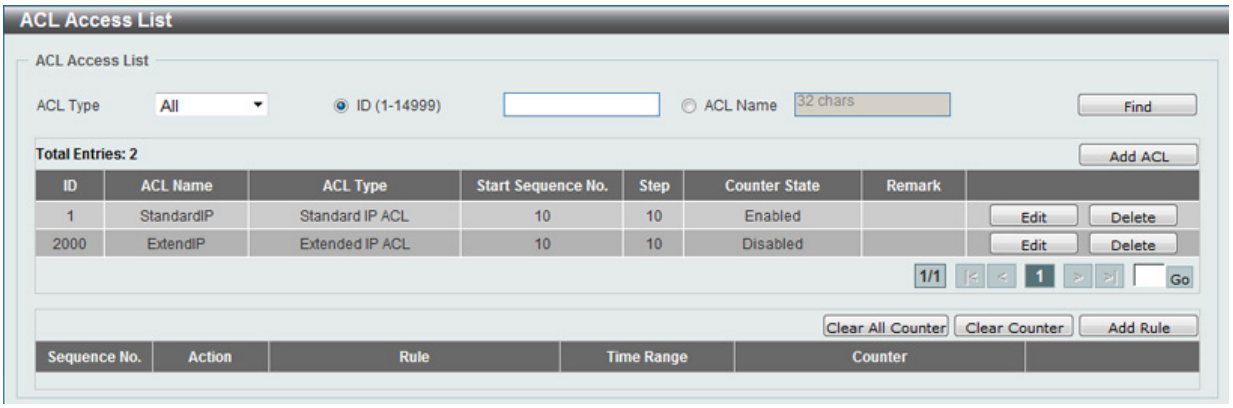


図 11-37　Extended IP ACL (Main) 画面

「Edit」をクリックし、指定 ACL プロファイルの編集を行います。
「Delete」ボタンをクリックし、指定 ACL プロファイルの削除を行います。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

ACL プロファイルにルールを追加する場合、ACL プロファイルを選択後「Add Rule」ボタンをクリックします。

ACL ルールの追加（Add Rule）（Extended IP ACL）

「Add Rule」をクリックし新しい ACL ルールを追加します。
ACL プロファイルを選択後「Add Rule」ボタンをクリックすると、以下の画面が表示され新しい ACL ルールを設定できます。

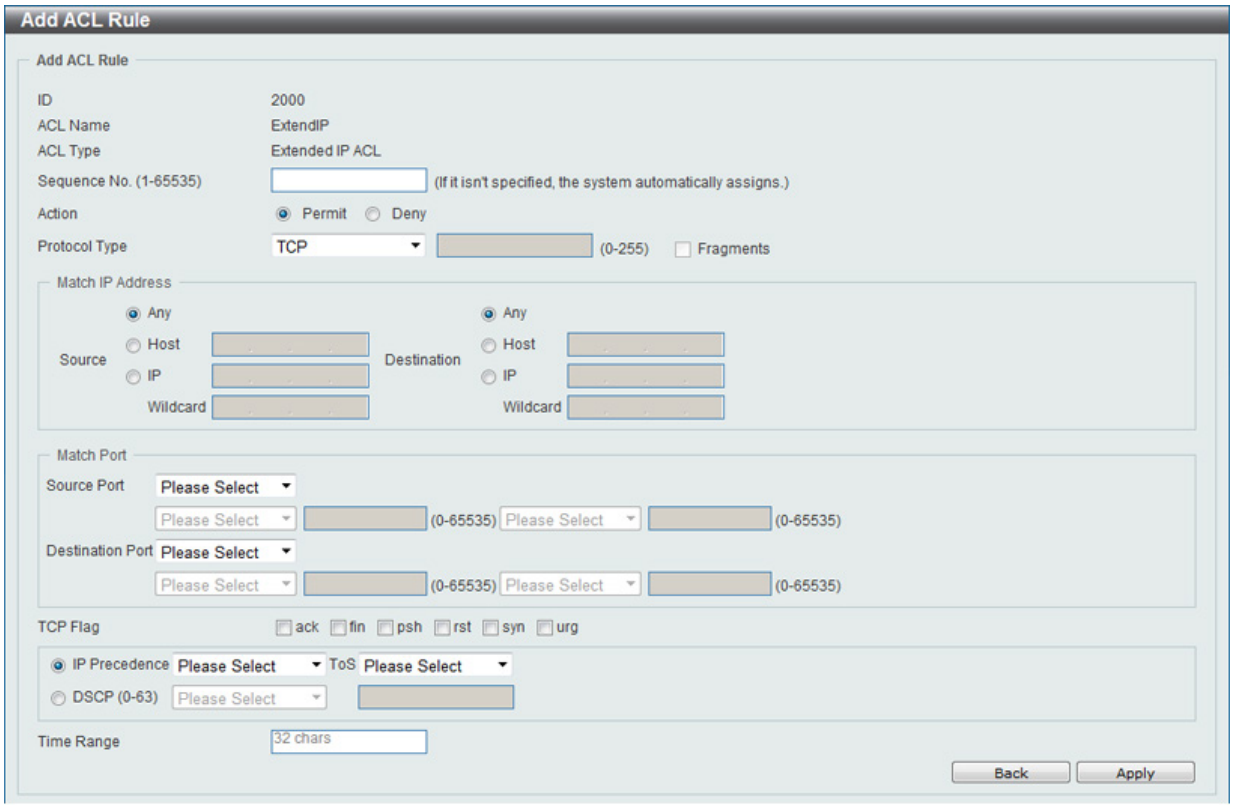


図 11-38　Extended IP ACL (Add Rule) 画面

画面に表示される項目

項目	説明
Sequence No. (1-65535):	シーケンス番号を指定します。「1」から「65535」の間で指定できます。値が指定されないと自動的に番号が割り振られます。
Action	ルール動作に関する設定を行います。「Permit」または「Deny」から指定できます。
Protocol Type	プロトコルの種類を選択します。「TCP」「UDP」「ICMP」「EIGRP」「ESP」「GRE」「IGMP」「OSPF」「PIM」「VRRP」「IP-in-IP」「PCP」「Protocol ID」「None」から選択します。 選択したプロトコルの種類によってはプロトコルに関連する数値（ID 等）を右の欄に入力する必要があります。その際、欄の右にある制限値（0-255 等）に注意して入力してください。

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

「TCP」選択時に表示される項目（Extended IP ACL / Protocol Type）

「Protocol Type」で TCP 選択時に表示される項目です。

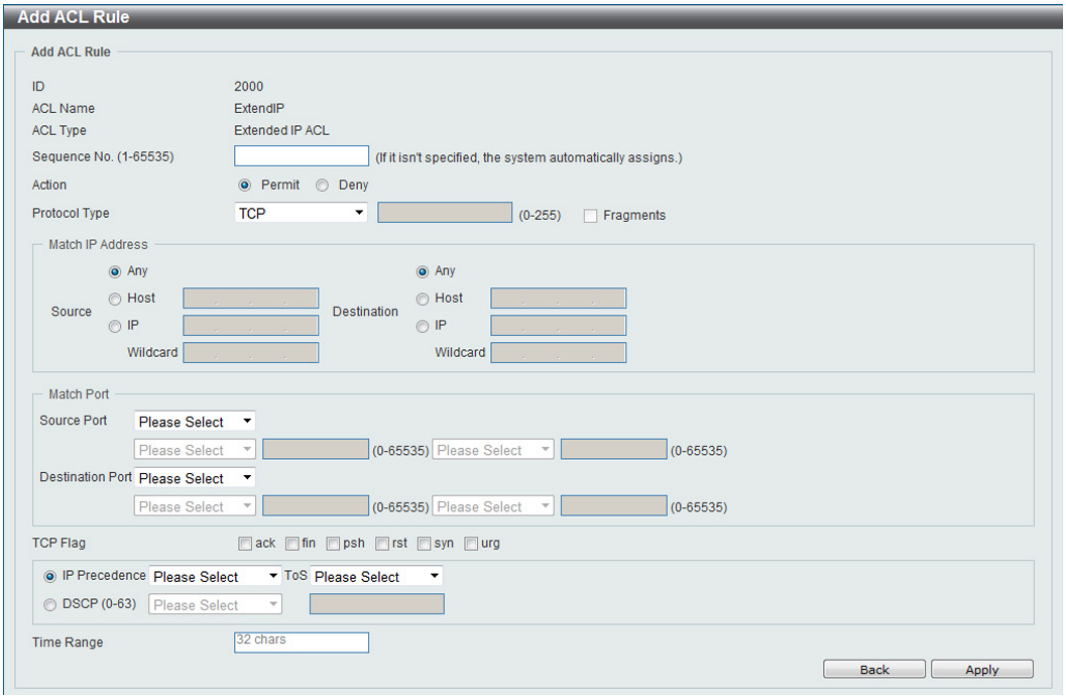


図 11-39　Extended IP ACL (Add Rule) TCP 画面

項目	説明
Source	送信元のアドレスを指定します。「Any」「Host」「IP」から指定します。 「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IP アドレスを入力します。 「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い送信元 IP アドレス群を入力します。ビットは 1 の値が無視され、0 が認識されます。
Destination	宛先のアドレスを指定します。「Any」「Host」「IP」から指定します。 「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IP アドレスを入力します。 「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い宛先 IP アドレス群を入力します。ビットは 1 の値が無視され、0 が認識されます。
Source Port	送信元ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選択した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択すると選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポートが使用されます。「Range」を選択すると指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。
Destination Port	宛先ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選択した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択すると選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポートが使用されます。「Range」を選択すると指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。
TCP Flag	TCP フラグを本ルールに含める場合、該当のフラグにチェックを入れます。「ack」「fin」「psh」「rst」「syn」「urg」から指定できます。
IP Precedence	IP 優先値を指定します。「0 (routine)」「1 (priority)」「2 (immediate)」「3 (flash)」「4 (flash-override)」「5 (critical)」「6 (internet)」「7 (network)」から指定できます。
ToS	IP 優先値を選択後、使用する「Type-of-Service」(ToS) の値を指定します。「0 (normal)」「1 (min-monetary-cost)」「2 (max-reliability)」「3, 4(max-throughput)」「5, 6, 7, 8 (min-delay)」「9」「10」「11」「12」「13」「14」「15」から指定できます。
DSCP	使用する DSCP 値を入力します。0 から 63 で入力できます。
Time Range	ACL ルールに関するタイムレンジ名を指定します。

「Back」ボタンをクリックして、変更を破棄し前の画面に戻ります。
「Apply」ボタンをクリックして、設定を適用します。

「UDP」選択時に表示される項目（Extended IP ACL / Protocol Type）

「Protocol Type」で UDP 選択時に表示される項目です。

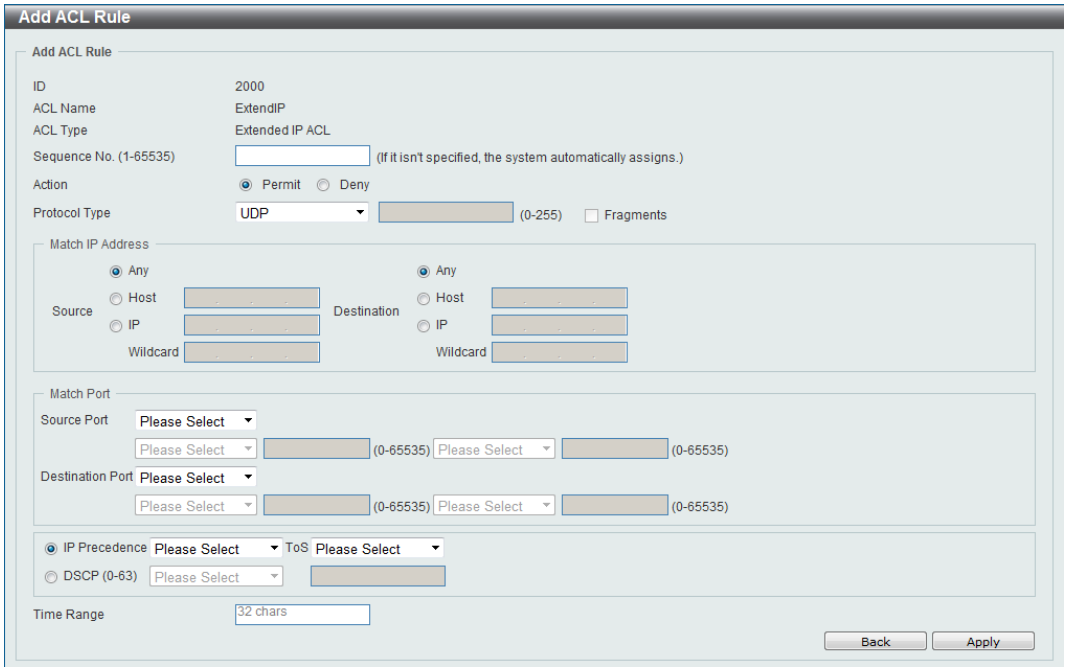


図 11-40　Extended IP ACL (Add Rule) UDP 画面

項目	説明
Source	送信元のアドレスを指定します。「Any」「Host」「IP」から指定します。 「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IP アドレスを入力します。 「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い送信元 IP アドレス群を入力します。ビットは 1 の値が無視され、0 が認識されます。
Destination	宛先のアドレスを指定します。「Any」「Host」「IP」から指定します。 「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IP アドレスを入力します。 「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い宛先 IP アドレス群を入力します。ビットは 1 の値が無視され、0 が認識されます。
Source Port	送信元ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選択した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択すると選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポートが使用されます。「Range」を選択すると指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。
Destination Port	宛先ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選択した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択すると選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポートが使用されます。「Range」を選択すると指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。
IP Precedence	IP 優先値を指定します。「0 (routine)」「1 (priority)」「2 (immediate)」「3 (flash)」「4 (flash-override)」「5 (critical)」「6 (internet)」「7 (network)」から指定できます。
ToS	IP 優先値を選択後、使用する「Type-of-Service」(ToS) の値を指定します。「0 (normal)」「1 (min-monetary-cost)」「2 (max-reliability)」「3, 4(max-throughput)」「5, 6, 7, 8 (min-delay)」「9」「10」「11」「12」「13」「14」「15」から指定できます。
DSCP	使用する DSCP 値を入力します。0 から 63 で入力できます。
Time Range	ACL ルールに関するタイムレンジ名を指定します。

「Back」ボタンをクリックして、変更を破棄し前の画面に戻ります。
「Apply」ボタンをクリックして、設定を適用します。

「ICMP」選択時に表示される項目（Extended IP ACL / Protocol Type）

「Protocol Type」で ICMP 選択時に表示される項目です。

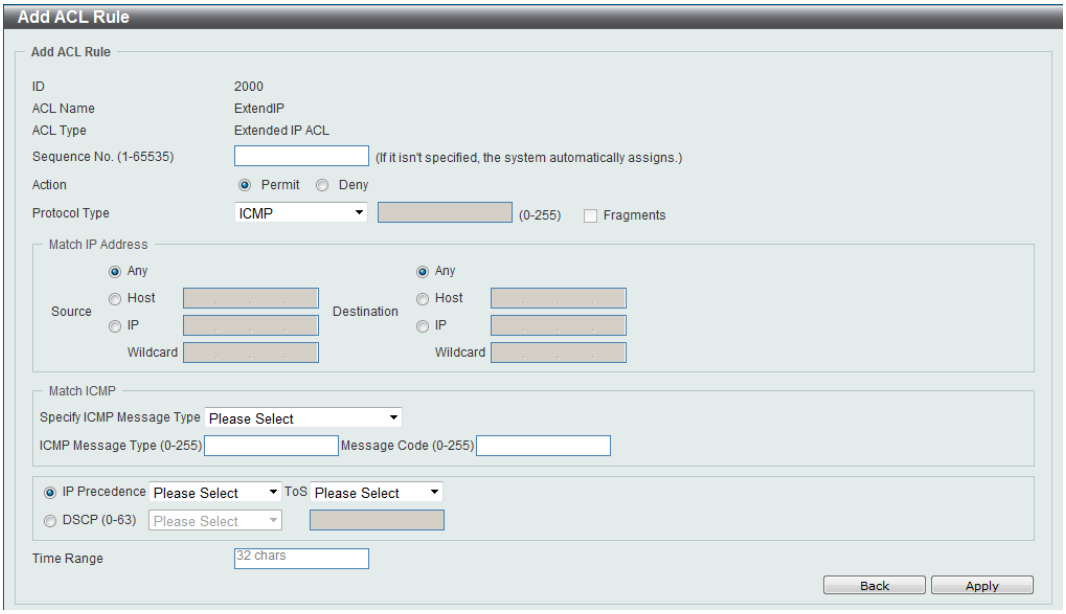


図 11-41　Extended IP ACL (Add Rule) ICMP 画面

項目	説明
Source	送信元のアドレスを指定します。「Any」「Host」「IP」から指定します。 「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IP アドレスを入力します。 「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い送信元 IP アドレス群を入力します。ビットは 1 の値が無視され、0 が認識されます。
Destination	宛先のアドレスを指定します。「Any」「Host」「IP」から指定します。 「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IP アドレスを入力します。 「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い宛先 IP アドレス群を入力します。ビットは 1 の値が無視され、0 が認識されます。
Specify ICMP Message Type	使用する ICMP メッセージの種類を指定します。自動的に ICMP メッセージ種類の数値とメッセージコードは指定されます。
ICMP Message Type	ICMP メッセージを指定しない場合、手動で ICMP メッセージ種類の数値を指定します。
Message Code	ICMP メッセージを指定しない場合、手動でメッセージコードを指定します。
IP Precedence	IP 優先値を指定します。「0 (routine)」「1 (priority)」「2 (immediate)」「3 (flash)」「4 (flash-override)」「5 (critical)」「6 (internet)」「7 (network)」から指定できます。
ToS	IP 優先値を選択後、使用する「Type-of-Service」(ToS) の値を指定します。「0 (normal)」「1 (min-monetary-cost)」「2 (max-reliability)」「3, 4(max-throughput)」「5, 6, 7, 8 (min-delay)」「9」「10」「11」「12」「13」「14」「15」から指定できます。
DSCP	使用する DSCP 値を入力します。0 から 63 で入力できます。
Time Range	ACL ルールに関するタイムレンジ名を指定します。

「Back」ボタンをクリックして、変更を破棄し前の画面に戻ります。
「Apply」ボタンをクリックして、設定を適用します。

「EIGRP」「ESP」「GRE」「IGMP」「OSPF」「PIM」「VRRP」「IP-in-IP」「PCP」「Protocol ID」「None」選択時に表示される項目（Extended IP ACL / Protocol Type）

「Protocol Type」で「ESP」「GRE」「IGMP」「OSPF」「PIM」「VRRP」「IP-in-IP」「PCP」「Protocol ID」「None」選択時に表示される項目です。

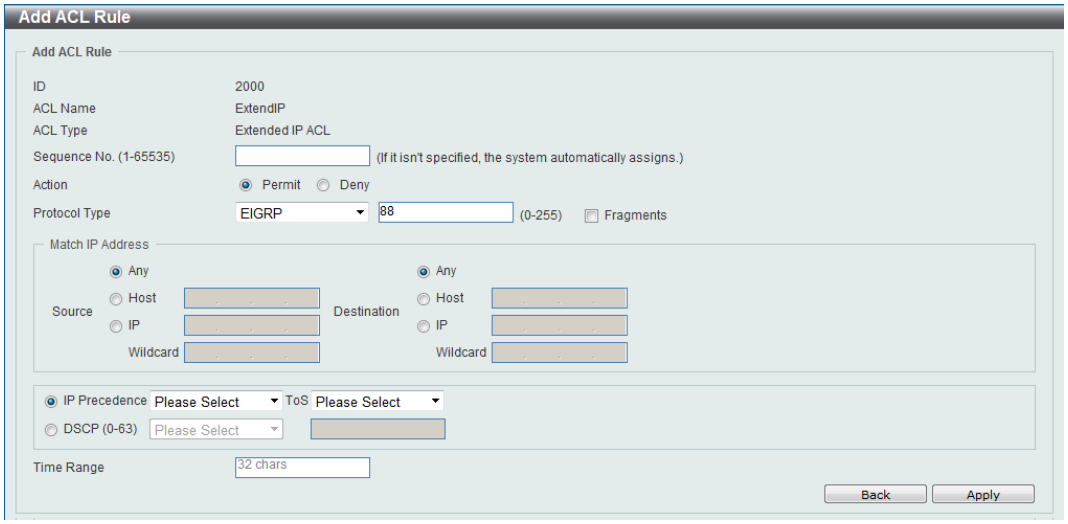


図 11-42　Extended IP ACL (Add Rule) EIGRP 画面

項目	説明
Fragments	パケットフラグメントフィルタリングを使用する場合、選択します。
Source:	送信元のアドレスを指定します。「Any」「Host」「IP」から指定します。 「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IP アドレスを入力します。 「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い送信元 IP アドレス群を入力します。ビットは 1 の値が無視され、0 が認識されます。
Destination:	宛先のアドレスを指定します。「Any」「Host」「IP」から指定します。 「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IP アドレスを入力します。 「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い宛先 IP アドレス群を入力します。ビットは 1 の値が無視され、0 が認識されます。
IP Precedence	IP 優先値を指定します。「0 (routine)」「1 (priority)」「2 (immediate)」「3 (flash)」「4 (flash-override)」「5 (critical)」「6 (internet)」「7 (network)」から指定できます。
ToS	IP 優先値を選択後、使用する「Type-of-Service」(ToS) の値を指定します。「0 (normal)」「1 (min-monetary-cost)」「2 (max-reliability)」「3, 4(max-throughput)」「5, 6, 7, 8 (min-delay)」「9」「10」「11」「12」「13」「14」「15」から指定できます。
DSCP	使用する DSCP 値を入力します。0 から 63 で入力できます。
Time Range	ACL ルールに関するタイムレンジ名を指定します。

「Back」ボタンをクリックして、変更を破棄し前の画面に戻ります。

「Apply」ボタンをクリックして、設定を適用します。

ACL ルールの編集（Edit）（Extended IP ACL）

「Counter State」オプションの有効化やプロファイルへの「Remark」の入力など ACL ルールの編集を行う場合、「ACL Profile Table」で該当するプロファイル横の「Edit」ボタンをクリックします。以下の画面が表示されます。

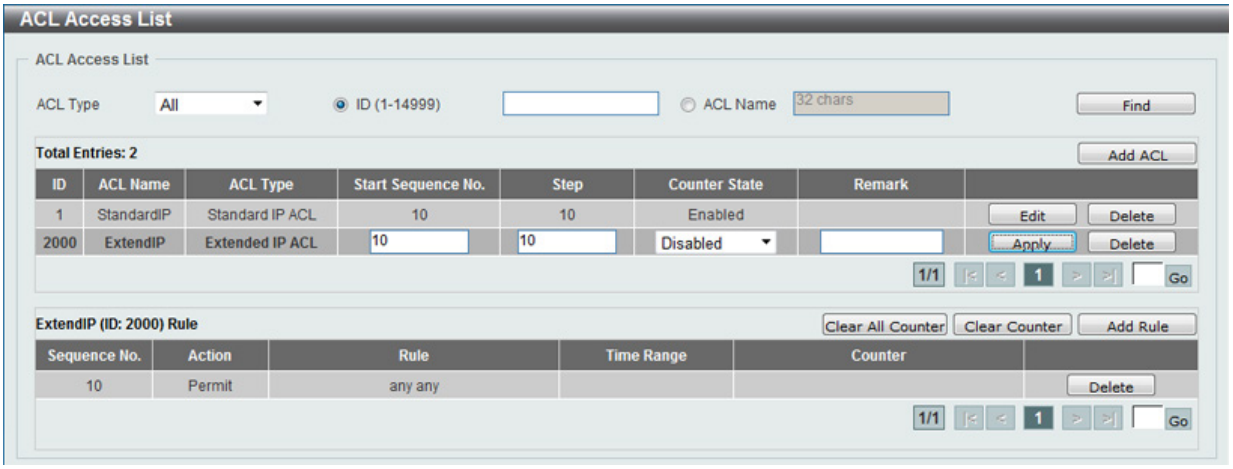


図 11-43　Extended IP ACL (Edit ACL) 画面

画面に表示される項目

項目	説明
Start Sequence No.	シーケンス番号の開始番号を指定します。
Step	シーケンス番号の増加番号を指定します。
Counter State	カウンタ機能の有効 / 無効を指定します。
Remark	指定プロファイルと関連するリマークを入力します。

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

特定の ACL プロファイルに関連する ACL ルール表示するには「ACL Profile Table」で該当の ACL プロファイルを選択します。ACL ルールが表示されます。

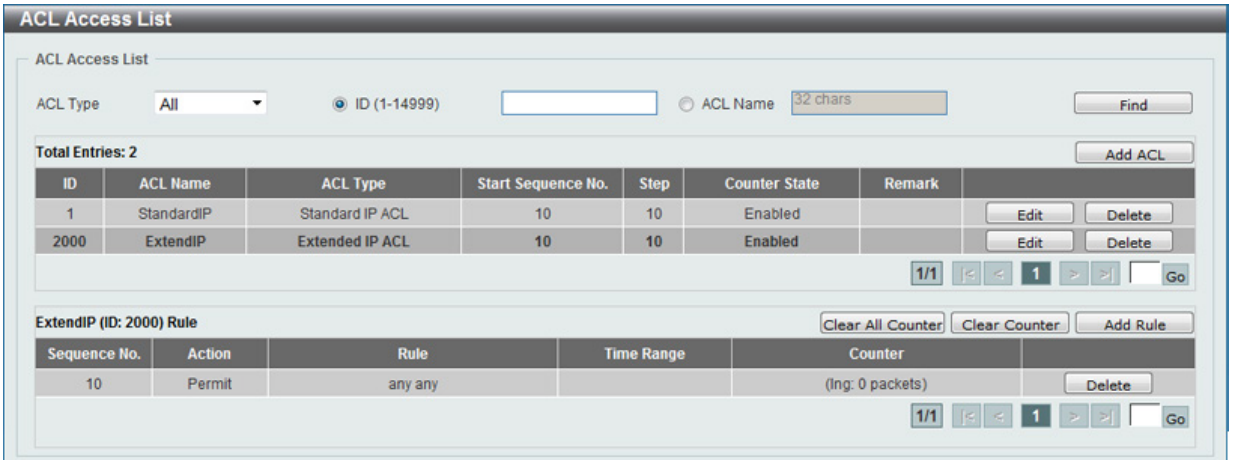


図 11-44　Extended IP ACL (Rule Display) 画面

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

Standard IPv6 ACL（通常 IPv6 ACL）

Standard IPv6 ACL の作成（Add ACL）

「Add ACL」をクリックし新しい ACL プロファイルを作成します。以下の画面が表示されます。

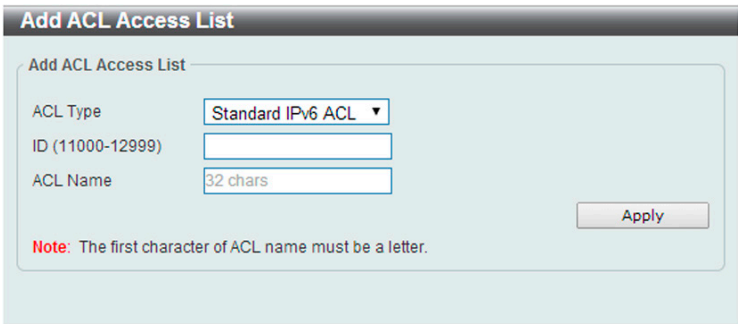


図 11-45　Standard IPv6 ACL (Add ACL Access List) 画面

画面に表示される項目

項目	説明
ACL Type	ACL プロファイルの種類を選択します。「Standard IP ACL」「Extended IP ACL」「Standard IPv6 ACL」「Extended IPv6 ACL」「Extended MAC ACL」「Extended Expert ACL」から選択します。
ID	ACL ID を入力します。11000 から 12999 の範囲で入力できます。
ACL Name	ACL 名を入力します。32 文字まで指定できます。

「Apply」ボタンをクリックして、設定を適用します。

ACL プロファイルを作成すると、「ACL Profile Table」に新しく作成した ACL プロファイルが以下の様に表示されます。

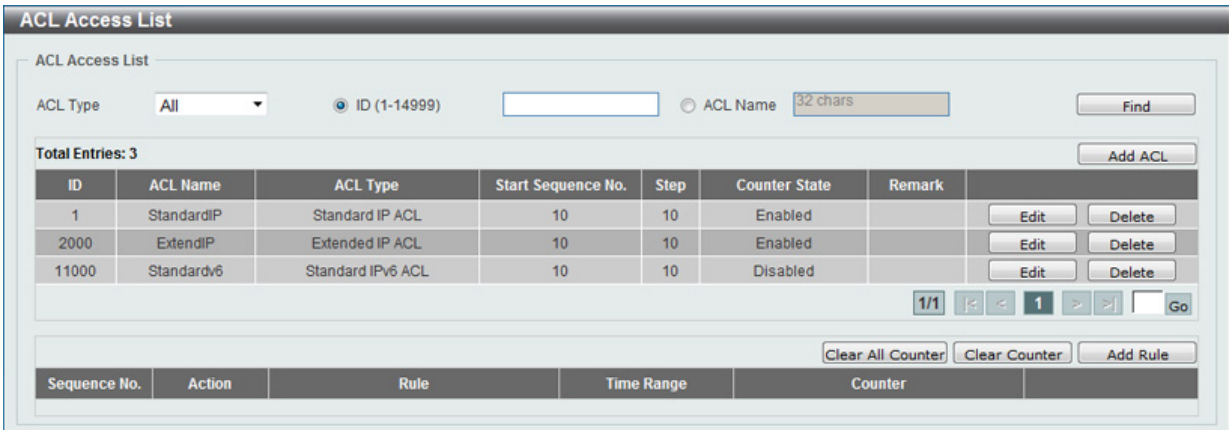


図 11-46　Standard IPv6 ACL (Main) 画面

「Edit」をクリックし、指定 ACL プロファイルの編集を行います。
「Delete」ボタンをクリックし、指定 ACL プロファイルの削除を行います。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

ACL プロファイルにルールを追加する場合、ACL プロファイルを選択後「Add Rule」ボタンをクリックします。

ACL ルールの追加（Add Rule）（Standard IPv6 ACL）

「Add Rule」をクリックし新しい ACL ルールを追加します。
ACL プロファイルを選択後「Add Rule」ボタンをクリックすると、以下の画面が表示され新しい ACL ルールを設定できます。

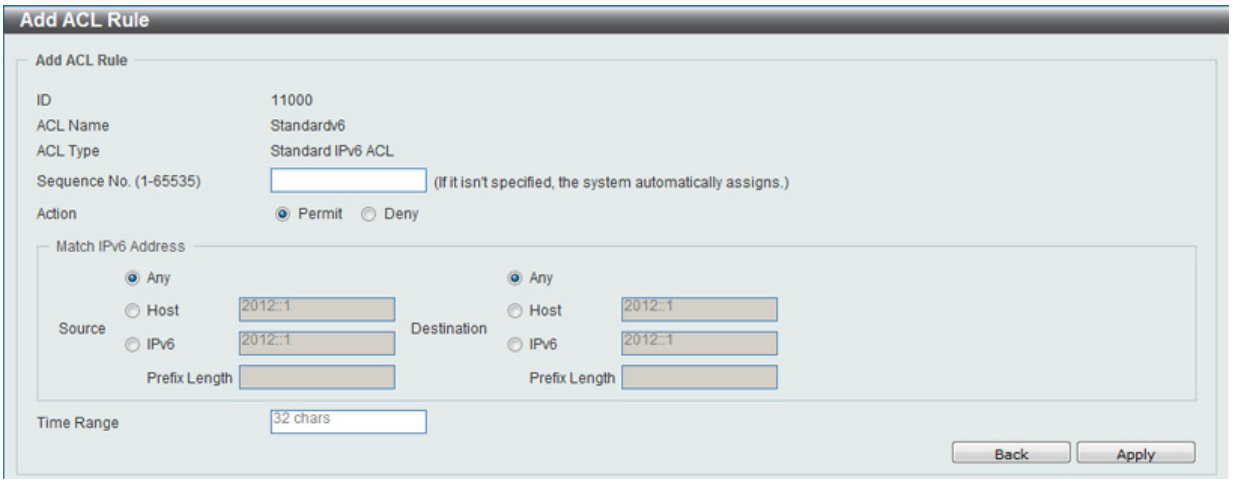


図 11-47　Standard IPv6 ACL (Add Rule) 画面

画面に表示される項目

項目	説明
Sequence No. (1-65535)	シーケンス番号を指定します。「1」から「65535」の間で指定できます。値が指定されないと自動的に番号が割り振られます。
Action	ルール動作に関する設定を行います。「Permit」または「Deny」から指定できます。
Source	送信元のアドレスを指定します。「Any」「Host」「IPv6」から指定します。 「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IPv6 アドレスを入力します。 「IPv6」を選択すると「Prefix Length」オプションが選択可能になり、送信元 IPv6 アドレスと Prefix Length を入力します。
Destination	宛先のアドレスを指定します。「Any」「Host」「IPv6」から指定します。 「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IPv6 アドレスを入力します。 「IPv6」を選択すると「Prefix Length」オプションが選択可能になり、宛先 IPv6 アドレスと Prefix Length を入力します。
Time Range	ACL ルールに関するタイムレンジ名を指定します。

「Back」ボタンをクリックして、変更を破棄し前の画面に戻ります。
「Apply」ボタンをクリックして、設定を適用します。

ACL ルールの編集（Edit）（Standard IPv6 ACL）

「Counter State」オプションの有効化やプロファイルへの「Remark」の入力など ACL ルールの編集を行う場合、「ACL Profile Table」で該当するプロファイル横の「Edit」ボタンをクリックします。以下の画面が表示されます。

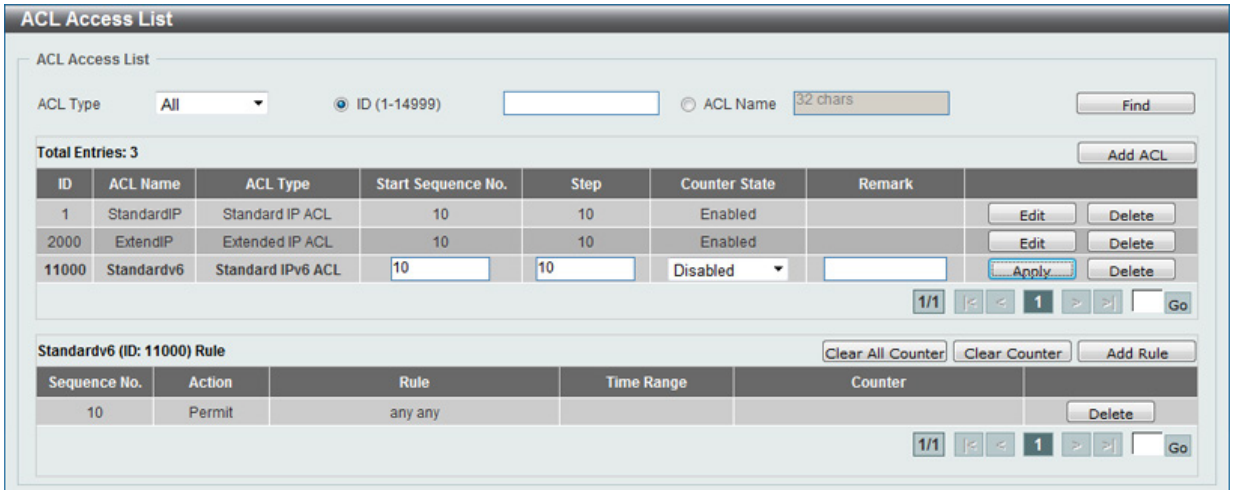


図 11-48　Standard IPv6 ACL (Edit ACL) 画面

画面に表示される項目

項目	説明
Start Sequence No.	シーケンス番号の開始番号を指定します。
Step	シーケンス番号の増加番号を指定します。
Counter State	カウンタ機能の有効 / 無効を指定します。
Remark	指定プロファイルと関連するリマークを入力します。

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

特定の ACL プロファイルに関連する ACL ルール表示するには「ACL Profile Table」で該当の ACL プロファイルを選択します。ACL ルールが表示されます。

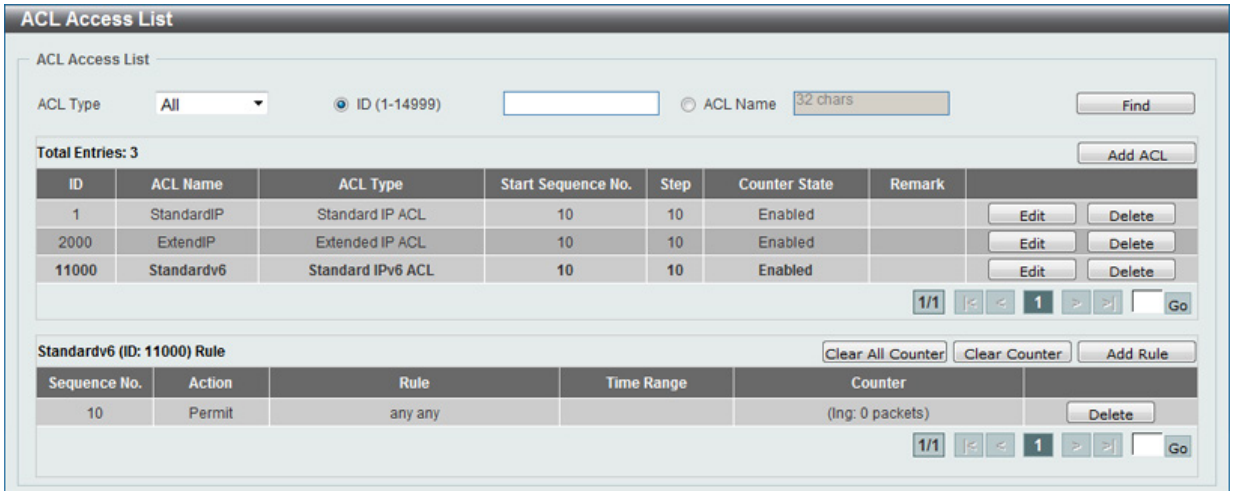


図 11-49　Standard IPv6 ACL (Rule Display) 画面

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

Extended IPv6 ACL（拡張 IPv6 ACL）

Extended IPv6 ACL の作成（Add ACL）

「Add ACL」をクリックし新しい ACL プロファイルを作成します。以下の画面が表示されます。

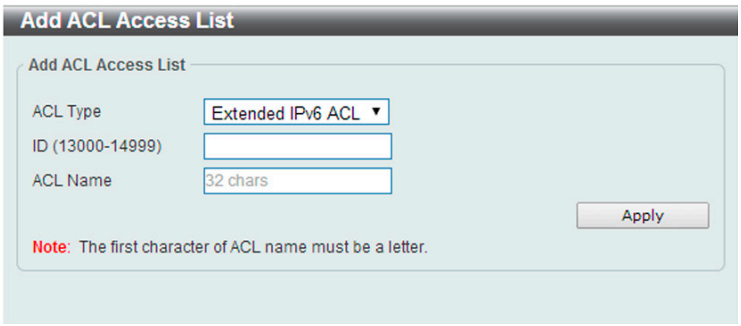


図 11-50　Extended IPv6 ACL (Add ACL Access List) 画面

画面に表示される項目

項目	説明
ACL Type	ACL プロファイルの種類を選択します。「Standard IP ACL」「Extended IP ACL」「Standard IPv6 ACL」「Extended IPv6 ACL」「Extended MAC ACL」「Extended Expert ACL」から選択します。
ID	ACL ID を入力します。13000 から 14999 の範囲で入力できます。
ACL Name	ACL 名を入力します。32 文字まで指定できます。

「Apply」ボタンをクリックして、設定を適用します。

ACL プロファイルを作成すると、「ACL Profile Table」に新しく作成した ACL プロファイルが以下の様に表示されます。

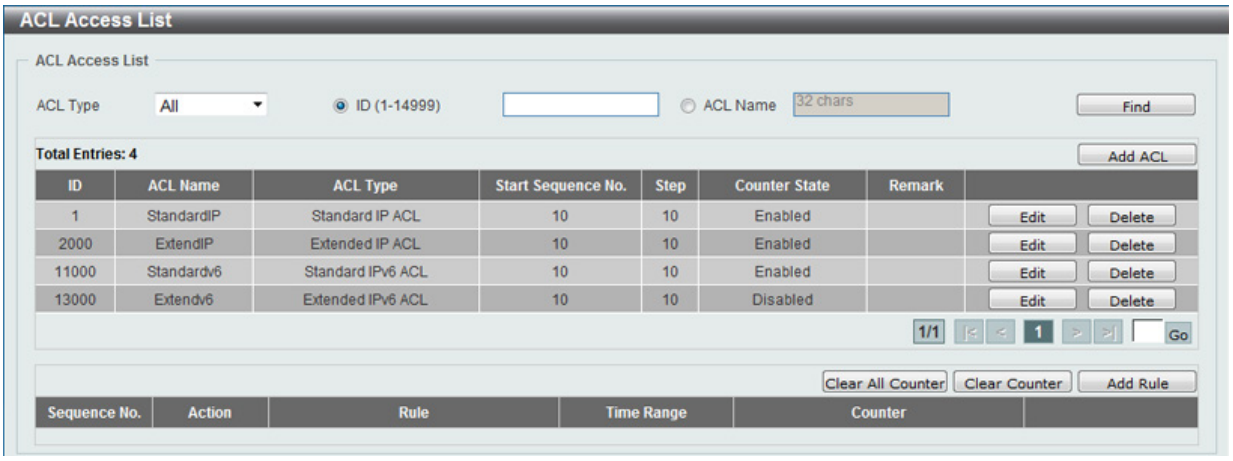


図 11-51　Extended IPv6 ACL (Main) 画面

「Edit」をクリックし、指定 ACL プロファイルの編集を行います。
「Delete」ボタンをクリックし、指定 ACL プロファイルの削除を行います。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

ACL プロファイルにルールを追加する場合、ACL プロファイルを選択後「Add Rule」ボタンをクリックします。

ACL ルールの追加（Add Rule）（Extended IPv6 ACL）

「Add Rule」をクリックし新しい ACL ルールを追加します。
ACL プロファイルを選択後「Add Rule」ボタンをクリックすると、以下の画面が表示され新しい ACL ルールを設定できます。

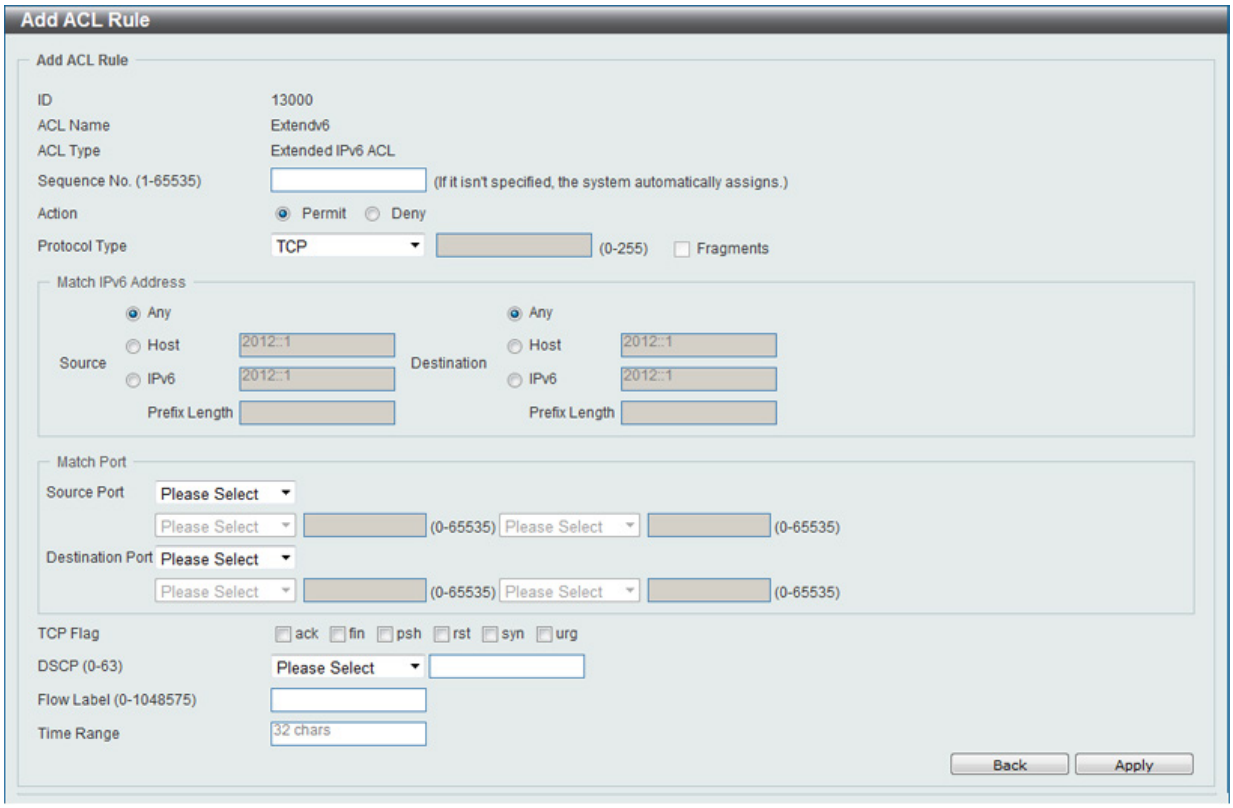


図 11-52　Extended IPv6 ACL (Add Rule) 画面

画面に表示される項目

項目	説明
Sequence No. (1-65535)	シーケンス番号を指定します。「1」から「65535」の間で指定できます。値が指定されないと自動的に番号が割り振られます。
Action	ルール動作に関する設定を行います。「Permit」または「Deny」から指定できます。
Protocol Type	プロトコルの種類を選択します。「TCP」「UDP」「ICMP」「ESP」「PCP」「Protocol ID」「SCTP」「None」から選択します。選択したプロトコルの種類によってはプロトコルに関連する数値（ID 等）を右の欄に入力する必要があります。その際、欄の右にある制限値（0-255 等）に注意して入力してください。

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

「TCP」選択時に表示される項目（Extended IPv6 ACL / Protocol Type）

「Protocol Type」で TCP 選択時に表示される項目です。

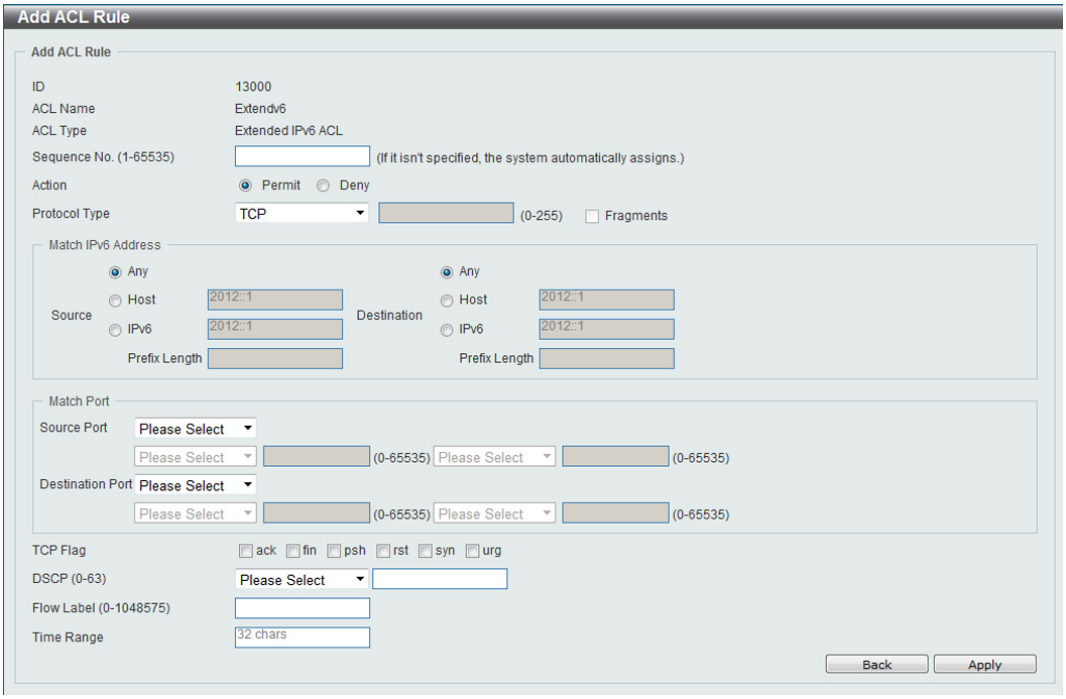


図 11-53　Extended IPv6 ACL (Add Rule) TCP 画面

項目	説明
Source	送信元のアドレスを指定します。「Any」「Host」「IPv6」から指定します。 「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IPv6 アドレスを入力します。 「IPv6」を選択すると「Prefix Length」が指定可能になり、送信元 IPv6 アドレスと Prefix Length を入力します。
Destination	宛先のアドレスを指定します。「Any」「Host」「IPv6」から指定します。 「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IPv6 アドレスを入力します。 「IPv6」を選択すると「Prefix Length」が指定可能になり、宛先 IPv6 アドレスと Prefix Length を入力します。
Source Port	送信元ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選択した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択すると選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポートが使用されます。「Range」を選択すると指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。
Destination Port	宛先ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選択した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択すると選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポートが使用されます。「Range」を選択すると指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。
TCP Flag	TCP フラグを本ルールに含める場合、該当のフラグにチェックを入れます。「ack」「fin」「psh」「rst」「syn」「urg」から指定できます。
DSCP	使用する DSCP 値を入力します。0 から 63 で入力できます。
Flow Label	フローラベルの値を入力します。0 から 1048575 まで指定可能です。
Time Range	ACL ルールに関するタイムレンジ名を指定します。

「Back」ボタンをクリックして、変更を破棄し前の画面に戻ります。
「Apply」ボタンをクリックして、設定を適用します。

「UDP」選択時に表示される項目（Extended IPv6 ACL / Protocol Type）

「Protocol Type」で UDP 選択時に表示される項目です。

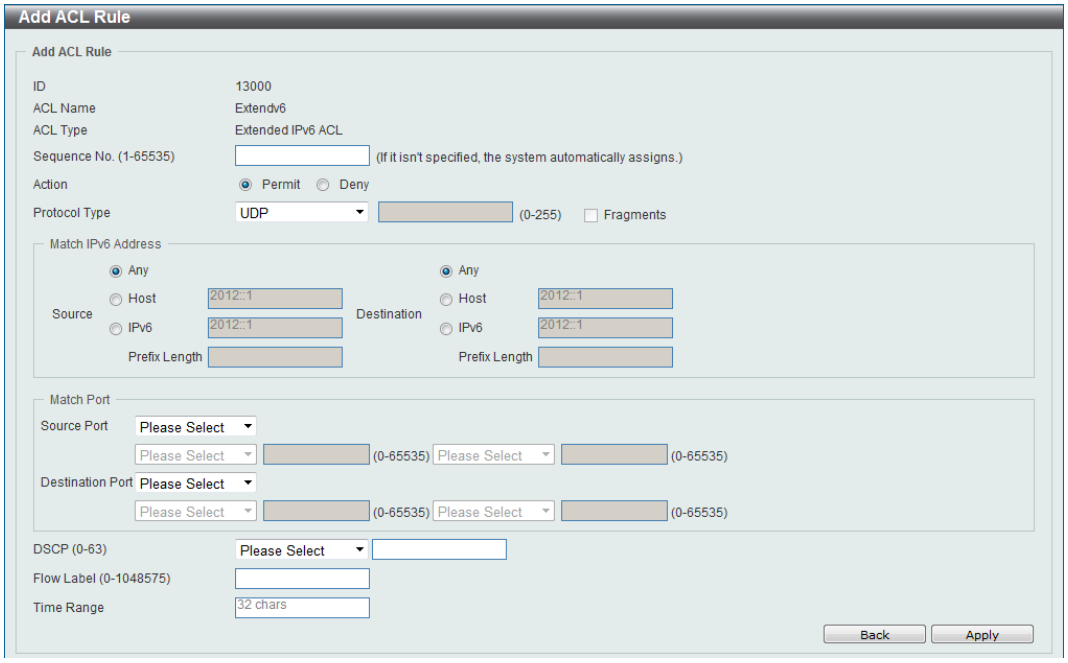


図 11-54　Extended IPv6 ACL (Add Rule) UDP 画面

項目	説明
Source	送信元のアドレスを指定します。「Any」「Host」「IPv6」から指定します。 「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IPv6 アドレスを入力します。 「IPv6」を選択すると「Prefix Length」が指定可能になり、送信元 IPv6 アドレスと Prefix Length を入力します。
Destination	宛先のアドレスを指定します。「Any」「Host」「IPv6」から指定します。 「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IPv6 アドレスを入力します。 「IPv6」を選択すると「Prefix Length」が指定可能になり、宛先 IPv6 アドレスと Prefix Length を入力します。
Source Port	送信元ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選択した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択すると選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポートが使用されます。「Range」を選択すると指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。
Destination Port	宛先ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選択した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択すると選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポートが使用されます。「Range」を選択すると指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。
DSCP	使用する DSCP 値を入力します。0 から 63 で入力できます。
Flow Label	フローラベルの値を入力します。0 から 1048575 まで指定可能です。
Time Range	ACL ルールに関するタイムレンジ名を指定します。

「Back」ボタンをクリックして、変更を破棄し前の画面に戻ります。
「Apply」ボタンをクリックして、設定を適用します。

「ICMP」選択時に表示される項目（Extended IPv6 ACL / Protocol Type）

「Protocol Type」で ICMP 選択時に表示される項目です。

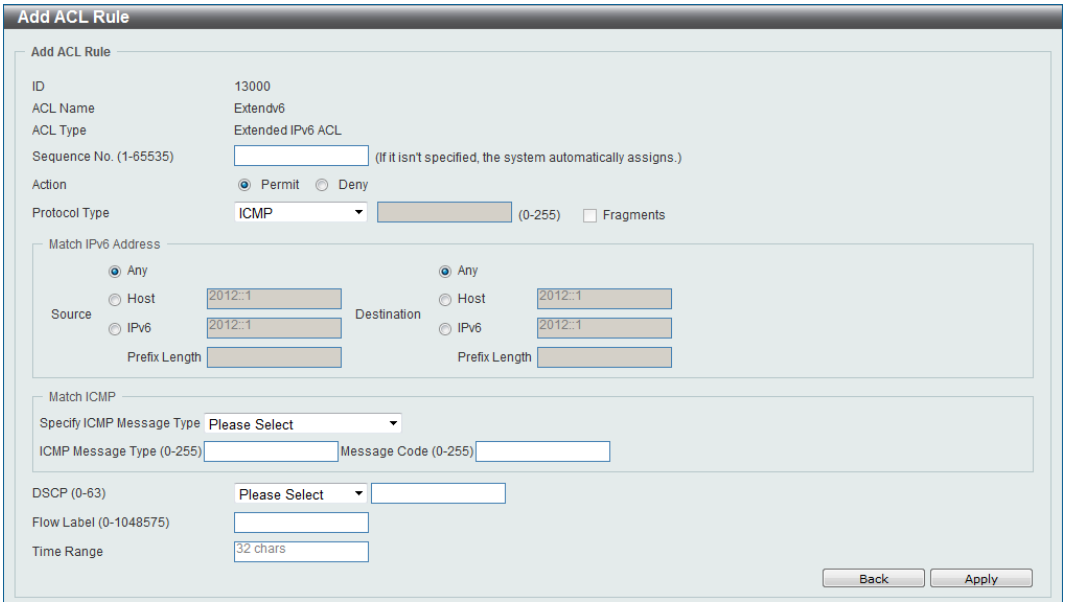


図 11-55　Extended IPv6 ACL (Add Rule) ICMP 画面

項目	説明
Source	送信元のアドレスを指定します。「Any」「Host」「IPv6」から指定します。 「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IPv6 アドレスを入力します。 「IPv6」を選択すると「Prefix Length」が指定可能になり、送信元 IPv6 アドレスと Prefix Length を入力します。
Destination	宛先のアドレスを指定します。「Any」「Host」「IPv6」から指定します。 「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IPv6 アドレスを入力します。 「IPv6」を選択すると「Prefix Length」が指定可能になり、宛先 IPv6 アドレスと Prefix Length を入力します。
Specify ICMP Message Type	使用する ICMP メッセージの種類を指定します。自動的に ICMP メッセージ種類の数値とメッセージコードは指定されます。
ICMP Message Type	ICMP メッセージを指定しない場合、手動で ICMP メッセージ種類の数値を指定します。
Message Code	ICMP メッセージを指定しない場合、手動でメッセージコードを指定します。
DSCP	使用する DSCP 値を入力します。0 から 63 で入力できます。
Flow Label	フローラベルの値を入力します。0 から 1048575 まで指定可能です。
Time Range	ACL ルールに関するタイムレンジ名を指定します。

「Back」ボタンをクリックして、変更を破棄し前の画面に戻ります。

「Apply」ボタンをクリックして、設定を適用します。

「ESP」「PCP」「Protocol ID」「SCTP」「None」選択時に表示される項目（Extended IPv6 ACL / Protocol Type）

「Protocol Type」で「ESP」「PCP」「Protocol ID」「SCTP」「None」選択時に表示される項目選択時に表示される項目です。

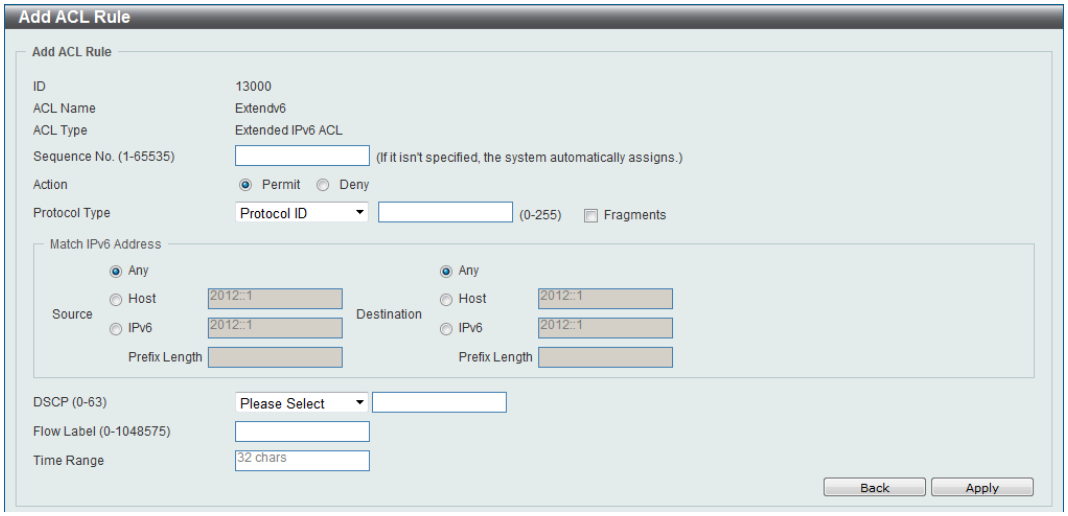


図 11-56　Extended IPv6 ACL (Add Rule) Protocol ID 画面

項目	説明
Protocol	プロトコル ID（0-255）を指定します。
Fragments	パケットフラグメントフィルタリングを使用する場合、選択します。
Source	送信元のアドレスを指定します。「Any」「Host」「IPv6」から指定します。 「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IPv6 アドレスを入力します。 「IPv6」を選択すると「Prefix Length」が指定可能になり、送信元 IPv6 アドレスと Prefix Length を入力します。
Destination	宛先のアドレスを指定します。「Any」「Host」「IPv6」から指定します。 「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IPv6 アドレスを入力します。 「IPv6」を選択すると「Prefix Length」が指定可能になり、宛先 IPv6 アドレスと Prefix Length を入力します。
DSCP	使用する DSCP 値を入力します。0 から 63 で入力できます。
Flow Label	フローラベルの値を入力します。0 から 1048575 まで指定可能です。
Time Range	ACL ルールに関するタイムレンジ名を指定します。

「Back」ボタンをクリックして、変更を破棄し前の画面に戻ります。
「Apply」ボタンをクリックして、設定を適用します。

ACL ルールの編集（Edit）（Extended IPv6 ACL）

「Counter State」オプションの有効化やプロファイルへの「Remark」の入力など ACL ルールの編集を行う場合、「ACL Profile Table」で該当するプロファイル横の「Edit」ボタンをクリックします。以下の画面が表示されます。

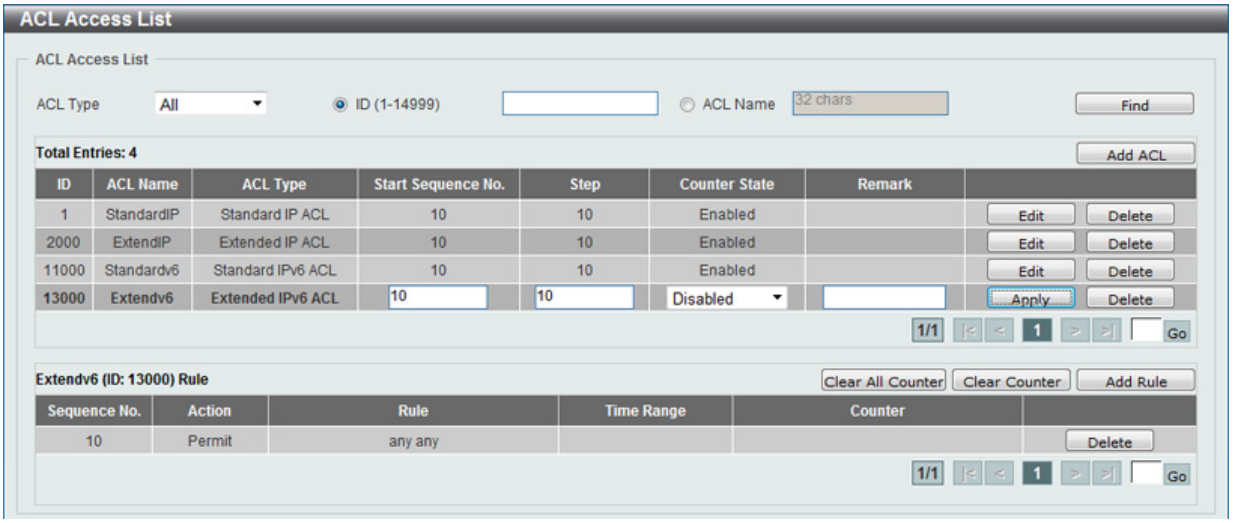


図 11-57　Extended IPv6 ACL (Edit ACL) 画面

画面に表示される項目

項目	説明
Start Sequence No.	シーケンス番号の開始番号を指定します。
Step	シーケンス番号の増加番号を指定します。
Counter State	カウンタ機能の有効 / 無効を指定します。
Remark	指定プロファイルと関連するリマークを入力します。

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

特定の ACL プロファイルに関連する ACL ルール表示するには「ACL Profile Table」で該当の ACL プロファイルを選択します。ACL ルールが表示されます。

Extended MAC ACL（拡張 MAC ACL）

Extended MAC ACL の作成（Add ACL）

「Add ACL」をクリックし新しい ACL プロファイルを作成します。以下の画面が表示されます。

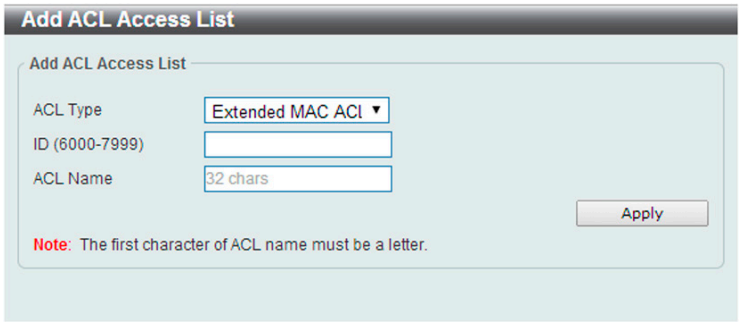


図 11-58　Extended MAC ACL (Add ACL Access List) 画面

画面に表示される項目

項目	説明
ACL Type	ACL プロファイルの種類を選択します。「Standard IP ACL」「Extended IP ACL」「Standard IPv6 ACL」「Extended IPv6 ACL」「Extended MAC ACL」「Extended Expert ACL」から選択します。
ID	ACL ID を入力します。6000 から 7999 の範囲で入力できます。
ACL Name	ACL 名を入力します。32 文字まで指定できます。

「Apply」ボタンをクリックして、設定を適用します。

ACL プロファイルを作成すると、「ACL Profile Table」に新しく作成した ACL プロファイルが以下の様に表示されます。

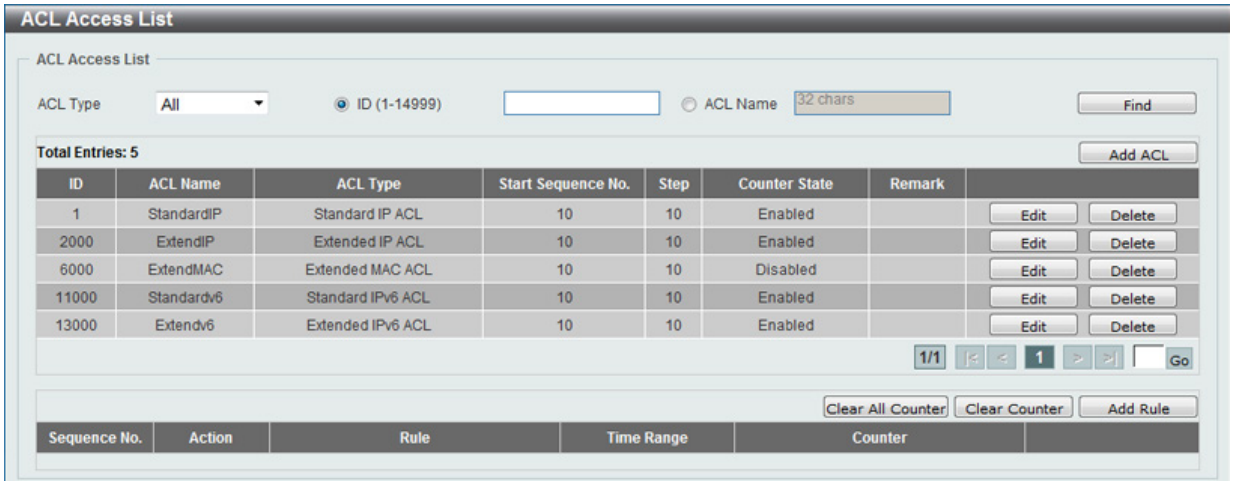


図 11-59　Extended MAC ACL (Main) 画面

「Edit」をクリックし、指定 ACL プロファイルの編集を行います。
「Delete」ボタンをクリックし、指定 ACL プロファイルの削除を行います。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

ACL プロファイルにルールを追加する場合、ACL プロファイルを選択後「Add Rule」ボタンをクリックします。

ACL ルールの追加（Add Rule）（Extended MAC ACL）

「Add Rule」をクリックし新しい ACL ルールを追加します。
ACL プロファイルを選択後「Add Rule」ボタンをクリックすると、以下の画面が表示され新しい ACL ルールを設定できます。

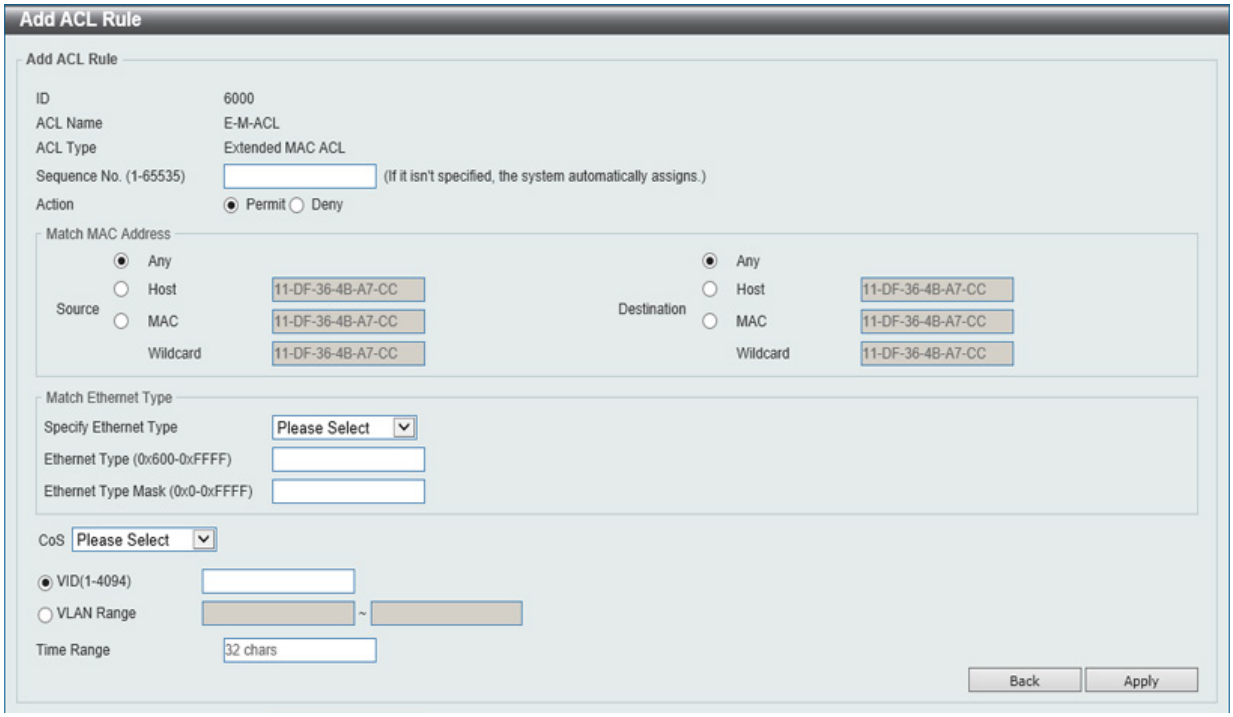


図 11-60　Extended MAC ACL (Add Rule) 画面

画面に表示される項目

項目	説明
Sequence No. (1-65535)	シーケンス番号を指定します。「1」から「65535」の間で指定できます。
Action	ルール動作に関する設定を行います。「Permit」または「Deny」から指定できます。
Source	送信元の MAC アドレスを指定します。「Any」「Host」「MAC」から指定します。 「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの MAC アドレスを入力します。 「MAC」を選択すると「Wildcard」オプションが選択可能になり送信元 MAC アドレスとワイルドカードを入力することができます。

項目	説明
Destination	宛先の MAC アドレスを指定します。「Any」「Host」「MAC」から指定します。 「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。 「Host」を選択すると宛先ホストの MAC アドレスを入力します。 「MAC」を選択すると「Wildcard」オプションが選択可能になり宛先 MAC アドレスとワイルドカードを入力することができます。
Specify Ethernet Type	イーサネットタイプを選択します。「aarp」「appletalk」「decent-iv」「etype-6000」「etype-8042」「lat」「lavc-sca」「mop-console」「mop-dump」「vines-echo」「vines-ip」「xns-idp」「arp」から選択します。
Ethernet Type	イーサネットタイプの 16 進数値を指定します。0x600 から 0xFFFF の間で指定できます。「Specify Ethernet Type」で指定したイーサネットタイプに基づき適切な値が入力されます。
Ethernet Type Mask	イーサネットタイプマスクの 16 進数値を指定します。0x0 から 0xFFFF の間で指定できます。「Specify Ethernet Type」で指定したイーサネットタイプに基づき適切な値が入力されます。
CoS	CoS の値を入力します。0 から 7 の間で入力できます。
VID	ACL ルールに関連する VLAN ID を入力します。1 から 4094 の間で入力可能です。
VLAN Range	VLAN の範囲を VLAN ID で指定します。
Time Range	ACL ルールに関するタイムレンジ名を指定します。

「Back」ボタンをクリックして、変更を破棄し前の画面に戻ります。
「Apply」ボタンをクリックして、設定を適用します。

ACL ルールの編集（Edit）（Extended MAC ACL）

「Counter State」オプションの有効化やプロファイルへの「Remark」の入力など ACL ルールの編集を行う場合、「ACL Profile Table」で該当するプロファイル横の「Edit」ボタンをクリックします。以下の画面が表示されます。

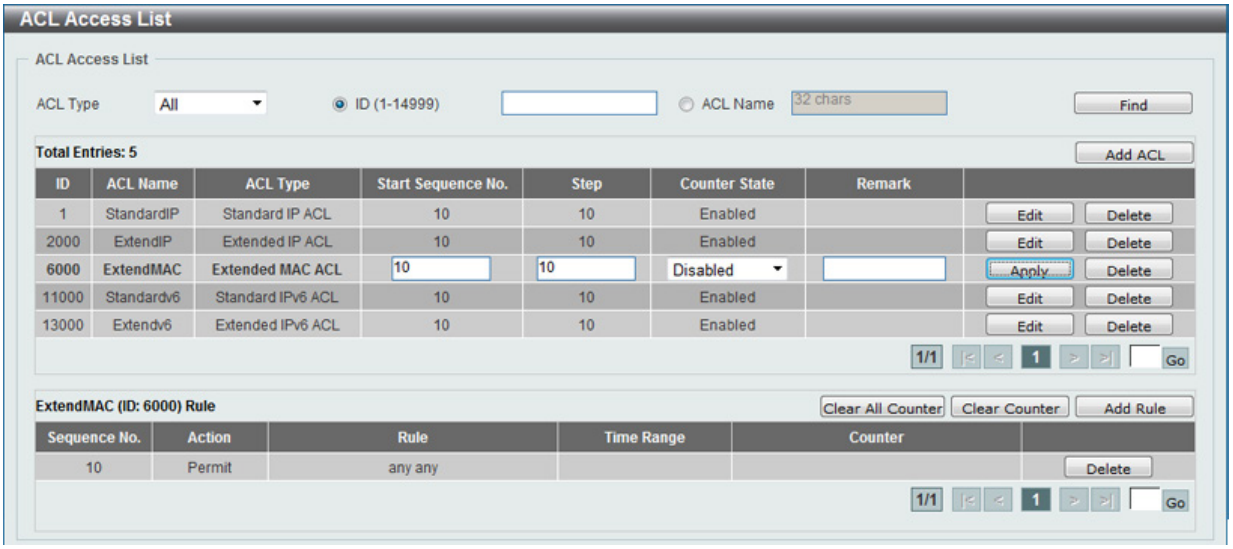


図 11-61　Extended MAC ACL (Edit ACL) 画面

画面に表示される項目

項目	説明
Start Sequence No.	シーケンス番号の開始番号を指定します。
Step	シーケンス番号の増加番号を指定します。
Counter State	カウンタ機能の有効 / 無効を指定します。
Remark	指定プロファイルと関連するリマークを入力します。

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

特定の ACL プロファイルに関連する ACL ルール表示するには「ACL Profile Table」で該当の ACL プロファイルを選択します。ACL ルールが表示されます。

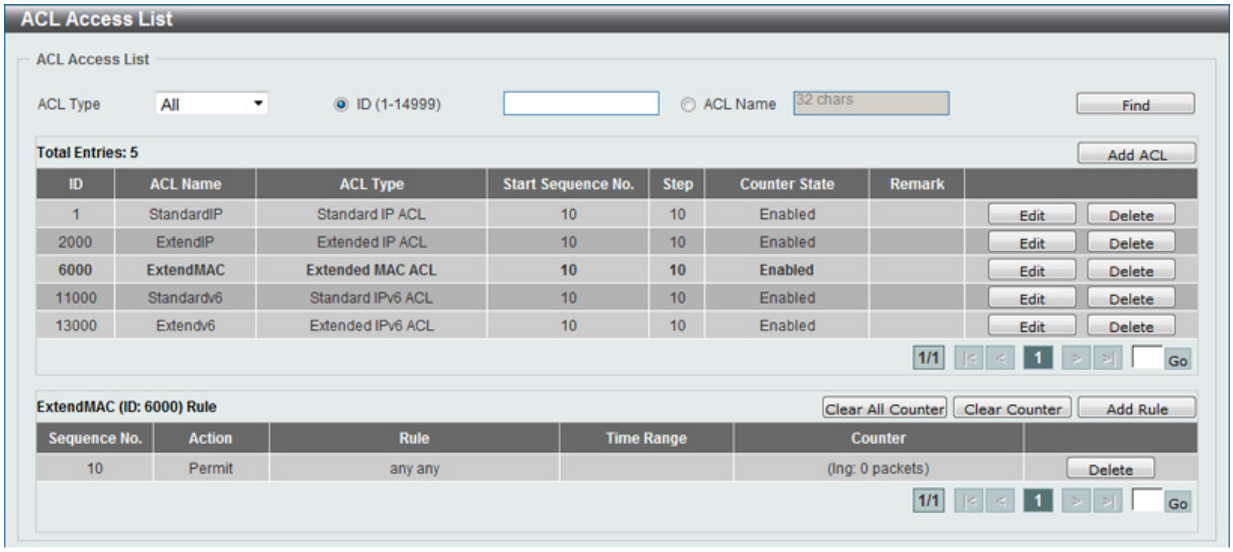


図 11-62　Extended MAC ACL (Rule Display) 画面

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

Extended Expert ACL（拡張詳細 ACL）

Extended Expert ACL の作成（Add ACL）

「Add ACL」をクリックし新しい ACL プロファイルを作成します。以下の画面が表示されます。

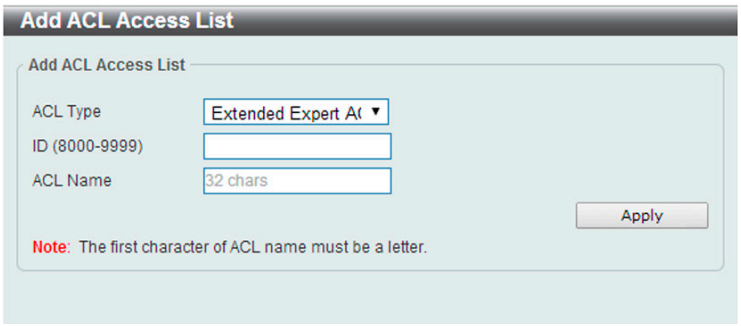


図 11-63　Extended Expert ACL (Add ACL Access List) 画面

画面に表示される項目

項目	説明
ACL Type	ACL プロファイルの種類を選択します。「Standard IP ACL」「Extended IP ACL」「Standard IPv6 ACL」「Extended IPv6 ACL」「Extended MAC ACL」「Extended Expert ACL」から選択します。
ID	ACL ID を入力します。8000 から 9999 の範囲で入力できます。
ACL Name	ACL 名を入力します。32 文字まで指定できます。

「Apply」ボタンをクリックして、設定を適用します。

ACL プロファイルを作成すると、「ACL Profile Table」に新しく作成した ACL プロファイルが以下の様に表示されます。

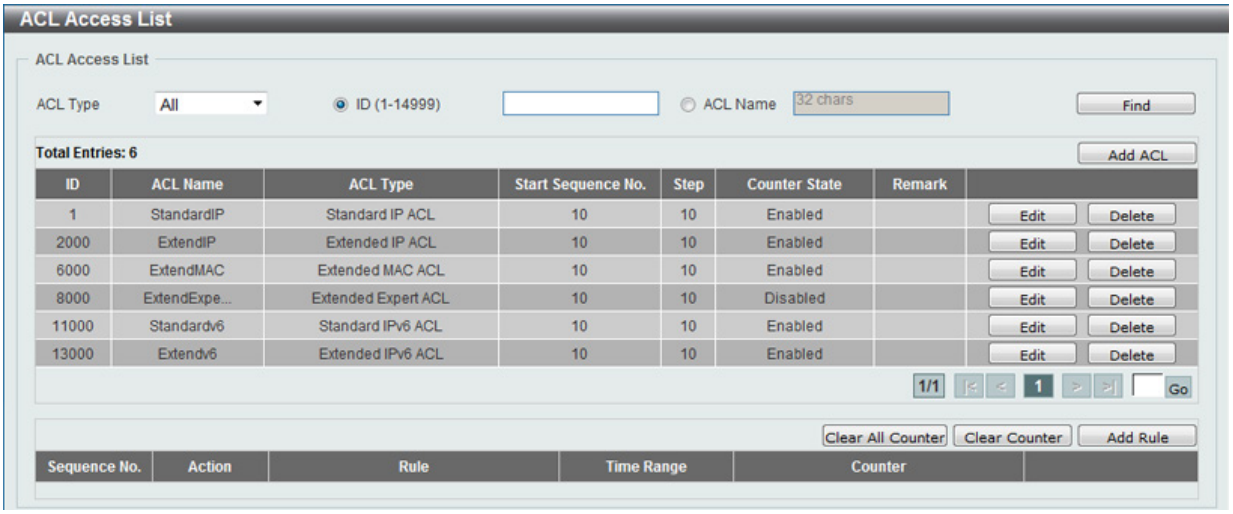


図 11-64　Extended Expert ACL (Main) 画面

「Edit」をクリックし、指定 ACL プロファイルの編集を行います。
「Delete」ボタンをクリックし、指定 ACL プロファイルの削除を行います。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

ACL プロファイルにルールを追加する場合、ACL プロファイルを選択後「Add Rule」ボタンをクリックします。

ACL ルールの追加（Add Rule）（Extended Expert ACL）

「Add Rule」をクリックし新しい ACL ルールを追加します。
ACL プロファイルを選択後「Add Rule」ボタンをクリックすると、以下の画面が表示され新しい ACL ルールを設定できます。

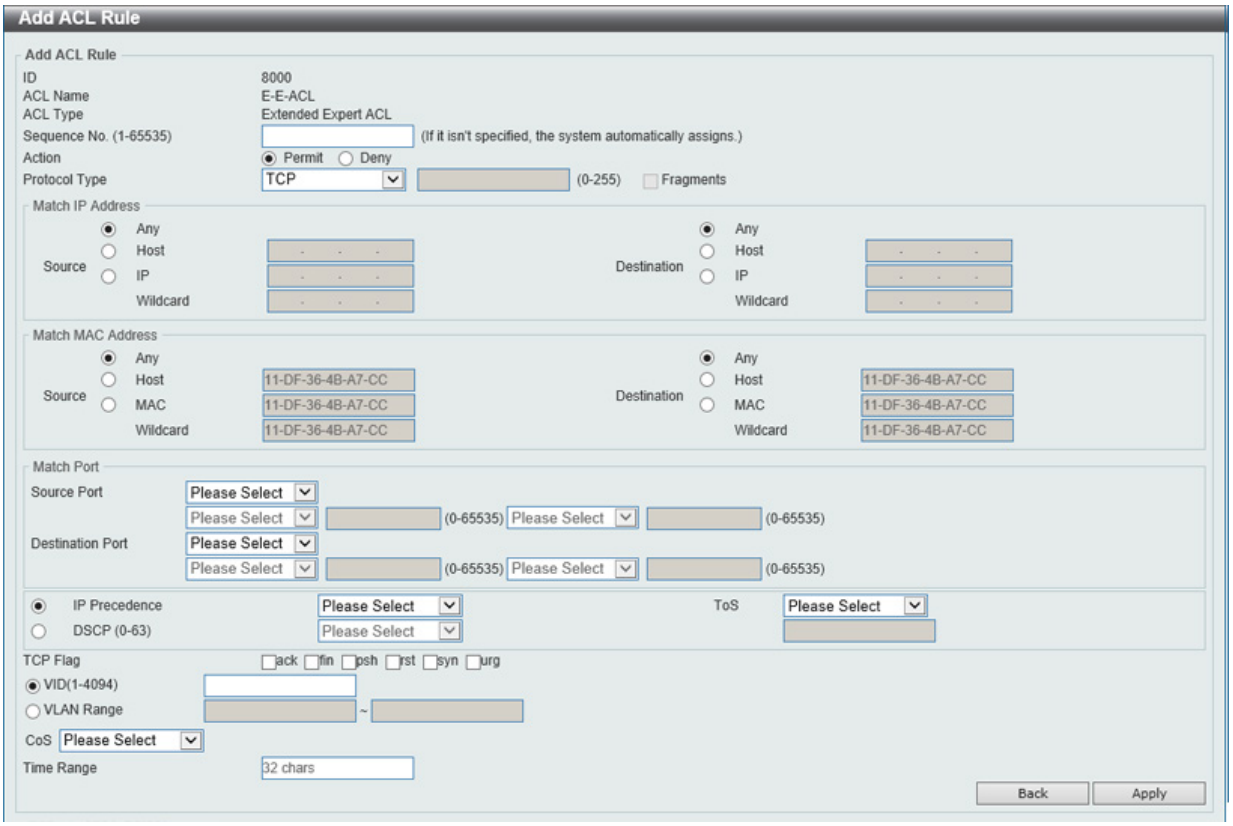


図 11-65　Extended Expert ACL (Add Rule) 画面

画面に表示される項目

項目	説明
Sequence No. (1-65535)	シーケンス番号を指定します。「1」から「65535」の間で指定できます。値が指定されないと自動的に番号が割り振られます。
Action	ルール動作に関する設定を行います。「Permit」または「Deny」から指定できます。

項目	説明
Protocol Type	プロトコルの種類を選択します。「TCP」「UDP」「ICMP」「EIGRP」「ESP」「GRE」「IGMP」「OSPF」「PIM」「VRRP」「IP-in-IP」「PCP」「Protocol ID」「None」から選択します。 選択したプロトコルの種類によってはプロトコルに関連する数値（ID 等）を右の欄に入力する必要があります。その際、欄の右にある制限値（0-255 等）に注意して入力してください。

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

「TCP」選択時に表示される項目（Extended Expert ACL / Protocol Type）

「Protocol Type」で TCP 選択時に表示される項目です。

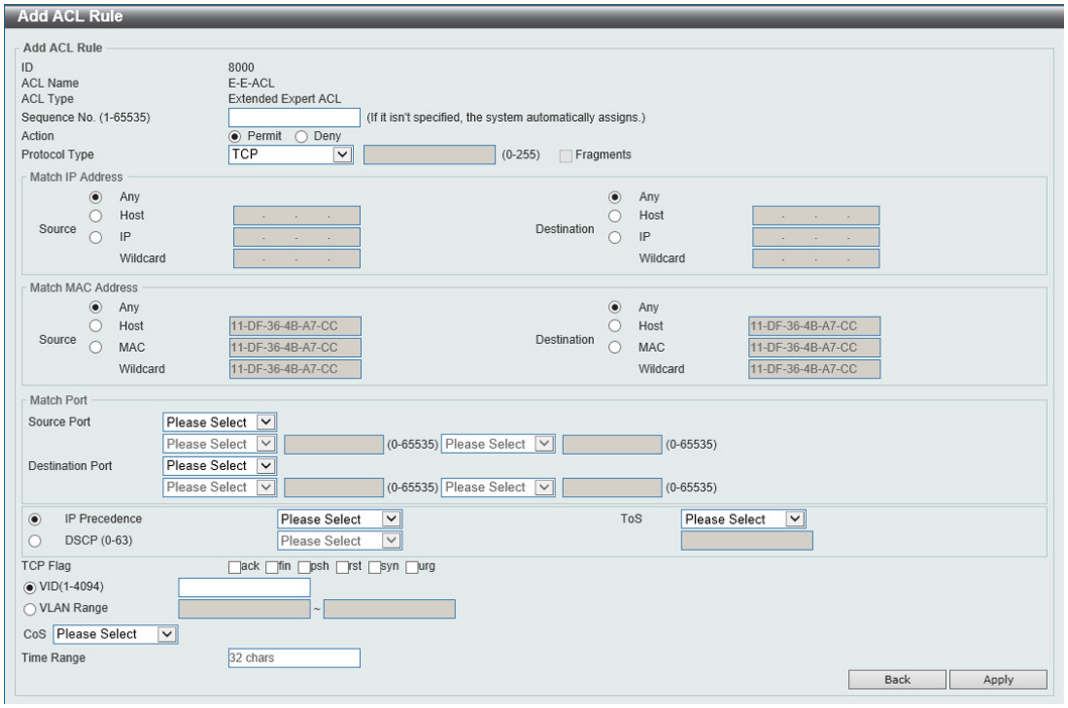


図 11-66　Extended Expert ACL (Add Rule) TCP 画面

すべてのプロトコル選択時に表示される項目（Extended Expert ACL）

項目	説明
Source IP Address	送信元のアドレスを指定します。「Any」「Host」「IP」から指定します。 「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IP アドレスを入力します。 「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い送信元 IP アドレス群を入力します。ビットは 1 の値が無視され、0 が認識されます。
Destination IP Address	宛先のアドレスを指定します。「Any」「Host」「IP」から指定します。 「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IP アドレスを入力します。 「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い宛先 IP アドレス群を入力します。ビットは 1 の値が無視され、0 が認識されます。
Source MAC Address	送信元の MAC アドレスを指定します。「Any」「Host」「MAC」から指定します。 「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの MAC アドレスを入力します。 「MAC」を選択すると「Wildcard」オプションが選択可能になり送信元 MAC アドレスとワイルドカードを入力することができます。
Destination MAC Address	宛先の MAC アドレスを指定します。「Any」「Host」「MAC」から指定します。 「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。 「Host」を選択すると宛先ホストの MAC アドレスを入力します。 「MAC」を選択すると「Wildcard」オプションが選択可能になり宛先 MAC アドレスとワイルドカードを入力することができます。

項目	説明
Source Port	送信元ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選択した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択すると選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポートが使用されます。「Range」を選択すると指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。
Destination Port	宛先ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選択した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択すると選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポートが使用されます。「Range」を選択すると指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。
IP Precedence	IP 優先値を指定します。「0 (routine)」「1 (priority)」「2, (immediate)」「3 (flash)」「4 (flash-override)」「5 (critical)」「6 (internet)」「7 (network)」から指定できます。
ToS	IP 優先値を選択後、使用する「Type-of-Service」(ToS) の値を指定します。「0 (normal)」「1 (min-monetary-cost)」「2 (max-reliability)」「3, 4(max-throughput)」「5, 6, 7, 8 (min-delay)」「9」「10」「11」「12」「13」「14」「15」から指定できます。
DSCP	使用する DSCP 値を入力します。0 から 63 で入力できます。
TCP Flag	TCP フラグを本ルールに含める場合、該当のフラグにチェックを入れます。「ack」「fin」「psh」「rst」「syn」「urg」から指定できます。
VID	関連する VLAN ID（1-4094）を指定します。
VLAN Range	VLAN の範囲を VLAN ID で指定します。
CoS	Class of Service（CoS）の値（0-7）を指定します。
Time Range	ACL ルールに関するタイムレンジ名を指定します。

「Back」ボタンをクリックして、変更を破棄し前の画面に戻ります。
「Apply」ボタンをクリックして、設定を適用します。

「UDP」選択時に表示される項目（Extended Expert ACL / Protocol Type）

「Protocol Type」で UDP 選択時に表示される項目です。

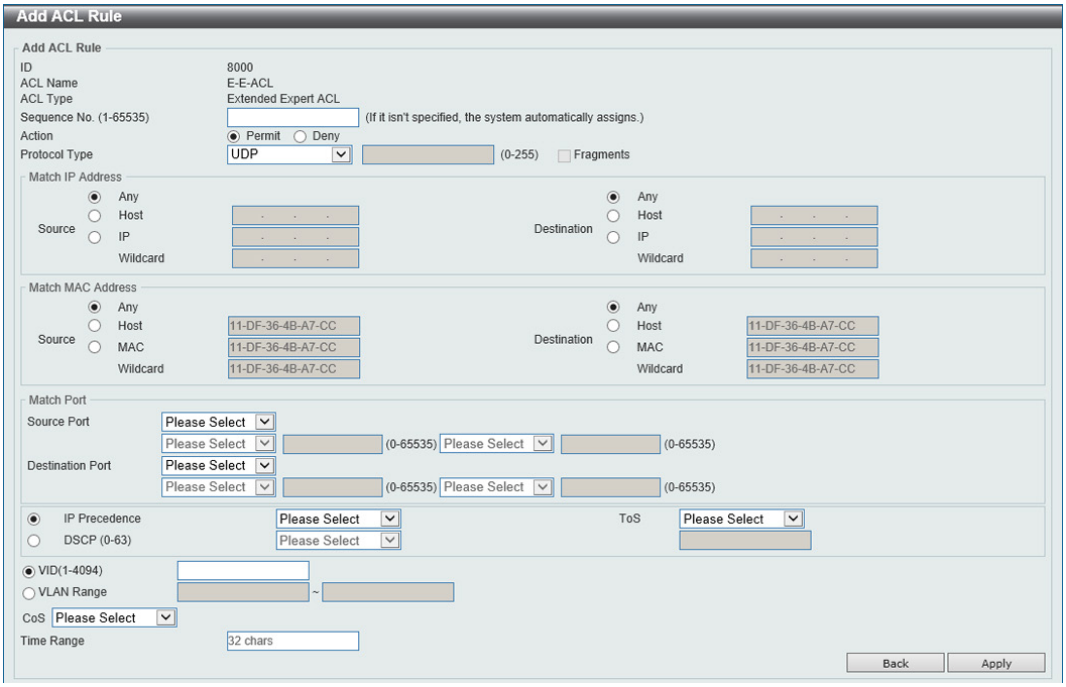


図 11-67　Extended Expert ACL (Add Rule) UDP 画面

項目	説明
Source IP Address	送信元のアドレスを指定します。「Any」「Host」「IP」から指定します。 「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IP アドレスを入力します。 「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い送信元 IP アドレス群を入力します。ビットは 1 の値が無視され、0 が認識されます。

項目	説明
Destination IP Address	宛先のアドレスを指定します。「Any」「Host」「IP」から指定します。 「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IP アドレスを入力します。 「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い宛先 IP アドレス群を入力します。ビットは 1 の値が無視され、0 が認識されます。
Source MAC Address	送信元の MAC アドレスを指定します。「Any」「Host」「MAC」から指定します。 「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの MAC アドレスを入力します。 「MAC」を選択すると「Wildcard」オプションが選択可能になり送信元 MAC アドレスとワイルドカードを入力することができます。
Destination MAC Address	宛先の MAC アドレスを指定します。「Any」「Host」「MAC」から指定します。 「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。 「Host」を選択すると宛先ホストの MAC アドレスを入力します。 「MAC」を選択すると「Wildcard」オプションが選択可能になり宛先 MAC アドレスとワイルドカードを入力することができます。
Source Port	送信元ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選択した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択すると選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポートが使用されます。「Range」を選択すると指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。
Destination Port	宛先ポートの値を選択し、指定します。「=」「>」「<」「≠」「Range」から指定可能です。「=」を選択すると選択した指定のポート番号が使用されます。「>」選択ポートよりも数の多いポートが使用されます。「<」を選択すると選択ポートより少ない数のポートが使用されます。「≠」を選択すると選択ポートは除外されそれ以外のポートが使用されます。「Range」を選択すると指定した始めと終わりのポート番号の範囲が使用されます。ドロップダウンリストに選択するポート番号がない場合は項目欄に手動で指定できます。
IP Precedence	IP 優先値を指定します。「0 (routine)」「1 (priority)」「2, (immediate)」「3 (flash)」「4 (flash-override)」「5 (critical)」「6 (internet)」「7 (network)」から指定できます。
ToS	IP 優先値を選択後、使用する「Type-of-Service」(ToS) の値を指定します。「0 (normal)」「1 (min-monetary-cost)」「2 (max-reliability)」「3, 4(max-throughput)」「5, 6, 7, 8 (min-delay)」「9」「10」「11」「12」「13」「14」「15」から指定できます。
DSCP	使用する DSCP 値を入力します。0 から 63 で入力できます。
VID	関連する VLAN ID（1-4094）を指定します。
VLAN Range	VLAN の範囲を VLAN ID で指定します。
CoS	Class of Service（CoS）の値（0-7）を指定します。
Time Range	ACL ルールに関するタイムレンジ名を指定します。

「Back」ボタンをクリックして、変更を破棄し前の画面に戻ります。
「Apply」ボタンをクリックして、設定を適用します。

「ICMP」選択時に表示される項目（Extended Expert ACL / Protocol Type）

「Protocol Type」で ICMP 選択時に表示される項目です。

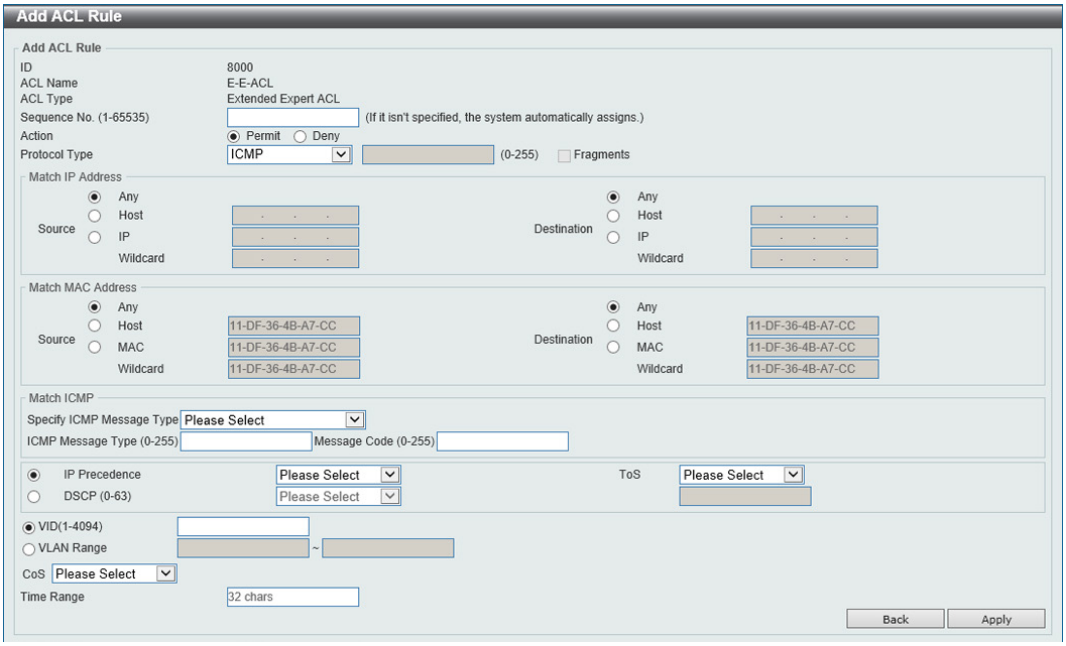


図 11-68　Extended Expert ACL (Add Rule) ICMP 画面

項目	説明
Source IP Address	送信元のアドレスを指定します。「Any」「Host」「IP」から指定します。 「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IP アドレスを入力します。 「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い送信元 IP アドレス群を入力します。ビットは 1 の値が無視され、0 が認識されます。
Destination IP Address	宛先のアドレスを指定します。「Any」「Host」「IP」から指定します。 「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IP アドレスを入力します。 「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い宛先 IP アドレス群を入力します。ビットは 1 の値が無視され、0 が認識されます。
Source MAC Address	送信元の MAC アドレスを指定します。「Any」「Host」「MAC」から指定します。 「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの MAC アドレスを入力します。 「MAC」を選択すると「Wildcard」オプションが選択可能になり送信元 MAC アドレスとワイルドカードを入力することができます。
Destination MAC Address	宛先の MAC アドレスを指定します。「Any」「Host」「MAC」から指定します。 「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。 「Host」を選択すると宛先ホストの MAC アドレスを入力します。 「MAC」を選択すると「Wildcard」オプションが選択可能になり宛先 MAC アドレスとワイルドカードを入力することができます。
Specify ICMP Message Type	使用するICMPメッセージの種類を指定します。自動的にICMPメッセージ種類の数値とメッセージコードは指定されます。
ICMP Message Type	ICMP メッセージを指定しない場合、手動で ICMP メッセージ種類の数値を指定します。
Message Code	ICMP メッセージを指定しない場合、手動でメッセージコードを指定します。
IP Precedence	IP 優先値を指定します。「0 (routine)」「1 (priority)」「2, (immediate)」「3 (flash)」「4 (flash-override)」「5 (critical)」「6 (internet)」「7 (network)」から指定できます。
ToS	IP 優先値を選択後、使用する「Type-of-Service」(ToS) の値を指定します。「0 (normal)」「1 (min-monetary-cost)」「2 (max-reliability)」「3, 4(max-throughput)」「5, 6, 7, 8 (min-delay)」「9」「10」「11」「12」「13」「14」「15」から指定できます。
DSCP	使用する DSCP 値を入力します。0 から 63 で入力できます。
VID	関連する VLAN ID（1-4094）を指定します。
VLAN Range	VLAN の範囲を VLAN ID で指定します。
CoS	Class of Service（CoS）の値（0-7）を指定します。
Time Range	ACL ルールに関するタイムレンジ名を指定します。

「Back」ボタンをクリックして、変更を破棄し前の画面に戻ります。

「Apply」ボタンをクリックして、設定を適用します。

「EIGRP」「ESP」「GRE」「IGMP」「OSPF」「PIM」「VRRP」「IP-in-IP」「PCP」「Protocol ID」「None」選択時に表示される項目（Extended Expert ACL / Protocol Type）

「Protocol Type」で「EIGRP」「ESP」「GRE」「IGMP」「OSPF」「PIM」「VRRP」「IP-in-IP」「PCP」「Protocol ID」「None」選択時に表示される項目です。

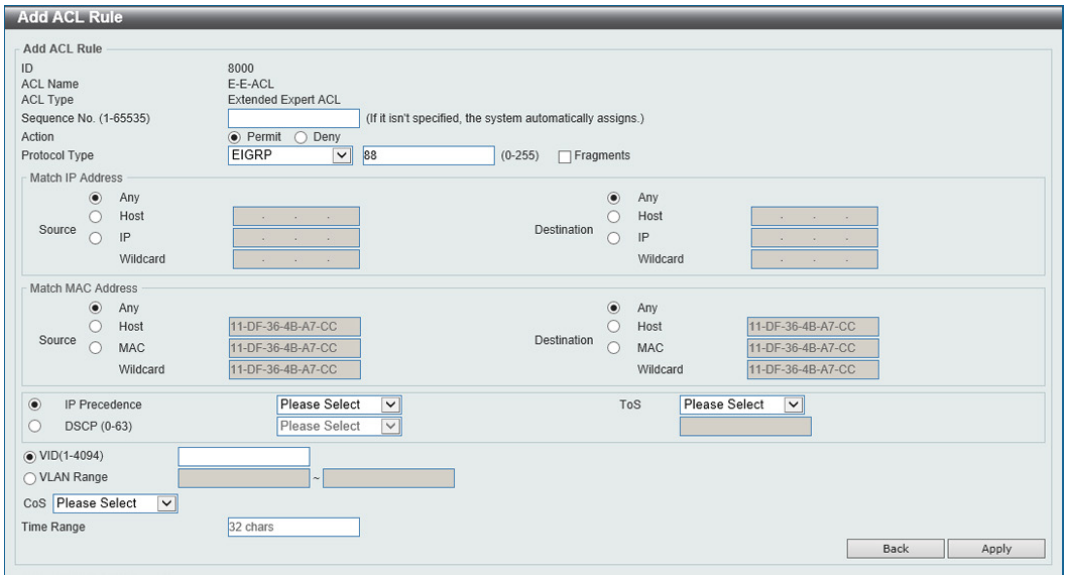


図 11-69　Extended Expert ACL (Add Rule) EIGRP 画面

項目	説明
Fragments	パケットフラグメントフィルタリングを使用する場合、選択します。
Source IP Address	送信元のアドレスを指定します。「Any」「Host」「IP」から指定します。 「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IP アドレスを入力します。 「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い送信元 IP アドレス群を入力します。ビットは 1 の値が無視され、0 が認識されます。
Destination IP Address	宛先のアドレスを指定します。「Any」「Host」「IP」から指定します。 「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの IP アドレスを入力します。 「IP」を選択すると「Wildcard」オプションが選択可能になり、ワイルドカードビットマップを使い宛先 IP アドレス群を入力します。ビットは 1 の値が無視され、0 が認識されます。
Source MAC Address	送信元の MAC アドレスを指定します。「Any」「Host」「MAC」から指定します。 「Any」を選択するとどの送信元トラフィックでも本ルールに従って評価されます。 「Host」を選択するとホストの MAC アドレスを入力します。 「MAC」を選択すると「Wildcard」オプションが選択可能になり送信元 MAC アドレスとワイルドカードを入力することができます。
Destination MAC Address	宛先の MAC アドレスを指定します。「Any」「Host」「MAC」から指定します。 「Any」を選択するとどの宛先トラフィックでも本ルールに従って評価されます。 「Host」を選択すると宛先ホストの MAC アドレスを入力します。 「MAC」を選択すると「Wildcard」オプションが選択可能になり宛先 MAC アドレスとワイルドカードを入力することができます。
IP Precedence	IP 優先値を指定します。「0 (routine)」「1 (priority)」「2, (immediate)」「3 (flash)」「4 (flash-override)」「5 (critical)」「6 (internet)」「7 (network)」から指定できます。
ToS	IP 優先値を選択後、使用する「Type-of-Service」(ToS) の値を指定します。「0 (normal)」「1 (min-monetary-cost)」「2 (max-reliability)」「3, 4(max-throughput)」「5, 6, 7, 8 (min-delay)」「9」「10」「11」「12」「13」「14」「15」から指定できます。
DSCP	使用する DSCP 値を入力します。0 から 63 で入力できます。
VID	関連する VLAN ID（1-4094）を指定します。
VLAN Range	VLAN の範囲を VLAN ID で指定します。
CoS	Class of Service（CoS）の値（0-7）を指定します。
Time Range	ACL ルールに関するタイムレンジ名を指定します。

「Back」ボタンをクリックして、変更を破棄し前の画面に戻ります。
「Apply」ボタンをクリックして、設定を適用します。

ACL ルールの編集（Edit）（Extended Expert ACL）

「Counter State」オプションの有効化やプロファイルへの「Remark」の入力など ACL ルールの編集を行う場合、「ACL Profile Table」で該当するプロファイル横の「Edit」ボタンをクリックします。以下の画面が表示されます。

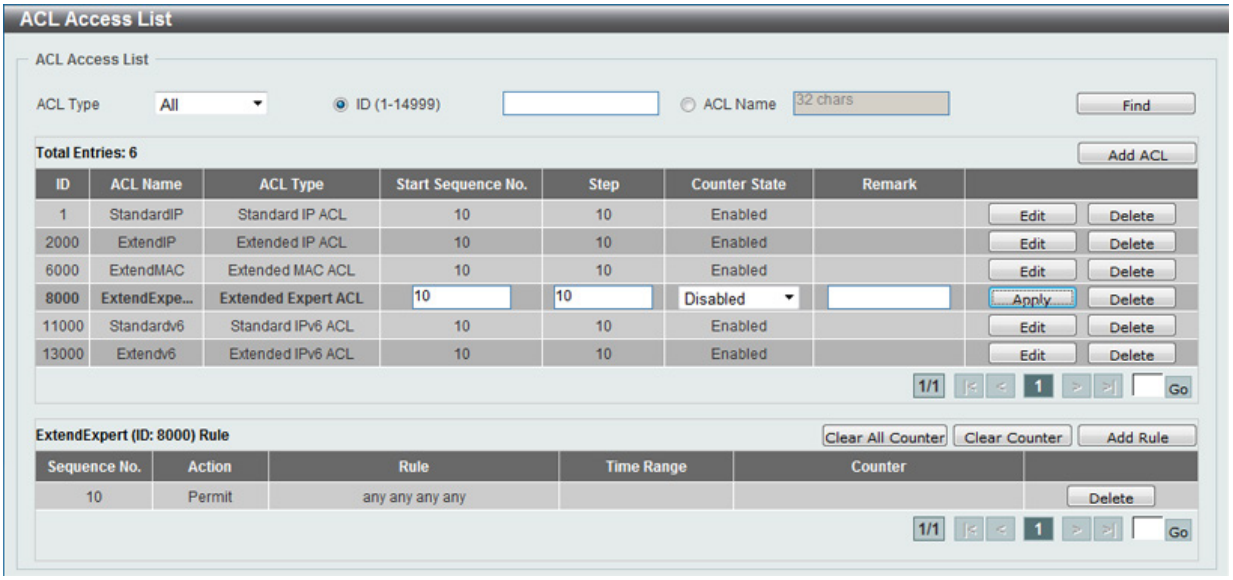


図 11-70　Extended Expert ACL (Edit ACL) 画面

画面に表示される項目

項目	説明
Start Sequence No.	シーケンス番号の開始番号を指定します。
Step	シーケンス番号の増加番号を指定します。
Counter State	カウンタ機能の有効 / 無効を指定します。
Remark	指定プロファイルと関連するリマークを入力します。

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

特定の ACL プロファイルに関連する ACL ルール表示するには「ACL Profile Table」で該当の ACL プロファイルを選択します。ACL ルールが表示されます。

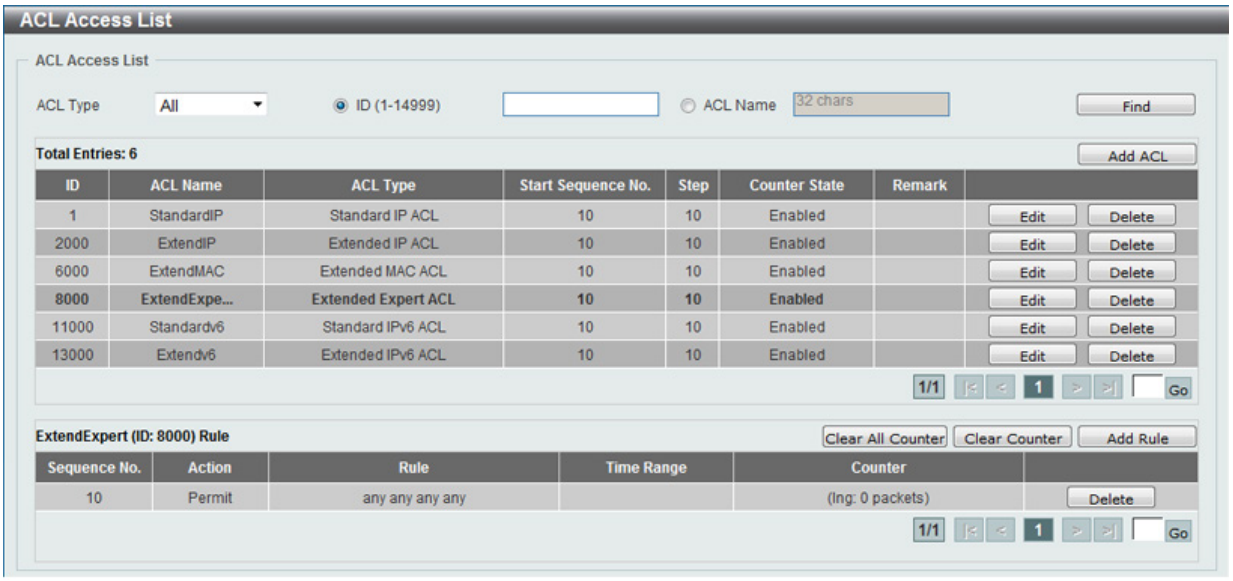


図 11-71　Extended Expert ACL (Rule Display) 画面

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

ACL Interface Access Group（ACL インタフェースアクセスグループ）

ACL インタフェースアクセスグループの設定、表示を行います。
ACL > ACL Interface Access Group の順にメニューをクリックし、以下の画面を表示します。

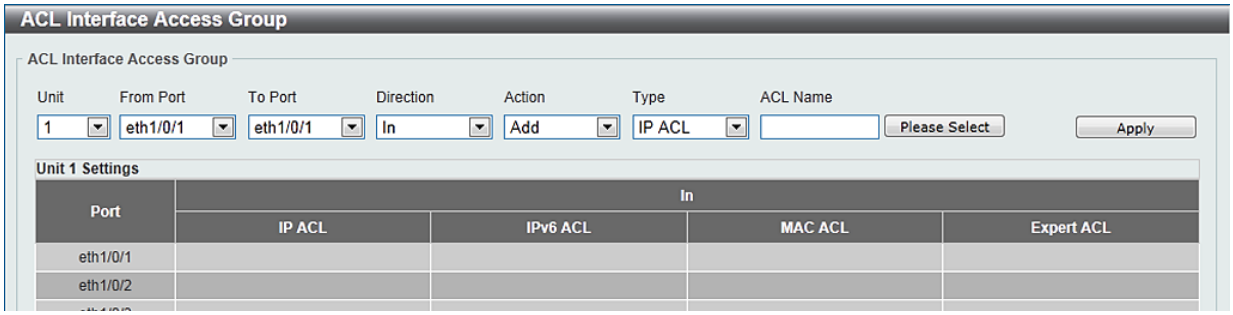


図 11-72　ACL Interface Access Group 画面

画面に表示される項目

項目	説明
Unit	設定するユニットを指定します。
From Port/To Port	設定の対象となるポートを指定します。
Direction	方向を指定します。「In」が選択可能です。
Action	ACL インタフェースアクセスグループの追加 / 削除をします。「Add」「Delete」から選択します。
Type	ACL の種類を選択します。「IP ACL」「IPv6 ACL」「MAC ACL」「Expert ACL」から選択します。
ACL Name	ACL 名を入力します。32 文字以内で入力できます。

「Please Select」ボタンをクリックし、作成した ACL プロファイルを選択します。
「Apply」ボタンをクリックして、設定を適用します。

ACL VLAN Access Map（ACL VLAN アクセスマップ）

ACL VLAN アクセスマップの設定、表示を行います。
ACL > ACL VLAN Access Map の順にメニューをクリックし、以下の画面を表示します。

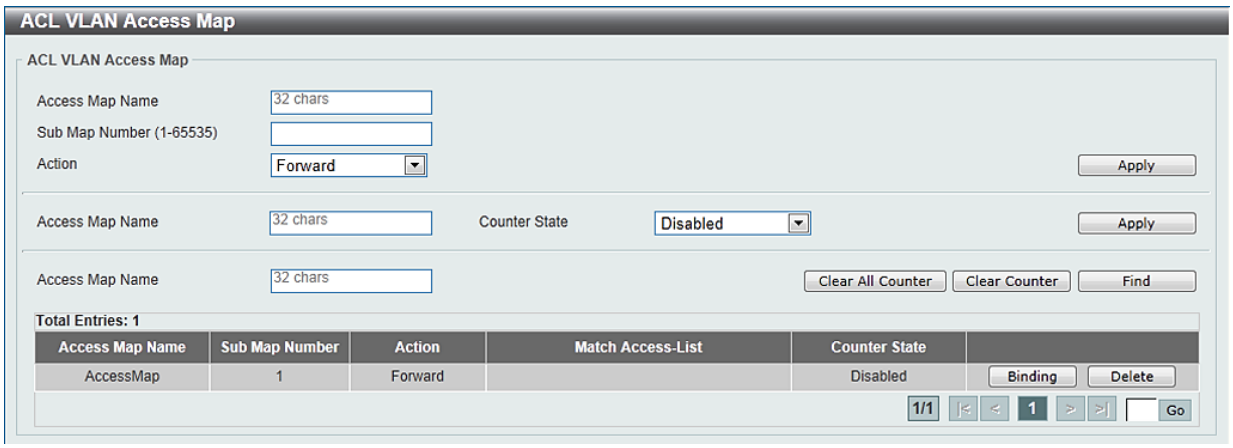


図 11-73　ACL VLAN Access Map 画面

画面に表示される項目

項目	説明
Access Map Name	アクセスマップ名を入力します。32 文字以内で入力できます。
Sub Map Number	サイトマップ番号を入力します。1 から 65535 までで指定できます。
Action	本項目の動作を指定します。「Forward」「Drop」「Redirect」から指定可能です。「Redirect」を選択すると、ドロップダウンリストからリダイレクトされるインタフェースを選択できます。
Counter State	カウンターの有効 / 無効を指定します。

「Apply」ボタンをクリックして、設定を適用します。
「Clear All Counter」ボタンをクリックし、表示されたすべてのカウンタ情報を消去します。
「Clear Counter」ボタンをクリックし、表示された指定ルールのカウンタ情報を消去します。
「Find」ボタンをクリックし、入力した情報を元に特定のエントリを指定します。
「Binding」ボタンをクリックし、新しく合致したアクセスリストを指定します。
「Delete」ボタンをクリックし、指定エントリを削除します。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

Match Access-List（合致するアクセスリスト設定）

「Binding」ボタンをクリックすると以下の画面が表示されます。

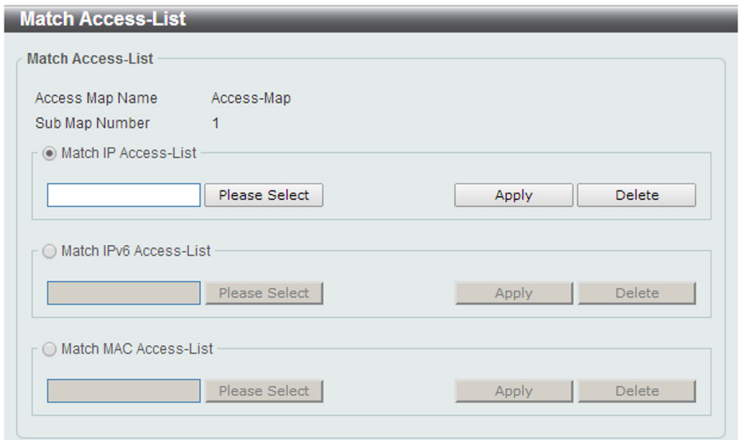


図 11-74　Match Access-List 画面

画面に表示される項目

項目	説明
Match IP Access-List	「Standard」（通常）または「Extended」（拡張）の IP ACL を選択します。
Match IPv6 Access-List	「Standard」（通常）または「Extended」（拡張）の IPv6 ACL を選択します。
Match MAC Access-List	「Standard」（通常）または「Extended」（拡張）の MAC ACL を選択します。

「Please Select」ボタンをクリックし、作成した ACL プロファイルを選択します。
「Apply」ボタンをクリックして、設定を適用します。
「Delete」ボタンをクリックし、指定エントリを削除します。

ACL VLAN Filter（ACL VLAN フィルタ設定）

ACL VLAN フィルタの設定、表示を行います。
ACL > ACL VLAN Filter の順にメニューをクリックし、以下の画面を表示します。



図 11-75　ACL VLAN Filter 画面

画面に表示される項目

項目	説明
Access Map Name	アクセスマップ名を入力します。32 文字以内で入力できます。
Action	ACL VLAN フィルタの追加 / 削除をします。「Add」「Delete」から選択します。
VID List	使用する VLAN ID リストを入力します。「All VLAN」を選択するとスイッチに設定されているすべての VLAN が対象となります。

「Apply」ボタンをクリックして、設定を適用します。
「Delete」ボタンをクリックし、指定エントリを削除します。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

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。
TACACS+（TACACS+ 設定）	TACACS+ の設定を行います。
IMPB（IP-MAC-Port Binding / IP-MAC- ポートバインディング）	IP-MAC 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。
BPDU Attack Protection（BPDU アタック防止設定）	BPDU アタック防止設定を行います。
MAC Authentication（MAC 認証）	MAC 認証の設定を行います。
Web-based Access Control（Web 認証）	Web 認証（WAC）の設定を行います。
Japanese Web-based Access Control（JWAC 設定）	JWAC 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）	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）	ストームコントロールの設定を行います。
DoS Attack Prevention Settings（DoS 攻撃防止設定）	DoS 攻撃防止設定を行います。
SSH（Secure Shell の設定）	SSH（Secure Shell）の設定を行います。
SSL（Secure Socket Layer）	SSL（Secure Socket Layer）の設定を行います。

Port Security（ポートセキュリティ）

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

本項目ではポートセキュリティ機能のグローバルでの設定 / 表示を行います。ポートセキュリティは、MAC アドレスのある不正 / 不可知なコンピュータからの、ロック済みポートへの接続とネットワークへのアクセスを防ぐセキュリティ機能です。

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

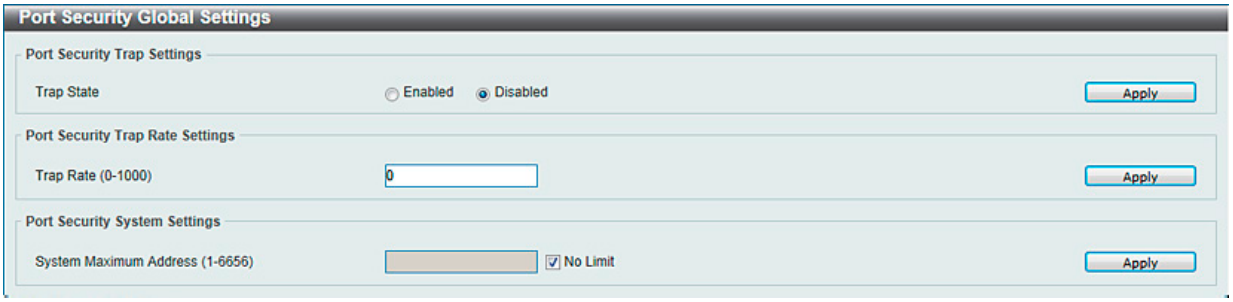


図 12-1　Port Security Global Settings 画面

本画面には以下の項目があります。

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

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

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

ポートセキュリティのポート設定と設定内容の表示を行います。

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

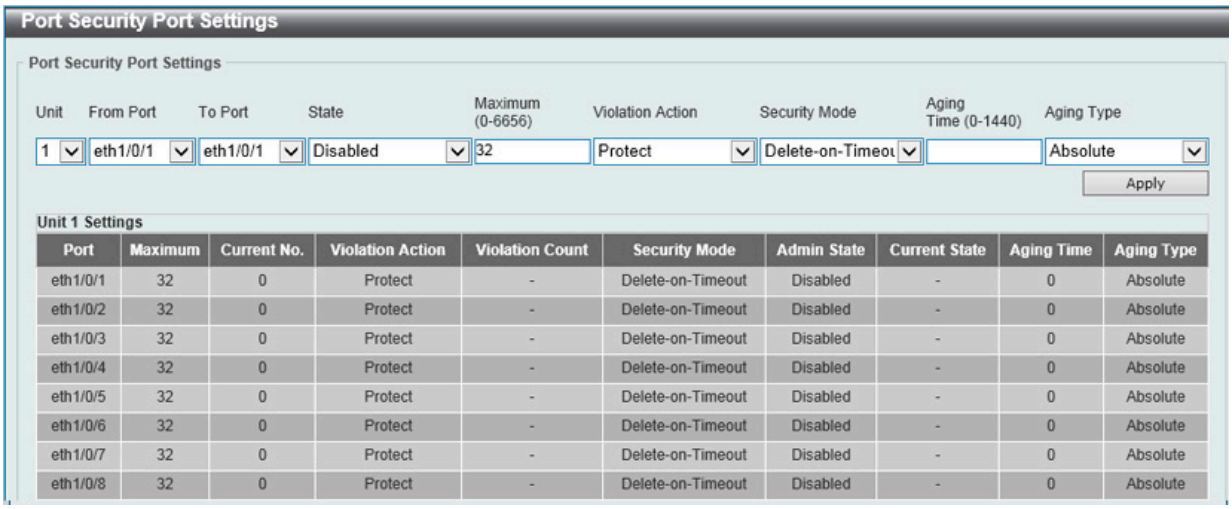


図 12-2　Port Security Port Settings 画面

本画面には以下の項目があります。

項目	説明
Unit	設定するユニットを指定します。
From Port/To Port	設定の対象となるポートを指定します。
State	指定ポートへのポートセキュリティ機能を有効 / 無効にします。
Maximum	指定ポートで許可される安全な MAC アドレスの最大数を指定します。0 から 6656 まで指定可能で初期値は 32 です。
Violation Action	違反に対する動作を指定します。「Protect」「Restrict」「Shutdown」から指定可能です。 「Protect」を選択すると、ポートセキュリティレベルで不正ホストからのパケットをすべて破棄しますが、セキュリティ違反カウントとしては数えられません。 「Restrict」を選択すると、ポートセキュリティレベルで不正ホストからのパケットをすべて破棄し、セキュリティ違反としてカウントされシステムログに記録されます。 「Shutdown」を選択すると、セキュリティ違反があるとポートをシャットダウンし、システムログに記録されます。
Security Mode	セキィリティモードを選択します。「Permanent」「Delete-on-Timeout」から選択可能です。「Permanent」を選択するとすべての学習した MAC アドレスは手動でエントリを削除しない限り削除されません。「Delete-on-Timeout」を選択するとすべての学習した MAC アドレスはタイムアウトにより自動的に削除されるか、手動でエントリを削除します。
Aging Time	指定ポートの自動取得アドレスに使用するエージングタイムです。0 から 1440 分の間で指定可能です。
Aging Type	エージングの種類を指定します。「Absolute」「Inactivity」から指定します。「Absolute」を指定するとポート上のすべてのアドレスは指定された時間を過ぎるとアドレスリストから削除されます。これが初期値です。「Inactivity」を指定すると指定の期間安全なアドレスからのトラフィックがない場合に限り、このポートのアドレスがエージアウトします。

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

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

ポートセキュリティアドレスエントリの設定、表示を行います。

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

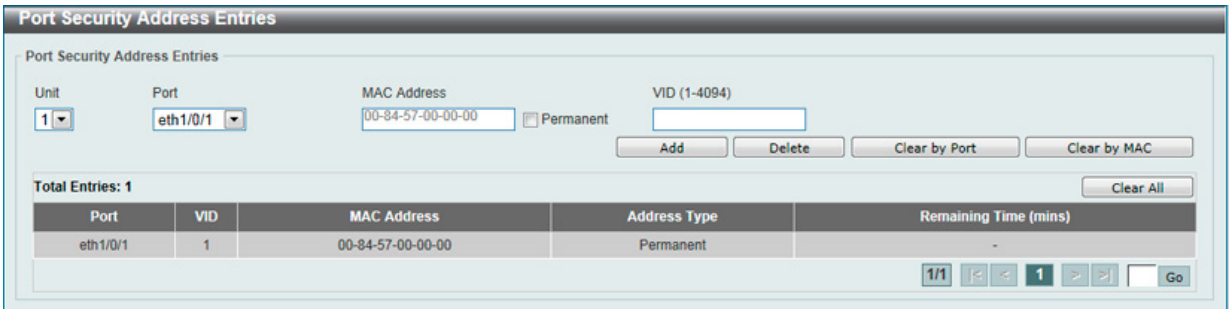


図 12-3　Port Security Address Entries 画面

本画面には以下の項目があります。

項目	説明
Unit	設定するユニットを指定します。
From Port/To Port	設定の対象となるポートを指定します。
MAC Address	MAC アドレスを入力します。 「Permanent」にチェックを入れると学習した MAC アドレスは、ユーザが手動で削除しない限り、削除されません。
VID	VLAN ID を指定します。1 から 4094 の間で指定できます。

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

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。

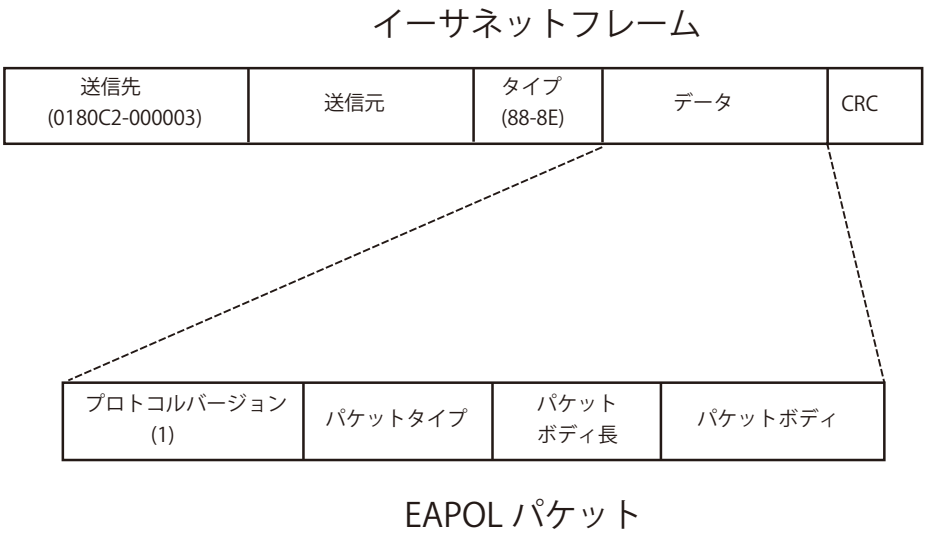


図 12-4　EAPOL パケット

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。

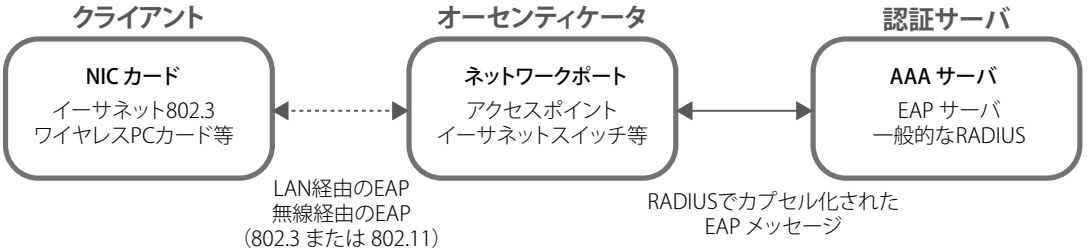


図 12-5　802.1X の 3 つの要素

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。

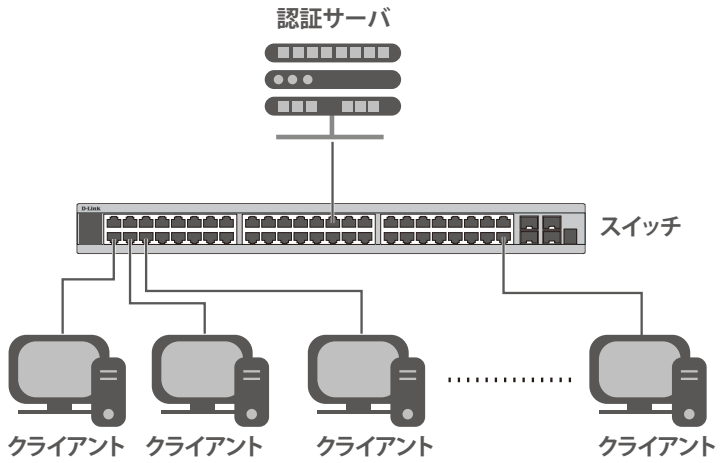


図 12-6　認証サーバ

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**）

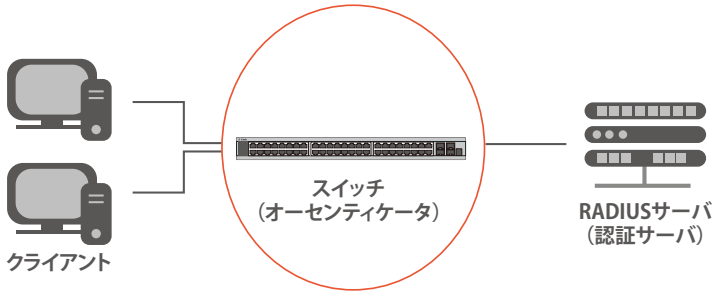


図 12-7　オーセンティケータ

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。

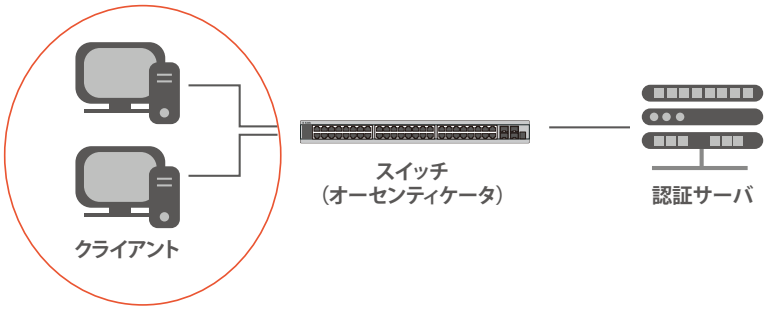


図 12-8　クライアント

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。

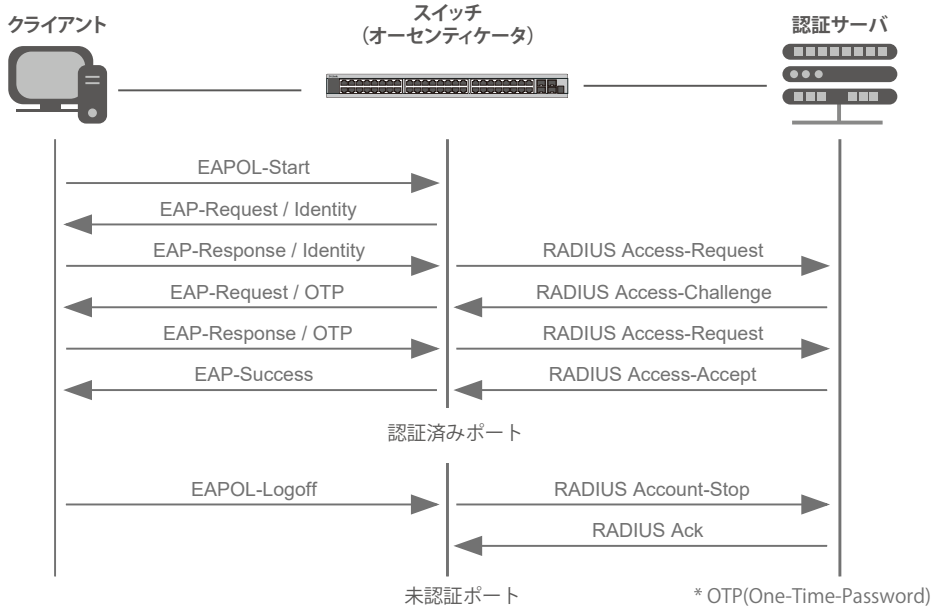


図 12-9　802.1X 認証プロセス

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。

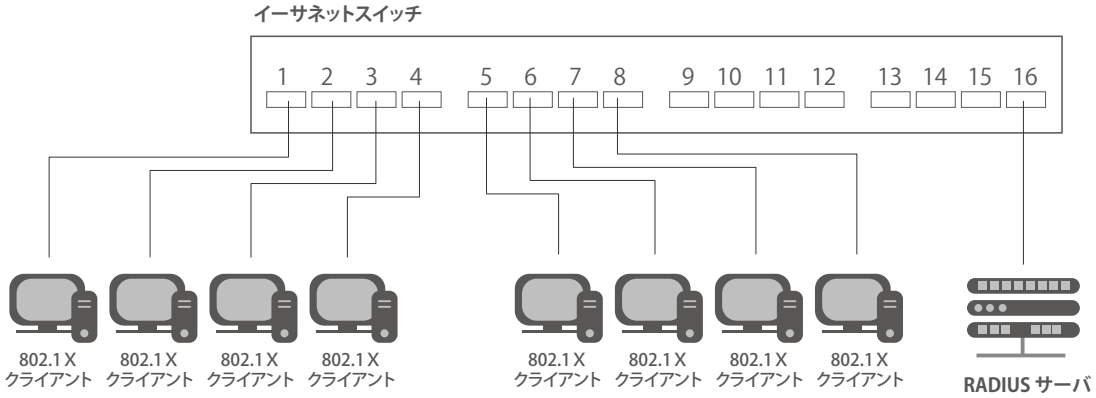


図 12-10　ポートベースアクセスコントロールのネットワーク構成例

■ 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。

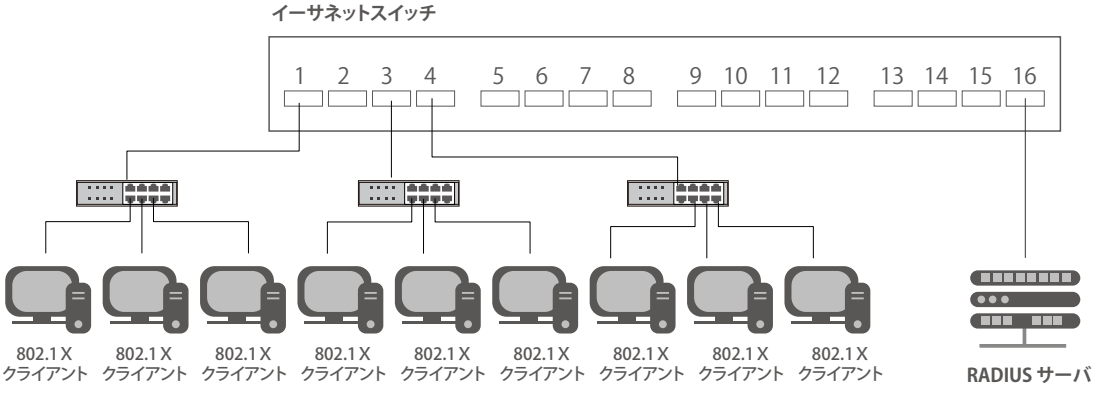


図 12-11　ホストベースアクセスコントロールのネットワーク構成例

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。

802.1X 認証設定をするには、**Security > 802.1X > 802.1X Global Settings** の順にメニューをクリックします。

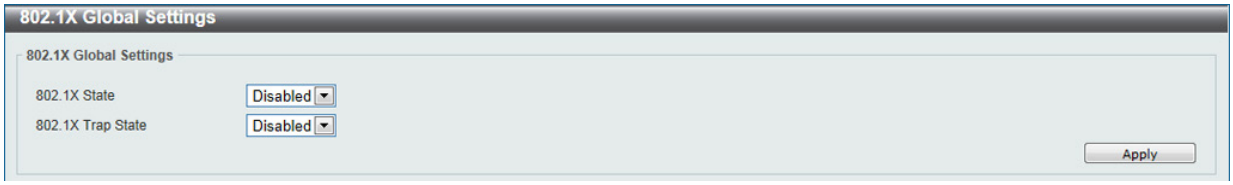


図 12-12　802.1X Global Settings 画面

この画面では以下の機能を設定できます。

項目	説明
802.1X State	802.1X 認証をグローバルに有効 / 無効に設定します。
802.1X Trap State	802.1X トラップを有効 / 無効に設定します。

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

802.1X Port Settings（802.1X ポート設定）

802.1X 認証ポートを設定します。

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

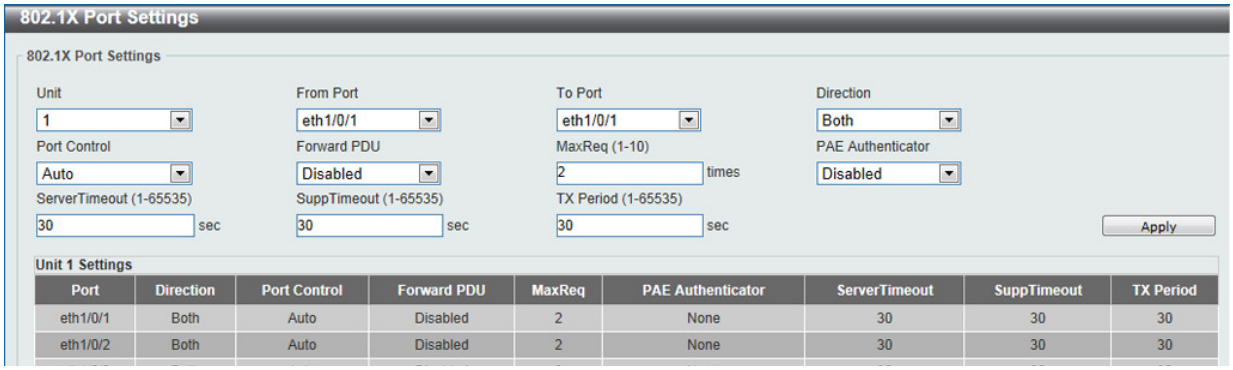


図 12-13　802.1X Settings 画面

この画面では以下の機能を設定できます。

項目	説明
Unit	設定するユニットを表示します。
From Port/To Port	設定対象のポート範囲を指定します。
Direction	制御するトラフィックの方向を指定します。初期値は「Both」です。 • In - 指定したポートへの入力トラフィックのみ制御対象となります。（ポートベースの認証時のみ有効です。） • Both - ポートが受信送信する両方向のトラフィックについて処理します。
Port Control	ポートの認証状態を指定します。 • ForceAuthorized - 802.1X を無効にします。この場合、ポートが認証状態になるのに、どのような認証の交換も必要ありません。つまり、ポートは 802.1X ベースの認証無しのトラフィックを送受信します。 • ForceUnauthorized - ポートは常に認証されていない状態になり、クライアントからの認証要求を無視します。スイッチはクライアントに対して認証サービスを提供しません。 • Auto - 802.1X を有効にし、ポートはまず、認証されていない EAPOL フレームだけを送受信できる状態になります。リンク状態が接続、切断と変化したり、EAPOL-start フレームを受け取ると認証プロセスが始まります。スイッチはクライアントの識別を要求し、クライアントと認証サーバ間の認証メッセージの中継を開始します。（初期値）
Forward PDU	PDU 要求の再送を有効 / 無効にします。
MaxReq (1-10)	認証プロセスを再開する前に、バックエンド認証ステートマシンが拡張認証プロトコル（EAP）要求フレームをサプリカントに再送信する最大回数を設定します。1 から 10 までの間で指定可能です。初期値は 2 です。
PAE Authenticator	PAE Authenticator を有効 / 無効に指定します。 本項目では特定ポートを IEEE 802.1X Port Access Entity（PAE）認証として指定します。
ServerTimeout (1-65535)	Authenticator と認証サーバの通信が切れてタイムアウト状態となる時間を指定します。初期値は 30（秒）です。
SuppTimeout (1-65535)	Authenticator とクライアントの通信が切れてタイムアウト状態となる時間を指定します。初期値は 30（秒）です。
TxPeriod (1-65535)	PAE を管理する Authenticator の TxPeriod の値を指定します。EAP Request/Identity パケットがクライアントに送信される間隔を決定します。初期値は 30（秒）です。

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

Authentication Session Information（オーセンティケーションセッションの状態）

オーセンティケーションセッションの状態を表示します。

Security > 802.1X > Authentication Session Information の順にメニューをクリックし、以下の画面を表示します。

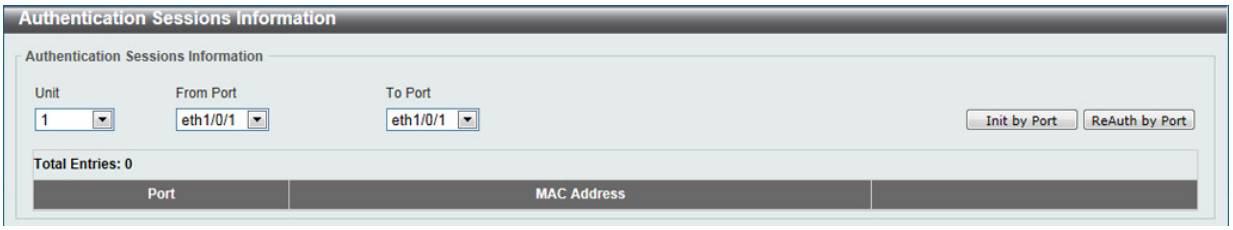


図 12-14　Authentication Session Information 画面

設定対象となる項目は以下の通りです。

項目	説明
Unit	設定するユニットを表示します。
From Port/To Port	設定対象のポート範囲を指定します。

「Init by Port」ボタンをクリックして、入力した情報に基づくセッション情報を起動します。
「ReAuth by Port」ボタンをクリックして、入力した情報に基づく再認証（Re-Authenticate）を行います。

Authenticator Statistics（オーセンティケータ統計情報）

オーセンティケータの統計情報を表示します。

Security > 802.1X > Authenticator Statistics の順にメニューをクリックし、以下の画面を表示します。

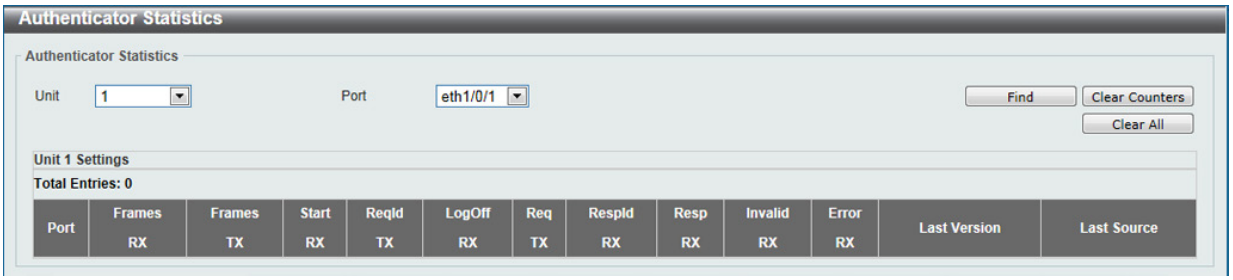


図 12-15　Authenticator Statics 画面

設定対象となる項目は以下の通りです。

項目	説明
Unit	表示するユニットを選択します。
Port	プルダウンメニューを使用して表示するポート範囲を指定します。

「Find」ボタンをクリックし、入力した情報に基づくエントリを検出します。
「Clear Counters」ボタンをクリックし、選択に基づく情報を消去します。
「Clear All」ボタンをクリックし、テーブル上のすべての情報を消去します。

Authenticator Session Statistics（オーセンティケータセッション統計情報）

オーセンティケータセッションの統計情報を表示します。

Security > 802.1X > Authenticator Session Statistics の順にメニューをクリックし、以下の画面を表示します。

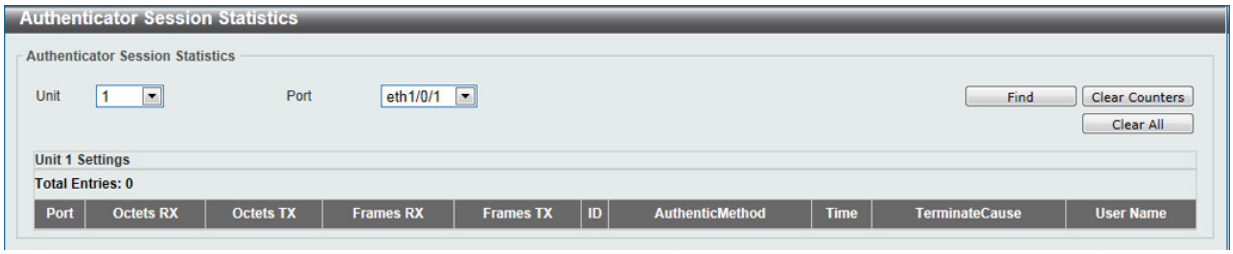


図 12-16　Authenticator Session Statistics 画面

設定対象となる項目は以下の通りです。

項目	説明
Unit	表示するユニットを選択します。
Port	プルダウンメニューを使用して表示するポート範囲を指定します。

「Find」ボタンをクリックし、入力した情報に基づくエントリを検出します。
「Clear Counters」ボタンをクリックし、選択に基づく情報を消去します。
「Clear All」ボタンをクリックし、テーブル上のすべての情報を消去します。

Authenticator Diagnostics（オーセンティケータ診断）

オーセンティケータ診断情報を表示します。

Security > 802.1X > Authenticator Diagnostics の順にメニューをクリックし、以下の画面を表示します。

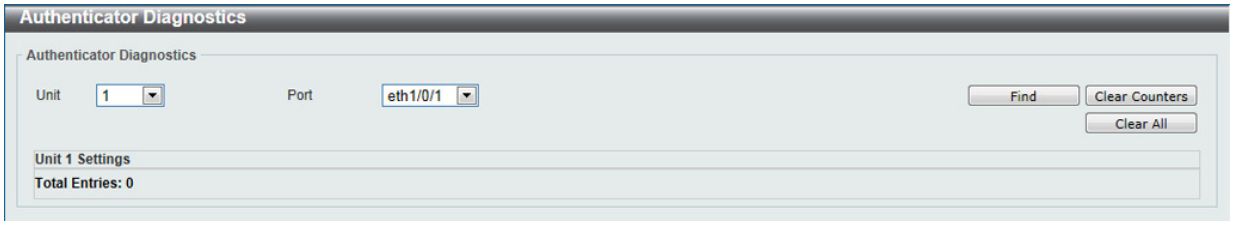


図 12-17　Authenticator Diagnostics 画面

設定対象となる項目は以下の通りです。

項目	説明
Unit	表示するユニットを選択します。
Port	プルダウンメニューを使用して表示するポート範囲を指定します。

「Find」ボタンをクリックし、入力した情報に基づくエントリを検出します。
「Clear Counters」ボタンをクリックし、選択に基づく情報を消去します。
「Clear All」ボタンをクリックし、テーブル上のすべての情報を消去します。

AAA（AAA 設定）

本項目では AAA（Authentication、Authorization、Accounting）の有効 / 無効を行います。

AAA Global Settings（AAA グローバル設定）

本項目では AAA をグローバルに有効 / 無効に設定します。

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

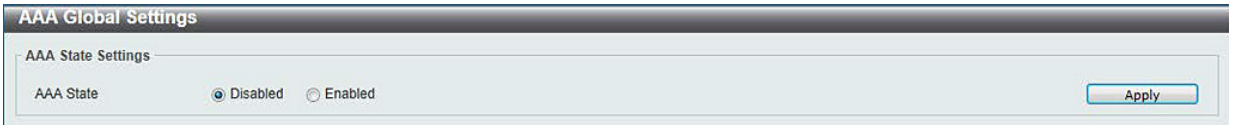


図 12-18　AAA Global Settings 画面

以下の項目を使用して、設定を行います。

項目	説明
AAA State	AAA をグローバルに「有効」(Eneable) /「無効」(Disable) に指定します。

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

Application Authentication Settings（アプリケーションの認証設定）

ログインする際に使用するスイッチの設定用アプリケーション（コンソール、Telnet、SSH、HTTP）を設定します。

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

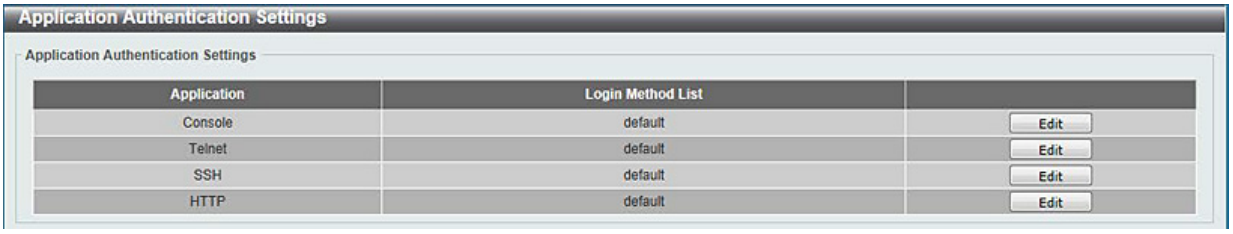


図 12-19　Application Authentication Settings 画面

以下の項目を使用して、設定を行います。

項目	説明
Login Method List	指定エントリの「Edit」ボタンをクリックし編集を行います。使用するログインメソッドリスト名を入力します。

指定エントリの「Edit」ボタンをクリックし編集を行います。
設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

Application Accounting Settings（アプリケーションアカウント設定）

アプリケーションアカウントを設定します。

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

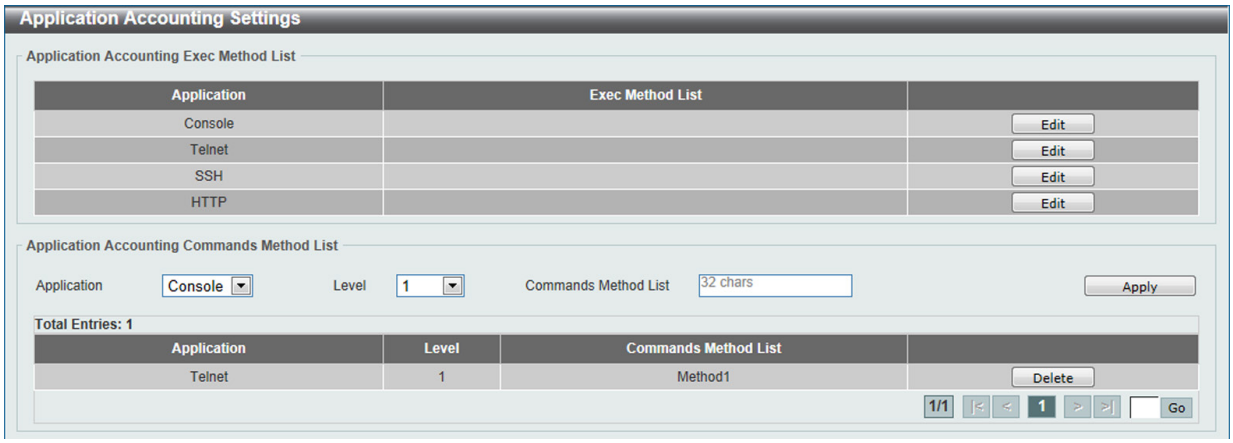


図 12-20　Application Accounting Settings 画面

以下の項目を使用して、設定を行います。

項目	説明
Exec Method List	指定エントリの「Edit」ボタンをクリックし編集を行います。使用する EXEC メソッドリスト名を入力します。
Application	使用するアプリケーションを選択します。「Console」「Telnet」「SSH」から選択します。
Level	権限レベルを指定します。1 から 15 の間で指定できます。
Commands Method List	使用するコマンドメソッドリスト名を入力します。

「Edit」をクリックして指定エントリの設定を行います。
「Delete」をクリックして指定エントリを削除します。
設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

Authentication Settings（認証設定）

AAA ネットワークと EXEC 認証設定を行います。

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

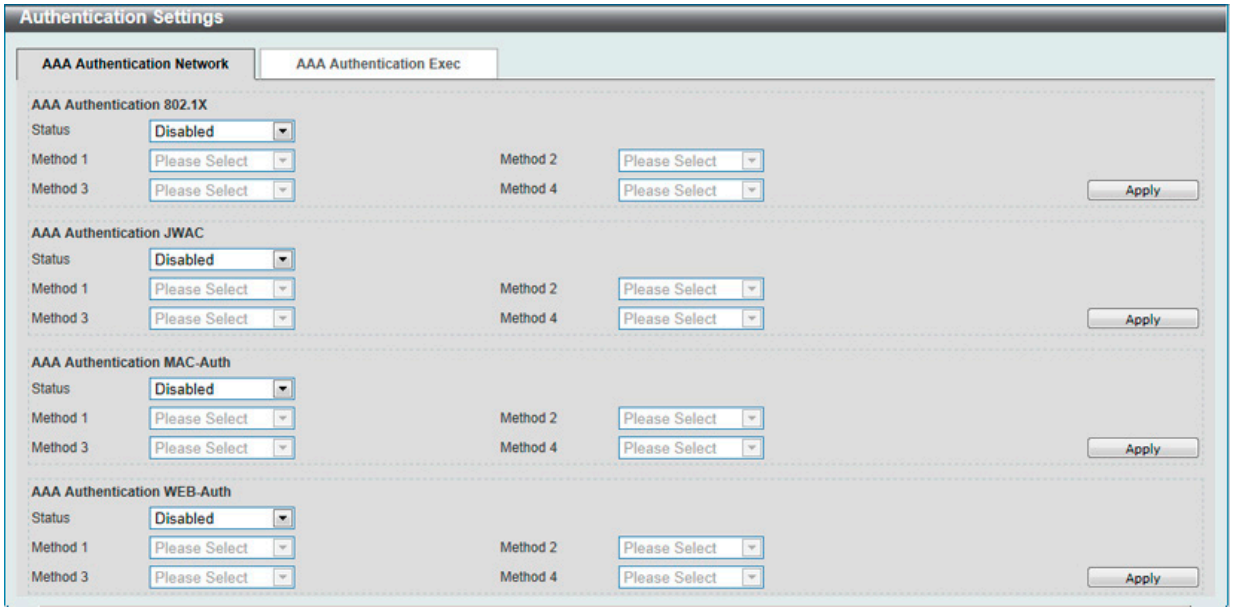


図 12-21　Authentication Settings -AAA Authentication Settings タブ画面

「AAA Authentication Network」タブ

「AAA Authentication Network」タブ内の設定を行います。
「AAA Authentication 802.1X」「AAA Authentication JWAC」「AAA Authentication MAC-Auth」「AAA Authentication WEB-Auth」それぞれの項目において設定を行います。

項目	説明
Status	各項目の認証設定の「有効」（Eneable）/「無効」（Disable）を設定します。
Method 1 to 4	本背亭項目のメソッドリストを選択します。「none」「local」「group」「radius」から選択します。

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

「AAA Authentication Exec」タブ

「AAA Authentication Exec」タブをクリックして、タブ内の設定を行います。

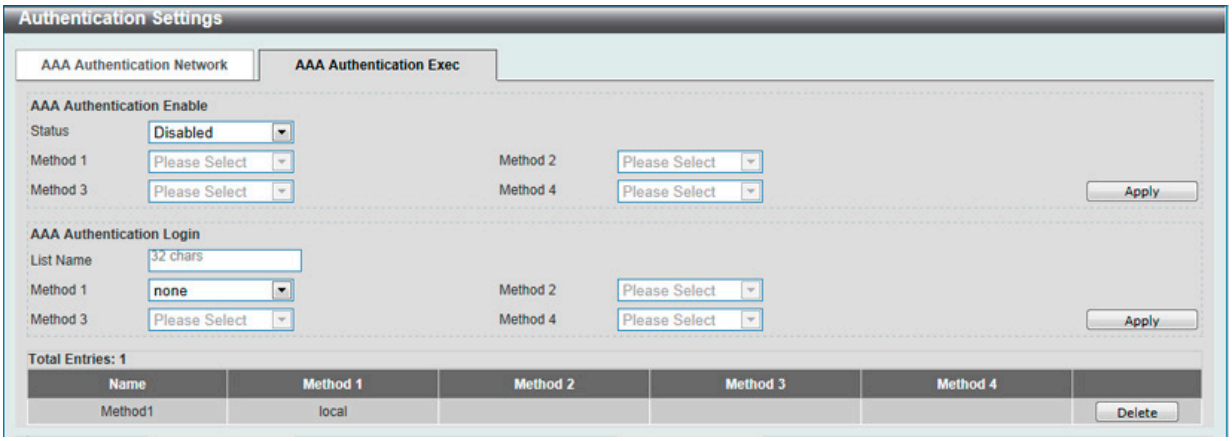


図 12-22　Authentication Settings -AAA Authentication Exec タブ画面

項目	説明
AAA Authentication Enable（AAA 認証有効）	
Status	AAA 認証設定の「有効」（Eneable）/「無効」（Disable）を設定します。
Method 1 to 4	本設定項目のメソッドリストを選択します。「none」「enable」「group」「radius」「TACACS+」から選択します。
AAA Authentication Login（AAA 認証ログイン）	
List Name	AAA 認証ログインオプションを使用するメソッドリスト名を入力します。
Status	AAA 認証設定の「有効」（Eneable）/「無効」（Disable）を設定します。
Method 1 to 4	使用するメソッドリストを選択します。「none」「enable」「group」「radius」「TACACS+」から選択します。

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

Accounting Settings（アカウンティング設定）

アカウンティングの設定を行います。

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

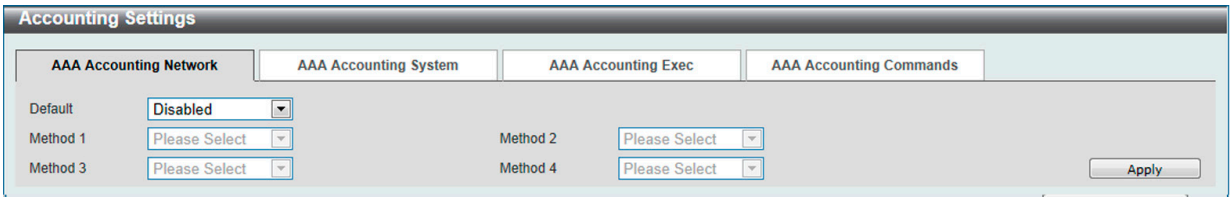


図 12-23　Accounting Settings 画面

「AAA Accounting Network」「AAA Accounting System」「AAA Accounting Exec」「AAA Accounting Commands」それぞれのタブにおいて設定を行います。

項目	説明
「AAA Accounting Network」タブ	
Default	メソッドリストの有効 / 無効を指定します。
Method 1 to 4	使用するメソッドリストを選択します。「none」「group」「radius」「TACACS+」から選択します。
「AAA Accounting System」タブ	
Default	メソッドリストの有効 / 無効を指定します。
Method 1 to 4	使用するメソッドリストを選択します。「none」「group」「radius」「TACACS+」から選択します。
「AAA Accounting Exec」タブ	
List Name	使用する AAA アカウンティング EXE オプションのメソッドリストを入力します。
Method 1 to 4	使用するメソッドリストを選択します。「none」「group」「radius」「TACACS+」から選択します。
「AAA Accounting Commands」タブ	
Level	権限レベルを指定します。1 から 15 までで指定可能です。
List Name	使用する AAA アカウンティングコマンドオプションのメソッドリストを入力します。
Method 1 to 4	使用するメソッドリストを選択します。「none」「group」「TACACS+」から選択します。

「Delete」をクリックして指定エントリを削除します。
設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

Server RADIUS Dynamic Author Settings（サーバ RADIUS Dynamic Author 設定）

RADIUS サーバの Dynamic Author 設定を行います。

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

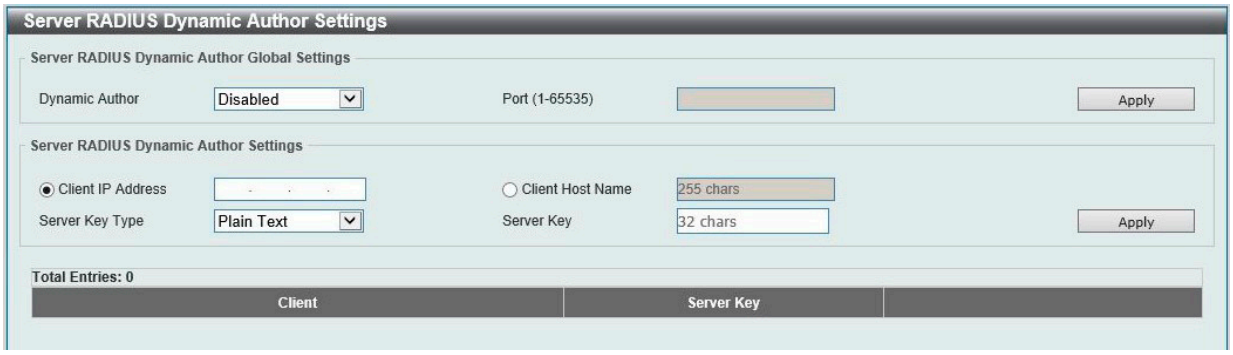


図 12-24　Server RADIUS Dynamic Author Settings 画面

この画面では以下の情報を確認、設定できます。

項目	説明
Server RADIUS Dynamic Author Global Settings	
Dynamic Author	Dynamic Author 機能の有効 / 無効を指定します。ダイナミック認証では、外部のポリシーサーバからデバイスに対する動的な更新の送信を行うことができます。
Port	更新パケットのデータ送信に使用されるポート番号を 1 から 65535 の範囲で指定します。
Server RADIUS Dynamic Author Settings	
Client IP Address	ラジオボタンを選択し、RADIUS クライアントの IP アドレスを入力します。
Client Host Name	ラジオボタンを選択し、RADIUS クライアントのホスト名を入力します。

項目	説明
Server Key Type	RADIUS サーバのキーの種類を選択します。 • Plain Text - 平文タイプのキーを使用します。 • Encrypted - 暗号化タイプのキーを使用します。
Server Key	キーの種類として「Plain Text」が選択されている場合、RADIUS サーバ通信に使用する平文のキーを入力します。32 文字までで入力可能です。キーの種類として「Encrypted」が選択されている場合、RADIUS サーバ通信に使用する暗号化されたキーを入力します。64 文字までで入力可能です。

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

RADIUS（RADIUS 設定）

RADIUS Global Settings（RADIUS グローバル設定）

RADIUS をグローバルに有効 / 無効にします。

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

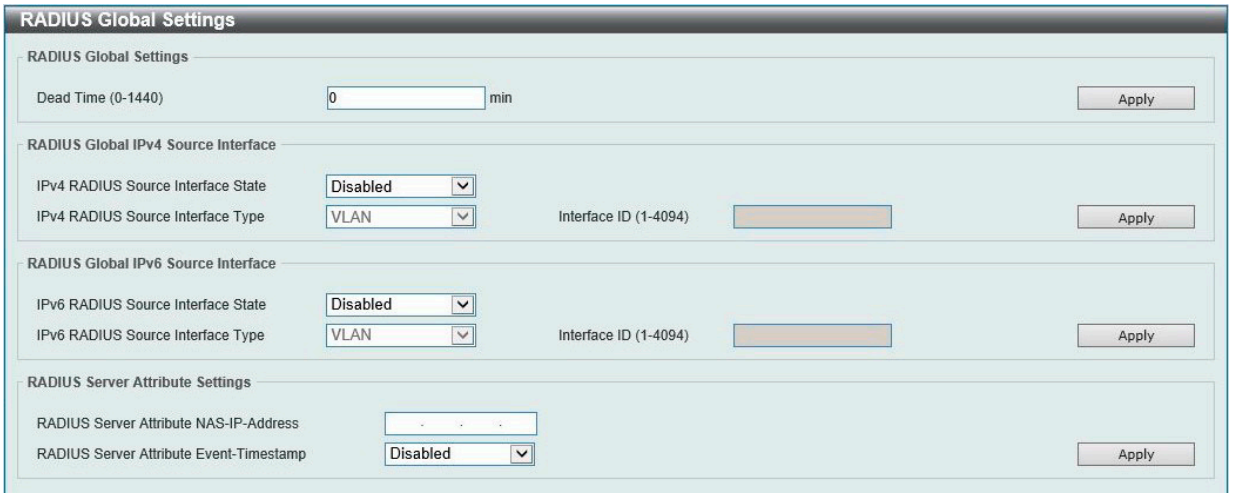


図 12-25　RADIUS Global Settings 画面

以下の項目を使用して、設定を行います。

項目	説明
RADIUS Global Settings	
DeadTime (0-1440)	デッドタイムの設定を行います。1 から 1440（分）の間で指定できます。初期値は「0」です。0 に設定されている場合、応答しないサーバは「Dead」として認識されることはありません。この設定により、応答しないサーバホストエントリをスキップする「デッドタイム」が設定され認証プロセスは改善されます。システムが認証サーバと連携して動作する場合、一度に一つのサーバと連携します。もし連携しようとしたサーバが応答しない場合、システムは次のサーバとの連携を模索します。システムにより応答しないサーバが見つけられると、該当のサーバは「down」として認識され、「デッドタイム」タイマーが開始され、それ以後のリクエスト認証はデッドタイム時間が過ぎるまでスキップされます。
RADIUS Global IPv4 Source Interface	
IPv4 RADIUS Source Interface State	IPv4 RADIUS ソースインタフェースの「有効」（Eneable）/「無効」（Disable）を設定します。
IPv4 RADIUS Source Interface Type	IPv4 RADIUS ソースインタフェースの種類を指定します。 • VLAN - IPv4 RADIUS ソースインタフェースの種類として VLAN を指定します。
Interface ID	VLAN インタフェース ID を 1 から 4094 の範囲で指定します。
RADIUS Global IPv6 Source Interface	
IPv6 RADIUS Source Interface State	IPv6 RADIUS ソースインタフェースの「有効」（Eneable）/「無効」（Disable）を設定します。
IPv6 RADIUS Source Interface Type	IPv6 RADIUS ソースインタフェースの種類を指定します。 • VLAN - IPv6 RADIUS ソースインタフェースの種類として VLAN を指定します。
Interface ID	VLAN インタフェース ID を 1 から 4094 の範囲で指定します。
RADIUS Server Attribute Settings	
RADIUS Server Attribute NAS-IP-Address	RADIUS パケットに含まれる RADIUS サーバアトリビュート 4 の IPv4 アドレスを入力します。

項目	説明
RADIUS Server Attribute Event-Timestamp	RADIUS サーバアトリビュート Event-Timestamp 機能の有効 / 無効を指定します。

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

RADIUS Server Settings（RADIUS サーバの設定）

外部 RADIUS サーバの設定を行います。

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

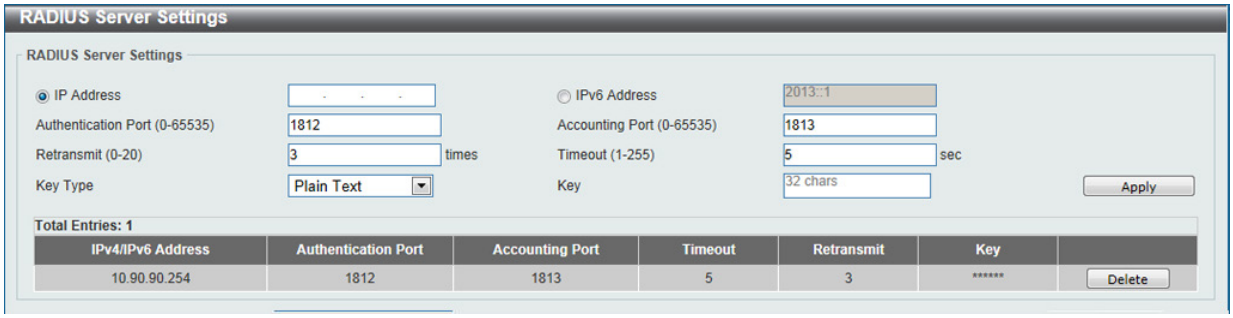


図 12-26　RADIUS Server Settings 画面

この画面では以下の情報を確認、設定できます。

項目	説明
IP Address	RADIUS サーバの IPv4 アドレスを入力します。
IPv6 Address	RADIUS サーバの IPv6 アドレスを入力します。
Authentication Port (0-65535)	RADIUS 認証サーバの UDP ポートです。初期値は 1812 です。認証しない場合は、0 を使用します。
Accounting Port (0-65535)	RADIUS アカウントサーバのポートです。初期値は 1813 です。アカウンティングを使用しない場合は、0 を使用します。
Retransmit (0-20)	RADIUS サーバの再転送間隔（秒）を設定します。初期値は 3（秒）です。
Timeout (1-255)	RADIUS サーバのタイムアウト時間（秒）を設定します。初期値は 5（秒）です。
Key Type	RADIUS サーバに設定する鍵の種類を選択します。「Plain Text」「Encrypted」から選択します。
Key	RADIUS サーバに設定したものと同一の鍵を指定します。32 文字以内で指定します。

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

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

RADIUS グループサーバの表示、設定を行います。

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

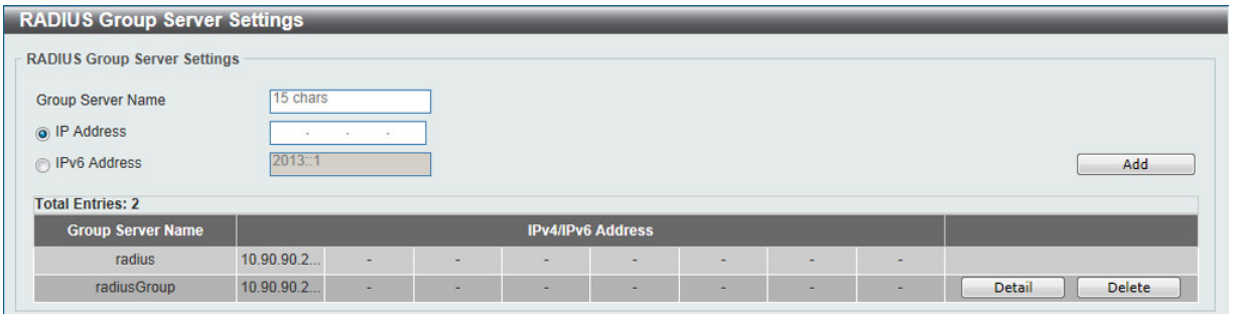


図 12-27　RADIUS Group Server Settings 画面

この画面では以下の情報を確認、設定できます。

項目	説明
Group Server Name	RADIUS グループサーバ名を入力します。15 文字までで指定可能です。
IP Address	RADIUS サーバの IPv4 アドレスを入力します。
IPv6 Address	RADIUS サーバの IPv6 アドレスを入力します。

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

RADIUS Group Server Settings - Detail（RADIUS グループサーバ詳細設定）

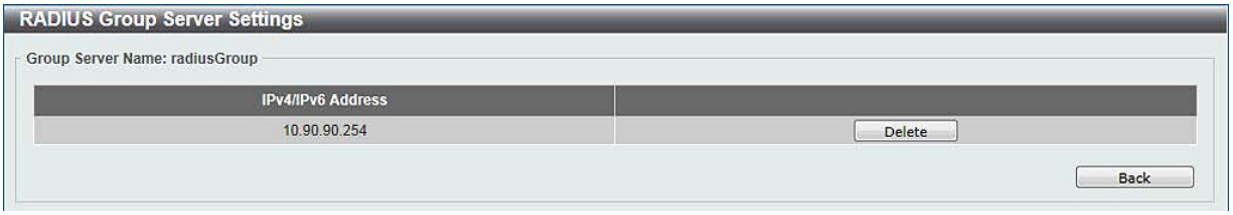


図 12-28　RADIUS Group Server Settings - Detail 画面

「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。

注意 IPv6 をご利用の環境において、Radius Server 間の認証に Stateless IPv6 Address を使用する場合があるため、Radius Server には Static IPv6 Address と Stateless IPv6 Address を登録する必要があります。

RADIUS Statistic（RADIUS 統計情報）

RADIUS 統計情報の表示、設定を行います。

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

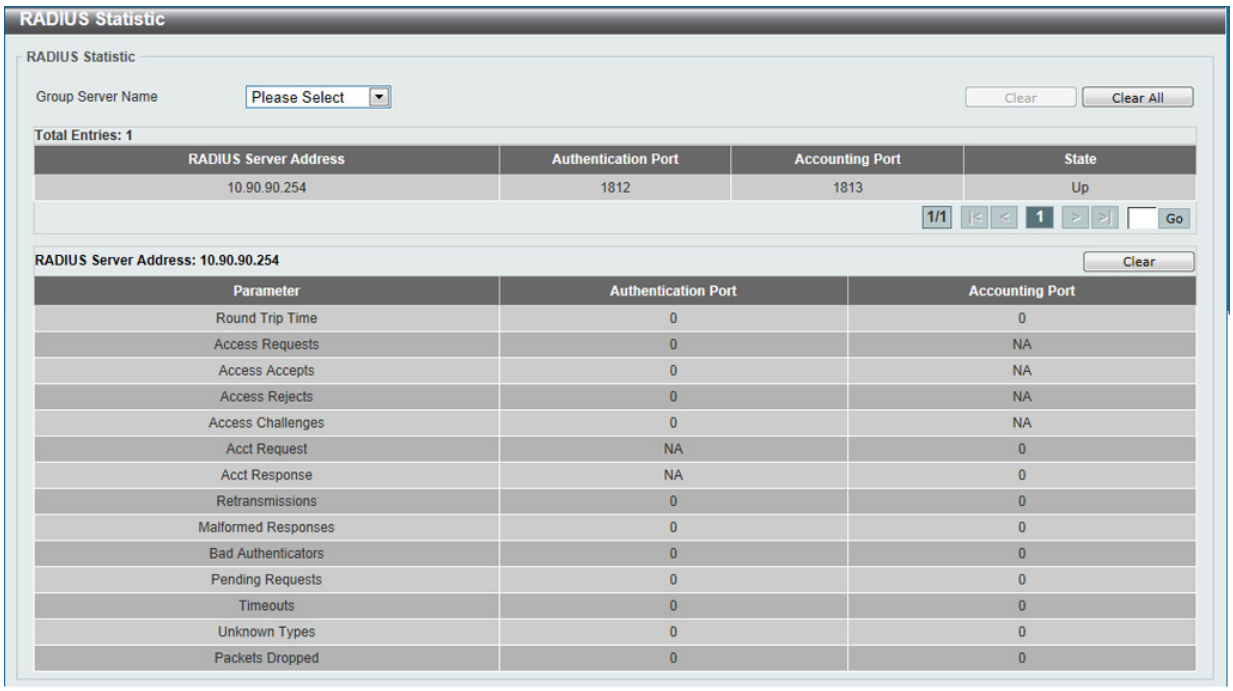


図 12-29　RADIUS Statistic 画面

この画面では以下の情報を確認、設定できます。

項目	説明
Group Server Name	表示する RADIUS グループサーバ名を選択します。

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。
「Clear」ボタンをクリックし、選択に基づいて表示した情報を消去します。
「Clear All」ボタンをクリックし、テーブル上のすべての情報を消去します。

TACACS+（TACACS+ 設定）

TACACS+ Global Settings（TACACS+ グローバル設定）

TACACS+ サーバのグローバル設定を行います。

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

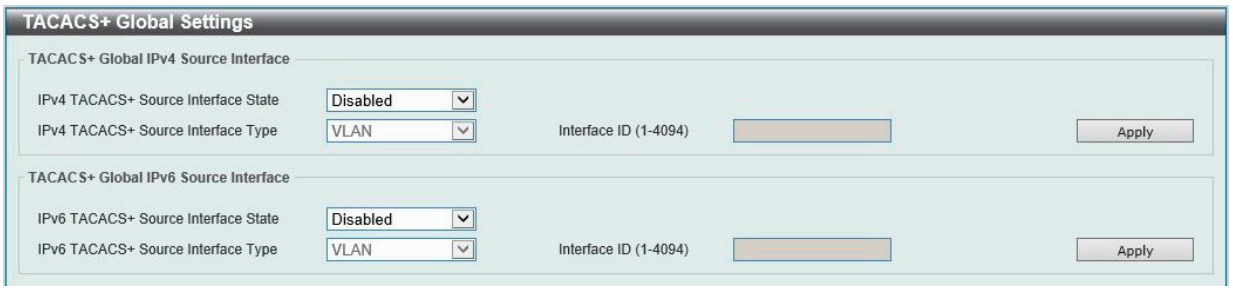


図 12-30　TACACS+ Global Settings 画面

以下の項目を使用して、設定を行います。

項目	説明
TACACS+ Global IPv4 Source Interface	
IPv4 TACACS+ Source Interface State	IPv4 TACACS+ ソースインタフェースの「有効」（Eneable）/「無効」（Disable）を設定します。
IPv4 TACACS+ Source Interface Type	IPv4 TACACS+ ソースインタフェースの種類を指定します。 • VLAN - IPv4 TACACS+ ソースインタフェースの種類として VLAN を指定します。
Interface ID	VLAN インタフェース ID を 1 から 4094 の範囲で指定します。
TACACS+ Global IPv6 Source Interface	
IPv6 TACACS+ Source Interface State	IPv6 TACACS+ ソースインタフェースの「有効」（Eneable）/「無効」（Disable）を設定します。
IPv6 TACACS+ Source Interface Type	IPv6 TACACS+ ソースインタフェースの種類を指定します。 • VLAN - IPv6 TACACS+ ソースインタフェースの種類として VLAN を指定します。
Interface ID	VLAN インタフェース ID を 1 から 4094 の範囲で指定します。

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

TACACS+ Server Settings（TACACS+ サーバの設定）

TACACS+ サーバの表示、設定を行います。

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



図 12-31　TACACS+ Server Settings 画面

この画面では以下の情報を確認、設定できます。

項目	説明
IP Address	TACACS+ サーバの IPv4 アドレスを入力します。
IPv6 Address	TACACS+ サーバの IPv6 アドレスを入力します。
Port (1-65535)	TACACS+ サーバのポートです。初期値は 49 です。
Timeout (1-255)	TACACS+ サーバのタイムアウト時間（秒）を設定します。初期値は 5（秒）です。
Key Type	TACACS+ サーバに設定する鍵の種類を選択します。「Plain Text」「Encrypted」から選択します。
Key	TACACS+ サーバに設定したものと同一の鍵を指定します。254 文字以内で指定します。

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

TACACS+ Group Server Settings（TACACS+ グループサーバの設定）

TACACS+ グループサーバの表示、設定を行います。

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

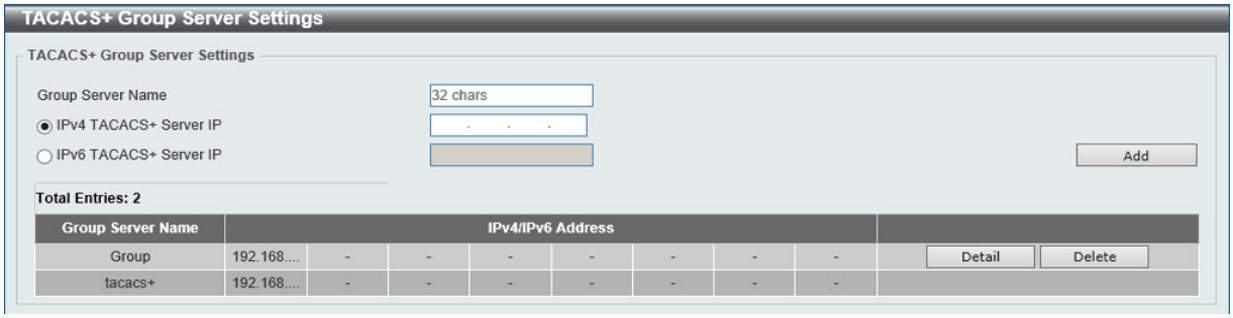


図 12-32　TACACS+ Group Server Settings 画面

この画面では以下の情報を確認、設定できます。

項目	説明
Group Server Name	TACACS+ グループサーバ名を入力します。15 文字までで指定可能です。
IPv4 TACACS+ Server IP	TACACS+ サーバの IPv4 アドレスを入力します。
IPv6 TACACS+ Server IP	TACACS+ サーバの IPv6 アドレスを入力します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Delete」をクリックして指定エントリを削除します。
「Detail」をクリックすると TACACS+ グループサーバの詳細情報について表示されます。

TACACS+ Group Server Settings - Detail（TACACS+ グループサーバ詳細設定）

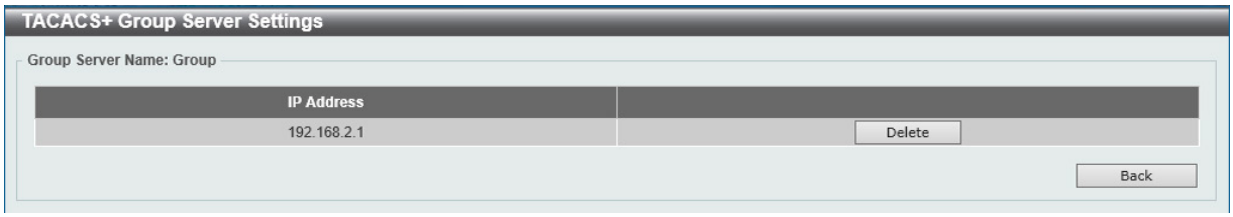


図 12-33　TACACS+ Group Server Settings - Detail 画面

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

TACACS+ Statistic（TACACS+ 統計情報）

TACACS+ 統計情報の表示、設定を行います。

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

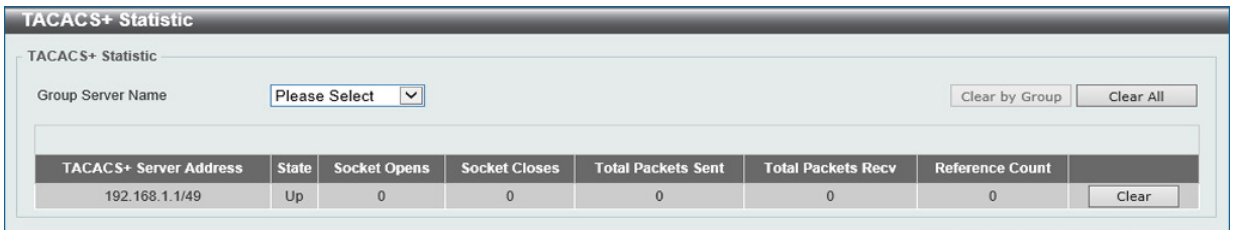


図 12-34　TACACS+ Statistic 画面

この画面では以下の情報を確認、設定できます。

項目	説明
Group Server Name	表示する TACACS+ グループサーバ名を選択します。

「Clear」ボタンをクリックし、選択に基づいて表示した情報を消去します。
「Clear by Group」ボタンをクリックし、選択したグループのすべての情報を消去します。
「Clear All」ボタンをクリックし、テーブル上のすべての情報を消去します。

IMPB（IP-MAC-Port Binding / IP-MAC- ポートバインディング）

IP ネットワークレイヤ（IP レベル）では 4 バイトのアドレスを使用し、イーサネットリンクレイヤ（データリンクレベル）では 6 バイトの MAC アドレスを使用します。これらの 2 つのアドレスタイプを結合させることにより、レイヤ間のデータ転送を可能にします。IP-MAC バインディングの第一の目的は、スイッチにアクセスするユーザ数を制限することです。IP アドレスと MAC アドレスのペアを、事前に設定したデータベースと比較を行い、認証クライアントのみがスイッチのポートアクセスできるようにします。もしくは DHCP スヌーピングが有効な場合において、スイッチがスヌーピング DHCP パケットから自動的に IP/MAC ペアを学習し、IMPB ホワイトリストに保存することで、認証クライアントのポートアクセスが可能になります。未認証ユーザが IP-MAC バインディングが有効なポートにアクセスしようとすると、システムはアクセスをブロックして、パケットを廃棄します。本機能はポートベースであるため、ポートごとに本機能を有効 / 無効にすることができます。

IPv4

DHCPv4 Snooping（DHCPv4 スヌーピング）

DHCP Snooping Global Settings（DHCP スヌーピンググローバル設定）

DHCP スヌーピンググローバル設定を表示、設定します。

Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping Global Settings の順にクリックして、以下の画面を表示します。



図 12-35　DHCP Snooping Global Settings 画面

本画面には以下の項目があります。

項目	説明
DHCP Snooping	DHCP スヌーピングをグローバルに「Enabled」（有効）または「Disabled」（無効）にします。
Information Option Allow Untrusted	アントラストインタフェースのリレーオプション 82 付き DHCP パケットをグローバルに「Enabled」（有効）または「Disabled」（無効）にします。
Source MAC Verification	クライアントのハードウェアアドレスと DHCP パケットの送信元 MAC アドレスの合致確認を「Enabled」（有効）または「Disabled」（無効）にします。
Station Move Deny	DHCP スヌーピングステーションムーブを有効 / 無効にします。 有効の場合、指定ポートにある同じ VLAN ID と MAC アドレスを持つダイナミック DHCP スヌーピングバインディングエントリは、新しい DHCP プロセスが同じ VLAN ID と MAC アドレスに属している事を検出した場合、他のポートへ移動することが可能です。

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

DHCP Snooping Port Settings（DHCP スヌーピングポート設定）

DHCP スヌーピングポートの表示、設定を行います。

Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping Port Settings の順にクリックして、以下の画面を表示します。

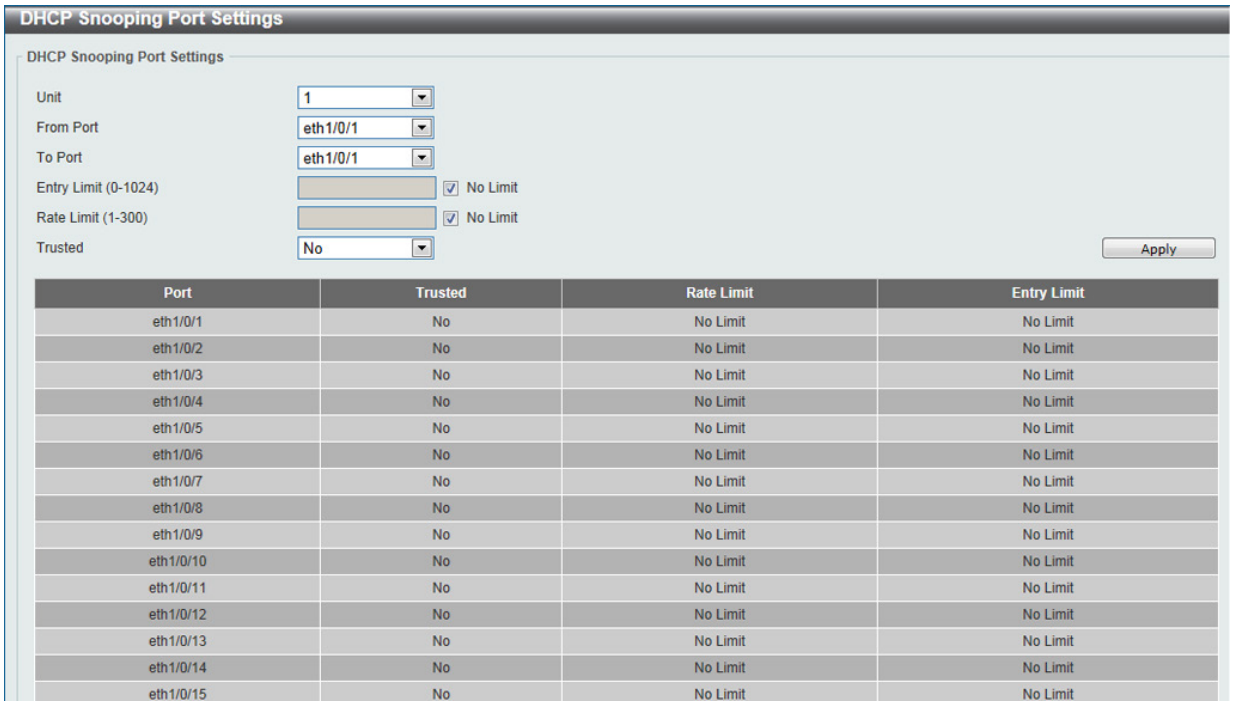


図 12-36　DHCP Snooping Port Settings 画面

本画面には以下の項目があります。

項目	説明
Unit	設定するユニットを表示します。
From Port/To Port	設定対象のポート範囲を指定します。
Entry Limit	エントリリミットの値を入力します。0 から 1024 の間で入力可能です。「No Limit」にチェックをすると、本機能は無効になります。
Rate Limit	レートリミットの値を入力します。1 から 300 の間で入力可能です。「No Limit」にチェックをすると、本機能は無効になります。
Trusted	トラストのオプションを選択します。「No」または「Yes」から選択します。DHCP サーバや他のスイッチなどに接続しているポートはトラストインタフェースとして設定される必要があります。DHCP クライアントに接続しているポートはアントラストとして設定します。DHCP スヌーピングは DHCP サーバとアントラストインタフェースの間でファイアウォールとして動作します。

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

DHCP Snooping VLAN Settings（DHCP スヌーピング VLAN 設定）

DHCP スヌーピング VLAN の設定、表示を行います。

Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping VLAN Settings の順にクリックして、以下の画面を表示します。

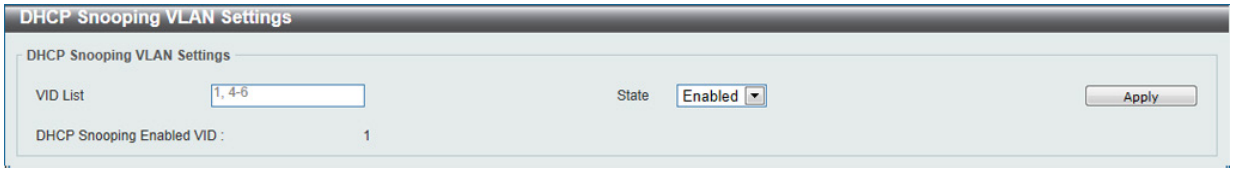


図 12-37　DHCP Snooping VLAN Settings 画面

本画面には以下の項目があります。

項目	説明
VID List	設定する VLAN ID リストを入力します。
State	DHCP スヌーピング VLAN を有効 / 無効に指定します。

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

DHCP Snooping Database（DHCP スヌーピングデータベース）

DHCP スヌーピングデータベースの表示、設定を行います。

Security > IMPB > IPv4 > DHCPv4 Snooping > DHCP Snooping Database の順にクリックして、以下の画面を表示します。

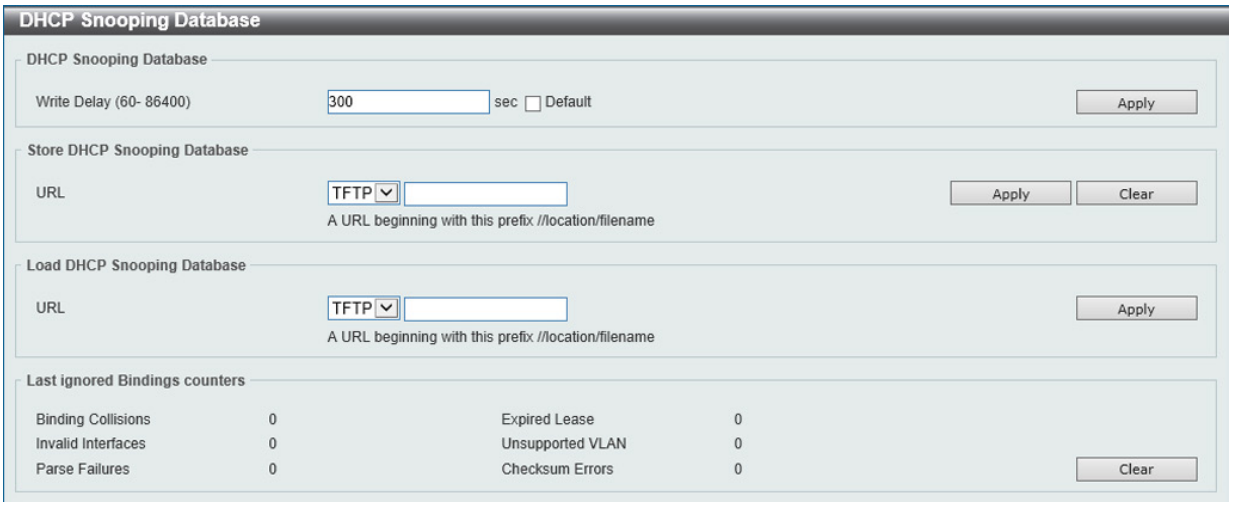


図 12-38　DHCP Snooping Database 画面

本画面には以下の項目があります。

項目	説明
DHCP Snooping Database	
Write Delay	書き込み遅延の値を入力します。60 から 86400（秒）の間で指定できます。初期値は 300 秒です。 「Apply」ボタンをクリックし、設定内容を適用してください。
Store DHCP Snooping Database	
URL	ロケーションをドロップダウンメニューから選択し、DHCP スヌーピングデータベースが保存される URL を入力します。選択できるロケーションは TFTP です。
Load DHCP Snooping Database	
URL	ロケーションをドロップダウンメニューから選択し、DHCP スヌーピングデータベースを起動する URL を入力します。選択できるロケーションは TFTP です。

「Apply」ボタンをクリックし、設定内容を適用してください。
「Clear」ボタンをクリックするとカウンタ情報が消去されます。

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。

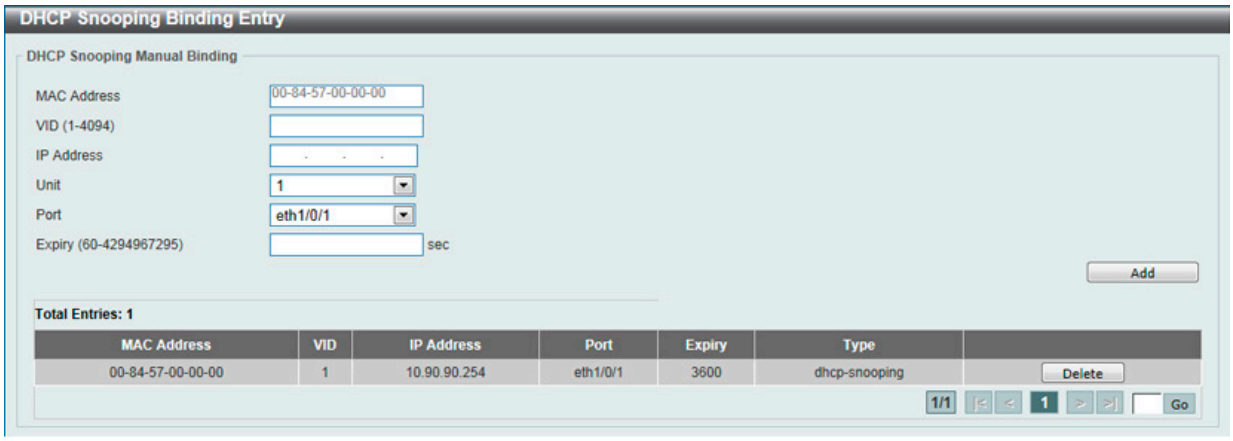


図 12-39　DHCP Snooping Binding Entry 画面

本画面には以下の項目があります。

項目	説明
MAC Address	DHCP スヌーピングバインディングエントリの MAC アドレスを入力します。
VID	DHCP スヌーピングバインディングエントリの VLAN ID を入力します。1 から 4094 の間で入力可能です。
IP Address	DHCP スヌーピングバインディングエントリの IP アドレスを入力します。
Unit	設定するユニットを指定します。
Port	設定するポートを指定します。
Expiry	有効期限を入力します。60 から 4294967295（秒）で指定可能です。

「Add」をクリックして入力した情報を元に新しいエントリを追加します。
「Delete」をクリックして指定エントリを削除します。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

Dynamic ARP Inspection（ダイナミック ARP インスペクション）

ARP Access List（ARP アクセスリスト）

ARP アクセスリストの設定、表示を行います。

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

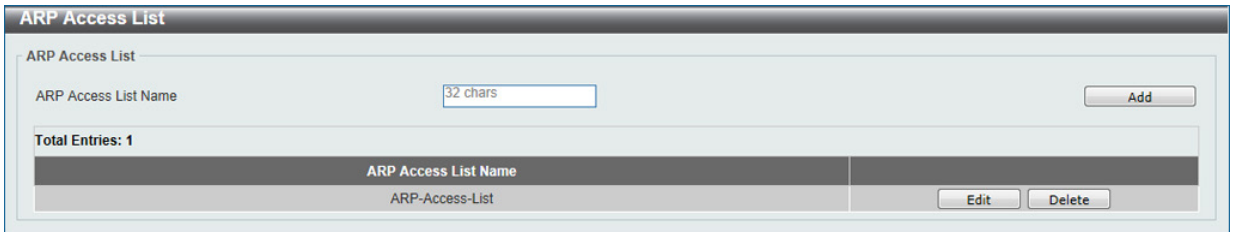


図 12-40　ARP Access List 画面

本画面には以下の項目があります。

項目	説明
ARP Access List Name	ARP アクセスリスト名を入力します。32 文字まで入力可能です。

「Add」をクリックして入力した情報を元に新しいエントリを追加します。
「Delete」をクリックして指定エントリを削除します。

エントリの編集

「Edit」ボタンをクリックして指定のエントリを編集します。以下の画面が表示されます。

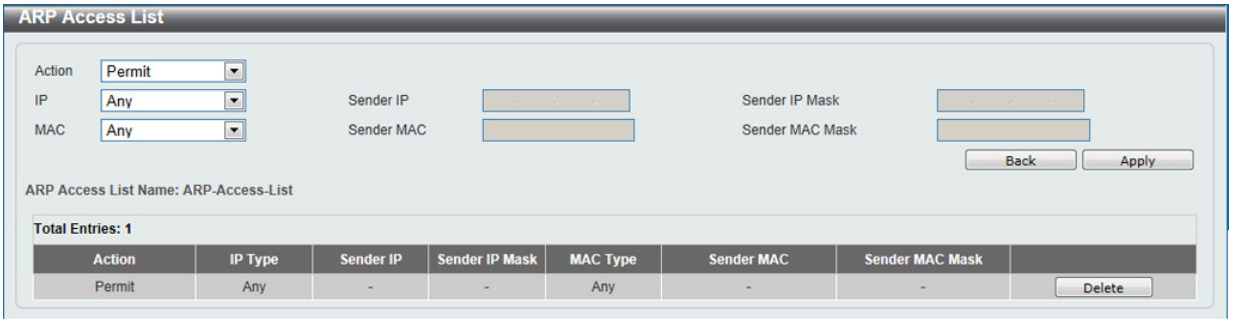


図 12-41　ARP Access List - Edit 画面

本画面には以下の項目があります。

項目	説明
Action	動作について指定します。「Permit」「Deny」から選択します。
IP	使用する送信者の IP アドレスの種類を指定します。「Any」「Host」「IP with Mask」から指定します。
Sender IP	送信者の IP アドレスを「Host」「IP with Mask」から選択した後、使用する送信者の IP アドレスを入力します。
Sender IP Mask	「IP with Mask」を選択した場合、使用する送信者の IP マスクを入力します。
MAC	送信者の MAC アドレスの種類を指定します。「Any」「Host」「MAC with Mask」から指定します。
Sender MAC	送信者の MAC アドレスを「Host」「MAC with Mask」から選択した後、使用する送信者の MAC アドレスを入力します。
Sender MAC Mask	「MAC with Mask」を選択した場合、使用する送信者の MAC マスクを入力します。

「Back」をクリックして前のページに戻ります。

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

「Delete」をクリックして指定エントリを削除します。

ARP Inspection Settings（ARP インスペクション設定）

ARP インスペクションの設定、表示を行います。

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

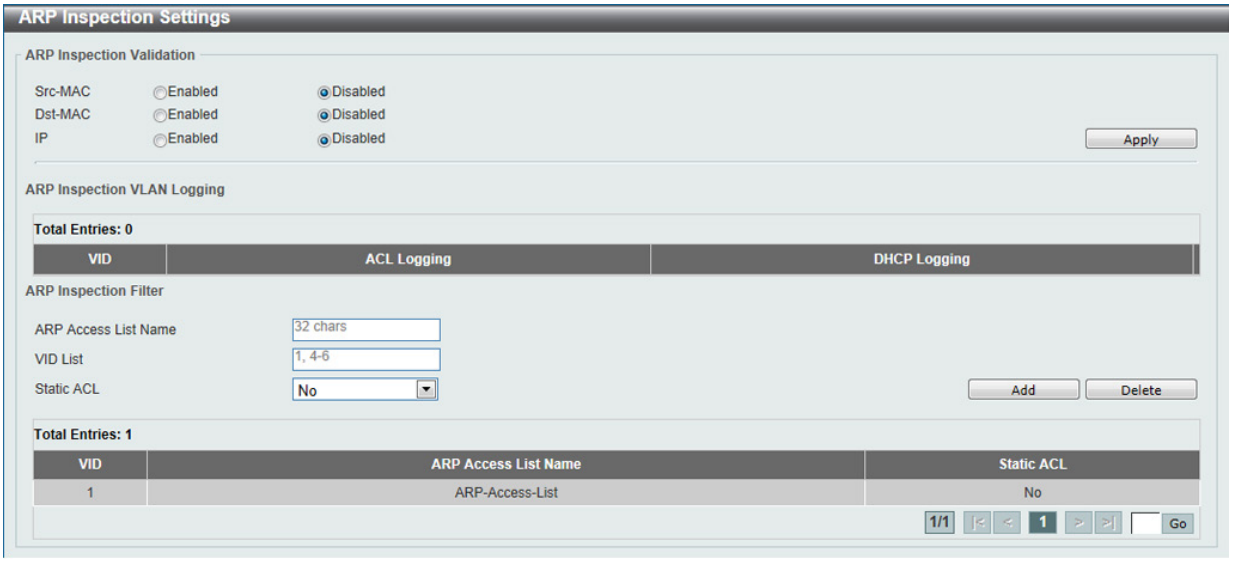


図 12-42　ARP Inspection Settings 画面

本画面には以下の項目があります。

項目	説明
Src-MAC	送信元 MAC のオプションについて有効 / 無効に設定します。本オプションを有効にすると ARP 要求と応答パケット、およびイーサネットヘッダー内の送信元 MAC アドレスと ARP ペイロード内の送信側 MAC アドレスとの整合性をチェックします。
Dst-MAC	宛先 MAC のオプションについて有効 / 無効に設定します。本オプションを有効にすると ARP 応答パケットと、イーサネットヘッダー内の宛先 MAC アドレスと ARP ペイロード内のターゲット MAC アドレスとの整合性をチェックします。
IP	IP のオプションについて有効 / 無効に設定します。本オプションを有効にすると不正や予期せぬ IP アドレスの ARP 本体をチェックします。本オプションはまた ARP ペイロードにおける IP アドレスの妥当性もチェックします。ARP リクエストとレスポンスの両方の送信元 IP および ARP レスポンスのターゲット IP の妥当性を確認します。IP アドレス「0.0.0.0」「255.255.255.255」に向かうパケットとすべての IP マルチキャスト当てのパケットは、破棄されます。送信者 IP アドレスはすべての ARP リクエストとレスポンスでチェックされ、宛先 IP アドレスは ARP レスポンス内のみでチェックされます。

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

本画面の「ARP Inspection Filter」には以下の項目があります。

項目	説明
ARP Access List Name	ARP アクセスリスト名を入力します。32 文字まで入力可能です。
VID List	使用する VLAN ID リストを指定します。
Static ACL	スタティック ACL を使用する（Yes）か否か（No）を選択します。

「Add」をクリックして入力した情報を元に新しいエントリを追加します。
「Delete」をクリックして指定エントリを削除します。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

ARP Inspection Port Settings（ARP インスペクションポート設定）

ポートでの ARP インスペクションの設定、表示を行います。

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

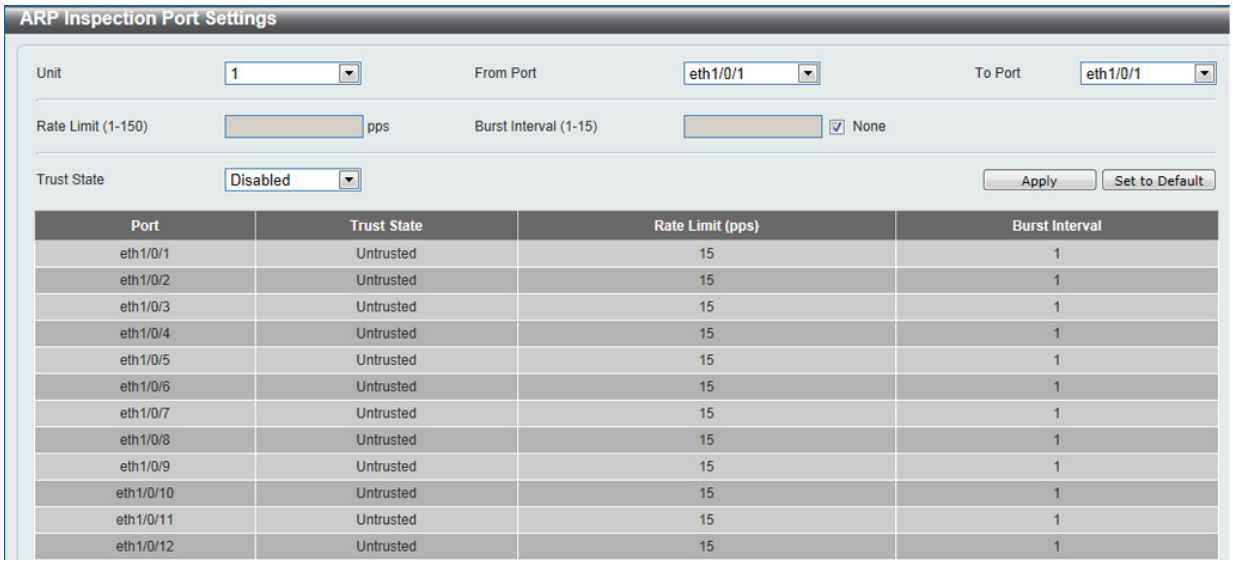


図 12-43　ARP Inspection Port Settings 画面

本画面には以下の項目があります。

項目	説明
Unit	設定するユニットを指定します。
From Port/ To Port	選択したポートから連続した複数のポートを設定できます。
Rate Limit	レート制限の値を入力します。1 から 150（パケット / 秒）の間で設定します。
Burst Interval	バーストインターバルの値を入力します。1 から 15 の間で設定します。「None」にチェックをするとオプションは無効になります。
Trust State	トラスト状態について有効 / 無効にします。

「Apply」ボタンをクリックし、設定内容を適用してください。
「Set to Default」ボタンをクリックすると、設定内容は初期値に変更します。

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

VLAN での ARP インスペクションの設定、表示を行います。

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

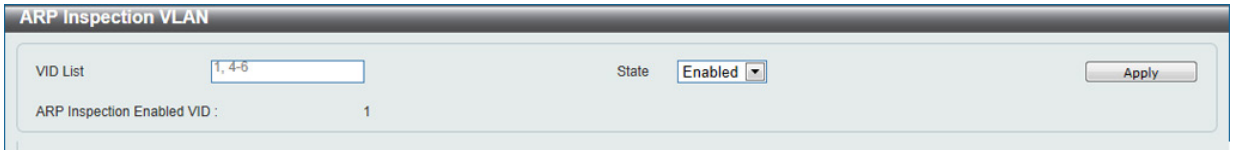


図 12-44　ARP Inspection VLAN 画面

本画面には以下の項目があります。

項目	説明
VID List	設定する VLAN ID リストを入力します。
State	指定 VLAN の ARP インスペクションについて有効 / 無効に設定します。

「Apply」ボタンをクリックし、設定内容を適用してください。

ARP Inspection Statistics（ARP インスペクション統計）

ARP インスペクションの統計情報の表示、消去を行います。

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

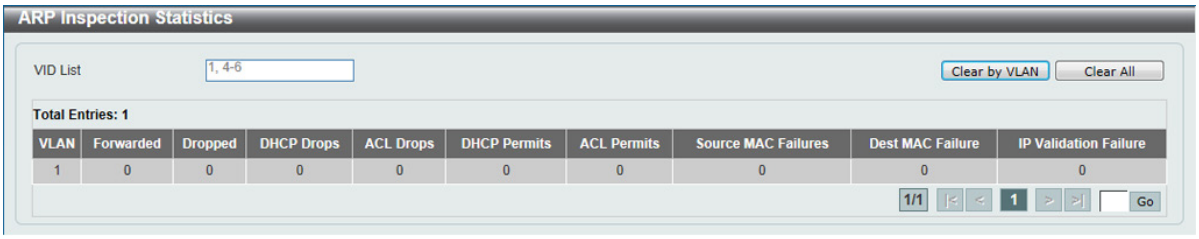


図 12-45　ARP Inspection Statistics 画面

本画面には以下の項目があります。

項目	説明
VID List	設定する VLAN ID リストを入力します。

「Clear by VLAN」ボタンをクリックし、入力した VLAN ID についての情報を消去します。
「Clear All」ボタンをクリックし、テーブルのすべての情報を消去します。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

ARP Inspection Log（ARP インスペクションログ）

ARP インスペクションログ情報の表示、消去、設定を行います。

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



図 12-46　ARP Inspection Log 画面

本画面には以下の項目があります。

項目	説明
Log Buffer	使用するログバッファの値を入力します。1 から 1024 の間で指定可能です。初期値は 32 です。

「Apply」ボタンをクリックし、設定内容を適用してください。「Clear Log」ボタンをクリックし、ログを消去します。

IP Source Guard（IP ソースガード）

注意　IP ソースガードを使用する場合は、必ず、有効にするポートに所属しているすべての VLAN が”DHCP Snooping VLAN Settings”のページで有効に設定している必要があります。

IP Source Guard Port Settings（IP ソースガードポート設定）

IP ソースガードの表示、設定を行います。

Security > IMPB > IPv4 > IP Source Guard > IP Source Guard Port Settings の順にクリックして、以下の画面を表示します。

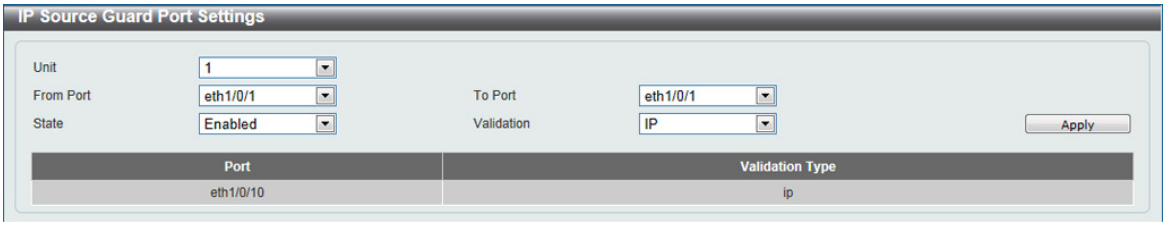


図 12-47　IP Source Guard Port Settings 画面

本画面には以下の項目があります。

項目	説明
Unit	設定するユニットを指定します。
From Port/To Port	選択したポートから連続した複数のポートを設定できます。
State	指定ポートの IP ソースガードを有効 / 無効に設定します。
Validation	検証方法について選択します。「IP」「IP-MAC」から選択します。「IP」を選択すると受信パケットの IP アドレスがチェックされます。「IP-MAC」を選択すると受信パケットの IP アドレスと MAC アドレスがチェックされます。

「Apply」ボタンをクリックし、設定内容を適用してください。

IP Source Guard Binding（IP ソースガードバインディング）

IP ソースガードバインディングの表示、設定を行います。

Security > IMPB > IPv4 > IP Source Guard > IP Source Guard Binding の順にクリックして、以下の画面を表示します。

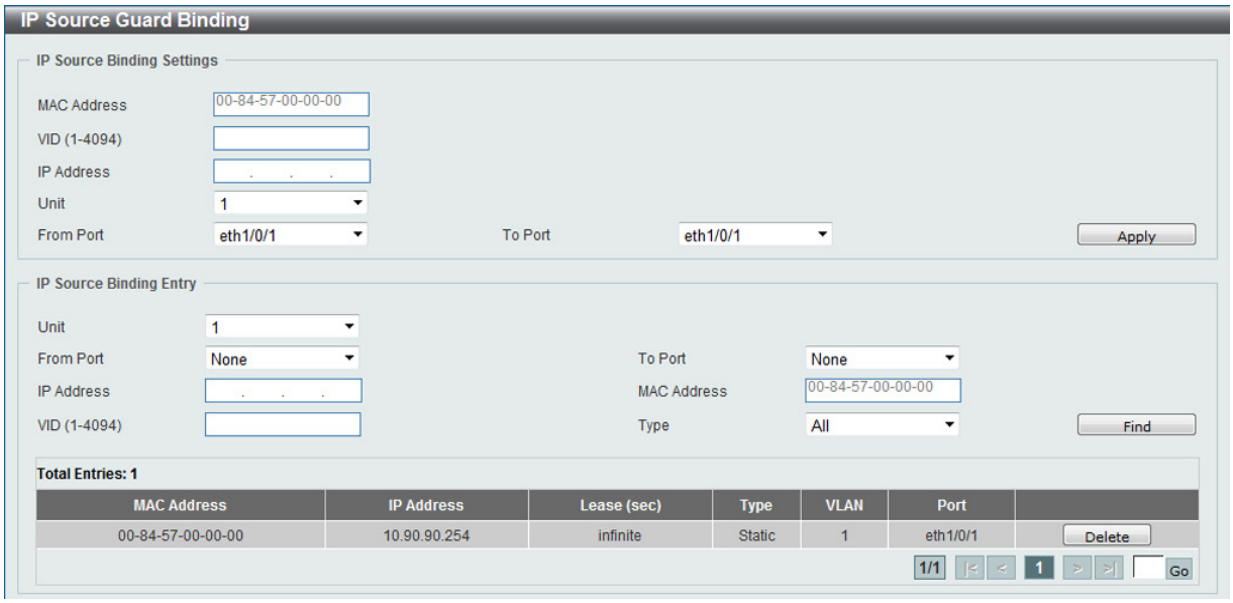


図 12-48　IP Source Guard Binding 画面

本画面には以下の項目があります。

項目	説明
IP Source Binding Settings	
MAC Address	バインディングエントリの MAC アドレスを入力します。
VID	バインディングエントリの VLAN ID を入力します。
IP Address	バインディングエントリの IP アドレスを入力します。
Unit	設定するユニットを指定します。
From Port/ To Port	選択したポートから連続した複数のポートを設定できます。

「Apply」ボタンをクリックし、設定内容を適用してください。

IP Source Binding Entry	
Unit	このクエリで設定するユニットを指定します。
From Port/ To Port	このクエリで選択したポートから連続した複数のポートを設定できます。
IP Address	バインディングエントリの IP アドレスを入力します。
MAC Address	バインディングエントリの MAC アドレスを入力します。
VID	バインディングエントリの VLAN ID を入力します。
Type	バインディングエントリの種類を選択します。「All」「DHCP Snooping」「Static」から選択します。「All」を選択するとすべての DHCP バインディングエントリが表示されます。「DHCP Snooping」を選択すると、DHCP バインディングスヌーピングにに習得された IP ソースガードバインディングが表示されます。「Static」を選択すると手動で設定した IP ソースガードバインディングが表示されます。

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。
「Delete」をクリックして指定エントリを削除します。
「Find」をクリックして入力した情報を元に指定のエントリを表示します。

IP Source Guard HW Entry（IP ソースガードハードウェアエントリ）

IP ソースガードハードウェアエントリの表示を行います。

Security > IMPB > IPv4 > IP Source Guard > IP Source Guard HW Entry の順にクリックして、以下の画面を表示します。



図 12-49　IP Source Guard HW Entry 画面

本画面には以下の項目があります。

項目	説明
Unit	このクエリで使用するユニットを指定します。
From Port/ To Port	このクエリで選択したポートから連続した複数のポートを設定できます。

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。
「Find」をクリックして入力した情報を元に指定のエントリを表示します。

Advanced Settings（アドバンス設定）

IP-MAC-Port Binding Settings（IP-MAC ポートバインディング設定）

IP-MAC ポートバインディングの設定、表示を行います。

Security > IMPB > IPv4 > Advanced Settings > IP-MAC-Port Binding Settings の順にクリックして、以下の画面を表示します。

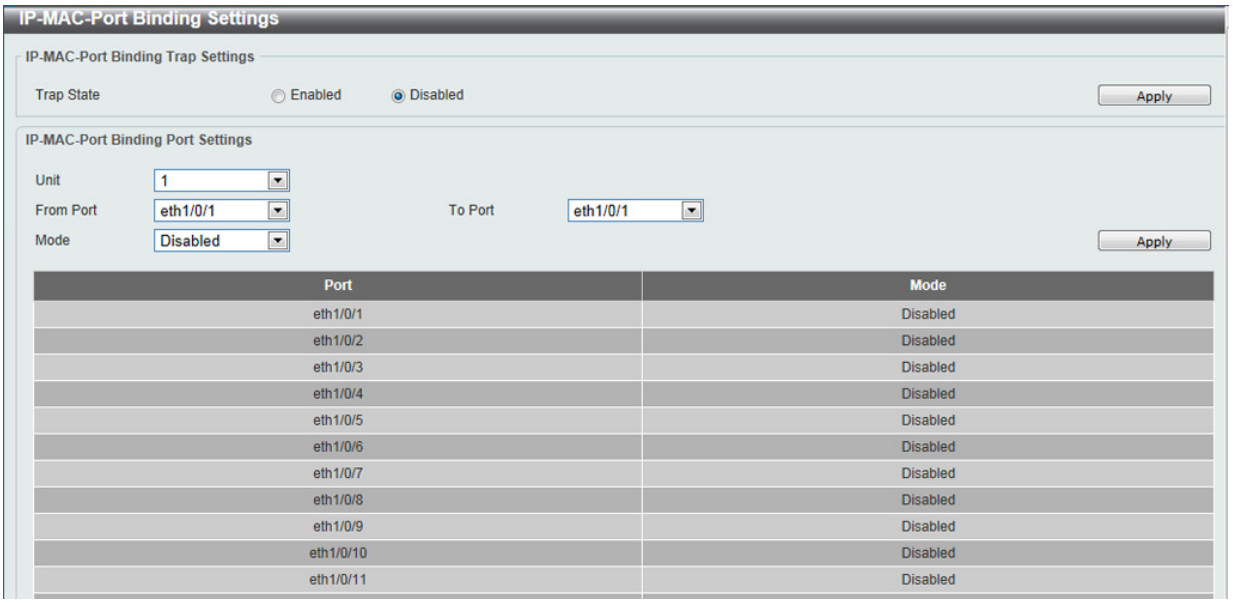


図 12-50　IP-MAC-Port Binding Settings 画面

本画面には以下の項目があります。

項目	説明
IP-MAC-Port Binding Trap Settings	
Trap State	IP-MAC ポートバインディングのトラップ設定を有効 / 無効に指定します。

「Apply」ボタンをクリックし、設定内容を適用してください。

IP-MAC-Port Binding Port Settings	
Unit	設定するユニットを指定します。
From Port/ To Port	選択したポートから連続した複数のポートを設定できます。

項目	説明
Mode	アクセスコントロールのモードを選択します。「Disabled」「Strict」「Loose」から選択します。ポートが「Strict」モードのアクセスコントロールを有効にしている時は、ホストは ARP/IP パケット送信後にそれらの ARP/IP パケットがバインディングチェックを通過した後のみ、ポートへアクセスできます。バインディングチェックを通過するには、送信元 IP アドレス、送信元 MAC アドレス、VLAN ID、そして受領ポート番号が、IP ソースガードスタティックバインディングエントリ、または DHCP スヌーピング学習済みダイナミックバインディングエントリに定義されたエントリにマッチする必要があります。ポートが「Loose」モードのアクセスコントロールを有効にしている場合、ホストが ARP パケットもしくは IP パケットを送信した後、ホストがポートにアクセスすることを拒否され、ホストから送信された ARP パケットもしくは IP パケットはバインディングチェックを通過しません。バインディングチェックを通過するには、送信元 IP アドレス、送信元 MAC アドレス、VLAN ID、そして受領ポート番号が、IP ソースガードスタティックバインディングエントリ、または DHCP スヌーピング学習済みダイナミックバインディングエントリに定義されたエントリにマッチする必要があります。

設定後、「Apply」ボタンをクリックして設定を有効にします。

IP-MAC-Port Binding Blocked Entry（IP-MAC ポートバインディングブロックエントリ）

IP-MAC ポートバインディングブロックエントリの表示、消去を行います。

Security > IMPB > IPv4 > Advanced Settings > IP-MAC-Port Binding Blocked Entry の順にクリックして、以下の画面を表示します。

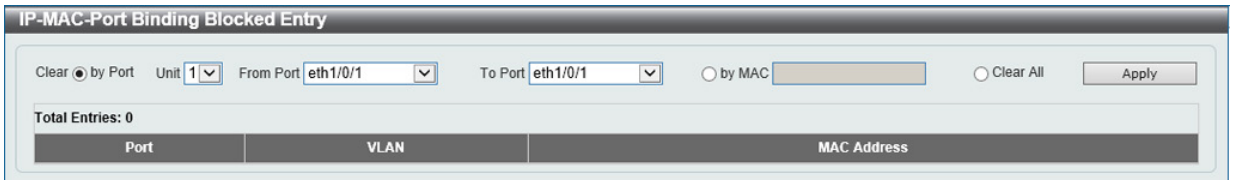


図 12-51　IP-MAC-Port Binding Blocked Entry 画面

本画面には以下の項目があります。

項目	説明
Clear by Port	選択ポートに基づいたエントリテーブルをクリアにします。
Unit	設定するユニットを指定します。
From Port/ To Port	選択したポートから連続した複数のポートを設定できます。
Clear by MAC	MAC アドレスを含むエントリを消去します。項目欄にクリアされる MAC アドレスを入力します。
Clear All	MAC アドレスを含むすべてのエントリを消去します。

設定後、「Apply」ボタンをクリックして設定を有効にします。

IPv6

IPv6 Snooping（IPv6 スヌーピング）

IPv6 スヌーピングについて表示、設定します。

Security > IMPB > IPv6 > IPv6 Snooping の順にクリックして、以下の画面を表示します。

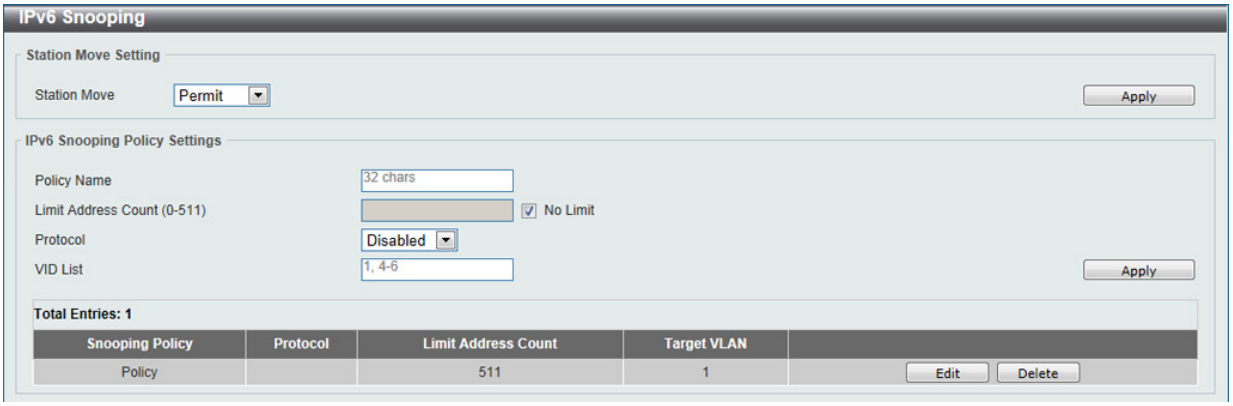


図 12-52　IPv6 Snooping 画面

本画面には以下の項目があります。

項目	説明
Station Move Setting	
Station Move	ステーション動作について設定します。「Permit」「Deny」から指定します。

「Apply」ボタンをクリックし、設定内容を適用してください。

IPv6 Snooping Policy Settings	
Policy Name	IPv6 スヌーピングポリシー名を入力します。32 文字内で指定可能です。
Limit Address Count	アドレスカウント制限の値を指定します。0 から 511 まで指定可能です。 「No Limit」を指定するとアドレスカウント制限は無効になります。
Protocol	本ポリシーに対応するプロトコルを選択します。「Disabled」「DHCP」「NDP」「All」から選択可能です。DHCPv6 スヌーピングはアドレス割り当ての段階での DHCPv6 クライアントとサーバ間の DHCPv6 パケットを傍受します。DHCPv6 クライアントが有効な IPv6 アドレスを取得すると、DHCPv6 スヌーピングはバインディングデータベースを作成します。ND スヌーピングはステートレスな自動設定 IPv6 アドレスと手動設定 IPv6 アドレスのための機能です。IPv6 アドレスをアサインする前に、ホストは「Duplicate Address Detection」（DAD）を実行する必要があります。ND スヌーピングは DAD メッセージ（DAD NS と DAD NA）を検出し、バインディングデータベースを構築します。NDP パケット (NS と NA) もまたホストが到達可能かを判断しバインディングを削除するかどうかを決定するために使用されます。
VID List	使用する VLAN ID リストを入力します。

設定後、「Apply」ボタンをクリックして設定を有効にします。
「Delete」をクリックして指定エントリを削除します。
「Edit」をクリックして指定エントリを編集します。

IPv6 ND Inspection（IPv6 ND インスペクション）

IPv6 ND インスペクションについて表示、設定します。

Security > IMPB > IPv6 > IPv6 ND Inspection の順にクリックして、以下の画面を表示します。

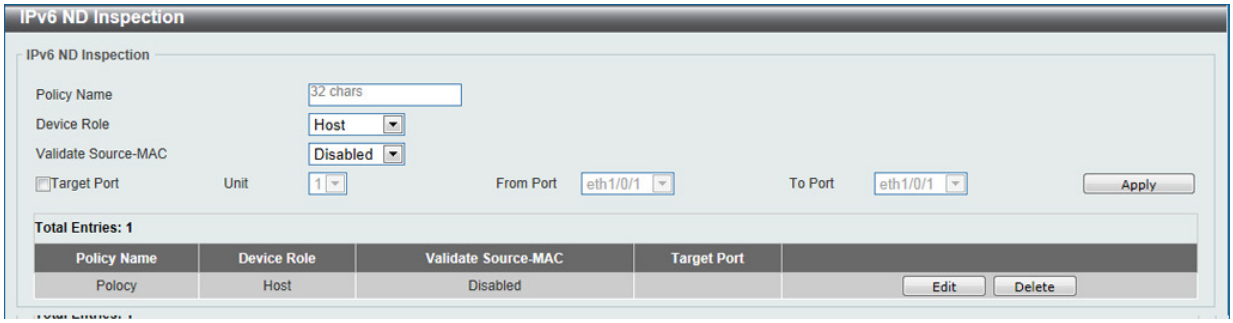


図 12-53　IPv6 ND Inspection 画面

本画面には以下の項目があります。

項目	説明
Policy Name	ポリシー名を入力します。32 文字内で指定可能です。
Device Role	デバイスロールを選択します。「Host」「Router」から選択します。初期値では「Host」に設定され、NS、NA メッセージのインスペクションは動作します。「Router」を選択した場合、NS、NA のインスペクションは動作しません。NS/NA インスペクションを動作させるときは、DHCP もしくは ND プロトコルから学習したダイナミックバインディングテーブルに対しての妥当性の確認が必要です。
Validate Source-MAC	送信 MAC アドレスオプションの妥当性確認を有効 / 無効にします。リンクレイヤアドレスを含む ND メッセージを受信した時に、リンクレイヤアドレスに対する送信元 MAC アドレスを確認します。リンクレイヤアドレスと MAC アドレスが違う場合、パケットは破棄されます。
Target Port	チェックを入れターゲットポートを指定します。
Unit	設定するユニットを指定します。
From Port/ To Port	選択したポートから連続した複数のポートを設定できます。

設定後、「Apply」ボタンをクリックして設定を有効にします。
「Delete」をクリックして指定エントリを削除します。
「Edit」をクリックして指定エントリを編集します。

IPv6 RA Guard（IPv6 RA ガード）

IPv6 RA ガードについて表示、設定します。

Security > IMPB > IPv6 > IPv6 RA Guard の順にクリックして、以下の画面を表示します。



図 12-54　IPv6 RA Guard 画面

本画面には以下の項目があります。

項目	説明
Policy Name	ポリシー名を入力します。32 文字内で指定可能です。
Device Role	デバイスロールを選択します。「Host」「Router」から選択します。初期値では「Host」に設定され、RA パケットはすべてブロックされます。「Router」を選択した場合、RA パケットはポート宛ての ACL に従い転送されます。
Match IPv6 Access List	マッチさせる IPv6 アクセスリストを入力、選択します。
Target Port	チェックを入れターゲットポートを指定します。
Unit	設定するユニットを指定します。

項目	説明
From Port/ To Port	選択したポートから連続した複数のポートを設定できます。

設定後、「Apply」ボタンをクリックして設定を有効にします。
「Delete」をクリックして指定エントリを削除します。
「Edit」をクリックして指定エントリを編集します。

IPv6 DHCP Guard（IPv6 DHCP ガード）

IPv6 DHCP ガードについて表示、設定します。

Security > IMPB > IPv6 > IPv6 DHCP Guard の順にクリックして、以下の画面を表示します。



図 12-55　IPv6 DHCP Guard 画面

本画面には以下の項目があります。

項目	説明
Policy Name	ポリシー名を入力します。32 文字内で指定可能です。
Device Role	デバイスロールを選択します。「Client」「Server」から選択します。初期値では「Client」に設定され、DHCPv6 サーバからの DHCPv6 パケットはすべてブロックされます。「Server」を選択した場合、DHCPv6 サーバパケットはポート宛ての ACL に従い転送されます。
Match IPv6 Access List	マッチさせる IPv6 アクセスリストを入力、選択します。
Target Port	チェックを入れターゲットポートを指定します。
Unit	設定するユニットを指定します。
From Port/ To Port	選択したポートから連続した複数のポートを設定できます。

設定後、「Apply」ボタンをクリックして設定を有効にします。
「Delete」をクリックして指定エントリを削除します。
「Edit」をクリックして指定エントリを編集します。

IPv6 Source Guard（IPv6 ソースガード）

IPv6 Source Guard Settings（IPv6 ソースガード設定）

IPv6 ソースガードの表示、設定を行います。

Security > IMPB > IPv6 > IPv6 Source Guard > IPv6 Source Guard Settings の順にクリックして、以下の画面を表示します。



図 12-56　IPv6 Source Guard Settings 画面

本画面には以下の項目があります。

項目	説明
Policy Name	ポリシー名を入力します。32 文字内で指定可能です。
Global Auto-Configure Address	自動設定グローバルアドレスからのデータトラフィックの許可 / 拒否を選択します。リンクのすべてのグローバルアドレスが DHCP および送信トラフィックから設定したアドレスを持つホストをブロックしたい管理者により割り当てられている場合に有効です。
Link Local Traffic	リンクローカルアドレスによって送信されたデータトラフィックの許可 / 拒否を選択します。
Target Port	チェックを入れターゲットポートを指定します。
Unit	設定するユニットを指定します。
From Port/To Port	選択したポートから連続した複数のポートを設定できます。

「Apply」ボタンをクリックし、設定内容を適用してください。

IPv6 Neighbor Binding（IPv6 ネイババインディング）

IPv6 ネイババインディングの表示、設定を行います。

Security > IMPB > IPv6 > IPv6 Source Guard > IPv6 Neighbor Binding の順にクリックして、以下の画面を表示します。

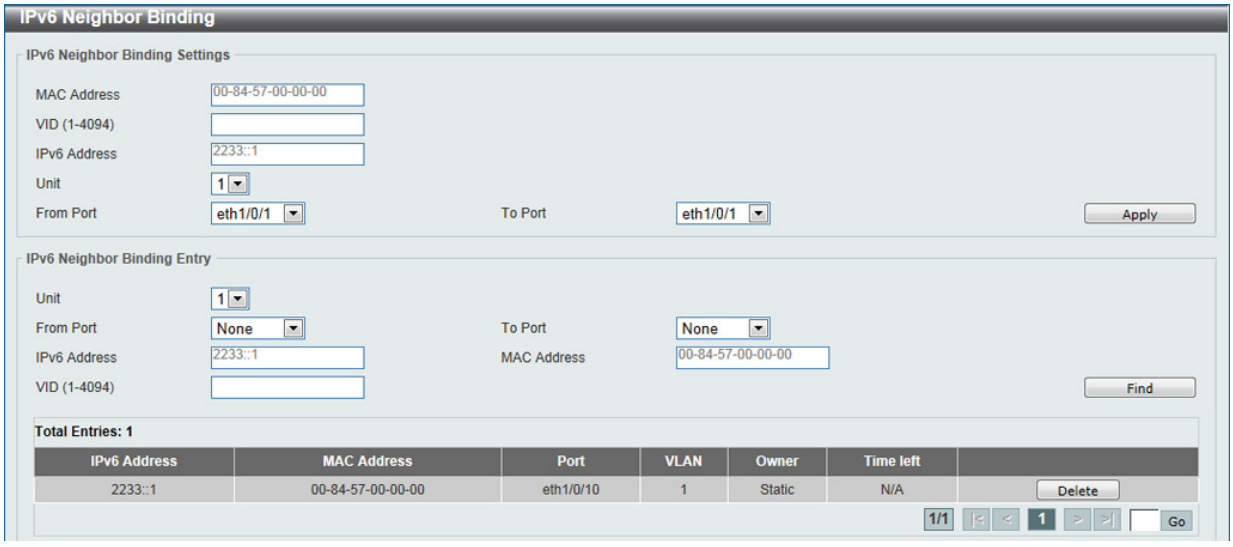


図 12-57　IPv6 Neighbor Binding 画面

本画面には以下の項目があります。

項目	説明
IPv6 Neighbor Binding Settings	
MAC Address	バインディングエントリの MAC アドレスを入力します。
VID	バインディングエントリの VLAN ID を入力します。1 から 4094 の間で指定します。
IPv6 Address	バインディングエントリの IPv6 アドレスを入力します。
Unit	設定するユニットを指定します。
From Port/To Port	選択したポートから連続した複数のポートを設定できます。

「Apply」ボタンをクリックし、設定内容を適用してください。

項目	説明
IPv6 Neighbor Binding Entry	
Unit	このクエリで設定するユニットを指定します。
From Port/ To Port	このクエリで選択したポートから連続した複数のポートを設定できます。
IPv6 Address	バインディングエントリの IPv6 アドレスを入力します。
MAC Address	バインディングエントリの MAC アドレスを入力します。
VID	表示する VLAN ID を入力します。

「Delete」をクリックして指定エントリを削除します。
「Find」をクリックして入力した情報を元に指定のエントリを表示します。

DHCP Server Screening（DHCP サーバスクリーニング設定）

本機能は DHCP サーバパケットの制限だけでなく、特定の DHCP クライアントが特定の DHCP サーバパケットを受信することを許可することが可能です。ネットワークに一つ以上の DHCP サーバがあり複数のクライアントグループに DHCP サービスを提供している場合において有効です。初めて DHCP フィルタを有効にすると、ポートプロファイルごとにアクセスプロファイルエントリとアクセスルールの両方が作成され、その他のアクセスルールも作成されます。これらのルールはすべての DHCP サーバパケットをブロックします。許可 DHCP エントリに加えて、初めて DHCP クライアント MAC アドレスがクライアント MAC アドレスとして使用される際、アクセスプロファイルおよびアクセスルールエントリも作成されます。送信元 IP アドレスは DHCP サーバの IP アドレス（UDP ポート番号 67）と同じです。これらのルールはユーザが指定した特定のフィールドを持った DHCP サーバパケットの許可に使用します。DHCP サーバフィルタ機能が有効な場合、指定ポートからのすべての DHCP サーバパケットはフィルタされます。

DHCP Server Screening Global Settings（DHCP サーバスクリーニンググローバル設定）

DHCP サーバスクリーニンググローバル設定の表示、設定をします。

Security > DHCP Server Screening > DHCP Server Screening Global Settings の順にメニューをクリックして画面を表示します。

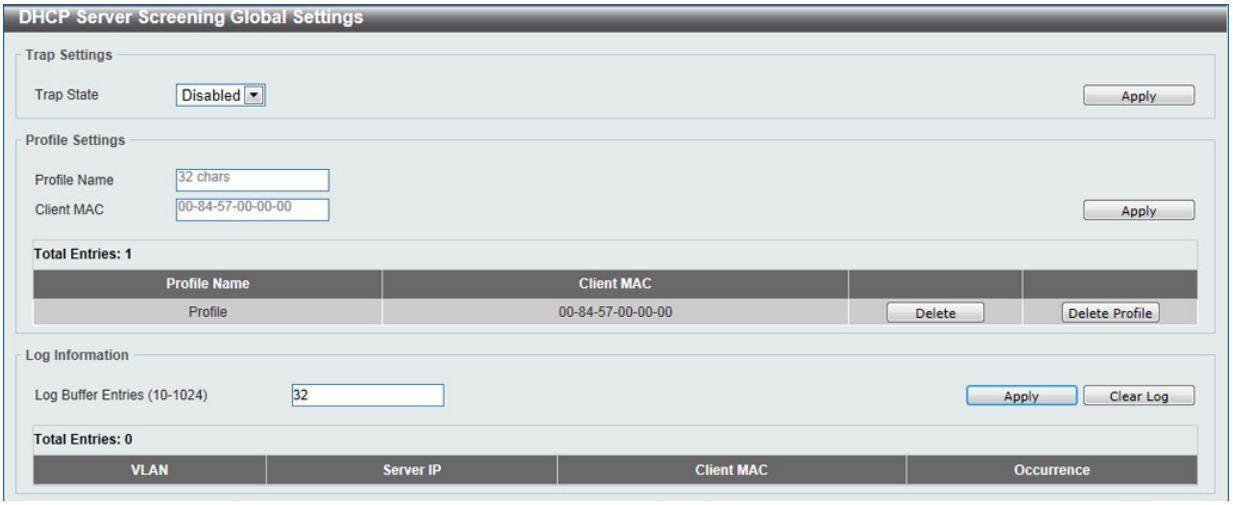


図 12-58　DHCP Server Screening Global Settings 画面

本画面には以下の項目があります。

項目	説明
Trap Settings	
Trap State	DHCP サーバスクリーニングトラップ機能を「Enabled」（有効）/「Disabled」（無効）にします。

「Apply」ボタンをクリックし、設定内容を適用してください。

Profile Settings	
Profile Name	プロファイル名を入力します。32 文字内で指定可能です。
Client MAC	クライアントの MAC アドレスを入力します。

「Apply」ボタンをクリックし、設定内容を適用してください。
「Delete」をクリックして指定エントリを削除します。
「Delete Profile」をクリックして指定プロファイルを削除します。

Log Information	
Log Buffer Entries	ログバッファエントリ数を入力します。10 から 1024 までで指定します。初期値は 32 です。

設定後、「Apply」ボタンをクリックして設定を有効にします。「Clear Log」ボタンをクリックしてログを消去します。

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 12-59　DHCP Server Screening Port Settings 画面

本画面には以下の項目があります。

項目	説明
Unit	設定するユニットを指定します。
From Port/ To Port	選択したポートから連続した複数のポートを設定できます。
State	指定ポートでの DHCP サーバスクリーニング機能を有効 / 無効にします。
Server IP	DHCP サーバの IP アドレスを入力します。
Profile Name	ポートに設定する DHCP サーバスクリーニングプロファイル名を入力します。

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

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

ARP スプーフィング防止の設定を行います。エントリが作成されると、送信元 IP アドレスがゲートウェイ IP アドレスに合致するが、送信元 MAC アドレスがゲートウェイ MAC アドレスに合致しない ARP パケットは、破棄されます。ASP は、送信元 IP アドレスが設定したゲートウェイ IP アドレスに合致しない ARP パケットをバイパスします。ARP アドレスが、設定されたゲートウェイ IP アドレス、MAC アドレス、ポートリストに合致した場合、受信しているポートが ARP 信頼もしくは未信頼であるかに関係なく、ダイナミック ARP インスペクション（DAI）をバイパスします。

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

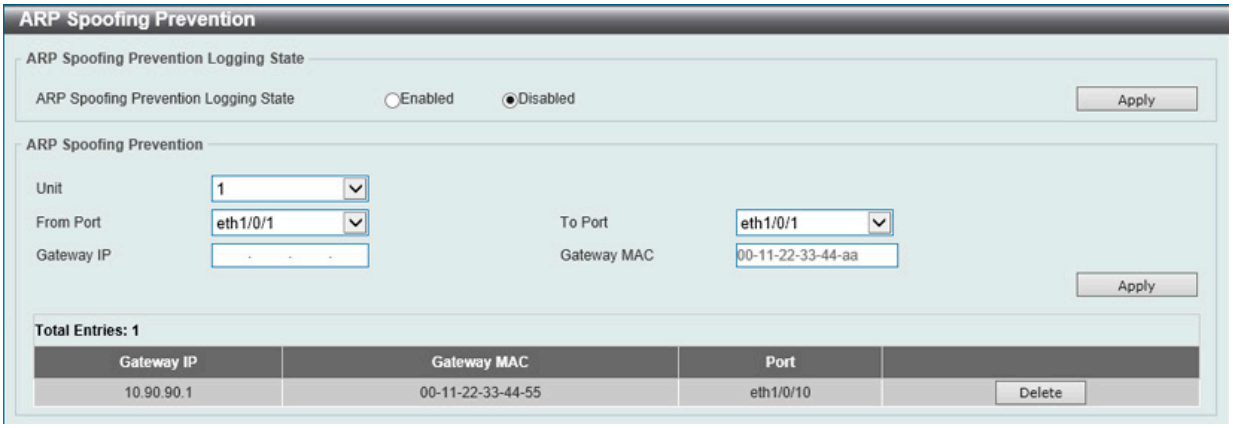


図 12-60　ARP Spoofing Prevention 画面

以下の項目を使用して、設定します。

項目	説明
ARP Spoofing Prevention Logging	
ARP Spoofing Prevention Logging State	ARP スプーフィングのログ設定を有効 / 無効に指定します。
ARP Spoofing Prevention	
Unit	設定するユニットを指定します。
From Port / To Port	選択したポートから連続した複数のポートを設定できます。
Gateway IP	ゲートウェイの IP アドレスを入力します。
Gateway MAC	ゲートウェイの MAC アドレスを入力します。

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

BPDU Attack Protection（BPDU アタック防止設定）

スイッチのポートに BPDU アタック防止機能を設定します。通常、BPDU アタック防止機能には 2 つの状態があります。1 つは正常な状態で、もう 1 つはアタック状態です。アタック状態には、3 つのモード（破棄、ブロックおよびシャットダウン）があります。BPDU アタック防止が有効なポートは、STP BPDU パケットを受信するとアタック状態に入ります。そして、設定に基づいてアクションを行います。BPDU アタック防止は STP が無効なポートにだけ有効にすることができます。BPDU アタック防止は、「STP コマンド」における「FBPDU」に設定したものより高い優先度を持っています。つまり、ポートが「FBPDU」で「STP BPDU 転送」に設定されていても、BPDU アタック防止が有効であると、ポートは STP BPDU を転送しません。

BPDU アタック防止では、BPDU の処理を決定するために設定した BPDU トンネルポートより高い優先度を持っています。つまり、ポートが「STP」で BPDU トンネルポートとして設定されていると、ポートは STP BPDU を転送します。しかし、ポートで BPDU アタック防止が有効であると、ポートは STP BPDU を転送しません。

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

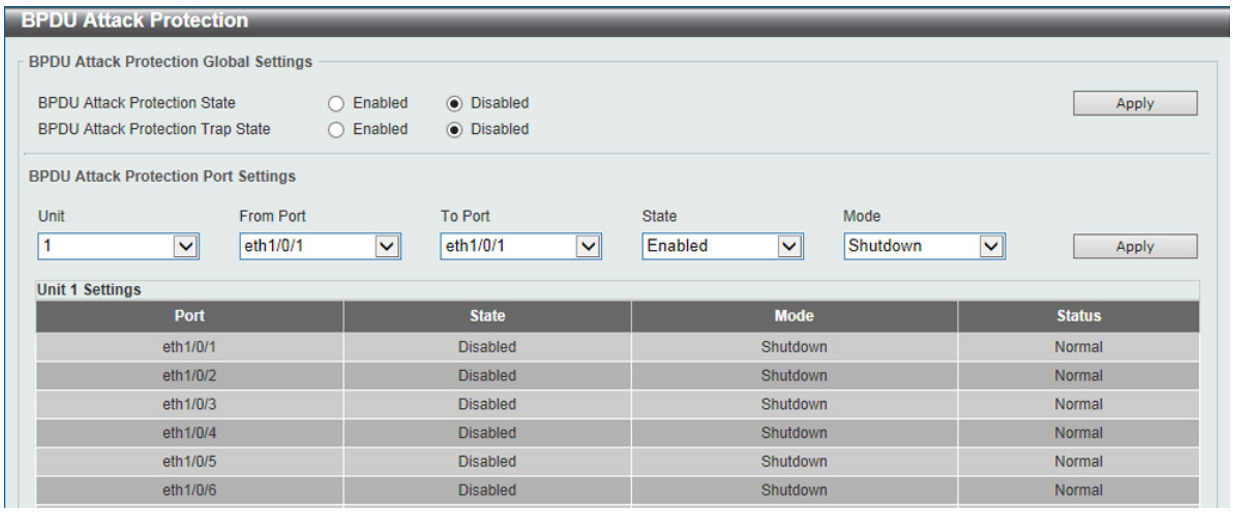


図 12-61　BPDU Attack Protection 画面

以下の項目を使用して、設定します。

項目	説明
BPDU Attack Protection State	BPDU アタック防止機能を有効または無効にします。初期値は無効です。
BPDU Attack Protection Trap State	トラップの状態を有効 / 無効にします。
Unit	設定するユニットを選択します。
From Port / To Port	設定を使用するポート範囲を選択します。
State	指定ポートに対してモードを有効または無効にします。
Mode	BPDU 防止モードを指定します。 • Drop - ポートがアタック状態に入るとすべての受信 BPDU パケットを破棄します。 • Block - ポートがアタック状態に入るとすべてのパケット（BPDU と正常なパケットを含む）を破棄します。 • Shutdown - ポートがアタック状態に入るとポートをシャットダウンします。

「Apply」ボタンをクリックし、変更を有効にします。

MAC Authentication（MAC 認証）

MAC 認証機能は、MAC アドレスにてネットワークの認証を設定する方法です。
本スイッチはローカル認証方式、リモート RADIUS サーバと RAIDUS プロトコルを使って認証を行う RADIUS クライアントになる方式のどちらもサポートされています。

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

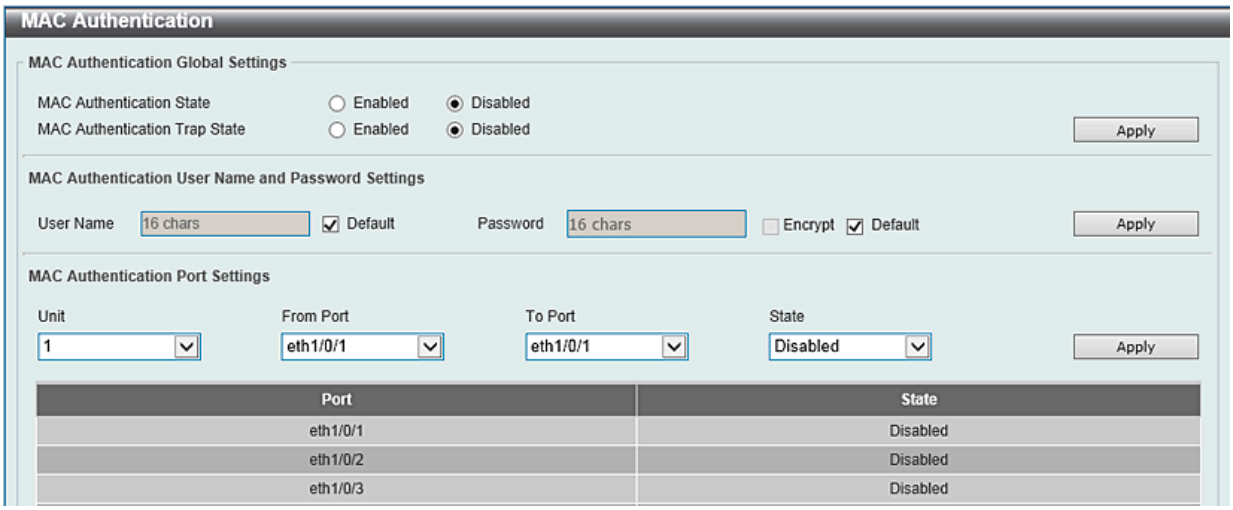


図 12-62　MAC Authentication 画面

以下の項目を参照、または設定可能です。

項目	説明
MAC Authentication Global Settings	
MAC Authentication State	「Enabled」（有効）または「Disabled」（無効）を選択し、スイッチの MAC 認証をグローバルに設定します。初期値は「Disabled」です。
MAC Authentication Trap State	MAC 認証のトラップのステータスを有効 / 無効にします。

「Apply」ボタンをクリックし、設定内容を適用してください。

MAC Authentication User Name and Password Settings	
User Name	MAC 認証のユーザ名を入力します。16 文字まで入力可能です。「Default」にチェックを入れるとクライアントの MAC アドレスがユーザ名として指定されます。
Password	MAC 認証のパスワードを入力します。「Encrypt」にチェックを入れると、パスワードを暗号化します。「Default」にチェックを入れると、クライアントの MAC アドレスをパスワードとして指定します。

「Apply」ボタンをクリックし、設定内容を適用してください。

MAC Authentication Port Settings	
Unit	設定するユニットを指定します。
From Port / To Port	選択したポートから連続した複数のポートを設定できます。
State	MAC 認証のポート設定を有効 / 無効にします。

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

注意　ホストベースの MAC 認証において、Guest VLAN 使用時、IP Broadcast 以外の パケット契機による、認証済みの MAC アドレスの Port 間の移動はできません。

注意　MAC 認証において、Guest VLAN を有効にした際、端末の Port 間の移動を許可する場合、"no ingress-checking" を設定する必要があります。

Web-based Access Control（Web 認証）

Web ベース認証のログインは、スイッチを経由してインターネットにアクセスを試みる場合に、ユーザを認証するように設計された機能で、認証処理には HTTP/HTTPS プロトコルを使用します。

Web ブラウザ経由で Web ページ (例 : https://www.dlink.com) の閲覧を行う場合に、スイッチは認証を行います。スイッチは、HTTP/HTTPS パケットを検出し、このポートが未認証である場合に、ユーザ名とパスワードの画面を表示して、ユーザに入力を促します。認証処理を通過するまで、ユーザはインターネットにアクセスすることはできません。

スイッチは、認証サーバとなってローカルデータベースに基づく認証を行うか、または RADIUS クライアントとなってリモート RADIUS サーバと共に RADIUS プロトコルを介する認証処理を実行します。Web へのアクセスを試みることによって、クライアントユーザは WAC の認証処理を開始します。

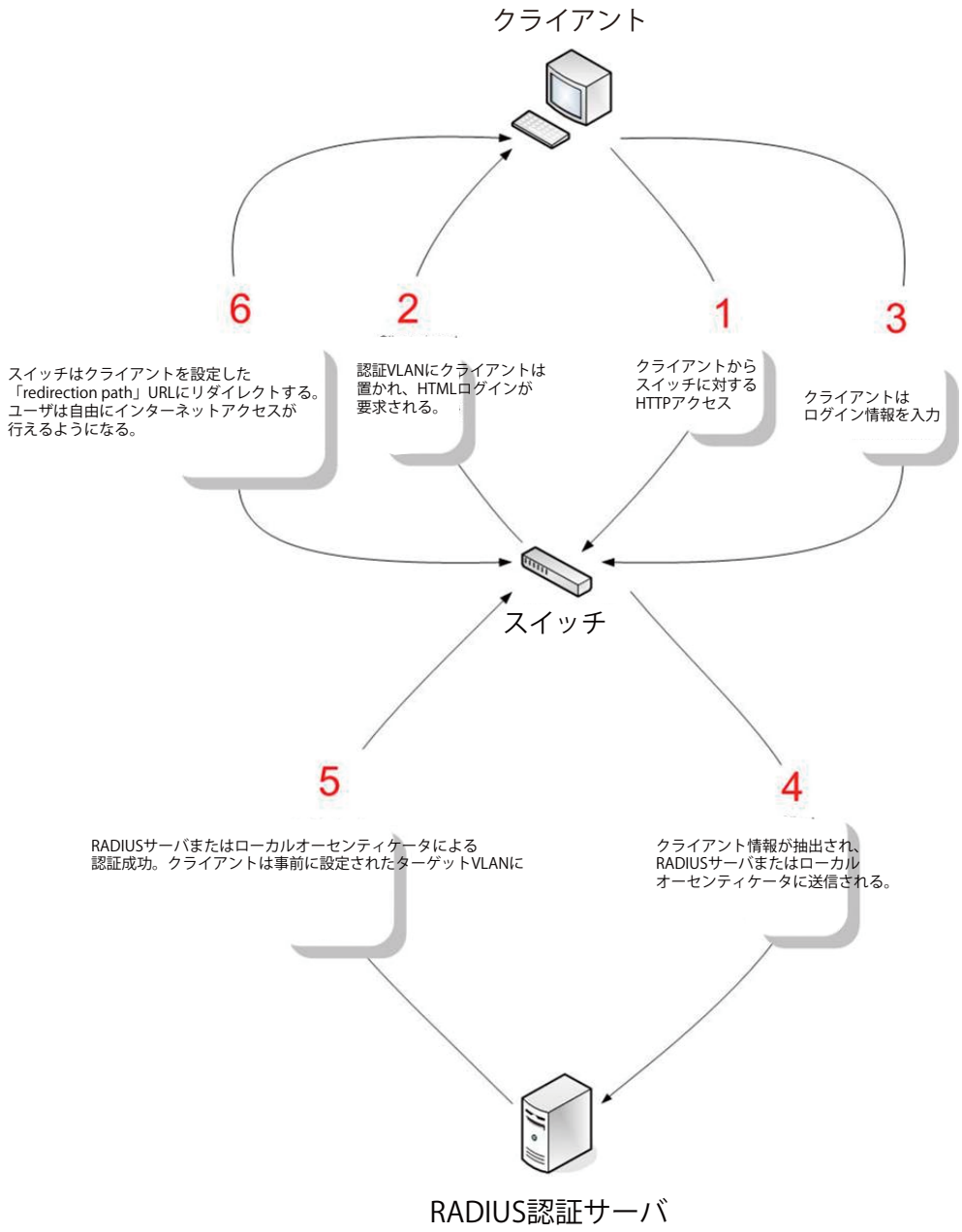
D-Link の WAC の実行には、WAC 機能が排他的に使用し、スイッチの他のモジュールで使用されていない仮想 IP を使用します。実際は、スイッチの他の機能への影響を避ける場合にだけ、WAC は仮想 IP アドレスを使用してホストとの通信を行います。そのため、すべての認証要求を仮想 IP アドレスに送信し、スイッチの物理インタフェースの IP アドレスには送信しないようする必要があります。

ホスト PC が仮想 IP 経由で WAC スイッチと通信する場合、仮想 IP は、スイッチの物理的な IPIF(IP インタフェース) アドレスに変換されて通信を可能にします。ホスト PC と他のサーバの IP 構成は WAC の仮想 IP に依存しません。仮想 IP は、ICMP パケットまたは ARP リクエストに応答しません。つまり、仮想 IP は、スイッチの IPIF(IP インタフェース) と同じサブネット、またはホスト PC のサブネットと同じサブネットには設定することはできません。

PC と同じであると、WAC が有効なポートに接続するホストは、IP アドレスを実際に所有しているサーバまたは PC とは通信ができません。ホストがサーバまたは PC にアクセスする必要がある場合、仮想 IP をサーバまたは PC の 1 つと同じにすることはできません。ホスト PC がプロキシを使用して Web にアクセスする場合、PC のユーザは、認証を適切に実行するために、プロキシ設定の例外として仮想 IP を加える必要があります。

スイッチの WAC の実行は、ユーザ定義のポート番号により HTTP または HTTPS プロトコルのいずれかに対して TCP ポートを設定できることを特徴としています。HTTP か HTTPS に対するこの TCP ポートは、認証処理のために CPU にトラップされる HTTP か HTTPS パケットを識別するためやログインページにアクセスするために使用されます。指定しない場合、HTTP に対するポート番号の初期値は 80、HTTPS に対するポート番号の初期値は 443 となります。プロトコルも指定されないと、プロトコルの初期値は HTTP になります。

次の図は、Web ベースのアクセスコントロールを実現させるために、認証に関わる各ノードで行われる基本の 6 つのステップを例示しています。



条件および制限

1. クライアントが IP アドレス取得のために DHCP を使用している場合、認証 VLAN はクライアントが IP アドレス取得を行えるように、DHCP サーバまたは DHCP リレー機能を持つ必要があります。
2. アクセスプロファイル機能のように、スイッチ上に存在する機能の中には HTTP パケットをフィルタしてしまうものがあります。ターゲット VLAN にフィルタ機能の設定を行う際には、HTTP パケットがスイッチにより拒否されないように、十分に注意してください。
3. 認証に RADIUS サーバを使用する場合、Web 認証を有効にする前に、ターゲット VLAN を含む必要な項目を入力して RADIUS サーバの設定を行ってください。

Web Authentication（Web 認証設定）

スイッチの Web 認証設定をに行います。

Security > Web-based Access Control > Web Authentication をクリックして、以下の画面から設定します。



図 12-63　Web Authentication 画面

以下の項目を使用して、設定を行います。

項目	説明
Web Authentication State	Web 認証機能を「Enable」（有効）/「Disable」（無効）にします。
Trap State	Web 認証のトラップの状態を有効 / 無効にします。
Virtual IPv4	仮想 IP アドレスを入力します。Web 認証の仮想 IP は WAC にだけ使用され、スイッチの他のモジュールでは使用されません。すべての Web 認証のプロセスはこの IPv4 アドレスとの連携で行われますが、しかし仮想 IP はどの ICMP パケットや ARP リクエストにも応答しません。そのため仮想 IP はスイッチのインタフェースやホスト PC と同じサブネットに設定することはできません。でなければ Web 認証は正しく動作しません。設定した URL は仮想 IP アドレスが設定されている場合のみ有効です。DNS サーバに格納されている FQDN URL を取得して仮想 IP アドレスを取得します。取得した IP アドレスは本コマンドで指定した仮想 IP アドレスと一致する必要があります。もし仮想 IPv4 アドレスが設定されない場合、IPv4 アクセスは Web 認証を開始することができません。
Virtual IPv6	仮想 IPv6 アドレスを入力します。もし仮想 IPv6 アドレスが設定されない場合、IPv6 アクセスは Web 認証を開始することができません。
Virtual URL	仮想 URL を指定します。128 文字以内で指定できます。
Redirection Path	認証に成功し、ターゲット VLAN に割り当てられたユーザを導く Web サイトの URL を入力します。128 文字以内で指定できます。

「Apply」ボタンをクリックし、設定を有効にします。

注意　仮想 IP アドレスを「0.0.0.0」もしくはスイッチの IPIF（IP インターフェイス）と同一のサブネットに設定した場合、WAC 機能は正常に動作しません。

WAC Port Settings（Web 認証ポート設定）

Web 認証用のユーザアカウントを登録するには、**Security > Web-based Access Control > WAC Port Settings** をクリックし、以下の設定用画面を表示します。

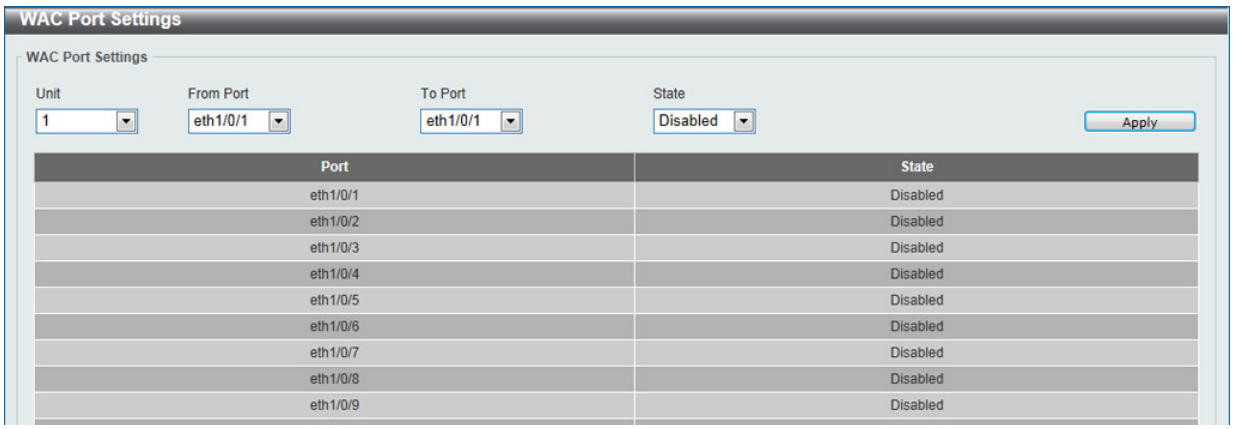


図 12-64　WAC Port Settings 画面

以下の項目を使用して、設定を行います。

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	ポート範囲を設定します。
State	本機能を「Enabled」（有効）/「Disabled」（無効）にします。

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

WAC Customize Page（WAC カスタマイズページ設定）

Web 認証ページの項目をカスタマイズします。

Security > Web-based Access Control > WAC Customize Page の順にメニューをクリックし、以下の画面を表示します。

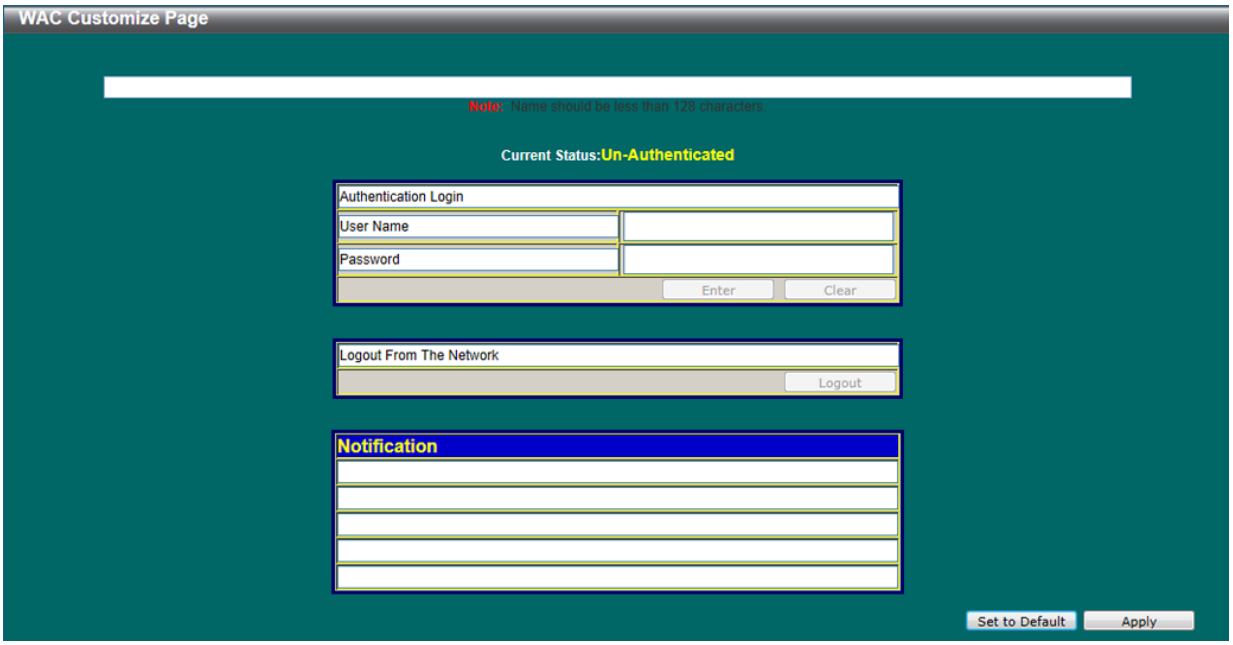


図 12-65　WAC Customize Page 画面

以下の項目を使用して、設定を行います。

項目	説明
Page Title	カスタムページタイトルとなるメッセージを入力します。128 文字まで入力可能です。
Login window Title	カスタムログインウィンドウタイトルを入力します。64 文字まで入力可能です。
User Name Title	カスタムユーザ名タイトルを入力します。32 文字まで入力可能です。
Password Title	カスタムパスワードタイトルを入力します。32 文字まで入力可能です。
Logout window Title	カスタムログアウトウィンドウタイトルを入力します。64 文字まで入力可能です。
Notification	通知エリアに表示させる情報を入力します。各ライン 128 文字以内で入力可能です。5 ライン入力できます。

WAC ページの設定を行うためにはこの画面の WAC 認証情報をすべて入力して「Apply」ボタンをクリックして行った変更を適用します。
「Set to Default」ボタンをクリックして、全項目を初期設定に復元します。

Japanese Web-based Access Control（JWAC 設定）

JWAC Global Settings（JWAC グローバル設定）

スイッチにおける JWAC（Japanese Web-based Access Control）の有効化および設定をします。

Security > Japanese Web-based Access Control > JWAC Global Settings の順にメニューをクリックし、以下の画面を表示します。

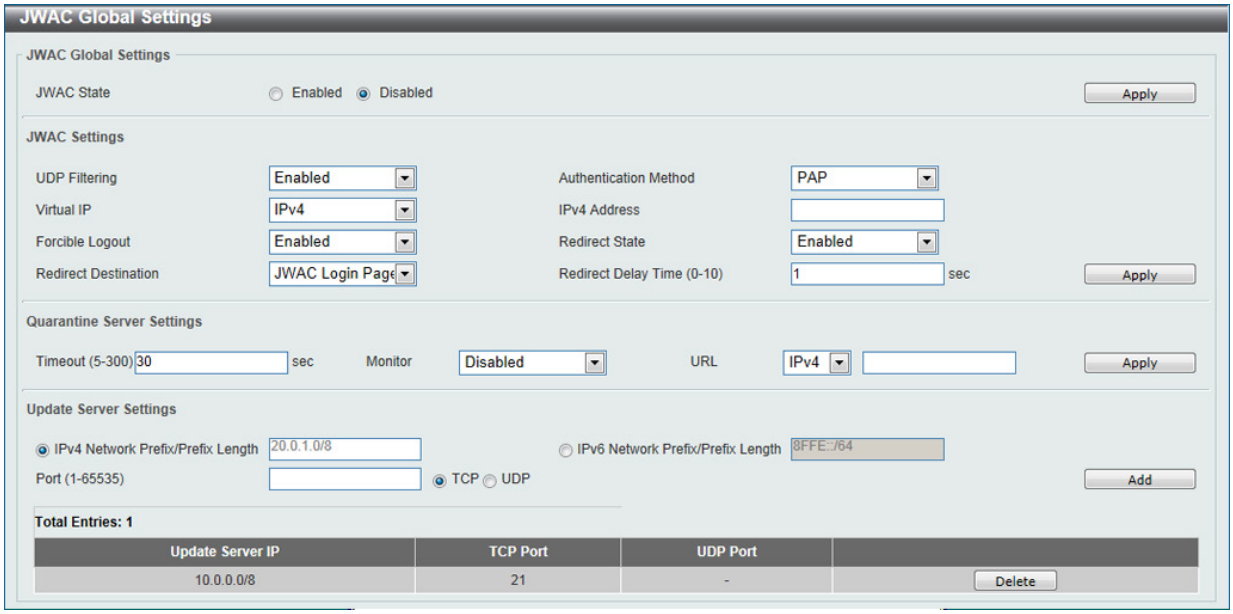


図 12-66　JWAC Global Settings

以下の項目を設定可能です。

項目	説明
JWAC Global Settings	
JWAC State	JWAC 機能を「Enabled」（有効）/「Disabled」（無効）にします。設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
JWAC Settings	
UDP Filtering	JWAC UDP フィルタリングを「Enabled」（有効）/「Disabled」（無効）にします。
Authentication Method	JWAC に使用される認証方法を指定します。オプションには MD5、PAP、CHAP、MS-CHAP、および MS-CHAPv2 があります。
Virtual IP	使用する仮想 IP の種類を選択します。「IPv4」「IPv6」「URL」から選択可能です。
IPv4 Address	「IPv4」を「Virtual IP」で選択した後、項目が表示されます。仮想 IP アドレスを入力します。Web 認証の仮想 IP は WAC にだけ使用され、スイッチの他のモジュールでは使用されません。すべての Web 認証のプロセスはこの IPv4 アドレスとの連携で行われますが、しかし仮想 IP はどの ICMP パケットや ARP リクエストにも応答しません。そのため仮想 IP はスイッチのインタフェースやホスト PC と同じサブネットに設定することはできません。でなければ Web 認証は正しく動作しません。設定した URL は仮想 IP アドレスが設定されている場合のみ有効です。DNS サーバに格納されている FQDN URL を取得して仮想 IP アドレスを取得します。取得した IP アドレスは本コマンドで指定した仮想 IP アドレスと一致する必要があります。もし仮想 IPv4 アドレスが設定されない場合、IPv4 アクセスは Web 認証を開始することができません。
IPv6 Address	未認証ホストからの認証リクエストを受け入れるために使用する JWAC 仮想 IPv6 アドレスを入力します。もし仮想 IPv6 アドレスが設定されない場合、IPv6 アクセスは JWAC 認証を開始することができません。
Virtual URL	「URL」を「Virtual IP」で選択した後、使用する仮想 URL を入力します。
Forcible Logout	JWAC Forcible Logout を「Enabled」（有効）/「Disabled」（無効）にします。「Enabled」の場合、認証ホストから JWAC スイッチに TTL=1 を持つ ping パケットはログアウトリクエストと見なされ、ホストは未認証状態に戻ります。
Redirected State	JWAC リダイレクト機能を「Enabled」（有効）/「Disabled」（無効）にします。リダイレクトが「Enabled」な場合、すべての Web アクセスは検疫サーバや、スイッチの JWAC Login Page にリダイレクトされます。
Redirect Destination	リダイレクト先を「Quarantine Server（検疫サーバ）」または「JWAC Login Page」に指定します。 リダイレクト先に検疫サーバを指定した場合、ランダムな URL にアクセスしようとする未認証ホストは検疫サーバにリダイレクトされます。「JWAC login page」を選択した場合、未認証ホストはスイッチの「JWAC login page」にリダイレクトされ認証を完了します。検疫サーバをリダイレクト先に指定する場合、JWAC 機能をグローバルに有効にする前に検疫サーバの設定を完了してください。リダイレクトを無効にすると、すべての Web アクセスは JWAC ログインページや検疫サーバなどを除き拒否されます。

項目	説明
Redirect Delay Time (0-10)	未認証ホストが Quarantine Server（検疫サーバ）または JWAC Login Page にリダイレクトされる場合の遅延時間 0-10（秒）を指定します。0 はリダイレクトの遅延がないことを示します。
Quarantine Server Settings	
Timeout (5-300)	Quarantine Server のエラータイムアウトを設定します。5-300（秒）で指定します。初期値は 30 秒です。
Monitor	JWAC Quarantine Server モニタを「Enabled」（有効）/「Disabled」（無効）にします。Quarantine Server モニタが有効な場合、JWAC スイッチは、定期的に検疫サーバが正常かどうかをチェックします。検疫サーバを検出できない場合、リダイレクトオプションが有効で、リダイレクト先が検疫サーバに設定されている場合、未認証のすべての HTTP アクセスが JWAC ログインページにリダイレクトされます。
URL	検疫サーバの URL（IPv4/IPv6）を指定します。
Update Server Settings	
IPv4 Network Prefix/Prefix Length	更新用サーバの IPv4 アドレス / プリフィクス長を指定します。 認証が必要なあらゆるサーバはその IP アドレスもしくはネットワークアドレスを追加する必要があります。ネットワークアドレスを追加する事により、エントリは同じネットワークの複数のアップデートサーバにデータを供給することが可能になります。複数のアップデートサーバもしくはネットワークアドレスを設定することが可能です。
IPv6 Network Prefix/Prefix Length	更新用サーバの IPv6 アドレス / プリフィクス長を指定します。
Port (1-65535)	更新サーバが使用するポート番号を選択します。 • TCP - TCP ポートを使う場合、選択します。 • UDP - UDP ポートを使う場合、選択します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Delete」ボタンをクリックして、指定エントリを削除します。
「Add」ボタンをクリックして、入力した情報に基づいたエントリを追加します。

JWAC Port Settings（JWAC ポート設定）

スイッチに JWAC ポート設定を行います。

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

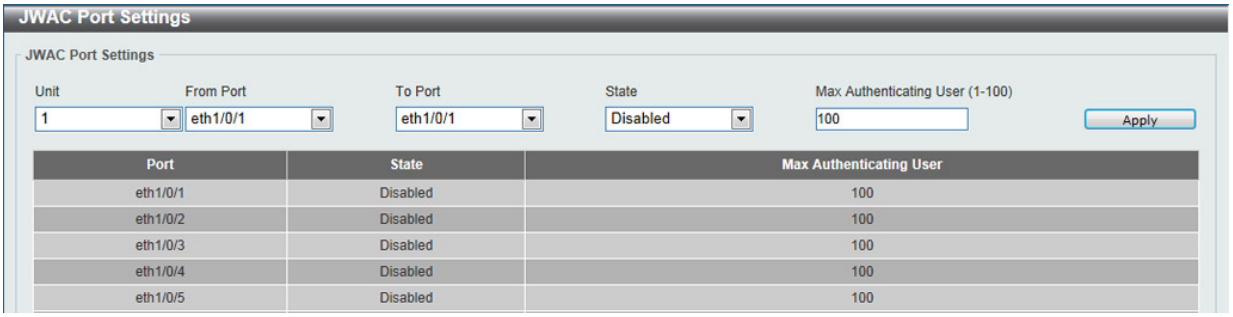


図 12-67　JWAC Port Settings 画面

以下の項目を設定可能です。

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	設定するポート範囲を指定します。
State	プルダウンメニューを使用して JWAC ポートとして設定するポートを有効にします。
Max Authenticating Host (1-100)	同時に各ポートに許可される認証処理を試みるホストの最大数を指定します。

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

JWAC Customize Page Language（JWAC カスタムページ言語設定）

JWAC カスタムページの言語設定を行います。

Security > Japanese Web-based Access Control > JWAC Customize Page Language の順にメニューをクリックし、以下の画面を表示します。



図 12-68　JWAC Customize Page Language 画面

以下の項目を設定可能です。

項目	説明
Customize Page Language	JWAC ログイン時の表示言語を「English」「Japanese」から指定します。

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

JWAC Customize Page（JWAC 画面のカスタマイズ）

JWAC 画面の設定を行います。

Security > Japanese Web-based Access Control > JWAC Customize Page の順にメニューをクリックし、以下の画面を表示します。

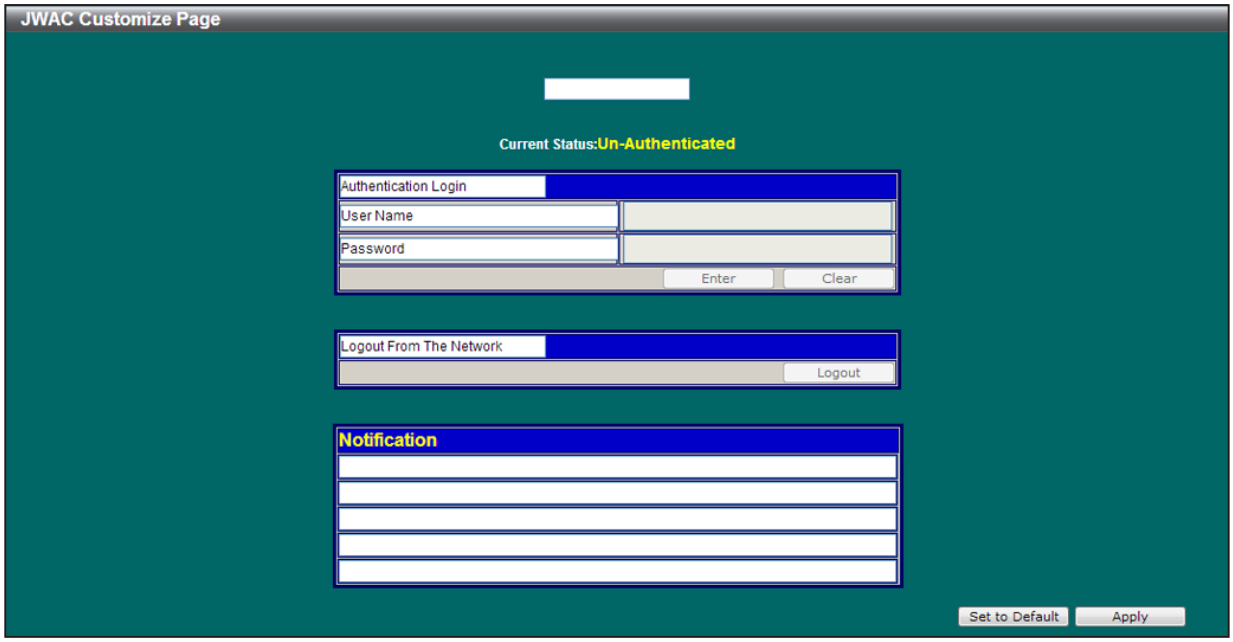


図 12-69　JWAC Customize Page 画面（English）

言語選択で「Japanese」を選択すると以下の画面が表示されます。

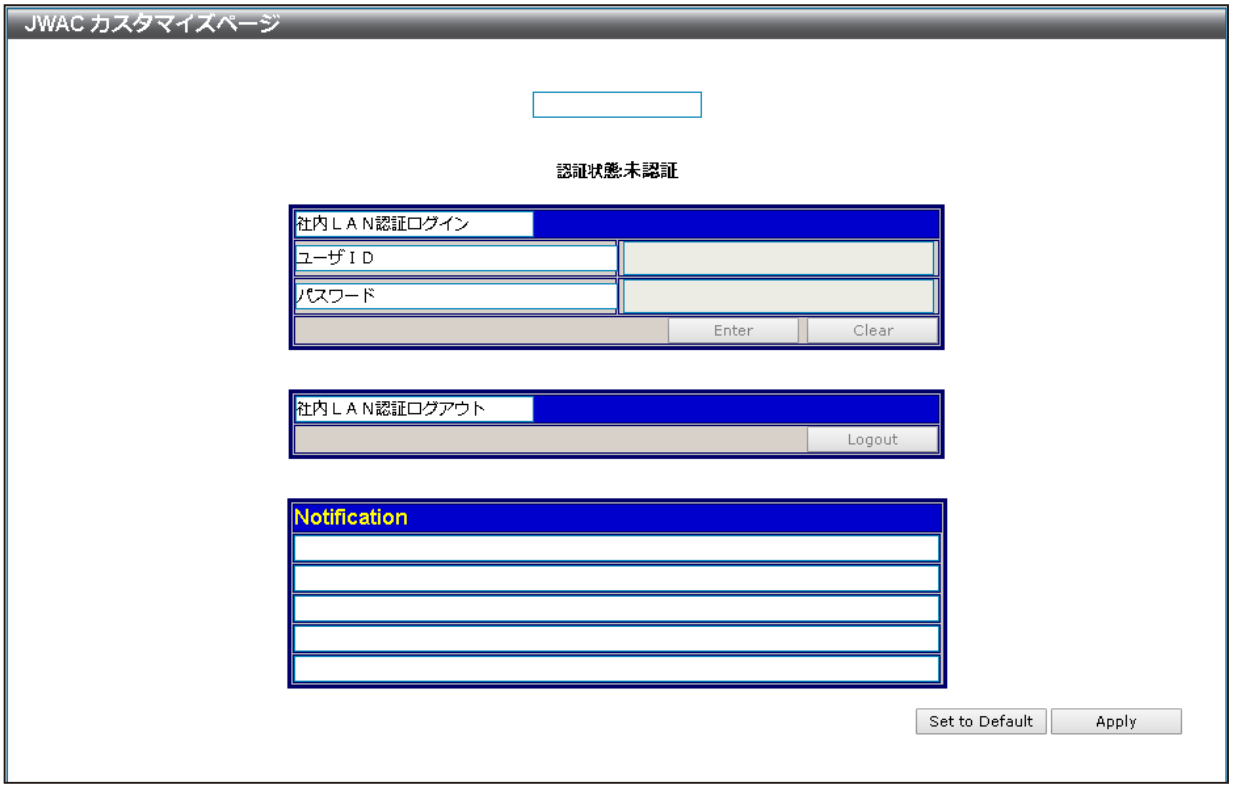


図 12-70　JWAC Customize Page 画面（Japanese）

JWAC 認証情報を入力して、JWAC 画面の設定を行います。最初の欄に認証名を入力し、「Apply」ボタンをクリックします。次にユーザ名とパスワードを入力し、「Enter」ボタンをクリックします。

以下の項目を使用して、設定を行います。

項目	説明
Page Title	カスタムページタイトルとなるメッセージを入力します。128 文字まで入力可能です。
Login window Title	カスタムログインウィンドウタイトルを入力します。64 文字まで入力可能です。
User Name Title	カスタムユーザ名タイトルを入力します。32 文字まで入力可能です。
Password Title	カスタムパスワードタイトルを入力します。32 文字まで入力可能です。
Logout window Title	カスタムログアウトウィンドウタイトルを入力します。64 文字まで入力可能です。
Notification	通知エリアに表示させる情報を入力します。各ライン 128 文字以内で入力可能です。5 ライン入力できます。

「Apply」ボタンをクリックして行った変更を適用します。
「Set to Default」ボタンをクリックして、全項目を初期設定に復元します。

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

Guest VLAN（ゲスト VLAN 設定）

ネットワークアクセス認証のゲスト VLAN の表示、設定を行います。

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

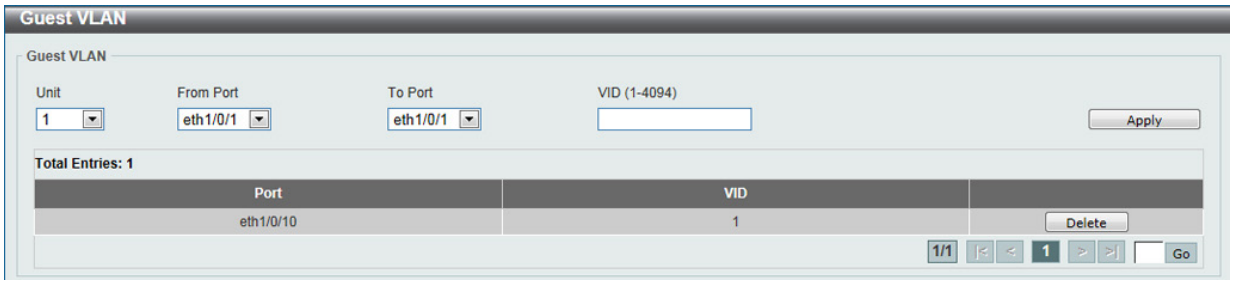


図 12-71　Guest VLAN 画面

以下の項目を使用して設定を行います。

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	設定するポート範囲を指定します。
VID	設定する VLAN ID を入力します。1 から 4094 まで指定できます。

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

Network Access Authentication Global Settings（ネットワークアクセス認証グローバル設定）

ネットワークアクセス認証のグローバルに設定します。

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

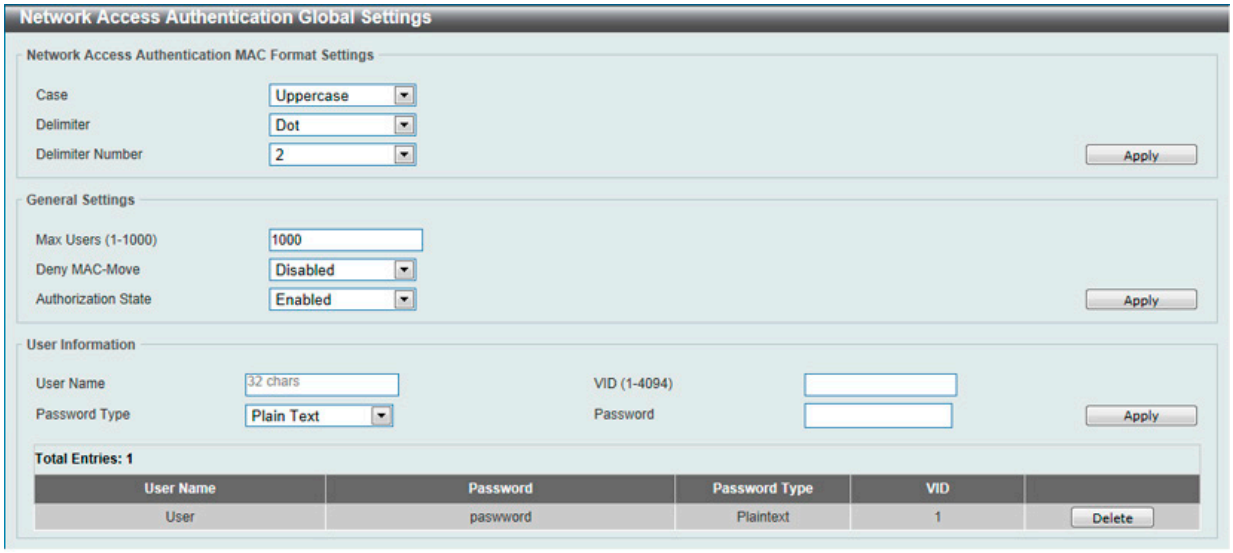


図 12-72　Network Access Authentication Global Settings 画面

本画面には以下の項目があります。

項目	説明
Network Access Authentication MAC Format Settings	
Case	ネットワークアクセス認証に使用する MAC アドレスの形式を「uppercase」（大文字）または「lowercase」（小文字）から選択します。
Delimiter	MAC アドレスを入力する際の区切り「Hyphen」（ハイフン）、「Colon」（コロン）または「Dot」（ドット）を選択します。区切り文字を持たない場合には「None」を選択します。
Delimiter Number	MAC アドレスにおける区切り数を選択します。「1」「2」「5」から指定します。
General Settings	
Max Users	最大ユーザ数を指定します。1 から 1000 の間で指定できます。初期値は 1000 です。

項目	説明
Deny MAC-Move	「MAC-move」機能の拒否を有効 / 無効に指定します。本オプションは、マルチ認証モードに設定されたポートで認証されたホストが、別のスイッチポートにローミングすることを許可するかどうかを設定します。ホストの移動が許可された場合、2 パターンの動作が考えられます。以下に記載するルールに従い、再認証が必要になるか、あるいは再認証なしで新しいポートへ直接移動します。 新しいポートが元々のポートと同じ認証設定である場合： 再認証は不要です。ホストは新しいポートで同じ認証属性を引き継ぎます。認証ホストはポート 1 からポート 2 へローミングが可能であり、再認証なしで認証属性を引き継ぎます。 新しいポートが元々のポートと違う認証設定の場合： 再認証が必要となります。ポート 1 の認証ホストはポート 2 へ移動し、再認証が行われます。新しいポートが認証方式を有効にしていない場合、ホストは直接新しいポートへ移動します。元々のポートとのセッションは削除されます。ポート 1 の認証ホストはポート 2 へ移動可能です。 本機能が無効の場合、認証ホストは他のポートへ移動可能ですが違反エラーとして認識されます。
Authorization State	認証許可の有効 / 無効を指定します。本項目が有効化されている場合、認証に対して認可が行われると、RADIUS サーバにより付与される権限属性（VLAN、802.1p default priority、bandwidth、ACL など）が許可されます。「Bandwidth」「ACL」はポートベースでアサインされます。マルチ認証モードの場合「VLAN」と「802.1p」は各ホストベースでアサインされます。認証が有効でない場合、「Bandwidth」「ACL」は各ポートベースでアサインされます。
User Information	
User Name	ユーザ名を入力します。32 文字まで入力可能です。
VID	VLAN ID を入力します。
Password Type	パスワード種類を選択します。「Plain Text」「Encrypted」から選択可能です。
Password	パスワードを入力します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Delete」ボタンをクリックして、指定エントリを削除します。

Network Access Authentication Port Settings（ネットワークアクセス認証ポート設定）

ネットワークアクセス認証のポート設定を行います。

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

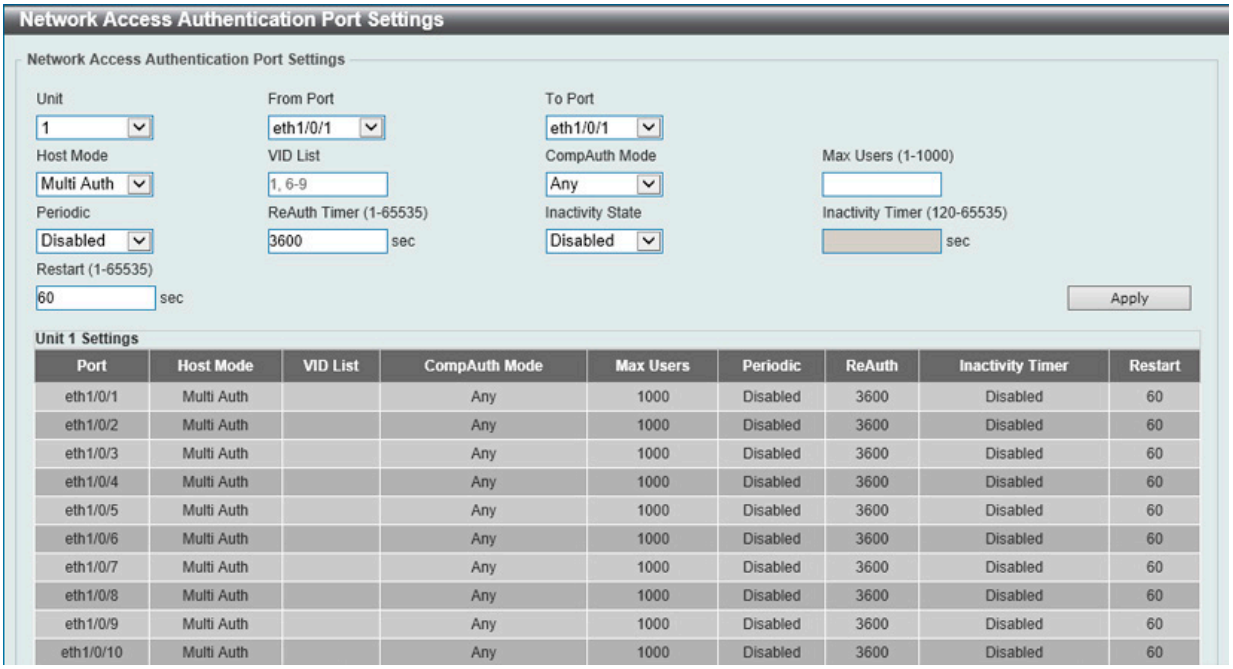


図 12-73　Network Access Authentication Port Settings 画面

以下の項目を使用して設定を行います。

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	設定するポート範囲を指定します。

項目	説明
Host Mode	選択ポートと関連するホストモードを選択します。「Multi Host」「Multi Auth」から選択します。ポートがマルチホストモードで動作していて一つのホストが認証されている場合、すべての他のホストはポートへのアクセスを許可されます。802.1X 認証に従い、再認証失敗や認証ユーザーのログオフなどの場合、ポートはしばらくの間ブロックされます。一定期間終了後 EAPOL パケットのプロセスにてポートはリストアします。ポートがマルチ認証モードで動作しており、各ホストがポートへのアクセスに認証が必要な場合、ホストは MAC アドレスにより識別され、認証されたホストのみポートへのアクセスが可能になります。
VID List	ホストモードでマルチ認証オプション（Multi Auth）を選択した後、次のパラメータが有効になります。使用する VLAN ID を入力します。スイッチ上の各 VLAN が異なる認証要件を持つ場合に有効です。クライアントが認証されたのちに、他の VLAN から受信してもクライアントは再認証されません。このオプションは、トランクポートで VLAN 単位の認証制御を行う場合に有効です。ポートの認証モードがマルチホストに変更された場合、ポートにある以前の認証 VLAN はクリアされます。
CompAuth Mode	コンパウンド認証モードのオプションを選択します。「Any」「MAC-JWAC」「MAC-WAC」から選択します。「Any」を選択すると、あらゆる認証方式（802.1X, MAC-based Access Control, WAC, JWAC）のどれかで認証します。「MAC-JWAC」を選択すると MAC ベースの認証を最初に検証します。クライアントがパスした場合、JWAC が次に検証されます。両方の認証方法をパスする必要があります。「MAC-WAC」を選択すると MAC ベースの認証を最初に検証します。クライアントがパスをすると、WAC が次に検証され、最終的には両方が認証がパスされる必要があります。
Max Users	最大ユーザ数を指定します。1 から 1000 の間で指定できます。
Periodic	選択ポートの定期再認証を有効 / 無効にします。802.1X プロトコルにのみ影響します。
ReAuth Timer	再認証時間を指定します。1 から 65535（秒）で指定します。初期値では 3600 秒です。
Inactivity State	「Inactivity」（休止）を有効 / 無効に指定します。
Inactivity Timer	「Inactivity」（休止）を有効にした場合、休止時間の値を入力します。120 から 65535（秒）です。このパラメータは WAC と JWAC の認証プロトコルにのみ影響します。
Restart	リスタート時間を入力します。1 から 65535（秒）の間で指定可能です。

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

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

ネットワークアクセス認証セッションの情報表示、クリアを行います。

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

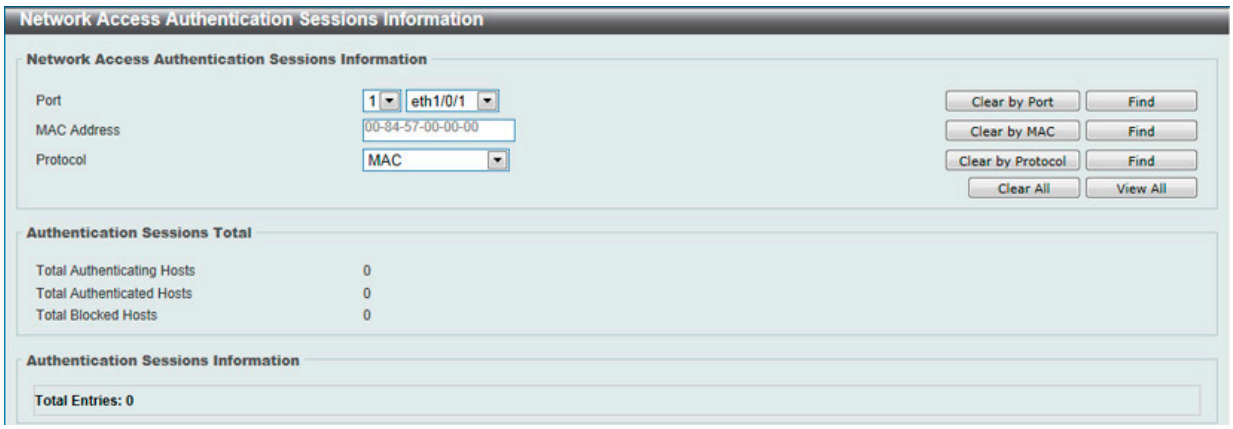


図 12-74　Network Access Authentication Sessions Information 画面

以下の項目を使用して設定を行います。

項目	説明
Port	表示するポートとユニットを指定します。
MAC Address	表示する MAC アドレスを指定します。
Protocol	プロトコルオプションを選択します。「MAC」「WAC」「JWAC」「DOT1X」から選択します。

「Apply」ボタンをクリックし、設定を有効にします。
「Clear by Port」ボタンをクリックし、選択したポートに基づく情報を消去します。
「Clear by MAC」ボタンをクリックし、選択した MAC アドレスに基づく情報を消去します。
「Clear by Protocol」ボタンをクリックし、選択したプロトコルに基づく情報を消去します。
「Clear All」ボタンをクリックし、テーブル上のすべての情報を消去します。
「Find」ボタンをクリックし、入力した情報を元に指定のエントリを検出します。
「View All」ボタンをクリックし、すべてのエントリを表示します。

Safeguard Engine（セーフガードエンジン）

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

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

CPU に宛てられるパケットは 3 つのグループに分類されます。サブインタフェースとしても知られるこれらのグループは CPU が特定の種類のトラフィックを認識するうえで使用する論理的なインタフェースです。この 3 つのグループは「Protocol」「Manage」「Route」があります。通常、「Protocol」グループは、スイッチの CPU プロセスがパケットを受信した時に、最高のプライオリティ受信し、そして「Route」グループは、スイッチの CPU が入り込むルーティングパケットのプロセスの中で、グループの最低の優先値を受信します。「Protocol」グループでのパケットはルータによって識別されたプロトコルコントロールパケットです。管理（Manage）グループ内で、パケットは Telent や SSH と同様に、インタラクティブアクセスプロトコルの内容でルータやシステムネットワークマネジメントインタフェースへ向かいます。「Route」グループではパケットは 通常ルータ CPU トラバース（行ったり来たり）するルートパケットとして認識されます。

以下の表ではプロトコルと対応するサブインタフェースを表示します。

プロトコル名	サブインタフェース（グループ）	概要
802.1X	Protocol	Port-based Network Access Control（ポートベースアクセスコントロール）
ARP	Protocol	Address resolution Protocol (ARP)
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-Neighbor）
ICMPv6-Other	Protocol	IPv6 Internet Control Message Protocol except Neighbor Discovery Protocol (NS/NA/RS/RA)（ICMPv6-Other）
IGMP	Protocol	Internet Group Management Protocol（IGMP）
LACP	Protocol	Link Aggregation Control Protocol（LACP）
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 / 毎秒）、を管理インタフェースで指定された全てまたは個々のプロトコルとしてセーフガードエンジンのサブインタフェースにアサインすることが可能です。不適切なレート制限により、スイッチがパケットを以上に処理する可能性があるため、この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は注意してください。

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

Safeguard Engine Settings（セーフガードエンジン設定）

スイッチにセーフガードエンジンの設定を行うためには、**Security > Safeguard Engine > Safeguard Engine Settings** の順にクリックし、以下の画面を表示します。

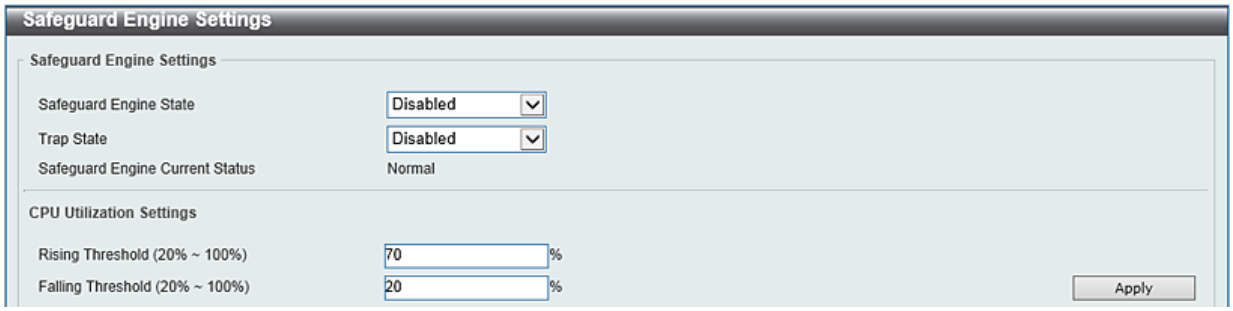


図 12-75　Safeguard Engine Settings 画面

以下の項目を使用して、設定を行います。

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

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

CPU Protect Counters（CPU プロテクトカウンタ）

CPU プロテクションのカウンタ情報を表示、消去します。
Security > Safeguard Engine > CPU Protect Counters の順にクリックし、以下の画面を表示します。

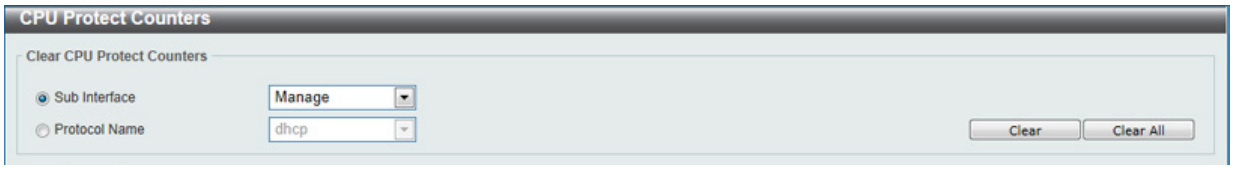


図 12-76　CPU Protect Counters 画面

以下の項目を使用して、設定を行います。

項目	説明
Sub Interface	サブインタフェースのオプションを選択します。「Manage」「Protocol」「Route」「All」から選択します。 CPU プロテクトに関連したサブインタフェースのカウンタの消去を指定します。
Protocol Name	プロトコル名のオプションを選択します。「DHCP」「ARP」「DNS」「GVRP」「ICMPv4」「ICMPv6-Neighbor」「ICMPv6-Other」「IGMP」「LACP」「SNMP」「SSH」「STP」「Telnet」「TFTP」「Web」「802.1X」「All」から指定します。

「Clear」ボタンをクリックし、設定に基づいた情報を消去します。
「Clear All」ボタンをクリックし、すべての情報を消去します。

CPU Protect Sub-Interface（CPU プロテクトサブインタフェース）

CPU プロテクションのサブインタフェースを設定、表示します。
Security > Safeguard Engine > CPU Protect Sub-Interface の順にクリックし、以下の画面を表示します。

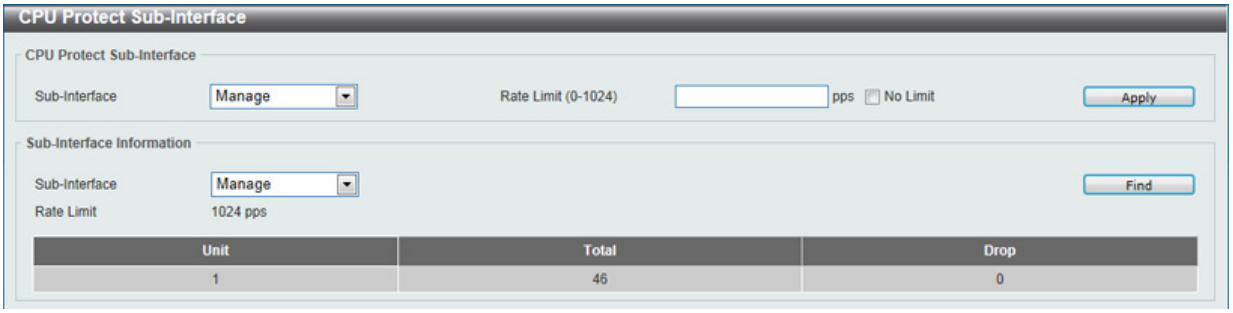


図 12-77　CPU Protect Sub-Interface 画面

以下の項目を使用して、設定を行います。

項目	説明
CPU Protect Sub-Interface（CPU プロテクトサブインタフェース）	
Sub Interface	サブインタフェースのオプションを選択します。「Manage」「Protocol」「Route」から選択します。
Rate Limit	レートリミットの値を入力します。0 から 1024 パケット / 毎秒の間で指定できます。 「No Limit」を指定するとレートリミットを無効にします。

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

項目	説明
Sub-Interface Information（サブインタフェース情報）	
Sub Interface	サブインタフェースのオプションを選択します。「Manage」「Protocol」「Route」から選択します。

「Find」ボタンをクリックし、入力した情報を元に指定エントリを検出します。

CPU Protect Type（CPU プロテクトタイプ）

CPU プロテクションの種類の設定、表示します。
Security > Safeguard Engine > CPU Protect Type の順にクリックし、以下の画面を表示します。

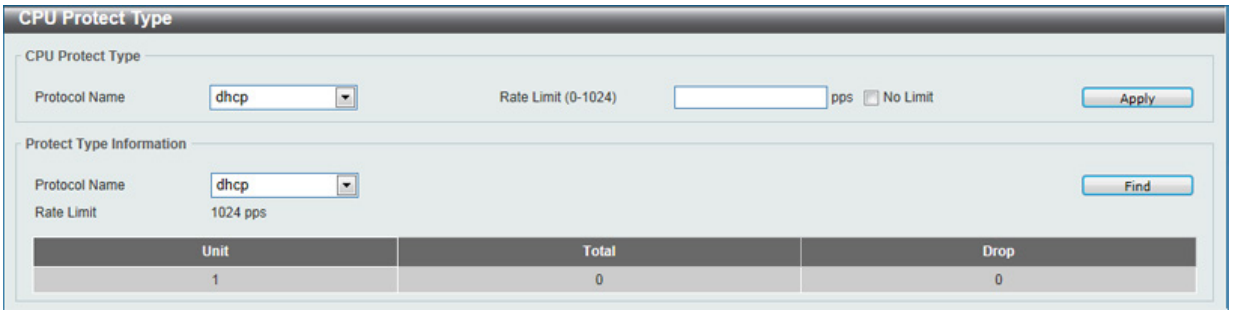


図 12-78　CPU Protect Type 画面

以下の項目を使用して、設定を行います。

項目	説明
CPU Protect Type（CPU プロテクトタイプ）	
Protocol Name	プロトコル名のオプションを選択します。「DHCP」「ARP」「DNS」「GVRP」「ICMPv4」「ICMPv6-Neighbor」「ICMPv6-Other」「IGMP」「LACP」「SNMP」「SSH」「STP」「Telnet」「TFTP」「Web」「802.1X」から指定します。
Rate Limit	レートリミットの値を入力します。0 から 1024 パケット / 毎秒の間で指定できます。 「No Limit」を指定するとレートリミットを無効にします。

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

項目	説明
Protect Type Information（プロテクトタイプ情報）	
Protocol Name	プロトコル名のオプションを選択します。「DHCP」「ARP」「DNS」「GVRP」「ICMPv4」「ICMPv6-Neighbor」「ICMPv6-Other」「IGMP」「LACP」「SNMP」「SSH」「STP」「Telnet」「TFTP」「Web」「802.1X」から指定します。

「Find」ボタンをクリックし、入力した情報を元に指定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。

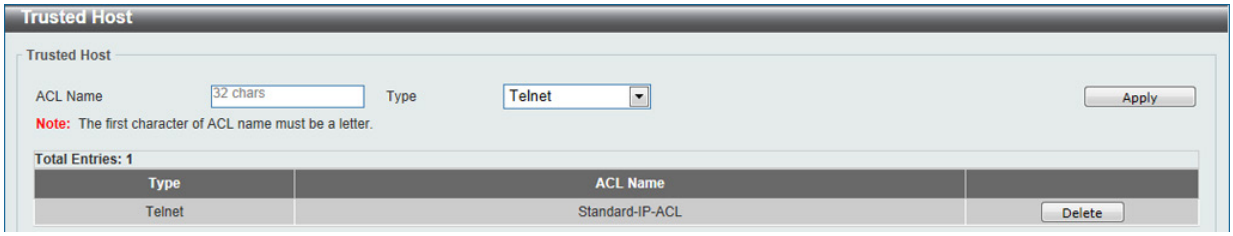


図 12-79　Trusted Host 画面

以下の項目を使用して、設定を行います。

項目	説明
ACL Name	使用する ACL 名を入力します。32 文字までで指定可能です。
Type	トラストホストの種類を指定します。「Telnet」「SSH」「Ping」「HTTP」「HTTPS」から指定します。

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

Traffic Segmentation 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。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、ポートに受信するパケットはドメイン内のインタフェースに転送される L2 パケットに制限されます。ポートの転送ドメインが空の場合、ポートに受信したパケットの L2 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メンバリストは認証が有効でない場合、コマンドによってポートチャンネルを含めたインタフェースが指定されると、ポートチャネルのすべてのメンバポートは転送ドメインに含まれます。インタフェースの転送ドメインが空の場合、ポートに受信したパケットの L2 転送は制限されません。

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

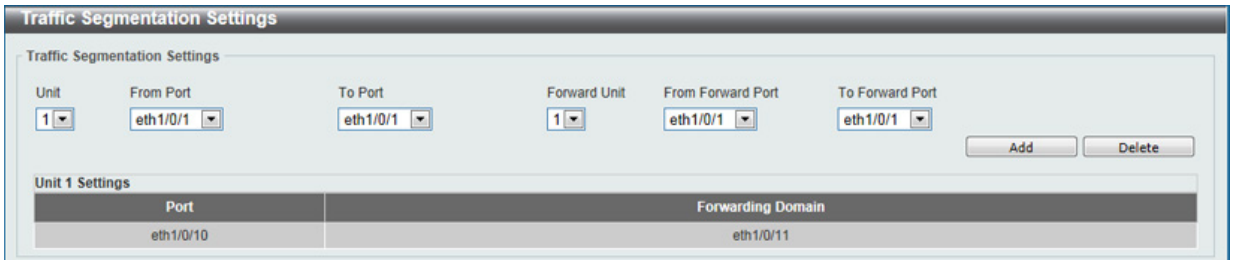


図 12-80　Traffic Segmentation Settings 画面

以下の項目を使用して設定を行います。

項目	説明
Unit	設定する受信スイッチユニットを選択します。
From Port / To Port	設定する受信ポート範囲を指定します。
Forward Unit	設定する転送スイッチユニットを指定します。
From Forward Port / To Forward Port	設定する転送ポート範囲を指定します。

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

Storm Control Settings（ストームコントロール設定）

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

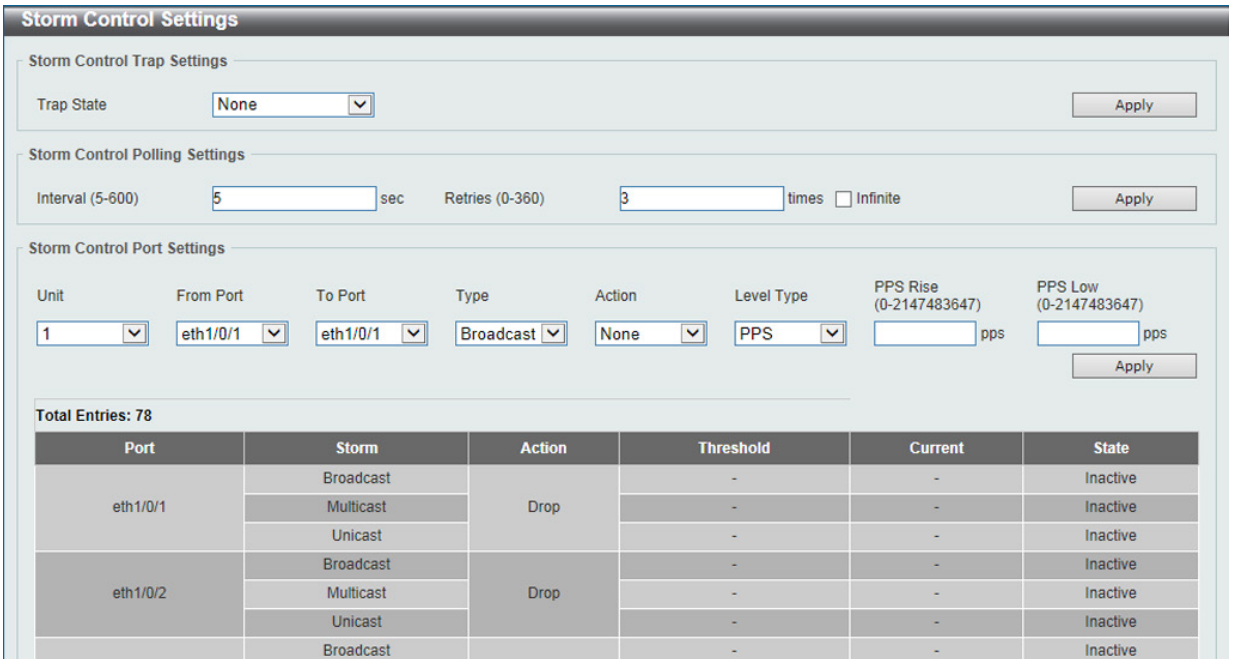


図 12-81　Storm Control Settings 画面

以下の項目を使用して、設定を行います。

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

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

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

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

項目	説明
Storm Control Port Settings（ストームコントロールポート設定）	
Unit	設定するユニットを選択します。
From Port / To Port	設定するポート範囲を指定します。
Type	コントロールするストームの種類を選択します。「Broadcast」「Multicast」「Unicast」から指定できます。シャットダウンモードで選択すると、ユニキャストは「Known」「Unknown」両方が設定してある場合、どちらにも対応しポートはシャットダウンします。そうでない場合は「Unknown」にのみ対応します。
Action	動作について指定します。「None」「Shutdown」「Drop」から指定します。「None」を指定するとストームパケットをフィルタしません。「Shutdown」は選択すると、指定したしきい値に達するとポートはシャットダウンされます。「Drop」を選択すると指定したしきい値に達するとパケットを破棄します。
Level Type	レベルタイプを指定します。「PPS」「Kbps」「Level」から選択します。
PPS Rise	毎秒のパケット増加の上限値について指定します。毎秒増加するパケットの量について上限しきい値を指定します。0 から 2147483647 パケット毎秒で指定できます。「Low PPS」の値が指定されていない場合、初期値は増加したパケット毎秒の 80%に指定されます。
PPS Low	毎秒のパケット減少の下限値について指定します。毎秒減少するパケットの量について下限しきい値を指定します。0 から 2147483647 パケット毎秒で指定できます。「Low PPS」の値が指定されていない場合、初期値は増加したパケット毎秒の 80%に指定されます。

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

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

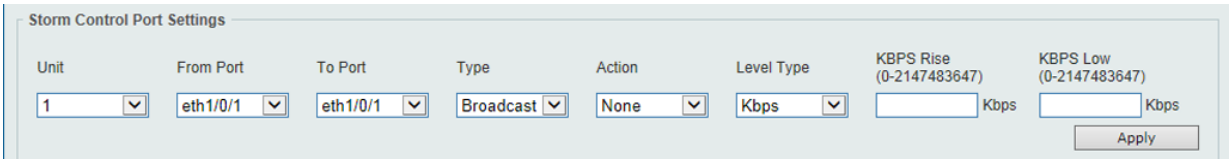


図 12-82　Storm Control (Kbps) 画面

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

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

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

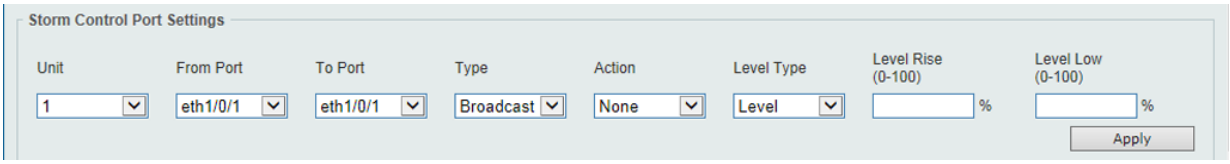


図 12-83　Storm Control (Level) 画面

項目	説明
Level Rise	下限レベルについて入力します。本オプションはポートに受信するトラフィックの総帯域のパーセンテージを上限のしきい値として指定します。0 から 100%で指定可能です。
Level Low	下限レベルについて入力します。本オプションはポートに受信するトラフィックの総帯域のパーセンテージを下限のしきい値として指定します。0 から 100%で指定可能です。「Level Low」の値が指定されていない場合、初期値は増加したパケット毎秒の 80%に指定されます。

注意　Level に 0 を指定した場合、H/W Entry が作成されるまでの間、スイッチは対象の通信を許可します。

注意　Multicast を指定した場合、予約 MAC Address(VRRP、OSPF、IGMP、MLD など) に対する制限は適用されません。

注意　% および kbps を指定した場合は、受信 Frame Size を　64 Octet 固定長とし、Packet per second に基づいて表示するため、状態を正しく反映しません。

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

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

各 DoS 攻撃に対して防御設定を行います。

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

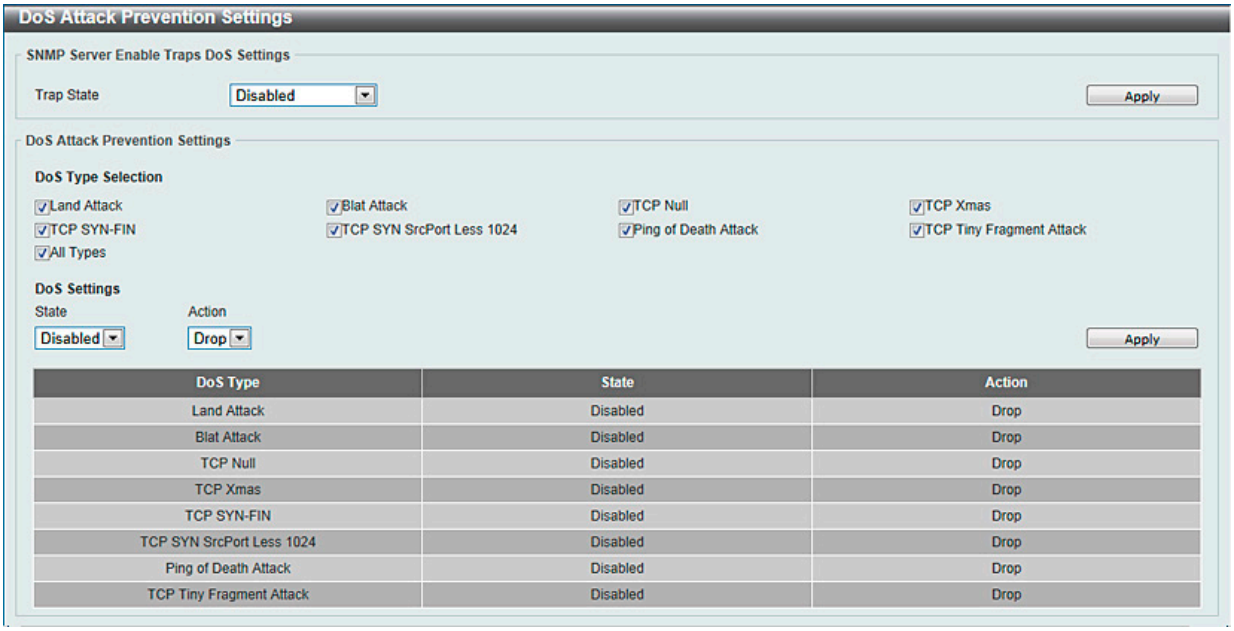


図 12-84　DoS Attack Prevention Settings 画面

設定および表示する項目は以下の通りです。

項目	説明
SNMP Server Enable Traps DoS Settings	
Trap State	本オプションは、DoS 攻撃防止トラップ状態を有効または無効にします。
DoS Attack Prevention Settings	
DoS Type Selection	適切な DoS 攻撃防御のタイプを選択します。 • Land Attack - DoS 攻撃防止タイプに LAND 攻撃を指定します。 • Blat Attack - DoS 攻撃防止タイプに BLAT 攻撃を指定します。 • TCP Null - DoS 攻撃防止タイプに TCP Null Scan 攻撃を指定します。 • TCP Xmas - DoS 攻撃防止タイプに TCP Xmascan 攻撃を指定します。 • TCP SYN-FIN - DoS 攻撃防止タイプに TCP SYNFIN 攻撃を指定します。 • TCP SYN SrcPort Less 1024 - DoS 攻撃防止タイプに TCP SYN Source Port Less 1024 攻撃を指定します。 • Ping Death Attack -「Ping Death Attack」はコンピュータに対し変形した、または悪意のある Ping を送信するタイプの攻撃です。Ping は通常 64 バイト（多くのコンピュータは最大 IP パケットサイズを超えた Ping を処理できない）ですが、「Death Ping」は 65535 バイトです。このサイズの Ping の送信は攻撃対象のコンピュータをクラッシュさせます。歴史的にこのバグは比較的安易に使用されてきました。通常 65536 バイトの Ping パケット送信はネットワーキングプロトコルにおいて不法ですが、分割されたものであれば送信できてしまいます。（コンピュータによるパケット結合作業はしばしばオーバーフロウを発生させ、システムをクラッシュさせます。） • TCP Tiny Fragment Attack -「Tiny TCP Fragment 攻撃者」は IP フラグメンテーションを使用し、極端に小さいフラグメントを作成、ルータのチェックをパスさせ攻撃を発生させるために、分割したパケットフラグメントに TCP ヘッダ情報を強制します。 • All Types - DoS 攻撃防止タイプにすべての攻撃を指定します。
State	DoS 攻撃防止の状態を指定します。 • Enabled - DoS 攻撃防止の状態を有効にします。 • Disabled - DoS 攻撃防止の状態を無効にします。
Action	DoS 攻撃防止機能により行われる操作を指定します。 • Drop - 一致する DoS 攻撃パケットをすべて破棄します。

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

SSH（Secure Shell 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」**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 Authentication Mode」画面を使用して、ユーザアカウントを設定します。この時スイッチが SSH 接続の確立を許可する際のユーザの認証方法を指定します。この認証方法には、「Host Based」、「Password」、「Public Key」の 3 つがあります。
3. 「SSH Authmode and Algorithm Settings」画面を使用して、SSH クライアントとサーバ間で送受信するメッセージの暗号化、復号化に用いる暗号化アルゴリズムを設定します。
4. 最後に「SSH Configuration」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。

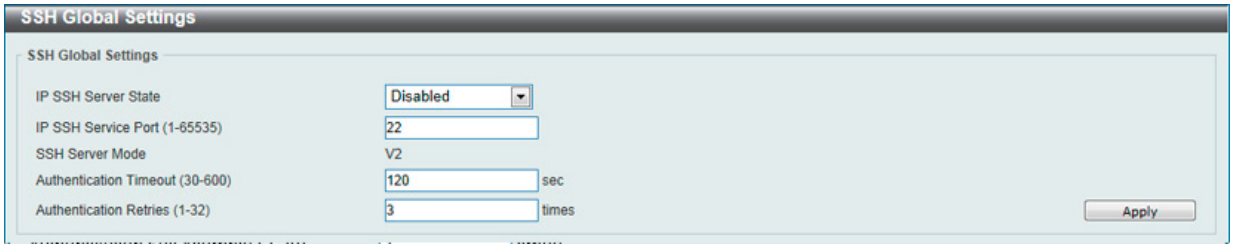


図 12-85　SSH Global Settings 画面

設定および表示する項目は以下の通りです。

項目	説明
IP SSH Server State	グローバルに SSH 機能を「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Disabled」です。
IP SSH Service Port (1-65535)	SSH サービスポート番号を設定します。初期値は 22 です。
Authentication Timeout(30-600)	認証のタイムアウト時間を指定します。30 から 600（秒）が指定できます。初期値は 120（秒）です。
Authentication Retries (1-32)	ユーザが SSH サーバに対して認証を試みることができる回数を指定します。指定した回数を超えるとスイッチは接続を切り、ユーザは再度スイッチに接続する必要があります。1 から 32 が指定できます。初期値は 3 です。

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

Host Key（Host Key 設定）

SSH ホスト鍵の設定（有効化）および設定内容の確認に使用します。

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

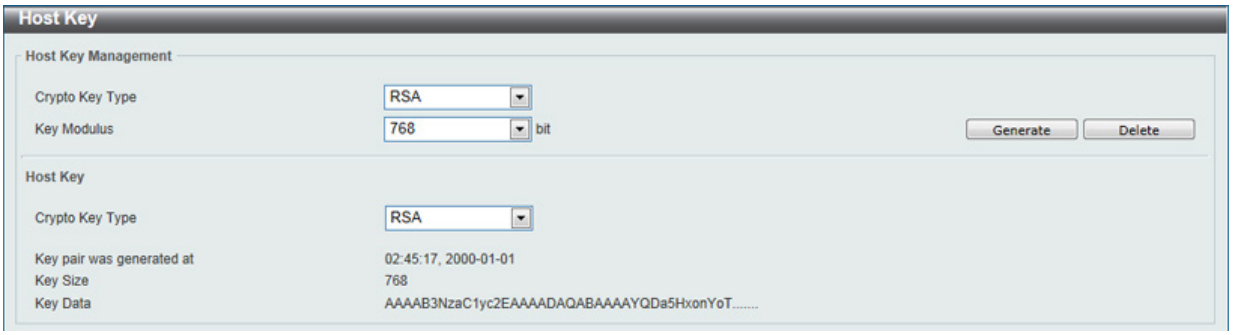


図 12-86　Host Key 画面

設定および表示する項目は以下の通りです。

項目	説明
Host Key Management	
Crypto Key Type	暗号鍵の種類を選択します。「Rivest Shamir Adleman (RSA)」または「Digital Signature Algorithm (DSA)」から選択します。
Key Modulus	鍵係数の値を入力します。「360」「512」「768」「1024」「2048」ビットから選択します。
Host Key	
Crypto Key Type	暗号鍵の種類を選択します。「Rivest Shamir Adleman (RSA)」または「Digital Signature Algorithm (DSA)」から選択します。

「Generate」ボタンをクリックし、指定したホスト鍵を有効にします。
「Delete」ボタンをクリックし、指定したホスト鍵を削除します。

注意　スタック構成において、設定済みで「Key」の無い「Stack slave」を組み込んだ場合は同期されません。

SSH Server Connection（SSH サーバ接続）

SSH サーバ接続テーブルの内容を確認します。

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



図 12-87　SSH Server Connection 画面

表示されるエントリの内容を確認します。

SSH User Settings（SSH ユーザ設定）

SSH ユーザの設定および設定内容を確認します。

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



図 12-88　SSH User Settings 画面

以下の項目を使用して、参照または設定を行います。

項目	説明
User Name	SSH ユーザを識別するユーザ名を 32 文字までの半角英数字で指定します。
Authentication Method	スイッチにアクセスを試みるユーザの認証モードを以下から指定します。 • Host Based - 認証用にリモート SSH サーバを使用する場合に選択します。本項目を選択すると、SSH ユーザ識別のために以下の情報を入力することが必要になります。 • Password - 管理者定義のパスワードを使用して認証を行う場合に選択します。本項目を選択すると、スイッチは管理者にパスワードの入力（確認のため 2 回）を促します。 • Public Key - SSH サーバ上の公開鍵を使用して認証を行う場合に選択します。
Key File	「Public Key」または「Host-based」を選択した場合ここで公開鍵（Public Key）を入力します。
Host Name	リモート SSH ユーザのホスト名を入力します。本項目は「Authentication Method」で「Host Based」を選択した場合のみ入力が必要です。
IPv4 Address	SSH ユーザの IPv4 アドレスを入力します。本項目は「Authentication Method」で「Host Based」を選択した場合のみ入力が必要です。
IPv6 Address	SSH ユーザの IPv6 アドレスを入力します。本項目は「Authentication Method」で「Host Based」を選択した場合のみ入力が必要です。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

SSL（Secure Socket Layer）

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

1. 鍵交換（Key Exchange）
   暗号スイート文字列の最初の部分では、使用する公開鍵アルゴリズムを規定しています。本スイッチは、RSA（Rivest Shamir Adleman）公開鍵アルゴリズムとデジタル署名アルゴリズム（DSA、ここでは DHE : DHE DSS Diffie-Hellman 公開鍵アルゴリズムとして指定）を使用します。これはクライアントとホスト間の最初の認証プロセスであり、「鍵交換」を行って一致した場合、認証が受諾され、以下のレベルで暗号化のネゴシエーションが行われます。
2. 暗号化（Encryption）
   暗号スイートの次の部分は、クライアントとホスト間で送受信するメッセージの暗号化を含む暗号化方式です。本スイッチは 2 種類の暗号化アルゴリズムをサポートしています。
   - ストリーム暗号（Stream Ciphers）– スイッチは 2 種類のストリーム暗号（40 ビット鍵での RC4 と、128 ビット鍵での RC4）に対応しています。これらの鍵はメッセージの暗号化に使用され、最適に利用するためにはクライアントとホスト間で一致させる必要があります。
   - CBC ブロック暗号 – CBC（Cipher Block Chaining : 暗号ブロック連鎖）とは、1 つ前の暗号化テキストのブロックを使用して、現在のブロックの暗号化を行う方法です。本スイッチは、DES（Data Encryption Standard）で定義される 3 DES EDE 暗号化コードと高度な暗号化規格（AES）をサポートし、暗号化されたテキストを生成します。
3. ハッシュアルゴリズム（Hash Algorithm）
   暗号スイートの最後の段階では、メッセージ認証コードを決定するメッセージダイジェスト機能を規定します。このメッセージ認証コードは送信されたメッセージと共に暗号化され、整合性を提供し、リプレイアタックを防止します。本スイッチは、MD5（Message Digest 5）と SHA（Secure Hash Algorithm）、SHA-256 の 3 つのハッシュアルゴリズムをサポートします。

サーバとホスト間で安全な通信を行うための 3 層の暗号化コードを生成するために、これら 3 つのパラメータの一意の組み合わせである 11 種類の暗号化スイートについてスイッチ上で設定が可能です。それぞれの暗号化スイートに対して有効 / 無効の設定を行うことが可能ですが、選択する暗号スイートによりセキュリティレベルや安全な接続時のパフォーマンスは変化します。また、本スイッチは、TLSv1/v2/v3 をサポートしています。それ以外のバージョンは本スイッチとは互換性がない恐れがあり、クライアントからホストへの認証やメッセージ送信時に問題が発生する可能性があります。

「SSL Global Settings」および「SSL Service Policy」画面では、スイッチで SSL を有効にして各種暗号スイートのステータスを設定することができます。暗号スイートは、認証セッションに使用される正確な暗号のパラメータ、特定の暗号化アルゴリズム、および鍵のサイズを決定するセキュリティ文字列です。スイッチには 11 個の暗号スイート設定が用意されています。特定の暗号スイートのみ有効にして、他のものを無効にすることが可能です。

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

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

SSL Global Settings（SSL グローバル設定）

SSL グローバル設定を行います。

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

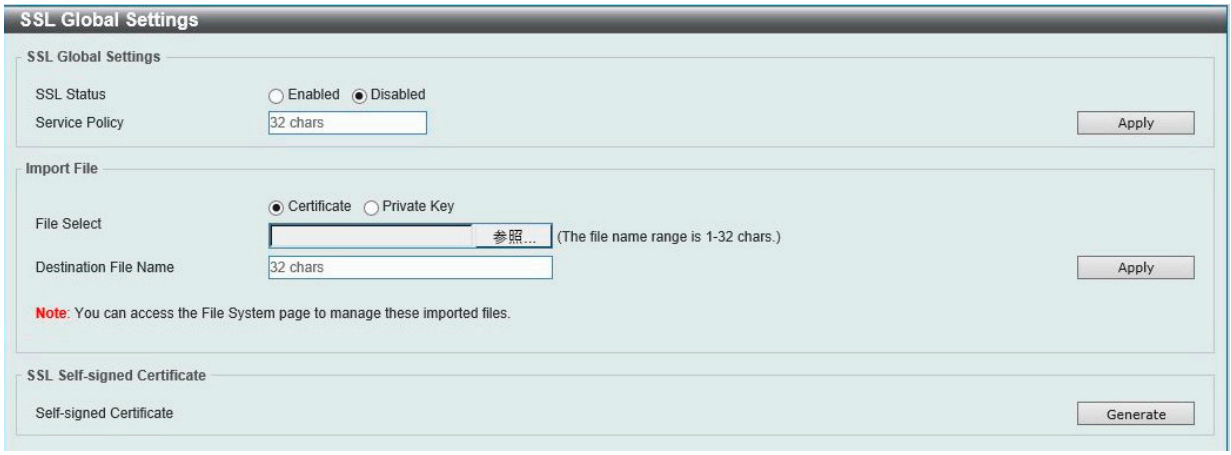


図 12-89　SSL Global Settings 画面

以下の項目を使用して、参照または設定を行います。

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

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

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

「SSL-Self-signed Certificate」セクションの「Generate」ボタンをクリックすると、既存の自己署名証明書の有無にかかわらず、新しい自己署名証明書が生成されます。ユーザがダウンロードした証明書には影響ありません。

注意　本 SSL 自己署名証明書は、2048bit キー長の自己署名 RSA 証明書のみをサポートしています。

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

暗号 PKI トラストポイントの表示、設定を行います。

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

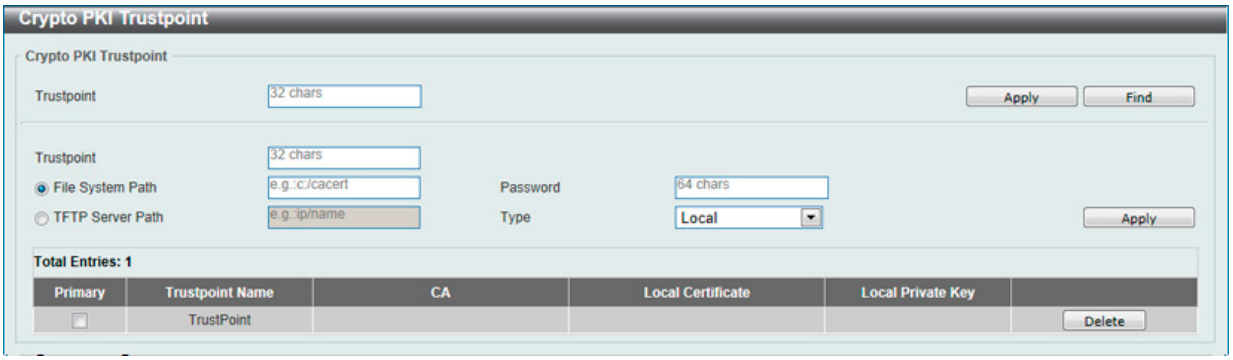


図 12-90　Crypto PKI Trustpoint 画面

以下の項目を使用して、参照または設定を行います。

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

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

SSL Service Policy（SSL サービスポリシー）

SSL サービスポリシーの表示、設定を行います。

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

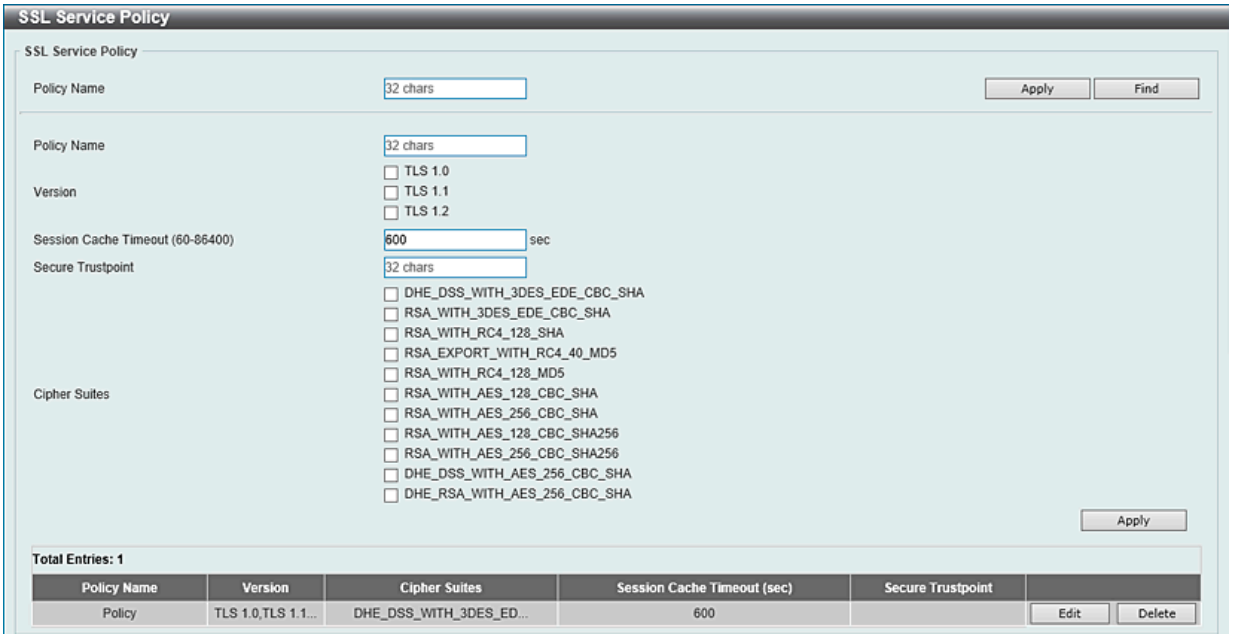


図 12-91　SSL Service Policy 画面

以下の項目を使用して、参照または設定を行います。

項目	説明
Policy Name	SSL サービスポリシー名を入力します。32 文字まで指定可能です。

項目	説明
Version	「TLS 1.0」「TLS 1.1」「TLS1.2」から TLS のバージョンを指定します。
Session Cache Timeout	セッションキャッシュタイムアウトの時間（60-86400）秒を指定します。初期値は 600（秒）です。
Secure Trustpoint	セキュアなトラストポイントの名前を入力します。32 文字まで指定可能です。
Cipher Suites	本プロファイルの暗号スイートを選択します。

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

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、以下の画面を表示します。



図 12-92　Network Protocol Port Protection Settings 画面

以下の項目を使用して、設定を行います。

項目	説明
TCP Port Protect State	TCP ネットワークプロトコルポートプロテクション機能の有効 / 無効を指定します。
UDP Port Protect State	UDP ネットワークプロトコルポートプロテクション機能の有効 / 無効を指定します。

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

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

故障診断機能を設定します。

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

サブメニュー	説明
Cable Diagnostics（ケーブル診断機能）	ケーブル診断を行います。
DDM（DDM 設定）	DDM の設定を行います。

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主に管理者とカスタマサービス担当者が UTP ケーブルを検査、テストするために設計されています。ケーブルの品質やエラーの種類を即座に診断します。

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

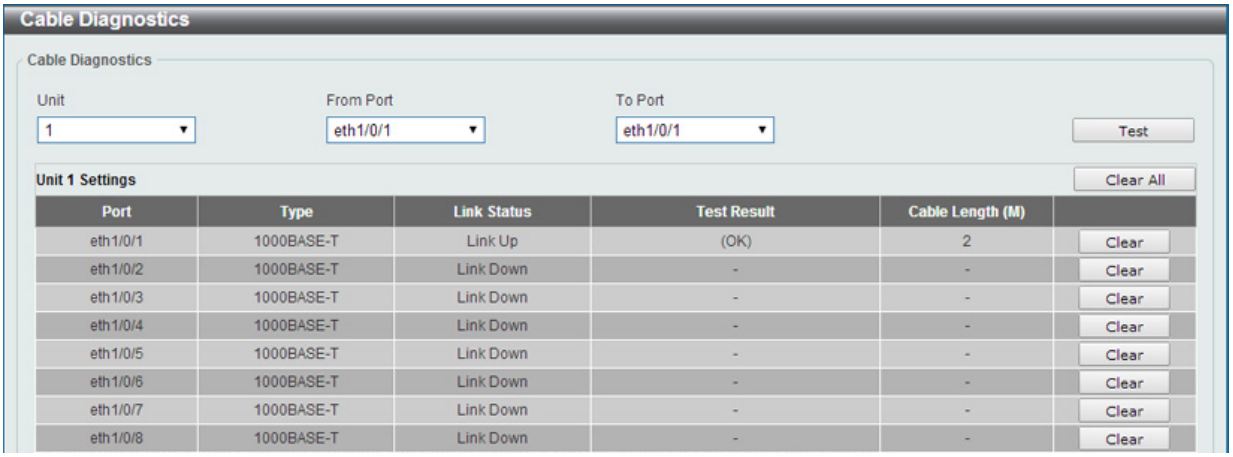


図 13-1　Cable Diagnostics 画面

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

DDM（DDM 設定）

本フォルダにはスイッチに Digital Diagnostic Monitoring（DDM）機能を実行する画面があります。これらの画面により、スイッチに挿入した SFP モジュールの DDM 状態の参照、各種設定（アラーム設定、警告設定、温度しきい値設定、電圧しきい値設定、バイアス電流しきい値設定、Tx（送信）電力しきい値設定、および Rx（受信）電力しきい値設定）を行うことができます。

DDM Settings（DDM 設定）

超過しているアラームしきい値または警告しきい値を超過するイベントが発生した場合に、指定ポートに行う動作を設定します。

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

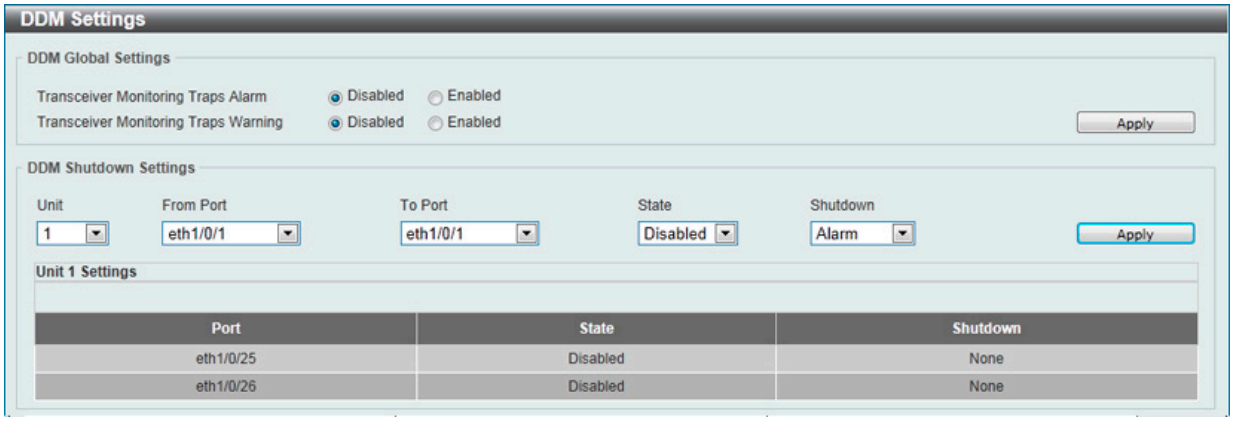


図 13-2　DDM Settings 画面

以下の項目を使用して設定します。

項目	説明
Transceiver Monitoring Traps Alarm	アラームしきい値を超過した際にトラップを送信するか否かを指定します。
Transceiver Monitoring Traps Warning	警告しきい値を超過した際にトラップを送信するか否かを指定します。
Unit	設定するユニットを選択します。
From Port / To Port	設定するポート範囲を指定します。
State	DDM の状態を有効または無効にします。
Shutdown	操作パラメータが Alarm または Warning しきい値を超過した際に、ポートをシャットダウンするか否か指定します。「None」を選択するとしきい値の超過に関わらずシャットダウンは実行されません。初期値になります。

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

DDM Temperature Threshold Settings（DDM 温度しきい値設定）

スイッチの特定ポートに DDM 温度しきい値設定を行います。

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

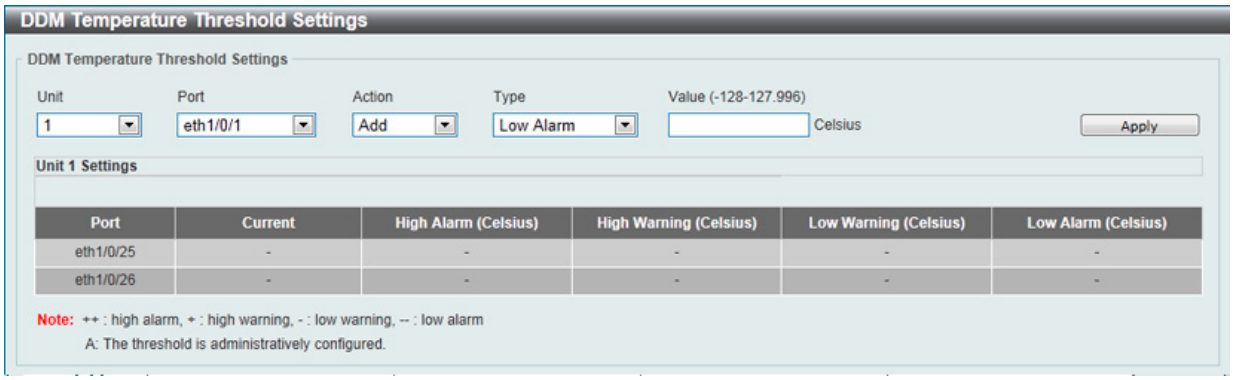


図 13-3　DDM Temperature Threshold Settings 画面

以下の項目を使用して設定します。

項目	説明
Unit	設定するユニット番号を指定します。
Port	適用するポートを指定します。

項目	説明
Action	作動する動作について指定します。「Add」「Delete」から指定できます。
Type	温度しきい値の種類について指定します。「High Alarm」「Low Alarm」「High Warning」「Low Warning」から指定できます。
Value	温度しきい値の値について指定します。「-128」から「127.996」（℃）までの間で指定可能です。

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

DDM Voltage Threshold Settings（DDM 電圧しきい値設定）

スイッチの特定ポートに電圧しきい値を設定します。

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

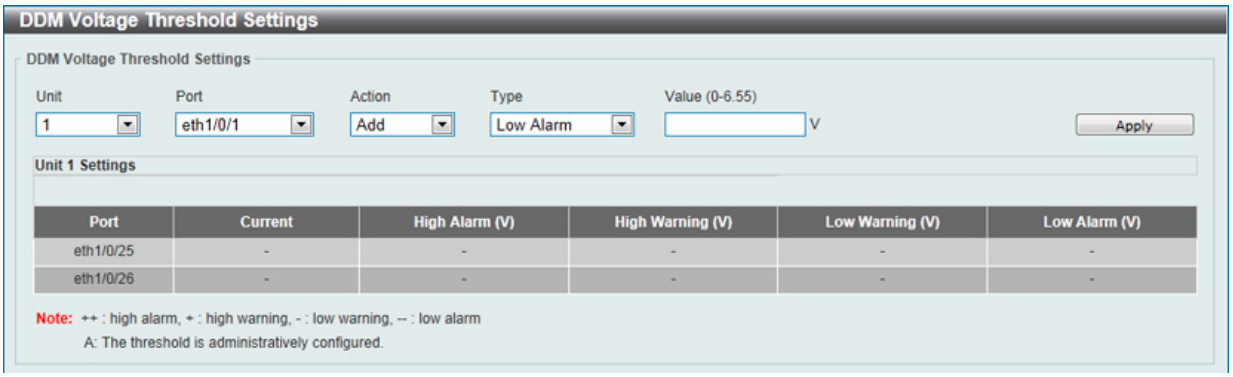


図 13-4　DDM Voltage Threshold Settings 画面

以下の項目を使用して設定します。

項目	説明
Unit	設定するユニット番号を指定します。
Port	適用するポートを指定します。
Action	作動する動作について指定します。「Add」「Delete」から指定できます。
Type	電圧しきい値の種類について指定します。「High Alarm」「Low Alarm」「High Warning」「Low Warning」から指定できます。
Value	電圧しきい値の値について指定します。「0」から「6.55」（V）までの間で指定可能です。

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

DDM Bias Current Threshold Settings（DDM バイアス電流しきい値設定）

スイッチの特定ポートにバイアス電流しきい値を設定します。

OAM > DDM > DDM Bias Current Threshold Settings の順にメニューをクリックし、以下の画面を表示します。

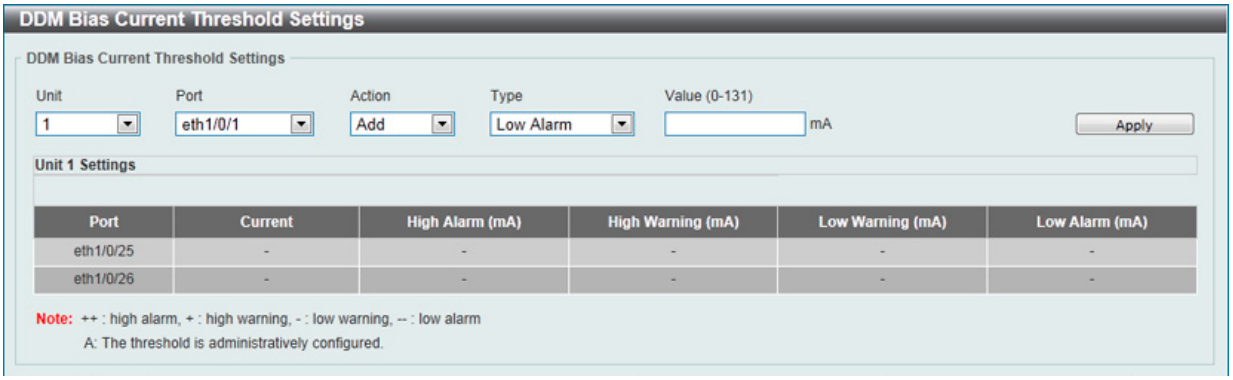


図 13-5　DDM Bias Current Threshold Settings 画面

以下の項目を使用して設定します。

項目	説明
Unit	設定するユニット番号を指定します。
Port	適用するポートを指定します。
Action	作動する動作について指定します。「Add」「Delete」から指定できます。
Type	電流しきい値の種類について指定します。「High Alarm」「Low Alarm」「High Warning」「Low Warning」から指定できます。
Value	電流しきい値の値について指定します。「0」から「131」（mA）までの間で指定可能です。

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

DDM TX Power Threshold Settings（DDM 送信電力しきい値設定）

スイッチの特定ポートに送信電力しきい値を設定します。

OAM > DDM > DDM TX Power Threshold Settings の順にメニューをクリックし、以下の画面を表示します。

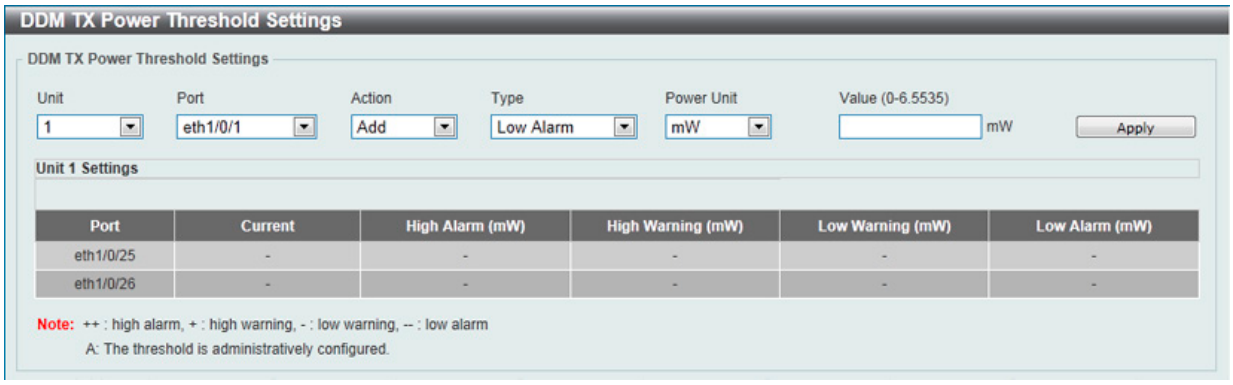


図 13-6　DDM TX Power Threshold Settings 画面

以下の項目を使用して設定します。

項目	説明
Unit	設定するユニット番号を指定します。
Port	適用するポートを指定します。
Action	作動する動作について指定します。「Add」「Delete」から指定できます。
Type	送信電力しきい値の種類について指定します。 「High Alarm」「Low Alarm」「High Warning」「Low Warning」から指定できます。
Power Unit	送信電力単位について指定します。「mW」「dBm」から指定できます。
Value	送信電力しきい値の値について指定します。 「Power Unit」で「mW」を選択した場合、「0」から「6.5535」の間で指定します。「dBm」を選択した場合、「-40」から「8.1647」までの間で指定可能です。

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

DDM RX Power Threshold Settings（DDM 受信電力しきい値設定）

スイッチの特定ポートに受信電力しきい値を設定します。

OAM > DDM > DDM RX Power Threshold Settings の順にメニューをクリックし、以下の画面を表示します。

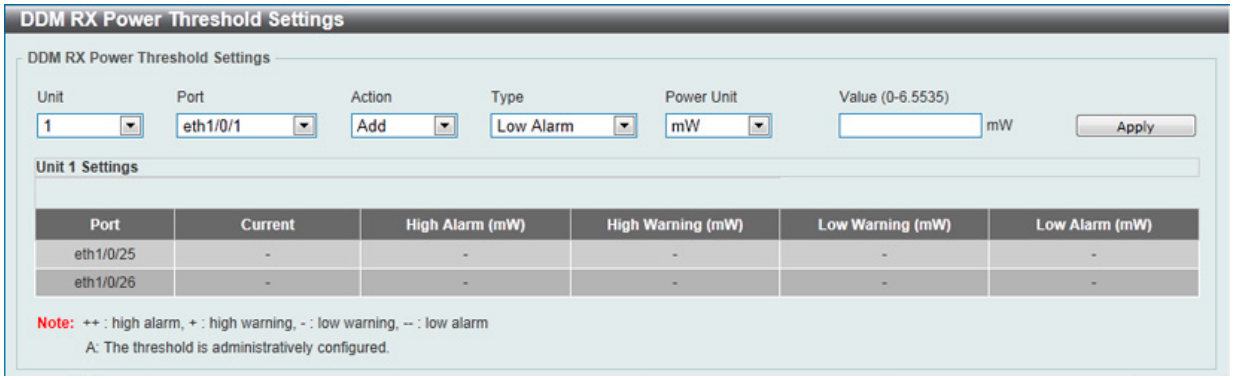


図 13-7　DDM RX Power Threshold Settings 画面

以下の項目を使用して設定します。

項目	説明
Unit	設定するユニット番号を指定します。
Port	適用するポートを指定します。
Action	作動する動作について指定します。「Add」「Delete」から指定できます。
Type	受信電力しきい値の種類について指定します。 「High Alarm」「Low Alarm」「High Warning」「Low Warning」から指定できます。
Power Unit	受信電力単位について指定します。「mW」「dBm」から指定できます。

項目	説明
Value	受信電力しきい値の値について指定します。 「Power Unit」で「mW」を選択した場合、「0」から「6.5535」の間で指定します。「dBm」を選択した場合、「-40」から「8.1647」までの間で指定可能です。

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

DDM Status Table（DDM ステータステーブル）

指定ポートで現在操作中の DDM パラメータと SFP モジュールの値を表示します。

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

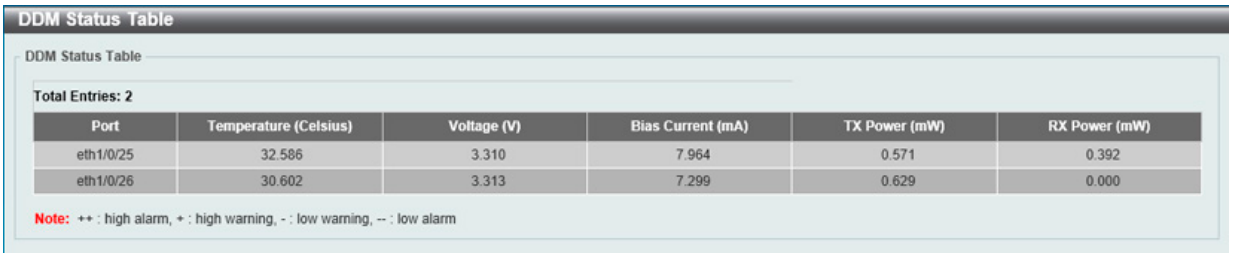


図 13-8　DDM Status Table 画面

以下の項目を表示します。

項目	説明
Port	ポート番号を表示します。
Temperature	ポートの現在の温度を表示します。
Voltage	ポートの現在の電圧を表示します。
Bias Current	ポートの現在のバイアス電流を表示します。
TX Power	ポートの現在の送信電力を表示します。
RX Power	ポートの現在の受信電力を表示します。

第 14 章　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）	CPU 使用率、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。
sFlow（sFlow 設定）	sFlow を設定し、スイッチやルータを経由するネットワークトラフィックをモニタします。
Device Environment（機器環境確認）	機器環境の設定、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。

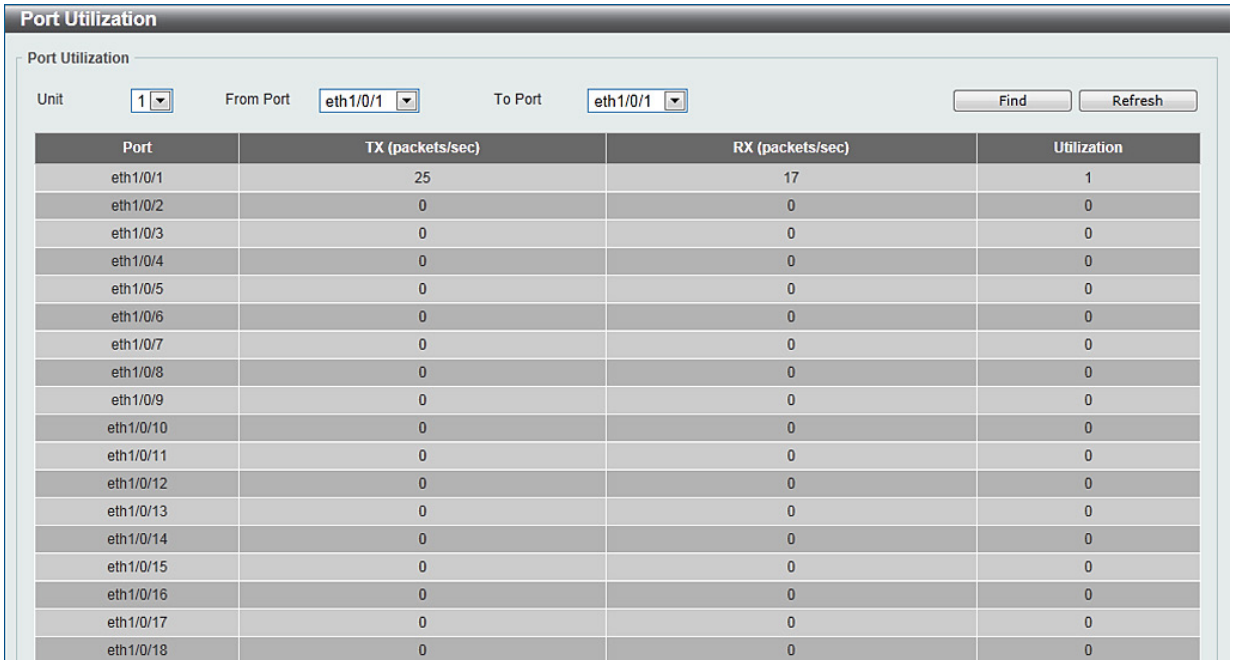


図 14-1　Port Utilization 画面

以下の設定項目が使用できます。

項目	説明
Unit	表示するユニットを指定します。
Port	プルダウンメニューで統計情報を表示するポート番号を選択します。

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

Statistics（統計情報）

Port（ポート統計情報）

ポートのパケット情報を表示します。

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

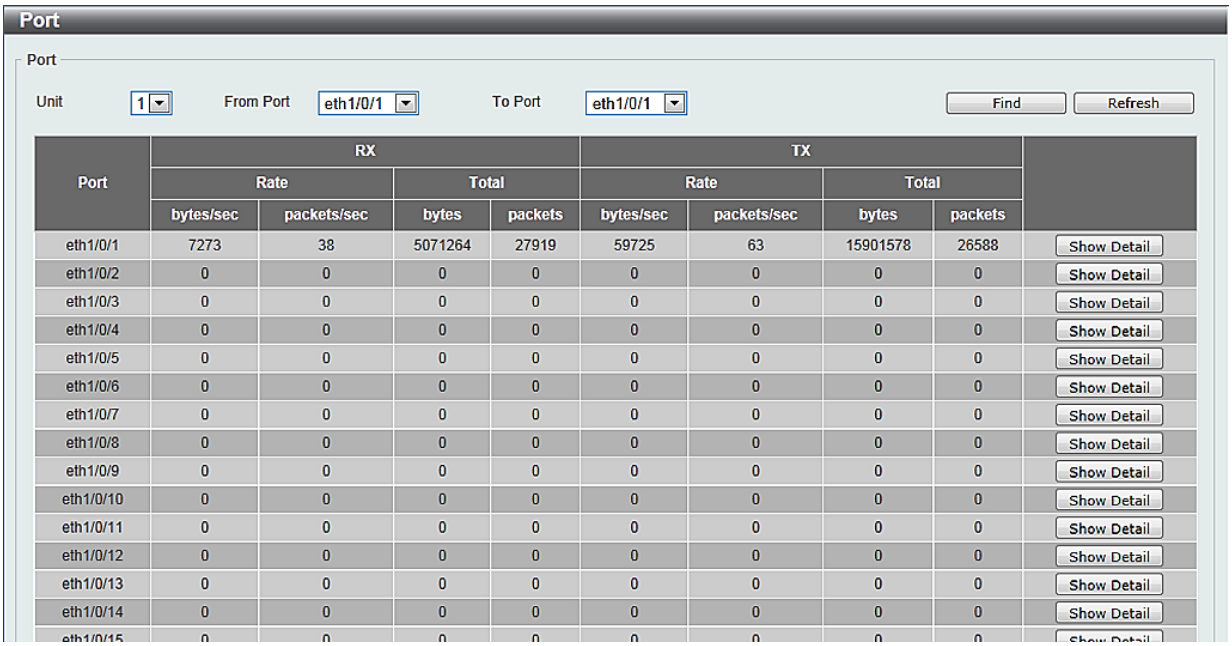


図 14-2　Port Statistics 画面

以下の設定項目を使用して、設定および表示を行います。

項目	説明
Unit	表示するユニットを選択します。
From Port / To Port	表示するポート範囲を指定します。

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

「Show Detail」ボタンをクリックすると以下の画面が表示されます。

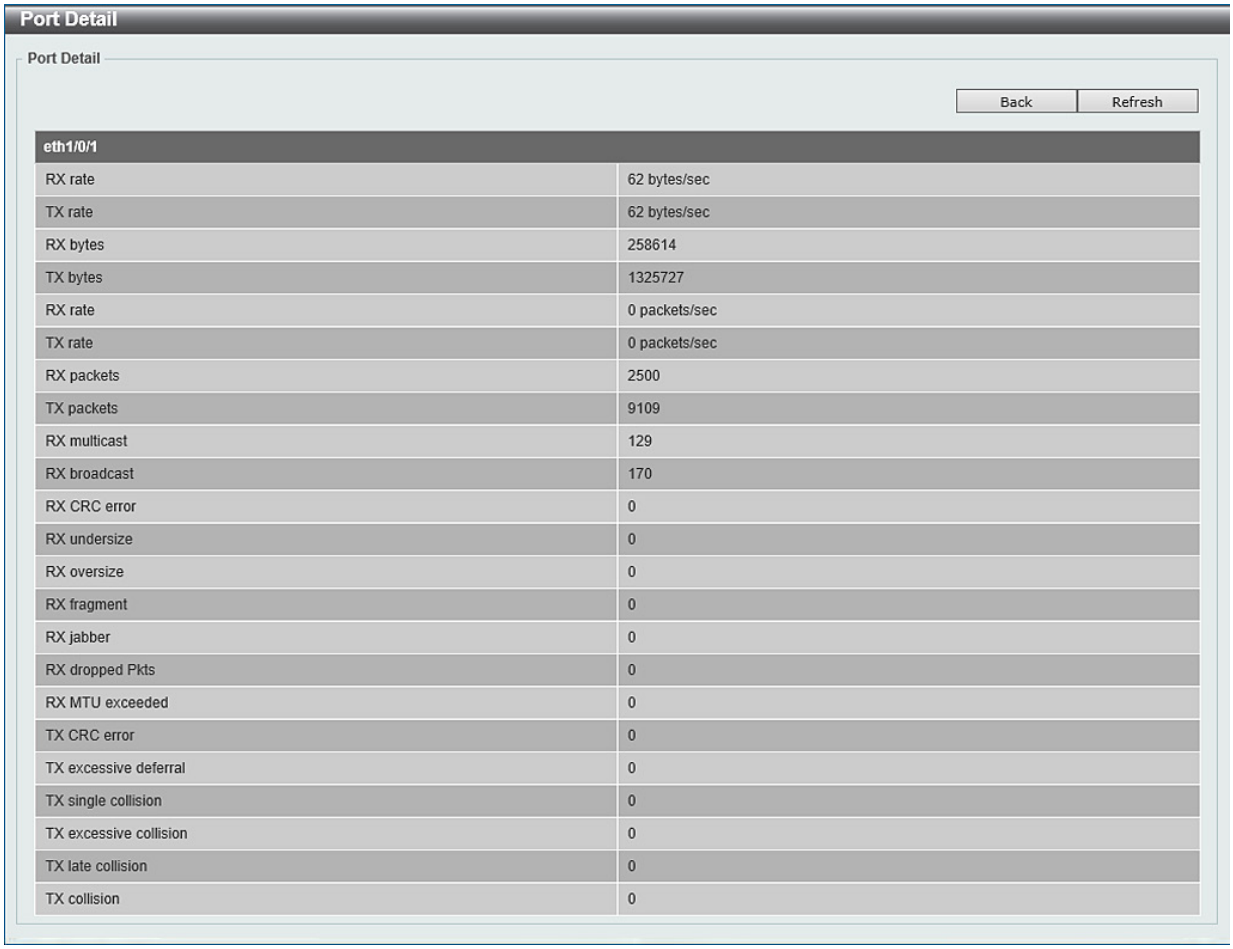


図 14-3　Port Statistics - Show Detail 画面

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

Port Counters（ポートカウンタ）

ポートのカウンタ情報を表示します。

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

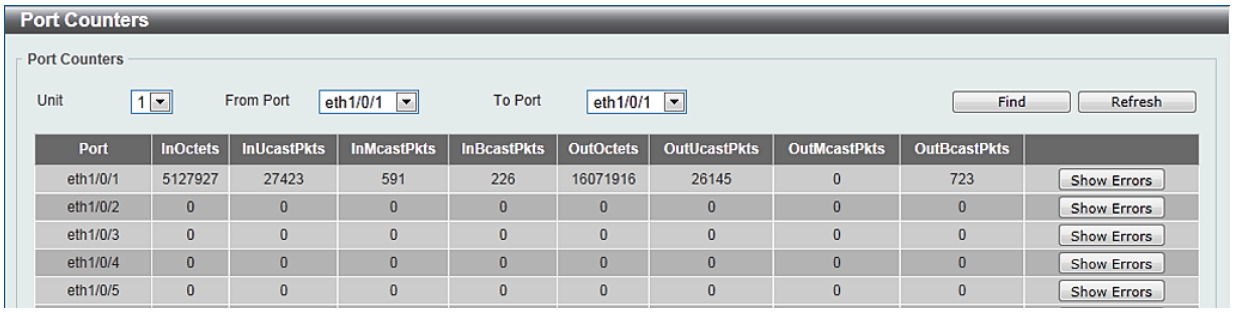


図 14-4　Port Counters 画面

以下の設定項目を使用して、設定および表示を行います。

項目	説明
Unit	表示するユニットを選択します。
From Port / To Port	表示するポート範囲を指定します。

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

「Show Errors」ボタンをクリックすると以下の画面が表示されます。

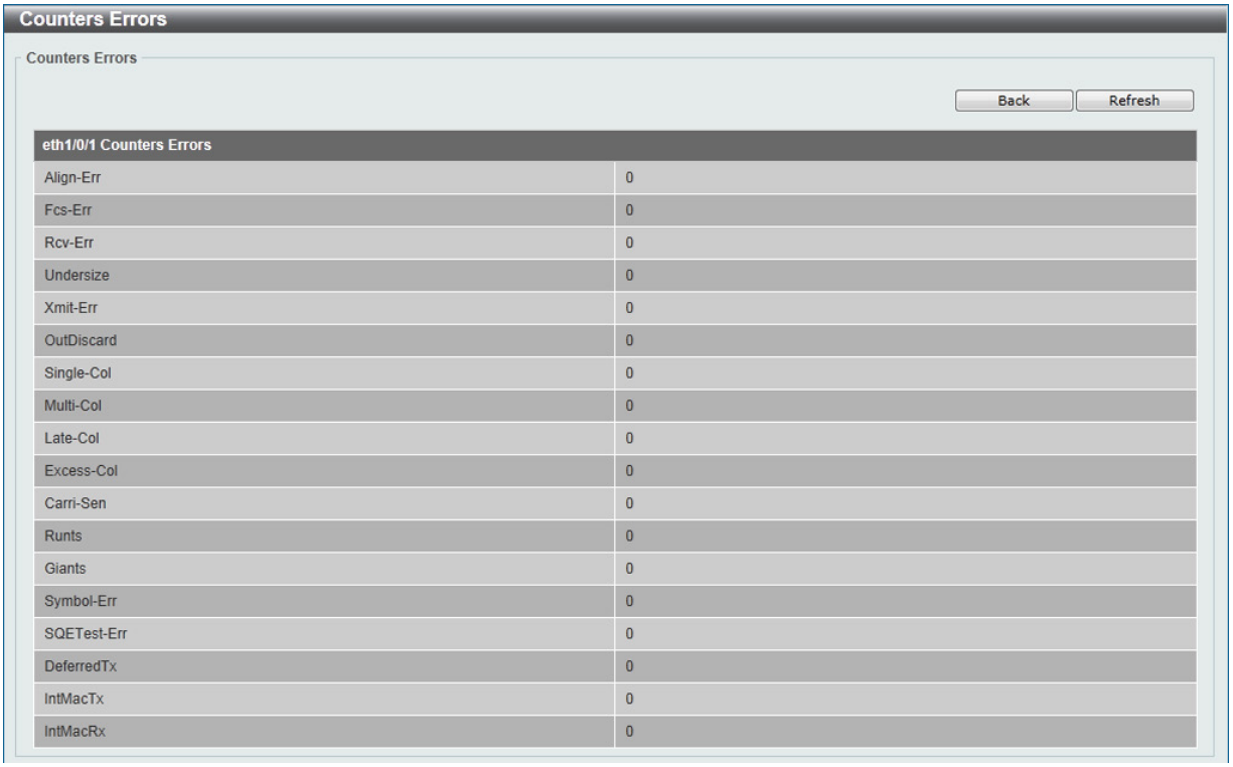


図 14-5　Port Statistics - Show Errors 画面

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

Counters（カウンタ）

すべてのポートのカウンタ情報を表示、消去します。

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

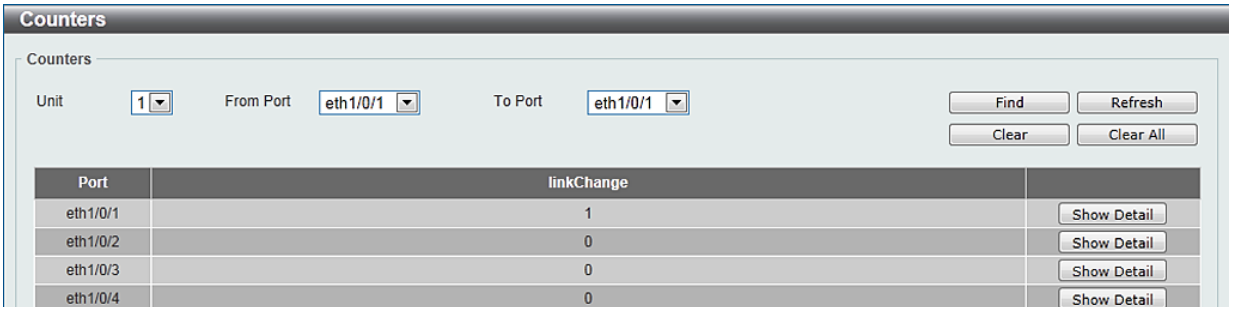


図 14-6　Counters 画面

以下の設定項目を使用して、設定および表示を行います。

項目	説明
Unit	表示するユニットを選択します。
From Port / To Port	表示するポート範囲を指定します。

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

「Show Detail」ボタンをクリックすると以下の画面が表示されます。

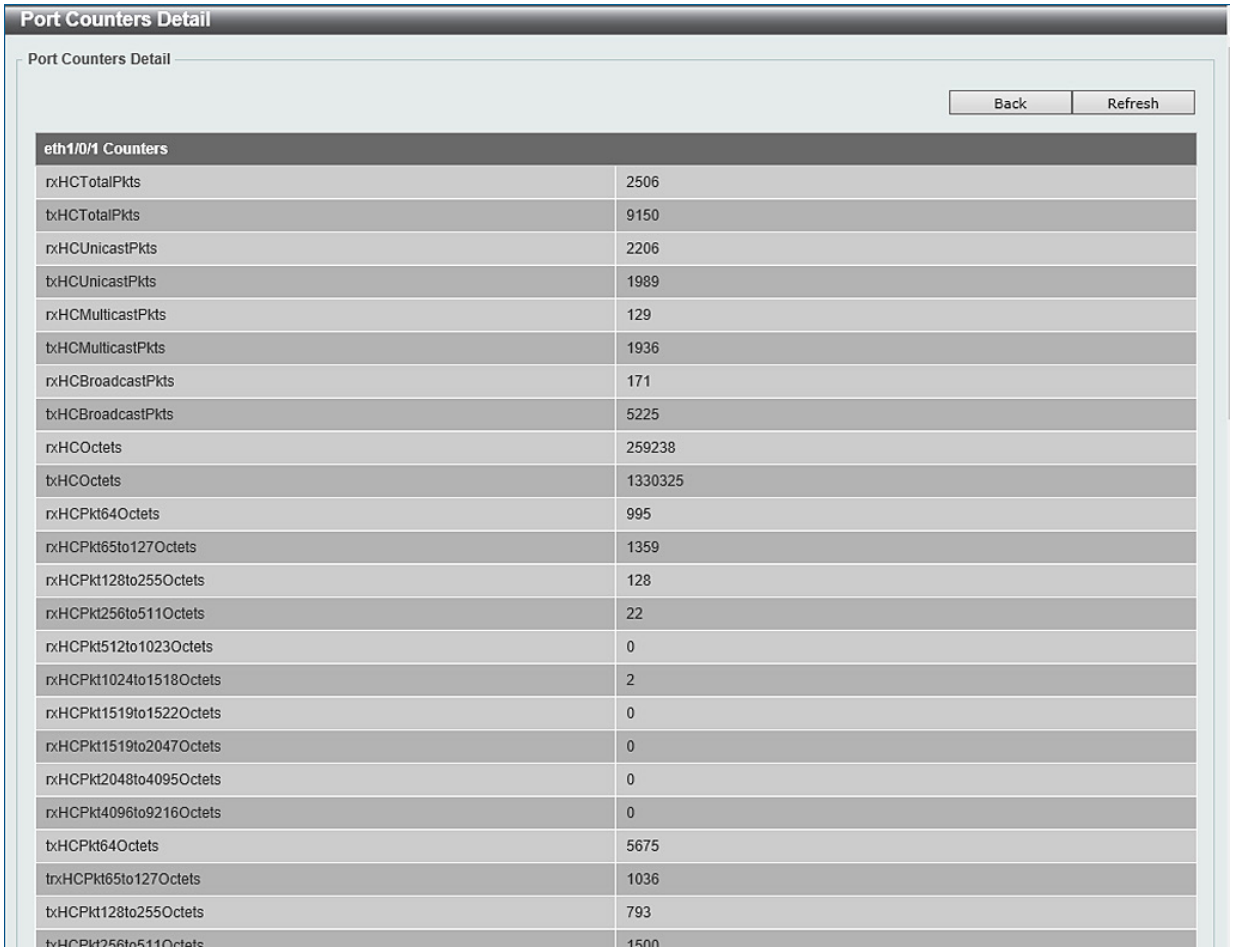


図 14-7　Port Counters Detail 画面

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

Mirror Settings（ミラー設定）

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

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

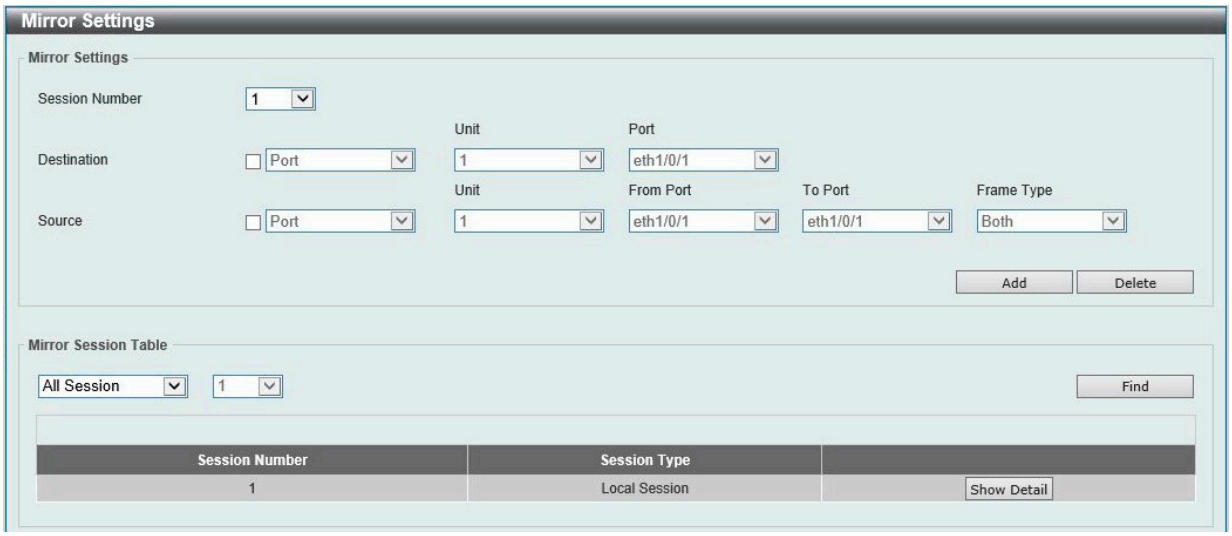


図 14-8　Mirror Settings 画面

以下の情報が表示されます。

項目	説明
Mirror Settings	
Session Number	該当エントリのセッション番号を指定します。1 から 4 までで指定可能です。
Destination	チェックボックスにチェックを入れポートミラーエントリの宛先について設定します。 宛先タイプオプションとして「Port」を選択します。「Port」を選択した後に、宛先ユニットやポート番号を指定します。
Source	チェックボックスにチェックを入れポートミラーエントリの送信元について設定します。 送信元タイプオプションとして「Port」または「ACL」を選択します。「Port」を選択した後に、「From Port」と「To Port」の番号を指定します。最後に「Frame Type」オプションを指定します。「Frame Type」で指定可能なオプションは「Both」「RX」「TX」「TX Forwarding」です。「Both」を選択すると送受信どちらのトラフィックもミラーされます。「RX」の場合、受信トラフィックのみミラーされ、「TX」は送信トラフィックのみミラーされます。「TX Forwarding」はポートが「STG Forwarding」状態の場合、送信トラフィックのみミラーされます。「ACL」オプションを選択した場合は ACL プロファイル名を表示される項目欄に入力します。

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

項目	説明
Mirror Session Table	
Mirror Session Type	表示する情報のミラーセッションを選択します。「All Session」「Session Number」から選択します。 「Session Number」を選択すると表示されるドロップダウンメニューからセッション番号を選択します。1 から 4 の間で選択可能です。

「Find」ボタンをクリックして、入力した情報に基づいたエントリを検出します。

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

注意　各セッションの Destination のポートは別々のポートに設定することはできません。（Destination のポートは 1 ポートのみ対応）

「Show Detail」リンクをクリックし、以下の画面を表示します。



図 14-9　Mirror Settings - Show Detail 画面

sFlow（sFlow 設定）

sFlow は（RFC3176）、スイッチやルータを経由するネットワークトラフィックをモニタする機能です。sFlow によるモニタリングは「sFlow エージェント」（スイッチやルータ内に内蔵）と「セントラル sFlow コレクタ」によって構成されています。sFlow モニタリングシステムのアーキテクチャとサンプル技術は、サイトレベル、または企業レベルでの高速スイッチ / ルータネットワークにおける継続的なトラフィックモニタリングを提供します。

注意　sFlow の機能において、「Agent Address」は「Vlan 1」に設定された IP アドレスを使用し、これを変更する事はできません。「Vlan 1」の IP アドレスが設定されていない場合、または「Interface vlan 1」が存在しない場合は「Agent Address」は「0.0.0.0」となります。

sFlow Agent Information（sFlow エージェント情報）

sFlow エージェント情報を表示します。

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

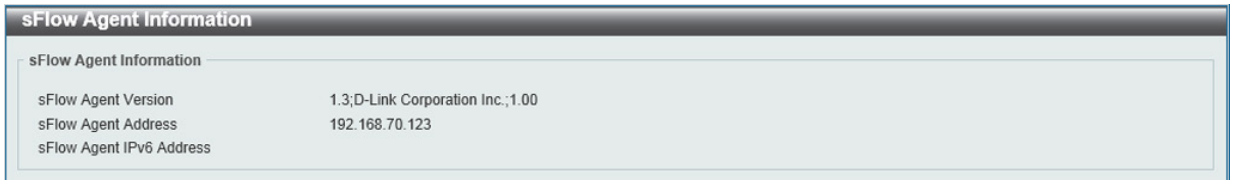


図 14-10　sFlow Agent Information 画面

以下の項目が表示されます。

項目	説明
sFlow Agent Version	現在の sFlow エージェントバージョンを表示します。
sFlow Agent Address	sFlow エージェント IP アドレスを表示します。
sFlow Agent IPv6 Address	sFlow エージェント IPv6 アドレスを表示します。

「Apply」ボタンをクリックして、設定を有効にします。

sFlow Receiver Settings（sFlow レシーバ設定）

sFlow エージェントのレシーバ設定と設定表示を行います。レシーバは sFlow エージェントから消去や追加することはできません。

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

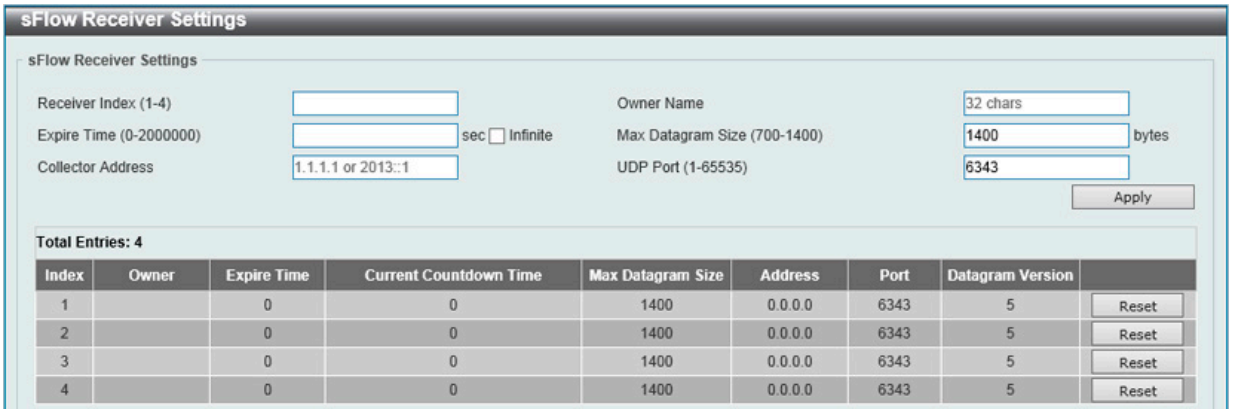


図 14-11　sFlow Receiver Settings 画面

以下の項目が表示されます。

項目	説明
Receiver Index	追加する sFlow レシーバの識別子（1-4）を指定します。最大 4 個のエントリを追加できます。
Owner Name	sFlow レシーバオーナ名を指定します。32 文字まで指定できます。
Expire Time	タイムアウト時間を指定します。期限になるとエントリはリセットされます。0-2000000（秒）の範囲から指定します。「Infinite」を設定するとサーバはタイムアウトしません。
Max Datagram Size (700-1400)	1 つの sFlow データにパッケージ化する最大データバイト数を指定します。 700 から 1400 で設定でき、初期値は 1400（バイト）です。
Collector Address	リモート sFlow コレクタの IP（v4/v6）アドレスを指定します。
UDP Port (1-65535)	リモート sFlow コレクタの UDP ポートを指定します。初期値は 6343 です。

「Apply」ボタンをクリックして、設定を有効にします。「Reset」ボタンをクリックして、指定エントリの設定を初期値に戻します。

sFlow Sampler Settings（sFlow サンプラ設定）

ネットワークからサンプルパケットを取得するための設定をします。これには、サンプリングのレートや抽出されるパケットヘッダの量も含まれます。

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

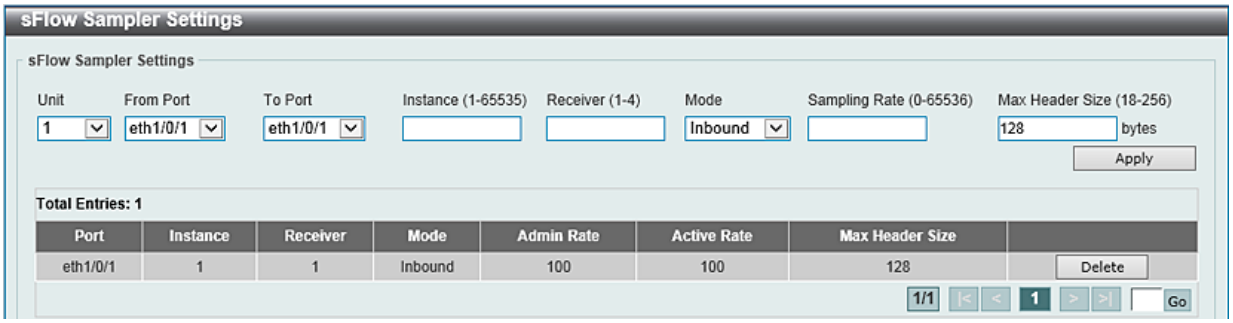


図 14-12　sFlow Sampler Settings 画面

以下の項目が表示されます。

項目	説明
Unit	設定するユニットを指定します。
From Port / To Port	パケットサンプリングの設定を行うポートおよびポート範囲を指定します。
Instance	複数のサンプラを一つのインスタンスで使用する場合、インスタンスの識別番号を指定します。
Receiver (1-4)	レシーバの識別番号を指定します。何も指定しない場合、値は「0」になります。1 から 4 までの間で指定可能です。
Mode	モードを指定します。「Inbound」または「Outbound」から指定します。「Inbound」を選択するとサンプルのイングレスパケットを指定します（初期値）。「Outbound」を選択するとサンプルのイーグレスパケットを指定します。
Sampling Rate	パケットサンプリングのレートを設定します。0-65535 の値を指定します。エントリ「0」は、パケットのサンプリングを無効にします。0 が初期値であるため、指定しないと本機能は動作しません。
MAX Header Size (18-256)	本項目はサンプリングされるパケットヘッダのバイト数を設定します。このサンプルサンプリングされるヘッダは、アナライザサーバに送信されるデータと共にカプセル化されます。18-256 バイトの値を設定します。初期値は 128 バイトです。

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

sFlow Poller Settings（sFlow ポーラ設定）

スイッチのポーラの設定を行います。

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

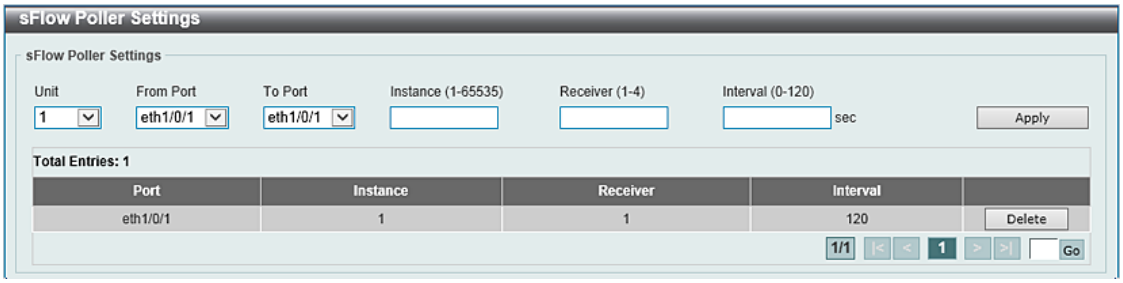


図 14-13　sFlow Poller Settings 画面

以下の項目が表示されます。

項目	説明
Unit	設定するユニットを選択します。
From Port / To Port	ポーリングの設定を行うポートおよびポート範囲を指定します。
Instance	複数のサンプラを一つのインスタンスで使用する場合、インスタンスの識別番号を指定します。
Receiver (1-4)	レシーバの識別番号を指定します。何も指定しない場合、値は「0」になります。1 から 4 までの間で指定可能です。
Interval (0-120)	ポーリングサンプリングの間隔を設定します。0 から 120（秒）で指定可能です。「0」を入力すると機能は無効になります。初期値は「0」です。

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

Device Environment（機器環境確認）

本画面ではスイッチの内部温度状態を表示します。

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

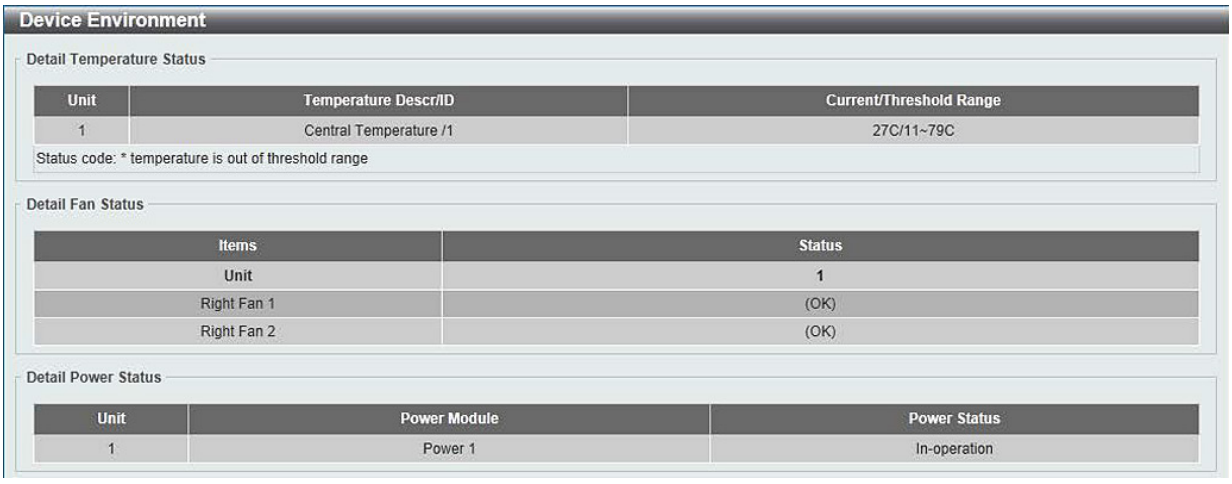


図 14-14　Device Environment 画面

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）	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）	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

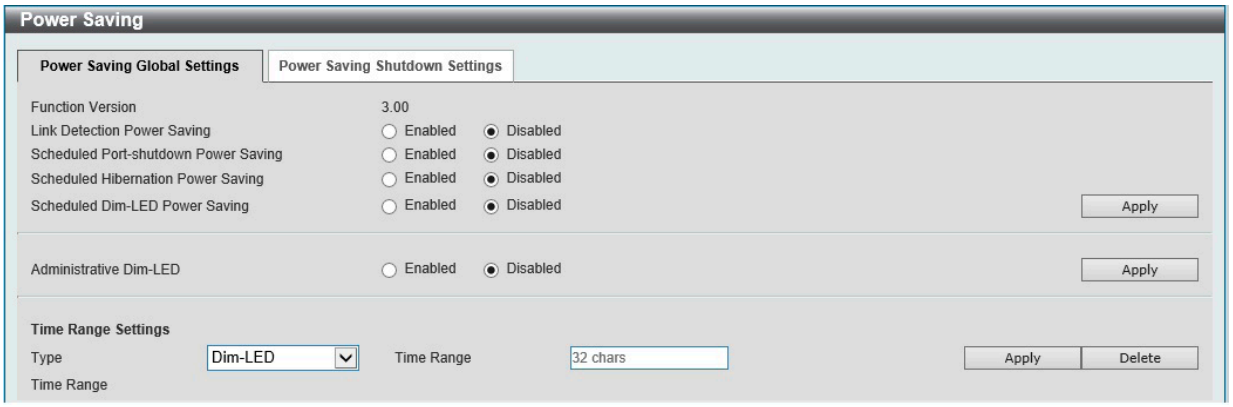


図 15-1　Power Saving - Power Saving Global Settings タブ画面

以下の設定項目を使用して表示を変更します。

項目	説明
Power Saving Global Settings タブ	
Link Detection Power Saving	「リンク検出」を有効 / 無効に指定します。有効にするとリンクダウンしているポートへの電力供給は止められ、スイッチの消費電力を抑えます。これによりリンクアップしているポートへの影響はありません。
Scheduled Port-shutdown Power Saving	スケジュールによるポートシャットダウン機能の有効 / 無効を指定します。
Scheduled Hibernation Power Saving	スケジュールによるシステムスリープ機能の有効 / 無効を指定します。
Scheduled Dim-LED Power Saving	スケジュールによりスイッチの LED 照明を消すことで、消費電力を抑えます。
Administrative Dim-LED	ポート LED 機能の有効 / 無効を指定します。
Type	省電力モードの種類を指定します。「Dim-LED」「Hibernation」から指定できます。
Time Range	上記省電力機能に対応するスケジュールを指定します。

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

注意　「Hibernation」（休止）機能を有効にする場合、物理スタック機能は無効である必要があります。

Power Saving Shutdown Settings タブ

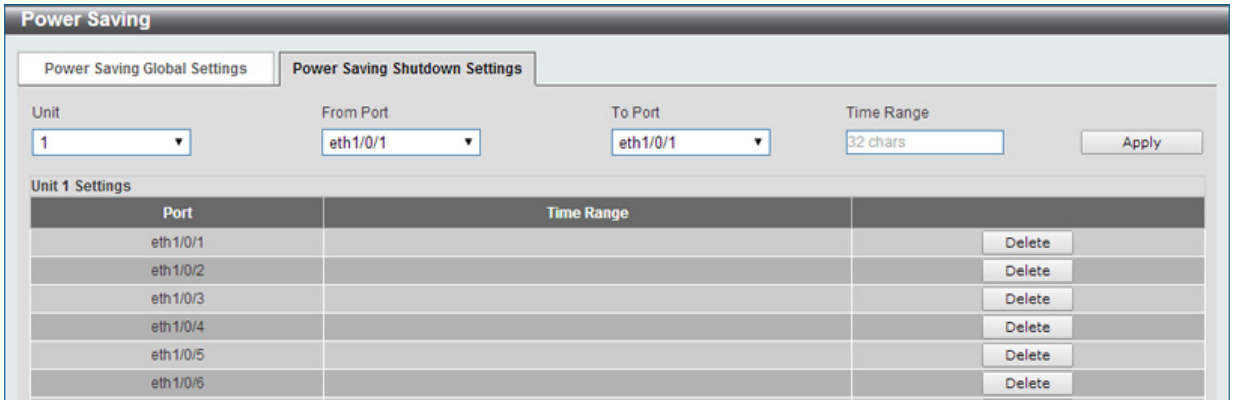


図 15-2　Power Saving - Power Saving Shutdown Settings タブ画面

以下の設定項目を使用して表示を変更します。

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

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

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

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

Green > EEE メニューをクリックし、以下の画面を表示します。

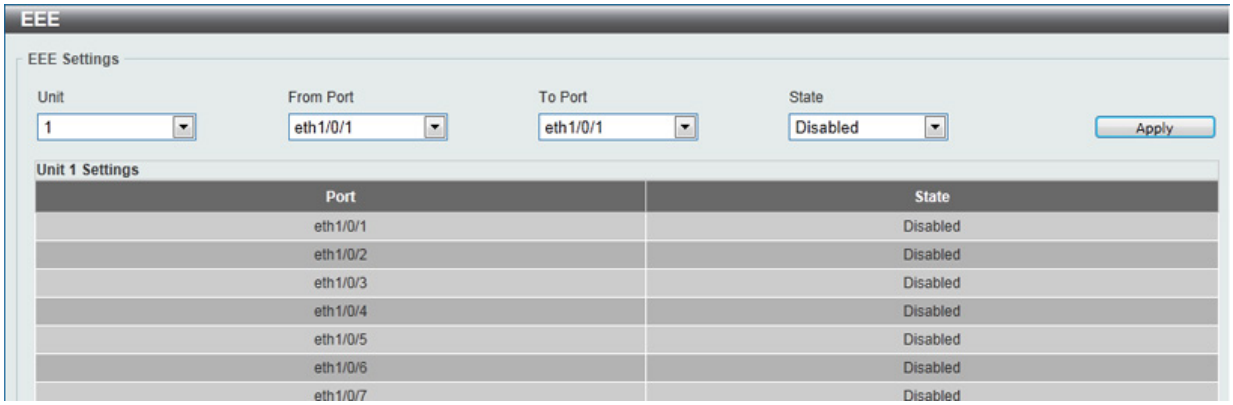


図 15-3　EEE 画面

以下の設定項目を使用して表示を変更します。

項目	説明
Power Saving Shutdown Settings タブ	
Unit	設定するユニットを選択します。
From Port / To Port	設定するポート範囲を指定します。
State	本機能を有効 / 無効に指定します。

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

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

第 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」「Surveillance 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。

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）	Save Configuration（コンフィグレーションの保存）	コンフィグレーションをスイッチに保存します。
Tools（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）	ファームウエアのアップグレードとバックアップをします。
	Configuration Restore & Backup（コンフィグレーションリストア＆バックアップ）	コンフィグレーションのリストアとバックアップをします。
	Log Backup（ログファイルのバックアップ）	ログファイルのバックアップをします。
	Ping	Ping を実行します。
	Trace Route（トレースルート）	トレースルートの設定を行います。
	Language Management（言語管理）	使用する言語を設定します。
	Reset（リセット）	機器をリセットします。
	Reboot System（システム再起動）	システムの再起動を行います。
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（サポートサイト / 英語版）	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）	—	Web モードを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）

Save Configuration（コンフィグレーションの保存）

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

コンフィグレーションの保存

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

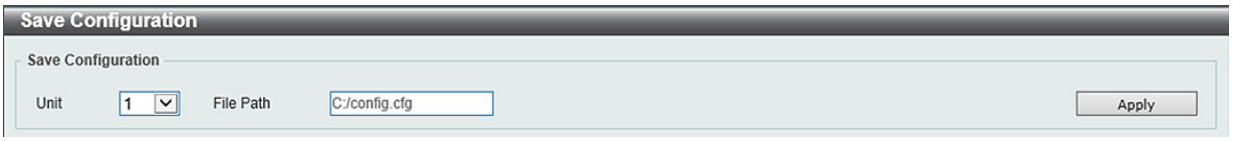


図 16-2　Save Configuration 画面

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）

注意　DGS-1510-52X/A3 では、1.60.B031 より古いファームウェアは使用できません。

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。

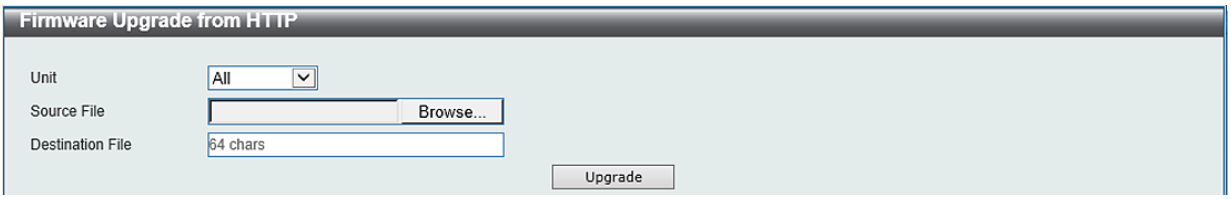


図 16-3　Firmware Upgrade from HTTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Unit	設定するユニットを選択します。
Source File	「Browse/ 参照」ボタンをクリックしてローカル PC 上のファームウェアファイルの場所を指定できます。
Destination File	ファームウェアがストアされるスイッチの場所 / ファイル名を指定します。64 文字までで指定できます。 （例：C:/DGS-1510_Run_0_00_B000.had）

「Upgrade」ボタンをクリックしてアップグレードを開始します。

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

TFTP を使用してファームウェアアップグレードを実行します。

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

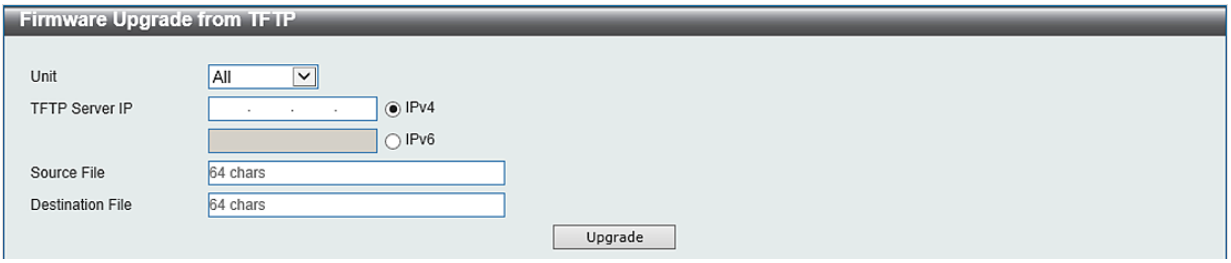


図 16-4　Firmware Upgrade from TFTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Unit	設定するユニットを選択します。
TFTP Server IP	TFTP サーバの IP アドレスを入力します。「IPv4」オプションを選択した場合、TFTP サーバの IPv4 アドレスを入力します。「IPv6」オプションを選択した場合、TFTP サーバの IPv6 アドレスを入力します。
Source File	ローカル PC にあるファームウェアファイル名を入力します。64 文字まで指定します。（例：DGS-1510_Run_0_00_B000.had）
Destination File	ファームウェア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。64 文字までで指定できます。 （例：C:/DGS-1510_Run_0_00_B000.had）

「Upgrade」ボタンをクリックしてアップグレードを開始します。

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

HTTP プロトコルを使用して、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。

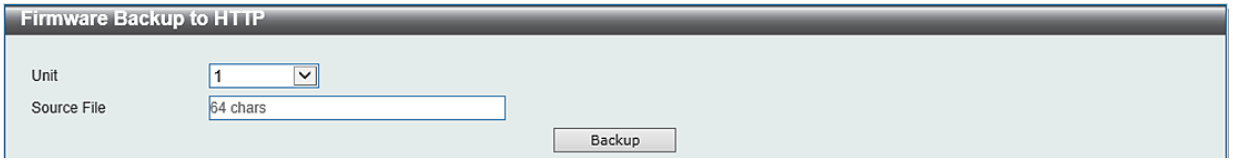


図 16-5　Firmware Backup to HTTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Unit	設定するユニットを選択します。
Source File	スイッチにあるパスとファイル名を入力します。64 文字まで指定します。（例：C:/DGS-1510_Run_0_00_B000.had） Source File（送信元ファイル名 / パス）は「File System（ファイルシステム）」にて確認できます。

「Backup」ボタンをクリックしてバックアップを開始します。

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

TFTP サーバへの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。

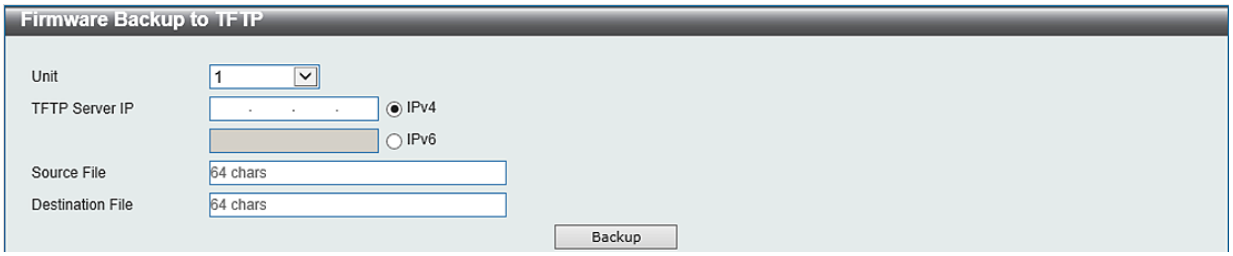


図 16-6　Firmware Backup to TFTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Unit	設定するユニットを選択します。
TFTP Server IP	ファームウェアファイルがバックアップされる TFTP サーバの IP アドレスを入力します。「IPv4」オプションを選択した場合、TFTP サーバの IPv4 アドレスを入力します。「IPv6」オプションを選択した場合、TFTP サーバの IPv6 アドレスを入力します。
Source File	スイッチにあるパスとファイル名を入力します。64 文字まで指定します。（例：C:/DGS-1510_Run_0_00_B000.had）
Destination File	TFTP サーバにバックアップされるファイル名を指定します。64 文字までで指定できます。 （例：DGS-1510_Run_0_00_B000.had）

「Backup」ボタンをクリックしてバックアップを開始します。

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

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

HTTP サーバを使用してローカル PC からスイッチへ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

以下の項目を使用して、設定および表示を行います。

項目	説明
Unit	設定するユニットを選択します。
Source File	「Browse/ 参照」ボタンをクリックしてローカル PC 上のコンフィグレーションファイルの場所を指定できます。
Destination File	コンフィグレーションファイルがストアされるスイッチの場所 / ファイル名を指定します。64 文字までで指定できます。 （例：C:/config_xxx.cfg） 「running-config」オプションを選択するとリストアと同時に実行中のコンフィグレーションファイルは上書きされます。 「startup-config」オプションを選択するとスタートアップコンフィグレーションファイルがリストア＆上書きされます。
Replace	現在実行中のコンフィグレーションを置き換えます。

「Restore」ボタンをクリックしてコンフィグレーションのリストアを開始します。

Configuration Restore from TFTP（TFTP サーバからコンフィグレーションのリストア）

TFTP サーバを使用してローカル PC からスイッチへ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

以下の項目を使用して、設定および表示を行います。

項目	説明
Unit	設定するユニットを選択します。
TFTP Server IP	TFTP サーバの IP アドレスを入力します。「IPv4」オプションを選択した場合、TFTP サーバの IPv4 アドレスを入力します。「IPv6」オプションを選択した場合、TFTP サーバの IPv6 アドレスを入力します。
Source File	TFTP サーバにあるコンフィグレーションファイル名を入力します。64 文字まで指定します。（例：config_xxx.cfg）
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。64 文字までで指定できます。 （例：C:/config_xxx.cfg） 「running-config」オプションを選択するとリストアと同時に実行中のコンフィグレーションファイルは上書きされます。 「startup-config」オプションを選択するとスタートアップコンフィグレーションファイルがリストア＆上書きされます。
Replace	現在実行中のコンフィグレーションを置き換えます。

「Restore」ボタンをクリックしてコンフィグレーションのリストアを開始します。

Configuration Backup to HTTP（HTTP を使用したコンフィグレーションバックアップ）

HTTP プロトコルを使用して、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。

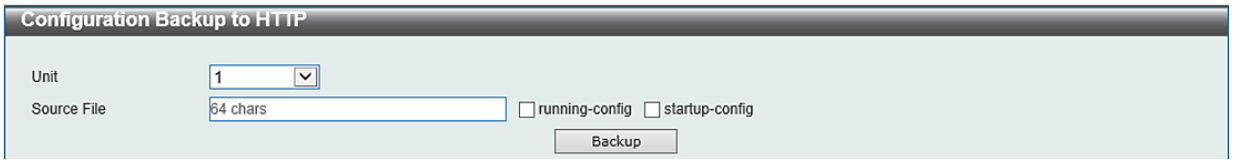


図 16-9　Configuration Backup to HTTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Unit	設定するユニットを選択します。
Source File	スイッチにあるパスとファイル名を入力します。64 文字まで指定します。（例：C:/config_xxx.cfg） 「running-config」オプションを選択すると実行中のコンフィグレーションファイルがバックアップされます。「startup-config」オプションを選択するとスタートアップコンフィグレーションファイルがバックアップされます。 Source File（送信元ファイル名 / パス）は「File System（ファイルシステム）」にて確認できます。

「Backup」ボタンをクリックしてバックアップを開始します。

Configuration Backup to 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。

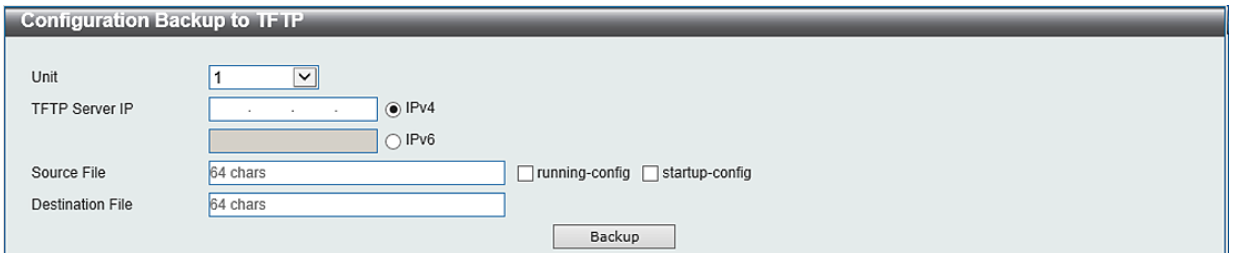


図 16-10　Configuration Backup to TFTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Unit	設定するユニットを選択します。
TFTP Server IP	TFTP サーバの IP アドレスを入力します。「IPv4」オプションを選択した場合、TFTP サーバの IPv4 アドレスを入力します。「IPv6」オプションを選択した場合、TFTP サーバの IPv6 アドレスを入力します。
Source File	スイッチにあるパスとファイル名を入力します。64 文字まで指定します。（例：C:/config_xxx.cfg） 「running-config」オプションを選択すると実行中のコンフィグレーションファイルがバックアップされます。「startup-config」オプションを選択するとスタートアップコンフィグレーションファイルがバックアップされます。
Destination File	TFTP サーバにストアされるコンフィグレーションファイル名を指定します。64 文字までで指定できます。 （例：config_xxx.cfg）

「Backup」ボタンをクリックしてバックアップを開始します。

Log Backup（ログファイルのバックアップ）

Log Backup to HTTP（HTTP サーバを使用したログファイルのバックアップ）

HTTP プロトコルを使用して、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 16-11　Log Backup to HTTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Log Type	HTTP を使用してローカル PC にバックアップするログの種類を選択します。「System Log」オプションを選択するとシステムログエントリをバックアップします。「Attack Log」オプションを選択すると攻撃関連のログをバックアップします。

「Backup」ボタンをクリックしてバックアップを開始します。

Log Backup to TFTP（TFTP サーバを使用したログファイルのバックアップ）

TFTP サーバへのシステムログのバックアップを行います。

Tools > Log Backup > Log Backup to TFTP をクリックし、設定画面を表示します。

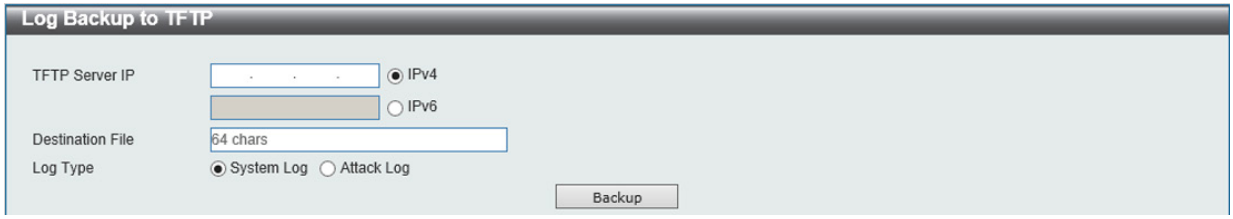


図 16-12　Log Backup to TFTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
TFTP Server IP	TFTP サーバの IP アドレスを入力します。「IPv4」オプションを選択した場合、TFTP サーバの IPv4 アドレスを入力します。「IPv6」オプションを選択した場合、TFTP サーバの IPv6 アドレスを入力します。
Destination File	TFTP サーバにストアされるログファイル名を指定します。64 文字までで指定できます。（例：log.txt）
Log Type	バックアップするログの種類を選択します。「System Log」オプションを選択するとシステムログエントリをバックアップします。「Attack Log」オプションを選択すると攻撃関連のログをバックアップします。

「Backup」ボタンをクリックしてバックアップを開始します。

Ping

「Ping」は指定した IP アドレスに ICMP Echo パケットを送信するプログラムです。宛先の機器はスイッチから送信された "echoes" に応答します。これはネットワーク上のスイッチと機器の接続状況を確認するうえで非常に有効です。

Tools > Ping をクリックし、設定画面を表示します。

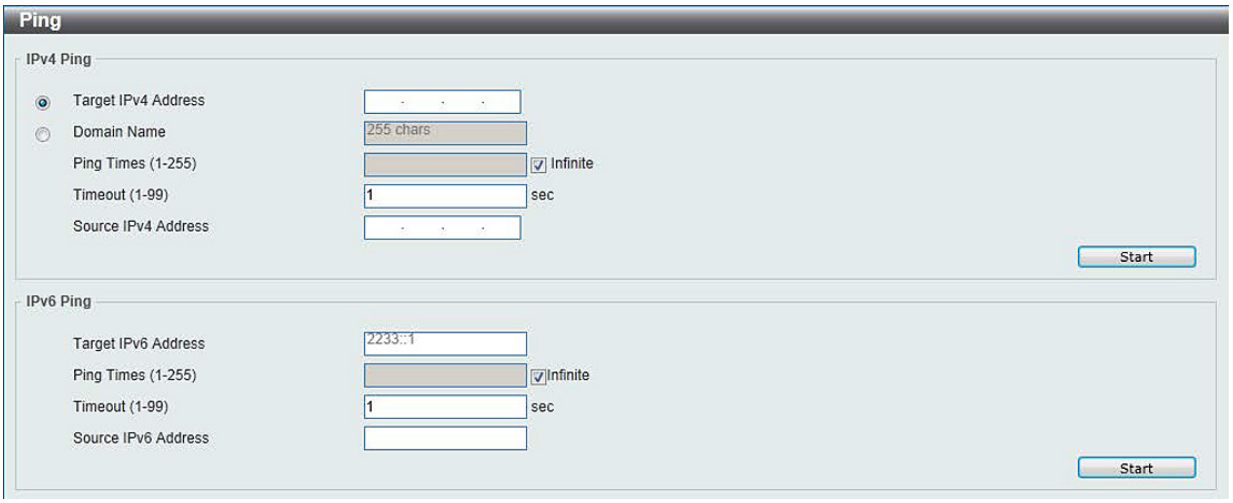


図 16-13　Ping 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
IPv4 Ping	
Target IPv4 Address	Ping する IPv4 アドレスを入力します。
Domain Name	検出するシステムのドメイン名を入力します。
Ping Times	繰り返し行う Ping の回数を入力します。1 から 255 の間で指定できます。「Infinite」にチェックを入れるとプログラムが停止されるまで「ICMP Echo」パケットを送信します。
Timeout	Ping メッセージが到達するまでのタイムアウトの時間を指定します。1 から 99（秒）までの間で指定できます。指定時間内にパケットが IP アドレスを検出できない場合、Ping パケットは破棄されます。
Source IPv4 Address	送信元 IPv4 アドレスを入力します。もし現在のスイッチが一つ以上の IP アドレスを保持している場合、そのうちのどれかを入力することが可能です。入力した IPv4 アドレスはリモートホストに送信されるパケットの送信元 IP アドレスやプライマリ IP アドレスになります。
IPv6 Ping	
Target IPv6 Address	Ping する IPv6 アドレスを入力します。
Ping Times	繰り返し行う Ping の回数を入力します。1 から 255 の間で指定できます。 「Infinite」にチェックを入れるとプログラムが停止するまで「ICMP Echo」パケットを送信します。
Timeout	Ping メッセージが到達するまでのタイムアウトの時間を指定します。1 から 99（秒）までの間で指定できます。指定時間内にパケットが IP アドレスを検出できない場合、Ping パケットは破棄されます。
Source IPv6 Address	送信元 IPv6 アドレスを入力します。もし現在のスイッチが一つ以上の IP アドレスを保持している場合、そのうちのどれかを入力することが可能です。入力した IPv6 アドレスはリモートホストに送信されるパケットの送信元 IP アドレスやプライマリ IP アドレスになります。

「Start」ボタンをクリックして、各個別セクションでの Ping テストを実行します。

「IPv4 Ping」セクションで「Start」をクリックすると以下の「IPv4 Ping Result」画面が表示されます。

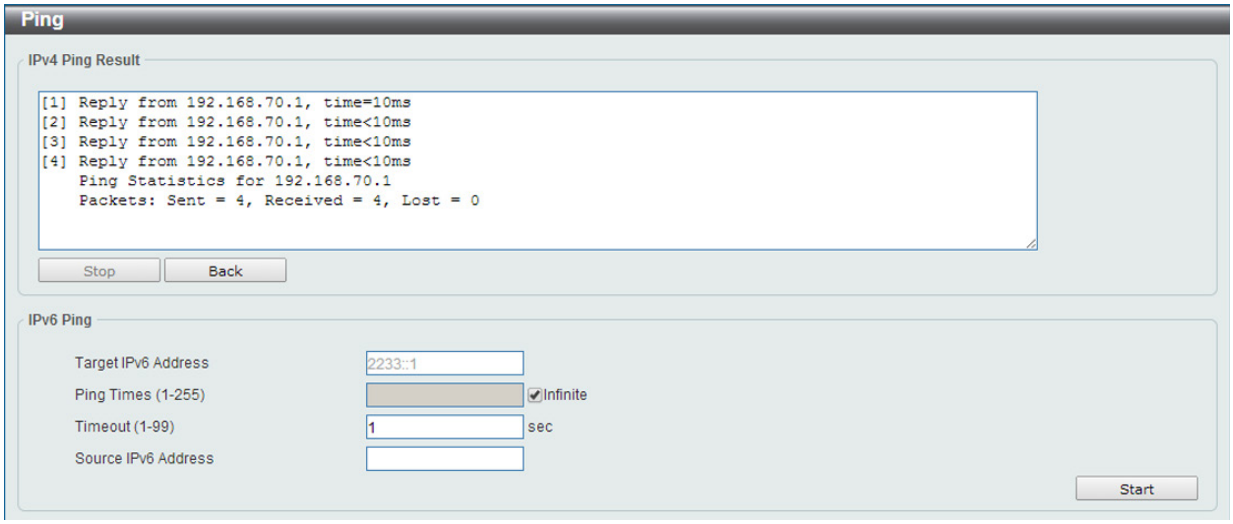


図 16-14　IPv4 Ping Result 画面

「Stop」ボタンをクリックして、Ping テストを停止します。
「Back」ボタンをクリックして、前の画面に戻ります。

「IPv6 Ping」セクションで「Start」をクリックすると以下の「IPv6 Ping Result」画面が表示されます。

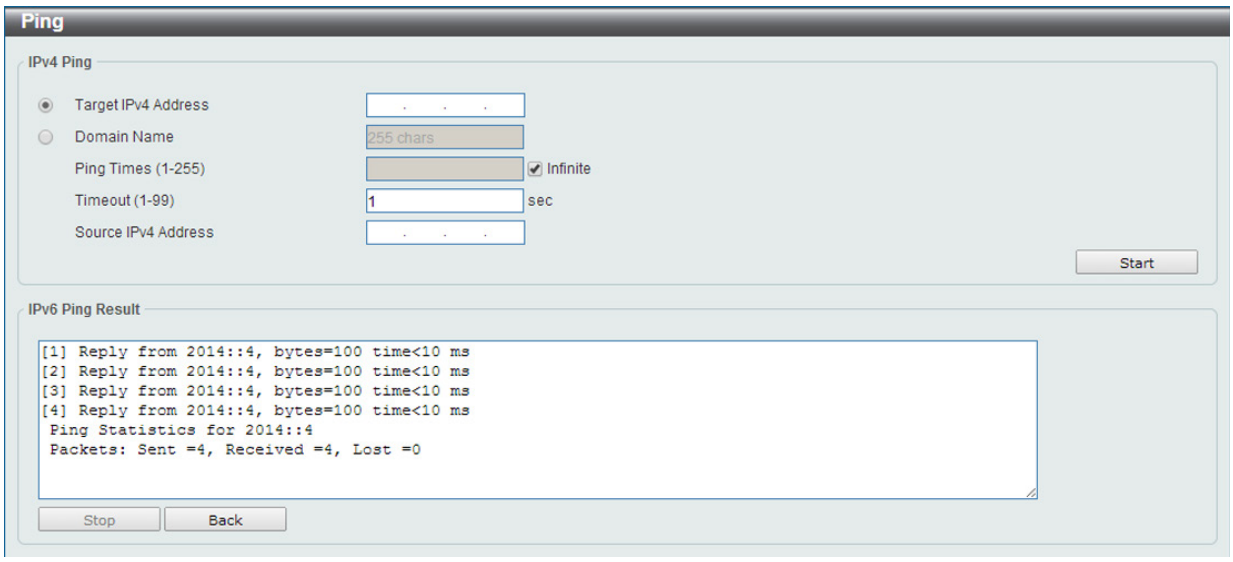


図 16-15　IPv6 Ping Result 画面

「Stop」ボタンをクリックして、Ping テストを停止します。
「Back」ボタンをクリックして、前の画面に戻ります。

Trace Route（トレースルート）

パケットの経路をスイッチに到着する前に遡ってトレースすることができます。

Tools > Trace Route の順にメニューをクリックし、以下の画面を表示します。

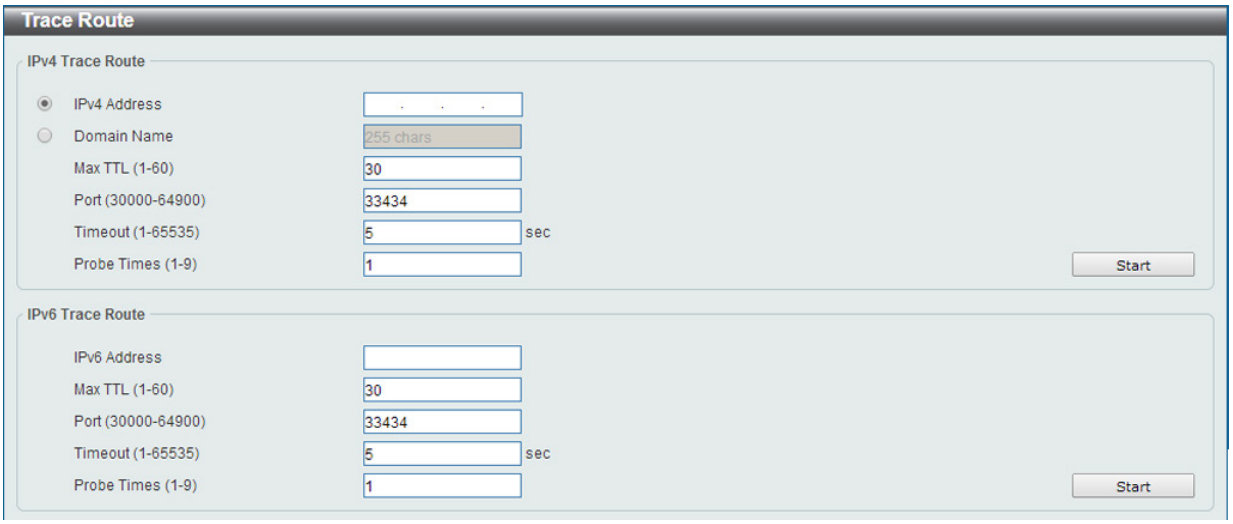


図 16-16　Trace Route 画面

以下の項目を使用して設定、表示を行います。

項目	説明
IPv4 Trace Route	
IPv4 Address	宛先 IPv4 アドレスを入力します。
Domain Name	宛先のドメイン名を入力します。
Max TTL(1-60)	トレースルートリクエストの有効期間。２つのデバイス間のネットワークパスを検索する場合に traceroute コマンドが通過するルータの最大数です。
Port (30000-64900)	仮想ポート数。ポート番号 30000 - 64900 で指定します。
Timeout (1-65535)	リモートデバイスからのレスポンスを待つ場合のタイムアウトの時間を定義します。1-65535（秒）で指定します。
Probe Times(1-9)	予定された traceroute パス上の次のホップに probe パケットをスイッチが送信する回数を指定します。初期値は 1 です。

「Start」ボタンをクリックし、Traceroute プログラムを開始します。

項目	説明
IPv6 Trace Route	
IPv6 Address	宛先ステーションの IPv6 アドレス
Max TTL(1-60)	トレースルートリクエストの有効期間。２つのデバイス間のネットワークパスを検索する場合に traceroute コマンドが通過するルータの最大数です。
Port (30000-64900)	仮想ポート数。ポート番号 30000 - 64900 で指定します。
Timeout (1-65535)	リモートデバイスからのレスポンスを待つ場合のタイムアウトの時間を定義します。1-65535（秒）で指定します。
Probe Times(1-9)	予定された traceroute パス上の次のホップに probe パケットをスイッチが送信する回数を指定します。初期値は 1 です。

「Start」ボタンをクリックし、Traceroute プログラムを開始します。

以下の結果画面が表示されます。

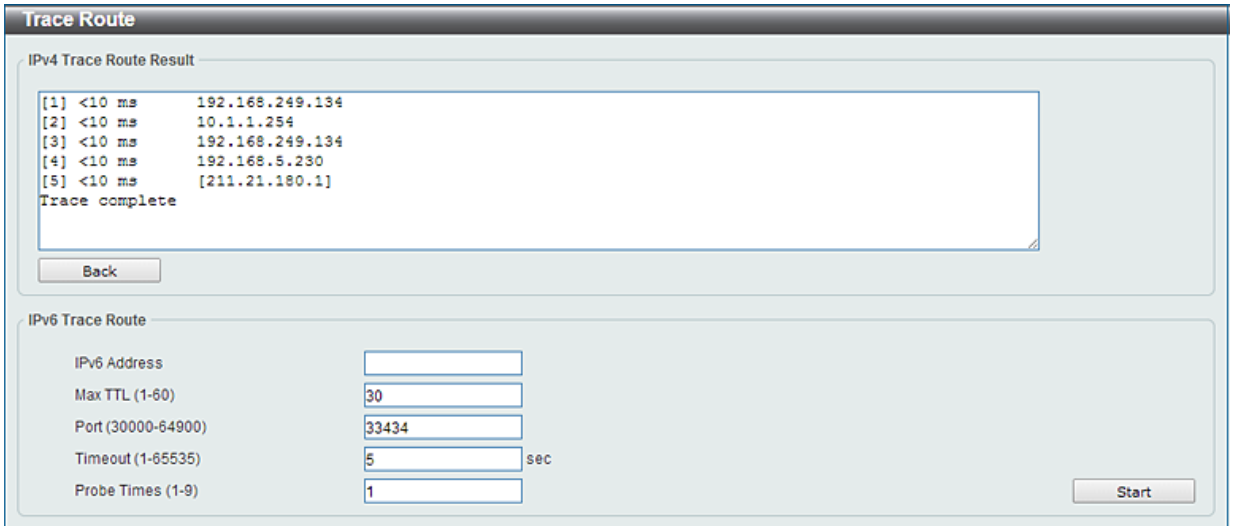


図 16-17　Trace Route Result（IPv4）画面

「Back」ボタンをクリックして、前の画面に戻ります。

Language Management（言語管理）

スイッチへの言語ファイルのインストールを行うことが可能です。

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。

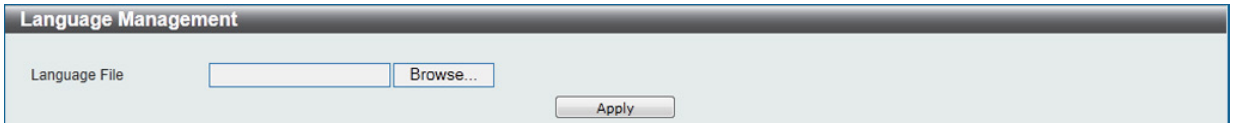


図 16-18　Language Management 画面

以下の項目を使用して設定、表示を行います。

項目	説明
Language File	「Browse/ 参照」ボタンをクリックしてローカル PC にある言語ファイルの場所を指定します。

「Apply」ボタンをクリックし、言語パックのインストールを実行します。

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。

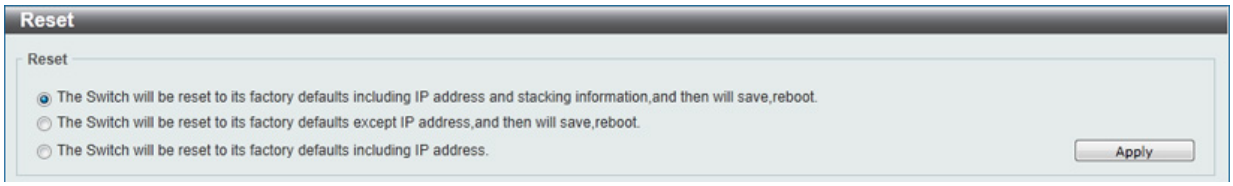


図 16-19　Reset System 画面

項目	説明
The Switch will be reset to its factory defaults including IP address and stacking information, and the will save, reboot	IP アドレス、スタック情報を含むスイッチを工場出荷時設定にリセットして、保存、再起動を実行します。
The Switch will be reset to its factory default except IP address, and then will save, reboot	IP アドレスを除いてスイッチを工場出荷時の設定に戻し、保存、再起動を実行します。
The Switch will be reset to its factory defaults including IP address	IP アドレスを含むスイッチを工場出荷時設定にリセットしますが、再起動は行いません。

「Apply」ボタンをクリックして、リセット操作を開始します。

Reboot System（システム再起動）

スイッチの再起動を行います。

Tools > Reboot をクリックし、以下の設定画面を表示します。

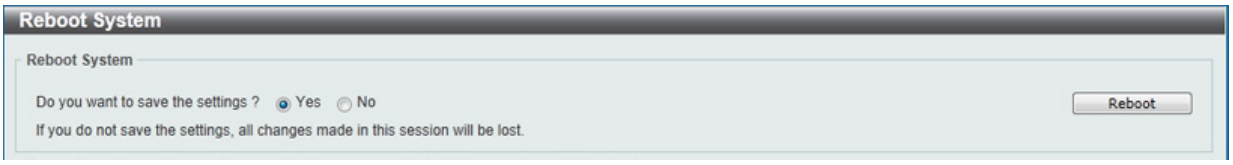


図 16-20　Reboot System 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Yes	スイッチは再起動する前に現在の設定を保存されます。
No	スイッチは再起動する前に現在の設定を保存しません。すべての設定情報は破棄され、最後に保存した時の設定が使われます。
Reboot	スイッチは再起動します。

「Reboot」をクリックして再起動を開始します。

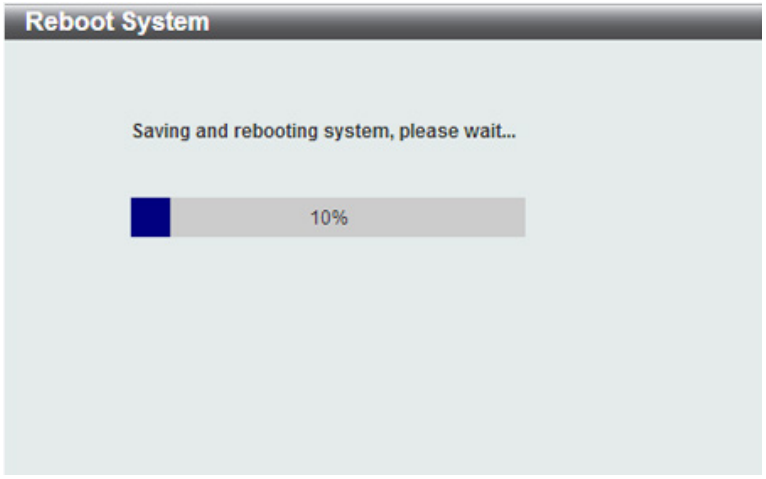


図 16-21　System Rebooting 画面

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 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。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単一の場合において変更することができます。他のユーザセッションがある場合に、Web モードを変更することはできません。

「Surveillance Mode」をクリックすると次の画面が表示されます。複数の設定が自動的に変更される旨のメッセージです。

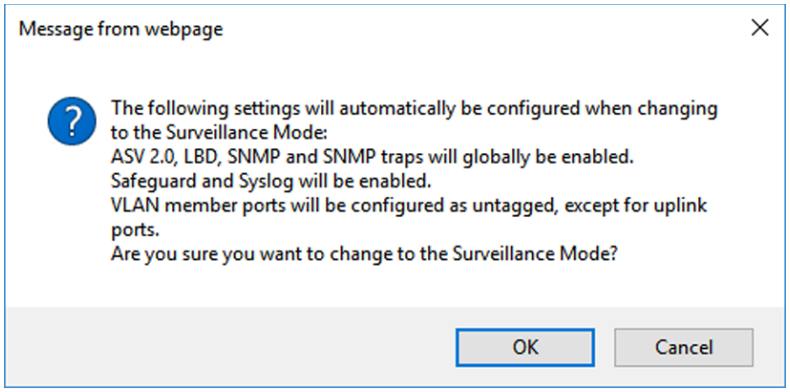


図 16-22　Surveillance Mode Confirmation Message 画面

「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。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。

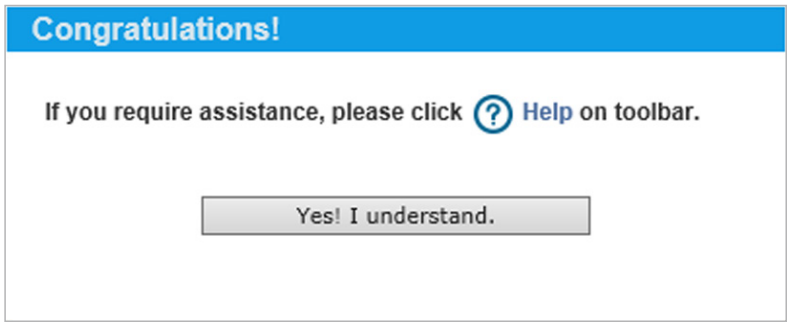


図 16-23　Surveillance Mode 'Congratulations' Message 画面

「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 が用意されています。「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。この二つのモード切替は「Smart Wizard」により行うことが可能です。

- 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）
- PoE Information（PoE 情報）（PoE モデルのみ）
- PoE Scheduling（PoE スケジューリング）（PoE モデルのみ）
- 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）

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。さらに「more」リンクをクリックするとポートに接続されているデバイスの詳細情報にアクセスします。

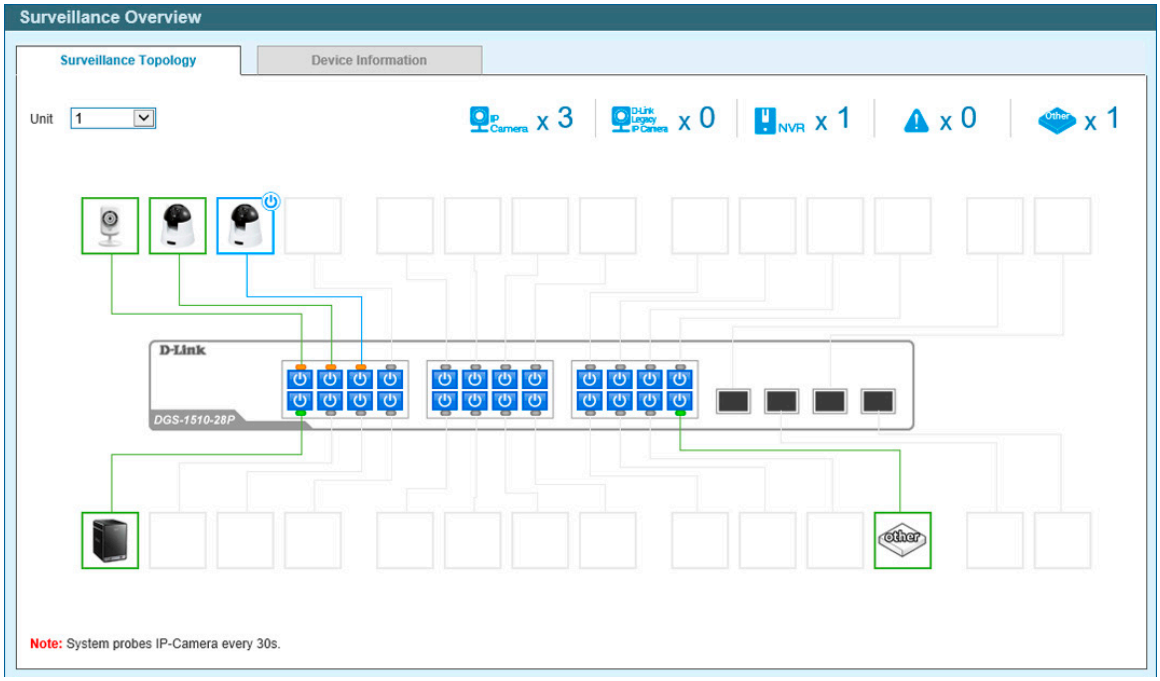


図 17-1　Surveillance Overview 画面

「Unit」で表示するユニットを指定します。

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 数です。
	システム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。緑枠で囲われている機器は PoE 受電機器ではありません。
	スイッチに接続している機器を表示します。青枠で囲われている機器は PoE 受電機器でスイッチから受電しています。「PD Alive」機能が使用可能です。

各ポートの PoE 有効 / 無効状況について以下のように表示されます。

アイコン	説明
	ポートの PoE が有効です。クリックすると無効になります。
	ポートの PoE が無効です。クリックすると有効になります。

PoE の設定について

各ポートの PoE 電力の有効 / 無効についてはアイコンをクリックすることで切り替えることが可能です。初期値では有効です。をクリックすると以下のダイアログが表示されるので、電力を指定し「Apply」をクリックします。

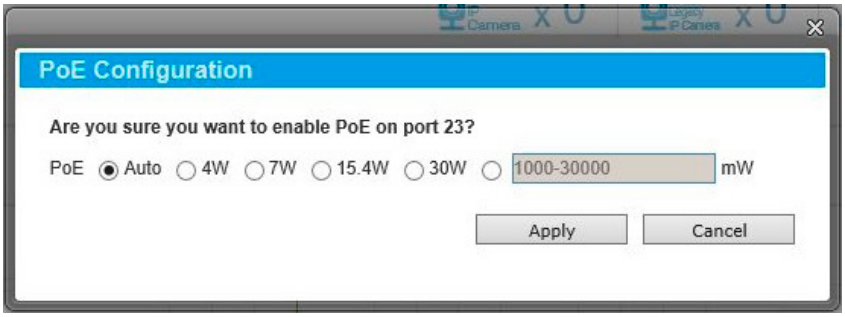


図 17-2　PoE 設定画面

以下の項目が表示されます。

項目	説明
PoE	PoE ポートで提供される電力を指定します。「0W」「4W」「7W」「15.4W」「30W」から指定可能です。チェックボックスにチェックを入れ、自動検出 PD へ供給する最大電力数（W）を指定します。数値を指定しない場合は PD のクラスは供給可能な最大の電力で指定されます。「1000 mW」から「30000 mW」までで指定可能です。

「Apply」ボタンをクリックし、設定を適用します。
「Cancel」をクリックすると、設定は適用されず破棄されます。

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。

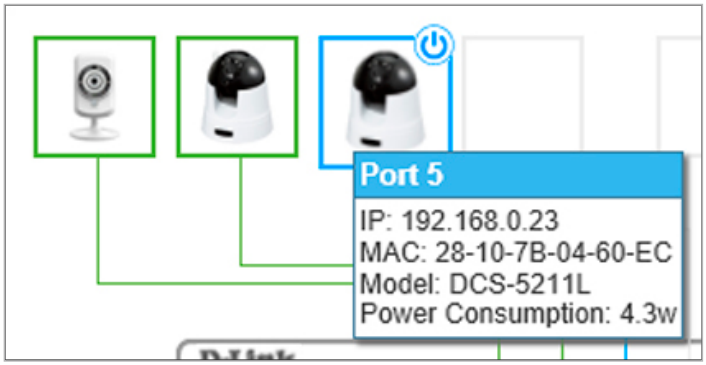


図 17-3　機器情報画面

さらにデバイスアイコンをクリックすると、「PD Alive」について次の画面が表示されます。

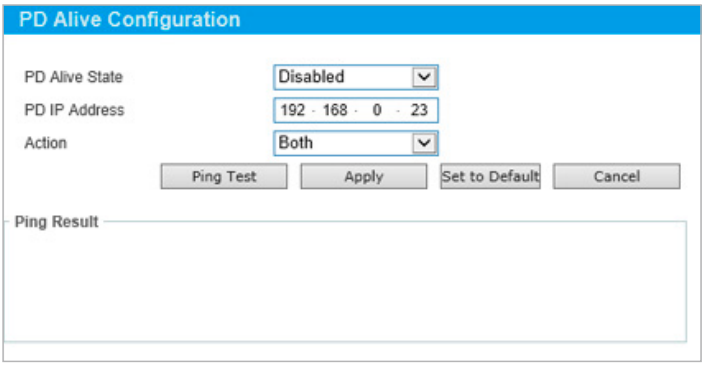


図 17-4　PD Alive Configuration 画面

以下の項目が表示されます。

項目	説明
PD Alive State	「PD Alive」を有効 / 無効に指定します。
PD IP Address	PD（PoE 機器）の IP アドレスを指定します。
Action	「Reset」「Notify」「Both」から実行する動作を指定します。 • Reset - PoE ポートのリセット（PoE のオフ / オン）を実行します。 • Notify - ログとトラップを管理者へ送信します。 • Both - ログとトラップを管理者へ送信し、PoE ポートのリセット（PoE のオフ / オン）を実行します。

「Apply」ボタンをクリックし、設定を適用します。
「Set to Default」ボタンをクリックし、PD を初期設定に戻します。
「Cancel」をクリックすると、設定は適用されず破棄されます。

「Ping Test」ボタンをクリックし、Ping を実行し PD の有効性を確認します。次の画面が表示されます。

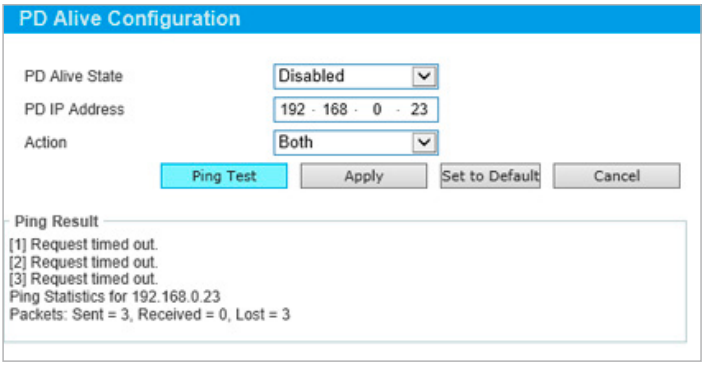


図 17-5　PD Alive Configuration (Ping Result) 画面

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 基準を準拠していない場合があります。「検出されない」など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）

「Device Information」タブでは、3 つのセクション（デバイス情報、PoE 使用情報、帯域使用情報）が表示されます。
他の画面を開いている場合、「機能一覧」の機種名をクリックし、「Device Information」タブを選択して本画面を表示することが可能です。

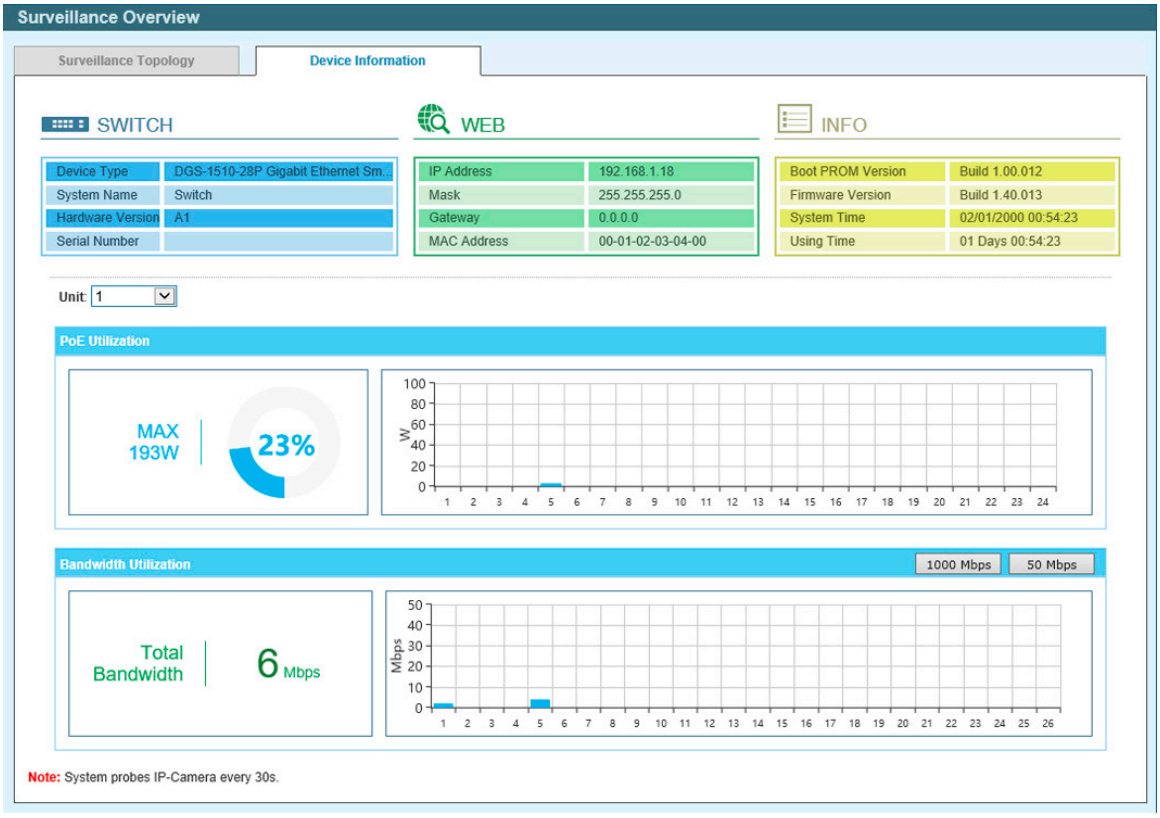


図 17-6　Device Information 画面

「Unit」で表示するユニットを指定します。

以下の項目が表示されます。

表示項目	説明
SWITCH	
Device Type	機種名を表示します。
System Name	システム名を表示します。
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。
WEB	
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。
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。
INFO	
Boot PROM Version	デバイスのブートバージョンを表示します。
Firmware Version	デバイスのファームウェアバージョンを表示します。
System Time	最後のデバイスリセットからの経過時間を表示します。日、時、分、秒の形式で表示します。
Using Time	使用している時間を表示します。日、時、分、秒の形式で表示します。
PoE Utilization（PoE モデルのみ）	
PoE の使用状況を表示します。 左側には PoE 最大供給電力と現在の合計使用率が表示され、右側にはポート毎の使用量がグラフで表示されます。	
Bandwidth Utilization	
帯域（速度）使用状況を表示します。 左側には全ポートにおける受信トラフィックの合計量が表示されます。右側にはポート毎の受信トラフィック帯域使用量がグラフで表示されます。 グラフのスケールは「1000Mbps」「50Mbps」をクリックして変更することができます。 補足 「1000Mbps」ボタンをクリックすると、「Bandwidth Utilization」に表示される最大帯域が 1Gbps となります。「50Mbps」ボタンをクリックすると、「Bandwidth Utilization」に表示される最大帯域が 50Mbps となります。	

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、PoE ステータス、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。各アイコンにマウスカーソルを合わせると、項目名が表示されます。

機能一覧から「Port Information」をクリックします。

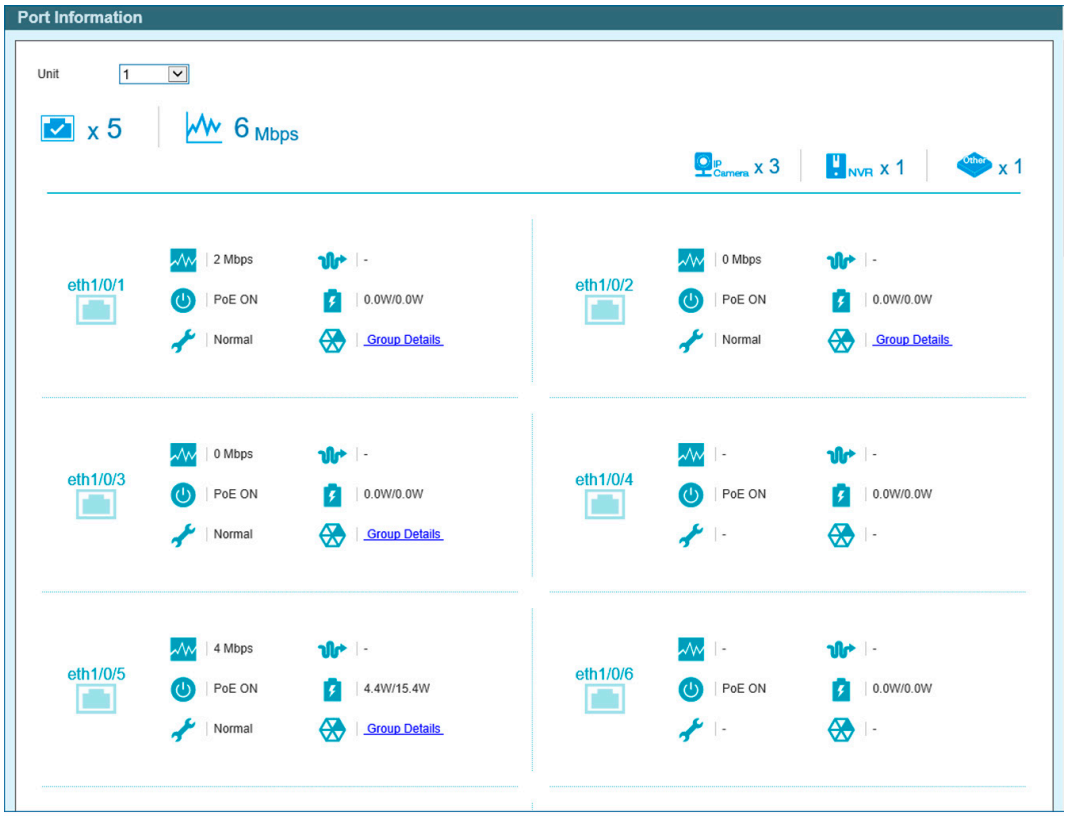
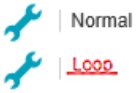


図 17-7　Port Information 画面

「Unit」で表示するユニットを指定します。

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。

アイコン	説明
	接続しているケーブルのケーブル長です。
	ポートの PoE ステータス（PoE の有効 / 無効）です。
	ポートの PoE 電力消費量（使用電力 / 供給可能電力）を表示します。
	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。ループが検出されると、「Normal」は「Loop」表記となり「Health Diagnostics」ページ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）へのリンクアイコンへと変化します。
	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。

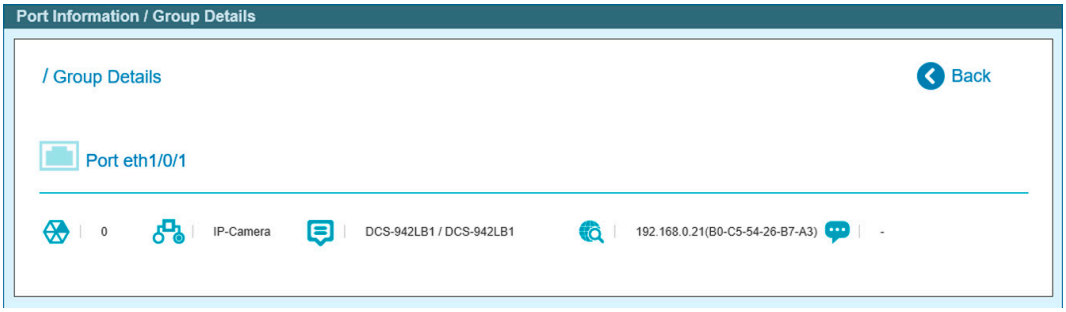


図 17-8　Port Information / Group Details 画面

以下のアイコン、項目が表示されます。

アイコン	説明
	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。ポート番号、デバイスの種類、帯域、IP アドレス、その他の情報（ポートの説明など）、電力消費量が表示されます。各アイコンにマウスカーソルを合わせると、項目名が表示されます。

機能一覧から「IP-Camera Information」をクリックします。

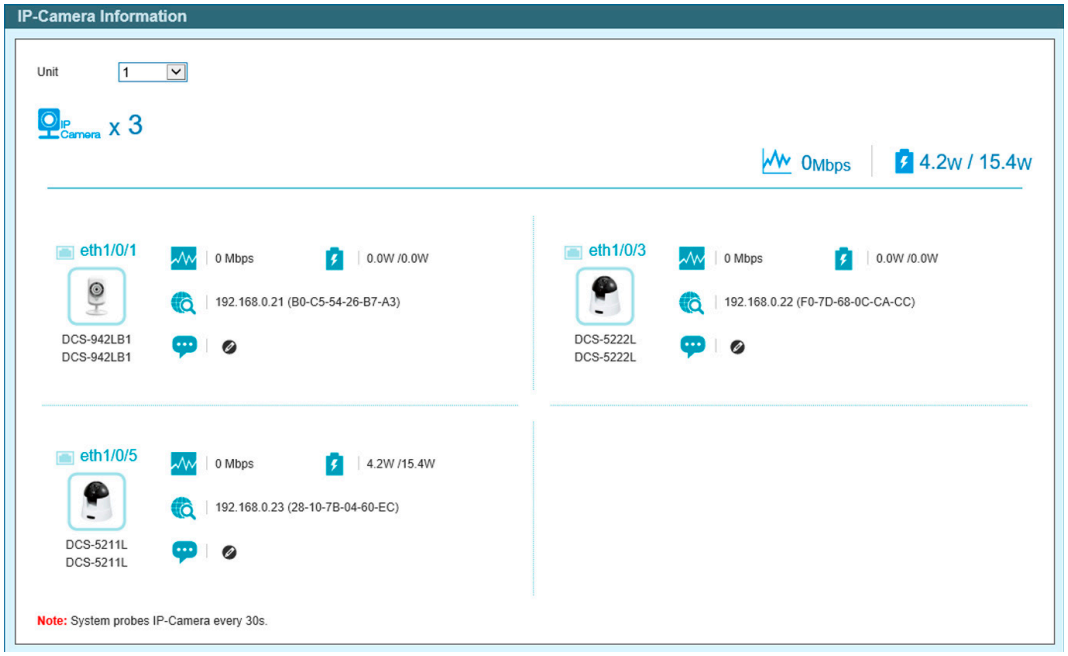


図 17-9　IP-Camera Information 画面

「Unit」で表示するユニットを指定します。

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	
IP Camera	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。
	スイッチのイーサネットポートに接続した ONVIF IP カメラの PoE 電力消費量と PD クラスを表示します。
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。
	ポートの PoE 電力消費量と IP カメラの PD クラスを表示します。
	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。

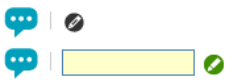
機能一覧から「NVR Information」をクリックします。



図 17-10　NVR Information 画面

「Unit」で表示するユニットを指定します。

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。

PoE Information（PoE 情報）（PoE モデルのみ）

各ポートの Power-over-Ethernet（PoE）使用情報を表示します。

機能一覧から「PoE Information」をクリックします。

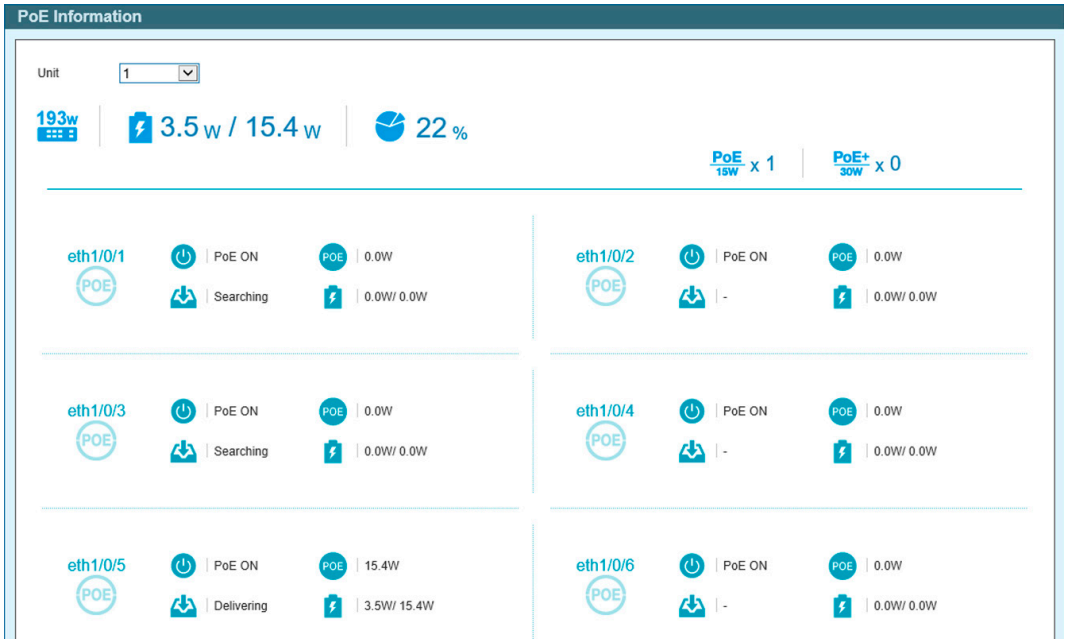


図 17-11　PoE Information 画面

「Unit」で表示するユニットを指定します。

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	
193w	PoE の給電可能電力です。
	PoE 電力消費量と PoE クラスを表示します。
	PoE 給電の使用率（%）について表示します。
PoE 15W	15w の PoE 給電を受ける PoE 受電機器数です。
PoE+ 30W	30w の PoE 給電を受ける PoE 受電機器数です。
各機器情報	
POE	ポート番号です。
	ポートの PoE ステータス（PoE ON / OFF）です。
POE	ポートの最大 PoE 供給可能電力です。
Delivering Power Denied	PoE の状態です。正常に供給されている場合は「Delivering」と表示されます。「Searching」は検出中、「Power Denied」は給電不可（エラー発生）を意味します。「Power Denied」と表示された場合、問題の概要表示と「Health Diagnostic」へのリンクになります。
	ポートの PoE 電力消費量（使用電力 / 供給可能電力）を表示します。

PoE Scheduling（PoE スケジューリング）（PoE モデルのみ）

PoE ポートに電力が供給される時間を設定します。これにより、デバイス未使用時の電力を抑制したり、セキュリティ面の強化として、ビジネス時間外の無線アクセスを遮断したりすることが可能です。スケジュール名、開始時間、終了時間、適用ポートを指定することができます。

機能一覧から「PoE Scheduling」をクリックします。

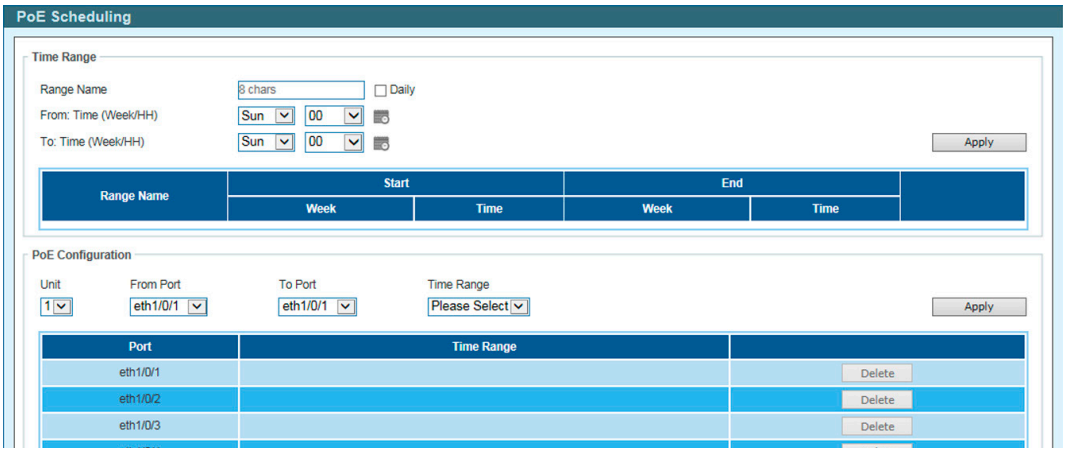


図 17-12　PoE Schedule 画面

新しいタイムレンジの作成：

1. 「Time Range」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。

■ 画面に表示される項目

項目	説明
Range Name	タイムレンジ名を設定します。
From/To: Time (Week/HH)	開始する曜日と時間、終了の曜日と時間を指定します。 「」をクリックするとカレンダー（下図）が表示され、視覚的に日時を指定することができます。  選択後「OK」をクリックします。
Daily	チェックボックスにチェックを入れると曜日設定が「毎日」に指定されます。

2. 「Apply」をクリックしてタイムレンジを作成します。

作成したプロファイルを削除するには、「Delete」をクリックします。

タイムプロファイルの適用：

1. 「PoE Configuration」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。

■ 画面に表示される項目

項目	説明
Unit	設定するユニットを指定します。
From Port / To Port	設定対象のポート範囲を指定します。
Time Range	ポートに適用するタイムスケジュールを指定します。

2. 「Apply」をクリックして設定を有効にします。

設定内容を削除するには、「Delete」をクリックします。

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。

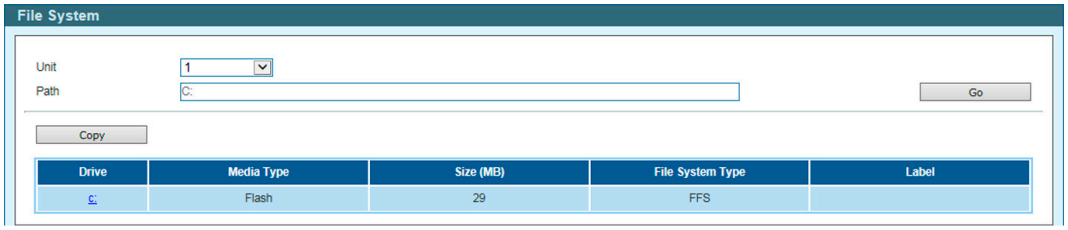


図 17-13　File System 画面

2. 設定したい内容に応じて以下から操作を選択します。

■ 画面に表示される項目

項目	説明
Unit	設定するユニットを指定します。
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。

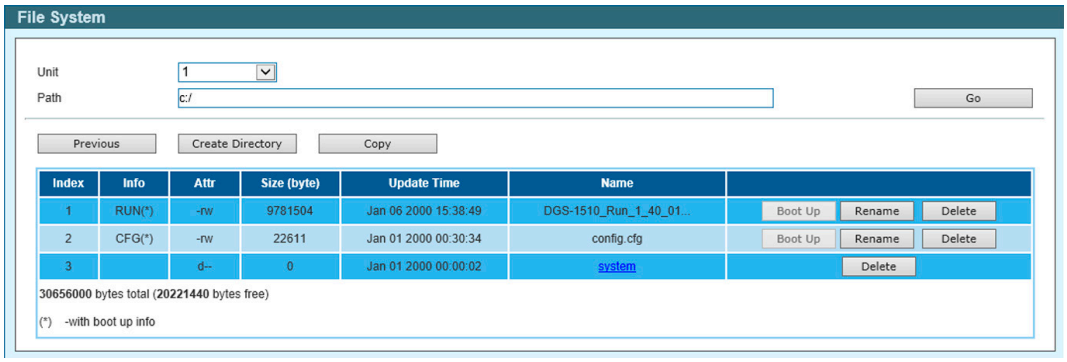


図 17-14　File System（c:）画面

前の画面へ戻るには、「Previous」をクリックします。
ファイルシステムに新しいディレクトリを作成するには、「Create Directory」をクリックします。
指定ランタイムイメージを起動イメージとして設定するには、「Boot Up」をクリックします。
指定ファイル名を編集するには、「Rename」をクリックします。
指定ファイルをファイルシステムから削除するには、「Delete」をクリックします。

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。

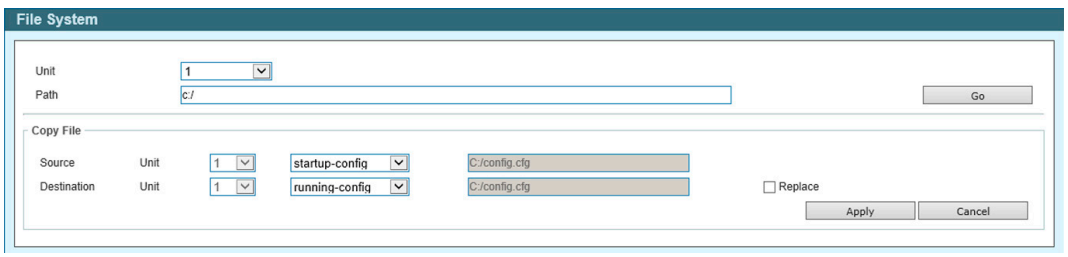


図 17-15　File System（Copy）画面

■ 画面に表示される項目

項目	説明
Source	コピー元のファイルを指定します。
Destination	コピー先のファイルを指定します。
Unit	設定するユニットを指定します。
startup-config	スイッチ開始時のコンフィグを指定します。
running-config	現在のコンフィグを指定します。
Source File	コピー元のファイル名を手動で指定します。
Destination File	コピー先のファイル名を手動で指定します。
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。

注意 本シリーズは RTC を持っていないため、再起動すると設定した時間は消去されます。

1. 「Time」>「Clock Settings」の順にメニューをクリックします。

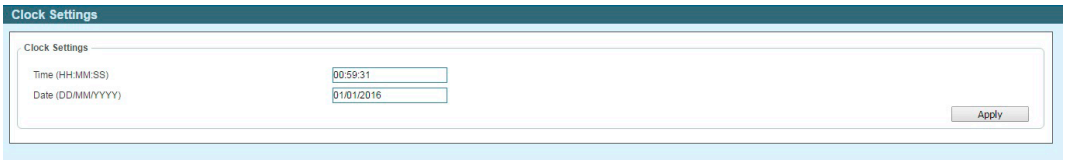


図 17-16　Clock Settings 画面

2. 設定したい内容に応じて以下から操作を選択します。

■ 画面に表示される項目

項目	説明
Time (HH:MM:SS)	システムの時刻を「HH:MM:SS」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」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）

外部の時刻サーバを設定します。Simple Network Time Protocol（SNTP）は NTP プロトコルの簡易版であり、ネットワーク上の時刻サーバと同期してシステムの時刻を調整します。

1. 「Time」>「SNTP Settings」の順にメニューをクリックします。

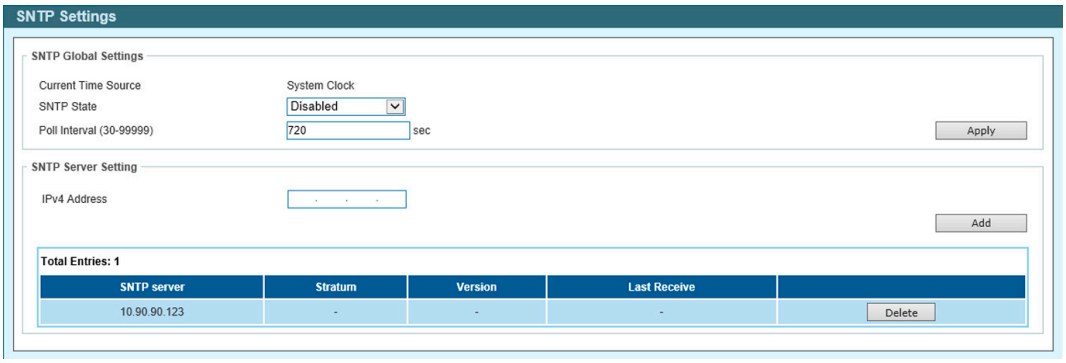


図 17-17　SNTP Settings 画面

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。

■ 画面に表示される項目

項目	説明
SNTP State	SNTP 機能を「Enabled」(有効) または「Disabled」(無効) にします。
Poll Interval (30-99999)	ポーリング間隔を指定します。 初期値：720（秒） 選択可能範囲：30-99999（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。

■ 画面に表示される項目

項目	説明
IPv4 Address	SNTP サーバの IPv4 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 NVR のようなサーベイランスデバイスを認識させることもサポートしています。

「Time」>「Surveillance Settings」の順にメニューをクリックします。

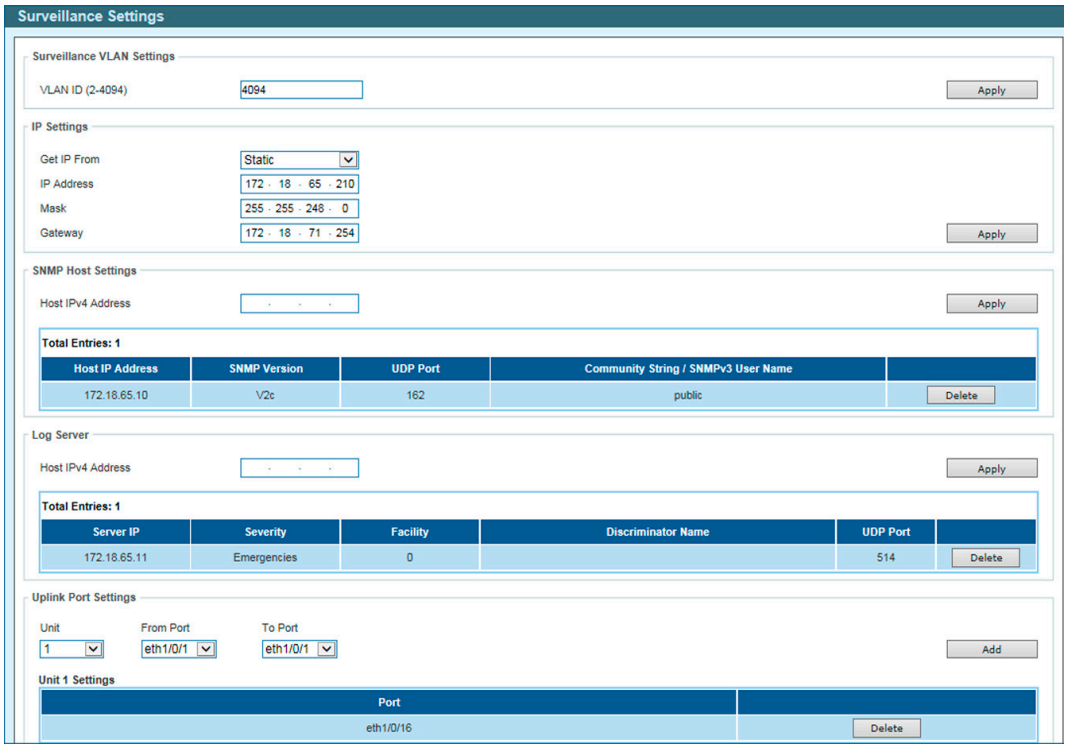


図 17-18　Surveillance Settings 画面

以下の項目が表示されます。

項目	説明
Surveillance VLAN Settings	
VLAN ID (2-4094)	サーベイランス VLAN の ID を指定します。 選択可能範囲：2-4094（秒）
IP Settings	
Get IP From	サーベイランス VLAN の管理 IP の種類を指定します。 選択肢：「Statc」「DHCP」 「Static」を指定した場合、以下の項目の指定を行います。

項目	説明
IP Address	サーベイランス VLAN の管理 IP アドレスを手動で指定します。
Mask	サーベイランス VLAN の管理 IP アドレスのマスクを指定します。
Gateway	サーベイランス VLAN のゲートウェイを指定します。
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	Syslog メッセージを受信する Syslog サーバの IPv4 アドレスを指定します。
Uplink Port Settings	
Unit	設定するユニットを指定します。
From Port / To Port	「From Port」で開始ポート、「To Port」で終了ポートを指定します。 「Delete」で指定ポートを解除することが可能です。

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。

注意 他のスイッチへのサーベイランストラフィックの転送のために、アップリンクポートは全サーベイランス VLAN に所属します。これらのポートでは検出プロセスが無効になっているため、アップリンクポートを他のスイッチに接続することを推奨します。

注意 サーベイランスモードで接続中の IP カメラにアクセスしようとすると、Web GUI でのアクセスが切断される場合があります。その場合、コマンドを使用して「管理 PC が繋がっているポート」のサーベイランス VLAN を無効にするか、MAC アドレスのキャッシュを削除してから再度接続をしてください。

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。

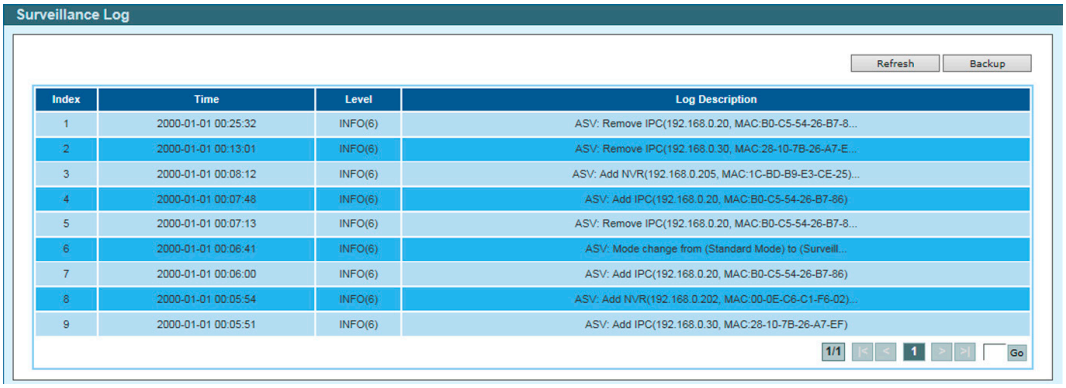


図 17-19　Surveillance Log 画面

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、サーベイランスログを HTTP を使用して、PC へアップロードします。

Health Diagnostic（正常性診断）

ヘルス診断情報、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。

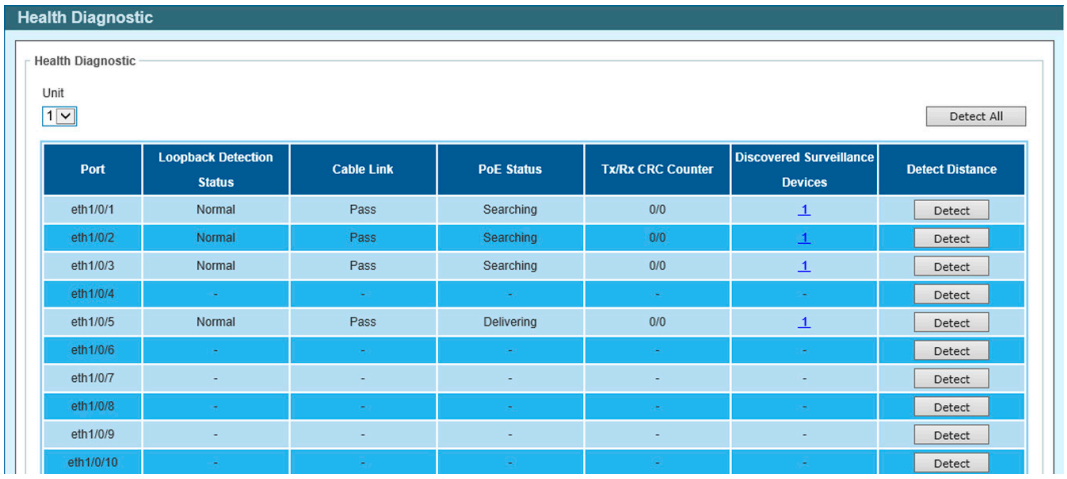


図 17-20　Health Diagnostic 画面

「Unit」で表示するユニットを指定します。以下の項目が表示されます。

項目	説明
Port	表示のポート番号です。
Loopback Detection Status	ポートのループバック検出状況です。 • 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です。 • PASS - 全二重モードでリンクアップしています。 • 10M Half - 10M/ 半二重モードでリンクアップしています。 • 100M Harf - 100M/ 半二重モードでリンクアップしています。
PoE Status	PoE 状況について下記の中から表示します。 「PASS」「MPS (Maintain Power Signature) Absent」「PD Short」「Overload」「Power Denied」「Thermal Shutdown」「Startup Failure」「Classification Failure」
Tx/Rx CRC Counter	TX/RX CRC カウンタについて表示されます。
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」指定ポートのケーブル長テストを開始します。

ケーブル長の検出

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。
スイッチの特定のポートでケーブル長を検出するには、該当ポートの「Detect」をクリックします。

ポートで検出されたデバイスの情報（Group Details）

ポートに接続されたデバイスの情報を確認するには、「Discovered Surveillance Devices」項目のリンクをクリックします。以下の画面が表示されます。

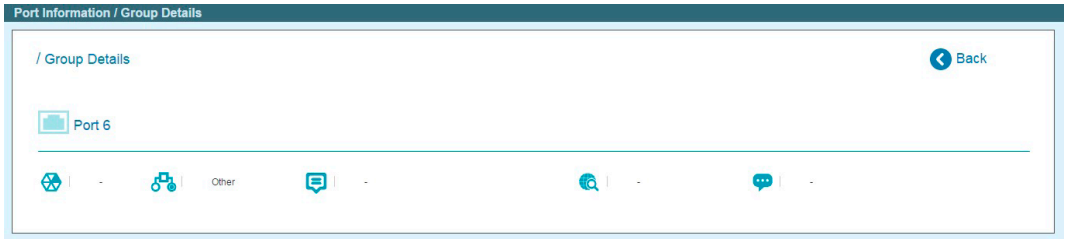


図 17-21　Groupe Details 画面

前の画面に戻るには「Back」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。

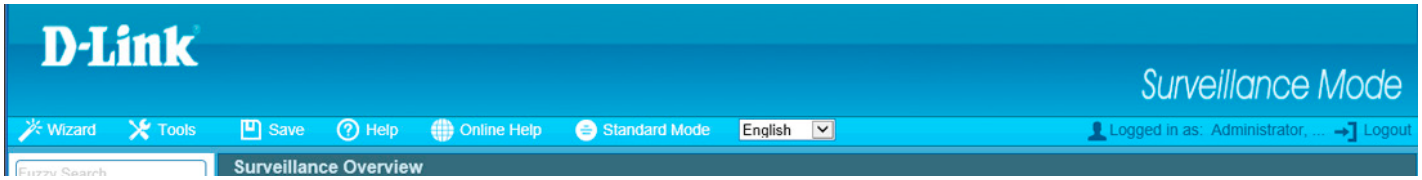


図 17-22　Toolbar（サーベイランスモード）

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。

Toos（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。

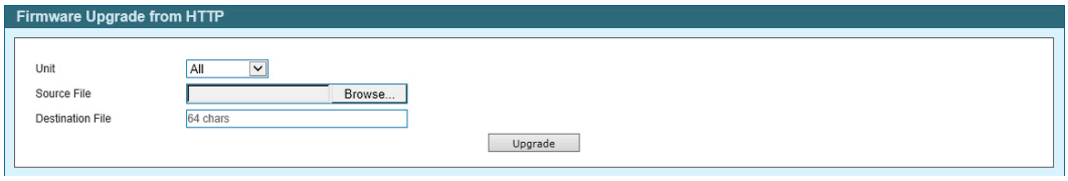


図 17-23　Firmware Upgrade & Backup (HTTP) 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Unit	設定するユニットを選択します。
Source File	ローカル PC にあるファームウェアのパスとファームウェアファイル名を入力します。64 文字まで指定します。「Browse/ 参照」ボタンをクリックしてローカル PC 上のファームウェアファイルの場所を指定できます。
Destination File	ファームウェアがストアされるスイッチの場所を指定します。64 文字までで指定できます。

「Upgrade」ボタンをクリックしてアップグレードを開始します。

注意　ファイルの更新が完全に終了する前に PC との接続を切断したり、電源コードを外したりしないでください。
ファームウェアの更新が終了しないと、スイッチが破損する可能性があります。

Firmware Backup to HTTP（HTTP を使用したファームウェアバックアップ）

HTTP プロトコルを使用して、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。

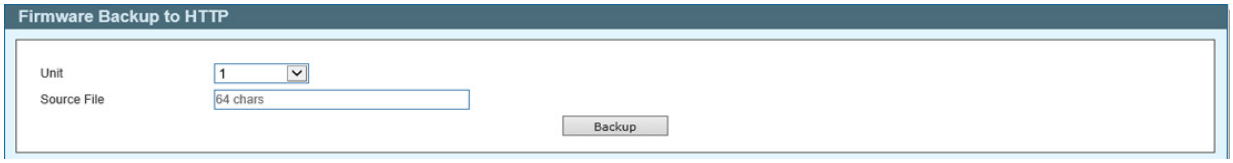


図 17-24　Firmware Backup to HTTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Unit	設定するユニットを選択します。
Source File	スイッチにあるパスとファイル名を入力します。64 文字まで指定します。 Source File（送信元ファイル名 / パス）は「File System（ファイルシステム）」にて確認できます。

「Backup」ボタンをクリックしてバックアップを開始します。

Configuration Restore & Backup（コンフィグレーションリストア＆バックアップ）

Configuration Restore from HTTP（HTTP サーバからコンフィグレーションのリストア）

HTTP サーバを使用してローカル PC からスイッチへ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。

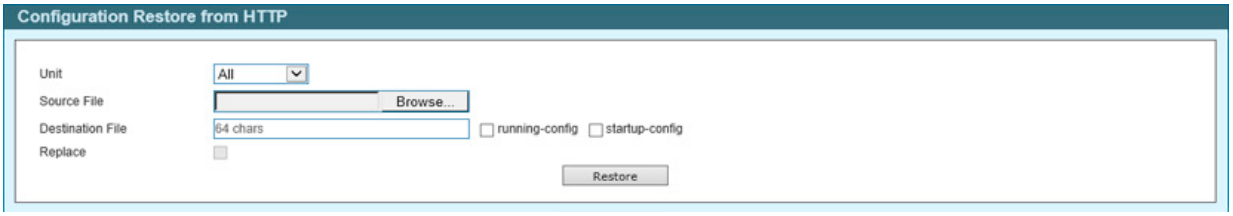


図 17-25　Configuration Restore from HTTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Unit	設定するユニットを選択します。
Source File	ローカル PC にあるコンフィグレーションのパスとコンフィグレーションファイル名を入力します。64 文字まで指定します。 「Browse/ 参照」ボタンをクリックしてローカル PC 上のコンフィグレーションファイルの場所を指定できます。
Destination File	コンフィグレーションファイルがストアされるスイッチの場所を指定します。64 文字までで指定できます。 「running-config」オプションを選択するとリストアと同時に実行中のコンフィグレーションファイルは上書きされます。 「startup-config」オプションを選択すると起動時にコンフィグレーションファイルはリストア＆上書きされます。
Replace	現在実行中のコンフィグレーションを置き換えます。

「Restore」ボタンをクリックしてコンフィグレーションのリストアを開始します。

Configuration 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 プロトコルを使用して、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。

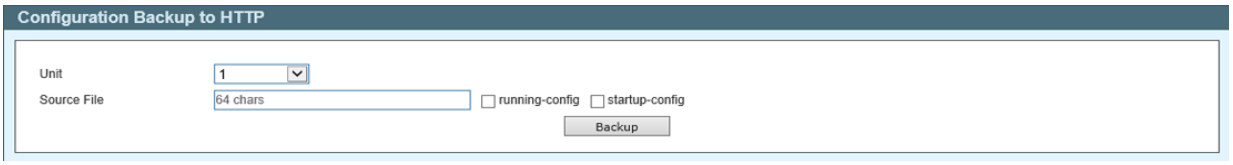


図 17-26　Configuration Backup to HTTP 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Unit	設定するユニットを選択します。
Source File	スイッチにあるパスとファイル名を入力します。64 文字まで指定します。 「running-config」オプションを選択すると実行中のコンフィグレーションファイルがバックアップされます。「startup-config」オプションを選択すると起動時のコンフィグレーションファイルがバックアップされます。 Source File（送信元ファイル名 / パス）は「File System（ファイルシステム）」にて確認できます。

「Backup」ボタンをクリックしてバックアップを開始します。

Language Management（言語管理）

スイッチへの言語ファイルのインストールを行うことが可能です。

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。

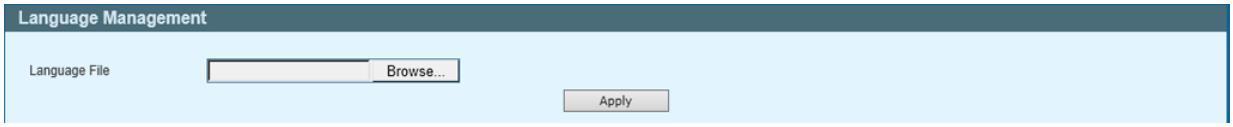


図 17-27　Language Management 画面

以下の項目を使用して設定、表示を行います。

項目	説明
Language File	「Browse/ 参照」ボタンをクリックしてローカル PC にある言語ファイルの場所を指定します。

「Apply」ボタンをクリックし、言語パックのインストールを実行します。

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。

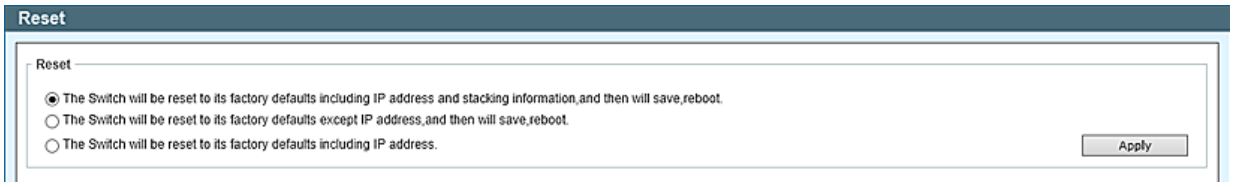


図 17-28　Reset 画面

項目	説明
The Switch will be reset to its factory defaults including IP address and stacking information, and the will save, reboot	IP アドレス、スタック情報を含むスイッチを工場出荷時設定にリセットして、保存、再起動を実行します。
The Switch will be reset to its factory default except IP address, and then will save, reboot	IP アドレスを除いてスイッチを工場出荷時の設定に戻し、保存、再起動を実行します。
The Switch will be reset to its factory defaults including IP address	IP アドレスを含むスイッチを工場出荷時設定にリセットしますが、再起動は行いません。

「Apply」ボタンをクリックして、リセット操作を開始します。

Reboot System（システム再起動）

スイッチの再起動を行います。

Tools > Reboot をクリックし、以下の設定画面を表示します。

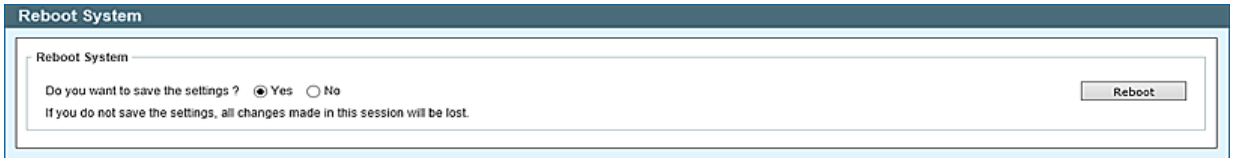


図 17-29　Reboot System 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Yes	スイッチは再起動する前に現在の設定を保存されます。
No	スイッチは再起動する前に現在の設定を保存しません。すべての設定情報は破棄され、最後に保存した時の設定が使われます。
Reboot	スイッチは再起動します。

「Reboot」をクリックして再起動を開始します。

Save（保存）

Save Configuration（コンフィグレーションの保存）

Save > **Save Configuration** をクリックし、以下の画面を表示します。

コンフィグレーションの保存

「Save Configuration」では現在のコンフィグレーションをスイッチに保存します。ユニットを選択し、スイッチのファイルシステムにおけるパス名を「File Path」に入力して「Apply」ボタンをクリックします。

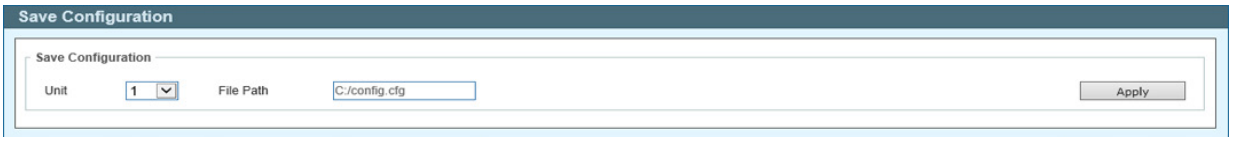


図 17-30　Save Configuration 画面

警告　「Save Config」をクリックしたあと、30 秒間以上経過するまで電源を切らないでください。
30 秒以上経過する前に電源を切ると、設定が正しく保存されないか、設定が工場出荷時状態に戻ります。

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。

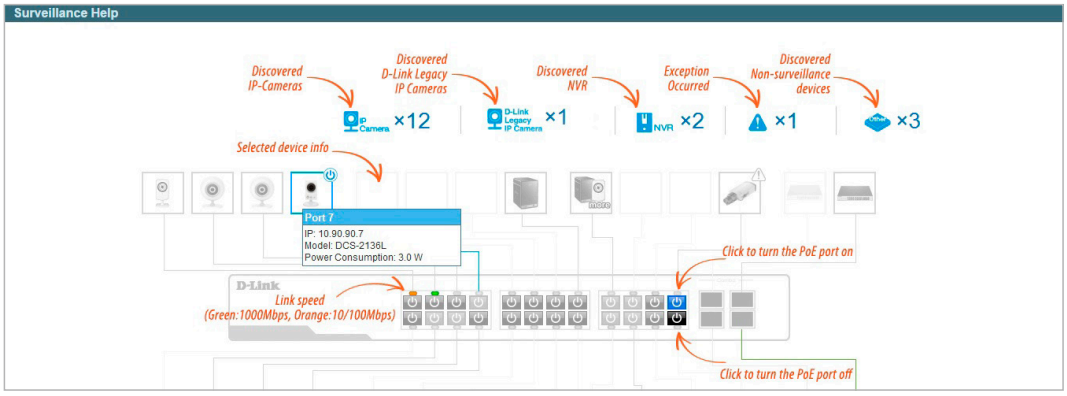


図 17-31　Surveillance Help - Diagram 画面



図 17-32　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。



セッションが複数接続されている場合、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）

クリックするとログアウトします。

【付録 A】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エントリとそれらの意味を以下に示します。

カテゴリ	イベントの説明	ログの内容	緊急度	摘要
802.1X	802.1X 認証失敗	802.1X authentication fail [due to < 原因 >] from (Username: < ユーザ名 >, < インタフェース ID>, MAC: <MAC アドレス >)	Critical	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. : サーバ応答ナシ (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
	802.1X 認証成功	802.1X authentication success (Username: < ユーザ名 >, < インタフェース ID>, MAC: <MAC アドレス >)	Informational	
AAA	AAA がグローバルに有効 / 無効化した。	AAA is <status>.	Informational	
	ログイン成功	Successful login through < 認証種類 > < クライアント IP> authenticated by AAA <AAA 方式 > < サーバ IP> (Username: < ユーザ名 >).	Informational	
	ログイン失敗	Login failed through < 認証種類 > < クライアント IP> authenticated by AAA <AAA 方式 > < サーバ IP> (Username: < ユーザ名 >).	Warning	
	リモートサーバによるログインリクエストへの未応答	Login failed through < 認証種類 > < クライアント IP> due to AAA server < サーバ IP> timeout (Username: < ユーザ名 >).	Warning	
	権限の有効化成功	Successful enable privilege through < 認証種類 > < クライアント IP> authenticated by AAA <AAA 方式 > < サーバ IP> (Username: < ユーザ名 >).	Informational	
	権限有効化失敗	Enable privilege failed through < 認証種類 > < クライアント IP> authenticated by AAA <AAA 方式 > < サーバ IP> (Username: < ユーザ名 >).	Warning	
	リモートサーバによるパスワードリクエストへの未応答	Enable privilege failed through < 認証種類 > < クライアント IP> due to AAA server < サーバ IP> timeout (Username: < ユーザ名 >).	Warning	
	RADIUS サーバにより有効な VLAN ID がアサインされました。	RADIUS server < サーバ IP> assigned VID: <VLAN ID> to port < インタフェース ID> (Username: < ユーザ名 >)	Informational	
	RADIUS サーバにより有効な帯域属性がアサインされました。	RADIUS server < サーバ IP> assigned <direction> bandwidth: < しきい値 > to port < インタフェース ID> (Username: < ユーザ名 >)	Informational	
	RADIUS サーバにより有効な優先値属性がアサインされました。	RADIUS server < サーバ IP> assigned 802.1p default priortiy: < 優先値 > to port < インタフェース ID> (Username: < ユーザ名 >)	Informational	
	RADIUS サーバにより有効な ACL スクリプトがアサインされましたが、不十分なリソースによりアプライに失敗しました。	RADIUS server < サーバ IP> assigns < ユーザ名 > ACL failure at port < インタフェース ID> (<ACL スクリプト >)	Warning	
	RADIUS サーバにより有効な ACL スクリプトがアサインされました。	RADIUS server < サーバ IP> assigns < ユーザ名 > ACL success at port < インタフェース ID> (<ACL スクリプト >)	Informational	

カテゴリ	イベントの説明	ログの内容	緊急度	摘要
ARP Spoofing Prevention	ARP スプーフィング防止で偽 ARP パケットが検出されました。	Gateway <IP アドレス > is under attack by <MAC アドレス > from < インタフェース ID>	Warning	
Auto Save Configuration	DDP 設定情報の自動保存時のイベントを記録しました。	CONFIG-6-DDPSAVECONFIG: [Unit < ユニット ID>,] Configuration automatically saved to flash due to configuring from DDP(Username: < ユーザ名 >, IP: <IP アドレス >)	Informational	
サーベイランス VLAN	ポートに新しくサーベイランス機器が検出されました。	New surveillance device detected (< インタフェース ID>, MAC: <MAC アドレス >)	Informational	
	ポートのサーベイランス VLAN が有効であると、サーベイランス VLAN に自動的に参加します。	< インタフェース ID> add into surveillance VLAN <VLAN ID>	Informational	
	ポートがサーベイランス VLAN から離脱し、同時にポートのエージングタイム内にサーベイランス VLAN が検出されない場合に、本ログメッセージが送信されます。	< インタフェース ID> remove from surveillance VLAN <VLAN ID>	Informational	
	IPC がサーベイランス VLAN に追加された場合、本ログメッセージが送信されます。	ASV: Add IPC(<IP アドレス >)	Informational	
	IPC がサーベイランス VLAN から削除された場合、本ログメッセージが送信されます。	ASV: Remove IPC(<IP アドレス >)	Informational	
	NVR がサーベイランス VLAN に追加された場合、本ログメッセージが送信されます。	ASV: Add NVR(<IP アドレス >)	Informational	
	NVR がサーベイランス VLAN から削除された場合、本ログメッセージが送信されます。	ASV: Remove NVR(<IP アドレス >)	Informational	
	Web GUI で ASV2.0 のモードが変更された場合、本ログメッセージが送信されます。	ASV: Mode change from < モード > to < モード >	Informational	
BPDU 保護	BPDU アタック解消時に記録します。	< インタフェース ID> enter STP BPDU under protection state (mode: < モード >)	Informational	
	BPDU アタックが発生時に記録します。	< インタフェース ID> recover from BPDU under protection state.	Informational	

カテゴリ	イベントの説明	ログの内容	緊急度	摘要
コンフィグレーション / ファームウェア	ファームウェアの更新成功	[Unit < ユニット ID>,]Firmware upgraded by < セッション > successfully (Username: < ユーザ名 >[, IP: <IP アドレス >, MAC: <MAC アドレス >], Server IP: < サーバ IP>, File Name: < ファイル名 >)	Informational	
	ファームウェアの更新失敗	[Unit < ユニット ID>,]Firmware upgraded by < セッション > unsuccessfully (Username: < ユーザ名 >[, IP: <IP アドレス >, MAC: <MAC アドレス >], Server IP: < サーバ IP>, File Name: < ファイル名 >)	Warning	
	ファームウェアのアップロード成功	[Unit < ユニット ID>,]Firmware uploaded by < セッション > successfully (Username: < ユーザ名 >[, IP: <IP アドレス >, MAC: <MAC アドレス >], Server IP: < サーバ IP>, File Name: < ファイル名 >)	Informational	
	ファームウェアのアップロード失敗	[Unit < ユニット ID>,]Firmware uploaded by < セッション > unsuccessfully (Username: < ユーザ名 >[, IP: <IP アドレス >, MAC: <MAC アドレス >], Server IP: < サーバ IP>, File Name: < ファイル名 >)	Warning	
	コンフィグレーションファイルのダウンロード成功	[Unit < ユニット ID>,]Configuration downloaded by < セッション > successfully. (Username: < ユーザ名 >[, IP: <IP アドレス >, MAC: <MAC アドレス >], Server IP: < サーバ IP>, File Name: < ファイル名 >)	Informational	
	コンフィグレーションファイルのダウンロード失敗	[Unit < ユニット ID>,]Configuration downloaded by < セッション > unsuccessfully. (Username: < ユーザ名 >[, IP: <IP アドレス >, MAC: <MAC アドレス >], Server IP: < サーバ IP>, File Name: < ファイル名 >)	Warning	
	コンフィグレーションファイルのアップロード成功	[Unit < ユニット ID>,]Configuration uploaded by < セッション > successfully. (Username: < ユーザ名 >[, IP: <IP アドレス >, MAC: <MAC アドレス >], Server IP: < サーバ IP>, File Name: < ファイル名 >)	Informational	
	コンフィグレーションファイルのアップロード失敗	[Unit < ユニット ID>,] Configuration uploaded by < セッション > unsuccessfully. (Username: < ユーザ名 >[, IP: <IP アドレス >, MAC: <MAC アドレス >], Server IP: < サーバ IP>, File Name: < ファイル名 >)	Warning	
	コンソールによるコンフィグレーションファイルのフラッシュへの保存	[Unit < ユニット ID>,]Configuration saved to flash by console (Username: < ユーザ名 >)	Informational	
	リモートによるコンフィグレーションファイルのフラッシュへの保存	[Unit < ユニット ID>,]Configuration saved to flash (Username: < ユーザ名 >, IP: <IP アドレス >)	Informational	
	ログメッセージのアップロード成功	[Unit < ユニット ID>,] Log message uploaded by < セッション > successfully. (Username: < ユーザ名 >[, IP: <IP アドレス >, MAC: <MAC アドレス >])	Informational	
	ログメッセージのアップロード失敗	Log message uploaded unsuccessfully. Log Message: [Unit < ユニット ID>,] Log message uploaded by < セッション > unsuccessfully. (Username: < ユーザ名 >[, IP: <IP アドレス >, MAC: <MAC アドレス >])	Warning	
	不明な種類のファイルのダウンロード失敗	[Unit < ユニット ID>,]Downloaded by < セッション > unsuccessfully. (Username: < ユーザ名 >[, IP: <IP アドレス >, MAC: <MAC アドレス >], Server IP: < サーバ IP>, File Name: < ファイル名 >)	Warning	

カテゴリ	イベントの説明	ログの内容	緊急度	摘要
DAI	DAI による不正な ARP パケットの検出	Illegal ARP < タイプ > packets (IP: <IP アドレス >, MAC: <MAC アドレス >, VLAN <VLAN ID>, on < インタフェース ID>).	Warning	
	DAI による適正な ARP パケットの検出	Legal ARP < タイプ > packets (IP: <IP アドレス >, MAC: <MAC アドレス >, VLAN <VLAN ID>, on < インタフェース ID>).	Informational	
DDM	SFP の警告しきい値超過	Optical transceiver < インタフェース ID> < しきい値タイプ > < 上限 / 下限 > warning threshold exceeded.	Warning	
	SFP のアラームしきい値超過	Optical transceiver < インタフェース ID> < しきい値タイプ > < 上限 / 下限 > alarm threshold exceeded.	Critical	
	SFP の警告しきい値回復	Optical transceiver < インタフェース ID> < しきい値タイプ > < 上限 / 下限 > warning threshold exceeding back to normal.	Warning	
DHCPv6 クライアント	インタフェースの DHCPv6 クライアントを有効または無効に変更しました。	DHCPv6 client on interface <IP インタフェース名 > changed state to [enabled | disabled].	Informational	
	DHCPv6 クライアントはインタフェースに IPv6 アドレスを取得しました。	DHCPv6 client obtains an ipv6 address <IPv6 アドレス > on interface <IP インタフェース名 >.	Informational	
	DHCPv6 サーバから取得した IPv6 アドレスの更新を開始しました。	The IPv6 address <IPv6 アドレス > on interface <IP インタフェース名 > starts renewing.	Informational	
	DHCPv6 サーバから取得した IPv6 アドレスの更新に成功しました。	The IPv6 address <IPv6 アドレス > on interface <IP インタフェース名 > renews success.	Informational	
	DHCPv6 サーバから取得した IPv6 アドレスの再割り付けを開始しました。	The IPv6 address <IPv6 アドレス > on interface <IP インタフェース名 > starts rebinding.	Informational	
	DHCPv6 サーバから取得した IPv6 アドレスの再割り付けに成功しました。	The IPv6 address <IPv6 アドレス > on interface <IP インタフェース名 > rebinds success.	Informational	
	DHCPv6 サーバから取得した IPv6 アドレスは削除されました。	The IPv6 address <IPv6 アドレス > on interface <IP インタフェース名 > was deleted.	Informational	
DHCPv6 リレー	指定インタフェース DHCPv6 リレーの管理モードが変更されました。	DHCPv6 relay on interface <IP インタフェース名 > changed state to [enabled | disabled]	Informational	
DNS リゾルバ	重複するドメイン名が追加されたため、ダイナミックドメイン名が削除されました。	[DNS_RESOLVER(1):]Duplicate Domain name case name: < ドメイン名 >, static IP: <IP アドレス >, dynamic IP:<IP アドレス >	Informational	
DoS 防御	DoS 攻撃の検出	<dos-type> is dropped from (IP: <IP アドレス > Port < インタフェース ID>).	Notice	

カテゴリ	イベントの説明	ログの内容	緊急度	摘要
エラーディセーブル	ポートがエラーディセーブル状態に移行しました	Port < インタフェース ID> enters error disable state due to < 原因 >	Warning	< 原因 > の値： • Loopback Detection • Port Security Violation • Storm Control, BPDU Protect • ARP Rate Limit • DHCP Rate Limit • Digital Diagnostics Monitoring • Scheduled Port-shutdown by Power Saving • Scheduled Hibernation by Power Saving
	ポートがエラーディセーブル状態からリカバリしました	Port < インタフェース ID> leaves the error disable state which is previously caused by < 原因 >	Warning	< 原因 > の値： • Loopback Detection • Port Security Violation • Storm Control, BPDU Protect • ARP Rate Limit • DHCP Rate Limit • Digital Diagnostics Monitoring • Scheduled Port-shutdown by Power Saving • Scheduled Hibernation by Power Saving
	ポートがエラーディセーブル状態に移行しました	Port < インタフェース ID> VLAN <VLAN ID> enters error disable state due to < 原因 >		< 原因 > の値： • Loopback Detection • Port Security Violation • Storm Control, BPDU Protect • ARP Rate Limit • DHCP Rate Limit • Digital Diagnostics Monitoring • Scheduled Port-shutdown by Power Saving • Scheduled Hibernation by Power Saving
	ポートがエラーディセーブル状態からリカバリしました	Port < インタフェース ID> VLAN <VLAN ID> leaves the error disable state which is previously caused by < 原因 >		< 原因 > の値： • Loopback Detection • Port Security Violation • Storm Control, BPDU Protect • ARP Rate Limit • DHCP Rate Limit • Digital Diagnostics Monitoring • Scheduled Port-shutdown by Power Saving • Scheduled Hibernation by Power Saving
インタフェース	ポートダウン	Port < ポートタイプ >< インタフェース ID> link down	Informational	
	ポートアップ	Port < ポートタイプ >< インタフェース ID> link up, < リンク速度 >	Informational	
	ポートが半二重モードでリンク	ASV: Port < インタフェース ID> Half duplex detected	Informational	
JWAC	ホストによる認証通過	JWAC host login success (Username: < 文字列 >, IP: <IP アドレス | IPv6 アドレス >, MAC: <MAC アドレス >, < インタフェース ID>, VID: <VLAN ID>).	Informational	
	ホストによる認証失敗	JWAC host login fail (Username: < 文字列 >, IP: <IP アドレス | IPv6 アドレス >, MAC: <MAC アドレス >, < インタフェース ID>, VID: <VLAN ID>)	Critical	
	認証ユーザ数が上限に達しました。	JWAC enters stop learning state.	Warning	
	認証ユーザ数が上限を下回りました。	JWAC recovered from stop learning state.	Warning	

カテゴリ	イベントの説明	ログの内容	緊急度	摘要
LACP	リンクアグリゲーショングループのリンクアップ	Link Aggregation Group < グループ ID> link up.	Informational	
	リンクアグリゲーショングループのリンクダウン	Link Aggregation Group < グループ ID> link down.	Informational	
	メンバポートのリンクアグリゲーショングループへの参加	< インタフェース名 > attach to Link Aggregation Group < グループ ID>.	Informational	
	メンバポートのリンクアグリゲーショングループからの離脱	< インタフェース名 > detach from Link Aggregation Group < グループ ID>.	Informational	
ループバック検知（LBD）	ポートでループが発生	< インタフェース ID> LBD loop occurred.	Critical	
	VLAN でループが発生	< インタフェース ID> VLAN <VLAN ID> LBD loop occurred.	Critical	
	インタフェースでのループが回復	< インタフェース ID> LBD loop recovered.	Critical	
	VLAN でのループが回復	< インタフェース ID> VLAN <VLAN ID> LBD loop recovered.	Critical	
	ループバックが発生した VLAN の数が予約数を超えています。	Loop VLAN number overflow	Critical	

カテゴリ	イベントの説明	ログの内容	緊急度	摘要
LLDP	LLDP-MED トポロジの変更が検出されました。	LLDP-MED topology change detected (on port < ポート番号 >. chassis id: < シャーシ種類>, < シャーシ ID>, port id: < ポートタイプ>, < ポート ID>, device class: < デバイスクラス >)	notice	< シャーシ種類 > の値のリスト： 1. chassisComponent(1) 2. interfaceAlias(2) 3. portComponent(3) 4. macAddress(4) 5. networkAddress(5) 6. interfaceName(6) 7. local(7) < ポートタイプ > の値のリスト： 1. interfaceAlias(1) 2. portComponent(2) 3. macAddress(3) 4. networkAddress(4) 5. interfaceName(5) 6. agentCircuitId(6) 7. local(7)
	LLDP-MED デバイスタイプの重複が検出されました	Conflict LLDP-MED device type detected (on port < ポート番号 >, chassis id: < シャーシ種類>, < シャーシ ID>, port id: < ポートタイプ>, < ポート ID>, device class: < デバイスクラス >)	notice	< シャーシ種類 > の値のリスト： 1. chassisComponent(1) 2. interfaceAlias(2) 3. portComponent(3) 4. macAddress(4) 5. networkAddress(5) 6. interfaceName(6) 7. local(7) < ポートタイプ > の値のリスト： 1. interfaceAlias(1) 2. portComponent(2) 3. macAddress(3) 4. networkAddress(4) 5. interfaceName(5) 6. agentCircuitId(6) 7. local(7)
	互換性のない LLDP-MED TLV が検出されました。	Incompatible LLDP-MED TLV set detected (on port < ポート番号 >, chassis id: < シャーシタイプ >, < シャーシ ID>, port id: < ポートタイプ >, < ポート ID>, device class: < デバイスクラス >)	notice	< シャーシ種類 > の値のリスト： 1. chassisComponent(1) 2. interfaceAlias(2) 3. portComponent(3) 4. macAddress(4) 5. networkAddress(5) 6. interfaceName(6) 7. local(7) < ポートタイプ > の値のリスト： 1. interfaceAlias(1) 2. portComponent(2) 3. macAddress(3) 4. networkAddress(4) 5. interfaceName(5) 6. agentCircuitId(6) 7. local(7)

カテゴリ	イベントの説明	ログの内容	緊急度	摘要
ログイン / ログアウト CLI	コンソール経由のログイン成功	Unit < ユニット ID>, Successful login through Console（Username: < ユーザ名 >）	Informational	
	コンソール経由のログイン失敗	Unit< ユニット ID>, Login failed through Console（Username: < ユーザ名 >）	Warning	
	コンソールセッション、タイムアウト	Unit< ユニット ID>, Console session timed out（Username: < ユーザ名 >）	Informational	
	コンソール経由でログアウト	Unit< ユニット ID>, Logout through Console（Username: < ユーザ名 >）	Informational	
	Telnet 経由のログイン成功	Successful login through Telnet（Username: < ユーザ名 >, IP: <IP アドレス >）	Informational	
	Telnet 経由のログイン失敗	Login failed through Telnet（Username: < ユーザ名 >, IP: <IP アドレス >）	Warning	
	Telnet セッションタイムアウト	Telnet session timed out（Username: < ユーザ名 >, IP: <IP アドレス >）	Informational	
	Telnet 経由でログアウト	Logout through Telnet（Username: < ユーザ名 >, IP: <IP アドレス >）	Informational	
	SSH 経由のログイン成功	Successful login through SSH（Username: < ユーザ名 >, IP: <IP アドレス >）	Informational	
	SSH 経由のログイン失敗	Login failed through SSH（Username: < ユーザ名 >, IP: <IP アドレス >）	Critical	
	SSH セッション、タイムアウト	SSH session timed out（Username: < ユーザ名 >, IP: <IP アドレス >）	Informational	
	SSH 経由でログアウト	Logout through SSH（Username: < ユーザ名 >, IP: <IP アドレス >）	Informational	
MAC アクセスコントロール	ホストは認証を通過しました。	MAC-based Access Control host login success (MAC: <MAC アドレス >, < インタフェース ID>, VID: <VLAN ID>).	Informational	
	ホストはエージングアウトします。	MAC-based Access Control host aged out (MAC: <MAC アドレス >, < インタフェース ID>, VID: <VLAN ID>).	Informational	
	ホストは認証を通過しませんでした。	MAC-based Access Control host login fail (MAC: <MAC アドレス >, < インタフェース ID>, VID: <VLAN ID>).	Critical	
	機器の認証ユーザ数が最大に達しました。	MAC-based Access Control enters stop learning state.	Warning	
	機器の認証ユーザ数が最大を下回りました。	MAC-based Access Control recovers from stop learning state.	Warning	
	インタフェースの認証ユーザ数が最大に達しました。	< インタフェース ID> enters MAC-based Access Control stop learning state.	Warning	
	インタフェースの認証ユーザ数が最大を下回りました。	< インタフェース ID> recovers from MAC-based Access Control stop learning state.	Warning	

カテゴリ	イベントの説明	ログの内容	緊急度	摘要
MSTP デバッグ拡張	スパニングツリープロトコル有効化	Spanning Tree Protocol is enabled	Informational	
	スパニングツリープロトコル無効化	Spanning Tree Protocol is disabled	Informational	
	トポロジ変更	Topology changed [([Instance:< インスタンス ID>] ,port: <[ユニット ID:] ポート番号 > ,MAC: <MAC アドレス >)]	Notice	
	スパニングツリーの新規ルートブリッジを選択	[CIST | CIST Regional | MSTI Regional] New Root bridge selected ([Instance: < インスタンス ID>] MAC: <MAC アドレス > Priority :< 値 >)	Informational	
	新しいルートポートが選択されました。	New root port selected [([Instance:< インスタンス ID>], port:<[ユニット ID:] ポート番号 >)]	Notice	
	スパニングツリーポートステータスが変更されました。	Spanning Tree port status change (Instance :< インスタンス ID>, < インタフェース ID>) < 旧状態 > -> < 新状態 >	Notice	
	スパニングツリーポートロールが変更されました。	Spanning Tree port role change (Instance :< インスタンス ID>, < インタフェース ID>) < 旧ロール > -> < 新ロール >	Informational	
	スパニングツリーインスタンスが作成されました。	Spanning Tree instance created. Instance:< インスタンス ID> InstanceID: インスタンス ID	Informational	
	スパニングツリーインスタンスが削除されました。	Spanning Tree instance deleted. Instance:< インスタンス ID> InstanceID: インスタンス ID	Informational	
	スパニングツリーのバージョンが変更されました。	Spanning Tree version changed. New version: < 新バージョン >	Informational	
	スパニングツリー MST コンフィグレーション ID 名とリビジョンが変更されました。	Spanning Tree MST configuration ID name and revision level changed (name: < 名称 > ,revision level < 新しいリビジョンレベル >).	Informational	
	スパニングツリー MST コンフィグレーション ID VLAN マッピングテーブルが追加されました。	Spanning Tree MST configuration ID VLAN mapping table changed (instance: < インスタンス ID> add vlan < 開始 VLAN ID> [- < 終わり VLAN ID>]).	Informational	
	スパニングツリー MST コンフィグレーション ID VLAN マッピングテーブルが削除されました。	Spanning Tree MST configuration ID VLAN mapping table changed (instance: < インスタンス ID> delete vlan < 開始 VLAN ID> [- < 終わり VLAN ID>])	Informational	
	ガードルートの都合で STP ポートロールは代替に変更されました。	Spanning Tree port role change (Instance :< インスタンス ID>, < インタフェース ID>) to alternate port due to the guard root	Informational	
周辺機器	ファン回復	Unit < ユニット ID>, < ファン > back to normal.	Critical	
	ファン不動作	Unit < ユニット ID> < ファン > failed	Critical	
	温度センサのアラーム状態への移行	Unit < ユニット ID> < 温度センサ > detects abnormal temperature < 温度 >	Critical	
	温度の通常回復	Unit < ユニット ID> < 温度センサ > temperature back to normal	Critical	
	電源喪失	Unit < ユニット ID> < 電源 > failed	Critical	
	電源回復	Unit < ユニット ID> < 電源 > back to normal	Critical	
	ファクトリリセットボタンの押下	Unit < ユニット ID> factory reset button pressed.	Critical	

カテゴリ	イベントの説明	ログの内容	緊急度	摘要
PoE	使用電力のしきい値越え	Unit < ユニット ID> usage threshold < パーセンテージ > is exceeded	Warning	
	使用電力のしきい値回復	Unit < ユニット ID> usage threshold < パーセンテージ > is recovered	Warning	
	PD による Ping 未応答	PD alive check failed. (Port: < ポート番号 >, PD: <IP アドレス >)	Warning	
	Maintain Power Signature（MPS）の喪失による電力供給の停止	ASV: Port < ポート種類 > < インタフェース ID> PoE MPS Absent	Warning	
	短絡の検出	ASV: Port < ポート種類 < インタフェース ID> PoE PD short	Warning	
	オーバーロードの検出	ASV: Port < ポート種類 < インタフェース ID> PoE Overload	Warning	
	不具合による電力供給の停止または拒否	ASV: Port < ポート種類 > < インタフェース ID> PoE Power Denied	Warning	
	過熱による電力供給の停止または拒否	ASV: Port < ポート種類 > < インタフェース ID> PoE Thermal Shutdown	Warning	
	ポートでの PoE 開始失敗	ASV: Port < ポート種類 > < インタフェース ID> PoE Startup Failure	Warning	
	PD の識別不可	ASV: Port < ポート種類 > < インタフェース ID> PoE Classification Failure	Warning	
Port Security	ポートアドレスの最大値到達	MAC address <MAC アドレス > causes port security violation on < インタフェース ID>.	Warning	
	システムアドレスの最大値到達	Limit on system entry number has been exceeded.	Warning	
セーフガードエンジン	セーフガードエンジン機能がフィルタリングパケットモードに遷移しました。	Unit < ユニット ID>,Safeguard Engine enters EXHAUSTED mode	Warning	
	セーフガードエンジン機能がノーマルモードに遷移しました。	Unit < ユニット ID>,SafeGuard Engine enters NORMAL mode	Informational	
SNMP	無効なコミュニティ名を含む SNMP request 受信	SNMP request received from <IP アドレス > with invalid community string!	Informational	
SSH	SSH サーバ有効化	SSH server is enabled	Informational	
	SSH サーバ無効化	SSH server is disabled	Informational	

カテゴリ	イベントの説明	ログの内容	緊急度	摘要
Stacking	ホットインサーション	Unit: < ユニット ID>, MAC: <MAC アドレス > Hot insertion.	Informational	
	ホットリムーバル	Unit: < ユニット ID>, MAC: <MAC アドレス > Hot removal.	Informational	
	スタッキングトポロジの変更	Stacking topology is < スタックトポロジタイプ >. Master(Unit< ユニット ID>, MAC:<MAC アドレス >)	Informational	
	バックアップマスタのマスタへの変更	Backup master changed to master. Master (Unit< ユニット ID>)	Informational	
	スレーブのマスタへの変更	Slave changed to master. Master (Unit< ユニット ID>)	Informational	
	Box ID の衝突	Hot insert failed, box ID conflict: Unit <ユニット ID> conflict (MAC: <MAC アドレス > and MAC: <MAC アドレス >).	Critical	
	スタッキングポートがリンクアップしています。	Stacking port < ポート > link up	Critical	スタッキングポートは SIO インタフェースまたはそのメンバ（SIO Trunk）として動作します。本ログエントリはデバイスパネルのポート番号識別にスタッキングポートが表示されている場合のみ有効です。
	スタッキングポートがリンクダウンしています。	Stacking port < ポート > link down	Critical	スタッキングポートは SIO インタフェースまたはそのメンバ（SIO Trunk）として動作します。本ログエントリはデバイスパネルのポート番号識別にスタッキングポートが表示されている場合のみ有効です。
	SIO インタフェースがリンクアップしています。	SIO interface Unit < ユニット ID> <SIO インタフェース番号 > link up	Critical	SIO Trunk の場合、最初のメンバポートのリンクアップがトリガとなります。
	SIO インタフェースがリンクダウンしています。	SIO interface Unit < ユニット ID> <SIO インタフェース番号 > link down	Critical	SIO Trunk の場合、最後のメンバポートのリンクアップがトリガとなります。
Storm Control	ストーム発生	<Broadcast | Multicast | Unicast> storm is occurring on < インタフェース ID>.	Warning	
	ストーム解消	<Broadcast | Multicast | Unicast> storm is cleared on < インタフェース ID>.	Informational	
	パケットストーム発生によるポートシャットダウン	< インタフェース ID> is currently shut down due to the <Broadcast | Multicast | Unicast> storm.	Warning	
システムログサマリ	システムウォームスタート	[Unit < ユニット ID>,]System warm start	Critical	
	システムコールドスタート	[Unit < ユニット ID>,]System cold start	Critical	
	システム起動	[Unit < ユニット ID>,]System started up.	Critical	
Telnet	Telnet 経由のログイン成功	Successful login through Telnet（Username: < ユーザ名 >, IP: <IP アドレス >）	Informational	
	Telnet 経由のログイン失敗	Login failed through Telnet（Username: < ユーザ名 >, IP: <IP アドレス >）	Warning	
	Telnet 経由でログアウト	Logout through Telnet（Username: < ユーザ名 >, IP: <IP アドレス >）	Informational	
	Telnet セッションタイムアウト	Telnet session timed out（Username: < ユーザ名 >, IP: <IP アドレス >）	Informational	

カテゴリ	イベントの説明	ログの内容	緊急度	摘要
音声 VLAN	新しい音声機器を検出	New voice device detected (< インタフェース ID>, MAC: <MAC アドレス >)	Informational	
	自動音声 VLAN モードのインタフェースを音声 VLAN に追加しました。	< interface-id > add into voice VLAN <VLAN ID>	Informational	
	インタフェースが音声 VLAN から離脱し、同時にそのインタフェースのエージングタイム内に音声 VLAN が見つからないとログメッセージを送信します。	< interface-id > remove from voice VLAN <VLAN ID>	Informational	
Web	Web 経由のログイン成功	Successful login through Web（Username: < ユーザ名 >, IP: <IP アドレス >）	Informational	
	Web 経由のログイン失敗	Login failed through Web（Username: < ユーザ名 >, IP: <IP アドレス >）	Warning	
	Web セッションタイムアウト	Web session timed out (Username: < ユーザ名 >, IP: <IP アドレス >)	Informational	
	Web 経由でログアウト	Logout through Web（Username: < ユーザ名 >, IP: <IP アドレス >）	Informational	
	Web（SSL）経由のログイン成功	Successful login through Web (SSL) (Username: < ユーザ名 >, IP: <IP アドレス >)	Informational	
	Web（SSL）経由のログイン失敗	Login failed through Web (SSL) (Username: < ユーザ名 >, IP: <IP アドレス >)	Informational	
	Web（SSL）セッションタイムアウト	Web (SSL) session timed out (Username: < ユーザ名 >, IP: <IP アドレス >)	Informational	
	Web（SSL）経由でログアウト	Logout through Web(SSL) (Username: < ユーザ名 >, IP: <IP アドレス >)	Informational	
Web 認証	ホストによる認証通過	Web-Authentication host login success (Username: < 文字列 >, IP: <IP アドレス | IPv6 アドレス >, MAC: <MAC アドレス >, < インタフェース ID>, VID: <VLAN ID>)	Informational	
	ホストによる認証失敗	Web-Authentication host login fail (Username: < 文字列 >, IP: <IP アドレス | IPv6 アドレス >, MAC: <MAC アドレス >, < インタフェース ID>, VID: <VLAN ID>).	Critical	
	機器の最大認証ユーザ数の到達	Web-Authentication enters stop learning state.	Warning	
	機器の最大認証ユーザ数到達からの回復	Web-Authentication recovers from stop learning state.	Warning	

【付録 B】トラップログ

本製品では、以下のトラップログが検出されます。

トラップ名	説明	OID
802.1X		
dDot1xExtLoggedSuccess	802.1X クライアントが認証を通過すると、トラップが送信されます。 関連オブジェクト : (1) ifIndex (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan (4) dnaSessionAuthUserName	1.3.6.1.4.1.171.14.30.0.1
dDot1xExtLoggedFail	802.1X クライアントが認証エラーになると、トラップが送信されます。 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
認証失敗		
authenticationFailure	管理者である SNMPv2 エンティティが正しく認証されなかった旨プロトコルメッセージを受信すると、送信されます。 SNMPv2 関連はすべて本トラップを送信可能です。「snmpEnableAuthenTraps」オブジェクトは本トラップが実行されたことを意味します。	1.3.6.1.6.3.1.1.5.5
BPDU 攻撃防御		
dBpduProtectionAttackOccur	インタフェース上でＢＰＤＵアタックが発生すると送信されます。 関連オブジェクト : (1) ifIndex (2) dBpduProtectionIfCfgMode	1.3.6.1.4.1.171.14.47.0.1
dBpduProtectionAttackRecover	インタフェース上のＢＰＤＵアタックから回復すると送信されます。 関連オブジェクト : (1) ifIndex	1.3.6.1.4.1.171.14.47.0.2
DDM		
dDdmAlarmTrap	異常なアラーム状況の発生やアラーム状況からの回復時に送信されます。 関連オブジェクト : (1) dDdmNotifyInfoIfIndex (2) dDdmNotifyInfoComponent (3) dDdmNotifyInfoAbnormalLevel (4) dDdmNotifyInfoThresholdExceedOrRecover	1.3.6.1.4.1.171.14.72.0.1
dDdmWarningTrap	異常な警告状況の発生や警告状況からの回復時に送信されます。 関連オブジェクト : (1) dDdmNotifyInfoIfIndex, (2) dDdmNotifyInfoComponent (3) dDdmNotifyInfoAbnormalLevel (4) dDdmNotifyInfoThresholdExceedOrRecover	1.3.6.1.4.1.171.14.72.0.2
DHCP Server Screen Prevention		
dDhcpFilterAttackDetected	DHCP サーバスクリーニング有効時に偽のＤＨＣＰサーバパケットを受信するとほかの攻撃的パケット受信時と同様にトラップを送信します。 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

トラップ名	説明	OID
DoS		
dDosPreveAttackDetectedPacket	DoS 攻撃検出時に送信されます。 関連オブジェクト： (1) dDoSPrevCtrlAttackType (2) dDosPrevNotiInfoDropIpAddr (3) dDosPrevNotiInfoDropPortNumber	1.3.6.1.4.1.171.14.59.0.2
ErrDisable		
dErrDisNotifyPortDisabledAssert	ポートがエラー無効状態になった時に送信されます。 関連オブジェクト： (1) dErrDisNotifyInfoPortIfIndex (2) dErrDisNotifyInfoReasonID	1.3.6.1.4.1.171.14.45.0.1
dErrDisNotifyPortDisabledClear	時間をおいてポートループが再開した時送信されます。 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		
dGenMgmtLoginFail	ユーザがログインに失敗した時送信されます。 関連オブジェクト： (1) dGenMgmtNotifyInfoLoginType (2) dGenMgmtNotifyInfoUserName	1.3.6.1.4.1.171.14.165.0.1
Gratuitous ARP Function		
agentGratuitousARPTrap	IP アドレスの競合があった時に送信されます。 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		
dImpbViolationTrap	「IP-MAC ポートバインディングアドレス」侵害が起きた時に通知が送信されます。 関連オブジェクト： (1) ifIndex (2) dImpbViolationIpAddrType (3) dImpbViolationIpAddress (4) dImpbViolationMacAddress	1.3.6.1.4.1.171.14.22.0.1
LACP		
linkUp	管理者ロールである SNMP エンティティが「ifOperStatus」オブジェクトのリンクアップを検出した時に送信されます。 関連オブジェクト： (1) ifIndex, (2) if AdminStatus (3) ifOperStatu	1.3.6.1.6.3.1.1.5.4
linkDown	管理者ロールである SNMP エンティティが「ifOperStatus」オブジェクトのリンクダウンを検出した時に送信されます。 関連オブジェクト： (1) ifIndex, (2) if AdminStatus (3) ifOperStatu	1.3.6.1.6.3.1.1.5.3
LBD		
dLbdLoopOccurred	インタフェースループ発生時に送信されます。 関連オブジェクト： (1) dLbdNotifyInfoIfIndex	1.3.6.1.4.1.171.14.46.0.1
dLbdLoopRestart	インタフェースループが時間をおいて再開した時に送信されます。 関連オブジェクト： (1) dLbdNotifyInfoIfIndex	1.3.6.1.4.1.171.14.46.0.2
dLbdVlanLoopOccurred	VID ループがインタフェース上で発生した時に送信されます。 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
dLbdVlanLoopRestart	VID ループがインタフェース上で時間をおいて再開した時に送信されます。 関連オブジェクト： (1) dLbdNotifyInfoIfIndex (2) dLbdNotifyInfoVlanId	1.3.6.1.4.1.171.14.46.0.4
LLDP		
lldpRemTablesChange	「lldpStatsRemTableLastChangeTime」の値が変更されたときに送信されます。NMS により LLDP リモートシステムテーブルメンテナンスポールのトリガとして使用されます。 関連オブジェクト： (1) lldpStatsRemTablesInserts (2) lldpStatsRemTablesDeletes (3) lldpStatsRemTablesDrops (4) lldpStatsRemTablesAgeouts	1.0.8802.1.1.2.0.0.1
lldpXMedTopologyChangeDetected	新しいリモートポートがローカルに付属された、またはリモート機器がポート切断かポート移動したなどのトポロジの変更をローカル機器が検出した時に送信されます。 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 アクセスコントロール		
dMacAuthLoggedSuccess	ＭＡＣアクセスコントロールホストがログイン成功した時に送信されます。 関連オブジェクト： (1) ifIndex, (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan	1.3.6.1.4.1.171.14.153.0.1
dMacAuthLoggedFail	ＭＡＣアクセスコントロールホストがログインに失敗した時に送信されます。 関連オブジェクト： (1) ifIndex, (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan	1.3.6.1.4.1.171.14.153.0.2
dMacAuthLoggedAgesOut	ＭＡＣアクセスコントロールホストがエージアウトした時に送信されます。 関連オブジェクト： (1) ifIndex, (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan	1.3.6.1.4.1.171.14.153.0.3
MAC 通知		
dL2FdbMacNotificatio	アドレステーブルのＭＡＣアドレスが変更されたときに送信されます。 関連オブジェクト： (1) dL2FdbMacChangeNotifyInfo	1.3.6.1.4.1.171.14.3.0.1
MSTP		
newRoot	送信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時に送信されます。新しいルートが決まり次第ブリッジによって送信されます。トポロジ変更タイマの期限切れに伴い、後続の決定後すぐに送信されます。	1.3.6.1.2.1.17.0.1
topologyChange	設定ポートがラーニング状態からフォワーディング状態へ変更した場合、またはフォワーディング状態からブロック状態に変更した場合にブリッジによって送信されます。「newRoot」トラップが同じ変更に伴い送信される場合、本トラップは送信されません。	1.3.6.1.2.1.17.0.2
周辺機器		
dEntityExtPowerStatusChg	電力状態が変更しました。 関連オブジェクト： (1) dEntityExtEnvPowerUnitId (2) dEntityExtEnvPowerIndex (3) dEntityExtEnvPowerStatus	1.3.6.1.4.1.171.14.5.0.3

トラップ名	説明	OID
dEntityExtFanStatusChg	ファンの状態が変更しました。 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
dEntityExtThermalStatusChg	温度が変更しました。 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
dEntityExtFactoryResetButton	ファクトリリセットボタンが押下されました。 関連オブジェクト： (1) dEntityExtUnitIndex	1.3.6.1.4.1.171.14.5.0.5
PoE		
pethMainPowerUsageOnNotification	PSE しきい値が設定され使用電力がしきい値を超えた場合に送信されます。同じオブジェクトインスタンスの通知が送信されてから最小 500 ミリ秒経過している必要があります。 関連オブジェクト： (1) pethMainPseConsumptionPower	1.3.6.1.2.1.105.0.2
pethMainPowerUsageOffNotification	PSE しきい値が設定されず、使用電力がしきい値を超えていない場合に送信されます。同じオブジェクトインスタンスの通知が送信されてから最小 500 ミリ秒経過している必要があります。 関連オブジェクト： (1) pethMainPseConsumptionPower	1.3.6.1.2.1.105.0.3
dPoeIfPowerDeniedNotification	PSE 状態のダイアグラムが「POWER_DENIED」になった時送信されます。同じオブジェクトインスタンスの通知が送信されてから最小 500 ミリ秒経過している必要があります。 関連オブジェクト： (1) pethPsePortPowerDeniedCounter	1.3.6.1.4.1.171.14.24.0.1
dPoeIfPowerOverLoadNotification	PSE 状態のダイアグラムが「ERROR_DELAY_OVER」になった時送信されます。同じオブジェクトインスタンスの通知が送信されてから最小 500 ミリ秒経過している必要があります。 関連オブジェクト： (1) pethPsePortOverLoadCounter	1.3.6.1.4.1.171.14.24.0.2
dPoeIfPowerShortCircuitNotification	PSE 状態のダイアグラムが「ERROR_DELAY_SHORT」になった時送信されます。同じオブジェクトインスタンスの通知が送信されてから最小 500 ミリ秒経過している必要があります。 関連オブジェクト： (1) pethPsePortShortCounter	1.3.6.1.4.1.171.14.24.0.3
dPoeIfPdAliveFailOccurNotification	PD 機器が停止、または返答がない状態です。同じオブジェクトインスタンスの通知が送信されてから最小 500 ミリ秒経過している必要があります。 関連オブジェクト： (1) pethMainPseGroupIndex (2) pethPsePortIndex (3) dPoeIfPdAliveCfgPdIpType (4) dPoeIfPdAliveCfgPdIpAddr	1.3.6.1.4.1.171.14.24.0.4
ポート		
linkUp	ポートリンクアップ時の通知 関連オブジェクト： (1) ifIndex (2) if AdminStatus (3) ifOperStatu	1.3.6.1.6.3.1.1.5.4
linkDown	ポートリンクダウン時の通知 関連オブジェクト： (1) ifIndex (2) if AdminStatus (3) ifOperStatu	1.3.6.1.6.3.1.1.5.3

トラップ名	説明	OID
ポートセキュリティ		
dPortSecMacAddrViolation	ポートセキュリティトラップが有効時に、事前に設定したポートセキュリティ設定を侵害している新しい MAC アドレスがトリガとなり送信。 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		
risingAlarm	アラームエントリが上限しきい値を超えた場合、SNMP トラップの送信。 関連オブジェクト : (1)alarmIndex (2)alarmVariable (3)alarmSampleType (4) alarmValue (5) alarmRisingThreshold	1.3.6.1.2.1.16.0.1
fallingAlarm	アラームエントリが下限しきい値を超えた場合、SNMP トラップの送信。 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
セーフガード		
dSafeguardChgToExhausted	システムが「exhaust（消耗）」モードから「normal（通常）」モードへ移行した時の通知。 関連オブジェクト : (1) dSafeguardEngineCurrentMode	1.3.6.1.4.1.171.14.19.1.1.0.1
dSafeguardChgToNormal	システムが「normal（通常）」モードから「exhaust（消耗）」モードへ移行した時の通知。 関連オブジェクト : (1) dSafeguardEngineCurrentMode	1.3.6.1.4.1.171.14.19.1.1.0.2
スタック		
dStackInsertNotification	ユニットホットインサート通知 関連オブジェクト : (1) dStackNotifyInfoBoxId (2) dStackInfoMacAddr	1.3.6.1.4.1.171.14.9.0.1
dStackRemoveNotification	ユニットホットリムーブ通知 関連オブジェクト : (1) dStackNotifyInfoBoxId (2) dStackInfoMacAddr	1.3.6.1.4.1.171.14.9.0.2
dStackFailureNotification	ユニット失敗通知 関連オブジェクト : (1) dStackNotifyInfoBoxId	1.3.6.1.4.1.171.14.9.0.3
dStackTPChangeNotification	スタックトポロジ変更通知 関連オブジェクト : (1) dStackNotifyInfoTopologyType (2) dStackNotifyInfoBoxId (3) dStackInfoMacAddr	1.3.6.1.4.1.171.14.9.0.4
dStackRoleChangeNotification	スタックユニット変更通知 関連オブジェクト : (1) dStackNotifyInfoRoleChangeType (2) dStackNotifyInfoBoxId	1.3.6.1.4.1.171.14.9.0.5
SIM		
swSingleIPMSColdStart	メンバのコールドスタート時にコマンダスイッチによる通知 関連オブジェクト : (1) swSingleIPMSID (2) swSingleIPMSMacAddr	1.3.6.1.4.1.171.12.8.6.0.11

トラップ名	説明	OID
swSingleIPMSWarmStart	メンバのウォームスタート時にコマンダスイッチによる通知 関連オブジェクト : (1) swSingleIPMSID (2) swSingleIPMSMacAddr	1.3.6.1.4.1.171.12.8.6.0.12
swSingleIPMSLinkDown	メンバのリンクダウン時にコマンダスイッチによる通知 関連オブジェクト : (1) swSingleIPMSID (2) swSingleIPMSMacAddr (3) ifIndex	1.3.6.1.4.1.171.12.8.6.0.13
swSingleIPMSLinkUp	メンバのリンクアップ時にコマンダスイッチによる通知 関連オブジェクト : (1) swSingleIPMSID (2) swSingleIPMSMacAddr (3) ifIndex	1.3.6.1.4.1.171.12.8.6.0.14
swSingleIPMSAuthFail	メンバの認証失敗時にコマンダスイッチによる通知 関連オブジェクト : (1) swSingleIPMSID (2) swSingleIPMSMacAddr	1.3.6.1.4.1.171.12.8.6.0.15
swSingleIPMSnewRoot	メンバの新ルート時にコマンダスイッチによる通知 関連オブジェクト : (1) swSingleIPMSID (2) swSingleIPMSMacAddr	1.3.6.1.4.1.171.12.8.6.0.16
swSingleIPMSTopologyChange	メンバのトポロジ変更時にコマンダスイッチによる通知 関連オブジェクト : (1) swSingleIPMSID (2) swSingleIPMSMacAddr	1.3.6.1.4.1.171.12.8.6.0.17
スタート		
coldStart	代理人としての SNMPv2 エンティティが再初期化され設定変更時の通知	1.3.6.1.6.3.1.1.5.1
warmStart	代理人としての SNMPv2 エンティティが再初期化され設定変更されない時の通知	1.3.6.1.6.3.1.1.5.2
ストームコントロール		
dStormCtrlOccurred	「dStormCtrlNotifyEnable」が 'stormOccurred' または 'both' のどちらかでストームが発生している時の通知 関連オブジェクト : (1) ifIndex, (2) dStormCtrlNotifyTrafficType	1.3.6.1.4.1.171.14.25.0.1
dStormCtrlStormCleared	「dStormCtrlNotifyEnable」が 'stormCleared' または 'both' のどちらかでストームが解消した時の通知 関連オブジェクト : (1) ifIndex, (2) dStormCtrlNotifyTrafficType	1.3.6.1.4.1.171.14.25.0.2
システムファイル		
dsfUploadImage	ユーザによるイメージファイルアップロード成功時の通知	1.3.6.1.4.1.171.14.14.0.1
dsfDownloadImage	ユーザによるイメージファイルダウンロード成功時の通知	1.3.6.1.4.1.171.14.14.0.2
dsfUploadCfg	ユーザによるコンフィグレーションファイルアップロード成功時の通知	1.3.6.1.4.1.171.14.14.0.3
dsfDownloadCfg	ユーザによるコンフィグレーションファイルダウンロード成功時の通知	1.3.6.1.4.1.171.14.14.0.4
dsfSaveCfg	ユーザによるコンフィグレーションファイル保存成功時の通知	1.3.6.1.4.1.171.14.14.0.5

トラップ名	説明	OID
Web 認証		
dWebAuthLoggedSuccess	ホストによるログイン成功時（Web 認証）の通知 関連オブジェクト : (1) ifIndex (2) dnaSessionAuthVlan (3) dnaSessionClientMacAddress (4) dnaSessionClientAddrType (5) dnaSessionClientAddress (6) dnaSessionAuthUserName	1.3.6.1.4.1.171.14.154.0.1
dWebAuthLoggedFail	ホストによるログイン失敗時（Web 認証）の通知 関連オブジェクト : (1) ifIndex (2) dnaSessionAuthVlan (3) dnaSessionClientMacAddress (4) dnaSessionClientAddrType (5) dnaSessionClientAddress (6) dnaSessionAuthUserName	1.3.6.1.4.1.171.14.154.0.2

【付録 C】RADIUS 属性の割り当て指定

DGS-1510 における RADIUS 属性の割り当ては、以下のモジュールで使用されます。
- Console
- Telnet
- SSH
- Web
- 802.1X（ポートベースとホストベース）
- MAC ベースのアクセスコントロール
- Web ベースアクセスコントロール（WAC）
- Japanese Web ベースアクセスコントロール（JWAC）

以下の RADIUS 属性割り当てタイプについて説明します。
- Privilege Level（権限レベル）
- Ingress/Egress 帯域
- 802.1p デフォルトプライオリティ
- VLAN
- ACL

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。以下の表では帯域幅のパラメータを示しています。

ベンダー指定の属性の項目は以下の通りです。

ベンダー指定の属性	説明	値	摘要
ベンダー ID	ベンダーを定義します。	171（DLINK）	必須
ベンダータイプ	本属性の定義	1	必須
属性指定フィールド	権限レベルを割り当てるために使用します。	権限レベル (1-15)	必須

RADIUS サーバの権限レベル幅属性（例 : 権限レベル 15）を設定し、Console、Telnet、SSH、Web 認証に成功すると、RADIUS サーバに従ってデバイスは正しい権限レベルをユーザに割り当てます。しかし、権限レベル幅属性を設定せずに認証に成功しても、デバイスは権限レベルをユーザに割り当てません。権限レベルに有効権限レベル幅より大きいまたは小さい数値を設定した場合、その権限レベルは無視されます。

RADIUS サーバで Ingress/Egress 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。以下の表では帯域幅のパラメータを示しています。

ベンダー指定の属性の項目は以下の通りです。

ベンダー指定の属性	説明	値	摘要
ベンダー ID	ベンダーを定義します。	171（DLINK）	必須
ベンダータイプ	本属性の定義	2（イングレス帯域用） 3（イーグレス帯域用）	必須
属性指定フィールド	ポートの帯域を割り当てるために使用します。	単位（Kbits）	必須

RADIUS サーバの帯域幅属性（例 : イングレス帯域幅 1000Kbps）を設定し、802.1X 認証に成功すると、RADIUS サーバに従ってデバイスは正しい帯域幅をポートに割り当てます。しかし、帯域幅属性を設定せずに認証に成功しても、デバイスは帯域幅をポートに割り当てません。帯域幅属性に 0 またはポートの有効帯域幅（イーサネットポートでは 100Mbps またはギガビットポートでは 1Gbps）より大きい数値を設定する場合、no_limit を指定します。

RADIUS サーバで 802.1p デフォルトプライオリティを割り当てるためには、適切な項目を RADIUS サーバに設定する必要があります。

ベンダー指定の属性の項目は以下の通りです。

ベンダー指定の属性	説明	値	摘要
ベンダー ID	ベンダーを定義します。	171（DLINK）	必須
ベンダータイプ	本属性の定義	4	必須
属性指定フィールド	ポートの 802.1p デフォルトプライオリティを割り当てるために使用します。	0-7	必須

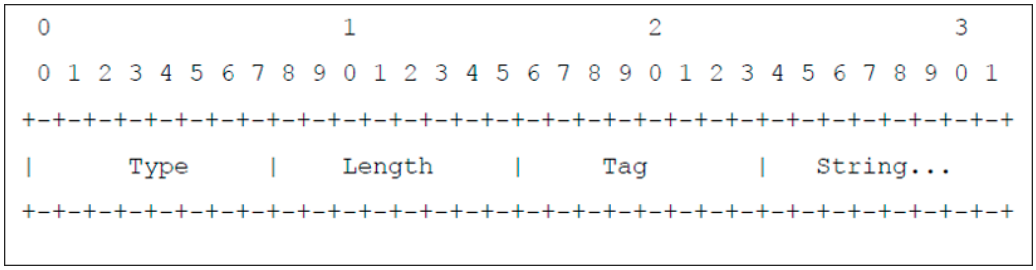
RADIUS サーバの 802.1p プライオリティ属性（例 : プライオリティ 7）を設定し、802.1X またはホストベース認証に成功すると、RADIUS サーバに従ってデバイスは 802.1p デフォルトプライオリティをポートに割り当てます。しかし、プライオリティ属性を設定せずに認証に成功しても、デバイスはプライオリティをポートに割り当てません。RADIUS サーバに設定されたプライオリティ属性が範囲外（7 より大きい）であると、そのデバイス

には設定されません。
RADIUS サーバで VLAN 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 の割り当てを使用するために、RFC3580 では RADIUS パケットに以下のトンネル属性を定義しています。

以下の表では VLAN の項目を示しています。

RADIUS トンネル属性	説明	値	摘要
トンネルタイプ	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。	文字列（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	備考
0x01	VLAN 名 (ASCII)	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。
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。	

RADIUS サーバの VLAN 属性 (例 : VID 3) を設定し、802.1X または MAC ベースアクセスコントロール認証に成功すると、ポートは VLAN 3 に追加されます。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。

RADIUS サーバが ACL を割り当てるためには、適切な項目を RADIUS サーバに設定する必要があります。以下の表では ACL の項目を示しています。RADIUS ACL の割り当ては、MAC ベースアクセスコントロールにて使用されるだけです。

■ VSA14 ACL スクリプト

ベンダー指定の属性の項目は以下の通りです。

RADIUS トンネル属性	説明	値	摘要
ベンダー ID	ベンダーを定義します。	171 (DLINK)	必須
ベンダータイプ	属性を定義します。	14（ACL スクリプト用）	必須
属性指定フィールド	ACL スクリプトを割り当てるために使用されます。フォーマットは ACL コマンドを基本とします。	ACL スクリプト 例 : `ip access-list a1;permit host 10.90.90.100;exit; mac access-list extended m1;permit host 00-00-00-01-90-10 any; exit;`	必須

RADIUS サーバの ACL 属性（例 : ACL プロファイル :「`create access_profile ethernet vlan 0xFFF profile_id 100`」、ACL ルール :「`config access_profile profile_id 100 add access_id auto_assign ethernet`」）を設定し、MAC ベースアクセスコントロール認証に成功すると、RADIUS サーバに従ってデバイスは ACL プロファイルとルールを割り当てます。ACL モジュールに関する詳しい情報については、「DGS-1510 CLI マニュアル」の「アクセスコントロールリスト（ACL）コマンド」を参照してください。

■ **NAS-Filter-Rule（92）**

NAS-Filter-Rule の定義は次の通りです。

RADIUS トンネル属性	説明	値	摘要
NAS-Filter-Rule	ユーザに割り当てるフィルタルールです。	文字列（個々のフィルタルールを含み、NULL (0x00) オクテットで区切られます。）	必須

フィルタルールのフォーマットに関する CLI コマンドについては、CLI マニュアルを参照してください。

ベンダー指定の属性の項目は以下の通りです。

RADIUS トンネル属性	説明	値	摘要
ベンダー ID	ベンダーを定義します。	171（DLINK）	必須
ベンダータイプ	属性を定義します。	14（ACL スクリプト用）	必須
属性指定フィールド	IPv6 フィルタルール。IPv6 関連の入力を受信するために使用されます。	NAS-Filter-Rule について以下のいずれかの IP モードを示します。 1=IPv4 及び IPv6 トラフィックを転送 2=IPv4 のみのトラフィックを転送（IPv6 トラフィックは破棄） この属性が RADIUS サーバによって割り当てられていない場合、IPv4 のみのトラフィックを転送し、IPv6 トラフィックは破棄されます。	必須

注意 固有 ACL スクリプト（VSA14）と標準の NAS-Filter-Rule（92）が同時に割り当てられた場合、NAS-Filter-Rule（92）が適用され、VSA14 は無視されます。

【付録 D】IETF RADIUS 属性のサポート

RADIUS（Remote Authentication Dial-In User Service）属性は要求と応答用に特定の認証、許可、情報、および構成の詳細を運びます。この付録では現在スイッチがサポートする RADIUS 属性を示します。RADIUS 属性は IETF 標準と VSA（Vendor-Specific Attribute : ベンダー固有属性）によってサポートされています。

VSA ではベンダーが独自の RADIUS 属性を追加作成することを許可します。D-Link VSA に関する詳しい情報については、「RADIUS 属性の割り当て」を参照してください。

IETF 標準の RADIUS 属性は RFC 2865 Remote Authentication Dial-In User Service (RADIUS)、RFC 2866 RADIUS Accounting, RFC 2868 RADIUS Attributes for Tunnel Protocol Support、および RFC 2869 RADIUS Extensions で定義されています。

以下の表は D-Link スイッチがサポートする IETF RADIUS 属性を示しています。

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

2. RADIUS アカウンティング属性

番号	IETF 属性
1	User-Name
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
8	Framed-IP-Address
31	Calling-Station-ID
32	NAS-Identifier
40	Acct-Status-Type
41	Acct-Delay-Time
42	Acct-Input-Octets
43	Acct-Output-Octets
44	Acct-Session-ID
45	Acct-Authentic
46	Acct-Session-Time
47	Acct-Input-Packets
48	Acct-Output-Packets
49	Acct-Terminate-Cause
52	Acct-Input-Gigawords
53	Acct-Output-Gigawords
61	NAS-Port-Type
95	NAS-IPv6-Address

【付録 E】ERPS 情報

イーサネットリングプロテクション（ERPS）のポート毎における「ハードウェア / ソフトウェアベース」情報を表示します。
「ハードウェアベース ERPS」(external PHY) のみ 50ms のリカバリタイムでの「fast link drop interrupt」（ファーストリンクドロップ防止）機能をサポートしています。

ERPS「ハードウェア / ソフトウェアベース」情報

機種	ERPS タイプ
DGS-1510-20	ソフトウェアベース ERPS：ポート 1 ～ 20（全ポート）
DGS-1510-28P DGS-1510-28X DGS-1510-28XMP	ハードウェアベース ERPS：ポート 1 ～ 8 ソフトウェアベース ERPS：ポート 9 ～ 28
DGS-1510-52X（H/W:A1） （品番：DGS-1510-52X）	ハードウェアベース ERPS：ポート 1 ～ 8、ポート 25 ～ 32、ポート 49、50 ソフトウェアベース ERPS：ポート 9 ～ 24、ポート 33 ～ 48、ポート 51、52
DGS-1510-52X（H/W:A2A3） （品番：DGS-1510-52X/A2、 DGS-1510-52X/A3）	ハードウェアベース ERPS：ポート 17 ～ 24、ポート 41 ～ 48 ソフトウェアベース ERPS：ポート 1 ～ 16、ポート 25 ～ 40、ポート 49 ～ 52

【付録 F】ケーブルとコネクタ

スイッチを別のスイッチ、ブリッジまたはハブに接続する場合、ノーマルケーブルが必要です。ケーブルピンアサインに合うことを再確認してください。
以下の図と表は標準の RJ-45 プラグ / コネクタとピンアサインです。

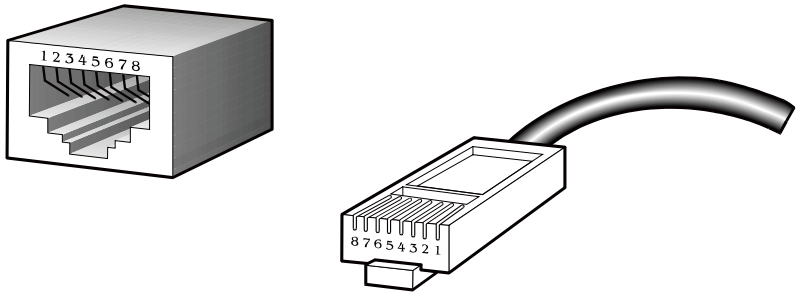


図 F-1　標準的な RJ-45 プラグとコネクタ

表 F-1　標準的な RJ-45 ピンアサイン

RJ-45 ピンアサイン		
コンタクト（ピン番号）	MDI-X 信号	MDI-II 信号
1	RD+（受信）	TD+（送信）
2	RD-（受信）	TD-（送信）
3	TD+（送信）	RD+（受信）
4	未使用	未使用
5	未使用	未使用
6	TD-（送信）	RD-（受信）
7	未使用	未使用
8	未使用	未使用

【付録 G】ケーブル長

以下の表は各規格に対応するケーブル長（最大）です。

規格	メディアタイプ	最大伝送距離
SFP	1000BASE-LX、シングルモードファイバモジュール 1000BASE-SX、マルチモードファイバモジュール 1000BASE-LH、シングルモードファイバモジュール 1000BASE-ZX、シングルモードファイバモジュール	10 km 550 m 40 km 80 km
1000BASE-T	エンハンスドカテゴリ 5 UTP ケーブル カテゴリ 5 UTP ケーブル（1000 Mbps）	100 m
100BASE-TX	カテゴリ 5 UTP ケーブル（100 Mbps）	100 m
10BASE-T	カテゴリ 3 UTP ケーブル（10 Mbps）	100 m

【付録 H】用語解説

用語	説明
1000BASE-LX	最大伝送速度 1Gbps の Gigabit Ethernet の規格のひとつ。長い光波長で長距離伝送用に使用されます。伝送距離（最大）はシングルモード光ファイバを使用した場合で 10km。
1000BASE-SX	最大伝送速度 1Gbps の Gigabit Ethernet の規格のひとつ。短い光波長でマルチモード光ファイバを使用した場合伝送距離（最大）は 550m。
100BASE-FX	光ファイバを使用する最大伝送速度 100Mbps の Fast Ethernet の規格のひとつ。
100BASE-TX	カテゴリ 5 以上の UTP ケーブルを使用する最大伝送速度 100Mbps の Fast Ethernet の規格のひとつ。
10BASE-T	IEEE 802.3 準拠でカテゴリ 3 以上の UTP ケーブルを使用する最大伝送速度 10Mbps の Ethernet の規格のひとつ。
エージング	タイムアウトし、無効のスイッチのダイナミックデータベースを自動的に消去します。
ATM	非同期転送モード。セルと呼ばれる固定長のセル（パケット）ベースで転送するプロトコル。ATM は音声、データおよびビデオ信号を含むユーザトラフィックの完全な列を転送するために開発されたものです。
オートネゴシエーション	スピード、デュプレックスおよびフローコントロールを自動的に認識する機能。オートネゴシエーションをサポートする端末と接続すると、リンクは自動的に最適なリンク条件に設定されます。
バックボーンポート	デバイスのアドレスを学習せず不明なアドレスを持つすべてのフレームを受信するポート。バックボーンポートは通常ご使用のネットワークのバックボーンにスイッチを接続するために使用されるポートです。バックボーンポートは以前はダウンリンクポートとして知られていました。
バックボーン	ネットワークセグメント間でトラフィックが転送される場合に優先パスとして使用されるネットワークの一部分。
帯域	1 秒あたりのビット数で計算される 1 チャンネルが転送できる情報量。イーサネットの帯域は 10Mbps、ファーストイーサネットは 100Mbps。
ボーレート	ラインのスイッチングスピード。ネットワークセグメント間のラインスピードとして知られています。
BOOTP	BOOTP プロトコルはデバイスが起動するたびに IP アドレスを MAC アドレスに自動マッピングします。さらにデバイスにサブネットマスク、デフォルトゲートウェイを割り当てます。
ブリッジ	たとえ高いレベルのプロトコルが関連してもローカルまたはリモートネットワークを相互接続するデバイス。ブリッジはネットワーク管理を中央に集めて 1 個の論理ネットワークを形成します。
ブロードキャスト	ネットワーク上のすべての終点デバイスに送信されるメッセージ。
ブロードキャストストーム	が主として可能なネットワーク帯域を奪い、ネットワークエラーを引き起こす Multiple simultaneous ブロードキャスト。
コンソールポート	端末またはモデムコネクタと接続可能なスイッチ上のポート。コンピュータ内でパラレル配列のデータをデータ転送リンクで使用されるシリアル形式に変換します。このポートはほとんどの場合ローカル管理のために使用されます。
CSMA/CD	イーサネットと IEEE 802.3 標準によって使用されるチャンネルアクセス方法で検索したデータチャンネルが一定期間後クリアされた後にだけデバイスに転送します。2 つのデバイスが同時に転送する場合、コリジョンが発生し、コリジョンを発生したデバイスは任意の時間再転送を遅らせます。
データセンタースイッチング	スイッチがサーバファームへの高パフォーマンスアクセス、高速バックボーン接続、およびネットワーク管理とセキュリティのためのコントロールポイントを提供するコーポレートネットワーク内のアグリゲーションポイント
イーサネット	Xerox、Intel および DEC が共同で開発した LAN 仕様。イーサネットネットワークは CSMA/CD を使用して 10Mbps で処理を行います。
ファーストイーサネット	Ethernet/CD ネットワークアクセス方法をベースにした 100Mbps 技術。
フローコントロール	(IEEE 802.3x) 端末に接続した転送ポートへのパケットを抑止します。受信バッファがあふれそうになった場合にパケットロスを防ぎます。
フォワーディング	中間のネットワークデバイスによりパケットを到達点に向けて送信するプロセス。
フルデュプレックス	同時にパケットの送受信を可能とし、スループットを 2 倍にするシステム。
ハーフデュプレックス	パケットの送受信を行うが、同時には行えないシステム。
IP アドレス	Internet Protocol アドレス。TCP/IP を使用するネットワークに付属するデバイスの固有な識別子。IPv4 アドレスは 8 ビットずつピリオドで区切られ、ネットワークセクション、サブネットセクション、ホストセクションで構成されます。
IPX（Internetwork Packet Exchange）	ネットワーク通信で使用するプロトコル。
LAN – ローカルエリアネットワーク	通常フロアもしくはビルのような規模の小さいエリアで PC、プリンタ、サーバのようなコンピュータリソースを接続するネットワーク。高速で低エラー率が特長です。
レイテンシ	デバイスがパケットを受信する時間とパケットが到達点ポートに転送される時間の遅延。
ラインスピード	ボーレートを参照。
メインポート	通常の操作条件でデータトラフィックを送信する Resilient リンク内のポート。

用語	説明
MDI （Medium Dependent Interface）	1 つのデバイスの送信装置が別のデバイスの受信装置に接続するイーサネットポート接続。
MDI-X （Medium Dependent Interface Cross-over）	接続送受信のラインが交差しているイーサネットポート接続。
MIB（Management Information Base）	デバイスの管理特性とパラメータを保持します。MIB は SNMP で使用され、管理システムの属性を持っています。スイッチは自身の内部 MIB を持っています。
マルチキャスト	シングルパケットはネットワークアドレスの特定のサブセットにコピーします。これらのアドレスはパケットの到達点アドレス内に記述されます。
プロトコル	ネットワーク上のデバイス間通信のルール。ルールは形式、タイミング、配列およびエラー制御を定義しています。
Resilient link	他のポートがエラーになった場合に一方のポートがデータ転送を引き継ぐように設定された 1 対のポート。
RJ-45	10BASE-T や 100BASE-TX などで使用する標準 8 線コネクタ
RMON	リモート監視。SNMP MIB II のサブセットはアドレッシングによって異なる最大 10 個のグループまでのモニタリングや管理を可能にします。
RPS （リダンダント電源システム）	スイッチに接続されて、バックアップ電源を供給するデバイス。
サーバファーム	大量のユーザにサービスを提供する中央に位置するサーバグループ。
SLIP （Serial Line Internet Protocol）	IP がシリアルライン接続を経由して動作することが可能なプロトコル。
SNMP （Simple Network Management Protocol）	当初は TCP/IP インターネットを管理するために開発されたプロトコル。SNMP は現在広範囲のコンピュータとネットワークの装置で実行され、多くのネットワークおよび端末操作の状況を管理するために使用されます。
スパニングツリープロトコル (STP)	ネットワーク上のフォールトトレランスを提供するブリッジベースのシステム。STP はネットワークトラフィックに対してパラレルパスを実行し、メインのパスにエラーが発生してもメインのパスが操作できる場合はリダンダントパスを無効にすることを保証します。
スタック	1 個の論理的なデバイスの形をとするために統合されたネットワークデバイスのグループ。
スタンバイポート	リンクしているメインポートにエラーが発生すると、Resilient リンク内のスタンバイポートはデータ転送を受け継ぎます。
スイッチ	パケットの終点アドレスを元にパケットのフィルタ、フォワードするデバイス。スイッチは各スイッチポートで関連するアドレスを学習し、この情報を元に表を作成してスイッチの決定に使用します。
TCP/IP	Telnet 端末エミュレーション、FTP ファイル転送などコンピュータ装置の広い範囲で通信サービスを提供する通信プロトコルです。
telnet	仮想端末サービスを提供する TCP/IP アプリケーションプロトコルで、ユーザが別のコンピュータシステムにログインし、ユーザが直接ホストに接続しているようにホストにアクセスすることができます。
TFTP （Trivial File Transfer Protocol）	スイッチのローカルの管理能力を使用してリモートデバイスからファイルを転送する（ソフトウェアアップグレードなど）ことができます。
UDP（User Datagram Protocol）	インターネットの標準プロトコルで、あるデバイスのアプリケーションプログラムがデータを別のデバイス上のアプリケーションプログラムに送信することができます。
VLAN（Virtual LAN）	物理的に接続した LAN のように通信する位置やトポロジが独立しているデバイスのグループ。
VLT（Virtual LAN Trunk）	各スイッチ上のすべての VLAN トラフィックを転送するスイッチ間のリンク。
VT100	ASCII コードを使用するターミナルタイプ。 VT100 画面はテキストベースの表示をします。

【付録 I】機能設定例

本項では、一般によく使う機能についての設定例を記載します。実際に設定を行う際の参考にしてください。

- Traffic Segmentation（トラフィックセグメンテーション）
- VLAN
- Link Aggregation（リンクアグリゲーション）
- Access List（アクセスリスト）
- Loopback Detection（LBD）（ループ検知）

対象機器について

本コンフィグレーションサンプルは以下の製品に対して有効な設定となります。

- DGS-1510

Traffic Segmentation（トラフィックセグメンテーション）

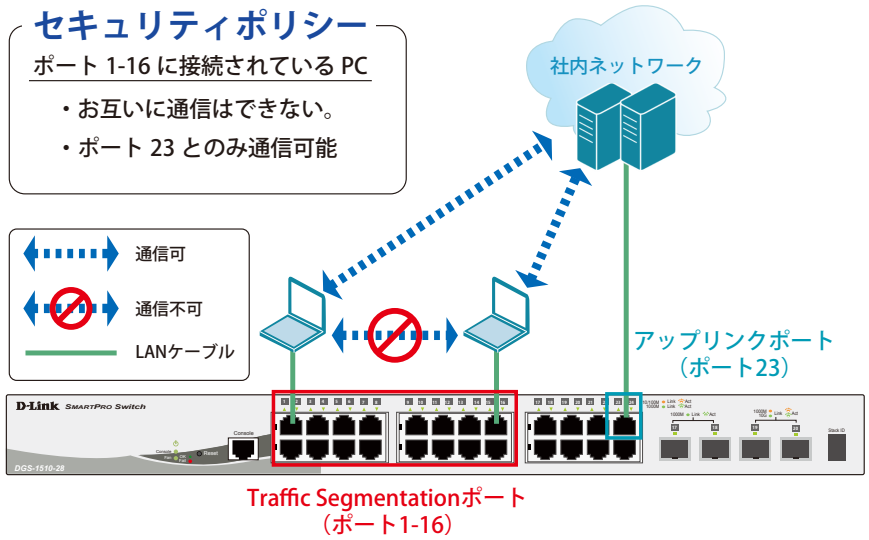


図 18-1　Traffic Segmentation（DGS-1510）

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 range ethernet 1/0/1-16 unicast
```

VLAN

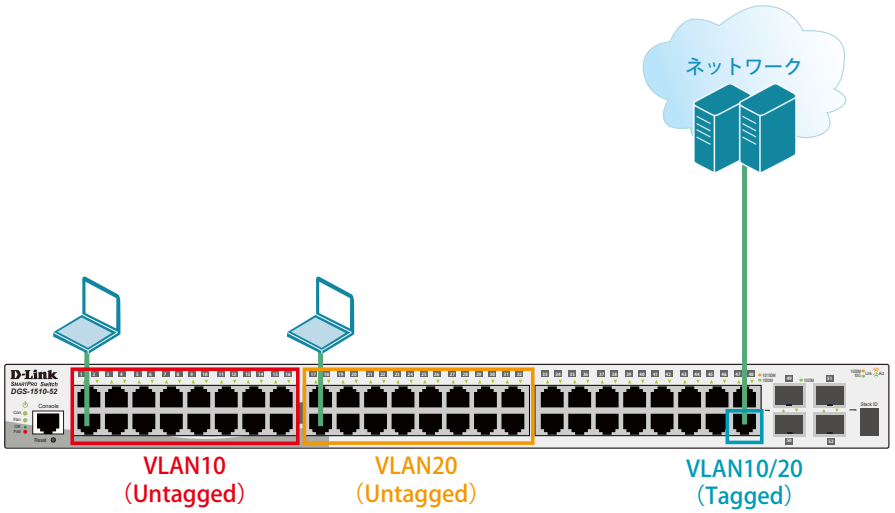


図 18-2　VLAN（DGS-1510）

概要

VLAN を設定します。ポート 1 ～ 16 に VLAN10 を「Untagged」で割り当て、ポート 17 ～ 32 に VLAN20 を「Untagged」で割り当て、ポート 48 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 1-16 に VLAN10、ポート 17-32 に VLAN20 を 割り当てます。

```
Switch#configure terminal
Switch(config)#interface range ethernet 1/0/1-16
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 1/0/17-32
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 48 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 1/0/48
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 1/0/48
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）

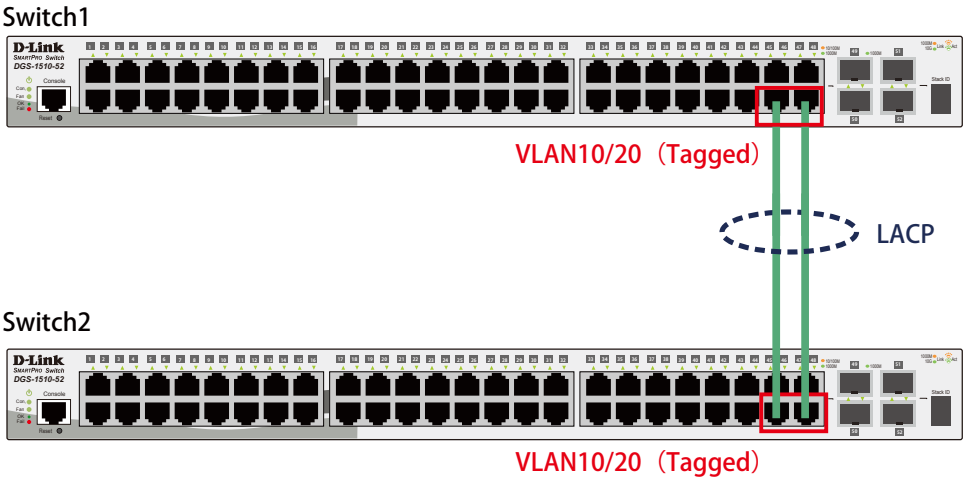


図 18-3　Link Aggregation（DGS-1510）

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 46 と 48 に VLAN10 と VLAN20 を「Tagged」で割り当て、ポート 46 と 48 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 1/0/46
Switch(config-if)#channel-group 1 mode active
Switch(config-if)#exit
Switch(config)#interface ethernet 1/0/48
Switch(config-if)#channel-group 1 mode active
Switch(config-if)#exit
```

3. Link Aggregation のポートを設定します。

```
Switch(config)#interface port-channel 1
```

4. 作成した port-channel に VLAN を設定します。
   LAG ポートに設定する VLAN は、各物理インターフェイス上では設定せず、Port-channel インターフェイス上で VLAN の設定を行います。

```
Switch(config)#interface port-channel 1
Switch(config if)#switchport mode trunk
Switch(config if)#switchport trunk native vlan 1
Switch(config if)#switchport trunk allowed vlan 1,10,20
Switch(config if)#exit
Switch(config)#exit
```

5. 設定を保存します。

```
Switch#copy running-config startup-config
```

6. 情報確認
   - Port-channel に設定されている VLAN 情報を表示します。

```
Switch#show vlan interface port-channel 1
```

   - グループ番号とグループで使用されている Protocol を表示します。

```
Switch#show channel-group
```

   - 各グループに所属している Port 番号と、リンクアグリゲーションの状態を表示します。

```
Switch#show channel-group channel 1 detail
```

Access List（アクセスリスト）

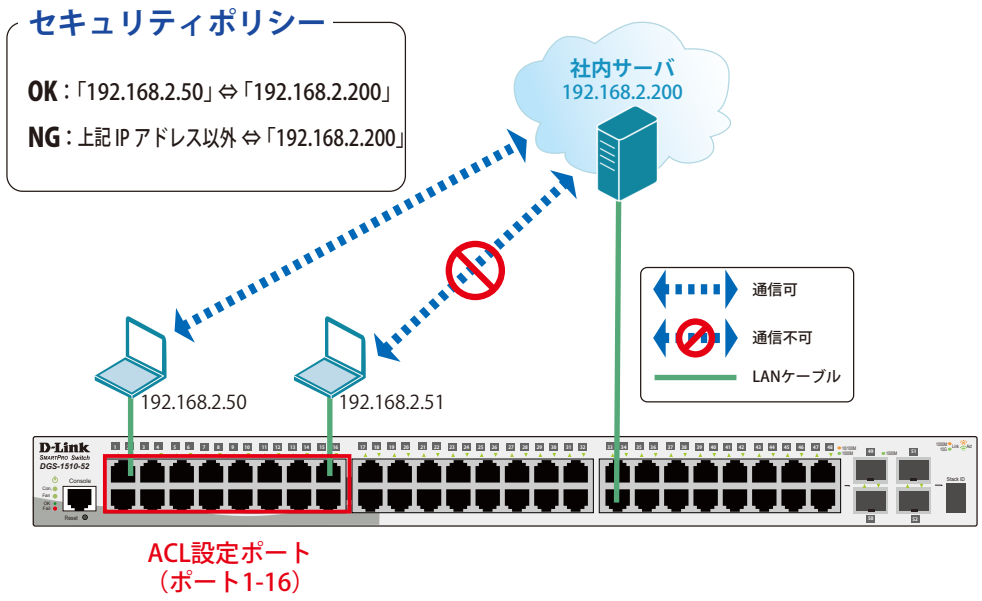


図 18-4　Access List（DGS-1510）

概要

ポート 1~16に対し、アクセスリストを設定します。ポート 1~16に接続される端末の IP の中から、「192.168.2.50」の端末から社内サーバ（192.168.2.200）へのアクセスは許可し、それ以外の端末から社内サーバへのアクセスは禁止するように設定します。

設定手順

1. アクセスリストに名前（extended ACL）を付けて定義します。
   「192.168.2.50 ⇔ 192.168.2.200」間の通信を許可するルールを追加します。
   「192.168.2.200」へのすべての通信を拒否するルールを追加します。

```
Switch#configure terminal
Switch(config)#ip access-list extended ACL
Switch(config-ip-ext-acl)#permit 192.168.2.50 0.0.0.0 192.168.2.200 0.0.0.0
Switch(config-ip-ext-acl)#deny any 192.168.2.200 0.0.0.0
Switch(config-ip-ext-acl)#end
```

2. アクセスリストのルールを、適用対象ポート 1 ～ 16 へ設定します。

```
Switch#configure terminal
Switch(config)#interface range ethernet 1/0/1-16
Switch(config-if-range)#ip access-group ACL in
Switch(config-if-range)#end
```

3. 設定を保存します。

```
Switch#copy running-config startup-config
```

4. 情報確認

```
Switch#show access-list
Switch#show access-list ip
Switch#show access-group
```

Loopback Detection（LBD）（ループ検知）

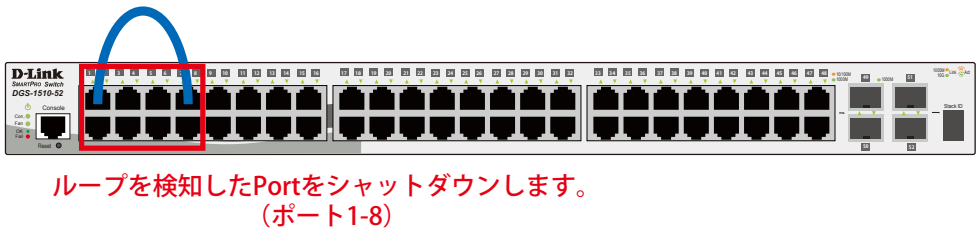


図 18-5　Loopback Detection（DGS-1510）

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、インターフェイスモードにて「no shutdown」コマンドを投入する必要があります。

4. ポート 1-8 でループバック検知機能を有効にします。

```
Switch(config)#interface range ethernet 1/0/1-8
Switch(config-if-range)#spanning-tree state disable
Switch(config-if-range)#loopback-detection
Switch(config-if-range)#end
```

注意 「spanning-tree」が「enable」になっている場合、ループ検知機能を設定できないため、設定するインターフェイスの「spanning-tree」の設定をまず「disable」にします。

注意 「spanning-tree」はデフォルトでグローバルでは「disable」に設定されていますが、各インターフェイス「enable」となっています。各インターフェイスにて「disable」設定が必要となります。

5. show コマンドで「Spanning Tree」が無効になっているかを確認します。

```
Switch#show spanning-tree configuration interface ethernet 1/0/1-8
```

6.「Spanning Tree」がポート単位で「disable」に設定されている場合、ステータスが Disabled と表示されます。

```
Spanning tree state : Disabled
```

7. 設定を保存します。

```
Switch#copy running-config startup-config
```

8. 情報確認

```
Switch#show loopback-detection
```

（ループ検知の有効 / 無効、設定しているモード、対象の VLAN、各ポートのループ状態等を表示します。）

```
Switch#show errdisable recovery
```

（ループ解消後の自動ポート解放設定 有効 / 無効、確認間隔を表示します。）