D-Link DES-3200 シリーズ

Layer2+ 10/100Mbps Metro Ethernet 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。

⚠警告	この表示を無視し、まちがった使いかたをすると、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、まちがった使いかたをすると、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。

⚠警告

分解禁止　分解・改造をしない
機器が故障したり、異物が混入すると、やけどや火災の原因となります。

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
故障の原因につながります。

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してください。

ぬれ手禁止　ぬれた手でさわらない
感電のおそれがあります。

水ぬれ禁止　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、または故障のおそれがあります。

禁止　油煙、湯気、湿気、ほこりの多い場所、振動の激しいところでは使わない
火災、感電、または故障のおそれがあります。

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、または故障のおそれがあります。

禁止　表示以外の電圧で使用しない
火災、感電、または故障のおそれがあります。

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。

禁止　設置、移動のときは電源プラグを抜く
火災、感電、または故障のおそれがあります。

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
感電のおそれがあります。

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、または故障につながります。

禁止　正しい電源ケーブル、コンセントを使用する
火災、感電、または故障の原因となります。

禁止　乳幼児の手の届く場所では使わない
やけど、ケガ、または感電の原因になります。

禁止　次のような場所では保管、使用をしない
・直射日光のあたる場所
・高温になる場所
・動作環境範囲外

禁止　光源をのぞかない
光ファイバケーブルの断面、コネクタ、および製品のコネクタ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。

⚠注意

❗　静電気注意
コネクタや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。

❗　コードを持って抜かない
コードを無理に曲げたり、引っ張りますと、コードや機器の破損の原因となります。

❗　振動が発生する場所では使用しない
接触不良や動作不良の原因となります。

禁止　付属品の使用は取扱説明書にしたがう
付属品は取扱説明書にしたがい、他の製品には使用しないでください。機器の破損の原因になります。

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。

- 保守マーク表示を守ってください。また、ドキュメント類に説明されている以外の方法でのご使用はやめてください。三角形の中に稲妻マークがついたカバー類をあけたり外したりすると、感電の危険性を招きます。筐体の内部は、訓練を受けた保守技術員が取り扱うようにしてください。
- 以下のような状況に陥った場合は、電源ケーブルをコンセントから抜いて、部品の交換をするかサービス会社に連絡してください。
  - 電源ケーブル、延長ケーブル、またはプラグが破損した。
  - 製品の中に異物が入った。
  - 製品に水がかかった。
  - 製品が落下した、または損傷を受けた。
  - 操作方法に従って運用しているのに正しく動作しない。
- 本製品をラジエータや熱源の近くに置かないでください。また冷却用通気孔を塞がないようにしてください。
- 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。万一製品が濡れてしまった場合は、トラブルシューティングガイドの該当する文をお読みになるか、サービス会社に連絡してください。
- 本システムの開口部に物を差し込まないでください。内部コンポーネントのショートによる火事や感電を引き起こすことがあります。
- 本製品と一緒にその他のデバイスを使用する場合は、弊社の認定を受けたデバイスを使用してください。
- カバーを外す際、あるいは内部コンポーネントに触れる際は、製品の温度が十分に下がってから行ってください。
- 電気定格ラベル標記と合致したタイプの外部電源を使用してください。正しい外部電源タイプがわからない場合は、サービス会社、あるいはお近くの電力会社にお問い合わせください。
- システムの損傷を防ぐために、電源装置の電圧選択スイッチ（装備されている場合のみ）がご利用の地域の設定と合致しているか確認してください。
  - 東日本では 100V/50Hz、西日本では 100V/60Hz
- また、付属するデバイスが、ご使用になる地域の電気定格に合致しているか確認してください。
- 付属の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、本システムと周辺装置の電源ケーブルは、正しく接地された電気コンセントに接続してください。このケーブルには、正しく接地されるように、3 ピンプラグが取り付けられています。アダプタプラグを使用したり、ケーブルから接地ピンを取り外したりしないでください。延長コードを使用する必要がある場合は、正しく接地されたプラグが付いている 3 線式コードを使用してください。
- 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システムコンポーネントを保護するには、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。踏みつけられたりつまず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。
- 電源ケーブルやプラグを改造しないでください。設置場所の変更をする場合は、資格を持った電気技術者または電力会社にお問い合わせください。国または地方自治体の配線規則に必ず従ってください。
- 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ください。
- 製品の移動は気をつけて行ってください。キャスタやスタビライザがしっかり装着されているか確認してください。急停止や、凹凸面上の移動は避けてください。

ラック搭載型製品に関する一般的な注意事項

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

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

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

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

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

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

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

静電気障害を防止するために

静電気は、システム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、マイクロプロセッサなどの電子部品に触れる前に、身体から静電気を逃がしてください。シャーシの塗装されていない金属面に定期的に触れることにより、身体の静電気を逃がすことができます。

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. 静電気に敏感なコンポーネントを箱から取り出す時は、コンポーネントをシステムに取り付ける準備が完了するまで、コンポーネント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してください。
2. 静電気に敏感な部品を運ぶ場合、最初に静電気防止容器またはパッケージに入れてください。
3. 静電気に敏感なコンポーネントの取り扱いは、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。

バッテリの取り扱いについて

警告 不適切なバッテリの使用により、爆発などの危険性が生じることがあります。バッテリの交換は、必ず同じものか、製造者が推奨する同等の仕様のものをご使用ください。バッテリの廃棄については、製造者の指示に従って行ってください。

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。

本製品には電源ケーブル抜け防止金具が同梱されております。本製品を製品背面の電源コネクタ部分に取り付けます。電源ケーブルを接続して金具に固定すると、ケーブルの抜けを防止することができます。

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、および同梱されている製品保証書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。

- 本書および同梱されている製品保証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。
- 本書および同梱されている製品保証書は大切に保管してください。
- 弊社製品を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。
http://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 3
ラック搭載型製品に関する一般的な注意事項 4
静電気障害を防止するために 4
バッテリの取り扱いについて 4
電源の異常 5

はじめに 12

本マニュアルの対象者 13
表記規則について 13

第 1 章　本製品のご利用にあたって 14

本スイッチについて 14
ポート 14
前面パネル 15
　LED 表示 17
背面パネル 19
側面パネル 20
ギガビットコンボポート 21

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
電源の投入 24

第 3 章　スイッチの接続 25

エンドノードと接続する 25
ハブまたはスイッチと接続する 26
　スイッチとの接続例 26
　スイッチ構成例 26
バックボーンまたはサーバと接続する 27

第 4 章　スイッチ管理の導入 28

管理オプション 28
端末をコンソールポートに接続する 28
スイッチへの初回接続 29
パスワード設定 29
SNMP 設定 30
　トラップ 31
　MIB 31
IP アドレスの割り当て 31

第 5 章　Web ベースのスイッチ管理 33

Web ベースの管理について 33
Web マネージャへのログイン 33
Web マネージャの画面構成 34
　Web マネージャのメイン画面について 34
Web マネージャのメニュー構成 35

第 6 章　Configuration（スイッチの主な設定） 38

Device Information（デバイス情報） 39
System Information（システム情報） 40
Serial Port Settings（シリアルポート設定） 41
IP Address Settings（IP アドレス設定） 42
　IP アドレス設定 42
　コンソールインタフェースを使用したスイッチの IP アドレス設定 43
IPv6 Interface Settings（IPv6 インタフェース設定） 44

IPv6 Route Settings（IPv6 ルートテーブル設定）.....44
IPv6 Neighbor Settings（IPv6 Neighbor 設定）.....45
Port Configuration（ポート設定）.....46
Port Settings（スイッチのポート設定）.....46
Port Description Settings（ポート名設定）.....47
Port Error Disabled（エラーによるポートの無効）.....47
Static ARP Settings（スタティック ARP 設定）.....48
User Accounts（ユーザアカウントの設定）.....49
System Log Configuration（システムログ構成）.....50
System Log Settings（システムログ設定）.....50
System Log Server（システムログの管理）.....51
DHCP Relay（DHCP リレー）.....52
DHCP Relay Global Settings（DHCP リレーグローバル設定）.....52
DHCP Relay Interface Settings（DHCP リレーインタフェース設定）.....54
DHCP Local Relay Settings（DHCP ローカルリレー設定）.....54
DHCP Auto Configuration Settings（DHCP 自動設定）.....55
MAC Address Aging Time（MAC アドレスエージングタイム）.....55
Web Settings（Web 設定）.....56
Telnet Settings（Telnet 設定）.....56
Password Encryption（パスワードの暗号化）.....57
CLI Paging Settings（CLI ページング設定）.....57
Firmware Information（ファームウェア情報）.....58
SNTP Settings（SNTP 設定）.....59
Time Settings（時刻設定）.....59
TimeZone Settings（タイムゾーン設定）.....60
SMTP Settings（SMTP 設定）.....61
SMTP Service Settings（SMTP サービスの設定）.....61
SMTP Service（SMTP サービス）.....62
MAC Notification Settings（MAC 通知設定）.....63
MAC Notification Global Settings（MAC 通知グローバル設定）.....63
MAC Notification Port Settings（MAC 通知ポート設定）.....63
SNMP Settings（SNMP 設定）.....64
SNMP View Table（SNMP ビューテーブル）.....65
SNMP Group Table（SNMP グループテーブル）.....66
SNMP User Table（SNMP ユーザテーブル）.....67
SNMP Community Table（SNMP コミュニティテーブル設定）.....68
SNMP Host Table（SNMP ホストテーブル）.....69
SNMP Engine ID（SNMP エンジン ID）.....69
SNMP Trap Configuration（SNMP トラップ設定）.....70
RMON（RMON 設定）.....70
Time Range Settings（タイムレンジ設定）.....71
Single IP Management（シングル IP マネジメント設定）.....72
シングル IP マネジメント（SIM）の概要.....72
バージョン 1.61 へのアップグレード.....73
Single IP Settings（シングル IP 設定）.....74
Topology（トポロジ）.....75
ツールヒント.....77
メニューバー.....80
Firmware Upgrade（ファームウェア更新）.....81
Configuration File Backup/ Restore（コンフィグレーションファイルの更新）.....81
Upload Log File（ログファイルのアップロード）.....81
Gratuitous ARP（Gratuitous ARP の設定）.....82
Gratuitous ARP Global Settings（Gratuitous ARP グローバル設定）.....82
Gratuitous ARP Settings（Gratuitous ARP 設定）.....82
ARP Spoofing Prevention Settings（ARP Spoofing 防止設定）.....83
PPPoE Circuit ID Insertion Settings（PPPoE Circuit ID の挿入）.....84

第 7 章　L2 Features（L2 機能の設定）　85

Jumbo Frame（ジャンボフレームの有効化）....85
802.1Q VLAN 設定....86
IEEE 802.1p プライオリティについて....86
VLAN について....86
本スイッチにおける VLAN について....86
IEEE 802.1Q VLAN....87
802.1Q VLAN タグ....88
ポート VLAN ID....89
タギングとアンタギング....89
Ingress フィルタリング....89
デフォルト VLAN....90
ポートベース VLAN....90
VLAN セグメンテーション....90
VLAN とトランクグループ....90
Q-in-Q VLAN（Q-in-Q VLAN 設定）....90
802.1Q Static VLAN（802.1Q スタティック VLAN 設定）....92
QinQ（QinQ 設定）....95
QinQ Settings（QinQ 設定）....95
VLAN Translation CVID Entry Settings（VLAN 変換 CVID エントリ機能の設定）....96
802.1v Protocol VLAN（802.1v プロトコル VLAN）....97
802.1v Protocol Group Settings（802.1v プロトコルグループ設定）....97
802.1v Protocol VLAN Settings（802.1v プロトコル VLAN 設定）....98
VLAN Trunk Settings（VLAN トランク設定）....100
GVRP Settings（GVRP の設定）....101
Asymmetric VLAN Settings（Asymmetric VLAN 設定）....102
MAC-based VLAN Settings（MAC ベース VLAN 設定）....102
PVID Auto Assign Settings（PVID 自動割り当て設定）....103
Port Trunking（ポートトランキングの設定）....103
ポートトランクグループについて....103
LACP Port Settings（LACP の設定）....106
Traffic Segmentation（トラフィックセグメンテーション）....107
L2PT Settings（レイヤ 2 プロトコルトンネリング設定）....107
BPDU Attack Protection Settings（BPDU アタック防止設定）....108
IGMP Snooping（IGMP Snooping の設定）....109
IGMP Snooping Settings（IGMP Snooping グローバル設定）....109
IGMP Access Control Settings（IGMP アクセスコントロール設定）....111
IGMP Snooping Multicast VLAN Settings（ISM VLAN 設定）....112
IP Multicast Profile Settings（IP マルチキャストプロファイル設定）....114
Limited Multicast Range Settings（IP マルチキャスト範囲の限定設定）....115
Max Multicast Group Settings（最大マルチキャストグループ設定）....116
MLD Snooping Settings（MLD Snooping 設定）....117
Port Mirror（ポートミラーリングの設定）....120
Loopback Detection Settings（ループバック検知設定）....121
Spanning Tree（スパニングツリーの設定）....122
802.1Q-2005 MSTP....122
802.1D-2004 Rapid Spanning Tree....122
ポートの状態遷移....123
STP Bridge Global Settings（STP ブリッジグローバル設定）....124
STP Port Settings（STP ポートの設定）....125
MST Configuration Identification（MST の設定）....127
STP Instance Settings（STP インタンス設定）....128
MSTP Port Information（MSTP ポート情報）....129
Forwarding & Filtering（フォワーディングとフィルタリングの設定）....131
Unicast Forwarding Settings（ユニキャストフォワーディング）....131
Multicast Forwarding Settings（マルチキャストフォワーディングの設定）....131
Multicast Filtering Mode Settings（マルチキャストフィルタリングモード）....132
NLB Settings（ネットワークロードバランシング設定）....133
LLDP（LLDP 設定）....134
LLDP Global Settings（LLDP グローバル設定）....134
LLDP Port Settings（LLDP ポート設定）....135
LLDP Basic TLVs Settings（LLDP ベーシック TLV 設定）....136
LLDP Dot1 TLVs Settings（LLDP Dot1 TLV 設定）....136
LLDP Dot3 TLVs Settings（LLDP Dot3 TLV 設定）....137

Ethernet OAM（イーサネット OAM）.....138
Ethernet OAM Port Settings（イーサネット OAM ポート設定）.....138
Ethernet OAM Event Configuration（イーサネット OAM イベント設定）.....139
CFM（Connectivity Fault Management : 接続性障害管理）.....140
CFM Settings（CFM 設定）.....142
CFM Port Settings（CFM ポート設定）.....146
CFM Loopback Settings（CFM ループバック設定）.....146
CFM Linktrace Settings（CFM リンクトレース設定）.....147
ERPS Settings（イーサネットリングプロテクション設定）.....148

第 8 章　QoS（QoS 機能の設定）　150

QoS の長所.....150
QoS について.....151
Bandwidth Control（帯域幅の設定）.....152
Traffic Control（トラフィックコントロールの設定）.....153
Queue Bandwidth Control Settings（キュー帯域幅制御設定）.....155
802.1p Default Priority（ポートへのパケットプライオリティの割り当て）.....156
802.1p User Priority（プライオリティのクラス（キュー）への割り当て）.....156
QoS Scheduling Settings（QoS スケジュールの設定）.....157
Priority Mapping（プライオリティマッピング設定）.....157
TOS Mapping（TOS マッピング設定）.....158
DSCP Mapping（DSCP マッピング設定）.....158

第 9 章　Security（セキュリティ機能の設定）　159

Safeguard Engine（セーフガードエンジン）.....159
Trusted Host（トラストホスト）.....161
IP-MAC-Port Binding（IMPB : IP-MAC- ポートバインディング）.....161
IMP Binding Global Settings（IP-MAC- ポートバインディンググローバル設定）.....162
IMP Binding Port Settings（ IP-MAC- ポートバインディング設定）.....163
IMP Binding Entry Settings（ IP-MAC- ポートバインディングエントリ設定）.....164
DHCP Snooping Entries（DHCP Snooping エントリ）.....165
MAC Block List（MAC ブロックリスト）.....165
Port Security（ポートセキュリティ）.....166
Port Security Port Settings（ポートセキュリティの設定）.....166
Port Security FDB Entries（ポートセキュリティ FDB エントリ）.....167
802.1X（802.1X ポートベース / ホストベースアクセスコントロール）.....168
802.1X Settings（802.1X 設定）.....172
802.1X User（802.1X ユーザ）.....173
Authentication RADIUS Server（認証 RADIUS サーバの設定）.....173
Guest VLAN（ゲスト VLAN の設定）.....175
Initialize Port(s)（ポートの初期化）.....177
Reauthenticate Port(s)（ポートの再認証）.....178
SSL Settings（Secure Socket Layer の設定）.....179
SSH（Secure Shell の設定）.....181
SSH Settings（SSH サーバ設定）.....181
SSH Authmode and Algorithm Settings（SSH 認証モードとアルゴリズム設定）.....182
SSH User Authentication Lists（SSH ユーザ認証モード）.....183
Access Authentication Control（アクセス認証コントロール）.....184
Authentication Policy Settings（認証ポリシー設定）.....185
Application Authentication Settings（アプリケーションの認証設定）.....185
Authentication Server Group（認証サーバグループ）.....186
Authentication Server（認証サーバ）.....187
Login Method Lists（ログインメソッドリスト）.....188
Enable Method Lists（メソッドリストの有効化）.....189
Local Enable Password Settings（ローカルユーザパスワード設定）.....190
MAC-based Access Control（MAC アドレス認証）.....191
MAC アドレス認証に関する注意.....191
MAC-based Access Control Settings（MAC アドレス認証設定）.....191
MAC-based Access Control Local Settings（MAC アドレス認証ローカル MAC 設定）.....193
DoS Prevention Settings（DoS 攻撃防止設定）.....194
DHCP Server Screening（DHCP サーバスクリーニング）.....195
DHCP Screening Port Settings（DHCP スクリーニングポート設定）.....195
DHCP Offer Filtering（DHCP Offer フィルタリング）.....196

第 10 章　ACL（ACL 機能の設定）　197

ACL Configuration Wizard（ACL 設定ウィザード）....197
Access Profile List（アクセスプロファイルリスト）....199
アクセスプロファイルリストの作成（Ethernet）....199
アクセスプロファイルリストの作成（IPv4）....202
アクセスプロファイルリストの作成（IPv6）....207
アクセスプロファイルリストの作成（パケットコンテンツ）....211
CPU Access Profile List（CPU アクセスプロファイルリスト）....215
CPU アクセスプロファイルの作成（Ethernet）....215
CPU アクセスプロファイルの作成（IPv4）....218
CPU アクセスプロファイルの作成（IPv6）....222
CPU アクセスプロファイルの作成（パケットコンテンツ）....225
ACL Finder（ACL 検索）....229
ACL Flow Meter（ACL フローメータ）....230

第 11 章　Monitoring（スイッチのモニタリング）　232

Cable Diagnostic（ケーブル診断機能）....232
CPU Utilization（CPU 使用率）....233
Port Utilization（ポート使用率）....234
Packet Size（パケットサイズ）....235
Memory Utilization（メモリ使用率）....236
Packets（パケット統計情報）....237
Received（Rx）（受信パケット状態の参照）....237
UMB_Cast（Rx）（UMB Cast パケット統計情報の参照）....238
Transmitted（Tx）（送信パケット統計情報）....240
Errors（パケットエラー）....241
Received（Rx）（受信エラーパケット統計情報の参照）....241
Transmitted（Tx）（送信エラーパケット統計情報の参照）....243
Port Access Control（ポートアクセスコントロール）....244
RADIUS Authentication（RADIUS 認証）....244
RADIUS Account Client（RADIUS アカウンティングクライアント）....245
Authenticator State（オーセンティケータの状態）....246
Authenticator Statistics（Authenticator 統計情報）....248
Authenticator Session Statistics（Authenticator セッション統計情報）....249
Authenticator Diagnostics（Authenticator 診断）....250
Browse ARP Table（ARP テーブルの参照）....252
Browse VLAN（VLAN の参照）....252
IGMP Snooping（IGMP Snooping 設定の参照）....253
Browse IGMP Router Port（ルータポート参照）....253
IGMP Snooping Group（IGMP Snooping グループ）....253
IGMP Snooping Host（IGMP Snooping ホストの参照）....254
MLD Snooping（MLD Snooping 設定の参照）....254
Browse MLD Router Port（MLD ルータポートの参照）....254
MLD Snooping Group（MLD Snooping グループ）....255
LLDP（LLDP 設定の参照）....256
LLDP Statistics System（LLDP 統計情報システム）....256
LLDP Local Port Information（LLDP ローカルポート情報）....256
LLDP Remote Port Information（LLDP リモートポート情報）....257
Ethernet OAM（イーサネット OAM）....257
Browse Ethernet OAM Event Log（イーサネット OAM イベントログ）....257
Browse Ethernet OAM Statistics（イーサネット OAM 統計情報の参照）....258
CFM（Connectivity Fault Management : 接続性障害管理）....259
CFM Fault Table（CFM 障害テーブル）....259
CFM MIPCCM Table（CFM MIPCCM テーブル）....259
CFM MP Table（CFM MP テーブル）....259
CFM Packet Counter（CFM パケットカウンタ）....260
Mac-based Access Control Authentication State（MAC ベースアクセスコントロール認証ステートの参照）....261
Browse Session Table（セッションテーブルの参照）....261
MAC Address Table（MAC アドレステーブル）....262
System Log（システムログ）....263

第 12 章　Maintenance（スイッチのメンテナンス） 264

Save（コンフィグレーションとログの保存） 264
Save Configuration（Configuration の保存） 264
Save Log（ログの保存） 265
Save All（コンフィグレーションファイルとログの保存） 265
Tools（ツールメニュー） 265
Configuration File Upload & Download（コンフィグレーションファイルのアップロードとダウンロード） 266
Upload Log File（ログファイルのアップロード） 266
Reset（リセット） 266
Ping Test（Ping テスト） 267
Download Firmware（ファームウェアのダウンロード） 268
Reboot System（システムの再起動） 268

付録 A ケーブルとコネクタ 269

付録 B ケーブル長 269

付録 C ログイベント 270

付録 D トラップログ 276

付録 E RADIUS 属性の割り当て指定 279

付録 F パスワードリカバリ手順 281

付録 G 用語解説 282

はじめに

DES-3200 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その機能について説明します。また、前面、背面、側面の各パネルと LED 表示について説明します。

第 2 章 システムの設置
- システムの基本的な設置方法について説明します。また、本スイッチの電源接続の方法についても紹介します。

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、またはバックボーンなどに接続する方法を説明します。

第 4 章 スイッチ管理の導入
- パスワード設定、SNMP 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の基本的なスイッチの管理について説明します。

第 5 章 Web ベースのスイッチ管理
- Web ベースの管理機能への接続方法および使用方法について説明します。

第 6 章 Configuration（スイッチの主な設定）
- スイッチ情報へのアクセス、IP アドレス、ユーザアカウント、システムログ、システム時刻、SNMP、シングル IP マネジメントなどのスイッチの設定について説明します。

第 7 章 L2 Features（L2 機能の設定）
- VLAN、トランキング、スパニングツリー、IGMP/MLD Snooping などスイッチの L2 機能について説明します。

第 8 章 QoS（QoS 機能の設定）
- スイッチの QoS の概要と設定について説明します。

第 9 章 Security（セキュリティ機能の設定）
- 802.1X 認証、アクセス認証コントロール、トラフィックコントロール、セーフガードエンジンなどスイッチのセキュリティ機能について説明します。

第 10 章 ACL（ACL 機能の設定）
- アクセスコントロールの設定について説明します。

第 11 章 Monitoring（スイッチのモニタリング）
- モニタリング機能で使用するグラフや画面について説明します。

第 12 章 Maintenance（スイッチのメンテナンス）
- 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。

付録 A ケーブルとコネクタ
- RJ-45 コンセント / コネクタ、ストレート / クロスオーバケーブルと標準的なピンの配置について説明します。

付録 B ケーブル長
- ケーブルの種類と最大ケーブル長についての情報を示します。

付録 C ログイベント
- スイッチのシステムログに表示される可能性のあるログイベントとそれらの意味について説明します。

付録 D トラップログ
- スイッチで検出でき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 E RADIUS 属性の割り当て
- Ingress/Egress 帯域、802.1p デフォルトプライオリティ、VLAN、および ACL の RADIUS 属性の割り当てについて説明します。

付録 F 用語集
- 本マニュアルに使用される用語の定義を示します。

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。

第 1 章　本製品のご利用にあたって

- 本スイッチについて
- ポート
- 前面パネル
- 背面パネル
- 側面パネル
- ギガビットコンボポート

本スイッチについて

DES-3200 シリーズスイッチは D-Link スイッチファミリーの製品です。本シリーズは、高性能、フォルトトレランス、スケーラブルな柔軟性、強健なセキュリティ、標準規格に準拠した相互運用性、および非常に高い技術をサポートしており、将来的な部門ネットワークおよびエンタプライズネットワーク構築への移行も簡単に行うことができます。

本マニュアルでは、D-Link DES-3200 シリーズの設置、設定、およびメンテナンスの方法について記述しています。これらのスイッチの基本的なハードウェア構成は似ており、設定方法、操作性はほぼ共通です。また、本マニュアル内の記載事項の多くが本スイッチシリーズで共通です。Web 画面は、シリーズの中の一製品を例にとって説明していますが、ポート数を除き設定方法は同じです。本マニュアル中での説明では主として DES-3200-28F の画面と設定を例題として使用しています。

ポート

DES-3200 シリーズスイッチはそれぞれ以下のポートを搭載しています。

型番	DES-3200-10	DES-3200-18	DES-3200-26	DES-3200-28	DES-3200-28F
10BASE-T/100BASE-TX ポート	8	16	24	24	—
10BASE-T/100BASE-TX/1000BASE-T ポート	2	2	2	4	4
SFP スロット（100BASE-X のみ）	—	—	—	—	24
SFP コンボスロット	2	2	2	4	4
RS-232C ポート（D-Sub 9 ピンメス）	1	1	1	1	1

型番	DES-3200-10/T	DES-3200-18/T	DES-3200-26/T	DES-3200-28/T
10BASE-T/100BASE-TX ポート	8	16	24	24
10BASE-T/100BASE-TX/1000BASE-T ポート	1	1	2	2
SFP スロット	1	1	—	2
SFP コンボスロット	1	1	2	2
RJ45 コンソールポート	1	1	1	1

DES-3200 シリーズの各ポートタイプの特長および使用可能なオプションは次の通りです。

10BASE-T/100BASE-TX	SFP コンボ	1000BASE-T
• IEEE 802.3 • IEEE 802.3u • 全二重通信 • 全二重モード時の IEEE 802.3x フローコントロール	• IEEE 802.3z 対応 SFP トランシーバ : • DEM-210（100BASE-FX） • DEM-211（100BASE-FX） • DEM-310GT（1000BASE-LX） • DEM-311GT（1000BASE-SX） • DEM-312GT2（1000BASE-SX2） • DEM-314GT（1000BASE-LH） • DEM-315GT（1000BASE-ZX） • DEM-220T/R（WDM） • DEM-330T/R（WDM） • DEM-331T/R（WDM）	• IEEE 802.3 • IEEE 802.3u • IEEE 802.3ab • IEEE 802.3X • 全二重通信 • 全二重モード時の IEEE 802.3x フローコントロール

注意 SFP コンボポートは、対応する 1000BASE-T ポートと同時に使用することはできません。同時に使用すると（例 : SFP のポート 25 と 1000BASE-T のポート 25）、SFP ポートが優先となり 1000BASE-T ポートは使用不可能となります。

前面パネル

前面パネルには、Power、Console、およびオプションモジュール用の SFP ポートを含む各ポートの Link/Act の状態を表示する LED を搭載しています。「LED 表示」の項で詳細の動作について説明します。

DES-3200-10

- 10BASE-T/100BASE-TX ポート x 8
- 1000BASE-T/SFP コンボポート x 2
- RS-232C（D-Sub9 ピンメス）コンソールポート x 1
- LED : Power、Console、Link/Act/Speed（各ポート）

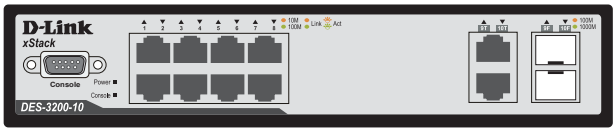


図 1-1　DES-3200-10 の前面パネル

DES-3200-18

- 10BASE-T/100BASE-TX ポート x 16
- 1000BASE-T/SFP コンボポート x 2
- RS-232C（D-Sub9 ピンメス）コンソールポート x 1
- LED : Power、Console、Link/Act/Speed（各ポート）

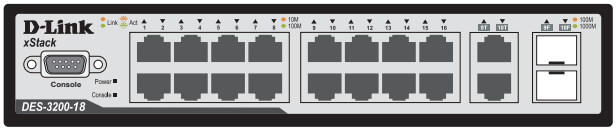


図 1-2　DES-3200-18 の前面パネル

DES-3200-26

- 10BASE-T/100BASE-TX ポート x 24
- 1000BASE-T/SFP コンボポート x 2
- LED : Power、Console、Link/Act/Speed（各ポート）

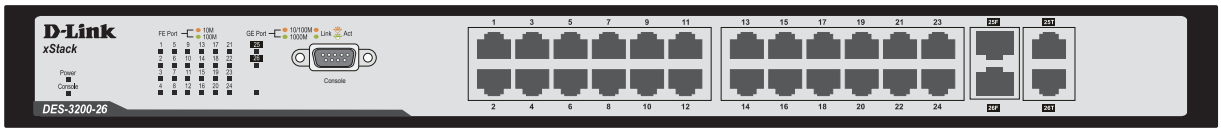


図 1-3　DES-3200-26 の前面パネル

DES-3200-28

- 10BASE-T/100BASE-TX ポート x 24
- 1000BASE-T/SFP コンボポート x 4
- LED : Power、Console、Link/Act/Speed（各ポート）

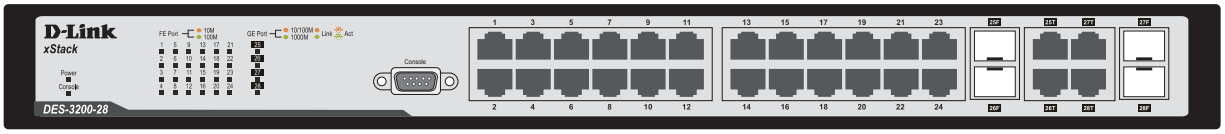


図 1-4　DES-3200-28 の前面パネル

DES-3200-28F

- SFP スロット x 24
- 1000BASE-T/SFP コンボポート x 4
- LED : Power、Console、Link/Act/Speed（各ポート）

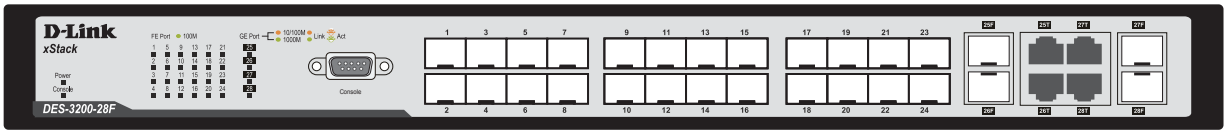


図 1-5　DES-3200-28F の前面パネル

DES-3200-10/T

- 10BASE-T/100BASE-TX ポート x 8
- 1000BASE-T/SFP コンボポート x 1
- SFP ポート x 1
- RJ45 コンソールポート x 1
- LED : Power、Console、Link/Act/Speed（各ポート）

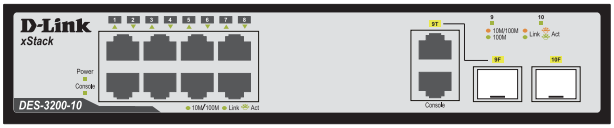


図 1-6　DES-3200-10/T の前面パネル

DES-3200-18/T

- 10BASE-T/100BASE-TX ポート x 16
- 1000BASE-T/SFP コンボポート x 1
- SFP ポート x 1
- RJ45 コンソールポート x 1
- LED : Power、Console、Link/Act/Speed（各ポート）

図 1-7　DES-3200-18/T の前面パネル

DES-3200-26/T

- 10BASE-T/100BASE-TX ポート x 24
- 1000BASE-T/SFP コンボポート x 2
- RJ45 コンソールポート x 1
- LED : Power、Console、Link/Act/Speed（各ポート）

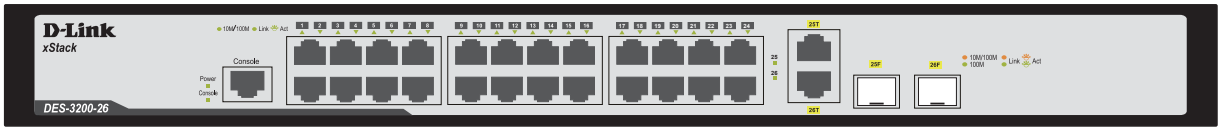


図 1-8　DES-3200-26/T の前面パネル

DES-3200-28/T

- 10BASE-T/100BASE-TX ポート x 24
- 1000BASE-T/SFP コンボポート x 2
- SFP ポート x 2
- RJ45 コンソールポート x 1
- LED : Power、Console、Link/Act/Speed（各ポート）

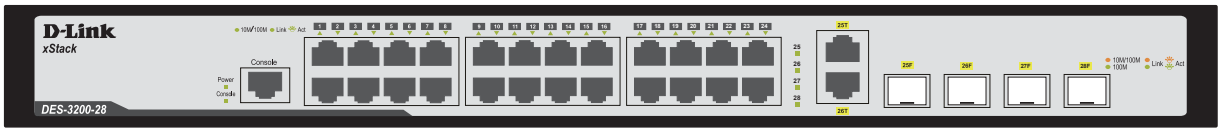


図 1-9　DES-3200-28/T の前面パネル

LED 表示

DES-3200 シリーズスイッチは、Power、Console、および各ポートについて LED をサポートします。

DES-3200-10 の LED

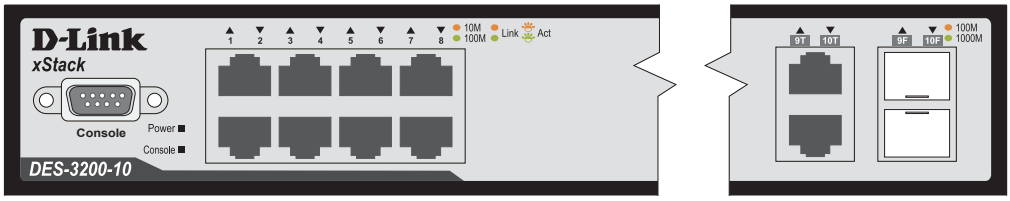


図 1-10　DES-3200-10 の前面パネル LED 配置図

DES-3200-18 の LED

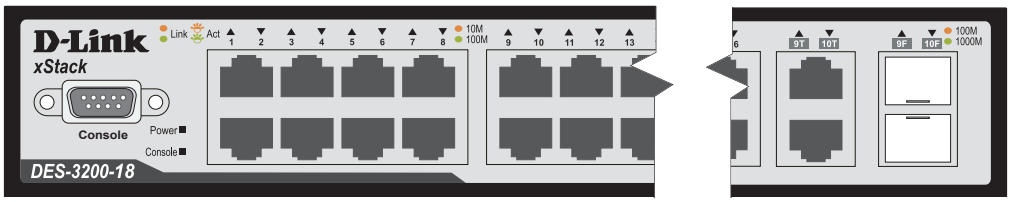


図 1-11　DES-3200-18 の前面パネル LED 配置図

DES-3200-26 の LED

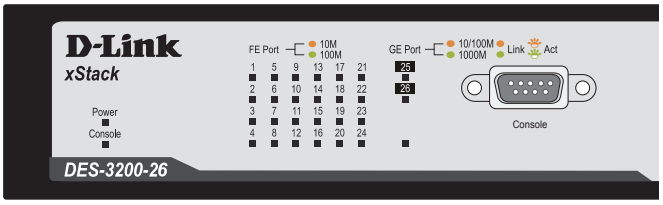


図 1-12　DES-3200-26 の前面パネル LED 配置図

DES-3200-28 の LED

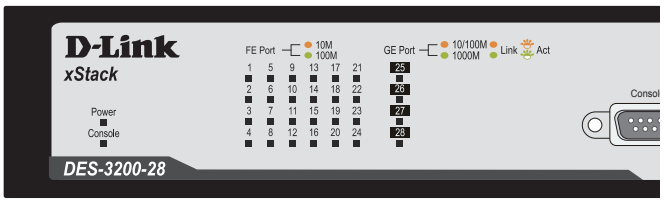


図 1-13　DES-3200-28 の前面パネル LED 配置図

DES-3200-28F の LED

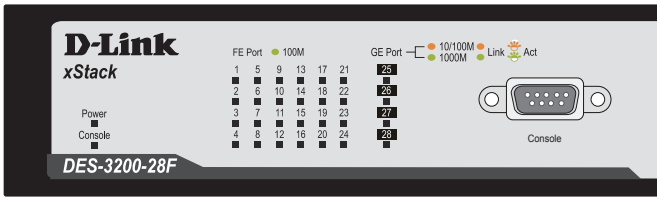


図 1-14　DES-3200-28F の前面パネル LED 配置図

DES-3200-10/T の LED

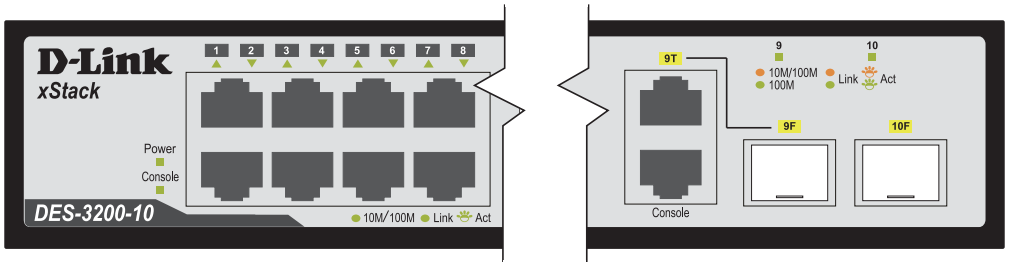


図 1-15　DES-3200-10/T の前面パネル LED 配置図

DES-3200-18/T の LED

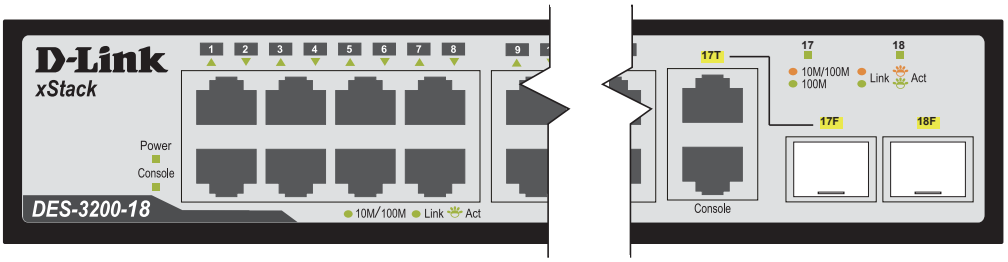


図 1-16　DES-3200-18/T の前面パネル LED 配置図

DES-3200-26/T の LED

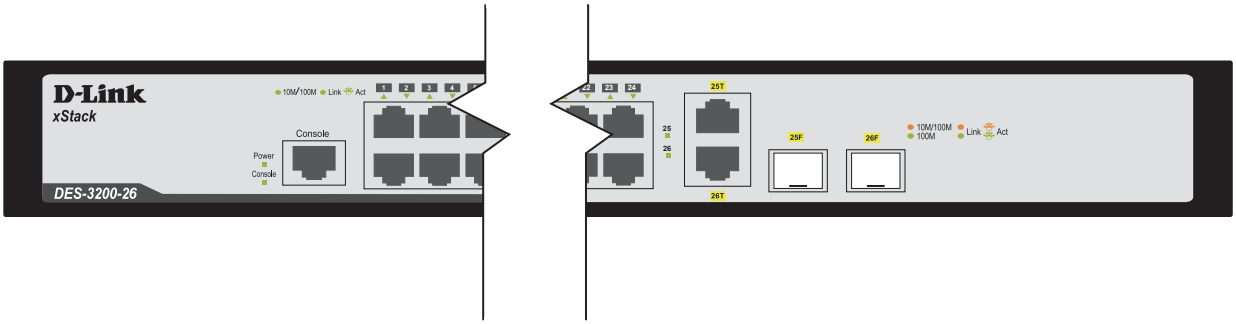


図 1-17　DES-3200-26/T の前面パネル LED 配置図

DES-3200-28/T の LED

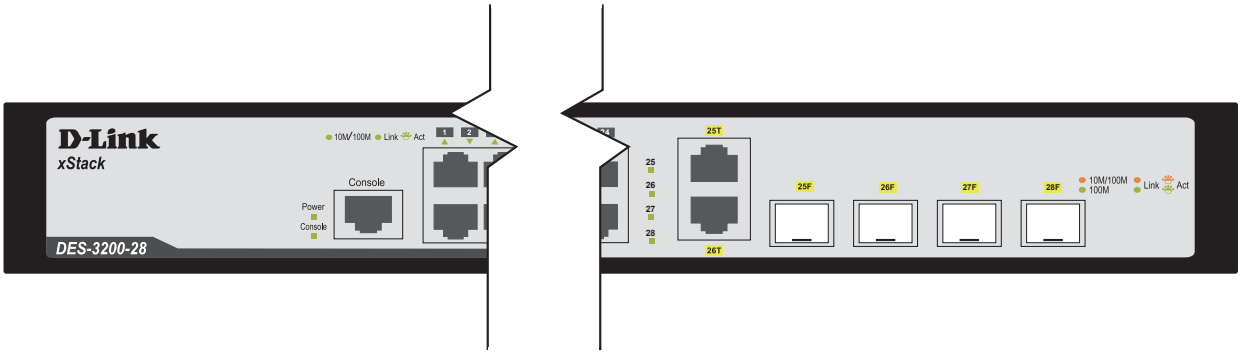


図 1-18　DES-3200-28/T の前面パネル LED 配置図

DES-3200 スイッチシリーズに搭載している LED は以下の通りです。以下の表より、ご使用のスイッチに搭載の LED について確認ください。

LED	状態	色	状態説明
Power	点灯	緑	スイッチに電源が供給され正常に動作しています。
	消灯	ー	スイッチに電源が供給されていません。
Console	点滅	緑	電源投入後の Power ON Self Test（POST）中に点滅し、終了すると消灯します。
	点灯		コンソールポートのリンクが確立しています。
10/100M Port LED（DES-3200-10/18/26/28）	点灯	緑	100Mbps でリンクが確立しています。
	点滅		100Mbps でデータを送受信しています。
	点灯	橙	10Mbps でリンクが確立しています。
	点滅		10Mbps でデータを送受信しています。
	消灯	ー	リンクが確立していません。
10/100M Port LED（DES-3200-28F、10/T、18/T、26/T、28/T）	点灯	緑	100Mbps でリンクが確立しています。
	点滅		100Mbps でデータを送受信しています。
	消灯	ー	リンクが確立していません。

LED	状態	色	状態説明
コンボポート	スイッチ上の 2/4 個の 1000BASE-T/SFP ポートそれぞれに LED が配置されています。		
SFP	点灯	緑	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。
	点灯	橙	100Mbps でリンクが確立しています。
	点滅		100Mbps でデータを送受信しています。
	消灯	ー	リンクが確立していません。
GE	点灯	緑	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。
	点灯	橙	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。
	消灯	ー	リンクが確立していません。

背面パネル

DES-3200 シリーズの背面パネルは次の通りです。

DES-3200-10 / DES-3200-18

電源コネクタおよびアース線用端子が配備されています。

図 1-19　DES-3200-10 / DES-3200-18 の背面パネル図

DES-3200-10/T、DES-3200-18/T

電源コネクタおよびアース線用端子が配備されています。

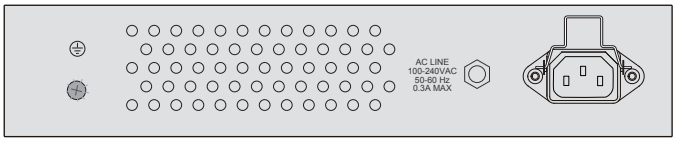


図 1-20　DES-3200-10/T、DES-3200-18/T の背面パネル図

DES-3200-26/DES-3200-28 / DES-3200-28F

電源コネクタおよびアース線用端子が配備されています。

図 1-21　DES-3200-26/DES-3200-28/DES-3200-28F の背面パネル図

DES-3200-26/T、DES-3200-28/T

電源コネクタおよびアース線用端子が配備されています。

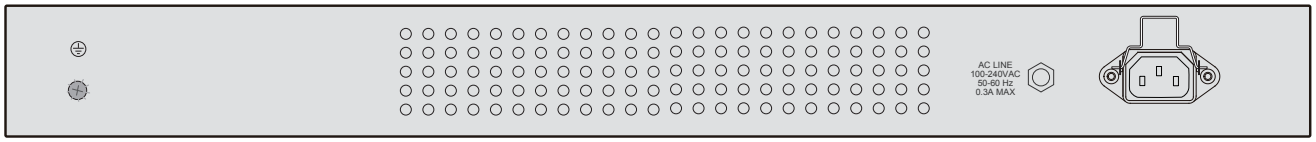


図 1-22　DES-3200-26/T、DES-3200-28/T の背面パネル図

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

システムのファンまたは通気口がスイッチの側面にあり内部の熱を放出します。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、少なくとも 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。

DES-3200-10、DES-3200-18

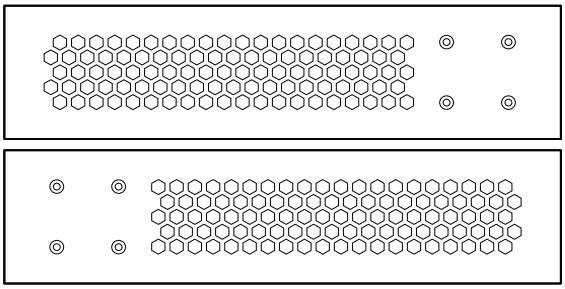


図 1-23　DES-3200-10、DES-3200-18 の側面パネル図

DES-3200-10/T、DES-3200-18/T

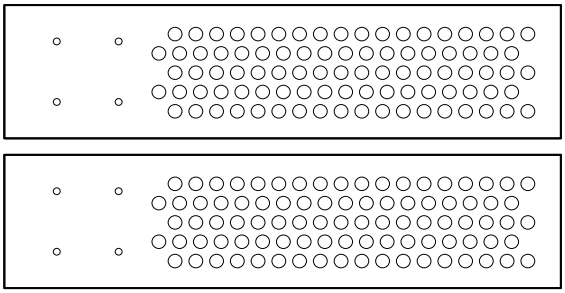


図 1-24　DES-3200-10/T、DES-3200-18/T の側面パネル図

DES-3200-28

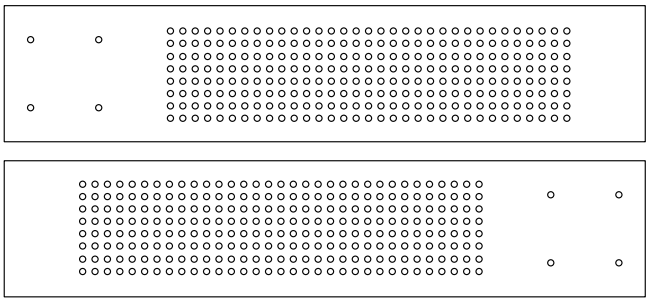


図 1-25　DES-3200-28 の側面パネル図

DES-3200-26、DES-3200-26/T、DES-3200-28/T

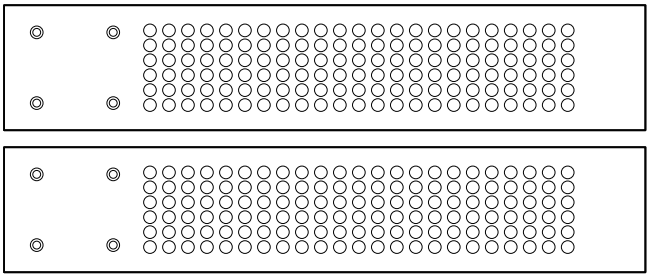


図 1-26　DES-3200-26、DES-3200-26/T、DES-3200-28/T の側面パネル図

DES-3200-28F

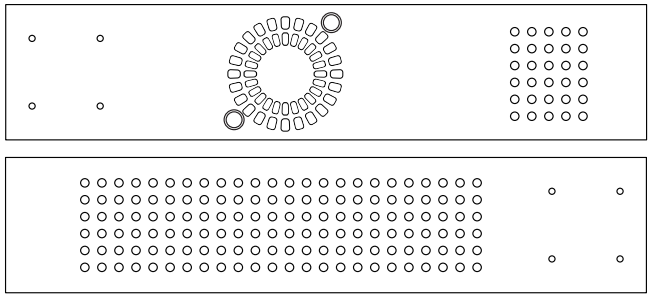


図 1-27　DES-3200-28F の側面パネル図

ギガビットコンボポート

DES-3200 シリーズスイッチは、スイッチの前面パネルに 1~4 つのギガビットイーサネット・コンボポートを装備しています。これらのポートは 1000BASE-T ポートと SFP ポート（オプション）の兼用ポートです。SFP ポートとしての使用時には SFP ポートマジュールを挿入します。以下に、スイッチに SFP ポートモジュールを挿入した図を示します。

注意　これらの前面パネルモジュールは同時に使用できますが、コンボポートの SFP ポートモジュール挿入時は 1000BASE-T ポートとしての使用はできません。SFP ポートが優先されます。

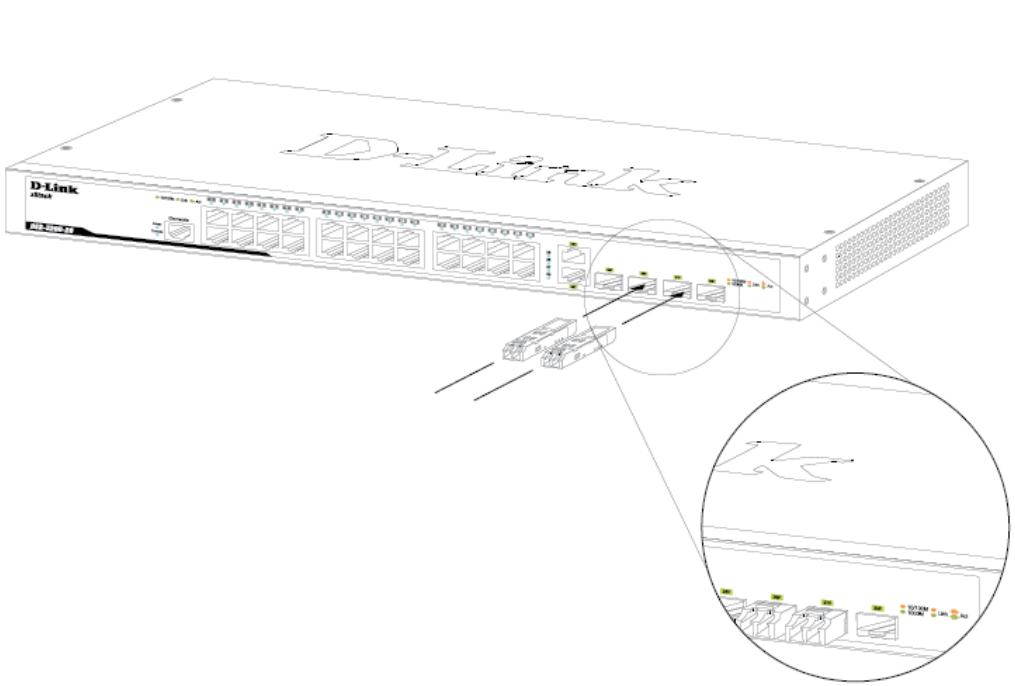


図 1-28　DES-3200-28/T シリーズスイッチに光トランシーバを取り付ける

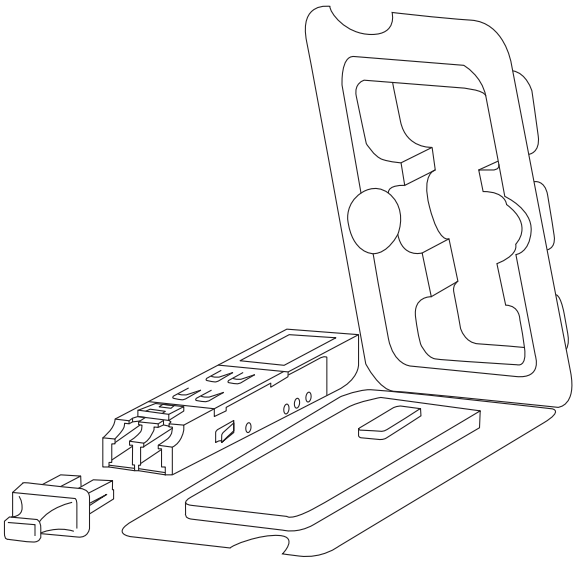


図 1-29　SFP モジュール図

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 インチラックに搭載しない場合）
- 19 インチラックへ取り付け
- 電源の投入
- ギガビットコンボポート

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
- ラックマウントキット 1 式（ブラケット 2 枚、ネジ）
- 電源ケーブル抜け防止金具　x　1
- ゴム足（貼り付けタイプ）　x　4
- シリアルラベル
- CD-ROM
- RS-232C コンソールケーブル（RS-232C ポート搭載機のみ）
- RJ45 コンソールケーブル（RJ-45 コンソールポート搭載機のみ）
- クイックインストールガイド（英語版）
- 製品保証書

万一、不足しているものや損傷を受けているものがありましたら、弊社ホームページにてユーザ登録を行い、サポート窓口までご連絡ください。

ネットワーク接続前の準備

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

- スイッチは、しっかりとした水平面で最低 3 キロの耐荷重性のある場所に設置してください。
- 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 16cm 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。

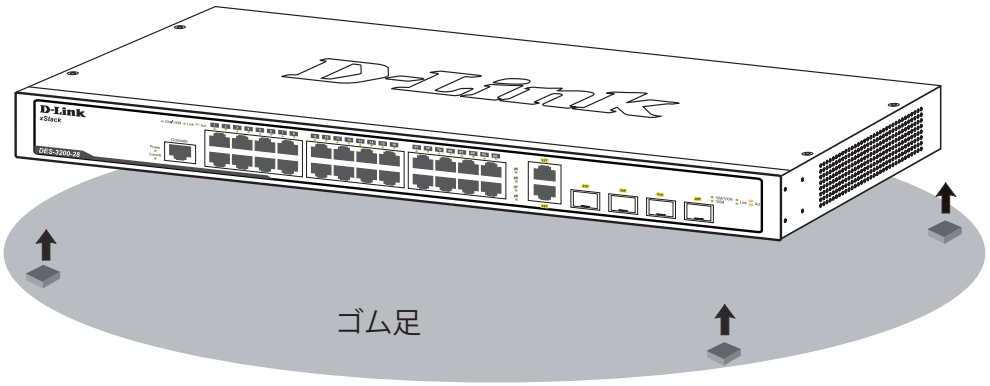


図 2-1　机や棚の上に設置する場合の準備図（DES-3200-28/T）

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。

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、スイッチの両側側面にブラケットを取り付けます。

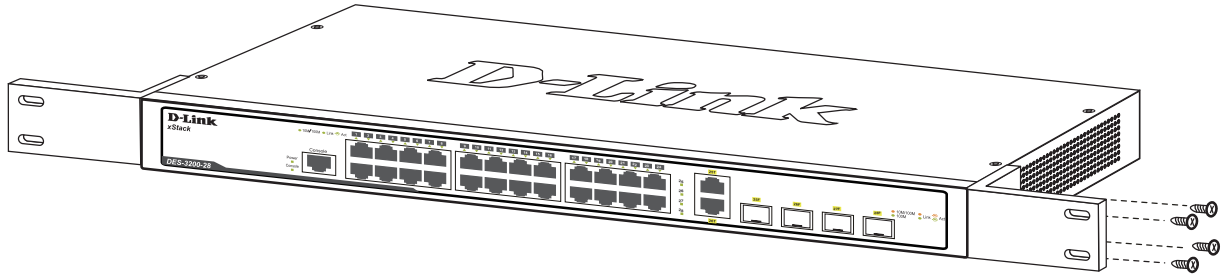


図 2-2　スイッチへのブラケットの取り付け図（DES-3200-28/T）

3. 完全にブラケットが固定されていることを確認し、本スイッチを以下の通り標準の 19 インチラックに固定します。

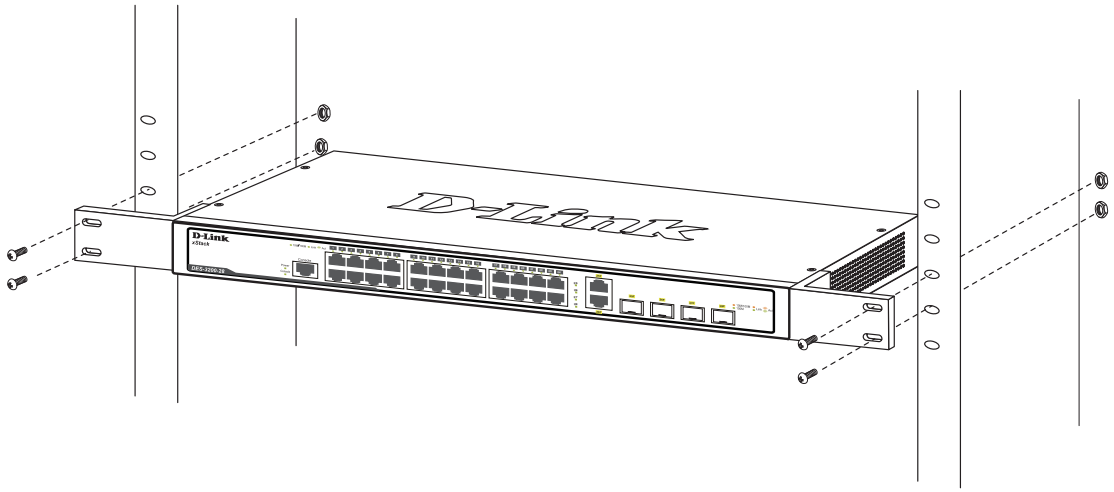


図 2-3　スイッチのラックへの設置図（DES-3200-28/T）

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、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 は点灯します。Console LED は点滅し、システムの設定が終了すると消灯します。

第 3 章　スイッチの接続

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

注意 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

本スイッチの 100BASE-TX または 1000BASE-T ポートとエンドノードをカテゴリ 3、4、5、エンハンスド 5、6 の UTP ケーブルを使用して接続します。エンドノードとは、RJ-45 コネクタ対応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。エンドノードとスイッチ間はカテゴリ 3、4、5、エンハンスド 5、6 の 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。

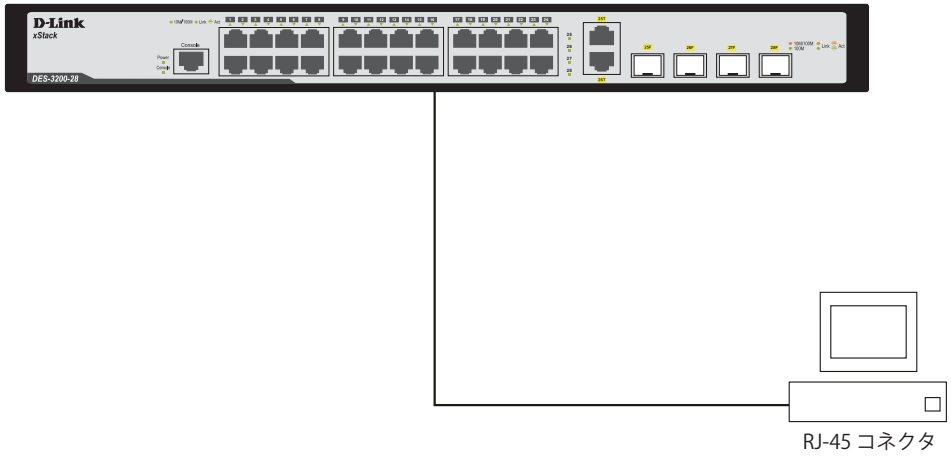


図 3-1　エンドノードと DES-3200-28/T の接続図

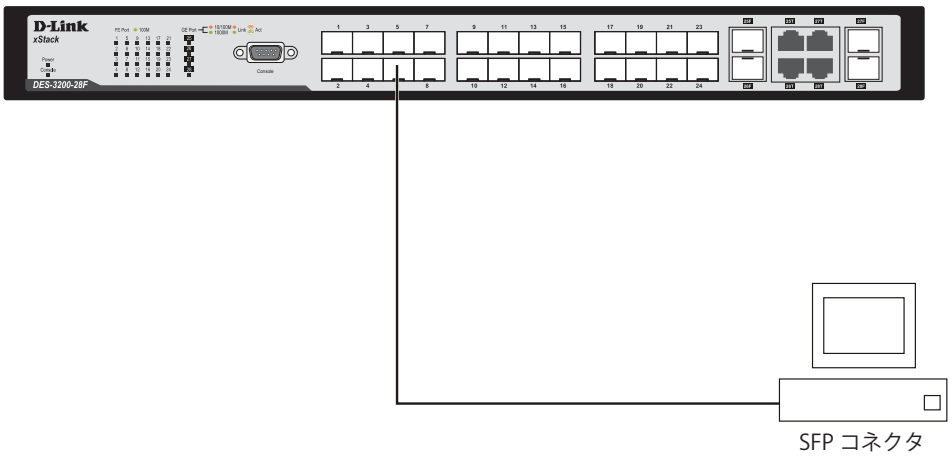


図 3-2　エンドノードと DES-3200-28F の接続図

エンドノードと正しくリンクが確立すると本スイッチの各ポートの 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。
- 光ファイバケーブル：SFP ポートを光ファイバネットワークに接続します。

ケーブル仕様については 269 ページの「付録 A ケーブルとコネクタ」を参照してください。

スイッチとの接続例

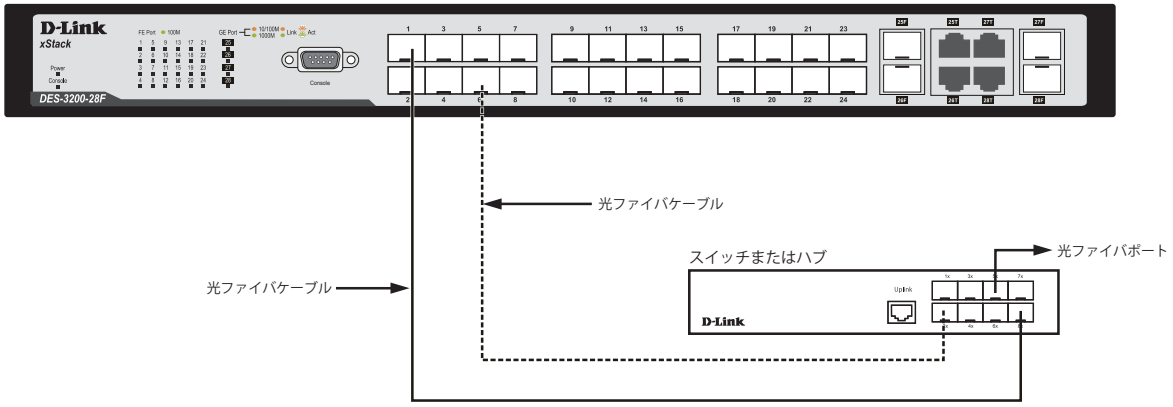


図 3-3　ストレート、クロスケーブルでスイッチ（DES-3200-28F）と接続する図

スイッチ構成例

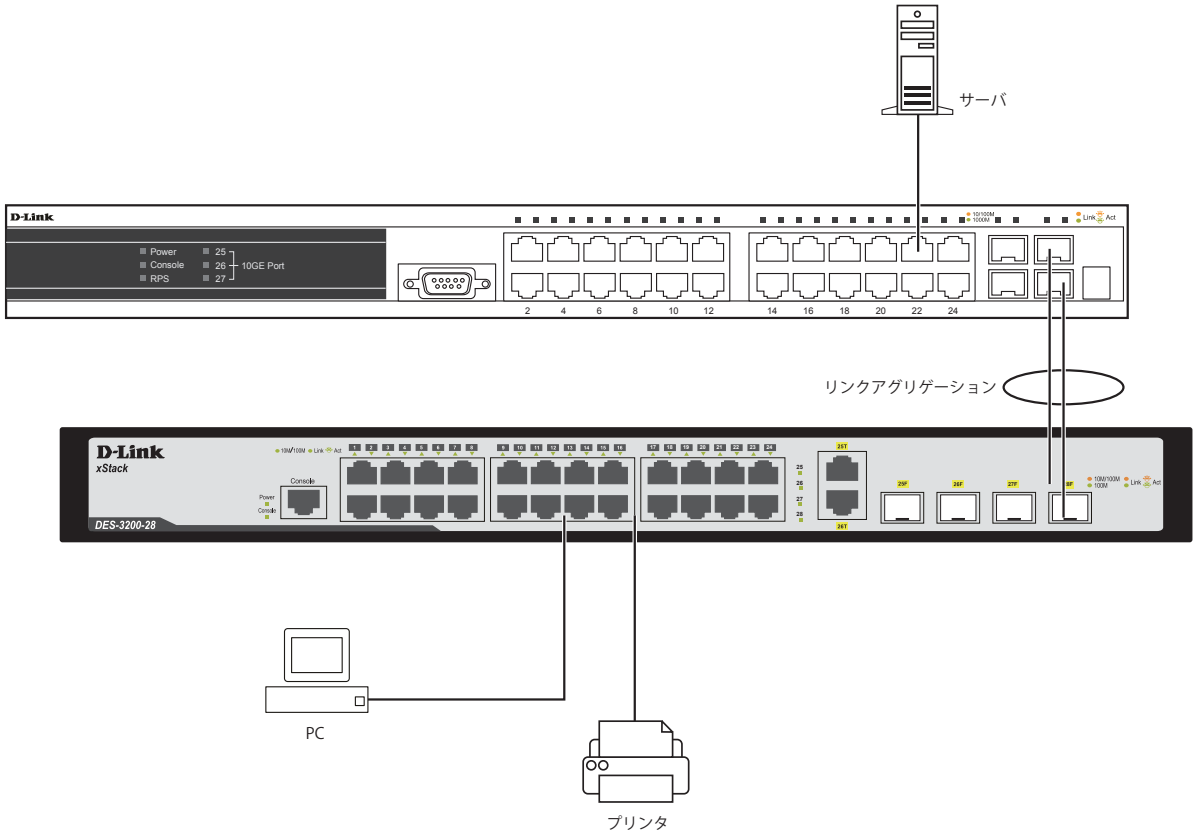


図 3-4　スイッチ構成例（DES-3200-28/T）

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 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。

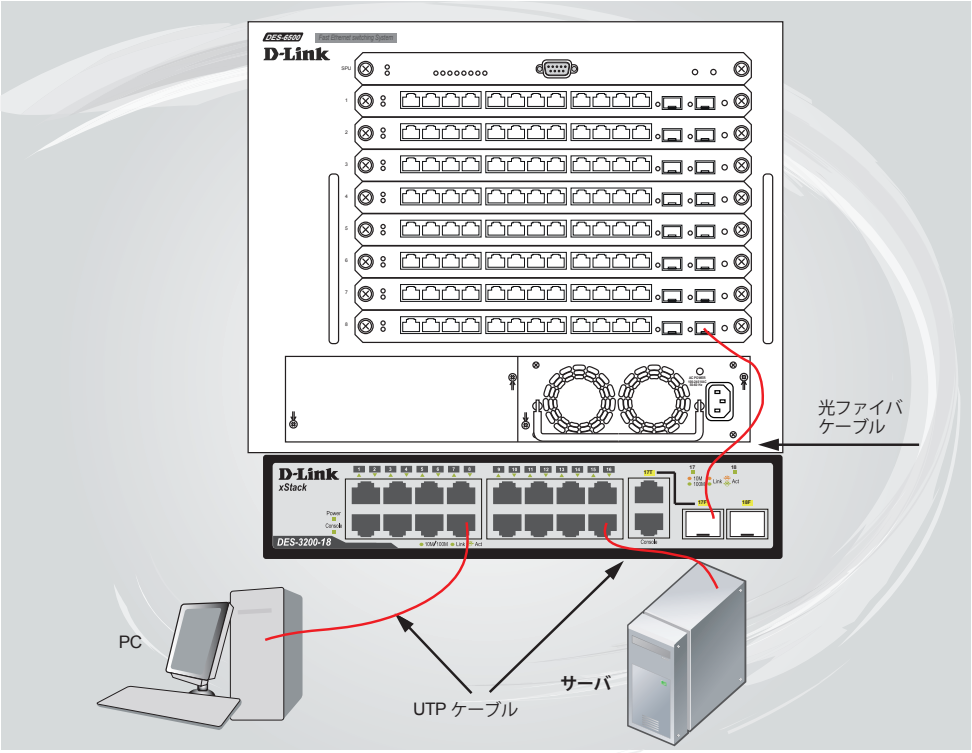


図 3-5　サーバ、PC、スイッチスタックとのアップリンク接続図（DES-3200-18/T）

第 4 章　スイッチ管理の導入

- 管理オプション
- 端末をコンソールポートに接続する
- スイッチへの初回接続
- パスワードの設定
- SNMP 設定
- IP アドレスの割り当て

管理オプション

本システムはコンソールポートを経由した接続や Telnet を使用した接続を行い管理することができます。さらに Web ブラウザによっても管理することができます。

- Web ベースの管理インタフェース
  本スイッチの設置完了後、Microsoft® Internet Explorer（バージョン 6.0 以上）によって本スイッチの設定、LED のモニタ、および統計情報をグラフィカルに表示することができます。

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

- コンソールポートの接続（RS-232 DCE / RJ-45）
  スイッチのモニタリングと設定のために RS-232C シリアルポート（D-Sub9 ピンメスコネクタ）と RJ-45 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
  - D-Sub9 ピン メスコネクタを持つモデムケーブル、または RS-232C クロスケーブル（RS-232C ポート搭載機のみ）
  - 同梱の RJ-45 コンソールケーブル（RJ-45 コンソールポート搭載機のみ）

端末をコンソールポートに接続する

RS-232C コンソールポート搭載機

1. RS-232C コンソールケーブルのメスコネクタをスイッチのコンソールポートに接続し、固定ボルトを締めます。

RJ-45 コンソールポート搭載機

1. 同梱の RJ-45 コンソールケーブルをスイッチのコンソールポートに接続します。

2. ケーブルのもう一方を端末またはターミナルソフトが動作するコンピュータのシリアルコネクタに接続します。以下の手順でターミナルソフトを設定します。
3. 「接続の設定」画面の「接続方法」で、適切なシリアルポート（COM ポート）を選択します。
4. 選択したポートの「プロパティ」画面で「9600」ビット / 秒にデータ速度を設定します。
5. 「データビット」は「8」、「ストップビット」は「1」、「パリティ」は「なし」に設定します。
6. 「フロー制御」は「なし」に設定します。
7. 「エミュレーションモード」を「VT100」に設定します。
8. 「ファンクションキー」、「方向キー」、「Ctrl キー」の使い方で「ターミナルキー」を選択します。「ターミナルキー」（Windows キーではない）の選択を確認します。

注意 Microsoft® Windows® 2000 でハイパーターミナルを使用する場合は、Windows 2000 Service Pack 2 以降がインストール済みであることを確認してください。Windows 2000 Service Pack 2 以降でないとハイパーターミナルの VT100 端末で矢印キーは使用できません。Windows 2000 Service Pack に関する情報はマイクロソフト社のホームページでご確認ください。

9. 端末設定の完了後、本スイッチに電源ケーブルを接続し、電源プラグをコンセントに接続します。端末でブートシーケンスが始まります。
10. ブートシーケンスが完了すると、コンソールのログイン画面が表示されます。
11. 購入後はじめてログインする場合は、ユーザ名（UserName）とパスワード（PassWord）プロンプトで Enter キーを押します。本スイッチには、ユーザ名（UserName）とパスワード（PassWord）の初期値はありません。はじめに、管理者によるユーザ名（UserName）とパスワード（PassWord）の作成が必要です。既にユーザアカウントを作成している場合は、ログインし、続けて本スイッチの設定をします。
12. コマンドを入力して設定を行います。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。次のセクションでユーザアカウントの設定について説明します。CLI のすべてのコマンドリストおよび追加情報については、製品付属 CD-ROM に収録された「DES-3200-10/18/26/28/28F CLI Reference Manual」を参照してください。

13. 管理プログラムを終了する場合は、logout コマンド使用するか、ターミナルソフトを終了します。
14. 接続する端末または PC が以上の通り設定されたことを確認してください。

端末上で接続に問題が発生した場合は、ターミナルソフトの設定で「エミュレーション」が「VT-100」となっていることを確認してください。「エミュレーション」は「ハイパーターミナル」画面の「ファイル」メニューから「プロパティ」をクリックし、「設定」タブにて設定します。何も表示されない場合はスイッチの電源を切り再起動してください。

コンソールに接続すると、コンソール画面が表示されます。この画面上でコマンドを入力し、管理機能を実行します。ユーザ名とパスワードの入力プロンプトが表示されます。初回接続時はユーザ名とパスワードは設定されていないため、「Enter」キーを 2 度押して CLI に接続します。

スイッチへの初回接続

本スイッチは本スイッチへのアクセス権限のないユーザのアクセスや設定変更を防ぐセキュリティ機能をサポートしています。このセクションではコンソール接続で本スイッチにログインする方法を説明します。

注意 パスワードは大文字小文字を区別します。例えば、「S」と「s」は別の文字として認識されます。

スイッチに初めて接続すると、次のログイン画面が表示されます。

```
                        DES-3200-28 Fast Ethernet Switch
                             Command Line Interface

                                Firmware: Build 1.28.005
                      Copyright(C) 2010 D-Link Corporation. All rights reserved.
UserName:
```

図 4-1　コマンドプロンプト

注意 「Ctrl」キーと「R」を同時に押下すると、コンソール画面のリフレッシュをします。本コマンドはコンソール画面をリフレッシュするために、いつでも実行することができます。

初回接続する場合、「UserName」または「PassWord」は登録されていません。「UserName」と「PassWord」には何も入力せず、「Enter」キーを押します。
既に設定されている場合は、「UserName」と「PassWord」の両方を入力します。
「DES-3200-10:4#」、「DES-3200-18:4#」、「DES-3200-26:4#」、「DES-3200-28:4#」または「DES-3200-28F:4#」というコマンドプロンプトが表示されます。

注意 はじめにログインしたユーザが自動的に管理者権限を取得します。少なくとも一つは管理者レベルのユーザカウントを登録することをお勧めします。

パスワード設定

本スイッチは、初期値としてユーザ名およびパスワードの設定はありません。はじめにユーザアカウントの作成を行います。定義済みの管理者レベルのユーザ名でログインすることでスイッチ管理ソフトウェアに接続できます。
はじめてログインした際に本スイッチに対する不正アクセスを防ぐために user name に対して必ず新しいパスワードを定義してください。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。
管理者レベルのアカウントを作成する手順は以下の通りです。

1. ログインプロンプトで「create account admin <user name>」を入力し、「Enter」キーを押下します。
2. パスワード入力プロンプトが表示されます。管理者アカウントに使用する <password> を入力し、「Enter」キーを押下します。
3. 確認のために再度同じ入力プロンプトが表示されます。同じパスワードを入力し、「Enter」キーを押下します。
4. 管理者アカウントが正しく登録されると、画面に「Success.」と表示されます。

注意 パスワードの大文字、小文字は区別されます。ユーザ名、パスワードのどちらも 15 文字以内の半角英数字を指定してください。

以下は新しい管理者レベルユーザに「newmanager」を指定する手順の例です。

```
DES-3200-28F:4#create account admin newmanager
Command: create account admin newmanager

Enter a case-sensitive new password:********
Enter the new password again for confirmation:********
Success.

DES-3200-28F:4#
```

図 4-2　newmanager を指定する手順画面

注意 CLI 設定コマンドは動作中の設定だけが変更され、本スイッチを再起動するとその設定内容は消去されます。フラッシュメモリ（NV-RAM）にすべての変更内容を保存するためには「save」コマンドを投入して稼動中のコンフィグレーションファイルを、スタートアップ設定に格納する必要があります。

SNMP 設定

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

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

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

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

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

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

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

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

個別のユーザや SNMP マネージャグループに SNMP バージョン 3 を使用すると、特定の SNMP 管理機能を許可または制限できるようになります。そのような管理機能の可否は、各 MIB に関連付けられる OID（Object Identifier）を使用して定義します。SNMP バージョン 3 では SNMP メッセージを暗号化することにより、さらに強固なセキュリティを実現できます。スイッチでの SNMP バージョン 3 の設定方法については 42 ページの「IP Address Settings（IP アドレス設定）」をご参照ください。

トラップ

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

MIB

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

IP アドレスの割り当て

各スイッチに対して、SNMP ネットワークマネージャまたは他の TCP/IP アプリケーション（例 : BOOTP、TFTP）と通信するために IP アドレスを割り当てる必要があります。

本スイッチの IP アドレスの初期値は 10.90.90.90 です。

この IP アドレスはご使用のネットワークのアドレス計画に基づいて変更することができます。

また、本スイッチには、出荷時に固有の MAC アドレスが割り当てられており、この MAC アドレスは変更できません。MAC アドレスは、CLI で「show switch」コマンドを入力することにより、以下のように参照することができます。

```
DES-3200-28:4#show switch
Command: show switch

Device Type         : DES-3200-28 Fast Ethernet Switch
MAC Address         : 00-63-32-28-01-01
IP Address          : 10.81.17.4 (Manual)
VLAN Name           : default
Subnet Mask         : 255.0.0.0
Default Gateway     : 0.0.0.0
Boot PROM Version   : Build 1.00.006
Firmware Version    : Build 1.28.005
Hardware Version    : B1
System Name         :
System Location     :
System Uptime       : 0 days, 0 hours, 22 minutes, 45 seconds
System Contact      :
Spanning Tree       : Disabled
GVRP                : Disabled
IGMP Snooping       : Disabled
VLAN Trunk          : Disabled
802.1X              : Disabled
Telnet              : Enabled (TCP 23)
Web                 : Enabled (TCP 80)
RMON                : Disabled
SSH                 : Disabled

CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

図 4-3　show switch コマンドによる表示画面

本スイッチの MAC アドレスは、Web ベース管理インタフェースの「Device Information」画面にも表示されます。

本スイッチの IP アドレスは、Web ベース管理インタフェースの使用前に設定する必要があります。スイッチの IP アドレスは BOOTP または DHCP プロトコルを使用して自動的に取得することもできます。この場合は、スイッチに割り当てた本来のアドレスを知っておく必要があります。

IP アドレスはコンソールから CLI を使用して、以下のように設定することができます。

コマンドラインプロンプトの後に、以下のコマンドを入力します。

config ipif System ipaddress xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy

xxx.xxx.xxx.xxx は IP アドレスを示し、System と名づけた IP インタフェースに割り当てられます。**yyy.yyy.yyy.yyy** は対応するサブネットマスクを示しています。

または **config ipif System ipaddress xxx.xxx.xxx.xxx/z** と入力することもできます。**xxx.xxx.xxx.xxx** は IP インタフェースに割り当てられた IP アドレスを示し、**z** は CIDR 表記で対応するサブネット数を表します。

本スイッチ上の「System」という名前の IP インタフェースに IP アドレスとサブネットマスクを割り当てて、管理ステーションから本スイッチの Telnet または Web ベースの管理エージェントに接続します。

```
DES-3200-28:4#config ipif System ipaddress 10.90.90.91/255.0.0.0
Command: config ipif System ipaddress 10.90.90.91/8

Success.

DES-3200-28:4#
```

図 4-4　スイッチへの IP アドレス割り当て時の表示画面

上記例では、スイッチに IP アドレス「10.24.22.100」とサブネットマスク「255.0.0.0」を割り当てています。CIDR 表記（10.24.22.100/8）でのアドレス指定も可能です。「Success.」というメッセージにより、コマンドの実行が成功したことが確認できます。スイッチのアドレス設定が終了すると、Telnet での CLI、または Web ベースによる管理を開始することができます。

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
- Web マネージャの画面構成
- Web マネージャのメニュー画面構成

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（以降、Web マネージャと記載）経由で管理、設定およびモニタできます。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。

Web マネージャ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。つまり、Web マネージャ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。

図 5-1　URL の入力画面

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あわせるか、本スイッチを端末側の IP インタフェースにあわせてください。

注意　安全のためにネットワークに接続する前にユーザ名とパスワードを必ず設定してください。

以下のユーザ認証画面が表示されます。

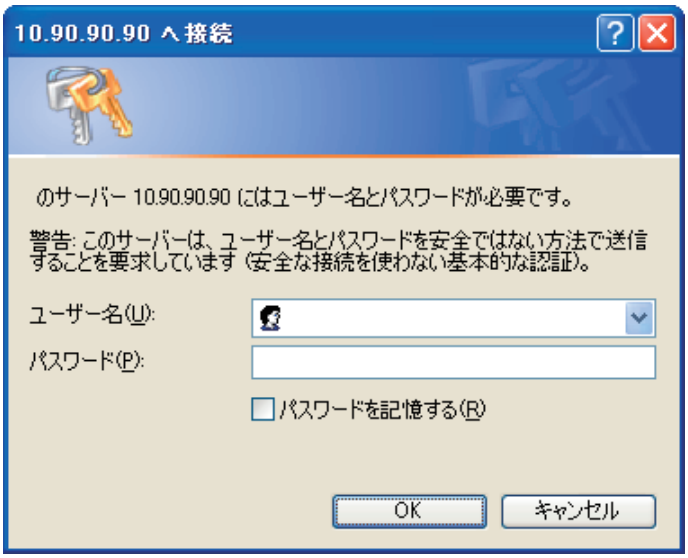


図 5-2　ログイン画面

「ユーザー名」と「パスワード」を空白のまま「OK」をクリックします。Web ベースユーザインタフェースに接続します。
CLI でユーザ名、パスワードを既に設定している場合は、設定した項目を入力します。

Web マネージャの画面構成

Web マネージャでスイッチの設定または管理画面にアクセスしたり、パフォーマンス状況やシステム状態をグラフィック表示で参照できます。

Web マネージャのメイン画面について

Web マネージャのメイン画面は 3 つのエリアで構成されています。

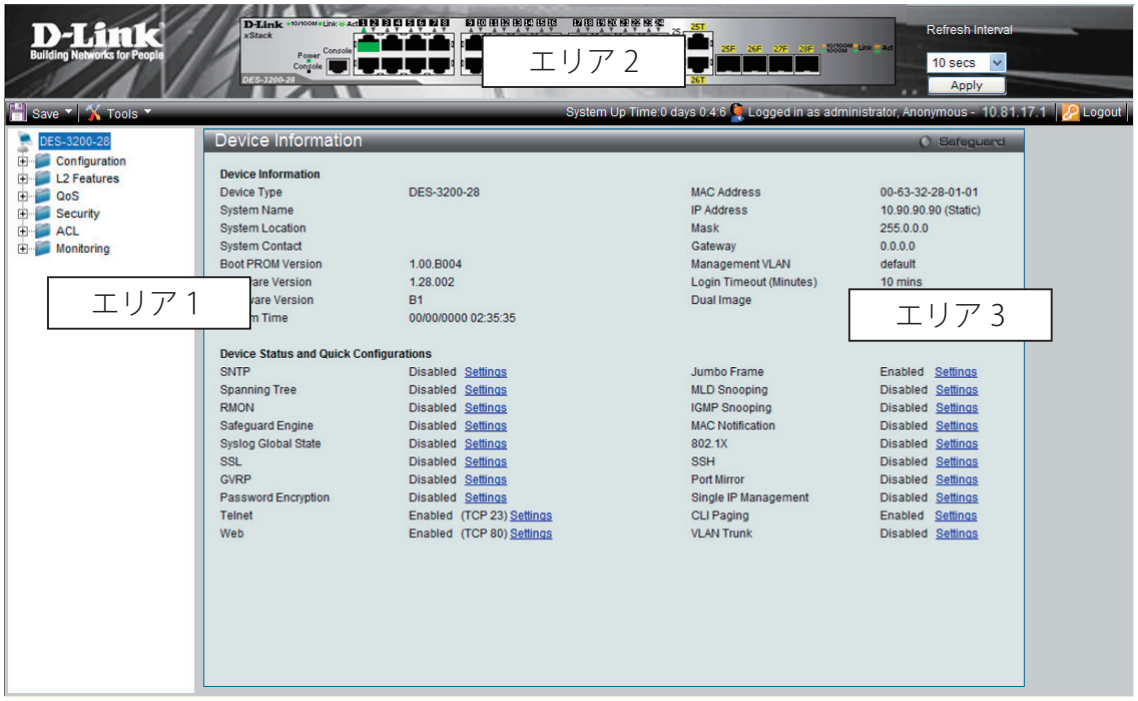


図 5-3　Web マネージャのメインページ

エリア	機能
エリア 1	表示するメニューまたは画面を選択します。メニューアイコンを開いて、ハイパーリンクしたメニューボタンの表示や、それらを格納するサブメニューを表示します。D-Link のロゴをクリックすると D-Link のホームページに接続します。
エリア 2	本スイッチの前面パネルをリアルタイムに近い画像で表示します。本エリアにはスイッチのポートや拡張モジュール、各ポートの状態、デュプレックスモード、フローコントロールの状態などが、指定したモードにより表示できます。
エリア 3	選択したスイッチ情報の表示と設定データの入力を行えます。

注意　スイッチ設定を変更した場合、以下で説明する Web マネージャの「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。

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は次ページで説明します。

メインメニュー	サブメニュー	説明	参照ページ
Configuration	Device Information	スイッチの主な設定情報を表示します。	39 ページ
	System Information	スイッチの基本情報を表示します。	40 ページ
	Serial Port Settings	ボーレートの値と自動ログアウト時間を調整します。	41 ページ
	IP Address Settings	IP アドレス設定を変更します。	42 ページ
	IPv6 Interface Settings	IPv6 インタフェース設定を行います。	44 ページ
	IPv6 Route Settings	IPv6 ルートテーブルのアドレスを設定します。	44 ページ
	IPv6 Neighbor Settings	IPv6 Neighbor の設定を行います。	45 ページ
	Port Configuration	物理ポートの属性やプロパティなどの設定および情報を表示します。	46 ページ
	Static ARP Settings	IP アドレスを物理的なアドレスに変換し、IP アドレスと MAC アドレスを対応させます。	48 ページ
	User Accounts	ユーザおよびユーザの権限を設定します。	49 ページ
	System Log Configuration	フラッシュメモリにスイッチのログを保存する方法、Syslog サーバの設定を行います。	50 ページ
	DHCP Relay	DHCP リレーのグローバル設定、DHCP サーバの登録を行います。	52 ページ
	DHCP Auto Configuration Settings	DHCP 自動設定機能を有効 / 無効にします。	55 ページ
	MAC Address Aging Time	MAC アドレスエージングタイムを設定します。	55 ページ
	Web Settings	スイッチに Web ステータスを設定します。	56 ページ
	Telnet Settings	スイッチに Telnet 設定をします。	56 ページ
	Password Encryption	スイッチのパスワードの暗号化設定をします。	57 ページ
	CLI Paging Settings	コマンドラインインタフェースの改頁処理を設定します。	57 ページ
	Firmware Information	スイッチに格納されているファームウェアイメージの情報の確認、起動ステータスの設定の削除を行います。	58 ページ
	SNTP Settings	本製品に時刻設定をします。	59 ページ
	SMTP Settings	問題が発生した場合に設定した E-mail アドレスに従ってスイッチのログファイルを送信する SMTP サーバを設定します。	61 ページ
	MAC Notification Settings	MAC 通知機能の設定を行います。	63 ページ
	SNMP Settings	SNMP 設定を行います。	63 ページ
	Time Range Settings	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。	71 ページ
	Single IP Management	シングル IP マネジメント機能を設定します。	72 ページ
	Gratuitous ARP	Gratuitous ARP の設定を行います。	82 ページ
	ARP Spoofing Prevention Settings	パケットコンテンツ ACL を使用して、ARP スプーフィング攻撃を防止します。	83 ページ
	PPPoE Circuit ID Insertion Settings	受信した PPPoE Discovery および Request パケットへの Circuit ID タグの挿入および削除を行います。	84 ページ

メインメニュー	サブメニュー	説明	参照ページ
L2 Features	Jumbo Frame	ジャンボフレーム機能を有効 / 無効にします。	85 ページ
	802.1Q Static VLAN	802.1Q スタティック VLAN 設定を行います。	92 ページ
	QinQ	Q-in-Q 機能を有効または無効にします。	95 ページ
	802.1v Protocol VLAN	802.1v プロトコル VLAN 設定を行います。	97 ページ
	VLAN Trunk Settings	多くの VLAN ポートを集約して VLAN トランクを作成します。	100 ページ
	GVRP Settings	VLAN 構成情報を共有するために GVRP 設定を行います。	101 ページ
	Asymmetric VLAN Settings	Asymmetric VLAN を設定します。	102 ページ
	MAC-based VLAN Settings	MAC ベース VLAN を設定します。	102 ページ
	PVID Auto Assign Settings	PVID 自動割り当てを設定します。	103 ページ
	Port Trunking	ポートトランキング設定を行います。	103 ページ
	LACP Port Settings	ポートトランキンググループを設定します。	106 ページ
	Traffic Segmentation	トラフィックフローの分割設定を行います。	107 ページ
	L2PT Settings	レイヤ 2 プロトコルトンネリング設定を行います。	107 ページ
	BPDU Protection Settings	ポートに BPDU 防止機能を設定します。	108 ページ
	IGMP Snooping	IGMP Snooping 機能を設定します。	109 ページ
	MLD Snooping Settings	MLD Snooping 機能を設定します。	117 ページ
	Port Mirror	ポートミラーリングの設定を行います。	120 ページ
	Loopback Detection Settings	ループバック検知機能の設定を行います。	121 ページ
	Spanning Tree	スパニングツリープロトコルの設定を行います。	122 ページ
	Forwarding & Filtering	ユニキャスト / マルチキャストフォワーディングとフィルタリングの設定を行います。	131 ページ
	NLB Settings	ネットワークロードバランシング設定を行います。	133 ページ
	LLDP	LLDP 設定を行います。	134 ページ
	Ethernet OAM	OAM 設定を行います。	138 ページ
	CFM	CFM 設定を行います。	140 ページ
	ERPS Settings	イーサネットリングプロテクション設定を有効にします。	148 ページ
QoS	Bandwidth Control	送信と受信のデータレートを制限します。	152 ページ
	Traffic Control	ストームコントロールの有効 / 無効の設定、およびマルチキャスト、ブロードキャストストームのしきい値を調整します。	153 ページ
	Queue Bandwidth Control Settings	キュー帯域制御の設定を行います。	155 ページ
	802.1p Default Priority	ポート単位にプライオリティを割り当てます。	156 ページ
	802.1p User Priority	クラス（キュー）にのプライオリティタグの割り当てをします。	156 ページ
	QoS Scheduling Settings	QoS スケジューリングを設定します。	157 ページ
	Priority Mapping	指定ポートにプライオリティマッピングを設定します。	157 ページ
	TOS Mapping	TOS マッピングの設定を行います。	158 ページ
	DSCP Mapping	DSCP Mapping を設定します。	158 ページ
Security	Safeguard Engine	セーフガードエンジンの設定を行います。	159 ページ
	Trusted Host	リモートのスイッチ管理用トラストホストを設定します。	161 ページ
	IP-MAC-Port Binding	IP アドレスと MAC アドレスを結合し、レイヤ間通信を行います。	161 ページ
	Port Security	ダイナミックな MAC アドレス学習をロックします。	166 ページ
	802.1X	ポート単位の 802.1X 認証を設定します。	168 ページ
	SSL Settings	証明書の設定、暗号スイートの設定を行います。	179 ページ
	SSH	SSH サーバ、SSH アルゴリズム、SSH ユーザ認証の設定を行います。	181 ページ
	Access Authentication Control	TACACS/XTACACSTACACS+/RADIUS 認証の設定を行います。	184 ページ
	MAC-based Access Control	MAC アドレス認証機能を設定します。	191 ページ
	DoS Prevention Settings	ハッカーや不正な送信元からの DoS（ Denial Of Service）攻撃を軽減する DoS 攻撃防止設定を行います。	194 ページ
	DHCP Server Screening	DHCP サーバスクリーニング機能を設定します。	195 ページ

メインメニュー	サブメニュー	説明	参照ページ
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。	197 ページ
	Access Profile List	パケットヘッダに含まれる情報に基づくパケット転送可否の基準を設定するプロファイルを設定します。	199 ページ
	CPU Access Profile List	CPU インタフェースフィルタリング機能を設定します。	215 ページ
	ACL Finder	ACL エントリを検索します。	229 ページ
	ACL Flow Meter	フローごとの帯域幅制御設定を行います。	230 ページ
Monitoring	Cable Diagnostic	ケーブルの品質やエラーの種類を診断します。	232 ページ
	CPU Utilization	CPU 使用率を表示します。	233 ページ
	Port Utilization	ポートの帯域使用率を表示します。	234 ページ
	Packet Size	受信パケット数を表示します。	235 ページ
	Memory Utilization	DRAM とフラッシュのメモリ使用率の情報を表示します。	236 ページ
	Packets	パケット統計情報を表示します。	237 ページ
	Errors	エラー統計情報を表示します。	241 ページ
	Port Access Control	802.1X 統計情報をポートごとに表示します。	244 ページ
	Browse ARP Table	スイッチ上の現在の ARP エントリを表示します。	252 ページ
	Browse VLAN	各ポートの VLAN ステータスを VLAN ごとに表示します。	252 ページ
	IGMP Snooping	IGMP Snooping 設定を表示します。	253 ページ
	MLD Snooping	MLD Snooping 設定を表示します。	254 ページ
	LLDP	LLDP 統計情報を表示します。	256 ページ
	Ethernet OAM	イーサネット OAM イベントログ情報と統計情報を表示します。	257 ページ
	CFM	MEP によって検出された障害状態、CFM ポート MP リストを表示します。	259 ページ
	Mac-based Access Control Authentication State	MAC ベースアクセスコントロールの認証情報を表示します。	261 ページ
	Browse Session Table	最後に起動してからの管理セッションを表示します。	261 ページ
	MAC Address Table	ダイナミック MAC アドレスフォワーディングテーブルを表示します。	262 ページ
	System Log	ヒストリログを表示します。	263 ページ
Save	Save Configuration	スイッチのメモリにコンフィグレーションを保存します	264 ページ
	Save Log	スイッチのメモリにログを保存します	265 ページ
	Save All	スイッチのメモリにコンフィグレーションとログを保存します	265 ページ
Tools	Configuration File Upload & Download	コンフィグレーションファイルのアップロードまたはダウンロードアップを行います。	266 ページ
	Upload Log File	スイッチのヒストリと攻撃ログを TFTP サーバにアップロードします。	266 ページ
	Reset	工場出荷時設定に戻し、メモリに保存します。	266 ページ
	Ping Test	スイッチとネットワーク上の他のノードとの接続性を確認します。	267 ページ
	Download Firmware	スイッチのファームウェアダウンロードを行います。	268 ページ
	Reboot System	スイッチの再起動を行います。	268 ページ

第 6 章　Configuration（スイッチの主な設定）

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

サブメニュー	説明	参照ページ
Device Information（デバイス情報）	スイッチの主な設定情報を表示します。	39 ページ
System Information（システム情報）	スイッチの基本情報を表示します。	40 ページ
Serial Port Settings（シリアルポート設定）	ボーレートの値と自動ログアウト時間を調整します。	41 ページ
IP Address Settings（IP アドレス設定）	IP アドレス設定を変更します。	42 ページ
IPv6 Interface Settings（IPv6 インタフェース設定）	IPv6 インタフェース設定を行います。	44 ページ
IPv6 Route Settings（IPv6 ルートテーブル設定）	IPv6 ルートテーブルのアドレスを設定します。	44 ページ
IPv6 Neighbor Settings（IPv6 Neighbor 設定）	IPv6 Neighbor の設定を行います。	45 ページ
Port Configuration（ポート設定）	物理ポートの属性やプロパティなどの設定および情報を表示します。	46 ページ
Static ARP Settings（スタティック ARP 設定）	IP アドレスを物理的なアドレスに変換し、IP アドレスと MAC アドレスを対応させます。	48 ページ
User Accounts（ユーザアカウントの設定）	ユーザおよびユーザの権限を設定します。	49 ページ
System Log Configuration（システムログ構成）	フラッシュメモリにスイッチのログを保存する方法、Syslog サーバの設定を行います。	50 ページ
DHCP Relay（DHCP リレー）	DHCP リレーのグローバル設定、DHCP サーバの登録を行います。	52 ページ
DHCP Auto Configuration Settings（DHCP 自動設定）	DHCP 自動設定機能を有効 / 無効にします。	55 ページ
MAC Address Aging Time（MAC アドレスエージングタイム）	MAC アドレスエージングタイムを設定します。	55 ページ
Web Settings（Web 設定）	スイッチに Web ステータスを設定します。	56 ページ
Telnet Settings（Telnet 設定）	スイッチに Telnet 設定をします。	56 ページ
Password Encryption（パスワードの暗号化）	スイッチのパスワードの暗号化設定をします。	57 ページ
CLI Paging Settings（CLI ページング設定）	コマンドラインインタフェースの改頁処理を設定します。	57 ページ
Firmware Information（ファームウェア情報）	スイッチに格納されているファームウェアイメージの情報の確認、起動ステータスの設定の削除を行います。	58 ページ
SNTP Settings（SNTP 設定）	本製品に時刻設定をします。	59 ページ
SMTP Settings（SMTP 設定）	問題が発生した場合に設定した E-mail アドレスに従ってスイッチのログファイルを送信する SMTP サーバを設定します。	61 ページ
MAC Notification Settings（MAC 通知設定）	MAC 通知機能の設定を行います。	63 ページ
SNMP Settings（SNMP 設定）	SNMP 設定を行います。	63 ページ
Time Range Settings（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。	71 ページ
Single IP Management（シングル IP マネジメント設定）	シングル IP マネジメント機能を設定します。	72 ページ
Gratuitous ARP（Gratuitous ARP の設定）	Gratuitous ARP の設定を行います。	82 ページ
ARP Spoofing Prevention Settings（ARP Spoofing 防止設定）	パケットコンテンツ ACL を使用して、ARP スプーフィング攻撃を防止します。	83 ページ
PPPoE Circuit ID Insertion Settings（PPPoE Circuit ID の挿入）	受信した PPPoE Discovery および Request パケットへの Circuit ID タグの挿入および削除を行います。	84 ページ

Device Information（デバイス情報）

本画面は、ログインを行うと自動的に表示される画面で、スイッチの主な設定情報を確認できます。本画面に戻るためには「DES-3200-10、DES-3200-18、DES-3200-26、DES-3200-28、DES-3200-28F」フォルダをクリックします。本画面には、スイッチの「MAC Address」（工場による設定のため変更不可）、「Boot PROM Version」と「Firmware Version」、「Hardware Version」などが表示されます。これらの情報は、PROM やファームウェアの更新状況の把握や他のネットワークデバイスのアドレステーブルにスイッチの MAC アドレスを登録する際の確認などに便利です。さらに、スイッチの各機能の状態を表示し、現在のグローバルステータスにアクセス可能です。いくつかの機能は、各設定画面にリンクしており、本画面から接続できます。

図 6-1　Device Information 画面

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 160 文字以内）
System Contact	担当者名を表示します。（半角英数字 31 文字以内）
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。
Hardware Version	デバイスのハード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。 例 : 41days 2 hours 22 mins 5 seconds
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。
Management VLAN	デバイスに割り当てられた VLAN 名を表示します。
Login Timeout (Minutes)	ユーザが何もしなかった場合にデバイスがタイムアウトするまでの時間を表示します。初期値は 10（分）です。
Dual Image	デュアルイメージ機能（複数のファームウェアコードを実行せずにスイッチ内に保存する）のサポート状況を表示します。
Device Status and Quick Configurations	
SNTP	SNTP 機能の状態（有効 / 無効）を表示します。SNTP 設定にリンクします。
Spanning Tree	STP 機能の状態（有効 / 無効）を表示します。STP 設定にリンクします。
RMON	RMON（リモートモニタリング）機能を有効 / 無効にします
Safeguard Engine	Safeguard エンジン機能の状態（有効 / 無効）の表示と、Safeguard エンジンの設定へのショートカットです。
Syslog Global State	Syslog 機能をグローバルに有効 / 無効にします。初期値は無効です。
SSL	SSL（Secure Socket Layer）機能の状態（有効 / 無効）の表示と、SSL の設定へのショートカットです。
GVRP	GVRP（Group VLAN Registration Protocol）機能の状態（有効 / 無効）の表示と、GVRP の設定へのショートカットです。
Password Encryption	パスワードの暗号化機能を有効 / 無効にします。

項目	説明
Telnet	Telnet 機能の状態（有効 / 無効）の表示と、Telnet 設定へのショートカットです。
Web	Web ベースの管理機能を有効 / 無効にします。Web ベースの管理は初期値で有効になっています。無効に設定し、システムに適用すると、Web インタフェースによるシステム設定は行えなくなります。
Jumbo Frame	Jumbo Frame 機能の状態（有効 / 無効）の表示と、Jumbo Frame の設定へのショートカットです。
MLD Snooping	MLD Snooping 機能の状態（有効 / 無効）の表示と、MLD の設定へのショートカットです。
IGMP Snooping	IGMP Snooping 機能の状態（有効 / 無効）の表示と、IGMP の設定へのショートカットです。
MAC Notification	MAC 通知機能の状態（有効 / 無効）を表示します。MAC 通知設定にリンクします。
802.1x	802.1X 機能の状態（有効 / 無効）の表示と、802.1X の設定へのショートカットです。
SSH	SSH（Secure Shell Protocol）機能の状態（有効 / 無効）の表示と、SSH の設定へのショートカットです。
Port Mirror	ポートミラーリング機能の状態（有効 / 無効）の表示と、ポートミラーリングの設定へのショートカットです。
Single IP Management	SIM 機能の状態（有効 / 無効）を表示します。SIM 設定にリンクします。
CLIpaging	CLI ページング機能を有効 / 無効にします。
VLAN Trunk	VLAN トランク機能を有効 / 無効にします。

デバイスの機能設定の参照手順

1. 「Device Status and Quick Configurations」セクションのデバイスの機能を選択します。
2. 機能名の後の Setting をクリックし、選択したデバイスの機能の設定画面を表示します。「Apply」ボタンをクリックし、設定を適用します。

System Information（システム情報）

ここでは、スイッチの詳細情報を表示します。本画面には、「System Name」、「System Location」、「System Contact」などを入力し、スイッチの定義を行う際にも利用できます。また、スイッチの「MAC Address」（工場による設定のため変更不可）、「Firmware Version」、「Hardware Version」が表示されます。

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

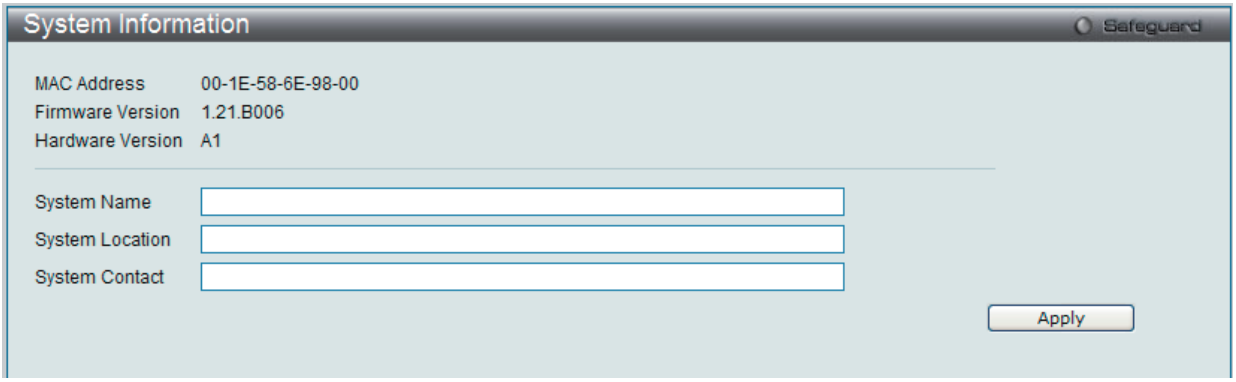


図 6-2　System Information 画面

画面には次の項目があります。

項目	説明
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。
Firmware Version	スイッチのファームウェアバージョンを表示します。
Hardware Version	スイッチのハードウェアバージョンを表示します。
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 160 文字以内）
System Contact	スイッチの管理者情報を入力します。

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。

Serial Port Settings（シリアルポート設定）

ボーレートの値と自動ログアウト時間を調整します。また、シリアルポート設定に関する情報を表示します。

スイッチにシリアルポート設定をするためには、**Configuration > Serial Port Settings** の順にメニューをクリックし、以下の画面を表示します。

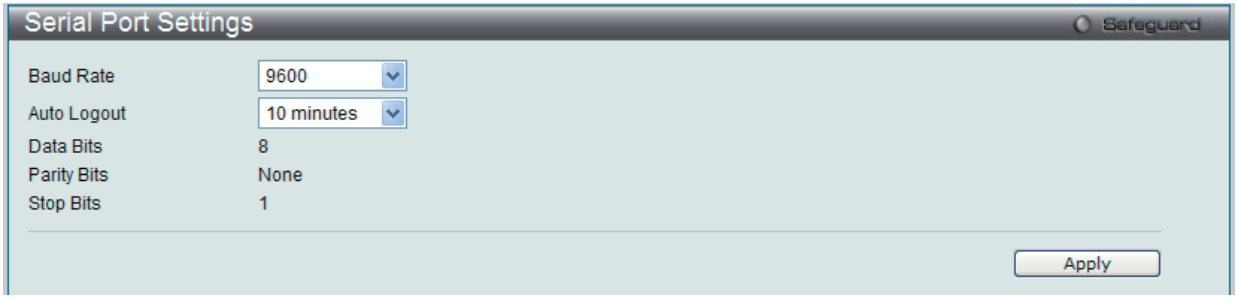


図 6-3　Serial Port Settings 画面

画面には次の項目があります。

項目	説明
Baud Rate	スイッチのシリアルポートのボーレートを指定します。9600、19200、38400、115200 から選択できます。 CLI インタフェースを使用したスイッチ接続には 9600（初期値）を指定します。
Auto Logout	コンソールインタフェースのログアウト時間を選択します。ここで設定した時間アイドル状態が続くと自動的にログアウトします。次のオプションから、選択します。2、5、10、15 minutes または Never（自動ログアウトを行わない）から選択できます。初期値 :10 minutes（分）。

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　シリアルポートのボーレートを設定すると、ボーレートは、直ちに適用され、保存されます。

IP Address Settings（IP アドレス設定）

IP 設定を変更します。

ネットワーク接続前に IP アドレスをコンソールより設定する必要があります。IP アドレスを設定または変更していない場合は、「DES-3200-10/18/26/28/28F CLI Reference Manual」の「INTRODUCTION」、または本マニュアルの 28 ページの「端末をコンソールポートに接続する」を参照し、設定を行ってください。

IP アドレス設定

スイッチの IP アドレス設定を変更します。

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

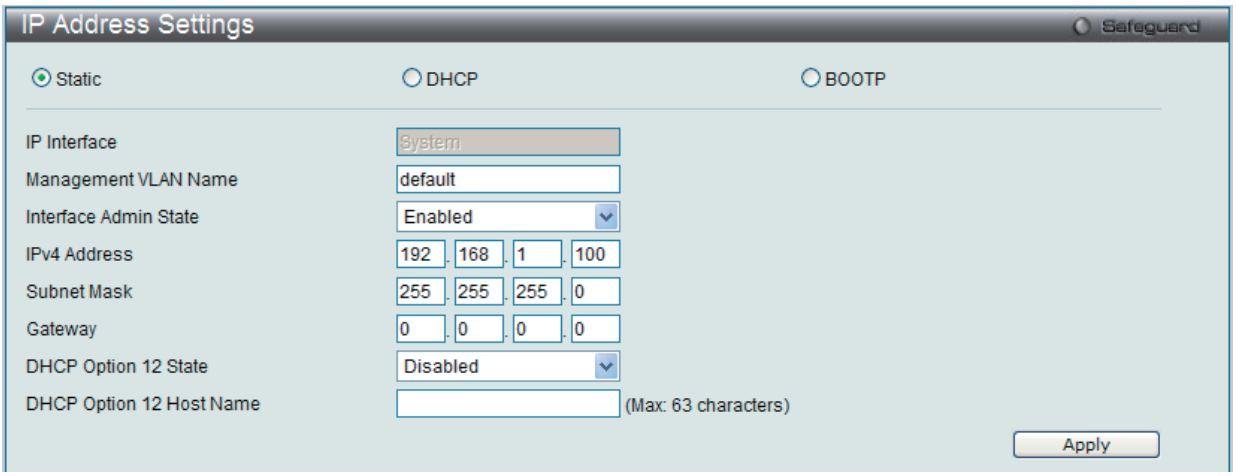


図 6-4　IP Address Settings 画面

スイッチの現在の IP 設定が表示されます。

本スイッチの IP アドレス、サブネットマスク、およびデフォルトゲートウェイを固定設定する方法を説明します。

1. 画面先頭のメニューから「Static」を選択します。

2. 適切な「IPv4 Address」と「Subnet Mask」を入力します。

3. 異なるサブネットから本スイッチにアクセスする場合は、「Gateway」の IP アドレスを入力します。同じサブネットからスイッチを管理する場合は、この項目内は初期値（0.0.0.0）のままにします。

4. 本スイッチに VLAN 設定をしていない場合は、デフォルトの「Management VLAN Name」を使用できます。本スイッチは、購入時に VLAN「default」が設定されていて、すべてのポートが所属しています。既に VLAN 設定をしている場合は、本スイッチにアクセスするためには、管理ステーションに接続しているポートが所属している VLAN の VLAN 名を入力します。

5. 設定が行われていない場合は、「Interface Admin State」プルダウンメニューから「Enabled」（有効）を選択します。

注意　工場出荷時は、IP アドレスに 10.90.90.90、サブネットマスクに 255.0.0.0、デフォルトゲートウェイに 0.0.0.0 が設定されています。

DHCP または BOOTP プロトコルを使用してスイッチに IP アドレス、サブネットマスクおよびデフォルトゲートウェイアドレスを割り当てるためには、画面先頭のメニューから「DHCP」または「BOOTP」を選択します。次回の再起動時に、ここで選択した方法により IP アドレスの割り当てが行われます。

IP アドレス設定用の項目およびオプション項目は以下の通りです。

項目	説明
Static	本スイッチの IPv4 アドレス、ネットマスク、およびデフォルトゲートウェイを固定設定します。アドレスはネットワーク管理者によって割り当てられる固有のアドレスを指定します。入力形式：xxx.xxx.xxx.xxx（x は 0 ～ 255 の数字）。本アドレスはネットワーク管理者により割り振られたネットワークに唯一のアドレスである必要があります。
DHCP	電源が投入されるとスイッチは DHCP ブロードキャストリクエストを送信します。DHCP プロトコルにより IP アドレス、ネットワークマスクおよびデフォルトゲートウェイは DHCP サーバにより割り当てられます。本オプションが選択されると、スイッチは初期設定や以前に登録された設定を使用する前に、DHCP サーバにアクセスし、これらの情報を取得します。
BOOTP	電源が投入されるとスイッチは BOOTP ブロードキャストリクエストを送信します。BOOTP プロトコルにより IP アドレス、ネットワークマスクおよびデフォルトゲートウェイは BOOTP サーバにより割り当てられます。本オプションが選択されると、スイッチは初期設定や以前に登録された設定を使用する前に、BOOTP サーバにアクセスし、これらの情報を取得します。
IP Interface	IP アドレスがに割り当てられている現在の IP インタフェース。

項目	説明
Management VLAN Name	管理ステーションが、TCP/IP（Web マネージャまたは Telnet 経由）によるスイッチ管理を行う時に使用する VLAN 名を入力します。本項目で登録した VLAN 以外に所属する管理ステーションからは、帯域内管理を行うことができません。ただし、そのアドレスが 161 ページの「Trusted Host（トラストホスト）」で登録されている場合は可能になります。スイッチにまだ VLAN が登録されていない場合は、スイッチ上のすべてのポートはデフォルト VLAN に所属しています。経由のインバンド「Security IP Management」テーブルにはエントリはないため、管理 VLAN が設定されるまで、または管理ステーションの IP アドレスが登録されるまでは、スイッチに接続している全管理ステーションがスイッチにアクセスできます。
Interface Admin State	「Enabled」(有効)/「Disabled」(無効) にします。IP アドレスを設定する場合は、「Enabled」を設定する必要があります。
IPv4 Address	IPv4 アドレスを入力します。本スイッチの IP アドレスの初期値は 10.90.90.90 です。
Subnet Mask	本スイッチのサブネットを指定します。入力形式：xxx.xxx.xxx.xxx（x は 0 ～ 255 の数字）。クラス A ネットワークには 255.0.0.0、クラス B ネットワークには 255.255.0.0、クラス C ネットワークには 255.255.255.0 を入力します。カスタムサブネットマスクも入力できます。
Gateway	所属するサブネット外の宛先アドレスを持つパケットの送信先。通常 IP ゲートウェイの役割をするルータやホストのアドレスを指定します。ご使用のネットワークがイントラネットの一部でない場合、またはローカルネットワーク外からのスイッチへのアクセスを許可しない場合は、本項目はそのままにします。
DHCP Option 12 State	DHCP オプション 12 を有効または無効にします。
DHCP Option 12 Host Name	オプション 12 に使用されるホスト名を入力します。最大 63 文字まで許可されます。

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。

コンソールインタフェースを使用したスイッチの IP アドレス設定

各スイッチに IP アドレスを設定し、設定した IP アドレスを使用して SNMP ネットワークマネージャや TCP/IP アプリケーション（例えば BOOTP、TFTP など）との通信をします。本スイッチの IP アドレスの初期値は 10.90.90.90 です。初期値の IP アドレスはご使用のネットワークアドレス体系に合うように変更してください。

IP アドレスは、Web マネージャを使用する前に設定してください。本スイッチの IP アドレスは、BOOTP または DHCP プロトコルを使用して自動的に設定することもできます。その場合は、スイッチに割り当てた本来のアドレスを知っておく必要があります。コンソールポートから Command Line Interface（CLI）を使用する設定方法は以下の通りです。

・コマンドラインプロンプトの後に、以下のコマンドを入力します。
`config ipif System ipaddress xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy`
（xxx.xxx.xxx.xxx: System という名前のインタフェースに割り当てる IP アドレス、yyy.yyy.yyy.yyy: 対応するサブネットマスク）

・**`config ipif System ipaddress xxx.xxx.xxx.xxx/z`** とコマンド入力することも可能です。
（xxx.xxx.xxx.xxx: System という名前のインタフェースに割り当てる IP アドレス、z: CIDR 表記によるサブネットマスク数）

スイッチ上の「System」と名付けた IP インタフェースには IP アドレスとサブネットマスクを割り当て、管理ステーションをスイッチの Telnet または Web ベース管理エージェントに接続するために使用します。

「Success.」というメッセージにより、コマンドの実行が成功したことを確認できます。スイッチのアドレス設定が終了すると、Telnet での CLI、または Web ベースによる管理を開始することができます。

IPv6 Interface Settings（IPv6 インタフェース設定）

スイッチの IPv6 インタフェース設定を行います。

Configuration > IPv6 Interfaces 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。

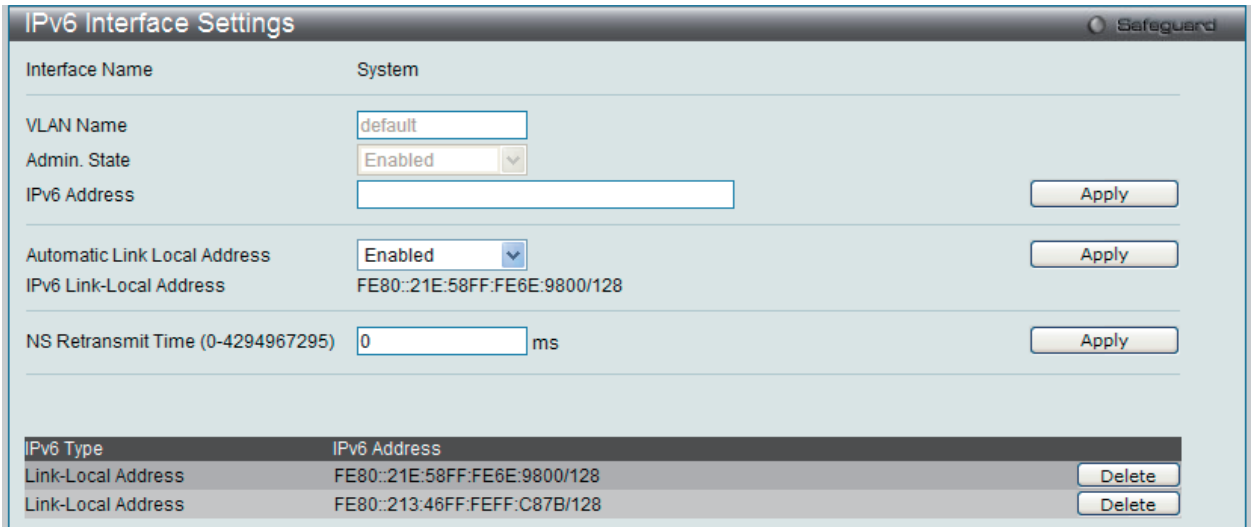


図 6-5　IPv6 Interface Settings 画面

Web マネージャにより、スイッチの現在の IPv6 インタフェース設定が表示されます。

IPv6 インタフェースの設定

1. 「IPv6 Address」を入力し、「Apply」ボタンをクリックします。
2. 新しいエントリが上記画面下半分に表示されます。

IPv6 インタフェースの削除

1. 本画面の下部のテーブルで、削除するエントリの「Delete」ボタンをクリックします。

以下の項目は画面の上部にあり、設定および参照できます。

項目	説明
Interface Name	IPv6 インタフェース名を入力します。
VLAN Name	IPv6 インタフェースの VLAN 名を入力します。
Admin. State	プルダウンメニューを使用して、ポート状態を「Enabled」（有効）または「Disabled」（無効）にします。
IPv6 Address	編集するインタフェースの IPv6 アドレスを入力します。
Automatic Link Local Address	「Enabled」（有効）/「Disabled」（無効）にします。外部ソースのネットワークアドレス指定情報が無効の場合、有効にします。設定後、隣接する「Apply」ボタンをクリックします。
NS Retransmit time (0-4294967295)	Neighbor ソリシテーションの再送タイマ (ミリ秒)。0-4294967295 の範囲で指定します。初期値は 0 です。

画面上のセクションにある「Apply」ボタンをクリックし、設定内容を適用してください。

IPv6 Route Settings（IPv6 ルートテーブル設定）

スイッチの IPv6 ルートテーブルのアドレスを設定します。

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

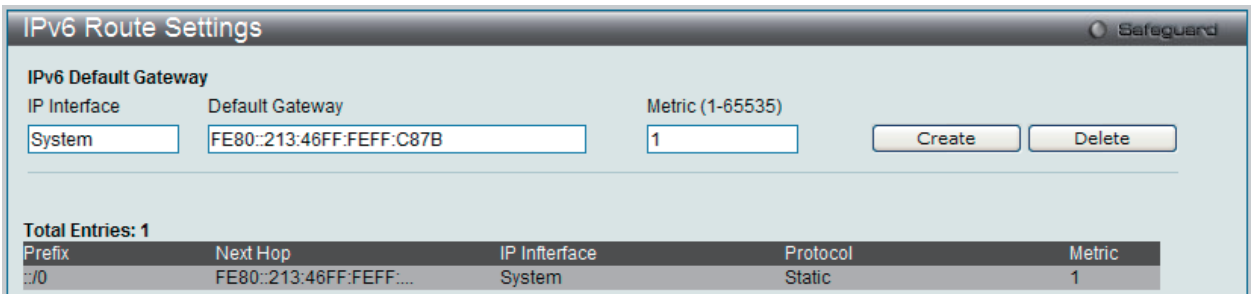


図 6-6　IPv6 Route Settings 画面

「IP Interface」に IP インタフェース、「Default Gateway」に IPv6 アドレスを指定して、「Create」ボタンをクリックします。さらに、「Metric」を 1-65535 範囲で入力することができます。新しい IPv6 ルートが画面下半分に表示されます。

IPv6 Neighbor Settings（IPv6 Neighbor 設定）

スイッチの IPv6 Neighbor 設定を行います。

Configuration > IPv6 Neighbor 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。

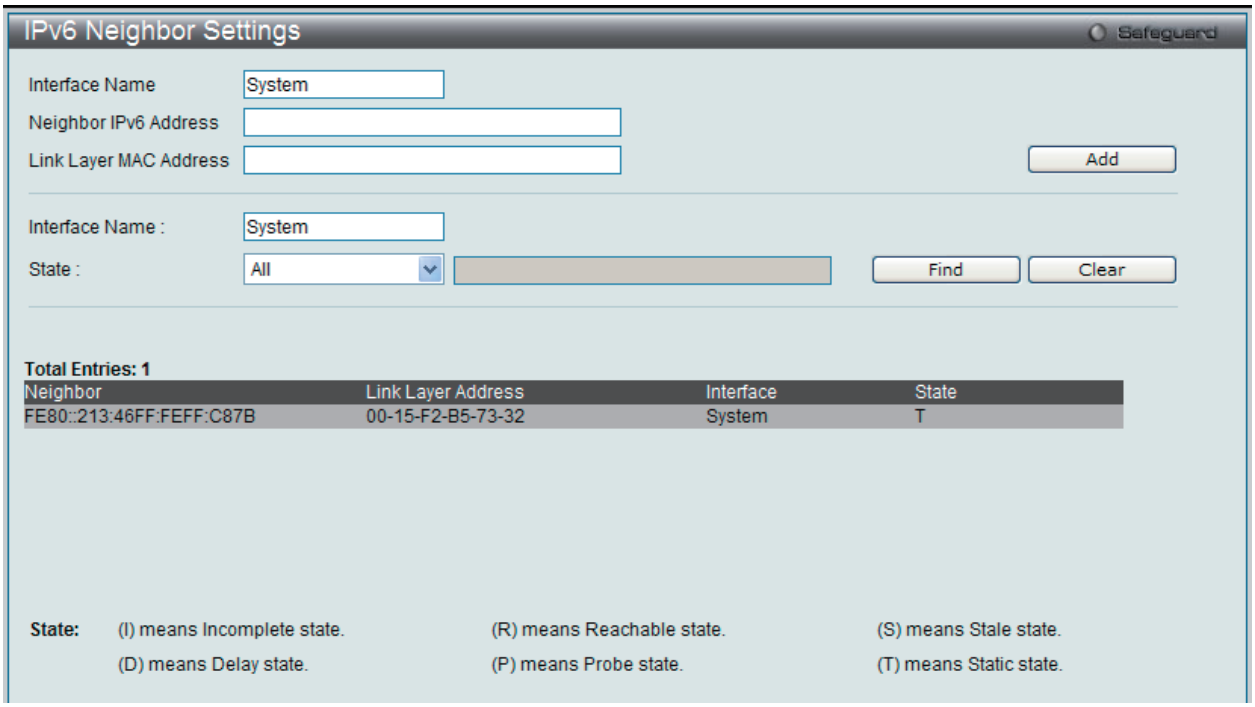


図 6-7　IPv6 Neighbor Settings 画面

スイッチの現在の IPv6 Neighbor 設定が表示されます。

IPv6 Neighbor の新規登録

「Interface Name」、「Neighbor IPv6 Address」および「Link Layer MAC Address」を入力し、「Add」ボタンをクリックします。「State」には、「All」、「Address」、「Static」または「Dynamic」を設定します。

エントリの検索

「IPv6 Neighbor Settings」テーブルエントリを検索するには、「Interface Name」を入力し、画面中央の「State」を選択後、「Find」ボタンをクリックします。

エントリの削除

本画面の下部のテーブルに表示されているすべてのエントリを削除するには、「Clear」ボタンをクリックします。

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 Name	IPv6 Neighbor 名を入力します。スイッチにおける現在の全インタフェースに対して検索するには、画面の中央部分にある 2 個目の「Interface Name」欄で「All」を選択し、「Find」ボタンをクリックします。
Neighbor IPv6 Address	Neighbor の IPv6 アドレスを入力します。
Link Layer MAC Address	Link Layer の MAC Address を入力します。
State	「All」、「Address」、「Static」または「Dynamic」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。

Port Configuration（ポート設定）

Port Configuration フォルダには「Port Settings」、「Port Description Settings」、および「Port Error Disabled」の３つのメニューがあります。

Port Settings（スイッチのポート設定）

「State」、「Speed/Duplex」、「Flow Control」、「Address Learning」、「Medium Type」、および「MDIX」を含むさまざまなポート設定をスイッチに行うことができます。

ポートの設定や情報の表示を行うには、**Configuration > Port Configuration > Port Settings** の順にメニューを選択し、以下の画面を表示します。

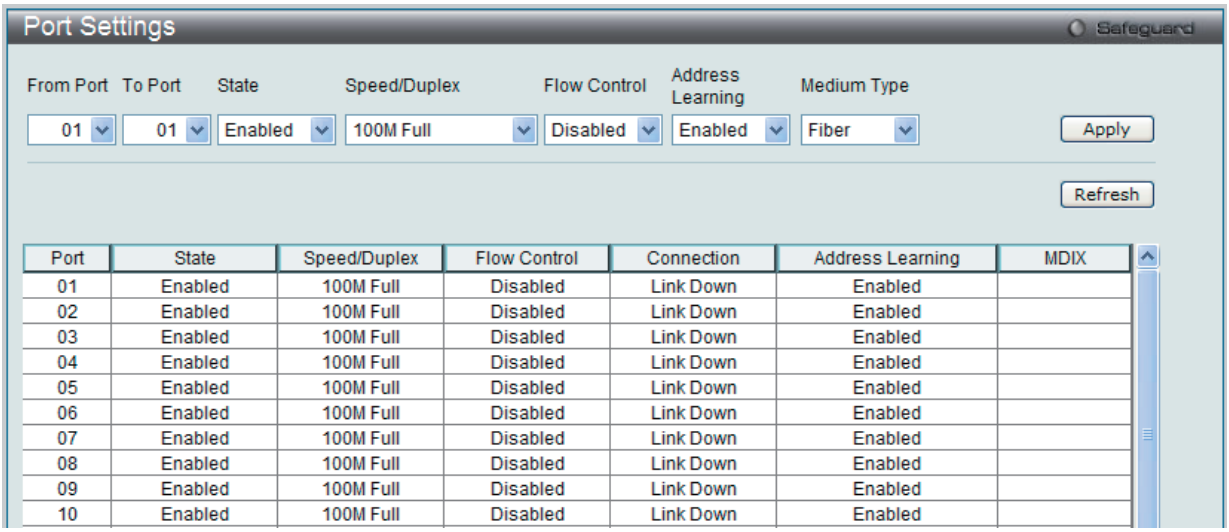


図 6-8　Port Settings 画面

「From Port」と「To Port」のプルダウンメニューからポートまたはポートの範囲を選択します。
残りのプルダウンメニューから以下に示す項目について設定を行います。

項目	説明
State	指定したポートまたはポート範囲を「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
Speed/ Duplex	ポートの速度および全二重 / 半二重の指定を行います。「Auto」は、10/100Mbps のデバイス間（全二重または半二重モード時）のオートネゴシエーションを示します。「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 Half」、「10M Full」、「100M Half」、「100M Full」、「1000M Full_Master」、「1000M Full_Slave」、および「1000M Full」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。 次の２つのタイプ（1000M Full_Master、1000M Full_Slave）はギガビット接続設定ができます。ギガビット接続はフルデュプレックス接続だけをサポートしており、他の選択肢とは異なる特長を持っています。 1000M Full_Master（マスタ）および 1000M Full_Slave（スレーブ）項目は、ギガビット接続が可能なスイッチポートと他のデバイス間を 1000BASE-T で結ぶ接続を表示しています。マスタ設定（1000M Full_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することができます。さらに２つの接続している物理レイヤ間のマスタおよびスレーブを決定します。この関係は２つの物理レイヤ間のタイミングコントロールを確立するために必要です。タイミングコントロールはローカルソースによってマスタ物理レイヤ上に設定されます。スレーブ設定（1000M Full_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 Full_Master を設定するともう一方の接続は 1000M Full_Slave に設定する必要があります。それ以外の設定をすると両ポートともリンクダウンします。
Flow Control	各ポートのフローコントロール設定を選択します。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。 初期値は「Disabled」（フロー制御なし）です。
Address Learning	選択ポートにおける MAC アドレスの学習の有無を設定します。 • Enabled - 終点と始点 MAC アドレスをフォワーディングテーブルに自動的にリストアップします。 • Disabled - MAC アドレスはフォワーディングテーブルに手動で登録します。セキュリティや効率上の理由で使用されることがあります。フォワーディングテーブルに MAC アドレスを登録する方法については、131 ページの「Forwarding & Filtering（フォワーディングとフィルタリングの設定）」を参照してください。初期値は「Enabled」です。
Medium Type	本設定はコンボポートだけに適用します。コンボポートを設定する場合、使用する変換メディアのタイプを選択します。SFP ポートの場合は「Fiber」、10/100/1000BASE-T の場合は「Copper」を設定します。
MDIX	Auto MDI/MDIX の状態が表示されます。

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 Description Settings（ポート名設定）

本スイッチはポート説明機能をサポートしており、ユーザはスイッチ上のポートに名前をつけることができます。

Configuration > Port Configuration > Port Description 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。

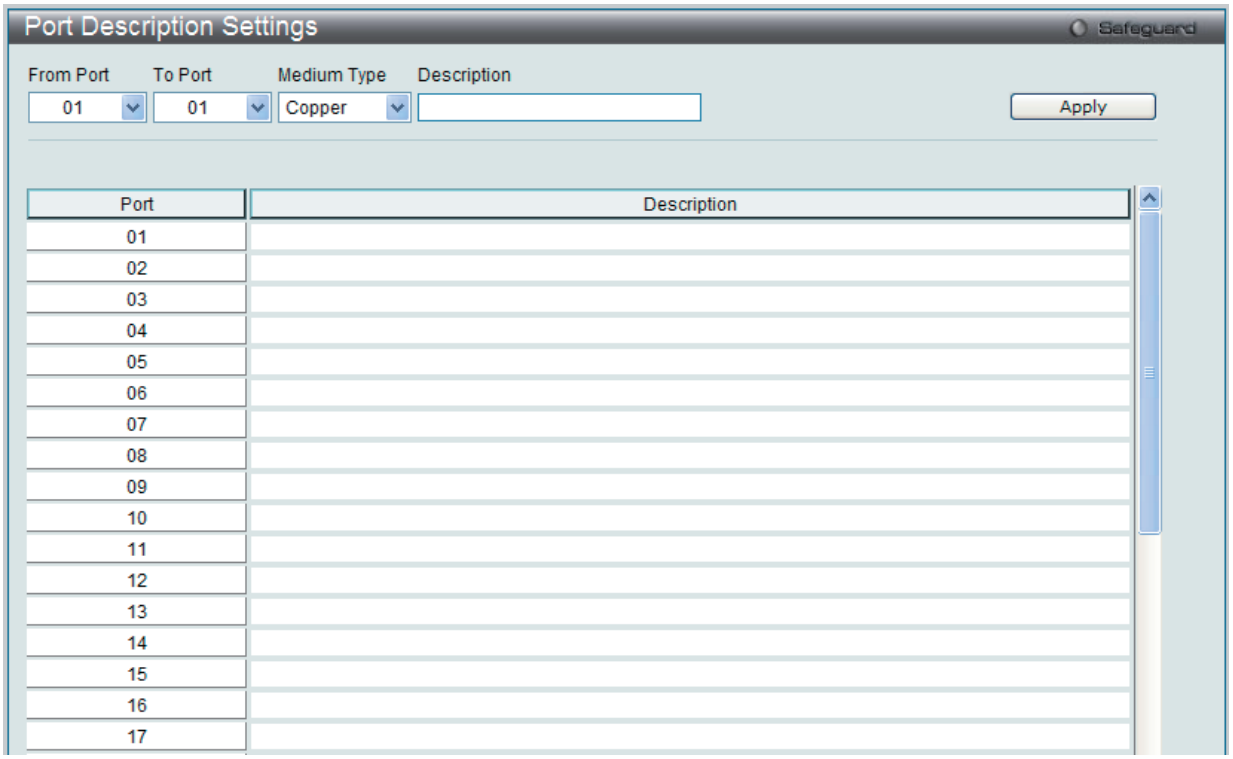


図 6-9　Port Description Settings 画面

ポート、またはポート範囲を「From」と「To」プルダウンメニューから選択し、それらのポートについての名前や説明を入力します。

以下の項目を使用して、設定します。

項目	説明
From Port / To Port	プルダウンメニューから、設定対象のポートまたはポート範囲を選択します。
Medium Type	Medium Type はコンボポートにだけ適用されます。コンボポートを設定する場合、使用している通信メディアのタイプを指定します。SFP ポートの場合は「Fiber」を指定し、10/100/1000BASE-T ポートの場合は「Copper」を指定します。設定結果は適応するスイッチポート番号欄に表示されます（Copper ポートは C、Fiber ポートは F）。
Description	ポートの説明文。

「Apply」ボタンをクリックすると、「Port Description」テーブルに追加されます。

Port Error Disabled（エラーによるポートの無効）

以下の画面では、接続が無効であるポートに関する情報（ストームコントロールの理由や接続ステータス）を表示します。

この画面を参照するためには、**Configuration > Port Configuration > Port Error Disabled** の順にメニューをクリックし、以下の画面を表示します。

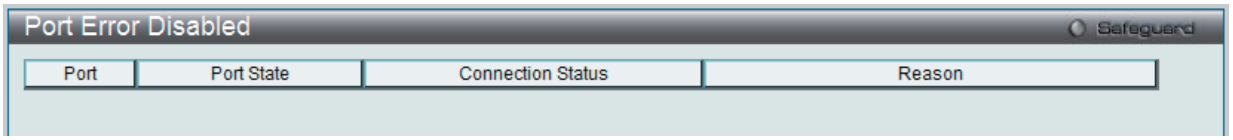


図 6-10　Port Error Disabled 画面

以下の項目が表示されます。

項目	説明
Port	エラーのために無効になっているポートを表示します。
Port State	現在のポートのステータス（「Enabled」または「Disabled」）を表示します。
Connection Status	各ポートのアップリンク状況（「Enabled」または「Disabled」）を表示します。
Reason	ストームコントロールのためにポートが無効になった理由を表示します。

Static ARP Settings（スタティック ARP 設定）

ARP（Address Resolution Protocol）は、IP アドレスを物理的なアドレスに変換し、IP アドレスと MAC アドレスを対応させます。ここでは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。
スタティックエントリを ARP テーブルに定義します。スタティックエントリを定義する場合、継続的なエントリを入力し、IP アドレスを MAC アドレスに変換するために使用します。以下の手順で ARP 情報を定義します。

1. **Configuration > Static ARP Settings** の順にクリックし、以下の画面を表示します。

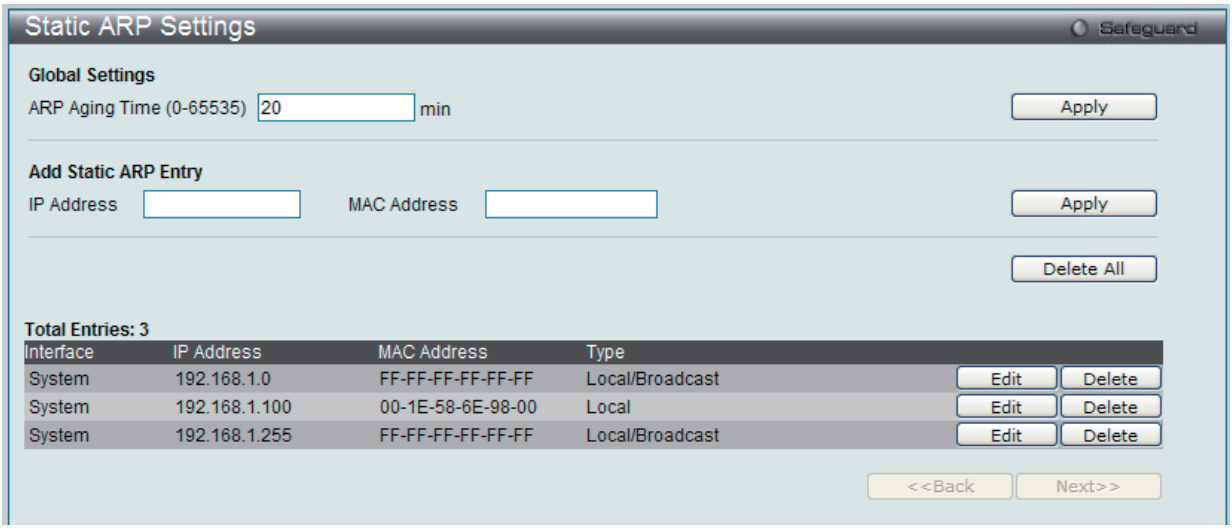


図 6-11　Static ARP Settings 画面

「Static ARP Settings」画面には次の項目があります。

項目	説明
Global Settings	
ARP Aging Time (0-65535)	ARP テーブルエントリがアクセスされないまま、破棄されないでエントリを保持する時間（秒）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。範囲は 0-65535（分）です。初期値は 20（分）です。
Add Static ARP Entry	
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。
MAC 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。
スタティック ARP リスト	
ユーザがスタティックに設定した IP アドレスと MAC アドレスの対応エントリを表示します。	

2. 「ARP Aging Time」を設定します。
3. 「Apply」ボタンをクリックし、ARP の全体的な設定を更新します。
4. 「IP Address」と「MAC Address」を設定します。
5. 「Apply」ボタンをクリックし、デバイスの ARP 設定を更新します。

Static ARP List 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 List 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。すべてのエントリを削除する場合は、「Delete All」ボタンをクリックします。

注意　本スイッチは、255 個のスタティック ARP エントリをサポートしています。

User Accounts（ユーザアカウントの設定）

ユーザパスワードとアクセス権限を含むユーザアカウントを設定します。以下の手順でユーザアカウント情報を設定します。

1. **Configuration > User Accounts** の順にクリックし、「User Accounts」画面を表示します。

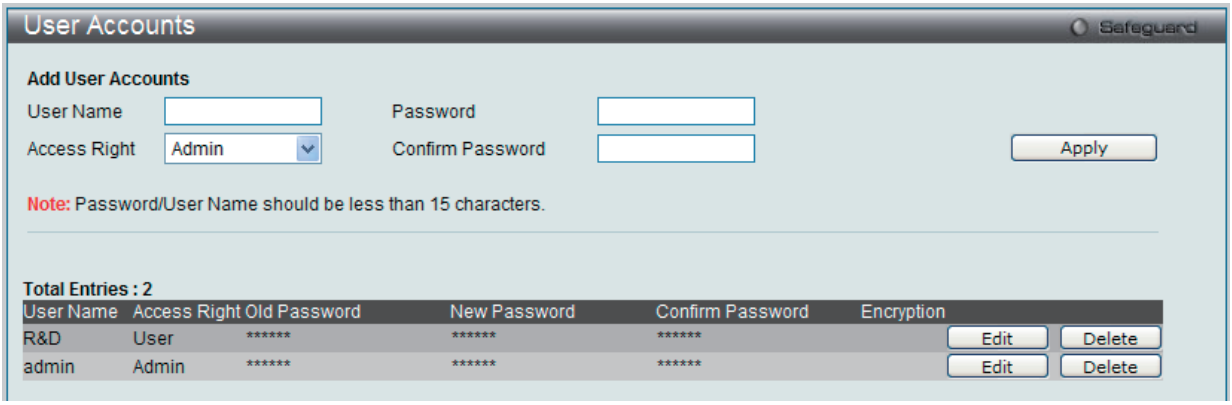


図 6-12　User Accounts 画面

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 15 文字以内）
Access Right	アクセスレベルを設定します。Admin レベルおよび User 権限の違いは、表 6-1 を参照してください。 • Admin - ユーザに管理者としての権限を与えます。 • User - ユーザに参照のみの権限を与えます。
Password	ユーザアカウントに対するパスワードを設定します。（半角英数字 15 文字以内）
Confirm Password	ユーザパスワードの確認入力をします。

2. 「User Name」を設定します。
3. アクセス権限を「Access Right」に設定します。
4. 新しいパスワードを「Password」に入力し、再度確認のために「Confirm Password」にも入力します。
5. 「Apply」ボタンをクリックし、新しいユーザアカウント、パスワード、アクセス権限をデバイスに適用します。

User Accounts 画面の編集

1. User List から編集するユーザ名の「Edit」ボタンをクリックし、以下の画面を表示します。

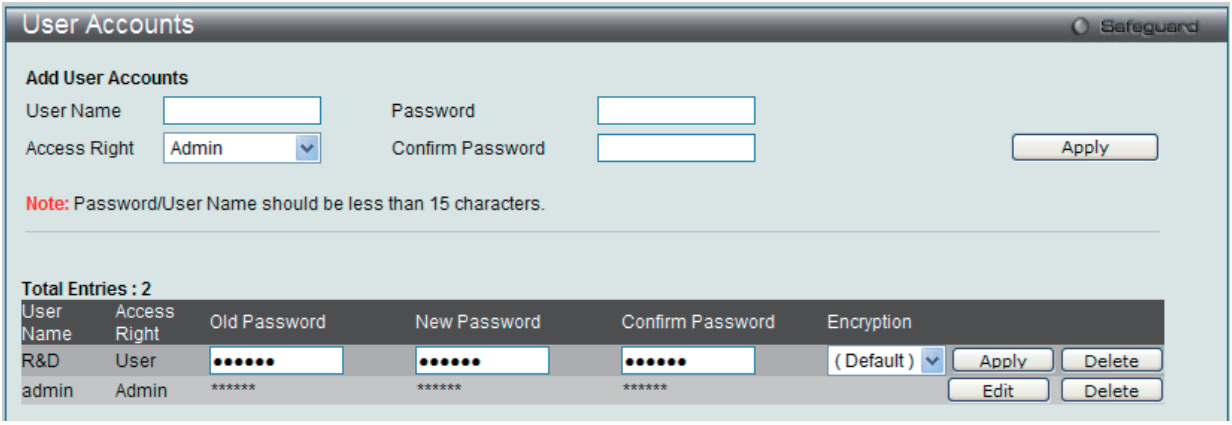


図 6-13　User Accounts 編集画面

2. 値を設定します。必要に応じ、「Encrypt」で暗号化タイプ（「Plain Text」または「SHA-1」）を選択します。
3. パスワードを変更する場合は、現在のパスワードを「Old Password」に、新しいパスワードを「New Password」に、確認のために新しいパスワードを「Confirm Password」に入力します。
4. 「Apply」ボタンをクリックし、新しいアクセス権限をデバイスに適用します。

注意 パスワードを忘れてしまった場合やパスワード不正の場合は、269 ページの「付録 A ケーブルとコネクタ」を参照してください。本問題を解決する手順が記載されています。

User Accounts 画面のエントリの削除

該当エントリの「Delete」ボタンをクリックします。ユーザアカウントが削除され、デバイスが更新されます。

Admin および User 権限
ユーザ権限には Admin と User の 2 つのレベルがあります。Admin 権限を持つユーザが利用可能なメニューのうちのいくつかは、User 権限では利用できません。

以下の表に、Admin レベルおよび User 権限の違いをまとめます。

表 6-1　Admin、User 権限

管理	Admin	User
コンフィグレーション設定	可	読み出しのみ
ネットワークモニタリング	可	読み出しのみ
コミュニティ名とトラップステーション	可	読み出しのみ
ファームウェアとコンフィグレーションファイルの更新	可	不可
システムユーティリティ	可	不可
リセット（工場出荷状態へ）	可	不可
ユーザアカウント管理		
ユーザアカウントの登録、更新、変更	可	不可
ユーザアカウントの確認	可	不可

System Log Configuration（システムログ構成）

「System Log Configuration」フォルダには「System Log Settings」と「System Log Server」の 2 つのメニューがあり、システムログ設定のための各属性やプロパティの情報があります。

System Log Settings（システムログ設定）

ここでは、システムログ機能を有効または無効にし、スイッチのフラッシュメモリにスイッチログを保存する方法を選択します。

Configuration > System Log Configuration > 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。

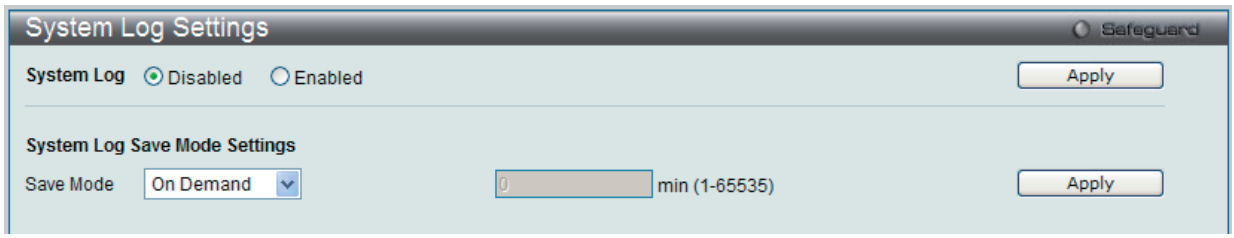


図 6-14　System Log Settings 画面

画面には次の項目があります。

項目	説明
System Log	システムログ機能を「Enabled」（有効）または「Disabled」（無効）にします。初期値は「Disabled」です。
Save Mode	プルダウンメニューよりフラッシュメモリにスイッチのログを保存する方法を指定します。３つのオプションがあります • Time Interval - 本項目横にある欄にログを保存する間隔（1-65535）（分）を設定します。 • On Demand - 手動でスイッチに、ログファイルを保存します。「Save」フォルダの「Save Log」リンクを使用するか、または本画面の「Save Log Now」ボタンをクリックして保存します。（初期値） • Log Trigger - スイッチにログイベントが発生すると、スイッチにログファイルを保存します。

1. 「System Log」を「Enabled」（有効）にし、「Apply」ボタンをクリックします。
2. プルダウンメニューよりフラッシュメモリにスイッチのログを保存する方法を指定します。「Time Interval」を選択した場合は、横にある欄にログを保存する間隔を入力します。
3. 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 Server（システムログの管理）

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。各メッセージの重要度によって、イベントメッセージの送信先となるイベントを記録するデバイスを決めることができます。

本スイッチは 4 台までの Syslog サーバに Syslog メッセージを送信できます。

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

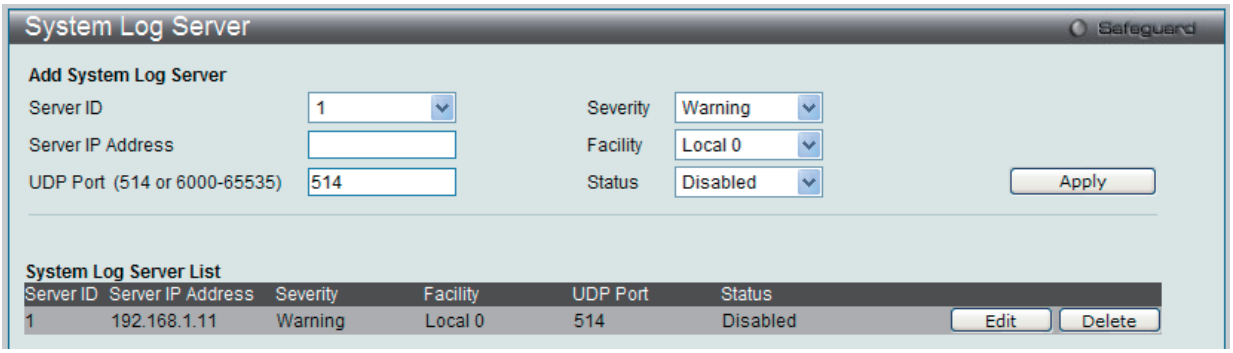


図 6-15　System Log Server 画面

本画面には次の項目があります。

項目	説明
Server ID	Syslog サーバ設定のインデックス（1-4）を設定します。
Server IP Address	ログを記録するサーバの IP アドレスを設定します。
UDP Port (514 or 6000-65535)	ログを送信するサーバの UDP ポートを設定します。514 または 6000-65535 が設定できます。初期値は 514 です。
Severity	サーバに送信する警告ログを選択するための重要度の識別名には 3 つのレベルがあります。 • Warning - 最も低いレベルのデバイス警告。デバイスは機能しているが、動作上の問題が発生しています。 • Informational - デバイス情報の提供。 • All - すべてのレベルのシステムログの提供。
Facility	オペレーティングシステムデーモンおよびプロセスでファシリティ値を割り当てている場合に設定します。ファシリティを割り当てていないプロセスとデーモンの場合は「local use」（アプリケーション用の汎用）のいずれかを使用するか、「user-level」を使用します。指定できるファシリティは以下の通りです。**太字**のものは、本システムで現在使用されるファシリティ値です。

コード	ファシリティ	コード	ファシリティ
0	カーネルメッセージ	11	FTP デーモン
1	ユーザプログラム	12	NTP サブシステム
2	メールプログラム	13	ログオーディット
3	デーモンプロセス	14	ログアラート
4	認証サービス	15	クロックデーモン
5	シスログライン・プリンタサブシステムにより内部生成されたメッセージ	**16**	**ローカル使用 0（local 0）**
		17	**ローカル使用 1（local 1）**
7	ネットワークニュース・サブシステム	**18**	**ローカル使用 2（local 2）**
8	UUCP サブシステム	**19**	**ローカル使用 3（local 3）**
9	クロックデーモン	**20**	**ローカル使用 4（local 4）**
10	認証サービス	**21**	**ローカル使用 5（local 5）**
		22	**ローカル使用 6（local 6）**
		23	**ローカル使用 7（local 7）**

Status	「Enabled」（有効）または「Disabled」（無効）を選択します。

各項目を設定します。「Apply」ボタンをクリックし、システムログホスト設定をデバイスに適用します。

エントリの変更

編集する場合は、該当エントリ横の「Edit」ボタンをクリックします。項目を入力後、「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、デバイスのエントリを削除します。

DHCP Relay（DHCP リレー）

DHCP メッセージが中継される最大のホップ（ルータの）数を DHCP Relay Hops Count Limit として、指定することができます。パケットのホップ数が、Relay Hops Count Limit より多くなれば、そのパケットは廃棄されます。値の範囲は 1-16 で、初期値は 4 です。DHCP Relay Time Threshold はスイッチが Boot Request パケットを送出する前に待つ最小の時間（秒）です。パケットの「Seconds」の値が DHCP Relay Time Threshold の値より小さければ、そのパケットは廃棄されます。値の範囲は 0-65535 で初期値は 0（秒）です。

「DHCP Relay」フォルダには「DHCP Relay Global Settings」、「DHCP Relay Interface Settings」および「DHCP Local Relay Settings」メニューがあります。

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

DHCP リレーグルーバル設定を行います。

Configuration > 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。DHCP リレーのグローバル設定を有効にして、設定を行います。

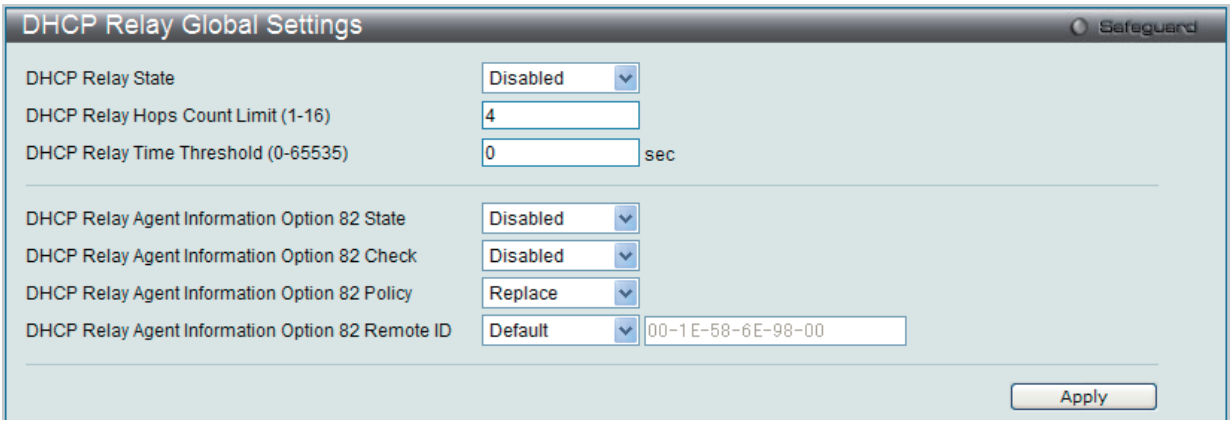


図 6-16　DHCP Relay Global Settings 画面

以下の項目が使用されます。

項目	説明
DHCP Relay State	プルダウンメニューから「Enabled」または「Disabled」を選択し、スイッチ上で DHCP リレーサービスを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Disabled」です。
DHCP Relay Hops Count Limit (1-16)	DHCP メッセージが中継されるルータホップの最大数（1-16）を定義します。初期値は 4 です。
DHCP Relay Time Threshold (0-65535)	DHCP パケットのルーティングを行うタイムリミットを定義します。0 が指定されると、スイッチは DHCP パケットの「Seconds」内の値のプロセスを行いません。0 以外の値を指定すると、スイッチはその値を使用し、ホップカウントと併用しながら DHCP パケットの送出を決定します。初期値は 0 です。
DHCP Relay Agent Information Option 82 State	スイッチ上で DHCP Agent Information Option 82 機能を「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Disabled」です。 • Enabled - リレーエージェントは DHCP サーバとクライアント間で交わすメッセージに DHCP Relay Information（「Option 82」欄）を挿入 / 削除します。リレーエージェントが DHCP リクエストを受信すると、Option 82 情報と（設定があれば）リレーエージェントの IP アドレスをパケットに付加します。Option 82 情報が付加されたパケットは DHCP サーバに送信されます。Option 82 をサポートする DHCP サーバがパケットを受信すると、そのサーバは remote ID、circuit ID、またはそれらの両方を使用して IP アドレスを割り当て、単一の remote ID または circuit ID に割り当て可能な IP アドレス制限などのポリシーを適用できます。それから、DHCP サーバは「Option-82」欄の値を DHCP reply の中にそのまま残します。DHCP サーバはスイッチが DHCP request を中継していた場合には、ユニキャストで reply を返します。スイッチは remote ID や circuit ID 欄を調べて、本来の Option-82 情報が insert されていたかを確認します。スイッチは「Option-82」欄を削除してからそのパケットを DHCP クライアントに接続されているスイッチポートに転送します。 • Disabled - リレーエージェントは DHCP サーバとクライアント間で交換するメッセージへの DHCP Relay Information（「Option 82」欄）の挿入 / 削除を行いません。また、以下の Option 82 のチェックとポリシーの項目は無効になります。
DHCP Relay Agent Information Option 82 Check	スイッチのパケットの Option 82 項目の妥当性のチェックを行う機能を「Enabled」（有効）/「Disabled」（無効）にします。 • Enabled - リレーエージェントはパケットの「Option 82」項目の妥当性のチェックを行います。スイッチが DHCP クライアントから Option 82 項目を含むパケットを受信すると、スイッチはこれらのパケットは不正だとしてパケットを廃棄します。リレーエージェントは DHCP サーバから受信したパケットから不正なメッセージを削除します。 • Disabled - リレーエージェントはパケットの「Option 82」項目の妥当性のチェックを行いません。

項目	説明
DHCP Relay Agent Information Option 82 Policy	プルダウンメニューから「Replace」、「Drop」または「Keep」を選択します。初期値は「Replace」です。 • Replace - DHCP クライアントから受信したパケット内の既存のリレー情報をスイッチの DHCP リレー情報に置き換えます。 • Drop - DHCP クライアントから受信したパケット内に既にリレー情報があった場合はそのパケットを削除します。 • Keep - DHCP クライアントから受信したパケット内の既存のリレー情報を保持します。
DHCP Relay Agent Information Option 82 Remote ID	Remote ID を入力します。「Default」に設定すると、Remote ID としてスイッチの MAC アドレスを使用します。

「Apply」ボタンをクリックして設定内容を有効にします。

注意 スイッチが、DHCP クライアントから「Option-82」項目を含むパケットを受信し、チェック機能が「Enabled」（有効）になっている場合、スイッチはこのようなパケットは不正だとして、パケットを破棄します。しかし、場合によってはクライアント側で Option-82 情報が設定されることもあります。そのような状況では、チェック機能を無効にしてスイッチがパケットを破棄しないようにします。DHCP クライアントから受信したパケット内に既にリレー情報があった場合のスイッチの動作を「DHCP Agent Information Option 82 Policy」で指定します。

DHCP Information Option 82 の実装

config dhcp_relay option_82 コマンドは、スイッチの DHCP リレーエージェント Information Option 82 の設定を行う際に使用します。Circuit ID サブオプションおよび Remote ID サブオプションのフォーマットは以下の通りです。

注意 スタンドアロンスイッチの場合、サーキット ID のサブオプションのモジュールフィールドは常に 0 です。

サーキット ID のサブオプションフォーマット

1.	2.	3.	4.	5.	6.	7.
1	6	0	4	VLAN	モジュール	ポート
1 バイト	1 バイト	1 バイト	1 バイト	2 バイト	1 バイト	1 バイト

1. サブオプションタイプ
2. サブオプションタイプ長
3. Circuit ID タイプ
4. Circuit ID 長
5. VLAN : DHCP クライアントパケットを受信した VLAN
6. モジュール : スタンドアロンスイッチの場合は常に 0。スタッカブルスイッチの場合は Unit ID。
7. ポート : DHCP クライアントパケットを受信したポート番号。ポート番号は 1 から始まります。

リモート ID のサブオプションフォーマット（初期値）

1.	2.	3.	4.	5.
2	8	0	6	MAC アドレス
1 バイト	1 バイト	1 バイト	1 バイト	6 バイト

1. サブオプションタイプ
2. サブオプション長
3. Remote ID タイプ
4. Remote ID 長
5. MAC アドレス : スイッチのシステム MAC アドレス

リモート ID のサブオプションフォーマット（ユーザ設定文字列）

1.	2.	3.	4.	5.
2	N+2	1	N	ASCII Remote ID 文字列（最大 127 文字）
1 バイト	1 バイト	1 バイト	1 バイト	N バイト

1. サブオプションタイプ
2. サブオプション長
3. Remote ID タイプ
4. Remote ID 長
5. ユーザ設定 Remote ID

図 6-17　Circuit ID と Remote ID のサブオプションフォーマット

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

「DHCP Relay Interface Settings」メニューでは、DHCP 情報をスイッチに中継するために、DHCP サーバの登録を行います。以下の画面を使用して、DHCP サーバに直接接続する、既に登録済みのスイッチの IP インタフェースアドレスを設定します。正しく入力を行い「Apply」ボタンをクリックすると、以下の画面の下部に位置する「DHCP Relay Interface Table」にリスト表示されます。スイッチの 1 つの IP インタフェースに対して 4 件までのサーバ IP アドレスを登録できます。エントリの削除は「Delete」ボタンをクリックして行います。

Configuration > DHCP Relay > DHCP 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。

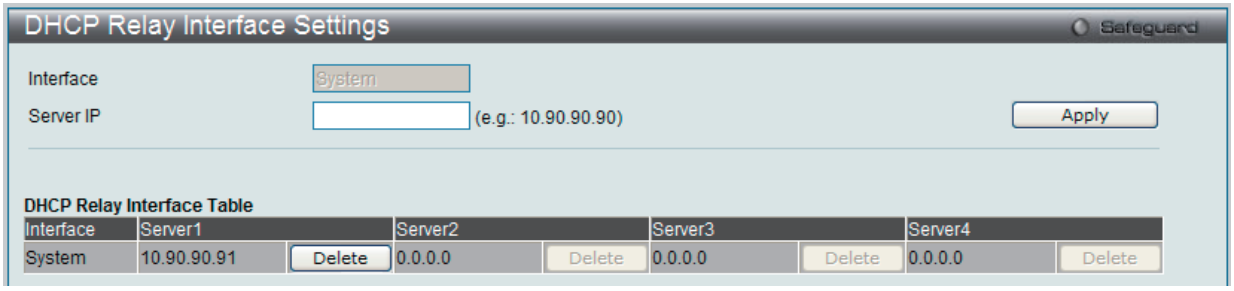


図 6-18　DHCP Relay Interface Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
Interface	DHCP サーバに直接接続するスイッチの IP インタフェース
Server IP	DHCP サーバの IP アドレス。1 つの IP インタフェースに対して 4 件までの入力が可能です。

「Apply」ボタンをクリックして設定内容を有効にします。

DHCP リレーインタフェース設定の削除

削除するエントリの「Delete」ボタンをクリックします。

DHCP Local Relay Settings（DHCP ローカルリレー設定）

DHCP ローカルリレーの設定を有効にして、設定を行います。

DHCP ローカルリレー設定では、DHCP クライアントが同じ VLAN から IP アドレスを取得する際、DHCP リクエストパケットにオプション 82 を追加できるようにします。DHCP ローカルリレー設定を行わない場合、スイッチはパケットを VLAN にフラッドします。DHCP リクエストパケットにオプション 82 を追加させるためには、DHCP ローカルリレー設定とグローバル VLAN のステートを有効にする必要があります。

Configuration > DHCP Relay > DHCP Local Relay 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。

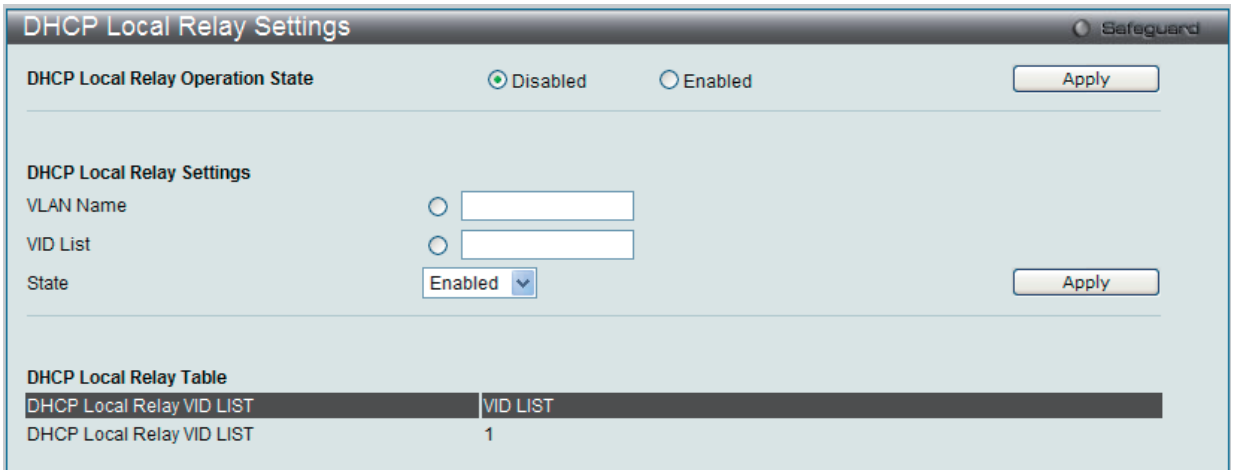


図 6-19　DHCP Local Relay Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
DHCP Local Relay Global State	ローカルリレーのグローバルステート機能を「Enabled」（有効）または「Disabled」（無効）にします。初期値は「Disabled」です。
VLAN Name	ラジオボタンを選択し、VLAN 名を入力します。DHCP ローカルリレーに適用する VLAN を識別するために使用します。
VID List	DHCP ローカルリレーに適用する VLAN を識別するために使用する VLAN ID を入力します。
State	DHCP ローカルリレー設定を「Enabled」（有効）または「Disabled」（無効）にします。
DHCP Local Relay VID LIST	ユーザが DHCP ローカルリレーに適用する VLAN ID のリストです。

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 Auto Configuration Settings（DHCP 自動設定）

スイッチにおける DHCP 自動設定機能は、現在使用中の保存済みコンフィグレーションファイルをロードします。DHCP 自動設定がスイッチで有効な場合、DHCP にはリプライにはコンフィグレーションファイルとパス名が含まれます。そして、リプライに指定された TFTP サーバからファイルを要求します。

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

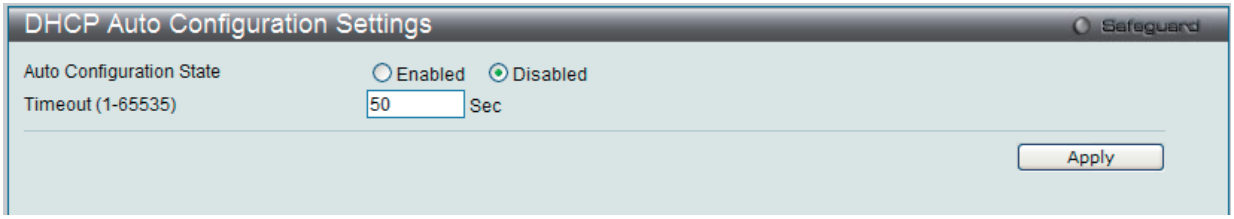


図 6-20　DHCP Auto Configuration Settings 画面

DHCP 自動設定が有効な場合、スイッチはリブート後自動的に DHCP クライアントになります。この方法を使用するためには、DHCP サーバは TFTP サーバの IP アドレスとコンフィグレーションファイル名を持ち、DHCP リプライパケットのデータフィールド内の本情報を渡すように設定される必要があります。TFTP サーバを起動し、スイッチからリクエストを受信する時、そのベースディレクトリ内にコンフィグレーションファイルを保管しておく必要があります。コンフィグレーションファイルのロードに関する情報については、DHCP サーバや TFTP サーバのソフトウェア説明書を参照してください。

本スイッチが DHCP 自動設定を完了できない場合はスイッチのメモリ内の以前に保存した設定が使用されます。

「Auto Configuration State」を有効にするためには、プルダウンメニューで「Enabled」を選択し、「Apply」ボタンをクリックします。

MAC Address Aging Time（MAC アドレスエージングタイム）

スイッチに MAC アドレスエージングタイムを設定します。

Configuration > MAC Address Aging Time の順にクリックし、以下の画面を表示します。

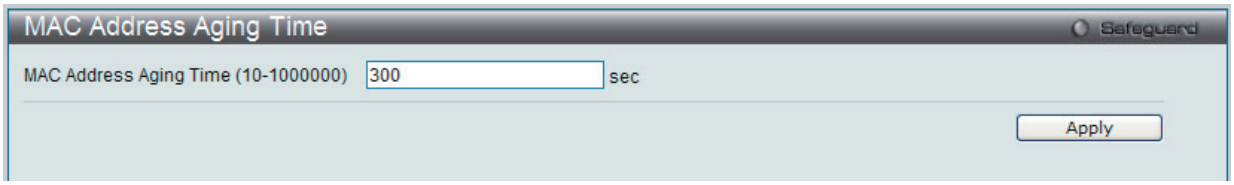


図 6-21　MAC Address Aging Time 画面

以下の項目を使用して設定、表示を行います。

項目	説明
MAC Address Aging Time (10-1000000)	学習した MAC アドレスが、アクセスされないでフォワーディングテーブルに保持される（学習した MAC アドレスの待機状態）時間（10-1000000）を指定します。これを変更するためには、現在の MAC アドレスが破棄される時間（秒）とは異なる値を入力します。初期値は 300（秒）。

「Apply」ボタンをクリックし、MAC アドレスエージングタイム設定を適用します。

Web Settings（Web 設定）

スイッチに Web ステータスを設定します。

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

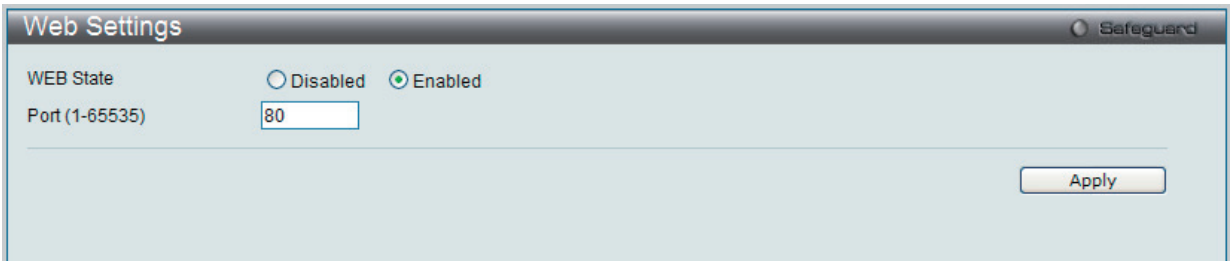


図 6-22　Web Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
WEB State	Web ベースマネジメントは初期値で「Enabled」（有効）です。「Disabled」を選択して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。

「Apply」ボタンをクリックし、Web 設定を適用します。

Telnet Settings（Telnet 設定）

スイッチに Telnet 設定をします。

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

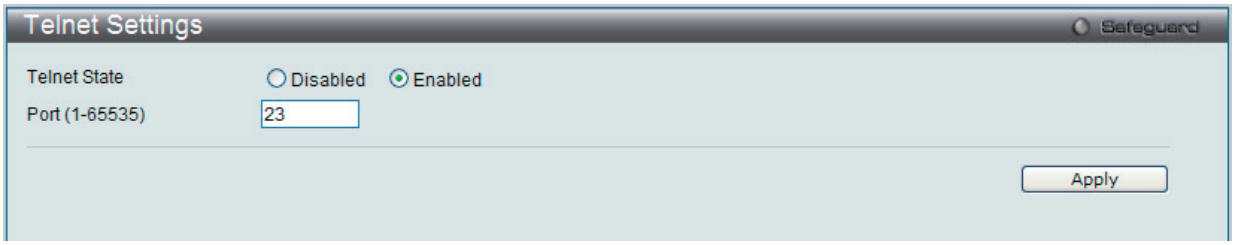


図 6-23　Telnet Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
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。Telnet プロトコルに通常使用される TCP ポートは 23 です。

「Apply」ボタンをクリックし、Telnet 設定を適用します。

Password Encryption（パスワードの暗号化）

スイッチのパスワードの暗号化機能を有効または無効にします。

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

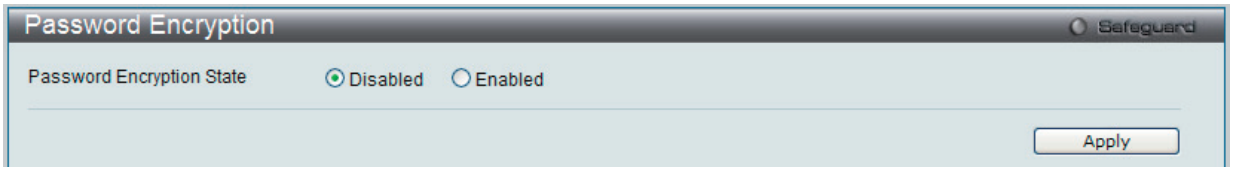


図 6-24　Password Encryption 画面

以下の項目を使用して設定、表示を行います。

項目	説明
Password Encryption State	パスワードの暗号化は初期値で「Disabled」（無効）です。「Enabled」を選択し、パスワードの暗号化を有効にします。 • Enabled- パスワードを暗号化形式に変更できます。 • Disabled - プレーンテキスト形式となります。

「Apply」ボタンをクリックし、パスワードの暗号化設定を適用します。

注意　暗号化された形式でパスワードを指定する場合、または最後に「enable password encryption」コマンドで暗号形式にパスワードが変換している場合、パスワードは既に暗号化形式となっており、プレーンなテキスト形式に戻すことはできません。

CLI Paging Settings（CLI ページング設定）

CLI ページング機能を有効または無効にします。CLI ページング設定は、コンソール画面で複数ページがすぐにスクロールしてしまう場合に使用します。「Enabled」を指定すると、各ページごとに休止します。

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

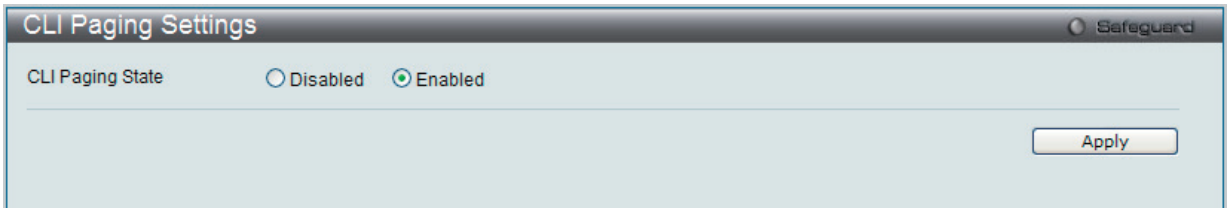


図 6-25　CLI Paging Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
Clipaging State	コマンドラインインタフェースの改頁処理をコンソール画面の最後で停止します。コンソール画面の範囲を超えてテキストが複数ページにスクロールしないようにします。初期値は「Enabled」（有効）です。無効にする場合は、「Disabled」を選択します。

「Apply」ボタンをクリックし、CLI ページング設定を適用します。

Firmware Information（ファームウェア情報）

以下に示す画面では、スイッチに格納されているファームウェアイメージの情報を確認、次回の起動ステータスの設定、および保存されている現在のファームウェアイメージの削除を行うことができます。

Configuration > Firmware Information の順にメニューを選択し、以下の画面を表示します。

図 6-26　Firmware Information 画面

本画面には以下の情報が表示されます。

項目	説明
ID	スイッチのメモリにあるファームウェアのイメージ ID を示します。スイッチのメモリには 2 件のファームウェアイメージを格納できます。Image ID 1 が初期設定のブートアップファームウェアです。
Version	ファームウェアのバージョンを示します。
Size（B）	ファームウェアのサイズ（バイト）を示します。
Update Time	ファームウェアがスイッチにダウンロードされた日時を示します。
From	ファームウェアのダウンロード元の IP アドレスを示します。スイッチへのダウンロード方法は以下の 6 種類のいずれかになります。起動ファイルには「*」が付加されています。 • CONSOLE - コンソールポート（RS-232）によってファームウェアの更新が行われたことを示します。 • Telnet - Telnet によってファームウェアの更新が行われたことを示します。 • SNMP - SNMP によってファームウェアの更新が行われたことを示します。 • Web - Web ベースの管理インタフェースによってファームウェアの更新が行われたことを示します。 • SSH - Secure Shell（SSH）によってファームウェアの更新が行われたことを示します。 • SIM - シングル IP マネジメント機能によってファームウェアの更新が行われたことを示します。
User	ファームウェアのダウンロードを行ったユーザを表示します。ユーザが認識できない場合は、「Anonymous」または「Unknown」と表示されます。

「Boot UP」ボタンをクリックし、スイッチが次回の再起動時に使用する起動ファームウェアを設定します。
「Delete」ボタンをクリックし、本画面からファームウェアを削除します。

SNTP Settings（SNTP 設定）

SNMP（Simple Network Time Protocol）は、コンピュータのクロックにスイッチを同期させるために使用されます。SNTP 設定には「Time Settings」と「Time Zone Settings」メニューがあります。

Time Settings（時刻設定）

スイッチに時刻を設定します。

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

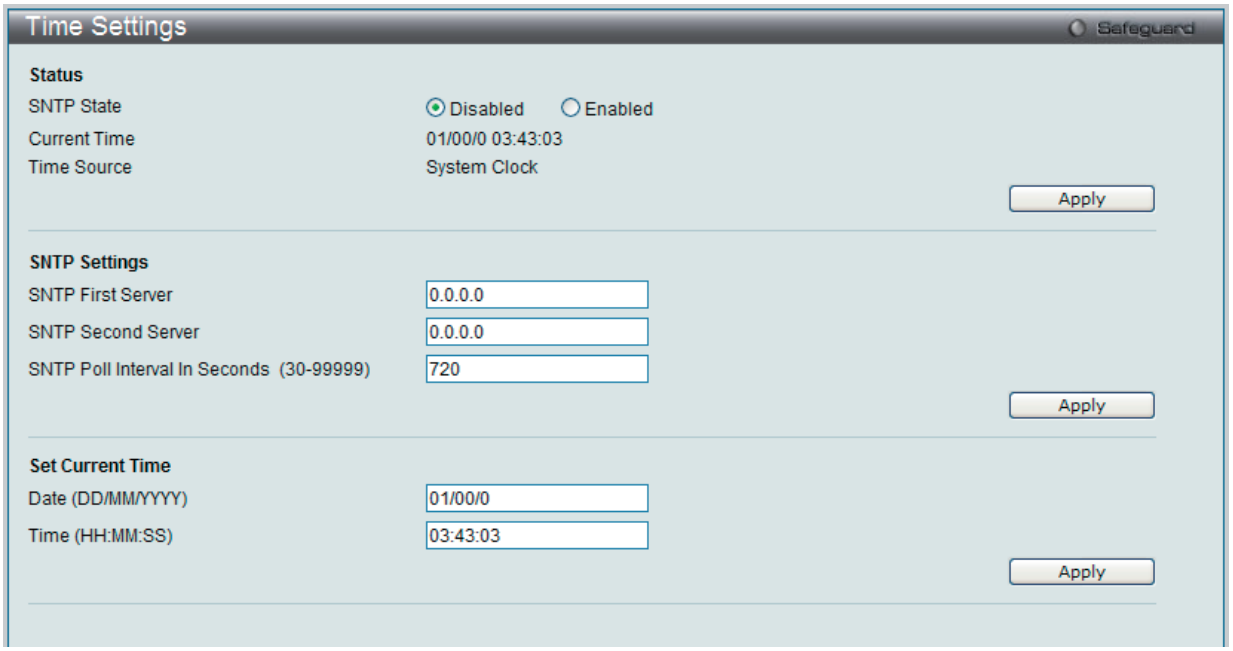


図 6-27　Time Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
Status	
SNTP State	SNTP を「Enabled」（有効）または「Disabled」（無効）にします。初期値は「Disabled」です。
Current Time	現在の日付と時刻を表示します。
Time Source	システム時刻を設定するタイムソースを設定します。 • SNTP - システム時刻を SNTP サーバから受信するように設定します。 • System Clock - システム時刻をデバイスに対して直接設定します。
SNTP Settings	
SNTP First Server	システム時刻を受け取るプライマリ SNTP サーバの IP アドレスを設定します。
SNTP Second Server	システム時刻を受け取るセカンダリ SNTP サーバの IP アドレスを設定します。
SNTP Poll Interval In Seconds (30-99999)	SNTP サーバにユニキャストによる問い合わせを行う間隔（30-99999 秒）を設定します。
Set Current Time	
Date（DD/MM/YY）	現在のシステム日付を設定します。項目のフォーマットは日 / 月 / 年です。
Time（HH:MM:SS）	現在のシステム時刻を時 : 分 : 秒（24 時間制）で設定します。例えば午後 9 時であれば 21:00:00 と指定します。

「Apply」ボタンをクリックし、デバイスに SNTP 設定を適用します。

TimeZone 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。

Configuration > SNTP Settings > TimeZone 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。

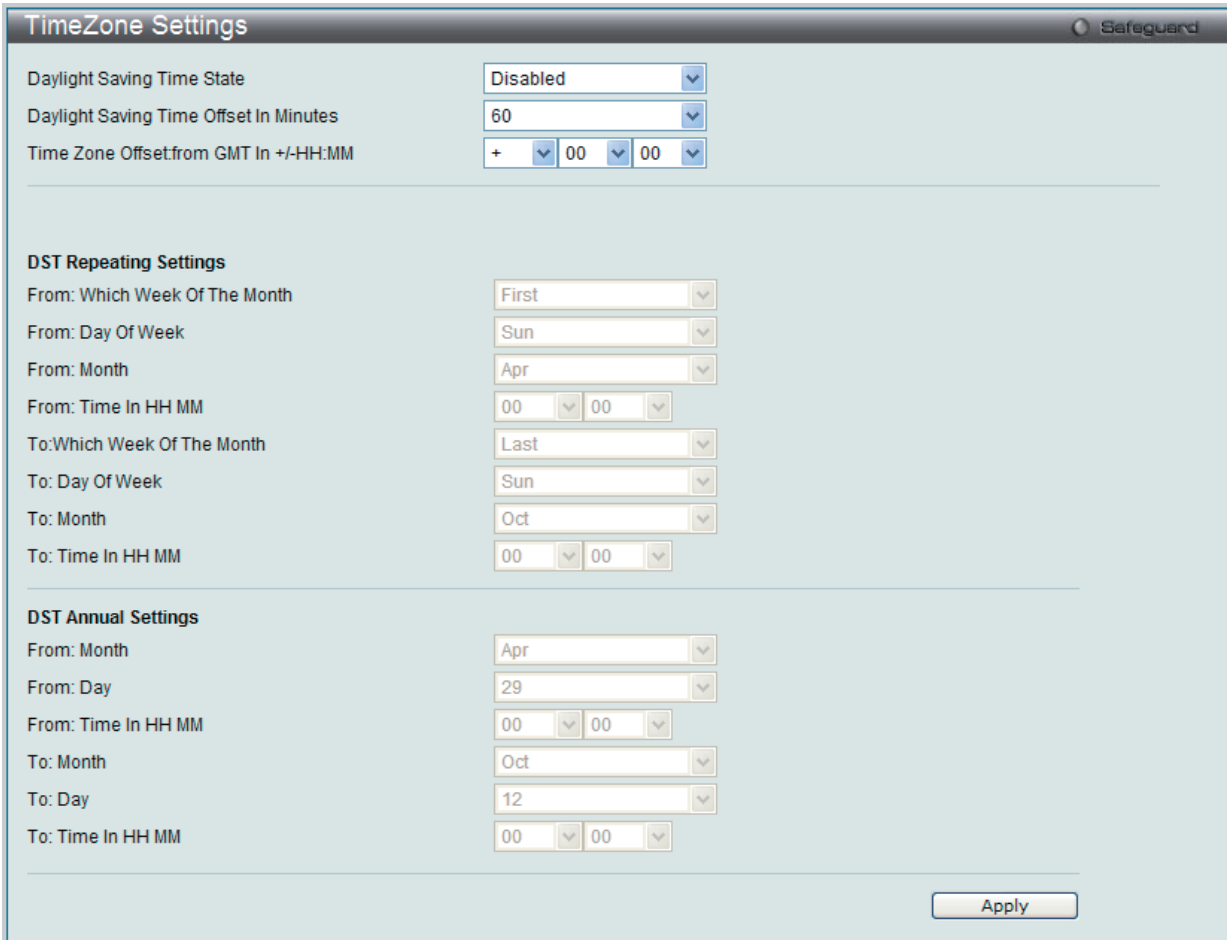


図 6-28　TimeZone Settings 画面

以下に、画面の各項目を示します。

項目	説明
Daylight Saving 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） • Repeating - 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設定する必要があります。 • Annual - 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。
Daylight Saving Time Offset In Minutes	プルダウンメニューを使用して、サマータイムによる調整時間を 30、60、90、120 分から選択します。
Time Zone Offset: from GMT In +/ - HH:MM	プルダウンメニューを使用して、GMT（グリニッジ標準時）からのオフセット時間を選択します。
DST Repeating Settings	
Repeating モードを使用すると、DST（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: Which Week Of The Month	月の第何週から DST が始まるかを設定します。 • First - 月の最初の週に設定します。 • Second - 月の 2 番目の週に設定します。 • Third - 月の 3 番目の週に設定します。 • Fourth - 月の 4 番目の週に設定します。
From: Day Of Week	DST が開始する曜日を指定します。Sun、Mon、Tue、Web、Tues、Fri、Sat
From: Month	DST が開始する月を指定します。Jan、Feb、May、Jun、Jul、Aug、Sep、Oct、Nov、Dec
From: Time In HH MM	DST が開始する時間を指定します。

項目	説明
To: Which Week Of The Month	月の第何週で DST が終わるかを設定します。 • First - 月の最初の週に設定します。 • Second - 月の 2 番目の週に設定します。 • Third - 月の 3 番目の週に設定します。 • Fourth - 月の 4 番目の週に設定します。
To: Day Of Week	DST が終了する曜日を指定します。
To: Month	DST が終了する月を指定します。
To: Time In HH MM	DST が終了する時間を指定します。
DST Annual Settings	
Annual モードを使用すると、DST（サマータイム）設定を指定した詳細な期日で自動的に調整できるようになります。例 : DST を 4 月 3 日から開始し、10 月 14 日を終了と設定します。	
From: Month	DST が開始する月を指定します。（毎年）
From: Day	DST が開始する日を指定します。（毎年）
From: Time In HH MM	DST が開始する時間を指定します。（毎年）
To: Month	DST が終了する月を指定します。（毎年）
To: Day	DST が終了する日を指定します。（毎年）
To: Time In HH MM	DST が終了する時間を指定します。（毎年）

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。

SMTP Settings（SMTP 設定）

SMTP（Simple Mail Transfer Protocol）は、以下の画面に入力した E-mail アドレスに基づいてメール受信者にスイッチのイベントを送信するスイッチの機能です。スイッチは SMTP のクライアントとして設定され、一方サーバはスイッチからのメッセージを受信し、E-mail に適切な情報を記載し、スイッチに設定した受信者に送信するリモートデバイスです。これはスイッチ上に発生した問題イベントの記録を行い、小ワークグループまたは配線用クローゼットの管理を簡素化し、緊急なスイッチイベントの処理速度を向上させ、セキュリティを強化することができます。

SMTP Service Settings（SMTP サービスの設定）

以下の画面でスイッチに問題が発生した場合に設定した E-mail アドレスに従ってスイッチのログファイルを送信する SMTP サーバを設定します。

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

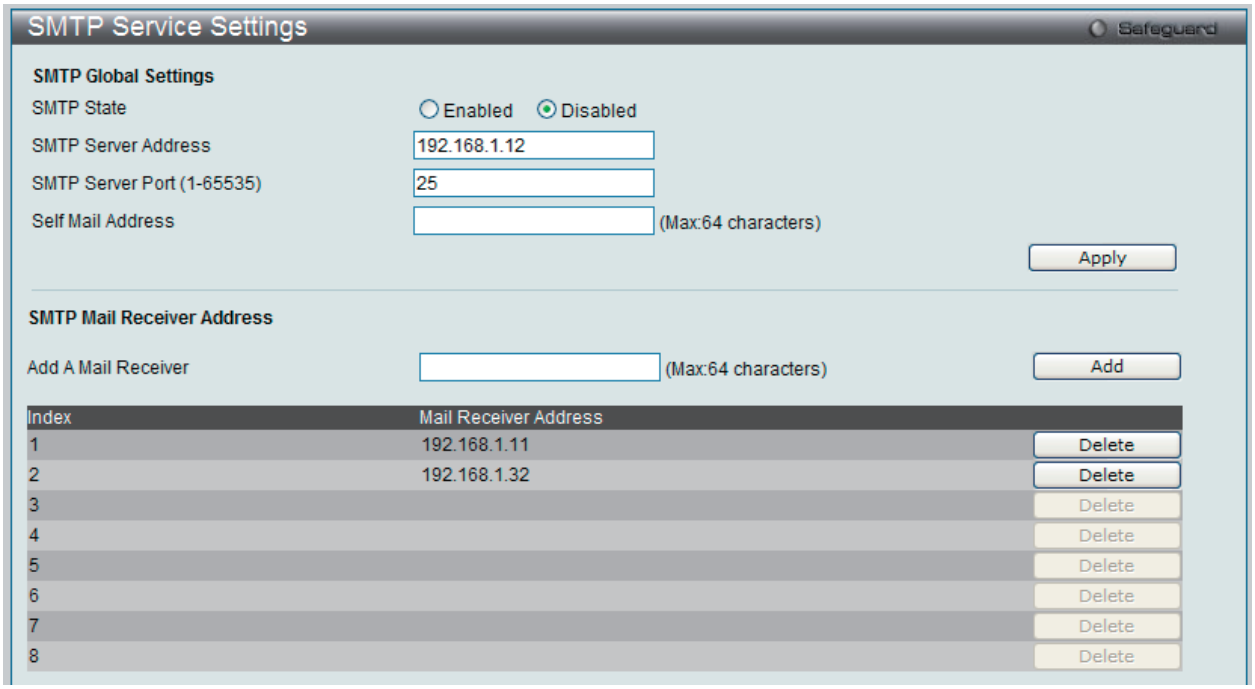


図 6-29　SMTP Service Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
SMTP Global Settings	
SMTP State	ラジオボタンを使用してこのデバイスの SMTP サービスを「Enabled」（有効）または「Disabled」（無効）にします。
SMTP Server Address	リモートデバイスの SMTP サーバの IP アドレスを入力します。これはメールを送信するデバイスとなります。
SMTP Server Port (1-65535)	SMTP サーバに接続するスイッチの仮想ポート番号（1-65535）を入力します。一般的なポート番号は 25 です。
Self Mail Address	メールメッセージを送信する E-mail アドレスを入力します。このアドレスは受信者に送信された E-mail メッセージにある"from"のアドレスとなります。本スイッチには Self Mail Address（半角英数字 64 文字以内）を 1 つだけ設定することができます。
SMTP Mail Receiver Address	
Add A Mail Receiver	E-mail アドレスを入力し、「Add」ボタンをクリックします。8 個までの E-mail アドレスを追加することができます。アドレスを削除する場合は、画面下部にある「Mail Receiver Address」テーブルで削除するエントリの「Delete」ボタンをクリックします。

SMTP Service（SMTP サービス）

前の画面で設定した SMTP サービス設定をテストします。

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

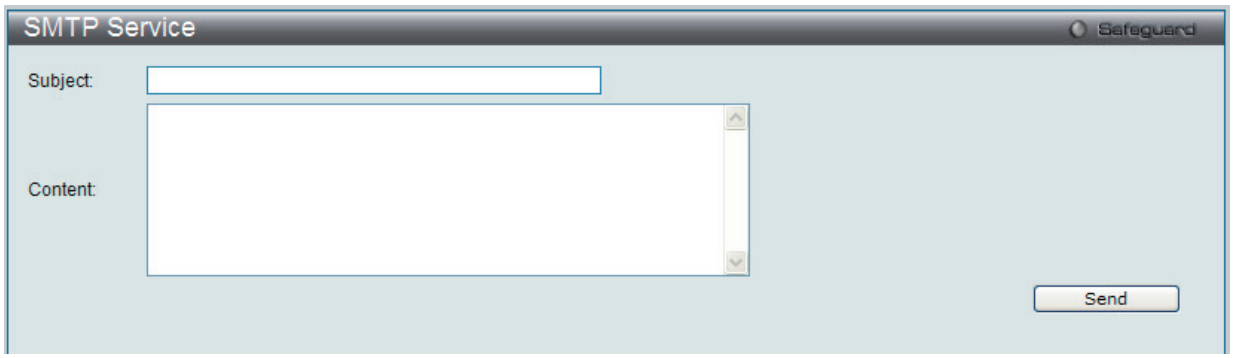


図 6-30　SMTP Service 画面

SMTP 設定が適切に動作しているかどうかをテストするためには、「Subject」、「Content」を入力し、「Send」ボタンをクリックします。

MAC Notification Settings（MAC 通知設定）

MAC Notification（通知）は、学習によりフォワーディングデータベースに記録された MAC アドレスの監視を行うために使用します。
「MAC Notification Settings」フォルダには、「MAC Notification Global Settings」と「MAC Notification Port Settings」メニューがあります。

注意 本機能をご使用になる場合、NMS 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 Notification Global Settings（MAC 通知グローバル設定）

スイッチの MAC 通知機能をグローバル（全ポート）に設定します。

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

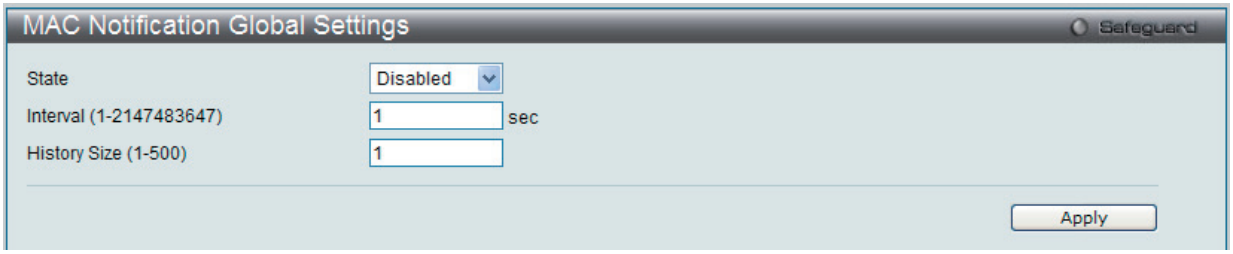


図 6-31　MAC Notification Global Settings 画面

以下の項目を使用して設定を行います。

項目	説明
State	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。初期値は「Disabled」です。
Interval (1-2147483647)	通知を行う間隔（秒）。初期値 : 1（秒）
History Size (1-500)	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

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 Port Settings（MAC 通知ポート設定）

ポートに MAC 通知設定を行います。

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

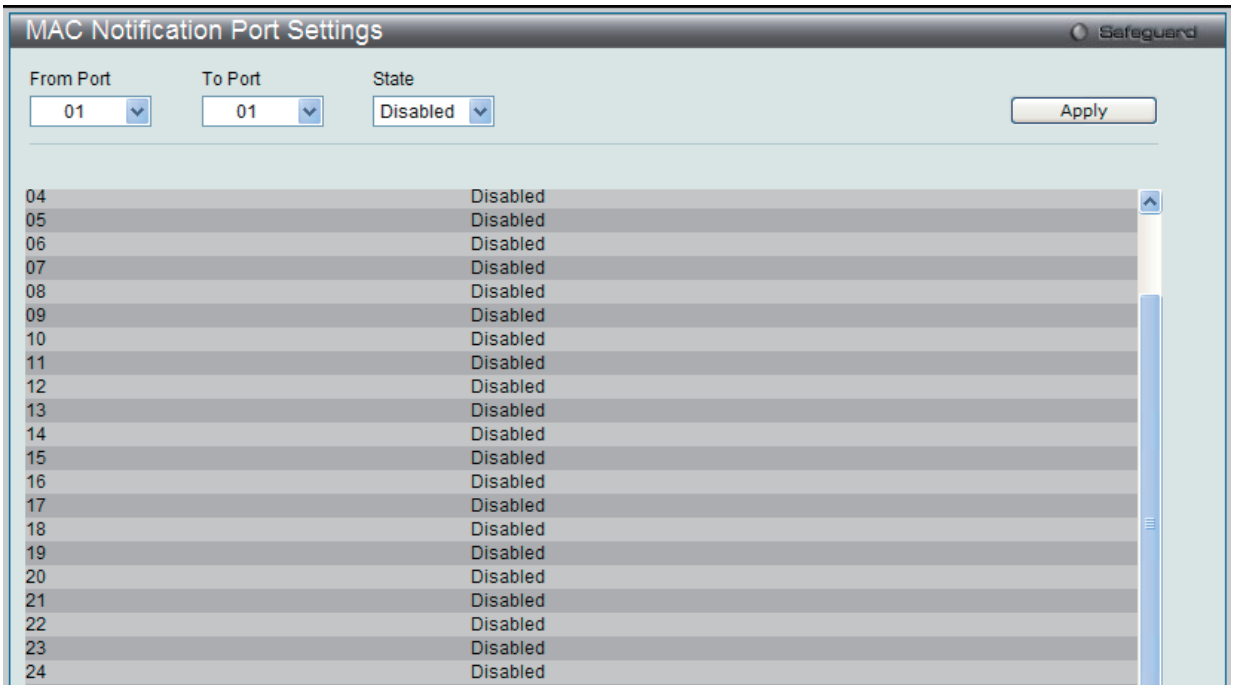


図 6-32　MAC Notification Port Settings 画面

以下の項目を使用し、MAC 通知設定をポートごと、またはポートグループごとに行います。

項目	説明
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。
State	指定したポートの MAC 通知設定を「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。

SNMP Settings（SNMP 設定）

SNMP（Simple Network Management Protocol）は、OSI 参照モデルの第 7 層（アプリケーション層）のプロトコルで、ネットワークデバイスの管理や監視を行います。ネットワーク管理デバイスは、SNMP を利用してゲートウェイ、ルータ、およびその他のネットワークデバイスの設定状態を確認または変更します。また、SNMP を利用してスイッチやスイッチ群、またはネットワークに対し、正常な動作を行うためのシステム設定、パフォーマンスの監視、問題の検出を行います。

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

DES-3200 シリーズは、SNMP バージョン 1（SNMP v1）、2c（SNMP v2c）、および 3（SNMP v3）をサポートしています。スイッチの監視と制御に使用する SNMP バージョンを選択することができます。これらの 3 つのバージョンでは、管理ステーションとネットワークデバイス間に適用されるセキュリティのレベルに違いがあります。

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

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

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

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

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

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

トラップ

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

MIB

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

本スイッチシリーズは、スイッチの環境に合わせた柔軟性のある SNMP 管理機能を採用しています。SNMP 管理機能は、ネットワークの要求やネットワーク管理者の好みに合わせてカスタマイズすることができます。SNMP バージョンの選択は、「SNMP Group Table」で行うことができます。

本スイッチシリーズは、SNMP バージョン 1、2c、および 3 をサポートします。管理者は、スイッチの監視と制御にどの SNMP バージョンを使用するかを指定できます。これらの 3 つのバージョンでは、管理ステーションとネットワークデバイス間に適用されるセキュリティのレベルに違いがあります。

SNMP View Table（SNMP ビューテーブル）

「SNMP View Table」画面は、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。

Configuration > SNMP Settings > SNMP View 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。

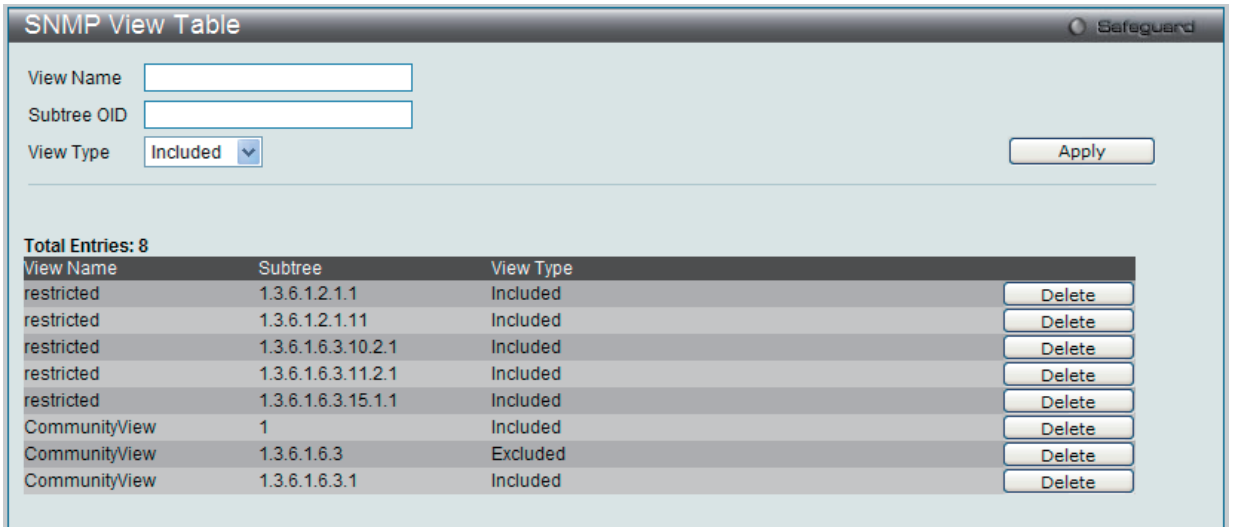


図 6-33　SNMP View Table 画面

エントリの削除

「SNMP View Table」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。

エントリの新規作成

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、「Apply」ボタンをクリックします。

SNMP ユーザ（「SNMP User Table」で設定）と本画面で登録するビューは、「SNMP Group Table」によって作成する SNMP グループによって関連付けます。

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 - アクセス可能になります。 • Excluded - アクセス不可になります。

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。

SNMP Group Table（SNMP グループテーブル）

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るものです。

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

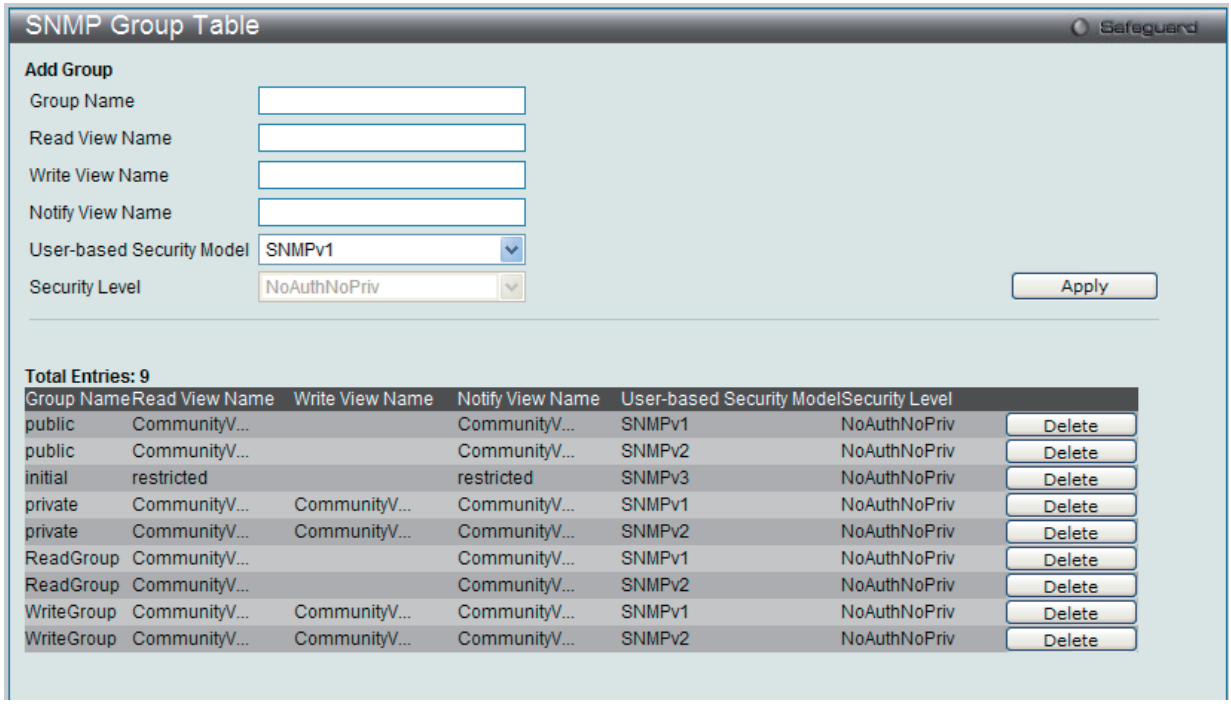


図 6-34　SNMP Group Table 画面

エントリの削除

削除するエントリの行の「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、「Apply」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。
Read View Name	SNMP メッセージを要求する SNMP グループ名を入力します。
Write View Name	スイッチの SNMP エージェントに書き込み権限を与える SNMP グループ名を入力します。
Notify View Name	スイッチの SNMP エージェントによるトラップメッセージを送信する SNMP グループ名を入力します。
User-based Security Model	• SNMPv1 - SNMP バージョン 1 が使用されます。 • SNMPv2 - SNMP バージョン 2c が使用されます。SNMP バージョン 2 は集中型、分散型どちらのネットワーク管理にも対応します。SNMP バージョン 1 と比較して SMI（Structure of Management Information）およびセキュリティ機能において強化されています。 • SNMPv3 - SNMP バージョン 3 が使用されます。ネットワーク上で認証とパケットの暗号化を併用することにより、デバイスへの安全なアクセスを提供します。
Security Level	セキュリティレベル設定は SNMP バージョン 3 にのみ適用されます。 • NoAuthNoPriv - 認証なし。スイッチとリモート SNMP マネージャ間の暗号化パケットの送信もないことを示します。 • AuthNoPriv - 認証あり。スイッチとリモート SNMP マネージャ間の暗号化パケットの送信がないことを示します。 • AuthPriv - 認証あり。スイッチとリモート SNMP マネージャ間のパケットも暗号化されて送信されることを示します。

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 User Table（SNMP ユーザテーブル）

SNMP ユーザを登録します。また、スイッチに現在設定されているすべての SNMP ユーザを表示します。

Configuration > SNMP Settings > SNMP User 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。

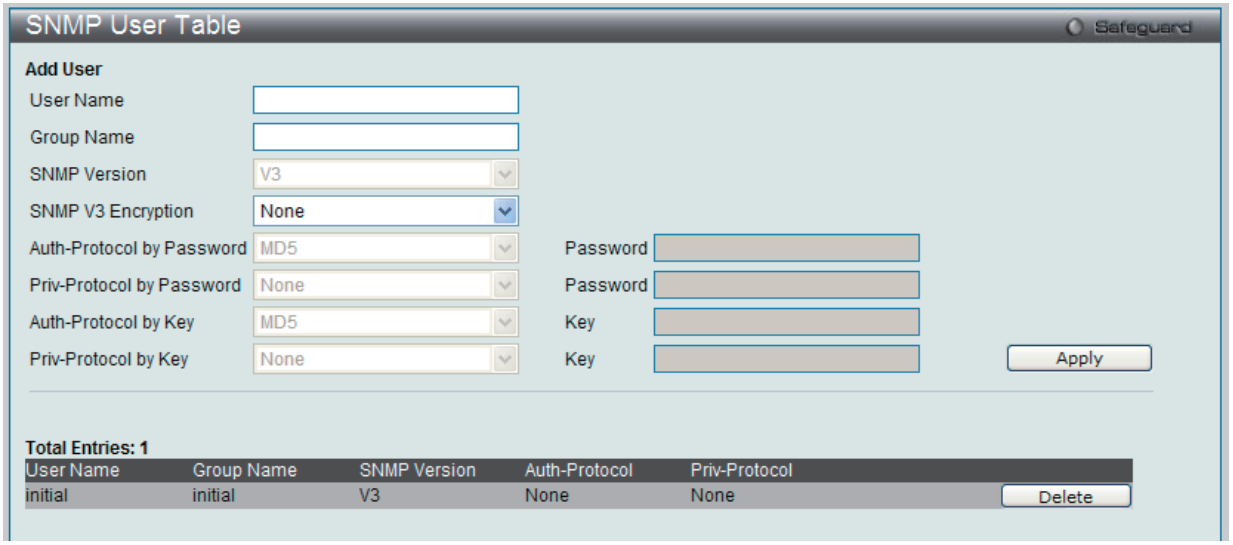


図 6-35　SNMP User Table 画面

エントリの削除

「SNMP User Table」から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、「Apply」ボタンをクリックします。

上記画面中の項目を以下に示します。

項目	説明
User Name	32 文字までの半角英数字。SNMP ユーザを識別します。
Group Name	作成した SNMP グループが SNMP メッセージを要求するために使用される名前です。
SNMP Version	• V1 - SNMP バージョン 1 が使用されています。 • V2 - SNMP バージョン 2 が使用されています。 • V3 - SNMP バージョン 3 が使用されています。
SNMP V3 Encryption	SNMP V3 に対して暗号化を有効にします。本項目は「SNMP Version」で「V3」を選択した場合に有効になります。 • None - ユーザ認証は使用しません。 • Key - HMAC-MD5 アルゴリズムまたは HMAC-SHA-96 アルゴリズムレベルのユーザ認証を行います。 • Password - HMAC-SHA-96 アルゴリズムレベルのパスワードか HMAC-MD5-96 パスワードによる認証を行います。
Auth-Protocol by Password/Key	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 by Password/Key	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ていません。 • DES - CBC-DES（DES-56）標準に基づく DES 56 ビット暗号化方式が使用されています。本項目を選択後、「Password」/「Key」にパスワード（半角英数字 8-16 文字）を入力します。

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 Community Table（SNMP コミュニティテーブル設定）

定義済みの SNMP コミュニティテーブルの参照、および、SNMP マネージャとエージェントの関係を定義する SNMP コミュニティ名を登録します。コミュニティ名は、スイッチのエージェントへのアクセスを行う際のパスワードの役割をします。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。

エントリの設定

「SNMP Community Table」画面でコミュニティエントリを設定します。

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

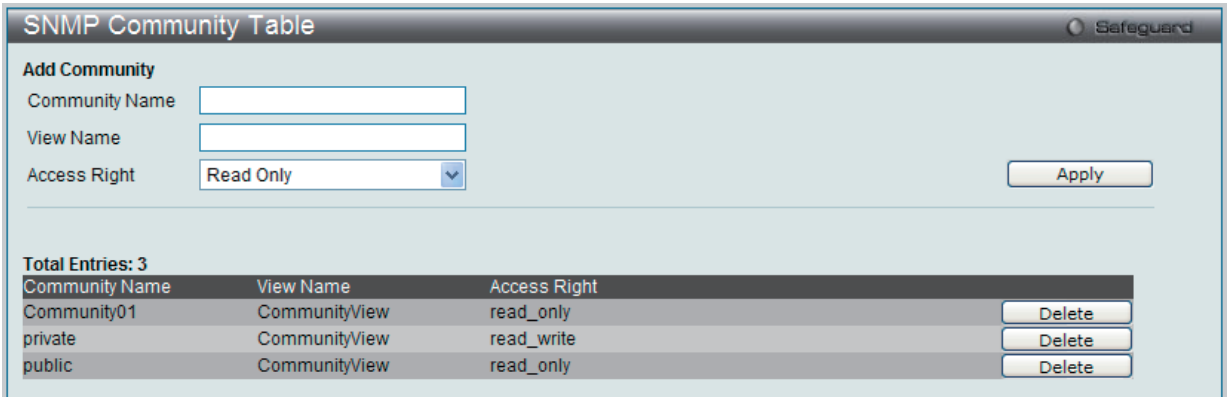


図 6-36　SNMP Community Table 画面

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

項目	説明
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 の内容について読み出し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 の内容について読み出し、および書き込みが可能です。

「Apply」ボタンをクリックし、新しい SNMP コミュニティテーブル設定を適用します。

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 Host Table（SNMP ホストテーブル）

IPv4 用の SNMP トラップの送信先を設定します。

Configuration > SNMP Settings > SNMP Host 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 6-37　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 IP 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 IP アドレスを入力します。
User-based Security Model	• SNMPv1 - SNMP バージョン 1 が使用されます。 • SNMPv2c - SNMP バージョン 2c が使用されます。 • SNMPv3 - SNMP バージョン 3 が使用されます。
Security Level	• NoAuthNoPriv - NoAuth-NoPriv セキュリティレベルが使用されます。 • AuthNoPriv - Auth-NoPriv セキュリティレベルが使用されます。 • AuthPriv - Auth-Priv セキュリティレベルが使用されます。
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。

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

「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。

SNMP Engine ID（SNMP エンジン ID）

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。

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

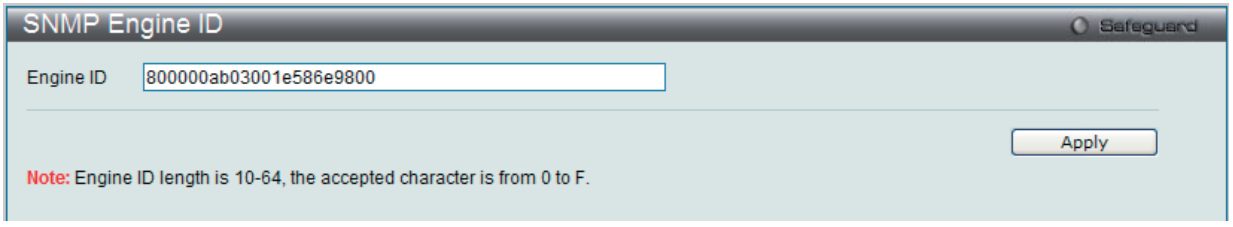


図 6-38　SNMP Engine ID 画面

以下の項目を使用します。

項目	説明
Engine ID	スイッチの SNMP エンジンの識別子を表示します。初期値は RFC2271 にて提示されています。 一番最初のビットは 1 で、最初の 4 つのオクテットには、IANA が割り当てるエージェントの SNMP マネジメントのプライベートエンタープライズ番号 (D-Link は 171) に相当する 2 進数が設定されます。5 番目のオクテットは 03 で、残りがこのデバイスの MAC アドレスであることを示しています。6 ～ 11 番目のオクテットは MAC アドレスです。

エンジン ID を変更するためには、新しいエンジン ID を入力し、「Apply」ボタンをクリックします。

SNMP Trap Configuration（SNMP トラップ設定）

スイッチの SNMP 機能のトラップ設定を有効または無効にします。

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

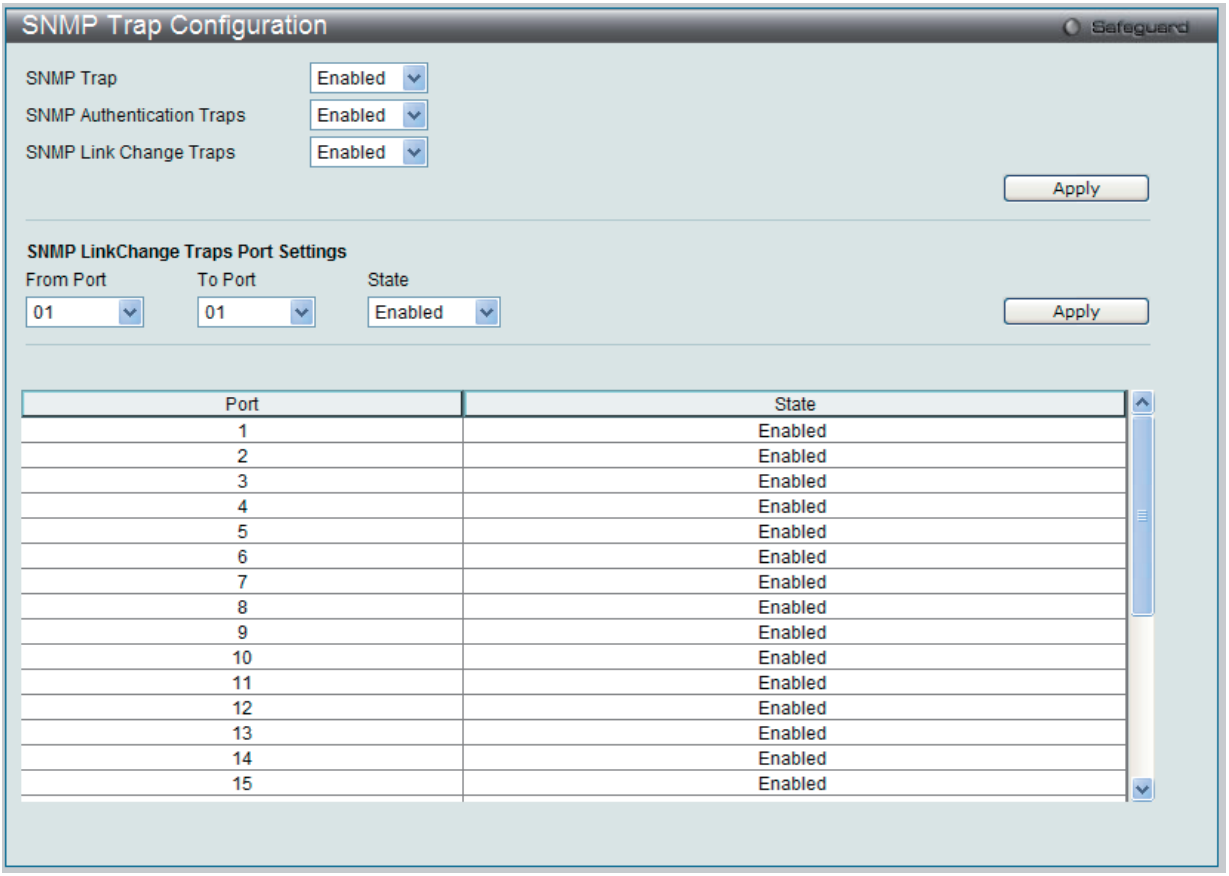


図 6-39　SNMP Trap Configuration 画面

各トラップのプルダウンメニューを「Enabled」（有効）、または「Disabled」（無効）にし、「Apply」ボタンをクリックします。

「SNMP Link Change Trap Port Settings」セクションでトラップを有効または無効にするポートまたはポート範囲を指定し、トラップのステート（有効 / 無効）を設定します。「Apply」ボタンをクリックして、設定を適用します。

RMON（RMON 設定）

ここでは、スイッチの SNMP 機能の RMON（remote monitoring）ステータスを有効または無効にします。

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

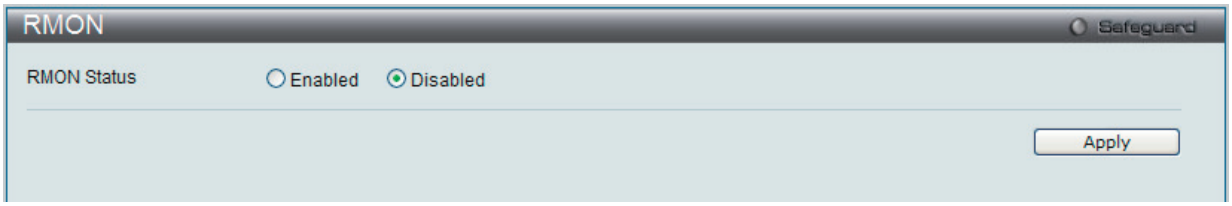


図 6-40　RMON 画面

SNMP に対する RMON を「Enabled」（有効）または「Disabled」（無効）にし、「Apply」ボタンをクリックします。

Time Range Settings（タイムレンジ設定）

スイッチのアクセスプロファイル設定が有効な場合、アクセスプロファイル機能を実行する期間（開始点と終了点）を一週間の特定の曜日によって決定します。本設定は、Access Profile テーブルのアクセスプロファイルに適用されます。64 個のタイムレンジを入力することができます。

注意 タイムレンジ機能は、スイッチの時刻設定をベースにしています。Time と SNTP コマンドのセクションにあるコマンドを使用して適切にスイッチに時刻設定されていることをご確認ください。

Configuration > Time Range 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。

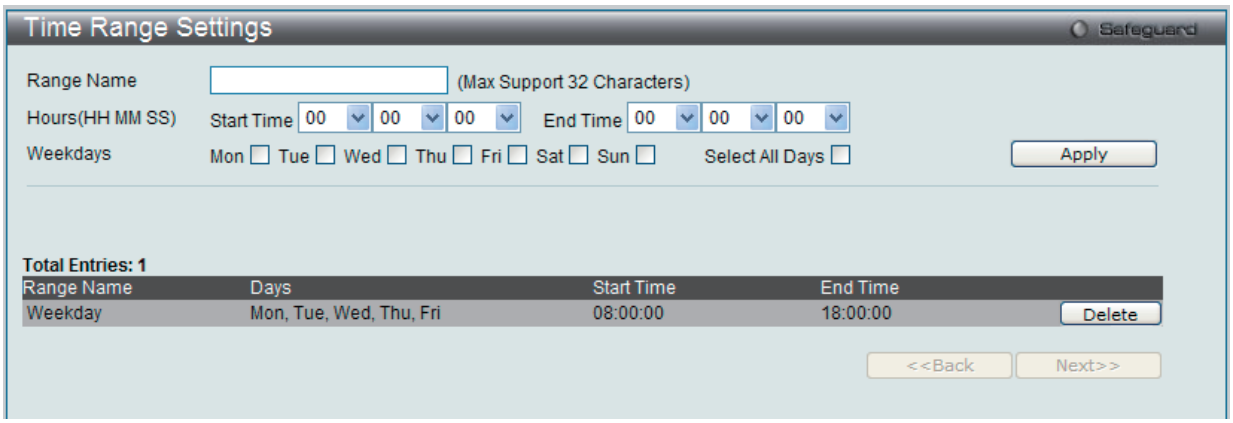


図 6-41　Time Range Settings 画面

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。このレンジ名は Access Profile テーブルで使用され、このタイムレンジで有効であるアクセスプロファイルと関連するルールを識別します。
Hours (HH MM SS)	プルダウンメニューを使用し、タイムレンジの時刻を以下の項目で設定します。 • Start Time - 開始時刻を時間、分、秒（24 時形式）で指定します。 • End Time - 終了時刻を時間、分、秒（24 時形式）で指定します。
Weekdays	チェックボックスを使用し、タイムレンジを有効にする曜日を選択します。「Select All Days」をチェックすると、すべての曜日を設定します。

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
設定したエントリは上記画面下半分にある「Time Range Information」テーブルに表示されます。

Single IP Management（シングル IP マネジメント設定）

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、スタックポートまたはモジュールを使用する代わりにイーサネット経由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。

1. ネットワークを拡大し、増大する帯域幅に対する要求に対処しながら、小規模のワークグループや、ワイヤリングクローゼット（ユーザ接続エリア）を簡単に管理できるようになります。
2. ネットワークに必要な IP アドレス数を減らします。
3. スタック接続のために特別なケーブル配線を必要とせず、他のスタック技術ではトポロジ上の問題になる距離的制限を取り除きます。

D-Link シングル IP マネジメント（以下 SIM と呼びます）機能を搭載するスイッチには、以下の基本的なルールがあります。

- 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 / 無効にできます。また、SIM グループはご使用のネットワーク内でスイッチの操作に影響を与えることはありません。
- SIM には 3 つのクラスのスイッチがあります。Commander Switch（CS）はグループのマスタスイッチ、Member Switch（MS）は 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）は 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です。
- 1 つの SIM グループには、Commander Switch（CS）を 1 つだけ持つことができます。
- 特定の SIM グループ内のすべてのスイッチは、同じ IP サブネット（ブロードキャストドメイン）内にある必要があります。ルータを越えた位置にあるメンバの設定はできません。
- 1 つの SIM グループには、Commander Switch（番号：0）を含めずに、最大 32 台のスイッチ（番号：1-32）が所属できます。
- 同じ IP サブネット（ブロードキャストドメイン）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。
- マルチプル VLAN が設定されていると、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 ホップ以上はな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 3 つの異なる役割を持っています。

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、以下の特長を持っています。
   - IP アドレスを 1 つ持つ。
   - 他のシングル IP 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）- シングル IP グループに所属するスイッチで、CS からアクセスが可能です。MS は以下の特徴を持ちます。
   - 他のシングル IP グループの CS や MS ではない。
   - CS 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。CaS を SIM グループ内の MS として、本スイッチの機能を使用して手動で登録することが可能です。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。
   - 他のシングル IP グループの CS や MS ではない。
   - CS マネジメント VLAN 経由で CS に接続する。

上記の役割には、以下のルールを適用します。

- 各デバイスは、まず CS の状態から始まります。
- CS は、はじめに CaS に、その後 MS となり、SIM グループの MS へと遷移します。つまり CS から MS へ直接遷移することはできません。
- ユーザは、CS から CaS へ手動で遷移させることができます。
- 以下のような場合に MS から CaS に遷移します。
  - CS を介して CaS として設定される時。
  - CS から MS への Report パケットがタイムアウトになった時。
- ユーザが手動で CaS から CS に遷移するように設定できます。
- CS を介して CaS は MS に遷移するように設定されます。

SIM グループの CS として運用するスイッチを 1 台登録した後、スイッチを手動によりグループに追加して MS とします。CS はその後 MS へのアクセスのために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 へのアクセスを制御します。

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する代わりに、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。処理後、CS は MS から Response パケットを受け取り、これを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（リード権 / ライト権、リード権だけを含む）のメンバになります。しかし、自身の IP アドレスを持つ MS 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。

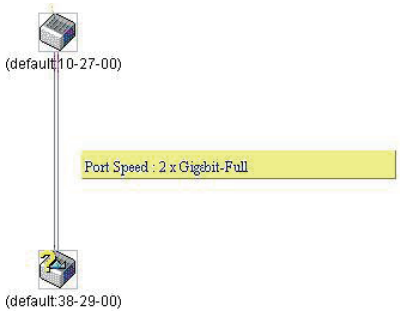
バージョン 1.61 へのアップグレード

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。これはポートトランクグループを構成するイーサネット接続の速度と接続数を表示する機能です。



3. 本バージョンでは、以下のファームウェア、コンフィグレーションファイル、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 サーバから複数の MS に対するファームウェアダウンロードがサポートされました。
- コンフィグレーションファイル : TFTP サーバを使用した複数の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 : 複数のログファイルを 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 **Configuration** > **Single IP Management** > **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。
2. 以下の画面のようにトポロジマップにはポートトランキングのメンバで接続という新しい機能があります。このポートトランキンググループに設定した速度やイーサネット接続数を表示します。

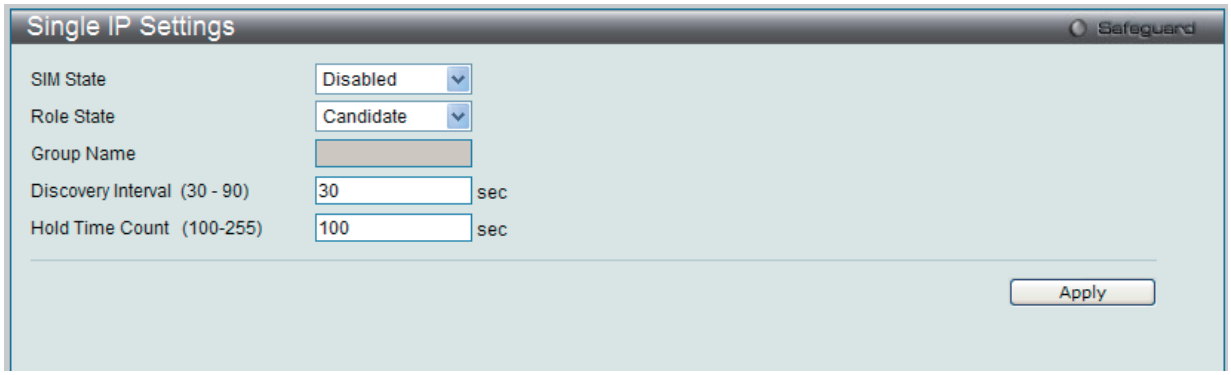


図 6-42　Single IP Settings 画面（CaS 無効状態）

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。「Apply」ボタンをクリックして、設定を有効にします。

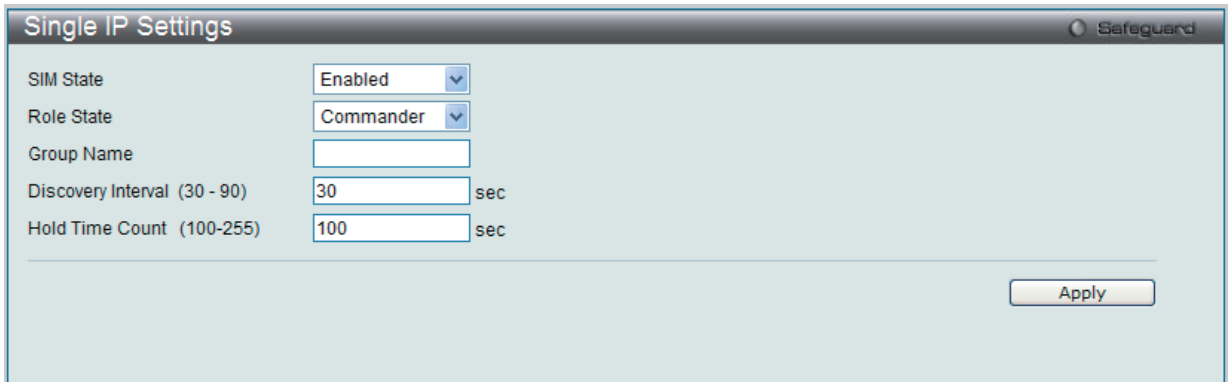


図 6-43　Single IP Settings 画面（CS 有効状態）

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。
Discovery 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 Count (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。

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）

SIM グループ内のスイッチの設定および管理を行います。本画面は表示のためには、ご使用のコンピュータに Java スクリプトが必要です。インストール方法についてはサンマイクロシステムズ社のホームページをご確認ください。

Configuration > **Single IP Management** > **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、以下の画面が表示されます。

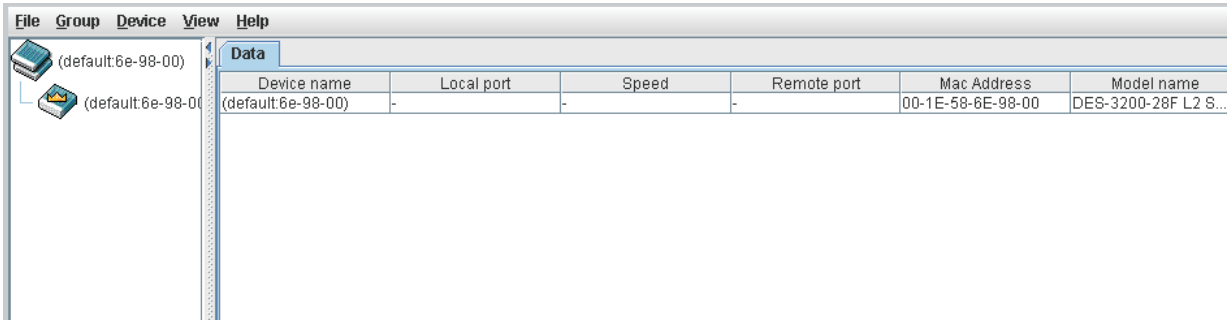


図 6-44　トポロジ画面

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。

トポロジマップの表示

ツールバーの「View」メニューから「Topology」を選択し、以下の画面を表示します。トポロジビューは定期的に（初期値：20 秒）更新されます。

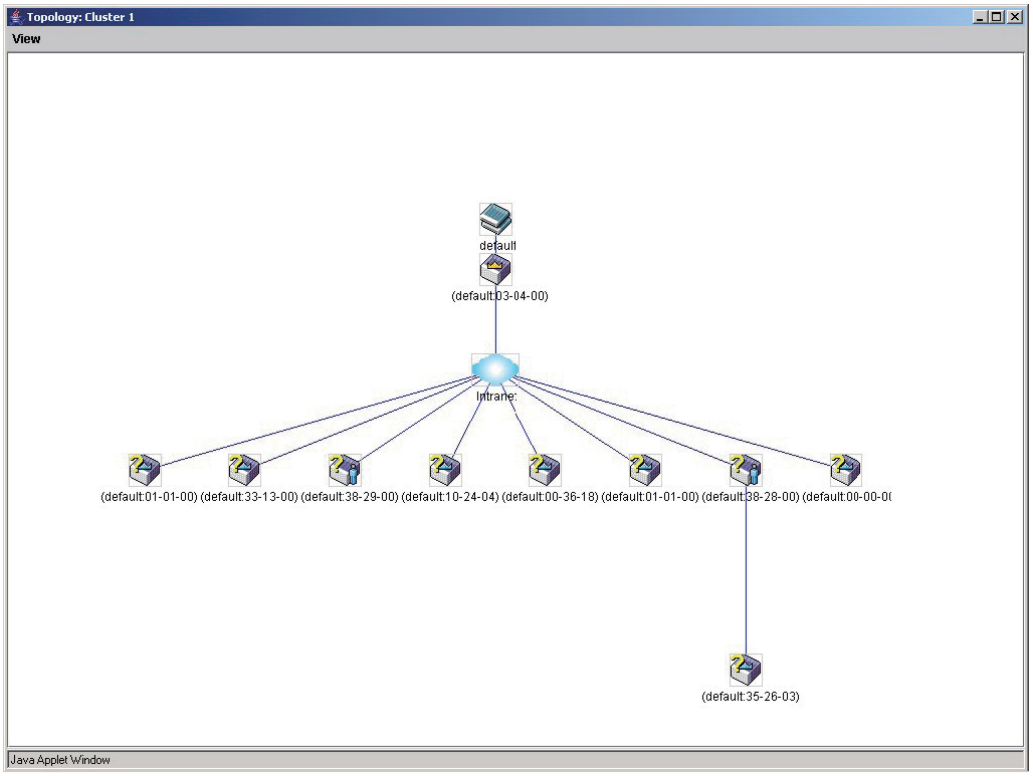
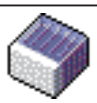


図 6-45　Topology 画面

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

本画面で表示されるアイコンは以下の通りです。

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

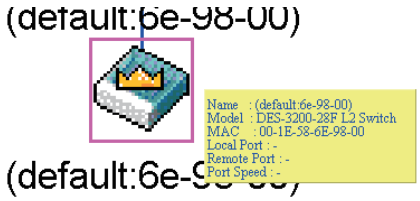


図 6-46　ツールヒントを利用したデバイス情報の表示

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。

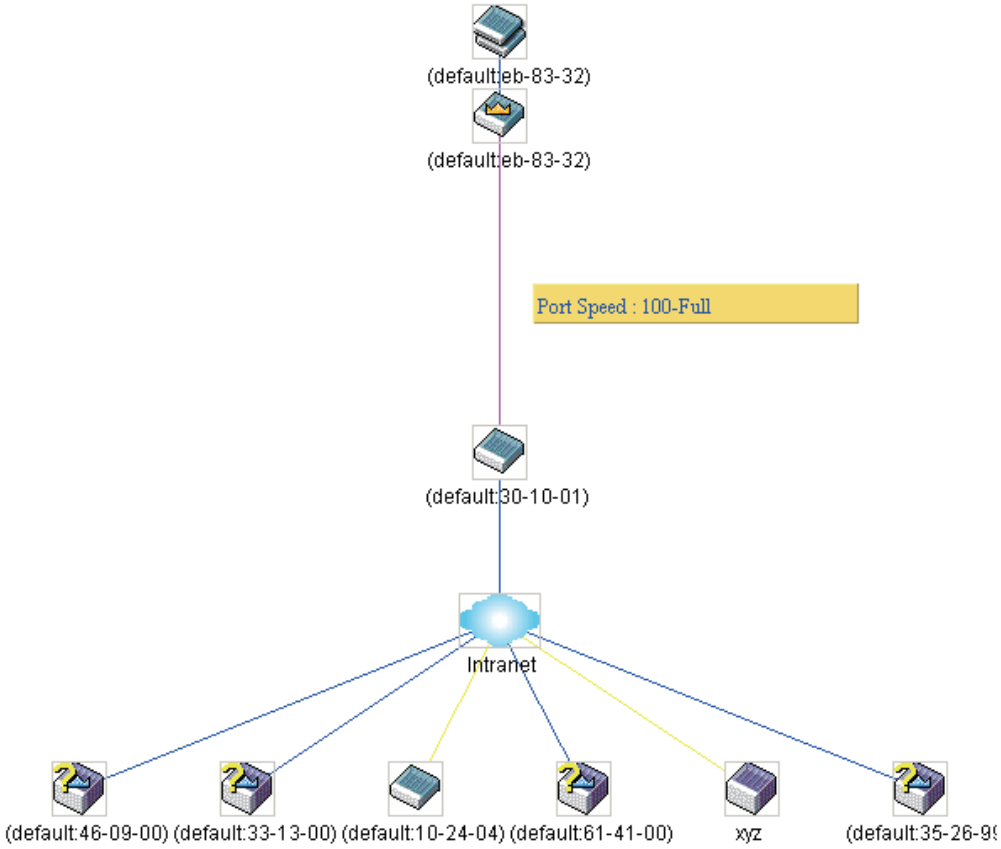


図 6-47　ツールヒントを利用したポート速度の表示

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。

グループアイコン

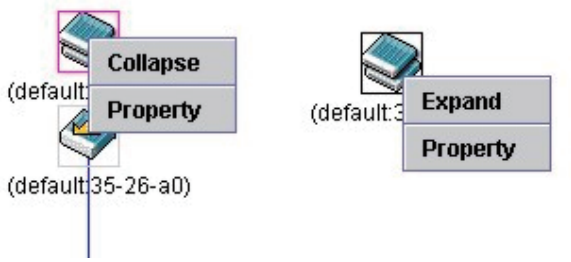


図 6-48　グループアイコン上での右クリック

以下のオプションが表示されます。

- Collapse – グループのアイコンを折りたたみ、1 つのアイコンに代表させます。
- Expand – グループのアイコンを展開し、隠れているすべてのアイコンを表示させます。
- Property – ポップアップ画面が開き、グループ情報を表示します。

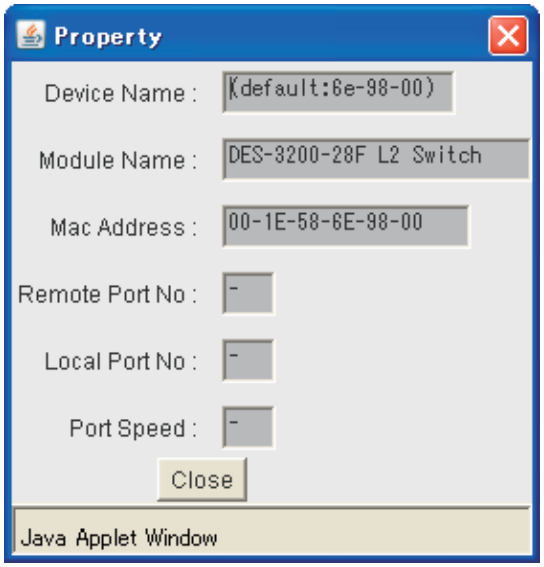


図 6-49　Property 画面

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。

「Close」ボタンをクリックし、「Property」画面を閉じます。

Commander スイッチアイコン

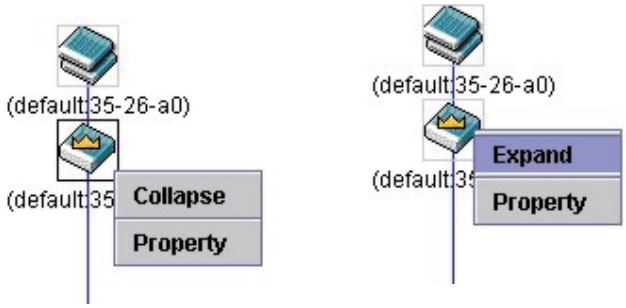


図 6-50　Commander スイッチアイコン上での右クリック

以下のオプションが表示されます。
- Collapse – グループのアイコンを折りたたみ、1 つのアイコンに代表させます。
- Expand – グループのアイコンを展開し、隠れているすべてのアイコンを表示させます。
- Property – ポップアップ画面が開き、グループの情報を表示します。

Member スイッチアイコン

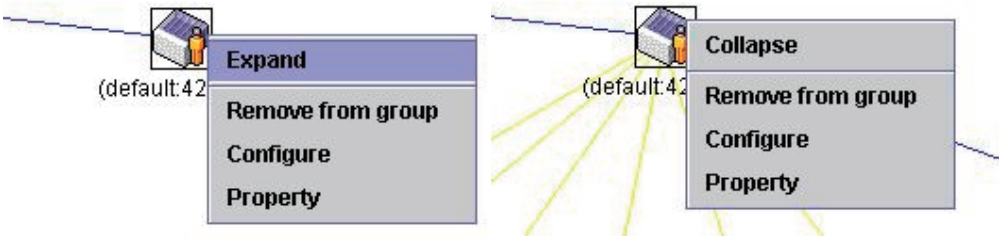


図 6-51　Member スイッチアイコン上での右クリック

以下のオプションが表示されます。
- Collapse – グループのアイコンを折りたたみ、1 つのアイコンに代表させます。
- Expand – グループのアイコンを展開し、隠れているすべてのアイコンを表示させます。
- Remove from group – メンバをグループから削除します。
- Configure - Web 管理機能を起動して、スイッチの設定を可能にします。
- Property – ポップアップ画面が開き、デバイスの情報を表示します。

Candidate スイッチアイコン

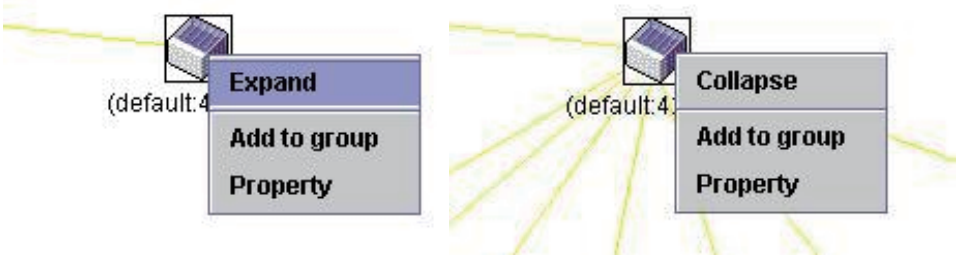


図 6-52　Candidate スイッチアイコン上での右クリック

以下のオプションが表示されます。
- Collapse – グループのアイコンを折りたたみ、1 つのアイコンに代表させます。
- Expand – グループのアイコンを展開し、隠れているすべてのアイコンを表示させます。
- Add to group – CaS をグループに追加します。このオプションを選択すると、以下のパスワード入力画面が表示され、CaS スイッチを SIM グループに追加するための認証を行います。パスワードを入力して「OK」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 6-53　Input password ダイアログボックス

- Property – ポップアップ画面が開き、デバイスの情報を表示します。

メニューバー

「Single IP Management」画面には、デバイスの設定のために以下のようなメニューバーが配置されています。

図 6-54　トポロジビュー内のメニューバー

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 Setup – 印刷イメージを表示します。
- Print Topology – トポロジマップを印刷します。
- Preference – ポーリング間隔、SIM 起動時にオープンするビューなどの表示プロパティを設定します。

「Group」メニュー

- Add to Group – グループに CaS を追加します。このオプションを選択すると、以下のパスワード入力画面が表示され、CaS を SIM グループに追加するための認証を行います。パスワードを入力して「OK」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 6-55　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。

「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。

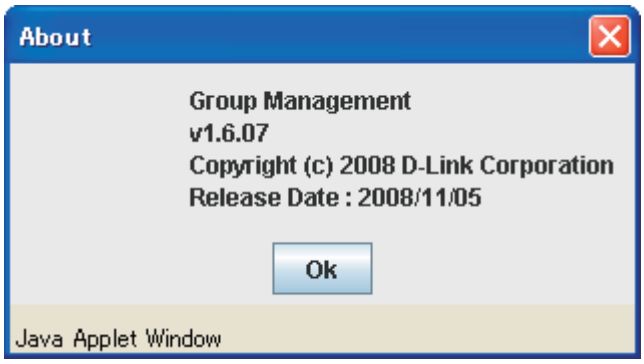


図 6-56　About ダイアログボックス

Firmware Upgrade（ファームウェア更新）

CS から MS へのファームウェアの更新を行います。

Configuration > Single IP Management > 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。

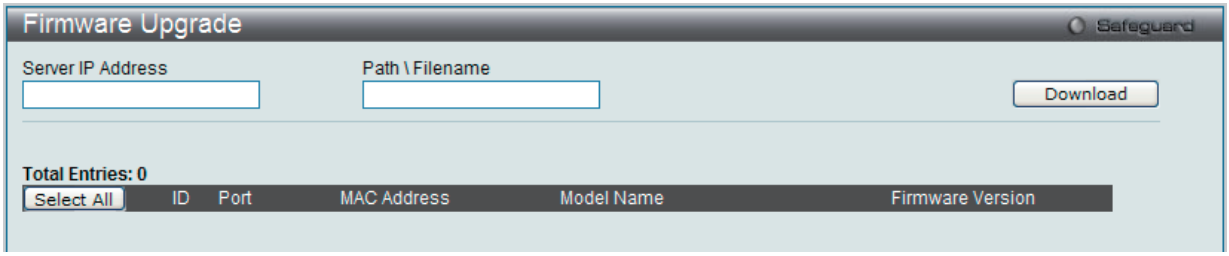


図 6-57　Firmware Upgrade 画面

MS は、「Port」（MS に接続する CS 上のポート）、「MAC Address」、「Model Name」、「Version」の情報と共にリスト表示されます。ダウンロード対象のスイッチは、「Port」欄の下のチェックボックスで選択します。ファームウェアを格納する「Server IP Address」を入力して、ファームウェアの「Path\Filename」を指定します。「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）

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

Configuration > Single IP Management > 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。

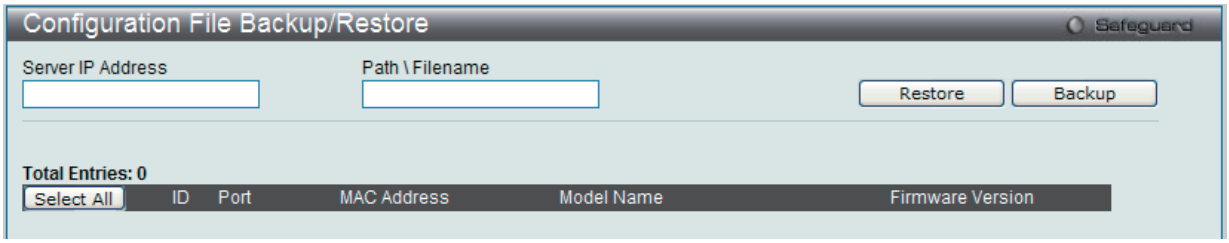


図 6-58　Configuration File Backup/Restore 画面

MS は「Port」（MS に接続する CS 上のポート）、「MAC Address」、「Model Name」、「Version」の情報と共にリスト表示されます。コンフィグレーションファイルのアップデート対象のスイッチは、「Port」欄の下のラジオボタンで選択します。ファームウェアを格納する「Server IP Address」を入力して、ファームウェアの「Path\Filename」を指定します。「Restore」ボタンをクリックすると、TFTP サーバからファイル転送が開始されます。「Backup」ボタンをクリックすると、TFTP サーバにファイルがバックアップされます。

Upload Log File（ログファイルのアップロード）

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います。

Configuration > Single IP Management > 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。

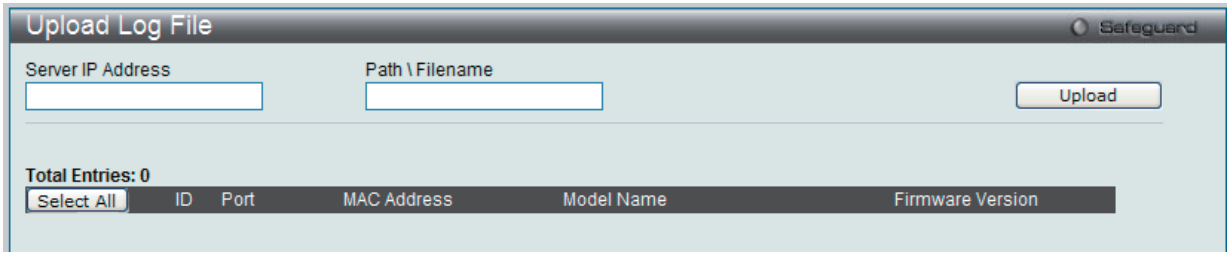


図 6-59　Upload Log File 画面

ログファイルをアップロードするためには、SIM メンバスイッチの IP アドレスと、ログファイルを保存する PC のパスを入力し、「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。

Gratuitous ARP（Gratuitous ARP の設定）

Gratuitous ARP として知られている ARP 通知は、TAP と SPA が等しい場合にそれを送信したホストに有効である SHA と SPA を含むパケット (通常 ARP リクエスト) です。このリクエストは、応答を求めることを意図されたものでなく、パケットを受信する他のホストの ARP キャッシュをまったく更新しません。

本機能は、起動時に多くのオペレーティングシステムで一般的に行われています。これは、ネットワークカードを変更したため、MAC アドレスに対する IP アドレスのマッピングが変更になっていても、他のホストがまだその ARP キャッシュに古いマップを持っているというような問題が発生した場合に、その問題を解決します。

Gratuitous ARP Global Settings（Gratuitous ARP グローバル設定）

Gratuitous ARP のグローバル設定を行います。

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

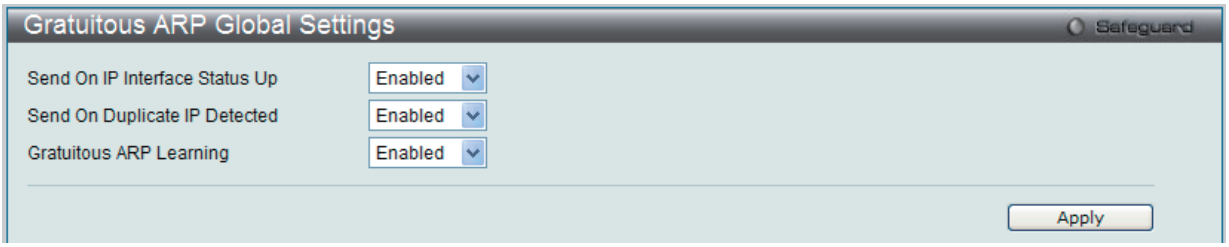


図 6-60　Gratuitous ARP Global Settings 画面

以下の項目を使用して、設定します。

項目	説明
Send On IP Interface Status Up	IP インタフェースの起動中に、Gratuitous ARP リクエストの送信を有効または無効にします。これは、自動的にインタフェースの IP アドレスを他のノードにアナウンスするために使用されます。初期値は「Enabled」（有効）です。
Send On Duplicate IP Detected	重複した IP アドレスが検知された場合の Gratuitous ARP リクエストパケットの送信を有効または無効にします。初期値は「Enabled」（有効）です。検出された重複 IP アドレスは、システム自身の IP アドレスに一致する IP アドレスによって送信された ARP リクエストパケットをシステムが受信したことを意味します。
Gratuitous ARP Learning	受信した Gratuitous ARP パケットに基づいて、ARP キャッシュの更新を有効または無効にします。スイッチが Gratuitous ARP パケットを受信した場合、ARP エントリを追加または更新する必要があります。初期値は「Enabled」（有効）です。

Gratuitous ARP 設定に変更を行った場合には、「Apply」ボタンをクリックします。

Gratuitous ARP Settings（Gratuitous ARP 設定）

Gratuitous ARP の詳細な設定を行います。

Configuration > Gratuitous ARP > Gratuitous ARP 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。

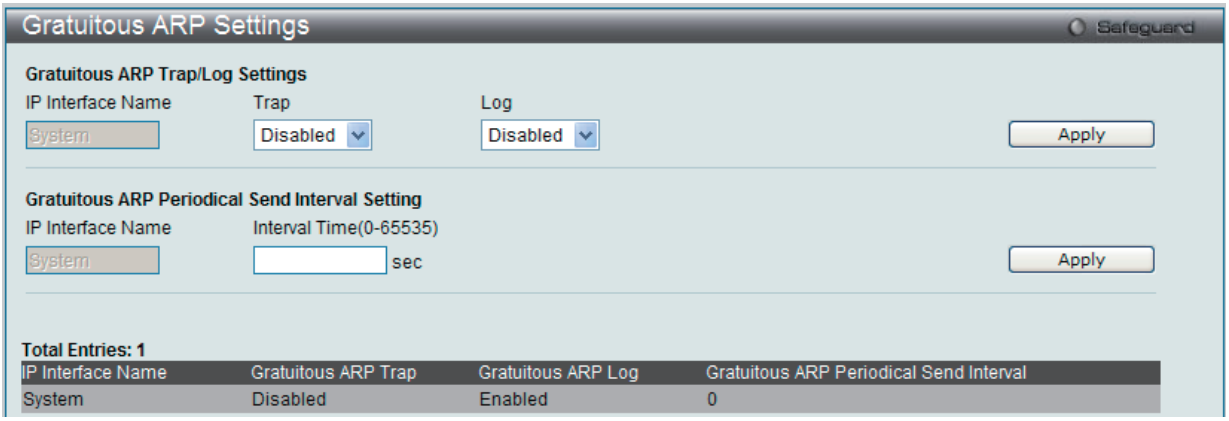


図 6-61　Gratuitous ARP Settings 画面

以下の項目を使用して、設定します。

項目	説明
Gratuitous ARP Trap/Log Settings	
Trap	スイッチは、IP の重複イベントをトラップし、管理者に通知します。初期値では、トラップは無効です。
Log	スイッチは、IP の重複イベントのログを取得し、管理者に通知します。初期値では、ログは有効です。
IP Interface Name	編集するインタフェース名を表示します。
Gratuitous ARP Periodical Send Interval Settings	
IP Interface Name	編集するインタフェース名を表示します。
Interval Time (0-65535)	Gratuitous ARP リクエストパケットの定期な送信間隔を設定します。初期値は 0(秒) です。

「Apply」ボタンをクリックし、変更を有効にします。

ARP Spoofing Prevention Settings（ARP Spoofing 防止設定）

ARP を汚染することで知られている ARP スプーフィングは、イーサネットネットワークを攻撃する方法で、DoS(Denial of Service) として知られているように、攻撃者は LAN 上のデータフレームをかぎつけてトラフィックを編集し、またはトラフィックを停止させてしまう可能性があります。ARP スプーフィングの原則は、偽造または改ざんした ARP メッセージをイーサネットネットワークに送信することです。一般に、目的は、デフォルトゲートウェイなどの別のノードの IP アドレスに攻撃者がでたらめの MAC アドレスを割り当ててしまうことです。その IP アドレスに向かう予定だったトラフィックが、攻撃者に指定されたノードに誤ってリダイレクトされてしまいます。

スイッチは、ARP スプーフィング攻撃を防ぐためにパケットコンテンツ ACL を使用して、偽造されたゲートウェイの MAC と IP バインディングを含む不正な ARP パケットを防御します。

Configuration > ARP Spoofing 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。

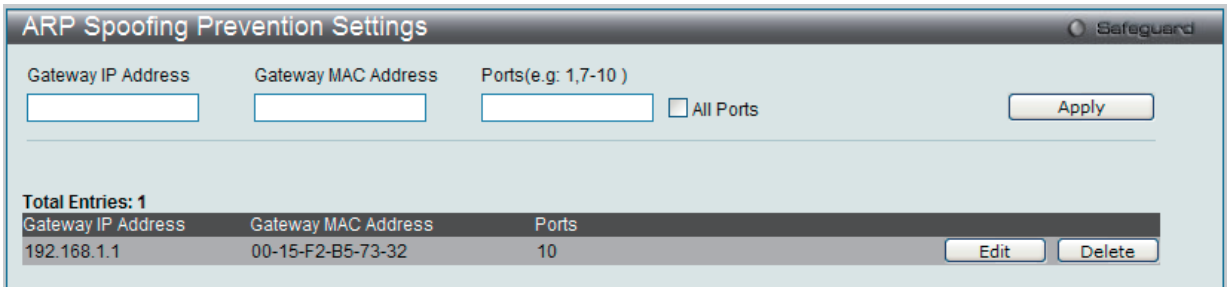


図 6-62　ARP Spoofing Prevention Settings 画面

以下の項目を使用して、設定します。

項目	説明
Gateway IP Address	ゲートウェイの IP アドレスを入力します。
Gateway MAC Address	ゲートウェイの MAC アドレスを入力します。
Ports (e.g.: 1, 7-10)	ARP Spoofing Prevention 設定を行うスイッチのポートを指定します。「All Ports」を指定すると、本エントリをスイッチのすべてのポートに設定します。

エントリの編集

1. 編集エントリの「Edit」ボタンをクリックし、以下の画面を表示します。

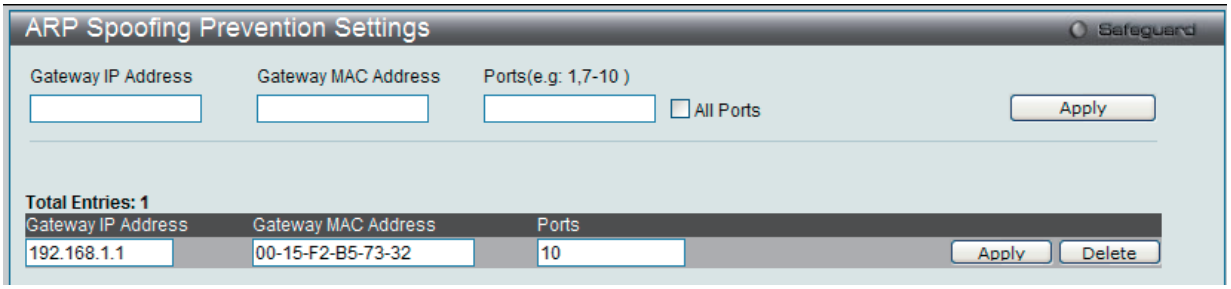


図 6-63　ARP Spoofing Prevention Settings 画面 - Edit

2. 項目を編集し、「Apply」ボタンをクリックし、変更を適用します。

PPPoE Circuit ID Insertion Settings（PPPoE Circuit ID の挿入）

本設定を有効にすると、システムは、受信した PPPoE Discovery および Request パケットにタグがない場合に Circuit ID タグを挿入します。また、受信 PPPoE Offer および Session Confirmation パケットから Circuit ID タグを削除します。

挿入する Circuit ID は次の情報を含んでいます。: クライアント MAC アドレス、Device ID、およびポート番号。
さらに、ユーザが定義する文字列のオプションを Circuit ID に挿入できます。初期値では、スイッチの IP アドレスが、Circuit ID オプションをコード化するためにデバイス ID として使用されます。

Configuration > PPPoE Circuit ID Insertion 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。

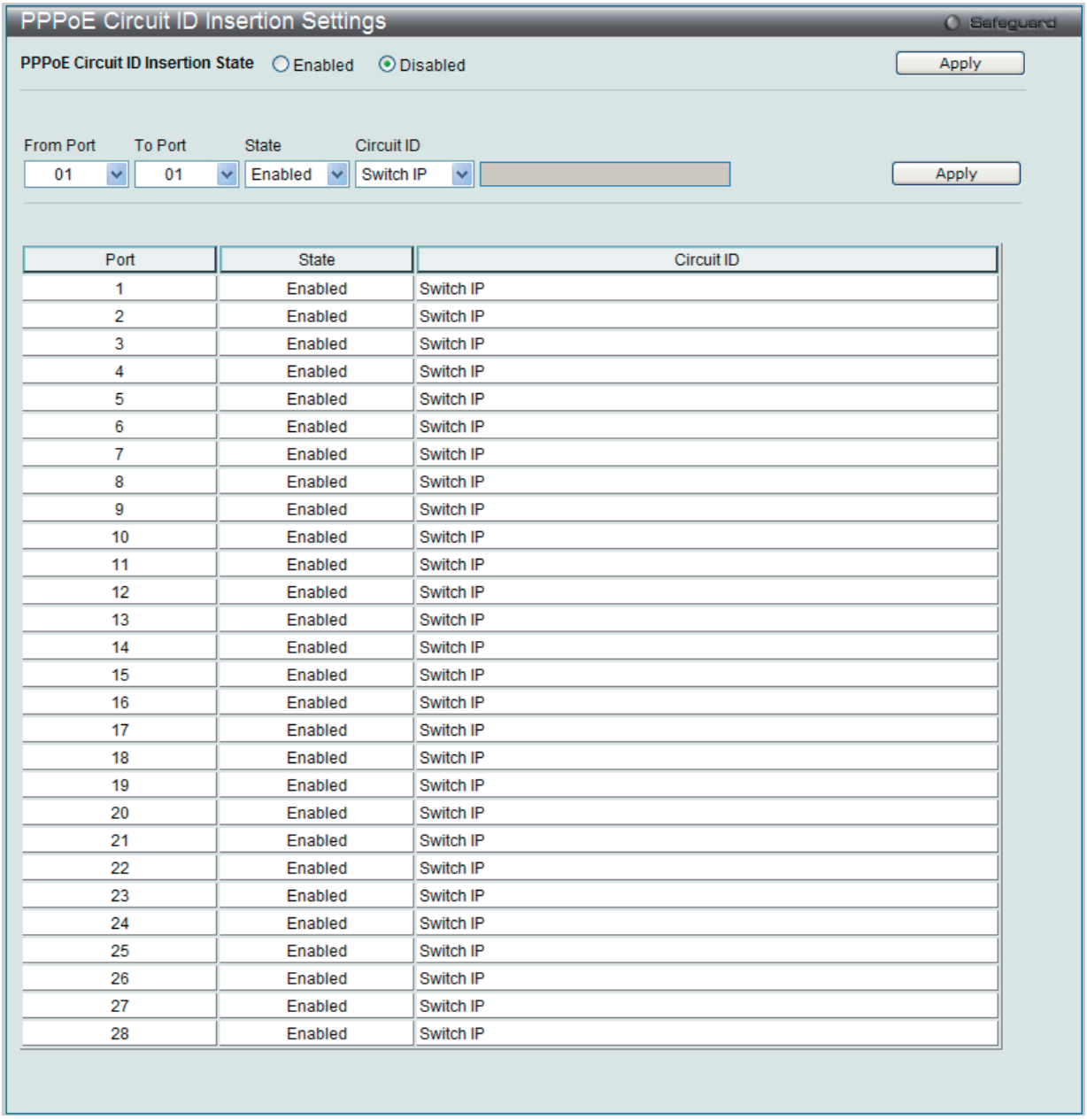


図 6-64　PPPoE Circuit ID Insertion 画面

以下の項目を使用して、設定します。

項目	説明
From Port / To Port	設定するポートを指定します。
State	選択ポートにおける PPPoE Circuit ID の挿入を有効または無効にします。
Circuit ID	Circuit ID のコード化のオプションに使用するデバイスの ID を選択します。以下のオプションが利用できます。 • Switch MAC - スイッチの MAC アドレスが Circuit ID の暗号化のオプションに使用されます。 • Switch IP - スイッチの IP アドレスが Circuit ID の暗号化のオプションに使用されます。（初期値） • UDF String - ユーザ定義の文字列（32 文字以内）が Circuit ID の暗号化のオプションに使用されます。

「Apply」ボタンをクリックし、変更を有効にします。

第 7 章　L2 Features（L2 機能の設定）

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

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

サブメニュー	説明	参照ページ
Jumbo Frame（ジャンボフレームの有効化）	ジャンボフレーム機能を有効 / 無効にします。	85 ページ
802.1Q Static VLAN（802.1Q スタティック VLAN 設定）	802.1Q スタティック VLAN 設定を行います。	92 ページ
QinQ（QinQ 設定）	Q-in-Q 機能を有効または無効にします。	95 ページ
802.1v Protocol VLAN（802.1v プロトコル VLAN）	802.1v プロトコル VLAN 設定を行います。	97 ページ
VLAN Trunk Settings（VLAN トランク設定）	多くの VLAN ポートを集約して VLAN トランクを作成します。	100 ページ
GVRP Settings（GVRP の設定）	VLAN 構成情報を共有するために GVRP 設定を行います。	101 ページ
Asymmetric VLAN Settings（Asymmetric VLAN 設定）	Asymmetric VLAN を設定します。	102 ページ
MAC-based VLAN Settings（MAC ベース VLAN 設定）	MAC ベース VLAN を設定します。	102 ページ
PVID Auto Assign Settings（PVID 自動割り当て設定）	PVID 自動割り当てを設定します。	103 ページ
Port Trunking（トランキングの設定）	ポートトランキング設定を行います。	103 ページ
LACP Port Settings（LACP の設定）	ポートトランキンググループを設定します。	106 ページ
Traffic Segmentation（トラフィックセグメンテーション）	トラフィックフローの分割設定を行います。	107 ページ
L2PT Settings（レイヤ 2 プロトコルトンネリング設定）	レイヤ 2 プロトコルトンネリング設定を行います。	107 ページ
BPDU Protection Settings（BPDU アタック防止設定）	ポートに BPDU 防止機能を設定します。	108 ページ
IGMP Snooping（IGMP Snooping の設定）	IGMP Snooping 機能を設定します。	109 ページ
MLD Snooping Settings（MLD Snooping 設定）	MLD Snooping 機能を設定します。	117 ページ
Port Mirror（ポートミラーリングの設定）	ポートミラーリングの設定を行います。	120 ページ
Loopback Detection Settings（ループバック検知設定）	ループバック検知機能の設定を行います。	121 ページ
Spanning Tree（スパニングツリーの設定）	スパニングツリープロトコルの設定を行います。	122 ページ
Forwarding & Filtering（フォワーディングとフィルタリングの設定）	ユニキャスト / マルチキャストフォワーディングとフィルタリングの設定を行います。	131 ページ
NLB Settings（ネットワークロードバランシング設定）	ネットワークロードバランシング設定を行います。	133 ページ
LLDP（LLDP 設定）	LLDP 設定を行います。	134 ページ
Ethernet OAM（イーサネット OAM）	OAM 設定を行います。	138 ページ
CFM（Connectivity Fault Management : 接続性障害管理）	CFM 設定を行います。	140 ページ
ERPS Settings（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有効にします。	148 ページ

以下では、VLAN 機能、トランキング、IGMP Snooping、MLD Snooping、スパニングツリーなどユーザがスイッチに L2 機能について説明します。

Jumbo Frame（ジャンボフレームの有効化）

ジャンボフレームにより、同じデータを少ないフレームで転送することができます。有効にすると、最大 2048 バイトを持つジャンボフレーム (1536 バイトの標準イーサネットフレームより大きいサイズのフレーム) の送信が可能になります。

ここでは、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。

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

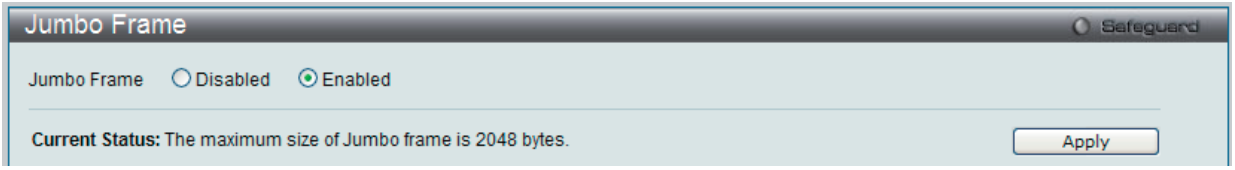


図 7-1　Jumbo Frame 画面

本画面には次の項目があります。

項目	説明
Jumbo Frame	ジャンボフレームを扱うかどうかを設定します。最大フレームサイズは 2048 バイトです。 • Enabled - デバイスでジャンボフレームを有効に設定します。 • Disabled - デバイスでジャンボフレームを無効に設定します。（初期値）

「Enabled」または「Disabled」を設定し、「Apply」ボタンをクリックします。

802.1Q VLAN 設定

IEEE 802.1p プライオリティについて

プライオリティのタグ付けは、IEEE 802.1p 標準規格で定義され、何種類ものデータが同時に送受信されるようなネットワーク内のトラフィックを管理するための方法です。本機能は混雑したネットワーク上でのタイムクリティカルなデータの伝送時に発生する問題を解決するために開発されました。例えばビデオ会議のような、データに依存するタイプのアプリケーションの品質は、ほんの少しの伝送遅延にも多大な影響を受けてしまいます。

IEEE 802.1p 標準規格に準拠するネットワークデバイスは、データパケットのプライオリティレベル（優先度）を認識することができます。また、これらのデバイスはパケットに対してプライオリティレベルやタグを割り当てることができ、パケットからタグを取り外すことも可能です。このプライオリティタグ（優先タグ）は、パケットの緊急度を決定し、またそのパケットがどのキューに割り当てられるかを決定します。

プライオリティタグは、0 から 7 までの値で示され、0 が最も低い優先度、7 が最も高い優先度を表します。一般的に、7 番のプライオリティタグは、少しの遅延にも影響されやすい音声や映像に関わるデータに対して、またはデータ転送速度が保証されているような特別なユーザに対して使用されます。プライオリティを与えられないパケットはキュー 0 に割り当てられ、最も低い送信優先度となります。

スイッチは Strict モードと WRR（重み付けラウンドロビン）システムをサポートし、それによりキューからパケットを送信する速度を決定します。速度の対比は 4 : 1 と設定されています。これは、最高のプライオリティのキュー（キュー 7）が 4 つのパケットを送信する間に、キュー 0 では 1 つのパケットを送信することを意味しています。

プライオリティキューの設定はスイッチ上のすべてのポートに対して行われるため、スイッチに接続されるすべてのデバイスがその影響を受けることに注意してください。このプライオリティキューイングシステムは、ご使用のネットワークがプライオリティタグ割り当て機能をサポートする場合、この機能は特にその効果を発揮します。

VLAN について

VLAN（Virtual Local Area Network : 仮想 LAN）とは、物理的なレイアウトではなく、論理的なスキームに従って構成されるネットワークトポロジです。VLAN は LAN セグメントの集まりを自律的なユーザグループへと結合させて、1 つの LAN のように見せるために使用します。また VLAN は VLAN 内のポート間にのみパケットが送信されるように、ネットワークを異なるブロードキャストドメインに論理的に分割します。一般的には 1 つの VLAN は 1 つのサブネットと関連付けられますが、必ずしもそうである必要はありません。

VLAN では、帯域を浪費せずにパフォーマンスを強化し、トラフィックを特定のドメイン内に制限することにより、セキュリティを増強します。

VLAN はエンドノードを物理的位置ではなく、論理的に束ねた集合体です。頻繁に通信を行うエンドノード同士は、それらのネットワーク上の物理的位置に関わらず、同じ VLAN を割り当てます。論理的には、VLAN とブロードキャストドメインは等しいと言えます。これは、ブロードキャストパケットはブロードキャストが行われた VLAN 内のメンバにのみ送信されるためです。

本スイッチにおける VLAN について

本スイッチにおける VLAN の特長は以下の通りです。

- どんな方法でエンドノードの識別を行い、エンドノードに VLAN メンバシップを割り当てたとしても、VLAN 間にルーティング機能を持つネットワークデバイスが存在しない限り、パケットは VLAN に所属しないポートに送信されることはありません。
- 本スイッチは、IEEE 802.1Q VLAN とポートベース VLAN をサポートしています。ポートアンタギング機能は、パケットヘッダから 802.1Q タグを取り外すことにより、タグを理解しないデバイスとの互換性を保ちます。
- スイッチの初期状態では、すべてのポートに「default」と名付けられた 802.1Q VLAN が割り当てられています。
  - 「default」VLAN の VID は 1 です。

IEEE 802.1Q VLAN

用語の説明

項目	内容
タグ付け	パケットのヘッダに 802.1Q VLAN 情報を挿入すること。
タグ取り	パケットのヘッダから 802.1Q VLAN 情報を削除すること。
Ingress ポート	スイッチ上のパケットを受信するポート。VLAN の照合が行われます。
Egress ポート	スイッチ上のパケットを送信するポート。タグ付けの決定が行われます。

本スイッチ上では IEEE 802.1Q（タグ付き）VLAN が実装されています。ネットワーク上のすべてのスイッチが IEEE 802.1Q 準拠である場合、ネットワーク全体に 802.1Q VLAN が有効となります。

VLAN はネットワークを分割し、ブロードキャストドメインのサイズを縮小します。ある VLAN に到着するすべてのパケットは、（IEEE 802.1Q をサポートするスイッチを通して）その VLAN のメンバであるステーションに送信されます。これには、送信元の不明なブロードキャスト、マルチキャスト、ユニキャストパケットも含まれます。

さらに、ネットワークでのセキュリティ機能を提供します。IEEE 802.1Q VLAN は、VLAN メンバであるステーションにのみパケットを送信します。

すべてのポートは、タグ付け / タグなしに設定されます。IEEE 802.1Q VLAN のタグ取り機能は、パケットヘッダ中の VLAN タグを認識しない旧式のスイッチとの連携に使用されます。タグ付け機能により、複数の 802.1Q 準拠のスイッチを 1 つの物理コネクションで結びつけ、すべてのポート上でスパニングツリーを有効にします。

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

IEEE 802.1Q 標準規格の主な機能は以下の通りです。
- フィルタリングによりパケットを VLAN に割り当てます。
- 全体で 1 つのスパニングツリーが構成されていると仮定します。
- 1 レベルのタグ付けによるタグ付けを行います。
- 802.1Q VLAN のパケット転送

パケットの転送は以下の 3 種類のルールに基づいて決定されます。
- Ingress ルール - 受け取ったパケットがどの VLAN に所属するかの分類に関するルール。
- ポート間のフォワーディングルール - 転送するかしないかを決定します。
- Egress ルール - パケットが送信される時にタグ付きかタグなしかを決定します。

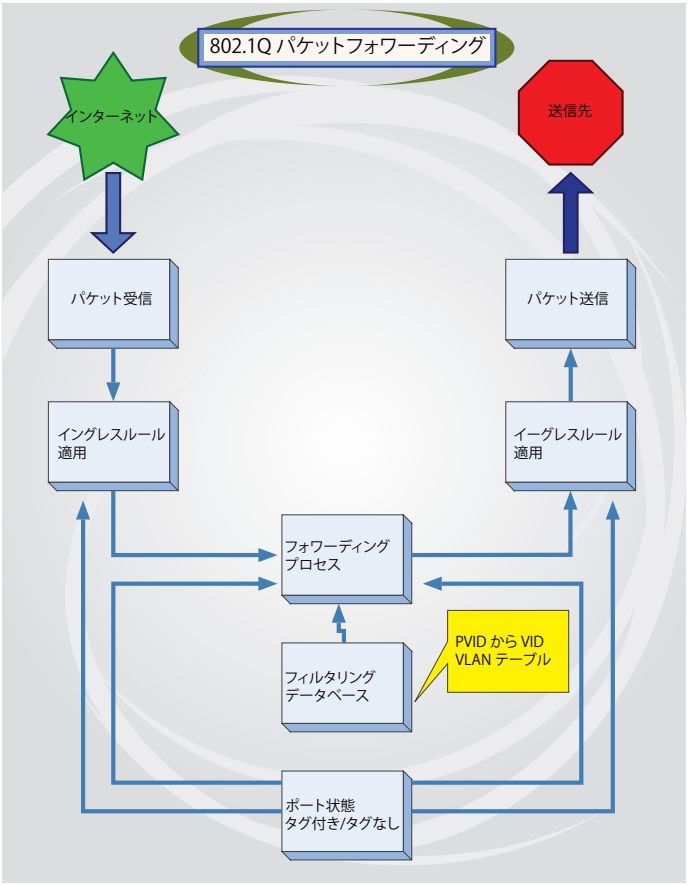


図 7-2　IEEE 802.1Q パケットフォワーディング

802.1Q VLAN タグ

次の図は 802.1Q VLAN のタグについて表示しています。ソース MAC アドレスの後に 4 オクテットのフィールドが挿入されています。それらが存在する場合、EtherType フィールドの値は 0x8100 になります。つまり、パケットの EtherType フィールドが 0x8100 と等しい時に、パケットには IEEE 802.1Q/802.1p タグが含まれています。タグは以下の 2 オクテットに含まれていてユーザプライオリティの 3 ビット、CFI（Canonical Format Identifier: トークンリングパケットをカプセル化してイーサネットバックボーンをはさんで転送するためのもの）の 1 ビット、および VID（VLAN ID）の 12 ビットからなります。ユーザプライオリティの 3 ビットは 802.1p によって使用されます。VID は VLAN を識別するためのもので 802.1Q 標準によって使用されます。VID は長さ 12 ビットなので 4094 のユニークな VLAN を構成することができます。
タグはパケットヘッダに埋め込まれ、パケット全体は 4 オクテット長くなります。そして、元々のパケットに含まれていた情報のすべてが保持されます。

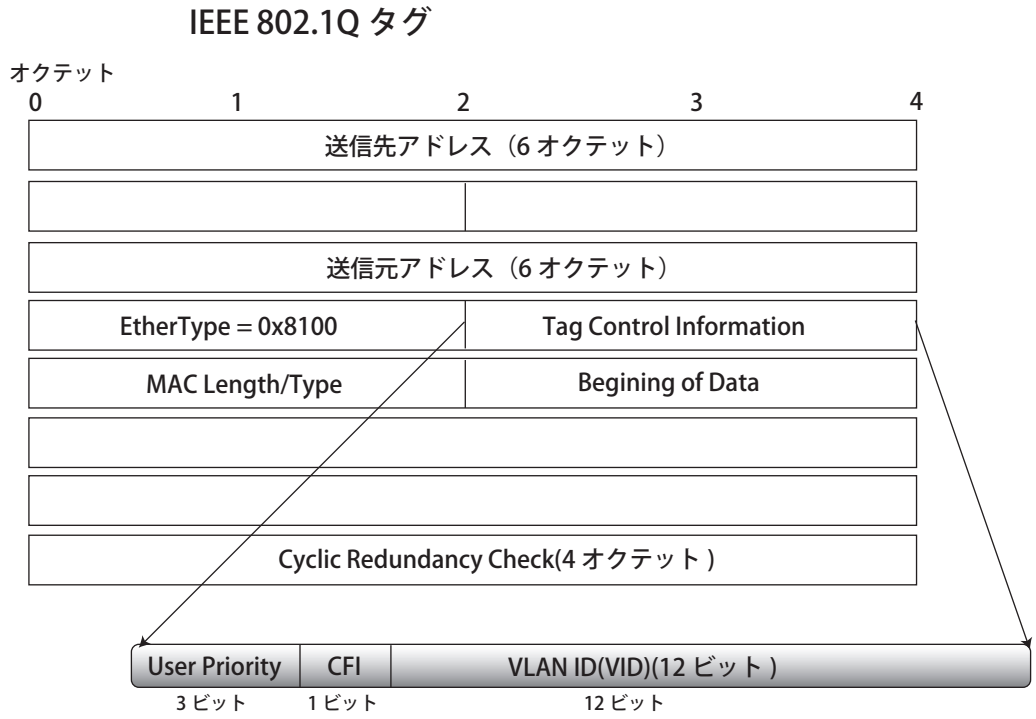


図 7-3　IEEE 802.1Q タグ

EtherType と VLAN ID はソース MAC アドレスと元の EtherType/Length か Logical Link Control の間に挿入されます。パケットよりは元のパケット長よりも少し長くなるので、CRC は再計算されます。

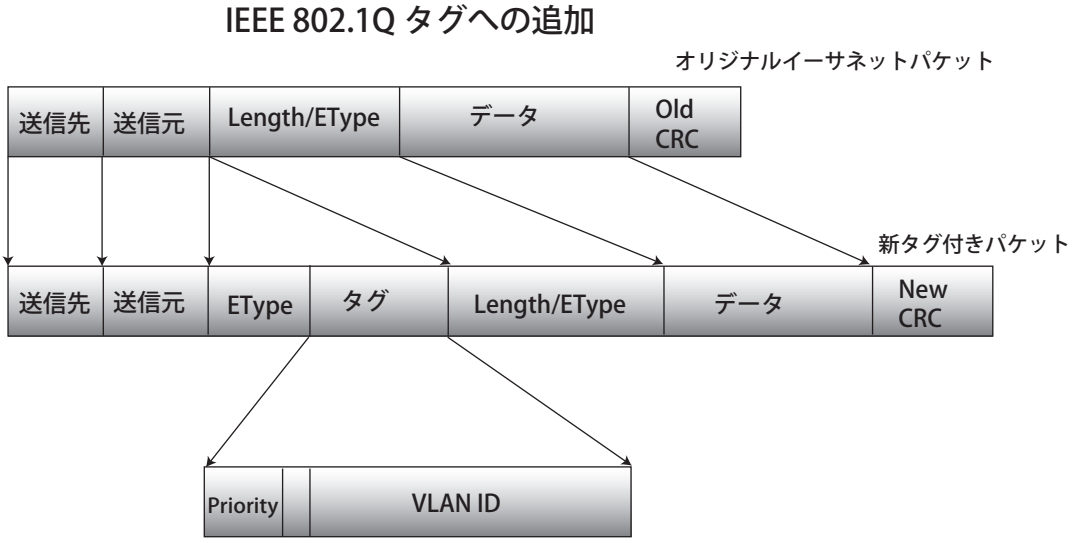


図 7-4　IEEE 802.1Q タグの挿入

ポート VLAN ID

802.1Q VID 情報を持ったタグを付けられたパケットは、802.1Q に対応したネットワークデバイスから他のデバイスまでは完全な VLAN 情報を保持したまま転送することができます。これにより、すべてのネットワークデバイスが 802.1Q に準拠していればネットワーク全体をまるごと 802.1Q VLAN で結ぶことができます。

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

802.1Q VLAN が採用される以前は、ポートベースや MAC ベースの VLAN が主流でした。これらの VLAN でのパケット送信はポート VLAN ID（PVID）を元に行われます。あるポートで受信したパケットには、そのポートの PVID を割り当てて、パケットの宛先アドレス（スイッチのフォワーディングテーブルで参照）へと送信されます。もしパケットを受信したポートの PVID がパケットの宛先ポートの PVID と異なる場合は、スイッチはそのパケットを廃棄します。

スイッチ内では、異なる PVID とは異なる VLAN を意味しています。（2 つの VLAN は外部ルータなしでは通信ができません。）そのため PVID をベースにした VLAN の識別はスイッチ外へ広がる（またはスイッチスタックの）VLAN を実現することができません。

スイッチのすべての物理ポートは PVID を持っています。802.1Q にも PVID が割り当てられ、スイッチ内で使用されます。スイッチ上に VLAN が定義されていなければ、すべてのポートはデフォルト VLAN と PVID 1 が割り当てられます。タグなしのパケットはそれらを受信したポートの PVID を割り当てられます。フォワーディングはこの PVID を元に決定され、タグ付きのパケットはタグ中に含まれる VID に従って送信されます。タグ付きのパケットにも PVID が割り当てられますが、パケットフォワーディングを決定するのは PVID ではなく VID です。

tag-aware（タグ認識可能）のスイッチはスイッチ内の PVID とネットワークの VID を関係付けるテーブルを保持しなければなりません。スイッチは送信されるパケットの VID と、パケット送信を行うポートの VID を比較します。この 2 つが一致しない場合、スイッチはこのパケットを廃棄します。タグなしパケット用に PVID が存在し、またタグ付きパケット用に VID が存在するので、タグを認識するネットワークデバイスも認識しないデバイスも、同じネットワーク内に共存が可能になります。

PVID は 1 ポートに 1 つしか持てませんが、VID はスイッチの VLAN テーブルメモリが可能なだけ持つことができます。

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

タギングとアンタギング

802.1Q 対応のスイッチの全ポートは、タグ付きかタグなしに設定できます。
タグ付きのポートは受信、送信するすべてのパケットのヘッダに、VID、プライオリティ、そしてそのほかの VLAN 情報を埋め込みます。パケットが既にタグ付けされていたなら、VLAN 情報を完全に保つためにポートはパケットを変更しません。ネットワーク上の他の 802.1Q 対応デバイスも、タグの VLAN 情報を使用してパケットの転送を決定します。
タグなしのポートは、受信、送信するすべてのパケットから 802.1Q タグを削除します。パケットに 802.1Q VLAN タグがなければ、ポートはパケットを変更しません。つまり、タグなしのポートが受信して、転送したすべてのパケットは 802.1Q VLAN 情報をまったく持ちません。PVID はスイッチの内部で使用されるだけです。タグなしはパケットを 802.1Q 対応のデバイスから、非対応のデバイスにパケットを送信するのに使用します。

Ingress フィルタリング

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

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

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

本プロセスは、Ingress フィルタリングと呼ばれ、同じ Ingress ポートと同じ VLAN 上のものではないパケットを受信時に廃棄することにより、スイッチ内での帯域を有効利用するために使用されます。これにより送信先ポートに届いてから廃棄されるだけとなるパケットを事前に処理することができるようになります。

デフォルト VLAN

スイッチでは、最初に「default」という名で VID が 1 の VLAN が設定されています。本製品の初期設定ではスイッチ上のすべてのポートが「default」に割り当てられています。

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

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

VLAN の設定例を以下に示します。

表 7-1　VLAN 設定例 – ポートの割り当て

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

ポートベース VLAN

ポートベース VLAN は、スイッチで送受信するトラフィックを制限します。あるポートに接続するすべてのデバイスは、スイッチにコンピュータが 1 台のみ直接接続されている場合でも、ある部署全体が接続されている場合でも、そのポートが所属する VLAN のメンバである必要があります。

ポートベース VLAN では、NIC はパケットヘッダ内の 802.1Q タグを識別できる必要はありません。NIC は通常のイーサネットパケットを送受信します。もしパケットの送信先が同じセグメント上にあれば、通信は通常のイーサネットプロトコルを使用して行われます。通常このように処理が行われますが、パケットの送信先が他のスイッチのポートである場合、スイッチがパケットを廃棄するか、転送を行うかは VLAN の照会を行い決定します。

VLAN セグメンテーション

あるデバイスの VLAN 2 に所属するポート 1 から送信されるパケットを例に説明します。もし、宛先があるポートである場合（通常のフォワーディングテーブル検索により発見）、スイッチはそのポート（ポート 10）は VLAN2 に所属しているか、否か（つまり VLAN 2 パケットを受け取れるか）どうかを確認します。ポート 10 が VLAN 2 のメンバでない場合は、スイッチはそのパケットを廃棄します。メンバである場合、パケットは送信されます。このように VLAN 基準にそった送信選択機能により VLAN セグメントネットワークが成り立っています。重要なのは、ポート 1 は VLAN 2 にのみ送信を行うということです。

プリンタやサーバなどのネットワーク機器は VLAN をまたいで共有することができます。これは VLAN を重複して設定することにより実現されています。つまり、ポートが複数の VLAN グループに所属することができるということです。例えば、VLAN 1 メンバをポート 1,2,3,4 に設定し、VLAN 2 メンバをポート 1,5,6,7 に設定することで、ポート 1 は 2 つの VLAN グループに所属するようになります。ポート 8,9,10 にはどの VLAN グループに対しても設定を行っておらず、この時、ポート 8、9、10 は、同じ VLAN グループに所属しています。

VLAN とトランクグループ

トランクグループに属するメンバは、同じ VLAN 設定内容を持っています。トランクグループメンバの VLAN 設定は他のメンバのポートにも適用されます。

注意 VLAN セグメンテーションをポートトランクグループと併用するためには、まずポートトランクグループの設定を行った後、VLAN 設定を行ってください。設定済みの VLAN のポートトランクグループを変更する場合、ポートトランクグループの設定を変更した後、VLAN 設定を変更する必要はありません。VLAN 設定は、ポートトランクグループの変更に伴って自動的に変更されます。

Q-in-Q VLAN（Q-in-Q VLAN 設定）

Q-in-Q VLAN またはダブル VLAN と呼ばれる技術を利用することにより、ネットワークプロバイダは規模の大きい包括的な VLAN の中に、顧客用の VLAN を設置し、VLAN 構成に新しい階層を導入することにより、その規模を拡張することができます。基本的には大規模な ISP のネットワーク内に、レイヤ 2 の VPN（Virtual Private Network）および、顧客用の透過型 LAN を配置することにより、クライアント側の構造を複雑にすることなく、複数の顧客の LAN を接続します。構造の複雑化が回避できるだけでなく、4000 以上の VLAN を定義できるようになるため、VLAN ネットワークを大幅に拡張し、複数の VLAN を使用する顧客数を増やすことができます。

Q-in-Q VLAN とは、基本的には既存の IEEE 802.1Q VLAN タグ中に挿入する VLAN タグのことで、SPVID（Service Provider VLAN ID）と呼ばれます。これらの VLAN タグは TPID（Tagged Protocol ID）でマークされ、16 進数形式で設定され、パケットの VLAN タグの内部にカプセル化されます。パケットは 2 つタグ付けされ、ネットワーク上の他の VLAN とは区別されます。このように 1 つのパケットの中に VLAN の階層を与えています。

以下に Q-in-Q タグ付きパケットの例を示します。

宛先アドレス	送信元アドレス	SPVLAN (TPID+ サービスプロバイダ VLAN タグ)	802.1Q CEVLAN タグ (TPID+ 顧客 VLAN タグ)	イーサタイプ	ペイロード

以下に Q-in-Q を使用した ISP ネットワークの例を示します。

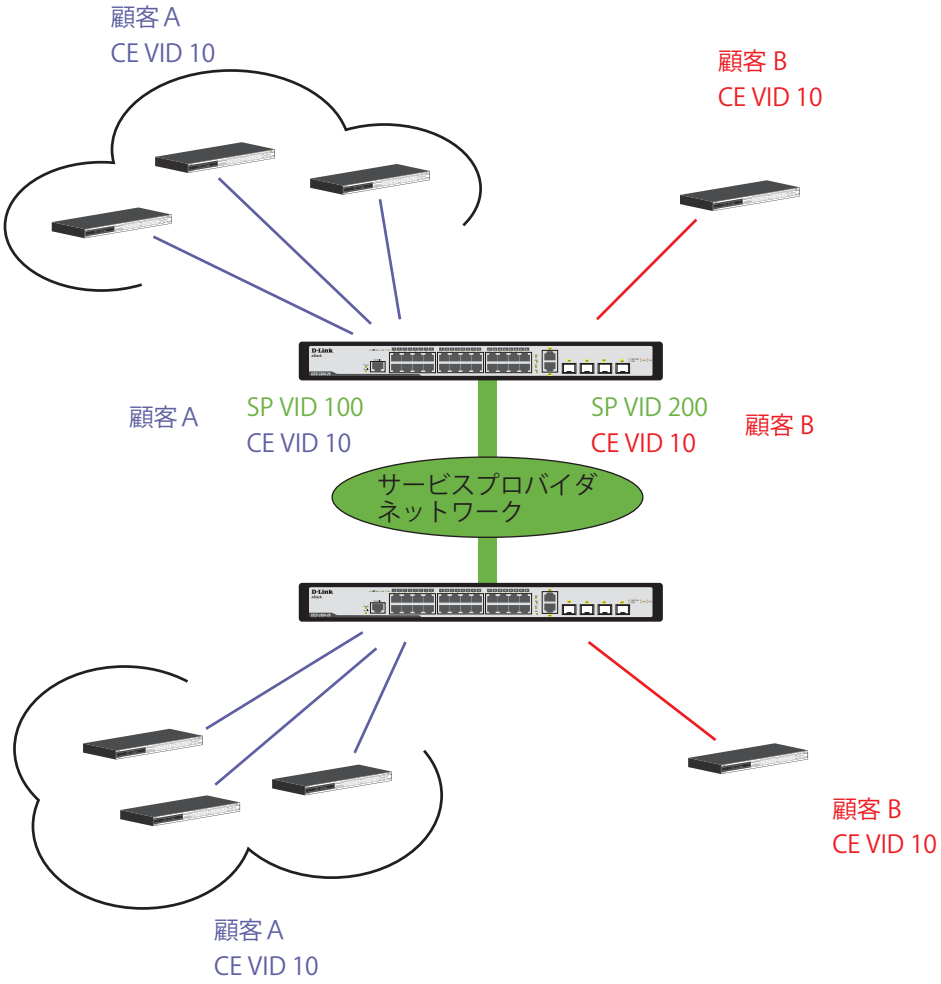


図 7-5　Q-in-Q を使用したネットワーク例

上の図例では、サービスプロバイダ・アクセスネットワーク・スイッチ (プロバイダのエッジスイッチ) は顧客 A と顧客 B という特定の顧客に対して異なる SPVID を持つ Q-in-Q VLAN を設定しているデバイスです。CEVLAN（Customer VLAN）10 は、サービスプロバイダ・アクセスネットワーク上で顧客 A には SPVID 100 を、顧客 B には SPVID 200 をタグ付けされるので、サービスプロバイダのネットワーク上では 2 つの VLAN に属していることになります。
このように、顧客は通常の VLAN を保持しながら、サービスプロバイダは、複数の顧客の VLAN を 1 つの SP VLAN によって集約することができ、サービスプロバイダのスイッチ上でのトラフィックとルーティングのプロセスを簡単にします。これらの情報はサービスプロバイダのメインのネットワークに送られ、1 セットのプロトコルと 1 つのルーティング動作を持つ 1 つの VLAN として認識されます。

Q-in-Q VLAN 使用時のルール

Q-in-Q VLAN を使用するために、以下のルールがあります。

1. すべてのポートに対して SPVID と関連するサービスプロバイダのエッジスイッチにおいて TPID の設定が必要です。
2. すべてのポートはアクセスポートまたはアップリンクポートとして設定される必要があります。アクセスポートはイーサネットポート、アップリンクポートはギガビットポートである必要があります。
3. プロバイダのエッジスイッチには SPVID タグが追加されるため、1522 バイト以上のフレームに対応する必要があります。
4. アクセスポートはサービスプロバイダ VLAN のタグなしポート、またアップリンクポートはサービスプロバイダ VLAN のタグ付きポートとします。
5. スイッチ上には Q-in-Q VLAN と通常の VLAN が混在できません。一度 VLAN を変更すると、すべてのアクセスコントロールリストがクリアになり、再設定が要求されます。
6. Q-in-Q VLAN を有効にする前に、STP と GVRP を手動で無効にします。
7. CPU からアクセスポートに送信されたすべてのパケットはタグなしになります。

802.1Q Static VLAN（802.1Q スタティック VLAN 設定）

802.1Q スタテック VLAN を設定します。

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

VLAN リストの表示

「VLAN List」タブでは、既に設定されている VLAN の VLAN ID と VLAN 名が表示されます。

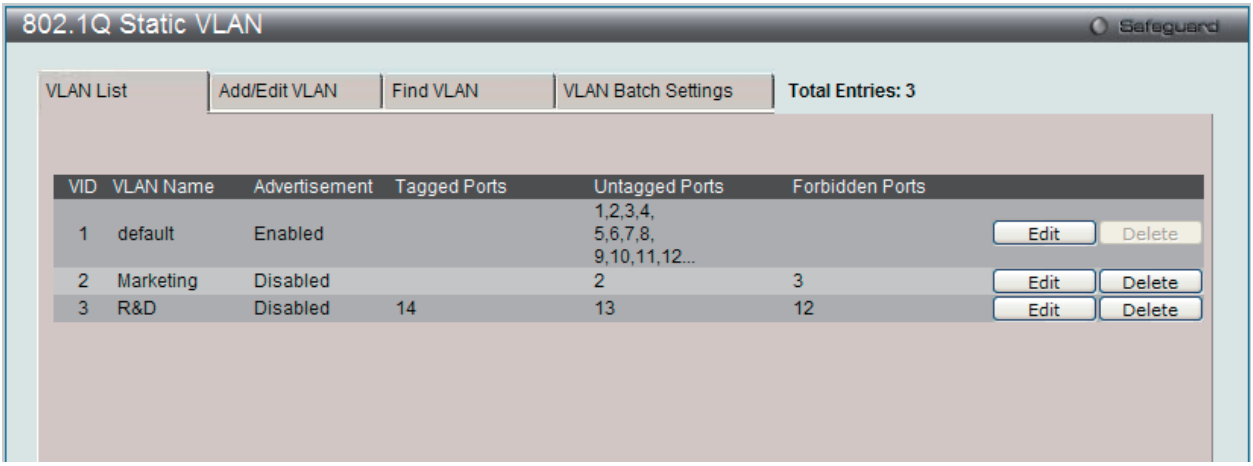


図 7-6　802.1Q Static VLAN - VLAN List タブ画面

エントリを削除するためには、対象のエントリの行の「Delete」ボタンをクリックします。

新規 802.1Q VLAN の登録

「Add/Edit VLAN」タブをクリックします。以下の画面でポート設定と新しい VLAN 名と番号を割り当てます。

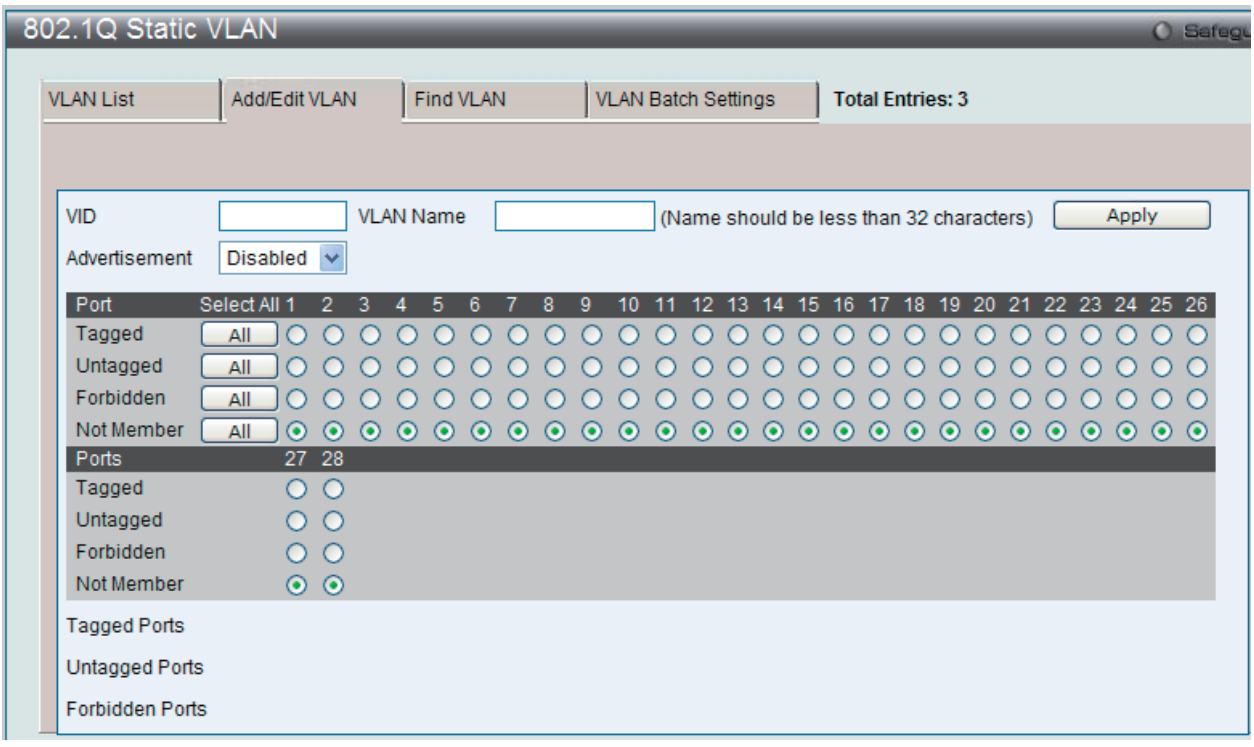


図 7-7　802.1Q Static VLAN - Add/Edit VLAN タブ画面（Add）

802.1Q VLAN の編集

設定済みの 802.1Q VLAN エントリを変更するためには、「VLAN List」タブで変更する VLAN エントリの横にある「Edit」ボタンをクリックします。以下の画面でエントリの設定を変更します。

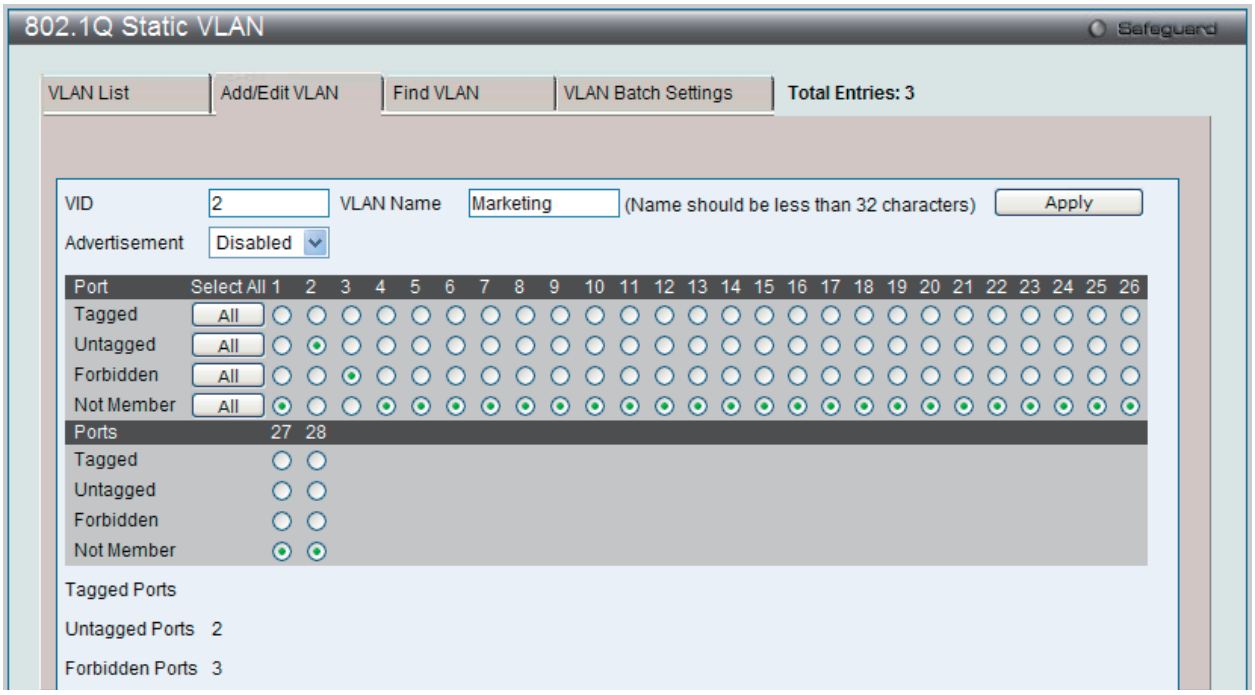


図 7-8　802.1Q Static VLAN - Add/Edit VLAN タブ画面（Edit）

「802.1Q Static VLAN」画面内の追加 / 変更の設定内容については、以下の表を参照してください。

注意　すべての IP インタフェースの設定後、VLAN は追加の手順なしでスイッチに送信されます。

「Add/Edit VLAN」タブには以下の項目が含まれます。

項目	内容
VID	VLAN ID の定義、または定義済みの VLAN の VLAN ID を表示します。VLAN は VID または VLAN 名で識別されます。
VLAN Name	VLAN 名の定義、または VLAN 名の編集をします。ユーザ定義の VLAN 名を定義します。（半角英数字 32 文字以内）
Advertisement	「Enabled」（有効）にすると、外部ソースに GVRP パケットを送信し、既存の VLAN に加わる可能性があることを通知します。
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。 • Forbidden - ポートを VLAN のメンバとならないことを定義し、ダイナミックにポートが VLAN のメンバになることを禁止します。 • Not Member - 各ポートが VLAN メンバでないことを定義します。 • Select All -「All」ボタンをクリックし、すべてのポートを選択します。

「Apply」ボタンをクリックし、デバイスに VLAN 設定を適用します。

VLAN の検索

「Find VLAN」タブをクリックします。以下の画面が表示されます。

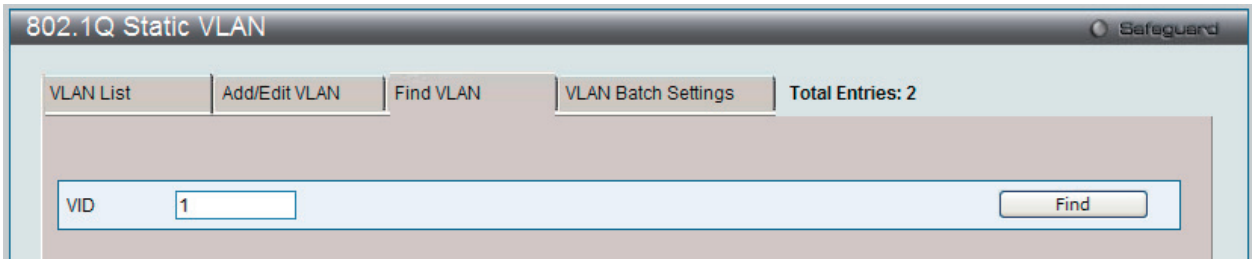


図 7-9　802.1Q Static VLAN - Find VLAN タブ画面

「VID」を入力し、「Find」ボタンをクリックします。「VLAN List」タブに結果が表示されます。

802.1Q VLAN バッチの作成

「VLAN Batch Settings」タブをクリックし、以下の画面を表示します。

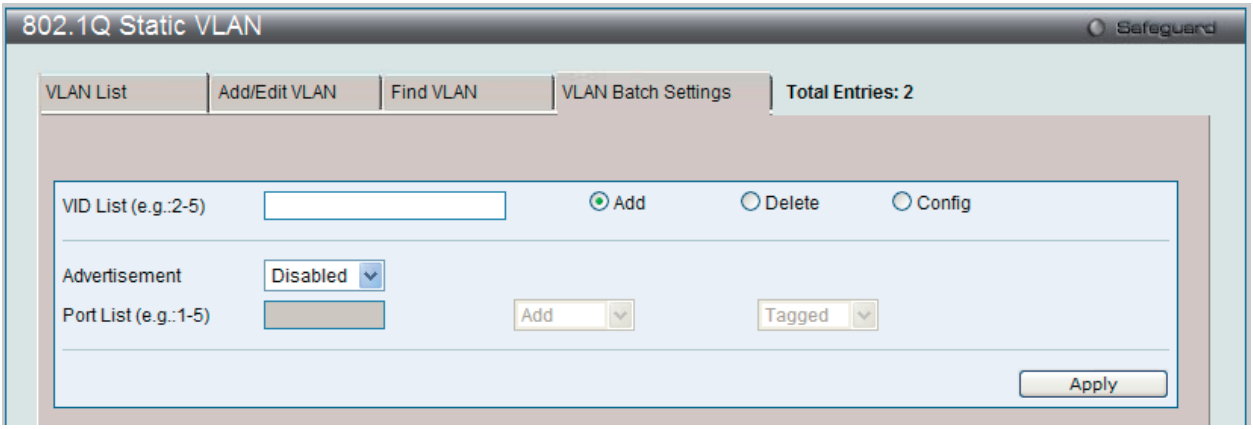


図 7-10　802.1Q Static VLAN - VLAN Batch Settings タブ画面

以下の項目を使用して設定します。

項目	説明
VID List (e.g. : 2-5)	VID の範囲（1-4094）を指定します。続いて、「Add」、「Delete」または「Config」をボタンをクリックし、指定した VID List を追加、削除または編集します。
Advertisement	本機能を「Enabled」（有効）にすると、スイッチは GVRP パケットを送信し、VLAN に参加できることを通知します。
Port List (e.g. : 1-5)	VLAN のメンバとして追加または削除するポートまたはポート範囲を指定します。 指定ポートに行う操作を指定します。 • Add - VLAN のメンバとして追加します。 • Delete - VLAN のメンバとして削除します。 指定ポートに以下の設定を行います。 • Tagged - ポートを 802.1Q タグ付きとして定義します。 • Untagged - ポートを 802.1Q タグなしとして定義します。 • Forbidden - ポートを VLAN のメンバではないポートとして定義します。動的に VLAN メンバになることが禁じられます。

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。

QinQ（QinQ 設定）

QinQ 機能を有効または無効にします。QinQ は、サービスプロバイダがネットワークを経由する複数ユーザからのトラフィックを送信するために設計されています。QinQ は、同じ VLAN ID を異なる顧客に使用している場合でも、顧客の指定 VLAN とレイヤ 2 プロトコル設定を維持するために使用されます。これは、サービスプロバイダのネットワークに入る場合に、SPVLAN タグを顧客のフレームに挿入して、フレームがネットワークを出る場合にはタグを取り除くことによって、実行されます。

サービスプロバイダの顧客には、サポートされる内部的な VLAN ID および VLAN 数について別の要求または明確な要求がある可能性があります。そのため、同じサービスプロバイダネットワーク内の顧客は、重複する VLAN 範囲を持つことがあり、トラフィックが混乱する可能性があります。そこで、各顧客に固有の VLAN ID 範囲を割り当てることは、VLAN がテーブルを積極的にマップする処理を必要としているいくつかの設定に制限をもたらす可能性があります。

QinQ は、複数の VLAN を持つ顧客に対して単一のサービスプロバイダ VLAN（SPVLAN）を使用します。顧客の VLAN ID は、同じ顧客の特定の VLAN ID を使用する場合でも、サービスプロバイダのネットワーク内で分離されます。顧客のオリジナルのタグ付きパケットを保存して、それぞれの新しいフレームに SPVLAN タグを加える場合、QinQ は利用可能な VLAN スペースを拡張します。

QinQ Settings（QinQ 設定）

L2 Features > QinQ > QinQ 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。

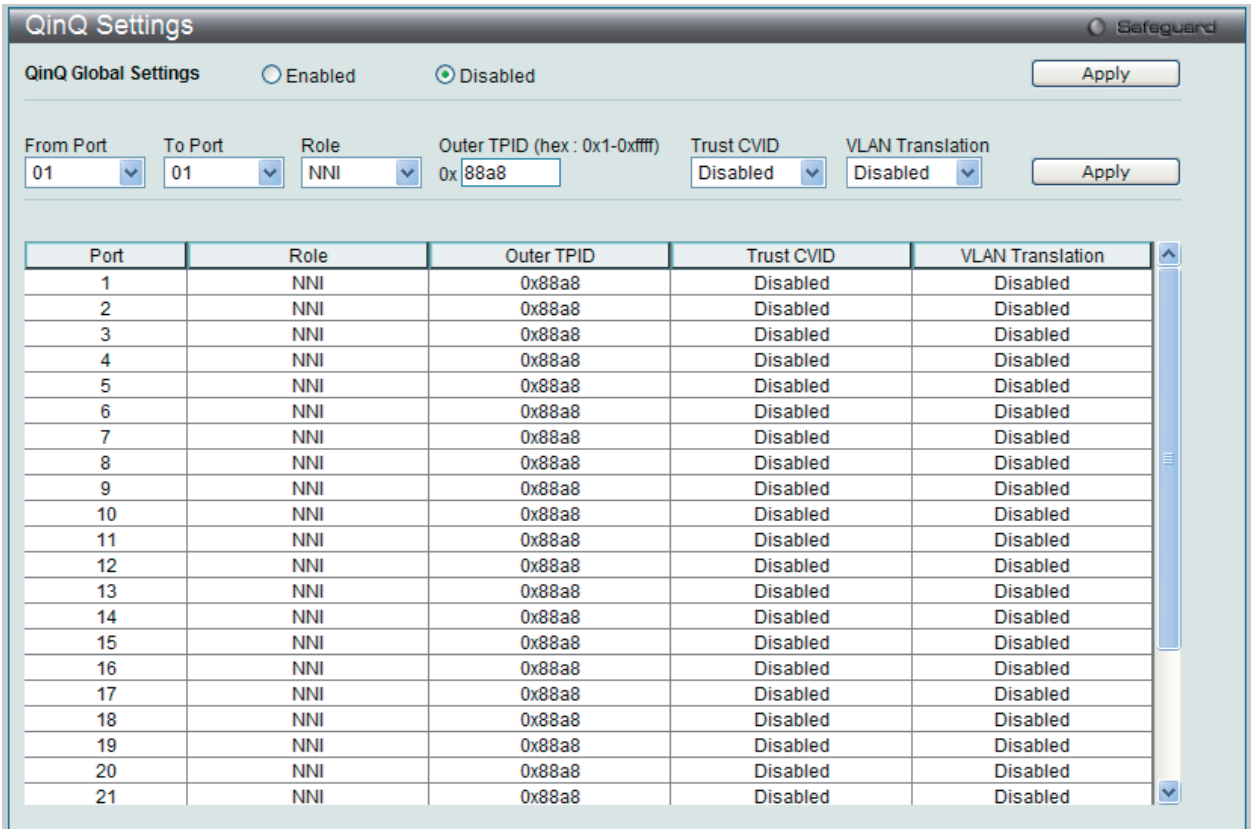


図 7-11　QinQ Settings 画面

以下の項目を使用して設定します。

項目	説明
QinQ Global Settings	QinQ 機能をグローバルに「Enabled」（有効）または「Disabled」（無効）にします。
From Port/To Port	VLAN 設定を行うポートグループの最初と最後の番号を設定します。
Role	役割（UNI または NNI）を選択します。 • UNI - UNI（user-network interface）を選択すると、指定ユーザと指定ネットワーク間の通信が行われることを示します。 • NNI - NNI（network-to-network interface）を選択すると、指定した 2 つのネットワーク間で通信が行われることを示します。
Outer TPID (hex: 0x1-0xffff)	Outer TPID は、パケットの学習および中継に使用されます。Outer TPID は VLAN ID と Inner Priority に基づいて、パケットにアウタータグを作成して挿入します。
Trust CVID	Trust Customer VLAN ID(CVID) を有効または無効にします。有効にすると、顧客パケットから得た CVID を SPVLAN タグの VLAN ID として使用します。初期値は無効です。
VLAN Translation	VLAN 変換機能を有効または無効にします。本機能は、プライベートネットワークから受信するデータパケットの VLAN ID をサービスプロバイダネットワークが使用するものに変換します。初期値は無効です。

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。

VLAN Translation CVID Entry Settings（VLAN 変換 CVID エントリ機能の設定）

VLAN 変換機能は、プライベートネットワークから受信するデータパケットの VLAN ID をサービスプロバイダネットワークに使用されるものに変換します。

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

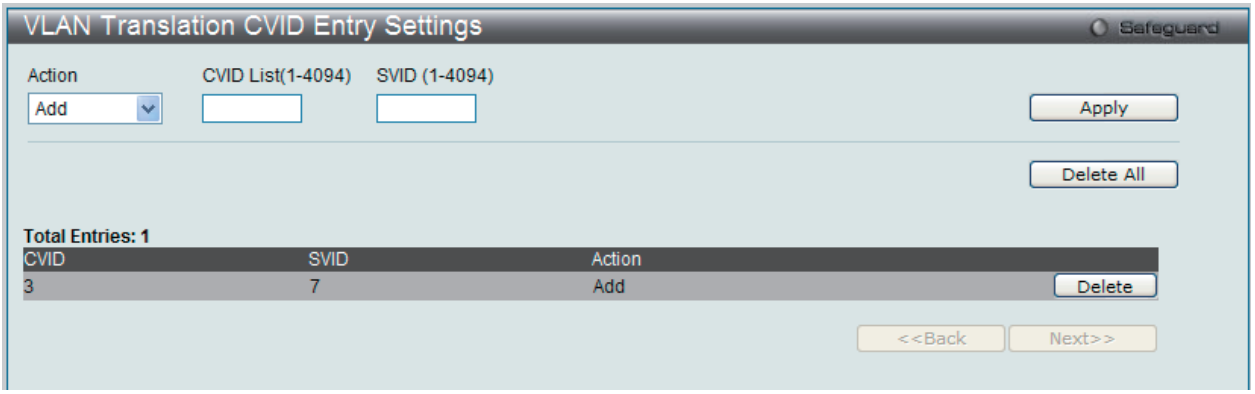


図 7-12　VLAN Translation CVID Entry Settings 画面

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
Action	追加または置き換えをするサービスプロバイダの VLAN ID (SVID) パケットを指定します。
CVID List (1-4094)	タグ付きパケットを追加する顧客の VLAN ID リストを指定します。
SVID(1-4094)	サービスプロバイダ VLAN に追加する VLAN をタグ付けメンバとして設定します。

「Apply」ボタンをクリックし、新しいエントリを追加します。

エントリの削除

エントリ横の「Delete」ボタンをクリックします。すべてのエントリを削除するためには「Delete All」ボタンをクリックします。

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 Group Settings」および「802.1v Protocol VLAN Settings」。

802.1v Protocol Group Settings（802.1v プロトコルグループ設定）

本テーブルで、プロトコル VLAN グループを作成し、そのグループにプロトコルを追加します。802.1v プロトコル VLAN グループ設定は、各プロトコルのためにマルチプル VLAN をサポートし、同じ物理ポートに異なるプロトコルを持つタグなしポートの設定が可能です。例えば、同じ物理ポートに 802.1Q と 802.1v タグなしポートを設定できます。

L2 Features > 802.1v Protocol VLAN > 802.1v Protocol 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。

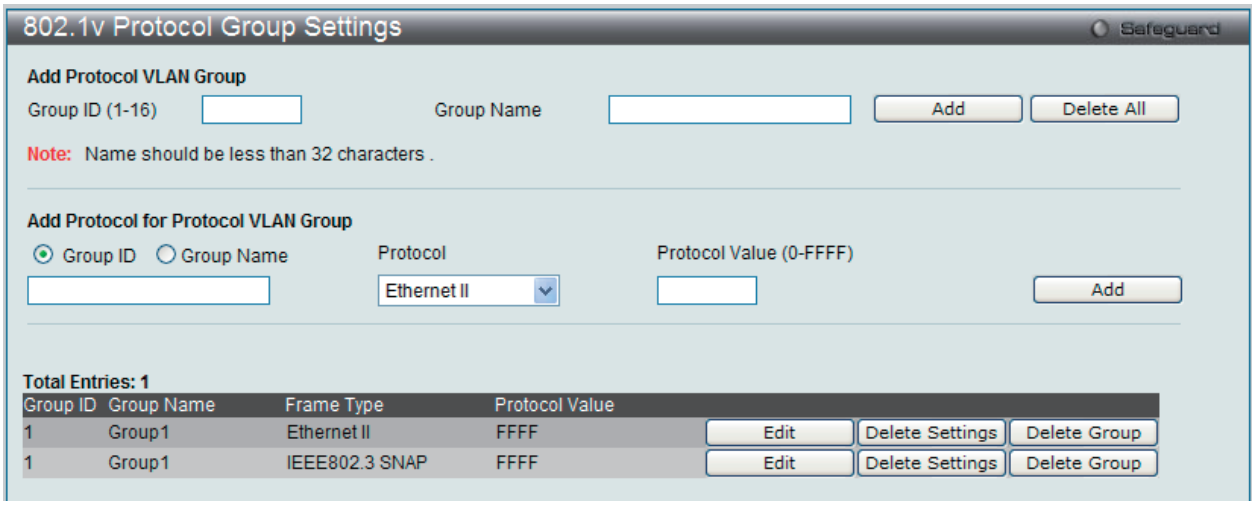


図 7-13　802.1v Protocol Group Settings 画面

テーブルの下半分は定義済みのすべてのグループを表示します。

以下の項目を使用して、設定します。

項目	説明
Add Protocol VLAN Group	
Group ID (1-16)	グループの ID 番号を 1-2147483647 の範囲から指定します。
Group Name	新しいプロトコル VLAN グループの識別に使用します。32 文字までの半角英数字を入力します。
Add Protocol for Protocol VLAN Group	
Group ID	グループの ID 番号を 1-2147483647 の範囲から指定します。
Group Name	新しいプロトコル VLAN グループの識別に使用します。32 文字までの半角英数字を入力します。
Protocol	本機能は、関連するプロトコルのタイプを検出するためにパケットヘッダのタイプオクテットを検証することで、パケットをプロトコルで定義された VLAN にマップします。 プルダウンメニューを使用して、Ethernet II、または IEEE802.3 SNAP から選択します。
Protocol Value (0-FFFF)	グループに対してプロトコル値を入力します。プロトコル値は、指定されたフレームタイプのプロトコルを識別するために使用されます。

プロトコル VLAN グループの新規追加

「Add Protocol VLAN Group」セクション内の項目を入力し、「Add」ボタンをクリックします。

プロトコル VLAN グループの編集

1. テーブル内のエントリの「Edit」ボタンをクリックし、以下の画面を表示します。

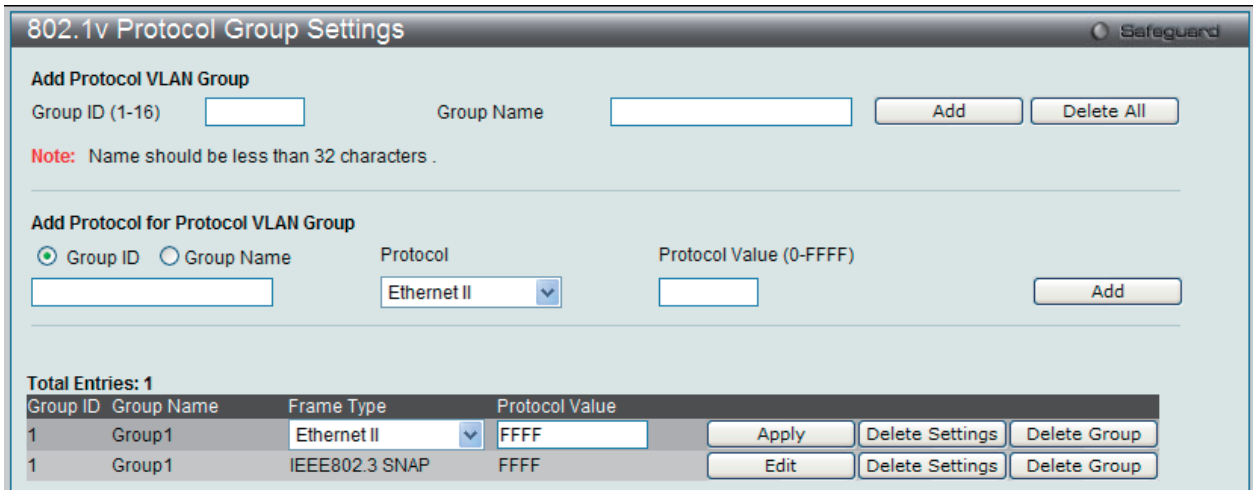


図 7-14　802.1v Protocol Group Settings 画面 - Edit

2. 項目を編集し、エントリの「Apply」ボタンをクリックします。

プロトコル VLAN グループの削除

画面下半分に表示されたテーブル内のエントリの「Delete Group」ボタンをクリックします。すべてのエントリを削除するためには、「Delete All」ボタンをクリックします。

プロトコル VLAN グループのプロトコル設定

「Add Protocol for Protocol VLAN Group」セクションの各項目を入力し、「Add」ボタンをクリックします。

プロトコル VLAN グループのプロトコルの削除

画面下半分に表示されたテーブル内のエントリの「Delete Settings」ボタンをクリックします。

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

プロトコル VLAN ポートの設定を行います。テーブルの下半分は定義済みのすべての設定を表示します。

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

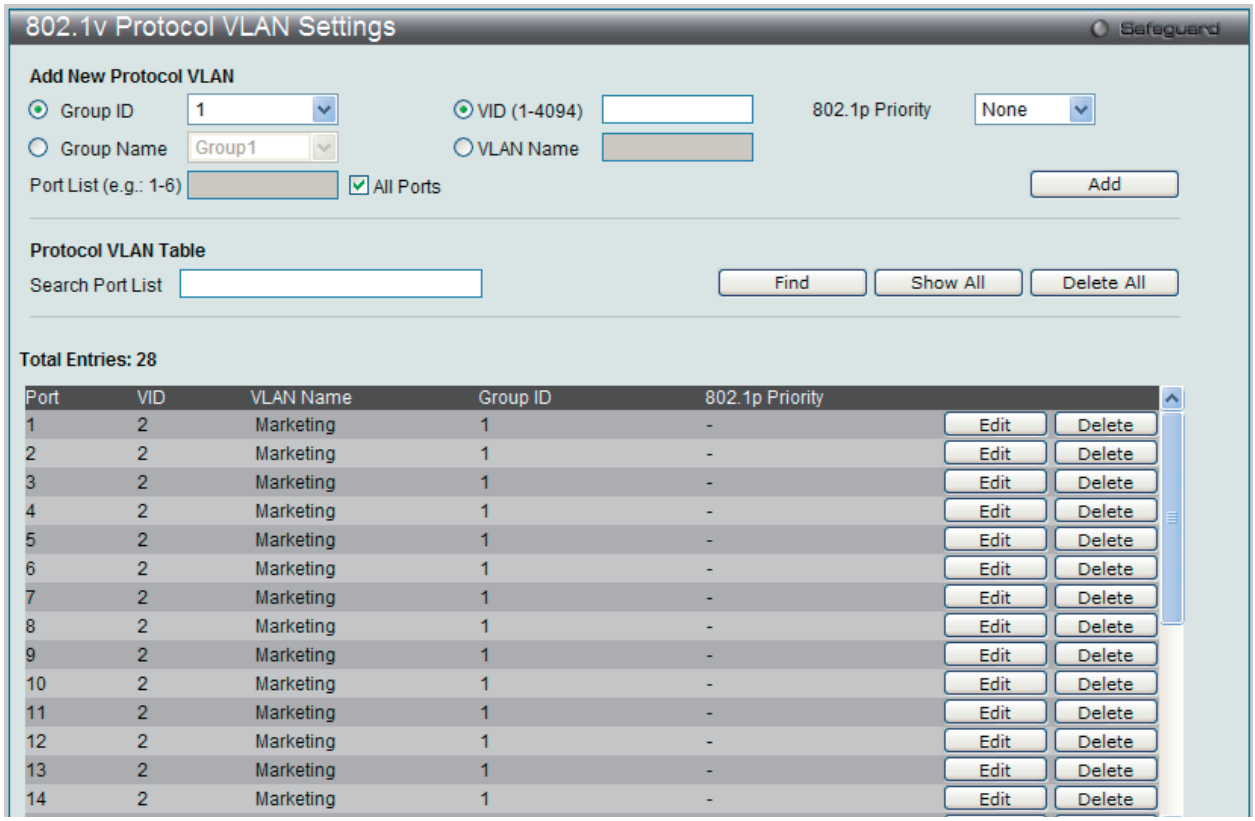


図 7-15　802.1v Protocol VLAN Settings 画面

以下の項目を使用して、設定します。

項目	説明
Add New Protocol VLAN	
Group ID	対応するボタンをチェックし、プルダウンメニューから定義済みの Group ID を選択します。
Group Name	対応するボタンをチェックし、プルダウンメニューから定義済みの Group Name を選択します。
VID (1-4094)	対応するボタンをチェックし、VID を入力します。これは、VLAN 名と共に、ユーザが作成する VLAN を識別するために使用する ID です。
VLAN Name	対応するボタンをチェックし、VLAN Name を入力します。これは、VLAN ID と共に、ユーザが作成する VLAN を識別するために使用する VLAN 名です。
802.1p Priority	スイッチに設定済みの 802.1p デフォルトプライオリティ（パケットが送られる CoS キューを決定するために使用）の設定を書き換える場合に使用します。本項目を選択すると、スイッチが受信したパケット内の本プライオリティに一致するパケットは、既に指定した CoS キューに送られます。 本画面で設定した基準に一致するパケットが、指定された CoS キューに送られる前に、パケットの 802.1p デフォルトプライオリティを、「Priority（0-7）」に指定した値に書き換える場合に対応するボックスをクリックします。指定しない場合は、パケットは送出される前に、入力用の 802.1p ユーザプライオリティを元の値に書き換えられます。 プライオリティキュー、CoS キューおよび 802.1p マッピングについての詳細な情報については、本マニュアルの 150 ページの「第 8 章 QoS（QoS 機能の設定）」を参照してください。
Port List (e.g.: 1-6)	本項目にポート番号を入力することで特定のポートを選択するか、または「All Ports」をチェックします。
Protocol VLAN Table	
Search Port List	定義済みの全ポートリスト設定を検索し、テーブルの下半分に結果を表示します。

注意 DES-3200 シリーズの現在のリリースでは、802.1v にポート範囲を指定できません。現在のリリースでは、全ポートの指定のみ可能です。

プロトコル VLAN ポートの新規設定
「Add New Protocol VLAN」セクションの各項目を入力し、「Add」ボタンをクリックします。

プロトコル VLAN ポートの設定編集

1. 編集するポートの「Edit」ボタンをクリックし、以下の画面を表示します。

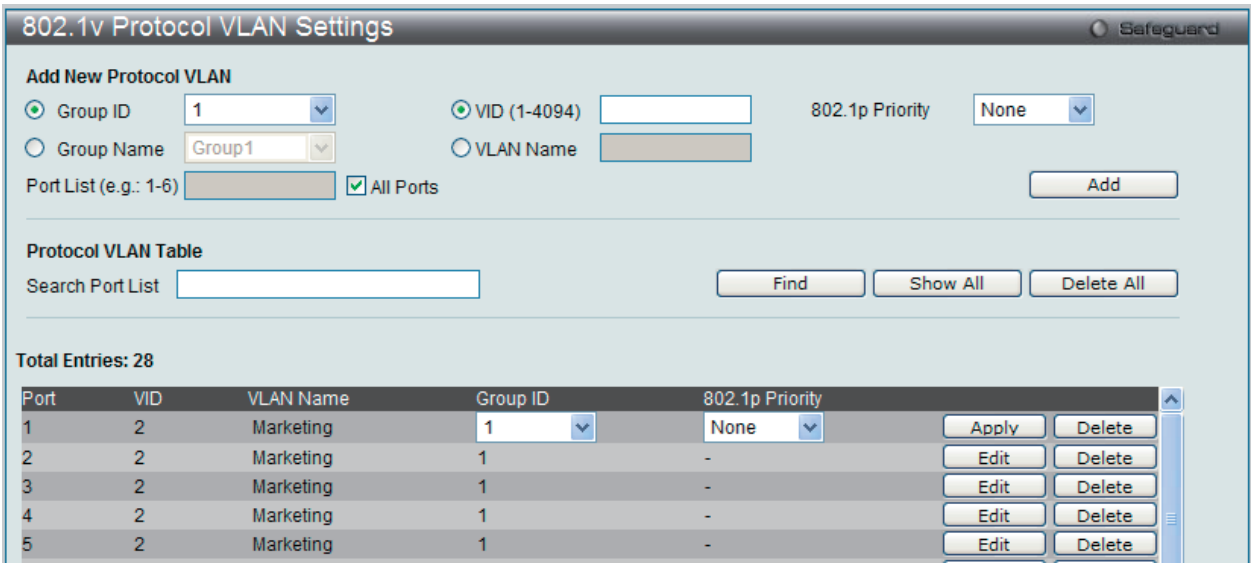


図 7-16　802.1v Protocol VLAN Settings 画面

2. 項目を編集し、エントリの「Apply」ボタンをクリックします。

プロトコル VLAN ポートの削除
画面下半分に表示されたポートリストで削除するポートの「Delete」ボタンをクリックします。

ポートリストの検索
ポートリストを検索するために、「Search Port List」に参照するポート番号を入力し、「Find」ボタンをクリックします。

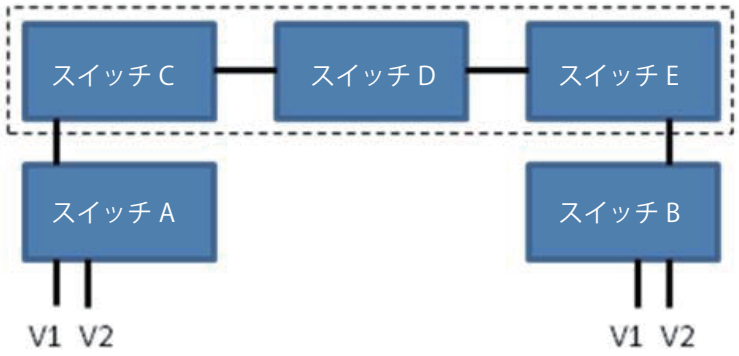
定義済み全ポートリストの表示
「Show All」ボタンをクリックします。

すべての設定リストのクリア
「Delete All」ボタンをクリックします。

VLAN Trunk Settings（VLAN トランク設定）

ポートの VLAN を有効にすることで、未知の VLAN グループに所属するフレームがそのポートを通過することができるようになります。これは、中継するデバイスに同じ VLAN グループを設定しないで、末端のデバイスに VLAN グループを設定する場合に便利です。

以下の図例を参照してください。
スイッチ A と B に VLAN グループ 1 と 2（V1 と V2）を作成するものとします。VLAN トランクを使用しない場合、はじめにすべての中継スイッチ C、D、E のすべてに VLAN グループ 1、2 を設定します。そうでない場合、未知の VLAN グループのタグを持つフレームを廃棄します。しかし、各中継スイッチのポートで VLAN トランクを有効にすれば、末端のデバイスに VLAN グループを作成するだけとなります。C、D、および E は、それらのスイッチにとって未知の VLAN グループのタグ 1 および 2 を持つフレームを自動的にそれらの VLAN トランキングポートから通過させます。



本画面では、多くの VLAN ポートを集約して VLAN トランクを作成します。

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

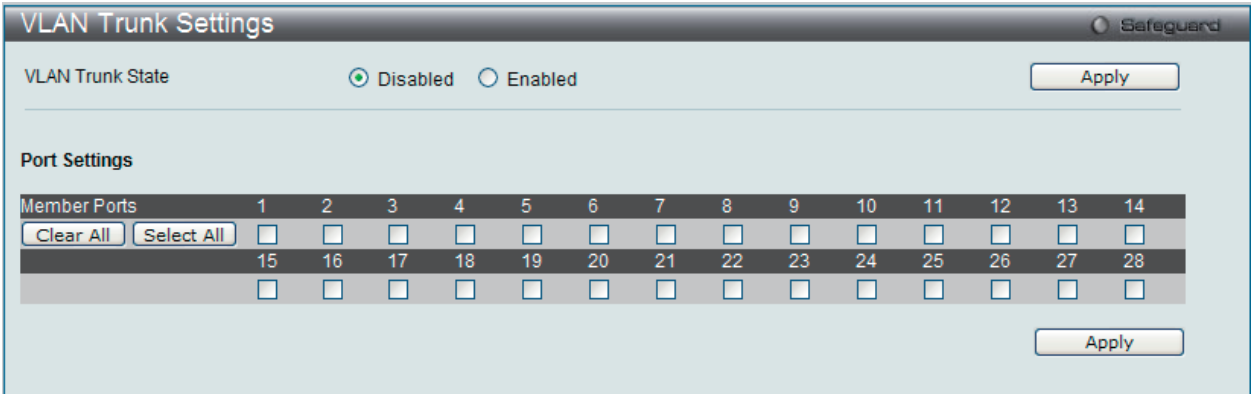


図 7-17　VLAN Trunk Settings 画面

本画面には次の項目があります。

項目	説明
VLAN Trunk Global State	VLAN トランキングのグローバルな状態を有効または無効にします。
Port Settings	設定するポートを指定します。

スイッチに VLAN トランクポートを設定するためには、設定するポートを指定し、ステータスを「Enabled」に変更して「Apply」ボタンをクリックします。

GVRP Settings（GVRP の設定）

GVRP（GARP VLAN Registration Protocol）が有効なスイッチ同士で VLAN 構成情報を共有するかどうかを指定することができます。さらに、Ingress を「Enabled」（有効）にすることで、PVID がポートの PVID と一致しない入力パケットをフィルタしてトラフィックを制限します。
設定内容は、設定画面下部のテーブルで参照することができます。

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

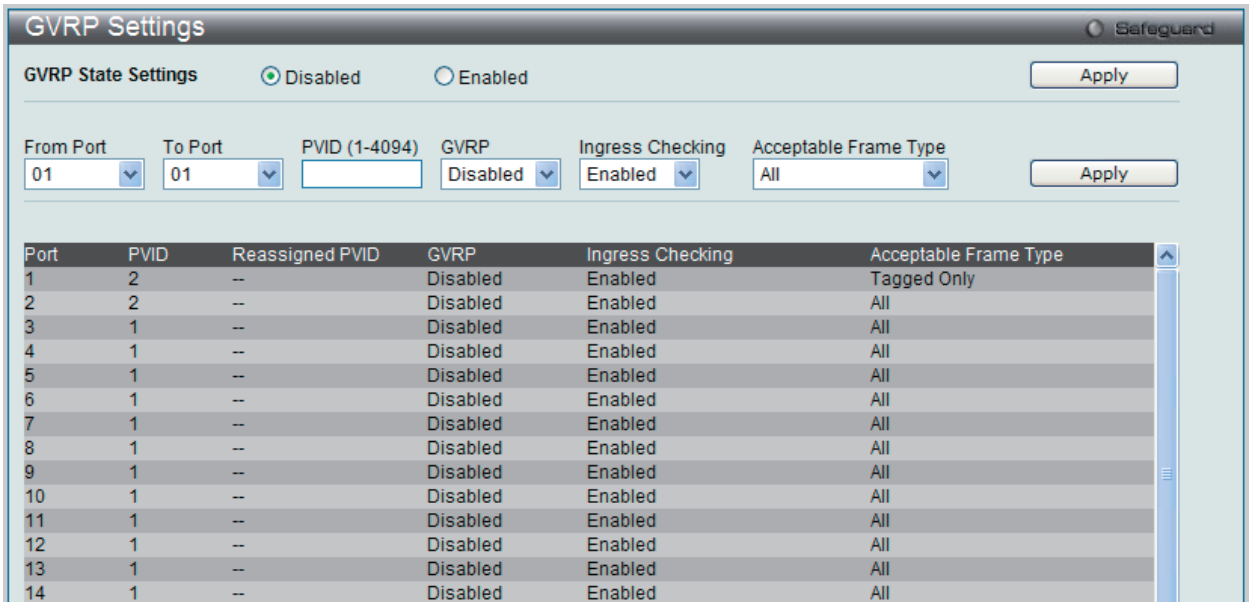


図 7-18　GVRP Setting 画面

本画面には次の項目があります。

項目	説明
GVRP State Settings	デバイスで GVRP を有効にするかを設定し、「Apply」ボタンをクリックします。 • Enabled - デバイスで GVRP を有効に設定します。 • Disabled - デバイスで GVRP を無効に設定します。（初期値）
From Port / To Port	「802.1Q Static VLAN」画面で作成したポートベース VLAN に含まれているポートの範囲を指定します。
PVID (1-4094)	PVID を VLAN に手動で割り当てます。スイッチには初期状態ですべてのポートが default VLAN（VID=1）に割り当てています。PVID はポートが送信時にタグなしパケットにタグ付けをしたり、受信時にフィルタリングをするためのものです。ポートがタグ付きフレームのみを受信すると指定し、タグ付けや、転送のためにタグなしパケットを送られた場合は、ポートはタグに組み込む VID として PVID を使用し 802.1Q タグを付加します。パケットが送信先に到着した時には、受信デバイスは PVID に基づき VLAN による転送を行います。ポートがパケットを受信し、Ingress フィルタリングが有効ならば、ポートは VID と自身の PVID を比較します。2 つが異なる場合、パケットは破棄され、同一ならばパケットは受信されます。
GVRP	GVRP が各ポートをダイナミックに VLAN メンバにするかどうかを設定します。 • Enabled - 選択したポートで GVRP を有効に設定します。 • Disabled - 選択したポートで GVRP を無効に設定します。（初期値）
Ingress Checking	Ingress フィルタリングの有効 / 無効を設定します。デバイスで Ingress チェックを有効にするかを設定します。 • Enabled - デバイスで Ingress チェックを有効に設定します。Ingress チェックにより、受信したタグ付きパケットの VID とポートに割り当てられた PVID を比較します。PVID が異なっていれば、ポートはパケットを破棄します。（初期値） • Disabled - デバイスで Ingress チェックを無効に設定します。
Acceptable FrameType	ポートが受け入れるパケットの種類を設定します。 • Tagged Only - タグ付きパケットのみポートは受け入れます。 • All - タグ付き、タグなし両方のパケットをポートは受け入れます。（初期値）

「Apply」ボタンをクリックし、デバイスに GVRP 設定を適用します。

Asymmetric VLAN Settings（Asymmetric VLAN 設定）

共有 VLAN 学習（SVL : Shared VLAN Learning）は Asymmetric VLAN のための第一の必要条件の例です。通常の環境下では、VLAN 環境で通信する 1 組の装置は、同じ VLAN を使用して送受信します。しかし、Asymmetric VLAN が必要とされる場合、B に送信するために A に使用される VLAN と A に送信するために使用される VLAN の 2 つの異なる VLAN を使用することが便利です。このタイプの設定が必要とされる例は、クライアントが異なる IP サブネットにある場合、機密性を確保する必要からクライアント間のトラフィックを分ける場合です。

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

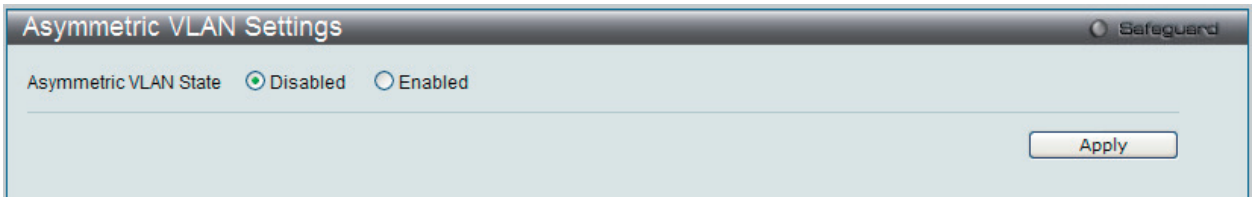


図 7-19　Asymmetric VLAN Settings 画面

「Asymmetric VLAN State」を「Enabled」（有効）または「Disabled」（無効）に設定し、「Apply」ボタンをクリックして変更を有効にします。

MAC-based VLAN Settings（MAC ベース VLAN 設定）

新しく MAC ベース VLAN エントリを作成し、設定済みのエントリを検索 / 編集 / 削除します。

エントリがポートに作成されると、ポートは自動的に指定した VLAN のタグなしメンバポートになります。スタティック MAC ベース VLAN のエントリがユーザに作成されると、このユーザからのトラフィックはこのポートで動作する認証機能に関わらず指定 VLAN の下で行われます。

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

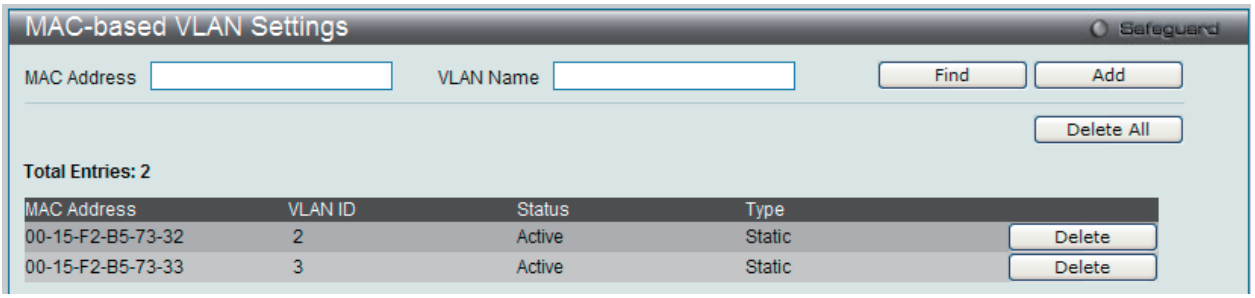


図 7-20　MAC-based VLAN Settings 画面

以下の項目を使用して設定します。

項目	説明
MAC Address	「MAC Address」に再認証を行う MAC アドレスを入力します。
VLAN Name	作成済みの VLAN の VLAN 名を指定します。

エントリの新規登録
MAC ベース VLAN に登録する MAC アドレスを「MAC Address」に入力し、関連付ける「VLAN Name」を指定後、「Add」ボタンをクリックします。

エントリの検索
「MAC Address」または「VLAN Name」を入力し、「Find」ボタンをクリックします。結果は画面下のテーブルに表示されます。

エントリの削除
テーブル内の削除するエントリの「Delete」ボタンをクリックします。すべてのエントリを削除するためには、「Delete All」ボタンをクリックします。

PVID Auto Assign Settings（PVID 自動割り当て設定）

PVID 自動割り当て設定を「Enabled」（有効）または「Disabled」（無効）にします。

PVID は、スイッチが転送やフィルタリングの目的のために使用する VLAN です。PVID の自動割り当てを有効にした場合、PVID は設定済みの PVID または VLAN により変更可能になります。ポートを VLAN x のタグなしメンバに設定する場合、このポートの PVID は VLAN x に従って更新されます。VLAN コマンドでは、PVID は VLAN コマンド構文の最後のパラメータを指定することで更新されます。PVID の VLAN におけるタグなしメンバからポートを削除すると、ポートの PVID は「default VLAN」に割り当てられます。PVID の自動割り当てを無効にすると、PVID はユーザによる PVID 設定だけで変更可能です。VLAN 設定により PVID が自動的に変更されることはありません。初期値は「Enabled」（有効）です。

L2 Features > PVID Auto Assign 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。

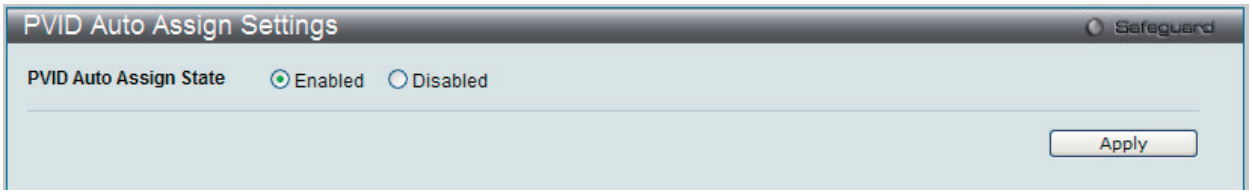


図 7-21　PVID Auto Assign Settings 画面

「Apply」ボタンをクリックし、デバイスに設定を適用します。

Port Trunking（ポートトランキングの設定）

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、多く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。本スイッチは各グループ 2 個から 8 個のポートを束ねた最大 5 グループ（DES-3200-10、DES-3200-10/T）、最大 9 グループ（DES-3200-18、DES-3200-18/T）、最大 13 グループ（DES-3200-26、DES-3200-26/T）、最大 14 グループ（DES-3200-28/28F、DES-3200-28/T）のポートトランクグループをサポートしています。

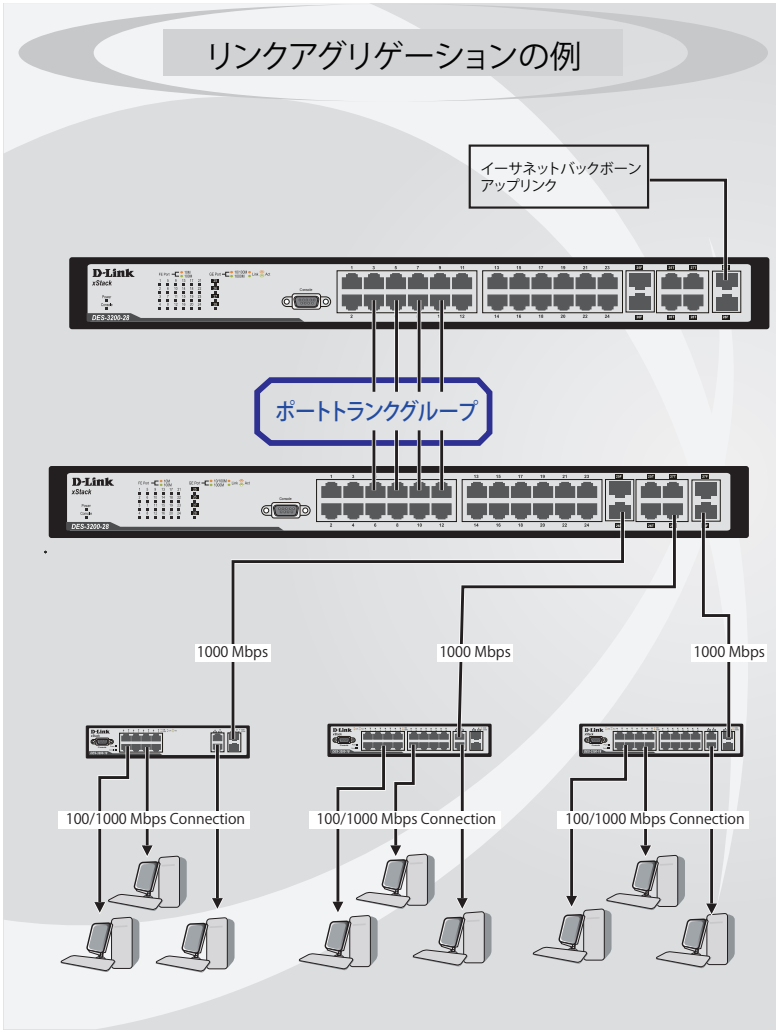


図 7-22　ポートトランクグループの例

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

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

リンクアグリゲーション機能により、 1 つのグループとして束ねられたポートは、1 つのリンクの働きをします。この時、 1 つのリンクの帯域は、束ねられたポート分拡張されます。

リンクアグリゲーションは、サーバやバックボーンなど、広帯域を必要とするネットワークデバイスにおいて広く利用されています。

本スイッチでは、2 から 8 のリンク (ポート) で構成する最大 14 個（DES-3200-28/28F、DES-3200-28/T の場合）のリンクアグリゲーショングループをサポートします。1 つのグループ内の全ポートは同じ VLAN に属し、それぞれのスパニングツリープロトコル（STP）ステータス、スタティックマルチキャスト、トラフィックコントロール、トラフィックセグメンテーション、および 802.1p デフォルトプライオリティの設定は同じである必要があります。また、ポートロッキング、ポートミラーリング、および 802.1X は有効化されていてはなりません。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。

グループのマスタポートの設定はユーザにより行われます。また、マスタポートに適用される VLAN 設定を含むすべての設定オプションは、グループ内全体に適用されます。

グループ内のポート間では自動的にロードバランスが行われ、グループ内でのリンク断によって発生するネットワークトラフィックは、グループ内の他のリンクに振り分けられます。

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

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

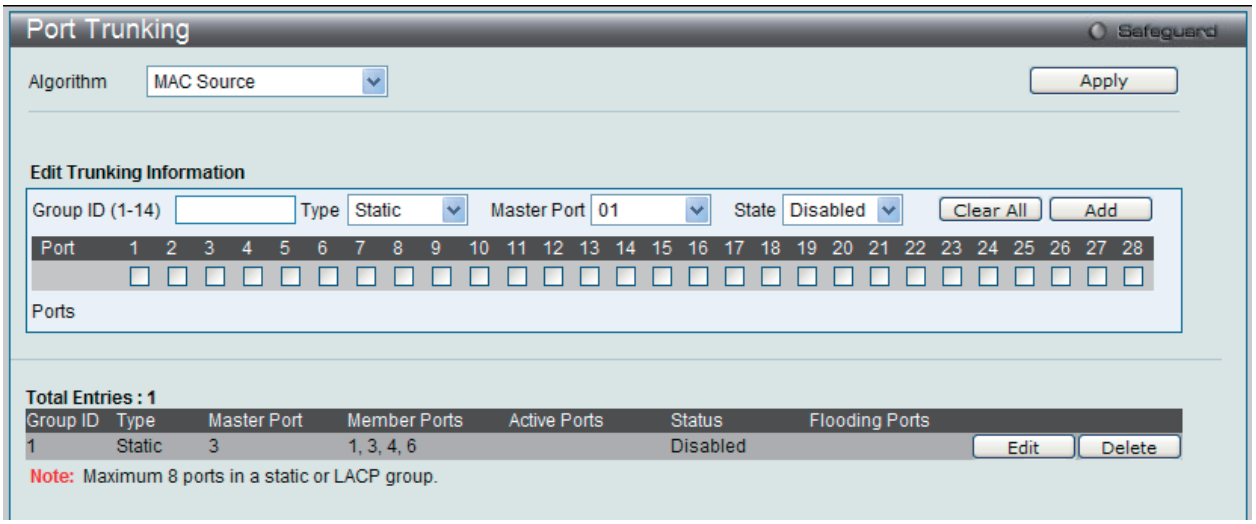


図 7-23　Port Trunking 画面

本画面には次の項目があります。

項目	説明
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。「MAC Source」、「MAC Destination」、「MAC Source Destination」、「IP Source」、「IP Destination」、「IP Source Destination」から指定してください。
Edit Trunking Information	
Group ID (1-14)	グループの ID 番号を 1-14 の範囲から指定します。
Type	トランキンググループの種類を設定します。 • Static - スタティックです。 • LACP - ポートトランキンググループのリンクを自動的に検出します。
Master Port	トランキンググループのマスタポートを選択します。
State	ポートトランキンググループを「Enabled」（有効）または「Disabled」（無効）にします。これは、診断、迅速に帯域が集中するネットワークデバイスの迅速な分離、または自動制御下にない独立したバックアップアグリゲーショングループを持つ場合に有益です。
Member Ports	トランキンググループのメンバポートを選択します。グループに 8 ポートまで割り当てることができます。
Active Ports	現在パケットの送出を行っているポートが表示されます。
Flooding Ports	本ポートは、トランクグループ内の CPU から送信されるフラッディングブロードキャスト、マルチキャスト、および DLF (unicast Destination Lookup Fail) パケットのために設計されています。また、ソフトウェアによって定義されており、ハードウェアには存在しません。

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

1. 画面上部で編集するグループの「Edit」ボタンをクリックし、以下の画面を表示します。

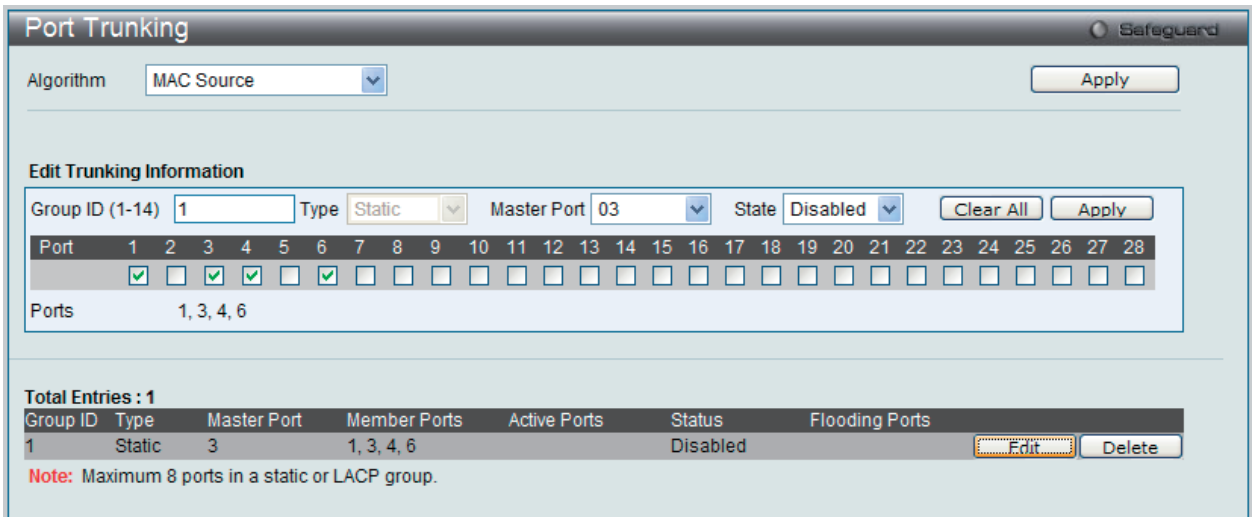


図 7-24　Port Trunking 画面 - Edit

2. 項目を編集後「Apply」ボタンをクリックします。

ポートトランキンググループの削除

編集するポートトランキンググループを削除するためには、削除するグループの「Delete」ボタンをクリックします。

項目を設定後、「Apply」ボタンをクリックし、デバイスに設定を適用します。

LACP Port Settings（LACP の設定）

スイッチにポートトランキンググループを作成します。LACP 制御フレームの処理と送出を行う際、どのポートが「Active」または「Passive」の役割を担うかを指定します。

L2 features > LACP Port Settings の順にメニュークリックし、以下の画面を表示します。

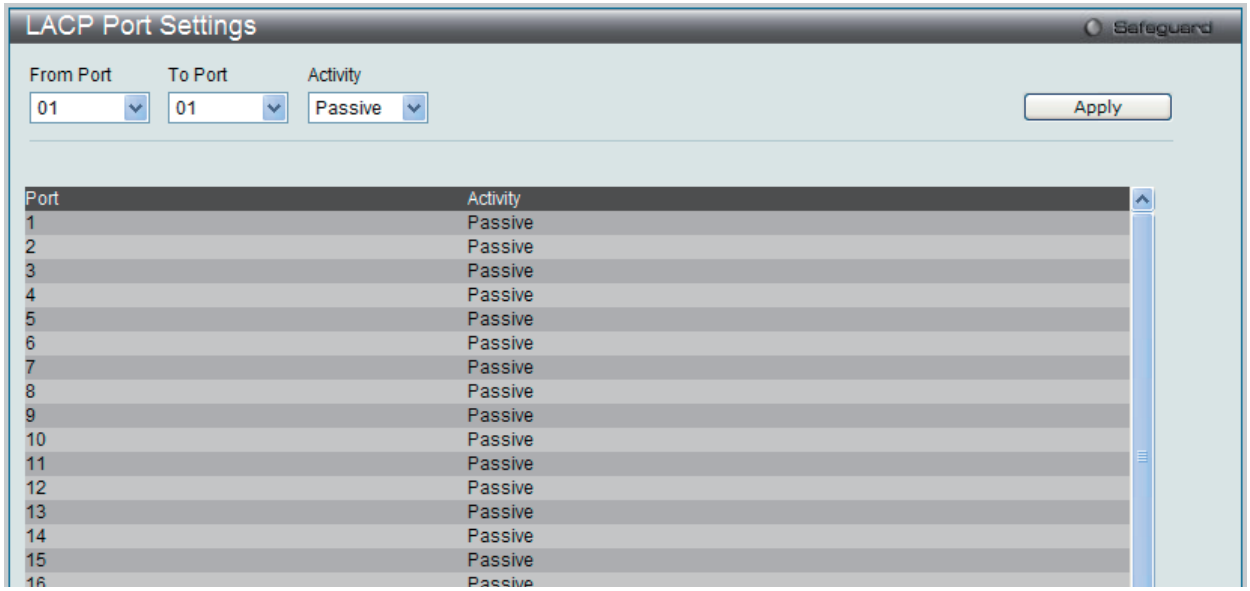


図 7-25　LACP Port Settings 画面

以下の項目を使用して設定を行います。

項目	説明
From Port / To Port	設定対象のポート範囲を指定します。
Activity	• 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、接続のどちらか一端が Active な LACP ポートである必要があります。（初期値）

「Apply」ボタンをクリックし、デバイスに LACP 設定を適用します。

Traffic Segmentation（トラフィックセグメンテーション）

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

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

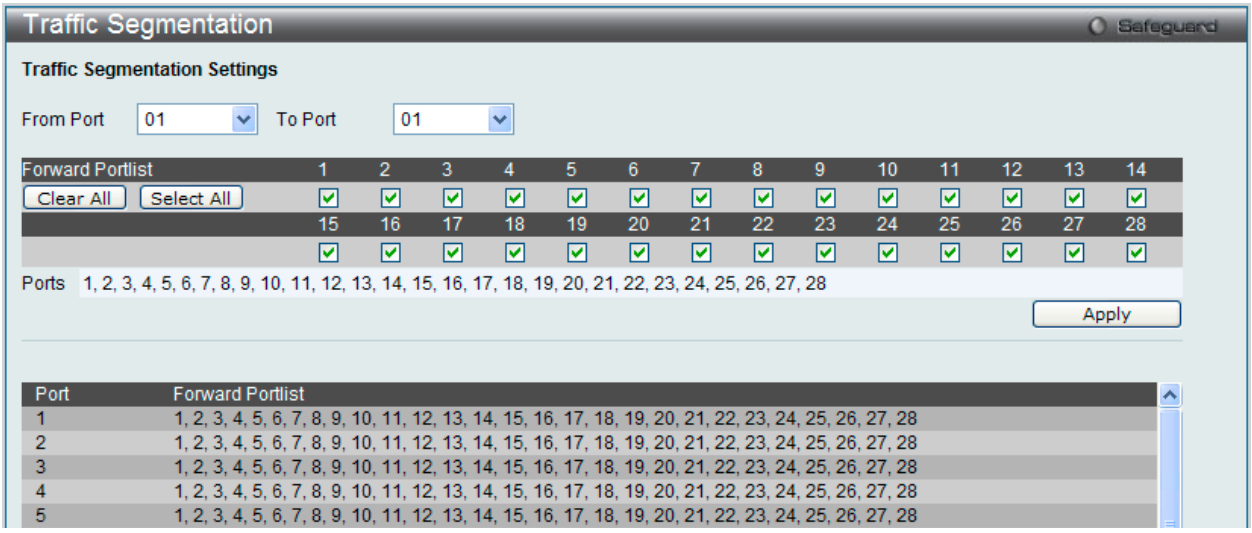


図 7-26　Traffic Segmentation 画面

以下の項目を使用して設定します。

項目	説明
From Port/To Port	パケットを送信するポートを指定します。
Forward Portlist	パケットの送信先となるスイッチのポートを指定します。

これらのポートは、上記「Port」欄で指定したポートからのパケットを受信します。「Apply」ボタンをクリックすると、転送ポートの組み合わせが入力され、設定内容がテーブルに反映されます。

L2PT Settings（レイヤ 2 プロトコルトンネリング設定）

レイヤプロトコルトンネリングの設定をします。

L2 Features > L2PT 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。

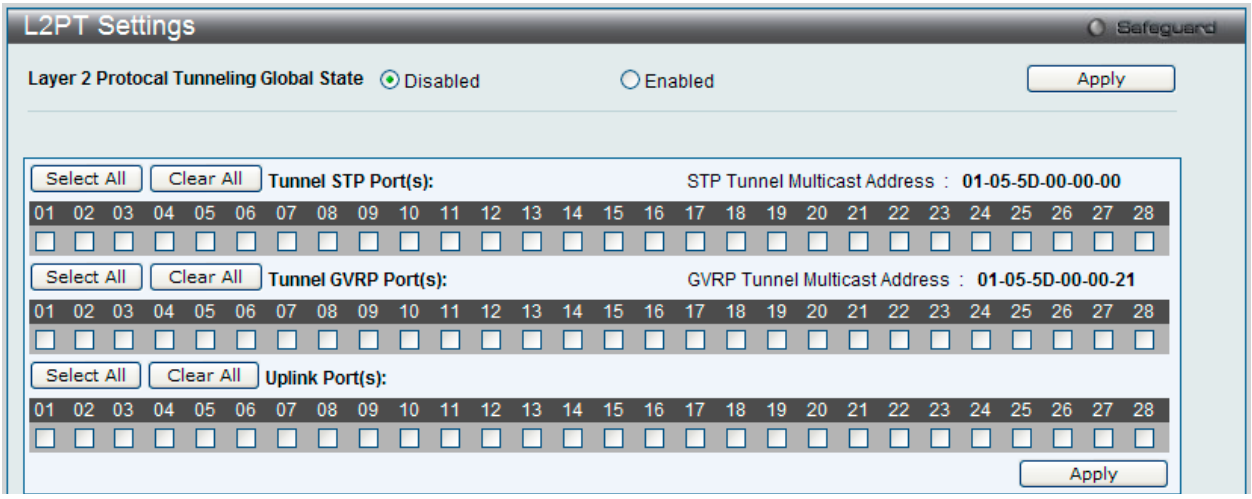


図 7-27　L2PT Settings 画面

以下の項目を使用して設定します。

項目	説明
Layer 2 Protocol Tunneling Global State	レイヤ 2 プロトコルトンネリング状態を有効または無効にします。
Port(s)	レイヤ 2 プロトコルトンネリング設定に含めるポート番号を選択します。

「Apply」ボタンをクリックし、変更を有効にします。

BPDU Attack Protection Settings（BPDU アタック防止設定）

スイッチのポートにBPDU防止機能を設定します。通常、BPDU防止機能には2つの状態があります。1つは正常な状態で、もう1つはアタック状態です。アタック状態には、3 つのモード（破棄、ブロックおよびシャットダウン）があります。BPDU 防止が有効なポートは、STP BPDU パケットを受信するとアタック状態に入ります。そして、設定に基づいてアクションを行います。このように、BPDU 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 防止では、「STP Port Settings」画面 (**L2 Features > Spanning Tree > STP Port Settings**) の「Forward BPDU」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「STP Port Settings」画面の「Forward BPDU」に設定されており、BPDU 防止が有効であると、ポートは STP BPDU を転送しません。

BPDU 防止では、BPDU の処理を決定するために設定したレイヤ 2 プロトコル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 **L2 Features > L2PT Settings** 画面の「Tunnel STP Port(s)」にレイヤ 2 プロトコル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 防止が有効であると、ポートは STP BPDU を転送しません。

L2 Features > BPDU 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。

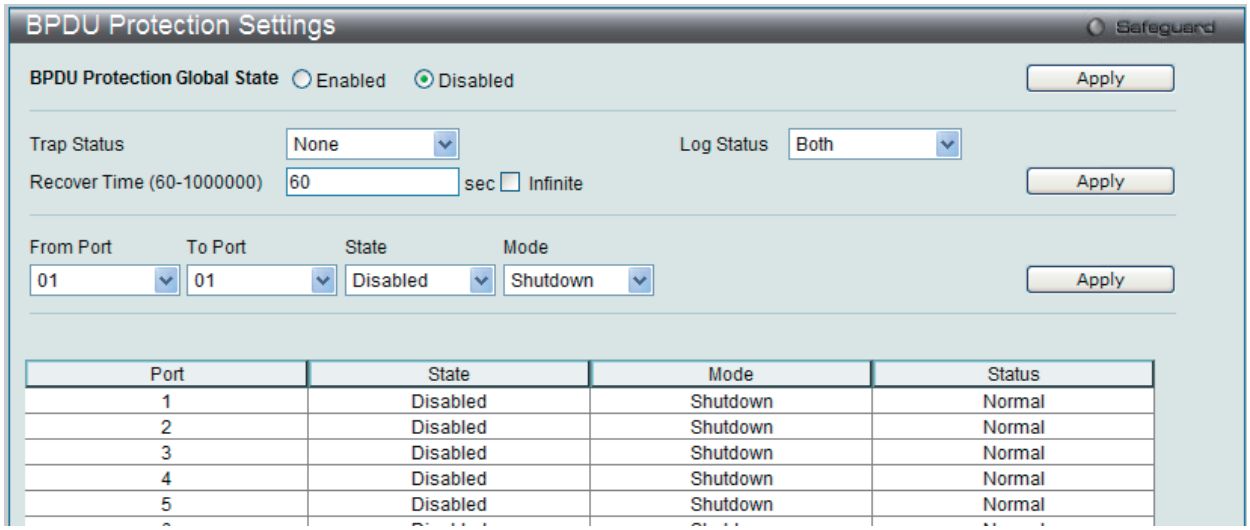


図 7-28　BPDU Protection Settings 画面

以下の項目を使用して、設定します。

項目	説明
BPDU Protection Global State	BPDU アタック防止機能をグローバルに有効または無効にします。初期値は無効です。
Trap State	トラップの状態を指定します。初期値は「None」（なし）です。
Log State	ログ出力の状態を指定します。初期値は「Both」です。
Recover Time	BPDU 防止の自動復帰タイマを指定します。復帰タイマの初期値は 60 です。60 から 1000000（秒）の範囲で指定できます。
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。（初期値）

「Apply」ボタンをクリックし、変更を有効にします。

IGMP Snooping（IGMP Snooping の設定）

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

注意 Source フィルタはサポートしていません。

IGMP Snooping Settings（IGMP Snooping グローバル設定）

IGMP Snooping 設定をグローバルに有効または無効にします。

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

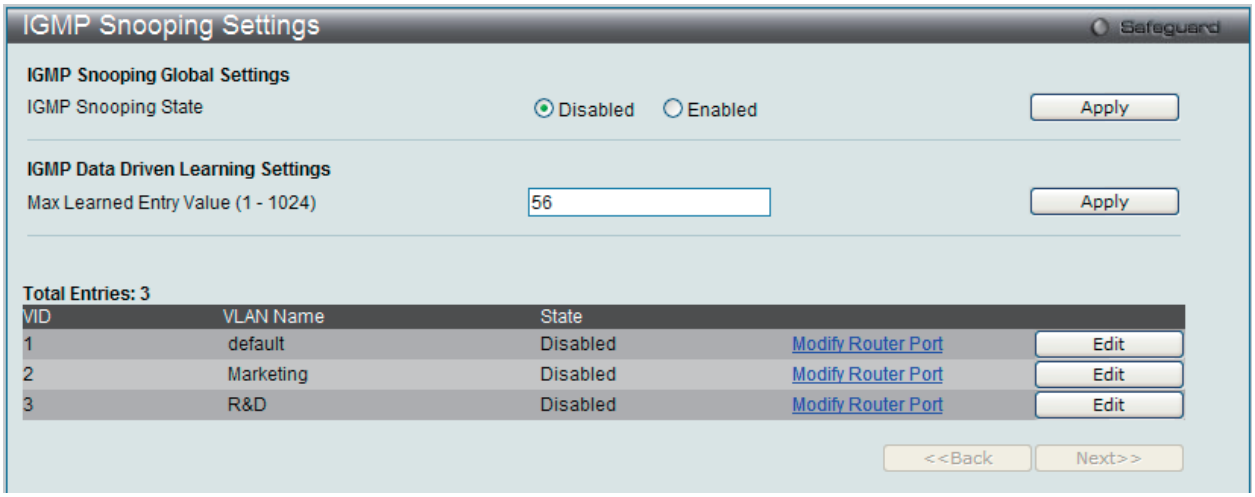


図 7-29　IGMP Snooping Settings 画面

画面には以下の項目があります。

項目	説明
IGMP Snooping Global Settings	
IGMP Snooping State	IGMP Snooping の有効 / 無効を設定します。IGMP Snooping を有効にするためには、はじめにマルチキャストフィルタリングのブリッジを有効にする必要があります。 • 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）
IGMP Data Driven Learning Settings	
Max Learned Entry Value (1-1024)	学習エントリの最大値を 1 から 1024 で入力します。

IGMP Snooping 機能の利用

画面上部の「IGMP Snooping Global Settings」セクションでスイッチ全体に機能を有効にします。

1. 「IGMP Snooping State」の「Enabled」ボタンをクリックします。
2. 「Apply」ボタンをクリックして、IGMP Snooping 設定を適用します。

IGMP Data Driven Learning の設定

1. 「IGMP Data Driven Learning Settings」セクションの「Max Learned Entry Value (1-1024)」に学習エントリの最大値を 1 から 1024 で入力します。
2. 「Apply」ボタンをクリックして、設定を適用します。

IGMP Snooping 機能の詳細設定

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 に対しての詳細な設定を行います。

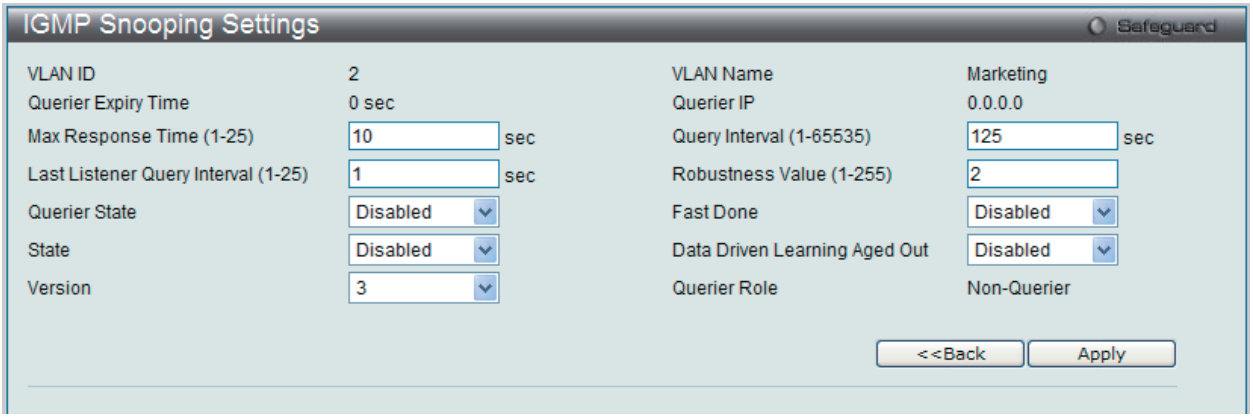


図 7-30　IGMP Snooping Settings 画面 - Edit

以下の項目を参照または編集することができます。

項目	説明
VLAN ID	VLAN 名と共に、IGMP Snooping 設定の対象となる VLAN を識別するために使用する ID です。
VLAN Name	VLAN ID と共に、IGMP Snooping 設定を行う対象の VLAN を識別します。
Querier Expiry Time	クエリの有効時間を表示します。
Querier IP	ネットワークに IGMP クエリを送信するデバイスの IP アドレスを入力します。
Max Response Time (1-25)	メンバからのレポートを待つ最大時間を 1-25（秒）で設定します。初期値は 10（秒）です。
Query Interval (1-65535)	IGMP クエリを送信する間隔を 1-65535（秒）の範囲から指定します。初期値は 125（秒）です。
Last Member Query Interval (1-25)	Group-Specific Query メッセージ（Leave Group メッセージに応じて送信されるものも含む）の最大送信間隔を指定します。初期値は 1 です。
Robustness Value (1-255)	予想されるパケット損失率に合わせて調整します。ご使用のサブネットワークで VLAN のパケット損失率が高いと予想される場合、高い値を指定します。多くのパケットが失われると予想される場合、高い値を指定します。1-255 の範囲から指定します。初期値は 2 です。
Querier State	有効または無効にして、IGMP Query パケットの送信を可能または不可能にします。初期値は無効です。
Fast Done	「Enabled」または「Disabled」を選択し、Fast Leave 機能を有効または無効にします。初期値は「Disabled」です。この機能を有効にすると、マルチキャストグループのメンバは、スイッチが IGMP Leave Report パケットを受信すると、Last Member Query Timer の実行を待たずに直ちにグループから脱退することができます。
State	指定した VLAN への IGMP Snooping 機能を「Enabled」（有効）/「Disabled」（無効）にします。初期値は無効です。
Data Driven Learning Aged Out	指定した VLAN の IGMP Snooping data driven データ学習のタイムアウトを有効または無効にします。
Version	指定ポートによって送信される IGMP パケットのバージョンを指定します。インタフェースが受信した IGMP パケットが指定のバージョン以降のバージョンを持つ場合、パケットは破棄されます。初期値は 3 です。
Querier Role	Query パケット送信についてのスイッチの動作を表示します。 • Querier - スイッチが IGMP Query パケットの送信を行います。 • Non-Querier - スイッチが IGMP Query パケットの送信を行いません 本項目は「Querier State」と「State」で「Enabled」指定時には「Querier」と表示されます。

上記項目設定後、「Apply」ボタンをクリックして変更を有効にします。

前の画面に戻るためには、「<< Back」ボタンをクリックします。

IGMP Snooping ルータポート設定の変更

対応する「Modify Router Port」リンクをクリックし、以下の画面を表示します。

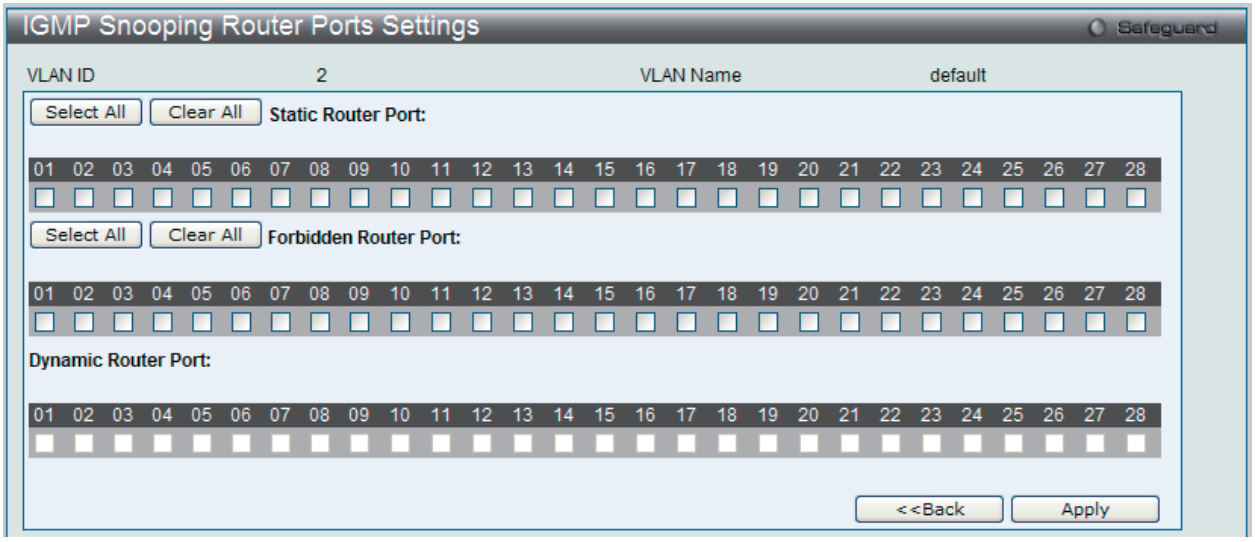


図 7-31　IGMP Snooping Router Ports Settings 画面

メンバにするポートのチェックボックスを選択して「Apply」ボタンをクリックします。

「IGMP Snooping Settings」画面に戻るためには、「<<Back」ボタンをクリックします。

IGMP Access Control Settings（IGMP アクセスコントロール設定）

ここでは、スイッチの IGMP アクセスコントロールの設定を行います。

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

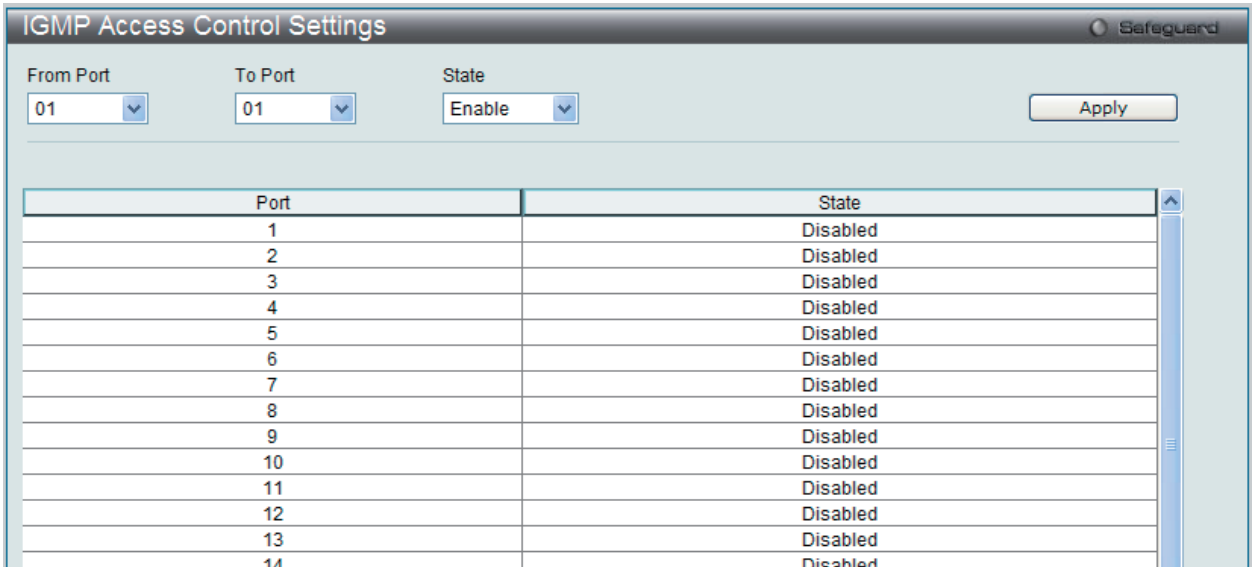


図 7-32　IGMP Access Control Settings 画面

以下の項目を参照または編集することができます。

項目	説明
From Port/To Port	ポート範囲を選択します。
State	IGMP アクセスコントロールを有効または無効にします。有効にした場合、スイッチは IGMP Join リクエストを受信すると、Access リクエストを RADIUS サーバに送信して認証を行います。

「Apply」ボタンをクリックし、変更を有効にします。

IGMP Snooping Multicast VLAN Settings（ISM VLAN 設定）

スイッチング環境には、マルチプル VLAN が存在する可能性があります。マルチキャストクエリがスイッチを通過する度に、スイッチはシステム上の各 VLAN にそれぞれ異なるデータのコピーを送信する必要があります。これは順々にデータトラフィックを増加していき、トラフィックのパスを塞いでしまう可能性があります。トラフィックの負荷を軽減するために、マルチキャスト VLAN を組み込むことができます。これらのマルチキャスト VLAN は、複数のコピーの代わりにこのマルチキャストトラフィックを 1 つのコピーとしてマルチキャスト VLAN の受信者に送信します。

スイッチに組み込まれている他の一般的な VLAN に関係なく、マルチキャストトラフィックを送信したいマルチプル VLAN に対してどんなポートも追加することができます。マルチキャストトラフィックがスイッチに入力されるソースポートを設定した後、入力マルチキャストトラフィックが送信されるべきポートを設定します。ソースポートは受信ポートとなることはできないため、そのように設定されると、スイッチはエラーメッセージを表示します。一度適切に設定されると、マルチキャストデータの流れはタイムリーで信頼できる方式で受信ポートに中継されます。

スイッチにマルチキャスト VLAN の作成と設定を行います。

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

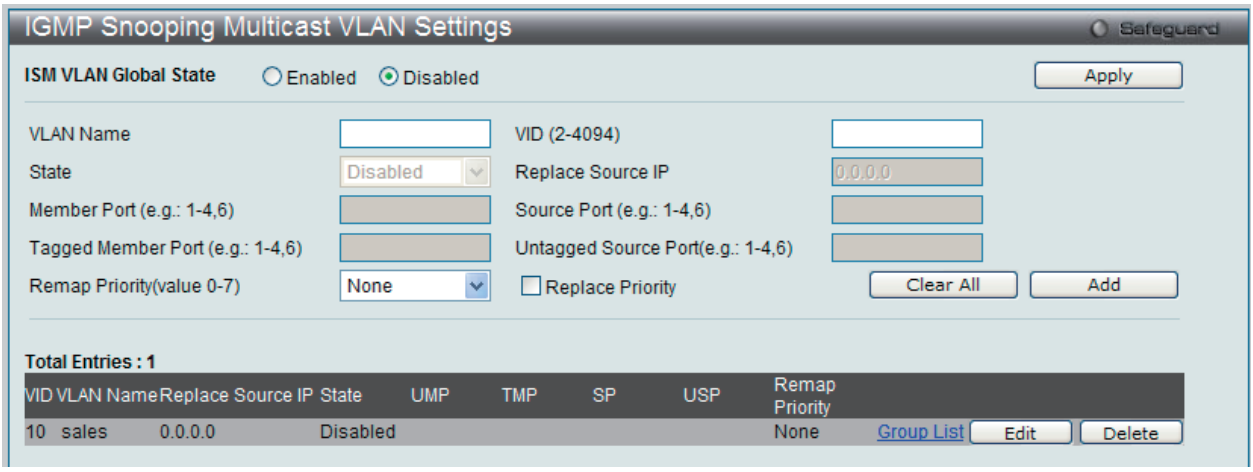


図 7-33　IGMP Snooping Multicast VLAN Settings 画面

マルチキャスト VLAN の登録

1. 「ISM VLAN Global State」を「Enabled」（有効）を選択し、「Apply」ボタンをクリックします。

2. 各項目を入力後、「Add」ボタンをクリックしてエントリを追加します。

以下の項目を使用して、設定します。

項目	説明
ISM VLAN Global State	IGMP Snooping Multicast（ISM）VLAN のグローバルな状態を有効または無効にします。
VLAN Name	作成するマルチキャスト VLAN 名（半角英数字 32 文字以内）を入力します。「Edit」画面では定義済みのマルチキャスト VLAN 名を表示します。
VID (2-4094)	マルチキャスト VLAN に対応する VLAN ID を追加または編集します。2-4094 の値を指定します。
State	選択した VLAN のマルチキャスト VLAN を「Enabled」（有効）または「Disabled」（無効）にします。
Replace Source IP	IGMP Snooping 機能を使用すると、ホストが送信した IGMP レポートパケットは送信元ポートに転送されます。パケットの転送の前に、Join パケット内の送信元 IP アドレスはこの IP アドレスに変更されます。設定しない場合、送信元 IP アドレスは変更されません。
Member Ports (e.g. : 1-4,6)	マルチキャスト VLAN に追加するメンバポートの範囲。メンバポートはマルチキャスト VLAN のタグなしメンバになります。
Source Ports (e.g. : 1-4,6	マルチキャスト VLAN 用の送信元ポートを選択します。
Tagged Member Port)	マルチキャスト VLAN のメンバとしてタグ付けをされるポートを選択します。
Untagged Source Port (e.g.: 1-4, 6)	マルチキャスト VLAN に追加するタグなし送信元ポートの範囲。再割り当てされたタグなし送信元ポートの PVID は、自動的にマルチキャスト VLAN に変更されます。
Remap Priority (Value 0-7)	リマップの優先順位は、マルチキャスト VLAN に送信されるデータトラフィックに対応しています。「None」を選択した場合、パケットの元の優先順位が使用されます。初期値は「None」です。
Replace Priority	選択すると、スイッチがリマップ優先順位に基づいてパケットの元の優先順位を変更します。本オプションは、リマップ優先順位を設定している場合にのみ有効です。

マルチキャスト VLAN の変更

1. 変更するエントリの「Edit」ボタンをクリックし、以下の画面を表示します。

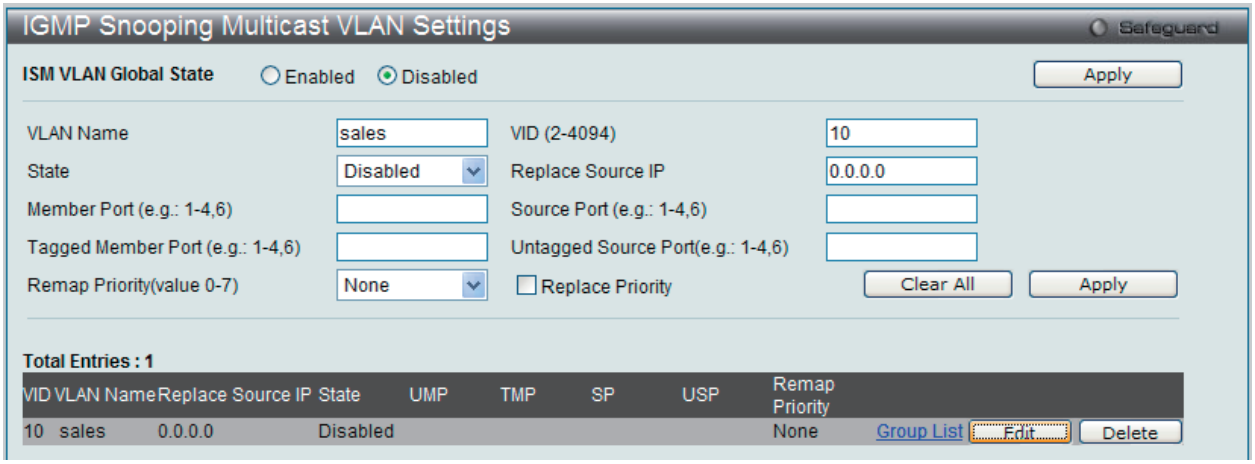


図 7-34　IGMP Snooping Multicast VLAN Settings 画面 - Edit

2. 画面上部に表示される定義済みの項目を変更し、「Apply」ボタンをクリックします。

マルチキャスト VLAN グループリストの設定

1. 既に作成したプロファイルにマルチキャスト VLAN を追加する場合は、追加するグループリストの「Group List」のリンクをクリックし、以下の画面を表示します。

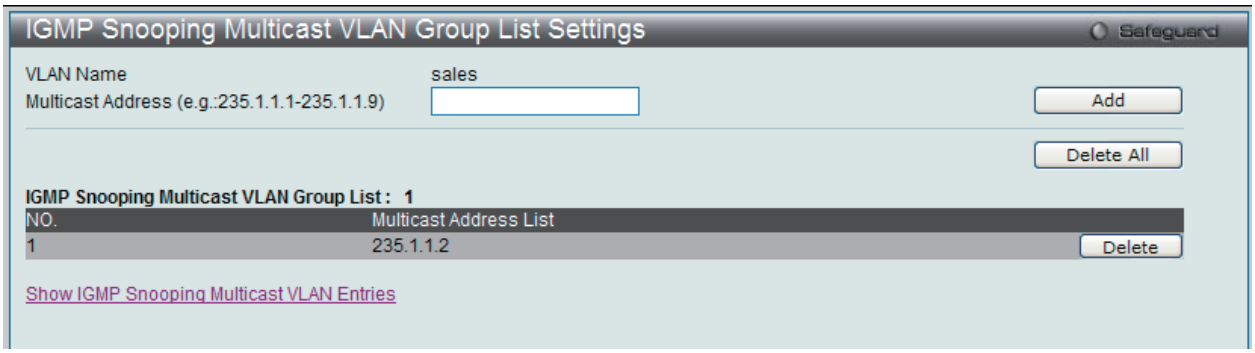


図 7-35　IGMP Snooping Multicast VLAN Group List Settings 画面

2. マルチキャストアドレスを入力し、「Add」ボタンをクリックしてエントリを追加します。

マルチキャスト VLAN グループリストの削除

1. ISM VLAN グループリストを削除する場合は、該当する行の「Delete」ボタンをクリックします。

「IGMP Snooping VLAN Settings」画面に戻るためには、「Show IGMP Snooping Multicast VLAN Entries」リンクをクリックします。
「Delete All」ボタンをクリックすると、この画面のすべてのエントリを削除します。

IP Multicast Profile Settings（IP マルチキャストプロファイル設定）

プロファイルを追加し、指定したスイッチポートに受信するマルチキャストアドレスレポートを設定します。本機能は、受信するレポート数とスイッチに設定するマルチキャストグループ数を制限することができます。
特定のスイッチポートに到着するレポートを受信する（Permit）またはレポートを拒否する（Deny）IP アドレス /IP アドレス範囲を設定することができます。

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

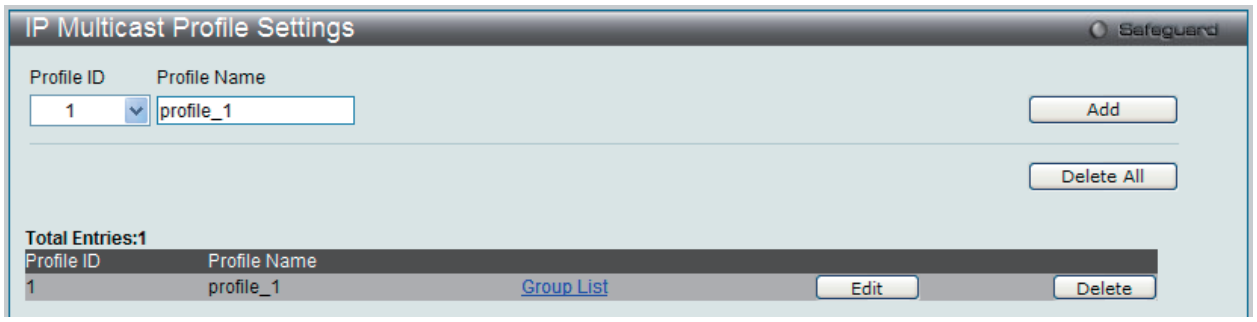


図 7-36　IP Multicast Profile Settings 画面

以下の項目を使用して設定します。

項目	説明
Profile ID	1-24 の Profile ID を指定します。
Profile Name	IP マルチキャストプロファイル名を入力します。

エントリ名の変更
対応する「Edit」ボタンをクリックし、以下の画面を表示します。

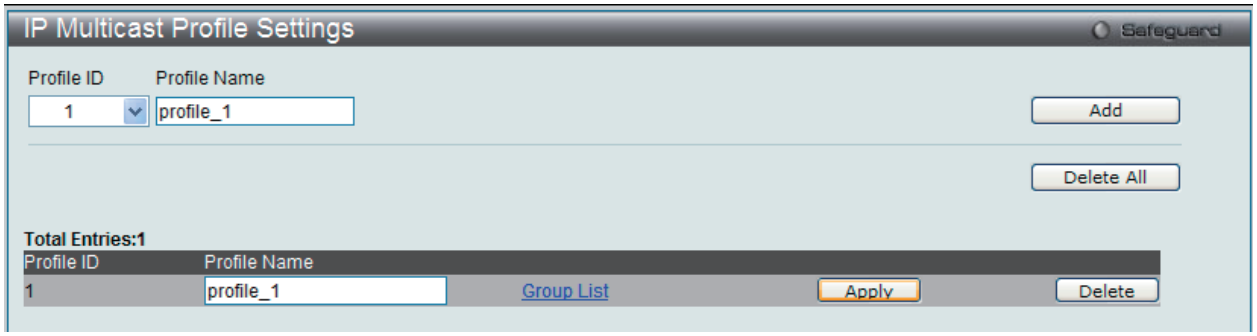


図 7-37　IP Multicast Profile Settings 画面 - エントリ名の変更

エントリの削除
削除するエントリの「Delete」ボタンをクリックします。

エントリの変更
1. 「Multicast Address List」欄の対応する「Group List」リンクをクリックし、以下の画面を表示します。

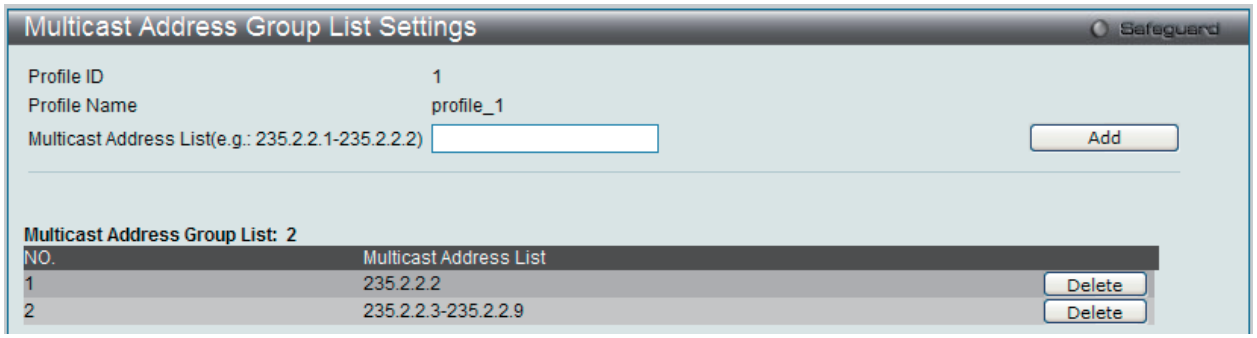


図 7-38　Multicast Address Group List Settings 画面

2. 「Multicast Address Group List」でアドレス範囲を入力し、「Add」ボタンをクリックします。

エントリの削除
該当するエントリの「Delete」ボタンをクリックします。

「IP Multicast Profile Settings」画面に戻るには、「Show IP Multicast Profile Entries」リンクをクリックします。

Limited Multicast Range Settings（IP マルチキャスト範囲の限定設定）

「Limited IP Multicast Range」に含まれるスイッチポートを設定します。

ポート範囲を設定し、IP マルチキャストプロファイルを関連付けすることで、プロファイル内に定義したマルチキャストグループに対する IGMP Join リクエストを許可または拒否します。送信元ポートによって受信ポートに送信可能だとして許容されるマルチキャストアドレスの範囲を設定します。

L2 Features > IGMP Snooping > Limited Multicast Range 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。

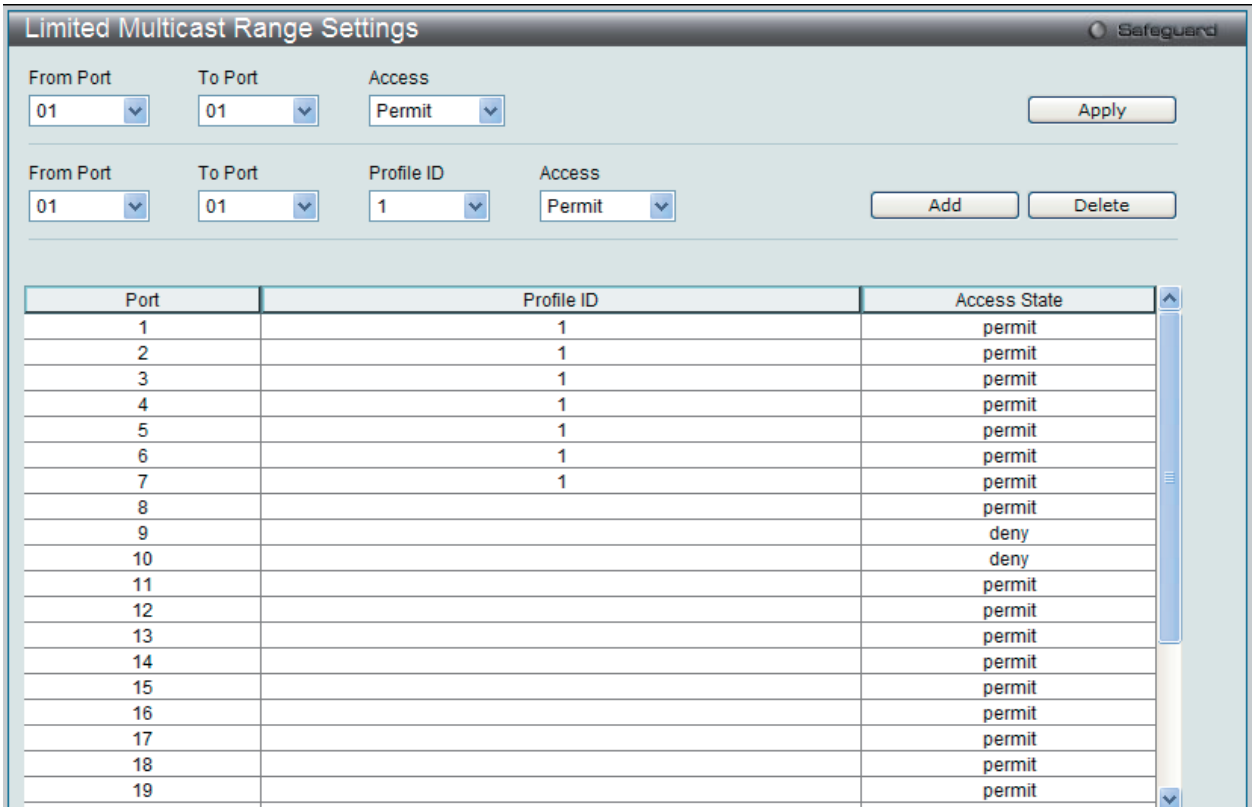


図 7-39　Limited Multicast Range Settings 画面

以下の項目を指定してポートにマルチキャストアドレスフィルタリング機能を設定します。

項目	説明
From Port / To Port	プルダウンメニューを使用して、マルチキャストアドレスフィルタ機能を追加または削除するポート範囲を指定します。
Access	プルダウンメニューを使用して、以下のオプションの一つを選択します。 • Permit -「From/To」プルダウンメニューで指定したポートに一致するパケットを許可することを指定します。 • Deny -「From/To」プルダウンメニューで指定したポートに一致するパケットを破棄することを指定します。

「Apply」ボタンをクリックし、設定を適用します。

画面中央にある項目を設定し、指定のプロファイルのポートにマルチキャストアドレスフィルタリング機能を設定します。

項目	説明
From Port / To Port	プルダウンメニューを使用して、マルチキャストアドレスフィルタ機能を追加または削除するポート範囲を指定します。
Profile ID	プルダウンメニューを使用して、指定したポート範囲に (から) 追加または削除するプロファイル ID を選択します。
Access	プルダウンメニューを使用して、以下のオプションの一つを選択します • Permit - プロファイル内に指定されているアドレスに一致するパケットを許可することを指定します。 • Deny - プロファイル内に指定されているアドレスに一致するパケットを破棄することを指定します。

新しいマルチキャストアドレス範囲の追加

適切な情報を入力し、「Add」ボタンをクリックします。

マルチキャストアドレス範囲の削除

情報を入力し、「Delete」ボタンをクリックします。

Max Multicast Group Settings（最大マルチキャストグループ設定）

ここでは、学習されるマルチキャストグループの最大数をスイッチのポートに設定します。

これらの設定を行うには、**L2 Features > IGMP Snooping > Max Multicast 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。

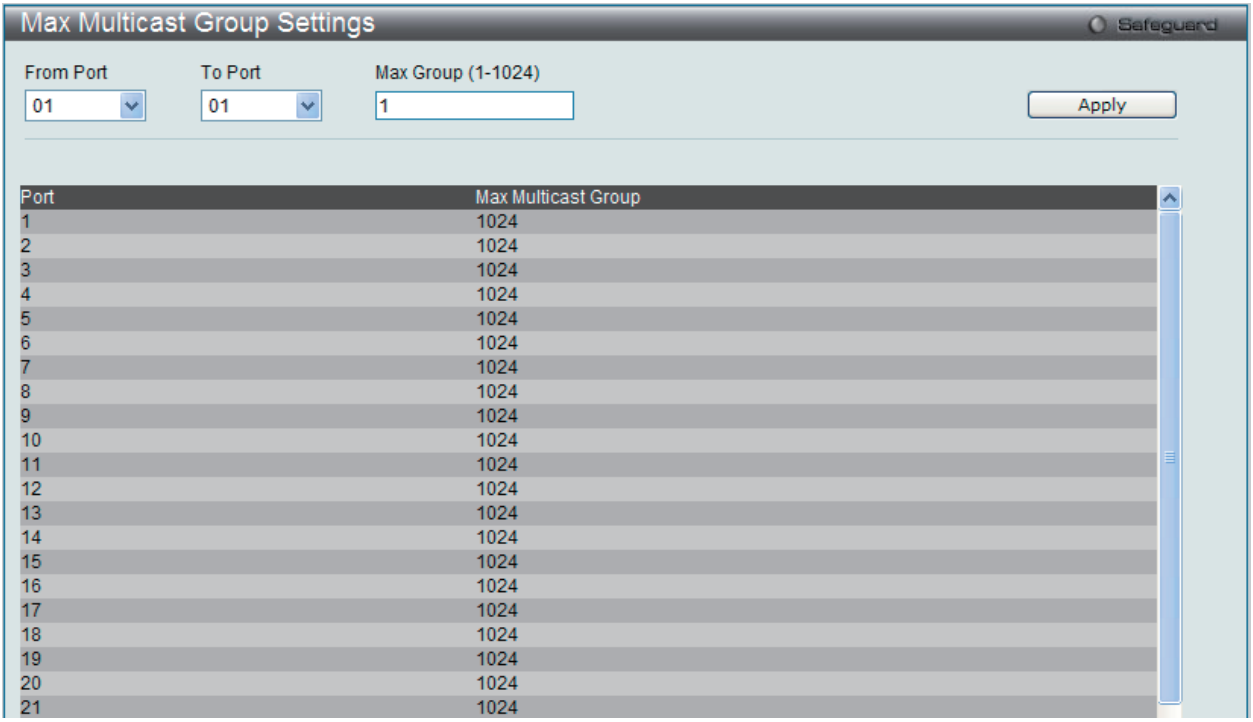


図 7-40　Max Multicast Group Settings 画面

以下の項目を使用して、設定します。

項目	説明
From Port/To Port	プルダウンメニューを使用して、ポート範囲を選択します。
Max Group (1-1024)	マルチキャストグループの最大数を指定します。範囲は 1-1024 です。

エントリを追加するためには、適切な情報を入力し「Apply」ボタンをクリックします。

MLD Snooping Settings（MLD Snooping 設定）

Multicast Listener Discovery（MLD）Snooping は、IPv4 の IGMP Snooping と同じように使用される IPv6 機能です。マルチキャストデータを要求する VLAN に接続しているポートを検出するために使用されます。選択した VLAN 上のすべてのポートにマルチキャストトラフィックが流れる替わりに、MLD Snooping は、リクエストポートとマルチキャストの送信元によって生成する MLD クエリと MLD レポートを使用してデータを受信したいポートにのみマルチキャストデータを転送します。
MLD Snooping は、エンドノードと MLD ルータ間で交換される MLD コントロールパケットのレイヤ 3 部分を調査することで実行されます。ルータがマルチキャストトラフィックをリクエストしていることをスイッチが検出すると、該当ポートを IPv6 マルチキャストテーブルに直接追加し、そのポートにマルチキャストトラフィックを転送する処理を開始します。マルチキャストルーティングテーブル内のこのエントリは該当ポート、その VLAN ID、および関連する IPv6 マルチキャストグループアドレスを記録し、このポートをアクティブな Listening ポートと見なします。アクティブな Listening ポートはマルチキャストグループデータの受信だけをします。

スイッチは、MLD Snooping バージョン 1 およびバージョン 2 をサポートしています。

注意 Source フィルタはサポートしていません。

MLD コントロールメッセージ
MLD Snooping バージョン 1 の実行には、デバイス間で 3 つのタイプのメッセージが送信されます。これらのメッセージは、130、131 および 132 にラベル付けされた 3 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 バージョン 1
IPv4 の IGMPv2 Host Membership Query（HMQ）と類似のものです。ルータは ICMPv6 パケットヘッダ内に 130 とラベル付けされた本メッセージを送信し、マルチキャストデータをリクエストしているリンクがあるかどうか問い合わせます。ルータが送信する MLD クエリメッセージには 2 つのタイプがあります。General Query は全マルチキャストアドレスに Listening ポートすべてにマルチキャストデータを送信する準備が整ったことを通知するために使用します。また、Multicast Specific query は特定のマルチキャストアドレスに送信準備が整ったことを通知するために使用します。 2 つのメッセージタイプは IPv6 ヘッダ内のマルチキャスト終点アドレス、および Multicast Listener クエリメッセージ内のマルチキャストアドレスによって区別します。

2. Multicast Listener Report Version1
IGMPv2 の Host Membership Report（HMR）と類似のものです。Listening ポートは、Multicast Listener クエリメッセージに応じて ICMPv6 パケットヘッダ内に 131 とラベル付けされた本メッセージをクエリスイッチに送信し、マルチキャストアドレスからマルチキャストデータを受信する希望があることを伝えます。

3. Multicast Listener Done
IGMPv2 の Leave Group Message と類似のものです。マルチキャスト Listening ポートは、ICMPv6 パケットヘッダ内に 132 とラベル付けされた本メッセージを送信し、特定のマルチキャストグループアドレスからマルチキャストデータを受信せず、このアドレスからのマルチキャストデータとともに" done"（完了）した旨を伝えます。スイッチは本メッセージを受信すると、この Listening ポートには特定のマルチキャストグループアドレスからのマルチキャストトラフィックを送信しません。

MLD Snooping バージョン 2 の実行には、デバイス間で 2 つのタイプのメッセージが送信されます。これらのメッセージは、130 および 143 にラベル付けされた 2 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、Version 2
IPv4 の IGMPv3 Membership Query と類似のものであり、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。MLD Snooping Version 2 では、ルータが送信する MLD クエリメッセージに次のような 3 つのタイプがあります。

- ルータが General Query メッセージを送信して、どのマルチキャストアドレスが接続しているリンクにリスナを持っているかを学習します。General Query では、マルチキャストアドレスフィールドと Source 数フィールドの値はともに 0 に設定されています。
- ルータが Multicast Address Specific Query メッセージを送信して、特定のマルチキャストアドレスが接続しているリンクにリスナを持っているかどうかを学習します。Multicast Address Specific Query では、マルチキャストアドレスフィールドにはルータが学習したいマルチキャストアドレスが設定され、一方、Source 数フィールドは 0 に設定されています。
- ルータがマルチキャストアドレスと Source Specific Query を送信して、特定のマルチキャストアドレスに向けた指定リストの中の送信元で接続するリンクにリスナを持っているものがあるかどうかを学習します。マルチキャストアドレスおよび Source Specific Query では、マルチキャストアドレスフィールドにはルータが学習したいマルチキャストが含まれ、一方 Source Address フィールドにはルータが学習したい送信元アドレスが含まれます。

2. Multicast Listener Report Version2
IGMPv3 の Host Membership Report（HMR）と類似のものです。Listening ポートは、Multicast Listener クエリメッセージに応じて ICMPv6 パケットヘッダ内に 143 とラベル付けされた本メッセージをクエリスイッチに送信し、マルチキャストアドレスからマルチキャストデータを受信する希望があることを伝えます。

ここでは、スイッチの MLD Snooping を有効にして、MLD snooping の設定を行います。
MLD Snooping 機能を有効にするためには、MLD Snooping Global Settings 欄の「Enable」をチェックして「Apply」ボタンをクリックします。

MLD Snooping 設定

L2 Features > MLD Snooping 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。

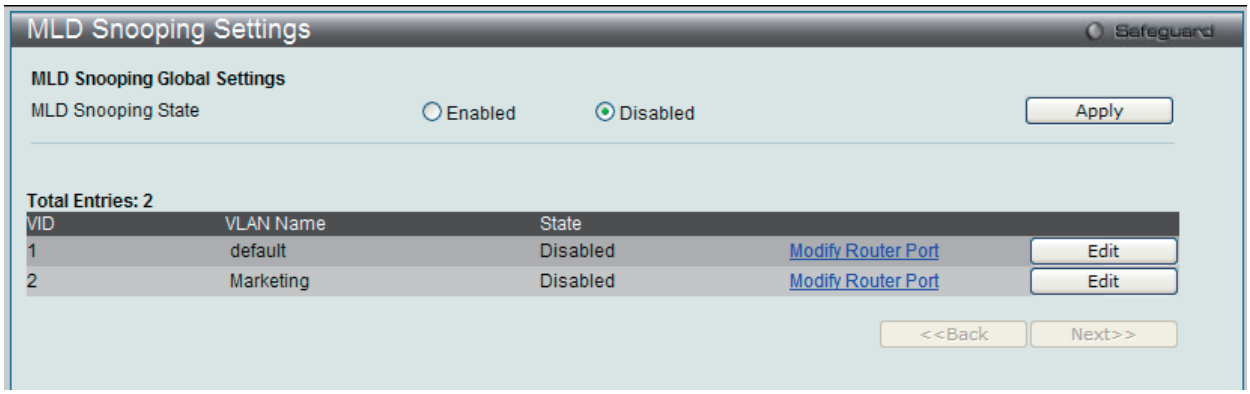


図 7-41　MLD Snooping Settings 画面

VLAN よって定義されているスイッチの現在の MLD Snooping 設定を表示します。

MLD Snooping のグローバル設定

「MLD Snooping State」で MLD Snooping 機能を「Enabled」（有効）または「Disabled」（無効）にします。

以下の項目を指定します。

項目	説明
MLD Snooping State	MLD Snooping を「Enabled」（有効）または「Disabled」（無効）にします。初期値は「Disabled」です。

「Apply」ボタンをクリックし、変更を有効にします。

MLD Snooping に特定の VLAN を設定する

対応する VLAN の「Edit」ボタンをクリックして以下の画面を表示します。

図 7-42　MLD Snooping Settings 画面 - Edit

以下の項目を設定します。

項目	説明
VLAN ID	VLAN 名と共に、MLD Snooping 設定の編集を行う VLAN を識別するために使用する ID です。
VLAN Name	VLAN ID と共に、IGMP Snooping 設定の編集を行う VLAN を識別するために使用する名称です。
Query Interval (1-65535)	MLD クエリを送信する間隔（秒）を設定します。1-65535 の範囲から指定します。初期値は 125（秒）です。
Max Response Time (1-25)	メンバからのレポートを待つ最大許容時間（秒）を設定します。1-25 の範囲から指定します。初期値は 10（秒）です。
Robustness Value (1-255)	予想されるパケット損失率に合わせて調整します。パケット損失率が高ければ大きい数値を指定します。1-255 の範囲から指定します。初期値は 2（秒）です。
Last Listener Query Interval (1-25)	Group-Specific Query メッセージ（Leave Group メッセージに応じて送信されるものも含む）の最大送信間隔を指定します。初期値は 1（秒）です。
Fast Done	有効にすると、Fast Leave 機能が有効になります。そして、マルチキャストグループのメンバは、スイッチが MLD Leave Report パケットを受信すると、Last Listener Query Interval の実行を待たずに直ちにグループから脱退することができます。初期値は無効です。
State	指定した VLAN からの MLD Snooping 機能を「Enabled」（有効）/「Disabled」（無効）にします。初期値は無効です。
Version	ここではスイッチの MLD バージョンが 2 であることを示しています。
Querier Role	Query パケット送信についてのスイッチの動作を表示します。 • Querier - スイッチが MLD query パケットの送信を行うことを示します。 • Non-Querier - スイッチが MLD query パケットの送信を行わないことを示します。

上記項目設定後、「Apply」ボタンをクリックして変更を有効にします。

MLD Snooping ルータポートの設定

MLD Snooping ルータポート設定を編集する場合は、対応する「Modify Router Port」リンクをクリックし、以下の画面を表示します。

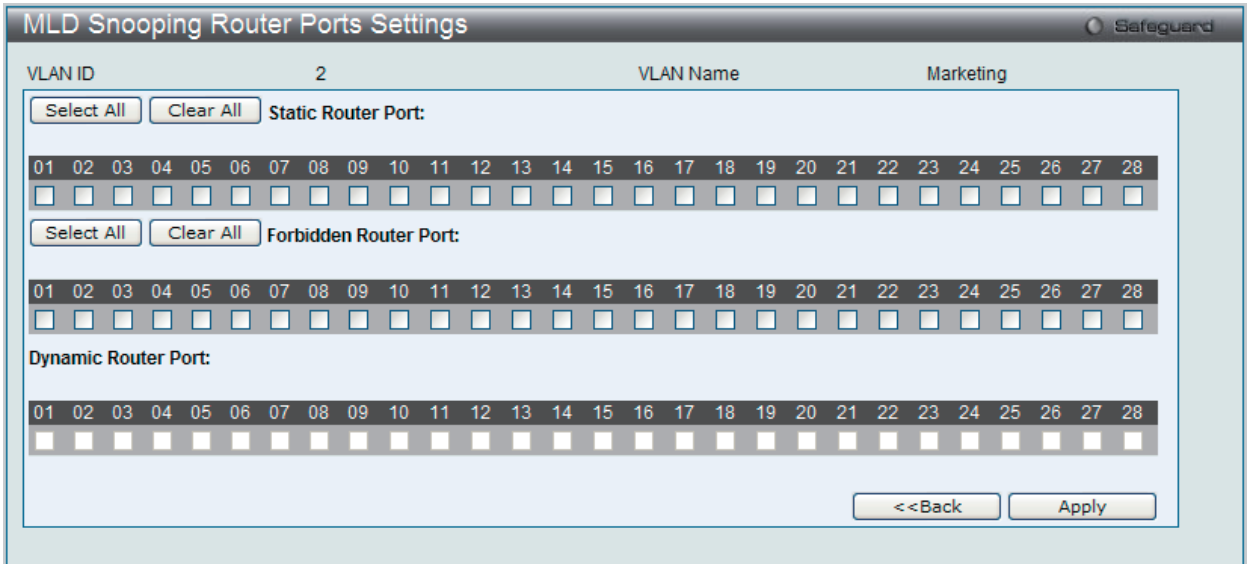


図 7-43　MLD Snooping Router Ports Settings 画面

設定変更後、適用するルータポートを選択し「Apply」ボタンをクリックします。

すべてのスタティックルータポート、またはすべての適用しないルータポートを選択するためには、「Select All」ボタンをクリックします。
選択したルータポートの選択をすべて解除するためには、「Clear All」ボタンをクリックします。

「<<Back」ボタンをクリックすると、「MLD Snooping Settings」画面に戻ります。

Port Mirror（ポートミラーリングの設定）

本スイッチはポート上で送受信したフレームをコピーし、別のポートに転送します。スニファーやRMON probeのようなモニタデバイスをミラーポートに接続し、最初のポートを通過するパケット情報を参照できます。ネットワーク監視とトラブルシューティングの目的で使用します。

ポートミラーリングの設定を行うには、**L2 Features > Port Mirror** の順にメニューをクリックし、以下の画面を表示します。

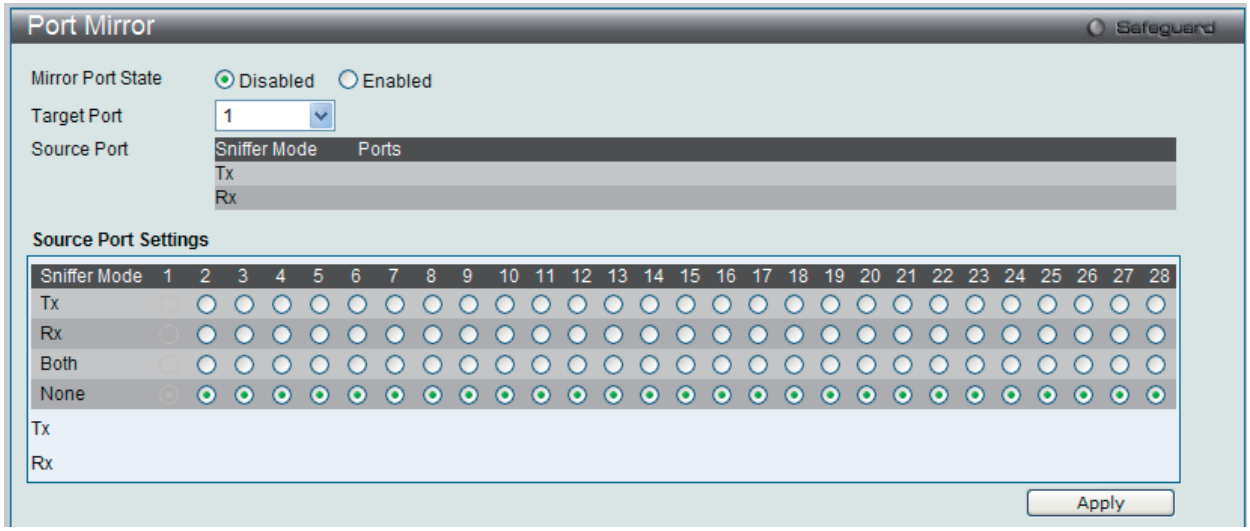


図 7-44　Port Mirror 画面

ミラーポートの設定手順：

1. 「Mirror Port State」で「Enabled」（有効）を選択します。
2. ソースポートからフレームのコピーを受信する「Target Port」（ターゲット）を選択します。
3. フレームのコピーを行う対象の「Source port」（ソースポート）とコピーを行うフレームの方向（入力：Tx、出力：Rx、両方：Both、なし：None）を選択します。
4. 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　転送速度の速いポートを遅いポートにミラーリングはできません。例えば、100Mbps ポートからのトラフィックを 10Mbps ポートにミラーリングしようとすると、スループットの問題が起こります。ソースポートの速度はターゲットポートと同じかそれ以下としてください。

注意　また、ターゲットポートはトランクグループに属することはできません。設定をしようとするとエラーメッセージが表示され、設定は無効になります。ターゲットポートとソースポートを同じポートにはできませんのでご注意ください。

本画面には次の項目があります。

項目	説明
Target Port Setting	
Mirror Port State	ターゲットポートを「Enabled」（有効）/Disabled（無効）に設定します。初期値は「Disabled」です。
Target Port	ターゲットポートを設定します。
Source Port	ソースデータの方向とソースポートを表示します。
Source Port Setting	
Tx	ポートから送信されるデータをモニタします。
Rx	ポートで受信するデータをモニタします。
Both	ポートで送受信するデータ両方をモニタします。
None	ポートのデータはモニタしません。

Loopback Detection Settings（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。ループ検知動作モードを選択します。ポートベースと VLAN ベースの 2 つのモードがサポートされています。ポートベースモードでは、ポートはループを検知すると、シャットダウン（無効）されます。VLAN ベースモードでは、ポートはループが検知される VLAN 上のパケットを処理することはできません。初期モードはポートベースです。Loopback Detection Recover Time がタイムアウトになると、ループバック検知ポートまたは VLAN は再起動 (Forwarding 状態へ遷移) を行います。ループバック検知機能はポート範囲に実行されます。

L2 Features > Loopback Detection 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。

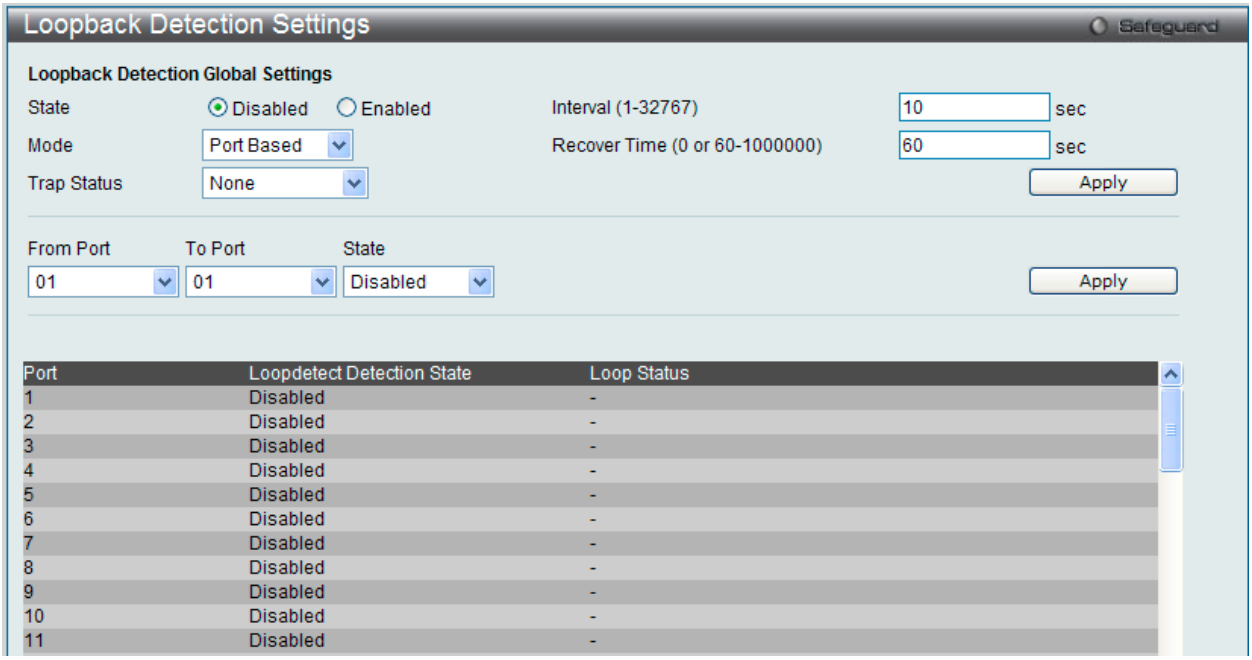


図 7-45　Loopback Detection Settings 画面

本画面には次の項目があります。

項目	説明
State	プルダウンメニューで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。
Interval (1-32767)	ループ検知間隔を設定します。（1-32767 秒）初期値は 10(秒) です。
Mode	「Port Based」または「VLAN Based」を選択します。
Recover Time (0 or 60-1000000)	ループが検知された場合にリカバリする時間 (秒) を指定します。指定時間に到達すると、スイッチはループをチェックします。ループが検知されないと、ポートが再度有効になります。0 または 60-1000000（秒）に設定します。0 を指定すると、ループバックリカバリタイムは無効になります。初期値は 60（秒）です。
From Port / To Port	プルダウンメニューで適用するポート範囲を選択します。
State	プルダウンメニューで「Enabled」（有効）または「Disabled」（無効）を指定します。
Trap Status	トラップを送信する状態を選択します。オプションは以下の通りです。 • Loop Detected - ループ状態を検知すると、トラップを送信します。 • Loop Cleared - ループ状態がクリアされると、トラップを送信します。 • None - ループバック検知のトラップを送信しません。(初期値)。 • Both - 検知およびクリアのトラップを両方送信します。

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

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。

Spanning Tree（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（STP、Rapid STP、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、STP、STP、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。

本プロトコルでは、BPDU（Bridge Protocol Data Unit）パケットにタグ付けを行い、受信するデバイスが、スパニングツリーインスタンス、スパニングツリーリージョン、またはそれらに関連付けられた VLAN を区別できるようにしています。MSTI ID（MST インスタンス ID）はこれらのインスタンスをクラス分けします。MSTP では、複数のスパニングツリーを CIST（Common and Internal Spanning Tree）で接続します。CIST は自動的に各 MSTP リージョンとその最大範囲を決定し、1 つのスパニングツリーを構成する 1 つの仮想ブリッジのように見せかけます。そのため、異なる VLAN を割り当てられたフレームは、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設定されたリージョン中の異なるデータ経路を通ります。

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

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

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

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

802.1D-2004 Rapid Spanning Tree

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

RSTP は 802.1D-1998 STP 標準の進化型です。RSTP は、STP を使用する上での制限を克服する目的で開発されました。制限とは、特に今日イーサネットスイッチに取り入れられているレイヤ 3 の諸機能を妨害するものを指しています。RSTP の基本的な機能や用語の多くは STP と同じであると言えます。STP 用の設定項目の多くも RSTP で同じように使用されます。本項では、スパニングツリーの新しいコンセプトと、これらの 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。表 7-3 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。

表 7-3　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 準拠の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。

STP/RSTP/MSTP 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 STP 形式に自動的に変換することができます。しかし、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 Bridge Global Settings（STP ブリッジグローバル設定）

STP をグローバルに設定します。

L2 Features > Spanning Tree > STP Bridge 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。
「STP State」でデバイスの STP をグローバルに有効または無効にします。また、「STP Version」で STP の方式を選択します。

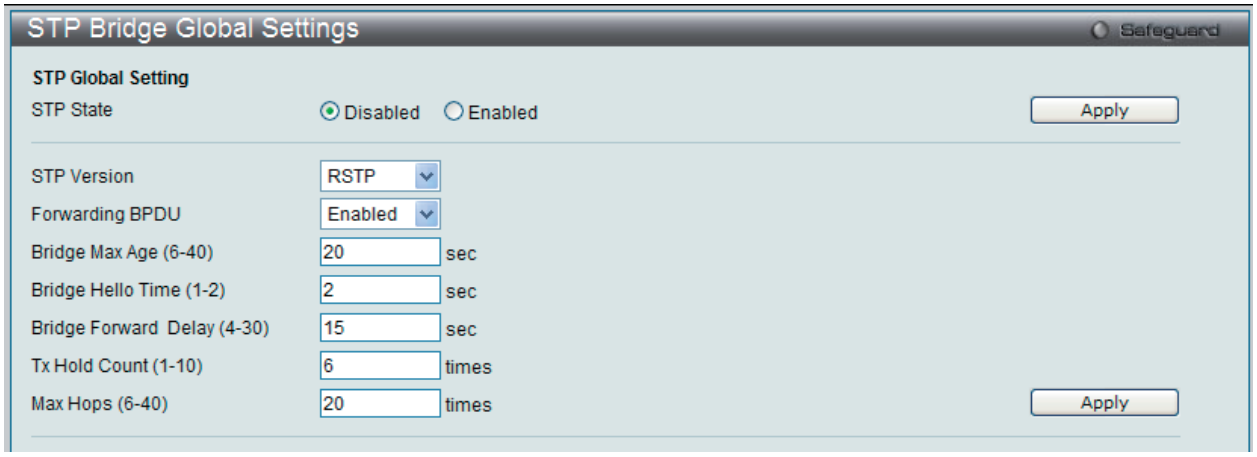


図 7-46　STP Bridge Global Settings 画面 : RSTP（初期値）

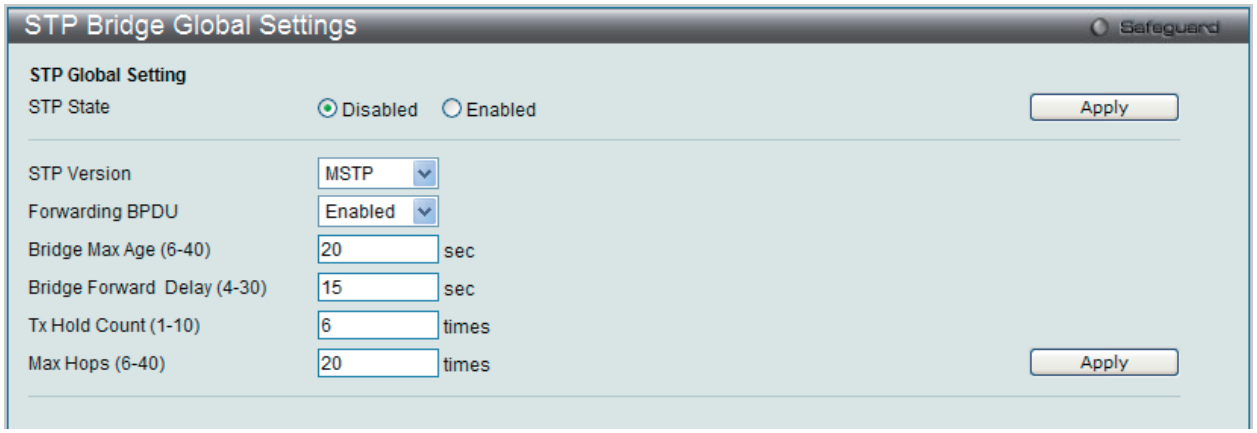


図 7-47　STP Bridge Global Settings 画面 : MSTP

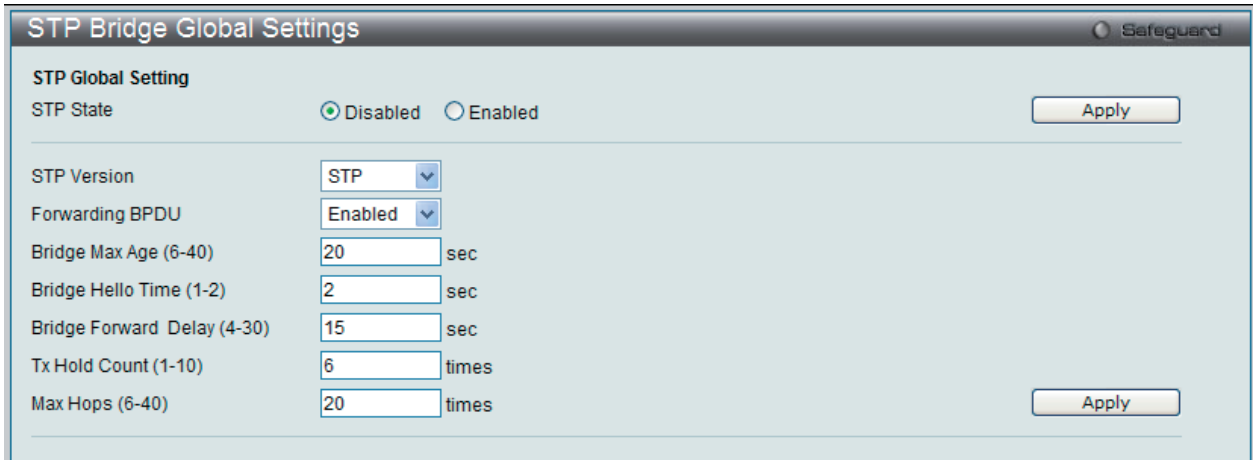


図 7-48　STP Bridge Global Settings 画面 : STP

STP バージョンと対応する設定オプションの説明は、以下の表で参照してください。

注意　Bridge Hello Time は Max. Age より長い時間を指定すると、コンフィグレーションエラーの原因となります。Hello Time と Max. Age の設定には以下の式に従って行ってください。

Bridge Max Age <= 2 x（Bridge Forward Delay - 1 秒）
Bridge Max Age <= 2 x（Bridge Hello Time + 1 秒）

設定には以下の項目が使用されます。

項目	説明
STP State	STP をグローバルに「Enabled」（有効）/「Disabled」（無効）にします。
STP Version	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。
Forwarding BPDU	「Enabled」（有効）または「Disabled」（無効）にします。「Enabled」にすると、STP BPDU パケットが他のネットワークデバイスから送信されます。初期値は「Enabled」です。
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永遠に循環し、新しい有効な情報の伝播を妨げるのを防ぐために設定します。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)	ルートブリッジは、他のスイッチに自分がルートブリッジであることを示すために BPDU パケットを 2 回送信します。本値は、1 回目の送信と 2 回目の送信との間の時間です。STP または RSTP が「STPVersion」で選択された場合だけ本項目は表示されます。MSTP に対して、Hello Time はポートごとに設定される必要があります。詳しくは「STP ポート設定」セクションを参照してください。1-2 秒で指定します。初期値は 2（秒）です。
Bridge Forward Delay (4-30)	スイッチ上のすべてのポートは、Blocking 状態から Forwarding 状態に移行する間に本値で指定した時間 Listening 状態を保ちます。4-30（秒）の範囲から指定します。初期値は 15（秒）です。
Tx Hold Count (1-10)	Hello パケットの最大送信回数を指定します。1-10 の範囲から指定します。初期値は 6 です。
Max Hops (6-40)	スイッチが送信した BPDU パケットが破棄される前のスパニングツリー範囲内のデバイス間のホップ数を設定します。値が 0 に到達するまで、各スイッチは 1 つずつホップカウントを減らしていきます。スイッチは、その後 BDPU パケットを破棄し、ポートに保持していた情報を解放します。ホップカウントは 6-40 で指定します。初期値は 20 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。

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

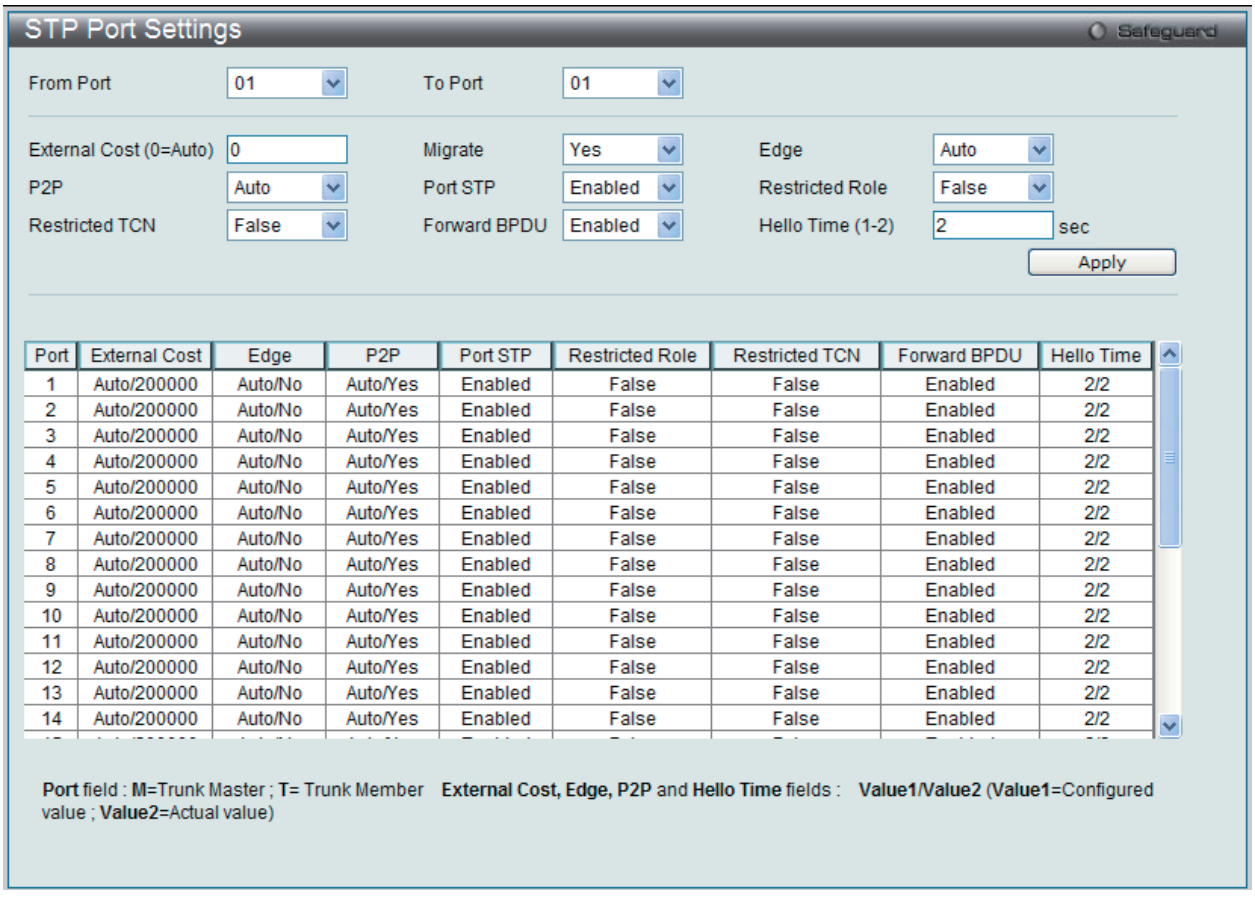


図 7-49　STP Port Setting 画面

スイッチレベルでのスパニングツリー設定のほかに、ポートをグループ分けして、各ポートグループに対してスパニングツリーの設定を行うことも可能です。STP グループは、スイッチレベルでの設定に使用した項目のほかに、ポートプライオリティとポートコストを使用します。

STP グループのスパニングツリーは、スイッチレベルのスパニングツリーと同様の働きをしますが、ルートブリッジの概念はルートポートに置き換えられて考えることができます。グループ内のルートポートは、ポートプライオリティとポートコストに基づいて選出され、ネットワークとグループを接続する役割を果たします。

スイッチレベルの場合と同様に、冗長リンクはブロックされます。スイッチレベルの STP は、スイッチ間、および同様にネットワーク装置間の冗長なリンクをブロックします。ポートレベルの STP は、STP グループ内の冗長リンクをブロックします。

STP グループと VLAN グループを関連付けて定義することをお勧めします。

本画面には以下の項目があります。

項目	説明
From Port / To Port	連続するポートグループを設定します。
External Cost (0=Auto)	指定ポートへのパケット転送をするための適切なコストを表すメトリックを指定します。ポートのコストは自動か、メトリックの値で設定します。初期値は 0（Auto）です。 • 0（Auto）- 選択ポートに可能な最良のパケット転送速度を自動的に設定します。 ポートコストの初期値 :100Mbps ポート = 200000、Gigabit ポート = 20000。 • 値 1-200000000 - 外部転送のコストとして 1 から 200000000 までの値を設定します。数字が低いほどパケット転送は頻繁に行われるようになります。
Migrate	「Yes」を設定すると、STP 設定に関する情報をリクエストする他のブリッジに BPDU パケットをポートが送信するように設定します。スイッチが RSTP に設定されると、ポートは 802.1D STP から 802.1w RSTP に移行することができます。セグメントのすべてまたは一部において 802.1w RSTP にアップグレード可能なネットワークステーションまたはセグメントに接続したポートでは Migration を「Yes」とします。
Edge	選択したポートをエッジポートとするかどうかを指定します。 • True - ポートはエッジポートになります。エッジポート自体はループを発生させることはありませんが、トポロジの変化によりループの可能性が生じると、エッジポートはエッジポートではなくなります。エッジポートは通常 BPDU パケットを受信しません。BPDU パケットを受信すると自動的にエッジポートではなくなります。 • False - ポートはエッジポートではなくなります。 • Auto - 必要であれば、ポートが自動的にエッジポートのステータスを有効にできることを示しています。
P2P	P2P ポートとするかどうかを設定します。 • True - 選択されたポートは P2P ポートとして指定されます。P2P（point-to-point）ポートとしてリンクを共有します。P2P ポートはエッジポートと似ていますが、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。RSTP の特長として、エッジポート同様、P2P ポートは迅速に Forwarding 状態に遷移します。 • False - そのポートに P2P ポートの資格がないことを示しています。 • Auto - ポートはいつでも可能な時に (True を指定した時と同様に)P2P ポートとして稼動します。ポートの資格を失う時 (例えば、半二重モードを指定された時など)、p2p ステータスは、p2p の値が False となるような指定と同様に変わります。 初期値は「True」です。初期値「True」は「Auto」と同等です。
Port STP	ポートに STP 機能を有効または無効にします。
Restricted Role	パケットの制限された役割の状態を「True」または「False」に設定します。初期値は「False」です。
Restricted TCN	「True」と「False」を切り替えます。「True」に設定すると、受信した TCN とトポロジ変化を他のポートに伝えることをやめます。初期値は「False」です。
Forward BPDU	STP が無効である場合に、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、STP BPDU パケットが他のネットワークデバイスから送信されます。初期値は有効です。
Hello Time (1-2)	ルートブリッジは、自分がルートブリッジであることを示すために BPDU パケットを 2 回送信します。本値は、1 回目の送信と 2 回目の送信時間の間隔です。1-2（秒）の範囲から指定します。初期値は 2（秒）です。

「Apply」ボタンをクリックし、デバイスに STP ポート設定を適用します。

MST Configuration Identification（MST の設定）

スイッチ上で MST インスタンスの設定を行います。本設定は MSTI（マルチプルスパニングツリーインスタンス）を識別するためのものです。スイッチは初期状態で 1 つの CIST（Common Internal 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 > Spanning Tree > 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。

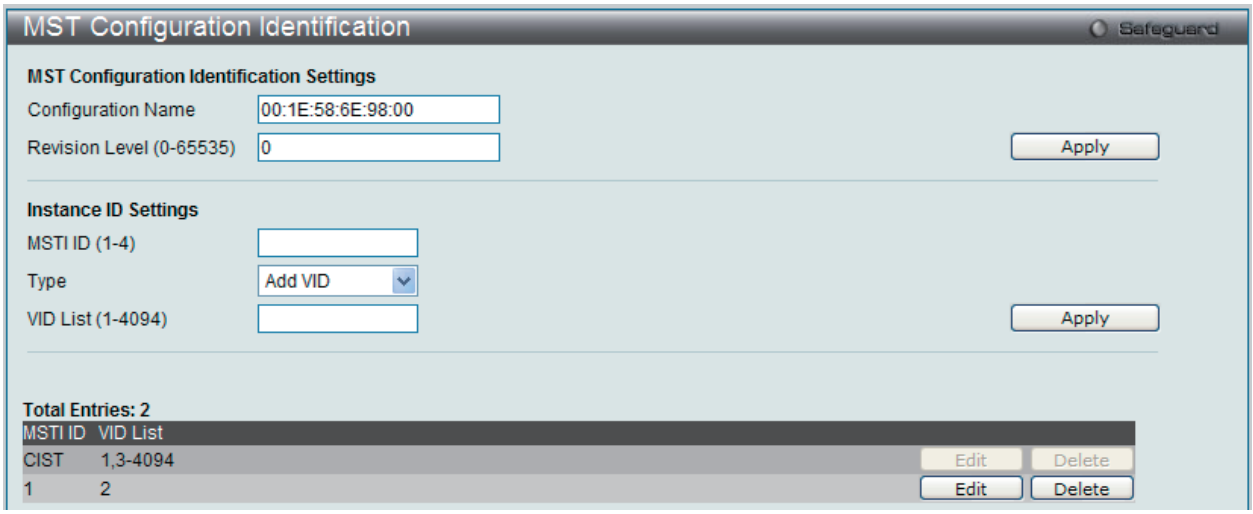


図 7-50　MST Configuration Identification 画面

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。本設定は「STP Bridge Global Settings」画面にて行うことができます。
Revision Level (0-65535)	スイッチ上に設定された MSTP リージョンの値を設定します。Configuration Name に同期しています。0 から 65535 の範囲で設定します。初期値は 0 です。
MSTI ID (1-4)	現在スイッチに設定されている MSTI ID が表示されます。通常、CIST MSTI と表示されます。この値は変更できますが、削除はできません。ID のリンクをクリックすると、その MSTI に関するパラメータを設定する画面が開きます。
Type	MSTI 設定の変更方法を指定します。2 つのタイプから選択します。 • Add VID - MSTI ID に「VID List」で指定する VID を追加します。 • Remove VID - MSTI ID から「VID List」で指定する VID を削除します。
VID List(1-4094)	この MSTI ID に設定する VLAN の VID の範囲を指定します。指定できる VID の範囲は 1 から 4094 までです。

「Apply」ボタンをクリックし、デバイスに MST 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、以下の画面を表示します。

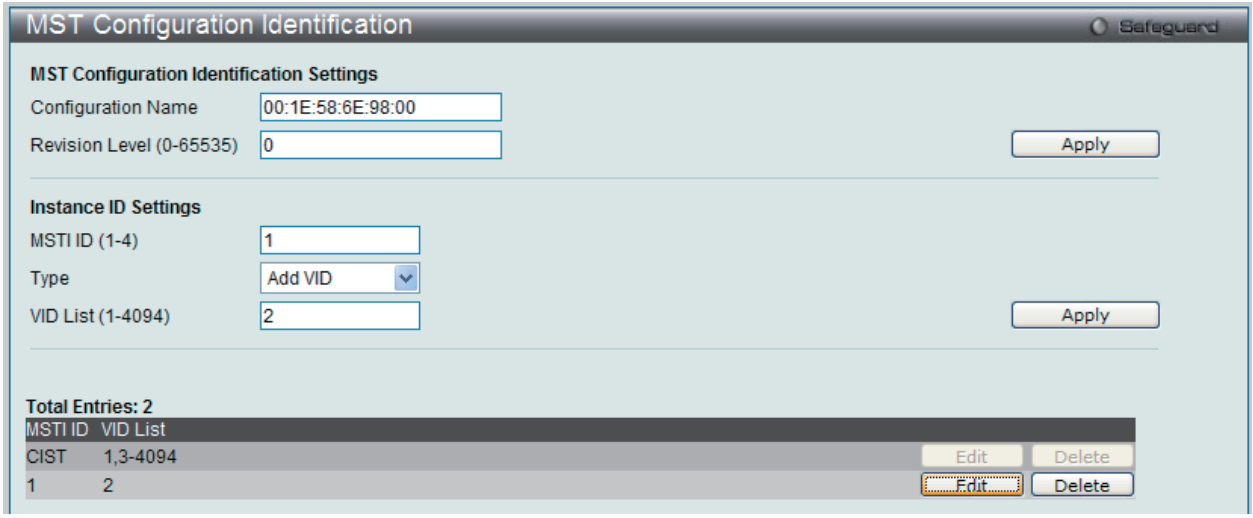


図 7-51　MST Configuration Identification 画面 - Edit

2. 「MST Configuration Identification Settings」セクションに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 Settings（STP インタンス設定）

以下の画面は、スイッチの MSTI に関する現在の設定を表示し、MSTI のプライオリティを変更できます。

MSTI を表示するためには、**L2 Features > Spanning Tree > STP Instance Settings** をクリックし、以下のテーブルを表示します。

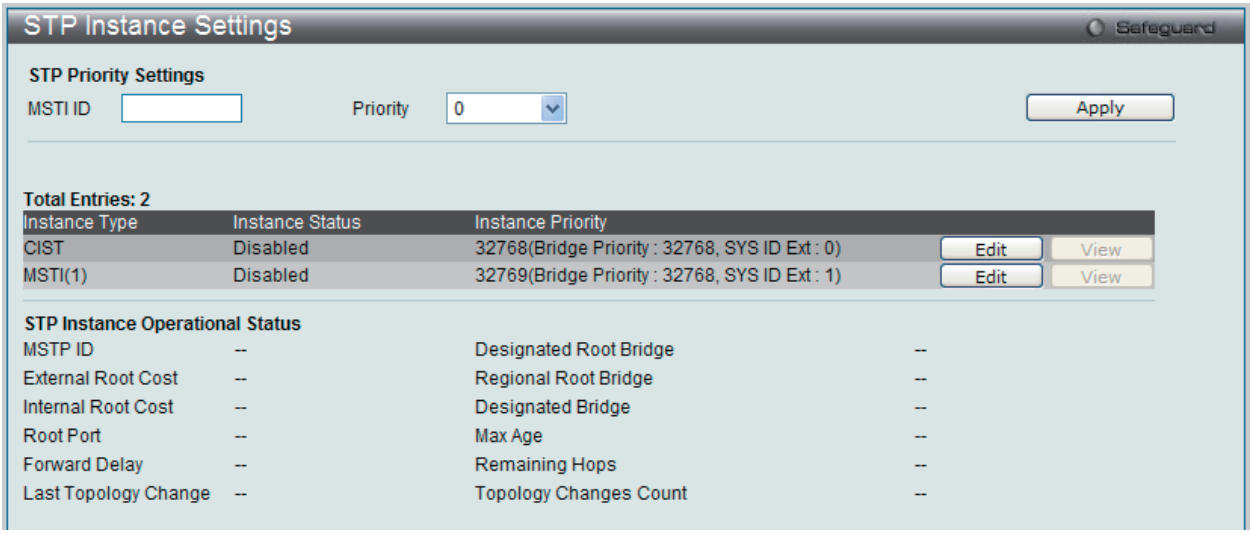


図 7-52　STP Instance Settings 画面

本画面には以下の情報があります。

項目	説明
MSTI ID	デバイスで設定した MSTP ID を設定します。0 は CIST（デフォルト MSTI）を表します。初期値は MSTI です。
Priority	指定したインスタンスのためのプライオリティ（0-61440）を設定します。

「Apply」ボタンをクリックし、新しいプライオリティ設定を適用します。

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、以下の画面を表示します。

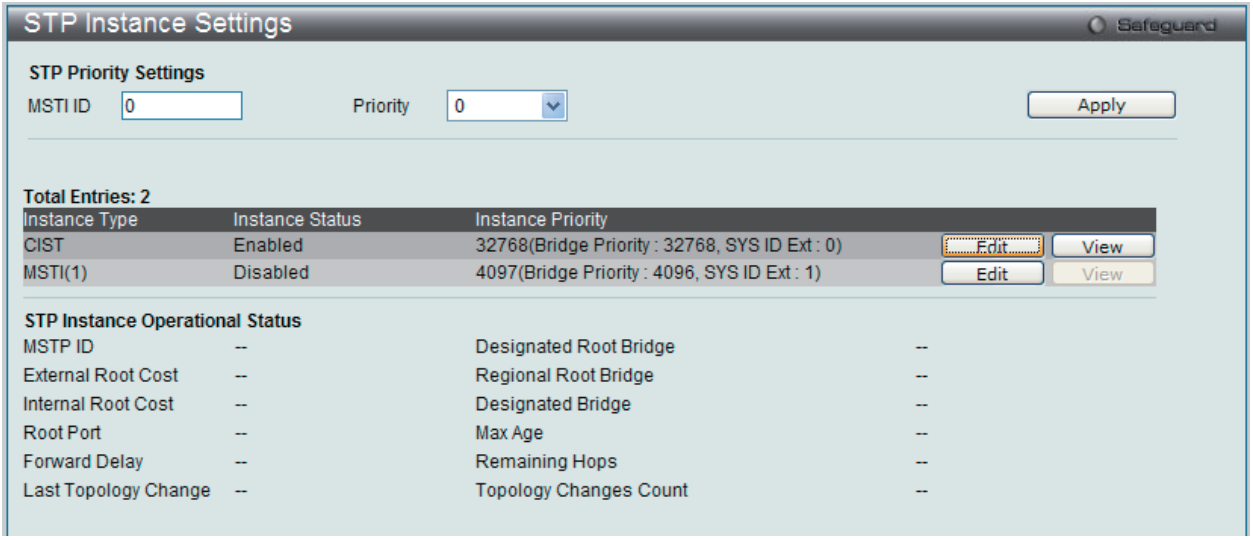


図 7-53　STP Instance Settings 画面 - Edit

2. 「STP Priority Settings」セクションに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、設定を適用します。

エントリの詳細情報の参照

1. 参照するエントリ横の「View」ボタンをクリックし、以下の画面を表示します。

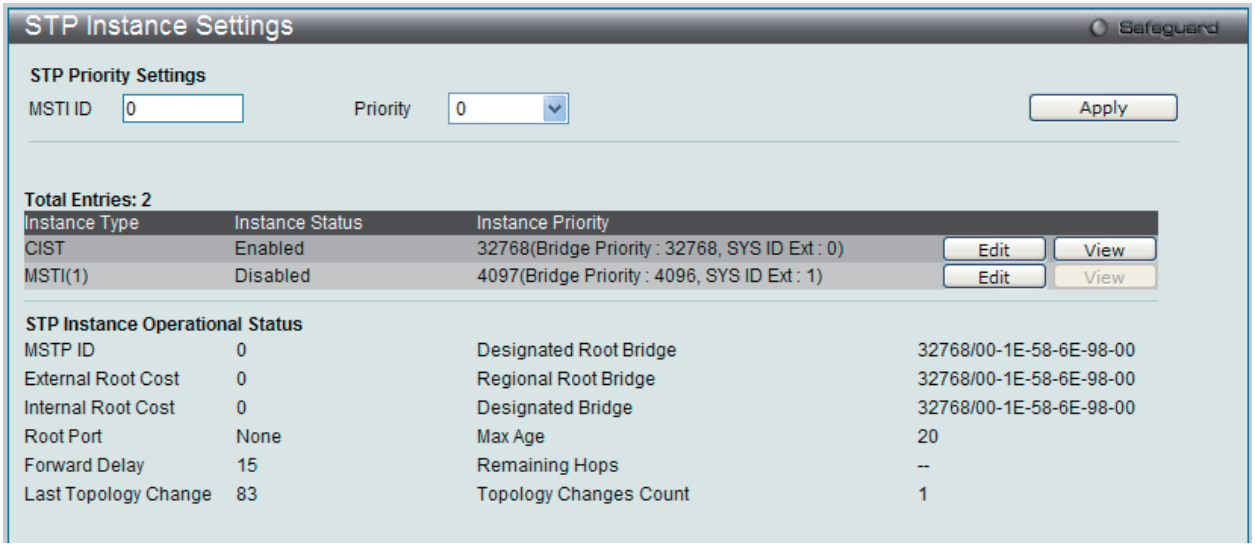


図 7-54　MST Configuration Identification 画面 - View

2. STP インスタンスの状態が表示されます。

MSTP Port Information（MSTP ポート情報）

本画面では現在の MSTP ポート情報が表示され、MSTI ID 単位でポート構成の更新を行うために使用します。ループが発生すると、MSTP 機能はポートプライオリティを使用して、Forwarding 状態に遷移させるインタフェースを選択します。最初に選択したいインタフェースには高いプライオリティ（小さい数値）を与え、最後に選択したいインタフェースには低いプライオリティ（大きい数値）を与えます。インタフェースに同じプライオリティ値が与えられている場合、MSTP は MAC アドレスの値が最小のインタフェースを Forwarding 状態にし、他のインタフェースをブロックします。低いプライオリティ値ほど転送パケットに対して高いプライオリティを意味することにご注意ください。

各ポートに MSTP の設定を行うには、**L2 Features > Spanning Tree > 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。

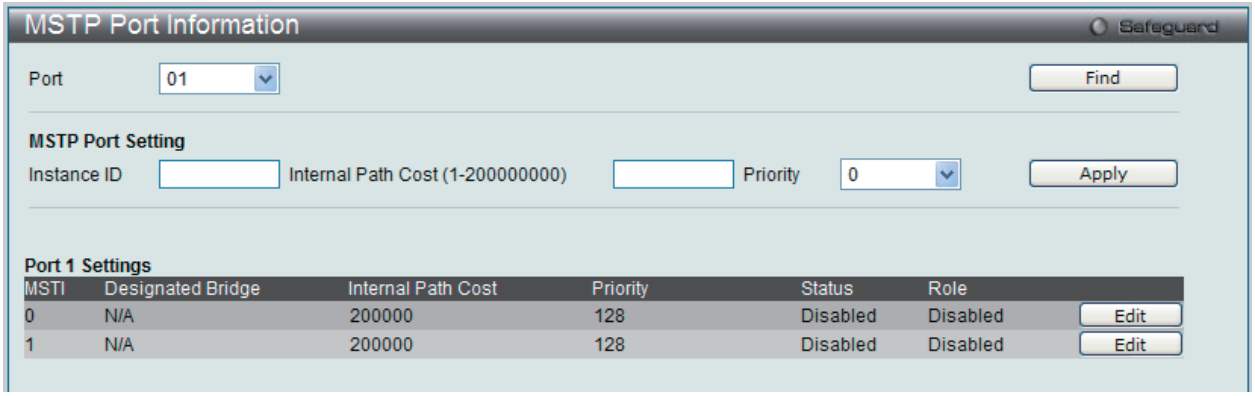


図 7-55　MSTP Port Information 画面

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、以下の画面を表示します。

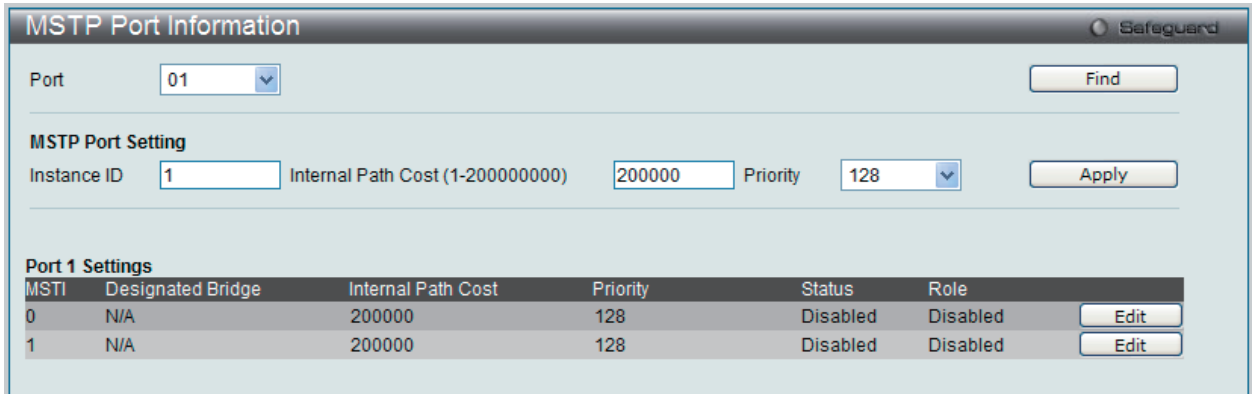


図 7-56　MSTP Port Information 画面

2. 「MSTP Port Settings」セクションに現在の設定が表示されます。「Internal Path Cost」に値を入力し、「Priority」のプルダウンメニューでプライオリティを選択し、「Apply」ボタンをクリックします。

以下の項目を設定または参照できます。

項目	説明
Port	適用するポートを選択します。
Instance ID	設定済みインスタンスの MSTI ID。0 は CIST を意味します（初期値は MSTI）。
Internal Path Cost (1-200000000)	インタフェースが STP インスタンス内で選択された場合にこのポートにパケットを転送するためにかかるコストを指定します。設定内容は以下の 2 種類に分けることができます。 • 0（auto）- 自動的に最も速い経路、最適なインタフェースを設定します。インタフェースに接続されたメディアの速度を元に計算されます。（初期値） • 値 1-200000000 - 最も速く最適な経路を設定します。低いコストを指定するほど速い転送となります。
Priority	ポートインタフェースのプライオリティ（0-240）までの値を指定します。高いプライオリティほど、パケットの転送は優先されます。値が低いほどプライオリティは高くなります。

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。

Forwarding & Filtering（フォワーディングとフィルタリングの設定）

「Forwarding & Filtering」フォルダには「Unicast Forwarding Settings」、「Multicast Forwarding Settings」および「Multicast Filtering Mode Settings」のメニューがあります。

Unicast Forwarding Settings（ユニキャストフォワーディング）

スイッチのユニキャストフォワーディングを設定します。

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

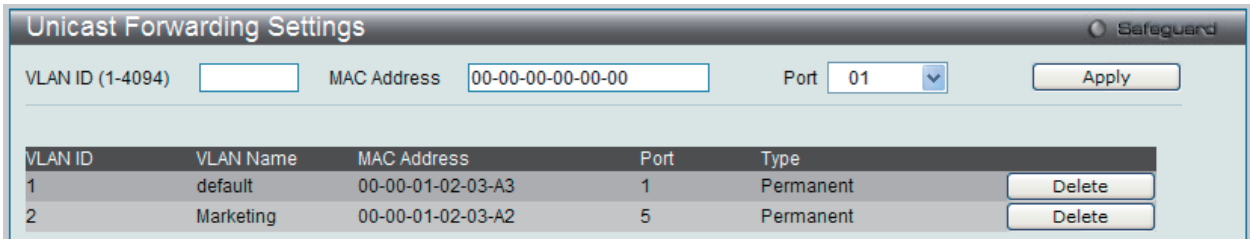


図 7-57　Unicast Forwarding Settings 画面

以下の項目を設定できます。

項目	説明
VLAN ID (1-4094)	ユニキャスト MAC アドレスが存在する VLAN ID。
MAC Address	パケットが静的に送信される宛先の MAC アドレス。ユニキャスト MAC アドレスを指定します。
Port	MAC アドレスが存在するポートの番号を選択します。

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。

エントリの追加

エントリを追加するためには、項目を定義し、「Apply」ボタンをクリックします。

エントリの削除

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

Multicast Forwarding Settings（マルチキャストフォワーディングの設定）

スイッチのマルチキャストフォワーディングを設定します。

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

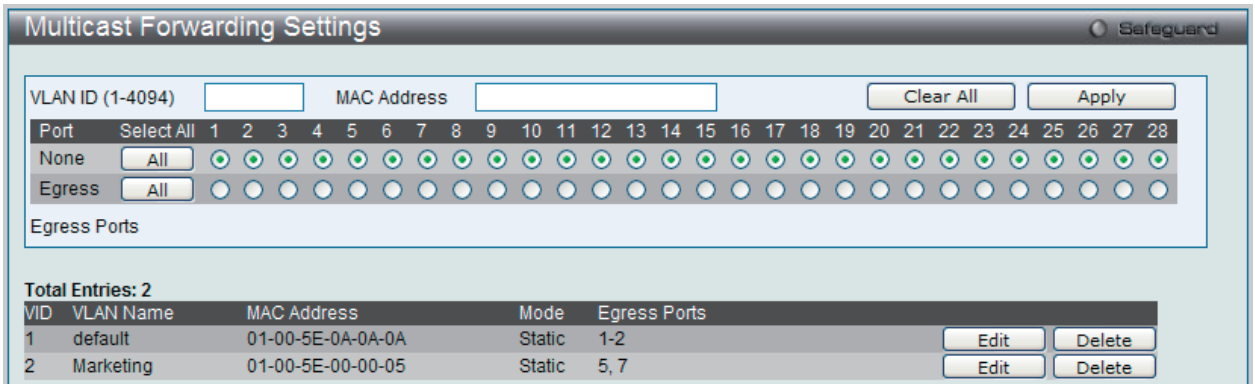


図 7-58　Multicast Forwarding Settings 画面

本画面はスイッチに設定されたスタティックマルチキャスト転送テーブルのすべてのエントリを表示します。

以下の項目を設定できます。

項目	説明
VLAN ID (1-4094)	指定の Multicast MAC アドレスが属する VLAN の VLAN ID。
MAC Address	マルチキャストフォワーディングテーブルに追加される MAC アドレス。
Port	スタティックマルチキャストグループのメンバとなるポートを選択します。「All」ボタンをクリックすると、全ポートが選択されます。 • None - ダイナミックにマルチキャスト参加を行います。指定すると、ポートはスタティックマルチキャストグループのメンバにはなりません。 • Egress - ポートはマルチキャストグループのスタティックメンバとなります。

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。

エントリの削除
テーブルからエントリを削除するためには、削除対象のエントリの列の「Delete」ボタンをクリックします。
「Clear All」ボタンをクリックすると、本画面のすべての設定がクリアされます。

エントリの追加
項目入力後、「Apply」ボタンをクリックします。

エントリの編集
1. エントリ横の「Edit」ボタンをクリックすると、画面上部に現在の設定が表示されます。

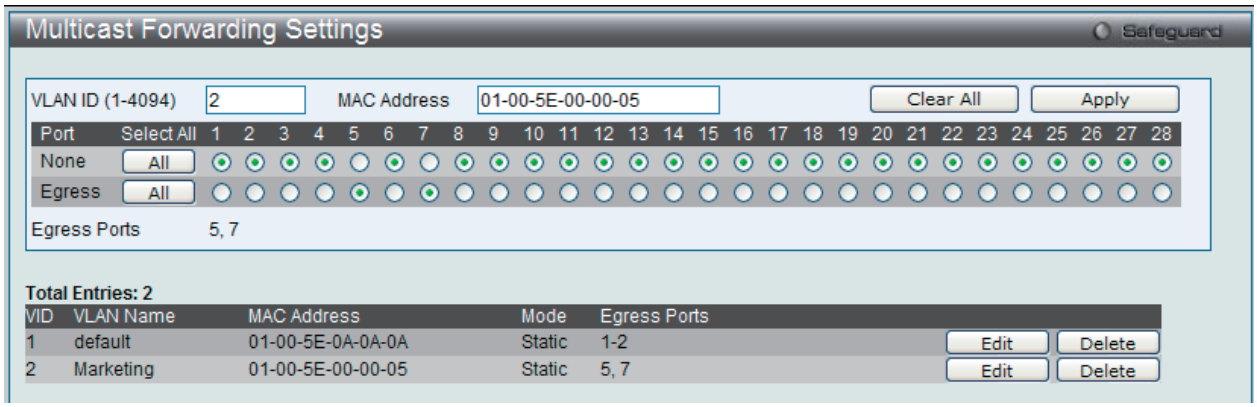


図 7-59　Multicast Forwarding Settings 画面 - Edit

2. 項目設定後、「Apply」ボタンをクリックします。

Multicast Filtering Mode Settings（マルチキャストフィルタリングモード）

スイッチのマルチキャストフィルタリングモードの設定を行います。

L2 Features > Forwarding & Filtering > Multicast Filtering Mode Settings の順にクリックし、以下の画面を表示します。

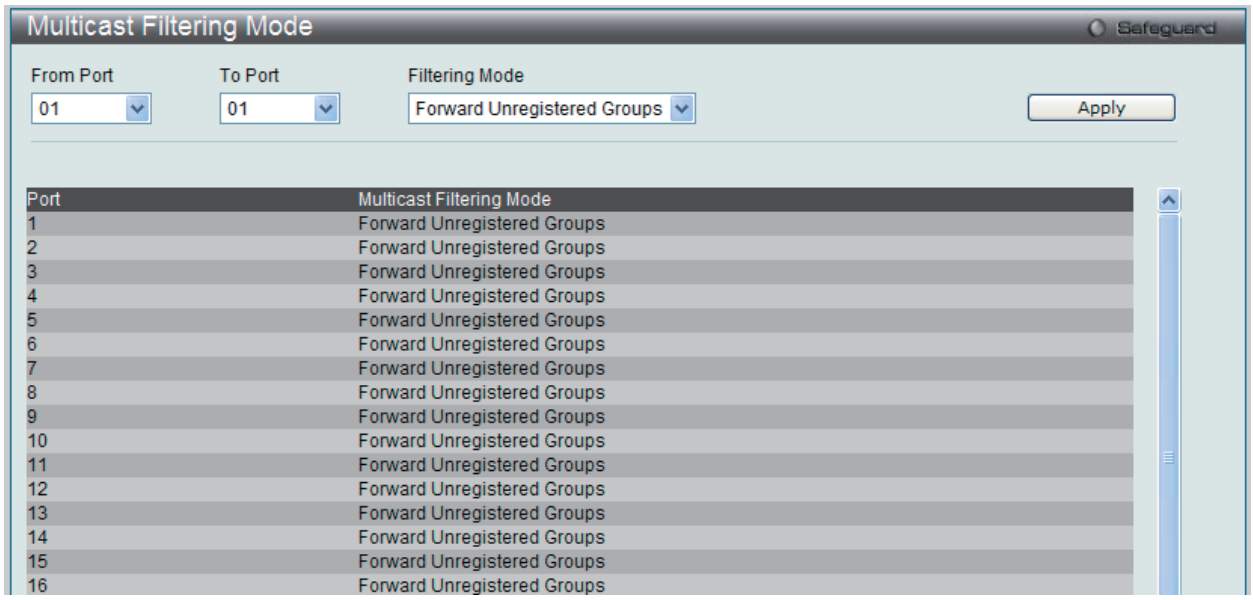


図 7-60　Multicast Filtering Mode 画面

以下の項目を設定できます。

項目	説明
From Port/To Port	フィルタリングを適用するポート範囲を指定します。
Filtering Mode	指定ポートに転送されるマルチキャストパケットを受信した時の動作を指定します。 • Forward Unregistered Groups - 指定ポート範囲に存在する登録されていないマルチキャストグループが受信先のマルチキャストパケットを転送します。 • Filter Unregistered Groups - 指定ポート範囲に存在する登録されていないマルチキャストグループが受信先のマルチキャストパケットを廃棄します。

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。

NLB Settings（ネットワークロードバランシング設定）

ネットワークロードバランシングコマンドは、FTP、VPN、および Web サーバなどの様々なステートレスアプリケーションに適応するように、Network Load Balancing(NLB)（マイクロソフト独自のサーバのクラスタリングとロードバランシングの実装）をサポートするようにスイッチを設定するために使用されます。そのようなアプリケーションのクライアントの要求は、1 つの IP アドレスと送信先 MAC アドレスを共有するクラスタ内の複数サーバに振り分けらます。クラスタ内の全サーバにクライアント要求は転送されますが、実際には 1 つだけがその要求を処理します。

スイッチはユニキャストモードまたはマルチキャストモードで NLB を操作します。ユニキャストは操作モードの初期値です。
このモードをサポートするためには、クライアントとサーバ間のスイッチは、L2 ユニキャストパケットが複数の NLB サーバに送信されることを許可する必要があります。もう 1 つのモードはマルチキャストモードです。マルチキャストモードを使用して、NLB サーバは同様にクラスタ IP と呼ばれるユニキャスト IP アドレスと Flooding MAC と呼ばれるマルチキャスト MAC アドレスを共有します。「Both」モードでは、共有される宛先 MAC アドレスは宛先 MAC アドレスとしてクライアント要求フレームに使用されますが、実際に要求を処理するサーバは、応答フレームには自身の MAC アドレスを使用します。

Windows サーバにおける NLBS の使用と設定に関するより詳しい情報についてはマイクロソフト社のサーバにあるドキュメントを参照してください。

L2 Features > NLB 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。

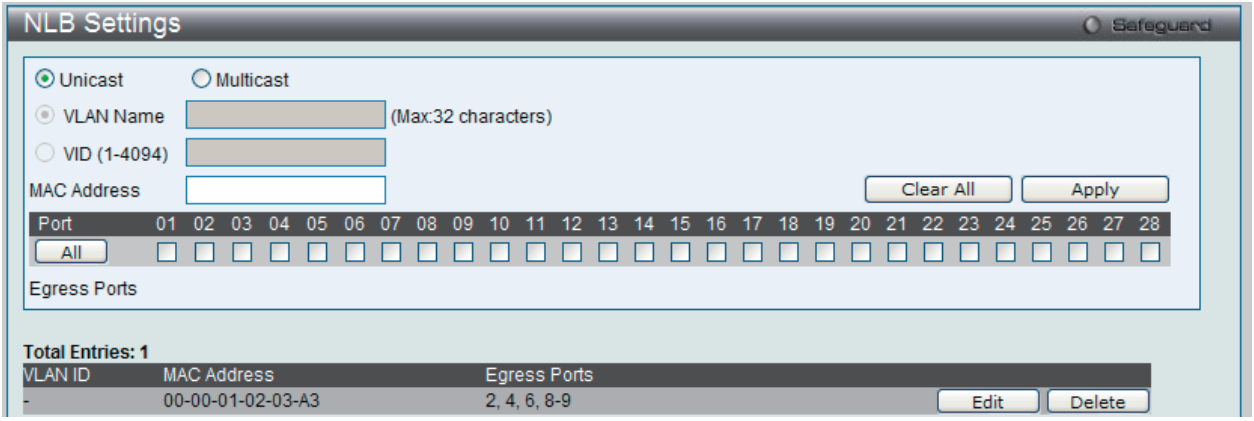


図 7-61　NLB Settings 画面

以下の項目を設定できます。

項目	説明
Unicast/Multicast	NLB が動作するモードのラジオボタンをクリックします。
VLAN Name	作成される NLB マルチキャスト FDB エントリの VLAN 名を入力します。
VID (1-4094)	作成される NLB マルチキャスト FDB エントリの VLAN ID を入力します。
MAC Address	NLB フォワーディングデータベースに入力する MAC アドレスを指定します。
Port	設定した NLB ユニキャスト FDB エントリに使用するフォワーディングポートを選択します。

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。

エントリの追加
項目入力後、「Apply」ボタンをクリックします。

エントリの編集
1. エントリ横の「Edit」ボタンをクリックすると、画面上部に現在の設定が表示されます。

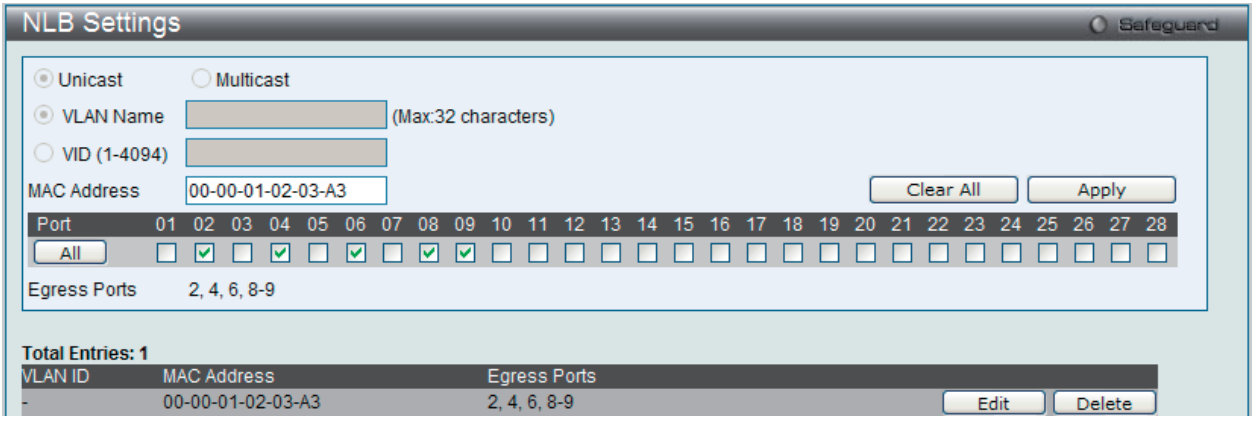


図 7-62　NLB Settings 画面 - Edit

2. 項目設定後、「Apply」ボタンをクリックします。

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。本システムが提供する主な機能は、ステーションまたは本機能の管理を提供するエンティティの管理アドレスと、管理エンティティが要求する IEEE 802 ネットワークへのステーションの接続点の識別子を組み合わせることです。

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）

LLDP 機能をグローバルに有効または無効にします。

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。

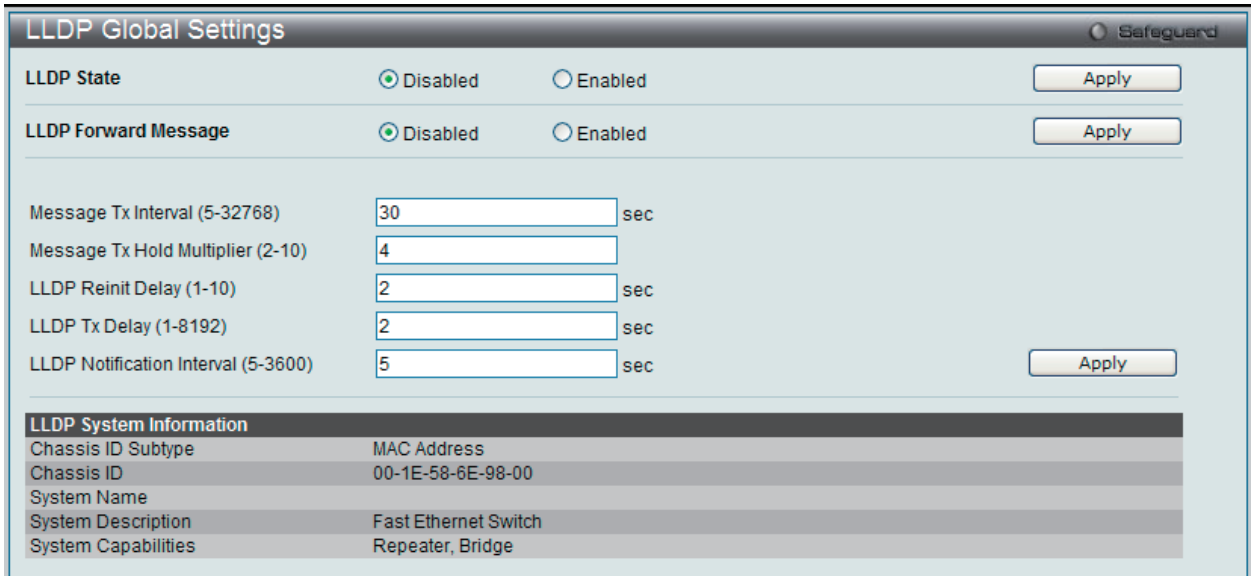


図 7-63　LLDP Global Settings 画面

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 Message	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。 • Enabled - 同一のポート VLAN を持つすべてのポートに LLDP パケットをフラッドして、同じ IEEE 802 LAN に接続している他のコンピュータに通知します。 • Disabled - 本機能が各ポートにおいて LLDP パケットのメッセージ転送を制御します。
Message Tx Interval (5-32768)	アクティブなポートが通知を再送する方法を制御します。パケット伝送間隔を変更するために、5-32768（秒）の範囲で値を入力します。
Message Tx Hold Multiplier (2-10)	LLDP スイッチに使用される乗数を変更することで LLDP Neighbor に LLDP 通知を作成して送信する有効期間（TTL : Time-to-Live）を計算します。指定通知の TTL（time-to-Live）の期限が来ると、通知データは Neighbor スイッチの MIB から削除されます。
LLDP Reinit Delay (1-10)	LLDP ポートが LLDP 無効にするコマンドを受け取った後、再初期化を行う前に待機する時間です。1-10（秒）から値を入力します。
LLDP Tx Delay (1-8192)	LLDP MIB のコンテンツの変更のために、LLDP ポートが連続した LLDP 通知の送信を遅らせる最短時間（遅延間隔）を変更します。LLDP TX Delay を変更するために、1-8192（秒）から値を入力します。
LLDP Notification Interval (5-3600)	LLDP データ変更が LLDP Neighbor からポートに受信した通知の中に検出される場合に定義済みの SNMP トラップレシーバに変更通知を送信する時に使用されます。5-3600（秒）から値を入力します。

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

LLDP Port Settings（LLDP ポート設定）

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。

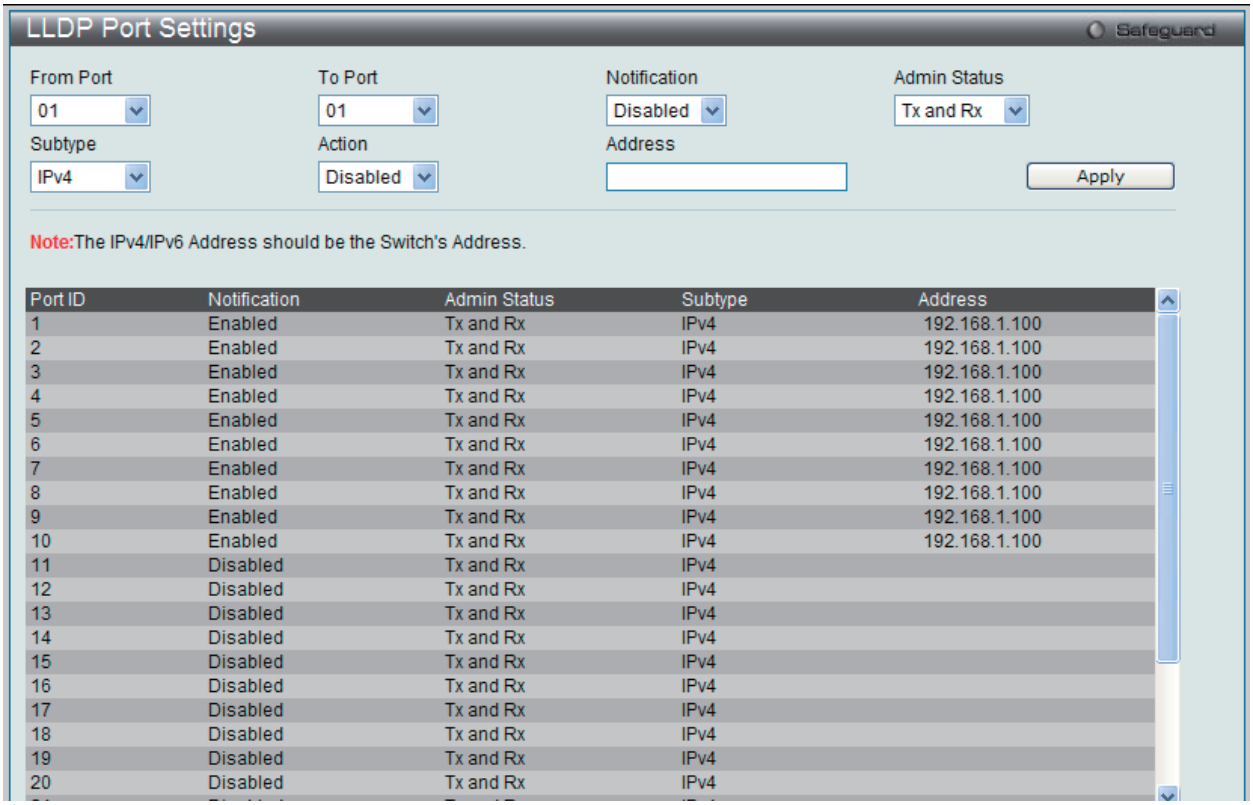


図 7-64　LLDP Port Settings 画面

以下の項目を設定できます。

項目	説明
From Port/To Port	プルダウンメニューを使用して設定するポート範囲を指定します。
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。本機能は SNMP トラップを制御し、無効にするとトラップを実行しません。
Admin Status	本機能はローカル LLDP エージェントを制御し、ポートで LLDP フレームの送受信を行うことができるようになります。通知のステータスを選択します。 • Tx - ローカル LLDP エージェントは LLDP フレームを送信します。 • Rx - ローカル LLDP エージェントは LLDP フレームを受信します。 • Tx and Rx - ローカル LLDP エージェントは LLDP フレームの送受信両方を行います。（初期値） • Disabled - ローカル LLDP エージェントは、LLDP フレームの送受信を行いません。
Subtype	IP アドレスのタイプが IPv4 であることを表示しています。
Action	ポートベースの管理アドレス機能を「Enabled」（有効）または「Disabled」（無効）にします。
Address	通知するエンティティの管理アドレスを入力します。本アドレスは管理 IP アドレスである必要があります。

「Apply」ボタンをクリックし、変更を有効にします。

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

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。

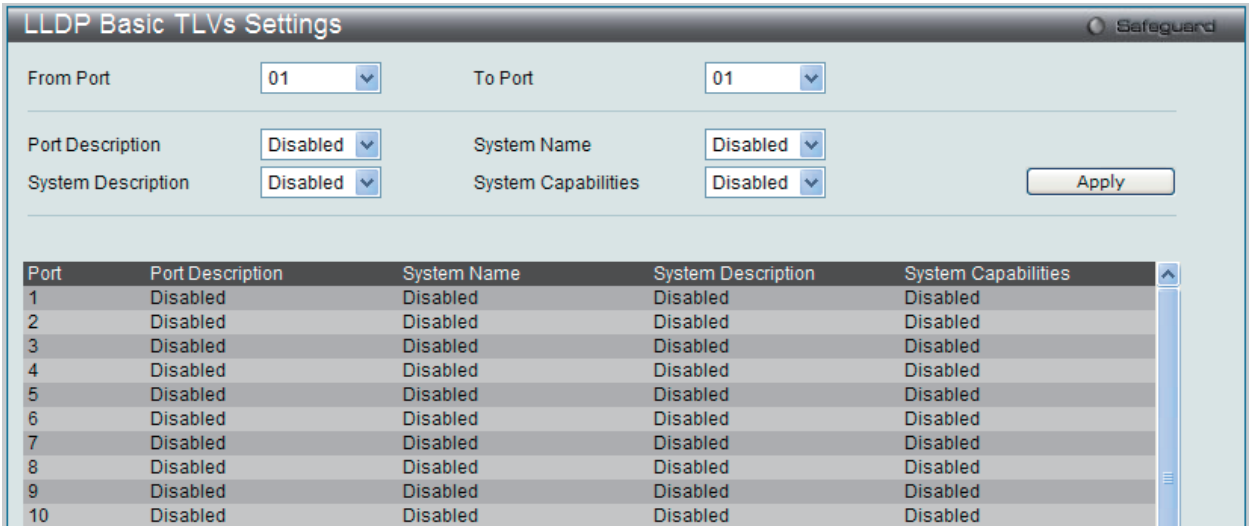


図 7-65　LLDP Basic TLVs Settings 画面

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

以下の項目を設定できます。

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

「Apply」ボタンをクリックし、変更を有効にします。

LLDP Dot1 TLVs Settings（LLDP Dot1 TLV 設定）

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

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

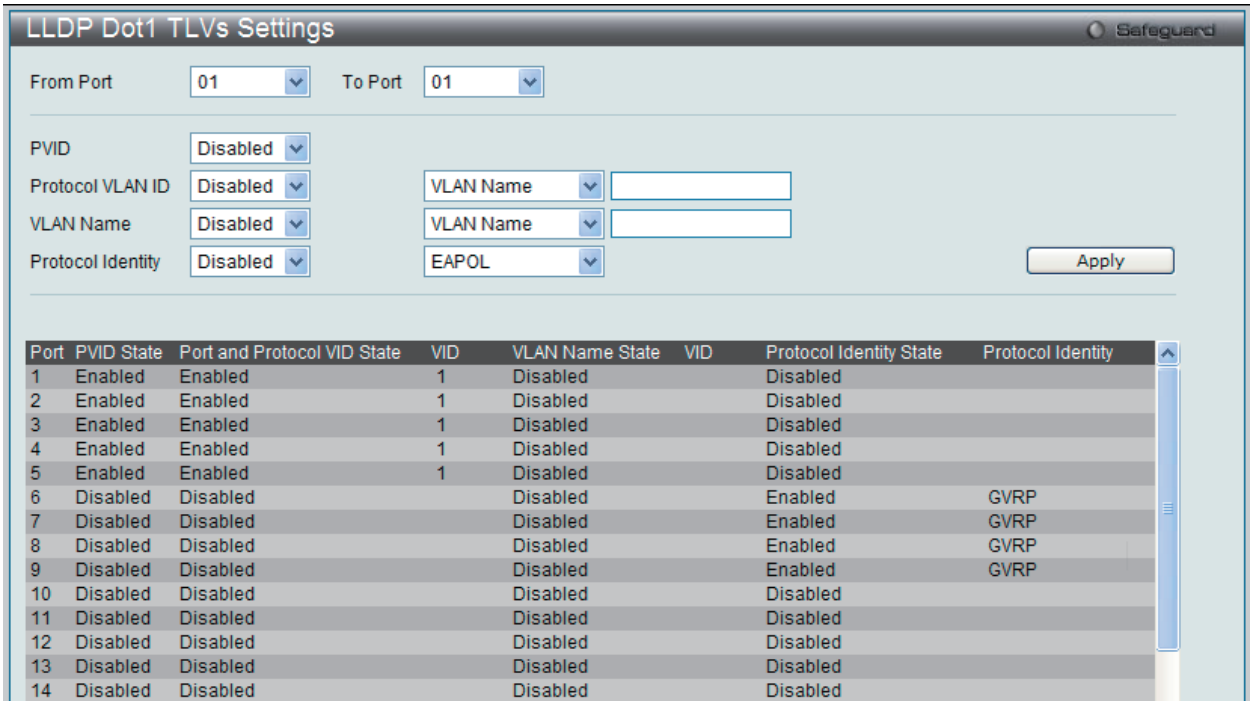


図 7-66　LLDP Dot1 TLVs Settings 画面

以下の項目が使用できます。

項目	説明
From Port/To Port	設定するポート範囲を指定します。
PVID	PVID の通知を「Enabled」（有効）/「Disabled」（無効）にします。
Protocol VLAN ID	プロトコル VLAN ID の通知を「Enabled」（有効）/「Disabled」（無効）にします。対象となるプロトコル VLAN を右の欄で指定します。 • VLAN Name - VLAN 名を指定します。 • VLAN ID - VLAN ID を指定します。 • All - すべてを対象とします。
VLAN Name	VLAN 名の通知を「Enabled」（有効）/「Disabled」（無効）にします。対象となるプロトコル VLAN を右の欄で指定します。 • VLAN Name - VLAN 名を指定します。 • VLAN ID - VLAN ID を指定します。 • All - すべてを対象とします。
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 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 通知から IEEE 802.3 規定のポート VLAN ID TLV データタイプを除外するように設定します。

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

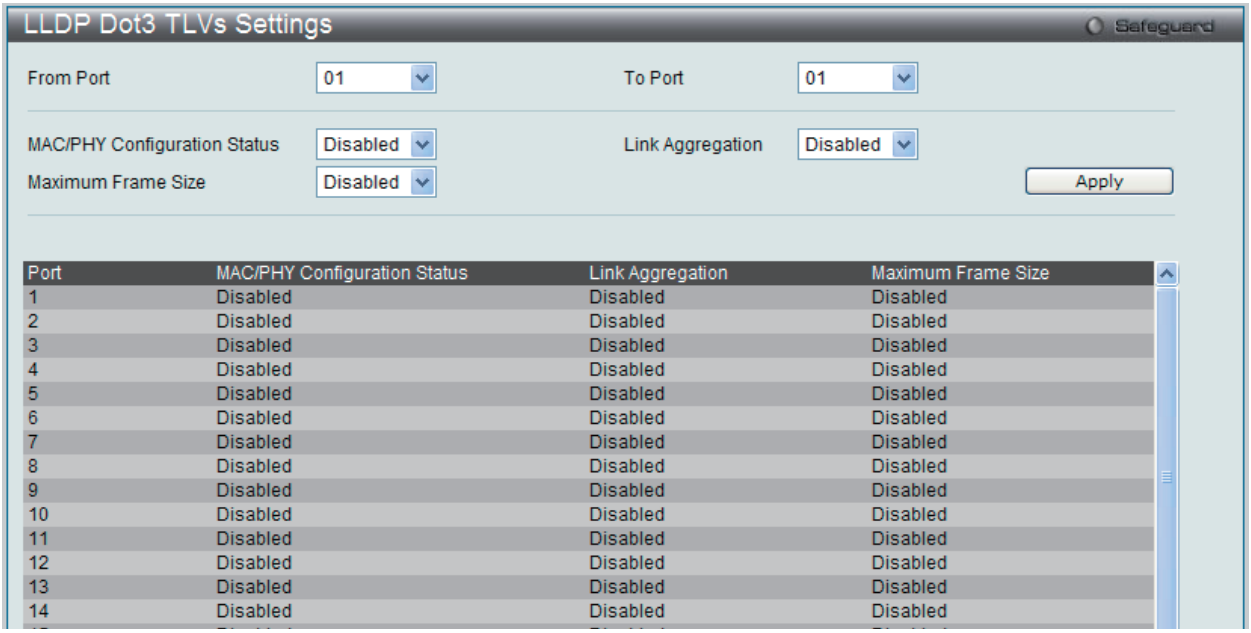


図 7-67　LLDP Dot3 TLVs Settings 画面

以下の項目を設定できます。

項目	説明
From Port/To Port	設定するポート範囲を指定します。
MAC/PHY Configuration Status	スイッチの MAC または PHY 状態の通知を「Enabled」（有効）/「Disabled」（無効）にします。 本 TLV のオプションデータタイプは、LLDP エージェントが「MAC/PHY configuration/status TLV」を送信する必要があることを示します。このタイプは、IEEE 802.3 リンクの 2 つの終端が異なる速度設定で、何らかの限定的な接続性を確立することが可能であることを示しています。情報には、ポートがオートネゴシエーション機能をサポートしているかどうか、機能が有効であるかどうか、自動通知機能、および操作可能な MAU タイプを含まれます。初期値は無効です。
Link Aggregation	スイッチのリンクアグリゲーション状態の通知を「Enabled」（有効）/「Disabled」（無効）にします。 これは、LLDP エージェントが「Link Aggregation TLV」を送信する必要があることを示します。このタイプは IEEE 802.3 MAC における現在のリンクアグリゲーションステータスを示します。情報には、ポートがリンクアグリゲーションができるかどうか、ポートが集約した 1 つのリンクにまとめられるかどうか、および束ねられたポートの ID が含まれる必要があります。初期値は無効です。
Maximum Frame Size	最大フレームサイズの通知を「Enabled」（有効）/「Disabled」（無効）にします。LLDP エージェントが「Maximum-frame-size TLV」を送信する必要があることを示します。初期値は無効です。

「Apply」ボタンをクリックし、変更を有効にします。

Ethernet OAM（イーサネット OAM）

イーサネットの OAM（Operations : 操作、Administration : 管理、および Maintenance : メンテナンス）は、ポイントツーポイントおよびエミュレートされたポイントツーポイントのイーサネットリンクにおけるネットワーク状態のモニタリング、障害が発生したリンクの位置や障害状況を素早く判断する能力をネットワーク管理者に提供するデータリンクレイヤプロトコルです。

Ethernet OAM Port Settings（イーサネット OAM ポート設定）

ポートにイーサネット OAM を設定します。

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

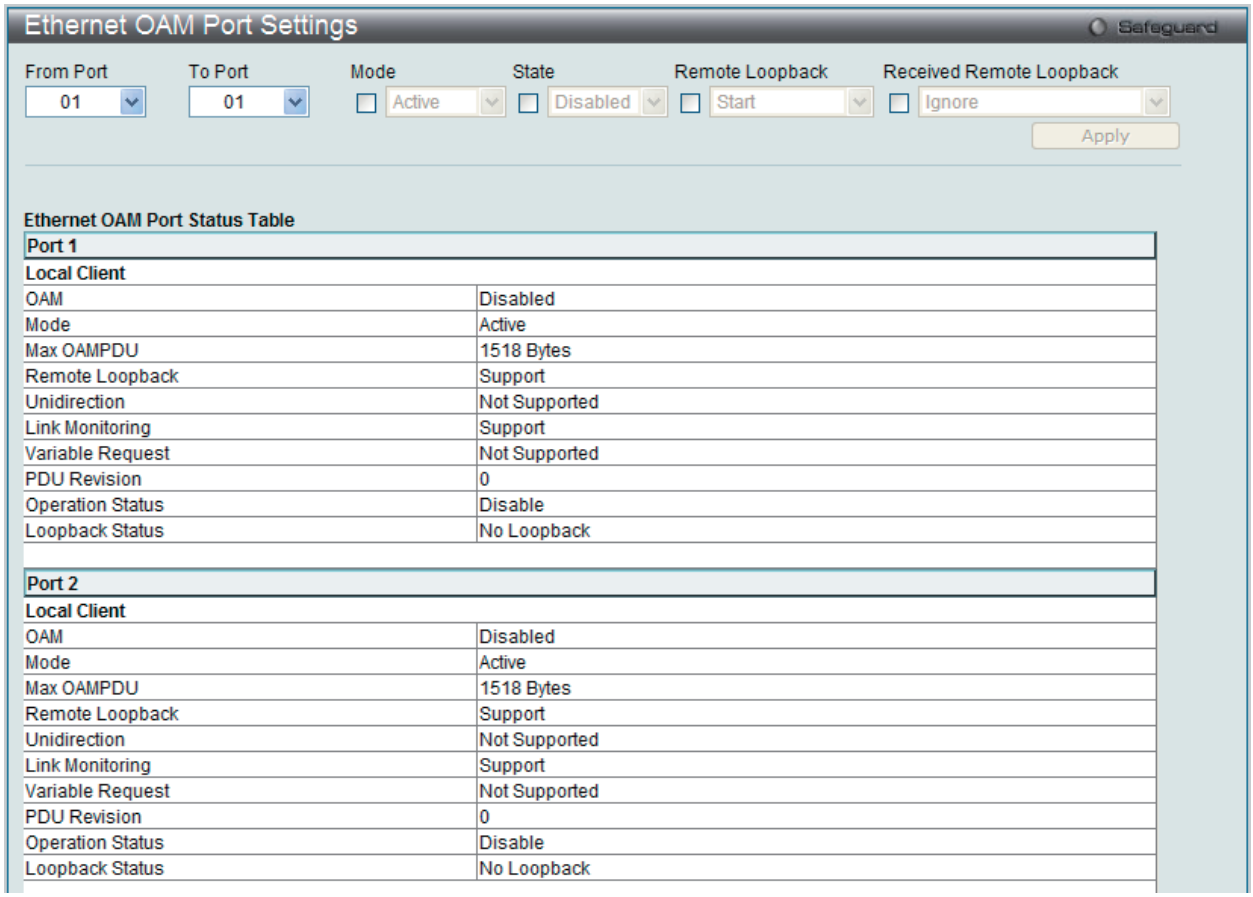


図 7-68　Ethernet OAM Port Settings 画面

以下の項目を設定できます。

項目	説明
From Port / To Port	設定するポート範囲を指定します。
Mode	動作するモード（「Active」または「Passive」）を指定します。初期モードは「Active」です。
State	OAM 機能を有効または無効にします。初期値は無効です。
Remote Loopback	「Start」を指定すると、リモートループバックモードに変更するようにピアに要求します。「Stop」を指定すると、通常の操作モードに変更するようにピアに要求します。
Received Remote Loopback	受信したイーサネット OAM リモートループバックコマンドの処理を指定します。 • Process - 処理します。 • Ignore - 無視します。（初期値）

「Apply」ボタンをクリックし、変更を有効にします。

Ethernet OAM Event Configuration（イーサネット OAM イベント設定）

ポートにイーサネット OAM のイベントを設定します。

L2 Features > Ethernet OAM > Ethernet OAM Event 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。

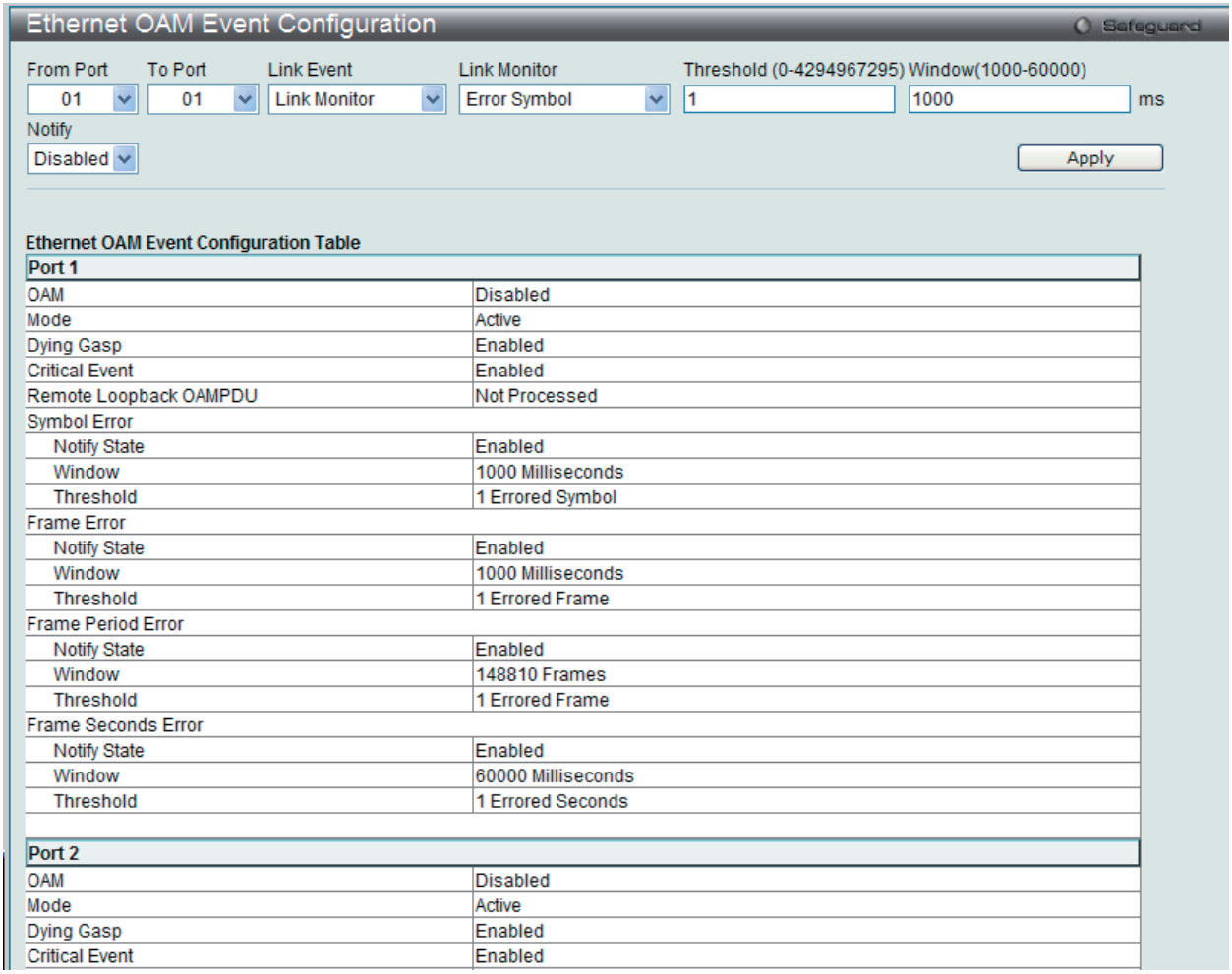


図 7-69　Ethernet OAM Event Configuration 画面

以下の項目を設定できます。

項目	説明
From Port / To Port	設定するポート範囲を指定します。
Link Event	リンクイベントのタイプ（「Link Monitor」または「Critical Link Event」）を選択します。
Link Monitor	ポートにイーサネット OAM リンクモニタ（Error Symbol、Error Frame、Error Frame Period、および Error Frame Seconds）を設定します。リンクモニタリング機能は、さまざまな条件の元でリンク障害を検出して示すメカニズムを提供します。OAM はコード化されたシンボルのエラー数と同様にフレームエラー数により統計情報をモニタリングします。エラーシンボルまたはエラーフレーム数が、Window オプションによって指定した期間内に定義したしきい値以上になると、イベント通知状態 (Notify) は有効となり、リモート OAM ピアに通知するイベントを生成します。 「Link Monitor」メニューを使用して、リンクモニタのタイプを定義し、しきい値、画面、および通知ステータスを設定します。
Critical Link Event	• Critical Event - 不特定のクリティカルなイベントを参照します。 • Dying Gasp - リモートデバイスの電源障害など回復不可能なイベントの発生の検出を指定します。
Threshold (0-4294967295)	指定期間内のエラーシンボル、エラーフレーム、エラーフレーム周期、またはエラーフレーム秒数を指定します。イベント生成のためには、指定した以上の値が要求されます。しきい値は 0 - 4294967295 の範囲です。初期値は 1 です。
Window (1000-6000)	エラーシンボルとエラーフレームの有効範囲は、1000 - 60000 ms（ミリ秒）で、初期値は 1000 ms です。エラーフレーム周期の有効範囲は、14881 - 89286000 で、初期値はファーストイーサネットポートに対して 148810 です。エラーフレーム秒数の有効範囲は、10000 - 900000 で、初期値は 60000 です。
Notify	イベント通知を有効または無効にします。初期値は有効です。

「Apply」ボタンをクリックし、設定を有効にします。

CFM（Connectivity Fault Management : 接続性障害管理）

CFM またはイーサネット CFM は、エンドツーエンドのイーサネットレイヤ OAM プロトコルです。CFM は IEEE 802.1ag によって定義されており、大きなイーサネットの MAN（メトロポリタンエリアネットワーク）と WAN において接続性のモニタリング、Fault Notification（障害通知）、および障害を隔離する手段を含んでいます。

イーサネットは隔離されている企業内 LAN を従来通りに動作させます。イーサネットが複数の管理ドメインを包含するよりスケールの大きいキャリアネットワークで動作するように拡張されているため、さらに大きく複雑なネットワークの需要は新しい OAM 機能が要求されます。これらのよりスケールの大きいネットワークは、多大なユーザベースを持ち、様々なネットワークアプリケーションを搭載し、通常、リンクの動作時間が重要である従来の企業イーサネット LAN よりはるかに広域に及ぶことから、イーサネットで動作可能な接続性障害に対処する手段が必要となりました。既存の OAM プロトコルのいずれも適切にこの新しい状況を扱うことができなかったため、イーサネット CFM は MAN と WAN にイーサネット技術を適用することで起こる新しい操作管理の必要に応じるように発展しました。

イーサネット CFM は、身近なイーサネットプラットホームの上位ですべてが操作される場合にイーサネットネットワークサービスプロバイダにエンドツーエンドのサービスレベルの OAM と低い運用コストなどの様々な利益を提供します。

CFM はいくつかの新しい期間と概念をイーサネットに導入しており、これらを以下で簡単に説明します。

Maintenance Domain（メンテナンスドメイン）
メンテナンスドメインは、ネットワークを管理する目的のために作成される管理エリアについて言及する一般的な用語です。メンテナンスドメインは、単一のエンティティまたはオーナーによって操作されます。また、境界内部に 1 セットのポートを持つ境界によって定義されます。

イーサネット CFM メンテナンスドメイン（本マニュアルでは MD として呼ぶ）は、他の MD と階層関係を構成します。通常、MAN または WAN は、カスタマ、サービスプロバイダ、およびオペレータの構造的な関係を反映するドメインのサイズに基づいた階層に分割することができます。オペレータがサブネットワークを経由したサービスの送信を提供している間、サービスプロバイダには、エンドツーエンドのサービスの責任があります。階層は 0-7 の範囲のメンテナンスレベル値で定義されます。7 が最も高いレベルで、0 が最も低いレベルとなります。MD が大きいほど、メンテナンスレベルは高くなります。例えば、カスタマのドメインが最も大きい MD である場合、メンテナンスレベル 7 が割り当てられる必要があり、オペレータ MD が最もレベルが低い場合、メンテナンスレベル 0 が割り当てられ、サービスプロバイダドメインはこれらの値の間となります。メンテナンスレベルは、ネットワーク管理者によって手動で割り当てられます。MD 階層のすべてのレベルが共に動作する必要があります。

MD のネストは許可されていますが、MD の管理が単一のオーナーによって実施されるという要求に違反するために、それらは交わることはできません。2 つ以上のドメインをネストさせる場合、外側のドメインにネストするドメインより高いメンテナンスレベルを割り当てる必要があります。

CFM の操作とメッセージ交換は、ドメインごとに行われます。これは、例えば、レベル 3 で動作する CFM が、より高いレベルによるレベル 3 のネットワーク検出を許可しないことを意味します。

Maintenance Association（メンテナンスアソシエーション）
CFM のメンテナンスアソシエーション (MA) は、同じ管理ドメインレベルとメンテナンスアソシエーション（MAID）で構成された MEP のセットです。

MD 内の異なる MA は、異なる MA 名を持つ必要があります。異なる MD の異なる MA は、同じ MA 名を持つことができます。MA に指定される MEP リストは、異なるデバイスに位置することができます。MEP は、これらのデバイスのポートに明示的に作成される必要があります。MEP は MA を経由して定期的に CCM パケットを送信します。受信する MEP は、構成の保全性チェックのために、本 MEP リストに対して他の MEP から受信した CCM パケットを検証します。

Maintenance Point（メンテナンスポイント）
CFM のメンテナンスポイントは、メンテナンスドメイン内のポートにおける境界のポイントです。メンテナンスポイントは、正しいメンテナンスレベルに所属しないフレームを破棄することで MD の境界内の CFM フレームをフィルタします。メンテナンスポイントには 2 つのタイプ、Maintenance Endpoint : MEP（メンテナンスエンドポイント）、および Maintenance Intermediate Point : MIP（メンテナンス中間ポイント）があります。MEP と MIP はネットワーク管理者によって手動で設定されます。

MEP は、メンテナンスドメインの端に存在し、MD の境界を定義しています。MEP 機能は、MD に制限されるようにフィルタする CFM メッセージを含みます。MEP は Connectivity Check Messages (CCM : 接続性チェックメッセージ) を転送するために設定され、設定されると、Traceroute およびループバックメッセージを送信します。MEP は、内向きまたは外向きが可能です。

内向き MEP は、MEP が設定されているブリッジポートを経由しないでブリッジリレー機能に CFM フレームを送信します。内向きの MEP は、内側から受信する同じかそれ以下のレベルにあるすべての CFM フレームを破棄します。そして、フレームの送信元が内向きまたは外向きにかかわらず、より高いレベルにあるすべての CFM フレームを転送します。内向き MEP が設定されているポートがスパニングツリープロトコルによりブロックされると、MEP はもう CFM メッセージの送信も受信もできません。

外向き MEP は、ブリッジポートにフレームを送信し、送信されるポートにだけ設定されます。外向きのポートは、ブリッジリレー機能側から受信する同じかそれ以下のレベルにあるすべての CFM フレームを破棄します。それは、そのレベルにあるすべての CFM フレームを処理して、ブリッジポートからから受信する低いレベルの CFM フレームすべてを破棄します。外向きポートは、フレームの送信先の方向にかかわらず、より高いレベルにあるすべての CFM フレームを転送します。外向き MEP が設定されているポートがスパニングツリープロトコルによりブロックされても、MEP はブリッジポートを経由して CFM メッセージの送信と受信が可能です。

MIP は、境界ではなく、MD 内部にあるメンテナンスポイントです。MIP は他の MIP および MEP から CFM フレームを受信します。これらのフレームは、ブリッジリレー機能とブリッジポートを使用することで分類されて送信されます。MIP より低レベルにあるすべての CFM フレームがブロックされ、送信元にかかわらず破棄されます。より高いレベルにあるすべての CFM フレームは、送信元にかかわらず転送されます。MIP が設定されているポートがスパニングツリープロトコルによりブロックされると、MIP はブリッジリレー機能側への CFM メッセージの受信、またはリレーはできません。しかし、MIP は、ブリッジポートから CFM メッセージの受信、または応答は可能です。

CFM メッセージには Continuity Check Message (CCM : 連続性チェックメッセージ)、Loopback Message（LBM : ループバックメッセージ）、および Link Trace Message（LTM : リンクトレースメッセージ）が含まれます。CFM はブリッジにより送信、停止、処理、およびリレーされる標準のイーサネットフレームを使用します。ルータは、限定的な CFM 機能をサポートしています。

Continuity Check Message (CCM : 連続性チェックメッセージ)
MEP 内で交換されるマルチキャストメッセージです。CCM は、ドメイン内の他の MEP に対して MIP の検出を許可し、また、MIP が MEP を検出することを許可します。CCM はメンテナンスドメインに対して制限されます。CCM は、同じメンテナンスレベルにある MIP によって分類され、同じメンテナンスレベルにあるリモート MEP によって停止されます。それらは、単方向 (無応答ソリシテーション) であり、MEP が設定されているポートの状態を伝送します。LBM は宛先に到達可能かどうかだけを示し、各ホップの発見を許可しないという点において Ping または ICMP メッセージに似ています。

Link Trace Messages (LTM : リンクトレースメッセージ)
同じメンテナンスレベルにあるリモート MEP および MIP と近接関係を示すために MEP が送信するマルチキャスト CFM フレームです。LTM のメッセージ本体は、リンクトレースを終了するターゲット MEP の宛先 MAC アドレスを含んでいます。MIP または MEP が LTM を受信すると、始動している MEP に対してユニキャスト Link Trace Reply(LTR : リンクトレースリプライ) を生成します。また、それはターゲット MEP の宛先 MAC アドレスに LTM を送信します。LTM はターゲット MEP または MIP までのパスを効果的にトレースします。

Loopback Messages (LBM : ループバックメッセージ)
宛先に到達可能かどうかだけを示し、各ホップの発見を許可しないという点において Ping または ICMP メッセージに似ています。

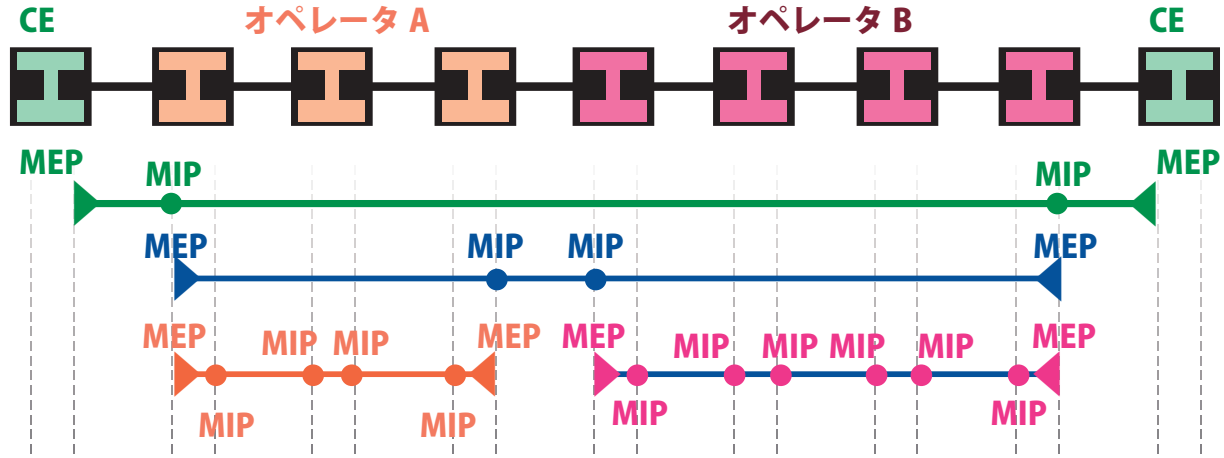


図 7-70　OAM ドメイン構造

- Maintenance Association (MA) - 管理者がネットワークをモニタリングしている部分の境界
- Maintenance Domain (MD) - 階層内のモニタリングのレベル
- Maintenance End Points (MEP) - MA または MD のエンドポイント
- Maintenance Intermediate Points (MIP) - MA または MD 内の中間点

注意　CE = Customer Equipment

CFM Settings（CFM 設定）

CFM 機能を設定します。

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

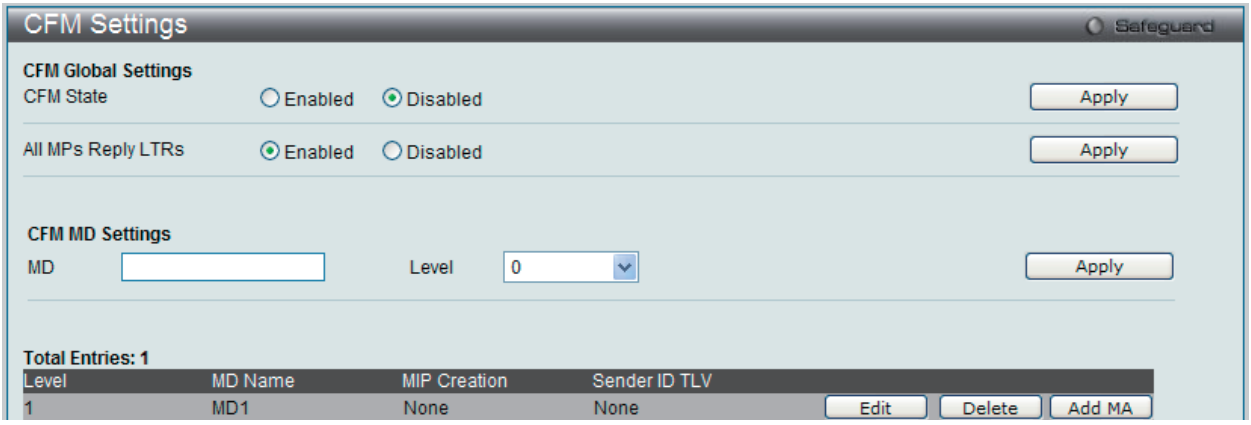


図 7-71　CFM Settings 画面

以下の項目を設定できます。

項目	説明
CFM State	CFM 機能を有効または無効にします。
All MPs Reply LTRs	Link Trace Reply(LTR) メッセージに応答するために、すべてのメンテナンスポイント (MEP と MIP) を有効、または無効にします。これらは、リンクトレースメッセージと共に使用され、MEP から別の MEP または MIP までの経路をトレースします。
CFM MD Settings	
MD	メンテナンスドメインの名称を入力します。メンテナンスドメイン名は、22 文字以内で指定します。
Level	メンテナンスドメインのレベルを選択します。レベルは、0-7 の範囲で設定します。0 が最も低く、7 が最も高いレベルです。
MIP Creation	MIP の作成を制御します。 • None - MIP を作成しません。（初期値） • Auto - ポートがこの MD の MEP で設定されないと、MIP は常にこの MD のどのポートにも作成されます。MA の中間スイッチでは、この設定は、MIP がこのデバイスで作成されるために「Auto」である必要があります。 • Explicit - 次に低レベルのものがポートに MEP を設定している場合にだけ、この MD のどのポートにも MIP を作成することができます。そのポートはこの MD の MEP では設定されません。
Sender ID TLV	SenderID TLV の転送を制御します。 • None - SenderID TLV を転送しません。（初期値） • Chassis - シャーシ ID 情報を持つ SenderID TLV を転送します。 • Manage - 管理アドレス情報を持つ SenderID TLV を転送します。 • Chassis Manage - シャーシ ID 情報と管理アドレス情報を持つ SenderID TLV を転送します。

エントリの追加

項目入力後、「Apply」ボタンをクリックします。

エントリの編集

1. エントリ横の「Edit」ボタンをクリックします。

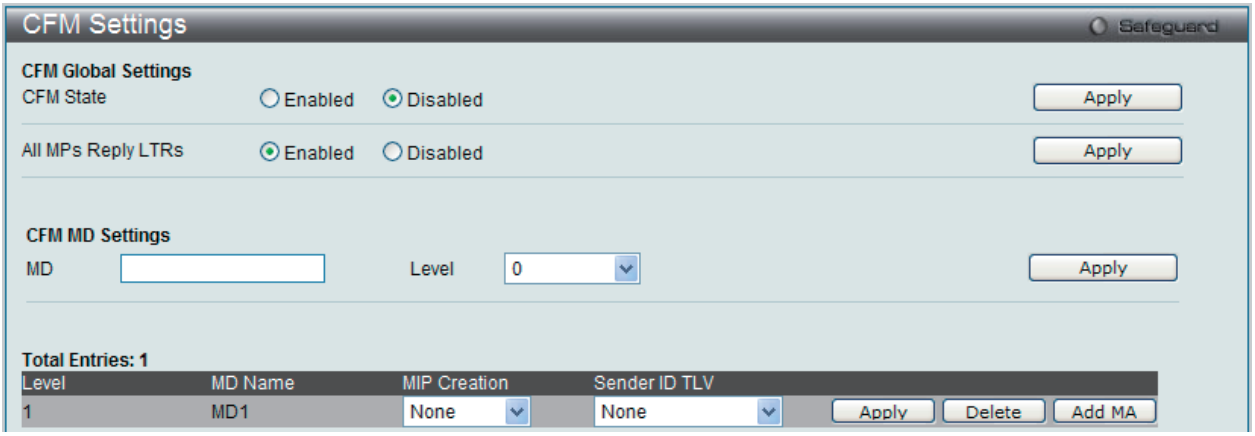


図 7-72　CFM Settings 画面 - Edit

2. 項目設定後、「Apply」ボタンをクリックします。

CFM メンテナンスアソシエーション（MA）設定

メンテナンスアソシエーションを設定します。

L2 Features > CFM > CFM Settings 画面で「Add MA」ボタンをクリックし、以下の画面を表示します。

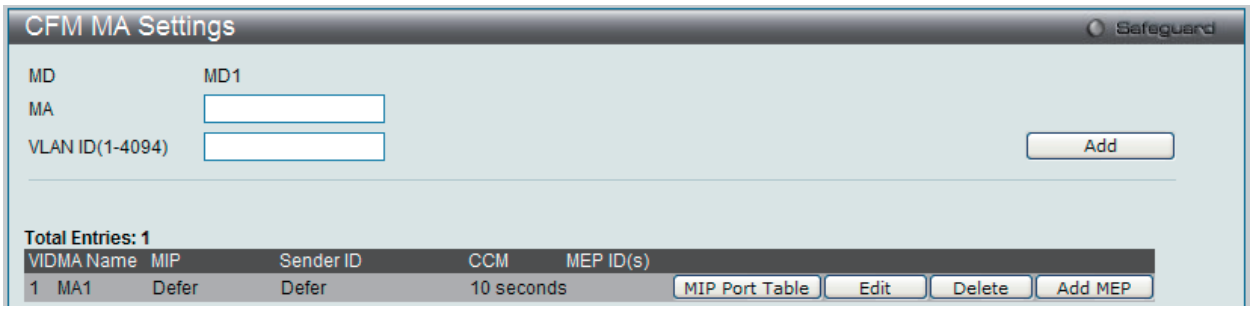


図 7-73　CFM MA Settings 画面

以下の項目が使用できます。

項目	説明
MA	メンテナンスアソシエーションの名称を入力します。
VLAN ID (1-4094)	VLAN 識別子。異なる MA は異なる VLAN に関連付ける必要があります。
エントリテーブル	
MIP	MIP の作成を制御します。 • None - MIP を作成しません。 • Auto - ポートがこの MA の MEP で設定されないと、MIP は常にこの MA のどのポートにも作成されます。 • Explicit - 次に低レベルのものがポートに MEP を設定している場合にだけ、この MA のどのポートにも MIP を作成することができます。そのポートはこの MA の MEP では設定されません。 • Defer - この MA が関連するメンテナンスドメインの設定を継承します。（初期値）
SenderID	これは、SenderID TLV の転送を制御します。 • None - SenderID TLV を転送しません。 • Chassis - シャーシ ID 情報を持つ SenderID TLV を転送します。 • Manage - 管理アドレス情報を持つ SenderID TLV を転送します。 • Chassis Manage - シャーシ ID 情報と管理アドレス情報を持つ SenderID TLV を転送します。 • Defer - この MA が関連するメンテナンスドメインの設定を継承します。（初期値）
CCM	これは CCM 送信間隔です。 • 10ms - 10（ミリ秒）推奨されません。テストの目的のために使用します。 • 100ms - 100（ミリ秒）推奨されません。テストの目的のために使用します。 • 1sec - 1（秒） • 10sec - 10（秒）（初期値） • 1min - 1（分） • 10min - 10（分）
MEP ID(s)	メンテナンスアソシエーションに含まれる MEP ID を指定します。 • Add - MEP ID を追加します。 • Delete - MEP ID を削除します。 初期値では、初めて作成されたメンテナンスアソシエーションには MEP ID はありません。MEP ID の範囲は、1-8191 です。

「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

テーブルからエントリを削除するためには、削除対象のエントリの列の「Delete」ボタンをクリックします。

エントリの追加

項目入力後、「Add」ボタンをクリックします。

エントリの編集

1. エントリ横の「Edit」ボタンをクリックすると項目の編集が可能となります。

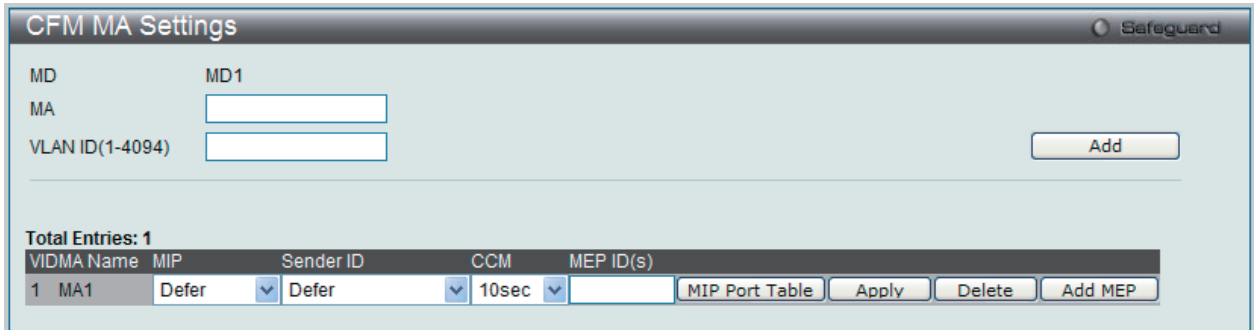


図 7-74　CFM MA Settings 画面 - Edit

2. 項目設定後、「Apply」ボタンをクリックします。

MIP ポートテーブルの参照

MIP ポートテーブルを参照します。

L2 Features > CFM > CFM Settings 画面で「MIP Port Table」ボタンをクリックします。

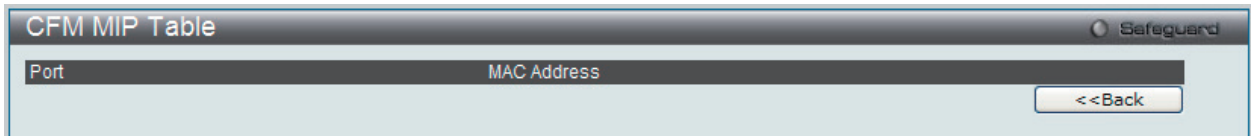


図 7-75　CFM MIP Table 画面

CFM MEP 設定

MEP を追加します。

L2 Features > CFM > CFM Settings 画面で「Add MEP」ボタンをクリックし、以下の画面を表示します。

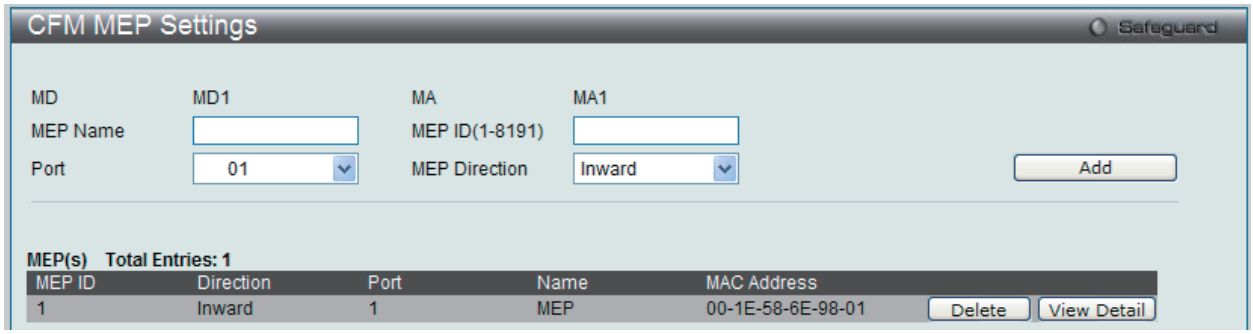


図 7-76　CFM MEP Settings 画面

以下の項目を設定できます。

項目	説明
MEP Name	MEP 名。デバイスに設定されたすべての MEP 内で固有です。
MEP ID	MEP ID。MA の MEP ID リストで設定される必要があります。
Port	ポート番号。本ポートは MA の関連付けられている VLAN メンバである必要があります。
MEP Direction	MEP の方向を指定します。 • Inward - 内向き（アップ）MEP。内向きの MEP は、内側から受信する同じかそれ以下のレベルにあるすべての CFM フレームを破棄します。そして、フレームの送信元が内向きまたは外向きにかかわらず、より高いレベルにあるすべての CFM フレームを転送します。 • Outward - 外向き（ダウン）MEP。外向きのポートは、ブリッジリレー機能側から受信する同じかそれ以下のレベルにあるすべての CFM フレームを破棄します。それは、そのレベルにあるすべての CFM フレームを処理して、ブリッジポートからから受信する低いレベルの CFM フレームすべてを破棄します。外向きポートは、フレームの送信先の方向にかかわらず、より高いレベルにあるすべての CFM フレームを転送します。

項目設定後、「Add」ボタンをクリックします。

MEP エントリに関する詳細情報の参照

「View Detail」ボタンをクリックし、以下の画面を表示します。

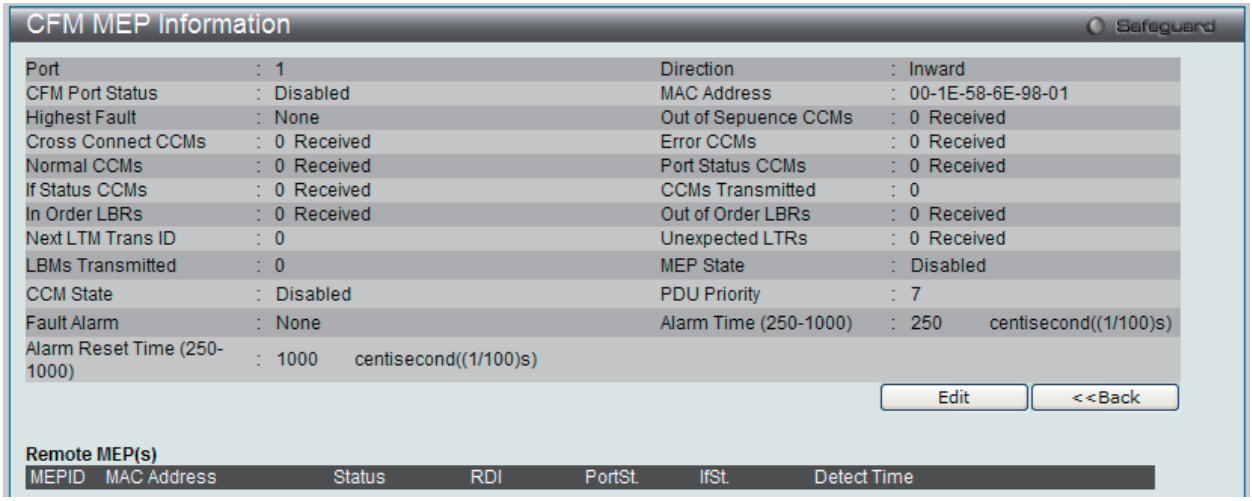


図 7-77　CFM MEP Information 画面

MEP の編集

「Edit」ボタンをクリックし、以下の画面を表示します。

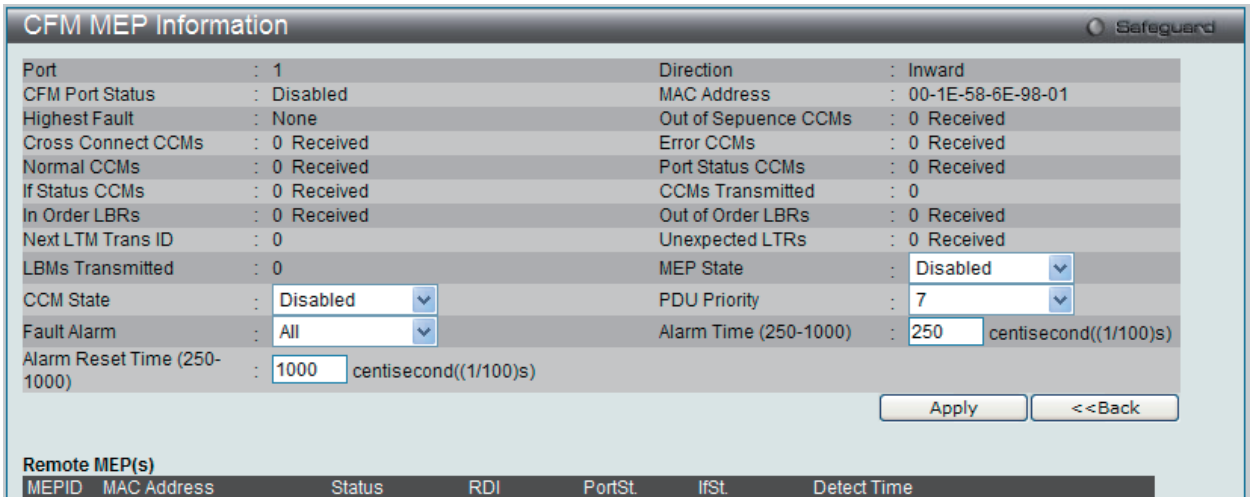


図 7-78　CFM MEP Information 画面 - Edit

以下の項目を設定または表示できます。

項目	説明
MEP State	MEP 管理状態を「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Disabled」です。
CCM State	CCM 送信状態を「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Disabled」です。
PDU Priority	802.1p 優先度は MEP によって送信された CCM および LTM メッセージに設定されます。初期値は 7 です。
Fault Alarm	これは、MEP によって送信される障害アラームの制御タイプです。 • All - すべての障害アラームのタイプが送信されます。 • Mac Status - 優先度が「Some Remote MEP MAC Status Error」（リモート MEP の MAC ステータスエラー）以上である障害アラームだけが送信されます。 • Remote CCM - 優先度が「Some Remote MEP Down」（リモート MEP のダウン）以上である障害アラームだけが送信されます。 • Error CCM - 優先度が「Error CCM Received」（エラー CCM の受信）以上である障害アラームだけが送信されます。 • Xcon CCM - 優先度が「Cross-connect CCM Received」（クロスコネクト CCM の受信）以上である障害アラームだけが送信されます。 • None - 障害アラームは送信されません。（初期値）
Alarm Time (250-1000)	これは、障害検出後に障害アラームが送信されるまでの経過時間です。範囲は 250-1000（センチ秒）です。初期値は 250（センチ秒）です。
Alarm Reset Time (250-1000)	これは、障害による再度アラーム送信前の検知が始動されるまでの待機時間です。範囲は 250-1000（センチ秒）です。初期値は 1000(センチ秒) です。
Remote MEP (s) テーブル	リモート MEP の読み出し用情報が表示されます。情報は、リモートの MEPID、MAC アドレス、ステータス、RDI、ポートステータス、インタフェースステータス、最後の CCM シリアル番号、送信元のシャーシ ID、送信元の管理アドレス、および検出時間を含みます。

CFM Port Settings（CFM ポート設定）

ポートに CFM を設定します。

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

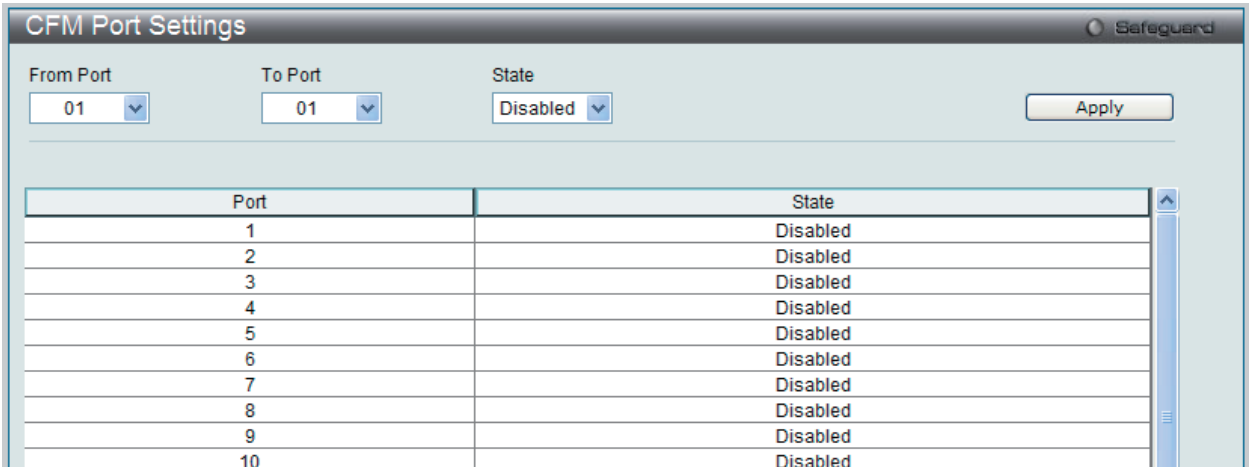


図 7-79　CFM Port Settings 画面

設定対象となる項目は以下の通りです。

項目	説明
From Port/To Port	本設定に使用されるポート範囲を選択します。
State	特定ポートの CFM 設定を有効または無効にします。初期値は無効です。

「Apply」ボタンをクリックし、変更を有効にします。

CFM Loopback Settings（CFM ループバック設定）

CFM ループバックを設定します。

L2 Features > CFM > CFM Loopback 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。

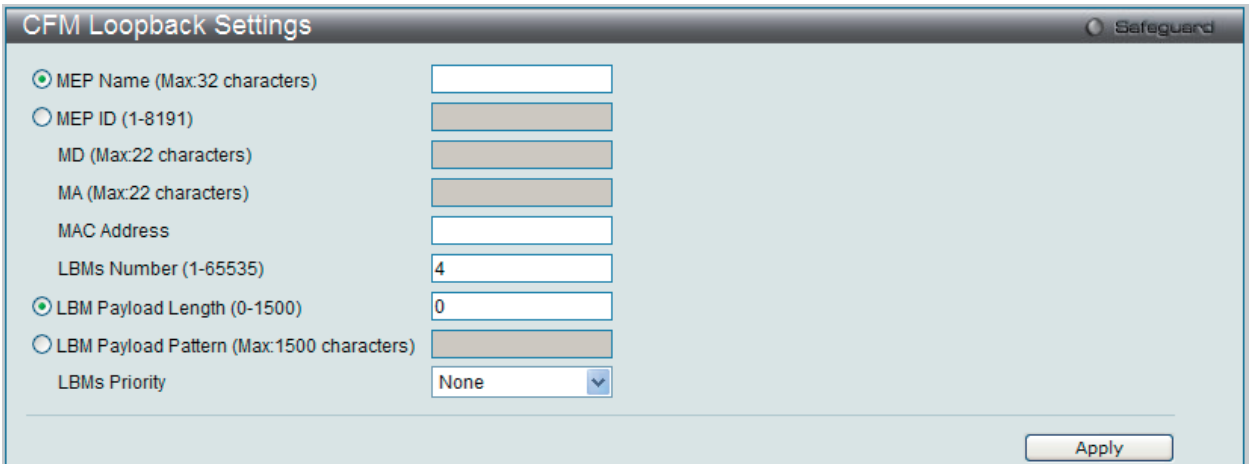


図 7-80　CFM Loopback Settings 画面

設定対象となる項目は以下の通りです。

項目	説明
MEP Name (Max: 32 characters)	MEP 名を入力します。
MEP ID (1-8191)	MEP ID を入力します。
MD (Max:22 characters)	メンテナンスドメインの名称を入力します。
MA (Max:22 characters)	メンテナンスアソシエーションの名称を入力します。
MAC Address	宛先 MAC アドレスを入力します。
LBMs Number (1-65535)	送信する LBM 数。初期値は 4 です。1 ～ 65525 の範囲で指定します。
LBM Payload Length (0-1500)	送信される LBM のペイロード長。初期値は 0 です。
LBM Payload Pattern (Max: 1500 characters)	データ TLV が含まれるかどうかの指示に伴うデータ TLV に含める任意データの量。
LBMs Priority	送信される LBM に設定される 802.1p 優先度（0-7）。指定しない場合、MA が送信した CCM と LTM と同じ優先度を使用します。初期値は「None」（なし）です。

「Apply」ボタンをクリックし、変更を有効にします。

CFM Linktrace Settings（CFM リンクトレース設定）

CFM リンクトラックメッセージを設定します。

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

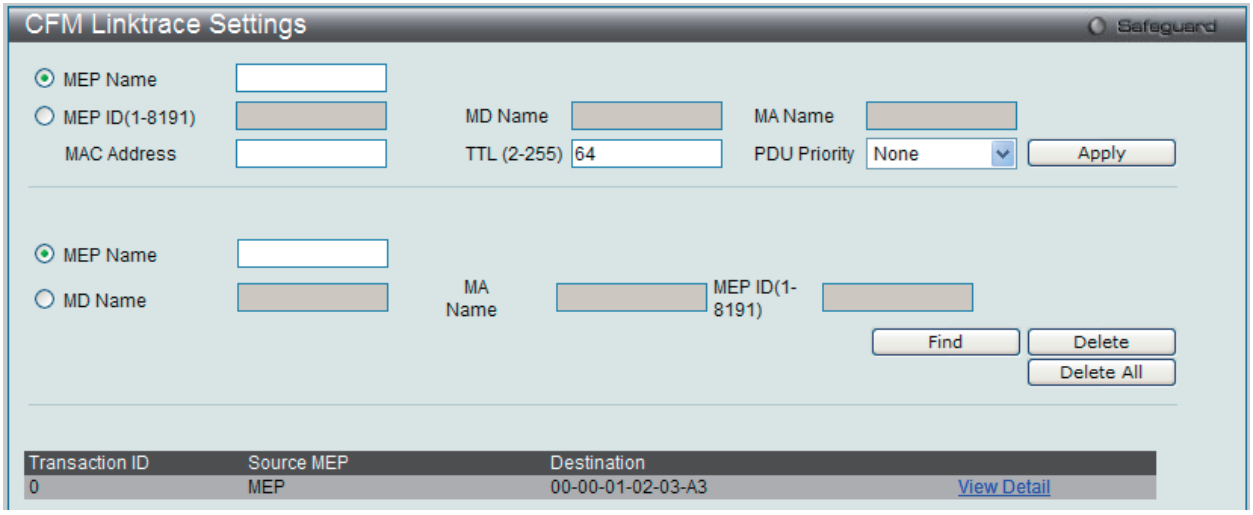


図 7-81　CFM Linktrace Settings 画面

設定対象となる項目は以下の通りです。

項目	説明
MEP Name	MEP 名を入力します。
MEP ID (1-8191)	MEP ID を入力します。
MD Name	メンテナンスドメインの名称を入力します。
MA Name	メンテナンスアソシエーションの名称を入力します。
MAC Address	宛先 MAC アドレスを入力します。
TTL (2-255)	リンクトレースメッセージの TTL 値。初期値は 64 です。範囲は、2-255 です。
PDU Priority	送信される LTM に設定される 802.1p 優先度（0-7）。指定しない場合、MEP が送信した CCM と CCM と同じ優先度を使用します。

「Apply」ボタンをクリックし、変更を有効にします。

「MEP Name」または「MEP ID」を入力し、「Find」ボタンをクリックして、画面下のテーブルにリンクトレースの詳細を表示します。
View Detail リンクをクリックすると、以下のようなリスト表示されているすべての CFM リンクトレース設定の詳細を表示します。

図 7-82　CFM Linktrace Settings 画面 - 参照

ERPS Settings（イーサネットリングプロテクション設定）

スイッチの Ethernet Ring Protection Switching (ERPS) 機能を有効にします。ERPS を有効にする前に、STP と LBD をリングポートで無効にする必要があります。

R-APS VLAN の作成前およびリングポート、RPL ポート、RPL オーナーの設定前に ERPS を有効にすることはできません。

注意 ERPS が有効になると、これらの項目を変更することはできません。

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

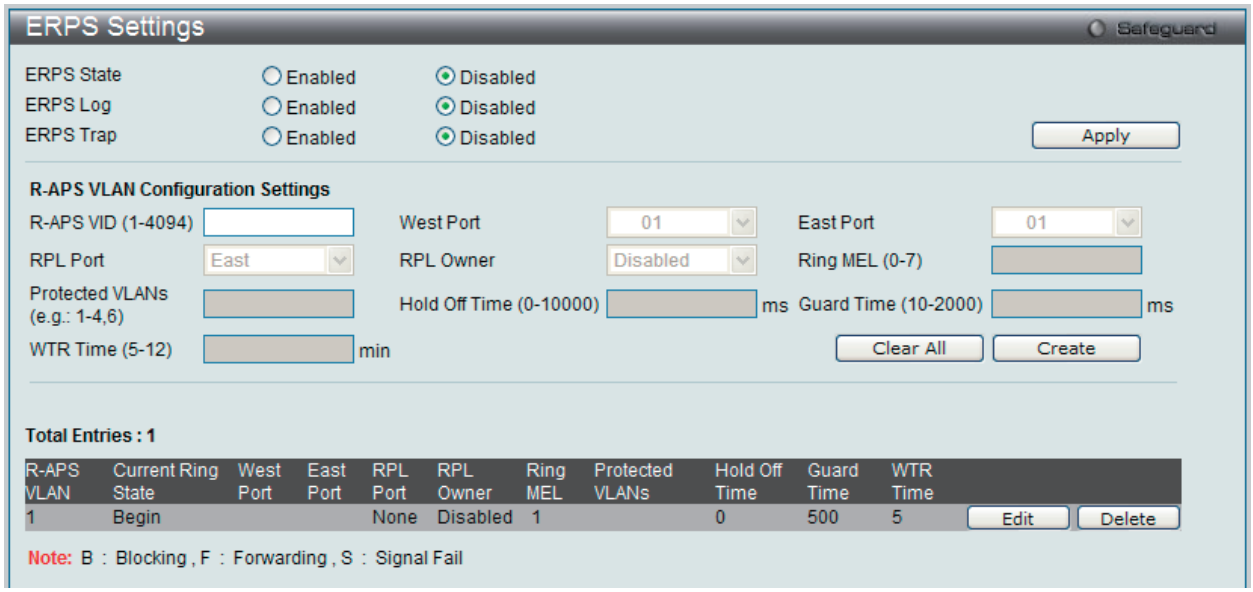


図 7-83　ERPS Settings 画面

設定対象となる項目は以下の通りです。

項目	説明
ERPS State	ERPS 状態を有効または無効にします。
ERPS Log	ERPS ログを有効または無効にします。
ERPS Trap	ERPS トラップを有効または無効にします。
R-APS VLAN Configuration Settings	R-APS VLAN とする VLAN を指定します。R-APS VLAN ID、West Port、East Port、RPL Owner ステータス、Ring MEL*、Protected VLAN、Hold Off Timer、Guard Time、および WTR Time を入力します。
West Port	West リングポートとしてポートを指定します。ERPS は、リングで内のノードのポートがどのようにリング自体に方向付けされるかを指定するために「East」および「West」という基本的な方向を使用します。リング上の各ノードには、East ポートと West ポートがあります。あるノードの West ポートは、リング内の隣接ノードの East ポートにリンクされます。
East Port	East リングポートとしてポートを指定します。ERPS は、リングで内のノードのポートがどのようにリング自体に方向付けされるかを指定するために「East」および「West」という基本的な方向を使用します。リング上の各ノードには、East ポートと West ポートがあります。あるノードの East ポートは、リング内の隣接ノードの West ポートにリンクされます。
RPL Port	Ring Protection Link (RPL : リングプロテクションリンク) ポートとしてリングポートを指定します。RPL は、リング上のすべてのリンクが機能している時、待機状態のままでトラフィックをブロックします。しかし、リング上にリンク障害があると、RPL ポートは、リングの周りの代替経路を許可するために RPL オーナーノードによってブロックを解除されます。
RPL Owner	デバイスを RPL オーナーノードとして有効または無効にします。このノードは、ネットワーク状態により必要に応じて RPL をブロックまたはブロックを解除します。Ethernet Ring Automatic Protection Switching (R-APS) メッセージプロトコルは、リング上のすべてのノードのプロテクション作業を調整します。リンク障害の場合、RPL オーナーはエラーとなったリンクをブロックし、RPL のブロックを解除するためにこれらのメッセージを使用します。リング上には 1 つの RPL オーナーのみ存在します。
Ring MEL	R-APS 機能のリング Maintenance Entity Group(MEG) レベル (MEL) を指定します。
Protected VLANs	本コマンドは、ERPS 機能により防御される VLAN を設定するために使用されます。

項目	説明
Hold Off Time	R-APS 機能ホールドオフタイムを指定します。ホールドオフタイマは、複数のレベルで ERPS のタイミングを調整するのに使用されます。その目的は、例えば、サーバレイヤスイッチがクライアントレイヤに切り替えられる前に問題を修正できるようにすることです。 新しい不良またはさらにサーバの不良が検出される場合、イベントはすぐには報告されません。代わりに、ホールドオフタイマの期限が切れた後にタイマを始動した形跡が不良がまだ存在しているかどうか確認するためにチェックされます。存在する場合、不良が報告され、ERPS は実施されます。
Guard Time	R-APS 機能のガードタイムを指定します。ガードタイマの動作中は、受信された R-APS メッセージは RPL オーナーに転送されません。これの目的は、2 つ以上の R-APS 信号エラーメッセージがリングのそれぞれの端から同時に送信される場合にループが形成される可能性を防ぐことです。
WTR Time	R-APS 機能の WTR タイム（復帰までの待ち時間）を指定します。WTR タイムは、条件のクリア後に経過するべき必須時間を定義します。WTR タイムの期限が切れた後に、RPL はアイドル状態に戻ります。(ブロック状態)。これは、断続的な信号エラーの検知による ERPS の過度の動作を防止するために使用されます。

*CFM（接続性障害管理）と ERPS が同時に使用される場合、R-APS PDU はイーサネット OAM PDU のセットの 1 つとなります。R-APS PDU の送信の動作は、イーサネット OAM に準じます。R-APS PDU の MEL がリングポートに同じ VLAN を持つ MEP（メンテナンスエンティティグループのエンドポイント）のレベルより高いと、R-APS PDU はリングに送信されません。

エントリの追加

新しい R-APS VLAN を作成するためには、メニューで必要な項目の設定を行い、「Create」ボタンをクリックします。

エントリの編集

1. エントリ横の「Edit」ボタンをクリックすると、画面上部に現在の設定が表示されます。

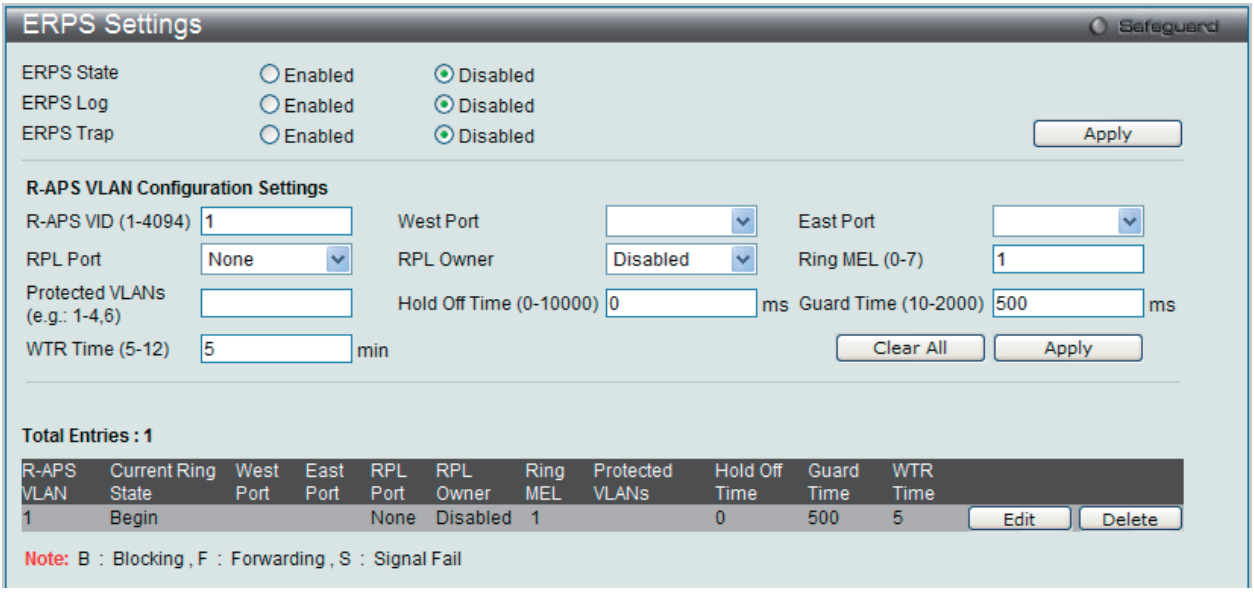


図 7-84　Multicast Forwarding Settings 画面 - Edit

2. 項目設定後、「Apply」ボタンをクリックして、ERPS、ERPS ログ、および ERPS トラップ設定への有効 / 無効状態の変更を適用します。

エントリの削除

テーブルからエントリを削除するためには、削除対象のエントリの列の「Delete」ボタンをクリックします。
「Clear All」ボタンをクリックすると、本画面のすべての設定がクリアされます。

第 8 章　QoS（QoS 機能の設定）

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

サブメニュー	説明	参照ページ
Bandwidth Control（帯域幅の設定）	送信と受信のデータレートを制限します。	152 ページ
Traffic Control（トラフィックコントロールの設定）	ストームコントロールの有効 / 無効の設定、およびマルチキャスト、ブロードキャストストームのしきい値を調整します。	153 ページ
Queue Bandwidth Control Settings（キュー帯域幅制御設定）	キュー帯域制御の設定を行います。	155 ページ
802.1p Default Priority（ポートへのパケットプライオリティの割り当て）	ポート単位にプライオリティを割り当てます。	156 ページ
802.1p User Priority（プライオリティのクラス（キュー）への割り当て）	クラス（キュー）にのプライオリティタグの割り当てをします。	156 ページ
QoS Scheduling Settings（QoS スケジュールの設定）	QoS スケジューリングを設定します。	157 ページ
Priority Mapping（プライオリティマッピング設定）	指定ポートにプライオリティマッピングを設定します。	157 ページ
TOS Mapping（TOS マッピング設定）	TOS マッピングの設定を行います。	158 ページ
DSCP Mapping（DSCP マッピング設定）	DSCP Mapping を設定します。	158 ページ

QoS メニューを使用し、本スイッチにセキュリティ機能を設定することができます。以下の項では QoS の機能と、802.1p プライオリティキューイングを利用するメリットについて説明します。

QoS の長所

QoS は IEEE 802.1p 標準で規定される技術で、ネットワーク管理者に、VoIP（Voice-over Internet Protocol）、Web 閲覧用アプリケーション、ファイルサーバアプリケーション、またはビデオ会議などの広帯域を必要とする、または高い優先順位を持つ重要なサービスのために、帯域を予約する方法を提供します。より大きい帯域を作成可能なだけではなく他の重要度の低いトラフィックを制限することで、ネットワークが必要以上の帯域を使用しないようにします。スイッチは各物理ポートで受信した様々なアプリケーションからのパケットをプライオリティに基づき独立したハードウェアキューに振り分けます。以下の図に、802.1p プライオリティキューイングがどのように本スイッチに実装されているかを示しています。

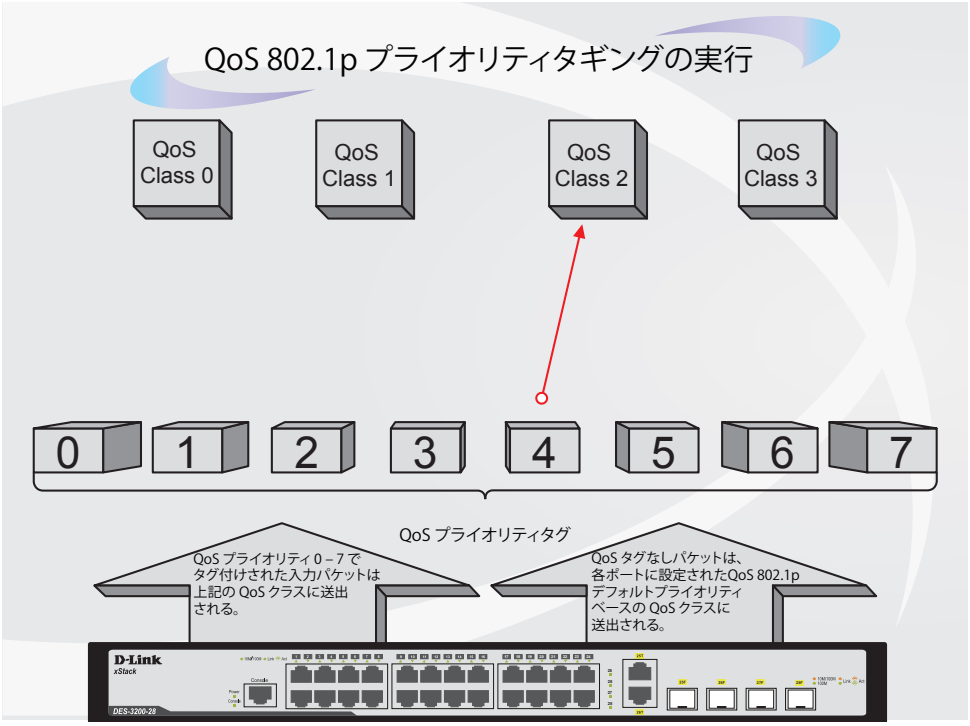


図 8-1　スイッチ上での QoS マッピングの例

上の図は本スイッチのプライオリティの初期設定です。クラス 3 は、スイッチの 4 つのプライオリティキューの中で、最も高い優先権を持っています。QoS を実行するためには、ユーザはスイッチに対し、パケットのヘッダに適切な識別タグが含まれているかを確認するように指示する必要があります。そして、ユーザはそれらのタグ付きパケットをスイッチ上の指定されたキューに送り、優先順序に従って送出するようにします。

例えば、遠隔地に設置した 2 台のコンピュータ間でビデオ会議を行うとします。管理者は Access Profile コマンドを使用して、送信するビデオパケットにプライオリティタグを付加します。次に受信側ではスイッチにそのタグの確認するよう指示を行い、タグ付きパケットを受信したら、それをスイッチのクラスキューに関連付けを行うようにします。また、管理者はこのキューに優先順位を与え、他のパケットが送出されるよりも前に送信されるように設定を行います。この結果、このサービス用のパケットは、できるだけ早く送信され、キューが最優先されることにより、中断されることなくパケットを受け取ることができるため、このビデオ会議用に帯域を最適化することが可能になります。

QoS について

本スイッチには、4 つのプライオリティキューがあります。これらのプライオリティキューには、0 から 3 までのラベルが付けられており、最高レベルの 3 番キューから最低レベルの 0 番キューまでがあります。IEEE 802.1p に規定される 8 つのプライオリティタグはスイッチのプライオリティタグと以下のように関連付けされます。

- プライオリティ 0 は、スイッチの Q1 キューに割り当てられます。
- プライオリティ 1 は、スイッチの Q0 キューに割り当てられます。
- プライオリティ 2 は、スイッチの Q0 キューに割り当てられます。
- プライオリティ 3 は、スイッチの Q1 キューに割り当てられます。
- プライオリティ 4 は、スイッチの Q2 キューに割り当てられます。
- プライオリティ 5 は、スイッチの Q2 キューに割り当てられます。
- プライオリティ 6 は、スイッチの Q3 キューに割り当てられます。
- プライオリティ 7 は、スイッチの Q3 キューに割り当てられます。

Strict（絶対優先）のプライオリティベースのスケジューリングでは、優先度の高いキューに属するパケットから送信されます。優先度の高いキューが複数ある場合は、プライオリティタグに従って送信されます。高プライオリティのキューが空である時にだけプライオリティの低いパケットは送信されます。

重み付けラウンドロビンキューイングでは、各プライオリティキューから送信されるパケットの数は、指定された重み付けによって決定されます。A から D までの QoS キューに、4 から 1 までの重み付けを設定したとすると、パケットは以下の順に送信されます。: A1, B1, C1, D1, A2, B2, C2, A3, B3, A4

重み付けラウンドロビンキューイングでは、各 QoS キューが同じ重み付けを持つならば、各 QoS キューのパケット送信の機会はラウンドロビンキューイングのように、全く同じになります。

本スイッチは、各ポートに 4 つのプライオリティキュー（と 8 つの CoS）を持っています。

Bandwidth Control（帯域幅の設定）

帯域制御の設定を行うことにより、すべての選択ポートに対して、送信と受信のデータレートを制限することができます。

ポートの帯域制御の設定を行うには、**QoS > Bandwidth Control** の順にメニューをクリックし、以下の画面を表示します。

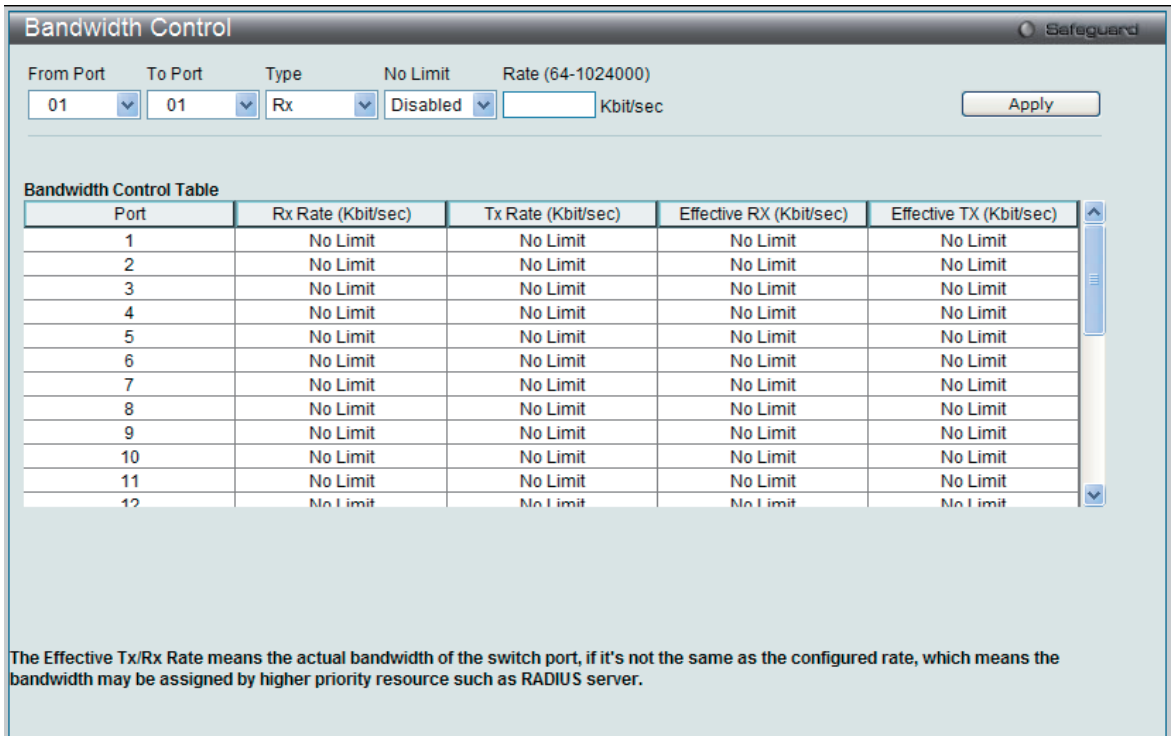


図 8-2　Bandwidth Control 画面

以下の項目を設定または表示できます。

項目	説明
From Port / To Port	設定対象のポート範囲を指定します。
Type	Rx（受信）、Tx（送信）および Both（両方）から選択します。帯域上限を受信、送信、送受信の両方のいずれに適用するのかを設定します。
No Limit	選択ポートに対する帯域制限を設定します。 • Enabled - ポートで帯域制限を行いません。 • Disabled - ポートで帯域制限を行います。（初期値）
Rate (64-1024000)	選択ポートのデータ速度の上限値（Kbit/ 秒）を指定します。値は 64 から 1024000 の間で、62.5 の倍数を入力します。

「Apply」ボタンをクリックし、選択ポートの帯域制御を設定します。設定の結果は、画面下部の「Bandwidth Control Table」に表示されます。

Traffic Control（トラフィックコントロールの設定）

コンピュータネットワーク上にはマルチキャストパケットやブロードキャストパケットなどのパケットが正常な状態でも絶えずあふれています。このトラフィックはネットワーク上の端末の不良や、故障したネットワークカードなどが誤動作することにより増加することもあります。そのため、スイッチのスループットに関する問題が発生し、その結果、ネットワークの全体的なパフォーマンスにも影響する可能性があります。このパケットストームを調整するために、本スイッチは状況を監視し、制御します。

パケットストームを監視し、ユーザが指定したしきい値を基にパケットがネットワークにあふれているどうか判断します。パケットストームが検出されると本スイッチはパケットストームが緩和されるまで受信したパケットを破棄します。この方法を使用するためには以下の画面の「Action」欄の「Drop」オプションを設定します。

スイッチのチップカウンタを監視することによりスイッチに入力するパケットのスキャンとモニタを行います。チップにはブロードキャストとマルチキャストパケット用のカウンタのみ存在するため、この方法はブロードキャストストームとマルチキャストストームに対してのみ有効です。ストームが検出されると（次に示す画面で設定するパケット数のしきい値を超過すると）、スイッチは STP BPDU パケットを除くすべてのトラフィックの入力に対して、「Count Down」欄で指定した時間、ポートをシャットダウンします。
ストームが検出されると (以下で設定するパケット数のしきい値を超過すると)、スイッチは STP BPDU パケットを除くすべてのトラフィックの入力に対して、「Countdown」フィールドで指定した時間、ポートをシャットダウンします。
Countdown タイマが期限が切れる前にパケットストームが停止すると、ポートは再度すべての入力トラフィックを許可します。本時間経過後もパケットストームが続くようであれば、そのポートは「Shutdown Rest」モードに遷移し、トラップレシーバに送信する警告メッセージを生成します。一度「Shutdown Rest」モードに入ると、本ポートは 5 分後に回復します。または、**Configuration > Port Configuration > Port Settings** 画面で、手動で無効なポートの状態を「Enabled」（有効）にして回復させます。このようなストームコントロール機能を利用するためには、次に示す画面の「Action」欄で「Shutdown」オプションを選択してください。
ストームコントロールの有効 / 無効の設定、およびマルチキャスト、ブロードキャストストームのしきい値を調整するために本画面を使用します。

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

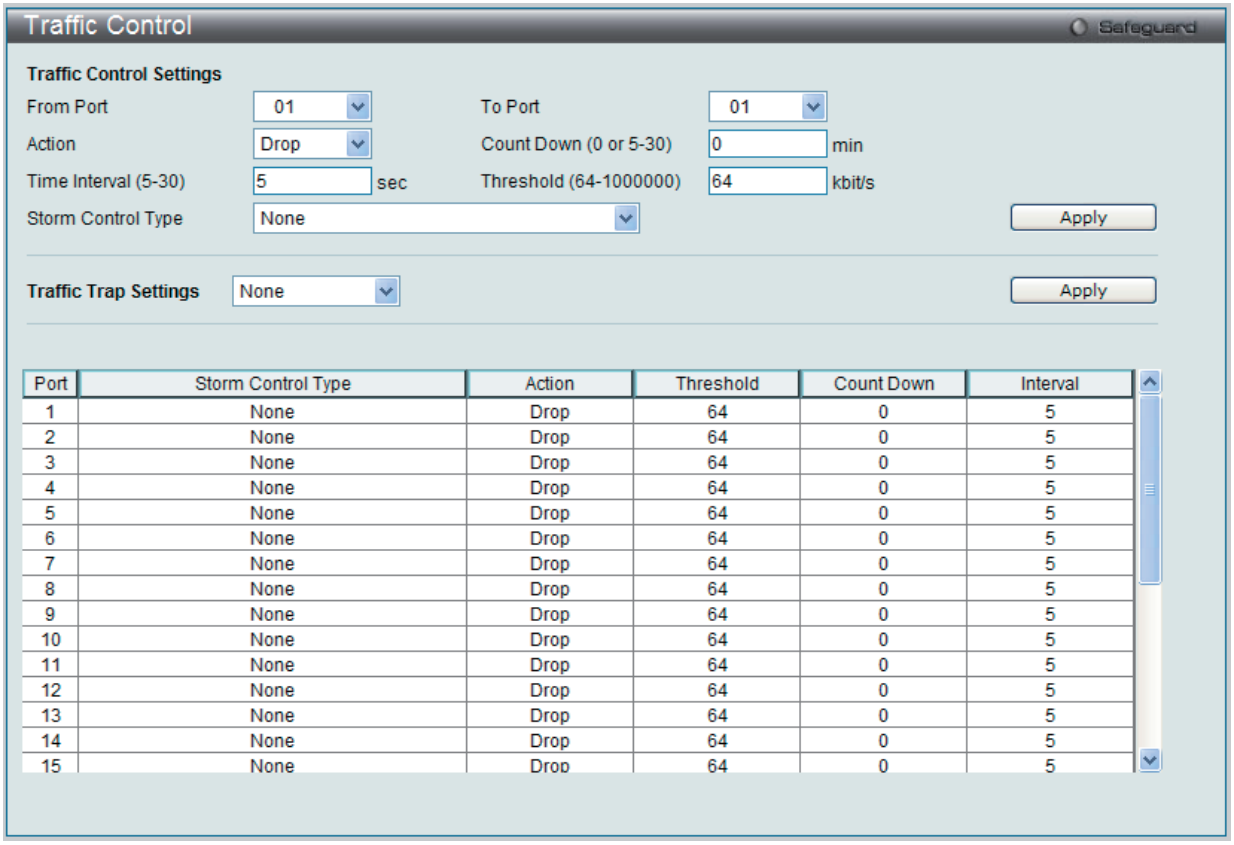


図 8-3　Traffic Control 画面

本画面には次の項目があります。

項目	説明
Traffic Control Settings	
From Port / To Port	ストームコントロールを表示するポート範囲を設定します。
Action	トラフィックコントロールの方法をプルダウンメニューで指定します。以下の方法を指定できます。 • Drop – ハードウェアトラフィックコントロールメカニズムを使用します。スイッチのハードウェアがしきい値に基づき収束するまでパケットを破棄します。 • Shutdown – ソフトウェアトラフィックコントロールメカニズムを使用します。検出すると STP を維持するのに必要な STP、BPDU パケットを除くすべての受信パケットに対してポートを閉鎖します。「Countdown」タイマ経過後もパケットストームが続くようであれば、そのポートは「Shutdown Rest」モードに遷移します。一度「Shutdown Rest」モードに入ると、本ポートは 5 分後に回復します。または、**Configuration > Port Configuration** 画面で、手動で無効なポートの状態を「Enabled」(有効) にして回復させます。このオプションを選んだ場合、Interval も設定する必要があります。この値はパケットストームが起こっているかを判断するためにスイッチチップからパケット数を取得する間隔です。
Count Down (0 or 5-30)	スイッチがトラフィックストームによってポートを閉鎖するまでの時間を指定します。このカウントダウンの期間、スイッチはトラフィックストームを受け続けると、ポートをシャットダウンします。この項目は「Action」で「Shutdown」が指定されている時のみ有効で、ハードウェアベースのトラフィックコントロールでは使用できません。0、5-30（分）が指定できます。0 は、ポートが「Shutdown Rest」モードに入らないことを意味します。
Time Interval (5-30)	マルチキャストやブロードキャストのパケット数をチップからトラフィックコントロール機能に渡す間隔を指定します。これらのパケット数により受信パケットがしきい値を超えているかを決定します。5-30（秒）まで指定でき、初期値は 5（秒）です。
Threshold (64-1000000)	本値は、指定されたトラフィックコントロールが起動するしきい値の上限を表します。「Action」が「Drop」モードに設定された場合、しきい値は Kbit/sec で測定され、「Action」が「Shutdown」モードに設定される場合、pps（パケット / 秒）で測定されます。つまり、ストームトラフィックコントロール測定のトリガーとなるスイッチが受信するブロードキャスト / マルチキャスト / 未知のユニキャストパケットの数値です。 64-1000000Kbps まで指定でき、初期値は 64Kbps です。 Actual rate = |rate entered/ minimum granularity| * minimal granularity 例 : 62.5=|100/62.5| *62.5" |number| は、近接したより小さい整数を意味します。
Storm Control Type	検知の対象となるストームの種類を選択します。 Broadcast、Multicast、Unknown Unicast、Broadcast + Multicast、Broadcast + Unknown Unicast、Multicast + Unknown Unicast、Broadcast + Multicast + Unknown Unicast、または None
Traffic Trap Setting	
Traffic Trap Settings	トラフィックストームに基づくトラフィックコントロール機能による動作に応じて以下のそれぞれの状況でストームトラップメッセージを送ります。 • None - トラフィックコントロールメカニズムによる動作に関わらずストームトラップ警告メッセージを送りません。 • Storm Occurred - トラフィックストームの発生時のみストームトラップ警告メッセージを送ります。 • Storm Cleared - スイッチによりトラフィックストームを収束できた時のみストームトラップメッセージを送ります。 • Both - トラフィックストームの発生時、スイッチによりトラフィックストームを収束できた時の両方で、ストームトラップメッセージを送ります。 本機能はハードウェアモード（「Action」項目で「Drop」が指定されている時）では使用できません。

「Apply」ボタンをクリックし、各項目の変更を適用します。

注意 トラフィックコントロールは、リンクアグリケーション（ポートトランキング）が設定されたポートに対しては行うことができません。

注意 「Shutdown Rest」モードになったポートは、これらのポートがスイッチの CPU に BPDU パケットを転送していたとしても Spanning Tree 画面でも機能上でも「Discarding」になります。

注意 「Shutdown Rest」モードになったポートはユーザがこれらのポートを復旧するまですべての画面上でリンクダウンとして表示されます。

Queue Bandwidth Control Settings（キュー帯域幅制御設定）

キュー帯域制御の設定は、ポートの優先度キューに対して送信データレートの上限を設定するために使用されます。

QoS > Queue Bandwidth Control 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。

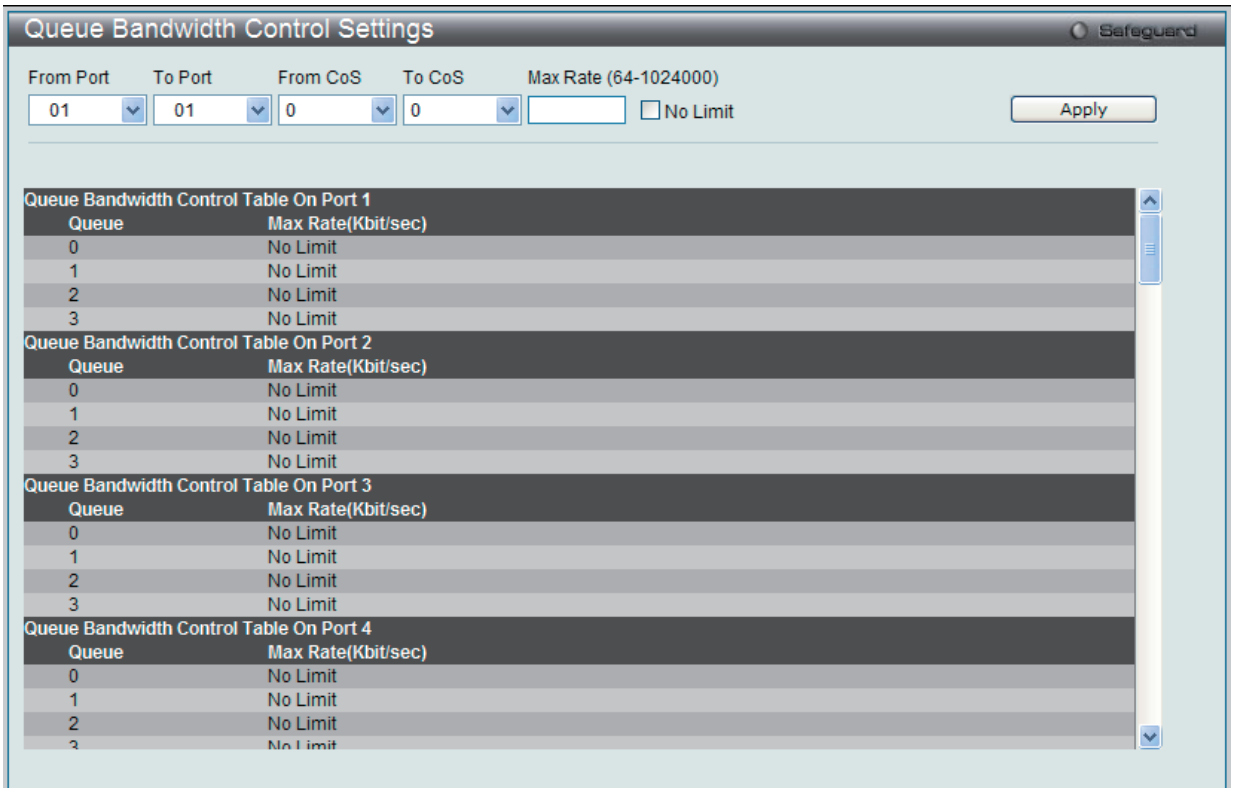


図 8-4　Queue Bandwidth Control Settings 画面

本画面には次の項目があります。

項目	説明
From Port / To Port	設定の対象となるポート範囲を指定します。
From CoS / To CoS	選択ポートに設定した CoS 値の範囲を定義します。
No Limit	チェックボックスを使用して選択ポートの帯域制限の有無を設定します。
Max Rate (64-1024000)	最大レートが制限です。指定される場合、例え帯域幅は利用可能であっても、キューから転送されたパケットは、指定した制限を超えることはありません。値は、64-1024000 の範囲で指定します。 Actual rate = |rate entered/ minimum granularity| * minimal granularity 例 : 62.5=|100/62.5| *62.5” |number| は、近接したより小さい整数を意味します。

「Apply」ボタンをクリックし、変更を設定します。

802.1p Default Priority（ポートへのパケットプライオリティの割り当て）

本スイッチは各ポートにデフォルトの 802.1p プライオリティを割り当てることができます。

QoS > 802.1p Default Priority の順にメニューをクリックし、以下の画面を表示します。

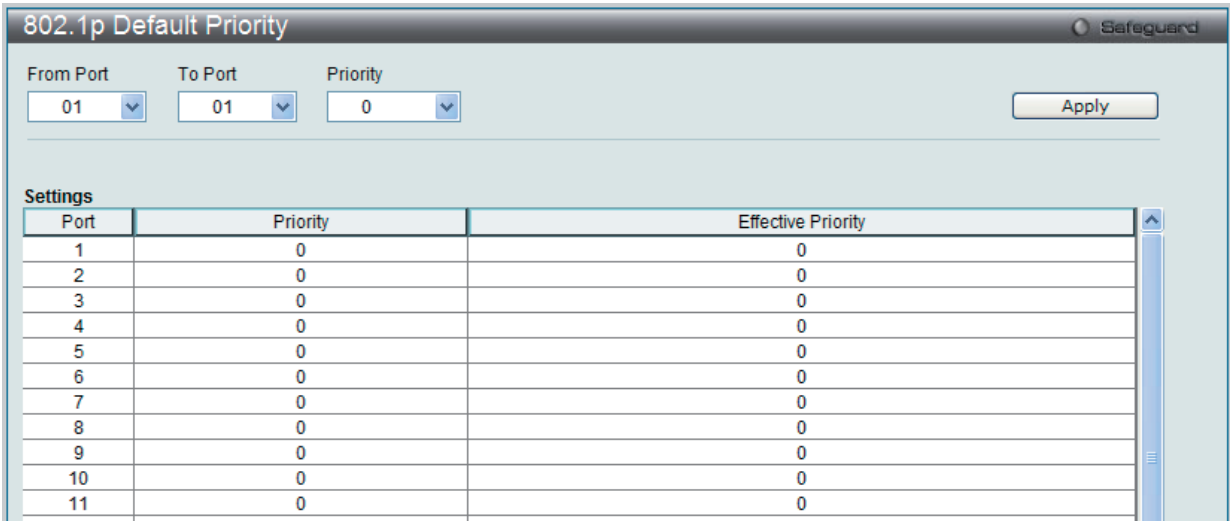


図 8-5　802.1p Default Priority 画面

プライオリティキューと有効なプライオリティタグは最低の 0 から最高の 7 まで指定できます。有効なプライオリティは、RADIUS に割り当てられた実際のプライオリティを示しています。RADIUS が割り当てた値が指定した制限を超えると、値はデフォルトプライオリティに設定されます。例えば、RADIUS が制限値に 8、デフォルトプライオリティに 0 を割り当てている場合、有効なプラオリティは 0 になります。

新しいデフォルトプライオリティを実行するためには、はじめに「From Port」、「To Port」プルダウンメニューでポート範囲を選択し、「Priority」プルダウンメニューで値 0 から 7 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。

802.1p User Priority（プライオリティのクラス（キュー）への割り当て）

スイッチは各 802.1p プライオリティにユーザプライオリティを割り当てることができます。

QoS > 802.1p User Priority の順にクリックし、以下の画面を表示します。

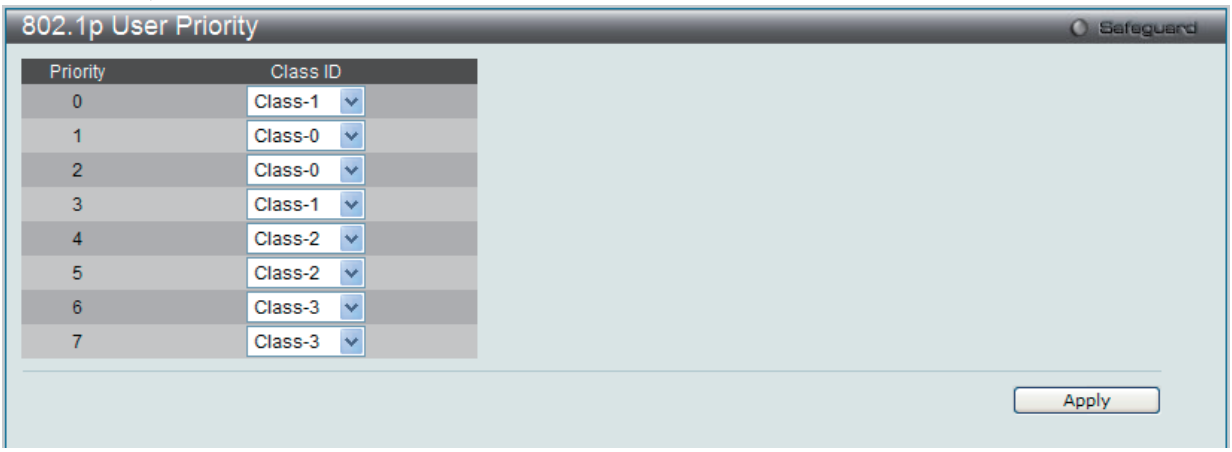


図 8-6　802.1P User Priority 画面

スイッチ上のポートグループにプライオリティを割り当てると、本画面のプルダウンメニューを使用して 802.1p プライオリティの 8 レベルのそれぞれに対してクラスを設定することができます。

本画面には以下の項目があります。

項目	説明
Priority	キューに割り当てられるプライオリティを表示します。
Class ID	プライオリティを割り当てるクラス（キュー）を設定します。「Class-0」（クラス 0）は最も低い優先度のキューで、「Class-3」（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。

QoS Scheduling Settings（QoS スケジュールの設定）

QoS のカスタマイズは、スイッチのハードウェアキューに使用する出力スケジュールを変更することにより実行できます。QoS 設定の変更は、どのような変更であっても気をつけて行う必要がありますが、特に優先度の低いキューでのネットワークトラフィックへの影響に注意が必要です。スケジュールの変更により、許容範囲外のパケットロスや重大な伝送遅延が発生することがあります。不適切な QoS 設定により急激なボトルネックが引き起こされる場合があるため、本設定をカスタマイズする際、特にトラフィックのピーク時には、ネットワークパフォーマンスをモニタしながら行うことが重要です。

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

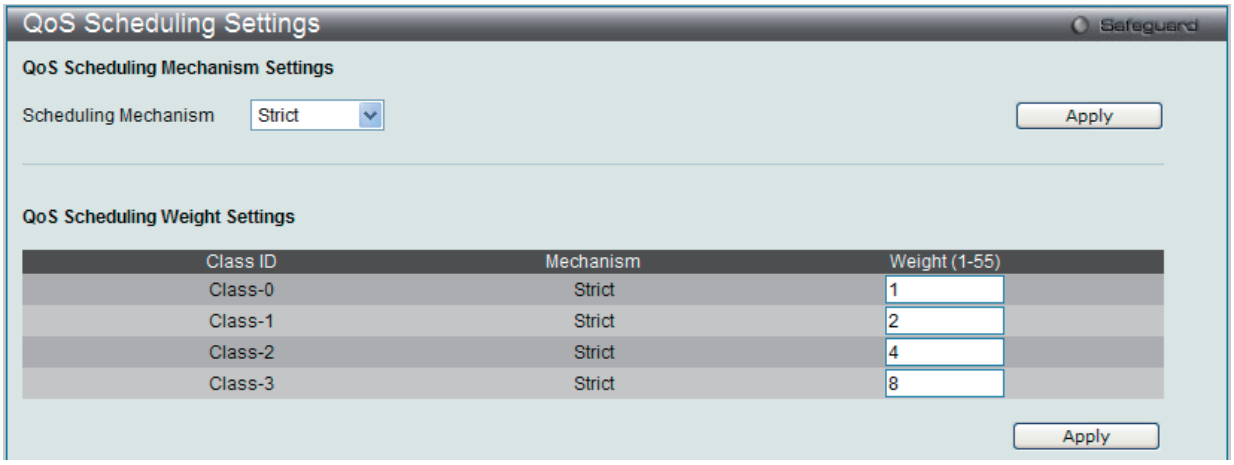


図 8-7　QoS Scheduling Settings 画面

本画面には以下の項目があります。

項目	説明
Scheduling Mechanism	「Strict」または「Weight Fair」を指定します。QoS におけるクラス（キュー）のスケジューリング方式を設定します。 • Strict - 最も高いサービスクラスのトラフィックを最初に処理します。上位キューの送信が完了するまで下位キューからはパケットは送信されません。 • Weight Fair - プライオリティのサービスクラスで配分されたパケットを重み付けされたラウンドロビン（WRR）アルゴリズムによって処理します。
Weight (1-55)	1-55 の値を指定します。

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。

Priority Mapping（プライオリティマッピング設定）

指定ポートにプライオリティマッピングを設定します。

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

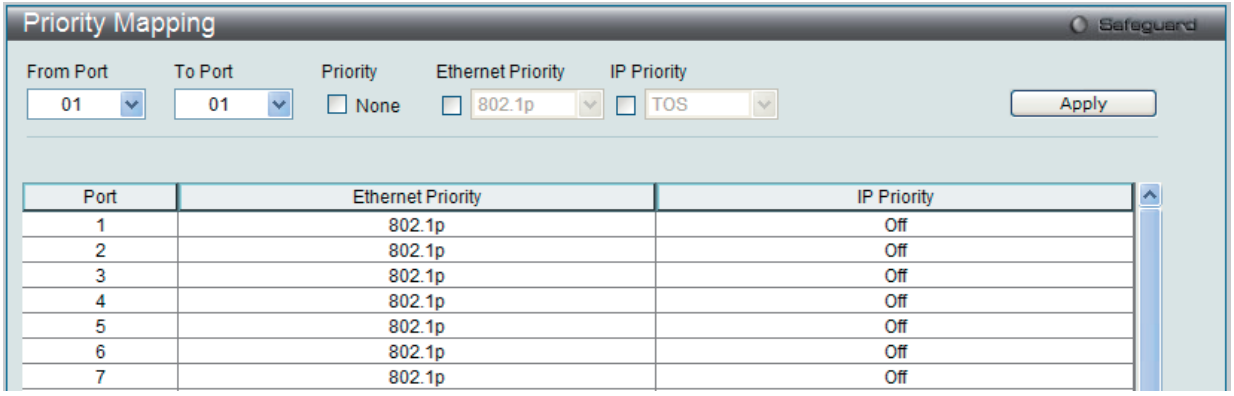


図 8-8　Priority Mapping 画面

以下の項目を設定または表示できます。

項目	説明
From Port / To Port	プライオリティ設定を割り当てるポートまたはポートグループを選択します。
Priority	イーサネットおよび IP プライオリティマッピングを使用しない場合は、「None」のチェックボタンをチェックします。
Ethernet Priority	チェックして 802.1p マッピングを設定します。
IP Priority	チェックしてプルダウンメニューから「TOS」または「DSCP」マッピングを選択します。

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。

TOS Mapping（TOS マッピング設定）

TOS マッピングの設定を行います。

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

図 8-9　TOS Mapping 画面

以下の項目を設定できます。

項目	説明
Class ID	Class ID を 0 ～ 3 から入力します。

「Apply」ボタンをクリックし、設定を有効にします。

DSCP Mapping（DSCP マッピング設定）

本画面では、DSCP Mapping を設定します。

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

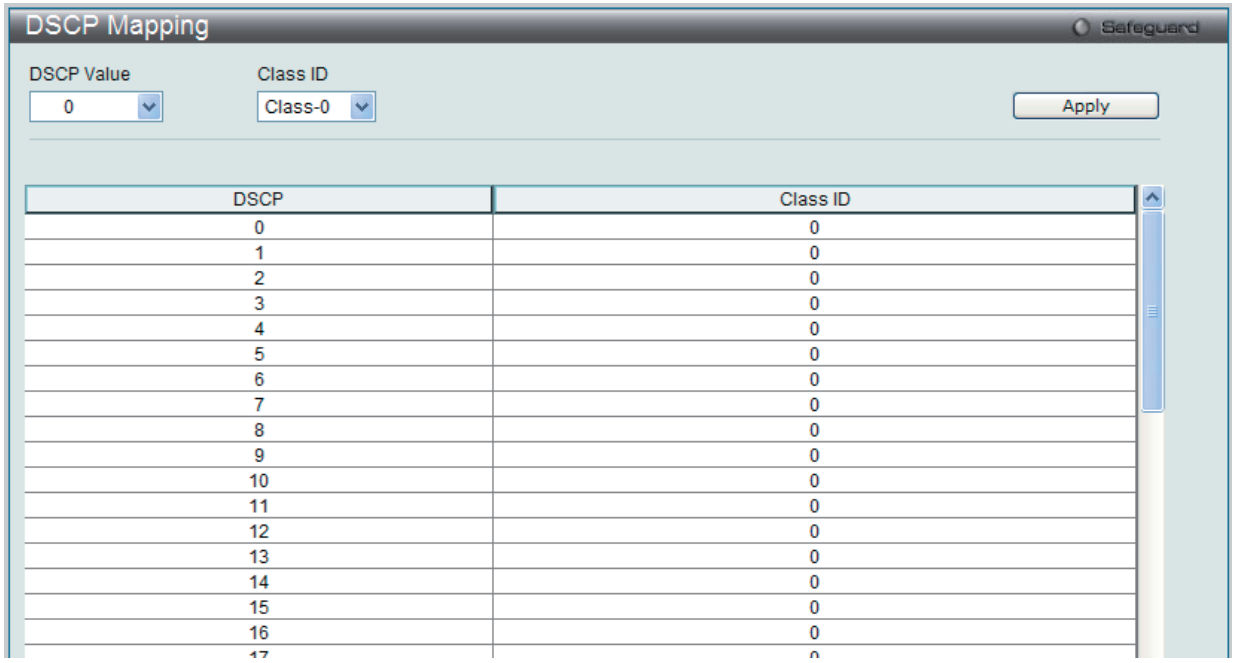


図 8-10　DSCP Mapping 画面

以下の項目を設定できます。

項目	説明
DSCP Value	DSCP 値を入力します。スイッチは各パケットヘッダの DiffServ コードを確認して、本値をパケットの送信基準 (またはその一部) とします。0 から 63 の範囲で設定します。
Class ID	Class-0 ～ Class-3 間で Class ID を指定します。

「Apply」ボタンをクリックし、変更を有効にします。

第 9 章　Security（セキュリティ機能の設定）

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

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

サブメニュー	説明	参照ページ
Safeguard Engine（セーフガードエンジン）	セーフガードエンジンの設定を行います。	159 ページ
Trusted Host（トラストホスト）	リモートのスイッチ管理用トラストホストを設定します。	161 ページ
IP-MAC-Port Binding（IMPB : IP-MAC- ポートバインディング）	IP アドレスと MAC アドレスを結合し、レイヤ間通信を行います。	161 ページ
Port Security（ポートセキュリティ）	ダイナミックな MAC アドレス学習をロックします。	166 ページ
802.1X（802.1X ポートベース / ホストベースアクセスコントロール）	ポート単位の 802.1X 認証を設定します。	168 ページ
SSL Settings（Secure Socket Layer の設定）	証明書の設定、暗号スイートの設定を行います。	179 ページ
SSH（Security Shell の設定）	SSH サーバ、SSH アルゴリズム、SSH ユーザ認証の設定を行います。	181 ページ
Access Authentication Control（アクセス認証コントロール）	TACACS/XTACACSTACACS+/RADIUS 認証の設定を行います。	184 ページ
MAC-based Access Control（MAC アドレス認証）	MAC アドレス認証機能を設定します。	191 ページ
DoS Prevention Settings（DoS 攻撃防止設定）	ハッカーや不正な送信元からの DoS（ Denial Of Service）攻撃を軽減する DoS 攻撃防止設定を行います。	194 ページ
DHCP Server Screening（DHCP サーバスクリーニング）	DHCP サーバスクリーニング機能を設定します。	195 ページ

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。これらの攻撃は正常なトラフィックフローに影響する可能性があります。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、限られ帯域を持つネットワークで必要不可欠なパケットの送受信を可能にします。セーフガードエンジンは、これを行うために、しきい値を使用してスイッチを「Exhausted」または「Normal」モードにします。

CPU 使用率が「Rising Threshold」を超えると、スイッチは「Exhausted」モードになります。「Exhausted」モードでは、スイッチは ARP パケットのために帯域幅を制限するため重要なパケットにはより多くの帯域幅を許容します。

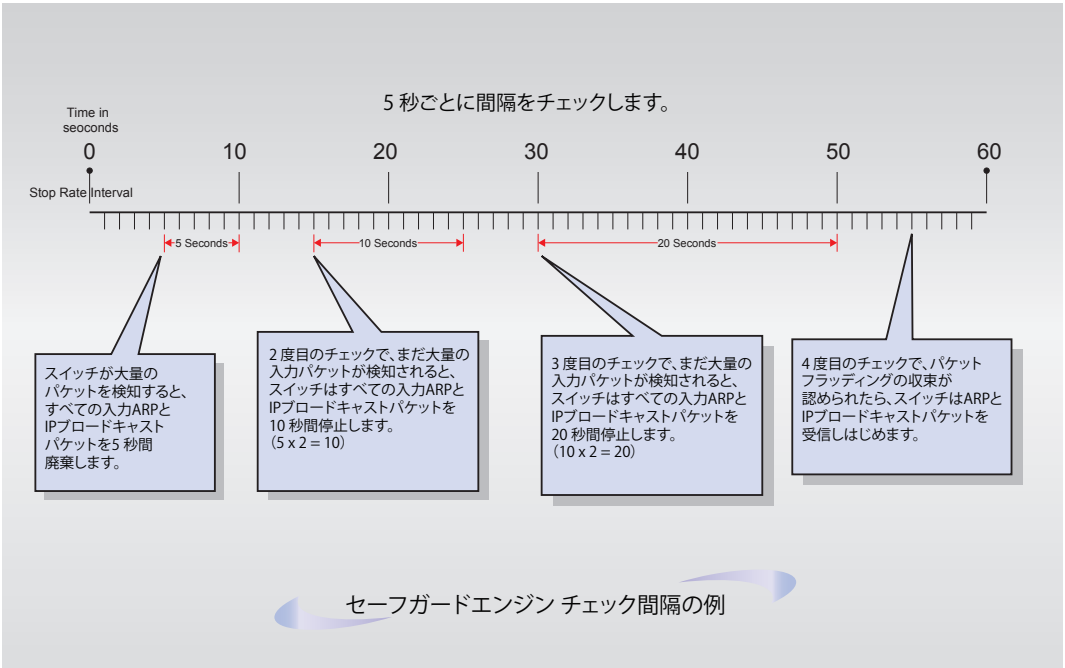


図 9-1　セーフガードエンジンの例

「Exhausted」モードでは、「Strict」および「Fuzzy」の 2 つのモードが ARP パケットに割り当てられた帯域幅を制限するために実行されます。

「Strict」モードでは、スイッチはすべての ARP パケットを廃棄します。スイッチは、どんなに CPU の稼働率が高くなっても、そのスイッチ行きでないパケットやブロードキャストパケットも ARP ストームにならない限りすべて処理します。

「Fuzzy」モードでは、スイッチはアルゴリズムを使用して ARP パケットに異なる帯域レベルを割り当てます。「Fuzzy」モードの時、スイッチは受信した ARP トラフィックの速度を分析し、ダイナミックに帯域の割り当てを行います。一度「Exhausted」モードになると、スイッチはパケットフローを本モード開始時の半分のレベルまで減少させます。パケットフローが安定すると、レートは処理するパケット量を徐々に増加させて、通常のパケットフローに戻ります。

「Strict」モードと「Fuzzy」モードの両方で、セーフガードエンジンはパケットのフラッド問題を一定の間隔でチェックします。
パケットのフラッディング問題を顕在化するために、すべての継続したチェック間隔に対して、スイッチはわずかな Ingress ARP パケットを受け入れる時間を倍にします。上の例題では継続したパケットのフラッディング問題が 5 秒間隔で検出された場合は ARP パケットを破棄する時間を倍にしています。（最初の破棄 = 5 秒、2 回目の破棄 = 10 秒、3 回目の破棄 = 20 秒）パケットのフラッディングを検出しなくなると、ARP パケットを制限する間隔を 5 秒に戻してプロセスを再開します。

スイッチのセーフガードエンジン機能の有効化およびセーフガードエンジンの設定を行います。

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

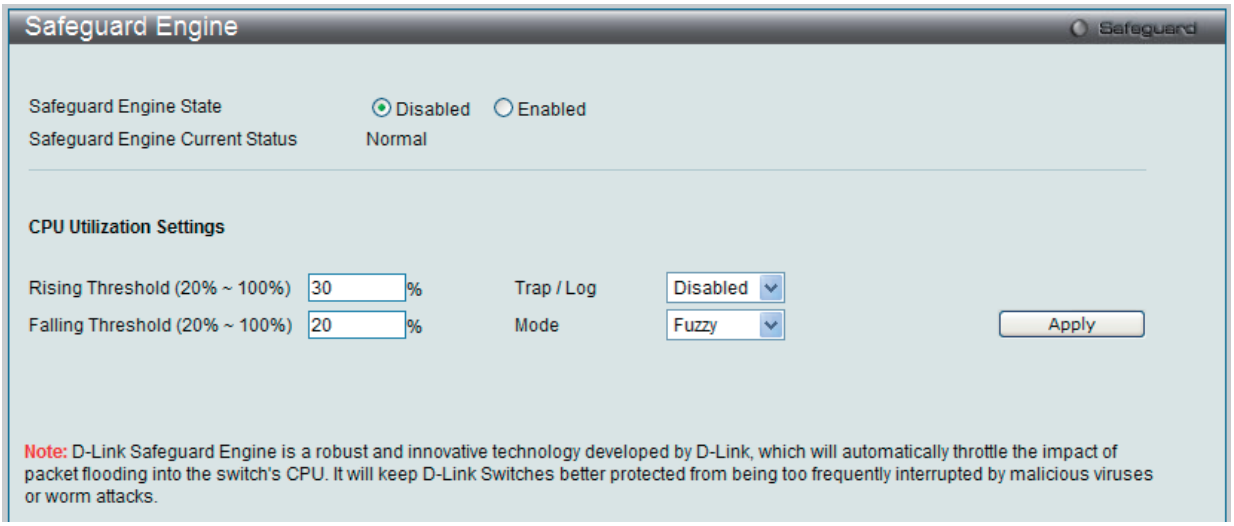


図 9-2　Safeguard Engine 画面

セーフガードエンジンオプションの有効化
「Safeguard Engine State」を「Enabled」にします。本画面上部にある「Safeguard」の隣にあるライトが緑色になります。

高度なセーフガードエンジン設定
以下の項目を設定し、「Apply」をクリックします。

以下の項目を使用し、設定を行います。

項目	説明
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。
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。
Rising Threshold (20% ~ 100%)	Safeguard Engine を有効にする前に許容可能な CPU 使用率のレベルを設定します。CPU 使用率がこのしきい値に到達すると、ここで設定した項目に基づいて、Exhausted モードに入ります。
Falling Threshold (20% ~ 100%)	許容可能な CPU 使用率のレベルを設定します。スイッチは CPU 使用率がこのしきい値に到達すると Exhausted モードから Normal モードに戻ります。
Trap/Log	CPU 使用率が高くなりセーフガードエンジン機能が作動した際にデバイスの SNMP エージェントとスイッチのログにメッセージを送信する機能を「Enabled」（有効）/「Disabled」（無効）にします。
Mode	CPU 高使用率に到達した際に起動する Safeguard Engine のタイプを選択します。 • Fuzzy – 本機能はすべてのトラフィックフローに対し平等に動的な帯域割り当てを行うことで CPU に対する IP と ARP トラフィックフローを最小化します。（初期値） • Strict – 本機能はストームがおさまるまで本スイッチ行きではないすべての ARP パケットの受信をストップし、不必要なブロードキャスト IP パケットの受信をストップします。

Trusted Host（トラストホスト）

リモートステーションがスイッチの管理を行うことを許可します。1 個以上の指定管理ステーションをユーザで制限した場合、IP アドレスによる制限の場合と同様、選択したステーションだけが Web マネージャ、Telnet セッションまたは SNMP マネージャを管理する権利を持つことができます。

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

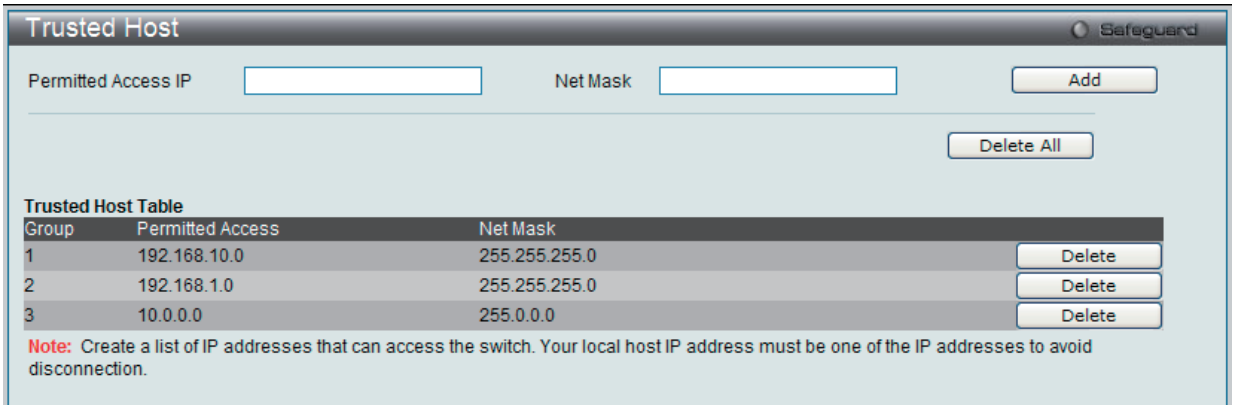


図 9-3　Trusted Host 画面

エントリの追加

管理ステーションの IP 設定を定義するためには、「Permitted Access IP」および「Net Mask」にそれぞれ IP アドレスとネットマスクを入力し、「Add」ボタンをクリックします。

エントリの削除

エントリを削除する場合は、削除するエントリの「Delete」ボタンをクリックします。トラストホストテーブルのすべてのエントリを削除するには、「Delete All」ボタンをクリックします。

IP-MAC-Port Binding（IMPB : 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 IP アドレスを、イーサネットリンクレイヤは 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- ポート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 アドレスと事前に設定したデータベースの組み合わせを確認することで、認証クライアントのみがスイッチのポートにアクセスできるようにします。未認証ユーザが IP-MAC- ポート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。IP-MAC- ポートバインディングの最大エントリ数は、チップの能力 (例えば ARP テーブルサイズ) およびデバイスのストレージサイズによって異なります。アクティブ、インアクティブエントリは同じデータベースを使用します。最大のエントリ番号は 500 です。認証クライアントのリストは、CLI または Web により手動で作成できます。
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。

IP-MAC-Port Binding フォルダには以下の 5 つの画面があります。
「IMP Binding Global Settings」、「IMP Binding Port Settings」、「IMP Binding Entry Settings」、「DHCP Snooping Entries」、および「MAC Block List」です。

IMP Binding Global Settings（IP-MAC- ポートバインディンググローバル設定）

スイッチのグローバルな IP-MAC バインディング設定（トラップログステータスおよび DHCP Snoop ステータス）を有効または無効にするのに使用します。「Trap/Log」欄では、IP-MAC バインディングのトラップログメッセージ送信を有効または無効にします。有効にすると、スイッチはスイッチに設定された IP-MAC バインディングに一致しない ARP パケットを受信した場合に、SNMP エージェントとスイッチログにトラップログメッセージを送信します。

Security > IP-MAC-Port Binding > IMP Binding Global Settings の順にメニュークリックして、以下の画面を表示します。

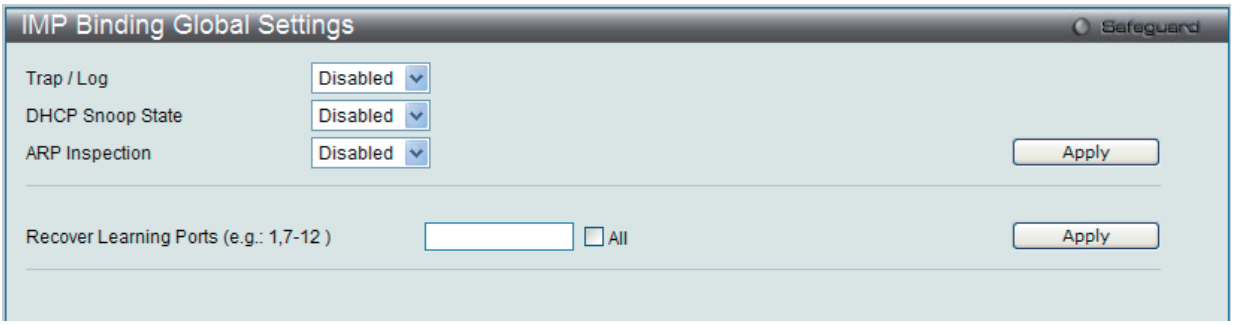


図 9-4　IMP Binding Global Settings 画面

以下の項目を使用して、設定または編集を行います。

項目	説明
Trap/Log	IP-MAC バインディングのトラップログメッセージ送信を有効または無効にします。有効にすると、スイッチはスイッチに設定された IP-MAC バインディングに一致しない ARP パケットを受信した場合に、SNMP エージェントとスイッチログにトラップログメッセージを送信します。
DHCP Snoop State	IP-MAC バインディングの DHCP Snooping オプションを「Enabled」（有効）または「Disabled」（無効）にします。DHCP Snooping が有効にされると、スイッチは、自動的に DHCP パケットについて検索し、IMPB ホワイトリストにそれら保存することで IP-MAC のペアを学習します。
ARP Inspection	IP-MAC バインディングの ARP Inspection オプションを「Enabled」（有効）または「Disabled」（無効）にします。本機能が有効な場合、スイッチは未認証の送信側 MAC、IP アドレスおよび Ingress ポートを持つ ARP パケットをフィルタリングします。本機能は、IP-MAC- ポートバインディングが有効なポートでのみ動作します。
Recover Learning Ports (e.g.: 1, 7-12)	動作を停止している ARP チェック機能を回復します。ARP チェック機能が停止しているポートまたはポート範囲を指定します。「All」をチェックすると、すべての学習ポートのリカバリを行います。

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。

IMP Binding Port Settings（IP-MAC- ポートバインディング設定）

ポートベースで IP-MAC- ポートバインディング設定を行います。

Security > IP-MAC Port Binding > IMP Binding 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。

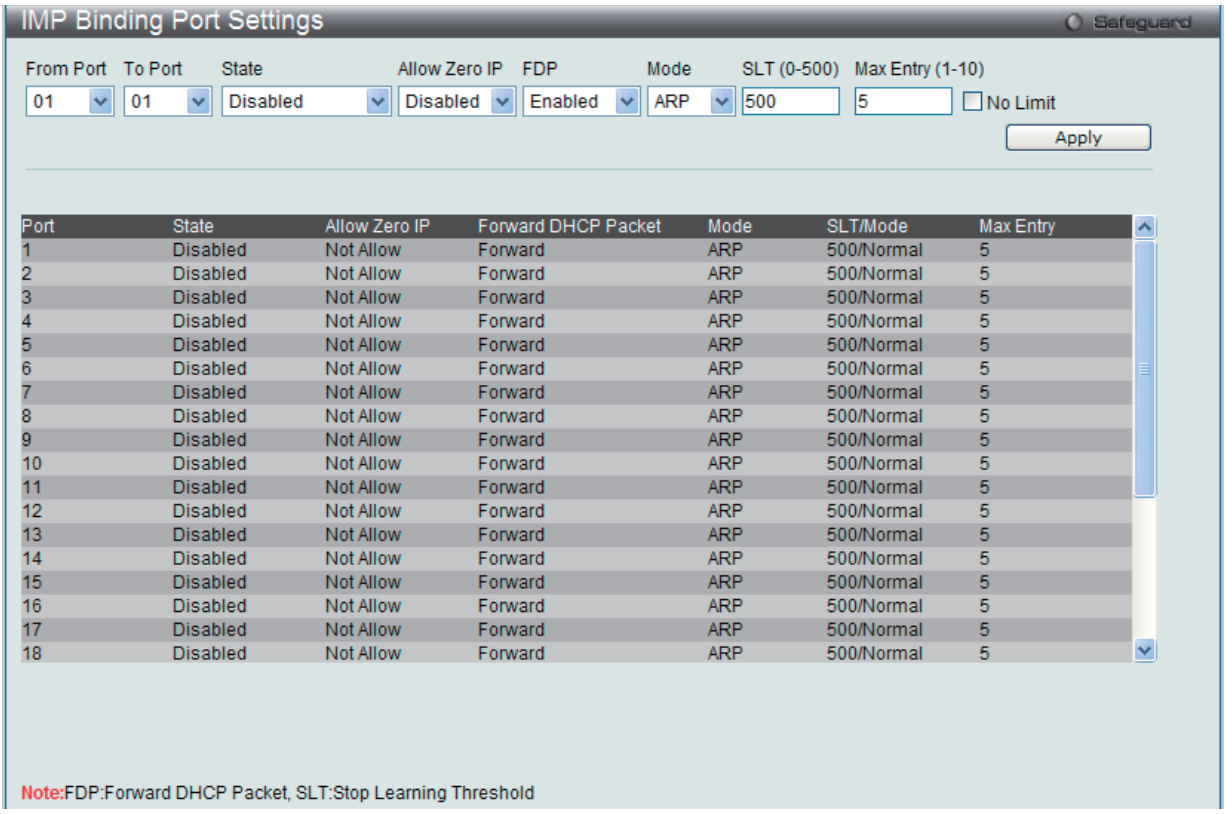


図 9-5　IMP Binding Port Settings 画面

以下の項目を使用して、設定または編集を行います。

項目	説明
From Port/To Port	IP-MAC- ポートバインディングを設定する対象のポートを指定します。
State	IP-MAC バインディングを「Enabled」(有効) または「Disabled」(無効) にします。 • Enabled (Strict) - 本モードはより厳しいコントロール方法を提供します。本モードを選択した場合、すべてのパケットは CPU に送られ、その結果 S/W にポートのエントリを入力するまで、ハードウェアはすべてのパケットを送信しません。ポートは、IP-MAC-PORT バインディングエントリによって ARP パケットと IP パケットをチェックします。パケットがエントリにあった場合、MAC アドレスは「dynamic」に設定されます。パケットがエントリにない場合、MAC アドレスは「block」に設定されます。そのほかのパケットは破棄されます。（初期値） • Enabled (Loose) - 本モードは、より緩いコントロール方法を提供します。本モードを選択した場合、ARP パケットと IP ブロードキャストパケットは CPU に送信されます。パケットは、特定の送信元 MAC アドレスがソフトウェアによってブロックされるまで、ハードウェアによって転送されます。ポートは、IP-MAC-PORT バインディングエントリに従って ARP パケットと IP ブロードキャストパケットをチェックします。パケットがエントリにあった場合、MAC アドレスは「dynamic」に設定されます。パケットがエントリにない場合、MAC アドレスは「block」に設定されます。その他のパケットは迂回します。
Allow Zero IP	本機能を「Enabled」(有効) /「Disabled」(無効) にします。一度有効にすると、スイッチは、0.0.0.0 の送信元 IP を持つ ARP パケットは通過することを許可します。
FDP	初期設定では、ブロードキャスト DA の DHCP パケットをフラッドします。無効にすると、ブロードキャスト DHCP パケットは特定のポートによって受信され、転送されません。
Mode	ARP または ACL を選択して、IP-MAC バインディング設定のモードを設定します。 • ACL - スイッチはこのポートのエントリに対応する ACL アクセスエントリを作成します。 • ARP - すべての ACL アクセスエントリが自動的に削除されます。（初期値）
SLT (0-500)	0-500 の範囲で学習を停止するしきい値を指定します。各ポートの初期値は 500 です。
Max Entry(1-10)	IP-MAC バインディングの最大エントリ数（1-10）を指定します。初期値は 5 です。エントリ数を制限しない場合には。「No Limit」をチェックします。

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。

IP-MAC- ポートバインディングの設定

1. 「From Port」と「To Port」欄でポートまたはポート範囲を指定します。
2. 「State」、「Allow Zero IP」、「Forward DHCP」、「Packet」、「Mode」および「SLT」を「Enabled」(有効) または「Disabled」(無効) にして、ポートの「Max Entry」値を設定します。
3. 「Apply」ボタンをクリックして設定を適用します。

IMP Binding Entry Settings（IP-MAC- ポートバインディングエントリ設定）

スイッチにスタティック IP-MAC- ポートバインディングエントリを作成します。

Security > IP-MAC-Port Binding > IMP Binding Entry Setting の順にメニューをクリックし、以下の画面を表示します。

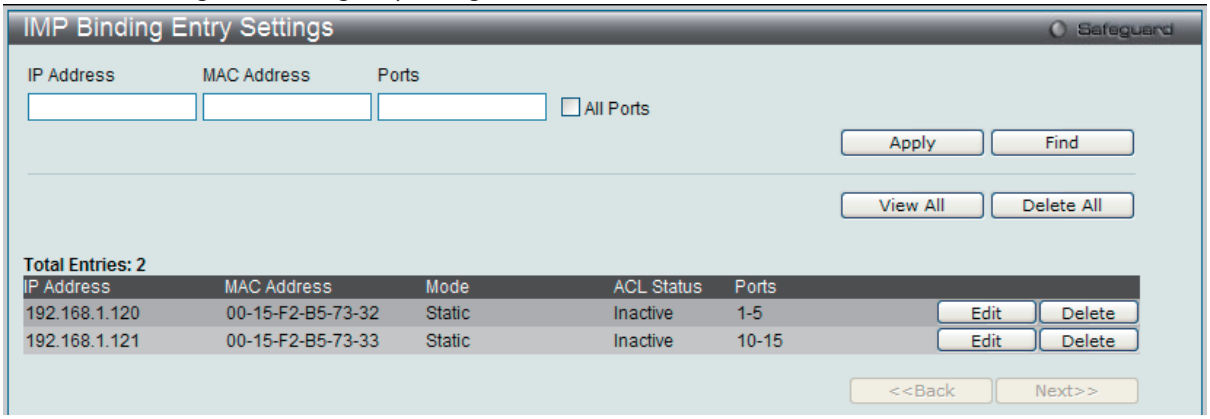


図 9-6　IMP Binding Entry Settings 画面

以下の項目を使用して、設定または編集を行います。

項目	説明
IP Address	MAC アドレスにバインドする IP アドレスを入力します。
MAC Address	IP アドレスとバインドする MAC アドレスを入力します。
Mode	「Static」または「Auto」が表示されます。
Ports	本 IP-MAC- ポートバインディングエントリを設定するポートを指定します。「All」を選択すると、スイッチのすべてのポートに設定します。

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。

エントリの追加

1. 「IP Address」、「MAC Address」および「Ports」にバインドする IP アドレス、MAC アドレスおよびポートを入力します。
2. 「Apply」ボタンをクリックします。

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、以下の画面を表示します。

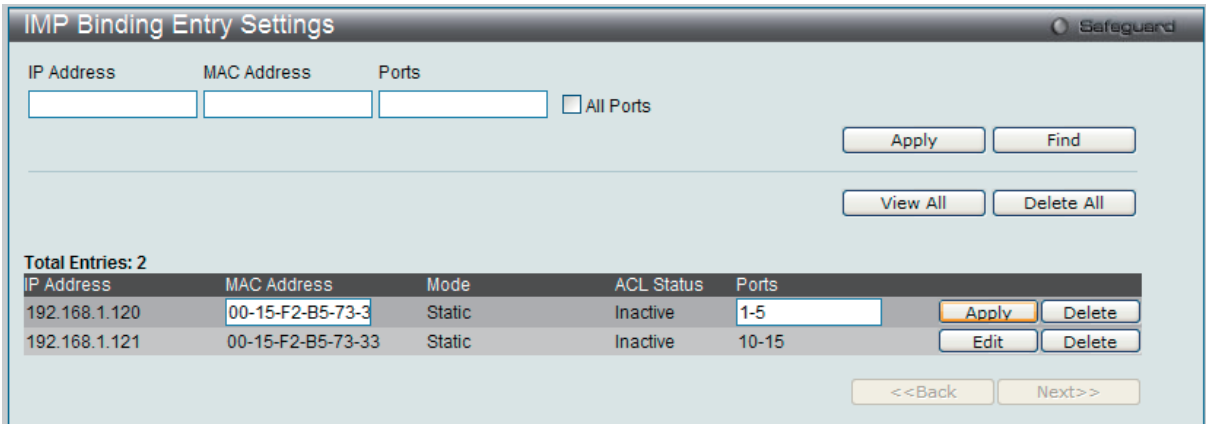


図 9-7　IMP Binding Entry Settings 画面 - Edit

2. 項目を編集し、エントリの「Apply」ボタンをクリックします。

エントリの検索

検索する項目を入力し、「Find」ボタンをクリックします。

すべてのエントリの表示

「View All」ボタンをクリックします。

エントリの削除

エントリの「Delete」ボタンをクリックします。すべてのエントリを削除する場合は、「Delete All」ボタンをクリックします。

DHCP Snooping Entries（DHCP Snooping エントリ）

特定ポートのダイナミックエントリを表示します。

Security > IP-MAC-Port Binding > DHCP Snooping Entries の順にクリックして、以下の画面を表示します。

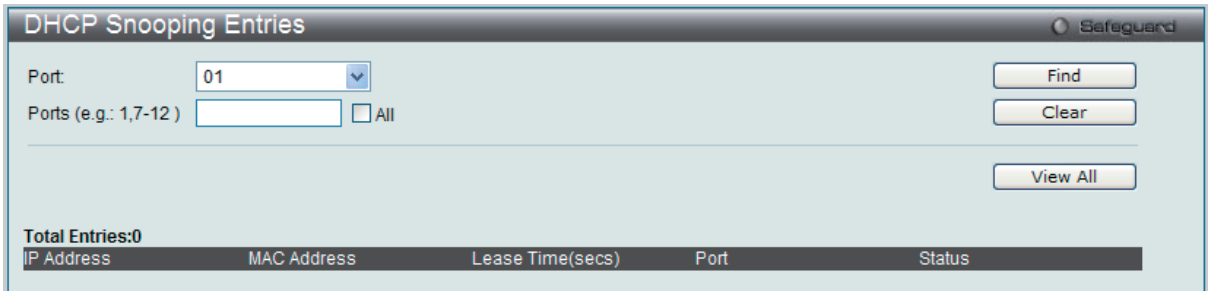


図 9-8　DHCP Snooping Entries 画面

以下の項目を使用して、設定または編集を行います。

項目	説明
Port	プルダウンメニューか設定するポートを選択します。
Ports (e.g.: 1, 7-12)	DHCP Snooping エントリを表示するポートを指定します。「All」を選択すると、本 IP-MAC バインディングエントリ (IP アドレス +MAC アドレス) をスイッチのすべてのポートに設定します。

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。

特定ポートの設定の表示

ポート番号を入力して「Find」ボタンをクリックします。

すべてのエントリの表示

「View All」ボタンをクリックします。

エントリの削除

「Clear」ボタンをクリックします。

MAC Block List（MAC ブロックリスト）

IP-MAC バインディング機能によりブロックされた未承認のデバイスを参照します。

Security > IP-MAC-Port Binding > MAC Block List の順にメニューをクリックして、以下の画面を表示します。

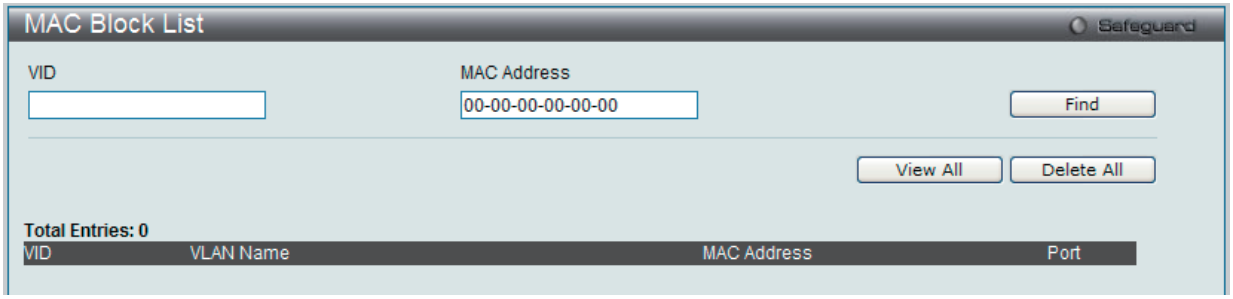


図 9-9　MAC Block List 画面

以下の項目を使用して、設定または編集を行います。

項目	説明
ID	検出または削除する VLAN の VLAN ID を入力します。
MAC Address	検出または削除する MAC アドレスを入力します。

VIP-MAC バインディング機能によりブロックされた未承認デバイスの検索

「VLAN ID」と「MAC Address」を入力し、「Find」ボタンをクリックします。

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。テーブル内のすべてのエントリを削除するためには、「Delete All」ボタンをクリックします。

エントリの表示

すべてのエントリを表示するためには、「View All」ボタンをクリックします。

Port Security（ポートセキュリティ）

「Port Security」フォルダには、「Port Security Port Settings」と「Port Security FDB Entries」メニューがあります。

Port Security Port Settings（ポートセキュリティの設定）

ポートやポート範囲を指定して、ダイナミックなMACアドレス学習をロックすることにより、MACアドレスフォワーディングテーブルへ、新しいソース MAC アドレスが追加されないよう設定することができます。「Admin State」のプルダウンメニューで「Enabled」を選択し、「Apply」ボタンをクリックするとポートをロックできます。

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

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

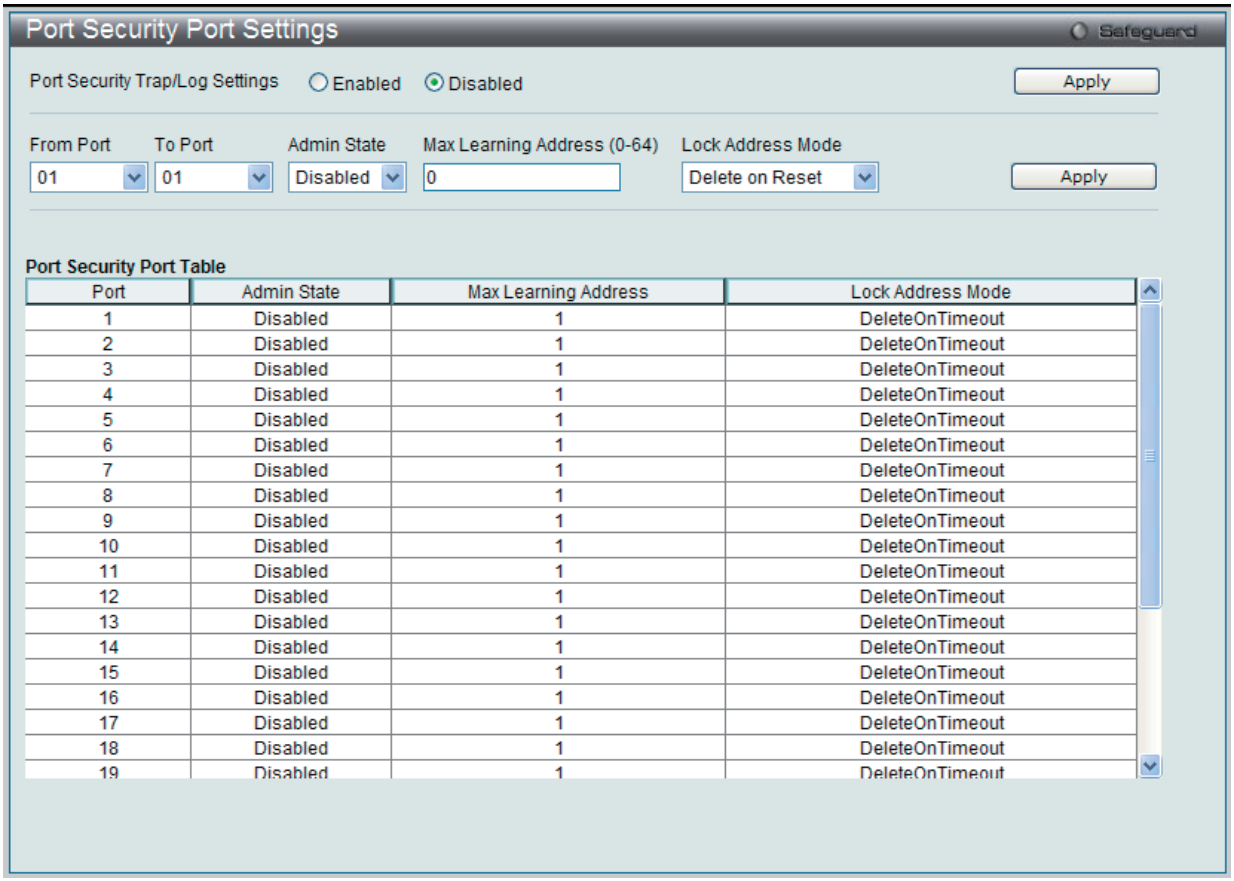


図 9-10　Port Security Port Settings 画面

本画面には次の項目があります。

項目	説明
Port Security Trap/Log Settings	スイッチのポートセキュリティトラップとログ設定を「Enabled」（有効）または「Disabled」（無効）にします。
From Port / To Port	ポートセキュリティ項目を表示するポート範囲を設定します。
Admin State	ポートセキュリティの有効 / 無効をプルダウンメニューで指定します。「Enabled」にすると、該当ポートは MAC アドレステーブルがロックされます。
Max Learning Address (0-64)	選択したスイッチとポートグループの MAC アドレス転送テーブルに保存できる MAC アドレス数を指定します。
Lock Address Mode	プルダウンメニューでスイッチの選択ポートグループに対して MAC アドレステーブルのロック動作の詳細を指定します。オプションは以下の通りです。 • Permanent – ロックされたアドレスは、エージングタイム経過後に削除されません。 • Delete On Timeout – ロックされたアドレスは、エージングタイム経過後に削除されます。 • Delete On Reset – ロックされたアドレスはリセットか再起動されるまで削除されません。

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。

Port Security FDB Entries（ポートセキュリティ FDB エントリ）

各ポートでポートロックエントリを削除します。

Security > Port Security > Port Security FDB 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。

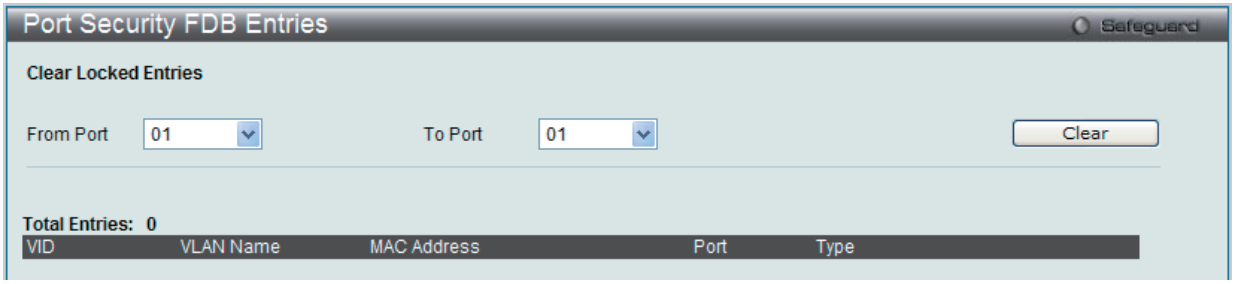


図 9-11　Port Security FDB Entries 画面

「From Port」および「To Port」でポート範囲を選択し、「Clear」ボタンをクリックしてエントリを削除します。

以下の情報を表示します。

項目	説明
VID	スイッチの転送データベーステーブルに登録されているエントリの VLAN ID です。
VLAN Name	スイッチの転送データベーステーブルに登録されているエントリの VLAN 名です。
MAC Address	スイッチの転送データベーステーブルに登録されているエントリの MAC アドレスです。
Port	MAC アドレスを記録しているポート番号です。
Type	転送データベーステーブルに登録されている MAC アドレスの種類です。「Permanent」または「DeleteOnReset」となっているエントリのみ削除できます。

802.1X（802.1X ポートベース / ホストベースアクセスコントロール）

IEEE 802.1X 標準規格は、クライアント・サーバベースのアクセスコントロールモデルの使用により、特定の LAN 上の様々な有線 / 無線デバイスへのアクセスを行う場合にユーザ認証を行うセキュリティ方式です。本方式は、ネットワークへアクセスするユーザを認証するために 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・サーバ間で中継することにより実現します。以下の図は基本的な EAPOL パケットの構成を示しています。

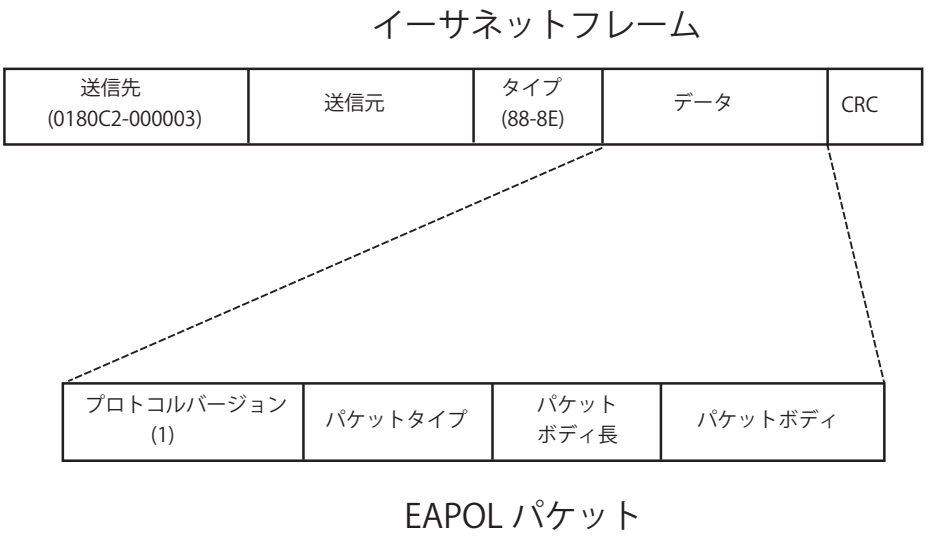


図 9-12　EAPOL パケット

本方法を使用すると、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、承認が与えられるまでの間指定ポート経由で送受信される唯一のトラフィックです。802.1X アクセスコントロール方式は 3 つの役割を持っており、それぞれがアクセスコントロールセキュリティ方法の作成、状態の保持および動作のために必要不可欠です。

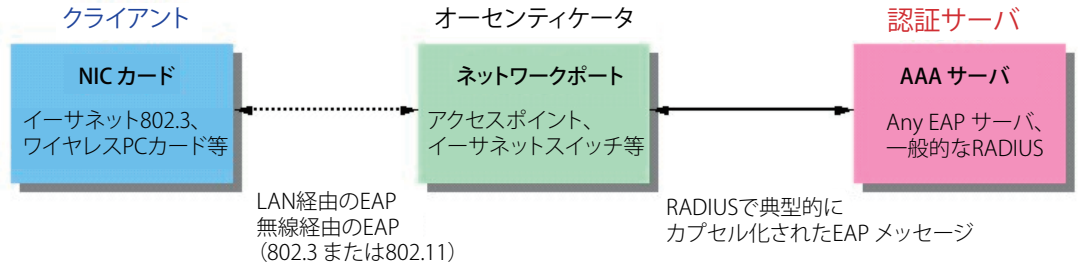


図 9-13　802.1X の 3 つの要素

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。認証サーバ上では RADIUS サーバプログラムを実行し、またそのサーバのデータがオーセンティケータ側（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受ける前に、認証サーバ（RADIUS）による認証を受ける必要があります。認証サーバは、RADIUS サーバとクライアントの間で EAPOL パケットを通じて信頼できる情報を交換し、そのクライアントの LAN やスイッチのサービスに対するアクセス許可の有無をスイッチに通知します。このように、認証サーバの役割は、ネットワークにアクセスを試みるクライアントの身元を保証することです。

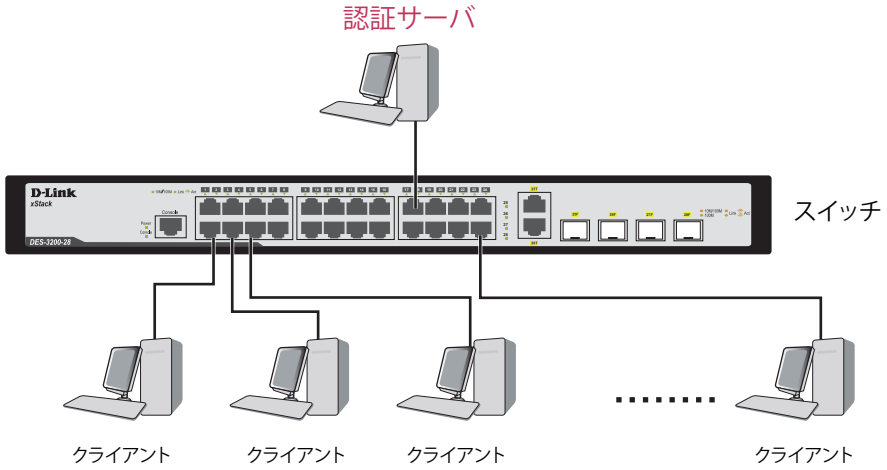


図 9-14　認証サーバ

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取り持つ、仲介の役割を果たします。802.1X を使用する場合、オーセンティケータサーバには 2 つの目的があります。 1 つ目の目的は、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 つ目の目的は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正しく設定するためには、以下の 3 つの手順を実行する必要があります。

1. 802.1X 機能を有効にします。（**Security > 802.1X > 802.1X Settings**）
2. 対象ポートに 802.1X の設定を行います。（**Security > 802.1X > 802.1X Settings**）
3. スイッチに RADIUS サーバの設定を行います。（**Security > 802.1X > Authentication RADIUS Server**）

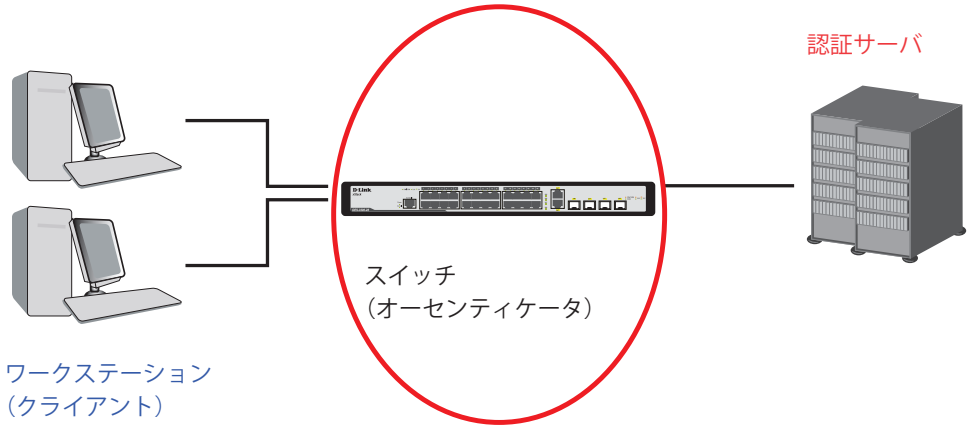


図 9-15　オーセンティケータ

クライアント

クライアントとは、簡単に言うと LAN やスイッチが提供するサービスへのアクセスを希望するワークステーションです。クライアントとなるワークステーションでは、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。Windows XP 使用の場合には、OS 内に既にそのようなソフトウェアが組み込まれています。それ以外の場合には、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、またスイッチからの要求に対しても応答します。

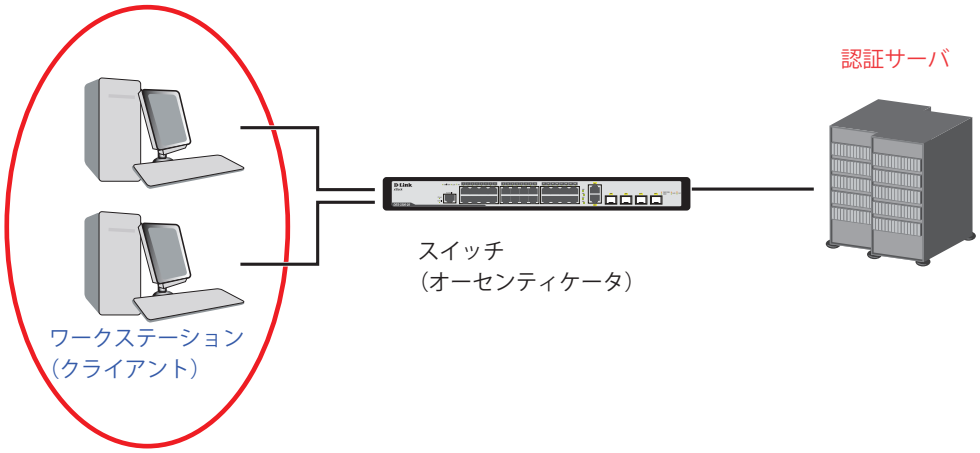


図 9-16　クライアント

認証プロセス

これらの 3 つの要素により、802.1X プロトコルはネットワークへのアクセスを試みるユーザの認証を安定的かつ安全に行います。認証に成功する前は、EAPOL トラフィックのみが特定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 の設定で MAC ベース（ホストベース）が指定されている場合は 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。D-Link が実装する 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。

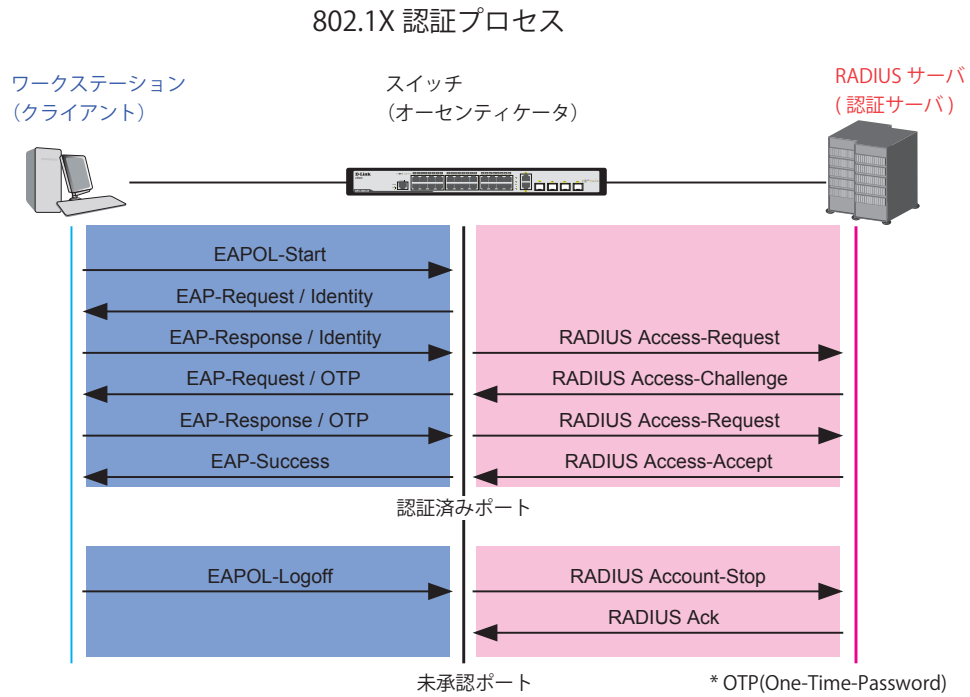


図 9-17　802.1X 認証プロセス

本スイッチの 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、1 人のユーザがリモートの RADIUS サーバにポートごとの認証をリクエストし、残りのユーザも同じポートをアクセスできるようにします。
2. MAC ベース（ホストベース）のアクセスコントロール
   本方式では、スイッチは自動的に各ポートに対して 16 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各 MAC アドレスの認証を行います。

802.1X ポートベース / 802.1X MAC ベース（ホストベース）でのネットワークアクセスコントロール

802.1X 開発の本来の目的は、LAN 上で Point to Point プロトコルの機能を利用することでした。インフラストラクチャのように単一の LAN セグメントが 2 個以上のデバイスを持たない場合、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あるアクティブなデバイスの接続を示すイベントや、アクティブなデバイスが非アクティブ状態に遷移することを示すイベントの検知を行います。これらのイベントをポートの認証状態の制御に利用し、ポートでの認証が行わない場合に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。

ポートベースのネットワークアクセスコントロール

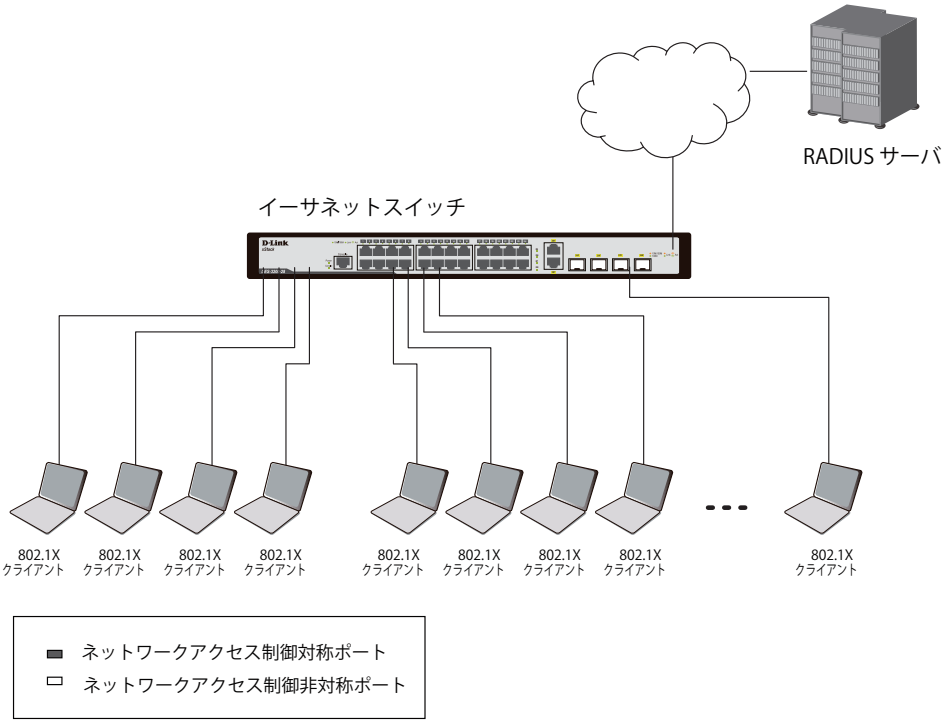


図 9-18　典型的なポートベース 802.1X ネットワークアクセスコントロールのネットワーク構成例

一度接続デバイスが認証に成功すると、ポートは Authorized（認証済み）状態になり、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となりません。そのため、ポートが 1 台以上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 に対して事実上アクセスを許可することになります。このような状態のセキュリティは明らかに脆弱であると言えます。

MAC ベース（ホストベース）のネットワークアクセスコントロール

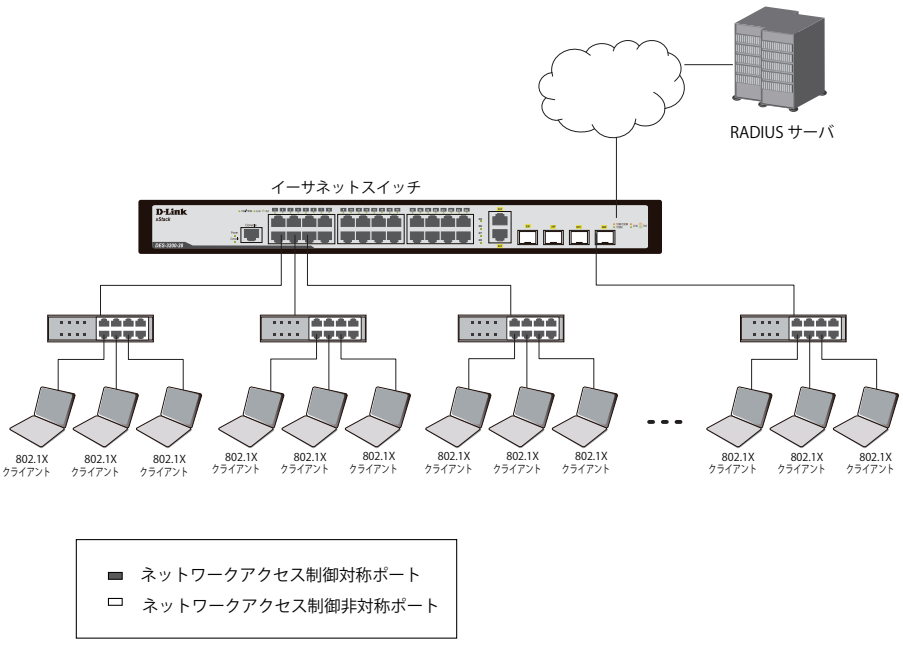


図 9-19　典型的な MAC ベース（ホストベース）802.1X ネットワークアクセスコントロールのネットワーク構成例

共有 LAN セグメント内で 802.1X を活用するためには、LAN へのアクセスを希望する各デバイスに「仮想」ポートを定義する必要があります。するとスイッチは共有 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、それら仮想ポートを EAPOL の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 と通信するための仮想ポートを確立します。

802.1X Settings（802.1X 設定）

802.1X 認証設定を行います。

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

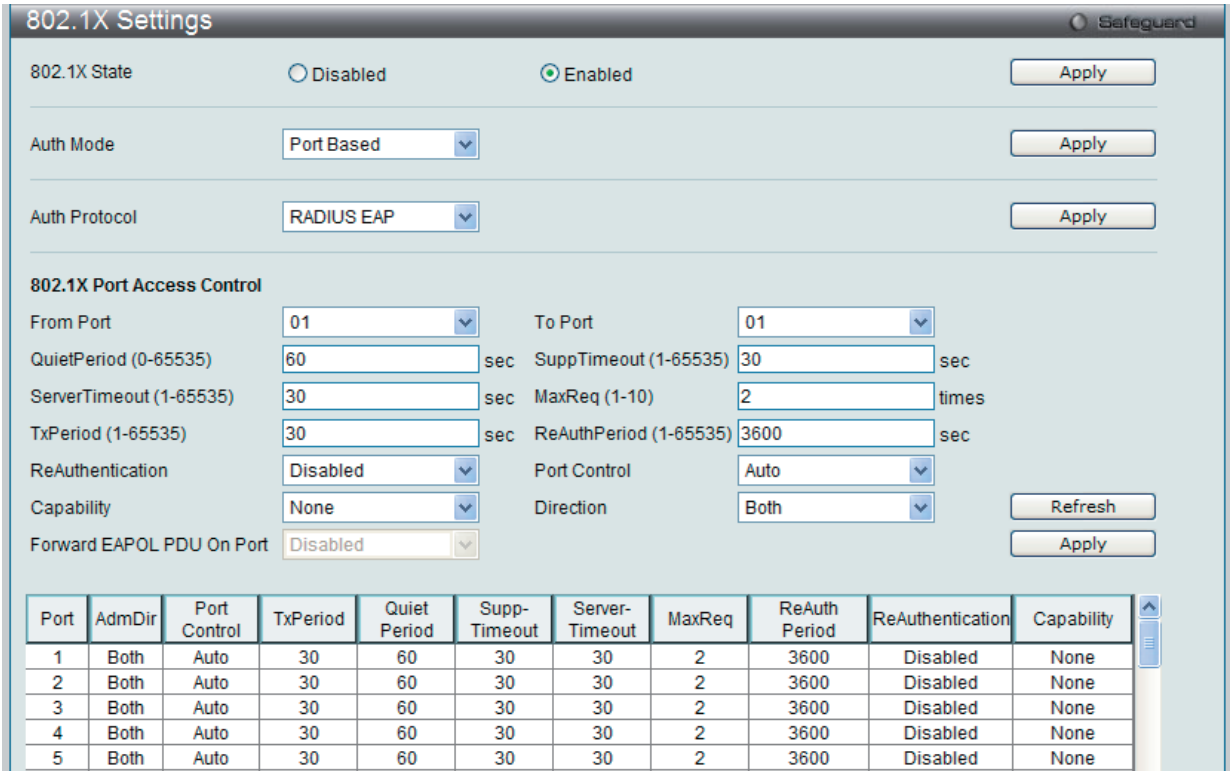


図 9-20　802.1X Settings 画面

「From Port」および「To Port」を使用して、ポート単位の設定を行います。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 認証を有効または無効にします。
Auth Mode	802.1X 認証モードを「Disabled」、「Port Based」、「MAC Based」から選択します。
Auth Protocol	認証プロトコルを「Local」または「RADIUS EAP」から選択します。
802.1 Port Access Control	
From Port / To Port	設定するポートまたはポート範囲を設定します。
QuietPeriod (0-65535)	クライアントと認証の交換を失敗した後スイッチが quiet 状態を維持する秒数を指定します。初期値は 60（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。
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。
MaxReq (1-10)	認証セッションがタイムアウトになるまでに EAP リクエストをクライアントに送信する最大回数を指定します。初期値は 2 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。
ReAuthPeriod (1-65535)	定期的クライアントの再認証の間隔を 0 以外で指定します。初期値は 3600（秒）です。
ReAuthentication	規則的に再認証を行うかを指定します。初期値は「Disabled」（無効）です。
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）
Capability	802.1X Authenticator 設定が各ポートに適用されます。 • Authenticator - ポートに設定を適用します。有効な場合、ネットワークアクセスするために認証を通過する必要があります。 • None - ポートへの 802.1X 機能は無効になります。
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。 • 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。
Forward EAPOL PDU On Port	スイッチのポートベースごとの EAPOL PDU 要求の再送を有効、または無効にします。

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。

802.1X User（802.1X ユーザ）

スイッチに異なるローカルユーザを設定します。

Security > 802.1X > 802.1X User の順にクリックし、以下の画面を表示します。

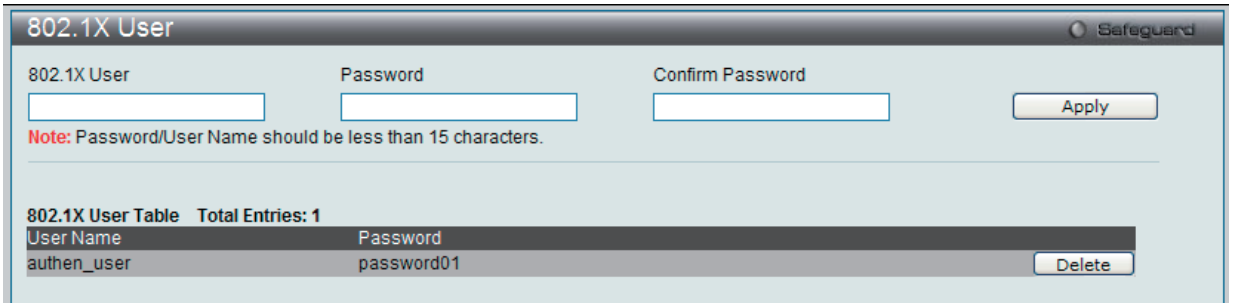


図 9-21　802.1X User 画面

「802.1X User」（ユーザ名）、「Password」（パスワード）および「Confirm Password」（確認用パスワード）を入力します。ローカルユーザの設定が完了すると、同じ画面に 802.1X User Table が表示されます。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。

Authentication RADIUS Server（認証 RADIUS サーバの設定）

RADIUS サーバによって集約したユーザ管理や Sniffing やハッカーからの保護が可能になります。

Security > 802.1X > Authentication RADIUS Server をクリックし、以下の画面を表示します。

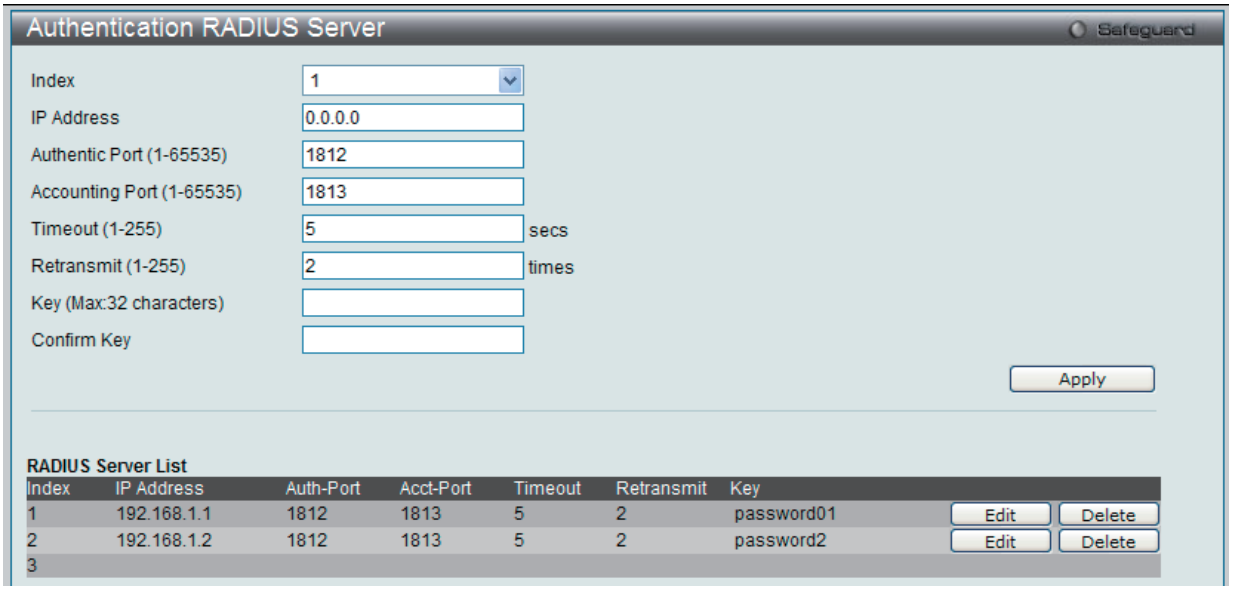


図 9-22　Authentication RADIUS Server 画面

この画面では以下の情報を確認、設定できます。

項目	説明
Index	設定する RADIUS サーバ（1-3）を指定します。
IP Address	RADIUS サーバの IP アドレスを入力します。
Authentic Port (1-65535)	スイッチと RADIUS サーバ間で RADIUS データを通信するために使用する RADIUS 認証サーバの UDP ポートを指定します。初期値は 1812 です。
Accounting Port (1-65535)	スイッチと RADIUS サーバ間で RADIUS アカウンティング統計情報を通信するために使用する RADIUS アカウントサーバの UDP ポートを指定します。初期値は 1813 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 です。
Retransmit (1-255)	RADIUS サーバの再転送間隔（秒）を設定します。初期値は 2 です。
Key (Max. 32 characters)	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
Confirm Key	確認のために上記を再度入力します。

認証 RADIUS サーバの設定

1. 項目設定を、「Apply」ボタンをクリックします。

2. 「RADIUS Server List」にエントリが表示されます。

エントリの編集

1. 編集するエントリの「Edit」ボタンをクリックすると、画面に現在の設定が表示されます。

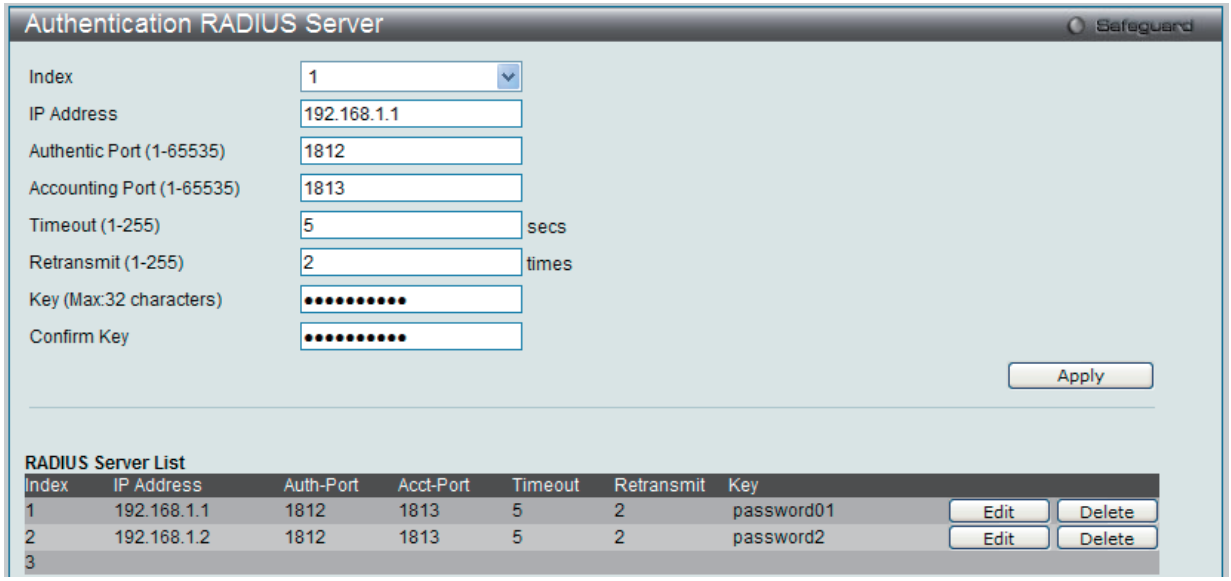


図 9-23　Authentication RADIUS Server 画面 - Edit

2. 項目設定後、「Apply」ボタンをクリックします。

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。

Guest VLAN（ゲスト VLAN の設定）

802.1X セキュリティが有効であるネットワークでは、Windows 98 やそれより以前の OS が動作するコンピュータのように適切な 802.1X ソフトウェアの欠落や互換性のないデバイス、またはゲストが限定した権限でネットワークに接続するために 802.1X をサポートしていないデバイスにも限られた範囲でアクセスできる必要があります。本スイッチは、802.1X ゲスト VLAN 機能を搭載しています。この VLAN には制限付きのアクセス権があり、他の VLAN とは分かれています。

802.1X ゲスト VLAN を実行するためには、はじめにネットワークに制限付き 802.1X ゲスト VLAN を作成し、この VLAN を有効にします。次に管理者は、ゲスト VLAN 内のスイッチにアクセスするゲストアカウントを作成します。スイッチへはじめてエントリする際には、スイッチにアクセスするクライアントは、リモート RADIUS サーバまたはフル操作が可能な VLAN 内に設置されているスイッチのローカル認証により認証される必要があります。認証され Authenticator が VLAN プレースメント情報を処理した場合、クライアントはフル操作が可能なターゲット VLAN にアクセスを許可され、通常のスイッチ機能がクライアントにサービスを開始します。Authenticator がターゲットの VLAN プレースメント情報を持たない場合、クライアントは元の VLAN に戻されます。クライアントが Authenticator によって認証を拒否されたら、制限付き権限を持つゲスト VLAN に置かれます。以下でゲスト VLAN プロセスについて説明しています。

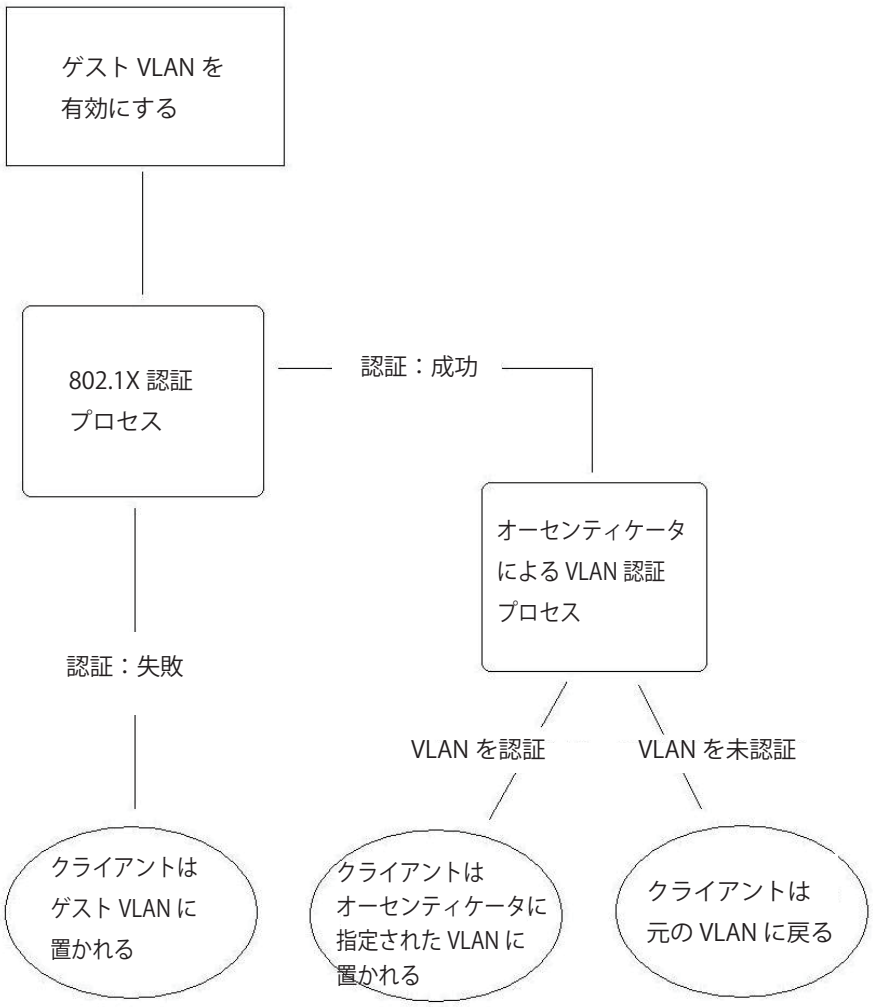


図 9-24　ゲスト VLAN 認証プロセス画面

ゲスト VLAN を使用する場合の制限事項

1. ゲスト VLAN をサポートしているポートは、GVRP を有効にすることはできません。同様に GVRP が有効な場合、ゲスト VLAN は使用できません。
2. ポートは同時にゲスト VLAN とスタティック VLAN のメンバになることはできません。
3. 一度クライアントがターゲット VLAN に許可されると、ゲスト VLAN にアクセスすることはできません。
4. ポートがマルチ VLAN のメンバである場合、ゲスト VLAN のメンバになることはできません。

Security > Guest VLAN の順にクリックし、以下の設定画面を表示します。

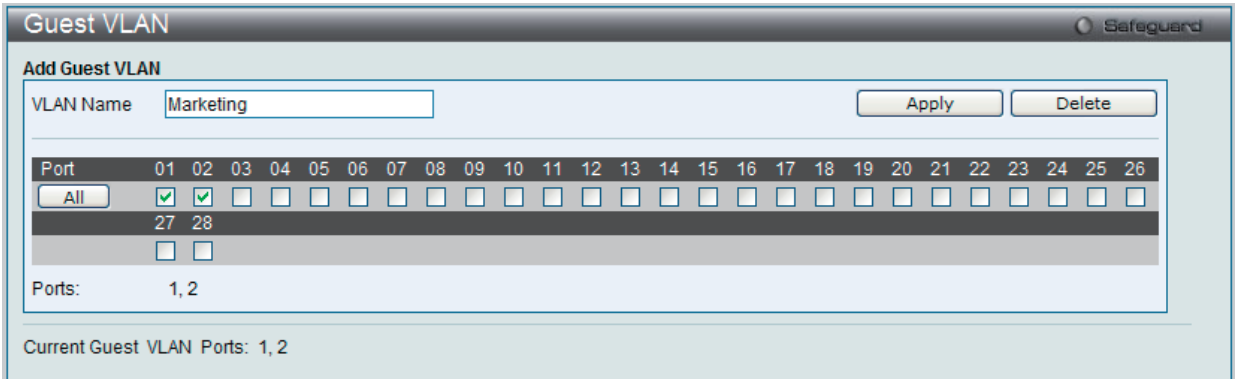


図 9-25　Guest VLAN 画面

注意　802.1X ゲスト VLAN を設定するためには、ここでゲスト VLAN ステータスを有効にできる VLAN をあらかじめ設定しておく必要があります。

以下の項目によりゲスト VLAN を有効にすることができます。

項目	説明
VLAN Name	802.1X ゲスト VLAN にする定義済みの VLAN 名を入力します。
Port	802.1X ゲスト VLAN を有効にするポートを設定します。「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。

ゲスト VLAN 設定

1. 「VLAN Name」に VLAN 名を入力し、ゲスト VLAN を有効にするポートを選択します。

2. 「Apply」ボタンをクリックし、入力したゲスト 802.1X VLAN を実行します。正しく設定されるとゲスト VLAN 名と対象のポートが画面の下部に表示されます。

エントリの削除

1. 削除する VLAN 名を「VLAN Name」に入力し、「Delete」ボタンをクリックします。

Initialize Port(s)（ポートの初期化）

既存の 802.1X ポートベースと MAC ベース設定が表示されます。以下の画面で表示および設定をします。

ポートベース 802.1X ポートの初期化

802.1X のポートを初期化するためには、はじめに「802.1X Settings」画面の「Auth Mode」で「Port Based」を選択しておく必要があります。

Security > 802.1X > Initialize Port(s) の順にクリックし、以下の画面を表示します。

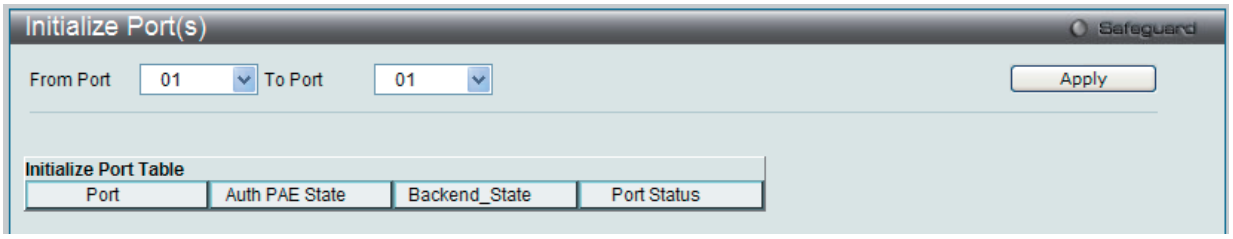


図 9-26　Initialize Port(s)（ポートベース 802.1X）画面

ここではポートまたはポート範囲の初期化を行います。画面の下部の「Initialize Port Table」はポートの現在のステータスを表示します。
ポートを初期化するためには、「From Port」および「To Port」でポート範囲を選択します。「Apply」ボタンをクリックすると、初期化を開始します。

MAC ベース 802.1X ポートの初期化

802.1X の MAC ベース側のポートを初期化するためには、はじめに「802.1X Settings」画面の「Auth Mode」で「MAC Based」を選択しておく必要があります。

Security > 802.1X > Initialize Port(s) の順にクリックし、以下の画面を表示します。

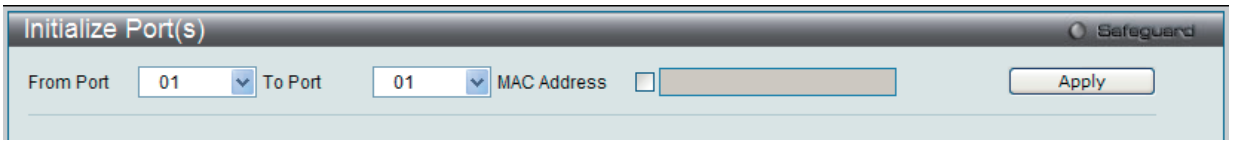


図 9-27　Initialize Port(s)（MAC ベース 802.1X）画面

ポートを初期化するためには、「From Port」および「To Port」でポート範囲を選択します。次に「MAC Address」欄にチェックを入れて、認証状態の初期化を行う MAC アドレスを入力します。「Apply」ボタンをクリックすると、初期化を開始します。

注意　ポートの初期化の前に「802.1X Settings」画面（**Security > 802.1X > 802.1X Settings**）で 802.1X をグローバルに有効にする必要があります。「Initialize Port Table」の情報は、「Port based 802.1X」または「Host based 802.1X」が有効でないと参照できません。

ポートの初期化画面では以下の情報が表示または設定できます。

項目	説明
From Port	初期化する開始ポートを選択します。
To Port	初期化する終了ポートを選択します。
Port	スイッチのポートを示す参照用項目です。
Auth PAE State	Authenticator PAE の状態を以下の項目のいずれかで表示します。: Initialize、Disconnected、Connecting、Authenticating、Authenticated、Aborting、Held、ForceAuth、ForceUnauth および N/A
Backend_State	Backend Authentication の状態を以下の項目のいずれかで表示します。: Request、Response、Success、Fail、Timeout、Idle、Initialize および N/A
Port Status	コントロールポートのステータスは Authorized、Unauthorized または N/A で表示します。
MAC Address	対応ポートに接続しているクライアントの認証 MAC アドレスです。

Reauthenticate Port(s)（ポートの再認証）

既存の 802.1X ポートベースと MAC ベースのポートを以下の 2 つ画面を使用して、表示および再認証設定をします。

ポートベース 802.1X ポートの再認証

ポートベースの 802.1X ポートを再認証するためには、はじめに「802.1X Settings」画面の「Auth Mode」で「Port Based」を選択しておく必要があります。

Security > 802.1X > Reauthenticate Port(s) の順でクリックし、以下の画面を表示します。

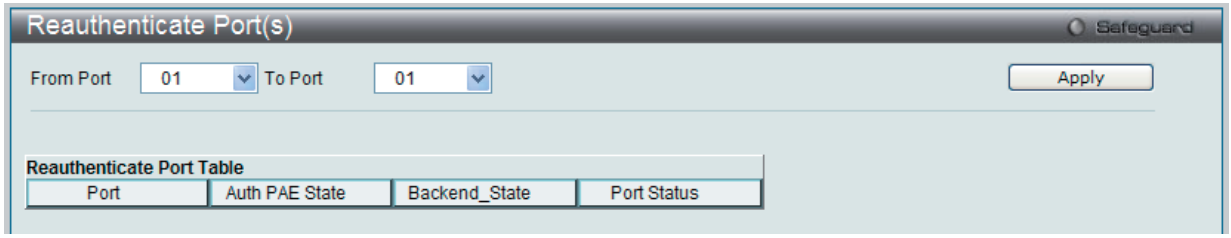


図 9-28　Reauthenticate Port(s)（ポートベース 802.1X）画面

「From Port」と「To Port」のプルダウンメニューでポートまたはポート範囲を選択し、「Apply」ボタンをクリックすることでポートの再認証を行います。「Apply」をクリックすると「Reauthenticate Port Table」には再認証ポートの現在のステータスが表示されます。

注意　ポートの再認証の前に「802.1X Settings」画面（**Security > 802.1X > 802.1X Settings**）で 802.1X をグローバルに有効にする必要があります。「Reauthenticate Port(s)」画面の情報は、「Port based 802.1X」または「MAC based 802.1X」が有効でないと参照できません。

MAC ベース 802.1X ポートの再認証

MACベースの802.1Xのポートを再認証するためには、はじめに「802.1X Settings」画面の「Auth Mode」で「MAC Based」を選択しておく必要があります。

Security > 802.1X > Reauthenticate Port(s) の順でクリックし、以下の画面を表示します。

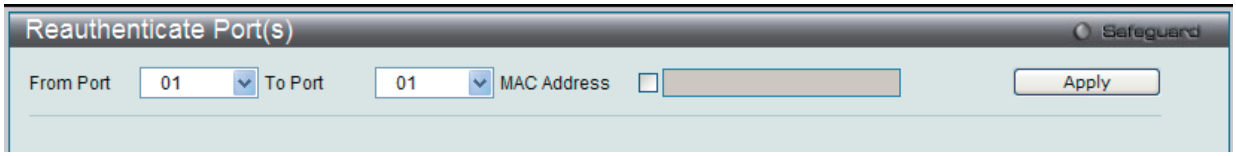


図 9-29　Reauthenticate Port(s)（MAC ベース 802.1X）画面

「From Port」と「To Port」のプルダウンメニューでポートまたはポート範囲を選択し、「Apply」ボタンをクリックすることでポートの再認証を行います。MAC アドレスを編集するためには、「MAC Address」をチェックし、隣接する欄に再認証する MAC アドレスを入力します。「Apply」ボタンをクリックすることでポートの再認証を行います。

ポートの再認証画面では以下の情報が表示または設定できます。

項目	説明
From Port	再認証する開始ポートを選択します。
To Port	再認証する終了ポートを選択します。
MAC Address	対応ポートに接続しているスイッチの MAC アドレスです
Auth PAE State	Authenticator PAE の状態を以下の項目のいずれかで表示します。: Initialize、Disconnected、Connecting、Authenticating、Authenticated、Aborting、Held、ForceAuth、ForceUnauth および N/A
Backend State	Backend Authentication の状態を以下の項目のいずれかで表示します。: Request、Response、Success、Fail、Timeout、Idle、Initialize および N/A
Port Status	コントロールポートのステータスは Authorized、Unauthorized または N/A で表示します。

SSL Settings（Secure Socket Layer の設定）

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、認証セッションに使用する厳密な暗号パラメータ、特定の暗号化アルゴリズムおよびキー長を決定する、暗号スイートと呼ばれるセキュリティ文字列により実現しています。SSL は、以下の 3 つの段階で構成されます。

1. 鍵交換
   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（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。本レベルは、鍵を交換して適合する相手を探し、暗号化のネゴシエーションを行うまでの認証を行って、次のレベルに進むというクライアント、ホスト間の最初のプロセスとなります。
2. 暗号化
   暗号スイートの次の段階は、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 – スイッチは 2 種類のストリーム暗号に対応します。1 つは 40 ビット鍵での RC4、もう 1 つは 128 ビット鍵での RC4 です。これらの鍵はメッセージの暗号化に使用され、最適な使用の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。
   - CRC ブロック暗号 – CBC（Cipher Block Chaining : 暗号ブロック連鎖）とは、前に暗号化したブロックの暗号文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）で定義する 3 DES EDE 暗号化コードをサポートし、暗号文を生成します。
3. ハッシュアルゴリズム
   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で暗号化され、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）の 2 種類のハッシュアルゴリズムをサポートします。

これら 3 つのパラメータは、スイッチ上での 4 つの選択肢として独自に組み合わされ、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します。暗号スイートの中から 1 つ、または複数を組み合わせて実行することができますが、選択する暗号スイートによりセキュリティレベルや安全な接続時のパフォーマンスは変化します。暗号スイートに含まれる情報はスイッチには存在していないため、証明書と呼ばれるファイルを第三者機関からダウンロードする必要があります。この証明書ファイルがないと本機能をスイッチ上で実行することができません。証明書ファイルは、TFTP サーバを使用してスイッチにダウンロードできます。本スイッチは、SSLv3 および TLSv1 をサポートしています。SSL の他のバージョンは本スイッチとは互換性がないおそれがあり、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場合があります。

証明書のダウンロード (Download Certificate)

本画面では、SSL を使用するための証明書ファイルを TFTP サーバからダウンロードします。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、所有者の情報や認証のための鍵や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、サーバとクライアントが一致した証明書ファイルを持つ必要があります。スイッチは、拡張子 ".der" を持つ証明書のみをサポートします。スイッチは証明書が既にロードされている形で発送されますが、ユーザの環境によっては、さらにダウンロードが必要になる場合があります。

暗号スイート

「SSL Configuration Settings」画面では、ネットワークマネージャが SSL を有効にしてスイッチに暗号スイートを設定できます。暗号スイートは認証セッションに使用する、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文字列です。スイッチは SSL 機能のための 4 つの暗号スイートを持ち、初期設定ではすべてを有効にしていますが、特定の暗号スイートのみ有効にして、他のものを無効にすることも可能です。

SSL 機能が有効になると、Web の使用はできなくなります。SSL 機能を使用しながら Web ベースの管理を行うためには、Web ブラウザが SSL 暗号化をサポートし、https:// で始まる URL を使用しなければなりません。（例 : https://10.90.90.90）これを守らないと、エラーが発生し、Web ベースの管理機能にアクセスできなくなります。

Security > SSL 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。

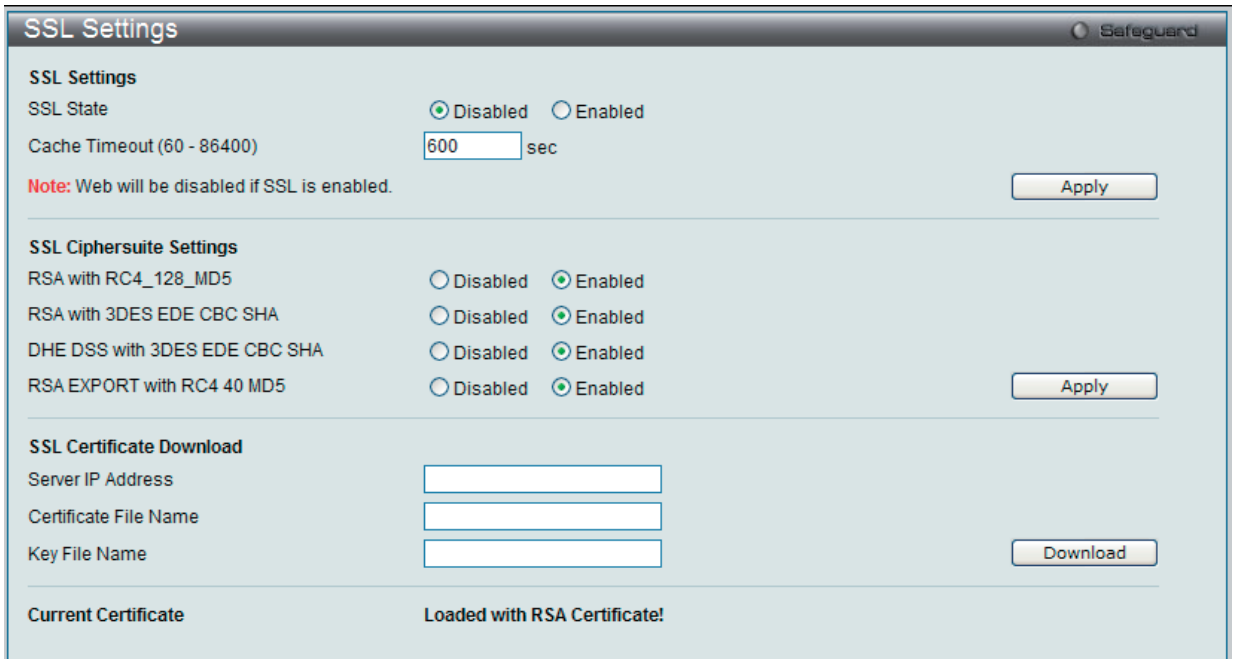


図 9-30　SSL Settings 画面

SSL 機能の設定

「SSL Settings」セクションの項目を設定し、「Apply」ボタンをクリックします。

SSL 暗号スイート機能の設定

「SSL Ciphersuite Settings」セクションの項目を設定し、「Apply」ボタンをクリックします。

SSL 証明書のダウンロード

「SSL Certificate Download」セクションの項目を設定し、「Download」ボタンをクリックします。

項目	説明
SSL Settings	
SSL State	スイッチの SSL の「Enabled」（有効）、「Disabled」（無効）を指定します。初期値は「Disabled」です。
Cache Timeout (60-86400)	クライアントとホストの間の SSL による新しい鍵交換の間隔を指定します。クライアントとホストが鍵交換をすると常に新しい SSL セッションが確立します。この値を長くすると SSL セッションによる特定のホストとの再接続には主鍵が再利用されます。それためネゴシエーション処理は速くなります。初期値は 600（秒）です。
SSL Ciphersuite Settings	
RSA with RC4_128_MD5	この暗号スイートは RSA key exchange、stream cipher C4（128-bit keys）、MD5 Hash Algorithm の組み合わせです。ラジオボタンで暗号スイートを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
RSA with 3DES EDE CBC SHA	この暗号スイートは RSA key exchange、CBC Block Cipher 3DES_EDE encryption、SHA Hash Algorithm の組み合わせです。ラジオボタンで暗号スイートを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
DHE DSS with 3DES EDE CBC SHA	この暗号スイートは DSA Diffie Hellman key exchange、CBC Block Cipher 3DES_EDE encryption、SHA Hash Algorithm の組み合わせです。ラジオボタンで暗号スイートを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
RSA EXPORT with RC4 40 MD5	この暗号スイートは RSA Export key exchange、stream cipher RC4（40-bit keys）、MD5 Hash Algorithm の組み合わせです。ラジオボタンで暗号スイートを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
SSL Certificate Download	
Server IP Address	証明書のファイルがある TFTP サーバの IP アドレスを指定します。
Certificate File Name	ダウンロードする証明書のパスとファイル名を指定します。ファイルには拡張子 ".der" が必要です。（例 c:/cert.der）
Key File Name	ダウンロードする鍵ファイルのパスとファイル名を指定します。ファイルには拡張子 ".der" が必要です。（例 c:/pkey.der）

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　SSL 機能が有効になると Web ベースマネージメントは無効になります。再度本スイッチにログオンするには URL の最初を https:// で始まるアドレスを Web ブラウザのアドレスに指定してもエラーになり、認証はされません。

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. **Configuration > 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 Settings（SSH サーバ設定）

本画面は SSH サーバの設定および設定内容の確認に使用します。

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

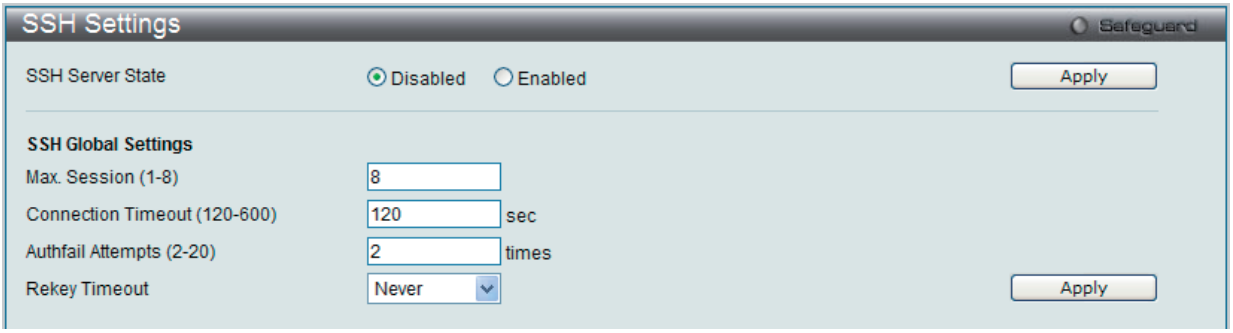


図 9-31　SSH Settings 画面

以下の項目を使用して、SSH サーバの設定を行います。

項目	説明
SSH Server State	スイッチ上で SSH 機能を「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Disabled」です。
Max. Session (1-8)	同時にスイッチに接続できる数を 1 から 8 の数字を設定します。初期値は 8 です。
Connection Timeout (120-600)	接続のタイムアウト時間を指定します。120 から 600（秒）が指定できます。初期値は 120（秒）です。
Authfail Attempts (2-20)	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。2 から 20 が指定できます。初期値は 2 です。
Rekey Timeout	スイッチが SSH 鍵の再交換を行う間隔をプルダウンメニューから選択します。「Never」、「10 min」、「30 min」、「60 min」です。初期値は「Never」（鍵再交換を行わない）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。

SSH Authmode and Algorithm Settings（SSH 認証モードとアルゴリズム設定）

認証および暗号化に使用する SSH アルゴリズムの種類を設定します。アルゴリズムは 3 つのカテゴリに分けてリスト表示され、各アルゴリズムは対応するチェックボックスを使用して有効、無効に設定できます。すべてのアルゴリズムは初期値で有効です。

Security > SSH > SSH Authmode and Algorithm 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。

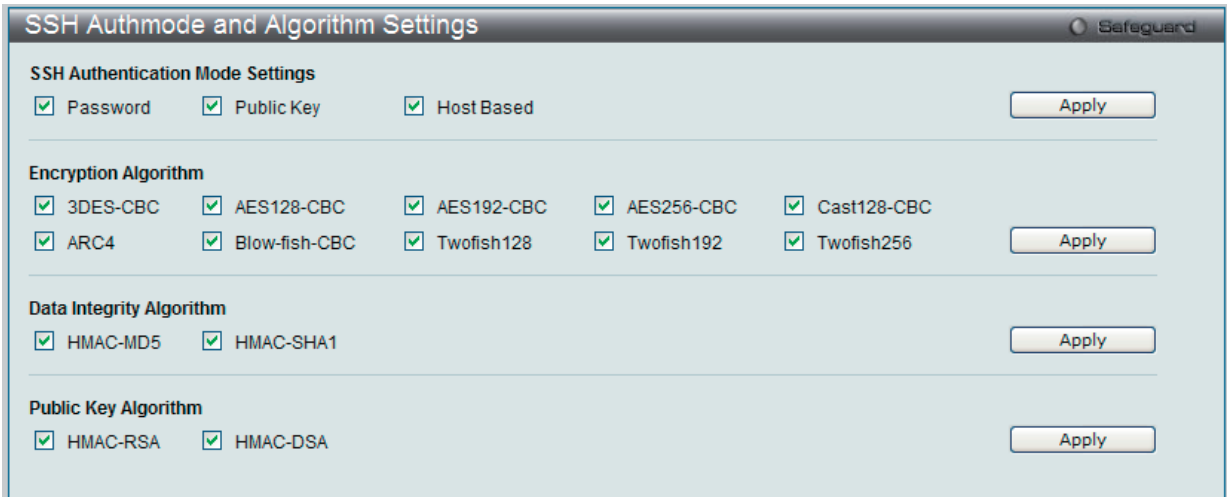


図 9-32　SSH Authmode and Algorithm Settings 画面

以下のアルゴリズムが設定できます。

項目	説明
SSH Authentication Mode Settings	
Password	スイッチにおける認証にローカルに設定したパスワードを使用する場合に「Enabled」（有効）にします。初期値は「Enabled」です。
Public Key	スイッチにおける認証に SSH サーバに設定した公開鍵を使用する場合に「Enabled」（有効）にします。初期値は「Enabled」です。
Host Based	認証にホストコンピュータを使用する場合に「Enabled」（有効）にします。本項目は SSH 認証機能を必要とする Linux ユーザ向けに設定されます。ホストコンピュータには SSH プログラムがインストールされ、Linux OS が起動している必要があります。初期値は「Enabled」です。
Encryption Algorithm	
3DES-CBC	CBC 方式で 3DES 暗号化アルゴリズムを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
Blow-fish-CBC	CBC 方式で Blowfish 暗号化アルゴリズムを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
AES128-CBC	CBC 方式で AES128 暗号化アルゴリズムを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
AES192-CBC	CBC 方式で AES192 暗号化アルゴリズムを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
AES256-CBC	CBC 方式で AES256 暗号化アルゴリズムを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
ARC4	ARC4 暗号化アルゴリズムを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
Cast128-CBC	CBC 方式で Cast128 暗号化アルゴリズムを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
Twofish128	Twofish128 暗号化アルゴリズムを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
Twofish192	Twofish192 暗号化アルゴリズムを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
Twofish256	Twofish256 暗号化アルゴリズムを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
Data Integrity Algorithm	
HMAC-SHA1	SHA1（セキュアハッシュ）暗号化アルゴリズムを使用した HMAC メカニズムを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
HMAC-MD5	MD5（メッセージダイジェスト）暗号化アルゴリズムを使用した HMAC メカニズムを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
Public Key Algorithm	
HMAC-RSA	RSA 暗号化アルゴリズムを使用した HMAC メカニズムを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
HMAC-DSA	DSA（デジタル署名）暗号化アルゴリズムを使用した HMAC メカニズムを「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」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。

SSH User Authentication Lists（SSH ユーザ認証モード）

SSH を使用してスイッチにアクセスを行うユーザの設定を行います。

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

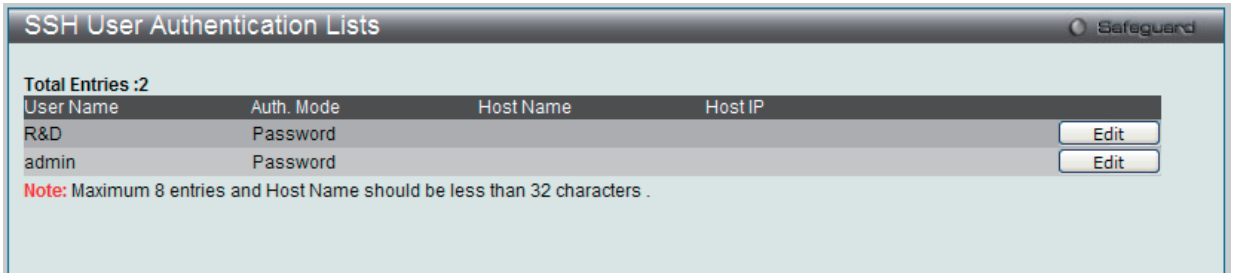


図 9-33　SSH User Authentication Lists 画面

上記画面例のユーザアカウントは **Configuration > User Accounts** で既に設定されているものとします。SSH ユーザとしての項目を設定するためには、ユーザアカウントをあらかじめ登録しておく必要があります。

SSH ユーザの設定

SSH ユーザとしての項目を設定するためには、本画面で対応するエントリの「Edit」ボタンをクリックし、以下の画面を表示します。

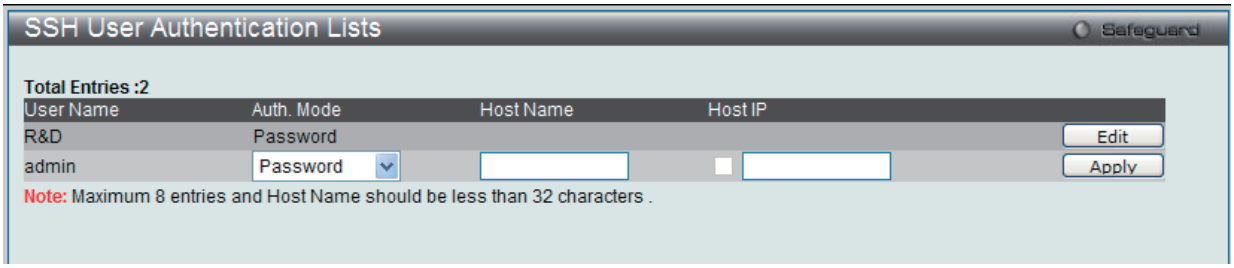


図 9-34　SSH User Authentication Lists 画面 - Edit

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 15 文字までの半角英数字で指定します。本ユーザ名はスイッチにユーザアカウントとして登録済みである必要があります。
Auth. Mode	スイッチにアクセスを試みるユーザの認証モードを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。 - Host Name - リモート SSH ユーザを識別する 31 文字までの半角英数字を入力します。 - Host IP - SSH ユーザの IP アドレスを入力します。 • 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。
Host Name	リモート SSH ユーザを識別する 31 文字までの半角英数字を入力します。本項目は「Auth. Mode」で「Host Based」を選択した場合のみ入力が必要です。
Host IP	SSH ユーザの IP アドレスを入力します。本項目は「Auth. Mode」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。

注意　SSH User Authentication Mode の項目を設定するためには、事前にユーザアカウントを登録しておく必要があります。スイッチのローカルユーザアカウント設定に関する詳しい情報に関しては、本マニュアルの「第 6 章 Configuration（スイッチの主な設定）」の 49 ページの「User Accounts（ユーザアカウントの設定）」を参照してください。

Access Authentication Control（アクセス認証コントロール）

TACACS/ XTACACS/ TACACS+/ RADIUS コマンドは、TACACS/ XTACACS/ TACACS+ /RADIUS プロトコルを使用してスイッチへの安全なアクセスを可能にします。ユーザがスイッチへのログインや、管理者レベルの特権へのアクセスを行おうとする時、パスワードの入力を求められます。TACACS/ XTACACS/ TACACS+/ RADIUS 認証がスイッチで有効になると、スイッチは TACACS/ XTACACS/ TACACS+/ RADIUS サーバと連絡し、ユーザの確認をします。確認が行われたユーザは、スイッチへのアクセスを許可されます。

現在 TACACS セキュリティプロトコルには異なるエンティティを持つ 3 つのバージョンが存在します。本スイッチのソフトウェアは TACACS の以下のバージョンをサポートします。

•TACACS（Terminal Access Controller Access Control System）
　セキュリティのためのパスワードチェック、認証、およびユーザアクションの通知を、1 台またはそれ以上の集中型の TACACS サーバを使用して行います。パケットの送受信には UDP プロトコルを使用します。
• XTACACS（拡張型 TACACS）
　TACACS プロトコルの拡張版で、TACACS プロトコルより多種類の認証リクエストとレスポンスコードに対応します。パケットの送受信に UDP プロトコルを使用します。
• TACACS+（Terminal Access Controller Access Control System plus）
　ネットワークデバイスの認証のために詳細なアクセス制御を提供します。TACACS+ は、1 台またはそれ以上の集中型のサーバを経由して認証コマンドを使用することができます。TACACS+ プロトコルは、スイッチと TACACS+ デーモンの間のすべてのトラフィックを暗号化します。また、TCP プロトコルを使用して信頼性の高い伝達を行います。

TACACS/ XTACACS/ TACACS+/ RADIUS のセキュリティ機能が正常に動作するためには、スイッチ以外の認証サーバホストと呼ばれるデバイス上で認証用のユーザ名とパスワードを含む TACACS/ XTACACS/ TACACS+/ RADIUS サーバの設定を行う必要があります。スイッチがユーザにユーザ名とパスワードの要求を行う時、スイッチは TACACS/ XTACACS/ TACACS+/ RADIUS サーバにユーザ認証の問い合わせを行います。サーバは以下の 3 つのうちの 1 つの応答を返します。

• サーバは、ユーザ名とパスワードを認証し、ユーザにスイッチへの通常のアクセス権を与えます。
• サーバは、入力されたユーザ名とパスワードを受け付けず、スイッチへのアクセスを拒否します。
• サーバは、認証の問い合わせに応じません。この時点でスイッチはサーバからタイムアウトを受け取り、メソッドリスト中に設定された次の認証方法へと移行します。

本スイッチには TACACS、XTACACS、TACACS+、RADIUS の各プロトコル用に 4 つの認証サーバグループがあらかじめ組み込まれています。これらの認証サーバグループはスイッチにアクセスを試みるユーザの認証に使用されます。認証サーバグループ内に任意の順番で認証サーバホストを設定し、ユーザがスイッチへのアクセス権を取得する場合、1 番目の認証サーバホストに認証を依頼します。認証が行われなければ、リストの 2 番目のサーバホストに依頼し、以下同様の処理が続きます。実装されている認証サーバグループには、特定のプロトコルが動作するホストのみを登録できます。例えば TACACS 認証サーバグループは、TACACS 認証サーバホストのみを登録できます。

スイッチの管理者は、ユーザ定義のメソッドリストに 6 種類の異なる認証方法（TACACS/ XTACACS/ TACACS+/ RADIUS/ local/ none）を設定できます。これらの方法は、任意に並べ替えることが可能で、スイッチ上での通常のユーザ認証に使用されます。リストには最大 8 つの認証方法を登録できます。ユーザがスイッチにアクセスしようとすると、スイッチはリストの 1 番目の認証方法を選択して認証を行います。1 番目の方法で認証サーバホストを通過しても認証が返ってこなければ、スイッチはリストの次の方法を試みます。この手順は、認証が成功するか、拒否されるか、またはリストのすべての認証方法を試し終わるまで繰り返されます。

スイッチへのアクセス権を取得したユーザは、通常のアクセス権を与えられていることにご注意ください。管理者特権レベルの権利を取得するためには、ユーザは「Enable Admin」画面にアクセスし、スイッチに管理者により事前に設定されているパスワードの入力が必要になります。

注意 TACACS、XTACACS、TACACS+、RADIUS は独立したエンティティであり、互換性はありません。スイッチとサーバ間は、同じプロトコルを使用した全く同じ設定を行う必要があります。（例えば、スイッチに TACACS 認証を設定した場合、ホストサーバにも同様の設定を行います。）

Authentication Policy Settings（認証ポリシー設定）

管理者が定義するスイッチにアクセスするユーザのための認証ポリシーを有効にします。有効にすると、デバイスはログインメソッドリストをチェックし、ログイン時のユーザ認証に使用する認証方法を選択します。

Security > Access Authentication Control > Authentication Policy 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。

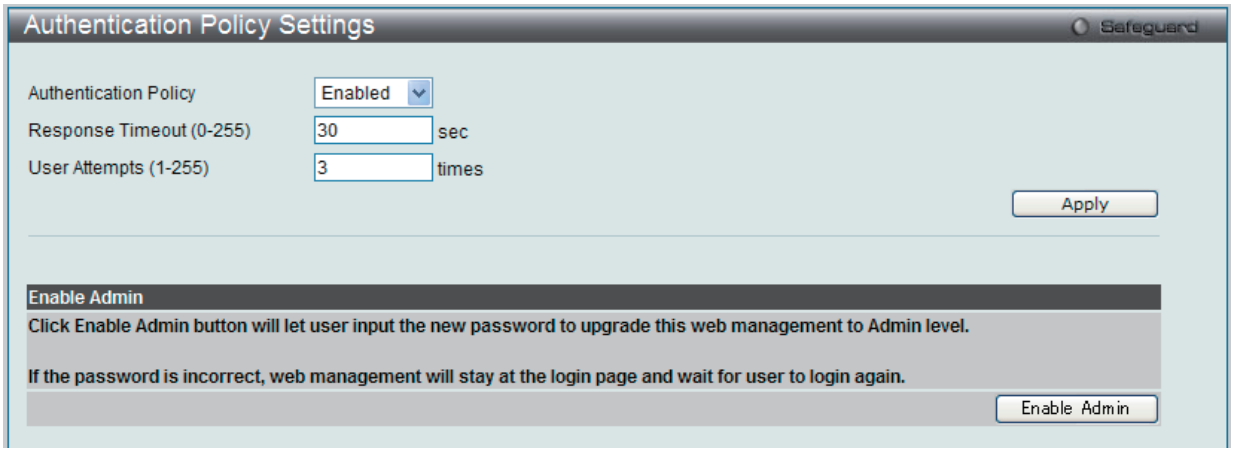


図 9-35　Authentication Policy Settings 画面

以下の項目を使用して設定を行います。

項目	説明
Authentication Policy	プルダウンメニューからスイッチの認証ポリシーの「Enabled」（有効）または「Disabled」（無効）を設定します。
Response Timeout (0 - 255)	ユーザからの認証のレスポンスに対するスイッチの待ち時間を指定します。0-255（秒）の範囲から指定します。初期値は 30（秒）です。
User Attempts (1 - 255)	ユーザが認証を試みることができる最大回数。指定回数認証に失敗すると、そのユーザはスイッチへのアクセスを拒否され、さらに認証を試みることができなくなります。CLI ユーザは、再度認証を行う前に 60 秒待つ必要があります。Telnet および Web ユーザはスイッチから切断されます。1–255 の範囲で指定します。初期値は 3（回）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。

「Enable Admin」ボタンをクリックすると、ユーザ認証ダイアログが表示されます。管理者レベルのユーザでログインします。
本ボタンは、管理者レベルでログインしている場合には表示されません。

Application Authentication Settings（アプリケーションの認証設定）

作成済みのメソッドリストを使用して、ユーザレベルおよび管理者レベル（Enable Admin）で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、Web）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。

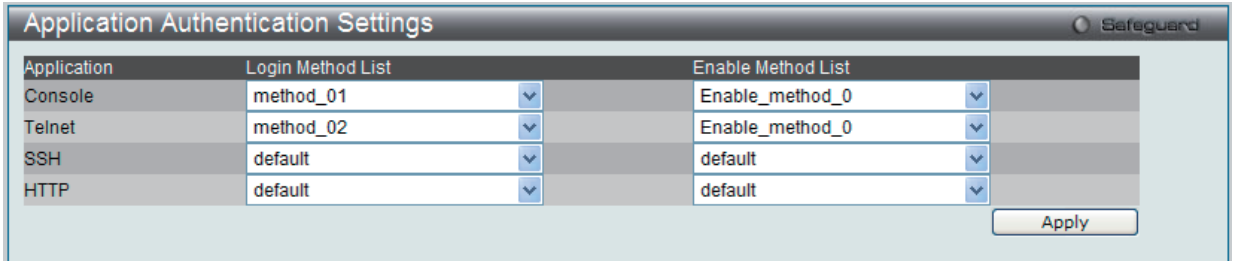


図 9-36　Application Authentication Settings 画面

以下の項目を使用して、設定を行います。

項目	説明
Application	スイッチ上の設定用アプリケーションをリスト表示しています。それぞれのアプリケーション（コンソール、Telnet、SSH、HTTP）を使用するユーザ認証用の「Login Method List」と「Enable Method List」を指定できます。
Login Method List	プルダウンメニューを使用し、登録済みのメソッドリストから、ユーザレベルの通常ログインを行うアプリケーションに適用するリストを選択します。初期設定のメソッドリスト、またはユーザ定義のメソッドリストを選択できます。詳細な情報は、後述の「Login Method Lists」画面を参照してください。
Enable Method List	プルダウンメニューを使用し、登録済みのメソッドリストから、ユーザレベルの通常ログインを行うアプリケーションに適用するリストを選択します。初期設定のメソッドリスト、またはユーザ定義のメソッドリストを選択できます。詳細な情報は、後述の「Enable Method Lists」画面を参照してください。

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 Server Group（認証サーバグループ）

スイッチに認証サーバグループの設定を行います。サーバグループとは、TACACS/ XTACACS/ TACACS+/ RADIUS のサーバホストを、ユーザ定義のメソッドリスト使用の認証カテゴリにグループ分けしたものです。プロトコルによって、または定義済みのサーバグループに組み込むことによりグループ分けを行います。スイッチには 4 つの認証サーバグループがあらかじめ組み込まれています。これらは削除することができませんが、内容の変更は可能です。1 つのグループにつき最大 8 個までの認証サーバホストを登録できます。

Security > Access Authentication Control > Authentication Server 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。

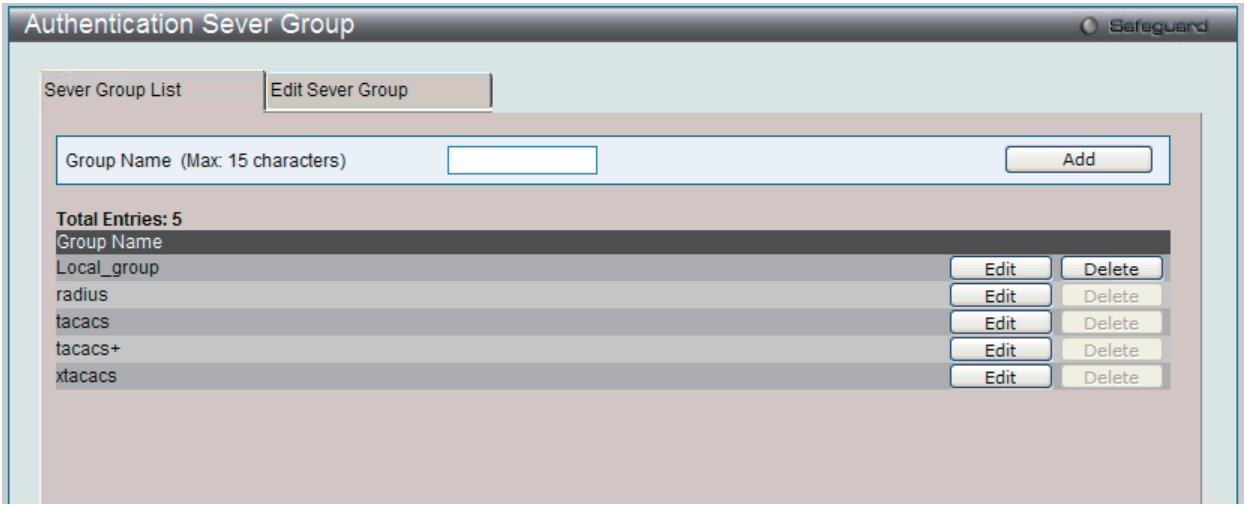


図 9-37　Authentication Server Group - Server Group List タブ画面

サーバグループの新規登録

「Server Group List」タブで「Group Name」に名前を入力し、「Add」ボタンをクリックします。

サーバグループの編集

編集するサーバグループの「Edit」ボタン（または「Edit Server Group」タブ）をクリックし、以下の画面を表示します。

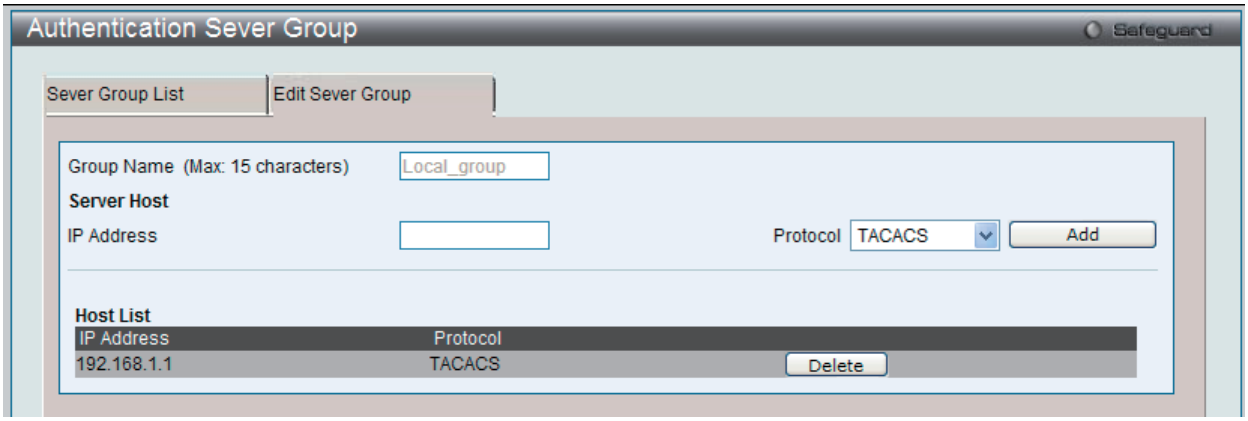


図 9-38　Authentication Server Group - Edit Server Group タブ画面 - Edit

Authentication Server のリストへの追加

1. 「Group Name」に名前、「IP Address」に IP アドレスを指定し、その IP アドレスを持つ認証サーバの Protocol を選択します。
2. 「Add」ボタンをクリックし、Authentication Server Host をグループに加えます。
3. 本タブの下部の Host List にエントリが表示されます。

注意　認証サーバホストをリストに追加する前に、「Authentication Server」画面にてホストの登録を行う必要があります。本機能を正しく動作させるためには、リモートの中央管理サーバ上でプロトコルを指定して認証サーバホストの設定を行う必要があります。

注意　あらかじめ組み込まれている 4 つのサーバグループには、同じ TACACS デーモンが起動されているサーバホストのみを入れることができます。TACACS/XTACACS/TACACS+ プロトコルは別のエンティティで、互換性はありません。

Authentication Server（認証サーバ）

スイッチに TACACS/ XTACACS/ TACACS+/ RADIUS セキュリティプロトコルに対応したユーザ定義の認証サーバホストを設定します。

ユーザが認証ポリシーを有効にしてスイッチにアクセスを試みると、スイッチはリモートホスト上の TACACS/ XTACACS/ TACACS+/ RADIUS サーバホストに認証パケットを送信します。すると TACACS/ XTACACS/ TACACS+/ RADIUS サーバホストはその要求を認証または拒否し、スイッチに適切なメッセージを返します。1 つの物理ホスト上で複数の認証プロトコルを動作させることは可能ですが、TACACS/ XTACACS/ TACACS+/ RADIUS は別のエンティティであり、互換性を持たないことに注意が必要です。サポート可能なサーバホストは最大 16 台です。

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

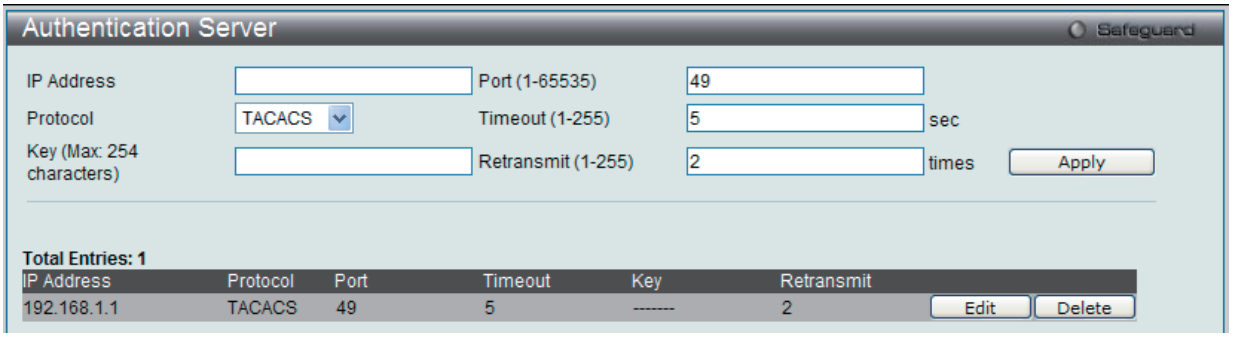


図 9-39　Authentication Server 画面

認証サーバホストを追加するためには、以下の項目を使用します。

項目	説明
IP Address	追加するリモートサーバホストの IP アドレス
Protocol	サーバホストで動作しているプロトコルを指定します。以下の一つを選ぶことができます。 • TACACS - ホストが TACACS プロトコルを使用している場合に選択します。 • XTACACS - ホストが XTACACS プロトコルを使用している場合に選択します。 • TACACS+ - ホストが TACACS+ プロトコルを使用している場合に選択します。 • RADIUS - ホストが RADIUS プロトコルを使用している場合に選択します。
Key (Max : 254 Characters)	TACACS+ と RADIUS サーバの場合に指定する共有キー。254 文字までの半角英数字を入力します。
Port (1-65535)	サーバホスト上で認証プロトコルに使用する仮想ポート番号。ポート番号の初期値は、TACACS/ XTACACS/ TACACS+ サーバの場合は 49、RADIUS サーバの場合は 1813 です。独自の番号を設定してセキュリティを向上することも可能です。
Timeout (1-255)	スイッチが、サーバホストからの認証リクエストへの応答を待つ時間（秒）。初期値は 5（秒）です。
Retransmit (1-255)	TACACS サーバからの応答がない場合に、デバイスが認証リクエストを再送する回数。初期値は 2 回です。

「Apply」ボタンをクリックしてサーバホストを追加します。

注意　1 つの物理ホスト上で複数の認証プロトコルを動作させることは可能ですが、TACACS/ XTACACS/ TACACS+ は個別のエンティティであり、互換性を持たないことに注意が必要です。

認証サーバの編集

1.　編集するエントリの「Edit」ボタンをクリックし、以下の画面を表示します。

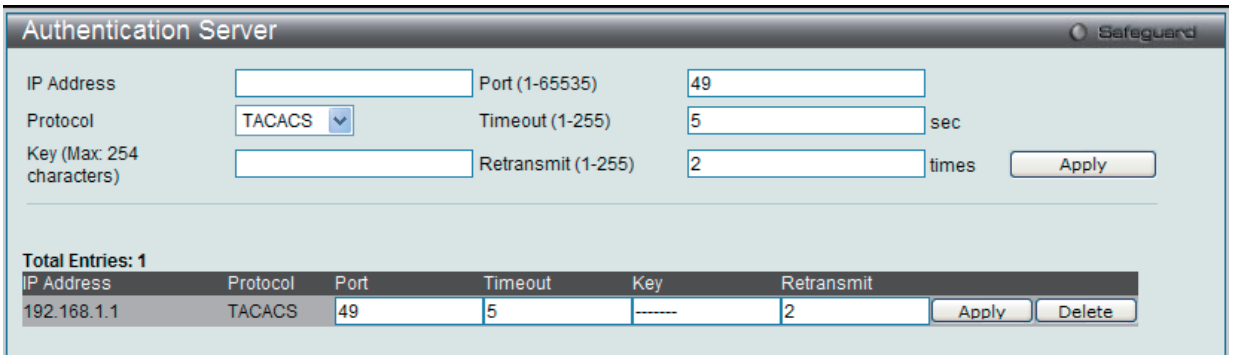


図 9-40　Authentication Server 画面 - Edit

2.　項目を編集し、「Apply」ボタンをクリックします。

認証サーバの削除

1.　削除するエントリの「Delete」ボタンをクリックします。

Login Method Lists（ログインメソッドリスト）

ユーザがスイッチにログインする際の認証方法を規定するユーザ定義または初期設定のログインメソッドリストを設定します。ここで設定した認証方法の順番が認証結果に影響します。例えば、ログインメソッドリストに TACACS-XTACACS-Local の順番で認証方法を指定すると、スイッチはまずサーバグループ内の 1 番目の TACACS ホストに認証リクエストを送信します。そのサーバホストから応答がない場合、2 番目の TACACS ホストに認証リクエストを送信します。このようにサーバグループ内のすべてのホストに順番に送信を試みても応答がない場合、スイッチは本メソッドリストの次の方法（XTACACS）を試します。それでも認証が行われなければ、スイッチ内に設定したローカルアカウントデータベースを使用して認証を行います。Local メソッドが使用される時、ユーザの権限はスイッチに設定されたローカルアカウントの権限に依存します。

これらの認証方法によって、認証に成功したユーザには「User」の権限のみが与えられます。ユーザが管理者レベルの権限を必要とするのであれば、「Enable Admin」画面にアクセスし、スイッチに管理者により事前に設定されているパスワードの入力が必要になります。詳細については、185 ページの「Authentication Policy Settings（認証ポリシー設定）」を参照してください。

Security > Access Authentication Control > Login Method Lists の順にメニューをクリックし、以下の画面を表示します。

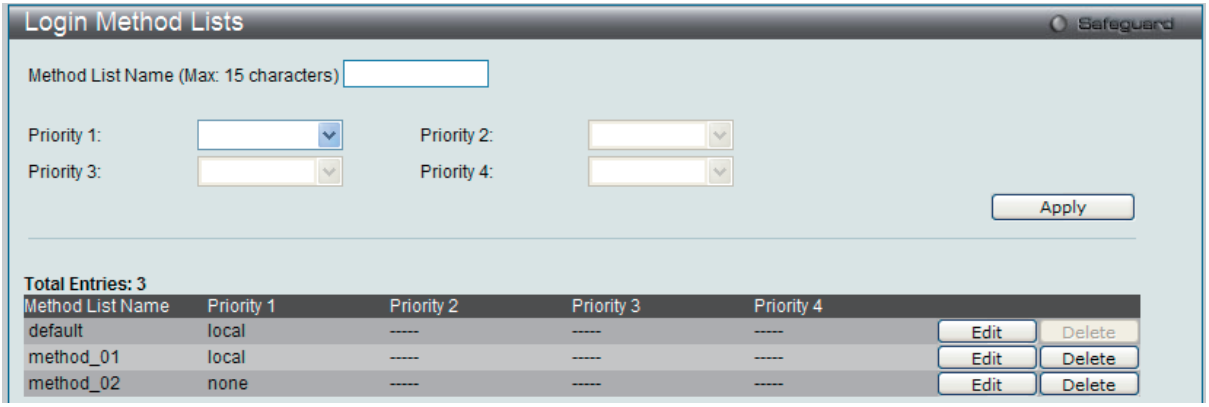


図 9-41　Login Method Lists 画面

スイッチには、あらかじめ削除できない Login Method List が登録されています。このリストの内容の変更は可能です。

Login Method List の新規登録

以下の項目を設定し、「Apply」ボタンをクリックします。

項目	説明
Method List Name	15 文字までの半角英数字でメソッドリスト名を入力します。
Priority 1, 2, 3, 4	本メソッドリストに追加する認証方法を最大 4 件まで指定します。 • tacacs – リモートの TACACS サーバから TACACS プロトコルを使用してユーザ認証を行います。 • xtacacs – リモートの XTACACS サーバから XTACACS プロトコルを使用してユーザ認証を行います。 • tacacs+ – リモートの TACACS+ サーバから TACACS+ プロトコルを使用してユーザ認証を行います。 • radius – リモートの RADIUS サーバから RADIUS プロトコルを使用してユーザ認証を行います。 • server_group – スイッチ上に設定したユーザ定義のサーバグループを使用してユーザ認証を行います。 • local – スイッチ上のローカルユーザアカウントデータベースを使用してユーザ認証を行います。 • none – スイッチへアクセスするための認証を行います。

Login Method List の変更

1. 対応する「Edit」ボタンをクリックし、以下の画面を表示します。

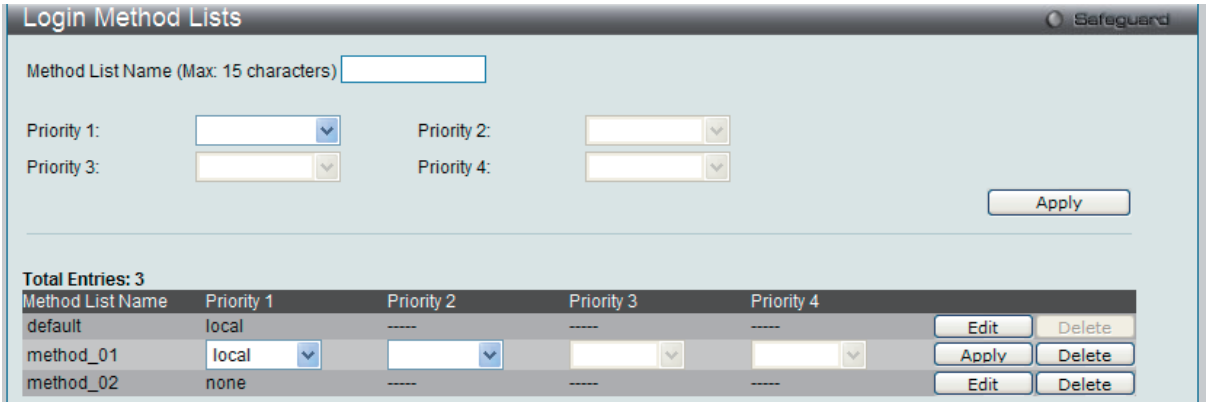


図 9-42　Login Method Lists 画面 - Edit

2. 項目を編集し、「Apply」ボタンをクリックします。

ユーザ定義の Login Method List の削除

1. 削除対象のエントリの行の「Delete」ボタンをクリックします。

Enable Method Lists（メソッドリストの有効化）

スイッチ上で認証メソッドを使用して、ユーザの権限をユーザレベルから管理者（Admin）レベルに上げる際に利用するメソッドリストの設定を行います。通常のユーザレベルの権限を取得したユーザが管理者特権を得るためには、管理者が定義した方法により認証を受ける必要があります。最大 8 件の Enable Method List が登録でき、そのうちの 1 つは default Enable メソッドリストになります。本 default Enable メソッドリストは内容の変更はできますが、削除はできません。

本メニューで定義した認証方法の順番が認証結果に影響します。例えば、ログインメソッドリストに TACACS-XTACACS-Local の順番で認証方法を指定した場合、スイッチはまずサーバグループ内の 1 番目の TACACS ホストに対して、認証リクエストを送信します。認証が確認できなければ、2 番目の TACACS ホストに認証リクエストを送信します。このようにサーバグループ内のすべてのホストに順番に送信を試みても応答がない場合、スイッチは本メソッドリスト中の次の方法（XTACACS）を試します。それでも認証が行われなければ、スイッチ内に設定したローカル Enable パスワードを使用してユーザの認証を行います。

以上のいずれかの方法で認証されたユーザは、「Admin」（管理者）権限を取得することができます。

注意 ローカル Enable パスワードの設定については 190 ページの「Local Enable Password Settings（ローカルユーザパスワード設定）」の項を参照してください。

Security > Access Authentication Control > Enable Method Lists の順にメニューをクリックし、以下の画面を表示します。

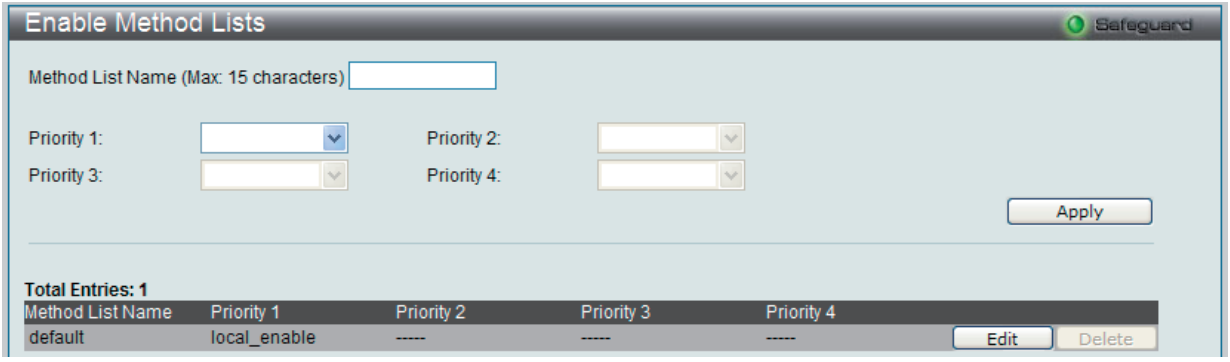


図 9-43　Enable Method Lists 画面

以下の項目を使用して、Enable Method List の設定を行います。入力後、「Apply」ボタンをクリックします。

項目	説明
Method List Name	15 文字までの半角英数字でメソッドリスト名を入力します。
Priority 1, 2, 3, 4	本メソッドリストに追加する認証方法を最大 4 件まで指定します。 • local_enable – スイッチ上のローカル Enable パスワードデータベースを使用してユーザ認証を行います。Local enable password は次セクションの 190 ページの「Local Enable Password Settings（ローカルユーザパスワード設定）」を参照し、設定してください。 • none – スイッチへアクセスするための認証を行います。 • radius – リモートの RADIUS サーバから RADIUS プロトコルを使用してユーザ認証を行います。 • tacacs – リモートの TACACS サーバから TACACS プロトコルを使用してユーザ認証を行います。 • xtacacs – リモートの XTACACS サーバから XTACACS プロトコルを使用してユーザ認証を行います。 • tacacs+ – リモートの TACACS+ サーバから TACACS+ プロトコルを使用してユーザ認証を行います。 • server_group – スイッチ上に設定したユーザ定義のサーバグループを使用してユーザ認証を行います。

メソッドリストの作成

1. メソッドリスト名を「Method List Name」に入力し、認証方法を「Priority 1-4」に設定します。

2. 「Apply」ボタンをクリックして設定を適用します。

ユーザ定義の Enable メソッドリストの削除

対象の行で「Delete」ボタンをクリックします。

メソッドリストの変更

1. 対応するメソッドリスト名の「Edit」ボタンをクリックし、以下の画面を表示します。

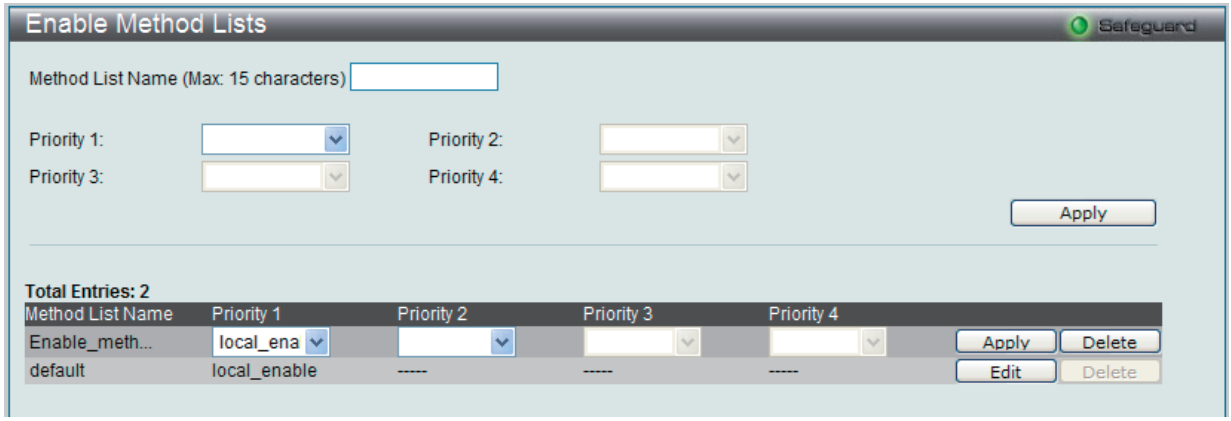


図 9-44　Enable Method Lists 画面 - Edit

2. 項目を編集後、エントリの「Apply」ボタンをクリックします。

Local Enable Password Settings（ローカルユーザパスワード設定）

本画面では、「Enable Admin」コマンド用の Local Enable Password を設定します。ユーザがその権限をユーザレベルから管理者レベルに変更する際の認証方法に、「local_enable」を選択している場合、本画面でスイッチに登録したパスワードの入力が要求されます。

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

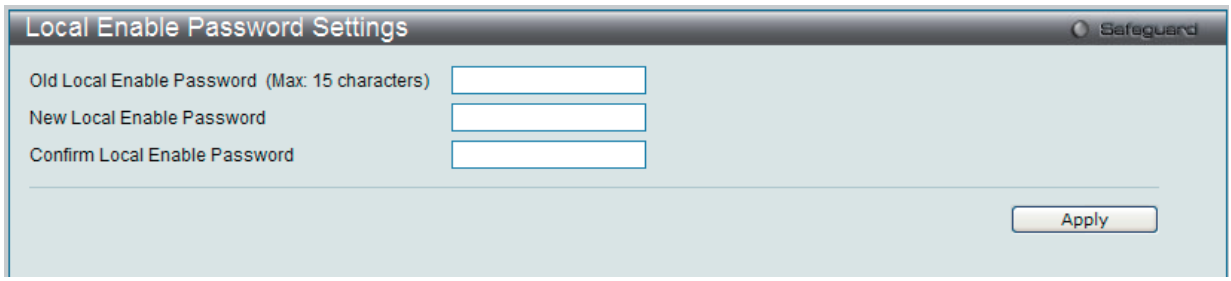


図 9-45　Local Enable Password Settings 画面

以下の項目を使用して、Local Enable Password を設定します。入力が完了後、「Apply」ボタンをクリックします。

項目	説明
Old Local Enable Password (Max: 15 characters)	登録済みのパスワードがある場合は、新しいパスワードに変更するために入力します。
New Local Enable Password	スイッチの管理者レベルでアクセスを試みるユーザの認証に使用する（新しい）パスワードを入力します。15 文字までの半角英数字を使用します。
Confirm Local Enable Password	確認のため、上記の新パスワードを再度入力します。先に入力したものと異なると、エラーメッセージが表示されます。

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。

MAC-based Access Control（MAC アドレス認証）

MAC アドレス認証は、ポートまたはホストを使用してアクセスを認証および認可する方式です。本方式は、ポートベース MAC にはポートアクセス権を決定し、一方ホストベース MAC には MAC アクセス権を決定します。

ネットワークへのアクセスを許可する前に MAC ユーザが認証される必要があります。本スイッチは、ローカル認証とリモート RADIUS サーバ認証の両方の方法をサポートしています。MAC アドレス認証では、ローカルデータベースまたは RADIUS サーバデータベース内の MAC ユーザ情報が認証のために検索されます。認証結果に基づいて、ユーザは異なるレベルの許可を取得します。

MAC アドレス認証に関する注意

MAC アドレス認証に関するいくつかの制限と規則があります。

1. 本機能がポートに有効になると、スイッチはそのポートの FDB をクリアします。
2. ポートが、ゲスト VLAN ではない VLAN で MAC アドレスをクリアする権利を認められている場合、そのポート上の他の MAC アドレスは、アクセスのために認証されている必要があり、そうでない場合、スイッチにブロックされます。
3. ポートは、ゲスト VLAN ではない VLAN の物理ポートごとに最大 200 個の認証 MAC アドレスを受け入れます。既に最大数の認証済み MAC アドレスを持つポートに対して認証を試みても、他の MAC アドレスはブロックされます。
4. リンクアグリゲーション、ポートセキュリティ、または GVRP 認証が有効なポートを MAC アドレス認証用に有効にすることはできません。

MAC-based Access Control Settings（MAC アドレス認証設定）

スイッチの MAC アドレス認証機能を設定します。動作状態、認証方式、RADIUS パスワードの設定、およびスイッチの MAC アドレス認証に関連するゲスト VLAN 設定の参照を行います。

Security > MAC-based Access Control > MAC-based Access Control 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。

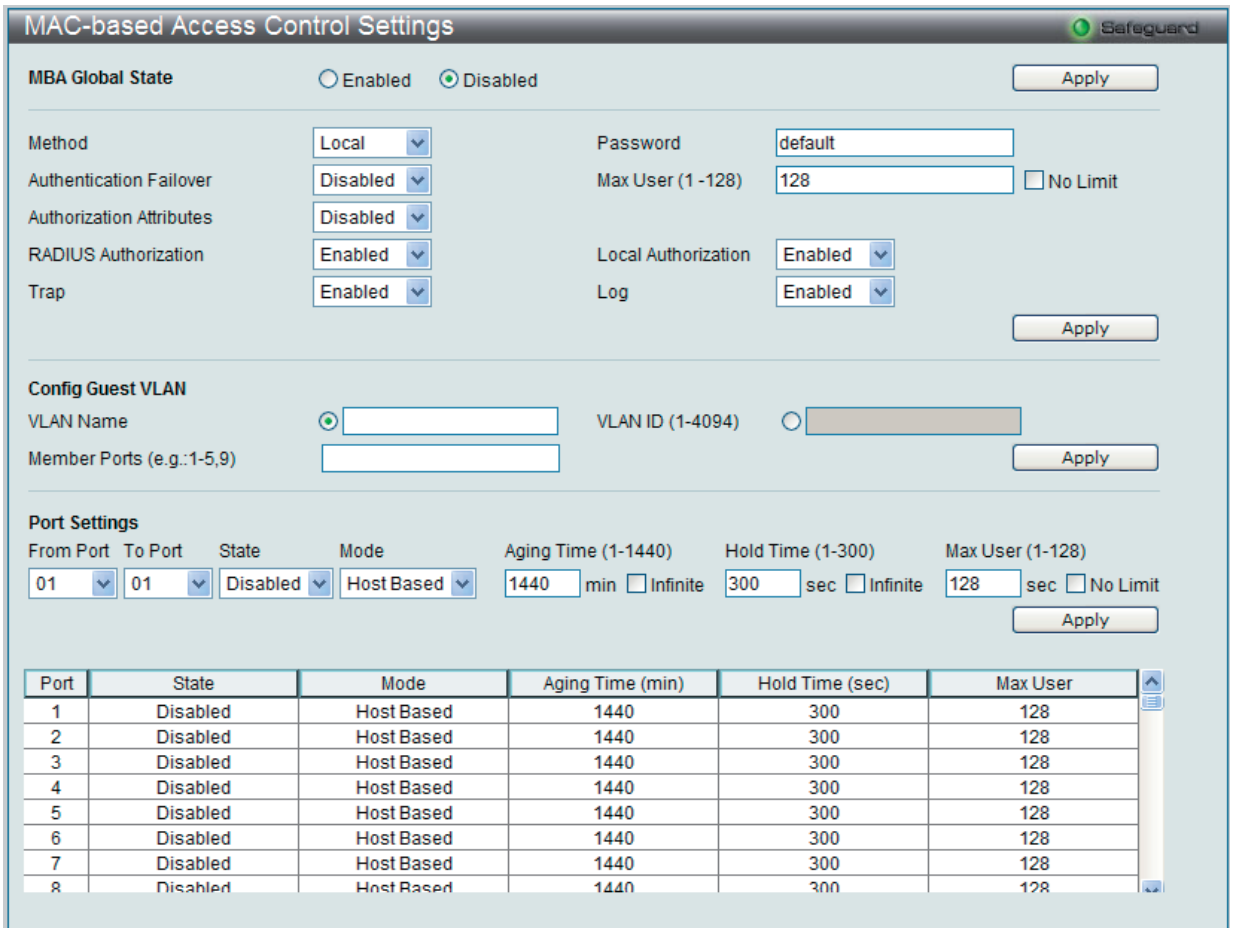


図 9-46　MAC-based Access Control Settings 画面

以下の項目を参照、または設定可能です。

項目	説明
MAC のグローバル設定	
MBA Global State	「Enabled」（有効）または「Disabled」（無効）を選択し、スイッチの MAC アドレス認証をグローバルに設定します。初期値は「Disabled」です。

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。

認証方式の設定

以下の項目を設定します。

項目	説明
Method	認証 MAC アドレスがポートにある場合、認証タイプをプルダウンメニューで選択します。認証タイプは以下の通りです。 • Local - MAC アドレス認証のオーセンティケータとしてローカルに設定された MAC アドレスデータベースを利用します。この MAC アドレスリストは、「MAC Based Access Control Local Database Settings」画面で設定します。 • RADIUS - MAC アドレス認証のオーセンティケータとしてリモート RADIUS サーバを利用します。MAC リストは、はじめに RADIUS サーバに設定されている必要があり、サーバの設定もスイッチに設定されている必要があることにご注意ください。
Password	認証リクエストのパケットを送信するために使用する RADIUS サーバのパスワードを入力します。初期値は「default」です。
Authentication Failover	初期値では認証フェイルオーバは無効です。RADIUS サーバに到達しないと、認証エラーとなります。認証フェイルオーバが有効な場合、RADIUS サーバ認証に到達しないとローカルデータベースが認証を行います。
Max User (1–128)	ユーザの最大数（1-128）を入力します。初期値は 128 です。
Authorization Attributes	有効にすると、RADUIS サーバまたはローカルデータベースによって割り当てられる属性（例 : VLAN、802.1p デフォルト優先度、および ACL）が認可されます。割り当てられる属性のタイプは、各モジュール設定に依存します。属性の認可は、初期値では「Disabled」(無効) になっています。
RADIUS Authorization	グローバル認可ステータスが有効な場合に有効にすると、RADUIS サーバが割り当てた認可属性 (例えば、VLAN、802.1p デフォルト優先度、および ACL) は許可されます。
Local Authorization	グローバル認可ステータスが有効な場合に有効にすると、ローカルデータベースが割り当てた認可属性は許可されます。
Trap	プルダウンメニューを使用して MAC ベースアクセスコントロールに対するトラップの送信を「Enabled」(有効) または「Disabled」(無効) にします。
Log	プルダウンメニューを使用して MAC ベースアクセスコントロールに対するログ出力を「Enabled」(有効) または「Disabled」(無効) にします。

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。

ゲスト VLAN の設定

以下の項目を設定します。

項目	説明
Config Guest Settings	
VLAN Name	本機能で使用する設定済みのゲスト VLAN 名を表示します。名前のリンクをクリックすると、Guest VLAN 設定画面が表示されます。
VLAN ID (1-4094)	VLAN ID 番号 (1-4094) を入力します。
VLAN Member Ports (e.g. : 1-5, 9)	ゲスト VLAN に設定されているポートリストを表示します。

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。

ポート設定

以下の項目を設定します。

項目	説明
Port Settings	
From Port / To Port	MAC アドレス認証に設定されるポート範囲を入力します。
State	選択したポートまたはポート範囲の MAC アドレス認証を「Enabled」（有効）または「Disabled」（無効）にします。
Mode	「Port Based」（ポートベース）または「Host Based」（ホストベース）を指定します。
Aging Time (1-1440)	エージングタイムを 1-1440（分）の範囲で設定します。初期値は 1440（分）です。隣接している「Infinite」をチェックして、エージングを無効にします。
Hold Time (1-300)	保持時間を 1-300（秒）の範囲で設定します。初期値は 300（秒）です。隣接している「Infinite」をチェックして、ホールドタイムを無効にします。
Max User (1–128)	ユーザの最大数（1-128）を入力します。初期値は 128 です。「No Limit」を選択すると、ユーザの最大数の設定を行いません。

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。

MAC-based Access Control Local Settings（MAC アドレス認証ローカル MAC 設定）

スイッチに対して認証されるターゲット VLAN と共に MAC アドレスリストを設定します。MAC アドレスのクエリが本テーブルに一致すると、MAC アドレスは、関連する VLAN に置かれます。スイッチ管理者は、ここで設定された local 方式を使用して、認証する最大 128 個の MAC アドレスを入力することができます。

Security > MAC-based Access Control > MAC-based Access Control Local Settings をクリックし、以下の画面を表示します。

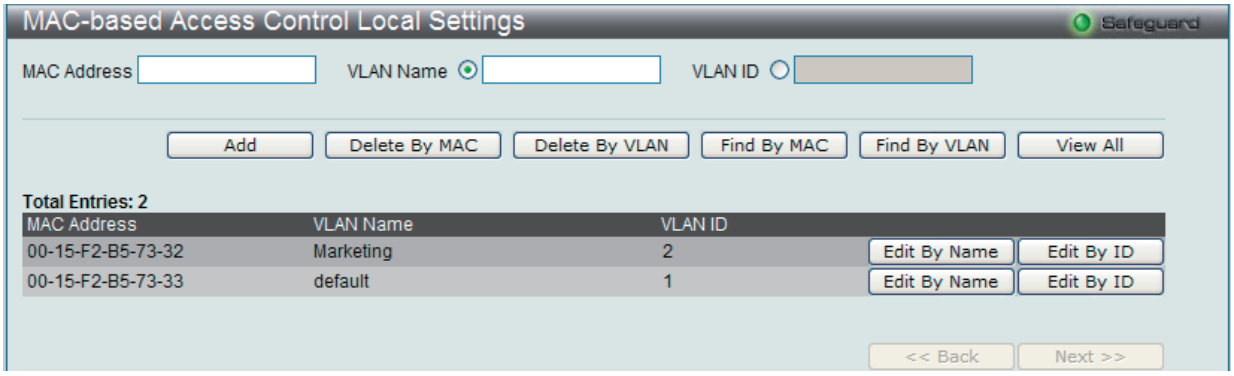


図 9-47　MAC-based Access Control Local Settings 画面

エントリの追加

MAC アドレスを Local Authentication List に追加するためには、「MAC Address」に MAC アドレス、「VLAN Name」または「VLAN ID」にターゲット VLAN 名または VLAN ID を入力し、「Add」ボタンをクリックします。

エントリの変更

1. MAC アドレスまたは VLAN を変更するためには、対応する「Edit by Name」または「Edit By ID」ボタンをクリックし、以下の画面を表示します。

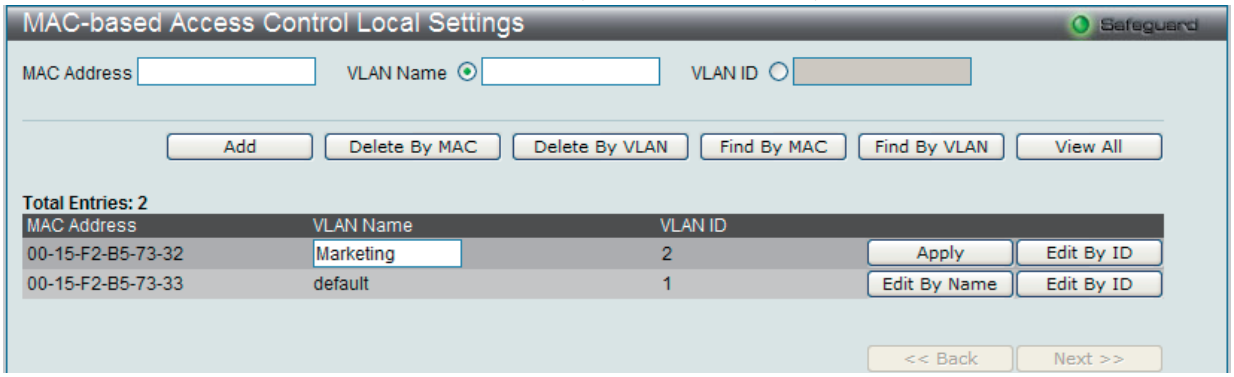


図 9-48　MAC-based Access Control Local Settings 画面 - Edit VLAN Name

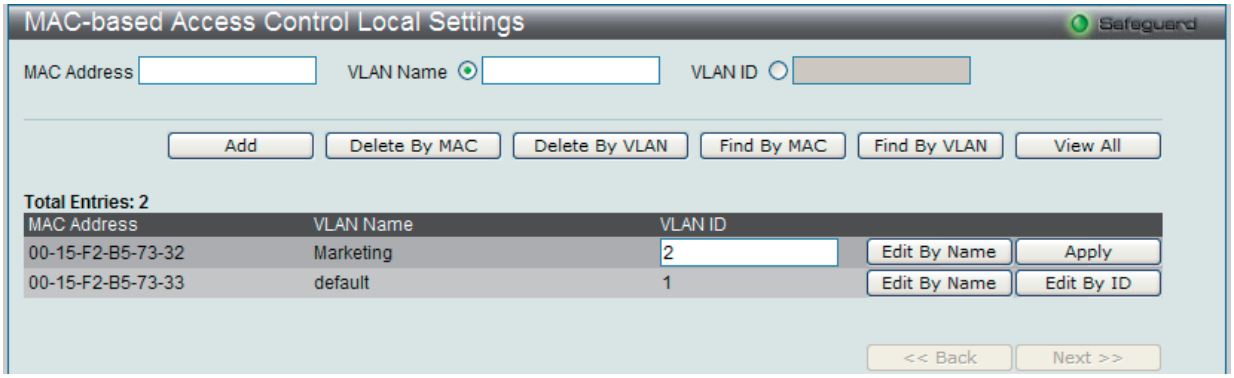


図 9-49　MAC-based Access Control Local Settings 画面 - Edit VLAN ID

2. 項目設定後、「Apply」ボタンをクリックします。

エントリの削除

MAC アドレスエントリを削除するために、該当欄に設定項目を入力し、「Delete By MAC」ボタンをクリックします。VLAN 名を削除するためには、該当欄に設定項目を入力し、「Delete By VLAN」ボタンをクリックします。

エントリの検索

特定の MAC アドレスを検索するためには、「MAC Address」に MAC アドレスを入力し、「Find By MAC」ボタンをクリックします。特定の VLAN 名を検索するためには、「VLAN Name」に VLAN 名を入力し、「Find By VLAN」ボタンをクリックします。

「View All」ボタンをクリックし、MAC アドレス、VLAN 名、および VLAN ID ごとに現在の MAC ベースアクセスコントロールのローカルデータベースエントリのすべてを表示します。

DoS Prevention Settings（DoS 攻撃防止設定）

ハッカーや不正な送信元からの DoS（Denial Of Service）攻撃を軽減する DoS 攻撃防止設定を行います。

Security > DoS 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。

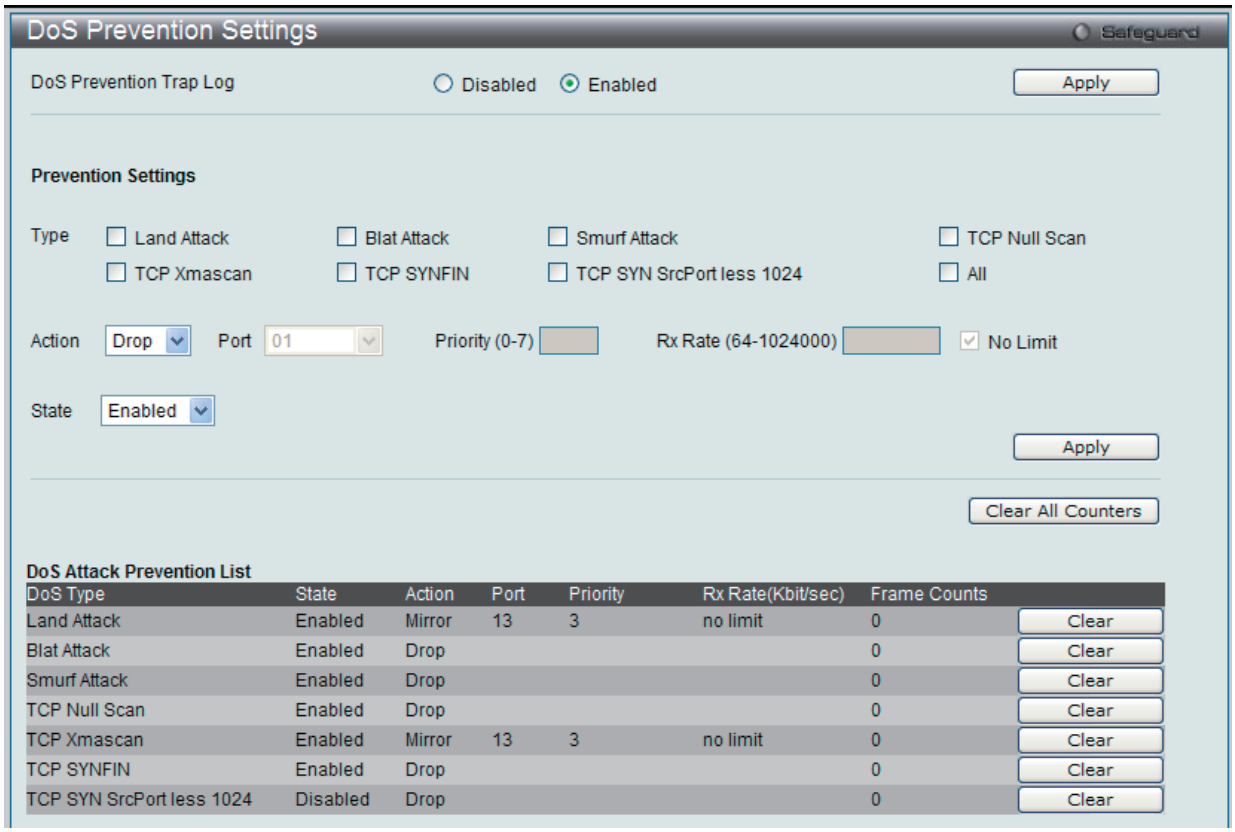


図 9-50　DoS Prevention Settings 画面

以下の項目を設定できます。

項目	説明
DoS Prevention Trap Log	DoS 攻撃防止機能のトラップログを有効または無効にします。
Type	DoS 攻撃のタイプを選択します。または「All」を指定してすべての攻撃タイプを選択します。 • Land Attack - コンピュータに送信先ホスト IP アドレスと同一の送信元ホスト IP アドレスを持つ偽造パケットを送信することで攻撃を行い、システムは自分自身に応答しようと試みて、システムのロックアップを引き起こします。 • Blat Attack - コンピュータに送信先ホストポートと同一の送信元ホストポートを持つ偽造パケットを送信することで攻撃を行い、システムは自分自身に応答しようと試みて、システムのロックアップを引き起こします。 • Smurf Attack - インターネットブロードキャストアドレスに PING 要求を送信することで攻撃を行い、インターネットブロードキャストアドレスはサブネットに接続しているホストに受信したすべてのメッセージをブロードキャストし、ネットワークの混雑を引き起こします。 • TCP Null Scan - 待ち受け TCP ポートを識別するフラグを持たない異常に設定した一連の TCP パケットを使用することで攻撃を行います。このタイプのスキャンは、ファイアウォールやと境界ルータをすり抜けることができます。 • TCP Xmascan - 0 数列、FIN、Push（PSH）、および Urgent（URG）を含む、異常に設定した一連の TCP パケットを送信することで攻撃を行います。このタイプのスキャンは、いくつかのファイアウォールと境界ルータをすり抜けることができます。 • TCP SYNFIN - TCP パケットに SYN フラグと FIN フラグを設定することによって攻撃を行います。これらのパケットは攻撃相手が正常な SYN パケットを得ることができないようにし、大量のパケットで相手を「CLOSE WAIT（閉鎖待機）」状態にします。 • TCP SYN SrcPort less 1024 - 1024 未満の送信元ポートを持つ SYN パケットを送信することで攻撃を行います。攻撃を受けると、インターネットデフォルトサービスは、1 と 1023 の間の L4 ポートを使用します。 • All - ボックスをチェックし、すべての攻撃タイプを選択します。
Action	選択した攻撃のタイプへの処理（「Drop」または「Mirror」）を指定します。
Port	ログをミラーリングするポートを指定します。
Priority(0-7)	ミラーポートの優先順位を設定します。
Rx Rate (64-1024000)	64-1024000 の範囲で値を指定するか、または「No Limit」をチェックします。
State	本機能を有効または無効にします。

「Apply」ボタンをクリックすると、設定した変更を適用します。
「Clear」ボタンをクリックすると、指定した攻撃タイプを取り消します。
「Clear All」ボタンをクリックすると、すべてのフレームカウントをクリアします。

DHCP Server Screening（DHCP サーバスクリーニング）

本機能は、すべての DHCP サーバパケットを制限できるだけでなく、指定されたどの DHCP クライアントからのどんな DHCP サーバパケットも受信することができます。これは 1 つ以上の DHCP サーバがネットワークに存在する場合に DHCP サービスを異なるクライアントグループを区別するのに役に立ちます。

DHCP Server Screening フォルダには次の 2 つの画面があります。:「DHCP Screening Port Settings」画面および「DHCP Offer Filtering」画面

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

不正な DHCP サーバへの接続を拒否する DHCP サーバスクリーニング機能をサポートしています。DHCP サーバフィルタ機能が有効の場合、指定されたポートからのすべての DHCP サーバパケットはフィルタリングされます。

Security > DHCP Server Screening > DHCP Screening Port Settings の順にメニューをクリックして画面を表示します。

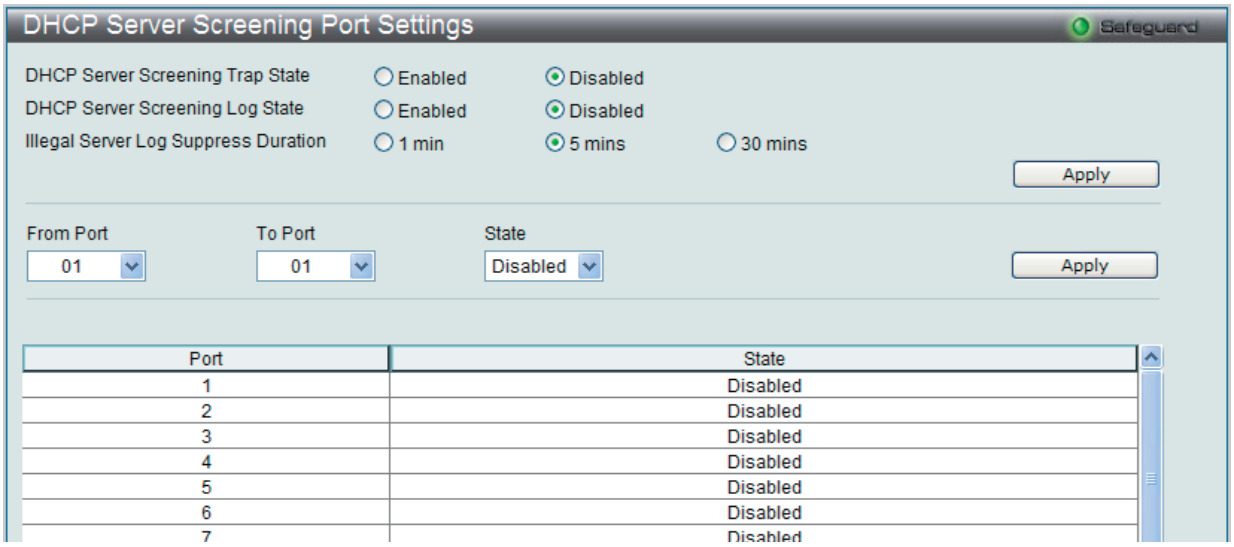


図 9-51　DHCP Server Screening Port Settings 画面

本画面には次の項目があります。

項目	説明
DHCP Server Screening Trap State	DHCP サーバのトラップのフィルタを「Enabled」（有効）または「Disabled」（無効）にします。
DHCP Server Screening Log State	DHCP サーバのログの状態を「Enabled」（有効）または「Disabled」（無効）にします。
Illegal Server Log Suppress Duration	不正なサーバログのサプレッション時間を 1、5、または 30 分から選択します。初期値は 5（分）です。

「Apply」ボタンをクリックして、設定を適用します。

ポートごとのスクリーニング設定のためには、プルダウンメニューを使用して、以下の項目を設定します。

項目	説明
From Port / To Port	設定の対象となるポート範囲を指定します。
State	DHCP サーバスクリーニングを「Enabled」（有効）または「Disabled」（無効）にします。初期値は「Disabled」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。
「DHCP Port Information Table」に、DHCP サーバスクリーニングのポートの状態（「Enabled」/「Disabled」）が表示されます。

DHCP Offer Filtering（DHCP Offer フィルタリング）

DHCP Offer パケットを許可するエントリを設定します。

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

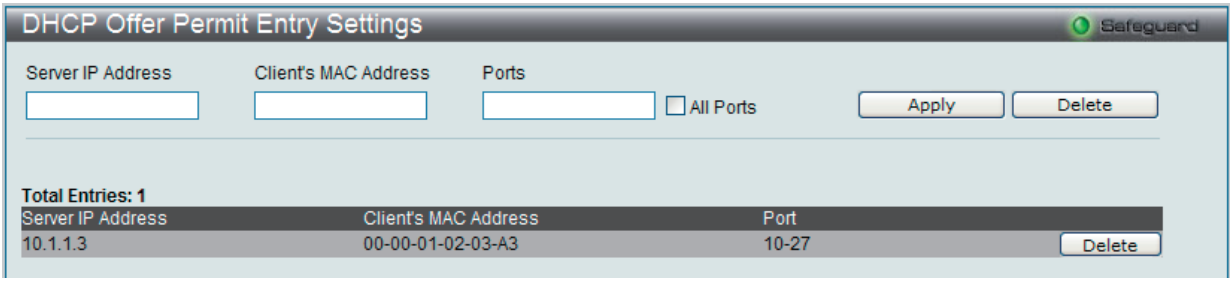


図 9-52　DHCP Offer Permit Entry Setting 画面

本画面には次の項目があります。

項目	説明
Server IP Address	DHCP サーバの IP アドレス。
Client's MAC Address	DHCP クライアントの MAC アドレス。ネットワーク上の正しい DHCP サーバが複数ある場合にだけ入力します。ネットワーク上に正しい DHCP サーバが 1 つしか存在しない場合は、入力することはできません。
Ports	DHCP サーバとして使用するポート範囲を選択します。スイッチのすべてのポートを使用する場合は「All Ports」をチェックします。

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。

認証サーバの削除

1. 削除するエントリの「Delete」ボタンをクリックします。

第 10 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	参照ページ
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。	197 ページ
Access Profile List（アクセスプロファイルリスト）	パケットヘッダに含まれる情報に基づくパケット転送可否の基準を設定するプロファイルを設定します。	199 ページ
CPU Access Profile List（CPU アクセスプロファイルリスト）	CPU インタフェースフィルタリング機能を設定します。	215 ページ
ACL Finder（ACL 検索）	ACL エントリを検索します。	229 ページ
ACL Flow Meter（ACL フローメータ）	フローごとの帯域幅制御設定を行います。	230 ページ

アクセスプロファイルを作成すると、パケットヘッダの中の情報に従い、スイッチがパケット送信を決定するための基準を設定できるようになります。この基準はパケットコンテンツ、MAC アドレスや IP アドレスをベースに設定が可能です。

ACL Configuration Wizard（ACL 設定ウィザード）

アクセスプロファイルと ACL ルールの新規作成を行います。ACL ウィザードにより自動的にアクセスルールとプロファイルを作成することができます。

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。

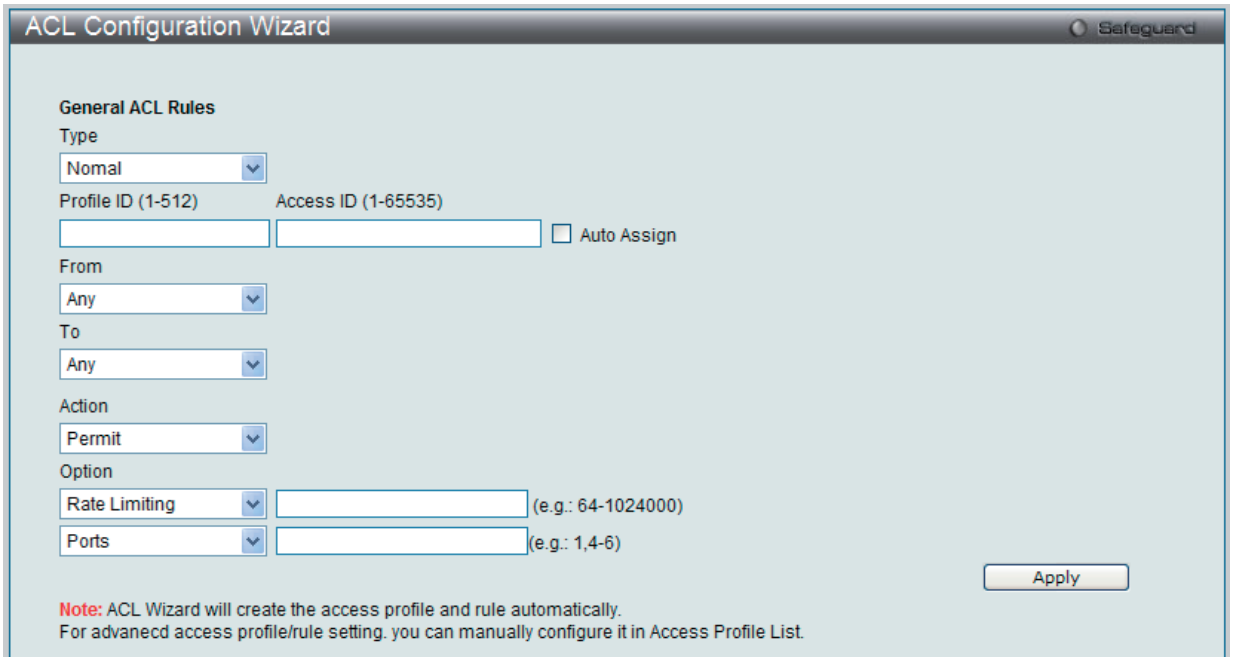


図 10-1　ACL Configuration Wizard 画面

1. ACL の種類 (Normal または CPU) を選択します。「Normal」を選択すると、スイッチのインタフェースの 1 つに受信したパケットに適用される ACL ルールを作成します。「CPU」を選択すると、スイッチに送信されるパケットにだけ適用される ACL ルールを作成します。
2. Profile ID (1-512) と Access ID (1-65535) を割り当てるか、またはこれを自動的に行うために「Auto Assign」欄をチェックします。
3. 範囲を From（Any、MAC Address、IPv4 Address または IPv6）と To（Any、MAC Address、IPv4 Address）から選択します。
4. 「Action」を「Permit」、「Deny」または「Mirror」から選択します。
5. 「Option」を「Rate Limiting」、「Change IP Priority」、または「Replace DSCP」から選択し、隣接している欄に 64-10214000 の値を入力します。
6. 新しい ACL ルール用のポートを「Ports」横の欄に入力し、「Apply」ボタンをクリックして設定を適用します。

以下の項目を使用して、設定を行います。

項目	説明
Type	作成する ACL の種類 (normal または CPU) を選択します。
Profile ID (1-512)	プロファイル設定用の固有の識別番号を指定します。値の範囲は 1-512 です。
Access ID(1-65535)	本アクセスの識別番号を入力します。値の範囲は 1-65535 です。
From	「MAC Address」、「IPv4 Address」、「IPv6」または「Any」を選択します。
To	「MAC Address」、「IPv4 Address」または「Any」を選択します。IPv6 を選択した場合は、IPv6 送信元アドレスまたは IPv6 宛先アドレスのみ入力することができます。
Action	• Permit - スイッチはアクセスプロファイルに一致するパケットの送信を、以下の項目で設定する追加のルールに従って行います。 • Deny - スイッチはアクセスプロファイルに一致するパケットの送信を行いません。 • Mirror - スイッチはアクセスプロファイルに一致するパケットを「Port Mirroring」画面で定義したポートにミラーリングします。ポートミラーリングが有効で、ターゲットポートが設定されている必要があります。
Option	「Rate Limiting」、「Change 1P Priority」、「Replace DSCP」の中から選択します。隣接している欄に 1-1024000 の値を入力します。
Ports	設定するポート範囲を指定します。

Access Profile List（アクセスプロファイルリスト）

アクセスプロファイルを使用することにより、それぞれのパケットヘッダに含まれる情報に基づくパケット転送可否の基準を設定することができます。スイッチは、4 つのプロファイルタイプ（イーサネット ACL、IPv4 ACL、IPv6 ACL およびパケットコンテンツ ACL）をサポートしています。

アクセスプロファイルの作成は 2 段階に分かれます。はじめにフレームのどの部分を調べるのか、送信元 MAC アドレスか、受信先 IP アドレスか、などを決定します。次に、そのフレームに対してどのような処理を行うのかという基準になる値を入力します。詳しくは以下で説明します。

アクセスプロファイルリストの作成（Ethernet）

アクセスプロファイルを作成し、プロファイルにルールを作成します。

ACL > Access Profile 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。 1 つのアクセスプロファイルが説明のために作成されています。

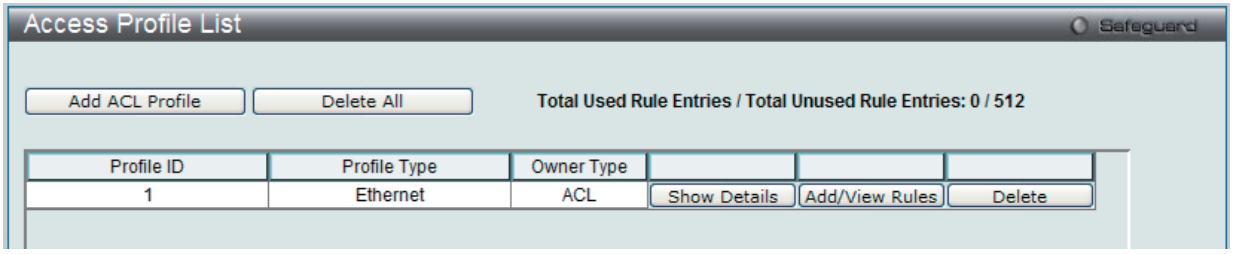


図 10-2　Access Profile List 画面

エントリの削除

エントリを削除するためには、エントリ横の「Delete」ボタンをクリックします。すべてのアクセスプロファイルを削除するためには、「Delete All」ボタンをクリックします。

エントリの追加

「Access Profile List」にエントリを追加するには、「Add ACL Profile」ボタンをクリックし、以下の画面を表示します。

イーサネットの「Add ACL Profile」画面

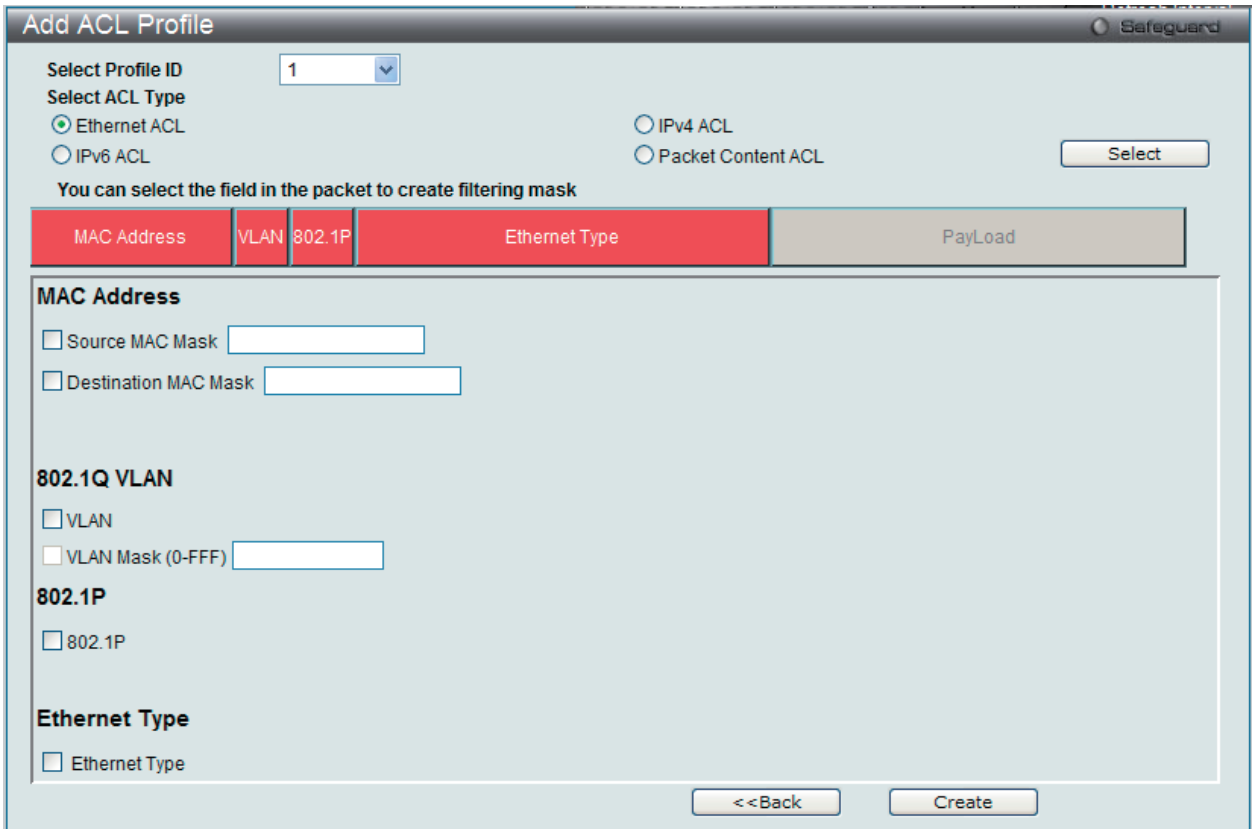


図 10-3　Add ACL Profile - Ethernet ACL 画面

「Profile ID」でプロファイル番号を 1-512 から選択し、「Select ACL Type」で「Ethernet」をチェック後、「Select」ボタンをクリックすることで画面を切り替えることができます。画面上部のボックスをクリックすると、赤色に変わり、設定用項目が表示されます。

以下の項目を Ethernet ACL タイプに設定します。

項目	説明
Select Profile ID	プロファイル設定のための固有の識別番号を指定します。1 から 512 が指定できます。
Select ACL Type	Ethernet（MAC アドレス）、IPv4 アドレス、IPv6 アドレスまたはパケットコンテンツからプロファイルのタイプを指定します。Type の変更に伴いメニューも変わります。ここでは、「Ethernet ACL」を選択します。 • Ethernet ACL - パケットヘッダのレイヤ 2 部分を検証します。
以下のオプションを指定すると各フレームヘッダのプロトコルタイプを調べます。転送基準にどのようなプロトコルを含めるかを指定します。	
MAC Address	• Source MAC Mask - 送信元 MAC アドレスをマスクする MAC アドレスを指定します。 • Destination MAC Mask - 送信先 MAC アドレスをマスクする MAC アドレスを指定します。
VLAN	本オプションを指定するパケットヘッダの 802.1Q VLAN 識別子を調べて、部分的もしくは全体を転送基準として使用します。 • VLAN - VLAN マスクを指定します。 • VLAN Mask (0-FFF) - VLAN マスクを指定します。
802.1P	本オプションを指定すると各パケットヘッダの 802.1p プライオリティを調べて、部分的または全体を転送基準として使用します。
Ethernet Type	このオプションを指定するとフレームヘッダでイーサネットタイプの値を調べます。

「Create」ボタンをクリックし、プロファイルを作成します。

作成したプロファイルの詳細の参照

「Access Profile List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

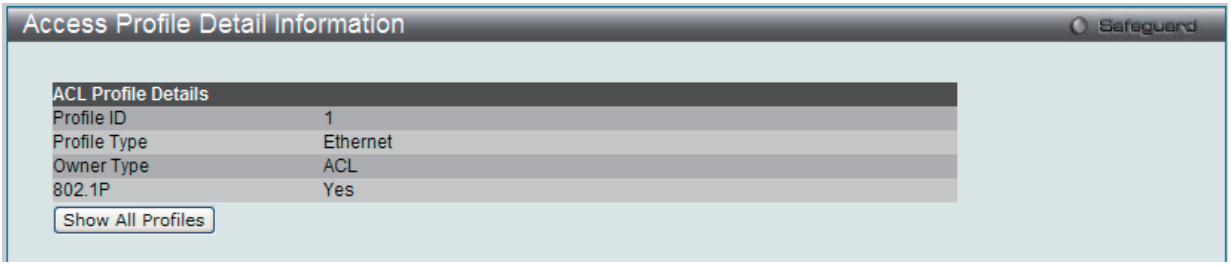


図 10-4　Access Profile Detail Information - Ethernet 画面

「Show All Profiles」ボタンをクリックすると、「Access Profile List」画面に戻ります。

作成したアクセスプロファイルに対するルールの設定手順（Ethernet）：

Ethernet アクセスルールの設定

1. 「Access Profile List」画面を表示します。

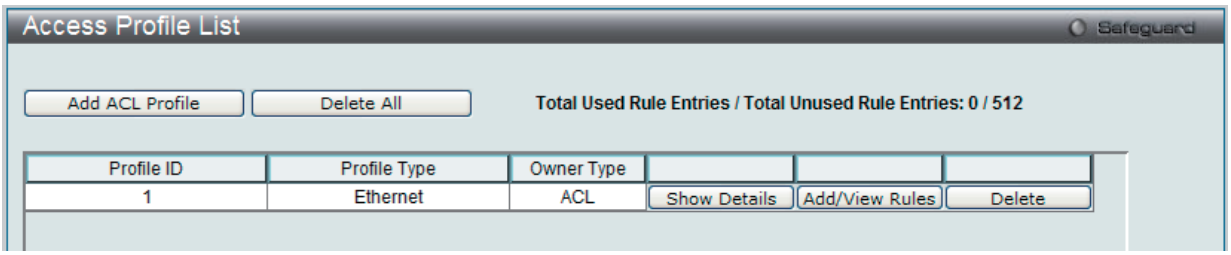


図 10-5　Access Profile List 画面

2. Ethernet エントリの「Add/View Rules」ボタンをクリックし、以下の画面を表示します。

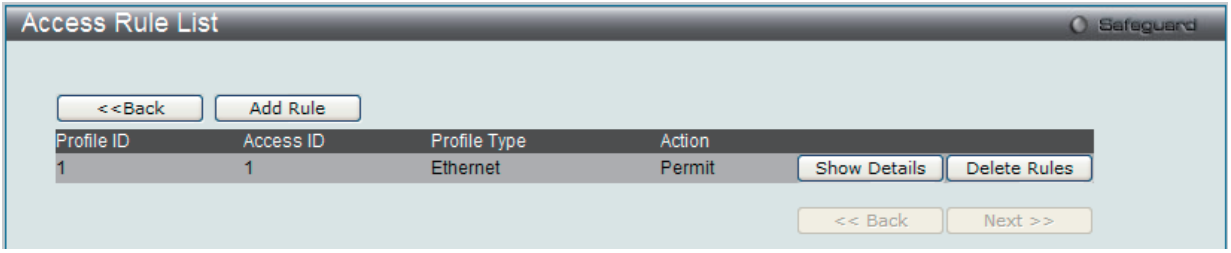


図 10-6　Access Rule List - Ethernet 画面

作成したルールの削除

該当の「Delete Rules」ボタンをクリックします。

ルールの新規作成

ルールを作成するためには、「Add Rule」ボタンをクリックし、以下の画面を表示します。

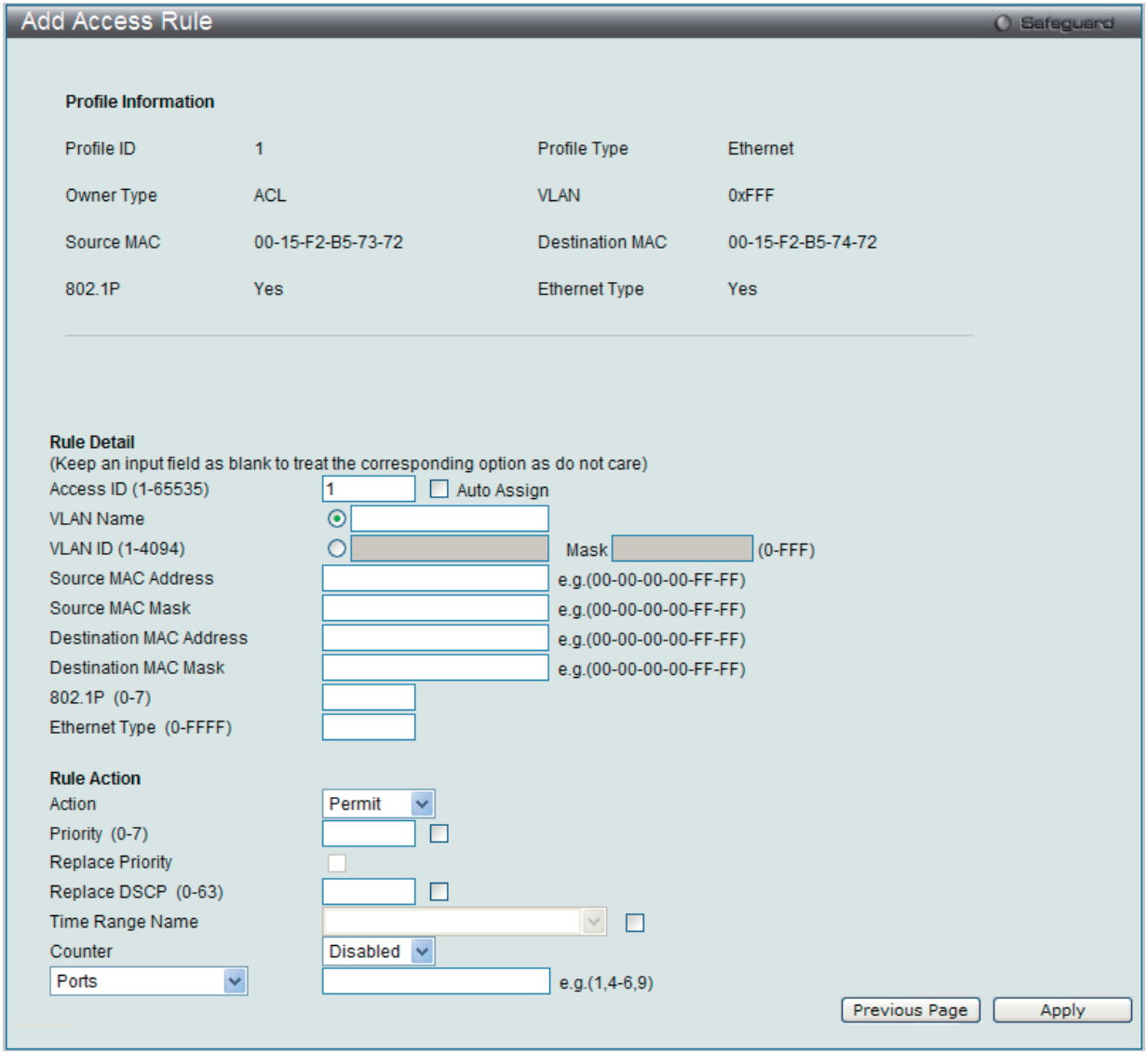


図 10-7　Add Access Rule - Ethernet 画面

Ethernet のアクセスルールを設定するためには以下の項目を設定して、「Apply」ボタンをクリックします。

項目	説明
Rule Detail	
Access ID (1-65535)	プロファイル設定のための固有の識別番号を指定します。1 から 65535 が指定できます。 • Auto Assign - 本項目をチェックするとスイッチは自動的に作成されるルールに Access ID を割り当てます。
VLAN Name	設定済みの VLAN 名を入力します。スイッチはパケットヘッダの VLAN を確認し、その結果をパケット送信の基準 (または基準の一部) とします。
VLAN ID (1-4094)	VLAN ID 番号を指定します。Mask (0-FFF) を指定します。
Source MAC Address	送信元 MAC アドレスの MAC アドレスマスクを指定します。
Source MAC Mask	送信元 MAC アドレスの MAC アドレスマスクを 16 進数形式で指定します。
Destination MAC Address	送信先 MAC アドレスの MAC アドレスマスクを入力します。
Destination MAC Mask	送信先 MAC アドレスの MAC アドレスマスクを 16 進数形式で入力します。
802.1P (0-7)	802.1p プライオリティ値を 0-7 で入力します。アクセスプロファイルをこの値を持つパケットに適用します。
Ethernet Type (0-FFFF)	アクセスプロファイルが適用されるパケットヘッダの 802.1Q イーサネットタイプの値を 16 進数（hex 0x0-0xffff）で指定します。イーサネットタイプは次の形式で指定します。: hex 0x0-0xffff（a-f の半角英文字、と 0-9999 の数字を使用します。）

項目	説明
Rule Action	
Action	• Permit - アクセスプロファイルに一致したパケットを転送します。この時、新しいルールが追加されることがあります（以下参照）。 • Deny - アクセスプロファイルに一致したパケットは転送せずにフィルタリングします。 • Mirror - アクセスプロファイルに一致するパケットを「Port Mirroring」画面で定義したポートにミラーリングします。ポートミラーリングが有効で、ターゲットポートに設定されている必要があります。
Priority (0-7)	本画面で設定した基準に一致するパケットが指定された CoS キューに送られる前に、パケットの 802.1p デフォルトプライオリティを本欄に指定した値に書き換える場合に使用します。入力しない場合、パケットはスイッチによって送信される前に書き換えた 802.1p ユーザプライオリティとなります。プライオリティキュー、CoS キュー、802.1p への割り当てに関する詳しい説明は本マニュアル 150 ページの「第 8 章 QoS（QoS 機能の設定）」のを参照してください。
Replace Priority	本画面で設定した基準に一致するパケットが、指定された CoS キューに送られる前に、パケットの 802.1p デフォルトプライオリティを、「Priority」欄に指定した値に書き換える場合に使用します。チェックしない場合、パケットはスイッチによって送信される前に書き換えた 802.1p ユーザプライオリティとなります。
Replace DSCP(0-63)	本オプションを選択すると、スイッチは本画面で指定した基準に一致するパケットの DSCP をチェックボックスの右側の欄に指定した値に書き換えます。
Time Range Name	チェックボックスをクリックし、「Time Range」画面に設定済みのタイムレンジ設定名を入力します。このアクセスルールをスイッチで実行する場合、ここに特定の時間を設定します。
Counter	「Counter」機能を「Enabled」（有効）/「Disabled」（無効）にします。カウンタ機能は、アクセスルールに一致するパケット数を記録するために使用されます。本機能はオプションです。初期値は無効です。
Ports	アクセスルールを設定するポート範囲を指定します。

作成したルールの詳細の参照

「Access Rule List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

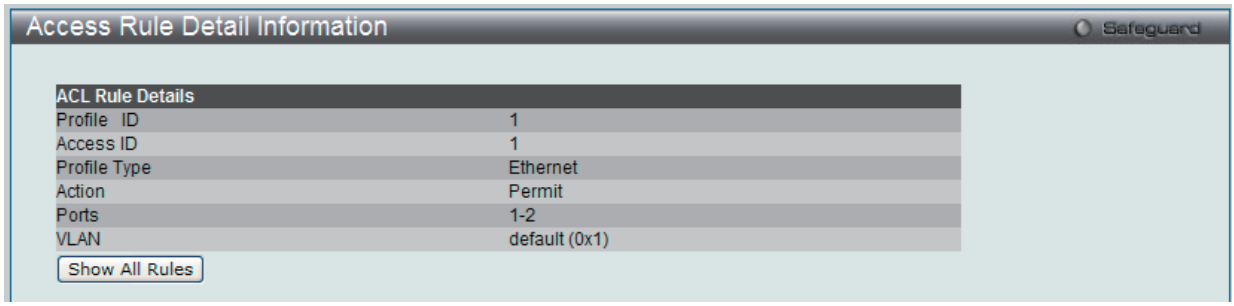


図 10-8　Access Rule Detail Information - Ethernet 画面

「Show All Rules」ボタンをクリックすると、「Access Rule List」画面に戻ります。

アクセスプロファイルリストの作成（IPv4）

アクセスプロファイルを作成し、プロファイルにルールを作成します。

ACL > Access Profile 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。1 つのアクセスプロファイルが説明のために作成されています。

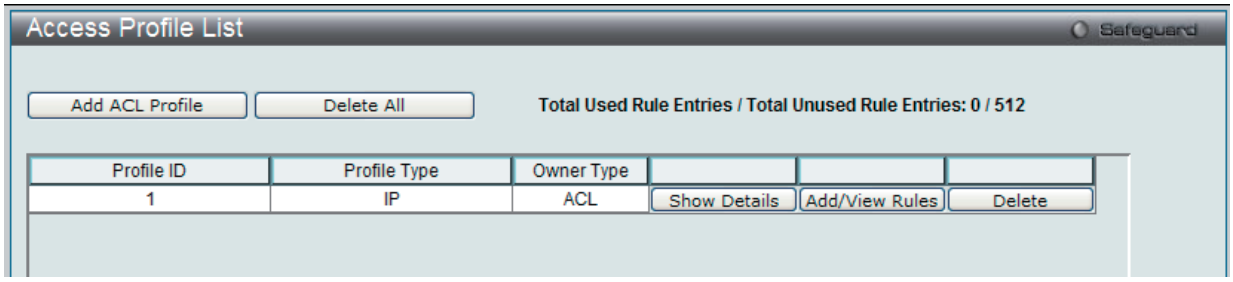


図 10-9　Access Profile List 画面

エントリの削除

エントリを削除するためには、エントリ横の「Delete」ボタンをクリックします。すべてのアクセスプロファイルを削除するためには、「Delete All」ボタンをクリックします。

エントリの追加

「Access Profile List」にエントリを追加するには、「Add ACL Profile」ボタンをクリックし、以下の画面を表示します。

IPv4 の「Add ACL Profile」画面

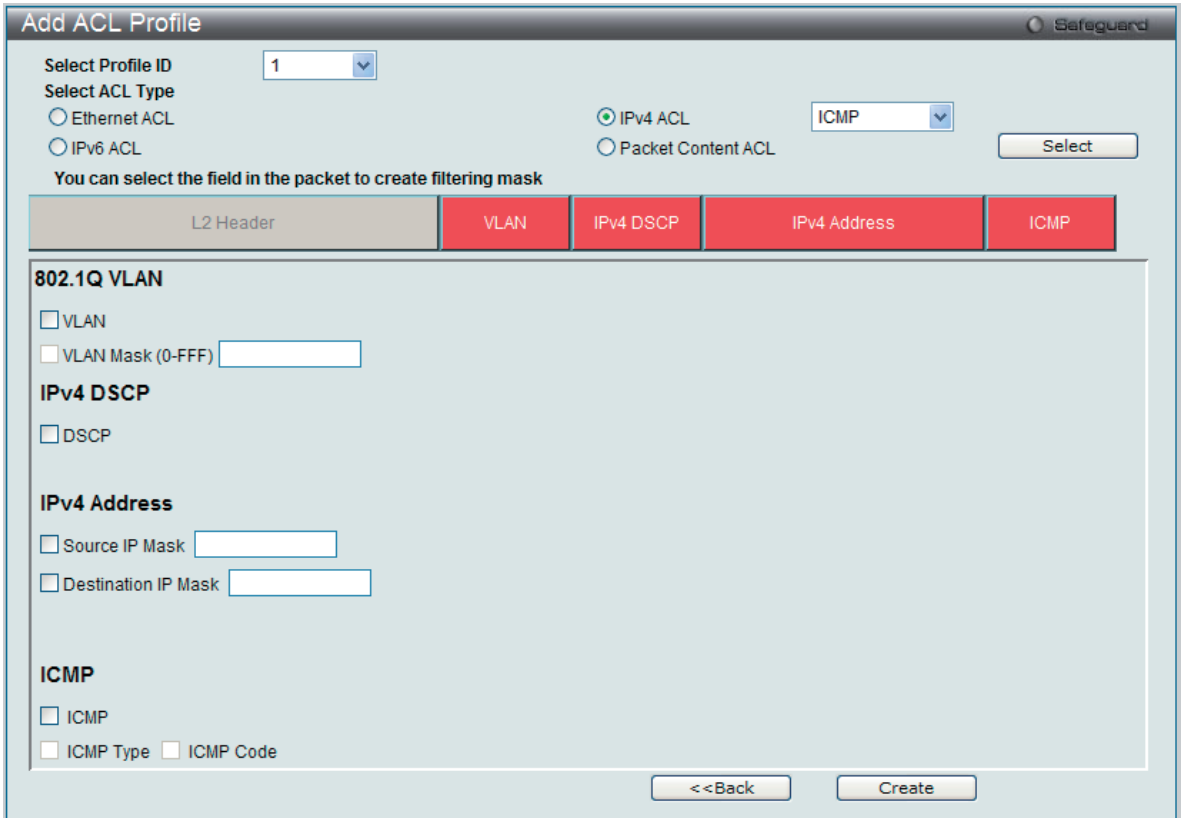


図 10-10　Add ACL Profile - IPv4 ACL 画面

「Profile ID」でプロファイル番号を 1-512 から選択し、「Select ACL Type」で「IPv4 ACL」をチェック後、隣接する欄で設定するフレームヘッダ（ICMP、IGMP、TCP、UDP、Protocol ID）選択して「Select」ボタンをクリックします。画面上部のボックスをクリックすると、赤色に変わり、設定用項目が表示されます。

以下の項目を IPv4 ACL タイプに設定します。

項目	説明
Select Profile ID	プロファイル設定のための固有の識別番号を指定します。1 から 512 が指定できます。
Select ACL Type	Ethernet（MAC アドレス）、IPv4 アドレス、IPv6 アドレスまたはパケットコンテンツの中からプロファイルのベースを指定します。Type の変更に伴いメニューも変わります。ここでは「IPv4 ACL」を選択します。 • IPv4 ACL - フレームヘッダの IPv4 アドレスを検証します。
以下のオプションを指定すると各フレームヘッダのプロトコルタイプを調べます。転送基準にどのようなプロトコルを含めるかを指定します。	
802.1Q VLAN	このオプションを指定するパケットヘッダの 802.1Q VLAN 識別子を調べて、部分的もしくは全体を転送基準として使用します。
IPv4 DSCP	このオプションを指定すると各パケットヘッダの DiffServ コードを調べて、部分的もしくは全体を転送基準として使用します。
IPv4 Address	• Source IP Mask - 送信元 IP アドレスをマスクする IP アドレスを指定します。 • Destination IP Mask - 送信先 IP アドレスをマスクする IP アドレスを指定します。
ICMP	各パケットのフレームヘッダの「Internet Control Message Protocol」（ICMP）項目を調べます。アクセスプロファイルが適用するタイプ（「ICMP Type」または「ICMP Code」）を選択します。 • ICMP Type - アクセスプロファイルを ICMP Type 値に適用します。 • ICMP Code - アクセスプロファイルを ICMP Code に適用します。
IGMP	それぞれのフレームヘッダの「Internet Group Management Protocol」（IGMP）項目を調べます。アクセスプロファイルが適用するタイプ「IGMP Type」を選択します。

項目	説明
TCP	転送基準となる受信したパケットの TCP ポート番号を使用します。TCP を選ぶと送信元ポートマスク（source port mask）と（または）送信先ポートマスク（dest port mask）を指定する必要があります。 - Source Port Mask（0-FFFF）- フィルタリングしたい送信元ポートをマスクする TCP ポートを 16 進数（hex 0x0-0xffff）で指定します。 - Destination Port Mask（0-FFFF）- フィルタリングしたい送信先ポートをマスクする TCP ポートを 16 進数（hex 0x0-0xffff）で指定します。 - TCP Flag Bits - フィルタするフラグビットを指定します。フラグビットはパケットがどのような振る舞いをするかを決定するパケットの一部です。パケットのフラグビットでフィルタリングするには「TCP」項目のフラグビットに一致する内容のボックスをチェックします。URG（urgent）、ACK（acknowledgement）、PSH（push）、RST（reset）、SYN（synchronize）、FIN（finish）または Check All（すべて）を選ぶことができます。
UDP	転送基準となる受信したパケットの UDP ポート番号を使用します。UDP を選ぶと送信元ポートマスク（source port mask）と（もしくは）送信先ポートマスク（dest port mask）を指定する必要があります。 - Source Port Mask（0-FFFF）- フィルタリングしたい送信元ポートをマスクする UDP ポートを 16 進数（hex 0x0-0xffff）で指定します。 - Destination Port Mask (0-FFFF) - フィルタリングしたい送信先ポートをマスクする UDP ポートを 16 進数（hex 0x0-0xffff）で指定します。
Protocol ID	マスクしたいパケットヘッダの Protocol ID Mask を指定します。「User Define」マスクは 16 進数（0-FF）で指定します。

「Create」ボタンをクリックし、設定を適用します。

作成したプロファイルの詳細の参照

作成したプロファイルの詳細を参照するには、「Access Profile List」画面の該当エントリの「Show Details」ボタンをクリックし、以下の画面を表示します。

図 10-11　Access Profile Detail Information - IPv4 画面

「Show All Profiles」ボタンをクリックすると、「Access Profile List」画面に戻ります。

作成したアクセスプロファイルに対するルールの設定手順（IPv4）：

IPv4 アクセスルールの設定

1. 「Access Profile List」画面を表示します。

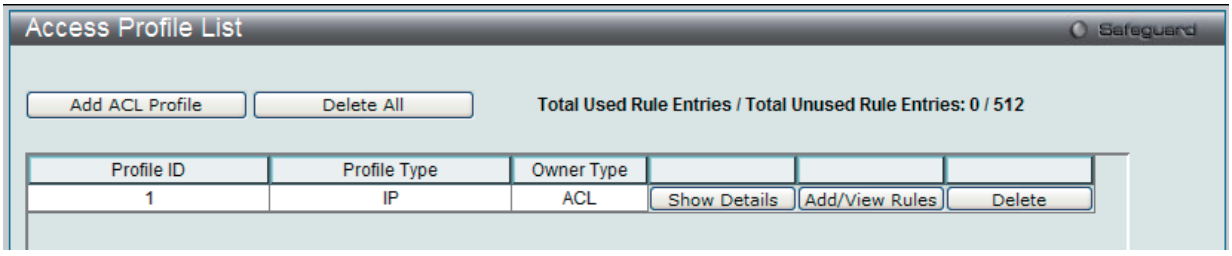


図 10-12　Access Profile List 画面

2. 「Access Profile List」画面を表示し、IPv4 エントリの「Add/View Rules」ボタンをクリックし、以下の画面を表示します。

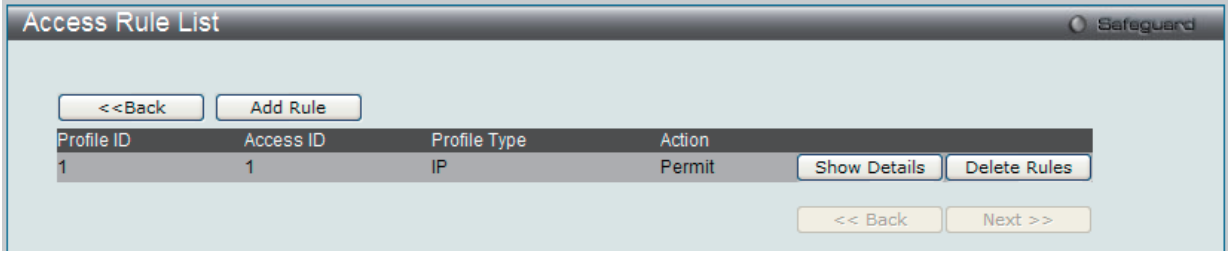


図 10-13　Access Rule List - IP 画面

ルールの削除

該当の「Delete Rules」ボタンをクリックします。

ルールの新規作成

新しいルールを作成するには、「Add Rule」ボタンをクリックし、以下の画面を表示します。

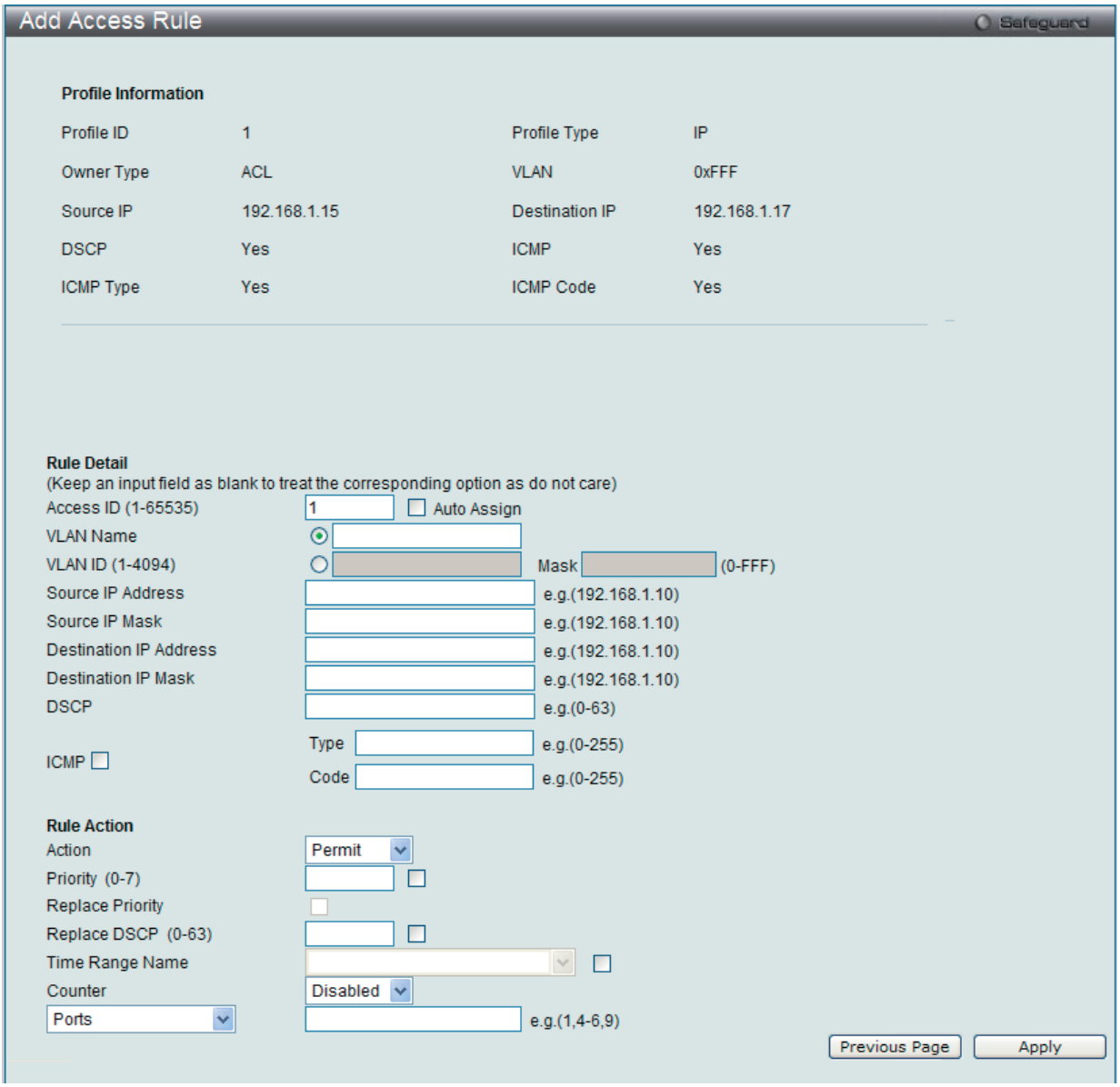


図 10-14　Add Access Rule - IP 画面

以下の項目を設定します。

項目	説明
Rule Detail	
Access ID (1-65535)	プロファイル設定のための固有の識別番号を指定します。1 から 65535 が指定できます。 • Auto Assign - 本項目をチェックするとスイッチは自動的に作成されるルールに Access ID を割り当てます。
VLAN Name	VLAN 名を入力します。
VLAN ID(1-4094)	VLAN ID を入力します。「Mask」（0-FFF）にマスク値を入力します。
Source IP Address	送信元の IP アドレスの IP アドレスを入力します。
Source IP Mask	送信元の IP アドレスの IP アドレスマスクを入力します。
Destination IP Address	宛先 IP アドレスの IP アドレスを入力します。
Destination IP Mask	送信先 IP アドレスの IP アドレスマスクを入力します。
DSCP	DSCP 値（0-63）を指定すると各パケットヘッダの DiffServ コードを調べて、部分的または全体を転送基準として使用します。
ICMP	各パケットのフレームヘッダの「Internet Control Message Protocol」（ICMP）項目を調べます。アクセスプロファイルが適用するタイプ（「ICMP Type」または「ICMP Code」）を選択します。 • Type - アクセスプロファイルを ICMP Type 値に適用します。 • Code - アクセスプロファイルを ICMP Code に適用します。
IGMP	それぞれのフレームヘッダの「Internet Group Management Protocol」（IGMP）項目を調べます。アクセスプロファイルが適用するタイプ「IGMP Type」を選択します。
TCP	転送基準となる受信したパケットの TCP ポート番号を使用します。TCP を選ぶと送信元ポートマスク（source port mask）と（または）送信先ポートマスク（dest port mask）を指定する必要があります。 - Source Port Mask（0-FFFF）- フィルタリングしたい送信元ポートをマスクする TCP ポートを 16 進数で指定します。 - Destination Port Mask（0-FFFF）- フィルタリングしたい送信先ポートをマスクする TCP ポートを 16 進数で指定します。 - Flag Bits - フィルタするフラグビットを指定します。フラグビットはパケットがどのような振る舞いをするかを決定するパケットの一部です。パケットのフラグビットでフィルタリングするには「TCP」項目のフラグビットに一致する内容のボックスをチェックします。URG（urgent）、ACK（acknowledgement）、PSH（push）、RST（reset）、SYN（synchronize）、FIN（finish）を選ぶことができます。
UDP	転送基準となる受信したパケットの UDP ポート番号を使用します。UDP を選ぶと送信元ポートマスク（source port mask）と（または）送信先ポートマスク（dest port mask）を指定する必要があります。 - Source Port Mask（0-FFFF）- フィルタリングしたい送信元ポートをマスクする UDP ポートを 16 進数（hex 0x0-0xffff）で指定します。 - Destination Port Mask（0-FFFF）- フィルタリングしたい送信先ポートをマスクする UDP ポートを 16 進数（hex 0x0-0xffff）で指定します。
Protocol ID	マスクしたいパケットヘッダの Protocol ID Mask を指定します。0-255 の値を入力します。
Rule Action	
Action	• Permit - アクセスプロファイルにマッチしたパケットを転送します。この時新しいルールが追加されることがあります（以下参照）。 • Deny - アクセスプロファイルに一致したパケットは転送せずにフィルタリングします。 • Mirror - アクセスプロファイルに一致するパケットを「Port Mirroring」画面で定義したポートにミラーリングします。ポートミラーリングが有効で、ターゲットポートに設定されている必要があります。
Priority (0-7)	本画面で設定した基準に一致するパケットが指定された CoS キューに送られる前に、パケットの 802.1p ユーザプライオリティを本欄に指定した値に書き換える場合に使用します。入力しない場合、パケットはスイッチによって送信される前に書き換えた 802.1p ユーザプライオリティとなります。プライオリティキュー、CoS キュー、802.1p への割り当てに関する詳しい説明は本マニュアル 150 ページの「第 8 章 QoS（QoS 機能の設定）」 を参照してください。
Replace Priority	チェックボックスをクリックし、本画面で設定した基準に一致するパケットが、指定された CoS キューに送られる前に、パケットの 802.1p ユーザプライオリティを、「Priority」欄に指定した値に書き換える場合に使用します。チェックしない場合、パケットはスイッチによって送信される前に書き換えた 802.1p ユーザプライオリティとなります。
Replace DSCP(0-63)	本オプションを選択すると、スイッチは本画面で指定した基準に一致するパケットの DSCP をチェックボックスの右側の欄に指定した値に書き換えます。
Time Range Name	チェックボックスをクリックし、「Time Range」画面に設定済みのタイムレンジ設定名を入力します。このアクセスルールをスイッチで実行する場合、ここに特定の時間を設定します。
Counter	「Counter」機能を「Enabled」（有効）/「Disabled」（無効）にします。カウンタ機能は、アクセスルールに一致するパケット数を記録するために使用されます。本機能はオプションです。初期値は無効です。
Ports	アクセスルールを設定するポート範囲を指定します。

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。

作成したルールの詳細の参照

「Access Rule List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

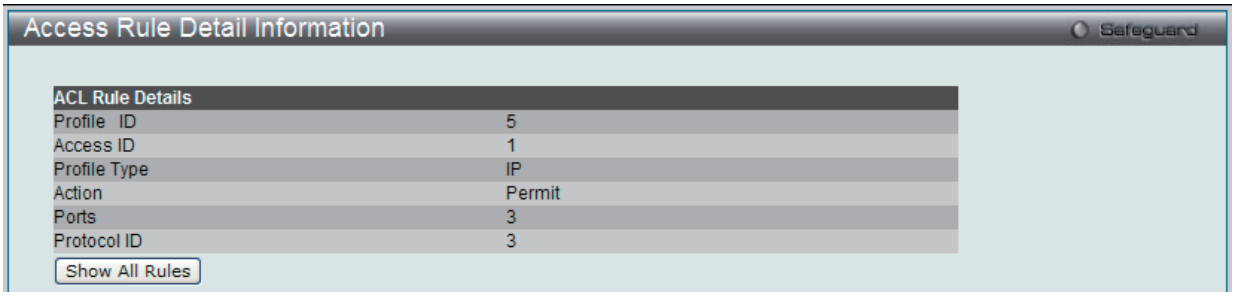


図 10-15 Access Rule Detail Information - IP 画面

「Show All Rules」ボタンをクリックすると、「Access Rule List」画面に戻ります。

アクセスプロファイルリストの作成（IPv6）

アクセスプロファイルを作成し、プロファイルにルールを作成します。

ACL > Access Profile 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。1 つのアクセスプロファイルが説明のために作成されています。

図 10-16 Access Profile List 画面

エントリの削除

エントリの削除は、エントリ横の「Delete」ボタンをクリックします。すべてのアクセスプロファイルの削除は、「Delete All」ボタンをクリックします。

エントリの追加

「Access Profile List」にエントリを追加するには、「Add ACL Profile」で「IPv6 ACL」ボタンをチェック後、隣接する欄で設定するフレームヘッダ（TCP または UDP）選択して「Select」ボタンをクリックします。

IPv6 の「Add ACL Profile」画面

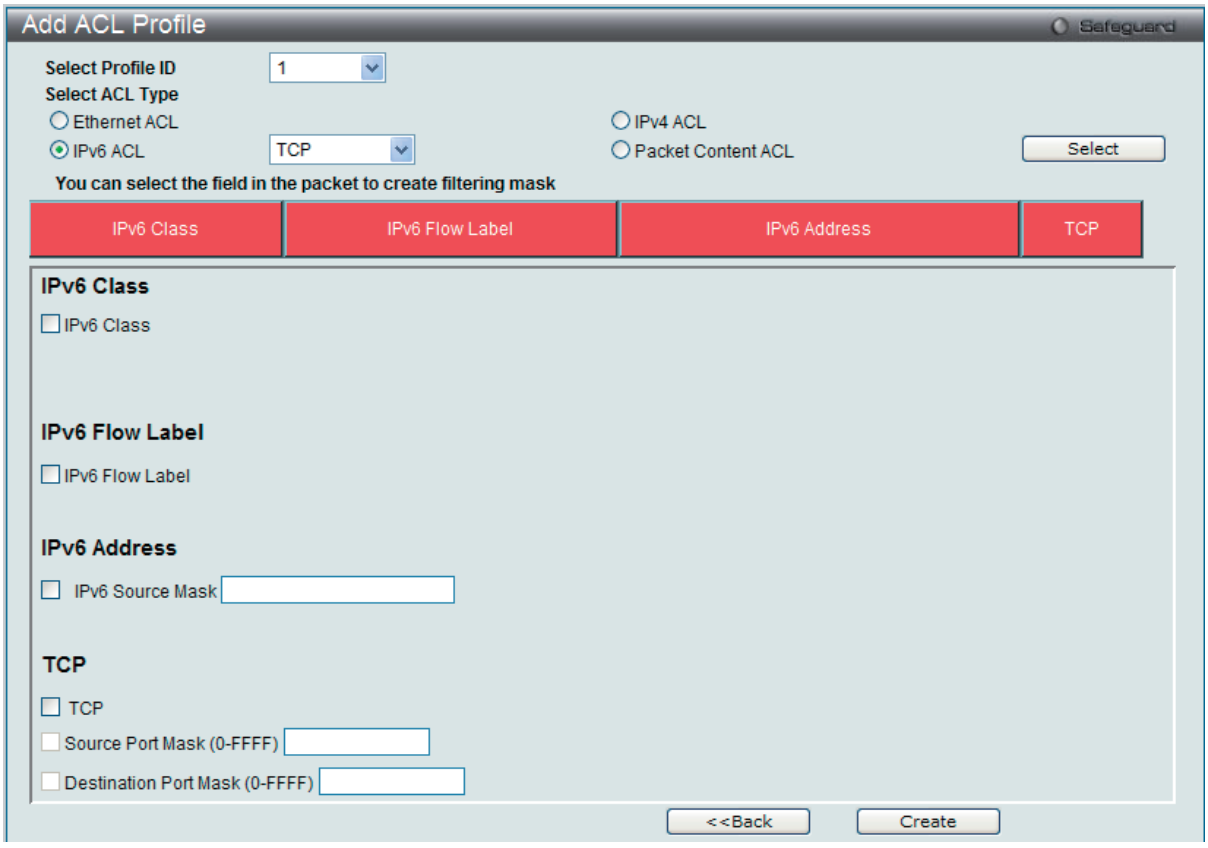


図 10-17 Add ACL Profile - IPv6 ACL 画面

「Profile ID」でプロファイル番号を 1-512 から選択し、「Select ACL Type」をチェック後、「Select」ボタンをクリックすることで画面を切り替えることができます。画面上部のボックスをクリックすると、赤色に変わり、設定用項目が表示されます。

以下の項目を IPv6 ACL タイプに設定します。

項目	説明
Select Profile ID	プロファイル設定のための固有の識別番号を指定します。1 から 512 が指定できます。
Select ACL Type	Ethernet（MAC アドレス）、IPv4 アドレス、IPv6 アドレスまたはパケットコンテンツの中からプロファイルのベースを指定します。Type の変更に伴いメニューも変わります。ここでは「IPv6 ACL」を選択します。 • IPv6 ACL - フレームヘッダの IPv6 アドレスを検証します。
以下のオプションを指定すると各フレームヘッダのプロトコルタイプを調べます。転送基準にどのようなプロトコルを含めるかを指定します。	
IPv6 Class	この項目を選ぶと IPv6 ヘッダの「Class」を調べます。「Class」は IPv4 における「Type of Service」（ToS）、「Precedence bits」のようなパケットヘッダの一部です。
IPv6 Flow Label	この項目を選ぶと IPv6 ヘッダの「flow label」を調べます。「flow label」は送信元で順番につけられる QoS やリアルタイムサービスパケットのためのデフォルトではない項目です。
IPv6 Address	• IPv6 Source Mask - ボックスにチェックをつけて送信元 IPv6 アドレスをマスクする IP アドレスを指定します。
TCP	• TCP - TCP トラフィックに適用するルールを指定します。 • Source Port Mask (0-FFFF) - TCP 送信元ポートマスクを指定します。 • Destination Port Mask (0-FFFF) - TCP 宛先ポートマスクを指定します。
UDP	UDP - ルールを UDP トラフィックに適用するように指定します。 • Source Port Mask (0-FFFF) - UDP 送信元ポートマスクを指定します。 • Destination Port Mask (0-FFFF) - UDP 宛先ポートマスクを指定します。

「Create」ボタンをクリックし、設定を適用します。

作成したプロファイルの詳細の参照

作成したプロファイルの詳細を参照する場合は、「Access Profile List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

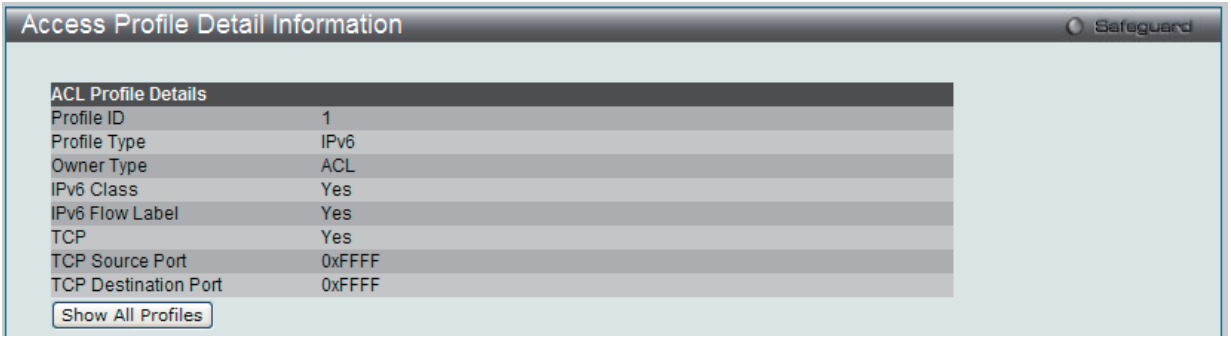


図 10-18　Access Profile Detail Information - IPv6 ACL 画面

「Show All Profiles」ボタンをクリックすると、「Access Profile List」画面に戻ります。

作成したアクセスプロファイルに対するルールの設定手順（IPv6）：

IPv6 アクセスルールの設定

1. 「Access Profile List」画面を表示します。

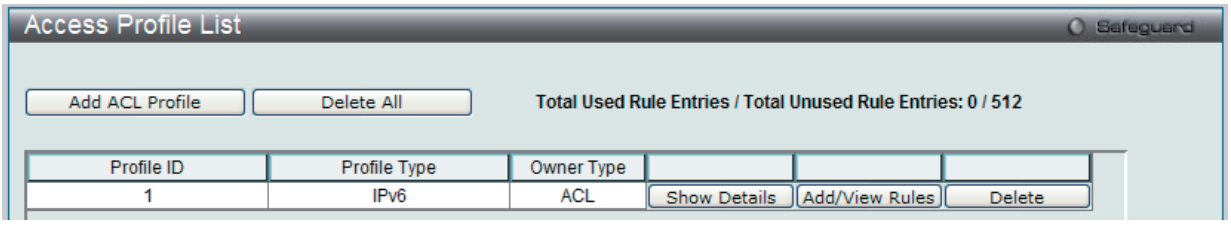


図 10-19　Access Profile List 画面

2. 「Access Profile List」画面を表示し、IPv6 エントリの「Add/View Rules」ボタンをクリックして以下の画面を表示します。

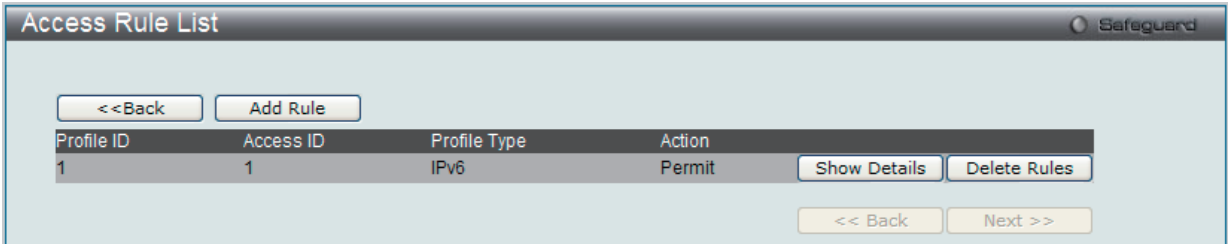


図 10-20　Access Rule List - IPv6 画面

作成済みのルールの削除
該当の「Delete Rules」ボタンをクリックします。

ルールの新規登録
新しいルールを作成するためには、「Add Rule」ボタンをクリックします。

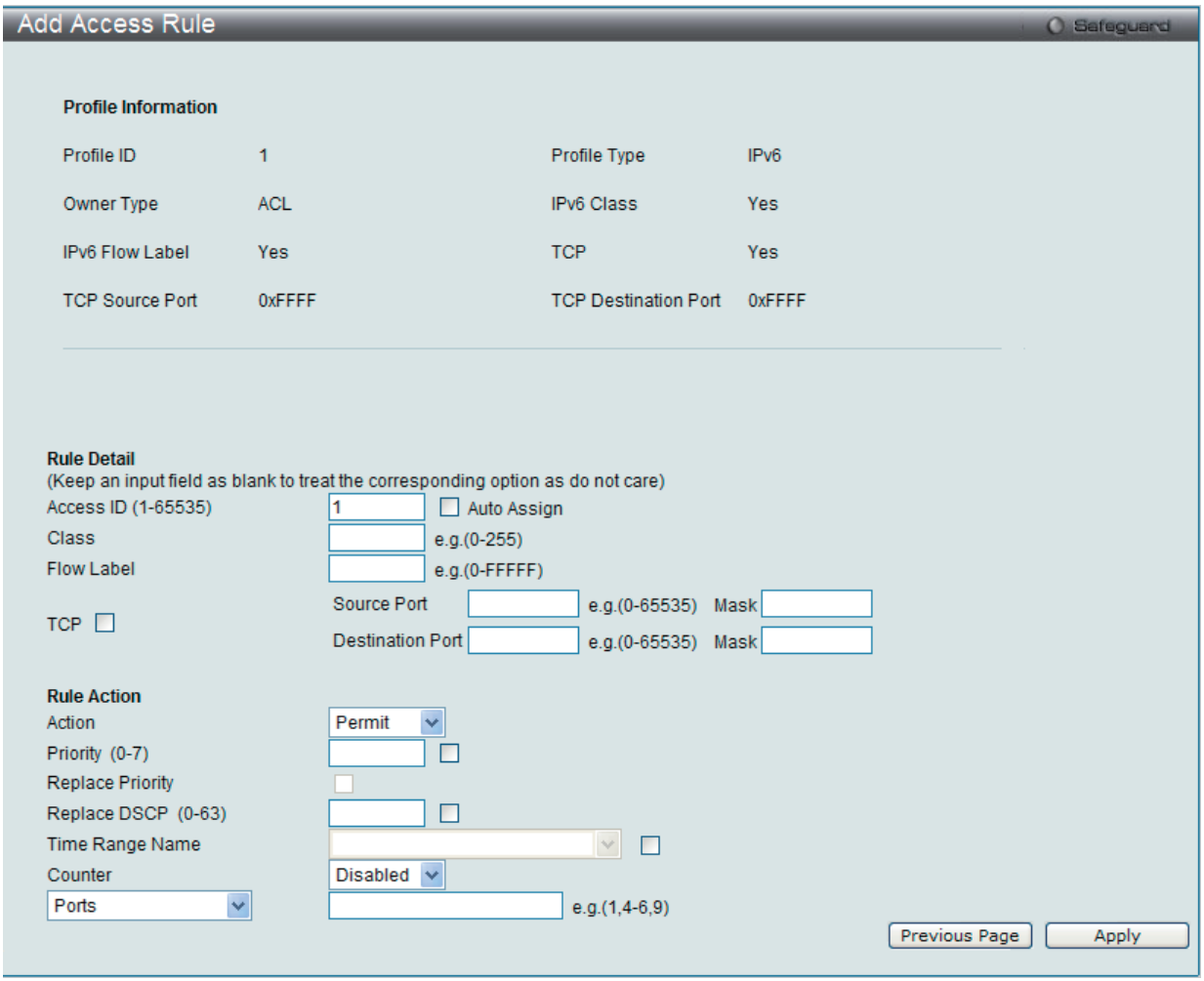


図 10-21　Add Access Rule - IPv6 画面

以下の項目を設定します。

項目	説明
Rule Detail	
Access ID (1-65535)	プロファイル設定のための固有の識別番号を指定します。1 から 65535 が指定できます。 • Auto Assign - 本項目をチェックするとスイッチは自動的に作成されるルールに Access ID を割り当てます。
Class	クラスを入力し、IPv6 ヘッダの「Class」フィールドを調べます。本フィールドは IPv4 における「Type of Service(ToS)」、「Precedence bits」フィールドのようなパケットヘッダの一部です。
Flow Label	IPv6 フローラベルマスクを指定します。0-FFFFF の範囲で指定します。
IPv6 Source Address	IPv6 送信元アドレスの IPv6 アドレスを入力します。
IPv6 Source Mask	IPv6 送信元サブマスクを指定します。送信元 IPv6 アドレスの最後の 44 ビット (LSB) のフィルタリングのみを行います。
TCP	• Source Port - IPv6 L4 TCP 送信元ポートサブマスクを指定します。 • Destination Port - IPv6 L4 TCP 送信先ポートサブマスクを指定します。
UDP	• Source Port - IPv6 L4 UDP 送信元ポートサブマスクを指定します。 • Destination Port - IPv6 L4 UDP 送信先ポートサブマスクを指定します。

項目	説明
Rule Action	
Action	• Permit - アクセスプロファイルにマッチしたパケットを転送します。この時新しいルールが追加されることがあります（以下参照）。 • Deny - アクセスプロファイルに一致したパケットは転送せずにフィルタリングします。 • Mirror - アクセスプロファイルに一致するパケットを「Port Mirroring」画面で定義したポートにミラーリングします。Port Mirroring が有効で、ターゲットポートに設定されている必要があります。
Priority (0-7)	本画面で設定した基準に一致するパケットが指定されたCoSキューに送られる前に、パケットの802.1pユーザプライオリティを本欄に指定した値に書き換える場合に使用します。入力しない場合、パケットはスイッチによって送信される前に書き換えた 802.1p ユーザプライオリティとなります。プライオリティキュー、CoS キュー、802.1p への割り当てに関する詳しい説明は本マニュアル 150 ページの「第 8 章 QoS（QoS 機能の設定）」を参照してください。
Replace Priority	チェックボックスをクリックし、本画面で設定した基準に一致するパケットが、指定された CoS キューに送られる前に、パケットの 802.1p ユーザプライオリティを、「Priority」欄に指定した値に書き換える場合に使用します。チェックしない場合、パケットはスイッチによって送信される前に書き換えた 802.1p ユーザプライオリティとなります。
Replace DSCP (0-63)	本オプションを選択すると、スイッチは本画面で指定した基準に一致するパケットの DSCP をチェックボックスの右側の欄に指定した値に書き換えます。
Time Range Name	チェックボックスをクリックし、「Time Range」画面に設定済みのタイムレンジ設定名を入力します。このアクセスルールをスイッチで実行する場合、ここに特定の時間を設定します。
Counter	プルダウンメニューを使用して、「Counter」機能を「Enabled」(有効)/「Disabled」(無効) にします。
Ports	アクセスルールを設定するポート範囲を指定します。

IPv6 のアクセスルールを設定するためには、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。

作成したルールの詳細の参照

「Access Rule List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

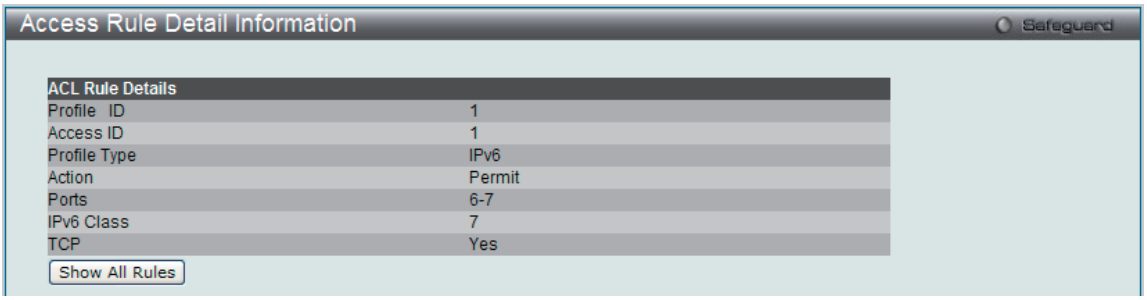


図 10-22 Access Rule Detail Information - IPv6 画面

「Show All Rules」ボタンをクリックすると、「Access Rule List」画面に戻ります。

アクセスプロファイルリストの作成（パケットコンテンツ）

アクセスプロファイルを作成し、プロファイルにルールを作成します。

ACL > Access Profile 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。 1 つのアクセスプロファイルが説明のために作成されています。

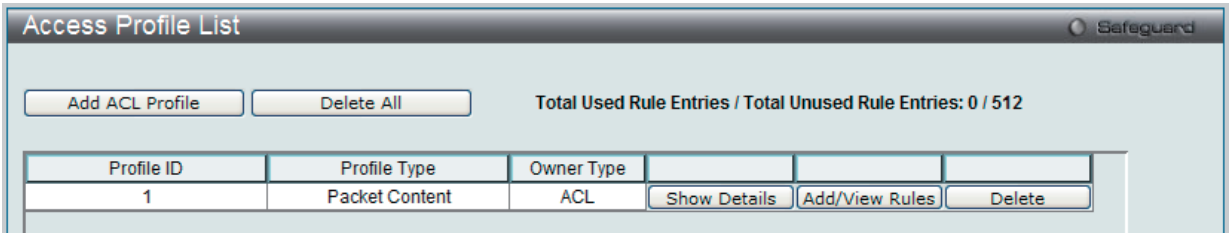


図 10-23　Access Profile List 画面

エントリの削除

エントリを削除するためには、エントリ横の「Delete」ボタンをクリックします。すべてのアクセスプロファイルを削除するためには、「Delete All」ボタンをクリックします。

エントリの追加

「Access Profile List」にエントリを追加するには、「Add ACL Profile」ボタンをクリックし、以下の画面を表示します。

パケットコンテンツの「Add ACL Profile」画面

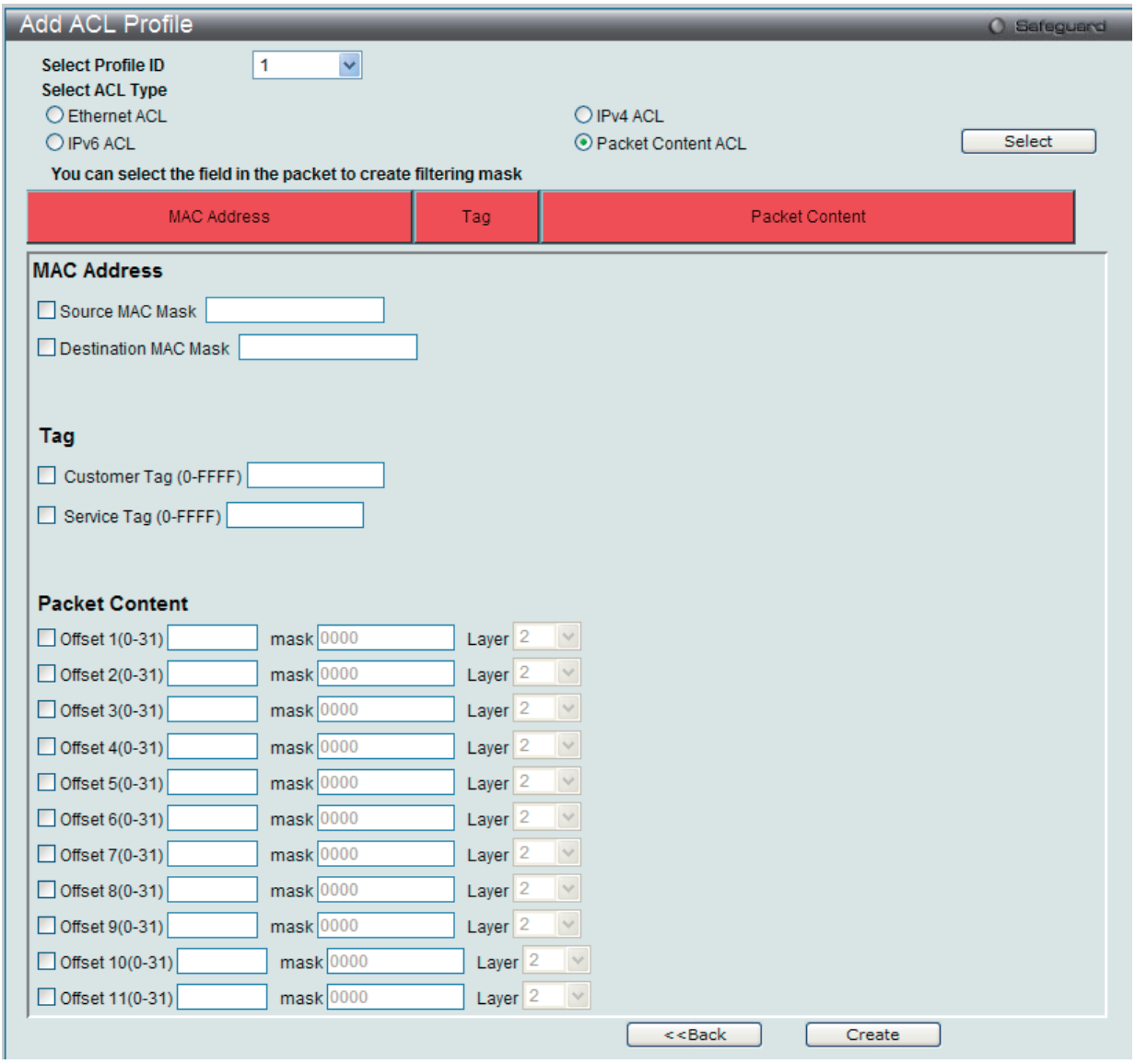


図 10-24　Add ACL Profile 画面 - パケットコンテンツ

「Profile ID」でプロファイル番号を 1-512 から選択し、「Select ACL Type」で「Packet Content ACL」をチェック後、「Select」ボタンをクリックします。画面上部のボックスをクリックすると、赤色に変わり、設定用項目が表示されます。

以下の項目をパケットコンテンツタイプに設定します。

項目	説明
Select Profile ID	プロファイル設定のための固有の識別番号を指定します。1 から 200 が指定できます。
Select ACL Type	Ethernet（MAC アドレス）、IPv4 アドレス、IPv6 アドレスまたはパケットコンテンツの中からプロファイルのベースを指定します。Type の変更に伴いメニューも変わります。ここでは「Packet Content」を選択します。 • Packet Content - フレームヘッダのパケットコンテンツを検証します。
MAC Address	送信元 MAC マスクをクリックして、MAC アドレスマスクを入力します。 • Source MAC Mask - MAC 送信元アドレスマスクを指定します。 • Destination MAC Mask - MAC 送信先アドレスマスクを指定します。
Tag	• Customer Tag (0-FFFF) - 適切なカスタマタグを 16 進数 (0x0-0xffff) で指定します。 • Service Tag (0-FFFF) - 適切なサービスタグを 16 進数 (0x0-0xffff) で指定します。
Packet Content	これは、ユーザに同時にパケット内の指定された 11 個のオフセットパケットコンテンツチャンクの検証を許可し、そのフレームコンテンツオフセット、マスクおよびレイヤを指定します。設定可能な 11 個のパケットコンテンツチャンクオフセットがあります。パケットコンテンツチャンクマスクは 2 バイトを提供します。最大 11 個のパケットコンテンツオフセットチャンクを選択することが可能です。 Offset 1 (0-31) ～ Offset 11 (0-31)、mask、Layer を指定します。 D-Link スイッチファミリは、高度なパケットコンテンツマスク (またはパケットコンテンツアクセスコントロールリスト -ACL として知られる) 機能を使用して、現在広く蔓延する ARP Spoofing などの一般的なネットワーク攻撃を効果的に軽減することができます。このため、パケットコンテンツ ACL が異なるプロトコル層におけるパケットのどんな指定コンテンツも検証できます。

「Apply」ボタンをクリックし、変更を有効にします。

作成したプロファイルの詳細の参照

作成したプロファイル設定を参照するためには、「Access Profile List」画面の対応する「Show Details」ボタンをクリックし、以下の画面を表示します。

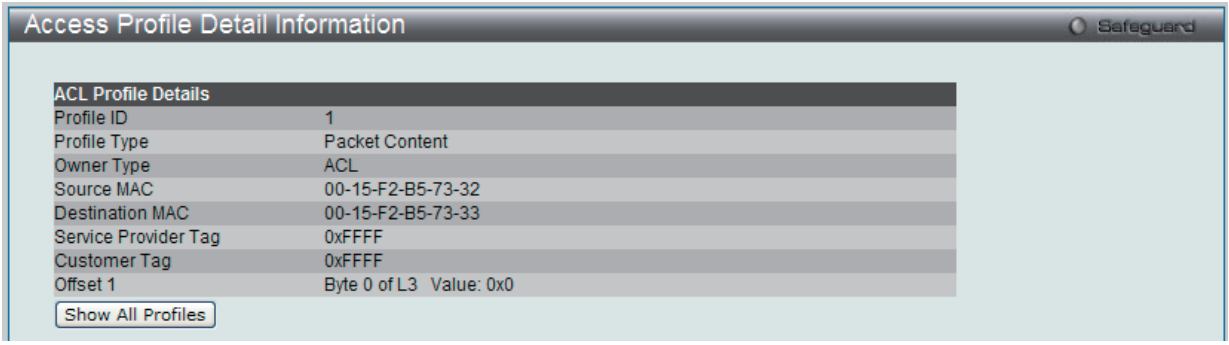


図 10-25 Access Profile Detail Information 画面 - パケットコンテンツ

「Show All Profiles」ボタンをクリックすると、「Access Profile List」画面に戻ります。

作成したアクセスプロファイルに対するルールの設定手順（パケットコンテンツ）：

パケットコンテンツアクセスルールの設定

1. 「Access Profile List」画面を表示します。

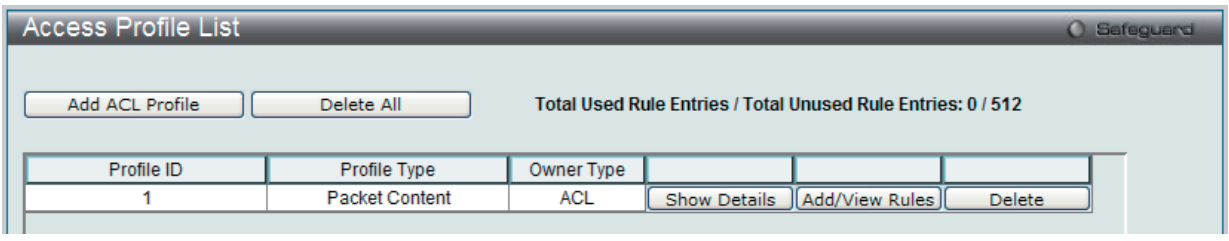


図 10-26 Access Profile List 画面

2. 「Access Profile List」画面を表示し、パケットコンテンツエントリの「Add/View Rules」ボタンをクリックして以下の画面を表示します。

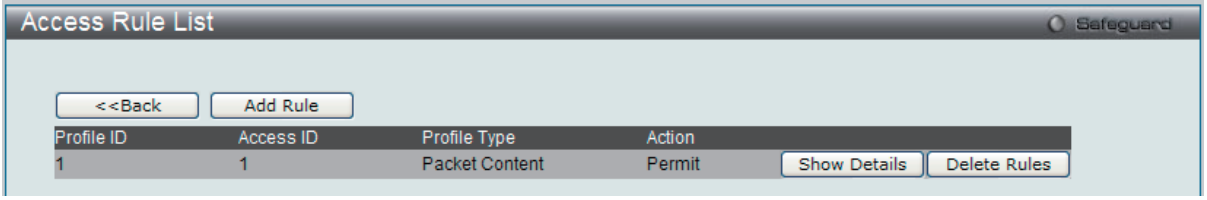


図 10-27 Access Rule List 画面 - パケットコンテンツ

既に作成したルールの削除
該当の「Delete Rules」ボタンをクリックします。

ルールの新規作成
新しいルールを作成するためには、「Add Rule」ボタンをクリックし、以下の画面を表示します。

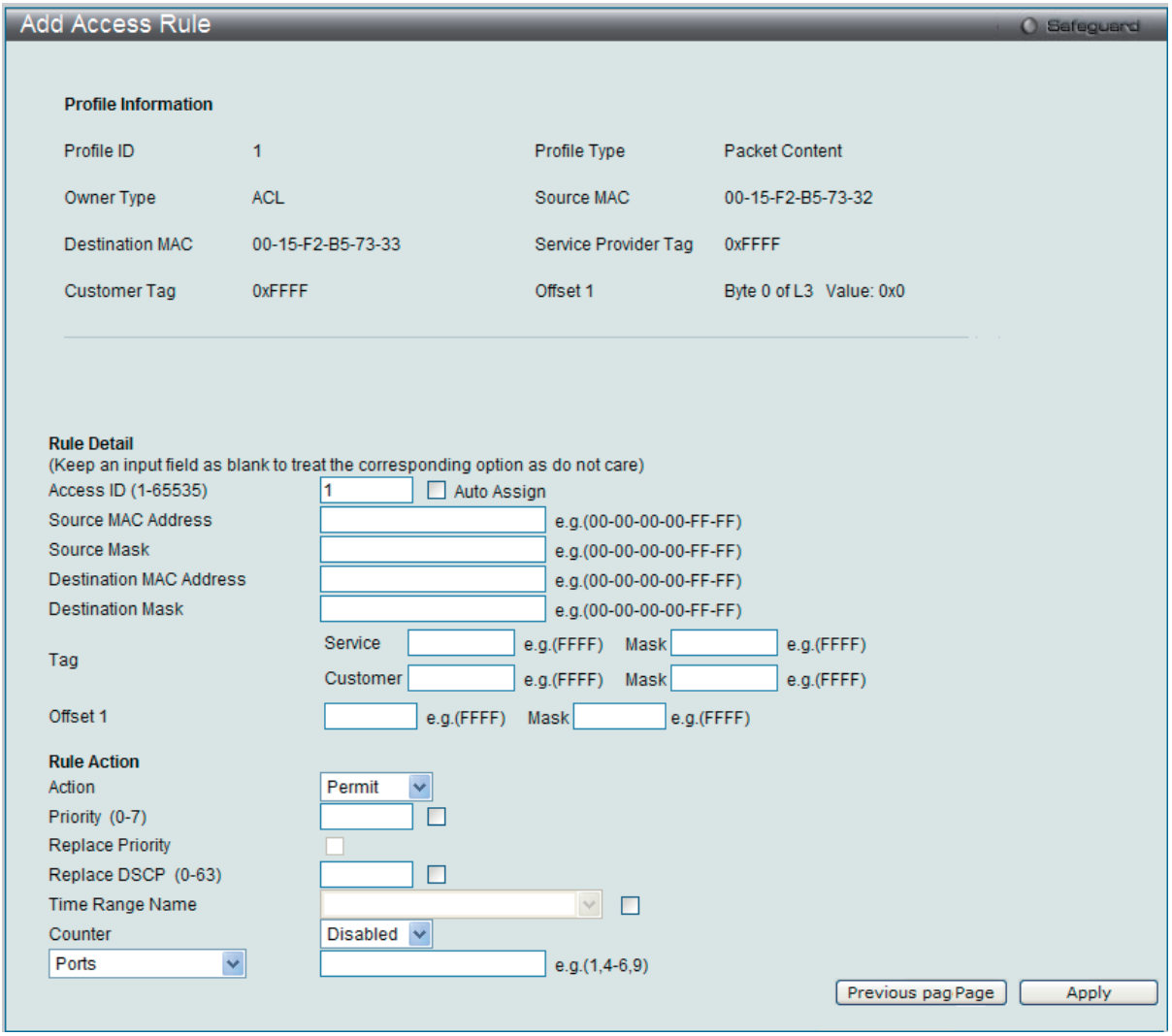


図 10-28　Add Access Rule 画面 - パケットコンテンツ

以下の項目を設定します。

項目	説明
Rule Detail	
Access ID (1-65535)	プロファイル設定のための固有の識別番号を指定します。1 から 65535 が指定できます。 • Auto Assign - 本項目をチェックするとスイッチは自動的に作成されるルールに Access ID を割り当てます。
Source MAC Address	調べる必要のあるパケットの送信元 MAC アドレスを指定します。
Source Mask	送信元 MAC アドレスのマスクを指定します。このマスクと送信元 MAC アドレスの AND 演算の結果、フィルタリングを行います。
Destination MAC Address	調べる必要のあるパケットの送信先 MAC アドレスを指定します。
Destination Mask	送信先 MAC アドレスのマスクを入力します。このマスクと送信先 MAC アドレスの AND 演算の結果、フィルタリングを行います。
Tag	「Customer」と「Service」に調べる必要のあるカスタマとサービスタグの値を指定します。「Mask」オプションはタグ値をマスクする場合に使用します。カスタマ / サービスタグ値と対応するマスクの AND 演算の結果、最終的なフィルタリングを行います。
Offset	調べる必要のある 2 バイトの値を指定します。マスクオプションは 2 バイトの値をマスクする場合に使用します。2 バイトの値と対応するマスクの AND 演算の結果、最終的なフィルタリングを行います。

項目	説明
Rule Action	
Action	• Permit - アクセスプロファイルにマッチしたパケットを転送します。この時新しいルールが追加されることがあります（以下参照）。 • Deny - アクセスプロファイルに一致したパケットは転送せずにフィルタリングします。 • Mirror - アクセスプロファイルに一致するパケットを「Port Mirroring」画面で定義したポートにミラーリングします。Port Mirroring が有効で、ターゲットポートに設定されている必要があります。
Priority (0-7)	本画面で設定した基準に一致するパケットが指定された CoS キューに送られる前に、パケットの 802.1p ユーザプライオリティを本欄に指定した値に書き換える場合に使用します。入力しない場合、パケットはスイッチによって送信される前に書き換えた 802.1p ユーザプライオリティとなります。プライオリティキュー、CoS キュー、802.1p への割り当てに関する詳しい説明は本マニュアル 150 ページの「第 8 章 QoS（QoS 機能の設定）」を参照してください。
Replace Priority	チェックボックスをクリックし、本画面で設定した基準に一致するパケットが、指定された CoS キューに送られる前に、パケットの 802.1p ユーザプライオリティを、「Priority」欄に指定した値に書き換える場合に使用します。チェックしない場合、パケットはスイッチによって送信される前に書き換えた 802.1p ユーザプライオリティとなります。
Replace DSCP (0-63)	DSCP 値を指定するとそれぞれのパケットヘッダの DiffServ コードを調べて、部分的もしくは全体を転送基準として使用します。0 から 63 まで指定できます。
Time Range Name	チェックボックスをクリックし、「Time Range」画面に設定済みのタイムレンジ設定名を入力します。このアクセスルールをスイッチで実行する場合、ここに特定の時間を設定します。
Counter	プルダウンメニューを使用して、「Counter」機能を「Enabled」(有効)/「Disabled」(無効) にします。
Ports	アクセスルールを設定するポート範囲を指定します。

パケットコンテンツマスクのアクセスルールを設定するためには、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。

作成したルールの詳細の参照

「Access Rule List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

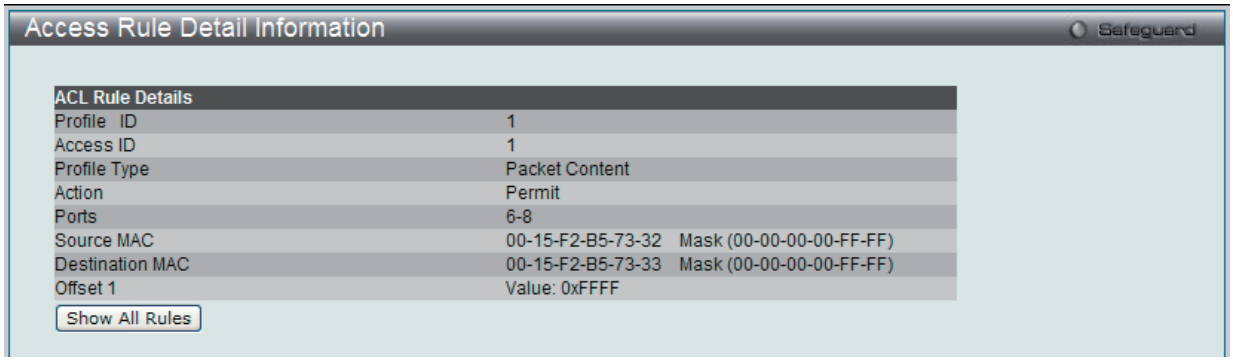


図 10-29 Access Rule Detail Information - パケットコンテンツ画面

「Show All Rules」ボタンをクリックすると、「Access Rule List」画面に戻ります。

注意 ARP（Address Resolution Protocol）は、ホストのハードウェアアドレス（MAC アドレス）を検索するための標準規格です。しかし、LAN を攻撃する（つまり、ARP スプーフィング攻撃）ために容易に利用できるため、ARP は被害を受けやすいという弱点があります。ARP プロトコルの動作方法、および ARP spoofing 攻撃を防ぐために D-Link 独自のパケットコンテンツ ACL を使用する方法について本マニュアル 83 ページの「ARP Spoofing Prevention Settings（ARP Spoofing 防止設定）」を参照してください。

CPU Access Profile List（CPU アクセスプロファイルリスト）

CPU インタフェースフィルタリング

チップセットの制限やスイッチのセキュリティの必要性などから、本スイッチは、CPU インタフェースフィルタリング機能を持っています。この追加機能によって CPU インタフェース向けのパケットアクセスルールリストの作成が可能になり、動作時のセキュリティが高くなります。既に説明したアクセスプロファイル機能と似た方法で CPU インタフェースフィルタリングは CPU に到達するイーサネット、IP およびパケットコンテンツマスクのパケットヘッダを調べて、ユーザ設定に基づきそれらを転送もしくはフィルタリングします。そして CPU フィルタリングの追加機能として、CPU フィルタリングでは多彩なルールのリストをあらかじめ用意しておき、必要に応じてグローバルに有効 / 無効を設定することができます。

CPU 用のアクセスプロファイルの作成は 2 段階に分かれます。はじめにフレームのどの部分を調べるのか、送信元 MAC アドレスか、送信先 IP アドレスか、などを決定します。次に、そのフレームに対してどのような処理を行うのかという基準になる値を入力します。詳しくは以下で 2 つに分けて説明します。

スイッチは、4 つの CPU アクセスプロファイルタイプ（イーサネット（MAC アドレスベース）プロファイル設定、IP（IPv4）アドレスベースのプロファイル設定、IP（IPv6）アドレスベースのプロファイル設定、パケットコンテンツのマスク設定）をサポートしています。

CPU アクセスプロファイルの作成（Ethernet）

CPU アクセスプロファイルを作成し、プロファイルにルールを作成します。

以下の画面では、ラジオボタンを使用し、CPU Interface Filtering State をグローバルに有効または無効にし、動作状態の変更をします。

ACL > CPU Access Profile List の順でメニューをクリックし、以下の画面を表示します。

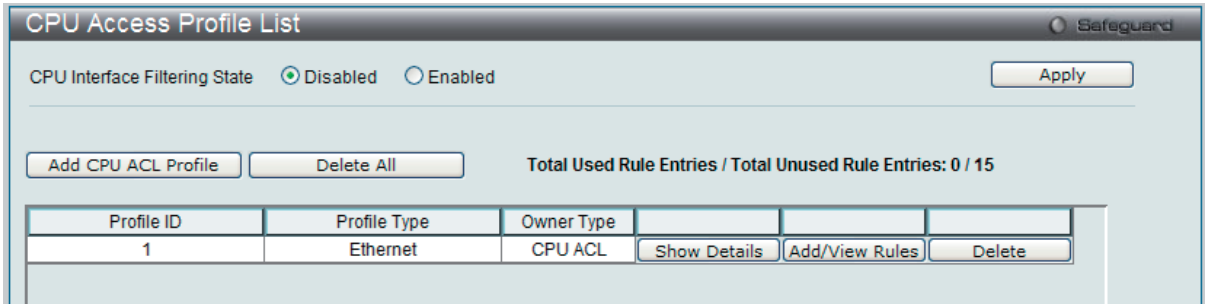


図 10-30　CPU Access Profile List 画面

スイッチに作成した CPU アクセスプロファイルリストを表示します。各タイプに 1 つのアクセスプロファイルが説明のために作成されています。「CPU Interface Filtering State」に「Enabled」を選択すると、スイッチは CPU パケットを詳しく調べます。また、「Disabled」を選択すると、調べません。

エントリの設定の参照

該当の「Show Details」ボタンをクリックします。

CPU Access Profile List のエントリの削除

エントリを削除するためには、エントリ横の「Delete」ボタンをクリックします。すべてのエントリを削除するためには、「Delete All」ボタンをクリックします。

CPU アクセスプロファイルリストの新規登録

「Add CPU ACL Profile」ボタンをクリックし、以下の画面を表示します。

イーサネットの「Add CPU ACL Profile」画面

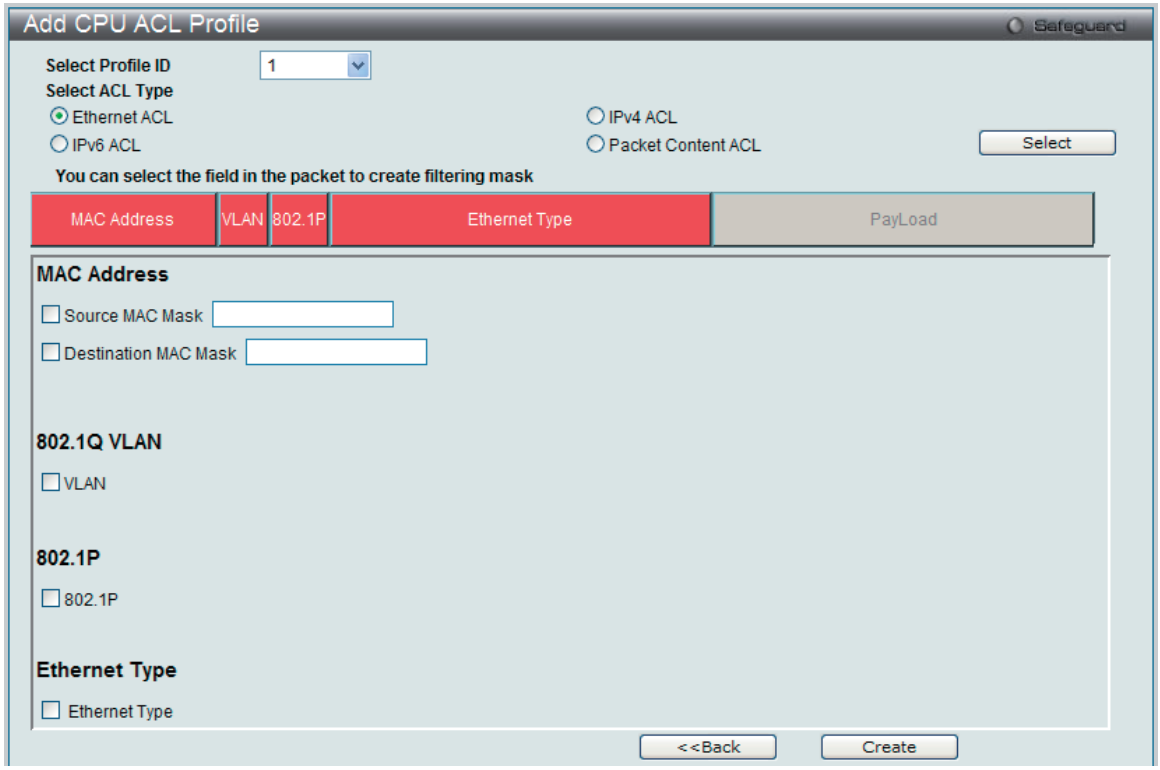


図 10-31　Add CPU ACL Profile - Ethernet 画面

「Add CPU ACL」画面で「Select Profile ID」（プロファイル ID）を指定し、「Select All Type」（ACL タイプ）に「Ether ACL」を選択して「Select」ボタンをクリックします。画面上部のボックスをクリックすると赤色に変わり、設定用項目が表示されます。

以下の項目を設定します。

項目	説明
Select Profile ID	プロファイルのための固有の識別番号を指定します。1 から 3 が指定できます。
Select ACL Type	Ethernet（MAC アドレス）、IPv4 アドレス、IPv6 アドレス、または Packet Content の中からプロファイルのベースを指定します。Type の変更に伴いメニューも変わります。ここでは「Ethernet」を選択します。 • Ethernet - パケットヘッダのレイヤ 2 部分を対象にします。
以下のオプションを指定すると各フレームヘッダのプロトコルタイプを調べます。基準にどのようなプロトコルを含めるかを指定します。	
MAC Address	• Source MAC Mask - 送信元 MAC アドレスをマスクする MAC アドレスを指定します。 • Destination MAC Mask - 送信先 MAC アドレスをマスクする MAC アドレスを指定します。
802.1Q VLAN	パケットヘッダの VLAN 識別子を調べて、部分的もしくは全体を転送基準として使用します。
802.1P	アクセスルールを設定する 802.1p プライオリティ値を指定できるようになります。
Ethernet Type	各フレームヘッダの Ethernet Type 値を調べます。

「Create」ボタンをクリックし、このエントリをスイッチに保存します。

作成したプロファイルの詳細の参照

「CPU Access Profile List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

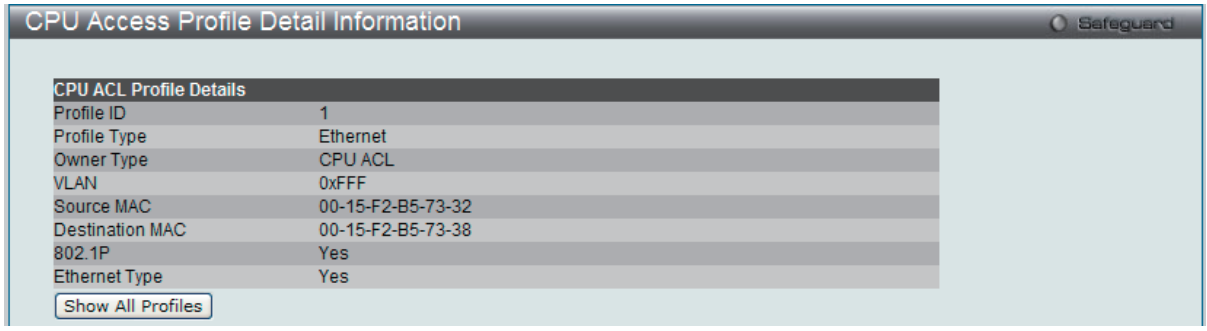


図 10-32　CPU Access Profile Detail Information - Ethernet 画面

「Show All Profiles」ボタンをクリックすると、「CPU Access Profile List」画面に戻ります。

作成した CPU アクセスプロファイルに対するルールの設定手順（Ethernet）

Ethernet アクセスルールの設定

1. 「CPU Access Profile List」画面を表示します。

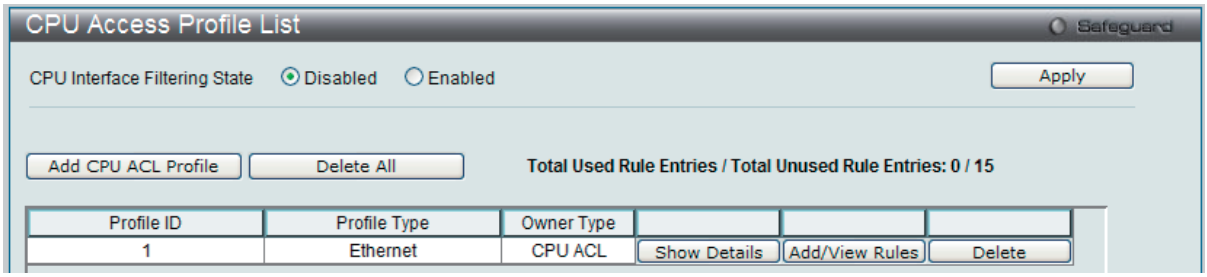


図 10-33 CPU Access Profile List 画面

2. 「CPU Access Profile List」画面を表示し、イーサネットエントリの「Add/View Rules」ボタンをクリックして以下の画面を表示します。

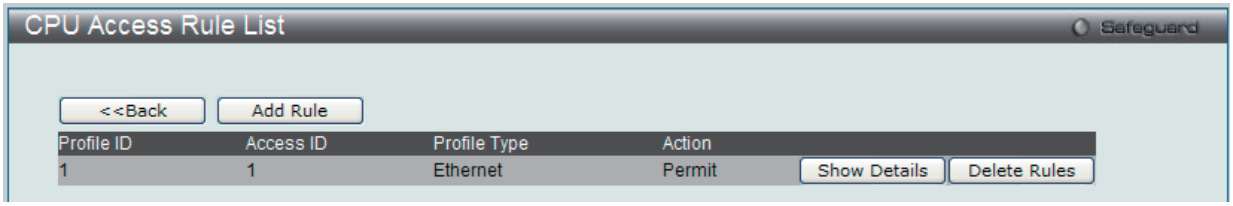


図 10-34 CPU Access Rule List - Ethernet 画面

既に作成したルールの削除

該当の「Delete Rules」ボタンをクリックします。

新しいルールの作成

「Add Rule」ボタンをクリックし、以下の画面を表示します。

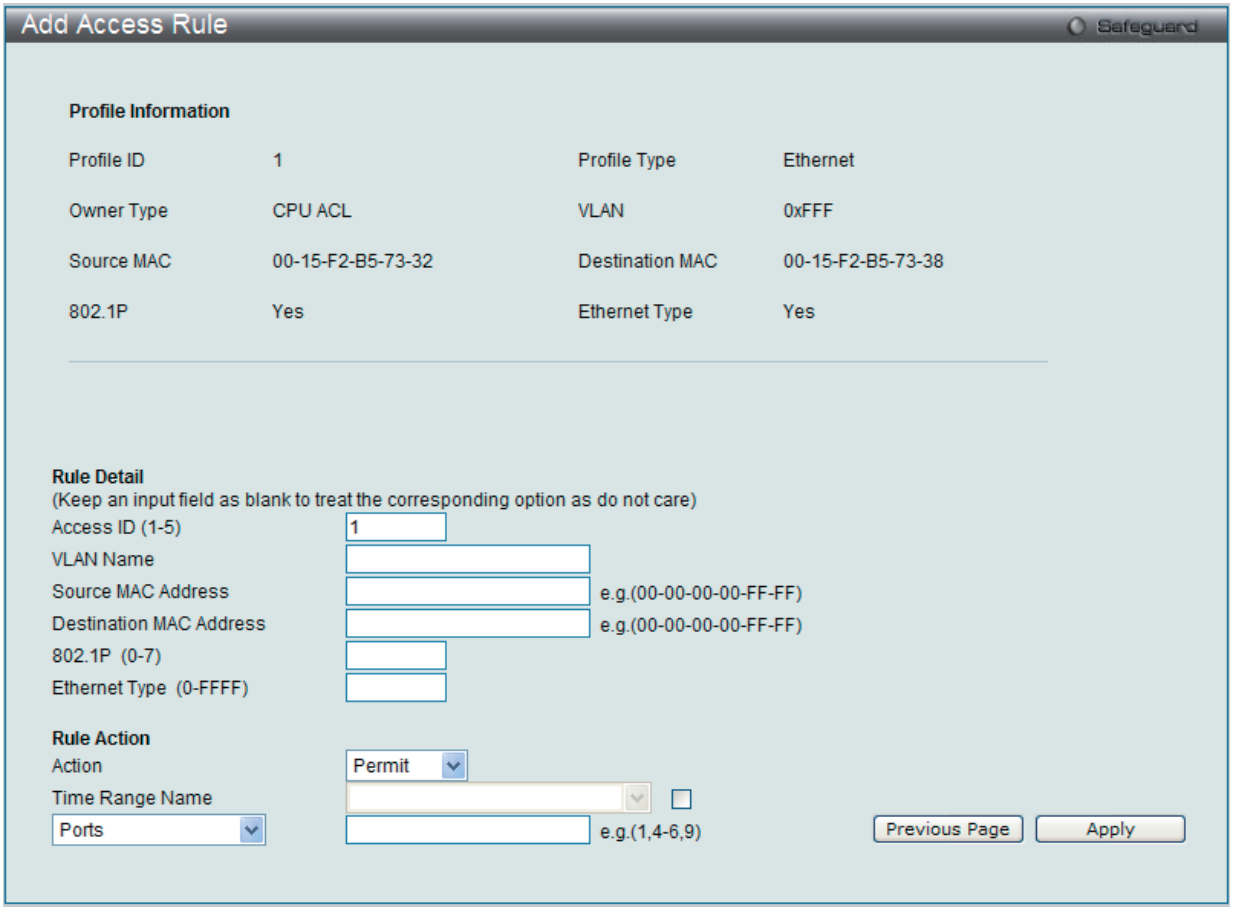


図 10-35 Add Access Rule - Ethernet 画面

以下の項目を設定します。

項目	説明
Rule Action	
Access ID (1-5)	それぞれのルールに固有の番号を指定します。1 から 5 が指定できます。
VLAN Name	設定済みの VLAN 名を入力します。スイッチはパケットヘッダの VLAN を確認し、その結果をパケット送信の基準 (または基準の一部) とします。
Source MAC Address	送信元 MAC アドレスの MAC アドレスマスクを指定します。
Destination MAC Address	送信先 MAC アドレスの MAC アドレスマスクを入力します。
802.1p (0-7)	• アクセスプロファイルは、ここで指定する 802.1p プライオリティ値 (0-7) を持つパケットにのみ適用されます。
Ethernet Type (0-FFFF)	アクセスプロファイルが適用されるパケットヘッダの 802.1Q イーサネットタイプの値を 16 進数（hex 0x0-0xffff）で指定します。イーサネットタイプは次の形式で指定します。: hex 0x0-0xffff（a-f の半角英文字、と 0-9999 の数字を使用します。）
Rule Action	
Action	• Permit - アクセスプロファイルにマッチしたパケットを転送します。この時新しいルールが追加されることがあります（以下参照）。 • Deny - Deny- スイッチはアクセスプロファイルに一致するパケットを送信せずにフィルタリングします。 • Mirror- スイッチはアクセスプロファイルに一致するパケットを「Port Mirroring」画面で定義したポートにミラーリングします。ポートミラーリングが有効で、ターゲットポートが設定されている必要があります。
Time Range Name	チェックボックスをクリックし、「Time Range」画面に設定済みのタイムレンジ設定名を入力します。このアクセスルールをスイッチで実行する場合、ここに特定の時間を設定します。
Ports	設定するポート範囲を指定します。

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。

作成したルールの詳細の参照

「CPU Access Rule List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

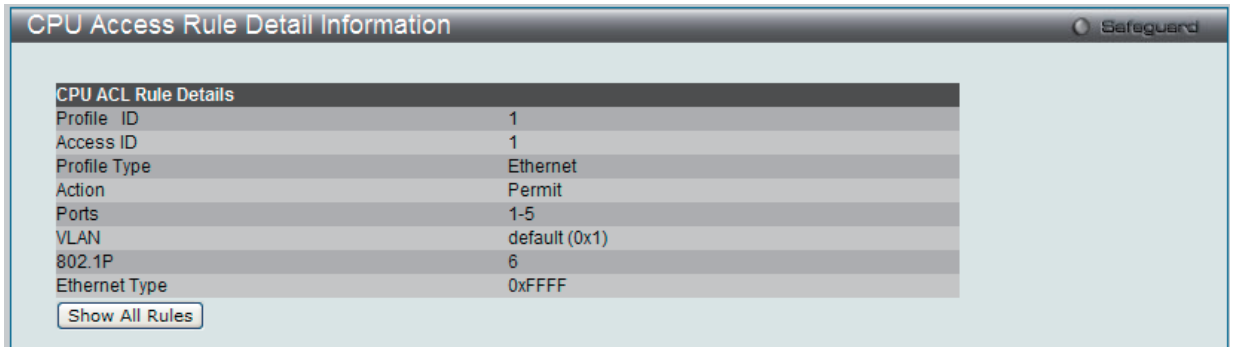


図 10-36 CPU Access Rule Detail Information - Ethernet 画面

「Show All Rules」ボタンをクリックすると、「CPU Access Rule List」画面に戻ります。

CPU アクセスプロファイルの作成（IPv4）

CPU アクセスプロファイルを作成し、プロファイルにルールを作成します。

以下の画面では、ラジオボタンを使用し、CPU Interface Filtering State をグローバルに有効または無効にし、動作状態の変更をします。

ACL > CPU Access Profile List の順でメニューをクリックし、以下の画面を表示します。

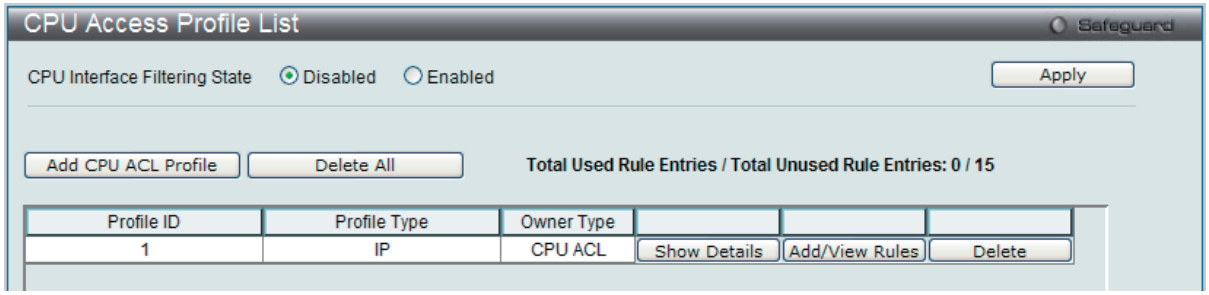


図 10-37 CPU Access Profile List 画面

スイッチに作成した CPU アクセスプロファイルリストを表示します。1 つのアクセスプロファイルが説明のために作成されています。「CPU Interface Filtering State」に「Enabled」を選択すると、スイッチは CPU パケットを詳しく調べます。また、「Disabled」を選択すると、調べません。

エントリの設定の参照
該当の「Show Details」ボタンをクリックします。

CPU Access Profile List のエントリの削除
エントリを削除するためには、エントリ横の「Delete」ボタンをクリックします。すべてのエントリを削除するためには、「Delete All」ボタンをクリックします。

CPU アクセスプロファイルリストの新規登録
「Add CPU ACL Profile」ボタンをクリックし、以下の画面を表示します。

IPv4 の「Add CPU ACL Profile」画面

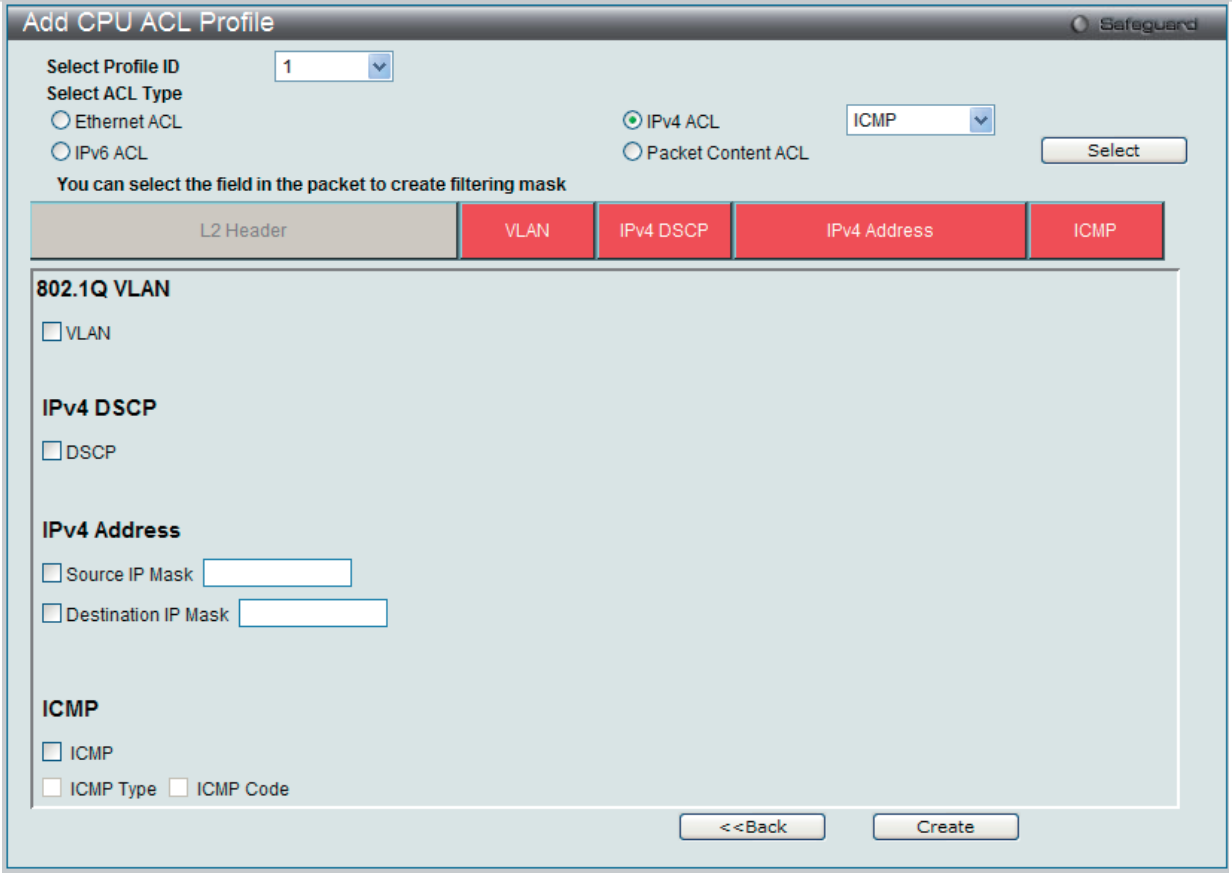


図 10-38　Add CPU ACL Profile - IPv4 画面

「Add CPU ACL」画面で「Select Profile ID」（プロファイル ID）を指定し、「Select All Type」（ACL タイプ）に「IPv4 ACL」を選択します。さらに、隣接する欄で設定するフレームヘッダ（ICMP、IGMP、TCP、UDP、Protocol ID）を指定して「Select」ボタンをクリックします。画面上部のボックスをクリックすると赤色に変わり、設定用項目が表示されます。

以下の項目を IP（IPv4）フィルタに設定できます。

項目	説明
Select Profile ID	プロファイルのための固有の識別番号を指定します。1 から 3 が指定できます。
Select ACL Type	Ethernet（MAC アドレス）、IPv4 アドレス、IPv6 アドレス、または Packet Content の中からプロファイルのベースを指定します。Type の変更に伴いメニューも変わります。ここでは「IPv4」を選択します。 • IPv4 - フレームヘッダの IP アドレスを対象にします。
以下のオプションを指定すると各フレームヘッダのプロトコルタイプを調べます。基準にどのようなプロトコルを含めるかを指定します。	
VLAN	このオプションを指定するパケットヘッダの VLAN 識別子を調べて、部分的もしくは全体を転送基準として使用します。
IPv4 DSCP	このオプションを指定すると各パケットヘッダの DiffServ コードを調べて、部分的もしくは全体を転送基準として使用します。
IPv4 Address	転送決定の基準として使用されます。 • Source IP Mask - 送信元 IP アドレスをマスクする IP アドレスを指定します。 • Destination IP Mask - 送信先 IP アドレスをマスクする IP アドレスを指定します。
ICMP	それぞれのフレームヘッダの「Internet Control Message Protocol」（ICMP）項目を調べます。アクセスプロファイルが適用するタイプ（「ICMP Type」または「ICMP Code」）を選択します。
IGMP	それぞれのフレームヘッダの「Internet Group Management Protocol」（IGMP）項目を調べます。アクセスプロファイルが適用するタイプ「IGMP Type」を選択します。

項目	説明
TCP	転送基準となる受信したパケットの TCP ポート番号を使用します。TCP を選ぶと送信元ポートマスク（source port mask）と（もしくは）送信先ポートマスク（dest port mask）を指定する必要があります。 - Source Port Mask（0-FFFF）- フィルタリングしたい送信元ポートをマスクする TCP ポートを 16 進数（hex 0x0-0xffff）で指定します。 - Destination Port Mask（0-FFFF）- フィルタリングしたい送信先ポートをマスクする TCP ポートを 16 進数（hex 0x0-0xffff）で指定します。 - TCP Flag Bits - フィルタするフラグビットを指定します。フラグビットはパケットがどのような振る舞いをするかを決定するパケットの一部です。パケットのフラグビットでフィルタリングするには TCP 項目のフラグビットに一致する内容のボックスをチェックします。URG（urgent）、ACK（acknowledgement）、PSH（push）、RST（reset）、SYN（synchronize）、FIN（finish）、または Check All（すべて）を選ぶことができます。
UDP	転送基準となる受信したパケットの UDP ポート番号を使用します。UDP を選ぶと送信元ポートマスクと (または) 送信先ポートマスクを指定する必要があります。 • Source Port Mask - フィルタリングする送信元ポートをマスクする UDP ポートを 16 進数 (hex 0x0-0xffff) で指定します。 • Destination Port Mask - フィルタリングする送信先ポートをマスクする TCP ポートを 16 進数 (hex 0x0-0xffff) で指定します。
Protocol ID	Protocol ID Mask をチェックし、マスクするパケットヘッダの protocol ID を定義する値を指定します。 • Protocol ID Mask (0-FF) - IP ヘッダの後のマスクオプションに定義する値を指定します。 • User Define (0-FFFFFFFF) - ユーザ定義の値を指定します。

「Create」ボタンをクリックし、このエントリをスイッチに保存します。

作成したプロファイルの詳細の参照

「CPU Access Profile List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

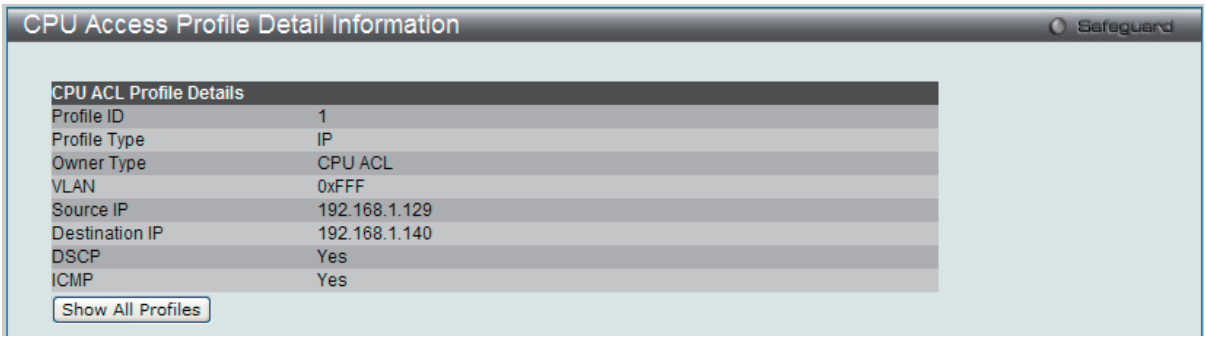


図 10-39 CPU Access Profile Detail Information - IP（IPv4）画面

「Show All Profiles」ボタンをクリックすると、「CPU Access Profile List」画面に戻ります。

作成した CPU アクセスプロファイルに対するルールの設定手順（IP）：

IP アクセスルールの設定

1. 「CPU Access Profile List」画面を表示します。

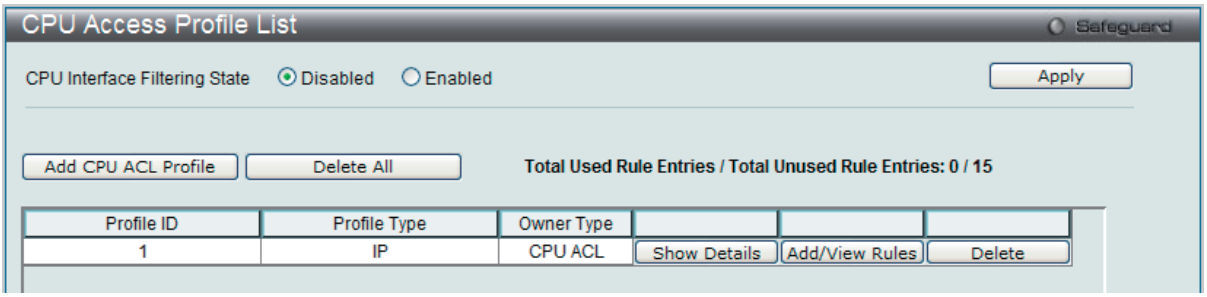


図 10-40 CPU Access Profile List 画面

2. 「CPU Access Profile List」画面を表示し、IP エントリの「Add/View Rules」ボタンをクリックして以下の画面を表示します。

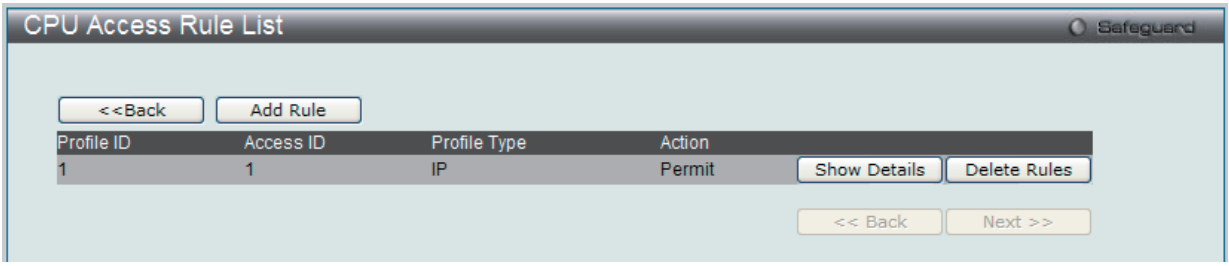


図 10-41 CPU Access Rule List - IP 画面

既に作成したルールの削除
該当の「Delete Rules」ボタンをクリックします。

ルールの新規登録
「Add Rule」ボタンをクリックします。

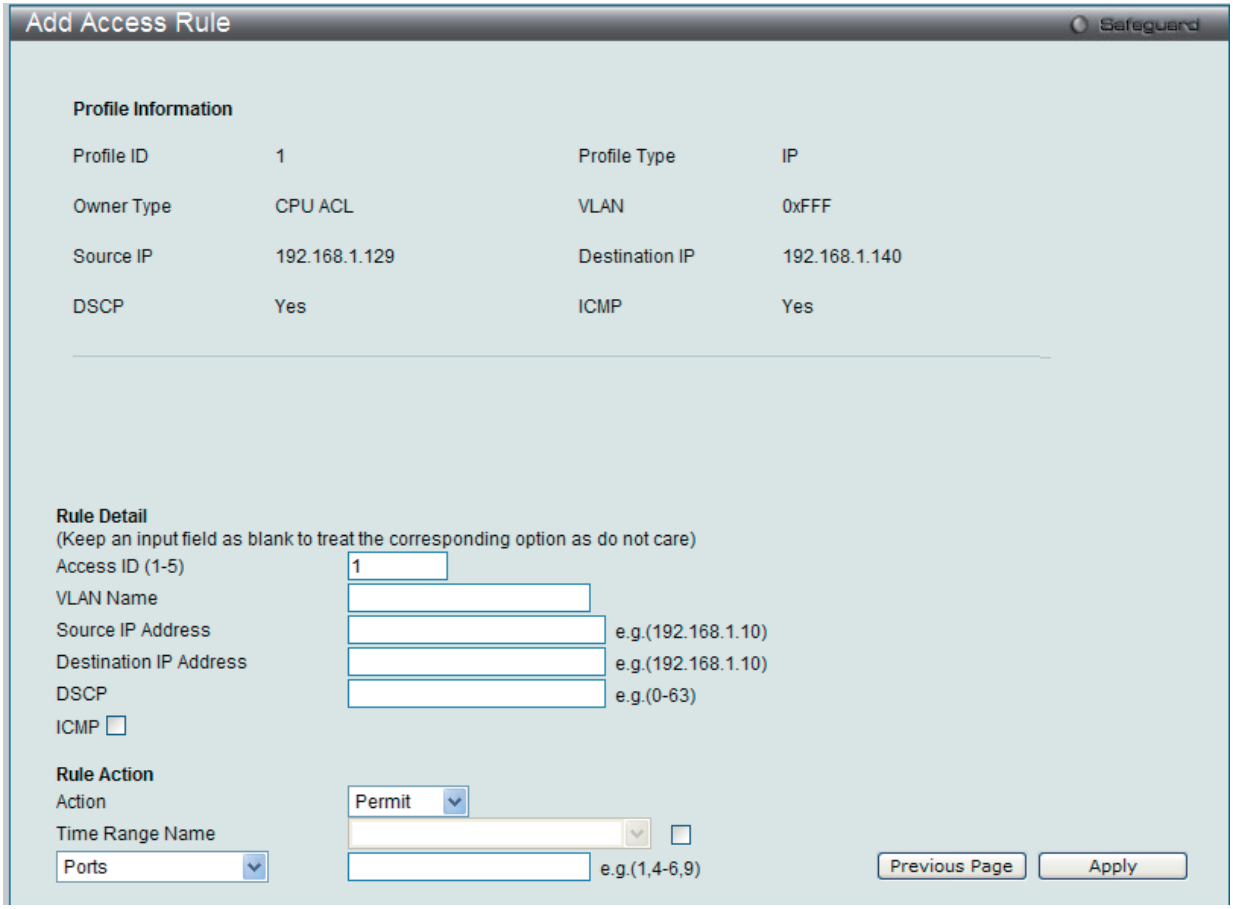


図 10-42　Add Access Rule - IP 画面

以下の項目を設定します。

項目	説明
Rule Detail	
Access ID (1-5)	それぞれのルールに固有の番号を指定します。1 から 5 が指定できます。
IGMP	それぞれのフレームヘッダの「Internet Group Management Protocol」（IGMP）項目を調べます。アクセスプロファイルが適用するタイプ「IGMP Type」を選択します。
VLAN Name	VLAN 名を入力します。
Source IP Address	送信元の IP アドレスの IP アドレスを入力します。
Destination IP Address	宛先 IP アドレスの IP アドレスを入力します。
TCP	転送基準となる受信したパケットの TCP ポート番号を使用します。TCP を選ぶと送信元ポートマスク（source port mask）と（または）送信先ポートマスク（dest port mask）を指定する必要があります。 - Source Port Mask（0-FFFF）- フィルタリングしたい送信元ポートをマスクする TCP ポートを 16 進数で指定します。 - Destination Port Mask（0-FFFF）- フィルタリングしたい送信先ポートをマスクする TCP ポートを 16 進数で指定します。 - Flag Bits - フィルタするフラグビットを指定します。フラグビットはパケットがどのような振る舞いをするかを決定するパケットの一部です。パケットのフラグビットでフィルタリングするには「TCP」項目のフラグビットに一致する内容のボックスをチェックします。URG（urgent）、ACK（acknowledgement）、PSH（push）、RST（reset）、SYN（synchronize）、FIN（finish）を選ぶことができます。
UDP	転送基準となる受信したパケットの UDP ポート番号を使用します。UDP を選ぶと送信元ポートマスク（source port mask）と（または）送信先ポートマスク（dest port mask）を指定する必要があります。 - Source Port Mask - フィルタリングしたい送信元ポートをマスクする UDP ポートを 16 進数（hex 0x0-0xffff）で指定します。 - Destination Port Mask（0-FFFF）- フィルタリングしたい送信先ポートをマスクする UDP ポートを 16 進数（hex 0x0-0xffff）で指定します。
Protocol ID	マスクしたいパケットヘッダの Protocol ID Mask を指定します。0-255 の値を入力します。「User Define」マスクは 16 進数（0-FF）で指定します。
DSCP	各パケットヘッダの DiffServ コードを調べて、部分的もしくは全体を転送基準として使用します。
ICMP	各フレームヘッダの Internet Control Message Protocol(ICMP) フィールドを調べます。

項目	説明
Rule Action	
Action	• Permit - アクセスプロファイルに一致したパケットを転送します。この時新しいルールが追加されることがあります（以下参照）。 • Deny - アクセスプロファイルに一致したパケットは転送せずにフィルタリングします。 • Mirror - アクセスプロファイルに一致するパケットを「Port Mirroring」画面で定義したポートにミラーリングします。Port Mirroring が有効で、ターゲットポートに設定されている必要があります。
Time Range Name	チェックボックスをクリックし、「Time Range」画面に設定済みのタイムレンジ設定名を入力します。このアクセスルールをスイッチで実行する場合、ここに特定の時間を設定します。
Ports	設定するポート範囲を指定します。

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。

作成したルールの詳細の参照

「CPU Access Rule List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

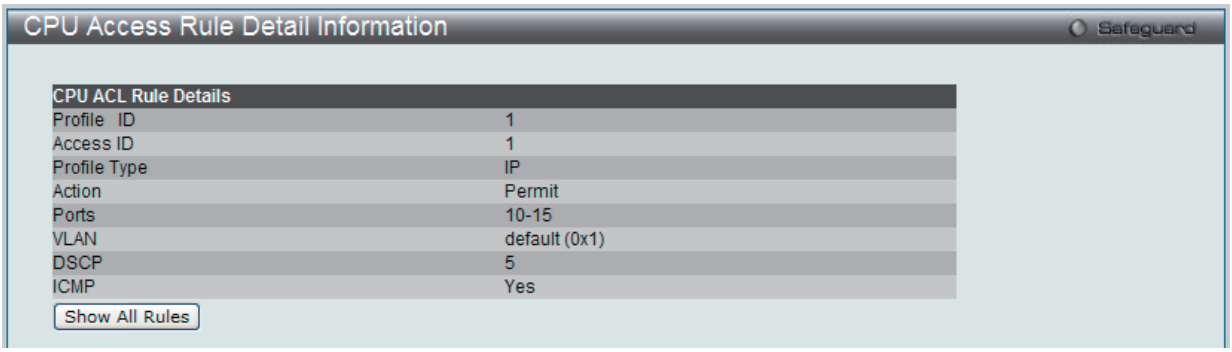


図 10-43 CPU Access Rule Detail Information - IP 画面

「Show All Rules」ボタンをクリックすると、「CPU Access Rule List」画面に戻ります。

CPU アクセスプロファイルの作成（IPv6）

CPU アクセスプロファイルを作成し、プロファイルにルールを作成します。

以下の画面では、ラジオボタンを使用し、CPU Interface Filtering State をグローバルに有効または無効にし、動作状態の変更をします。

ACL > CPU Access Profile List の順でメニューをクリックし、以下の画面を表示します。

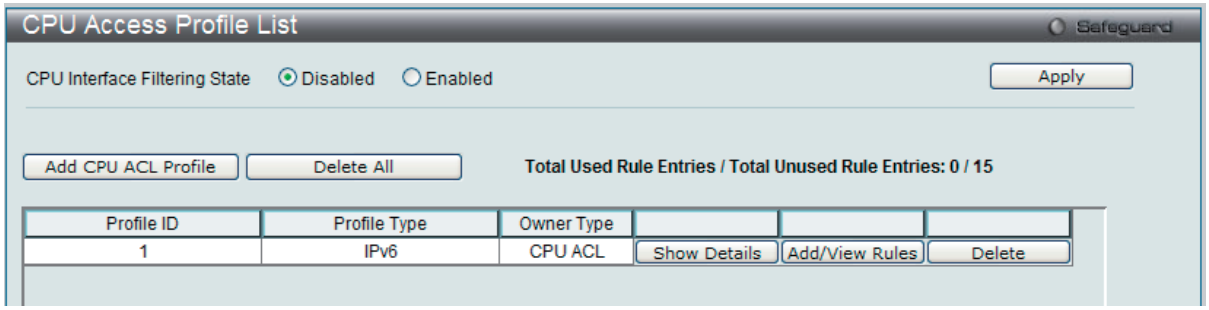


図 10-44 CPU Access Profile List 画面

スイッチに作成した CPU アクセスプロファイルリストを表示します。1 つのアクセスプロファイルが説明のために作成されています。「CPU Interface Filtering State」に「Enabled」を選択すると、スイッチは CPU パケットを詳しく調べます。また、「Disabled」を選択すると、調べません。

エントリの設定の参照

該当の「Show Details」ボタンをクリックします。

CPU Access Profile List のエントリの削除

エントリを削除するためには、エントリ横の「Delete」ボタンをクリックします。すべてのエントリを削除するためには、「Delete All」ボタンをクリックします。

CPU アクセスプロファイルリストの新規登録

「Add CPU ACL Profile」ボタンをクリックし、以下の画面を表示します。

IPv6 の「Add CPU ACL Profile」画面

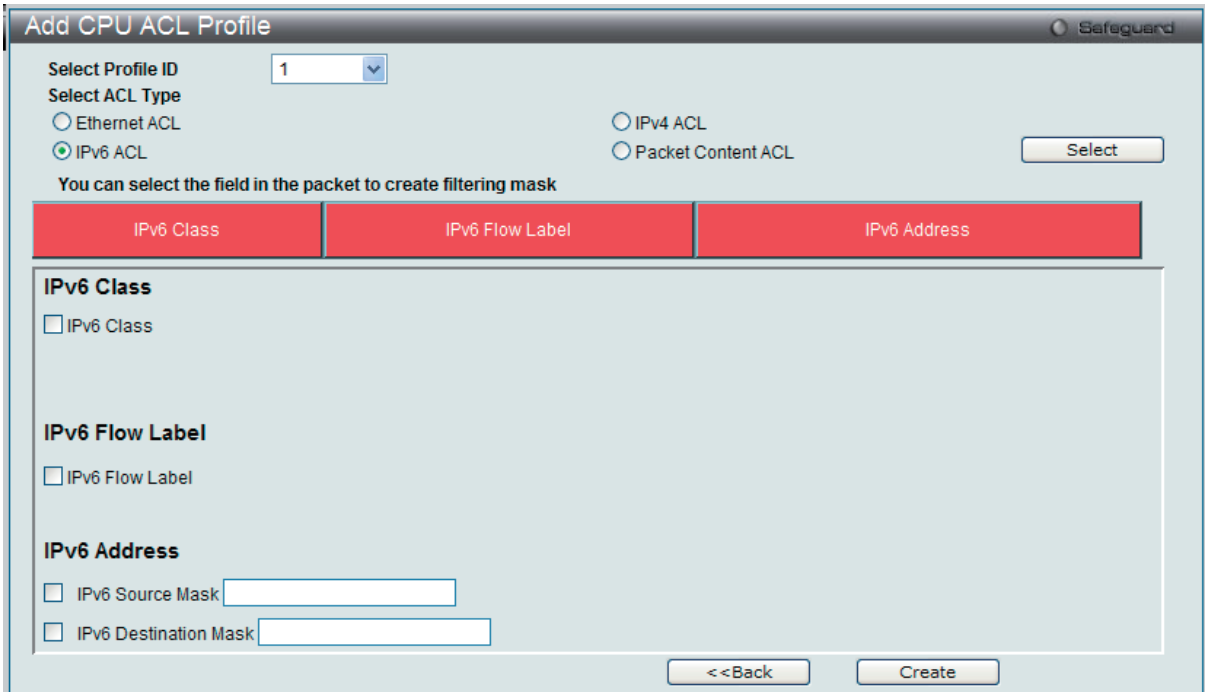


図 10-45　Add CPU ACL Profile - IPv6 画面

「Add CPU ACL」画面で「Select Profile ID」（プロファイル ID）を指定し、「Select All Type」（ACL タイプ）に「IPv6 ACL」を選択して「Select」ボタンをクリックします。画面上部のボックスをクリックすると赤色に変わり、設定用項目が表示されます。

以下の項目を IP（IPv6）フィルタに設定できます。

項目	説明
Select Profile ID	プロファイルのための固有の識別番号を指定します。1 から 3 が指定できます。
Select ACL Type	Ethernet（MAC アドレス）、IPv4 アドレス、IPv6 アドレス、または Packet Content の中からプロファイルのベースを指定します。Type の変更に伴いメニューも変わります。ここでは、「IPv6」を選択します。 • IPv6 - フレームヘッダの IP アドレスを対象にします。
以下のオプションを指定すると各フレームヘッダのプロトコルタイプを調べます。基準にどのようなプロトコルを含めるかを指定します。	
IPv6 Class	この項目を選ぶと IPv6 ヘッダの「Class」項目を調べます。「Class」項目は IPv4 における Type of Service（ToS）、「Precedence bits」項目のようなパケットヘッダの一部です。
IPv6 Flow Label	この項目を選ぶと IPv6 ヘッダの「flow label」を調べます。「flow label」は送信元で順番につけられる QoS やリアルタイムサービスパケットのためのデフォルトではない項目です。
IPv6 Address	• IPv6 Source Address - 送信元アドレスとして使用する IPv6 アドレスを入力します。 • IPv6 Destination Address - 宛先アドレスとして使用する IPv6 アドレスを入力します。 注意 いかなる場合も、IPv6 Class と IPv6 Flow Label は共に選択し、IPv6 アドレスは単体で選択します。

「create」ボタンをクリックし、このエントリをスイッチに保存します。

作成したプロファイルの詳細の参照

「CPU Access Profile List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

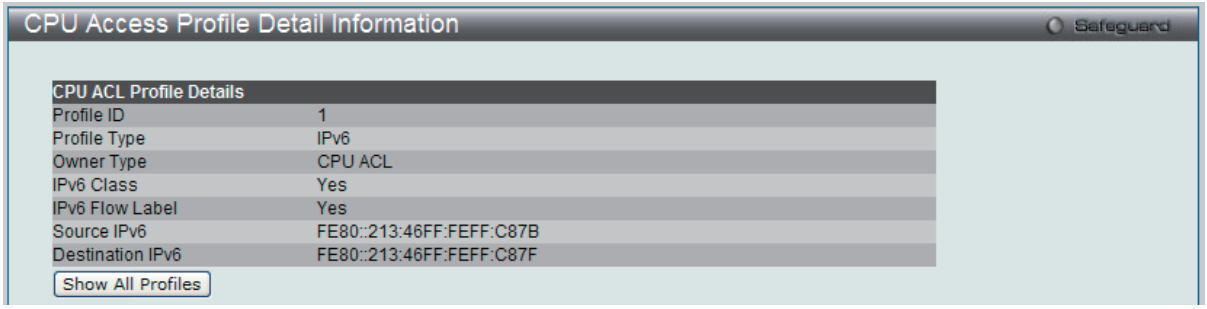


図 10-46　CPU Access Profile Detail Information - IPv6 画面

「Show All Profiles」ボタンをクリックすると、「CPU Access Profile List」画面に戻ります。

作成した CPU アクセスプロファイルに対するルールの設定手順（IPv6）：

IPv6 アクセスルールの設定

1. 「CPU Access Profile List」画面を表示します。

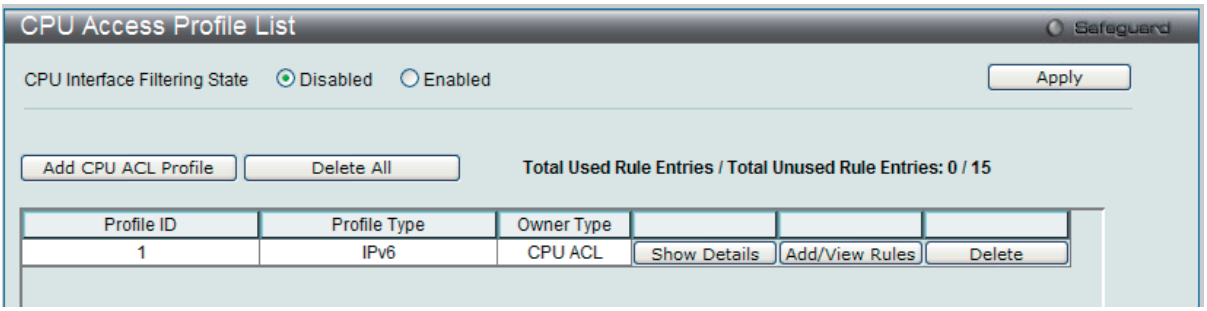


図 10-47　CPU Access Profile List 画面

2. 「CPU Access Profile List」画面を表示し、IPv6 エントリの「Add/View Rules」ボタンをクリックして以下の画面を表示します。

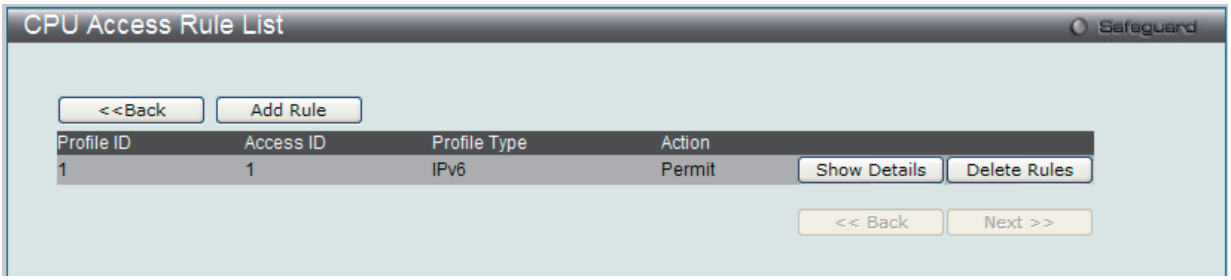


図 10-48　CPU Access Rule List - IPv6 画面

既に作成したルールの削除

「Show All Rules」ボタンをクリックすると、「CPU Access Rule List」画面に戻ります。該当の「Delete Rules」ボタンをクリックします。

ルールの新規登録

「Add Rule」ボタンをクリックし、以下の画面を表示します。

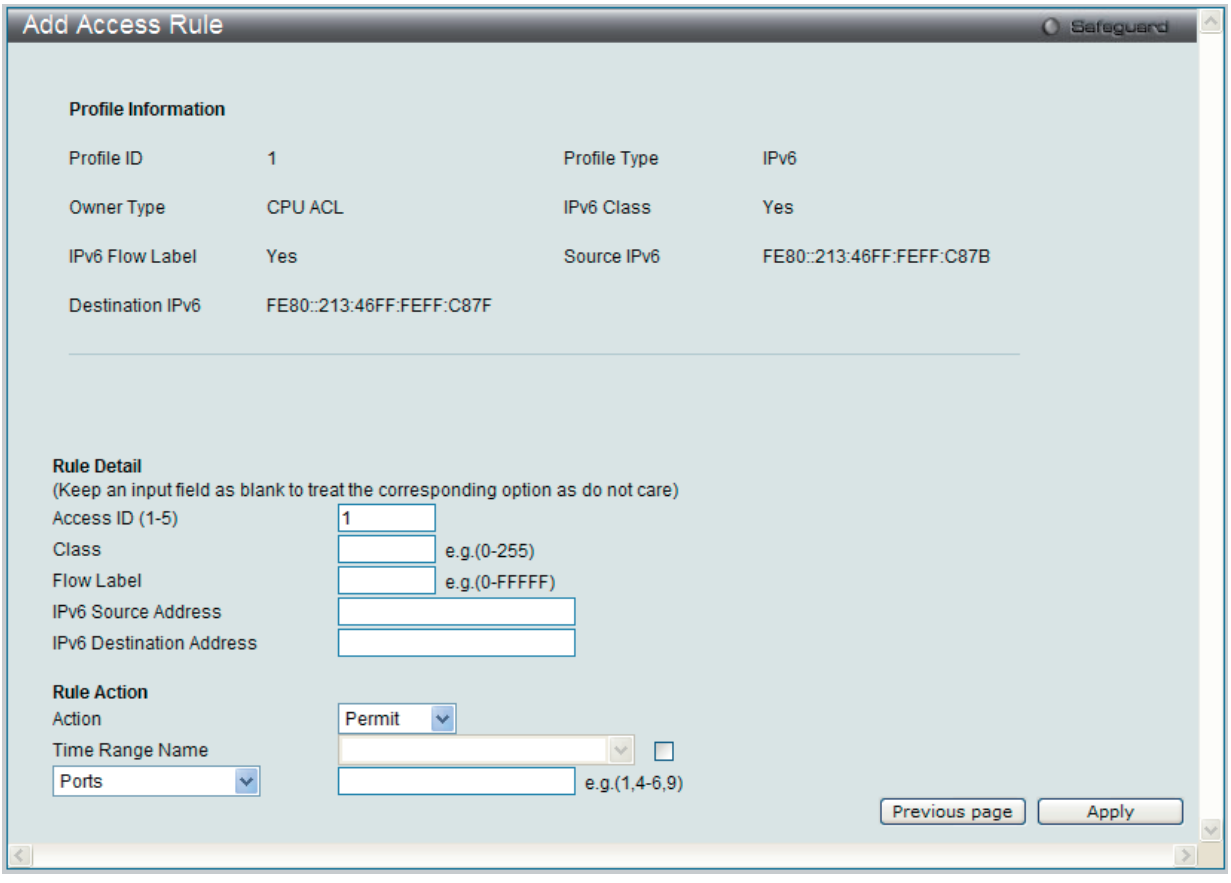


図 10-49　Add Access Rule - IPv6 画面

以下の項目を設定します。

項目	説明
Rule Detail	
Access ID (1-5)	それぞれのルールに固有の番号を指定します。1 から 5 が指定できます。
Class	クラスを入力し、IPv6 ヘッダの「Class」フィールドを調べます。本フィールドは IPv4 における「Type of Service(ToS)」、「Precedence bits」フィールドのようなパケットヘッダの一部です。
Flow Label	この項目を選ぶと IPv6 ヘッダの flow label 項目を調べます。flow label 項目は送信元で順番につけられる QoS やリアルタイムサービスパケットのためのデフォルトではない項目です。
IPv6 Source Address	IPv6 送信元アドレスの IPv6 アドレスを入力します。
IPv6 Destination Address	IPv6 送信先アドレスの IPv6 アドレスを入力します。
Rule Action	
Action	• Permit - アクセスプロファイルにマッチしたパケットを転送します。この時新しいルールが追加されることがあります（以下参照）。 • Deny - アクセスプロファイルに一致したパケットは転送せずにフィルタリングします。 • Mirror - アクセスプロファイルに一致するパケットを「Port Mirroring」画面で定義したポートにミラーリングします。Port Mirroring が有効で、ターゲットポートに設定されている必要があります。
Time Range Name	チェックボックスをクリックし、「Time Range」画面に設定済みのタイムレンジ設定名を入力します。このアクセスルールをスイッチで実行する場合、ここに特定の時間を設定します。
Ports	設定するポート範囲を指定します。

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。

作成したルールの詳細の参照

「CPU Access Rule List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

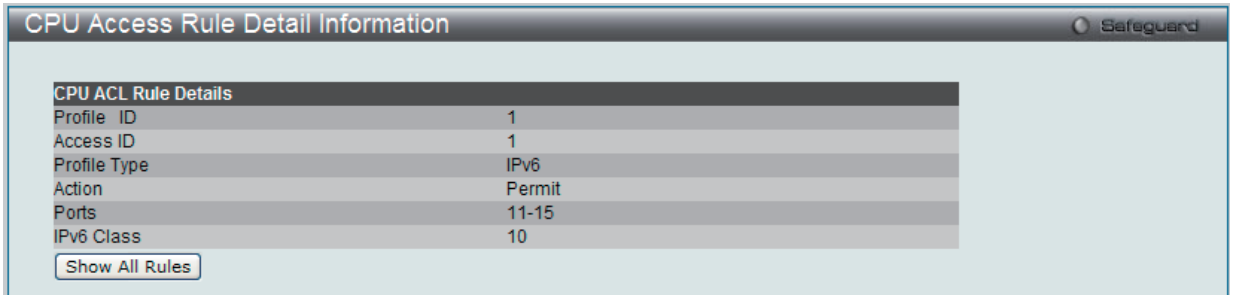


図 10-50 CPU Access Rule Detail Information - IPv6 画面

「Show All Rules」ボタンをクリックすると、「CPU Access Rule List」画面に戻ります。

CPU アクセスプロファイルの作成（パケットコンテンツ）

CPU アクセスプロファイルを作成し、プロファイルにルールを作成します。

以下の画面では、ラジオボタンを使用し、CPU Interface Filtering State をグローバルに有効または無効にし、動作状態の変更をします。

ACL > CPU Access Profile List の順でメニューをクリックし、以下の画面を表示します。

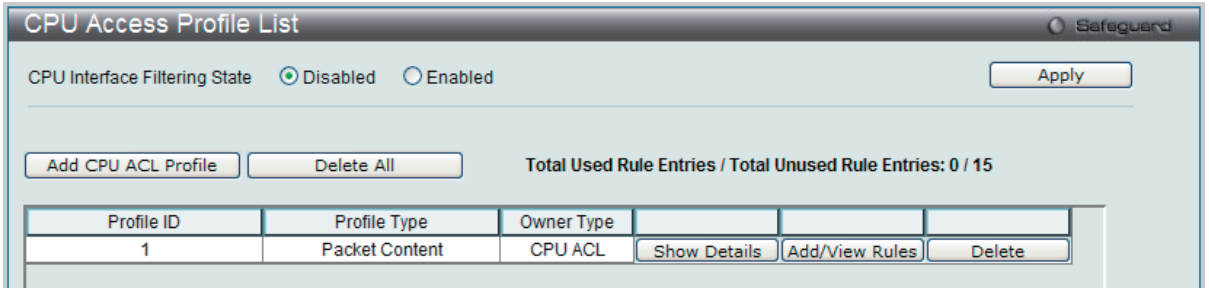


図 10-51 CPU Access Profile List 画面

本画面は、スイッチに作成した CPU アクセスプロファイルリストを表示します。各タイプに 1 つのアクセスプロファイルが説明のために作成されています。「Enabled」を選択すると、スイッチは CPU パケットを詳しく調べます。また、「CPU Interface Filtering State」に「Disabled」を選択すると、調べません。

エントリの設定の参照

該当の「Show Details」ボタンをクリックします。

CPU Access Profile List のエントリの削除

エントリを削除するためには、エントリ横の「Delete」ボタンをクリックします。すべてのエントリを削除するためには、「Delete All」ボタンをクリックします。

CPU アクセスプロファイルリストの新規登録

「Add CPU ACL Profile」ボタンをクリックし、以下の画面を表示します。

パケットコンテンツの「Add CPU ACL Profile」画面

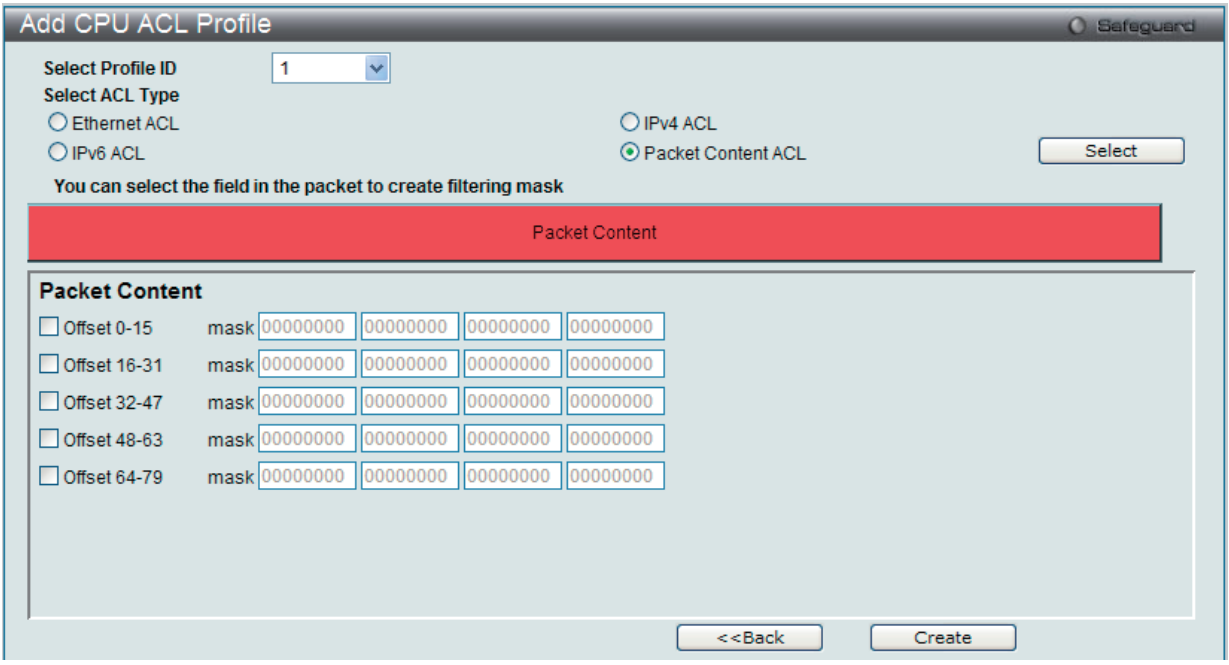


図 10-52　Add CPU ACL Profile - Packet Content 画面

「Add CPU ACL」画面で「Select Profile ID」（プロファイル ID）を指定し、「Select All Type」（ACL タイプ）に「Packet Content ACL」を選択して「Select」ボタンをクリックします。画面上部のボックスをクリックすると赤色に変わり、設定用項目が表示されます。

以下の項目を Packet Content フィルタに設定できます。

項目	説明
Select Profile ID	プロファイルのための固有の識別番号を指定します。1 から 3 が指定できます。
Select ACL Type	Ethernet（MAC アドレス）、IPv4 アドレス、IPv6 アドレス、または Packet Content の中からプロファイルのベースを指定します。Type の変更に伴いメニューも変わります。ここでは「Packet Content」を選択します。 • Packet Content - パケットヘッダの内容をマスクして隠します。
Packet Content	1 個のパケット内で最大 5 個のパケットコンテンツオフセットチャンクを同時に検証し、そのフレームコンテンツオフセット、マスクおよびレイヤを規定することができます。5 個のパケットコンテンツチャンクオフセットが設定できます。パケットコンテンツチャンクマスクは 4 バイトを示します。最大 5 個までパケットコンテンツオフセットチャンクを選択することが可能です。 パケットヘッダにマスクを開始するオフセットを指定します。 • Offset 0-15 - 16 進数でパケットの最初から 15 バイト目までのマスクを指定します。 • Offset 16-31 - 16 進数でパケットの 16 バイト目から 31 バイト目までのマスクを指定します。 • Offset 32-47 - 16 進数でパケットの 32 バイト目から 47 バイト目までのマスクを指定します。 • Offset 48-63 - 16 進数でパケットの 48 バイト目から 63 バイト目までのマスクを指定します。 • Offset 64-79 - 16 進数でパケットの 64 バイト目から 79 バイト目までのマスクを指定します。 **注意** 作成できるパケットコンテンツマスクプロファイルは 1 つだけです。本スイッチは、高度なパケットコンテンツマスク (またはパケットコンテンツアクセスコントロールリスト -ACL として知られる) 機能を使用して、ARP Spoofing などの一般的なネットワーク攻撃を効果的に軽減することができます。このため、パケットコンテンツ ACL が異なるプロトコル層におけるパケットのどんな指定コンテンツも検証できます。

「Create」ボタンをクリックし、このエントリをスイッチに保存します。

作成したプロファイルの詳細の参照

「CPU Access Profile List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

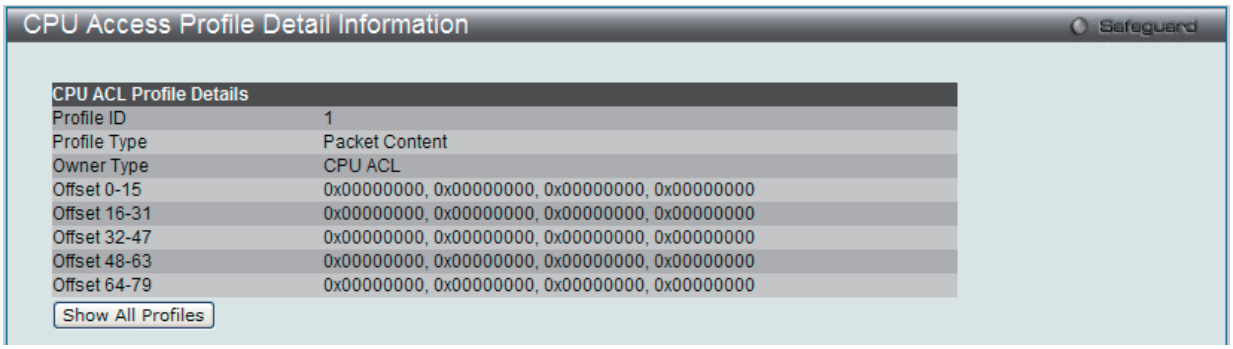


図 10-53　CPU Access Profile Detail Information - Packet Content 画面

「Show All Profiles」ボタンをクリックすると、「CPU Access Profile List」画面に戻ります。

作成した CPU アクセスプロファイルに対するルールの設定手順（Packet Content）：

Packet Content アクセスルールの設定

1. 「CPU Access Profile List」画面を表示します。

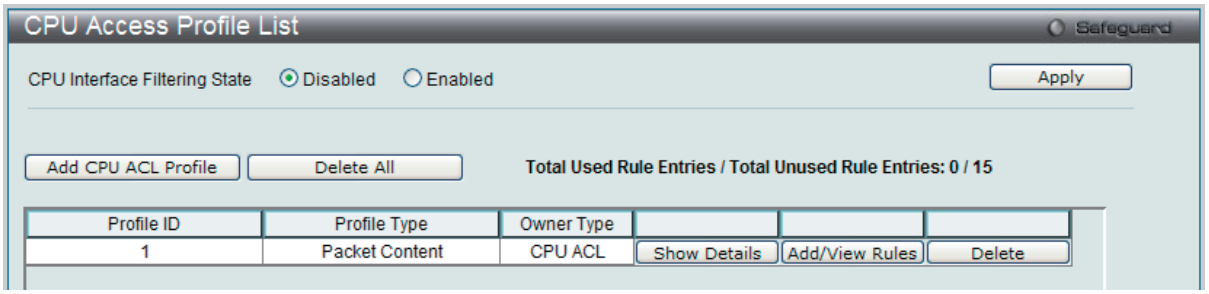


図 10-54　CPU Access Profile List 画面

2. 「CPU Access Profile List」画面を表示し、Packet Content エントリの「Add/View Rules」ボタンをクリックして以下の画面を表示します。

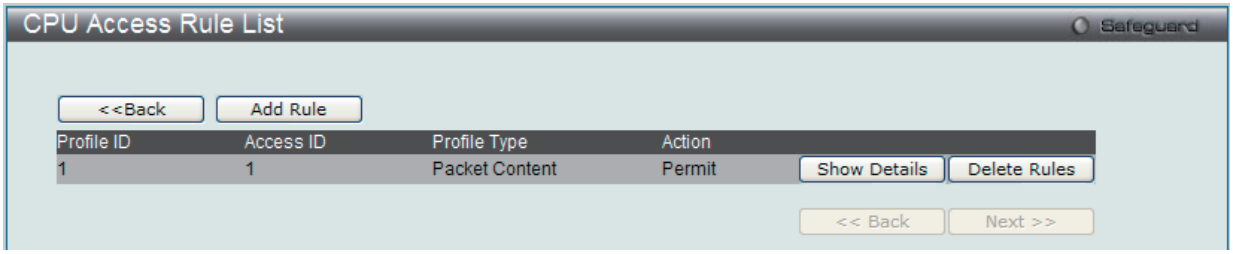


図 10-55　CPU Access Rule List - Packet Content 画面

作成済みのルールの削除

該当の「Delete Rules」ボタンをクリックします。

ルールの新規作成

「Add Rule」ボタンをクリックします。

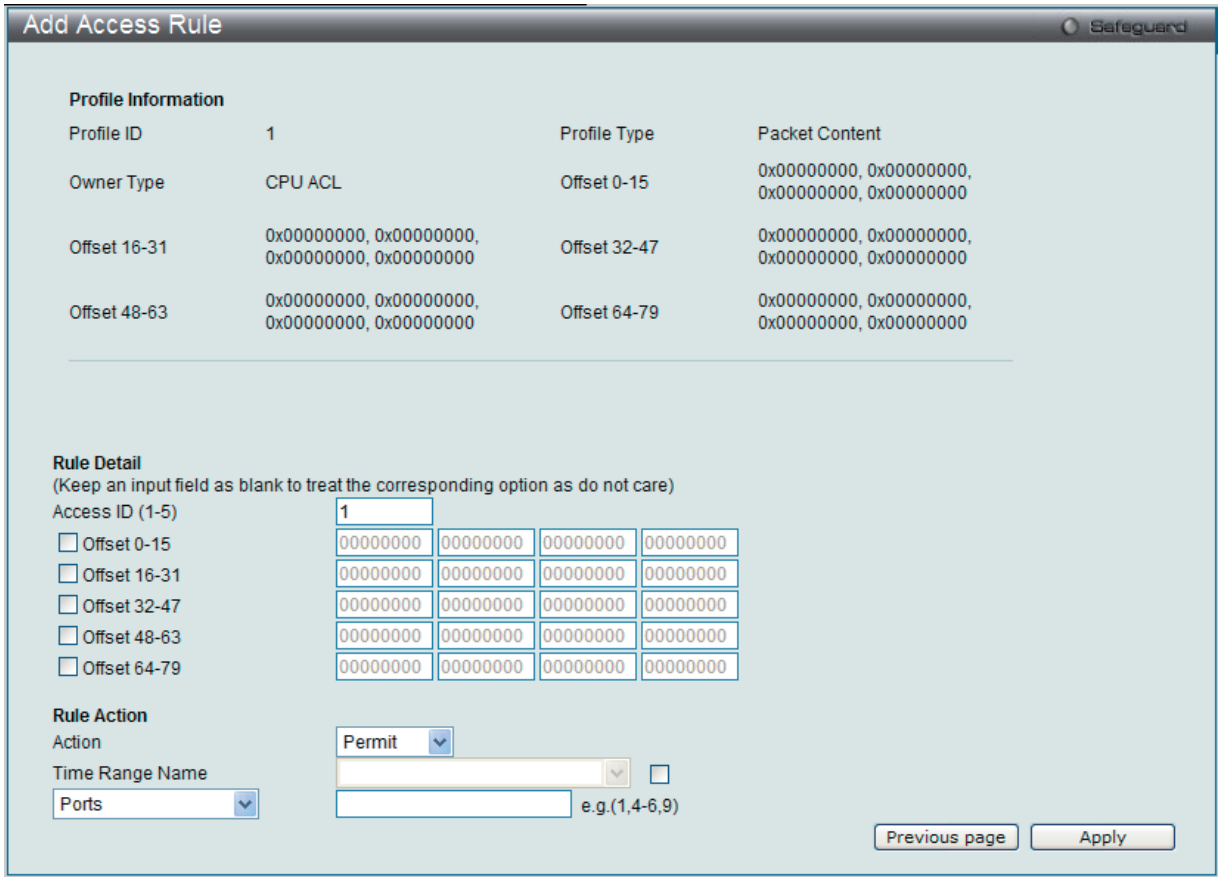


図 10-56　Add Access Rule - Packet Content 画面

項目	説明
Rule Detail	
Access ID (1-5)	それぞれのルールに固有の番号を指定します。1 から 5 が指定できます。
Offset	パケットヘッダにマスクを開始するオフセットを指定します。 • Offset 0-15 - 16 進数でパケットの最初から 15 バイト目までのマスクを指定します。 • Offset 16-31 - 16 進数でパケットの 16 バイト目から 31 バイト目までのマスクを指定します。 • Offset 32-47 - 16 進数でパケットの 32 バイト目から 47 バイト目までのマスクを指定します。 • Offset 48-63 - 16 進数でパケットの 48 バイト目から 63 バイト目までのマスクを指定します。 • Offset 64-79 - 16 進数でパケットの 64 バイト目から 79 バイト目までのマスクを指定します。
Rule Action	
Action	• Permit - アクセスプロファイルにマッチしたパケットを転送します。この時新しいルールが追加されることがあります（以下参照）。 • Deny - アクセスプロファイルに一致したパケットは転送せずにフィルタリングします。 • Mirror - アクセスプロファイルに一致するパケットを「Port Mirroring」画面で定義したポートにミラーリングします。Port Mirroring が有効で、ターゲットポートに設定されている必要があります。
Time Range Name	チェックし、「Time Range」画面に設定済みのタイムレンジ設定名を入力します。このアクセスルールをスイッチで実行する場合、ここに特定の時間を設定します。
Ports	設定するポート範囲を指定します。

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。

作成したルールの詳細の参照

「CPU Access Rule List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

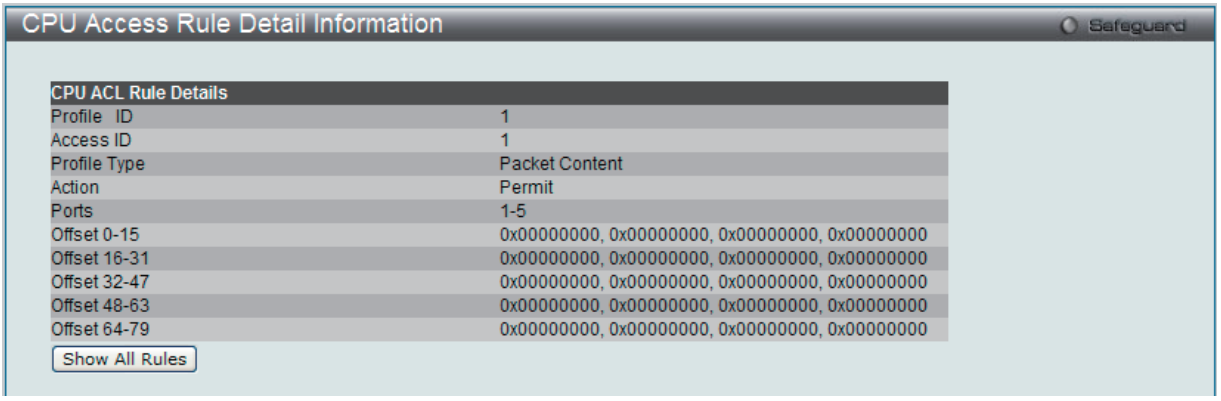


図 10-57　CPU Access Rule Detail Information - Packet Content 画面

「Show All Rules」ボタンをクリックすると、「CPU Access Rule List」画面に戻ります。

ACL Finder（ACL 検索）

定義済みの ACL エントリを検索します。

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

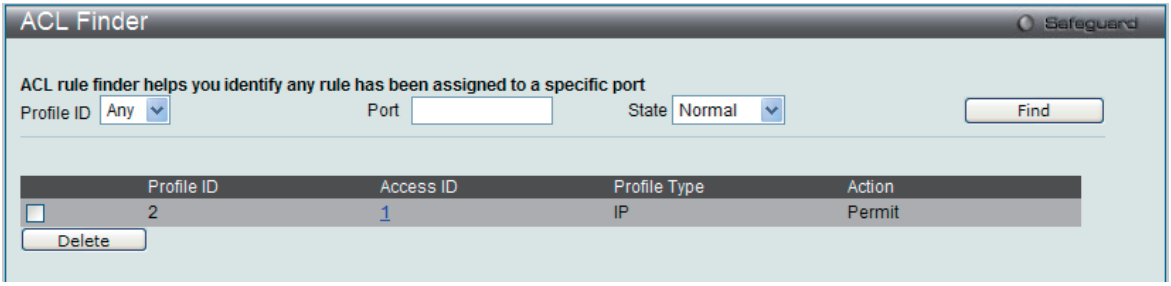


図 10-58　ACL Finder 画面

定義済みの ACL エントリの検索

エントリを検索するためには、「Profile ID」でプロファイル ID を、「Port」で参照するポートを指定し、さらに「State」（Normal または CPU）を定義して、「Find」ボタンをクリックします。画面下半分のテーブルにエントリは表示されます。

エントリの削除

削除するエントリのラジオボタンをチェックし、「Delete」ボタンをクリックします。

プロファイルの参照

参照するエントリの「Access ID」のリンクをクリックします。

ACL Flow Meter（ACL フローメータ）

Ingress トラフィックの帯域幅制限のために使用されるフローごとの帯域幅制御の設定を行います。パケットをフィルタリングする ACL ルールを作成すると、その ACL ルールに伴いトラフィックを制限するメータリングルールが作成されます。帯域幅の処理は 64 Kbps です。限定的なメータリングルールのため、すべての ACL ルールがメータリングルールに関連付けできないことにご注意ください。

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

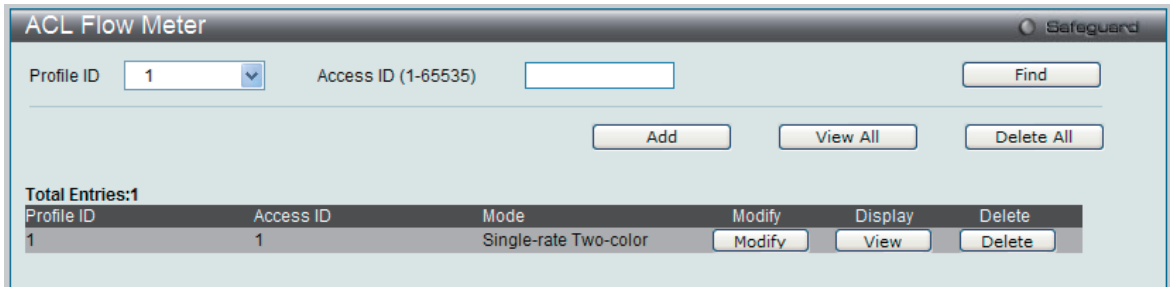


図 10-59 ACL Flow Meter 画面

以下の項目を使用して、設定を行います。

項目	説明
Profile ID	ACL フローメータリングパラメータを設定する定義済みプロファイル ID を指定します。
Access ID	ACL フローメータリングパラメータを設定する定義済みアクセス ID を指定します。

入力後、「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。

エントリの変更
対応する「Modify」ボタンをクリックします。

エントリの削除
対応する「Delete」ボタンをクリックします。すべてのエントリを削除するためには、「Delete All」ボタンをクリックします。

エントリの参照
すべてのエントリを参照するためには、「View All」ボタンをクリックします。
エントリを参照するためには、対応する「View」ボタンをクリックし、以下の画面を表示します。

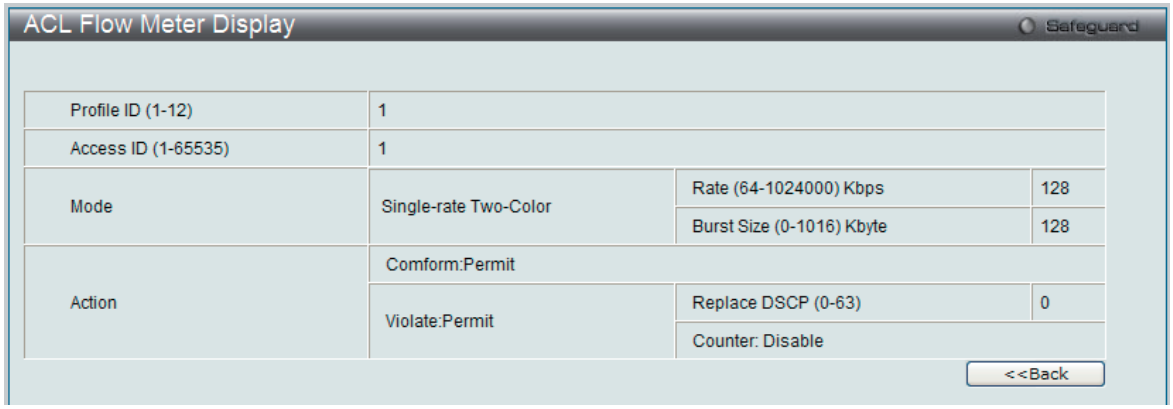


図 10-60 ACL Flow Meter Display 画面

「ACL Flow Meter」画面に戻るためには、「<<Back」ボタンをクリックします。

エントリの追加

「Add」ボタンをクリックし、以下の画面を表示します。

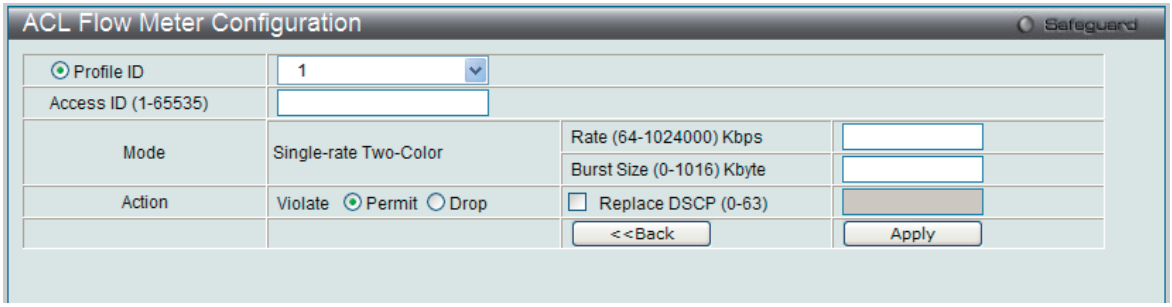


図 10-61　ACL Flow Meter Configuration 画面

以下の項目を使用して、設定を行います。

項目	説明
Profile ID	プルダウンメニューから、フローメータリングを設定する定義済みのプロファイル ID を指定します。
Access ID (1-65535)	ACL フローメータリングを設定する定義済みアクセス ID を 1-65535 の範囲で指定します。
Mode	シングルレート、ツーカラーマーカがレートとバーストサイズに基づいてパケットを緑色または赤色にマークします。本機能はバーストサイズのみが問題の時に有効です。 • Rate (64-1024000) Kbps - フローに規定する帯域幅（Kbps）を指定します。範囲は 64-1024000 です。 • Burst Size (0-1016) Kbyte - このフローのバーストサイズ（Kbps）を指定します。範囲は 0-1016 です。
Action	Violate - パケットが赤色モードの場合のアクションを指定します。 • Permit - パケットを許可します。 • Drop - パケットを破棄します。 「Replace DSCP」をチェックしてパケットの DSCP 値を変更します。

「Apply」ボタンをクリックして、設定を適用します。

「ACL Flow Meter」画面に戻るためには、「<<Back」ボタンをクリックします。

第 11 章　Monitoring（スイッチのモニタリング）

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

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

サブメニュー	説明	参照ページ
Cable Diagnostic（ケーブル診断機能）	ケーブルの品質やエラーの種類を診断します。	232 ページ
CPU Utilization（CPU 使用率）	CPU 使用率を表示します。	233 ページ
Port Utilization（ポート使用率）	ポートの帯域使用率を表示します。	234 ページ
Packet Size（パケットサイズ）	受信パケット数を表示します。	235 ページ
Memory Utilization（メモリ使用率）	DRAM とフラッシュのメモリ使用率の情報を表示します。	236 ページ
Packets（パケット統計情報）	パケット統計情報を表示します。	237 ページ
Errors（パケットエラー）	エラー統計情報を表示します。	241 ページ
Port Access Control（ポートアクセスコントロール）	802.1X 統計情報をポートごとに表示します。	244 ページ
Browse ARP Table（ARP テーブルの参照）	スイッチ上の現在の ARP エントリを表示します。	252 ページ
Browse VLAN（VLAN の参照）	各ポートの VLAN ステータスを VLAN ごとに表示します。	252 ページ
IGMP Snooping（IGMP Snooping 設定の参照）	IGMP Snooping 設定を表示します。	253 ページ
MLD Snooping（MLD Snooping 設定の参照）	MLD Snooping 設定を表示します。	254 ページ
LLDP（LLDP 設定の参照）	LLDP 統計情報を表示します。	256 ページ
Ethernet OAM（イーサネット OAM）	イーサネット OAM イベントログ情報と統計情報を表示します。	257 ページ
CFM（Connectivity Fault Management：接続性障害管理）	MEP によって検出された障害状態、CFM ポート MP リストを表示します。	259 ページ
Mac-based Access Control Authentication State MAC ベースアクセスコントロール認証ステートの参照）	MAC ベースアクセスコントロールの認証情報を表示します。	261 ページ
Browse Session Table（セッションテーブルの参照）	最後に起動してからの管理セッションを表示します。	261 ページ
MAC Address Table（MAC アドレステーブル）	ダイナミック MAC アドレスフォワーディングテーブルを表示します。	262 ページ
System Log（システムログ）	ヒストリログを表示します。	263 ページ

Cable Diagnostic（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。

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

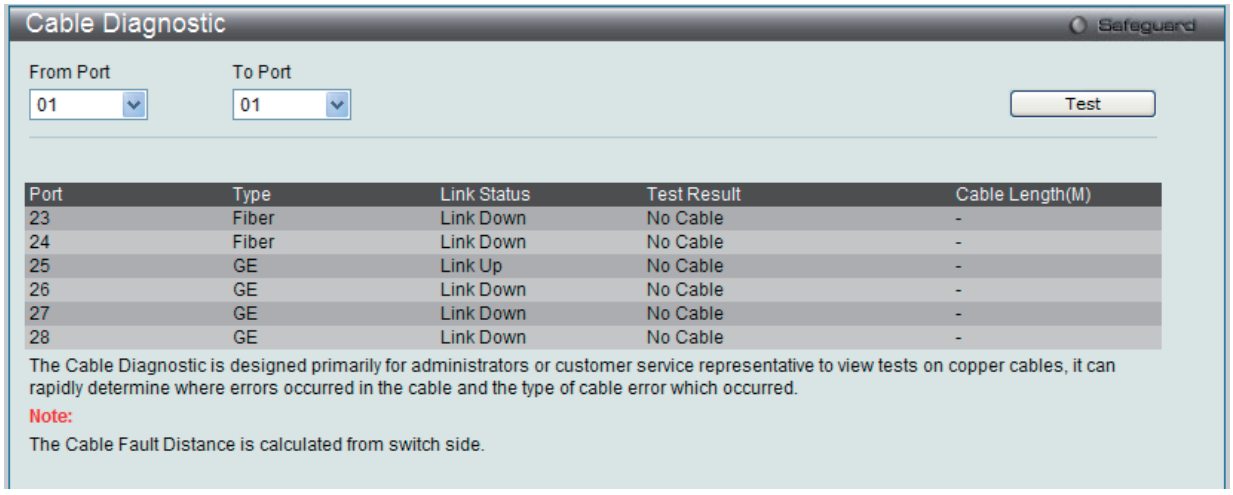


図 11-1　Cable Diagnostic 画面

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。

注意　インタフェースの「Link Status」欄に「Link Up」が表示されていると、「Cable Length」欄に表示される値は、インタフェースに対して正確でない可能性があります。

CPU Utilization（CPU 使用率）

「CPU Utilization」画面では、現在の CPU 使用率をパーセント表示し、また指定した時間間隔で計算した平均値も表示します。

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

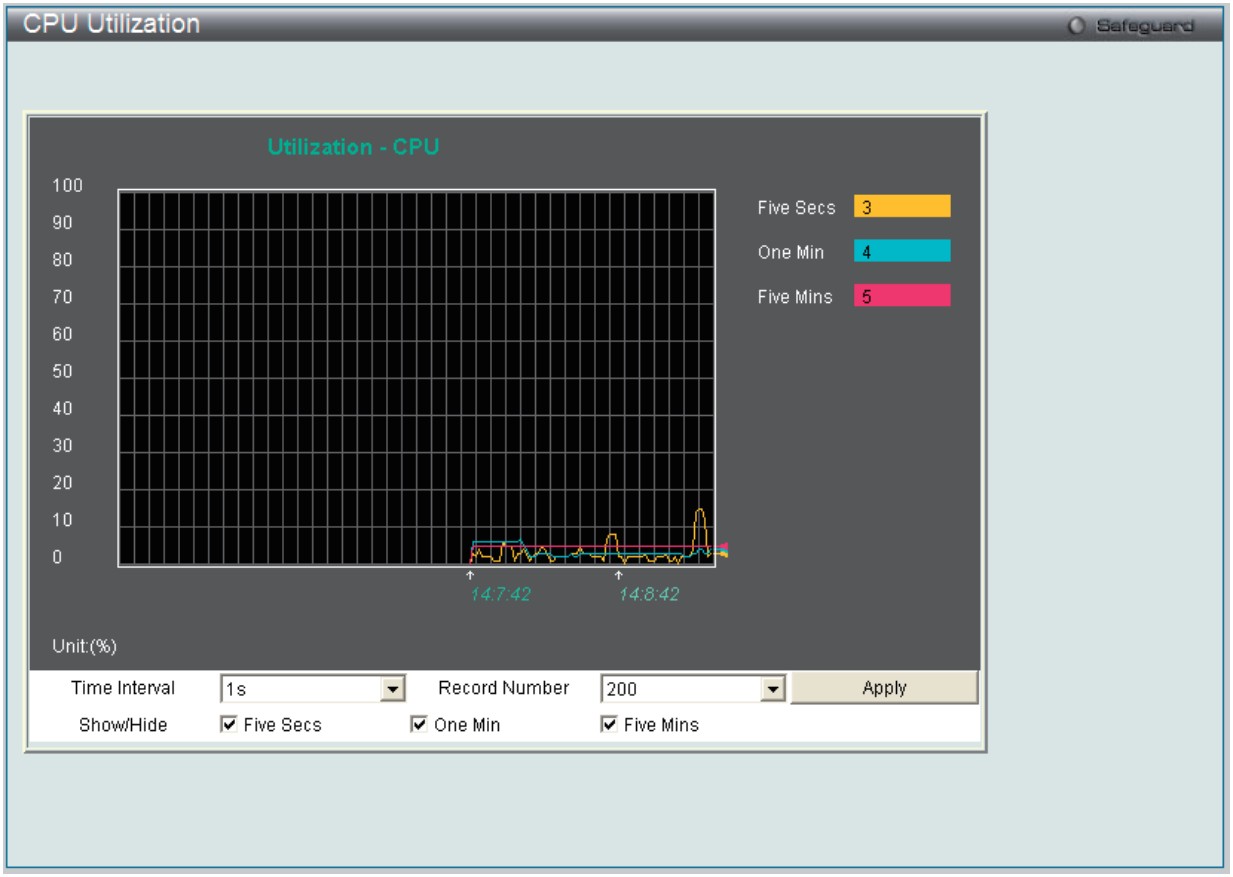


図 11-2　CPU Utilization 画面

以下の設定項目を使用して表示を変更します。

項目	説明
Timer Interval	1 秒から 60 秒で指定します。初期値は 1 秒です。
Record Number	20 から 200 でスイッチにポーリングを行う回数を指定します。初期値は 200 です。
Show/Hide	チェックボックスにて CPU 使用率を計算する時間経過を Five Secs、One Min および Five Mins から選択します。各時間経過は色分けされた線で表示されます。Five Secs は黄色、One Min は青、Five Mins はピンク色で表示されます。選択すると CPU 使用率を表示します。

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。

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 > 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。

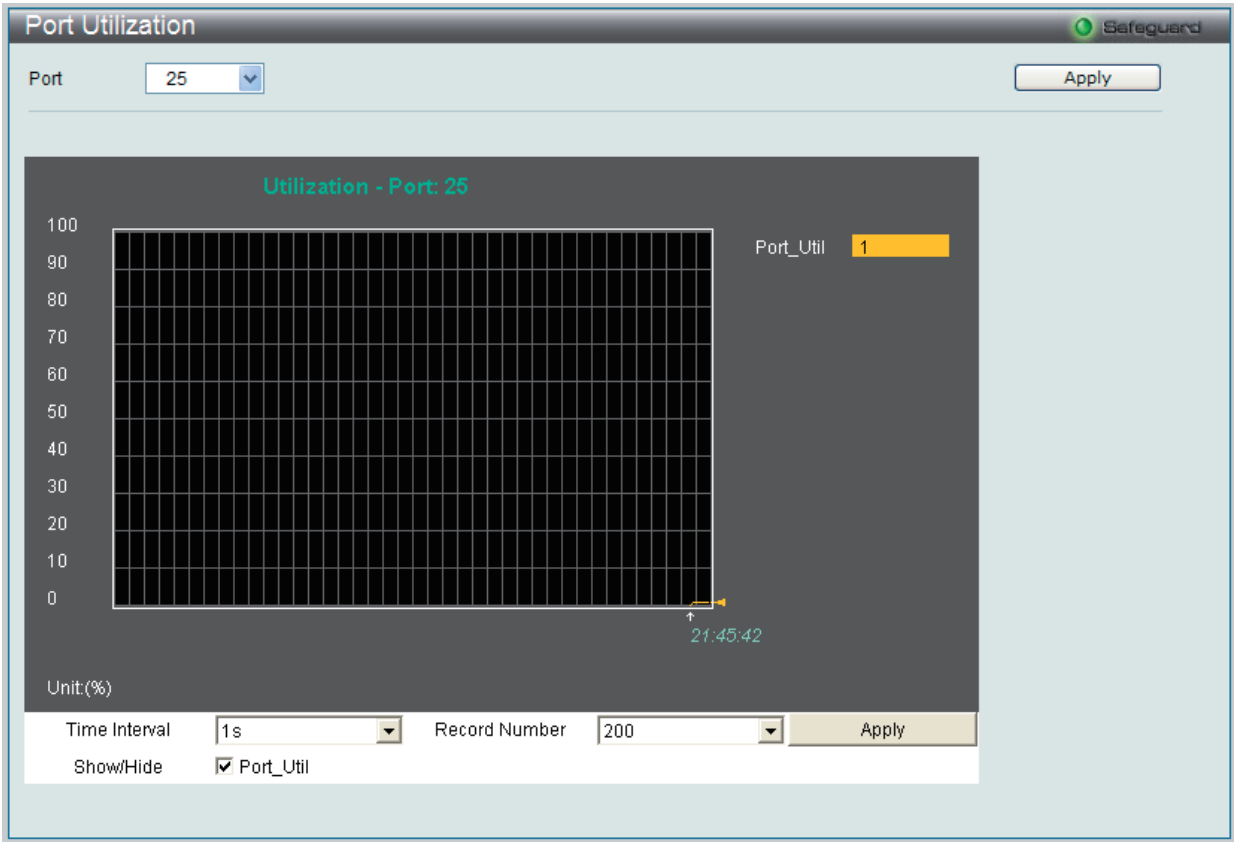


図 11-3　Port Utilization 画面

統計情報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ます。Web ページ先頭のポートをクリックすることで、スイッチのリアルタイムグラフィックを使用することができます。

以下の設定項目が使用できます。

項目	説明
Port	プルダウンメニューで統計情報を表示するポート番号を選択します。
Time Interval	1 秒から 60 秒で指定します。初期値は 1（秒）です。
Record Number	20 から 200 でスイッチにポーリングを行う回数を指定します。初期値は 200 です。
Show/ Hide	「Port_Util」にチェックすると、使用率を表示します。

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。

Packet Size（パケットサイズ）

Web マネージャはスイッチが受信したパケットを 6 個のグループに整理し、サイズによってクラス分けして折れ線グラフまたはテーブルにします。２つの画面が提供されます。プルダウンメニューでポートを選択し、統計情報を参照します。Web ページ先頭のポートをクリックすることで、スイッチのリアルタイムグラフィックを使用することができます。

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

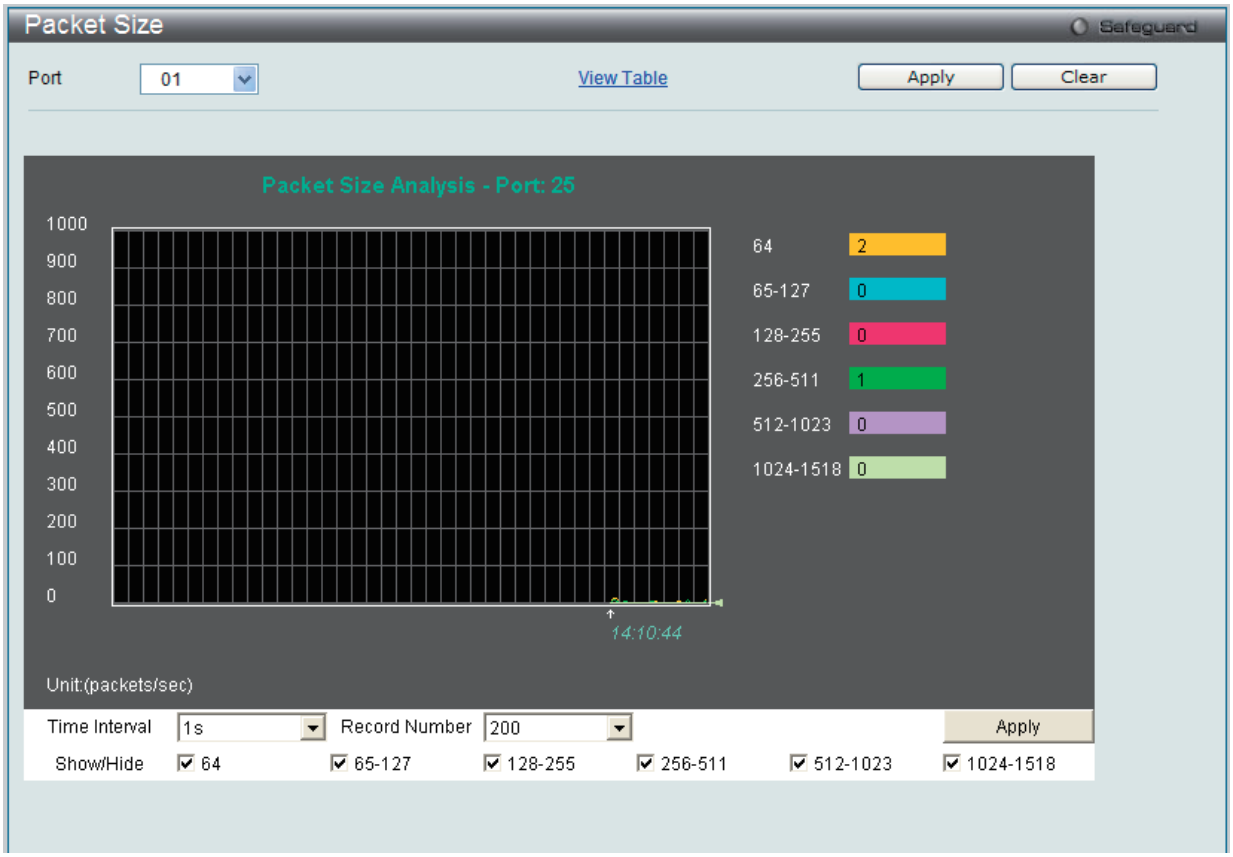


図 11-4　Packet Size 画面（折れ線グラフ）

「Packet Size Table」を表示するためには、「View Table」リンクをクリックします。

図 11-5　Packet Size Table 画面（表形式）

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
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。
Time Interval	1 秒から 60 秒で指定します。初期値は 1（秒）です。
Record Number	20 から 200 でスイッチにポーリングを行う回数を指定します。初期値は 200 です。
64	サイズが 64 オクテット（フレームビットを除き、FCS オクテットを含む）のパケット受信数（不正なパケットを含む）。
65-127	サイズが 65 から 127 オクテット（フレームビットを除き、FCS オクテットを含む）のパケット受信数（不正なパケットを含む）。
128-255	サイズが 128 から 255 オクテット（フレームビットを除き、FCS オクテットを含む）のパケット受信数（不正なパケットを含む）。
256-511	サイズが 256 から 511 オクテット（フレームビットを除き、FCS オクテットを含む）のパケット受信数（不正なパケットを含む）。
512-1023	サイズが 512 から 1023 オクテット（フレームビットを除き、FCS オクテットを含む）のパケット受信数（不正なパケットを含む）。
1024-1518	サイズが 1024 から 1518 オクテット（フレームビットを除き、FCS オクテットを含む）のパケット受信数（不正なパケットを含む）。
Show/ Hide	64、65-127、128-255、256-511、512-1023、または 1024-1518 の受信パケットを表示 / 非表示にします。
Clear	このボタンをクリックし、この画面のすべての統計情報をクリアします。
View Table	折れ線グラフ形式から表形式に表示を変更します。
View Graphic	表形式から折れ線グラフ形式に表示を変更します。

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。

Memory Utilization（メモリ使用率）

スイッチは DRAM とフラッシュのメモリ使用率の情報を表示します。

Monitoring > Memory 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。

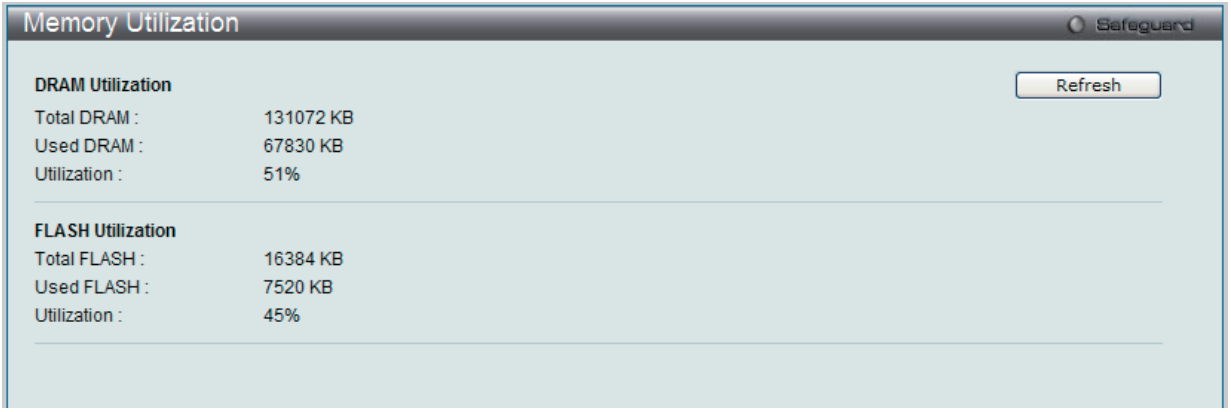


図 11-6　Memory Utilization 画面

Packets（パケット統計情報）

Web マネージャは、パケットの統計情報を折れ線グラフまたは表の形式で表示します。6 個の画面が表示されます。

Received（Rx）（受信パケット状態の参照）

スイッチが受信したパケットの情報を表示します。プルダウンメニューでポートを選択し、統計情報を参照します。Web ページ先頭のポートをクリックすることで、スイッチのリアルタイムグラフィックを使用することができます。

Monitoring > Packets > Received（Rx）の順にメニューをクリックし、以下の画面を表示します。

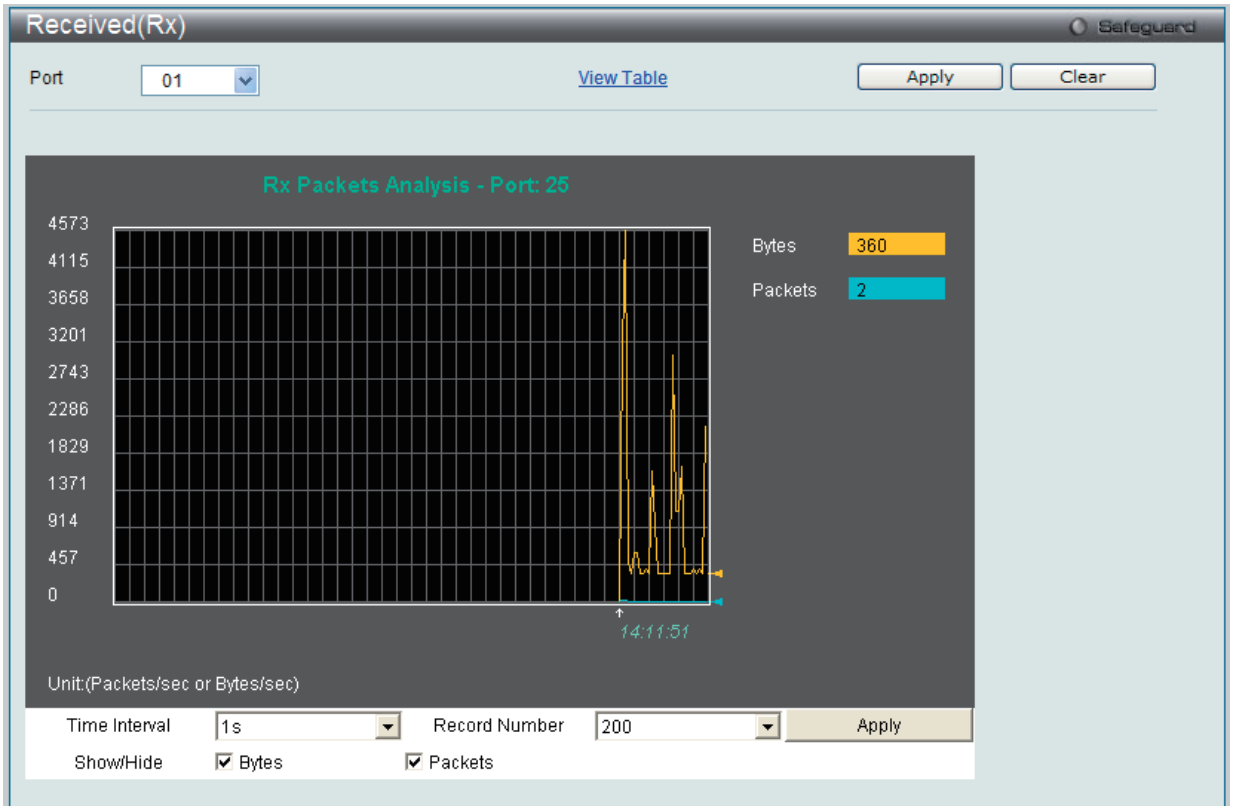


図 11-7　Received（Rx）Table 画面（バイトとパケットの折れ線グラフ）

「Received（RX）Table」を表示するには「View Table」リンクをクリックして、次の表を表示します。

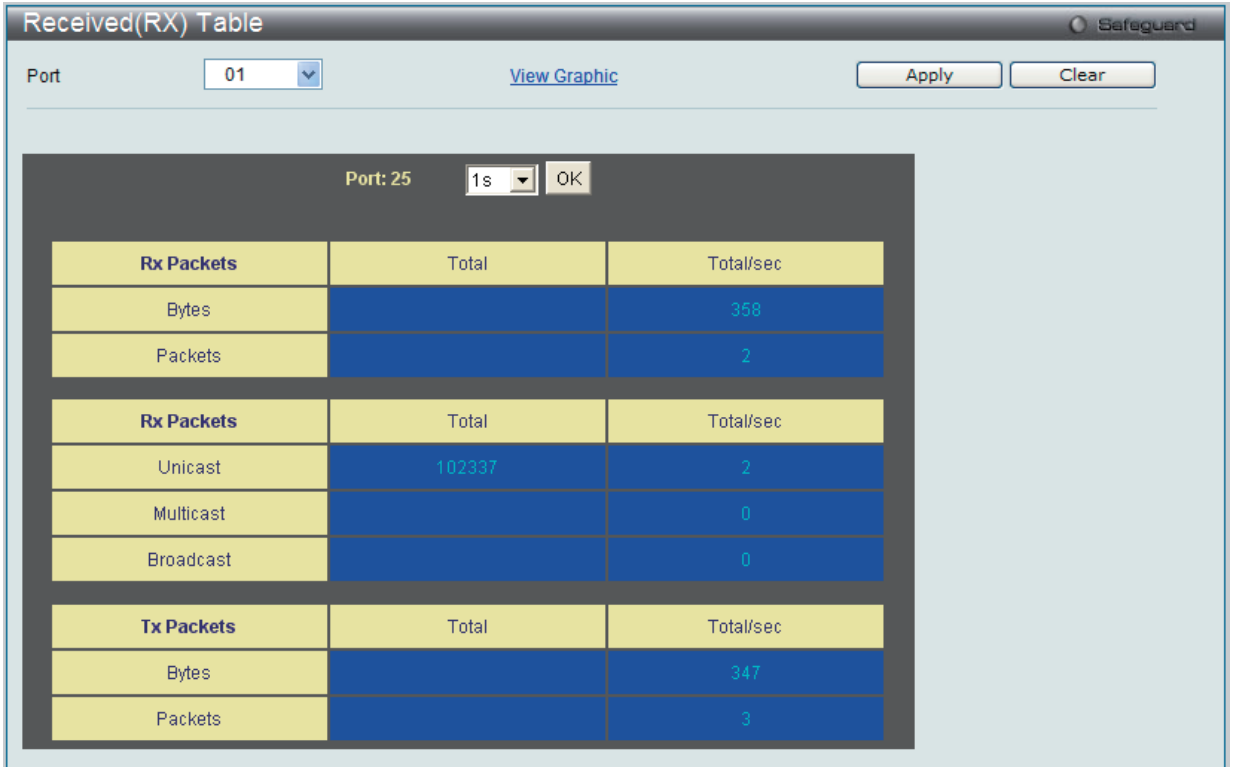


図 11-8　Received（RX）Table 画面（バイトとパケットの表）

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
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。
Time Interval	1 秒から 60 秒で指定します。初期値は 1 秒です。
Record Number	20 から 200 でスイッチにポーリングを行う回数を指定します。初期値は 200 です。
Bytes	ポートに受信したパケット量（バイト）
Packets	ポートに受信したパケット数
Unicast	ユニキャストアドレスが受信した正常なパケットの合計数をカウントします。
Multicast	マルチキャストアドレスが受信した正常なパケットの合計数をカウントします。
Broadcast	ブロードキャストキャストアドレスが受信した正常なパケットの合計数をカウントします。
Show/ Hide	Bytes と Packets を表示 / 非表示にします。
Clear	この画面のすべての統計情報をクリアします。
View Table	折れ線グラフ形式から表形式に表示を変更します。
View Graphic	表形式から折れ線グラフ形式に表示を変更します。

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。

UMB_Cast（Rx）（UMB Cast パケット統計情報の参照）

UMB（ユニキャスト、マルチキャスト、ブロードキャスト）に関する折れ線グラフを表示します。プルダウンメニューでポートを選択し、統計情報を参照します。Web ページ先頭のポートをクリックすることで、スイッチのリアルタイムグラフィックを使用することができます。

Monitoring > Packets > UMB_Cast（Rx）の順にメニューをクリックし、以下の画面を表示します。

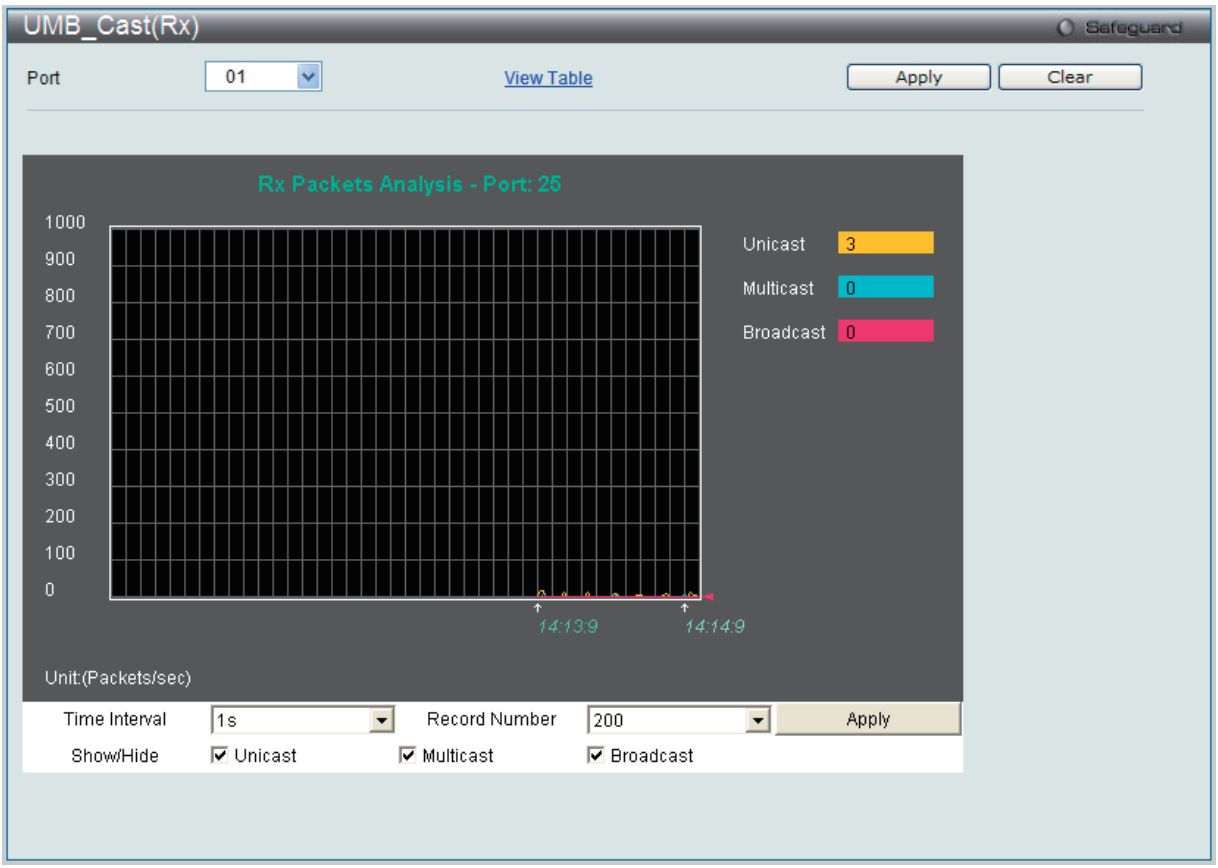


図 11-9　UMB_Cast（Rx）画面（ユニキャスト、マルチキャスト、ブロードキャスト情報の折れ線グラフ）

「UMB_cast（RX）Table」画面の表示を行うためには、「View Table」リンクをクリックします。

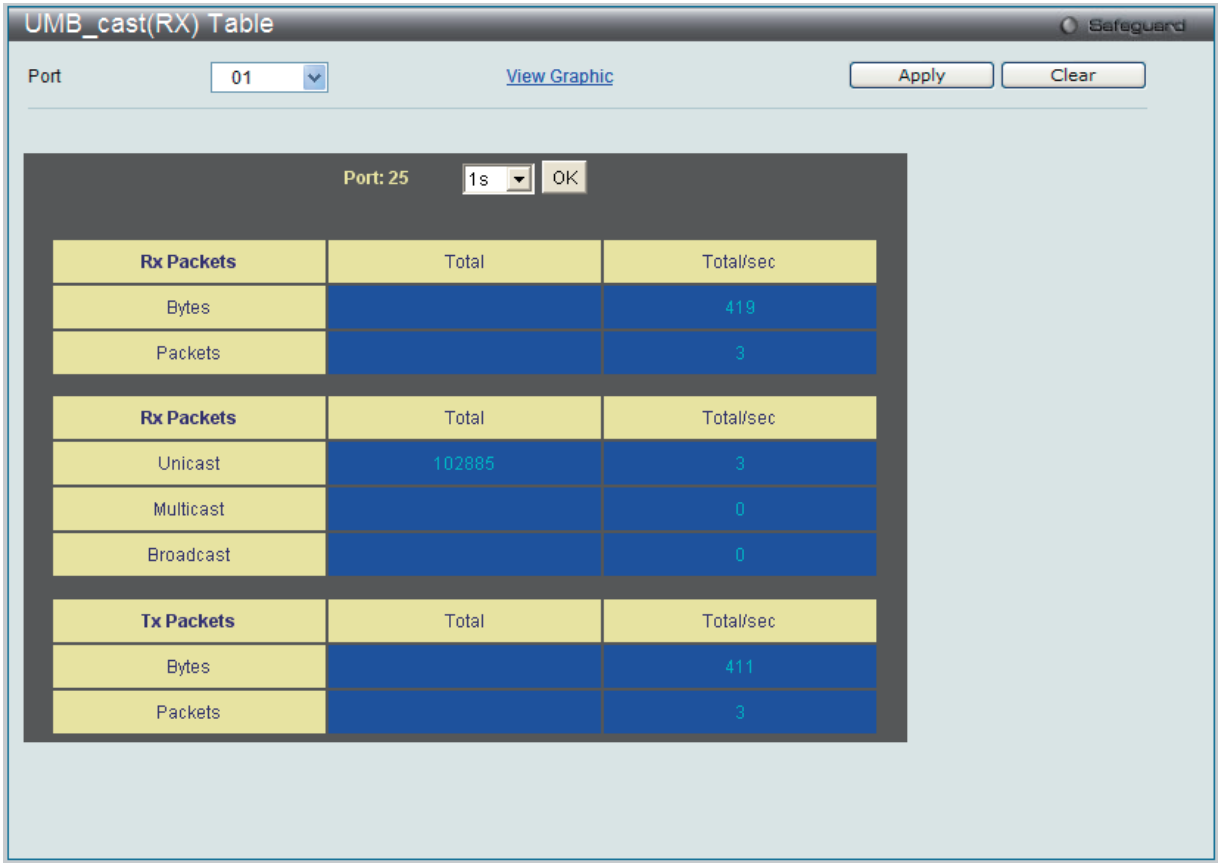


図 11-10　UMB_cast（RX）Table 画面（ユニキャスト、マルチキャスト、ブロードキャスト情報の表形式表示）

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
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。
Time Interval	1 秒から 60 秒で指定します。初期値は 1 秒です。
Record Number	20 から 200 でスイッチにポーリングを行う回数を指定します。初期値は 200 です。
Unicast	ユニキャストアドレスが受信した正常なパケットの合計数をカウントします。
Multicast	マルチキャストアドレスが受信した正常なパケットの合計数をカウントします。
Broadcast	ブロードキャストアドレスが受信した正常なパケットの合計数をカウントします。
Show/ Hide	Unicast、Multicast、Broadcast を表示 / 非表示にします。
Clear	この画面のすべての統計情報をクリアします。
View Table	折れ線グラフ形式から表形式に表示を変更します。
View Graphic	表形式から折れ線グラフ形式に表示を変更します。

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。

Transmitted（Tx）（送信パケット統計情報）

スイッチから送信したパケットの情報をグラフ表示します。プルダウンメニューでポートを選択し、統計情報を参照します。Web ページ先頭のポートをクリックすることで、スイッチのリアルタイムグラフィックを使用することができます。

Monitoring > Packets > Transmitted（Tx）の順にメニューをクリックし、以下の画面を表示します。

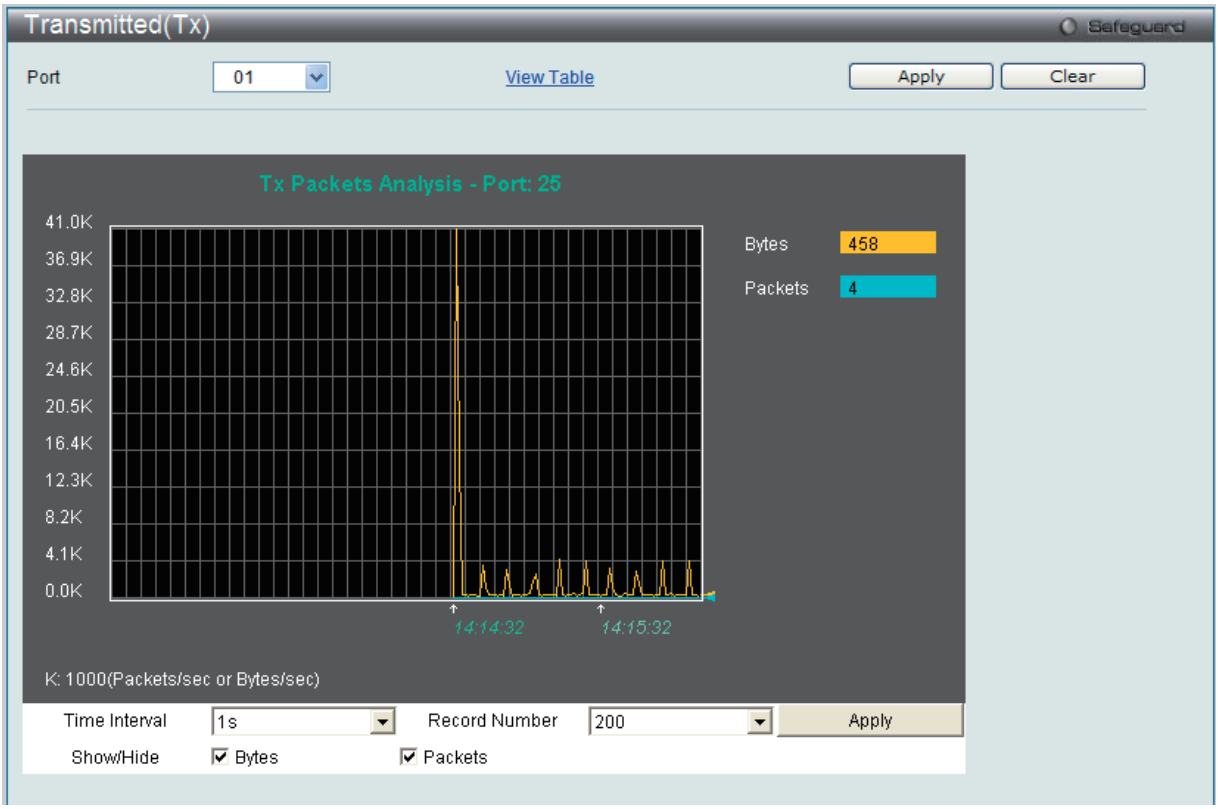


図 11-11　Transmitted（Tx）画面（パケットサイズ、パケット数の折れ線グラフ表示）

送信パケットの情報を、表形式で表示するには、「View Table」リンクをクリックし、以下の画面を表示します。

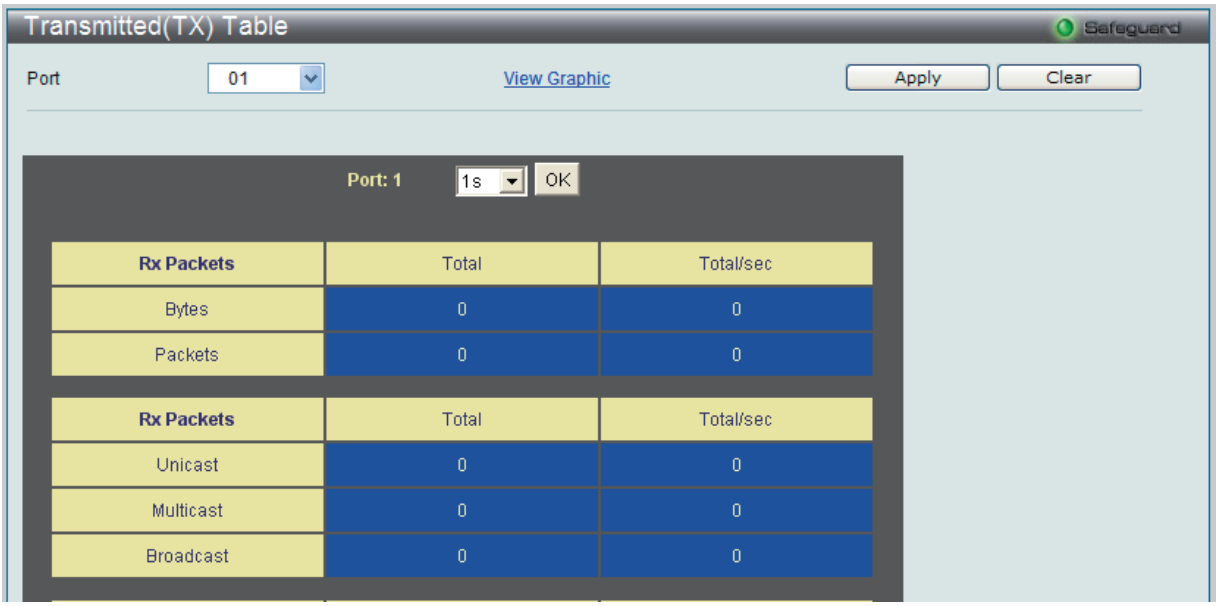


図 11-12　Transmitted（TX）Table 画面（パケットサイズ、パケット数の表示）

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
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。
Time Interval	1 秒から 60 秒で指定します。初期値は 1 秒です。
Record Number	20 から 200 でスイッチにポーリングを行う回数を指定します。初期値は 200 です。
Bytes	ポートから送信に成功したパケット量（バイト）。
Packets	ポートから送信に成功したパケット数。
Unicast	ユニキャストアドレスが送信した正常なパケットの合計数をカウントします。
Multicast	マルチキャストアドレスが送信した正常なパケットの合計数をカウントします。
Broadcast	ブロードキャストアドレスが送信した正常なパケットの合計数をカウントします。
Show/ Hide	Bytes と Packets を表示 / 非表示にします。
Clear	この画面のすべての統計情報をクリアします。
View Table	折れ線グラフ形式から表形式に表示を変更します。
View Graphic	表形式から折れ線グラフ形式に表示を変更します。

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。

Errors（パケットエラー）

Web マネージャは、スイッチの管理エージェントが集計したエラー統計情報を、折れ線グラフまたは表形式で表示します。以下の 4 つの画面で表示できます。

Received（Rx）（受信エラーパケット統計情報の参照）

スイッチが受信したエラーパケットの情報を表示します。プルダウンメニューでポートを選択し、統計情報を参照します。Web ページ先頭のポートをクリックすることで、スイッチのリアルタイムグラフィックを使用することができます。

Monitoring > Errors > Received（Rx）の順にメニューをクリックし、以下の画面を表示します。

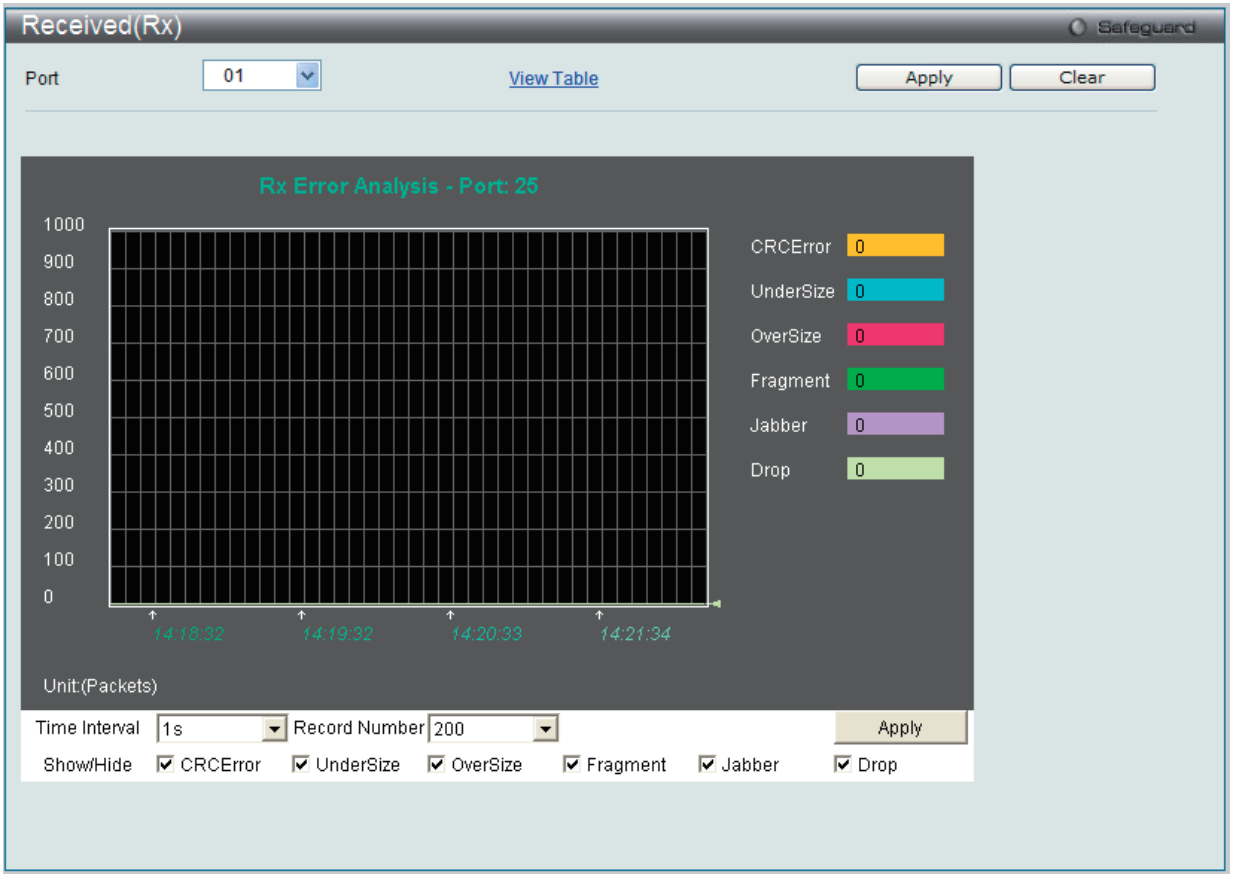


図 11-13　Received（Rx）- Error 画面（折れ線グラフ形式）

表形式の「Received（RX）Table」画面を表示するためには、「View Table」リンクをクリックします。

図 11-14　Received（RX）Table - Error 画面（表形式）

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	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。
Time Interval	1 秒から 60 秒で指定します。初期値は 1（秒）です。
Record Number	20 から 200 でスイッチにポーリングを行う回数を指定します。初期値は 200 です。
CRCError	CRC エラーがある受信パケット数。パケットの許容値のバイト（オクテット）で終了しない正常なパケットの数。
UnderSize	パケットの最小許容値である 64 バイト以下で、CRC 値は正常なパケットの受信数。アンダーサイズパケットはコリジョンの発生を示しています。
OverSize	エラーパケットが 1518 オクテットより長く、さらに MAX_PKT_LEN より短い正常な受信パケットをカウントします。内部的には MAX_PKT_LEN は 1536 オクテットです。
Fragment	64 バイト以下でフレーミングエラーや無効な CRC を含むパケット受信数。これらのパケットはコリジョンの発生に起因します。
Jabber	エラーパケットが 1518 オクテットより長く、さらに MAX_PKT_LEN より短い不正な受信パケットをカウントします。内部的には MAX_PKT_LEN は 1536 オクテットです。
Drop	前回の再起動からその時点までに廃棄したパケット数。
Symbol	物理的に配下にあるシンボル内に受信したエラーパケット数。
Show/ Hide	CRCError、UnderSize、OverSize、Fragment、Jabber、Drop および SymbolErr を表示するかどうかをチェックします。
Clear	この画面のすべての統計情報をクリアします。
View Table	折れ線グラフ形式から表形式に表示を変更します。
View Graphic	表形式から折れ線グラフ形式に表示を変更します。

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。

Transmitted（Tx）（送信エラーパケット統計情報の参照）

スイッチでの送信エラーパケットの情報を表示します。プルダウンメニューでポートを選択し、統計情報を参照します。Web ページ先頭のポートをクリックすることで、スイッチのリアルタイムグラフィックを使用することができます。

Monitoring > Error > Transmitted（Tx）の順にメニューをクリックし、以下の画面を表示します。

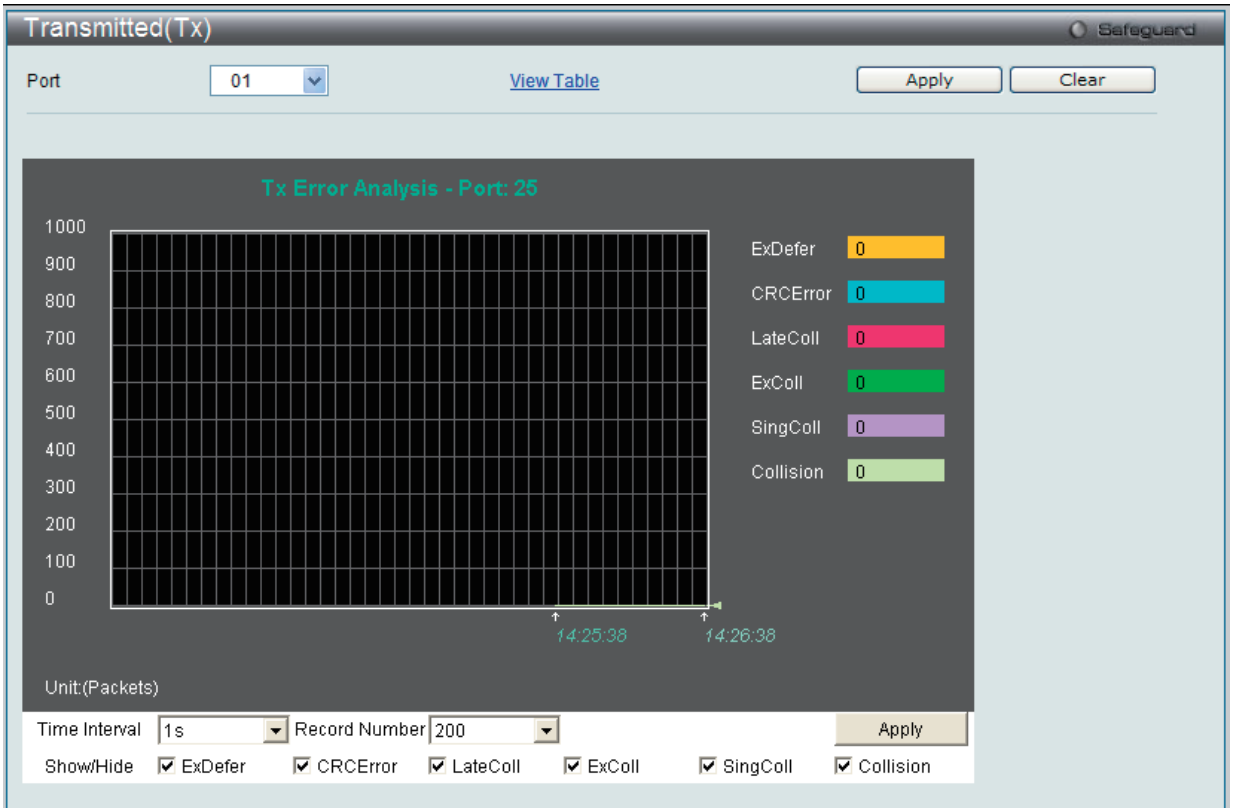


図 11-15　Transmitted（Tx）- Error 画面（折れ線グラフ形式）

表形式の「Transmitted（TX）」画面を表示するためには、「View Table」リンクをクリックします。

図 11-16　Transmitted（TX）Table - Error 画面（表形式）

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	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。
Time Interval	1 秒から 60 秒で指定します。初期値は 1 秒です。
Record Number	20 から 200 でスイッチにポーリングを行う回数を指定します。初期値は 200 です。
ExDefer	特定のインタフェースに対する最初の送信が回線ビジーのために遅延したパケット数をカウントします。
CRC Error	CRC エラーがある受信パケット数。パケットの許容値のバイト（オクテット）で終了しない正常なパケットの数。
LateColl	パケットの送信に 512bit times より大きい往復遅延時間を検出されたコリジョンの回数をカウントします。
ExColl	過度のコリジョンのために送信エラーとなったパケット数。
SingColl	シングルコリジョンフレーム数。1 個以上のコリジョンにより送信されていなかったパケットで送信に成功した数。
Collision	ネットワークセグメントにおける推定総コリジョン数。
Show/ Hide	CRCError、UnderSize、OverSize、Fragment、Jabber、Drop および SymbolErr を表示するかどうかをチェックします。
Clear	この画面のすべての統計情報をクリアします。
View Table	折れ線グラフ形式から表形式に表示を変更します。
View Graphic	表形式から折れ線グラフ形式に表示を変更します。

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。

Port Access Control（ポートアクセスコントロール）

以下の画面ではスイッチ上の 802.1X の統計情報をポートごとに表示します。「Port Access Control」フォルダ中の画面はスイッチの 802.1X 統計情報をポートごとに表示する際に使用します。

Monitoring > Port Access Control の順にメニューをクリックします。このセクションには 7 個のモニタ画面があります。

RADIUS Authentication（RADIUS 認証）

このテーブルは RADIUS 認証プロトコルでクライアント側の RADIUS 認証クライアントの動作に関連する情報を表示します。

「RADIUS Authentication」画面を参照するためには、**Monitoring > Port Access Control > RADIUS Authentication** をクリックします。

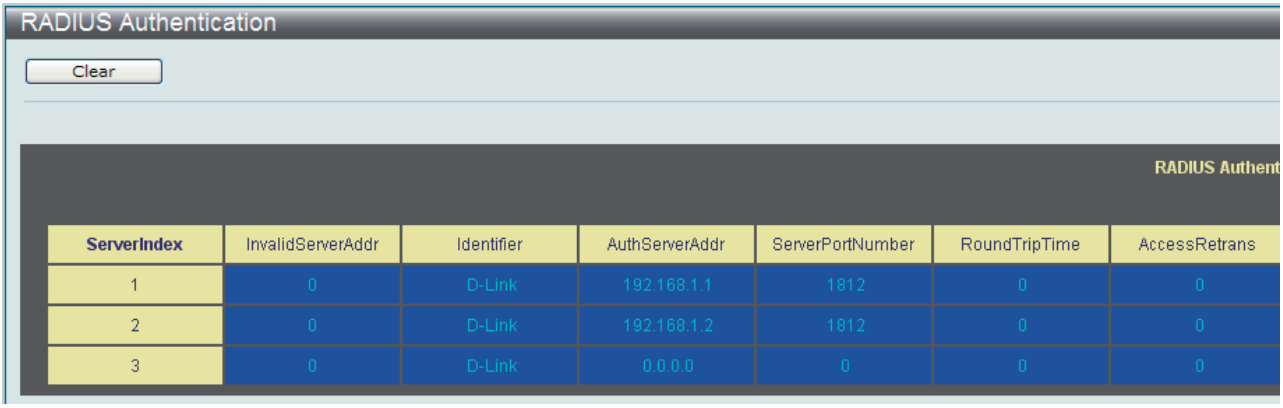


図 11-17　RADIUS Authentication 画面

統計情報の更新間隔を 1s から 60s（s：秒）で選択します。初期値は 1s（1 秒）です。現在の統計情報をクリアするためには左上角の「Clear」ボタンをクリックします。以下の情報が表示されます。

項目	説明
ServerIndex	クライアントが暗号鍵を共有している各 RADIUS 認証サーバに割り当てられた識別子の番号。
InvalidServerAddr	不明なアドレスから受信した RADIUS Access-Response パケット数。
Identifier	RADIUS 認証クライアントの NAS 識別子。（MIB II の sysName と同じである必要はありません。）
AuthServerAddr	クライアントが暗号鍵を共有している RADIUS 認証サーバを一覧にしているテーブル。
ServerPortNumber	クライアントがこのサーバにリクエストを送信するために使用する UDP ポート。
RoundTripTime	最も最近 RADIUS 認証サーバから送信された Access-Reply/Access-Challenge と Access-Request の間隔（1/100 秒単位）。
AccessRequests	サーバに送信された RADIUS Access-Request パケット数。再送信は含まれません。
AccessRetrans	本 RADIUS 認証サーバに再送信された RADIUS Access-Request パケット数。
AccessAccepts	本サーバから受信した RADIUS Access-Accept パケット数（有効 / 無効パケット）。
AccessRejects	本サーバより受信した RADIUS Access-Reject パケット数（有効 / 無効パケット）。
AccessChallenges	本サーバより受信した RADIUS Access-Challenge パケット数（有効 / 無効パケット）。
AccessResponses	本サーバより受信した不正な形式の RADIUS Access-Response パケット数。不正形式のパケットには不正な長さのパケットも含まれます。不正認証、署名属性、または不明なタイプは不正な Access Responses としては含まれません。
BadAuthenticators	本サーバより受信した不正認証や署名属性 RADIUS Access-Response パケット数。
PendingRequests	まだタイムアウトになっていない、またはレスポンスを受信していないこのサーバ行きの RADIUS Access-Request パケット数。この変数は Access-Request が送信されると 1 つ増加し、Access-Accept、Access-Reject または Access-Challenge の受信、タイムアウトまたは再転送時に 1 つ減少します。
Timeouts	本サーバへの認証タイムアウト数。タイムアウトの後、クライアントは同じサーバにリトライするか、異なるサーバに送信するか、または送信を終了します。同じサーバへのリトライはタイムアウトと同様に再転送としてカウントされます。異なるユーザへの送信はタイムアウトと同様に Request としてカウントされます。
UnknownTypes	本サーバから認証ポートに受信した不明なタイプの RADIUS パケット数。
PacketsDropped	本サーバから認証ポートに受信し、何らかの理由で破棄した RADIUS パケット数。

RADIUS Account Client（RADIUS アカウンティングクライアント）

本画面では RADIUS Accounting クライアントを管理するために使用する管理オブジェクトとそれらに関連した現在の統計情報を表示します。クライアントが暗号鍵を共有している RADIUS 認証サーバごとに列があります。

「RADIUS Accounting Client」画面を参照するためには、**Monitoring > Port Access Control > RADIUS Account Client** をクリックします。

図 11-18　RADIUS Account Client 画面

統計情報を更新するためには更新間隔を 1s ～ 60s（s は秒）から指定します。初期値は 1（秒）です。現在の統計情報をクリアするためには左上の「Clear」ボタンをクリックします。以下の情報が表示されます。

項目	説明
ServerIndex	クライアントが暗号鍵を共有する RADIUS Accounting サーバの IP アドレス。
InvalidServerAddr	不明なアドレスから受信した RADIUS Accounting-Response パケット数。
Identifier	RADIUS アカウンティングクライアントの NAS 識別子。（MIB II の sysName と同じである必要はありません。）
ServerAddr	クライアントが暗号鍵を共有している RADIUS アカウンティングサーバを一覧にしているテーブル。
ServerPortNumber	クライアントがこのサーバにリクエストを送信するために使用する UDP ポート。
RoundTripTime	RADIUS アカウンティングサーバからクライアントに送信される最も新しい Accounting-Response と Accounting-Request の間隔。
Requests	送信された RADIUS Accounting-Request パケット数。これは再転送のパケット数は含まれていません。
Retransmissions	RADIUS アカウンティングサーバに再送された RADIUS Accounting-Request 数。再送には、同じものが残るような Identifier および Acct-Delay が更新されるというリトライも含まれます。

項目	説明
Responses	本サーバから Accounting ポートに受信した RADIUS パケット数。
MalformedResponses	このサーバから受信した不正な形式の RADIUS Accounting-Response パケット数。Malformed packets には不正な長さのパケットを含まれます。認証エラーや不明なタイプは不正な accounting responses としては含まれません。
BadAuthenticators	このサーバから受信した不正な認証を含む RADIUS Accounting-Response パケット数。
PendingRequests	まだタイムアウトになっていない、またはレスポンスを受信していないサーバ行きの RADIUS Accounting-Request パケット数。この変数は Accounting-Request が送信された時に 1 つ加算し、Accounting-Response の受信、タイムアウトまたは再転送時に 1 つ減少します。
Timeouts	このサーバへの Accounting タイムアウト数。タイムアウトの後、クライアントは同じサーバにリトライするか、異なるサーバに送信するか、または送信を終了します。同じサーバへのリトライはタイムアウトと同様に再転送としてカウントされます。異なるユーザへの送信はタイムアウトと同様に Accounting-Request としてカウントされます。
UnknownTypes	このサーバから Accounting ポートに受信した不明なタイプの RADIUS パケット数。
PacketsDropped	このサーバから Accounting ポートに受信し、何らかの理由で破棄した RADIUS パケット数。

Authenticator State（オーセンティケータの状態）

スイッチの 802.1X 認証状態を表示します。

Monitoring > Port Access Control > Authenticator State の順にメニューをクリックし、「Authenticator Status」画面を表示します。

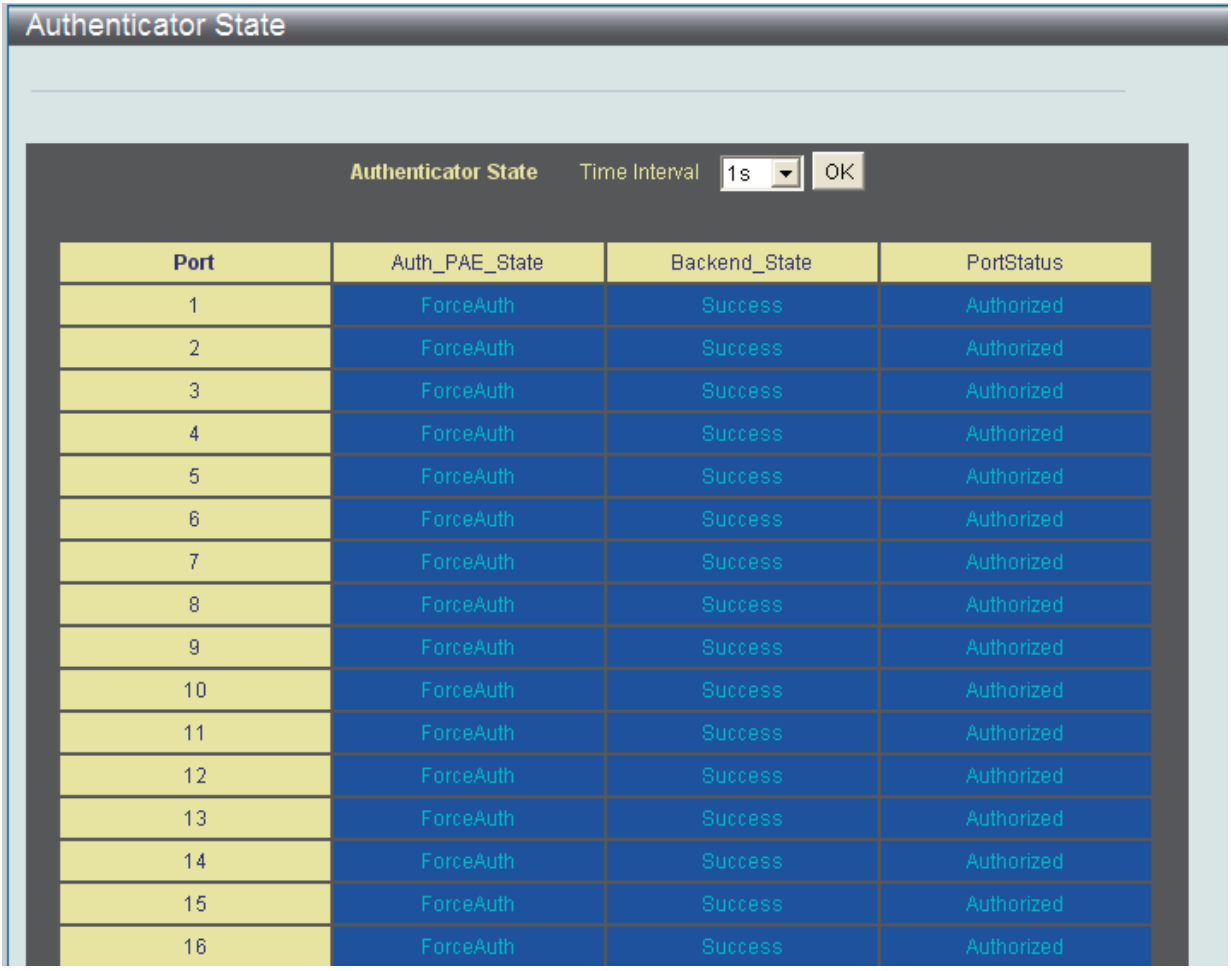


図 11-19　Authenticator State 画面（ポートベース 802.1X）

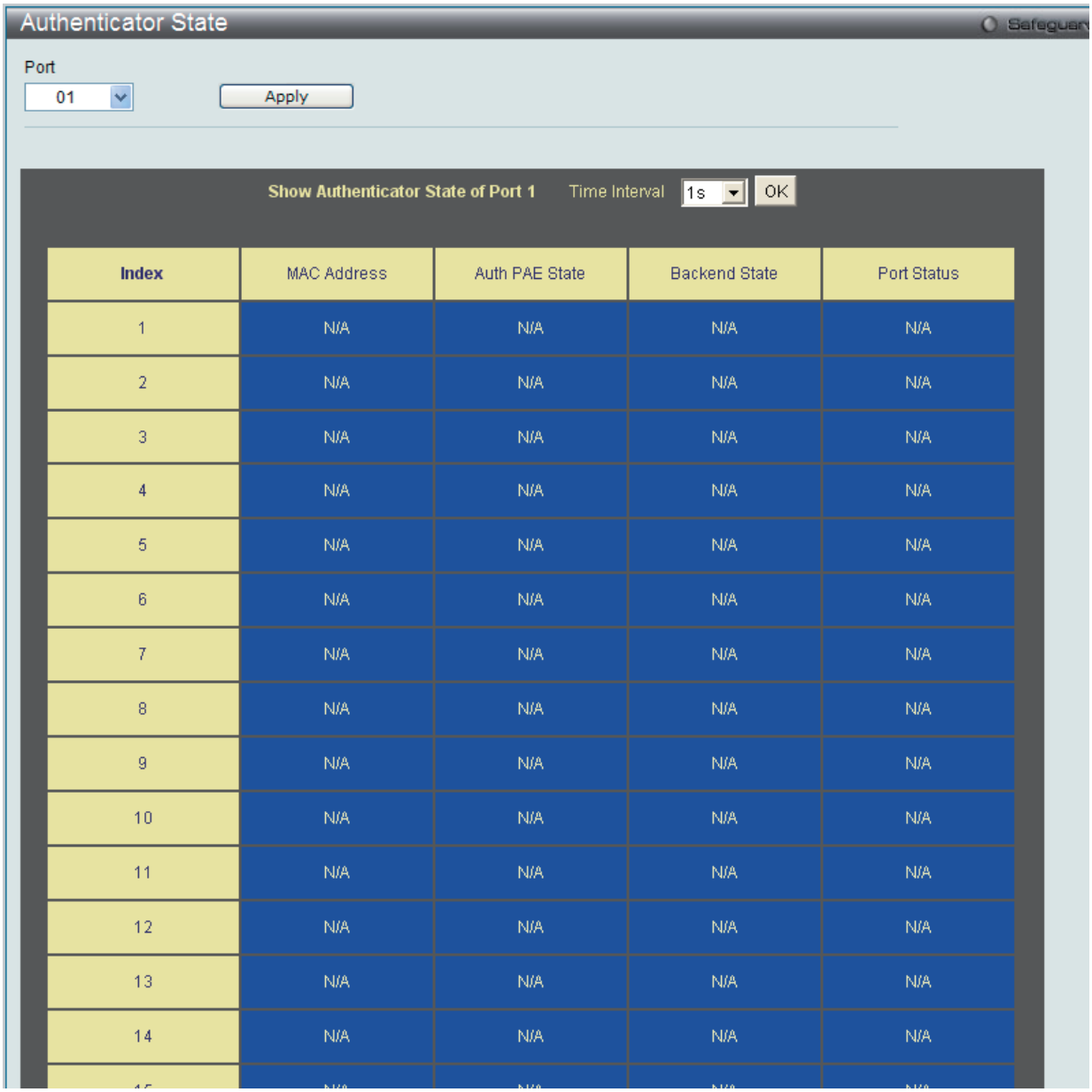


図 11-20　Authenticator State 画面（MAC ベース 802.1X）

本画面は、選択したデバイス上の各ポートについて、オーセンティケータの状態を表示します。プルダウンメニューを使用してポーリング間隔（モニタリング間隔）を 1 ～ 60 秒で選択し、「OK」ボタンをクリックします。

本画面で表示される内容は、以下の通りです。

項目	説明
Auth PAE State	オーセンティケータ PAE 状態として、「Initialize」、「Disconnected」、「Connecting」、「Authenticating」、「Authenticated」、「Aborting」、「Held」、「Force_Auth」、「Force_Unauth」、「N/A」のいずれかが表示されます。「N/A」（Not Available）はポートのオーセンティケータ機能が無効であることを示しています。
Backend State	バックエンド認証状態として、「Request」、「Response」、「Success」、「Fail」、「Timeout」、「Idle」、「Initialize」、「N/A」のいずれかが表示されます。「N/A」（Not Available）はポートのオーセンティケータ機能が無効であることを示しています。
Port Status	制御ポート状態として、「Authorized」、「Unauthorized」または「N/A」のいずれかが表示されます。
MAC Address	該当するインデックス番号のデバイスの MAC アドレスを表示します。

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。

Authenticator Statistics（Authenticator 統計情報）

この画面には各ポートに関連する Authenticator PAE に関する統計情報オブジェクトが含まれます。Authenticator 機能をサポートする各ポートの表にエントリが表示されます。

「Authenticator Statistics」画面を参照するためには、**Monitoring > Port Access Control > Authenticator Statistics** の順にクリックします。

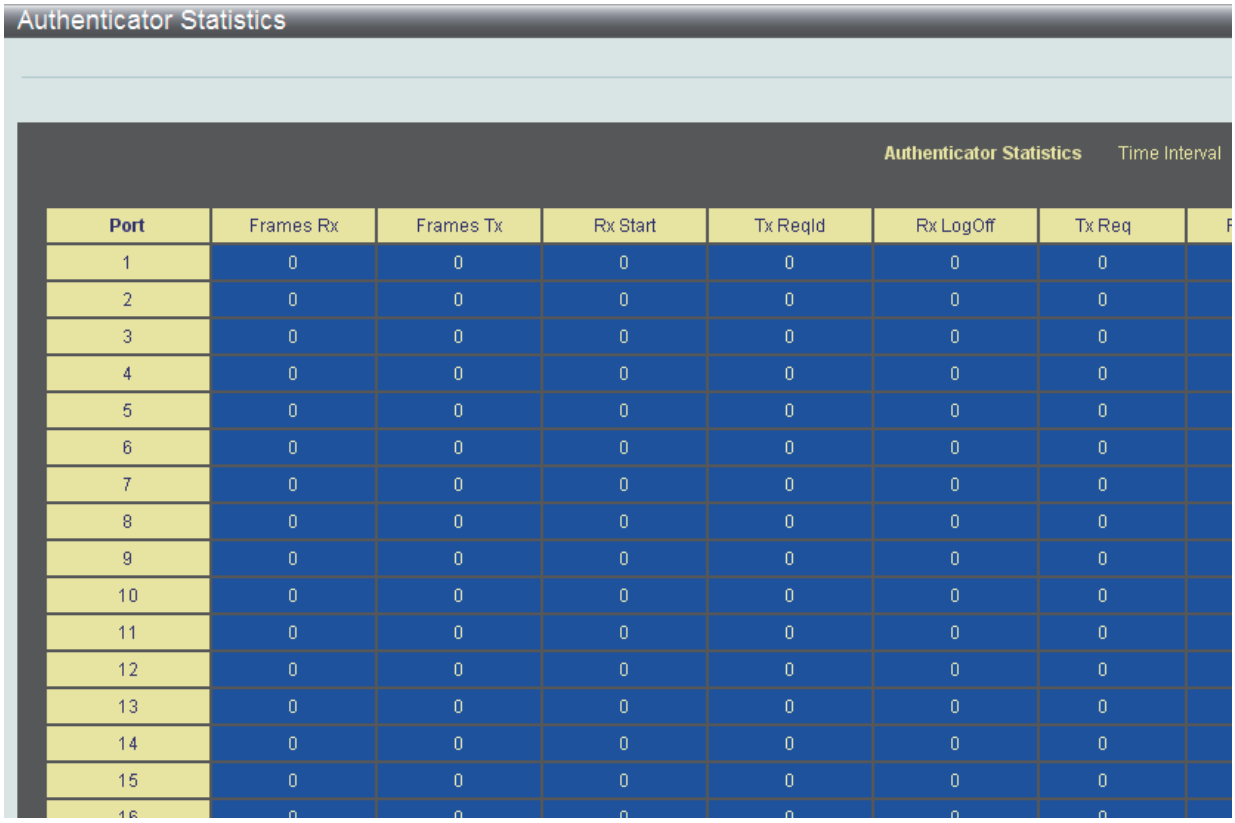


図 11-21　Authenticator Statistics 画面

統計情報を更新するためには更新間隔を 1s ～ 60s（s は秒）から指定します。初期値は 1 秒です。
以下の情報が表示されます。

項目	説明
Port	システムによってポートに割り当てられた識別番号。
Frames Rx	Authenticator が受信した有効な EAPOL フレーム数。
Frames Tx	Authenticator が送信した EAPOL フレーム数。
Rx Start	Authenticator が受信した EAPOL Start フレーム数。
Tx ReqId	Authenticator が送信した EAP Req/Id フレーム数。
Rx LogOff	Authenticator が受信した EAPOL Logoff フレーム数。
Tx Req	Authenticator が送信した EAP Request フレーム（Rq/Id フレーム以外）数。
Rx RespId	Authenticator が受信した EAP Resp/Id フレーム数。
Rx Resp	Authenticator が受信した有効な EAP Response フレーム（Resp/Id フレーム以外）数。
Rx Invalid	Authenticator が受信した認識されないフレームタイプを含む EAPOL フレーム数。
Rx Error	Authenticator が受信した Packet Body Length が不正な EAPOL フレーム数。
Last Version	受信 EAPOL フレームを最も最近送信したプロトコルバージョン。
Last Source	受信 EAPOL フレームを最も最近送信した送信元 MAC アドレス。

Authenticator Session Statistics（Authenticator セッション統計情報）

この表には各ポートに関連するAuthenticator PAEに関するセッションオブジェクト統計情報が含まれます。Authenticator機能をサポートする各ポートの表にエントリが表示されます。

「Authenticator Session Statistics」画面を参照するためには、**Monitoring > Port Access Control > Authenticator Session Statistics** の順にクリックします。

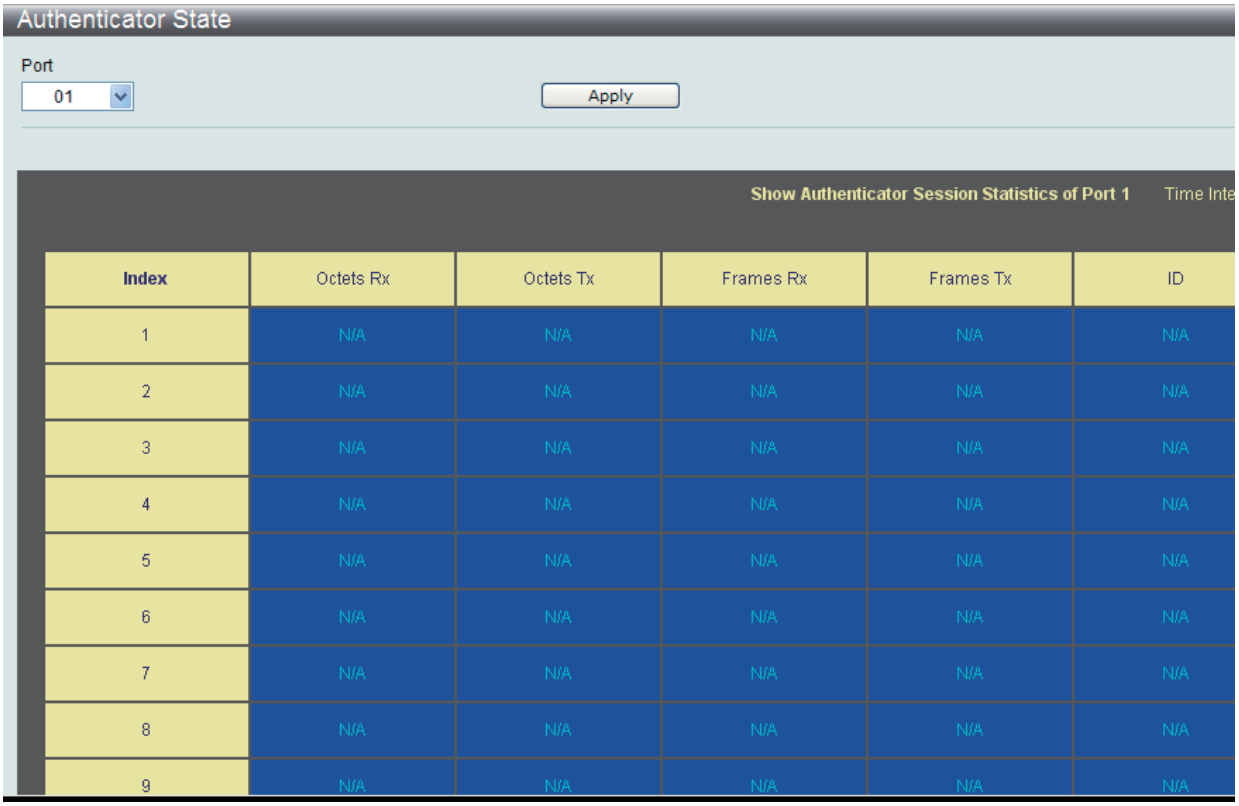


図 11-22　Authenticator Session Statistics 画面（MAC ベース 802.1X 認証）

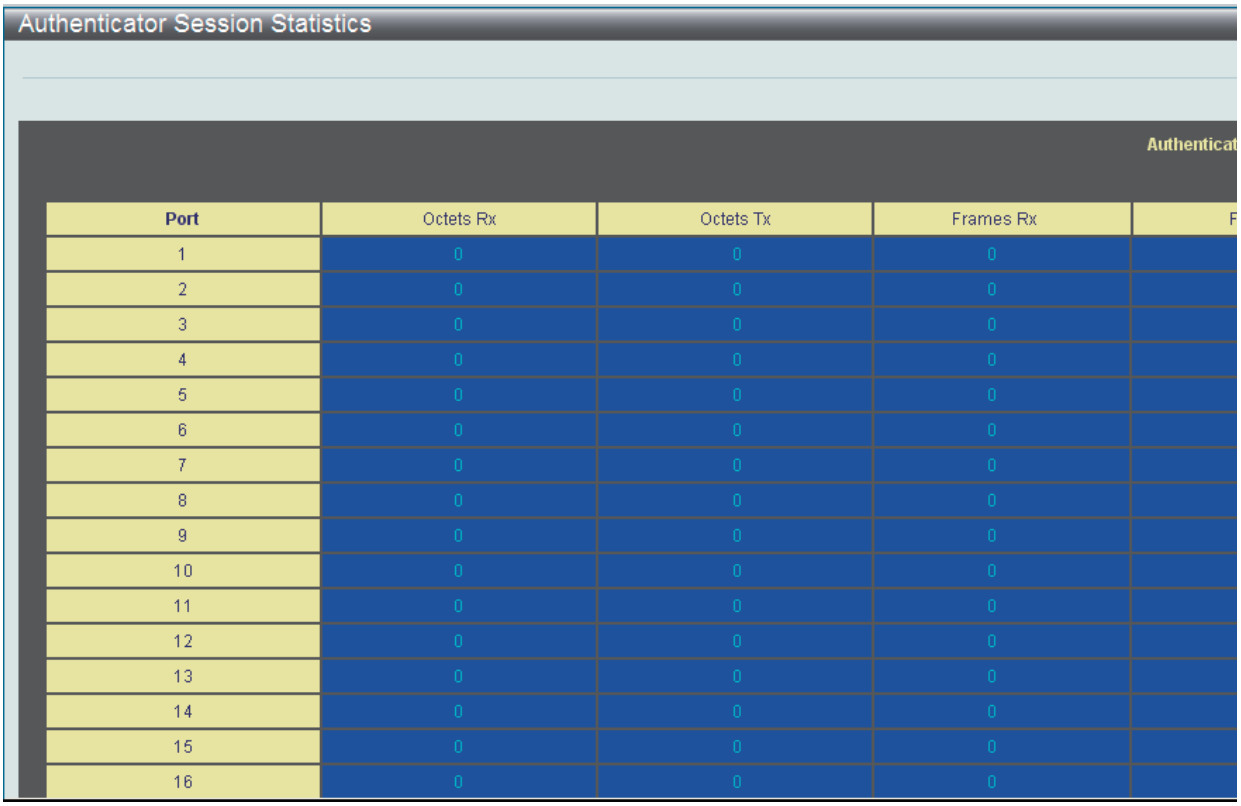


図 11-23　Authenticator Session Statistics 画面（ポートベース 802.1X 認証）

統計情報を更新するためには更新間隔を 1s ～ 60s（s は秒）から指定します。初期値は 1（秒）です。

項目	説明
Port / Index	ポートベースの 802.1X Authentication モードでは、システムがポートに割り当てた識別番号を表示します。MAC ベースの 802.1X Authentication モードでは、エントリのインデックス番号を表示します。
Octets Rx	このポートがセッション中にユーザデータフレーム内に受信したオクテット数。
Octets Tx	このポートがセッション中にユーザデータフレーム内に送信したオクテット数。
Frames Rx	このポートがセッション中に受信したユーザデータフレーム数。
Frames Tx	このポートがセッション中に送信したユーザデータフレーム数。
ID	セッションの識別子。（半角英数字 3 文字以上）。
Authentic Method	セッションを確立するために使用する認証方式。有効な方式は以下の通りです。 1）Remote Authentic Server - 認証サーバが Authenticator のシステムより外部にある。 2）Local Authentic Server - 認証サーバが Authenticator のシステム内にある。
Time	セッション時間（秒）。
Terminate Cause	セッションが終了した原因。以下の 8 個の原因があります。 1）Supplicant ログオフ 2）ポートのエラー 3）Supplicant 再起動 4）再認証の失敗 5）AuthControlledPortControl が ForceUnauthorized に設定された。 6）ポートの再初期化 7）ポート管理が無効 8）まだ終了していない
UserName	Supplicant PAE との一致を表すユーザ名。

Authenticator Diagnostics（Authenticator 診断）

この表には各ポートに関連する Authenticator の操作に関する診断情報が含まれ、Authenticator 機能をサポートする各ポートの表にエントリが表示されます。

「Authenticator Diagnostics」を参照するためには、**Monitoring > Port Access Control > Authenticator Diagnostics** の順にクリックします。

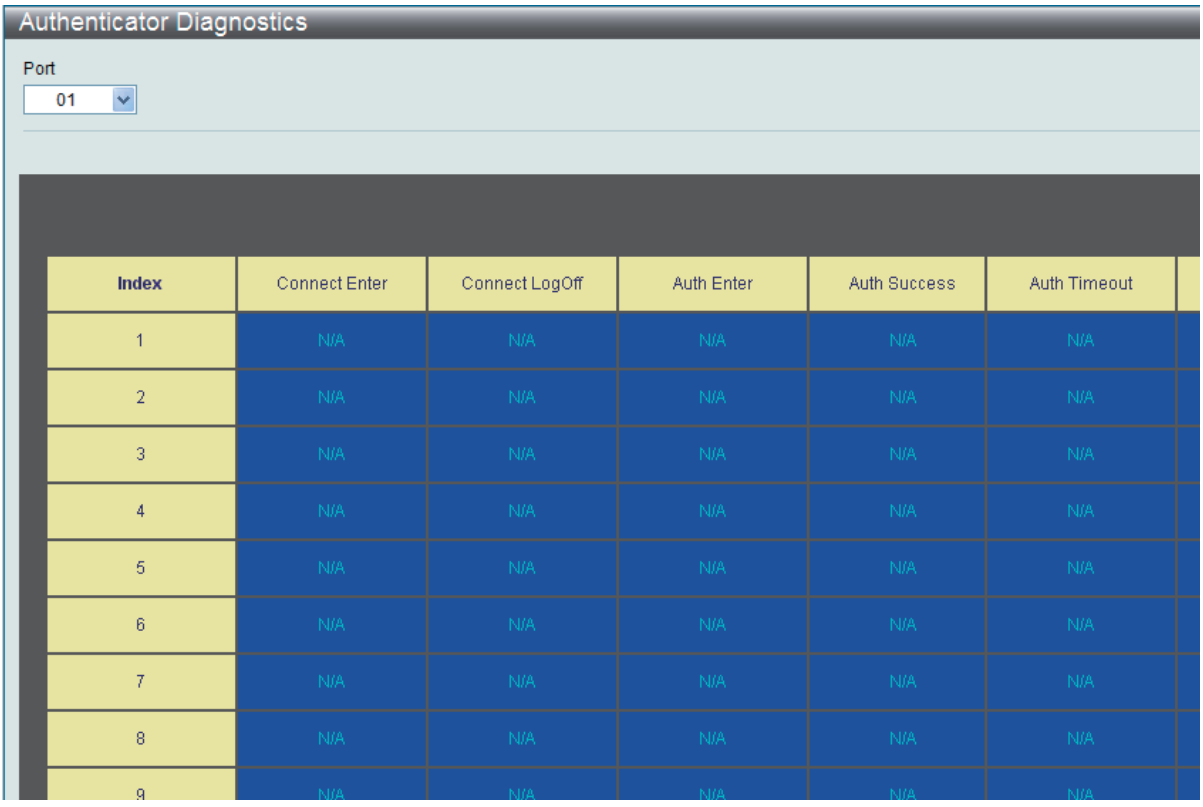


図 11-24　Authenticator Diagnostics 画面（MAC ベース 802.1X 認証モード）

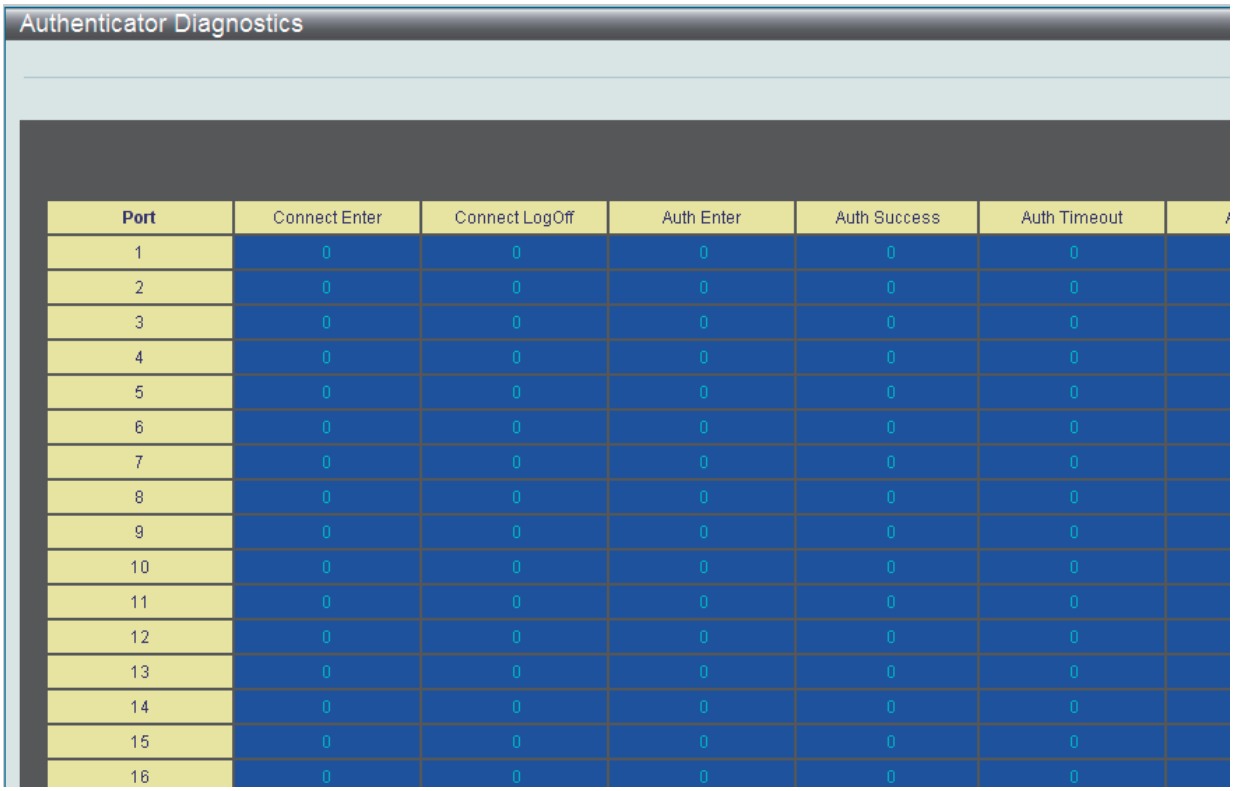


図 11-25　Authenticator Diagnostics 画面（ポートベース 802.1X 認証モード）

統計情報を更新するためには更新間隔を 1s ～ 60s（s は秒）から指定します。初期値は 1（秒）です。以下の情報が表示されます。

項目	説明
Port / Index	ポートベースの 802.1X Authentication モードでは、システムがポートに割り当てた識別番号を表示します。MAC ベースの 802.1X Authentication モードでは、エントリのインデックス番号を表示します。
Connect Enter	他の状態から CONNECTING 状態に状態遷移した回数をカウントします。
Connect LogOff	EAPOL-Logoff メッセージを受信した結果、CONNECTING から DISCONNECTED に状態遷移した回数をカウントします。
Auth Enter	サプリカントから EAP-Response/Identity メッセージを受信した結果、CONNECTING から AUTHENTICATING に状態遷移した回数をカウントします。
Auth Success	Backend Authentication 状態が Supplicant の認証成功（authSuccess = TRUE）となった結果、AUTHENTICATING から AUTHENTICATED に状態遷移した回数をカウントします。
Auth Timeout	Backend Authentication 状態が認証のタイムアウト（authTimeout = TRUE）となった結果、AUTHENTICATING から ABORTING に状態遷移した回数をカウントします。
Auth Fail	Backend Authentication 状態が認証失敗（authFail = TRUE）となった結果、AUTHENTICATING から HELD に状態遷移した回数をカウントします。
Auth Reauth	再認証リクエスト（reAuthenticate = TRUE）の結果、AUTHENTICATING から ABORTING に状態遷移した回数をカウントします。
Auth Start	サプリカントから EAPOL-Start メッセージを受信した結果、AUTHENTICATING から ABORTING に状態遷移した回数をカウントします。
Auth LogOff	サプリカントから EAPOL-Logoff メッセージを受信した結果、AUTHENTICATING から ABORTING に状態遷移した回数をカウントします。
Authed Reauth	再認証リクエスト（reAuthenticate = TRUE）の結果、AUTHENTICATED から CONNECTING に状態遷移した回数をカウントします。
Authed Start	サプリカントから EAPOL- Start メッセージを受信した結果、AUTHENTICATED から CONNECTING に状態遷移した回数をカウントします。
Authed LogOff	サプリカントから EAPOL-Logoff メッセージを受信した結果、AUTHENTICATED から DISCONNECTED に状態遷移した回数をカウントします。
Responses	State Machine が認証サーバに Initial Access-Request パケットを送信した（すなわちエントリ上の sendRespToServer が RESPONSE 状態となった）回数をカウントします。Authenticator が認証サーバとの通信を試みることを意味します。
AccessChallenges	State Machine が認証サーバから Initial Access-Challenge パケットを受信した（すなわち aReq が TRUE となり RESPONSE 状態を終了した）回数をカウントします。認証サーバが Authenticator との通信をしていることを意味します。
OtherReqToSupp	State Machine が EAP-Request パケット（Identity、Notification、Failure、または Success メッセージではない）をサプリカントに送信する（すなわちエントリ上の txReq が REQUEST 状態となった）回数をカウントします。Authenticator が EAP-method を選択したことを意味します。
OnNakRespFromSup	State Machine が Initial EAP-Request に対してパケットサプリカントからのレスポンスを受信し、そのレスポンスが EAP-NAK より他のものであった（すなわち rxResp が TRUE となり State Machine は REQUEST から RESPONSE 状態になったがそのレスポンスは EAP-NAK ではない）回数をカウントします。サプリカントが Authenticator の選択した EAP-method に応答することができることを意味します。
Bac Auth Success	State Machine が認証サーバから Accept メッセージを受信した（すなわち aSuccess が TRUE となり RESPONSE から SUCCESS に状態遷移した）回数をカウントします。サプリカントが認証サーバでの認証に成功したことを意味します。
Bac Auth Fail	State Machine が認証サーバから Reject メッセージを受信した（すなわち aFail が TRUE となり RESPONSE から FAIL に状態遷移した）回数をカウントします。サプリカントが認証サーバでの認証に失敗したことを意味します。

Browse ARP Table（ARP テーブルの参照）

本画面では、スイッチ上の現在の ARP エントリを表示します。

Monitoring > Browse ARP Table メニューをクリックし、「Browse ARP Table」画面を表示します。

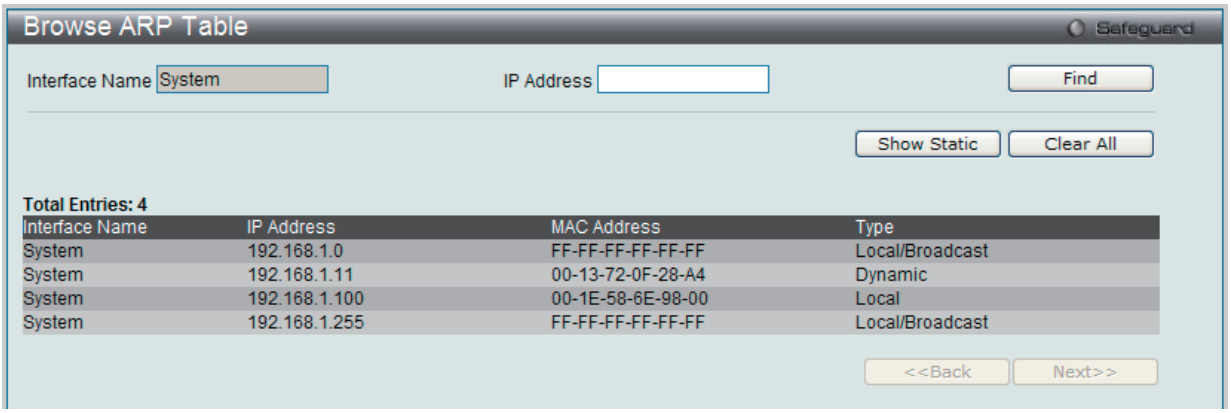


図 11-26　Browse ARP Table 画面

特定の ARP エントリを検索するためには、画面の上の「Interface Name」または「IP Address」を入力し、「Find」ボタンをクリックします。
スタティック ARP エントリを表示する場合は、「Show Static」ボタンをクリックします。
ARP テーブルをクリアする場合は、「Clear All」ボタンをクリックします。

Browse VLAN（VLAN の参照）

本画面では、スイッチの各ポートの VLAN ステータスを VLAN ごとに表示します。

Monitoring > Browse VLAN メニューをクリックし、「Browse VLAN」画面を表示します。

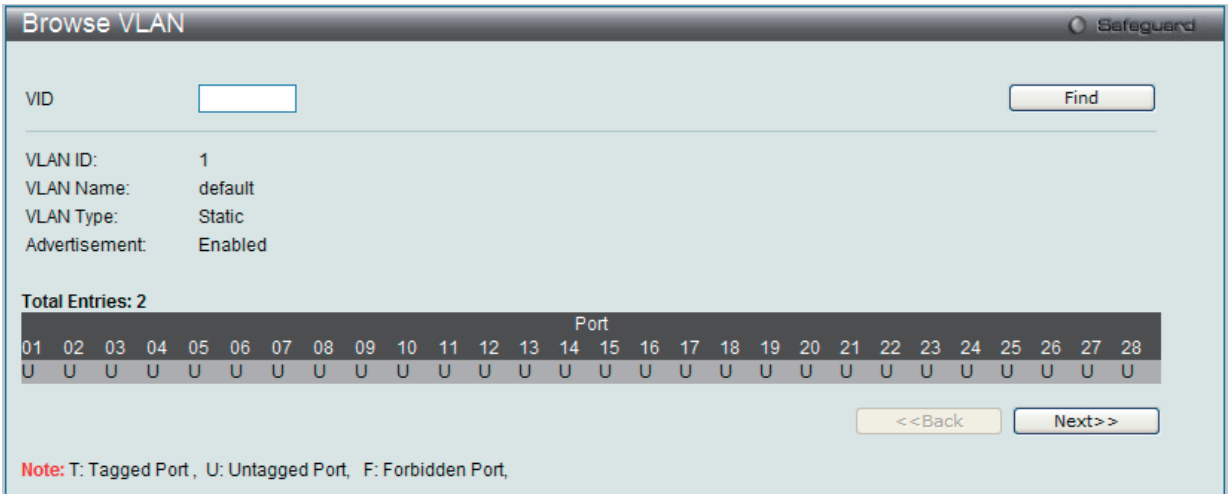


図 11-27　Browse VLAN 画面

画面上の「VID」に VLAN ID を入力し、「Find」ボタンをクリックします。

IGMP Snooping（IGMP Snooping 設定の参照）

スイッチの IGMP Snooping 設定を表示します。

Browse IGMP Router Port（ルータポート参照）

この画面ではスイッチのどのポートが現在ルータポートとして設定されているかを表示します。

Monitoring > IGMP Snooping > Browse IGMP Router Port メニューをクリックし、「Browse Router Port」画面を表示します。

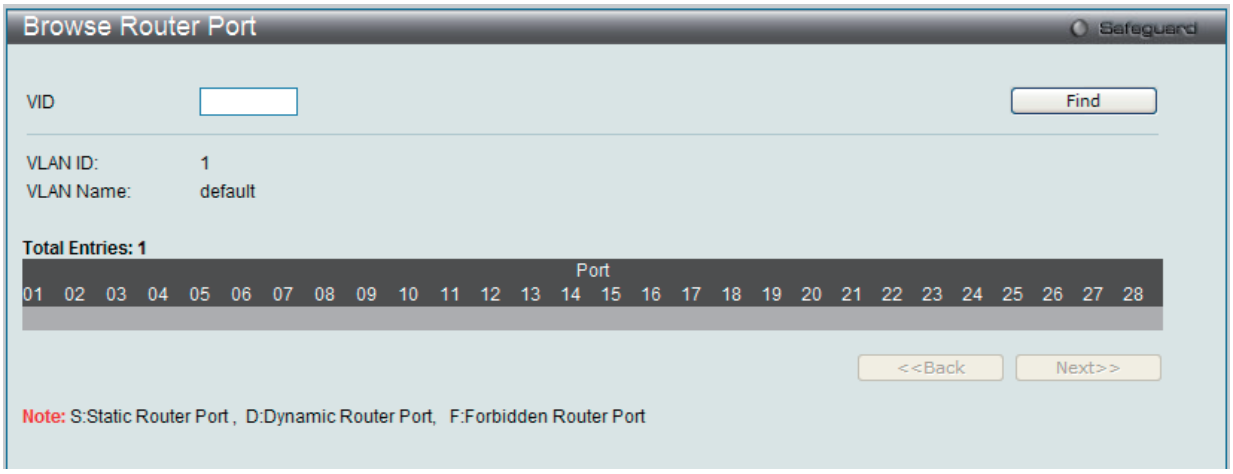


図 11-28　Browse Router Port 画面

コンソールまたは Web ベースの管理インタフェースで設定されたルータポートはスタティックルータポートとして「S」で表示されます。スイッチにダイナミックに設定されたルータポートは「D」と表示され、Forbidden ポートは「F」と表示されます。画面上の「VID」に VLAN ID を入力し、「Find」ボタンをクリックします。

IGMP Snooping Group（IGMP Snooping グループ）

スイッチの IGMP Snooping グループテーブルを参照します。
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の IP アドレスと送信元の IP アドレスを読み取ることができます。検索された IGMP レポートの数は「Reports」欄に表示されます。

Monitoring > IGMP Snooping > IGMP Snooping 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。

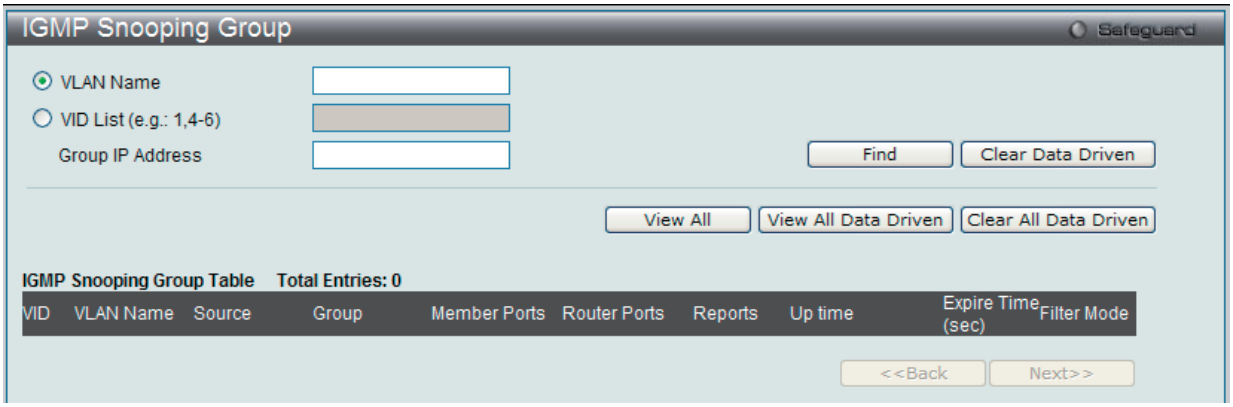


図 7-29　IGMP Snooping Group 画面

以下の項目を使用して、検索します。

項目	説明
VLAN Name	マルチキャストグループの VLAN 名。
VID List (e.g.: 1, 4-6)	マルチキャストグループの VLAN ポート。
Group IP Address	マルチキャストグループの IP アドレス。

適切な情報を入力して、「Find」ボタンをクリックします。検索されたエントリは「IGMP Snooping Group Table」に表示されます。

「View All」ボタンをクリックすると、すべてのエントリを表示します。
「View All Data Driven」ボタンをクリックすると、「IGMP Snooping Group Table」に学習されたすべての data driven グループが表示されます。
「Clear Data Driven」ボタンをクリックすると、「IGMP Snooping Group Table」内の学習された data driven グループがクリアされます。
「Clear All Data Driven」ボタンをクリックすると、「IGMP Snooping Group Table」内の学習された data driven グループがすべてクリアされます。

注意　スイッチの IGMP snooping を設定するためには、**L2 Features > IGMP Snooping** の順にメニューをクリックします。

IGMP Snooping Host（IGMP Snooping ホストの参照）

スイッチの現在の IGMP Snooping ホスト情報を表示します。

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

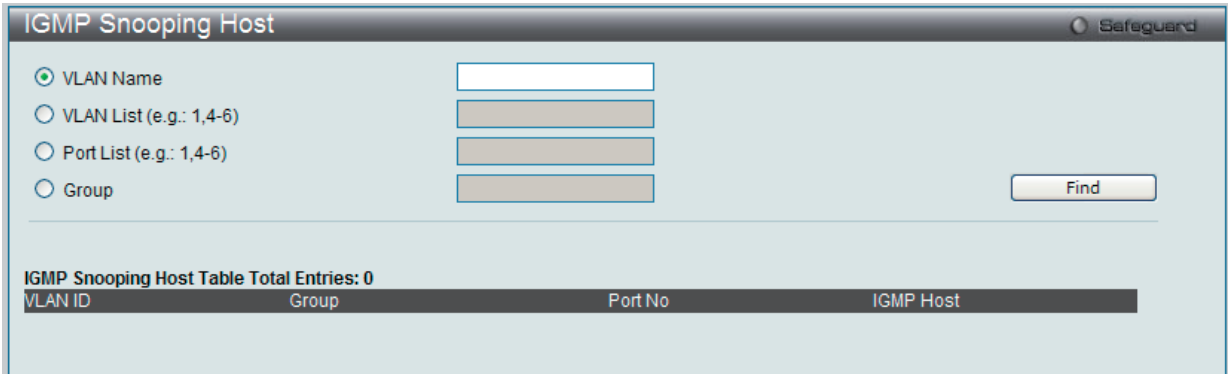


図 7-30　IGMP Snooping Host 画面

対応するラジオボタンをクリックし、「VLAN Name」、「VLAN List」、「Port List」または「Group」を入力し、「Find」ボタンをクリックします。検索されたエントリは、画面の下半分に表示されます。

MLD Snooping（MLD Snooping 設定の参照）

スイッチの MLD Snooping 設定を表示します。

Browse MLD Router Port（MLD ルータポートの参照）

本画面では、スイッチのどのポートが現在 IPv6 のルータポートとして設定されているかを表示します。

Monitoring > MLD Snooping > Browse MLD Router Port メニューをクリックし、以下の画面を表示します。

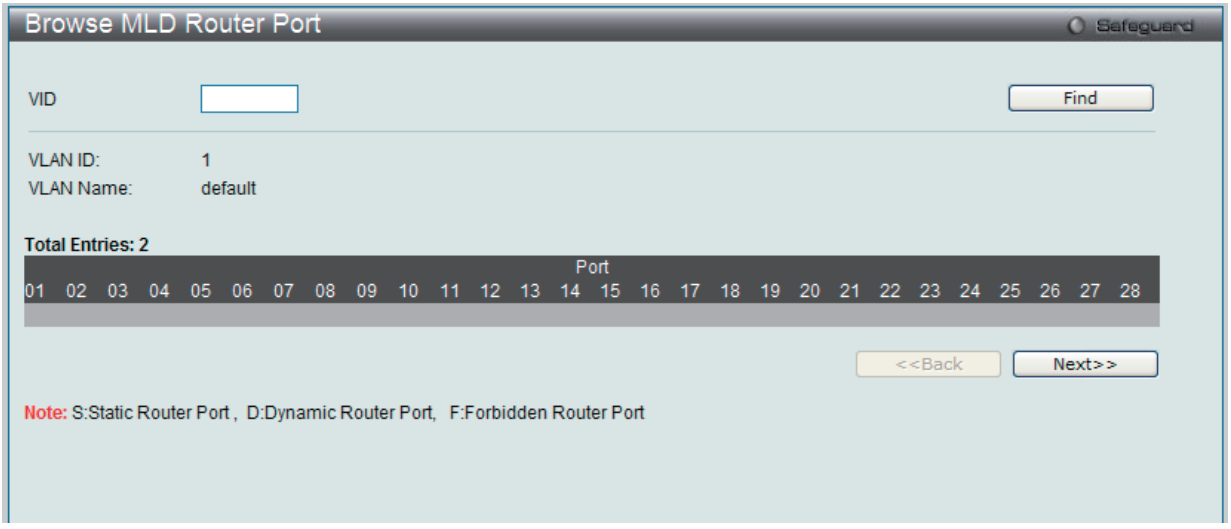


図 11-31　Browse MLD Router Port 画面

コンソールまたは Web ベースの管理インタフェースで設定されたルータポートはスタティックルータポートとして「S」で表示されます。スイッチにダイナミックに設定されたルータポートは「D」と表示され、Forbidden ポートは「F」と表示されます。画面上の「VID」に VLAN ID を入力し、「Find」ボタンをクリックします。

MLD Snooping Group（MLD Snooping グループ）

この画面でスイッチの MLD Snooping Group Table を参照します。MLD Snooping は、IPv4 の IGMP Snooping に相当する IPv6 の機能です。

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

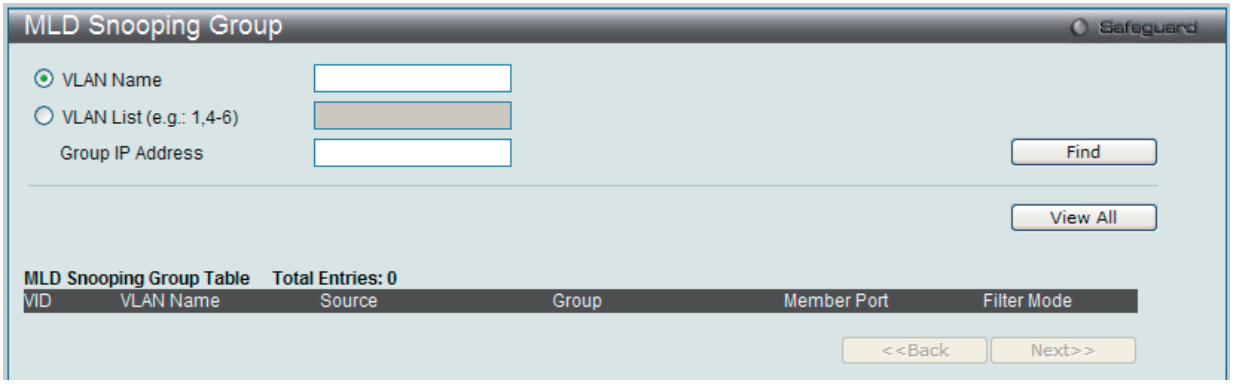


図 11-32　MLD Snooping Group 画面

以下の項目を使用して、検索します。

項目	説明
VLAN Name	マルチキャストグループの VLAN 名。
VID List (e.g.: 1, 4-6)	マルチキャストグループの VLAN ポート。
Group IP Address	マルチキャストグループの IP アドレス。

適切な情報を入力して、「Find」ボタンをクリックします。検索されたエントリは「MLD Snooping Group Table」に表示されます。

「View All」ボタンをクリックすると、すべてのエントリを表示します。
「View All Data Driven」ボタンをクリックすると、「MLD Snooping Group Table」に学習されたすべてのグループが表示されます。
「Clear Data Driven」ボタンをクリックすると、「MLD Snooping Group Table」内の学習されたグループがクリアされます。
「Clear All Data Driven」ボタンをクリックすると、「MLD Snooping Group Table」内の学習されたグループがすべてクリアされます。

注意　スイッチに MLD Snooping の設定を行うためには、**L2 Features > MLD Snooping Settings** を選択します。

LLDP（LLDP 設定の参照）

本製品には 3 つの LLDP 統計情報画面があります。

LLDP Statistics System（LLDP 統計情報システム）

LLDP の統計情報を表示します。

Monitoring > LLDP > LLDP Statistics 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。

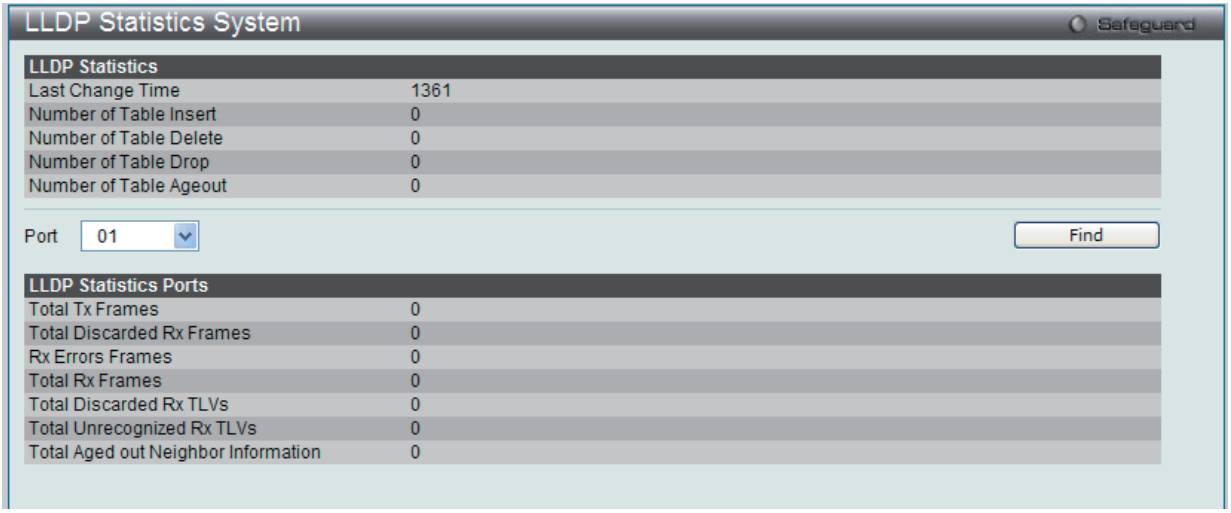


図 11-33　LLDP Statistics System 画面

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

LLDP のローカルポートの情報を表示します。

Monitoring > 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 :

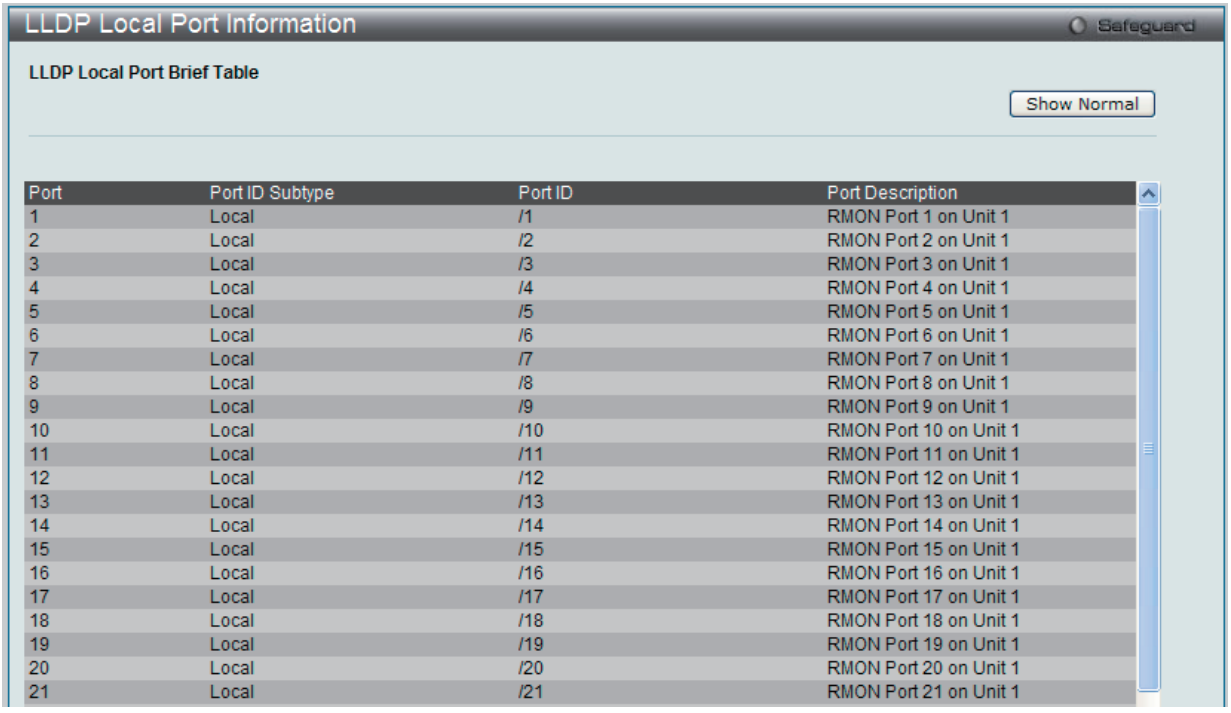


図 11-34　LLDP Local Port Information 画面

LLDP Remote Port Information（LLDP リモートポート情報）

LLDP のリモートポートの情報を表示します。

Monitoring > LLDP > LLDP Remote 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。

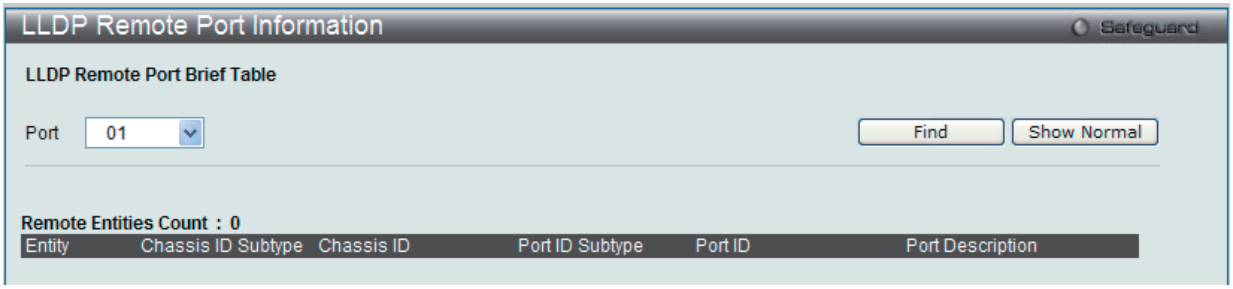


図 11-35　LLDP Remote Port Information 画面

Ethernet OAM（イーサネット OAM）

本フォルダには「Browse Ethernet OAM Event Log information」および「Browse Ethernet OAM Statistics」の 2 つの画面があります。

Browse Ethernet OAM Event Log（イーサネット OAM イベントログ）

イーサネット OAM イベントログ情報を表示します。本スイッチはバッファに 1000 個のイベントログを保存できます。イベントログは、各 OAM イベントに関する詳細な情報の提供と保存を行います。

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

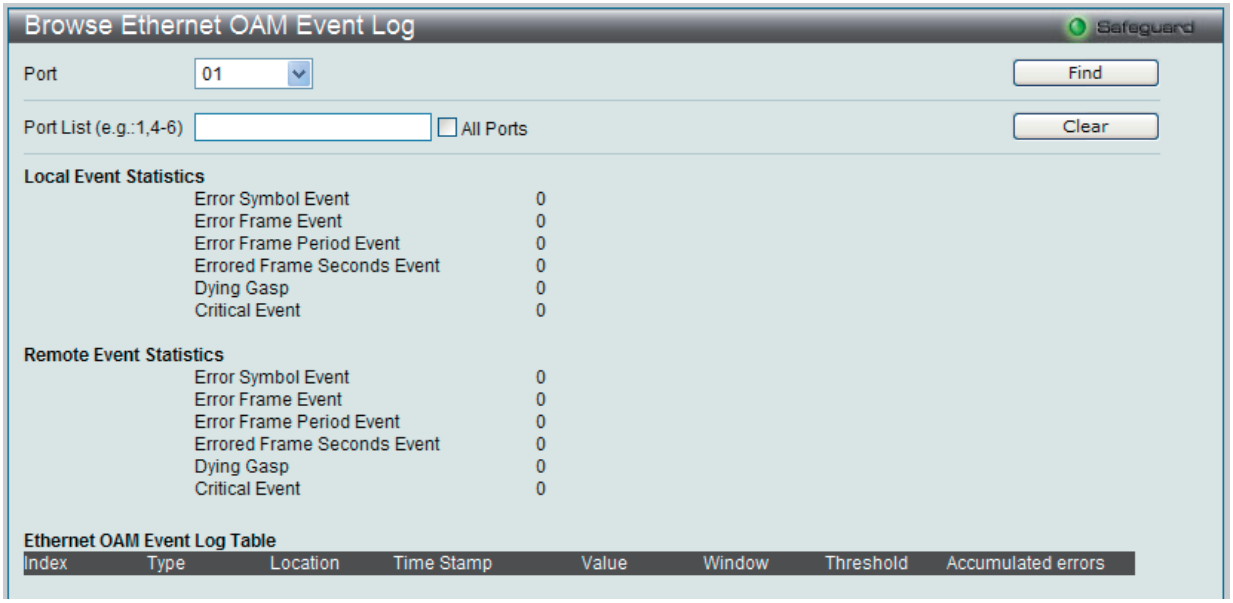


図 11-35　Browse Ethernet OAM Event Log 画面

参照するポート番号またはポートリストを指定し、「Find」ボタンをクリックします。
エントリを削除するためには、適切な情報を入力して、「Clear」ボタンをクリックします。

Browse Ethernet OAM Statistics（イーサネット OAM 統計情報の参照）

本画面はスイッチの各ポートに関するイーサネット OAM 統計情報を表示します。

Monitoring > Ethernet OAM > Browse Ethernet OAM 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。

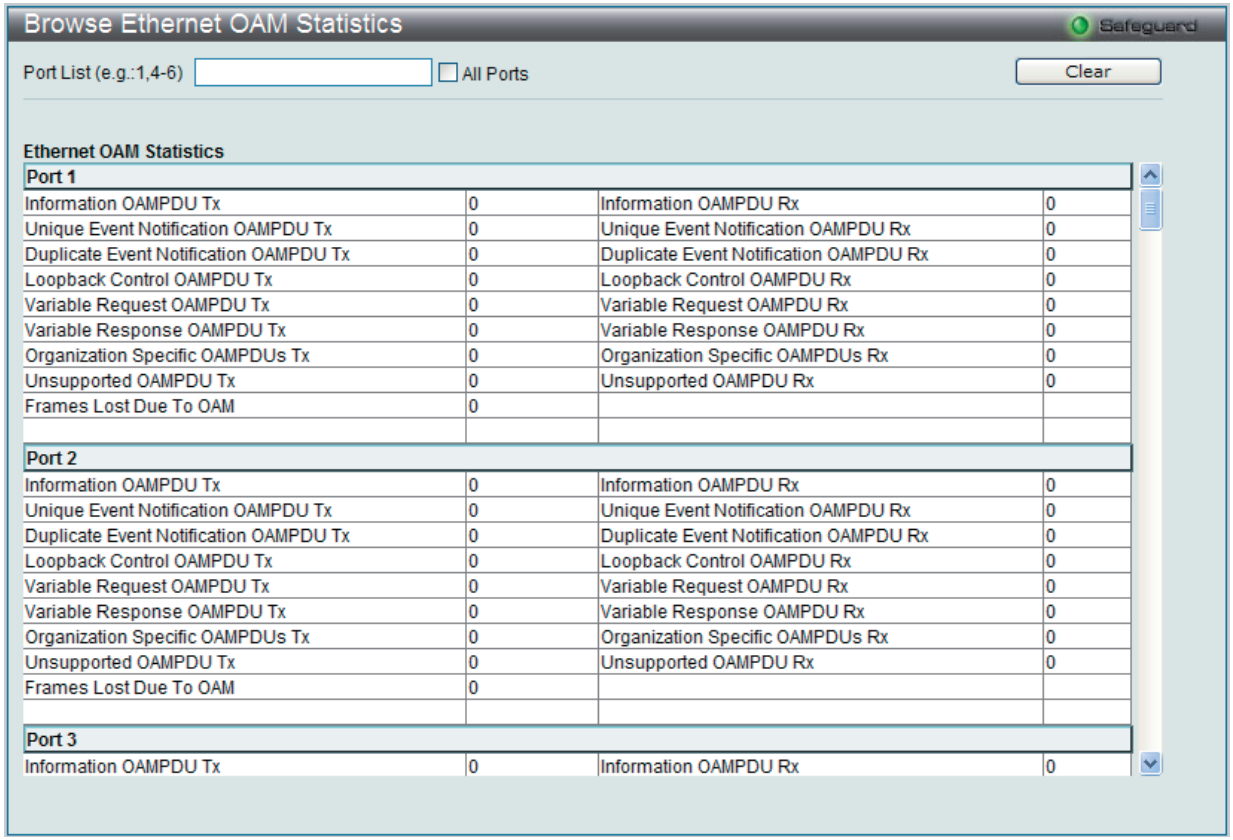


図 11-33　Browse Ethernet OAM Statistics 画面

特定のポートまたはポートリストの情報をクリアするためには、ポートを入力し、「Clear」ボタンをクリックします。

CFM（Connectivity Fault Management : 接続性障害管理）

CFM Fault Table（CFM 障害テーブル）

スイッチの MEP によって検出された障害状態を表示します。

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

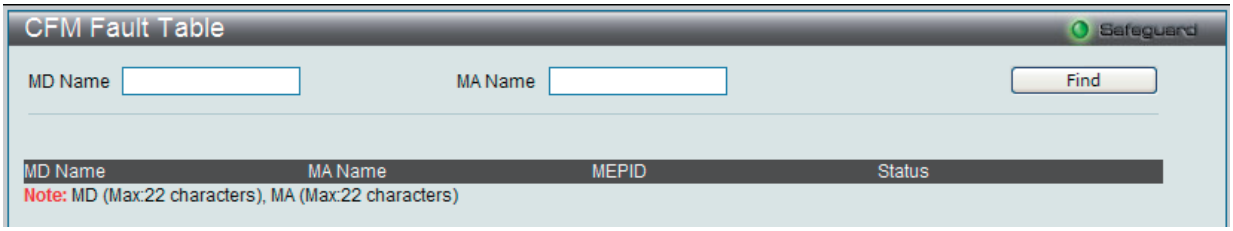


図 11-33　Browse CFM Fault MEP 画面

画面には以下の項目があります。

項目	説明
MD Name	表示するメンテナンスドメイン名を入力します。
MA Name	表示するメンテナンスアソシエーション名を入力します。

項目入力後、「Find」ボタンをクリックして、特定の MD および MA の接続障害を表示します。

CFM MIPCCM Table（CFM MIPCCM テーブル）

スイッチの CFM MIPCCM エントリを表示します。

Monitoring > CFM > CFM MIPCCM 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。

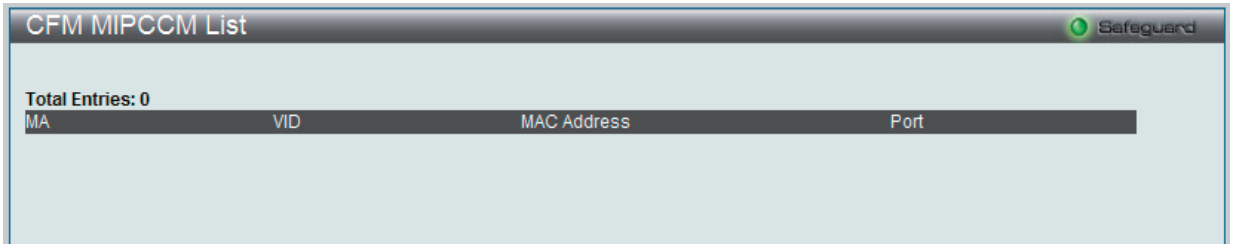


図 11-34　CFM MIPCCM Table 画面

CFM MP Table（CFM MP テーブル）

スイッチの CFM ポート MP リストを参照します。

Monitoring > CFM > CFM MP 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。

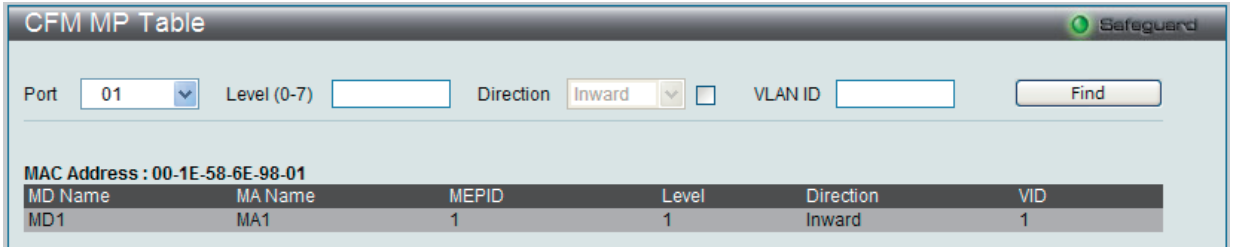


図 11-35　Browse CFM Port MP List 画面

画面には以下の項目があります。

項目	説明
Port	以下の MAC アドレスに対応するポート。
Level (0-7)	参照するエントリの MD レベル。
Direction	MEP の方向。 • Inward - 内向き MEP を示します。 • Outward - 外向き MEP を示します。
VLAN ID	参照するエントリの VLAN 識別子。

項目入力後、「Find」ボタンをクリックして、エントリをテーブルに表示します。

CFM Packet Counter（CFM パケットカウンタ）

スイッチの CFM パケットの送受信カウンタを表示します。

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

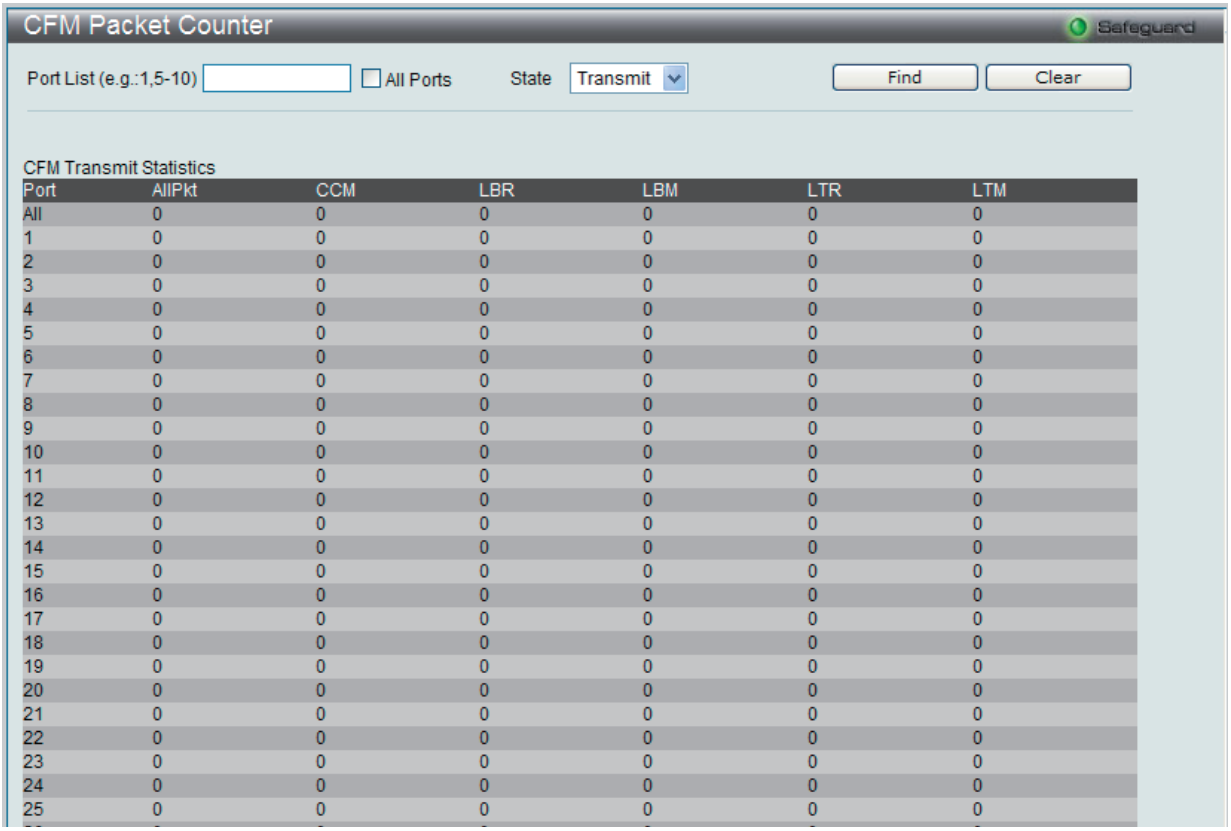


図 11-36　CFM Packet Counter List 画面

画面には以下の項目があります。

項目	説明
Port List	参照するポートを選択します。ポートを指定しない場合、すべてのポートの情報を表示します。
Type	• Receive - 受信したすべての CFM パケットを表示します。 • Transmit - 送信したすべての CFM パケットを表示します。 • CCM - 送受信したすべての CFM パケットを表示します。

参照するポート番号を入力し、「Find」ボタンをクリックします。

Mac-based Access Control Authentication State（MACベースアクセスコントロール認証ステートの参照）

MAC ベースのアクセスコントロール認証情報を参照することができます。

Monitoring > Mac-based Access Control Authentication State の順にメニューをクリックし、以下の画面を表示します :

図 11-37　Mac-based Access Control Authentication State 画面

ポートリストを検索するために、「Find」ボタンをクリックします。
エントリを削除するためには、正しい情報を入力し、「Clear By Port」ボタンをクリックします。
「View All Hosts」ボタンをクリックすると、すべてのエントリを参照します。
「Clear All Hosts」ボタンをクリックすると、すべてのアクセスプロファイルを削除します。

Browse Session Table（セッションテーブルの参照）

スイッチが最後に起動してからの管理セッションを表示します。

Monitoring > Browse Session Table メニューをクリックし、「Browse Session Table」画面を表示します。

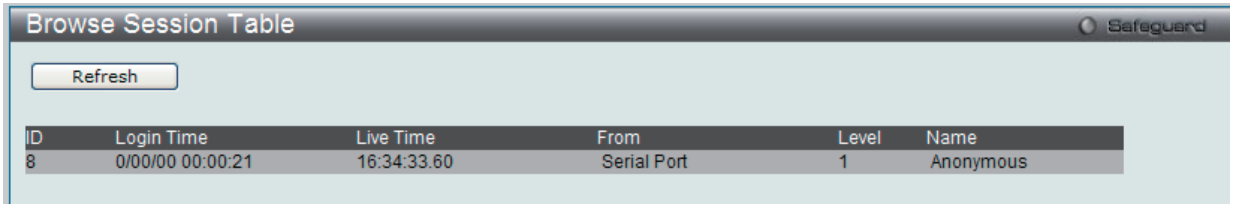


図 11-38　Browse Session Table 画面

MAC Address Table（MAC アドレステーブル）

スイッチのダイナミック MAC アドレスフォワーディングテーブルの表示を行います。スイッチは、MAC アドレスとポート番号の関連性を学習すると、フォワーディングテーブルにエントリとして登録します。それらのエントリは、スイッチ経由でパケットを転送するために使用されます。

Monitoring > 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。

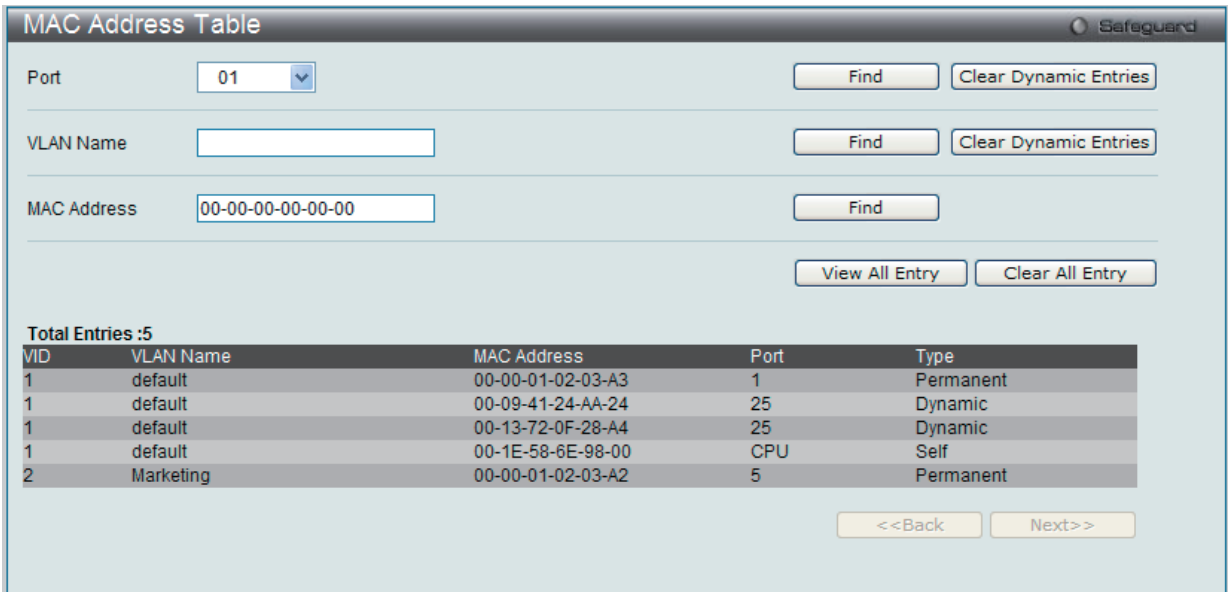


図 11-39　MAC Address Table 画面

以下の項目を使用して、設定および表示を行います。

項目	説明
Port	MAC アドレスと関連付けられるポート。
VLAN Name	フォワーディングテーブル内の検索のキーとする VLAN 名。
MAC Address	フォワーディングテーブル内の検索のキーとする MAC アドレス。
Find	指定したポート、VLAN または MAC アドレスをキーとして検索をする際にクリックします。
Clear Dynamic Entries	アドレステーブルのすべてのダイナミックエントリを削除します。
View All Entry	アドレステーブルのすべてのエントリを表示します。
Clear All Entry	アドレステーブルのすべてのエントリを削除します。

System Log（システムログ）

Web マネージャでは、スイッチの管理エージェントでまとめたスイッチのヒストリログを表示します。

Monitoring > System Log の順にメニューをクリックし、ヒストリログの表示を行います。

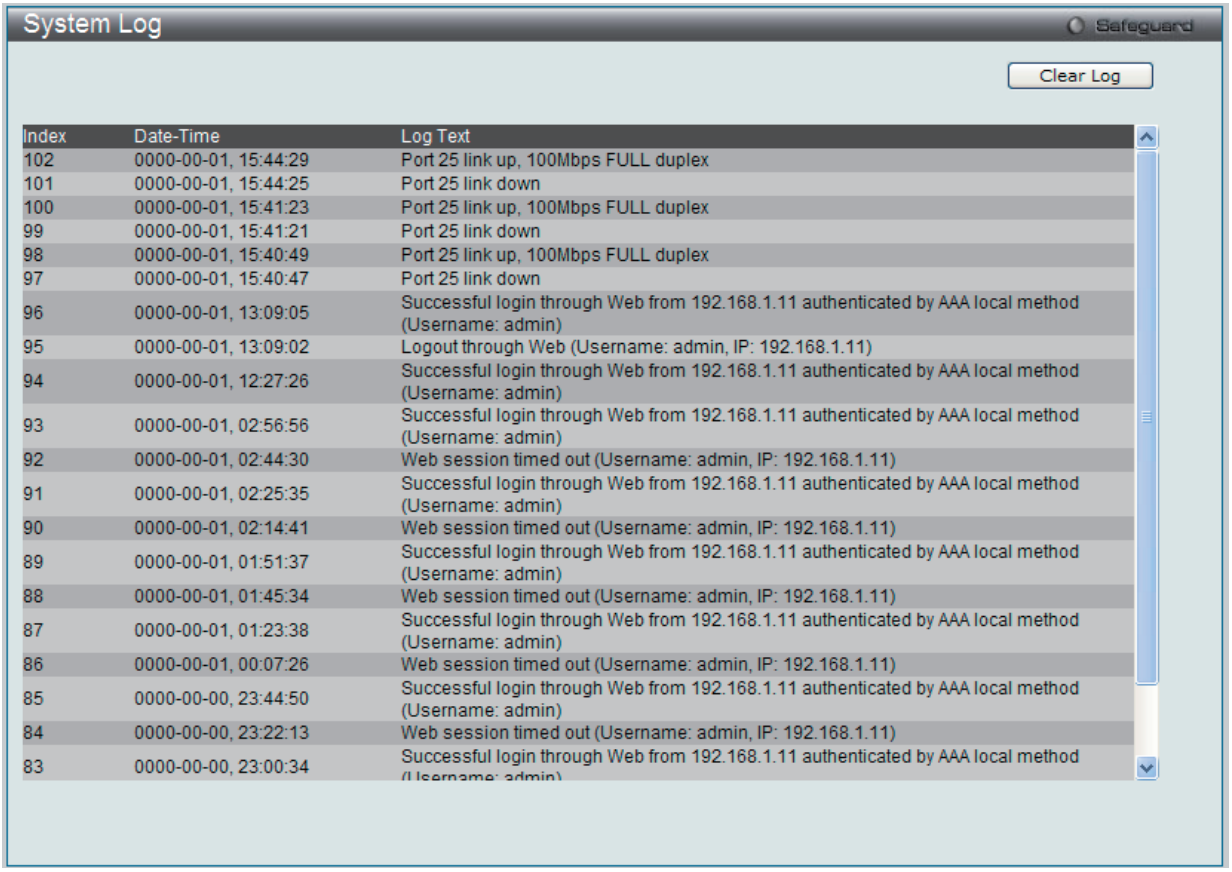


図 11-40　System Log 画面

スイッチはイベント情報を、自身のログおよび指定した SNMP トラップ受信ステーションやコンソールマネージャに接続した PC に記録することができます。「Clear Log」ボタンをクリックすると、ヒストリログがすべて削除されます。

以下の項目が表示されます。

項目	説明
Index	スイッチのヒストリログへのエントリが作成される時に加算されるカウンタ。最後のエントリ（最も高い数字の Sequence）を上に表示します。
Date-Time	スイッチの最後の再起動からの時間（日、時、分、秒）を表示します。
Log Text	ヒストリログエントリを発生させたイベントに関する説明を表示します。

注意 本画面中に表示されるログイベントについての詳細な情報については、本マニュアルの 270 ページの「付録 C ログイベント」を参照してください。

第 12 章　Maintenance（スイッチのメンテナンス）

メンテナンス用のメニューを使用し、本スイッチのリセットおよび再起動等を行うことができます。

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

サブメニュー	説明	参照ページ
Save（コンフィグレーションとログの保存）		
Save Configuration（Configuration の保存）	スイッチのメモリにコンフィグレーションを保存します	264 ページ
Save Log（ログの保存）	スイッチのメモリにログを保存します	265 ページ
Save All（コンフィグレーションとログの保存）	スイッチのメモリにコンフィグレーションとログを保存します	265 ページ
Tools（ツールメニュー）		
Configuration File Upload & Download（コンフィグレーションファイルのアップロードとダウンロード）	コンフィグレーションファイルのアップロードまたはダウンロードアップを行います。	266 ページ
Upload Log File（ログファイルのアップロード）	スイッチのヒストリと攻撃ログを TFTP サーバにアップロードします。	266 ページ
Reset（リセット）	工場出荷時設定に戻し、メモリに保存します。	266 ページ
Ping Test（Ping テスト）	スイッチとネットワーク上の他のノードとの接続性を確認します。	267 ページ
Download Firmware（ファームウェアのダウンロード）	スイッチのファームウェアダウンロードを行います。	268 ページ
Reboot System（システムの再起動）	スイッチの再起動を行います。	268 ページ

Save（コンフィグレーションとログの保存）

「Save」メニューには、次のオプションがあります。:「Save Configuration」、「Save Log」、「Save All」
それぞれが、スイッチのメモリにコンフィグレーションを保存します。

オプションには以下のものがあります。

項目	説明
Save Configuration	イメージファイルとして現在のコンフィグレーションファイルを保存します。
Save Log	現在のログのみを保存します。
Save All	イメージファイルとして現在のコンフィグレーションファイルを、また現在のログファイルを保存します。

Save Configuration（Configuration の保存）

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

図 12-1　Save Configuration 画面

Save Log（ログの保存）

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

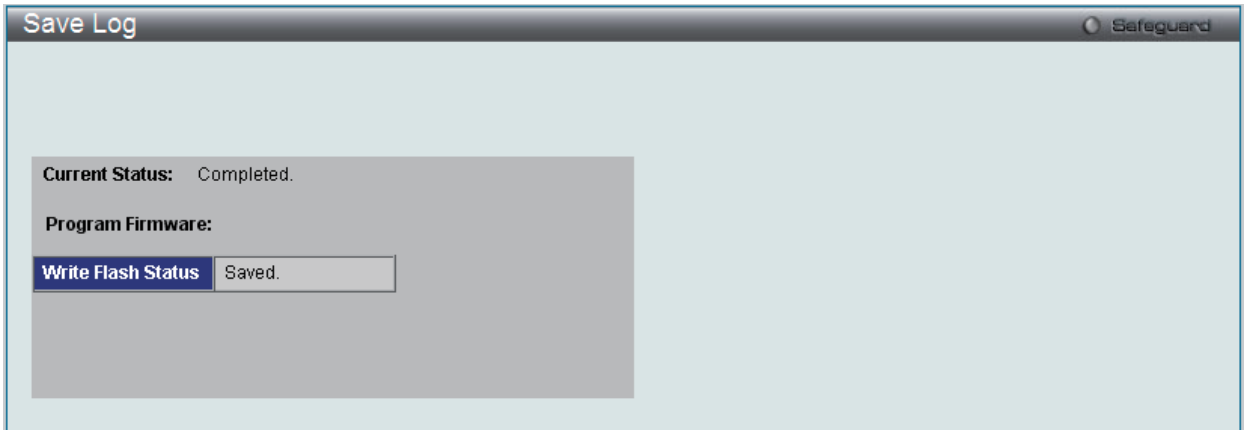


図 12-3　Save Log 画面

Save All（コンフィグレーションファイルとログの保存）

Web マネージャの先頭の **Save** > **Save All** をクリックし、以下の画面を表示します。

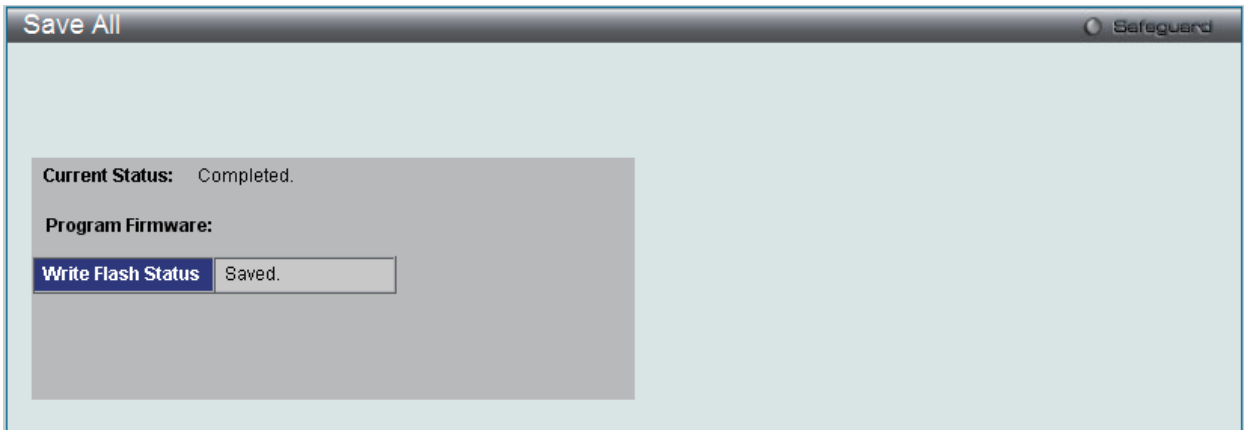


図 12-4　Save All 画面

Tools（ツールメニュー）

「Tools」メニューには、次のオプションがあります。:
「Configuration File Upload & Download」、「Upload Log File」、「Reset」、「Ping Test」、「Download Firmware」および「Reboot System」

Configuration File Upload & Download（コンフィグレーションファイルのアップロードとダウンロード）

コンフィグレーションファイルのアップロードまたはダウンロードアップを行います。

Tools > Configuration File Upload & Download をクリックし、以下の画面を表示します。

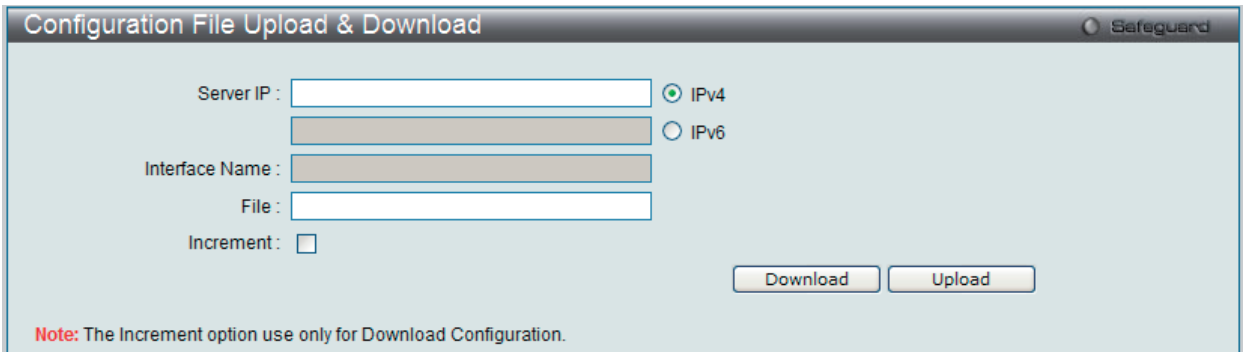


図 12-5　Configuration File Upload & Download 画面

「IPv4」を選択した場合には、「Server IP」にサーバの IP アドレス、「File」にファイル名とパスを指定します。「IPv6」を選択した場合には、「Server IP」にサーバの IP アドレス、「Interface Name」にインタフェース名、「File」にファイル名とパスを指定します。「Download」または「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。

Upload Log File（ログファイルのアップロード）

スイッチのヒストリをサーバにアップロードします。

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

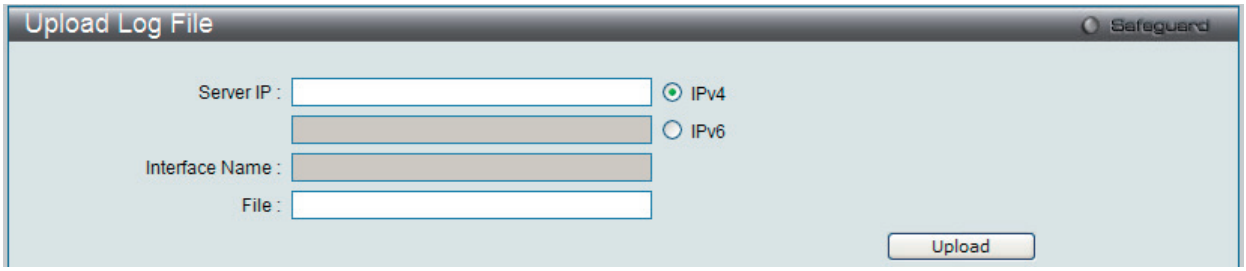


図 12-6　Upload Log File 画面

ログファイルをアップロードするためには、サーバの IP アドレスを入力します。「IPv4」を選択した場合には、「File」にログのパスとファイル名を入力します。「IPv6」を選択した場合には、「Interface Name」にインタフェース名、「File」にログのパスとファイル名を入力します。「Upload」ボタンをクリックします。

Reset（リセット）

スイッチのリセット機能にはいくつかのオプションがあります。現在のコンフィグレーション項目のいくつかを保持したままで、他のすべての設定内容を工場出荷時状態に戻すことが可能です。

Tools > Reset の順にクリックし、以下の画面を表示します。

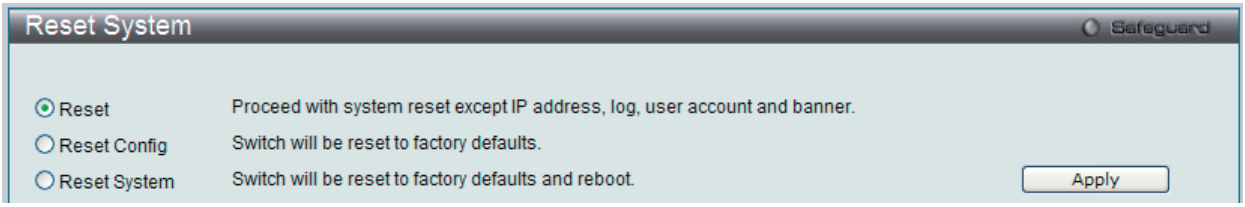


図 12-7　Reset System 画面

項目	説明
Reset	IP アドレス、ログ、ユーザアカウント、ログヒストリ、およびバナーを除くすべての設定が工場出荷時の初期設定に戻りますが、NV-RAM には書き込みません。本画面を使用してスイッチのリセットを行っても「Save Changes」を実行しなければ、リブート時には最後に保存されたコンフィグレーションに戻ります。
Reset Config	すべての設定が工場出荷時の初期設定に戻りますが、NV-RAM には書き込みません。本画面を使用してスイッチのリセットを行っても「Save Changes」を実行しなければ、リブート時には最後に保存されたコンフィグレーションに戻ります。
Reset System	すべての設定やエントリが工場出荷時の初期設定に戻し、その初期設定を NV-RAM に保存して再起動します。

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。

Ping Test（Ping テスト）

IPv4 アドレスまたは IPv6 アドレスに Ping することができます。

Ping とは、指定したアドレスに ICMP Echo パケットを送信する簡単なプログラムです。送信先のノードは、送信元のスイッチに応答を返すか、送信されたパケットをエコーバックします。本機能はスイッチとネットワーク上の他のノードとの接続性を確認するために使用します。

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

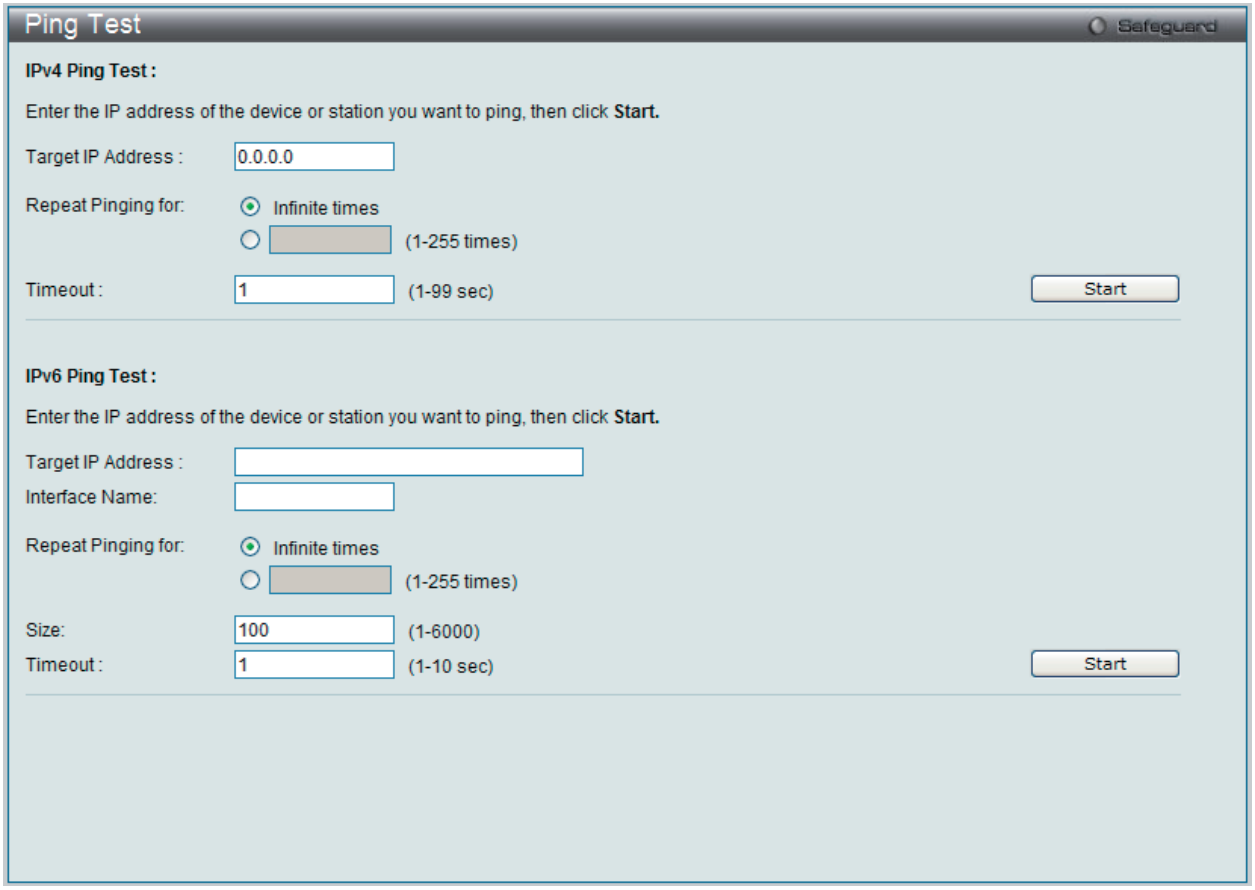


図 6-33　Ping Test 画面

「Repeat Pinging for」で「Infinite times」を選択すると、「Target IP Address」に指定した IP アドレス宛てに、ICMP Echo パケットをプログラムが停止するまで送信し続けます。または、「Repeat Pinging for」で 1-255 までの数字を指定して、送信回数を指定することもできます。

以下の項目を使用して設定、表示を行います。

項目	説明
Target IP Address	Ping する IP アドレスを入力します。
Interface Name	IPv6 の場合、Ping するインタフェース名を入力します。
Repeat Pinging for	送信先 IPv4 アドレスまたは IPv6 アドレスに Ping する回数（1-255）を指定します。 「Infinite times」を選択すると、ICMP Echo パケットをプログラムが停止するまで送信し続けます。
Size	IPv6 の場合、1-6000 の値を入力します。初期値は 100 です。
Timeout	IPv4 では、送信先への Ping メッセージの応答待ち時間 1-99（秒）で入力します。 IPv6 では、送信先への Ping メッセージの応答待ち時間 1-10（秒）で入力します。 いずれの場合もこの時間内に応答パケットの検出に失敗すると、Ping パケットを破棄します。

「Start」ボタンをクリックし、Ping プログラムを開始します。

Download Firmware（ファームウェアのダウンロード）

スイッチのファームウェアダウンロードを行います。

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

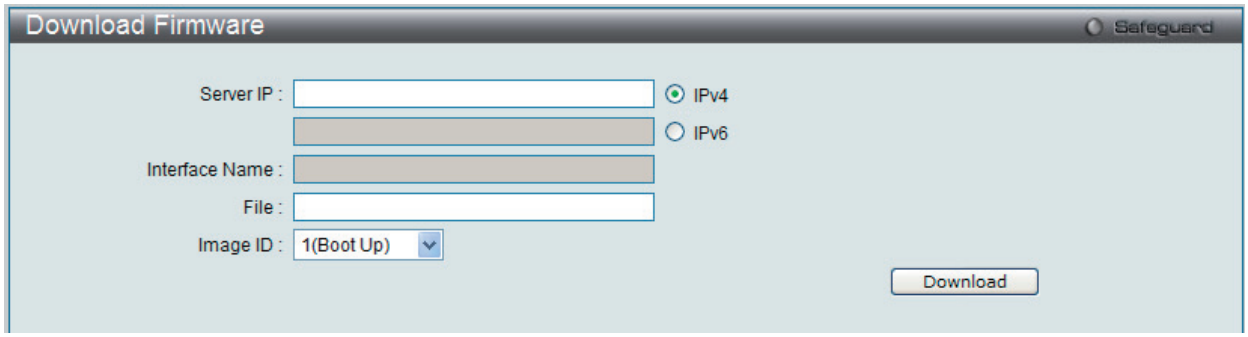


図 12-8　Download Firmware 画面

ファームウェアイメージは ID1 または 2 で示されます。「Server IP」にサーバの IP アドレス、「File」にファームウェアのファイル名とパスを入力します。次に「IPv4」または「IPv6」を選択して、「Image ID」では「Active」、「1」または「2」から選択します。「Download」ボタンをクリックし、ファイル転送を開始します。

以下のようなインジケータ画面が表示されます。

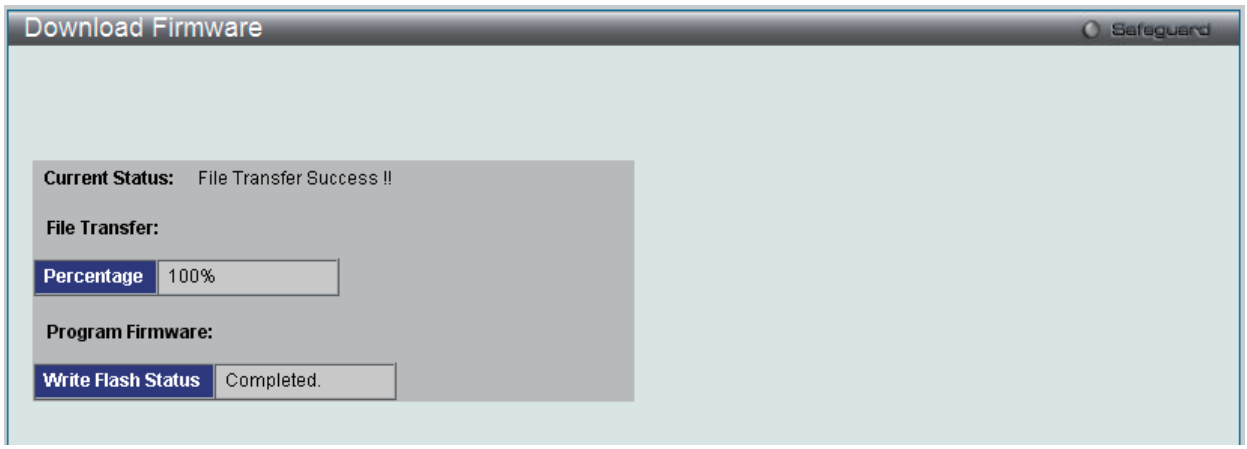


図 12-9　Download Firmware 画面

「Image ID」に「Active」を指定した場合は、ダウンロード完了後に再起動します。

Reboot System（システムの再起動）

以下の画面を使用してスイッチの再起動を行います。

Tools > Reboot の順にクリックし、以下の画面を表示します。

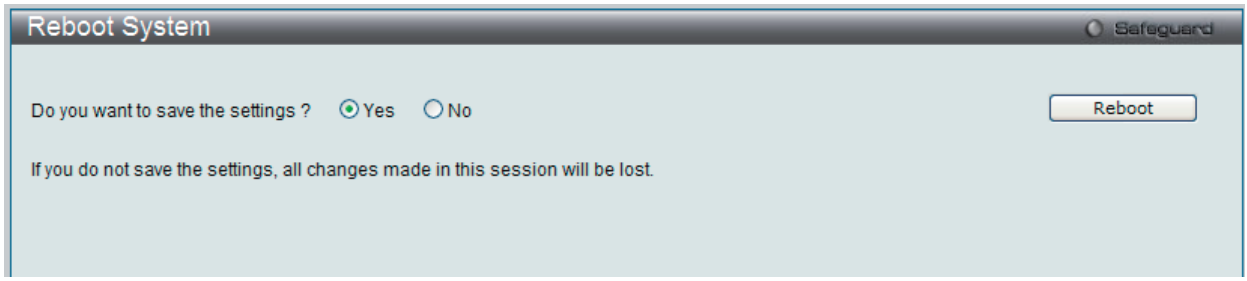


図 12-10　Reboot System 画面

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

付録 A ケーブルとコネクタ

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

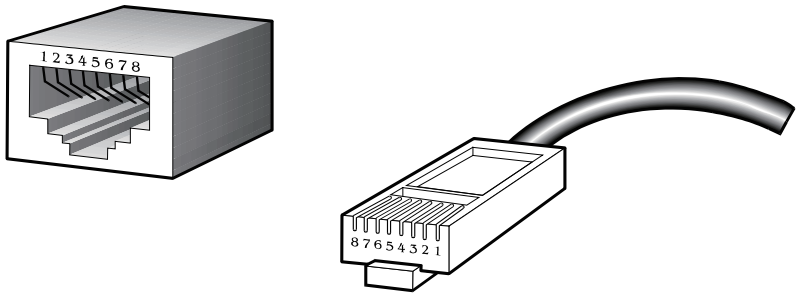


表 A-1　標準的な RJ-45 ピンアサイン

RJ-45 ピンアサイン		
コンタクト（ピン番号）	MDI-X 信号	MDI-II 信号
1	RD+（受信）	TD+（送信）
2	RD-（受信）	TD-（送信）
3	TD+（送信）	RD+（受信）
4	1000BASE-T	1000BASE-T
5	1000BASE-T	1000BASE-T
6	TD-（送信）	RD-（受信）
7	1000BASE-T	1000BASE-T
8	1000BASE-T	1000BASE-T

付録 B ケーブル長

以下の表は各規格に対応するケーブル長 (最大) です。

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

付録 C ログイベント

スイッチのシステムログに表示される可能性のあるログイベントとそれらの意味を以下に示します。

Critical（重大）、Warning（警告）、Informational（報告）

カテゴリ	ログの内容	緊急度	イベントの説明
システム	System warm start	Critical	システムのウォームスタート
	System cold start	Critical	システムのコールドスタート
	Configuration saved to flash (Username: < ユーザ名 >, IP: <IP アドレス >)	Informational	コンフィグレーションをフラッシュメモリに保存しました。
	Configuration saved to flash by console (Username: < ユーザ名 >)	Informational	コンソールでコンフィグレーションをフラッシュメモリに保存しました。
	System log saved to flash (Username: < ユーザ名 > IP: <IP アドレス >)	Informational	システムログをフラッシュメモリに保存しました。
	System log saved to flash by console (Username: < ユーザ名 >)	Informational	コンソールでシステムログをフラッシュメモリに保存しました。
	Configuration and log saved to flash(Username: < ユーザ名 > IP: <IP アドレス >)	Informational	コンフィグレーションとシステムログをフラッシュメモリに保存しました。
	Configuration and log saved to flash by console(Username: < ユーザ名 >)	Informational	コンソールでコンフィグレーションとシステムログをフラッシュメモリに保存しました。
アップロード / ダウンロード	Firmware upgraded successfully (Username: < ユーザ名 >, IP: <IP アドレス >)	Informational	ファームウェアの更新成功。
	Firmware upgraded by console successfully (Username: < ユーザ名 >)	Informational	コンソールによるファームウェアの更新成功。
	Firmware upgrade was unsuccessful! (Username: < ユーザ名 >, IP: <IP アドレス >)	Warning	ファームウェアの更新失敗。
	Firmware upgrade by console was unsuccessful! (Username: < ユーザ名 >)	Warning	コンソールによるファームウェアの更新失敗。
	Configuration successfully downloaded (Username: < ユーザ名 >, IP: <IP アドレス >)	Informational	コンフィグレーションファイルのダウンロード成功。
	Configuration successfully downloaded by console (Username: < ユーザ名 >)	Informational	コンソールによるコンフィグレーションファイルのダウンロード成功。
	Configuration download was unsuccessful! (Username: < ユーザ名 >, IP: <IP アドレス >)	Warning	コンフィグレーションファイルのダウンロード失敗。
	Configuration download by console was unsuccessful! (Username: < ユーザ名 >)	Warning	コンソールによるコンフィグレーションファイルのダウンロード失敗。
	Configuration successfully uploaded (Username: < ユーザ名 >, IP: <IP アドレス >)	Informational	コンフィグレーションファイルのアップロード成功。
	Configuration successfully uploaded by console (Username: <ユーザ名>)	Informational	コンソールによるコンフィグレーションファイルのアップロード成功。
	Configuration upload was unsuccessful! (Username: < ユーザ名 >, IP: <IP アドレス >)	Warning	コンフィグレーションファイルのアップロード失敗。
	Configuration upload by console was unsuccessful! (Username: <ユーザ名 >)	Warning	コンソールによるコンフィグレーションファイルのアップロード失敗。
	Log message successfully uploaded (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。
	Log message successfully uploaded by console (Username: < ユーザ名 >)	Informational	コンソールによるログメッセージのアップロード成功。
	Log message upload was unsuccessful! (Username: < ユーザ名 >, IP: <IP アドレス >)	Warning	ログメッセージのアップロード失敗。
	Log message upload by console was unsuccessful! (Username: < ユーザ名 >)	Warning	コンソールによるログメッセージのアップロード失敗。
インタフェース	Port < ポート番号 > link up, < リンク状態 >	Informational	ポートリンクアップ
	Port < ポート番号 > link down	Informational	ポートリンクダウン
コンソール	Successful login through Console (Username: < ユーザ名 >)	Informational	コンソール経由のログイン成功
	Login failed through Console (Username: < ユーザ名 >)	Warning	コンソール経由のログイン失敗
	Logout through Console (Username: < ユーザ名 >)	Informational	コンソール経由でログアウト
	Console session timed out (Username: < ユーザ名 >)	Informational	コンソールセッション、タイムアウト

カテゴリ	ログの内容	緊急度	イベントの説明
Web	Successful login through Web (Username: <ユーザ名>, IP: <IPアドレス>)	Informational	Web 経由のログイン成功
	Login failed through Web (Username: <ユーザ名>, IP: <IPアドレス>)	Warning	Web 経由のログイン失敗
	Logout through Web (Username: < ユーザ名 >, IP: <IP アドレス >)	Informational	Web 経由でログアウト
	Web session timed out (Username: < ユーザ名 >, IP:<ipaddr>)	Informational	Web セッションタイムアウト
Web (SSL)	Successful login through Web (SSL) (Username:< ユーザ名 >, IP: <IP アドレス >)	Informational	Web (SSL) 経由のログイン成功
	Login failed through Web (SSL) (Username: < ユーザ名 >,IP: <IP アドレス >)	Warning	Web (SSL) 経由のログイン失敗
	Login failed through Web (SSL) due to AAA server timeout or improper configuration	Informational	AAA サーバのタイムアウトまたは不適切なコンフィグレーションによる Web (SSL) 経由のログイン失敗
	Logout through Web (SSL) (Username: <ユーザ名>, IP:<IPアドレス>)	Informational	Web (SSL) 経由でログアウト
	Web (SSL) session timed out (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
Telnet	Successful login through Telnet (Username: < ユーザ名 >, IP: <IP アドレス >)	Informational	Telnet 経由のログイン成功
	Login failed through Telnet (Username: < ユーザ名 >, IP: <IP アドレス >)	Warning	Telnet 経由のログイン失敗
	Logout through Telnet (Username: < ユーザ名 >, IP: <IP アドレス >)	Informational	Telnet 経由でログアウト
	Telnet session timed out (Username: < ユーザ名 >, IP: <IP アドレス >)	Informational	Telnet セッションタイムアウト
SNMP	SNMP request received from < IP アドレス > with invalid community string !	Informational	無効なコミュニティ名を含む SNMP request 受信
STP	Topology changed (Instance:< インスタンス ID> port< ポート番号 >)	Informational	トポロジ変更
	[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	新規ルートを選択
	Spanning Tree Protocol is enabled	Informational	スパニングツリープロトコル有効化
	Spanning Tree Protocol is disabled	Informational	スパニングツリープロトコル無効化
	Port < ポート番号 > STP root restriction is enabled	Informational	ルート制限の有効化
	Port < ポート番号 > STP root restriction is Disabled	Informational	ルート制限の無効化
SSH	Successful login through SSH (Username: <ユーザ名>, IP: <IPアドレス>)	Informational	SSH 経由のログイン成功
	Login failed through SSH (Username: < ユーザ名 >, IP: <IP アドレス >)	Warning	SSH 経由のログイン失敗
	Logout through SSH (Username: < ユーザ名 >, IP: <IP アドレス >)	Informational	SSH 経由のログアウト
	SSH session timed out (Username: < ユーザ名 >, IP: <IP アドレス >)	Informational	SSH セッションタイムアウト
	SSH server is enabled	Informational	SSH サーバ有効化
	SSH server is disabled	Informational	SSH サーバ無効化
AAA	Authentication Policy is enabled (Module: AAA)	Informational	認証ポリシー有効化
	Authentication Policy is disabled (Module: AAA)	Informational	認証ポリシー無効化
	Successful login through Console authenticated by AAA local method (Username: < ユーザ名 >)	Informational	AAA ローカルメソッドによるコンソール経由のログイン認証成功
	Login failed through Console authenticated by AAA local method (Username: < ユーザ名 >)	Warning	AAA ローカルメソッドによるコンソール経由のログイン認証失敗
	Successful login through Web from < ユーザ IP> authenticated by AAA local method (Username: < ユーザ名 >)	Informational	AAA ローカルメソッドによる Web 経由のログイン認証成功
	Login failed through Web from < ユーザ IP> authenticated by AAA local method (Username: < ユーザ名 >)	Warning	AAA ローカルメソッドによる Web 経由のログイン認証失敗
	Successful login through Web(SSL) from < ユーザ IP> authenticated by AAA local method (Username: < ユーザ名 >)	Informational	AAA ローカルメソッドによる Web (SSL) 経由のログイン認証成功
	Login failed through Web(SSL) from < ユーザ IP> authenticated by AAA local method (Username: < ユーザ名 >)	Warning	AAA ローカルメソッドによる Web (SSL) 経由のログイン認証失敗
	Successful login through Telnet from < ユーザ IP> authenticated by AAA local method (Username: < ユーザ名 >)	Informational	AAA ローカルメソッドによる Telnet 経由のログイン認証成功
	Login failed through Telnet from < ユーザ IP> authenticated by AAA local method (Username: < ユーザ名 >)	Warning	AAA ローカルメソッドによる Telnet 経由のログイン認証失敗
	Successful login through SSH from < ユーザ IP> authenticated by AAA local method (Username: < ユーザ名 >)	Informational	AAA ローカルメソッドによる SSH 経由のログイン認証成功
	Login failed through SSH from < ユーザ IP> authenticated by AAA local method (Username: < ユーザ名 >)	Warning	AAA ローカルメソッドによる SSH 経由のログイン認証失敗

カテゴリ	ログの内容	緊急度	イベントの説明
AAA	Successful login through Console authenticated by AAA none method (Username: < ユーザ名 >)	Informational	AAA none メソッドによるコンソール経由のログイン認証成功
	Successful login through Web from < ユーザ IP> authenticated by AAA none method (Username: < ユーザ名 >)	Informational	AAA none メソッドによる Web 経由のログイン認証成功
	Successful login through Web(SSL) from < ユーザ IP> authenticated by AAA none method (Username: < ユーザ名 >)	Informational	AAA none メソッドによる Web (SSL) 経由のログイン認証成功
	Successful login through Telnet from < ユーザ IP> authenticated by AAA none method (Username: < ユーザ名 >)	Informational	AAA none メソッドによる Telnet 経由のログイン認証成功
	Successful login through SSH from < ユーザ IP> authenticated by AAA none method (Username: < ユーザ名 >)	Informational	AAA none メソッドによる SSH 経由のログイン認証成功
	Successful login through Console authenticated by AAA server< サーバ IP> (Username: < ユーザ名 >)	Informational	AAA サーバによるコンソール経由のログイン認証成功
	Login failed through Console authenticated by AAA server< サーバ IP> (Username: < ユーザ名 >)	Warning	AAA サーバによるコンソール経由のログイン認証失敗
	Login failed through Console due to AAA server timeout or improper configuration (Username: < ユーザ名 >)	Warning	AAA サーバタイムアウトまたは不正な設定による コンソール経由のログイン認証失敗
	Successful login through Web from < ユーザ IP> authenticated by AAA server< サーバ IP> (Username: < ユーザ名 >)	Informational	AAA サーバによる Web 経由のログイン認証成功
	Login failed through Web from < ユーザ IP> authenticated by AAA server< サーバ IP> (Username: < ユーザ名 >)	Warning	AAA サーバによる Web 経由のログイン認証失敗
	Login failed through Web from < ユーザ IP> due to AAA server timeout or improper configuration (Username: < ユーザ名 >)	Warning	AAA サーバタイムアウトまたは不正な設定による Web 経由の Admin レベル遷移失敗
	Successful login through Web(SSL) from < ユーザ IP> authenticated by AAA server< サーバ IP> (Username: < ユーザ名 >)	Informational	AAA サーバによる Web (SSL) 経由のログイン認証成功
	Login failed through Web(SSL) from < ユーザ IP> authenticated by AAA server< サーバ IP> (Username: < ユーザ名 >)	Warning	AAA サーバによる Web (SSL) 経由のログイン認証失敗
	Login failed through Web(SSL) from < ユーザ IP> due to AAA server timeout or improper configuration (Username: < ユーザ名 >)	Warning	AAA サーバタイムアウトまたは不正な設定による Web (SSL) 経由のログイン認証失敗
	Successful login through Telnet from < ユーザ IP> authenticated by AAA server< サーバ IP> (Username: < ユーザ名 >)	Informational	AAA サーバによる Telnet 経由のログイン認証成功
	Login failed through Telnet from < ユーザ IP> authenticated by AAA server< サーバ IP> (Username: < ユーザ名 >)	Warning	AAA サーバによる Telnet 経由のログイン認証失敗
	Login failed through Telnet from < ユーザ IP> due to AAA server timeout or improper configuration (Username: < ユーザ名 >)	Warning	AAA サーバタイムアウトまたは不正な設定による Telnet 経由のログイン失敗
	Successful login through SSH from < ユーザ IP> authenticated by AAA server< サーバ IP> (Username: < ユーザ名 >)	Informational	AAA サーバによる SSH 経由のログイン認証成功
	Login failed through SSH from < ユーザ IP> authenticated by AAA server< サーバ IP> (Username: < ユーザ名 >)	Warning	AAA サーバによる SSH 経由のログイン認証失敗
	Login failed through SSH from < ユーザ IP> due to AAA server timeout or improper configuration (Username: < ユーザ名 >)	Warning	AAA サーバタイムアウトまたは不正な設定による SSH 経由のログイン失敗
	Successful Enable Admin through Console authenticated by AAA local_enable method (Username: < ユーザ名 >)	Informational	AAA local_enable メソッドによるコンソール経由の Admin レベル遷移成功
	Enable Admin failed through Console authenticated by AAA local_enable method (Username: < ユーザ名 >)	Warning	AAA local_enable メソッドによるコンソール経由の Admin レベル遷移失敗
	Successful Enable Admin through Web from < ユーザ IP> authenticated by AAA local_enable method (Username: < ユーザ名 >)	Informational	AAA local_enable メソッドによる Web 経由の Admin レベル遷移成功
	Enable Admin failed through Web from < ユーザ IP> authenticated by AAA local_enable method (Username: < ユーザ名 >)	Warning	AAA local_enable メソッドによる Web 経由の Admin レベル遷移失敗
	Successful Enable Admin through Web(SSL) from < ユ ー ザ IP> authenticated by AAA local_enable method (Username: < ユーザ名 >)	Informational	AAA local_enable メソッドによる Web(SSL) 経由の Admin レベル遷移成功
	Enable Admin failed through Web(SSL) from < ユーザ IP> authenticated by AAA local_enable method (Username: < ユーザ名 >)	Warning	AAA local_enable メソッドによる Web(SSL) 経由の Admin レベル遷移失敗
	Successful Enable Admin through Telnet from < ユーザ IP> authenticated by AAA local_enable method (Username: < ユーザ名 >)	Informational	AAA local_enable メソッドによる Telnet 経由の Admin レベル遷移成功
	Enable Admin failed through Telnet from < ユーザ IP> authenticated by AAA local_enable method (Username: < ユーザ名 >)	Warning	AAA local_enable メソッドによる Telnet 経由の Admin レベル遷移失敗

カテゴリ	ログの内容	緊急度	イベントの説明
AAA	Successful Enable Admin through SSH from <ユーザ IP> authenticated by AAA local_enable method (Username: < ユーザ名 >)	Informational	AAA local_enable メソッドによる SSH 経由の Admin レベル遷移成功
	Enable Admin failed through SSH from < ユーザ IP> authenticated by AAA local_enable method (Username: < ユーザ名 >)	Warning	AAA local_enable メソッドによる SSH 経由の Admin レベル遷移失敗
	Successful Enable Admin through Console authenticated by AAA none method (Username: < ユーザ名 >)	Informational	AAA none メソッドによるコンソール経由の Admin レベル遷移成功
	Successful Enable Admin through Web from < ユーザ IP> authenticated by AAA none method (Username: < ユーザ名 >)	Informational	AAA none メソッドによる Web 経由の Admin レベル遷移成功
	Successful Enable Admin through Web(SSL) from < ユーザ IP> authenticated by AAA none method (Username: < ユーザ名 >)	Informational	AAA none メソッドによる Web(SSL) 経由の Admin レベル遷移成功
	Successful Enable Admin through Telnet from < ユーザ IP> authenticated by AAA none method (Username: < ユーザ名 >)	Informational	AAA none メソッドによる Telnet 経由の Admin レベル遷移成功
	Successful Enable Admin through SSH from < ユーザ IP> authenticated by AAA none method (Username: < ユーザ名 >)	Informational	AAA none メソッドによる SSH 経由の Admin レベル遷移成功
	Successful Enable Admin through Console authenticated by AAA server < サーバ IP> (Username: < ユーザ名 >)	Informational	AAA サーバによるコンソール経由の Admin レベル遷移成功
	Enable Admin failed through Console authenticated by AAA server < サーバ IP> (Username: < ユーザ名 >)	Warning	AAA サーバによるコンソール経由の Admin レベル遷移失敗
	Enable Admin failed through Console due to AAA server timeout or improper configuration (Username: < ユーザ名 >)	Warning	AAA サーバタイムアウトまたは不正な設定によるコンソール経由の Admin レベル遷移失敗
	Successful Enable Admin through Web from < ユーザ IP> authenticated by AAA server < サーバ IP> (Username: < ユーザ名 >)	Informational	AAA サーバによる Web 経由の Admin レベル遷移成功
	Enable Admin failed through Web from < ユーザ IP> authenticated by AAA server < サーバ IP> (Username: < ユーザ名 >)	Warning	AAA サーバによる Web 経由の Admin レベル遷移失敗
	Successful Enable Admin through Web(SSL) from < ユーザ IP> authenticated by AAA server < サーバ IP> (Username: < ユーザ名 >)	Informational	AAA サーバによる Web(SSL) 経由の Admin レベル遷移成功
	Enable Admin failed through Web(SSL) from < ユーザ IP> authenticated by AAA server < サーバ IP> (Username: < ユーザ名 >)	Warning	AAA サーバによる Web(SSL) 経由の Admin レベル遷移失敗
	Successful Enable Admin through Telnet from < ユ ー ザ IP> authenticated by AAA server < サーバ IP> (Username: < ユーザ名 >)	Informational	AAA サーバによる Telnet 経由の Admin レベル遷移成功
	Enable Admin failed through Telnet from < ユーザ IP> authenticated by AAA server < サーバ IP> (Username: < ユーザ名 >)	Warning	AAA サーバによる Telnet 経由の Admin レベル遷移失敗
	Enable Admin failed through Telnet from < ユーザ IP> due to AAA server timeout or improper configuration (Username: < ユーザ名 >)	Warning	AAA サーバタイムアウトまたは不正な設定による Telnet 経由の Admin レベル遷移失敗
	Successful Enable Admin through SSH from < ユーザ IP> authenticated by AAA server < サーバ IP> (Username: < ユーザ名 >)	Informational	AAA サーバによる SSH 経由の Admin レベル遷移成功
	Enable Admin failed through SSH from < ユーザ IP> authenticated by AAA server < サーバ IP> (Username: < ユーザ名 >)	Warning	AAA サーバによる SSH 経由の Admin レベル遷移失敗
	Enable Admin failed through SSH from < ユーザ IP> due to AAA server timeout or improper configuration (Username: < ユーザ名 >)	Warning	AAA サーバタイムアウトまたは不正な設定による SSH 経由の Admin レベル遷移失敗
	AAA server < サーバ IP> (Protocol: < プロトコル名 >) response is wrong	Warning	AAA サーバの応答が不正です。
	AAA doesn't support this functionality	Informational	AAA はこの機能を未サポートです。
	AAA server < サーバ IP> (Protocol: < プロトコル名 >) connection failed	Warning	AAA サーバのタイムアウト
ポートセキュリティ	Port security violation (Port: < ポート番号 >, MAC: <MAC アドレス >)	Warning	ポートセキュリティは最大学習サイズを超えたため、新しいアドレスを学習できません。
IP-MAC ポートバインディング	Unauthenticated IP-MAC address and discarded by ip mac port binding (IP: <IP アドレス >, MAC: <MAC アドレス >, Port < ポート番号 >)	Warning	IP-MAC ポートバインディング機能により、非認証の IP アドレスからのパケットを廃棄しました。
	Dynamic IMPB entry is conflicting with static ARP(IP: <IP アドレス >, MAC: <MAC アドレス >, Port: <[ユニット ID:] ポート番号 >)	Informational	ダイナミック IMPB エントリが、スタティック ARP とコンフリクトしています。
	Dynamic IMPB entry is conflicting with static FDB(IP: <IP アドレス >, MAC: <MAC アドレス >, Port: <[ユニット ID:] ポート番号 >)	Informational	ダイナミック FDB エントリが、スタティック ARP とコンフリクトしています。
	Dynamic IMPB entry is conflicting with static IMPB: IP: <IP アドレス >, MAC: <MAC アドレス >, Port: <[ユニット ID:] ポート番号 >	Informational	ダイナミック IMPB エントリが、スタティック IMPB とコンフリクトしています。

カテゴリ	ログの内容	緊急度	イベントの説明
IP-MAC ポートバインディング	Creating IMPB entry failed due to no ACL rule available: IP: <IP アドレス >, MAC: <MAC アドレス >, Port: < ポート番号 >	Informational	有効な ACL ルールがないため、IMPB エントリの作成に失敗しました。
	Port < ポート番号 > enters stop IMPB learning state	Informational	ブロックされるエントリ数がポートしきい値に到達しました。
	Port < ポート番号 > recovers from IMPB stop learning state	Informational	ポートは IMPB 学習の停止状態から手動で回復しました。
IP とパスワード変更	Management IP address was changed into <IP アドレス > by (Username: < ユーザ名 >,IP:<IP アドレス >)	Informational	IP アドレスが変更されました。
	Management IP address was changed into <IP アドレス > by console (Username: < ユーザ名 >)	Informational	コンソールにより IP アドレスが変更されました。
	Username: < ユーザ名 > Password was changed by (Username: < ユーザ名 >,IP:<IP アドレス >)	Informational	パスワードが変更されました。
	Username: < ユーザ名 > Password was changed by console (Username: < ユーザ名 >)	Informational	コンソールによりパスワードが変更されました。
セーフガードエンジン	SafeGuard Engine enters NORMAL mode	Informational	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。
	Safeguard Engine enters EXHAUSTED mode	Warning	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。
パケットストーム	Port < ポート番号 > Broadcast storm is occurring	Warning	ブロードキャストストーム発生中。
	Port < ポート番号 > Broadcast storm has cleared	Informational	ブロードキャストストーム停止。
	Port < ポート番号 > Multicast storm is occurring	Warning	マルチキャストストーム発生中。
	Port < ポート番号 > Multicast storm has cleared	Informational	マルチキャストストーム停止。
	Port < ポート番号 > is currently shut down due to a packet storm	Warning	パケットストームのためにポートはシャットダウン。
Gratuitous ARP	Conflict IP was detected with this device (IP: <IP アドレス >, MAC: <MAC アドレス >, Port < ポート番号 >, Interface: <ip インタフェース名 >)	Informational	重複 IP アドレスが本デバイスに検出されました。
802.1X	Radius server < サーバ IP> assigned VID: <VLAN ID> to Port < ポート番号 > (Account: < ユーザ名 >)	Informational	RADIUS サーがポートに VID を割り当てました。
	Radius server < サーバ IP> assigned ingress bandwidth:< 帯域値 > Kbits to Port< ポート番号 > (Account:< ユーザ名 >)	Informational	RADIUS サーバがポートに Ingress 帯域 Kbits を割り当てました。
	Radius server < サーバ IP> assigned ingress bandwidth: no limit to Port < ポート番号 > (Account: < ユーザ名 >)	Informational	RADIUS サーバがポートに Ingress 帯域（制限なし）を割り当てました。
	Radius server < サーバ IP> assigned egress bandwidth:< 帯域値 > Kbits to Port < ポート番号 > (Account: < ユーザ名 >)	Informational	RADIUS サーバがポートに Egress 帯域 Kbits を割り当てました。
	Radius server < サーバ IP> assigned egress bandwidth: no limit to Port< ポート番号 > (Account: < ユーザ名 >)	Informational	RADIUS サーバがポートに Egress 帯域（制限なし）を割り当てました。
	Radius server < サーバ IP> assigned 802.1p default priority: < プライオリティ 0-7> to Port < ポート番号 > (Account:< ユーザ名 >)	Informational	RADIUS サーバがポートに 802.1p デフォルトプライオリティを割り当てました。
	802.1x Authentication failure from (Username: < ユーザ名 >, Port < ポート番号 >, MAC: <MAC アドレス >)	Warning	802.1X 認証失敗
	802.1x Authentication failure for the radius server < サーバ IP> timeout from (Username: < ユーザ名 >, Port < ポート番号 >, MAC: <MAC アドレス >)	Warning	RADIUS サーバへの 802.1X 認証失敗
	802.1x Authentication failure for the 802.1X client session timeout from (Username: < ユーザ名 >, Port < ポート番号 >, MAC: <MAC アドレス >)	Warning	802.1X クライアントセッションのタイムアウトのため 802.1X 認証失敗
	802.1x Authentication success from (Username: < ユーザ名 >, Port < ポート番号 >, MAC: <MAC アドレス >)	Informational	802.1X 認証成功
ループバック検知	Port < ポート番号 > LBD loop occurred. Port blocked	Critical	ポートにループが発生し、ポートはブロックされました。
	Port < ポート番号 > LBD port recovered. Loop detection restarted	Informational	インターバルタイム後に LBD ポートが回復し、ループ検知が再スタートしました。
	Port < ポート番号 > VID <VLAN ID> LBD loop occurred. Packet discard begun	Critical	VID を持つポートにループが発生しました。パケットの破棄が開始されました。
	Port < ポート番号 > VID <VLAN ID> LBD recovered. Loop detection restarted	Informational	VID を持つポートが回復し、ループ検知が再スタートしました。
	Loop VLAN number overflow	Informational	VLAN ループ最大番号を超過しました。

カテゴリ	ログの内容	緊急度	イベントの説明
DoS	<DoS 攻撃名 > is detected from (IP: <IP アドレス > Port: < ポート番号 >)	Critical	DoS 攻撃がブロックされました。
MAC ベースアクセスコントロール	MAC-based Access Control unauthenticated host (MAC: <MAC アドレス >, Port < ポート番号 >, VID: <VLAN ID>)	Information	ホストは認証追加に失敗しました。インの成功。
	MAC-based Access Control host login successful (MAC: <MAC アドレス >, port: < ポート番号 >, VID: <VLAN ID>)	Information	ホストは認証に成功しました。の失敗。
	MAC-based Access Control host aged out (MAC: <MAC アドレス >, port: < ポート番号 >, VID: <VLAN ID>)	Information	ホストはエージングされました。
	RADIUS server <IP アドレス > assigns < ユーザ名 > ACL failure at port < ポート番号 > (<string>)	Warning	RADIUS サーバから ACL プロファイル / ルールの割り当てに失敗しました。
OAM	OAM dying gasp event received (Port < ポート番号 >)	Warning	Dying Gasp イベント（リモート）
	Device encountered an OAM dying gasp event.	Warning	Dying Gasp イベント（ローカル）
	OAM critical event event received (Port < ポート番号 >)	Warning	クリティカルイベント（リモート）
	Device encountered an OAM critical event	Warning	クリティカルイベント（ローカル）
	Event (remote) Errored symbol period event received (Port < ポート番号 >)	Warning	エラーシンボル期間
	Errored frame event received (Port < ポート番号 >)	Warning	エラーフレームイベント
	Event Errored frame period event received (Port < ポート番号 >)	Warning	エラーフレーム期間
	Errored frame seconds summary event received (Port < ポート番号 >)	Warning	エラーフレームセカンドサマリイベント
	OAM Remote loopback started (Port < ポート番号 >)	Warning	リモートループバックの開始
	OAM Remote loopback terminated (Port < ポート番号 >)	Warning	リモートループバックの終了
ERPS	Signal fail detected on node (MAC: <MAC アドレス >)	Informational	シグナルエラーの検出
	Signal fail cleared on node (MAC: <MAC アドレス >)	Informational	シグナルエラーのクリア
	RPL owner conflicted on the ring (MAC: <MAC アドレス >)	Warning	RPL オーナーの重複
BPDU 防御	Port < ポート番号 > enter BPDU under attacking state (mode: drop / block / shutdown)	Informational	攻撃状態下でポートは BPDU 防御（破棄 / ブロック / シャットダウン）に入りました。
	Port < ポート番号 > recover from BPDU under attacking state manually	Informational	攻撃状態下でポートは BPDU 防御から手動で回復しました。
	Port < ポート番号 > recover from BPDU under attacking state automatically	Informational	攻撃状態下でポートは BPDU 防御から自動的に回復しました。
CFM	CFM cross-connect. VLAN:<VLAN ID>, Local (MD Level:<MD レベル >, Port < ポート番号 >, Direction: <MEP direction>) Remote (MEPID:<MEP ID>, MAC: <MAC アドレス >)	Critical	クロスコネクトの検出
	CFM remote setting error. MD Level:<MD レベル >, VLAN:<VLAN ID>, Local(Port < ポート番号 >, Direction:<mepdirection>) Remote(MEPID:<mepid>, MAC:<MAC アドレス >)	Warning	エラー CFM CCM パケットの検出
	CFM remote down. MD Level:<MD レベル >, VLAN:<VLAN ID>, Local (Port < ポート番号 >, Direction:<MEP direction>)	Warning	リモート MEP の CCM パケットを受信できません。
	CFM remote MAC error. MD Level:<MD レベル l>, VLAN:<VLAN ID>, Local (Port < ポート番号 >, Direction:<MEP direction>)	Warning	リモート MEP の MAC はエラー状態を報告しています。
	CFM remote detects a defect. MD Level:<MD レベル >, VLAN:<VLAN ID>, Local (Port < ポート番号 >, Direction:<MEP direction>)	Informational	リモート MEP は CFM 不良を検出しています。
DHCP	Detected untrusted DHCP server(IP: <IP アドレス >, Port: < ポート番号 >)	Informational	信頼性の低い DHCP サーバの IP アドレスを検出。

付録 D トラップログ

Standard Trap リスト

トラップ名 /OID	変数バインド	形式	MIB 名
coldStart 1.3.6.1.6.3.1.1.5.1	None	V2	RFC1907 (SNMPv2-MIB)
warmStart 1.3.6.1.6.3.1.1.5.2	None	V2	RFC1907 (SNMPv2-MIB)
authenticationFailure 1.3.6.1.6.3.1.1.5.5	None	V2	RFC1907 (SNMPv2-MIB)
linkDown 1.3.6.1.6.3.1.1.5.3	ifIndex ifAdminStatus ifOperStatus	V2	RFC2863 (IF-MIB)
linkup 1.3.6.1.6.3.1.1.5.4	ifIndex ifAdminStatus ifOperStatus	V2	RFC2863 (IF-MIB)
newRoot 1.3.6.1.2.1.17.0.1	None	V2	RFC1493 (BRIDGE-MIB)
topologyChange 1.3.6.1.2.1.17.0.2	None	V2	RFC1493 (BRIDGE-MIB)
risingAlarm 1.3.6.1.2.1.16.0.1	alarmIndex alarmVariable alarmSampleType alarmValue alarmRisingThreshold	V2	RFC2819 (RMON-MIB)
fallingAlarm 1.3.6.1.2.1.16.0.2	alarmIndex alarmVariable alarmSampleType alarmValue alarmFallingThreshold	V2	RFC2819 (RMON-MIB)
LldpRemTablesChange 1.0.8802.1.1.2.0.0.1	lldpStatsRemTablesInserts lldpStatsRemTablesDeletes lldpStatsRemTablesDrops lldpStatsRemTablesAgeouts	V2	LLDP-MIB
dot1agCfmFaultAlarm	dot1agCfmMepHighestPrDefect	V2	IEEE8021-CFMMIB
dot3OamThresholdEvent 1.3.6.1.2.1.158.0.1	dot3OamEventLogTimestamp dot3OamEventLogOui dot3OamEventLogType dot3OamEventLogLocation dot3OamEventLogWindowHi dot3OamEventLogWindowLo dot3OamEventLogThresholdHi dot3OamEventLogThresholdLo dot3OamEventLogValue dot3OamEventLogRunningTotal dot3OamEventLogEventTotal	V2	DOT3-OAM-MIB
dot3OamNonThresholdEvent 1.3.6.1.2.1.158.0.2	dot3OamEventLogTimestamp dot3OamEventLogOui dot3OamEventLogType dot3OamEventLogLocation dot3OamEventLogEventTotal	V2	DOT3-OAM-MIB

Proprietary Trap リスト

トラップ名 /OID	変数バインド	形式	MIB 名
SwIpMacBindingViolationTrap 1.3.6.1.4.1.171.12.23.5.0.1	swIpMacBindingPortIndex swIpMacBindingViolationIP swIpMacBindingViolationMac	V2	IPMacBind-MIB
swIpMacBindingStopLearningTrap 1.3.6.1.4.1.171.12.23.5.0.2	swIpMacBindingPortIndex	V2	IPMacBind-MIB
swIpMacBindingRecoverLearningTrap 1.3.6.1.4.1.171.12.23.5.0.3	swIpMacBindingPortIndex	V2	IPMacBind-MIB
swMacBasedAuthLoggedSuccess 1.3.6.1.4.1.171.12.35.11.1.0.1	swMacBasedAuthInfoMacIndex swMacBasedAuthInfoPortIndex swMacBasedAuthVID	V2	MBA-MIB
SwMacBasedAuthLoggedFail 1.3.6.1.4.1.171.12.35.11.1.0.2	swMacBasedAuthInfoMacIndex swMacBasedAuthInfoPortIndex swMacBasedAuthVID	V2	MBA-MIB
SwMacBasedAuthAgesOut 1.3.6.1.4.1.171.12.35.11.1.0.3	swMacBasedAuthInfoMacIndex swMacBasedAuthInfoPortIndex swMacBasedAuthVID	V2	MBA-MIB
swPktStormOccurred 1.3.6.1.4.1.171.12.25.5.0.1	swPktStormCtrlPortIndex	V2	PktStormCtrl-MIB
swPktStormCleared 1.3.6.1.4.1.171.12.25.5.0.2	swPktStormCtrlPortIndex	V2	PktStormCtrl-MIB
agentGratuitousARPTrap 1.3.6.1.4.1.171.12.1.7.2.0.5	agentGratuitousARPIpAddr agentGratuitousARPMacAddr agentGratuitousARPPortNumber agentGratuitousARPInterfaceName	V2	Genmgmt-MIB
swSafeGuardChgToExhausted 1.3.6.1.4.1.171.12.19.4.1.0.1	swSafeGuardCurrentStatus	V2	SafeGuard Engine-MIB
swSafeGuardChgToNormal 1.3.6.1.4.1.171.12.19.4.1.0.2	swSafeGuardCurrentStatus	V2	SafeGuard Engine-MIB
swDoSAttackDetected 1.3.6.1.4.1.171.12.59.4.0.1	swDoSCtrlType swDoSNotifyVarIpAddr swDoSNotifyVarPortNumber	V2	DoSPrev-MIB
swSingleIPMSColdStart 1.3.6.1.4.1.171.12.8.6.0.11	swSingleIPMSID swSingleIPMSMacAddr	V2	SINGLE-IP-MIB
swSingleIPMSWarmStart 1.3.6.1.4.1.171.12.8.6.0.12	swSingleIPMSID swSingleIPMSMacAddr	V2	SINGLE-IP-MIB
swSingleIPMSLinkDown 1.3.6.1.4.1.171.12.8.6.0.13	swSingleIPMSID swSingleIPMSMacAddr ifIndex	V2	SINGLE-IP-MIB
swSingleIPMSLinkUp 1.3.6.1.4.1.171.12.8.6.0.14	swSingleIPMSID swSingleIPMSMacAddr ifIndex	V2	SINGLE-IP-MIB
swSingleIPMSAuthFail 1.3.6.1.4.1.171.12.8.6.0.15	swSingleIPMSID swSingleIPMSMacAddr	V2	SINGLE-IP-MIB
swSingleIPMSnewRoot 1.3.6.1.4.1.171.12.8.6.0.16	swSingleIPMSID swSingleIPMSMacAddr	V2	SINGLE-IP-MIB
swSingleIPMSTopologyChange 1.3.6.1.4.1.171.12.8.6.0.17	swSingleIPMSID swSingleIPMSMacAddr	V2	SINGLE-IP-MIB
swSingleIPMSrisingAlarm 1.3.6.1.4.1.171.12.8.6.0.18	swSingleIPMSID swSingleIPMSMacAddr	V2	SINGLE-IP-MIB
swSingleIPMSfallingAlarm 1.3.6.1.4.1.171.12.8.6.0.19	swSingleIPMSID swSingleIPMSMacAddr	V2	SINGLE-IP-MIB
swSingleIPMSmacNotification 1.3.6.1.4.1.171.12.8.6.0.20	swSingleIPMSID swSingleIPMSMacAddr swSingleIPMSTrapMessage	V2	SINGLE-IP-MIB
swERPSSFDetectedTrap 1.3.6.1.4.1.171.12.78.4.0.1	swERPSNodeId	V2	ERPS-MIB

トラップ名 /OID	変数バインド	形式	MIB 名
swERPSSFClearedTrap 1.3.6.1.4.1.171.12.78.4.0.2	swERPSNodeId	V2	ERPS-MIB
swERPSRPLOwnerConflictTrap 1.3.6.1.4.1.171.12.78.4.0.3	swERPSNodeId	V2	ERPS-MIB
swBpduProtectionUnderAttackingTrap 1.3.6.1.4.1.171.12.76.4.0.1	swBpduProtectionPortIndex swBpduProtectionPortMode	V2	BPDUPROTECTION-MIB
swBpduProtectionRecoveryTrap 1.3.6.1.4.1.171.12.76.4.0.2	swBpduProtectionPortIndex swBpduProtectionRecoveryMethod	V2	BPDUPROTECTION-MIB
swFilterDetectedTrap 1.3.6.1.4.1.171.12.37.100.0.1	swFilterDetectedIP swFilterDetectedport	V2	FILTER-MIB
swL2PortSecurityViolationTrap 1.3.6.1.4.1.171.11.113.1.1.2.20.0.1 1.3.6.1.4.1.171.11.113.1.2.2.20.0.1 1.3.6.1.4.1.171.11.113.1.3.2.20.0.1 1.3.6.1.4.1.171.11.113.1.4.2.20.0.1	swL2PortSecurityPortIndex swL2PortSecurityViolationMac	V2	des3200-10-L2mgmt.mib des3200-18-L2mgmt.mib des3200-28-L2mgmt.mib des3200-28f-L2mgmt.mib
swL2macNotification 1.3.6.1.4.1.171.11.113.1.1.2.20.0.2 1.3.6.1.4.1.171.11.113.1.2.2.20.0.2 1.3.6.1.4.1.171.11.113.1.3.2.20.0.2 1.3.6.1.4.1.171.11.113.1.4.2.20.0.2	swL2macNotifyInfo	V2	des3200-10-L2mgmt.mib des3200-18-L2mgmt.mib des3200-28-L2mgmt.mib des3200-28f-L2mgmt.mib
swL2PortLoopOccurred 1.3.6.1.4.1.171.11.113.1.1.2.20.0.3 1.3.6.1.4.1.171.11.113.1.2.2.20.0.3 1.3.6.1.4.1.171.11.113.1.3.2.20.0.3 1.3.6.1.4.1.171.11.113.1.4.2.20.0.3	swL2LoopDetectPortIndex	V2	des3200-10-L2mgmt.mib des3200-18-L2mgmt.mib des3200-28-L2mgmt.mib des3200-28f-L2mgmt.mib
swL2PortLoopRestart 1.3.6.1.4.1.171.11.113.1.1.2.20.0.4 1.3.6.1.4.1.171.11.113.1.2.2.20.0.4 1.3.6.1.4.1.171.11.113.1.3.2.20.0.4 1.3.6.1.4.1.171.11.113.1.4.2.20.0.4	swL2LoopDetectPortIndex	V2	des3200-10-L2mgmt.mib des3200-18-L2mgmt.mib des3200-26-L2mgmt.mib des3200-28-L2mgmt.mib des3200-28f-L2mgmt.mib
swL2VlanLoopOccurred 1.3.6.1.4.1.171.11.113.1.1.2.20.0.5 1.3.6.1.4.1.171.11.113.1.2.2.20.0.5 1.3.6.1.4.1.171.11.113.1.3.2.20.0.5 1.3.6.1.4.1.171.11.113.1.4.2.20.0.5	swL2LoopDetectPortIndex swL2VlanLoopDetectVID	V2	des3200-10-L2mgmt.mib des3200-18-L2mgmt.mib des3200-26-L2mgmt.mib des3200-28-L2mgmt.mib des3200-28f-L2mgmt.mib
swL2VlanLoopRestart 1.3.6.1.4.1.171.11.113.1.1.2.20.0.6 1.3.6.1.4.1.171.11.113.1.2.2.20.0.6 1.3.6.1.4.1.171.11.113.1.3.2.20.0.6 1.3.6.1.4.1.171.11.113.1.4.2.20.0.6	swL2LoopDetectPortIndex swL2VlanLoopDetectVID	V2	des3200-10-L2mgmt.mib des3200-18-L2mgmt.mib des3200-28-L2mgmt.mib des3200-28f-L2mgmt.mib

付録 E RADIUS 属性の割り当て指定

DES-3200 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。
- 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

以下の記述では、続く RADIUS 属性の割り当てのを説明します。
- 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 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

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。

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。	12（ACL プロファイル用） 13 (ACL ルール用)	必須

属性指定フィールド	ACL プロファイルまたはルールを割り当てるために使用されます。	ACL コマンド
		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 vlan_id default port all deny`
			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、「DES-3200 CLI Reference Manual」の「Access Control List (ACL) Commands」を参照してください。

付録 F パスワードリカバリ手順

ここでは、弊社スイッチのパスワードのリセットについて記述します。ネットワークにアクセスを試みるすべてのユーザに認証は必要で重要です。権限のあるユーザを受け入れるために使用する基本的な認証方法は、ローカルログイン時にユーザ名とパスワードを利用するこうとです。時々パスワードが忘れられたり、壊れたりするため、ネットワーク管理者は、これらのパスワードをリセットする必要があります。ここでは、パスワードリカバリ機能は、そのような場合にネットワーク管理者を助けるものです。以下の手順で、容易にパスワードを回復するパスワードリカバリ機能の使用方法を説明します。

これらの手順を終了するとパスワードはリセットされます。

1. セキュリティの理由のため、パスワードリカバリ機能は物理的にデバイスにアクセスすることが必要です。そのため、デバイスのコンソールポートへの直接接続を行っている場合だけ、本機能を適用することが可能です。ユーザは端末エミュレーションソフトを使用して、スイッチのコンソールポートに端末または PC を接続する必要があります。

2. 電源をオンにします。runtime image が 100% までロードされた後に、「Password Recovery Mode」に入るために、2 秒以内に、ホットキー「 ^ 」（シフト +6）を押します。「Password Recovery Mode」に一度入ると、スイッチのすべてのポートが無効になります。

```
Boot Procedure                                                    V1.00.B003
--------------------------------------------------------------------------------
Power On Self Test ..................................... 100%
MAC Address : 00-1E-58-6E-98-00
H/W Version : A1

Please wait, loading V1.10.B015 Runtime image.............. 00%
The switch is now entering Password Recovery Mode:_
```

```
The switch is currently in Password Recovery Mode.
>
```

3. 「Password Recovery Mode」では、以下のコマンドのみ使用できます。

コマンド	説明
reset config	リセットし、全設定を工場出荷時設定に戻します。
reboot	「Password Recovery Mode」を終了し、スイッチを再起動します。現在の設定を保存するように確認メッセージが表示されます。
reset account	作成済みのアカウントのすべてを削除します。
reset password	指定ユーザのパスワードをリセットします。
{< ユーザ名 >}	ユーザ名を指定しないと、すべてのユーザのパスワードがリセットされます。
show account	設定済みのすべてのアカウントを表示します。

付録 G 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 550km。
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 802.3z) 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。
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設定項目を保持します。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。

用語	説明
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。