D-Link DWS-3160 シリーズ

Unified Wired & Wireless Access System

ユーザマニュアル

ご注意

本書は、各製品ごとの機能の説明および設定方法を記載しています。本シリーズの仕様、設置方法など使用するために必要な基本的な取り扱い方法については、設置マニュアルをご覧ください。

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。

無線に関するご注意

電波に関するご注意

本製品は、電波法に基づく小電力データ通信システムの無線製品として、技術基準適合証明を受けています。従って、本製品の使用する上で、無線局の免許は必要ありません。
本製品は、日本国内でのみ使用できます。
以下の注意をよくお読みになりご使用ください。

◎ この機器を以下の場所では使用しないでください。
- 心臓ペースメーカー等の産業・科学・医療用機器の近くで使用すると電磁妨害を及ぼし、生命の危険があります。
- 工場の製造ライン等で使用されている移動体識別用の構内無線局(免許を必要とする無線局)および特定小電力無線局(免許を必要としない無線局)
- 電子レンジの近くで使用すると、電子レンジによって無線通信に電磁妨害が発生します。

◎ 本製品は技術基準適合証明を受けています。本製品の分解、改造、および裏面の製品ラベルをはがさないでください。

5GHz 帯使用の無線機器に関するご注意

◎ 電波法により、5GHz 帯（W52/W53）は屋外での使用が禁止されています。
◎ 従来の中心周波数（J52）を使用した機器とは通信チャンネルが異なるために通信できません。
◎ 5GHz 帯（W53/W56）使用時は気象レーダー等との電波干渉を避けるためにチャンネルを 自動的に変更する場合があります（DFS 機能）

2.4GHz 帯使用の無線機器の電波干渉に関するご注意

本製品の使用周波数帯では、電子レンジ等の産業・科学・医療用機器のほか工場の製造ライン等で使用している移動体識別用の構内無線局 (免許を必要とする無線局) および特定小電力無線局 (免許を必要としない無線局) 並びにアマチュア無線局 (免許を必要とする無線局) が運用されています。

◎ この機器を使用する前に、近くで移動体識別用の構内無線局および特定小電力無線局並びにアマチュア無線局が運用されていないことを確認してください。
◎ 万一、この機器から移動体識別用の構内無線局に対して有害な電波干渉の事例が発生した場合には、速やかに使用周波数を変更するか、または電波の発射を停止してください。
◎ その他、この機器から移動体通信用の特定小電力無線局に対して電波干渉の事例が発生した場合など、何かお困りのことが起きたときは、弊社サポート窓口へお問い合わせください。

使用周波数帯域	2.4GHz 帯
変調方式	DS-SS 方式 /OFDM 方式
想定干渉距離	40m 以下
周波数変更可否	全帯域を使用し、かつ移動体識別用の構内無線局および特定小電力無線局並びにアマチュア無線局の帯域を回避可能

無線 LAN 製品ご使用時におけるセキュリティに関するご注意

無線 LAN では、LAN ケーブルを使用する代わりに、電波を利用してパソコン等と無線アクセスポイント間で情報のやり取りを行うため、電波の届く範囲であれば自由に LAN 接続が可能であるという利点があります。
その反面、電波はある範囲内であれば障害物（壁等）を越えてすべての場所に届くため、セキュリティに関する設定を行っていない場合、以下のような問題が発生する可能性があります。

◎ 通信内容を盗み見られる
悪意ある第三者が、電波を故意に傍受し、以下の通信内容を盗み見られる可能性があります。
- ID やパスワード又はクレジットカード番号等の個人情報
- メールの内容

◎ 不正に侵入される
悪意ある第三者が、無断で個人や会社内のネットワークへアクセスし、以下の行為を行う可能性があります。
- 個人情報や機密情報を取り出す（情報漏洩）
- 特定の人物になりすまして通信し、不正な情報を流す（なりすまし）
- 傍受した通信内容を書き換えて発信する（改ざん）
- コンピュータウィルスなどを流しデータやシステムを破壊する（破壊）

本来、無線 LAN カードや無線アクセスポイントは、これらの問題に対応するためのセキュリティの仕組みを持っていますので、無線 LAN 製品のセキュリティに関する設定を行って製品を使用することで、その問題が発生する可能性は少なくなります。

セキュリティの設定を行わないで使用した場合の問題を充分理解した上で、お客様自身の判断と責任においてセキュリティに関する設定を行い、製品を使用することをお奨めします。

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分からない場合は、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。踏み付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。

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。

- 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。
- 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。

電源の異常について

万一停電などの電源異常が発生した場合は、必ず本製品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。

安全にお使いいただくために

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
無線に関するご注意 3
ご使用上の注意 4
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 5
バッテリの取り扱いについて 5
電源の異常について 5

はじめに 15

本マニュアルの対象者 16
表記規則について 16

第 1 章　本製品のご使用にあたって 17

本製品について 17
サポートする機能 17
ポート 19
前面パネル 20
LED 表示 21
背面パネル 22
側面パネル 22
SFP ポート 23

第 2 章　スイッチの設置 24

パッケージの内容 24
ネットワーク接続前の準備 24
ゴム足の取り付け (19 インチラックに設置しない場合) 25
19 インチラックへの取り付け 25
電源の投入 26
電源の異常 26
リダンダント電源システムの設置 26
DPS-200 26
DPS-800 27
DPS-900 28
DPS-700 29

第 3 章　スイッチの接続 30

エンドノードと接続する 30
ハブまたはスイッチと接続する 30
バックボーンまたはサーバと接続する 31
アクセスポイントと接続する 31

第 4 章　スイッチ管理の導入 32

管理オプション 32
端末をコンソールポートに接続する 32
スイッチへの初回接続 33
ユーザアカウント設定 34
IP アドレスの割り当て 35
SNMP を使用した設定 37
トラップ 38
MIB 38

第 5 章　Web ベースのスイッチ管理 39

Web ベースの管理について 39
Web マネージャへのログイン 39
Web マネージャの画面構成 40
Web マネージャのメイン画面について 40
Web マネージャのメニュー構成 41

第 6 章　D-Link 統合アクセスシステム 45

D-Link 統合アクセスシステム構成 45
D-Link 統合スイッチ 45
D-Link アクセスポイント 45
WLAN の視覚化 46
D-Link 統合アクセスシステムのトポロジ 47
1 台の統合スイッチの設置 47
ピア統合スイッチの配置 47

第 7 章 LAN タブ（LAN の設定） 48

7.1　System Configuration（スイッチの主な設定） 49

Device Information（デバイス情報） 50
System Information Settings（システム情報設定 ） 51
Port Configuration（ポート設定） 52
Port Settings（スイッチのポート設定） 52
Port Description Settings（ポート名設定） 53
Port Error Disabled（エラーによるポートの無効） 54
Jumbo Frame Settings（ジャンボフレームの有効化） 54
PoE Configuration（PoE 設定）（DWS-3160-24PC のみ） 55
PoE System Settings（PoE システムの設定） 55
PoE Port Settings（PoE ポート設定） 56
Serial Port Settings（シリアルポート設定） 57
Warning Temperature Settings（警告温度設定） 57
System Log Configuration（システムログ構成） 58
System Log Settings（システムログ設定） 58
System Log Server Settings（システムログサーバの設定） 58
System Log（Syslog ログ） 59
System Log & Trap Settings（Syslog とトラップ設定） 60
System Severity Settings（システムセベリティ設定） 60
Time Range Settings（タイムレンジ設定） 61
Port Group Settings（ポートグループ設定） 62
Time Settings（時刻設定） 62
User Accounts Settings（ユーザアカウントの設定） 63
Command Logging Settings（コマンドログ設定） 64

7.2　Management（スイッチの管理） 65

ARP（ARP 設定） 66
Static ARP Settings（スタティック ARP 設定） 66
Proxy ARP Settings（プロキシ ARP 設定） 67
ARP Table（ARP テーブルの参照） 68
Gratuitous ARP（Gratuitous ARP の設定） 69
Gratuitous ARP Global Settings（Gratuitous ARP グローバル設定） 69
Gratuitous ARP Settings（Gratuitous ARP 設定） 70
IPv6 Neighbor Settings（IPv6 Neighbor 設定） 71
IP Interface（IP インタフェース設定） 72
System IP Address Settings（IP アドレス設定） 72
Interface Settings（インタフェース設定） 73
Management Settings（管理設定） 76
Session Table（セッションテーブル） 77
Single IP Management（シングル IP マネジメント設定） 78
シングル IP マネジメント（SIM）の概要 78
バージョン 1.61 へのアップグレード 79
Single IP Settings（シングル IP 設定） 80
Topology（トポロジ） 81
ツールヒント 82
メニューバー 85
Firmware Upgrade（ファームウェア更新） 86
Configuration File Backup/ Restore（コンフィグレーションファイルの更新） 86
Upload Log File（ログファイルのアップロード） 86

SNMP Settings（SNMP 設定）....87
SNMP Global Settings（SNMP グローバル設定）....88
SNMP Trap Settings（SNMP トラップ設定）....88
SNMP Linkchange Traps Settings（SNMP リンクチェンジトラップ設定）....89
SNMP View Table Settings（SNMP ビューテーブル）....89
SNMP Community Table Settings（SNMP コミュニティテーブル設定）....90
SNMP Group Table Settings（SNMP グループテーブル）....91
SNMP Engine ID Settings（SNMP エンジン ID 設定）....92
SNMP User Table Settings（SNMP ユーザテーブル設定）....92
SNMP Host Table Settings（SNMP ホストテーブル設定）....93
SNMP v6Host Table Settings（SNMP v6 ホストテーブル設定）....94
RMON Settings（RMON 設定）....94
Telnet Settings（Telnet 設定）....95
Web Settings（Web 設定）....95

7.3 L2 Features（レイヤ 2 機能の設定） 96

VLAN について....97
IEEE 802.1p プライオリティについて....97
VLAN とは....97
IEEE 802.1Q VLAN....97
VLAN（VLAN 設定）....102
802.1Q VLAN Settings（802.1Q VLAN 設定）....102
802.1v Protocol VLAN（802.1v プロトコル VLAN）....105
Asymmetric VLAN Settings（Asymmetric VLAN 設定）....108
GVRP（GVRP の設定）....108
MAC-based VLAN Settings（MAC ベース VLAN 設定）....110
Private VLAN Settings（プライベート VLAN 設定）....111
PVID Auto Assign Settings（PVID 自動割り当て設定）....112
Voice VLAN（音声 VLAN）....113
VLAN Trunk Settings（VLAN トランク設定）....116
Browse VLAN（VLAN の参照）....117
Show VLAN Ports（VLAN ポートの参照）....117
QinQ（QinQ 設定）....118
QinQ Settings（QinQ 設定）....119
VLAN Translation Settings（VLAN 変換機能の設定）....120
Spanning Tree（スパニングツリーの設定）....121
802.1Q-2005 MSTP....121
802.1D-2004 Rapid Spanning Tree....121
ポートの状態遷移....121
STP Bridge Global Settings（STP ブリッジグローバル設定）....122
STP Port Settings（STP ポートの設定）....124
MST Configuration Identification（MST の設定）....125
STP Instance Settings（STP インタンス設定）....127
MSTP Port Information（MSTP ポート情報）....128
Link Aggregation（ポートトランキングの設定）....130
ポートトランクグループについて....130
Port Trunking Settings（ポートトランキング設定）....131
LACP Port Settings（LACP ポートの設定）....132
FDB（FDB 設定）....133
Static FDB Settings（スタティック FDB の設定）....133
MAC Notification Settings（MAC 通知設定）....135
MAC Address Aging Time Settings（MAC アドレスエージングタイムの設定）....135
MAC Address Table（MAC アドレステーブル）....136
ARP & FDB Table（ARP と FDB テーブル）....137
L2 Multicast Control（L2 マルチキャストコントロール）....138
IGMP Snooping（IGMP Snooping の設定）....138
IGMP Host Table（IGMP ホストテーブル）....145
MLD Snooping（MLD Snooping 設定）....146
MLD Host Table（MLD ホストテーブル）....154
Multicast VLAN（マルチキャスト VLAN）....154
Multicast Filtering（マルチキャストフィルタリング）....161
IPv4 Multicast Filtering（IPv4 マルチキャストフィルタリング）....161
IPv6 Multicast Filtering（IPv6 マルチキャストフィルタリング）....165
Multicast Filtering Mode（マルチキャストフィルタリングモード）....169
ERPS Settings（イーサネットリングプロテクション設定）....170

LLDP（LLDP 設定）.....173
LLDP Global Settings（LLDP グローバル設定）.....173
LLDP Port Settings（LLDP ポート設定）.....174
LLDP Management Address List（LLDP 管理アドレスリスト）.....174
LLDP Basic TLVs Settings（LLDP ベーシック TLV 設定）.....175
LLDP Dot1 TLVs Settings（LLDP Dot1 TLV 設定）.....176
LLDP Dot3 TLVs Settings（LLDP Dot3 TLV 設定）.....177
LLDP Statistics System（LLDP 統計情報システム）.....178
LLDP Local Port Information（LLDP ローカルポート情報）.....178
LLDP Remote Port Information（LLDP リモートポート情報）.....180
NLB FDB Settings（NLB FDB 設定）.....181

7.4 L3 Features（レイヤ 3 機能の設定） 182

IPv4 Static/Default Route Settings（IPv4 スタティック / デフォルトルート設定）.....182
IPv4 Route Table（IPv4 ルートテーブル）.....183
IPv6 Static/Default Route Settings（IPv6 スタティック / デフォルトルート設定）.....183
IP Forwarding Table（IP フォワーディングテーブル）.....184
VRRP（VRRP 設定）.....185
VRRP Global Settings（VRRP グローバル設定）.....185
VRRP Virtual Router Settings（VRRP 仮想ルータ設定）.....186
VRRP Authentication Settings（VRRP 認証設定）.....188

7.5 QoS（QoS 機能の設定） 189

QoS について.....190
802.1p Settings（802.1p 設定）.....191
802.1p Default Priority Settings（ポートへのパケットプライオリティの割り当て）.....191
802.1p User Priority Settings（802.1p ユーザプライオリティ）.....192
Bandwidth Control（帯域幅の設定）.....192
Bandwidth Control Settings（帯域幅の設定）.....192
Queue Bandwidth Control Settings（キュー帯域幅制御の設定）.....193
Traffic Control Settings（トラフィックコントロールの設定）.....194
DSCP（DSCP 設定）.....196
DSCP Trust Settings（DSCP トラスト設定）.....196
DSCP Map Settings（DSCP マップ設定）.....196
HOL Blocking Prevention（HOL ブロッキング防止）.....197
Scheduling Settings（スケジュール設定）.....198
QoS Scheduling（QoS スケジュール作成）.....198
QoS Scheduling Mechanism（QoS スケジュールメカニズム設定）.....199

7.6 ACL（ACL 機能の設定） 200

ACL Configuration Wizard（ACL 設定ウィザード）.....200
Access Profile List（アクセスプロファイルリスト）.....202
アクセスプロファイルリストの作成（Ethernet）.....202
アクセスプロファイルリストの作成（IPv4）.....206
アクセスプロファイルリストの作成（IPv6）.....211
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）.....215
CPU Access Profile List（CPU アクセスプロファイルリスト）.....219
CPU アクセスプロファイルの作成（Ethernet）.....220
CPU アクセスプロファイルの作成（IPv4）.....223
CPU アクセスプロファイルの作成（IPv6）.....227
CPU アクセスプロファイルの作成（パケットコンテンツ）.....231
ACL Finder（ACL 検索）.....235
ACL Flow Meter（ACL フローメータ）.....236
Egress Access Profile List（Egress アクセスプロファイルリスト）.....240
アクセスプロファイルリストの作成（Ethernet）.....240
アクセスプロファイルリストの作成（IPv4）.....244
アクセスプロファイルリストの作成（IPv6）.....249
Egress ACL Flow Meter（Egress ACL フローメータリング）.....253

7.7 Security（セキュリティ機能の設定） 256

802.1X（802.1X 設定）....257
Port Access Entity（ポートアクセスエンティティ）....257
802.1X Global Settings（802.1X グローバル設定）....261
802.1X Port Settings（802.1X ポート設定）....261
802.1X User Settings（802.1X ユーザ設定）....263
Guest VLAN（ゲスト VLAN の設定）....264
Authenticator State（オーセンティケータの状態）....265
Authenticator Statistics（オーセンティケータ統計情報）....266
Authenticator Session Statistics（オーセンティケータセッション統計情報）....267
Authenticator Diagnostics（オーセンティケータ診断）....268
Initialize Port(s)（初期化ポート ）....268
Reauthenticate Port(s)（再認証ポート）....269
RADIUS（RADIUS 設定）....270
Authentication RADIUS Server Settings（認証 RADIUS サーバ設定）....270
RADIUS Accounting Setting（RADIUS アカウンティング設定）....271
RADIUS Authentication（RADIUS 認証）....272
RADIUS Account Client（RADIUS アカウンティングクライアント）....273
IP-MAC-Port Binding（IMPB : IP-MAC- ポートバインディング）....274
IMPB Global Settings（IMPB グローバル設定）....274
IMPB Port Settings（IMPB ポート設定）....275
IMPB Entry Settings（IMPB エントリ設定）....276
MAC Block List（MAC ブロックリスト）....277
DHCP Snooping（DHCP Snooping 設定）....277
DHCP Snooping Entry（DHCP Snooping エントリ）....278
MAC-Based Access Control（MAC ベースアクセスコントロール）....279
MAC-based Access Control Settings（MAC ベースアクセスコントロール設定）....279
MAC-based Access Control Local Settings（MAC ベースアクセスコントロール ローカル設定）....281
MAC-based Access Control Authentication State（MAC ベースアクセスコントロールの認証状態）....282
Compound Authentication（コンパウンド認証）....283
Compound Authentication Settings（コンパウンド認証設定）....283
Compound Authentication Guest VLAN Settings（コンパウンド認証ゲスト VLAN の設定）....284
Port Security（ポートセキュリティ）....285
Port Security Settings（ポートセキュリティの設定）....285
Port Security VLAN Settings（ポートセキュリティ VLAN 設定）....287
Port Security Entries（ポートセキュリティエントリ）....288
ARP Spoofing Prevention Settings（ARP Spoofing 防止設定）....289
BPDU Attack Protection（BPDU アタック防止設定）....290
Loopback Detection Settings（ループバック検知設定）....291
Traffic Segmentation Settings（トラフィックセグメンテーション設定）....292
NetBIOS Filtering Setting（NetBIOS フィルタリング設定）....293
DHCP Server Screening（DHCP サーバスクリーニング）....294
DHCP Server Screening Port Settings（DHCP サーバスクリーニング設定）....294
DHCP Offer Permit Entry Settings（DHCP オファー許可エントリ設定）....295
Access Authentication Control（アクセス認証コントロール）....296
Enable Admin（管理者レベルの認証）....297
Authentication Policy Settings（認証ポリシー設定）....298
Application Authentication Settings（アプリケーションの認証設定）....298
Authentication Server Group Settings（認証サーバグループ設定）....299
Authentication Server Settings（認証サーバ設定）....300
Login Method Lists Settings（ログインメソッドリスト）....301
Enable Method Lists Settings（メソッドリストの有効化）....302
Local Enable Password Settings（ローカルユーザパスワード設定）....303
SSL Settings（Secure Socket Layer の設定）....304
SSH（Secure Shell の設定）....306
SSH Settings（SSH サーバ設定）....306
SSH Authentication Method and Algorithm Settings（SSH 認証モードとアルゴリズム設定）....307
SSH User Authentication Lists（SSH ユーザ認証リスト）....308
Trusted Host（トラストホスト）....309
Safeguard Engine Settings（セーフガードエンジン設定）....310

Captive Portal（キャプティブポータル）.....312
Global Configuration（グローバル設定）.....312
CP Configuration（CP 設定）.....313
CP Web ページのカスタマイズ.....315
Local User（ローカルユーザ）.....320
Interface Association（インタフェースアソシエーション）.....322
CP Status（CP 状態）.....322
Interface Status（インタフェース状態）.....324
Client Connection Status（クライアントの接続状態）.....325
SNMP Trap Configuration（SNMP トラップ設定）.....328
7.8 Network Application（ネットワークアプリケーション） 329
DHCP（DHCP 設定）.....329
DHCP Relay（DHCP リレー）.....329
DHCP Local Relay Settings（DHCP ローカルリレー設定）.....335
SNTP（SNTP 設定）.....336
SNTP Settings（SNTP 設定）.....336
Time Zone Settings（タイムゾーン設定）.....337
Flash File System Settings（フラッシュファイルシステム設定）.....338
7.9 OAM（Object Access Method : オブジェクトアクセス方式） 341
CFM（Connectivity Fault Management : 接続性障害管理）.....341
CFM Settings（CFM 設定）.....341
CFM Port Settings（CFM ポート設定）.....348
CFM MIPCCM Table（CFM MIPCCM テーブル）.....349
CFM Loopback Settings（CFM ループバック設定）.....349
CFM Linktrace Settings（CFM リンクトレース設定）.....350
CFM Packet Counter（CFM パケットカウンタ）.....351
CFM Fault Table（CFM 障害テーブル）.....351
CFM MP Table（CFM MP テーブル）.....352
Ethernet OAM（イーサネット OAM）.....353
Ethernet OAM Settings（イーサネット OAM 設定）.....353
Ethernet OAM Configuration Settings（イーサネット OAM コンフィグレーション設定）.....354
Ethernet OAM Event Log（イーサネット OAM イベントログ）.....355
Ethernet OAM Statistics（イーサネット OAM 統計情報）.....355
Cable Diagnostics（ケーブル診断機能）.....356
7.10 Monitoring（スイッチのモニタリング） 357
Utilization（使用率）.....357
CPU Utilization（CPU 使用率）.....357
DRAM & Flash Utilization（DRAM とフラッシュ利用率）.....358
Port Utilization（ポート使用率）.....358
Statistics（統計情報）.....359
Packets（パケット統計情報）.....359
Errors（パケットエラー）.....363
Packet Size（パケットサイズ）.....366
Mirror（ポートミラーリング）.....368
Port Mirror Settings（ポートミラーリング設定）.....368
RSPAN Settings（RSPAN 設定）.....369
sFlow（sFlow 設定）.....370
sFlow Global Settings（sFlow グローバル設定）.....370
sFlow Analyzer Server Settings（sFlow アナライザ設定）.....370
sFlow Flow Sampler Settings（sFlow サンプラ設定）.....371
sFlow Counter Poller Settings（sFlow カウンタポーラ設定）.....373
Ping Test（Ping テスト）.....374
Trace Route（トレースルート）.....375
Peripheral（周辺機器）.....376
Device Environment（デバイス環境の参照）.....376

第 8 章 WAN タブ（WAN の設定） 377

8.1 Security（セキュリティ機能の設定） 378

Captive Portal（キャプティブポータル）....378
Global Configuration（グローバル設定）....378
CP Configuration（CP 設定）....379
CP Web ページのカスタマイズ....381
Local User（ローカルユーザ）....386
Interface Association（インタフェースアソシエーション）....388
CP Status（CP 状態）....388
Interface Status（インタフェース状態）....390
Client Connection Status（クライアントの接続状態）....391
SNMP Trap Configuration（SNMP トラップ設定）....394

8.2 Monitoring（無線のモニタリング） 395

Global（無線グローバル情報）....395
Peer Switch（ピアスイッチ）....403
Status（ピアスイッチの状態）....403
Configuration（コンフィグレーション状態）....404
Managed AP（管理対象アクセスポイント）....405
Access Point（アクセスポイントのモニタ）....406
All AP Status（全アクセスポイントの状態）....406
Managed AP Status（管理対象アクセスポイントの状態）....407
AP Authentication Failure Status（アクセスポイント認証エラー状態）....421
AP RF Scan Status（アクセスポイントの RF スキャン状態）....422
AP De-Authentication Attack Status（アクセスポイント認証解除攻撃状態）....426
Client（クライアント）....427
Associated Clients（接続中のクライアント）....427
Detected Clients（検出クライアント）....438
Ad Hoc Clients（アドホッククライアント）....444
QoS（QoS 設定）....445
Access Control Lists（アクセスコントロールリスト）....445
Differentiated Services（DiffServ: ディフサーブ）....450

8.3 Administration（アクセスポイントの設定） 452

Basic Setup（基本設定）....452
Global タブ（無線グローバル基本設定）....453
Discovery タブ（無線ディスカバリの設定）....454
Profile タブ（プロファイル）....455
Radio タブ（周波数帯域）....455
SSID タブ（SSID 設定）....457
Valid AP タブ（Valid アクセスポイントの設定）....461
OUI タブ（OUI データベース）....463
AP Management（アクセスポイント管理）....464
AP Reboot（アクセスポイント再起動）....464
RF Management（RF 管理）....464
Software Downloads（アクセスポイントソフトウェアのダウンロード）....468
Advanced Settings（管理アクセスポイントの詳細設定）....470
AP Provisioning（アクセスポイントプロビジョニング）....471
Advanced Configuration（高度な設定）....473
Global（グローバル設定）....473
Networks（ネットワーク）....477
AP Profiles（AP プロファイル）....481
Peer Switch（ピアスイッチ）....489
WIDS Security（WIDS セキュリティ）....492
Clients（クライアント）....495
Switch Provisioning（スイッチのプロビジョニング）....496

8.4 QoS（QoS 機能の設定） 498
Access Control Lists（アクセスコントロールリスト） 498
IP Access Control Lists（IP アクセスコントロールリスト） 498
IPv6 Access Control Lists（IPv6 アクセスコントロールリスト） 505
MAC Access Control Lists（MAC アクセスコントロールリスト） 508
Differentiated Services（クラス別サービス） 511
Diffserv Configuration（Diffserv 設定） 511
Class Configuration（クラス設定） 511
Policy Configuration（ポリシー設定） 514
Policy Class Definition（ポリシークラス定義） 515
8.5 Network Visualization（無線ネットワークの視覚化） 517
Download Image（イメージのダウンロード） 517
Launch…（起動） 518
メニューバー 519
「Legend」メニューについて 520
第 9 章 Maintenance（スイッチのメンテナンス） 521
Save Configuration / Log（コンフィグレーションとログの保存） 521
Tools（ツールメニュー） 522
License Management（ライセンス管理） 522
Download Firmware（ファームウェアのダウンロード） 522
Upload Firmware（ファームウェアのアップロード） 523
Download Configuration（コンフィグレーションのダウンロード） 524
Upload Configuration（コンフィグレーションファイルのアップロード） 525
Upload Log File（ログファイルのアップロード） 526
Reset（リセット） 527
Reboot System（システムの再起動） 527
付録 A パケットコンテンツ ACL を使用した ARP スプーフィング攻撃の軽減 528
ARP を動作させる方法 528
ARP スプーフィングでネットワークを攻撃する方法 530
パケットコンテンツ ACL 経由で ARP スプーフィング攻撃を防止する 531
設定 532
付録 B パスワードのリカバリ手順 534
付録 C ログエントリ 535
付録 D トラップログ 545
付録 E RADIUS 属性の割り当て指定 549
付録 F 無線スイッチ仕様 554
キャプティブポータルガイドライン 554
認証ローミングとクラスタリング 554
クラスタコントローラ選定 554
X.509 Certification Mutual Authentication（X.509 証明書相互認証） 555
X.509 Certification Mutual Authentication（X.509 証明書相互認証） 555
無線システムにおける証明書の概要と利用法 555
アクセスポイントにおける証明書生成 555
スイッチにおける証明書生成 555
IP アドレスの割り当て 556
MBA および IMPB に対する IP トンネル 556
付録 G D-Link 統合アクセスシステムの初期設定 557
G.1 DWS-3160 の初期設定 557
G.2 D-Link アクセスポイントプロファイルの初期設定 558
G.3 キャプティブポータル設定の初期値 559
付録 H ケーブルとコネクタ 560
イーサネットケーブル 560
コンソールケーブル 560
リダンダント電源（RPS）ケーブル 561
ケーブル長 562

はじめに

DWS-3160 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 本製品のご使用にあたって

- 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 スイッチの設置

- 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ネットワークに接続する方法を説明します。

第 4 章 スイッチの管理

- パスワード設定、SNMP 設定、および各種デバイスからの本スイッチへの接続など基本的なスイッチの管理について説明します。

第 5 章 Web ベースのスイッチ設定

- 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 D-Link 統合アクセスシステム

- D-Link 統合アクセスシステムについて説明します。

第 7 章 LAN タブ（LAN の設定）

- System Configuration（スイッチの主な設定）
  デバイス情報、ポート設定、ユーザアカウント、システムログ設定、時刻設定、シリアルポートなどの基本機能の設定について説明します。
- Management（スイッチの管理）
  IP インタフェース設定、ARP 設定、シングル IP マネジメント設定、SNMP 設定、Telnet 設定、Web 設定などの管理機能について説明します。
- L2 Features（レイヤ 2 機能の設定）
  VLAN、トランキング、スパニングツリー、フォワーディング、LLDP などのレイヤ 2 機能について説明します。
- L3 Features（レイヤ 3 機能の設定）
  スタティック / ダイナミックルート設定、VRRP などのレイヤ 3 機能について説明します。
- QoS（QoS 機能の設定）
  QoS 機能について説明します。帯域制御、QoS スケジューリング、802.1p デフォルトプライオリティ、802.1p ユーザプライオリティなどの機能を含みます。
- ACL（ACL 機能の設定）
  アクセスプロファイルテーブルや CPU インタフェースフィルタリングなどの ACL（アクセスコントロールリスト）機能について説明します。
- Security（セキュリティ機能の設定）
  802.1X、トラストホスト、アクセス認証コントロール、ポートセキュリティ、トラフィックセグメンテーション、SSL、SSH、IP-MAC- ポートバインディング、IP マルチキャスト範囲の制限、およびセーフガードエンジン、およびキャプティブポータル設定などのセキュリティ機能について説明します。
- Network Application（ネットワークアプリケーション）
  DHCP サーバ設定、SNTP などのネットワークアプリケーション機能について説明します。
- OAM（Object Access Method : オブジェクトアクセス方式）
  CFM（接続性障害管理）、ケーブル診断機能などについて説明します。
- Monitoring（スイッチのモニタリング）
  CPU 使用率、パケット統計情報、エラー、パケットサイズ、ミラーリング、sFlow、Ping、トレースルートなどのモニタ機能について説明します。

第 8 章 WLAN（WLAN の設定）

- Security（セキュリティ機能の設定）
  キャプティブポータル機能について説明します。
- Monitoring（スイッチのモニタリング）
  アクセスポイント、クライアントの管理状態やパケット統計情報などのモニタ機能について説明します。
- Administration（アクセスポイントの設定）
  基本設定、アクセスポイントの管理設定、高度な設定について説明します。
- QoS（QoS 機能の設定）
  無線の QoS 機能について説明します。アクセスコントロールリストや DiffServ 機能について説明します。
- Network Visualization（無線ネットワークの視覚化）
  無線ネットワークの情報を図式化して表示する機能について説明します。

第 9 章 スイッチメンテナンス

- リセット、システムの再起動、変更の保存について説明します。

付録 A パケットコンテンツ ACL を使用した ARP スプーフィング攻撃の軽減

- ARP プロトコル、ARP スプーフィング攻撃、および D-Link スイッチが提供する ARP スプーフィング攻撃を防御する対策について説明します。

付録 B パスワードのリカバリ手順

- スイッチのパスワードのリセット方法について説明します。

付録 C ログエントリ

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

付録 D トラップログ

- スイッチで検出されるのトラップログとその意味について説明します。

付録 E RADIUS 属性の割り当て指定

- DWS-3160 における RADIUS 属性の割り当てについて説明します。

付録 F 無線スイッチ仕様

- キャプティブポータル、クラスタコントローラ選定、X.509 証明書相互認証などについて説明します。

付録 G D-Link 統合アクセスシステムの初期設定

- DWS-3160 システムの初期設定について示します。

付録 H ケーブルとコネクタ

- スイッチに使用されるケーブルとコネクタ形状について説明します。

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	コマンドパラメータ（可変または固定）。	*`value`*
< >	可変パラメータ。< > にあたる箇所に値または文字を入力します。	<*`value`*>
[ ]	任意の固定パラメータ。	[*`value`*]
[< >]	任意の可変パラメータ。	[<*`value`*>]
{ }	{ } 内の選択肢から 1 つ選択して入力するパラメータ。	{*`choice1`* | *`choice2`*}
|（垂直線）	相互排他的なパラメータ。	*`choice1`* | *`choice2`*
[{ }]	任意のパラメータで、指定する場合はどちらかを選択します。	[{*`choice1`* | *`choice2`*}]

第 1 章　本製品のご使用にあたって

- 本製品について
- サポートする機能
- ポート
- 前面パネル
- 背面パネル
- 側面パネル
- SFP ポート

本製品について

DWS-3160 シリーズギガビットイーサネット統合スイッチは、小規模及びリモートオフィス環境に特に適しており、増え続けるワイヤレス統合スイッチへの要望を満たすことができます。このシリーズは小規模及びリモートオフィスだけでなく、中規模エンタープライズでのワイヤレスネットワーク環境に対しても、最適化されたパフォーマンスや費用対効果のあるソリューションを提供することができます。

ご購入時、デフォルトでこのスイッチは 12 台までの統合アクセスポイントを管理することができます。D-Link から別途ライセンスをご購入いただき、アクティベーションすることで、統合スイッチ 1 台あたり 40 台までの統合アクセスポイントを管理することができます。本スイッチの最大の特徴は、4 台までのスイッチがクラスタを形成し、単一の IP アドレスで最大 192 台の統合アクセスポイントを集中管理できるという点です。

本スイッチは費用対効果の高いギガビットスイッチであり、管理者に手頃な価格でネットワークを高速のギガビット接続にアップグレードするソリューションを提供します。スイッチにおけるアドバンスド ACL およびユーザ認証機能はコアからエッジまでネットワークセキュリティの適用範囲を拡張します。D-Link 独自のセーフガードエンジンは外部ネットワークの脅威からスイッチを保護します。その結果、信頼度、実用性、および可用性を向上します。

スイッチは Copper ポート（10/100/1000Mbps）と SFP ポート（100/1000Mbps）を搭載しており、コンピュータ、ノート PC、プリントサーバ、NAS デバイス、IP カメラ、VoIP PBX デバイス、および他のスイッチなど様々なネットワークデバイスをネットワークに接続するために使用できます。SFP（Small Form Factor Portable）コンボポートは、光ファイバ接続用に光トランシーバを使用して、他の多様なネットワークデバイスをギガビットイーサネット速度で、長距離ネットワークに接続します。

DWS-3160-24PC の Copper ポートすべてが様々な利用用途で使われる Power over Ethernet（PoE）に対応しています。DWS-3160-24PC スイッチにおいて、個々のギガビットポートが（IEEE 802.11n 規格をサポートしている）アクセスポイントや VoIP 電話、IP カメラのような PoE デバイスをスイッチに接続して、同時に給電するために、IEEE 802.3af 及び IEEE 802.3at Power over Ethernet をサポートしています。これにより、設置をより簡単に行うことができる上、スイッチに接続するデバイスに必要な電源コンセント数を減らすことができます。

サポートする機能

- 無線マネージメント
  - 無線マネージメント AP 数 : 48 （直接接続およびスイッチ経由の間接接続）
  - AP 検出、Path MTU、AP-AP トンネル
- ローミング
  - ファーストローミング / インタースイッチ・ローミング /L3 ローミング /L2 ローミング
- RF マネージメントと帯域制御
  - マルチ SSID : 32 SSID/AP（16 SSID/RF Frequency Band）
  - 自動 AP チャンネル調整、自動 AP 送信出力電力調整、接続制限
- AP マネージメント
  - 管理 AP : DWL-8600AP/6600AP/3600AP
  - AP 自動検出 / リモート AP リブート
  - AP モニタ：管理 AP のリスト表示、不正 AP、認証エラー AP
  - クライアントモニタ：各管理 AP に関連するクライアントの表示、Ad-Hoc クライアントモニタ
  - AP 認証：ローカルユーザデータベース、RADIUS サーバ、中央管理 RF/ セキュリティポリシー管理、Visualization Tool
- 無線セキュリティ
  - 不正 AP 検知、クライアント /AP クラシフィケーション（RF チャンネル、MAC アドレス、SSID、時刻）
  - 不正 /Valid AP クラシフィケーション（MAC アドレスベース）、Captive portal（Web 認証）、WLAN クライアントパーティション
  - 無線侵入検知システム
  - WEP : 64/128/152bit
  - WPA : Personal/Enterprise
  - WPA2 : Personal/Enterprise
  - 暗号化方式 : TKIP/AES
  - IEEE 802.1X EAP タイプ : EAP-MD5、EAP-TLS、EAP-TTLS、EAP-FAST、EAP-SIM、PEAP-GTC、PEAP-TLS、PEAP-MS-CHAPv2

- L2 機能
  - IGMP スヌーピング：v1/v2/v3、スヌーピンググループ数：1K、IGMP Fast Leave
  - MLD スヌーピング：v1/v2、スヌーピンググループ数：1K
  - スパニングツリー：IEEE 802.1D STP、IEEE 802.1wRSTP、IEEE 802.1s MSTP、BPDU フィルタリング、ルートガード
  - ループバック検知（STP 無し）
  - IEEE 802.3ad リンクアグリゲーション：32 グループ / デバイス、8 ポート / グループ
  - ポートミラーリング：1 ポート対 1 ポート、1 ポート対多ポート、ACL モード、RSPAN（Remote Switched Port Analyzer）
  - ジャンボフレーム：13,312Byte
- VLAN
  - IEEE 802.1Q タグ VLAN、IEEE 802.1v プロトコルベース VLAN
  - VLAN グループ数：4094、VLAN ID レンジ：1-4094
  - GVRP、Voice VLAN、Praivate VLAN、ポートベース VLAN、MAC ベース VLAN、Asymmetric VLAN
  - ISM VLAN、VLAN トランキング
- L3 機能
  - ルーティングエントリ：512（IPv4 スタティック）
  - IP インタフェース数：16
  - VRRP、プロキシ ARP、Gratuitous ARP
- QoS
  - IEEE 802.1p 対応、ポートの帯域制御、フローの帯域制御
  - キュー：8 レベル / ポート
  - キューのスケジューリング：WRR（重み付けラウンドロビン）、Strict
  - CoS：VLAN ID、IEEE 802.1p プライオリティ、MAC アドレス、Ether タイプ、IPv4/v6 アドレス、DSCP、プロトコルタイプ、TCP/UDP ポート、IPv6 トラフィッククラス、IPv6 フローラベル、ユーザ定義パケット
  - QoS フローアクション：802.1p プライオリティマーク、ToS/DSCP リマーク、帯域制御
- ACL（アクセスコントロールリスト）
  - 最大 6 プロファイル、256 ルール
  - ACL 定義パラメータ：VLAN ID、IEEE 802.1p プライオリティ、MAC アドレス、IPv4/v6 アドレス、EtherType、DSCP、プロトコルタイプ、TCP/UDP ポート、IPv6 トラフィッククラス、IPv6 フローラベル、ユーザ定義パケット
  - タイムベース ACL
  - CPU インタフェースフィルタリング：5 プロファイル、100 ルール / プロファイル
- LAN セキュリティ
  - RADIUS、RADIUS アカウンティング、TACACS+、SSH v2、SSLv3、ポートセキュリティ：3072MAC アドレス / ポート
  - IEEE 802.1X 認証：ポートベース認証 / ホストベース認証
  - WEB 認証、MAC アドレス認証、Compound 認証
  - ゲスト VLAN：ポートベース / ホストベース
  - Microsoft® NAP 検疫（NAP-DHCP 方式）
  - ブロードキャスト / マルチキャストストームコントロール、トラフィックセグメンテーション
  - D-Link セーフガードエンジン、NetBIOS フィルタリング、DoS 攻撃防御
  - DHCP サーバスクリーニング、ARP スプーフィング防止、FDB セキュリティ
  - 認証 DB フェイルオーバ：802.1X/MAC/Compound/WEB
  - 認証バイパス
- マネージメント
  - LLDP、LLDP-MED、Web ベース GUI：IPv4/IPv6、CLI、ZMODEM
  - 4 レベルのユーザアクセス権限、Telnet サーバ（IPv4/IPv6）/ クライアント（IPv4/IPv6）
  - TFTP クライアント（IPv4/IPv6）、SNMP v1/v2c/v3、SNMP over IPv6、SNMP トラップ
  - RMON v1：4 グループコンフィグ、RMON v2：プルーブコンフィググループ
  - sFlow、DHCP 自動設定、DHCP リレーオプション 12 /82、SYSLOG（IPv4/IPv6）
  - CPU モニタリング、パスワードの暗号化、パスワードリカバリ、マルチコンフィグレーション、マルチイメージ
  - ポートディスクリプション、SNTP クライアント、トラストホスト、スイッチクラスタリング（4 台まで）、
  - ケーブル診断、802.3ah、ITU-T Y.1731 OAM、IPv6 Neighbor Discovery、タイムベース PoE（DGS-3160-24PC）
  - WMM-PS（WMM Power Save）、802.11e U-APSD、NLB、片方向リンク検知（DULD）
- 以下の MIB のサポート
  - MIBs MIBII（ RFC1213）
  - Bridge MIB（RFC1493）
  - SNMPv2 MIB（RFC1907）
  - RMON MIB（RFC1757, 2819）
  - RMONv2 MIB（RFC2021）
  - IEEE 802.1p MIB（RFC2674）
  - Etherlike MIB（RFC1643, 2358, 2665）
  - IF MIB（RFC2233, 2863）
  - RADIUS 認証クライアント MIB（RFC2618）
  - RADIUS アカウンティングクライアント MIB（RFC2620）
  - Ping MIB（RFC2925）

  - TRACEROUTE MIB（RFC2925）
  - プライベート MIB
  - IPv6 MIB（RFC1213, 2465, 4293）
  - IP MIB（RFC4293）
  - TCP MIB（RFC4022）
  - Zone Defense MIB
  - UDP/ICMP/ARP（RFC1213）
  - Entity MIB（RFC2737）
- スイッチ管理用 RJ-45 コンソールポート
- パラレルポート状態 LED 表示（リンク、アクション、スピード等）
- レート適応およびプロトコル変換に対応するための、非ブロック型ストアアンドフォワードスイッチング機能
- ワイヤスピードでのフォワーディング速度に対応するための自己学習機能およびアドレス認識メカニズム

ポート

DWS-3160 シリーズは以下のポートを搭載しています。

型番	DWS-3160-24TC	DWS-3160-24PC
10BASE-T/100BASE-TX/1000BASE-T ポート	24	
PoE 給電（IEEE 802.3af/at）	ー	24
SFP コンボスロット	4	
RJ-45 コンソールポート	1	
RPS コネクタ	1	
SD カードスロット	1	

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/1000BASE-T	SFP ポート
• IEEE 802.3 • IEEE 802.3u • IEEE 802.3ab • IEEE 802.3af/at（DWS-3160-24PC） • 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（シングルモード 100BASE-FX） • DEM-211（マルチモード 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）

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 24 と 1000BASE-T のポート 24）、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、10BASE-T/100BASE-TX/1000BASE-T ポート、SFP コンボポート、SD カードスロット、および RJ-45 コンソールポートが配置されています。また、電源、コンソール、RPS（冗長電源システム）、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/Speed 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。

DWS-3160-24TC

- 10BASE-T/100BASE-TX/1000BASE-T ポート x 24
- SFP コンボポート x 4
- SD カードスロット
- RJ-45 コンソールポート x 1
- LED: Power、Console、RPS、Fan、SD、Link/Act/Speed（各ポート）

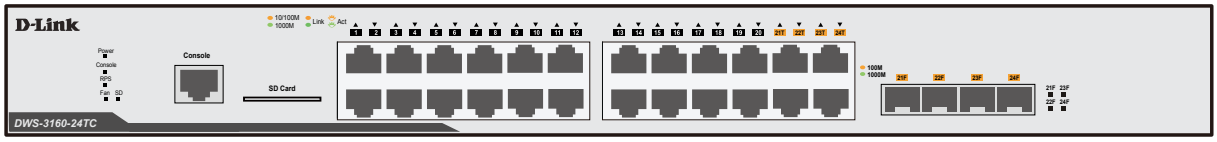


図 1-1　DWS-3160-24TC の前面パネル

DWS-3160-24PC

- 10BASE-T/100BASE-TX/1000BASE-T ポート x 24
- SFP コンボポート x 4
- SD カードスロット
- RJ-45 コンソールポート x 1
- LED: Power、Console、RPS、Fan、SD、Link/PoE、Link/Act/Speed（各ポート）

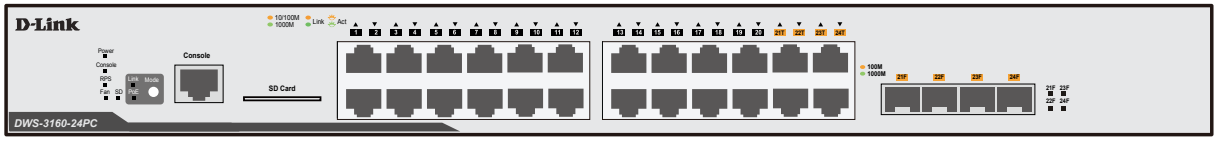


図 1-2　DWS-3160-24PC の前面パネル

LED 表示

LED はスイッチとネットワークの状態を表示します。Power、Console、SD、および各ポートについて LED をサポートします。以下に、スイッチ上の LED の配置と、各 LED の状態が表す意味を示します。

DWS-3160-24TC

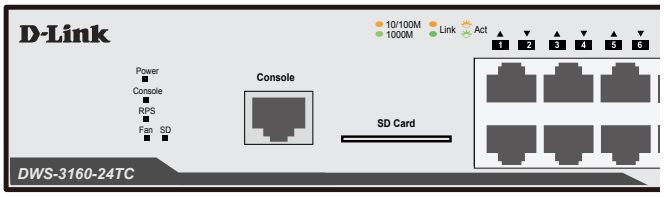


図 1-3　DWS-3160-24TC の前面パネル LED 配置図

DWS-3160-24PC

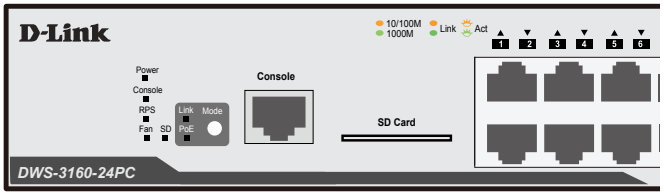


図 1-4　DWS-3160-24PC の前面パネル LED 配置図

以下の表に LED の状態が意味するスイッチの状態を示します。

LED	色	状態	状態説明
システム LED			
Power	緑	点灯	スイッチに電源が供給され正常に動作しています。
	ー	消灯	スイッチに電源が供給されていません。
Console	緑	点滅	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。
RPS	緑	点灯	内蔵電源ユニットの異常により、拡張のリダンダント電源ユニットが動作しています。
		点滅	RPS ケーブルの接続を検出しています。
	ー	消灯	リダンダント電源ユニットは動作していません。
Fan	赤	点滅	ファンが故障しています。
	ー	消灯	ファンは正常に動作しています。
SD	緑	点灯	SD スロットに SD カードが挿入されています。
		点滅	リード / ライト中です。
	ー	消灯	SD スロットに SD カードは挿入されていません。
	橙	点灯	SD カードに不具合が生じています。
Link（DWS-3160-24PC）	緑	点灯	Link/Act/Speed モードを選択中です。
PoE（DWS-3160-24PC）	緑	点灯	PoE モードを選択中です。
GE ポート LED			
Link/ACT/SPD	緑	点灯	1000Mbps でリンクが確立しています。
		点滅	1000Mbps でデータを送受信しています。
	橙	点灯	10/100Mbps でリンクが確立しています。
		点滅	10/100Mbps でデータを送受信しています。
	ー	消灯	リンクが確立していません。
PoE (DWS-3160-24PC)	緑	点灯	接続中の PoE 受電機器に給電中です。
	橙	点灯	PoE ポートにエラーが発生しました。
	ー	消灯	給電をしていません。(受電機器が未検出または未接続)
SFP ポート LED			
Link/ACT/SPD	緑	点灯	1000Mbps でリンクが確立しています。
		点滅	1000Mbps でデータを送受信しています。
	橙	点灯	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。
	ー	消灯	リンクが確立していません。

背面パネル

スイッチの背面パネルには、AC 電源コネクタ、オプションの外部リダンダント電源用のコネクタが配備されています。

DWS-3160-24TC

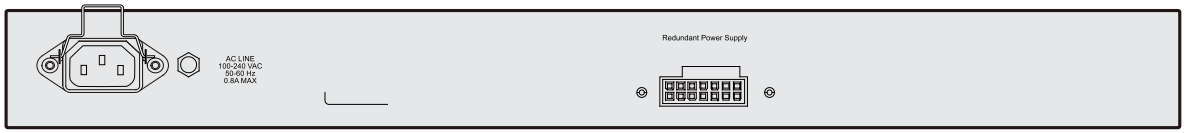


図 1-5　DWS-3160-24TC 背面パネル図

背面パネルにはオプションのリダンダント電源ユニット用のアウトレットがあります。内蔵電源ユニットに異常が発生した場合に外部リダンダント電源ユニット（オプション）が自動的にスイッチに電源を供給します。AC 電源コネクタは標準の電源ケーブルを接続する三極インレットです。ここに付属の電源ケーブルを接続します。スイッチは自動的に 50/60Hz、100 ～ 240VAC 内の電圧に調整されます。

DWS-3160-24PC

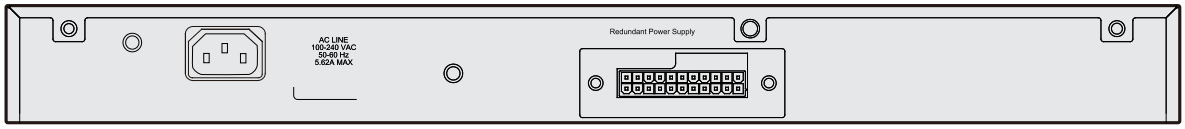


図 1-6　DWS-3160-24PC 背面パネル図

背面パネルにはオプションのリダンダント電源ユニット用のアウトレットがあります。内蔵電源ユニットに異常が発生した場合に外部リダンダント電源ユニット（オプション）が自動的にスイッチに電源を供給します。AC 電源コネクタは標準の電源ケーブルを接続する三極インレットです。ここに付属の電源ケーブルを接続します。スイッチは自動的に 50/60Hz、100 ～ 240VAC 内の電圧に調整されます。

PoE の目的は、スイッチにバックアップ電源を供給することです。内部電源が故障した場合に、電源を切り替えます。さらに、本製品は、802.3af PoE をサポートしており、すべてのポートが 30W の電源を供給します。RPS を併用した場合、供給可能な電力はフルパワーで 740W です。RPS 機能を使用せずに DWS-3160-24PC を操作する場合、ポートごとに 15.4W 供給するため、24 デバイスを動作させた場合、370W だけが使用されます。

側面パネル

システムのファンと通気口がスイッチ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。

DWS-3160-24TC

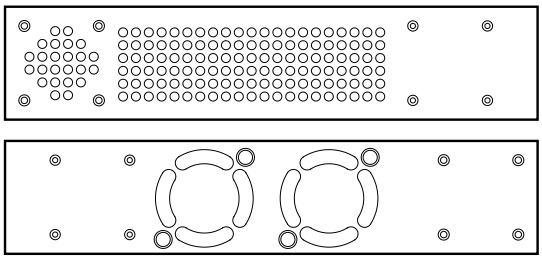


図 1-7　側面パネル図

DWS-3160-24PC

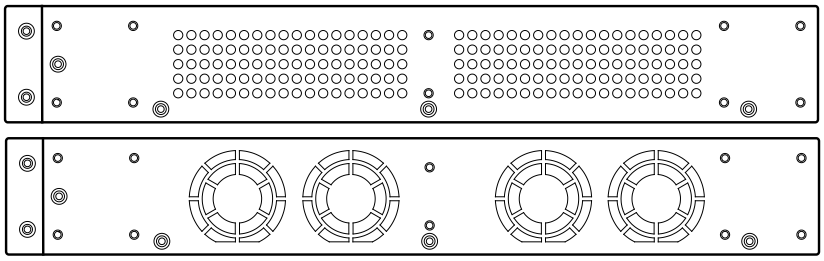


図 1-8　側面パネル図

SFP ポート

スイッチは SFP ポートを搭載しており、光ファイバケーブルに接続するフルデュプレックス転送、オートネゴシエーションをサポートする SFP ポートと共に使用されて、ギガビットネットワークをまたがる各種スイッチにアップリンクすることができます。SFP ポートは最大 1Gbps の転送速度をサポートしています。

以下に、スイッチに SFP ポートモジュールを挿入した例を図に示します。

注意 前面パネルの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。

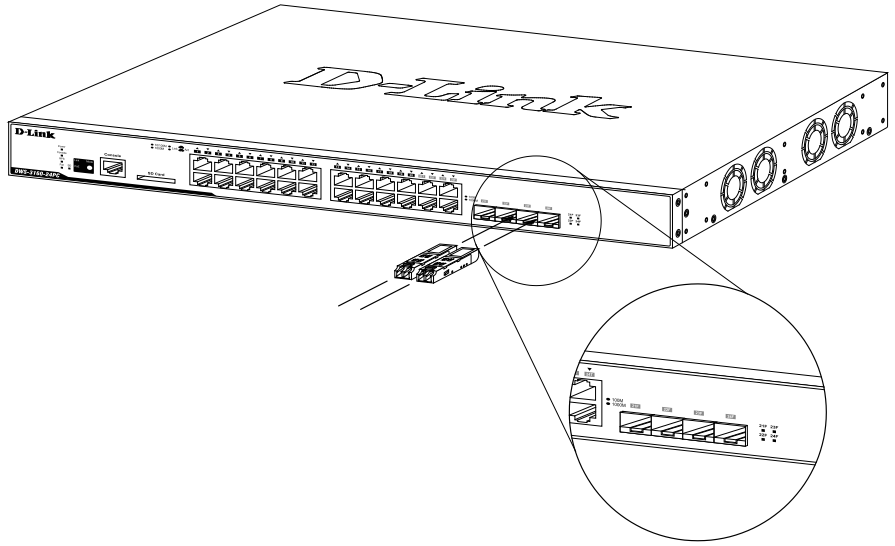


図 1-9　DWS-3160 シリーズ前面パネルの SFP ポートへのモジュールの挿入

第 2 章　スイッチの設置

- パッケージの内容
- ネットワーク接続前の準備
- ゴム足の取り付け（19 インチラックに設置しない場合）
- 19 インチラックへの取り付け
- 電源の投入
- リダンダント電源システムの設置

パッケージの内容

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

- 本体　x　1
- AC 電源ケーブル　x　1
- 電源抜け防止金具 x 1（DWS-3160-24PC には同梱されていません。）
- ラックマウントキット 1 式（ブラケット 2 枚、ネジ）
- ゴム足 (貼り付けタイプ)　x　4
- CD-ROM
- RS-232C/RJ-45 コンソールケーブル
- クイックインストールガイド
- シリアルラベル
- 製品保証書

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

ゴム足の取り付け (19 インチラックに設置しない場合)

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

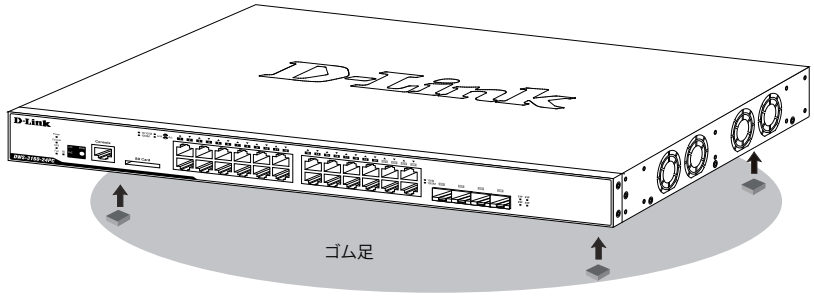


図 2-1　机や棚の上に設置する場合の準備

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。

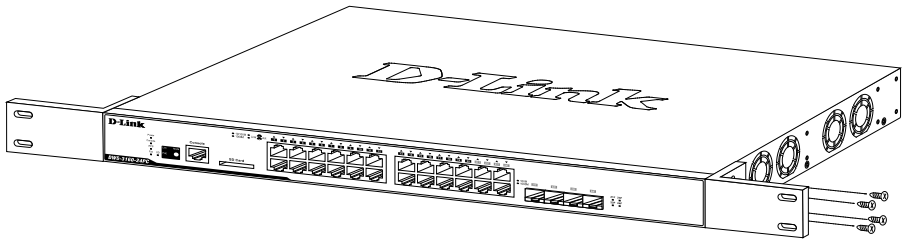


図 2-2　スイッチへのブラケットの取り付け図

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。

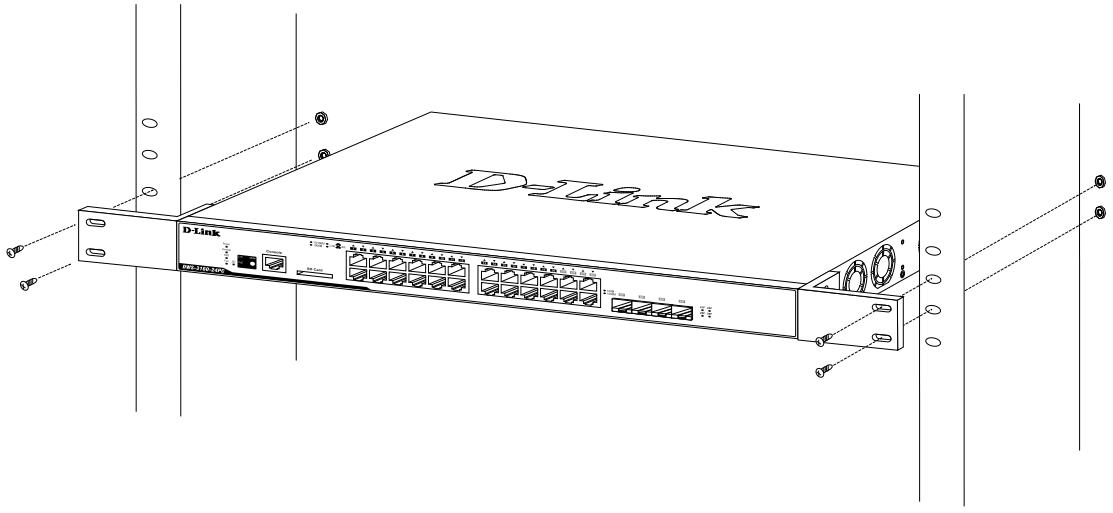


図 2-3　スイッチのラックへの設置図

電源の投入

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

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。

リダンダント電源システムの設置

DWS-3160-24TC および DWS-3160-24PC はリダンダント電源機能をサポートしています。DPS-200 および DPS-700 は必要な電力を供給するリダンダント電源ユニットであり、DPS-200 は DWS-3160-24TC、DPS-700 は DWS-3160-24PC に対応しています。また、DPS-200 は DPS-800 または DPS-900 に取り付けることができます。

本スイッチへリダンダント電源ユニットを接続する手順は以下の通りです。

警告 DPS-200 および DPS-700 の設置を行う前に、スイッチの AC 電源ケーブルを抜いておいてください。また、はじめに必ず電源ケーブルとコネクタの仕様書および設定手順をご確認ください。

警告 フロントおよびサイド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。ラックにシステムの搭載を行う前には、必ずスタビライザを装着してください。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。

DPS-200

DPS-200 は DWS-3160-24TC に対応しています。DPS-200 のマスタスイッチへの接続は、14 ピンの DC 電源ケーブルを使用して行います。標準の三極の AC 電源ケーブルでリダンダント電源装置とメイン電源を接続します。

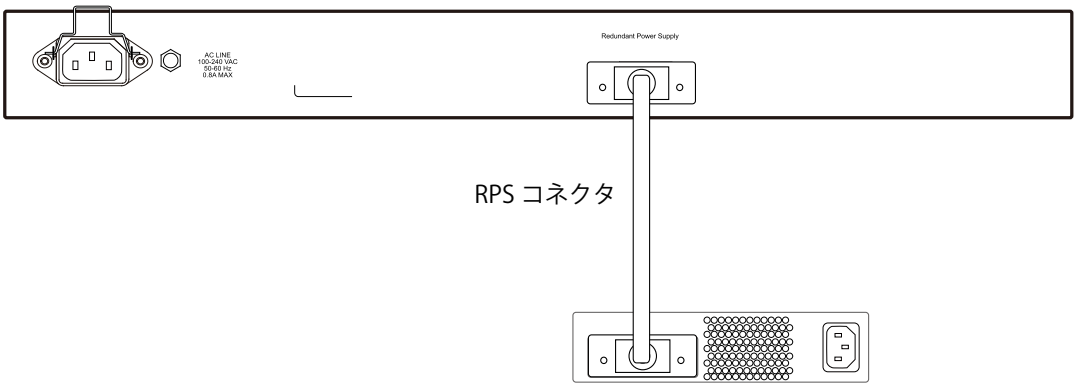


図 2-4　DWS-3160-24TC と DPS-200 RPS の接続

1. 14 ピン DC 電源ケーブルの一端をスイッチのソケットに挿入し、もう一端をリダンダント電源装置に挿入します。
2. 標準の AC 電源ケーブルでリダンダント電源装置とメインの AC 電源を接続します。DPS-200 前面の緑の LED 点灯により、正しく接続が行われたことが確認できます。
3. スイッチを再び AC 電源に接続します。RPS LED が点灯してリダンダント電源が動作していることを確認できます。
4. 本手順の実行による設定変更は必要ありません。

警告 DWS-3160-24TC に DPS-200 以外のリダンダント電源ユニットを使用しないでください。

注意 さらに詳細な情報については DPS-200 のマニュアルをご参照ください。

DPS-800

DPS-800 は標準サイズのラックマウント（1U サイズ）です。2 台までの DPS-200 を収容できます。

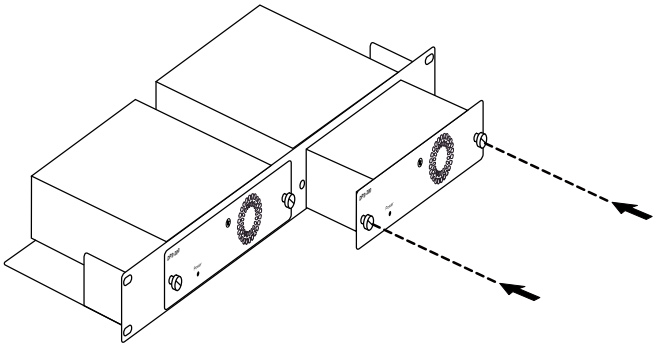


図 2-5　DPS-200 を DPS-800 に取り付ける

リダンダント電源システムは標準 19 インチラックにも取り付けることができます。以下の図を参照してください。

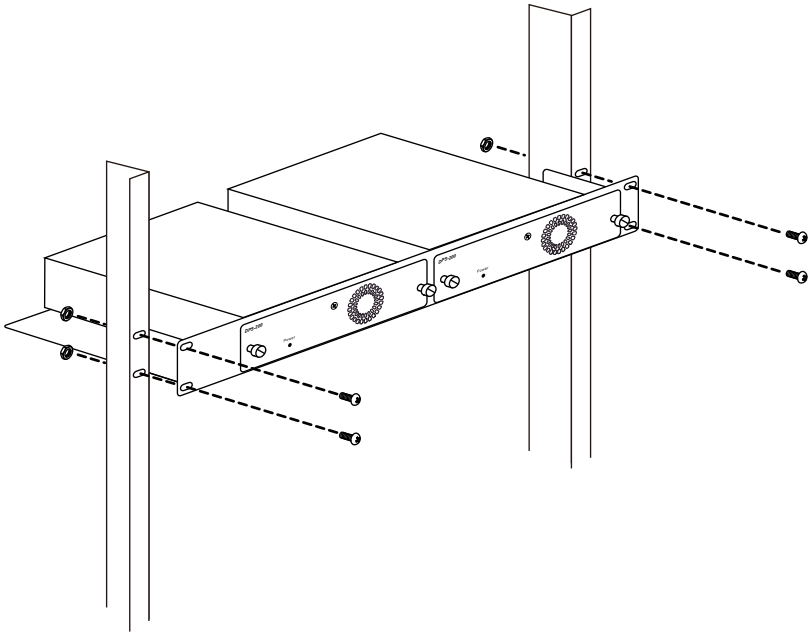


図 2-6　DPS-800 をラックに取り付ける

DPS-900

DPS-900 は標準サイズのラックマウント（5U サイズ）です。8 台までの DPS-200 を収容できます。

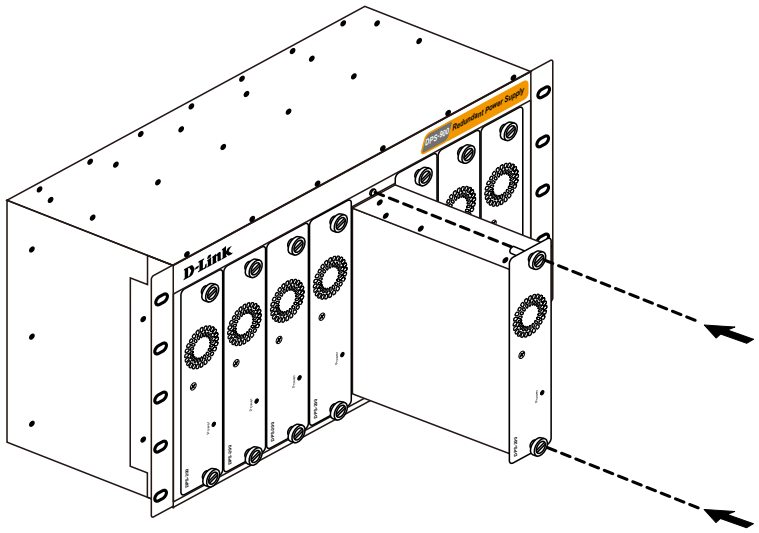


図 2-7　DPS-200 を DPS-900 に取り付ける

リダンダント電源は、標準 19 インチラックにも取り付けることができます。以下の図を参照してください。

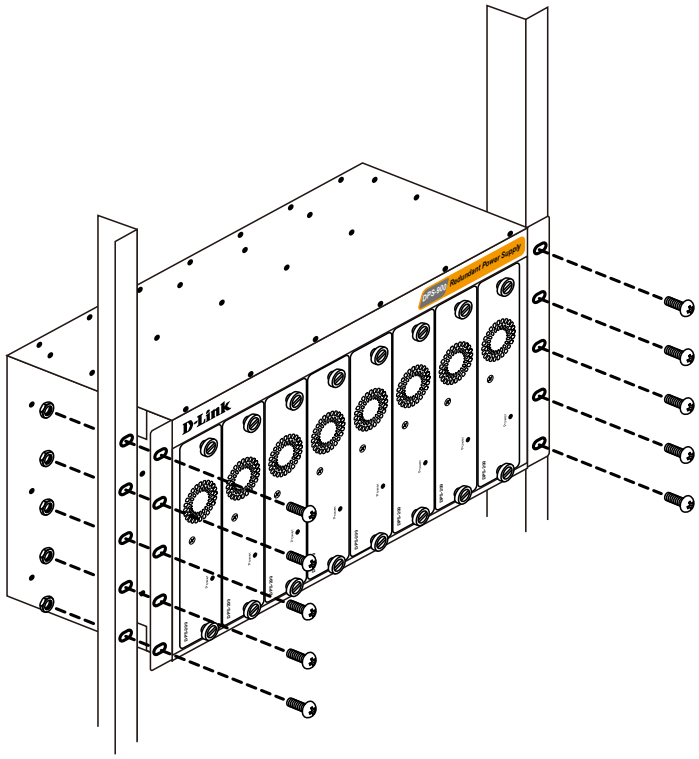


図 2-8　　DPS-900 をラックに取り付ける

DPS-700

DWS-3160-24PC は DPS-700 外部リダンダント電源ユニットに対応しています。

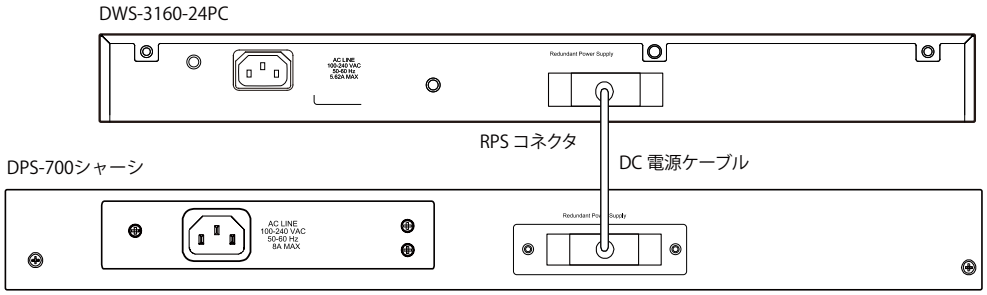


図 2-9　DPS-700 と DWS-3160-24PC の接続

初めて DPS-700 をスイッチに接続するために、以下の手順を行います。

1. スイッチの電源コネクタから電源ケーブルを抜いてください。
2. 22 ピン DC 電源ケーブルの一端をスイッチのソケットに挿入し、もう一端を DPS-700 の RPS ポートに挿入します。
3. 標準の AC 電源ケーブルで DPS-700 とメインの AC 電源を接続します。DPS-700 の前面にある緑の LED 点灯により、正しく接続が行われたことが確認できます。
4. スイッチを再び AC 電源に接続します。スイッチの LED が点灯し、リダンダント電源が動作していることを確認できます。
5. 本設置にはソフトウェア設定は必要ありません。

注意　さらに詳細な情報については DPS-700 のマニュアルをご参照ください。

警告　DWS-3160-24PC に DPS-700 以外のリダンダント電源を使用しないでください。

リダンダント電源システムは標準 19 インチラックにも取り付けることができます。以下の図を参照してください。

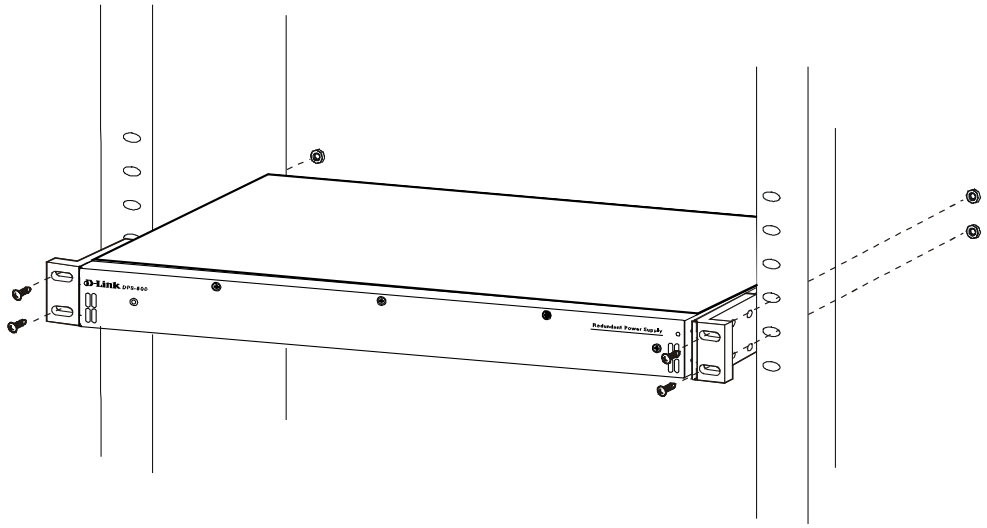


図 2-10　DPS-700 をラックに取り付ける

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
- アクセスポイントと接続する

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

エンドノードとは、スイッチに接続するエッジのネットワークデバイスの総称で、典型的な例は、パーソナルコンピュータ（PC）、ノート PC、アクセスポイント、プリントサーバ、および VoIP 電話などです。本スイッチの 10/100/1000Mbps RJ-45 ネットワークポートとエンドノードを接続します。エンドノードとスイッチ間はカテゴリ 3、4、 5、または 5e 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。

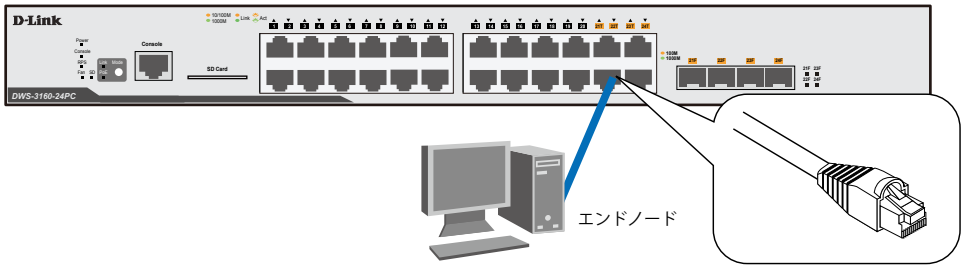


図 3-1　エンドノードと接続した図

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

ハブまたはスイッチと接続する

以下のネットワークの図は、スイッチにネットワーク内のすべてのエンドノードに提供するポート数が十分にない場合を想定しています。
スイッチ同士を接続するのに使用できるケーブルタイプには柔軟性があります。Copper ポートは、10BASE-T、100BASE-TX、および 1000BASE-T に準拠して動作するカテゴリ 3、4、5 および 5e ケーブルをサポートしています。また、スイッチの SFP ポート経由で光ファイバケーブルを使用して、2 つ以上のスイッチを接続できます。

使用するケーブルによって以下のように接続します。

- カテゴリ 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 ポート経由で光ファイバをサポートするスイッチにアップリンクする。

ケーブル仕様については「付録 H ケーブルとコネクタ」（560 ページ）を参照してください。

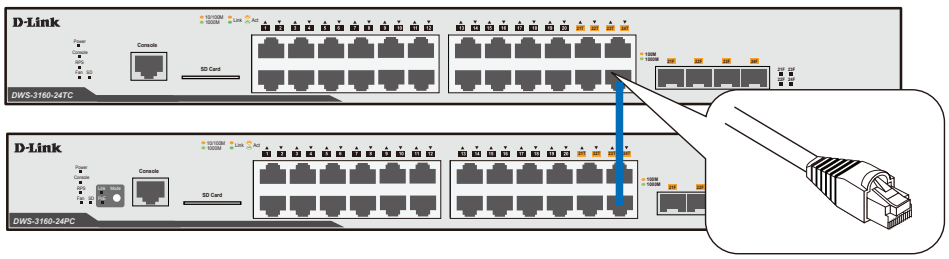


図 3-2　ストレート、クロスケーブルでハブまたはスイッチと接続する図

バックボーンまたはサーバと接続する

ネットワークを構築する場合、本スイッチに 1 つまたは 2 つのサーバを接続する必要があります。本スイッチのどのポートも、最大 1Gbps の速度で動作するため、サーバに接続することができます。

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。

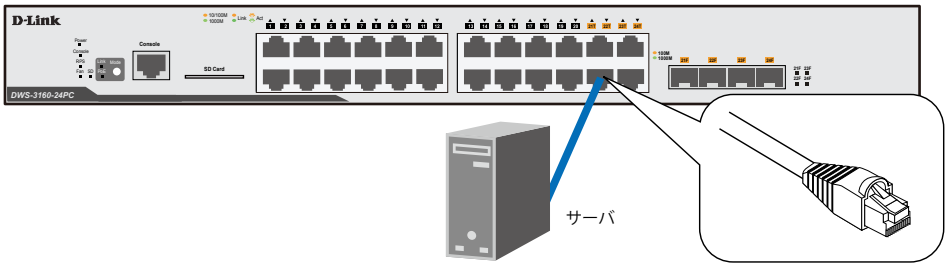


図 3-3　サーバ、PC、スイッチとのアップリンク接続図

アクセスポイントと接続する

スイッチは管理、設定およびモニタする無線アクセスポイント（DWL-8600AP、DWL-3600AP、および DWL-6600AP）に接続するのに使用されます。これらのアクセスポイントを「Standalone」または「Managed」アクセスポイントとして設定することができます。スイッチが管理する「Managed」アクセスポイントとして設定することで、統合システムが最適な性能と柔軟性をもって機能することができます。

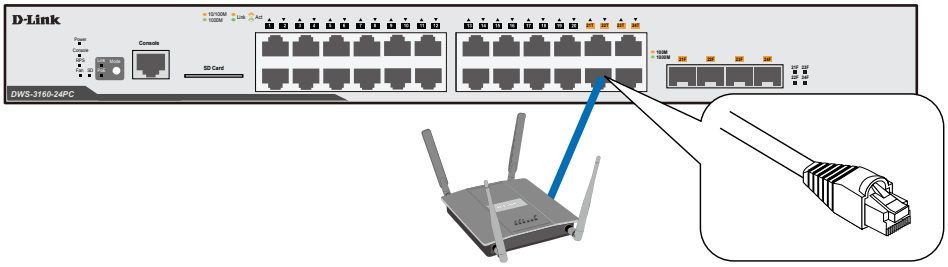


図 3-4　アクセスポイントとの接続図

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
- 管理ポートへの接続
- ユーザアカウント設定
- IP アドレスの割り当て
- SNMP を使用した設定

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）、Mozilla Firefox（バージョン 2.0 以上）、Safari（バージョン 4.0 以上）、および Google Chrome（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。

- シリアルポートまたはリモートの Telnet 経由のコマンドラインインタフェース管理
  スイッチのモニタリングと設定のために RJ-45 シリアルポートを搭載しています。
  コンソールポートを使用するためには以下をご用意ください。

  - ターミナルソフトを操作するシリアルポート搭載の端末またはコンピュータ
  - 同梱のコンソールケーブル（D-Sub9 ピン オスコネクタ / RJ-45 コネクタ）を使用して接続します。

端末をコンソールポートに接続する

1. 本製品付属の RS-232C ケーブルの RJ-45 コネクタをスイッチの RJ-45 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「115200」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。

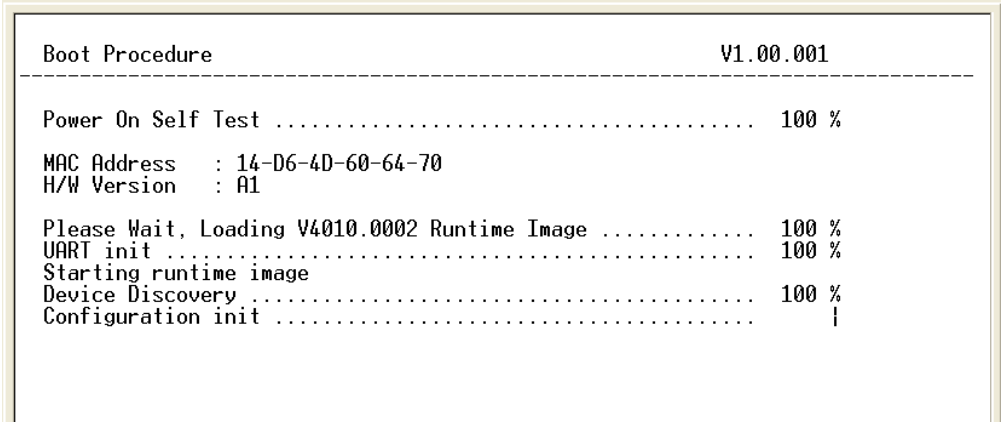


図 4-1　コンソールのブート画面

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「DWS-3160 Series CLI Reference Guide」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。

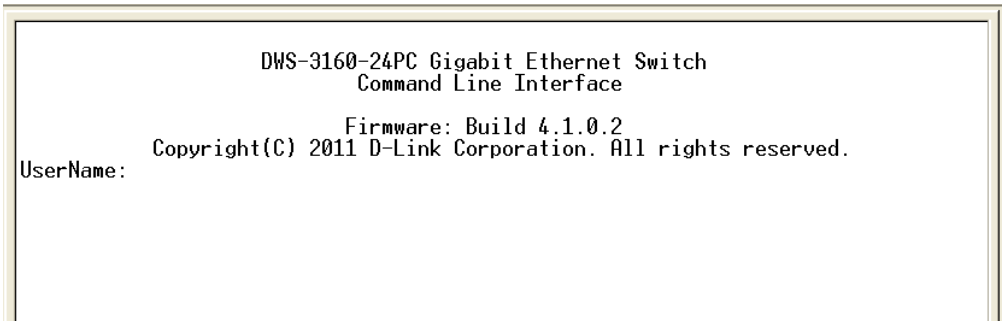


図 4-2　コマンドプロンプト

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。
「DWS-3160-24xx:admin#」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。

ユーザアカウント設定

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ユーザ名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「NewUser」を指定する手順の例です。

```
                    DWS-3160-24PC Gigabit Ethernet Switch
                            Command Line Interface

                                Firmware: Build 4.1.0.2
          Copyright(C) 2011 D-Link Corporation. All rights reserved.
UserName:
PassWord:

DWS-3160-24PC:admin#create account admin NewUser
Command: create account admin NewUser

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

DWS-3160-24PC:admin#
```

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。

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。

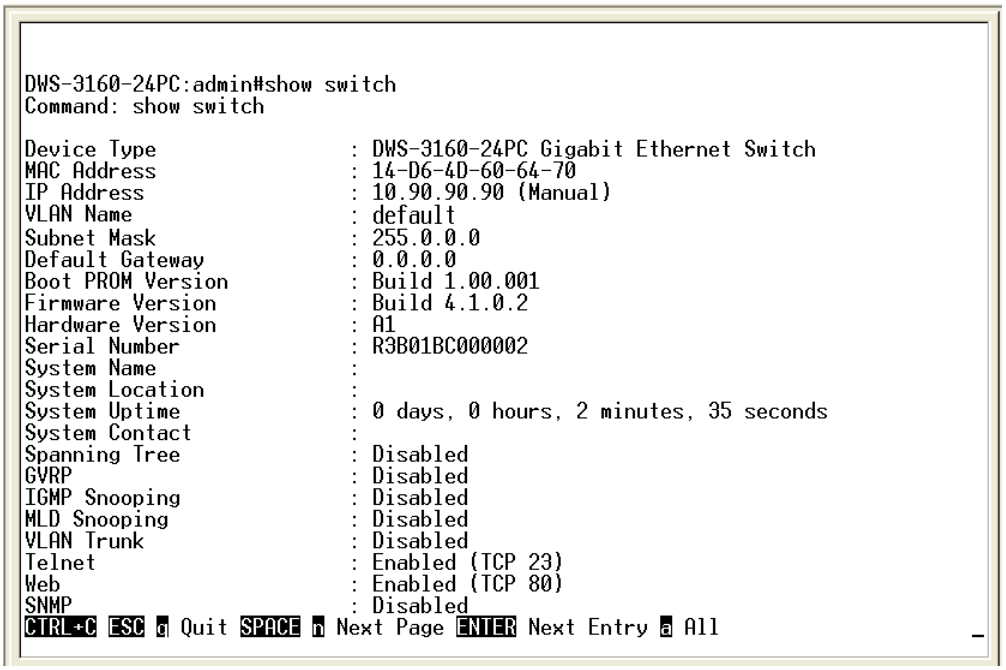


図 4-3　show switch コマンドによる表示画面

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」および「System 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。

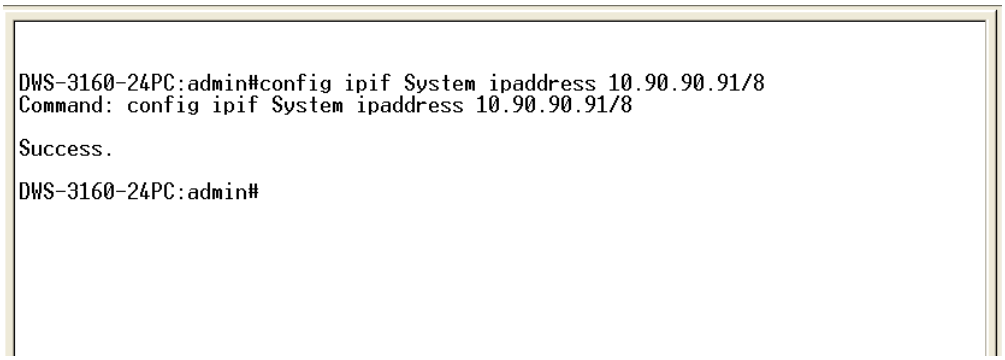


図 4-4　スイッチへの IP アドレス割り当て時の表示画面

上記例では、スイッチに IP アドレス「10.90.90.91」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（10.90.90.91/8）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。

SNMP を使用した設定

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のために設計されています。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。

プロフェッショナルネットワーク管理ソフトウェアのパッケージである「D-View」を使用して、本スイッチの設定、管理、モニタを行うことができます。D-View® 6.0 SNMP ネットワーク管理システムは、様々な SNMP が有効であるデバイスが属するネットワークにおいて中央管理を容易にするソフトウェアツールです。

1. D-Link D-View SNMP ソフトウェア

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）の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、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。

SNMPv1 と SNMPv2c 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、そのパケットは無視（廃棄）されます。

SNMPv1 と SNMPv2c 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。

```
DWS-3160-24PC:admin#show snmp community
Command: show snmp community

SNMP Community Table
Community Name                  View Name                       Access Right
------------------------------  ------------------------------  ------------
private                         CommunityView                   read_write
public                          CommunityView                   read_only

Total Entries: 2

DWS-3160-24PC:admin#_
```

図 4-5　SNMP コミュニティ名の参照

SNMP v3 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。

1. 最初のパートは SNMP マネージャとして動作することのできるユーザとその属性を掲載したリストを保持しています。
2. 次のパートではリスト上の各ユーザの 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「SNMPv1 を使用して読み取り専用の情報とトラップの受信のみを可能にするグループ」や「SNMPv3 を使用して高いセキュリティレベルを与え、読み書き可能にするグループ」を登録することができます。

個別のユーザや SNMP マネージャグループに SNMPv3 を使用すると、特定の SNMP 管理機能を許可または制限できるようになります。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。SNMPv3 では SNMP メッセージを暗号化することにより、さらに強固なセキュリティレイヤを実現できます。

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（Management Information Base）には管理情報およびカウンタ情報が格納されています。本スイッチは標準 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。

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 ベースのユーザインタフェース
- ユーザインタフェースの各エリア
- Web ページの構成

Web ベースの管理について

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

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

Web マネージャへのログイン

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

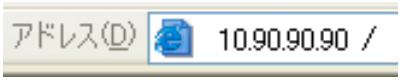


図 5-1　URL の入力

注意　工場出荷時設定では IP アドレス「10.90.90.90」、サブネットマスク「255.0.0.0」が設定されています。端末側の IP インタフェースを本スイッチにあわせるか、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。

以下のユーザ認証画面が表示されます。

図 5-2　パスワード入力用画面

「ユーザー名」欄と「パスワード」欄を空白のまま「OK」をクリックし、Web ベースユーザインタフェースに接続します。Web ブラウザによって使用可能な機能を以下で説明します。
CLI でユーザ名、パスワードを既に設定している場合は、設定したパラメータを入力します。

Web マネージャの画面構成

Web マネージャによるスイッチの設定または管理画面にアクセス、および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。

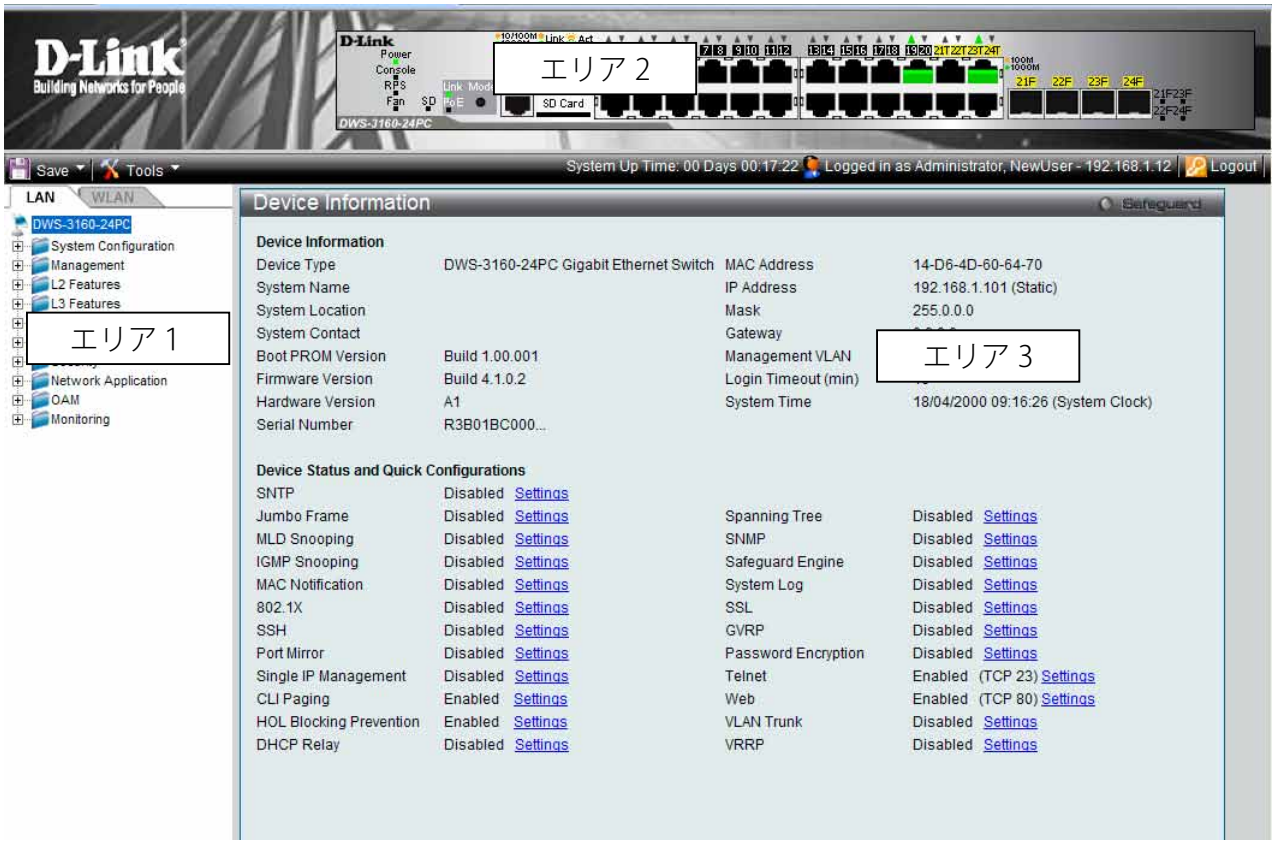


図 5-3　Web マネージャのメインページ

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。フォルダアイコンを開き、ハイパーリンクしたメニューボタンの表示、および格納するサブフォルダの表示ができます。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　現在のセッション中にスイッチのコンフィグレーションに行った変更は、「Save Configuration / Log」画面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を次に説明します。

メインメニュー	サブメニュー	説明	参照ページ
LAN タブ			
System Configuration	Device Information	スイッチの主な設定情報を表示します。	50
	System Information Settings	スイッチの基本情報を表示します。	51
	Port Configuration	ポート設定、ジャンボフレーム設定などを行います。以下のメニューがあります。 Port Settings、Port Description Settings、Port Error Disabled)、Jumbo Frame	52
	PoE Configuration (DWS-3160-24PC)	PoE システムの設定を行います。以下のメニューがあります。 PoE System Settings、PoE Port Settings	55
	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。	57
	Warning Temperature Settings	システムの警告温度パラメータを設定します。	57
	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。以下のメニューがあります。 System Log Settings、System Log Server Settings、System Log、System Log & Trap Settings、System Severity Settings	58
	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。	61
	Port Group Settings	ポートグループを作成します。	62
	Time Settings	スイッチに時刻を設定します。	62
	User Accounts Settings	ユーザおよびユーザの権限を設定します。	63
	Command Logging Settings	コマンドログ設定を有効または無効にします。	64
Management	ARP	スタティック ARP、プロキシ ARP 、ARP テーブルを設定します。次のメニューがあります。 Static ARP Settings、Proxy ARP Settings、ARP Table	66
	Gratuitous ARP	Gratuitous ARP の設定をします。次のメニューがあります。 Gratuitous ARP Global Settings、Gratuitous ARP Settings	69
	IPv6 Neighbor Settings	IPv6 Neighbor の設定を行います。	71
	IP Interface	スイッチの IP インタフェース設定を行います。次のメニューがあります。 System IP Address Settings、Interface Settings	72
	Management Settings	CLI ページング、DHCP 自動設定、省電力モードなどの管理設定を行います。	76
	Session Table	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。	77
	Single IP Management	シングル IP マネジメント機能を設定します。次のメニューがあります。 Single IP Settings、Firmware Upgrade、Configuration File Backup/ Restore、Upload Log File	78
	SNMP Settings	SNMP 設定を行います。次のメニューがあります。 SNMP Global Settings、SNMP Trap Settings、SNMP Link Change Traps Settings、SNMP View Table Settings、SNMP Community Table Settings、SNMP Group Table Settings、SNMP Engine ID Settings、SNMP User Table Settings、SNMP Host Table Settings、SNMP v6Host Table Settings、RMON Settings	87
	Telnet Settings	スイッチに Telnet 設定をします。	95
	Web Settings	スイッチに Web ステータスを設定します。	95
L2 Features	VLAN	802.1Q スタティック VLAN 設定を行います。以下のメニューがあります。 802.1Q VLAN Settings、802.1v Protocol VLAN、Asymmetric VLAN Settings、GVRP、MAC-based VLAN Settings、Private VLAN Settings、PVID Auto Assign Settings、Voice VLAN、VLAN Trunk Settings、Browse VLAN、Show VLAN Ports	102
	QinQ	Q-in-Q 機能を「Enabled」(有効) または「Disabled」(無効) にします。次のメニューがあります。 QinQ Settings、VLAN Translation Settings	118
	Spanning Tree	スパニングツリープロトコルの設定を行います。以下のメニューがあります。 STP Bridge Global Settings、STP Port Settings、MST Configuration Identification、STP Instance Settings、MSTP Port Information	121
	Link Aggregation	ポートトランキング設定を行います。以下のメニューがあります。 Port Trunking Settings 、LACP Port Settings	130
	FDB	スタティック FDB、MAC アドレスエージングタイム、MAC アドレステーブルなどを設定します。以下のメニューがあります。 Static FDB Settings、MAC Notification Settings、MAC Address Aging Time Settings、MAC Address Table、ARP & FDB Table	133

メインメニュー	サブメニュー	説明	参照ページ
L2 Features	L2 Multicast Control	IGMP Snooping、MLD Snooping の設定を行います。以下のメニューがあります。 IGMP Snooping、IGMP Host Table、MLD Snooping、MLD Host Table、Multicast VLAN	138
	Multicast Filtering	マルチキャストフィルタリングの設定を行います。以下のメニューがあります。 IPv4 Multicast Filtering、IPv6 Multicast Filtering、Multicast Filtering Mode	161
	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。	170
	LLDP	LLDP 設定を行います。 LLDP Global Settings、LLDP Port Settings、LLDP Management Address List、LLDP Basic TLVs Settings、LLDP Dot1 TLVs Settings（LLDP Dot1 TLV 設定）、LLDP Dot3 TLVs Settings、LLDP Statistics System、LLDP Local Port Information、LLDP Remote Port Information	173
	NLB FDB Settings	NLB 機能を設定します。	181
L3 Features	IPv4 Static/Default Route Settings	IPv4 スタティック / デフォルトルートの設定を行います。	182
	IPv4 Route Table	IPv4 ルーティングテーブルの外部経路情報を参照します。	183
	IPv6 Static/Default Route Settings	IPv6 スタティック / デフォルトルートの設定を行います。	183
	IP Forwarding Table	直接接続するすべての IP 情報を参照します。	184
	VRRP	VRRP リレーの設定を行います。次のメニューがあります。 VRRP Global Settings、VRRP Virtual Router Settings、VRRP Authentication Settings	185
QoS	802.1p Settings	ポート単位にプライオリティを割り当てます。以下のメニューがあります。 802.1p Default Priority Settings（ポートへのパケットプライオリティの割り当て）、802.1p User Priority Settings（802.1p ユーザプライオリティ）	191
	Bandwidth Control	送信と受信のデータレートを制限します。以下のメニューがあります。 Bandwidth Control Settings、Queue Bandwidth Control Settings	192
	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。	194
	DSCP	ポートの DSCP トラスト状態の設定および DSCP マッピング設定を行います。以下のメニューがあります。 DSCP Trust Settings、DSCP Map Settings	196
	HOL Blocking Prevention	HOL ブロッキング防止機能を「Enabled」（有効）または「Disabled」（無効）にします。	197
	Scheduling Settings	QoS スケジューリングを設定します。以下のメニューがあります。 Scheduling Profile Settings、Scheduling Group Settings	198
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。	200
	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。	202
	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。	219
	ACL Finder（ACL 検索）	ACL エントリを検索します。	235
	ACL Flow Meter	フローごとの帯域幅制御設定を行います。	236
	Egress Access Profile List	フローごとのパケット処理を実行します。	240
	Egress ACL Flow Meter	Egress アクセスプロファイルおよびルールに基づいてパケットフローベースのメータリングを設定します。	253
Security	802.1X	802.1X 認証を設定します。以下のメニューがあります。: 802.1X Global Settings、802.1X Port Settings、802.1X User Settings、Guest VLAN、Authenticator State、Authenticator Statistics、Authenticator Session Statistics、Authenticator Diagnostics、Initialize Port(s)、Reauthenticate Port(s)	257
	RADIUS	RADIUS サーバの設定を行います。以下のメニューがあります。 Authenticatio257n RADIUS Server Settings、RADIUS Accounting Setting、RADIUS Authentication、RADIUS Account Client	270
	IP-MAC-Port Binding	IP アドレス、MAC アドレスおよびポートを結合し、レイヤ間通信を行います。以下のメニューがあります。 IMPB Global Settings、IMPB Port Settings、IMPB Entry Settings、MAC Block List、DHCP Snooping、DHCP Snooping Entries	274
	MAC Based Access Control	MAC アドレス認証機能を設定します。以下のメニューがあります。 MAC-based Access Control Settings、MAC-based Access Control Local Settings、MAC-based Access Control Authentication State	279
	Compound Authentication	コンパウンド認証方式を設定します。以下のメニューがあります。 Compound Authentication Settings、Compound Authentication Guest VLAN Settings	283

メインメニュー	サブメニュー	説明	参照ページ
Security	Port Security	ダイナミックな MAC アドレス学習をロックします。以下のメニューがあります。 Port Security Settings、Port Security VLAN Settings、Port Security Entries	285
	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。	289
	BPDU Attack Protection	ポートに BPDU 防止機能を設定します。	290
	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。	291
	Traffic Segmentation Settings	ポートのトラフィックフローを制限します。	292
	NetBIOS Filtering Setting	NetBIOS フィルタ設定を行います。	293
	DHCP Server Screening	不正な DHCP サーバへのアクセスを拒否します。以下のメニューがあります。 DHCP Server Screening Port Settings、DHCP Offer Permit Entry Settings	294
	Access Authentication Control	TACACS/XTACACSTACACS+/RADIUS 認証の設定を行います。以下のメニューがあります。 Enable Admin、Authentication Policy Settings、Application Authentication Settings、Authentication Server Group Settings、Authentication Server Settings、Login Method Lists Settings、Enable Method Lists Settings、Local Enable Password Settings	296
	SSL Settings	証明書の設定、暗号スイートの設定を行います。	304
	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。以下のメニューがあります。: SSH Settings、SSH Authentication Method and Algorithm Settings、SSH User Authentication Lists	306
	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。	309
	Safeguard Engine Setting	セーフガードエンジンの設定を行います。	310
	Captive Portal	有線 / 無線ユーザ両方についてネットワークへの接続性を制御します。以下のメニューがあります。: CP Configuration、CP Web ページのカスタマイズ、Local User、Interface Association、CP Status、Interface Status、Client Connection Status、SNMP Trap Configuration	312
Network Application	DHCP	DHCP リレーの設定を行います。以下のメニューがあります。 DHCP Relay、DHCP Local Relay Settings	329
	SNTP	本製品に時刻設定をします。以下のメニューがあります。 SNTP Settings、Time Zone Settings	336
	Flash File System Settings	フラッシュファイルシステムを利用したファイル操作を行います。	338
OAM	CFM	CFM 機能を設定します。以下のメニューがあります。 CFM Settings、CFM Port Settings、CFM MIPCCM Table、CFM Loopback Settings、CFM Linktrace Settings、CFM Packet Counter、CFM Fault Table、CFM MP Table	341
	Ethernet OAM	ポートにイーサネット OAM モード、イベント、ログを設定します。以下のメニューがあります。 Ethernet OAM Settings、Ethernet OAM Configuration Settings、Ethernet OAM Event Log、Ethernet OAM Statistics	353
	Cable Diagnostics	ケーブル診断を行います。	356
Monitoring	Utilization	CPU 使用率、ポートの帯域使用率を表示します。次のメニューがあります。 CPU Utilization、DRAM & Flash Utilization、Port Utilization	357
	Statistics	パケット統計情報とエラー統計情報を表示します。次のメニューがあります。 Packets、Errors、Packet Size	359
	Mirror	ポートミラーリングの設定を行います。次のメニューがあります。 Port Mirror Settings、RSPAN Settings	368
	sFlow	sFlow 機能の設定を行います。次のメニューがあります。 sFlow Global Settings、sFlow Analyzer Server Settings、sFlow Flow Sampler Settings、sFlow Counter Poller Settings	370
	Ping Test	IPv4 アドレスまたは IPv6 アドレスに Ping することができます。	374
	Trace Route	ネットワーク上のスイッチとホスト間の経路をトレースします。	375
	Peripheral	デバイス環境機能はスイッチの内部温度ステータスを表示します。	376

メインメニュー	サブメニュー	説明	参照ページ
WAN タブ			
Security	Captive Portal	有線 / 無線ユーザ両方についてネットワークへの接続性を制御します。以下のメニューがあります。 CP Configuration、CP Web ページのカスタマイズ、Local User、Interface Association、CP Status、Interface Status、Client Connection Status、SNMP Trap Configuration	378
Monitoring	Global	スイッチや接続するデバイスの状況や統計情報をモニタします。	395
	Peer Switch	ネットワーク上の他の D-Link 統合スイッチの情報を参照します。次のメニューがあります。 Status、Configuration、Managed AP	403
	Access Point	検出したすべてのアクセスポイントの状態（管理下、接続失敗、不正等）を確認します。次のメニューがあります。 All AP Status、Managed AP Status、AP Authentication Failure Status、AP RF Scan Status、AP De-Authentication Attack Status	406
	Client	スイッチ管理対象のアクセスポイントが接続中の無線クライアントについて、さまざまな情報を参照します。次のメニューがあります。: Associated Clients、Detected Clients、Ad Hoc Clients	427
	QoS	アクセスコントロールリストおよび DiffServ に関する情報を表示します。次のメニューがあります。 Access Control Lists、Differentiated Services	445
Administration	Basic Setup	D-Link 統合スイッチに設定するアクセスポイントプロファイル、無線ネットワーク、およびローカルアクセスポイント・データベースについて説明します。次のメニューがあります。	452
	AP Management	無線インタフェースを設定します。次のメニューがあります。 AP Reboot 、RF Management、Software Downloads、Advanced Settings、AP Provisioning	464
	Advanced Configuration	各アクセスポイントにチャンネルや RF 信号送信電力レベルを指定します。また、AP モード、ローカル認証パスワード、アクセスポイントが使用するプロファイルを設定します。次のメニューがあります。 Global、Networks、AP Profiles、Peer Switch、WIDS Security、Clients、Switch Provisioning	473
QoS	Access Control Lists	トラフィックを定義済みのホップ単位の動作に基づいてストリームに分類して、特定の QoS 処理を行います。次のメニューがあります。 IP Access Control Lists、IPv6 Access Control Lists、MAC Access Control Lists	498
	Differentiated Services	CoS 設定を行います。次のメニューがあります。 Diffserv Configuration、Class Configuration、Policy Configuration、Policy Class Definition	511
Network Visualization	Download Image	WLAN 視覚化グラフ用画像をダウンロードします。	517
	Launch…	WLAN 視覚化アプリケーションの起動、メニューバーについて説明します。	518

第 6 章　D-Link 統合アクセスシステム

- D-Link 統合アクセスシステム構成
- D-Link 統合アクセスシステムのトポロジ

D-Link 統合アクセスシステムは、最新鋭の無線ネットワーク機能を実現しながら WLAN（無線 LAN）の展開を可能にします。さらに確実な接続性と、シームレスなレイヤ 2 とレイヤ 3 ローミングをエンドユーザに提供する拡張可能なソリューションです。

D-Link 統合アクセスシステム構成

D-Link 統合アクセスシステムのコンポーネントは D-Link 統合スイッチと D-Link アクセスポイント（AP）構成されます。

ご購入時、デフォルトでこのスイッチは 12 台までの統合アクセスポイントを管理することができます。D-Link から別途ライセンスをご購入いただき、アクティベーションすることで、統合スイッチ 1 台あたり 40 台までの統合アクセスポイントを管理することができます。本スイッチの最大の特徴は、4 台までのスイッチがクラスタを形成し、単一の IP アドレスで最大 192 台の統合アクセスポイントを集中管理できるということです。

本システムは配下にあるすべての WLAN のトラフィックとデバイスの状態および統計情報を追跡記録します。4 台までのピア統合スイッチを構成し、アクセスポイントと配下にある無線クライアントの様々な情報を共有することができます。ピア統合スイッチ同士は、直接接続したり、レイヤ 2 ブリッジによって分割したり、また異なる IP サブネットに所属することができます。また、無線クライアントは、アクセスポイント間を移動することができます。

D-Link 統合スイッチ

D-Link 統合スイッチは有線 LAN、無線 LAN の両方のトラフィックに対し、レイヤ 2+ のスイッチング機能を持っています。統合スイッチのユーザインタフェースを使用して、ネットワーク内のすべてのアクセスポイントについての設定、確認、およびデータの保守ができます。

統合スイッチは接続性の高いデータ経路の接続性、モビリティ制御、セキュリティ保護、無線・電力パラメータ制御、およびネットワークとネットワークエレメントの管理機能を提供します。また、不正 AP と不正クライアントの検出や状態を含むピア無線スイッチや D-Link アクセスポイント、また WLAN 上のクライアントの検出、確認、認証、および監視を行います。

D-Link 統合アクセスシステムでは以下のスイッチを使用できます。:

- DWS-3160-24TC
- DWS-3160-24PC

D-Link アクセスポイント

D-Link アクセスポイントは、2 つのモード（スタンドアロンモードまたは管理モード）のいずれかで動作します。

- スタンドアロンモードでは、D-Link アクセスポイントはネットワークで個々のアクセスポイントとして動作するため、管理者はアクセスポイントに接続して、Web ユーザインタフェース（UI）またはコマンドラインインタフェース（CLI）を使用することで管理します。

- 管理モードでは、D-Link アクセスポイントは D-Link 統合アクセスシステムの一部となり、D-Link 統合スイッチにより管理されます。アクセスポイントが管理モードの場合、アクセスポイントの管理者用 Web インタフェースは無効とされます。アクセスは Telnet を経由した CLI に制限されます。

スタンドアロンモードは 2,3 台のアクセスポイントを使用する小規模のネットワークに適しています。管理モードはどんな規模のネットワークにも使用できます。スタンドアロンモードで D-Link アクセスポイントの使用を開始しても、統合スイッチをネットワークに追加する際にその AP を管理モードに容易に移行することができます。管理モードでアクセスポイントを使用することにより、統合スイッチから配下のアクセスポイントに対しコンフィグレーションプロファイルの移行やソフトウェアアップグレードの指示が行われるため、アクセスポイント管理の集中化、アップグレードの効率化が実現できます。「Web UI Reference Guide」と「CLI Reference Guide」は主として「Managed」（管理）モードの D-Link アクセスポイントについて説明します。

D-Link 統合アクセスシステムは、以下の D-Link 製アクセスポイントと連携します。:

- DWL-3600AP
- DWL-8600AP
- DWL-6600AP

各アクセスポイントは各無線インタフェースにつき、16 個までの仮想アクセスポイント（VAP）をサポートします。VAP 機能により、各物理アクセスポイントを（無線インタフェース毎に）16 個の論理アクセスポイントに分割し、それぞれに異なる SSID、VLAN ID、およびセキュリティポリシーを持たせることができます。

WLAN の視覚化

D-Link 統合アクセスシステムが提供する WLAN 視覚化ツールを利用することにより、ユーザは Web ブラウザからご使用の無線ネットワークをグラフィカルに捉えることができます。WLAN 視覚化ツールは D-Link 統合スイッチ、D-Link アクセスポイント、他のアクセスポイントおよび D-Link アクセスポイントに接続する無線クライアントを検出し、表示することができます。現場の建物のレイアウトなどの情報をインポートし、ネットワークビューとしてカスタマイズすることも可能です。

以下の図では、フロアの見取り図および、D-Link 統合スイッチと配下の 2 台のアクセスポイントで構成するネットワークの例を示します。図には 1 組のピアスイッチと不正アクセスポイントも表示されています。

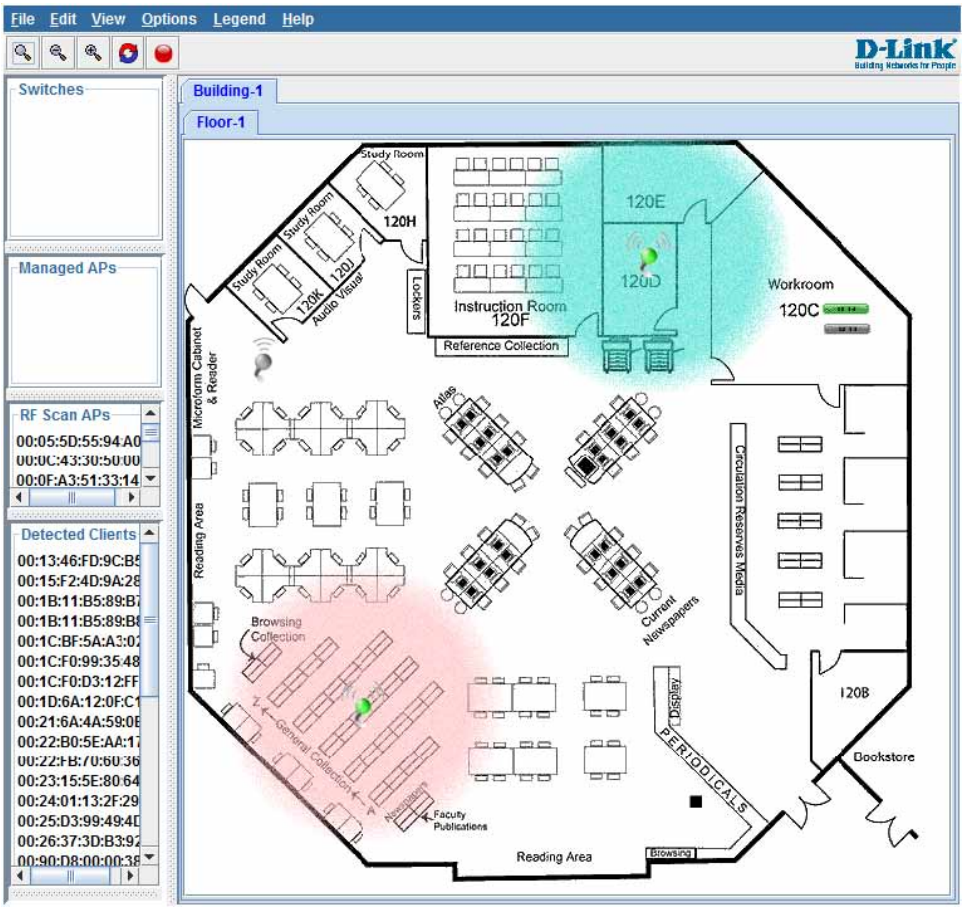


図 6-1　WLAN の視覚化

WLAN 視覚化ツールは、アクセスポイントの電波出力をチャンネルごとに色分けして表示するため、干渉を低減し、WLAN のカバー範囲を増強させるアクセスポイントの設置位置の決定などを補助します。

D-Link 統合アクセスシステムのトポロジ

WLAN のネットワークトポロジは、ご使用のネットワークの規模および要求事項によって異なります。小規模から中規模のネットワークでは、1 台の統合スイッチで少数の D-Link アクセスポイントを管理することができます。大規模なネットワークでは、無線クライアントによるローミングの機能がさらに必要となり、複数のピアスイッチを導入し、それぞれがアクセスポイントを管理します。

1 台の統合スイッチの設置

D-Link アクセスポイントを設置すると、D-Link 統合スイッチは自動的にアクセスポイントを検出し、自動 RF チャンネル選択や自動出力調整などを含むデフォルトプロファイルを適用します。

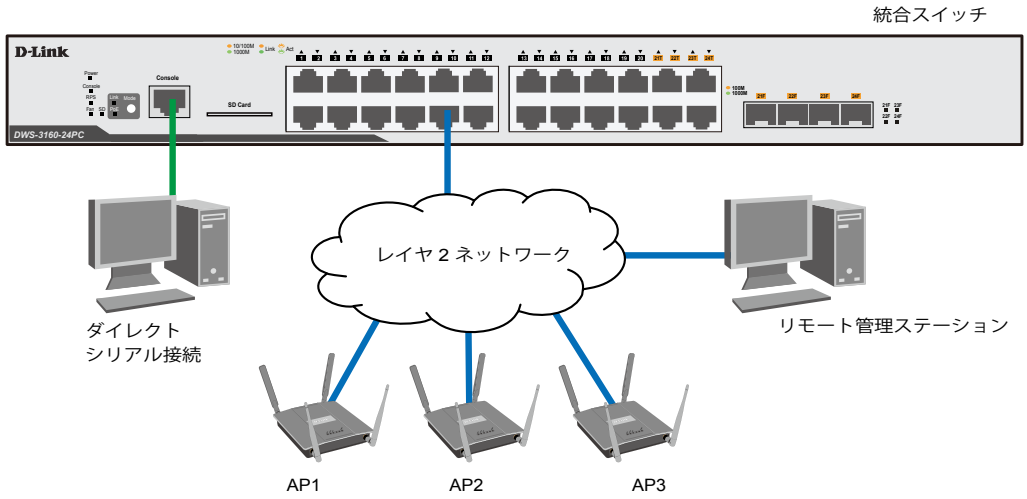


図 6-2　3 つのアクセスポイントを持つ 1 つの統合スイッチ

アクセスポイントが同じサブネットに属し、同じ SSID を持つ場合、無線クライアントはそれらの全アクセスポイント間でローミングを行い、途切れることなくネットワークにアクセスすることができます。その際、クライアントは同じ IP アドレスを使用し、異なるアクセスポイントのブロードキャストエリアに入るときも再認証の必要はありません。アクセスポイント間のコンフィグレーション変更は、スイッチが同時に、またはアクセスポイントごとに行います。

ピア統合スイッチの配置

規模の大きいネットワークを構築するためには、4 台のスイッチをピアとしてネットワークを構成することで WLAN の規模と無線通信範囲を増強することができます。統合スイッチと管理下にあるアクセスポイントは、同じサブネット内である必要はありません。

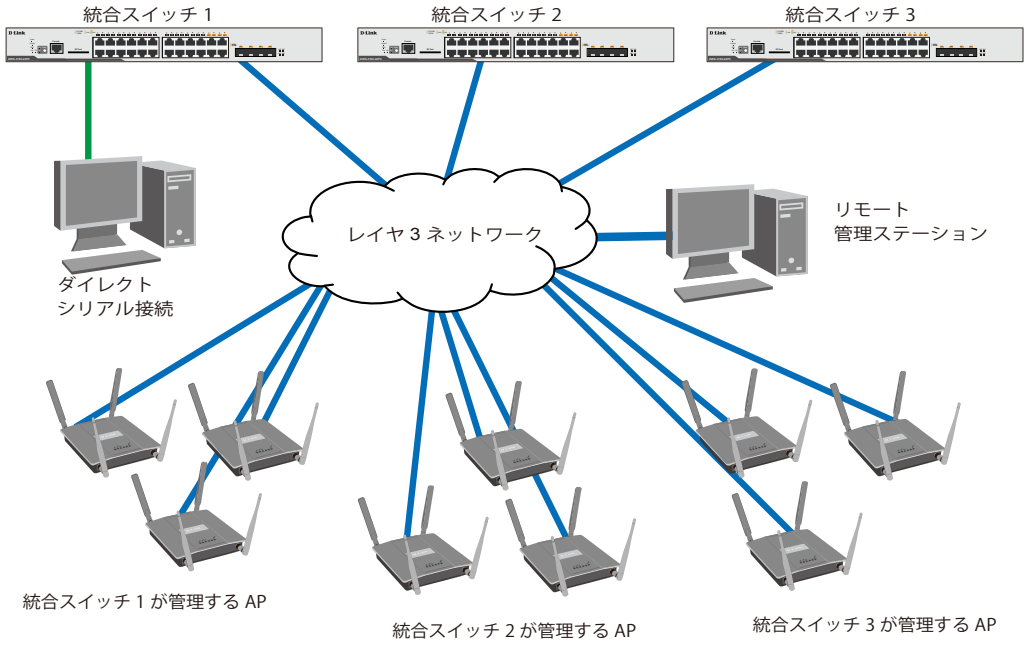


図 6-3　3 つの統合スイッチを持つ統合アクセスシステムの配置

ピアスイッチ間でアクセスポイントの情報を共有し、アクセスポイントのスイッチ間を越えたレイヤ 3 ローミングを可能にします。これを実現するために、ピアスイッチは IPv4 トンネルを構築し、無線クライアントが異なるサブネットに存在するアクセスポイントに接続する際も、同じ IP アドレスを使えるようにします。レイヤ 3 ローミングサービスによって、無線電話の利用者も、異なるサブネットに属するアクセスポイント間を、途切れることなく行き来することができます。

第 7 章 LAN タブ（LAN の設定）

7.1 System Configuration（スイッチの主な設定）

以下は、System 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。	50
System Information Settings（システム情報設定 ）	スイッチの基本情報を表示します。	51
Port Configuration（ポート設定）	ポート設定、ジャンボフレーム設定などを行います。以下のメニューがあります。 Port Settings（スイッチのポート設定）、Port Description Settings（ポート名設定）、Port Error Disabled（エラーによるポートの無効）、Jumbo Frame（ジャンボフレームの有効化）	52
PoE Configuration（PoE 設定）（DWS-3160-24PC）	PoE システムの設定を行います。以下のメニューがあります。 PoE System Settings（PoE システムの設定）、PoE Port Settings（PoE ポート設定）	55
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。	57
Warning Temperature Settings（警告温度設定）	システムの警告温度パラメータを設定します。	57
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。以下のメニューがあります。 System Log Settings（システムログ設定）、System Log Server Settings（システムログサーバの設定）、System Log（Syslog ログ）、System Log & Trap Settings（Syslog とトラップ設定）、System Severity Settings（システムセベリティ設定）	58
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。	61
Port Group Settings（ポートグループ設定）	ポートグループを作成します。	62
Time Settings（時刻設定）	スイッチに時刻を設定します。	62
User Accounts Settings（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。	63
Command Logging Settings（コマンドログ設定）	コマンドログ設定を有効または無効にします。	64

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「DWS-3160 シリーズ」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。また、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。

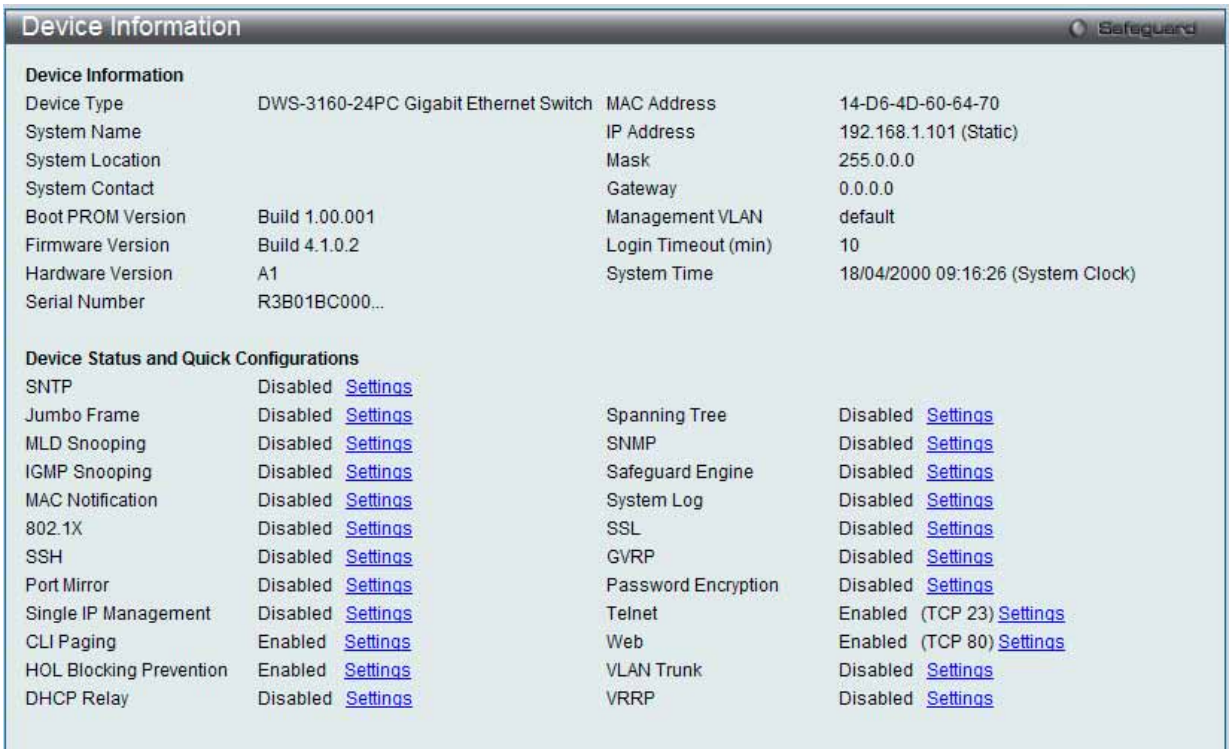


図 7.1-1　Device Information 画面

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。
Serial Number	デバイスのシリアル番号を表示します。
MAC Address	デバイスに割り当てられた MAC アドレスを表示します。
IP Address	デバイスに割り当てられた IP アドレスを表示します。
Mask	デバイスに割り当てられたサブネットマスクを表示します。
Gateway	デバイスに割り当てられたデフォルトゲートウェイを表示します。
Management VLAN	デバイスに割り当てられた VLAN 名を表示します。
Login Timeout (min)	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。
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
Device Status and Quick Configurations	
SNTP	SNTP 機能の状態（有効 / 無効）の表示と、SNTP 設定にリンクします。
Jumbo Frame	Jumbo Frame 機能の状態（有効 / 無効）の表示と、Jumbo Frame の設定にリンクします。
MLD Snooping	MLD Snooping 機能の状態（有効 / 無効）の表示と、MLD の設定にリンクします。
IGMP Snooping	IGMP Snooping 機能の状態（有効 / 無効）の表示と、IGMP の設定にリンクします。
MAC Notification	MAC 通知機能の状態（有効 / 無効）の表示と、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 の設定にリンクします。

項目	説明
SSH	SSH（Secure Shell Protocol）機能の状態（有効 / 無効）の表示と、SSH の設定にリンクします。
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にリンクします。
Single IP Management	SIM 機能の状態（有効 / 無効）の表示と、SIM 設定にリンクします。
CLI Paging	CLI ページング機能の状態（有効 / 無効）の表示と、CLI ページングの設定にリンクします。
HOL Blocking Prevention	HOL ブロッキング防止機能の状態（有効 / 無効）の表示と、HOL ブロッキング防止機能の設定にリンクします。
DHCP Relay	DHCP リレー機能の状態（有効 / 無効）の表示と、DHCP リレー機能の設定にリンクします。
Spanning Tree	STP 機能の状態（有効 / 無効）の表示と、STP 設定にリンクします。
SNMP	SNMP 機能の状態（有効 / 無効）の表示と、SNMP 設定にリンクします。
Safeguard Engine	Safeguard エンジン機能の状態（有効 / 無効）の表示と、Safeguard エンジンの設定にリンクします。
System Log	Syslog 機能のグローバルな状態（有効 / 無効）の表示と、Syslog の設定にリンクします。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 の設定にリンクします。
GVRP	GVRP（Group VLAN Registration Protocol）機能の状態（有効 / 無効）の表示と、GVRP の設定にリンクします。
Password Encryption	パスワードの暗号化機能の状態（有効 / 無効）の表示と、パスワードの設定にリンクします。
Telnet	Telnet 機能の状態（有効 / 無効）の表示と、Telnet 設定にリンクします。
Web	Web ベースの管理機能の状態（有効 / 無効）の表示と、Web ベースの設定にリンクします。Web ベースの管理は初期値では有効です。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。
VLAN Trunk	VLAN トランク機能の状態（有効 / 無効）の表示と、VLAN トランクの設定にリンクします。
VRRP	VRRP 機能の状態（有効 / 無効）の表示と、VRRP 機能の設定にリンクします。

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 Settings 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 Settings（システム情報設定 ）

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。

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

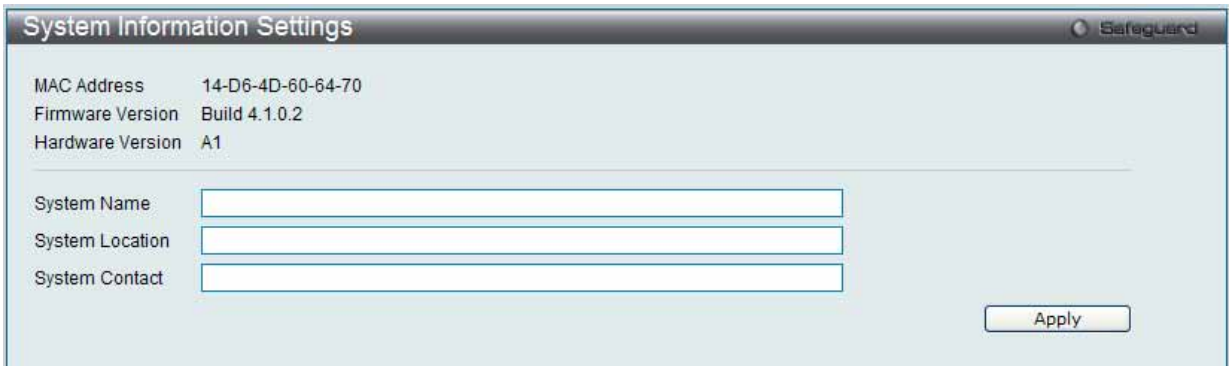


図 7.1-2　System Information Settings 画面

画面には以下の項目があります。

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。この名前はスイッチのネットワークにおける識別名です。
System Location	（必要に応じて）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	（必要に応じて）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。

Port Configuration（ポート設定）

Port Settings（スイッチのポート設定）

スイッチポートの詳細を設定します。

System 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。

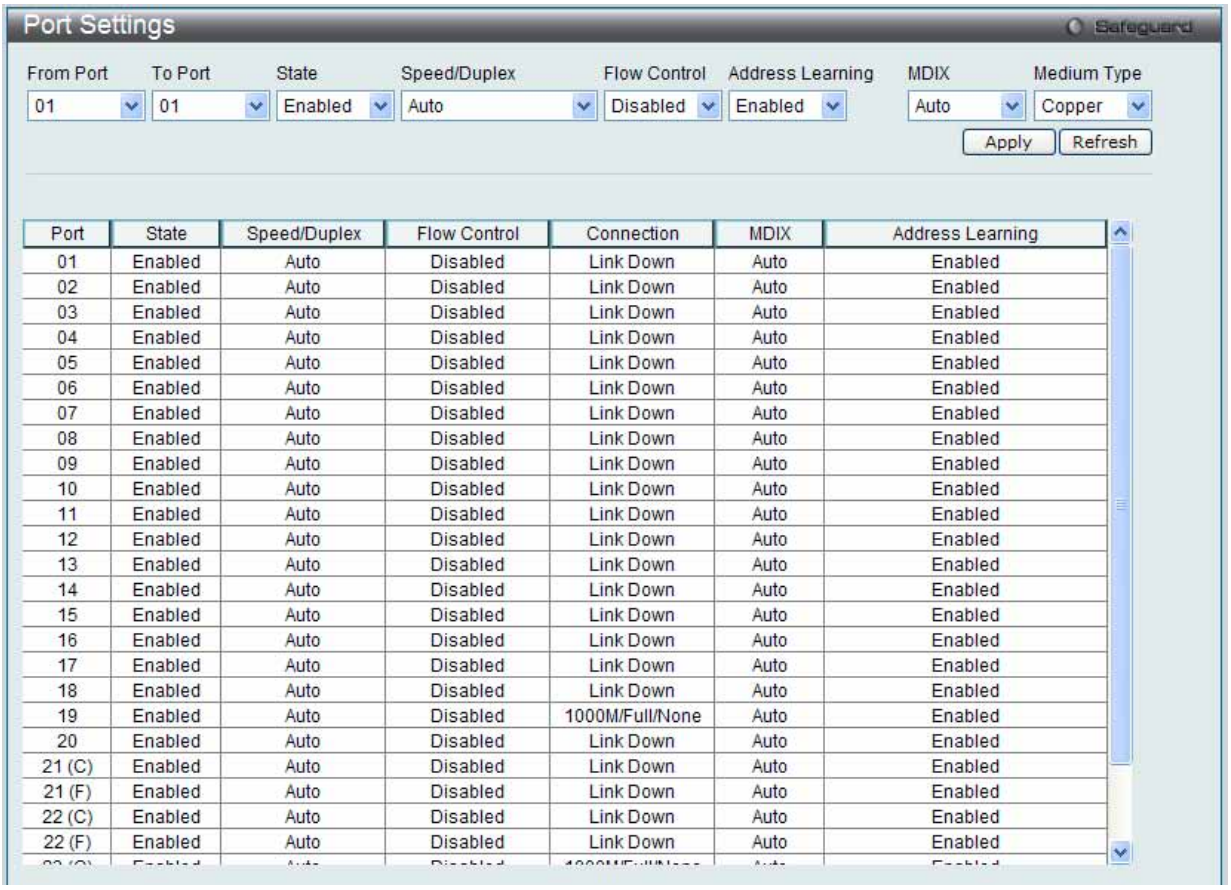


図 7.1-3　Port Settings 画面

スイッチポートの設定

1. 「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。
2. 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。

以下の項目を使用して設定および参照します。

項目	説明
From Port/To Port	本設定に使用される適切なポート範囲を選択します。
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、10/100/1000Mbps 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。 スイッチは 3 つのタイプ (1000M Full_Master および 1000M Full_Slave) の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徴を持っています。 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。その他の設定は両ポートのリンクダウンを引き起こします。

項目	説明
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。（初期値） • 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、「FDB（FDB 設定）」（133 ページ）を参照してください。
MDIX	• Auto - 最適なケーブル配線タイプを自動的に感知します。 • Normal - 標準のケーブル配線となります。「Normal」状態に設定すると、MDI モードになり、ストレートケーブルを通し PC の NIC に接続し、クロスケーブルを通して他のスイッチ上のポートに接続することができます。 • Cross - クロスケーブル接続のために選択します。ストレートケーブルを通して別のスイッチの上のポート（MDI モード）に接続することができます。
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。

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。
「Refresh」ボタンをクリックして、本画面を更新します。

注意 コンボポートにおいて、SFP の RX が信号を受信している状態では、SFP Port、Copper ポートともリンクアップしません。

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。

1. **System 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。

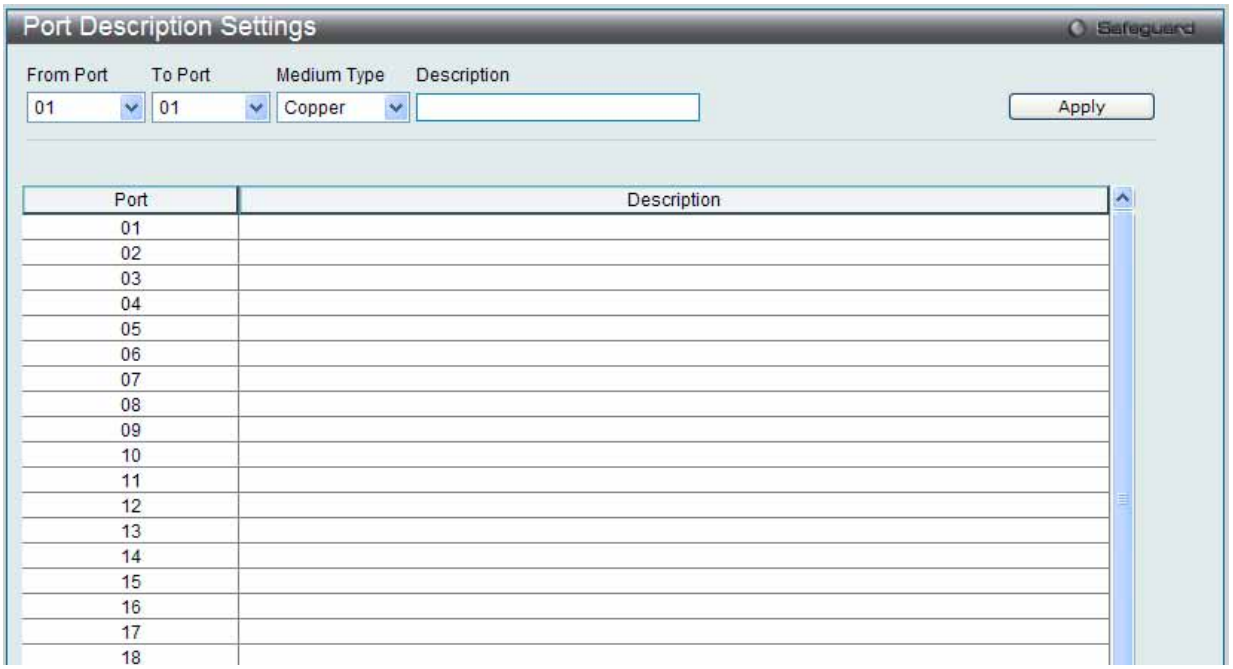


図 7.1-4　Port Description Settings 画面

2. 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および参照します。

項目	説明
From Port / To Port	本設定に使用される適切なポート範囲を選択します。
Medium Type	選択ポートのメディアタイプを指定します。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。
Description	選択ポートの説明を入力します。

「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）

パケットストームの発生やループバックの検出などの理由で、スイッチが切断したポートに関する情報を表示します。

System 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 7.1-5　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」（有効）または「Disabled」（無効））を表示します。
Connection Status	各ポートのアップリンク状況（「Enabled」（有効）または「Disabled」（無効））を表示します。
Reason	ストームコントロールによるポートのシャットダウンなどポートがエラーによって無効になった理由を表示します。

Jumbo Frame Settings（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 13312 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。

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

図 7.1-6　Jumbo Frame Settings 画面

2. 以下の項目を使用して設定および参照します。

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。無効時の最大フレームサイズは 1536 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。最大フレームサイズは 13312 バイトです。 • 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。

PoE Configuration（PoE 設定）（DWS-3160-24PC のみ）

DWS-3160-24PC は、IEEE 802.3af と 802.3at 規格で定義される PoE（Power over Ethernet）をサポートしており、すべてのポートが 30W までの PoE をサポートしています。

1-24 番ポートは、カテゴリ 5 以上の UTP イーサネットケーブル経由で受電機器に 48VDC の電力を供給します。スイッチは標準の PSE（Power Source over Ethernet）のピン配列 Alternative A に従い、電源出力は 1、2、3 および 6 番ピンで行われます。スイッチは、弊社の IEEE 802.3af 準拠製品すべてに給電することができます。

スイッチは以下の PoE 給電機能を持ちます。
- 自動検出機能により、パワーデバイスの接続を認識し、自動的に電源を出力します。
- 自動無効化機能は、以下の 2 つの条件下で動作します。
  - 使用電力の合計がシステムの供給電力の上限値（Power Limit）を超えた場合。
  - あるポートの使用電力がそのポートの供給電力の上限値（Power Limit）を超えた場合。
- ショートが発生した場合、アクティブ回路保護機能によりそのポートを無効にします。他のポートは有効のままです。

IEEE 802.3af/at に準拠する PD（受電機器）および PSE（給電機器）は、以下の電力クラスに応じた受電または給電を行います。

クラス	PD の最大使用電力	クラス	PSE の最大出力電力
0	15.4W	0	15.4W
1	4.0W	1	4.0W
2	7.0W	2	7.0W
3	15.4W	3	15.4W
		ユーザ定義	31.2W

PoE System Settings（PoE システムの設定）

電力制限値および全 PoE システムの給電停止方法について設定を行います。

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

図 7.1-7　PoE System Settings 画面

以下の項目を使用します。

項目	説明
Power Limit (37-740)	スイッチの給電機器から PoE ポート群に供給可能な電力の上限値（37-740）を設定します。初期値は 740 です。
Power Disconnect Method	PoE コントローラは、「Deny Next Port」または「Deny Low Priority Port」によって、供給可能な電力の上限値の超過を防ぎ、スイッチの給電レベルを一定内に保ちます。プルダウンメニューから電力の停止方法を選択します。 • Deny Next Port - スイッチが給電できる最大電力を到達した場合には、優先度に関わらず、新規に接続された PD に給電しません。未使用電力の最大は 19W です。（初期値） • Deny Low Priority Port - スイッチが給電できる最大電力に到達した場合に新規の PD が接続された場合は、ポート優先度の最も低いポートを切断し、高優先度でクリティカルなポートに給電します。
Legacy PD	プルダウンメニューを使用して、旧型の PD 信号の検知を「Enabled」（有効）/「Disabled」（無効）にします。

「Apply」ボタンをクリックし、設定内容を適用します。

PoE Port Settings（PoE ポート設定）

デバイスの各ポートに PoE 設定を行います。

1. **System Configuration > PoE > PoE 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。

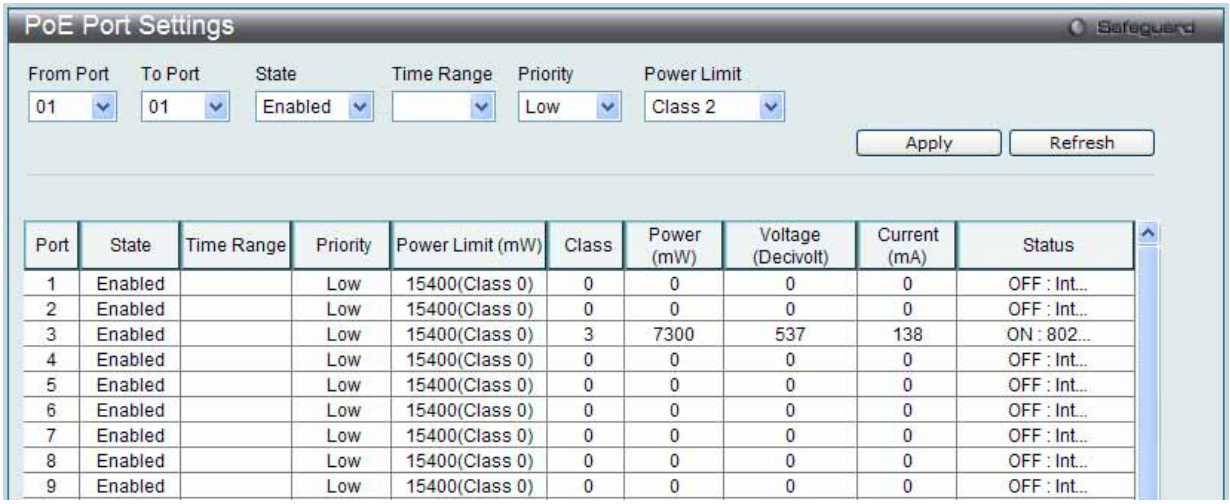


図 7.1-8　PoE Port Settings 画面

2. 以下の項目を使用して設定および参照します。

<table>
<tr><th>項目</th><th>説明</th></tr>
<tr><td>From Port / To Port</td><td>プルダウンメニューから PoE 機能を有効または無効にするポート範囲を選択します。</td></tr>
<tr><td>State</td><td>ポートの PoE 機能を「Enabled」（有効）/「Disabled」（無効）にします。</td></tr>
<tr><td>Time Range</td><td>設定した PoE ポートにタイムレンジを選択します。タイムレンジを設定すると、指定期間だけ電力が供給されます。</td></tr>
<tr><td>Priority</td><td>PoE ポートの優先度を指定します。ポート優先度はシステムがポートへの電力の供給を試みる優先度を決定します。ポート優先度には、高い順に「Critical」、「High」、「Low」の 3 つのレベルがあります。複数のポートに同じ優先レベルがたまたまある場合、ポート ID が優先度を決定するのに使用されます。低いポート ID ほど高い優先度を持ちます。優先度設定はポートに電力を供給する順番に影響します。「PoE System Settings」画面で停止方法に「Deny Low Priority Port」が設定されているかどうかにかかわらず、ポートへの電力供給を管理するためにシステムは各ポートの優先度を使用します。</td></tr>
<tr><td>Power Limit</td><td>1 ポートあたりの電力制限を設定します。ポートが電力制限を超過していると、シャットダウンされます。IEEE 802.3af/802.3at に基づいて、以下の PD クラスと電力消費の範囲があります。
<table>
<tr><th>クラス</th><th>PD の電力消費の範囲</th></tr>
<tr><td>0</td><td>0.44 ～ 15.4W</td></tr>
<tr><td>1</td><td>0.44 ～ 4.0W</td></tr>
<tr><td>2</td><td>4.0 ～ 7.0W</td></tr>
<tr><td>3</td><td>7.0 ～ 15.4W</td></tr>
</table>
これらの 5 つのクラスに対してポートに適用可能な電力の制限値は以下の通りです。各クラスの電力制限はそのクラスの電力範囲よりも若干大きくなっています。これはケーブル上の電力損失も考慮に入れているためです。そのため、標準値は以下のようになります。
<table>
<tr><th>クラス</th><th>PSE の最大出力電力</th></tr>
<tr><td>0</td><td>15400mW</td></tr>
<tr><td>1</td><td>4000mW</td></tr>
<tr><td>2</td><td>7000mW</td></tr>
<tr><td>3</td><td>15400mW</td></tr>
<tr><td>ユーザ定義</td><td>35000mW</td></tr>
</table>
</td></tr>
</table>

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。PoE 設定が行われたすべてのポートの状態は、上記画面下半分のテーブルに表示されます。

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。

1. スイッチにシリアルポート設定をするためには、**System 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 7.1-9　Serial Port Settings 画面

2. 以下の項目を使用して設定および参照します。

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 115200（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（分）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）
Data Bits	シリアルポート接続に使用されるデータビットを表示します。
Parity Bits	シリアルポート接続に使用されるパリティビットを表示します。
Stop Bits	シリアルポート接続に使用されるストップビットを表示します。

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。

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。

Warning Temperature Settings（警告温度設定）

システムの警告温度パラメータを設定します。

1. **System Configuration > Warning Temperature 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 7.1-10　Warning Temperature Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Traps State	警告温度設定のトラップ状態を「Enabled」（有効）または「Disabled」（無効）にします。初期値は「Disabled」です。
Log State	警告温度設定のログ状態を「Enabled」（有効）または「Disabled」（無効）にします。初期値は「Disabled」です。
High Threshold (-500-500)	警告温度設定の上のしきい値を入力します。
Low Threshold (-500-500)	警告温度設定の下のしきい値を入力します。

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。

System Log Configuration（システムログ構成）

System Log Settings（システムログ設定）

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。

System 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 7.1-11　System Log Settings 画面

以下の項目を使用して設定および参照します。

項目	説明
System Log	システムログ機能を「Enabled」（有効）または「Disabled」（無効）に設定します。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。以下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」フォルダを使用して保存します。（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 Settings（システムログサーバの設定）

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

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

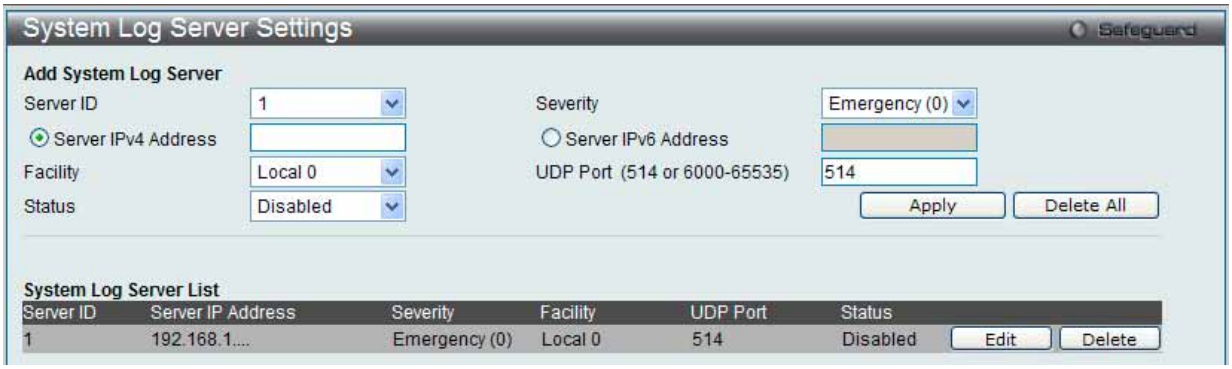


図 7.1-12　System Log Server Settings 画面

2. 以下の項目を使用して設定および参照します。

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。
Severity	送信されるメッセージレベルをプルダウンメニューから選択します。選択したレベル以上のメッセージをすべて送信します。オプションは Emergency (0)、Alert (1)、Critical (2)、Error (3)、Warning (4)、Notice (5)、Informational (6) および Debug (7) です。
Server IPv4 Address	ログを記録するサーバの IPv4 アドレスを設定します。
Server IPv6 Address	ログを記録するサーバの IPv6 アドレスを設定します。
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。Local 0、Local 1、Local 2、Local 3、Local 4、Local 5、Local 6、または Local 7 を選択します。
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。
Status	「Enabled」（有効）または「Disabled」（無効）設定します。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。

エントリの変更

1. 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て以下の画面を表示します。

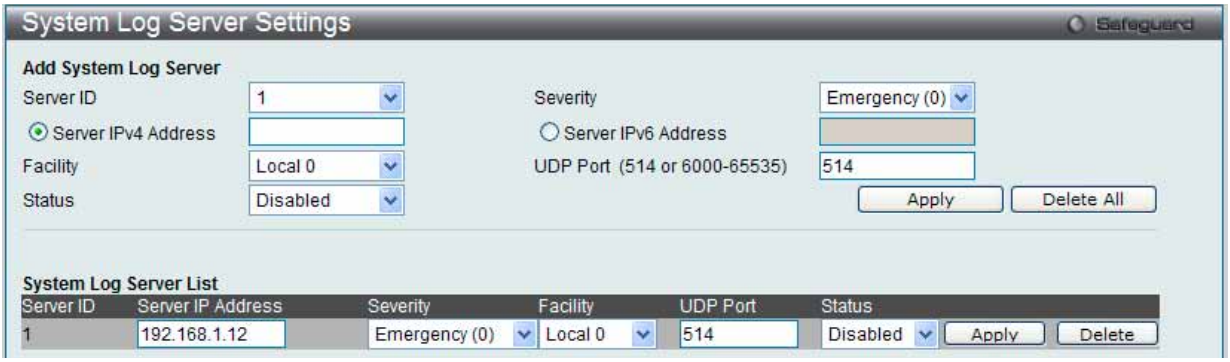


図 7.1-13　System Log Server Settings 画面 - Edit

2. 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。または、「Delete All」ボタンをクリックして、設定したすべてのサーバを削除します。

System Log（Syslog ログ）

スイッチの管理エージェントでまとめたローカルなヒストリログの表示および削除を行います。

1. **System Configuration > System Log Configuration > System 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。

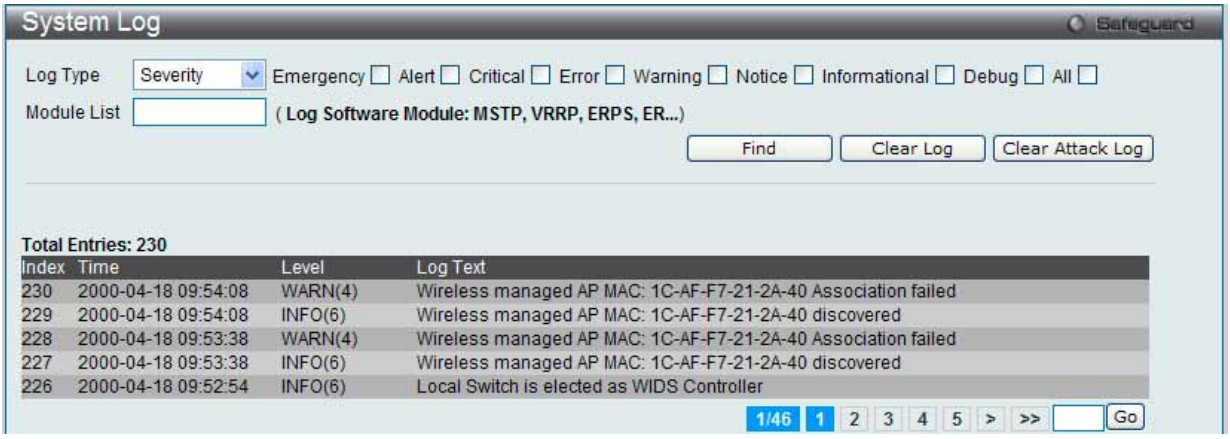


図 7.1-14　System Log 画面

スイッチは自身のログにイベント情報を記録できます。「Go」ボタンをクリックすると、「System Log」画面の次のページへ移動します。

2. 以下の項目を使用して設定および参照します。

項目	説明
Log Type	プルダウンメニューで表示するログタイプを選択します。 • Severity - これを選択する場合、次のチェックも行う必要があります。次にチェックするのは Emergency、Alert、Critical、Error、Warning、Notice、Informational および Debug です。ログ内の全情報を単に参照するには、「All」オプションを選択します。特定のモジュールを検索するためには、モジュール名を入力します。 • Module List - これを選択する場合、手動でモジュール名を入力する必要があります。利用可能なモジュールは、MSTP、ERROR_LOG、CFM_EXT および ERPS です。 • Attack Log - すべての攻撃が表示されます。
Index	エントリが加わるごとに 1 ずつ増加します。新しいエントリ順に表示されます。
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。
Level	ログエントリのレベルを表示します。
Log Text	イベントの内容を表示します。

ログの検索

「Find」ボタンをクリックして、選択に基づいて表示セクションにログを表示します。

ログのクリア

「Clear Log」ボタンをクリックして、表示画面内のすべてのエントリをクリアします。「Clear Attack Log」ボタンをクリックして、表示セクション内の攻撃ログからエントリをクリアします。

System Log & Trap Settings（Syslog とトラップ設定）

スイッチに Syslog の送信元 IP インタフェースアドレスを設定できます。

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

図 7.1-15　System Log & Trap Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
IP Interface	使用する IP インタフェース名を入力します。
IPv4 Address	使用する IPV4 アドレスを入力します。
IPv6 Address	使用する IPv6 アドレスを入力します。

設定を変更する際は、それぞれのセクションで「Apply」ボタンをクリックし、設定内容を適用してください。

情報のクリア

「Clear」ボタンをクリックして、欄内に入力されたすべての情報をクリアします。

System Severity Settings（システムセベリティ設定）

スイッチは、アラートが発生した場合、ログとして記録するか、または SNMP エージェントにトラップとして送信することができます。また、アラートの発生がログイベント、またはトラップメッセージをトリガにするレベルも指定することができます。ここではアラートの基準を設定します。「System Severity Table」セクションに現在の設定を表示します。

1. **System Configuration > System Log Configuration > System Severity Settings** の順にメニューを選択し、以下の設定画面を表示します。

注意　画面中に表示されるログイベントの詳細情報については、本マニュアル中の「付録 C ログエントリ」（535 ページ）を参照してください。

図 7.1-16　System Severity Settings 画面

2. プルダウンメニューを使用して、以下の項目の設定を行います。

項目	説明
System Severity	「Severity」タイプで指定したレベルのアラートが発生した時に実行するアクションを選択します。 • Log - 分析のためにスイッチのログに設定した「Severity Level」のアラートを送信します。 • Trap - 分析のために SNMP エージェントに送信します。 • All - 分析のために SNMP エージェントとスイッチのログに選択したアラートタイプを送信します。
Severity Level	送信されるメッセージレベルをプルダウンメニューから選択します。オプションは Emergency (0)、Alert (1)、Critical (2)、Error (3)、Warning (4)、Notice (5)、Informational (6) および Debug (7) です。

「Apply」ボタンをクリックして、システムのログレベル設定を適用します。

Time Range Settings（タイムレンジ設定）

各機能（ACL など）が作用する期間（タイムレンジ）を設定します。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。

例えば、管理者は週土日にインターネットの閲覧を許可し、一方平日はインターネットの閲覧を拒否するようなタイムベース ACL を設定することができます。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 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。

System 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。

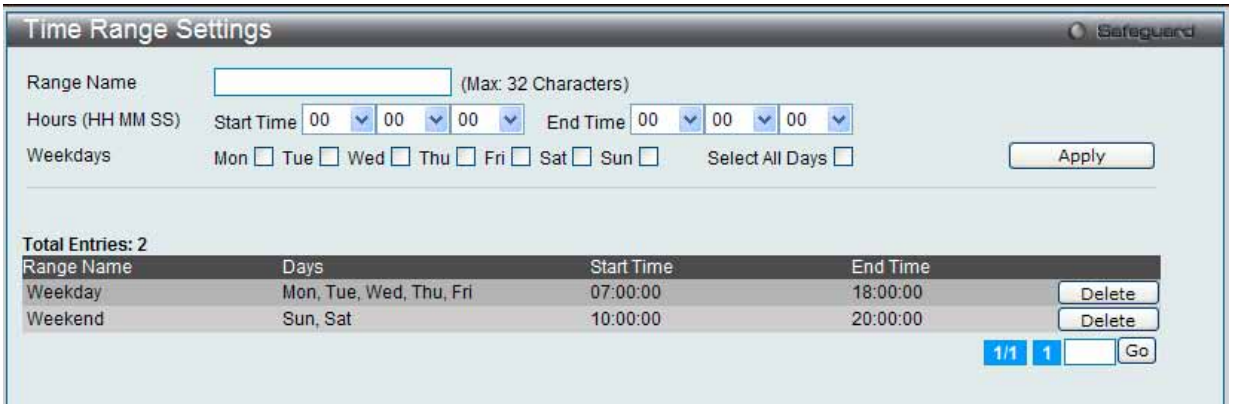


図 7.1-17　Time Range Settings 画面

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。このレンジ名はアクセスプロファイル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テーブルに表示されます。

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。

Port Group Settings（ポートグループ設定）

ポートグループを作成し、ポートグループへのポートの追加または削除を行います。

1. **System Configuration > Port Group Settings** の順にメニューをクリックして以下の画面を表示します。

図 7.1-18　Port Group Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Group Name	ポートグループ名を入力します。
Group ID (1-64)	グループ ID を入力します。
Port List	ポートまたはポートリストを入力します。「All」を選択すると、すべてのポートに適用します。
Action	プルダウンメニューを使用して、「Create Port Group」（ポートグループの作成）、「Add Ports」（ポートの追加）または「Delete Ports」（ポートの削除）を選択します。

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

エントリの削除

削除するエントリ横の「Delete」ボタンをクリックします。

Time Settings（時刻設定）

スイッチに時刻を設定します。

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

図 7.1-19　Time Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Date（DD/MM/YYYY）	システムクロックの更新を行うために現在の年月日を入力します。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、デバイスに時刻設定を適用します。

User Accounts Settings（ユーザアカウントの設定）

スイッチはユーザ権限の制御を行うことができます。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. **System Configuration > User Accounts Settings** の順にクリックし、以下の画面を表示します。

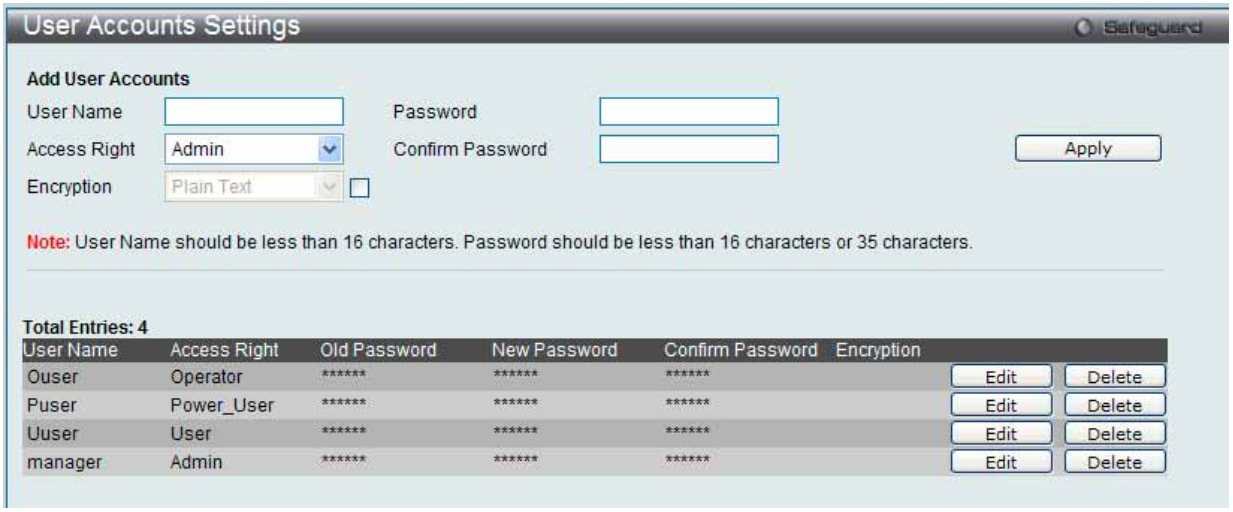


図 7.1-20　User Accounts Settings 画面

Admin レベル、Operator レベル、Power User および User レベルの権限は以下の通りです。

管理	Admin	Operator	Power User	User
コンフィグレーション設定	読み / 書き可	読み / 書き（一部）	読み / 書き（一部）	不可
ネットワークモニタリング	読み / 書き可	読み / 書き可	読み出しのみ	読み出しのみ
コミュニティ名とトラップステーション	読み / 書き可	読み出しのみ	読み出しのみ	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	読み / 書き可	読み / 書き可	不可	不可
システムユーティリティ	読み / 書き可	読み出しのみ	読み出しのみ	読み出しのみ
リセット（工場出荷状態へ）	読み / 書き可	不可	不可	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	読み / 書き可	不可	不可	不可
ユーザアカウントの確認	読み / 書き可	不可	不可	不可

画面には以下の項目があります。

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）
Password	スイッチに新しいパスワードを設定します。
Confirm Password	パスワードの確認のために再度入力をします。
Access Right	ユーザのアクセス権限（Admin、Operator、Power User および User）を指定します。
Encryption	本ボックスをチェックして、アカウントに適用する暗号化タイプ（Plain Text または SHA-1）を指定します。

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。

ユーザアカウントの編集

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。

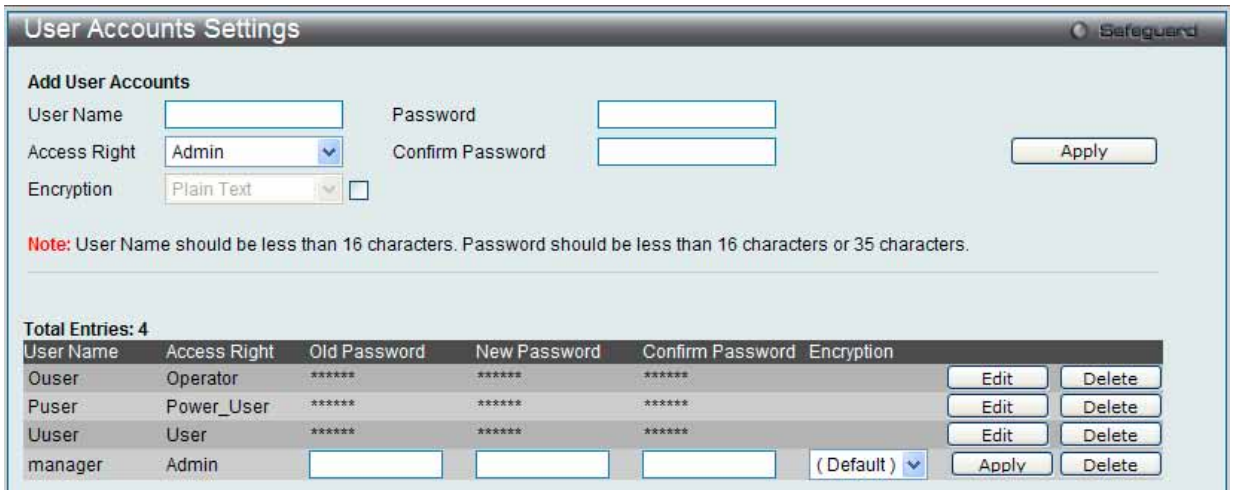


図 7.1-21　User Accounts Settings 画面 - 編集

2. 各項目を設定します。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、確認のために再度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、「付録 B　パスワードのリカバリ手順」（534 ページ）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。

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。

注意 ユーザ名とパスワードは 16 文字以内とします。

Command Logging Settings（コマンドログ設定）

コマンドログ設定を有効または無効にします。

1. **System Configuration > Command Logging 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 7.1-22　Command Logging Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Command Logging State	ラジオボタンを使用して機能を「Enabled」（有効）/「Disabled」（無効）にします。

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。

注意 スイッチの再起動中またはダウンロードしたコンフィグレーションの処理実行中は、すべてのコンフィグレーションコマンドがログに出力されるというわけではありません。または、ユーザが AAA 認証を使用してログインした際、ユーザが権限を取り替えるために「enable admin」コマンドを使用した場合には、ユーザ名を変更するべきではありません。

7.2 Management（スイッチの管理）

以下は、LAN タブの Management 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
ARP（ARP 設定）	スタティック ARP、プロキシ ARP 、ARP テーブルを設定します。次のメニューがあります。Static ARP Settings（スタティック ARP 設定）、Proxy ARP Settings（プロキシ ARP 設定）、ARP Table（ARP テーブルの参照）	66
Gratuitous ARP（Gratuitous ARP の設定）	Gratuitous ARP の設定をします。次のメニューがあります。Gratuitous ARP Global Settings（Gratuitous ARP グローバル設定）、Gratuitous ARP Settings（Gratuitous ARP 設定）	69
IPv6 Neighbor Settings（IPv6 Neighbor 設定）	IPv6 Neighbor の設定を行います。	71
IP Interface（IP インタフェース設定）	スイッチの IP インタフェース設定を行います。次のメニューがあります。System IP Address Settings（IP アドレス設定）、Interface Settings（インタフェース設定）	72
Management Settings（管理設定）	CLI ページング、DHCP 自動設定、省電力モードなどの管理設定を行います。	76
Session Table（セッションテーブル）	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。	77
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。次のメニューがあります。Single IP Settings（シングル IP 設定）、Firmware Upgrade（ファームウェア更新）、Configuration File Backup/ Restore（コンフィグレーションファイルの更新）、Upload Log File（ログファイルのアップロード）	78
SNMP Settings（SNMP 設定）	SNMP 設定を行います。次のメニューがあります。SNMP Global Settings（SNMP グローバル設定）、SNMP Trap Settings（SNMP トラップ設定）、SNMP Link Change Traps Settings（SNMP リンクチェンジトラップ設定）、SNMP View Table Settings（SNMP ビューテーブル）、SNMP Community Table Settings（SNMP コミュニティテーブル設定）、SNMP Group Table Settings（SNMP グループテーブル）、SNMP Engine ID Settings（SNMP エンジン ID 設定）、SNMP User Table Settings（SNMP ユーザテーブル設定）、SNMP Host Table Settings（SNMP ホストテーブル設定）、SNMP v6Host Table Settings（SNMP v6 ホストテーブル設定）、RMON Settings（RMON 設定）	87
Telnet Settings（Telnet 設定）	スイッチに Telnet 設定をします。	95
Web Settings（Web 設定）	スイッチに Web ステータスを設定します。	95

ARP（ARP 設定）

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する TCP/IP プロトコルです。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。また、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。

ARP 情報の定義

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

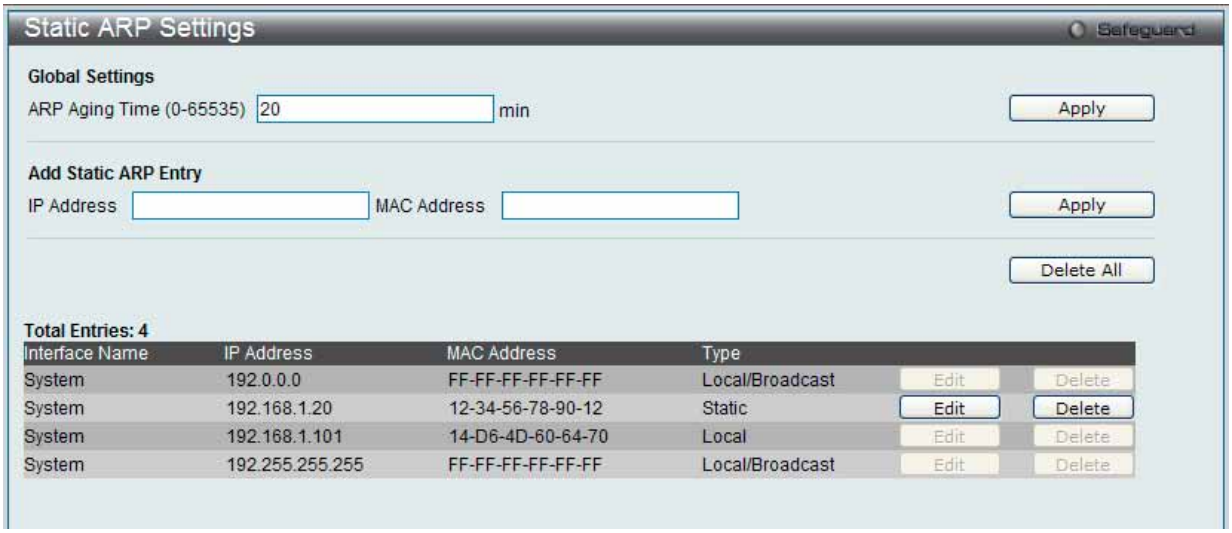


図 7.2-1　Static ARP Settings 画面

「Static ARP Settings」画面には以下の項目があります。

項目	説明
Global Settings	
ARP Aging Time (0-65535)	ARP エントリのエージングタイム（分）。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、以下の画面を表示します。

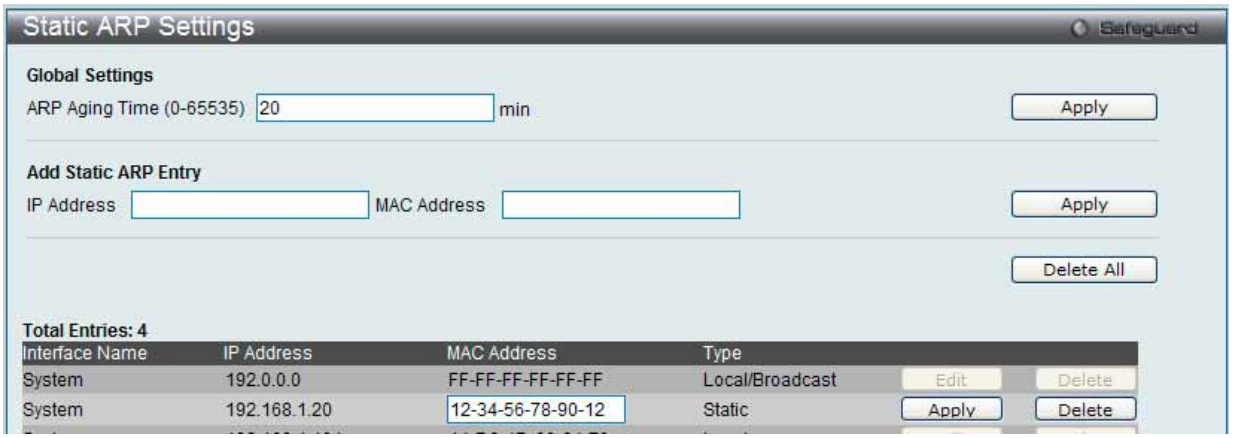


図 7.2-2　Static ARP Settings 画面

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

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。

Proxy ARP Settings（プロキシ ARP 設定）

プロキシ ARP 機能に関する基本設定を参照および編集します。

スイッチのプロキシ ARP（Address Resolution Protocol）機能を使用して、スイッチはオリジナルの ARP 応答者のように識別子（IP および MAC アドレス）を見せかけることによって別のデバイス宛ての ARP リクエストに応答することができます。そのため、スイッチは、スタティックルーティングまたはデフォルトゲートウェイを設定せずに、意図した宛先にパケットを送信することができます。

ホスト（通常レイヤ 3 スイッチ）は他のデバイス宛てのパケットに応答します。例えば、ホスト A と B が異なる物理ネットワークにあると、B は A から ARP ブロードキャストリクエストを受信しないため応答できません。しかし、A の物理ネットワークがルータまたはレイヤ 3 スイッチを使用して B に接続していると、ルータまたはレイヤ 3 スイッチは A からの ARP リクエストを参照します。

送信元 IP と宛先 IP が同じインタフェースにあると、スイッチはこのローカルなプロキシ ARP 機能によりプロキシ ARP に応答することができます。

Management > ARP > Proxy 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 7.2-3　Proxy ARP Settings 画面

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 7.2-4　Static ARP Settings 画面

2. 指定エントリを編集して、IP インタフェースのプロキシ ARP の状態を選択します。
3. 「Apply」ボタンをクリックします。

初期値では、「Proxy ARP State」と「Local Proxy ARP State」の両方とも「Disabled」（無効）です。

ARP Table（ARP テーブルの参照）

スイッチ上の現在の ARP エントリを表示します。

1. **Management > ARP > ARP Table** メニューをクリックし、以下の画面を表示します。

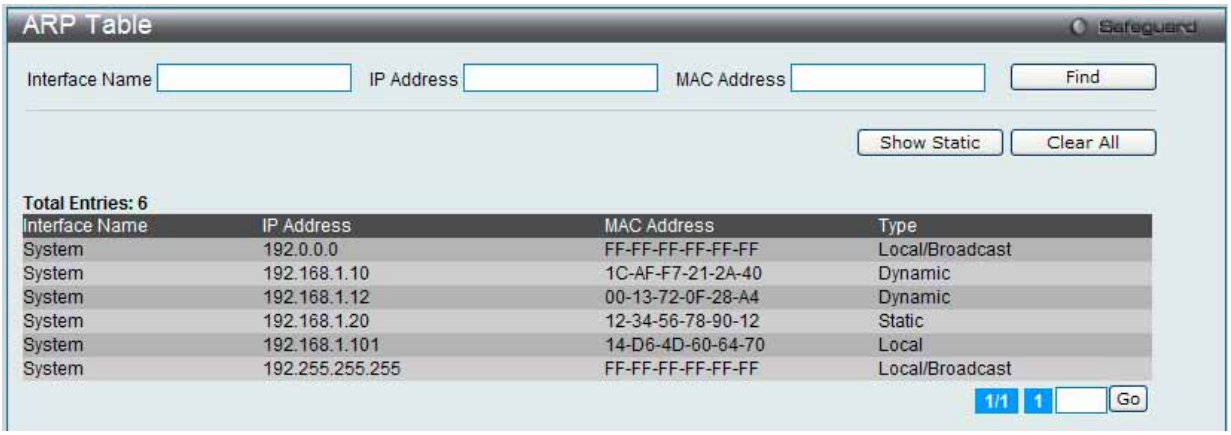


図 7.2-5　ARP Table 画面

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

2. 以下の項目を使用して設定および参照します。

項目	説明
Interface Name	使用する IP インタフェース名を入力または参照します。
IP Address	使用する IP アドレスを入力または参照します。
MAC Address	使用する MAC アドレスを入力または参照します。

ARP エントリの検索

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 エントリのクリア

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。

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、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によって一般的に行われています。これは、ネットワークカードの変更により、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。

1. **Management > 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 7.2-6　Gratuitous ARP Global Settings 画面

2. 以下の項目を使用して設定および参照します。

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「Enabled」（有効）または「Disabled」（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「Disabled」で、Gratuitous ARP パケットだけがブロードキャストされます。
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「Enabled」（有効）または「Disabled」（無効）にします。初期値は「Disabled」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。この場合、システムは、誰かがシステムと重複する IP アドレスを使用していることがわかります。この IP アドレスのホストを正しくするために、システムはこの重複 IP アドレスに Gratuitous ARP リクエストパケットを送信することができます。
Gratuitous ARP Learning	システムは、通常、システムの IP アドレスに一致している MAC アドレスを求める ARP 応答パケットか正常な ARP リクエストパケットを学習するだけです。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「Enabled」（有効）または「Disabled」（無効）にします。Gratuitous ARP パケットはパケットがクエリである IP と同じ送信元 IP アドレスによって送信されます。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。

注意 Gratuitous ARP を学習すると、システムは新しいエントリを学習しません。また、受信した Gratuitous ARP パケットに基づいて ARP テーブルの更新のみ行います。

Gratuitous ARP Settings（Gratuitous ARP 設定）

IP インタフェースの Gratuitous ARP パラメータを設定します。

1. **Management > 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。

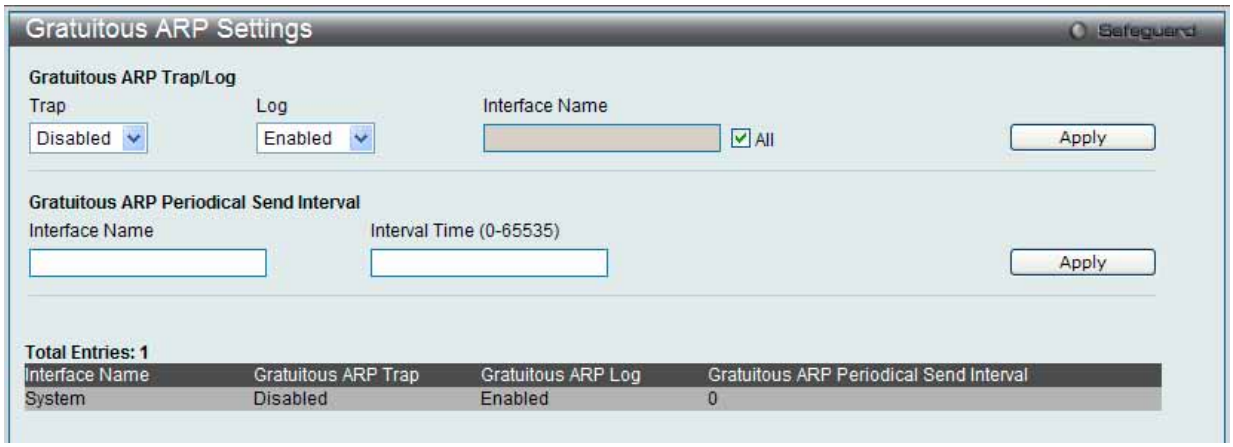


図 7.2-7　Gratuitous ARP Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Gratuitous ARP Trap/Log	
Trap	「Enabled」（有効）の場合、IP の重複イベントをトラップし、管理者に通知します。初期値は「Disabled」（無効）です。
Log	「Enabled」（有効）の場合、IP の重複イベントのログを取得し、管理者に通知します。初期値は「Enabled」（有効）です。
Interface Name	レイヤ 3 インフェース名を入力します。「All」を選択して全インタフェース上の Gratuitous ARP トラップを「Enabled」（有効）または「Disabled」（無効）にします。
Gratuitous ARP Periodical Send Interval	
Interface Name	編集するインタフェース名を表示します。
Interval Time (0-65535)	定期的に Gratuitous ARP を送信する間隔（秒）を入力します。0 は Gratuitous ARP リクエストが定期的に送信されないことを意味します。初期値は 0（秒）です。

各セクションにある設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

IPv6 Neighbor Settings（IPv6 Neighbor 設定）

スイッチの IPv6 Neighbor 設定を行います。

Management > 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。

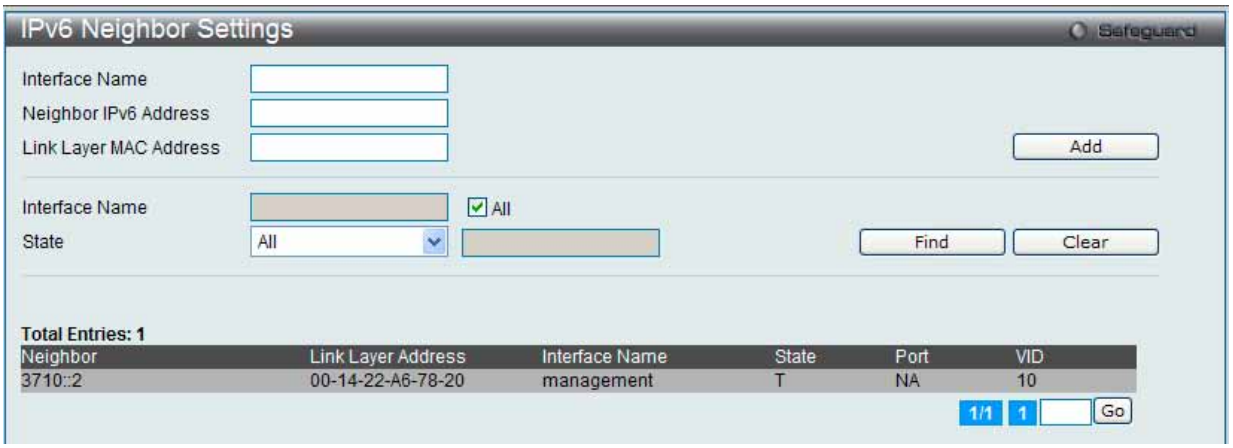


図 7.2-8　IPv6 Neighbor Settings 画面

スイッチの現在の IPv6 Neighbor 設定が下部に表示されます。複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、指定ページへ移動します。

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。

以下の項目を使用して設定および参照します。

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	リンクレイヤの MAC アドレスを入力します。
State	「All」、「Address」、「Static」または「Dynamic」を指定します。「Address」を選択すると、「State」オプション横にあるスペースに IP アドレスを入力できるようになります。

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。

IP Interface（IP インタフェース設定）

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。Web マネージャはスイッチの現在の IP 設定が表示します。

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

System IP Address Settings（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。

1. **Management > IP Interface > System 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 7.2-9　System IP Address Settings 画面

2. プロトコルを選択します。

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 プロトコルを使用して DHCP サーバが 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を割り当てます。本オプションを選択すると、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 プロトコルを使用して BOOTP サーバが 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を割り当てます。本オプションが選択すると、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。

3. 以下の項目を使用して設定および参照します。以下の表は「System」インタフェースに関する項目について説明します。

項目	説明
Interface Name	System インタフェース名が表示されます。
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「Trusted Host（トラストホスト）」（309 ページ）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 default VLAN に所属しています。「Trusted Host」テーブルには初期状態でエントリはないため、管理 VLAN が指定されるまで、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、スイッチに接続可能な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）または「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。
IP Address	IP インタフェースに割り当てる 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。

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。

Interface Settings（インタフェース設定）

スイッチの IP インタフェース設定を行います。

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

図 7.2-10　Interface Settings 画面

スイッチの現在の IP インタフェース設定が表示されます。

項目	説明
Interface Name	検索する IP インフェース名を入力します。

エントリの検索

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

エントリの削除

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

注意　IPv6 にインタフェースを作成するために、はじめに IPv4 インタフェースを作成して、それを IPv6 に編集する必要があります。

IP インタフェースの追加

1.　「Add」ボタンをクリックして以下の画面を表示します。

図 7.2-11　IPv4 Interface Settings 画面

2.　以下の項目を使用して設定および参照します。

項目	説明
Interface Name	作成するインフェース名を入力します。
IPv4 Address	使用する IPv4 アドレスを入力します。
Subnet Mask	使用する IPv4 サブネットを入力します。
VLAN Name	使用する VLAN 名を入力します。
Interface Admin State	インタフェースの管理を「Enabled」（有効）または「Disabled」（無効）にします。
Secondary Interface	このオプションを選択してセカンダリインタフェースとしてこのインタフェースを使用します。プライマリ IP が利用できない場合、VLAN はセカンダリインタフェースに切り替わります。プライマリ IP が回復すると、元に戻ります。

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

「<<Back」をボタンをクリックすると、変更は破棄されて前のページに戻ります。

IPv4 インタフェースの編集

1. 「Interface Settings」画面で編集するエントリの「IPv4 Edit」ボタンをクリックすると、以下の画面が表示されます。

図 7.2-12　IPv4 Interface Settings 画面 - Edit

2. 以下の項目を使用して設定および参照します。

項目	説明
Get IP From	このインタフェースが IP アドレスを取得するのに使用する方式（Static、DHCP、BOOTP）を指定します。
Interface Name	編集するインフェース名が表示されます。
IPv4 Address	使用する IPv4 アドレスを入力します。
Subnet Mask	使用する IPv4 サブネットを入力します。
VLAN Name	使用する VLAN 名を入力します。
IPv4 State	IPv4 の状態を「Enabled」（有効）または「Disabled」（無効）にします。
Interface Admin State	インタフェースの管理を「Enabled」（有効）または「Disabled」（無効）にします。

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。

「<<Back」をボタンをクリックすると、変更は破棄されて前のページに戻ります。

IPv6 インタフェースの編集

1. 「Interface Settings」画面で編集するエントリの「IPv6 Edit」ボタンをクリックすると、以下の画面が表示されます。

図 7.2-13　IPv6 Interface Settings 画面 - Edit

2. 以下の項目を使用して設定および参照します。

項目	説明
IPv6 Interface Settings	
Interface Name	IPv6 インタフェース名を表示します。
IPv6 State	IPv6 の状態を「Enabled」（有効）または「Disabled」（無効）にします。
Interface Admin State	インタフェースの管理を「Enabled」（有効）または「Disabled」（無効）にします。
IPv6 Network Address	Neighbor のグローバルまたはローカルリンクアドレスを入力します。
NS Retransmit Settings	
NS Retransmit Time	Neighbor Solicitation の再送タイマ（ミリ秒）を入力します。「config ipv6 nd ra」コマンドの設定における「ra retrans_time」と同じ値を持っています。本欄を設定する場合、「RA」欄への入力をコピーします。
Automatic Link Local Status Settings	
Automatic Link Local Address	自動リンクローカルアドレスを「Enabled」（有効）または「Disabled」（無効）にします。

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。

「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。
「View All IPv6 Address」リンクをクリックして、現在の全 IPv6 アドレスを参照します。

IPv6 アドレスの参照

1. 「View All IPv6 Address」リンクをクリックすると、以下の画面が表示されます。

図 7.2-14　IPv6 Interface Settings 画面

「<<Back」をボタンをクリックして前のページに戻ります。

IPv6 インタフェースの削除

「Interface Settings」画面で削除するエントリの「Delete」ボタンをクリックします。

Management Settings（管理設定）

本スイッチの管理設定を行います。

コマンドラインインタフェースを使用する場合、コンソールの制限を超えた複数ページのスクロールを停止することができます。また、本画面でスイッチの DHCP 自動設定機能を有効にするためにも利用されます。「Enabled」（有効）の時、本スイッチは TFTP サーバからコンフィグレーションファイルを受信して、起動時に自動的に DHCP クライアントになるように設定します。この方法を使用するためには、DHCP サーバは TFTP サーバに IP アドレスと DHCP リプライパケット内のコンフィグレーションファイル名情報を渡すように設定する必要があります。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。クライアントが使用するためのコンフィグレーションファイルに関する詳しい情報は、DHCP サーバまたは TFTP サーバソフトウェアの手順を参照してください。さらに、本マニュアルの「Tools」セクションの「Upload Log File」画面に関する説明を参照ください。

本スイッチが DHCP 自動コンフィグレーションを完了できない場合は、スイッチのメモリ内にある以前に保存したコンフィグレーションが使用されます。また、本画面では、スイッチの内蔵電源を節電する機能を実装するためにも利用されます。省電力機能が「Enabled」（有効）である場合、リンクダウン状態のポートは電源をオフにしてスイッチへの電力を節約します。ポート状態がリンクアップになっても、これはポートの性能に影響しません。また、スイッチにパスワードの暗号化機能を設定することができます。

1. **Management > Management 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 7.2-15　Management Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
CLI Paging State	コマンドラインインタフェースのページング機能はコンソールの終わりで各ページを停止します。これはコンソールの制限を超えた複数ページのスクロールを停止することができます。初期値は「Enabled」（有効）です。無効にするためには「Disabled」ボタンをクリックします。
DHCP Auto Configuration State	スイッチの DHCP 自動設定機能を「Enabled」（有効）または「Disabled」（無効）にします。 「Enabled」の時、本スイッチは TFTP サーバからコンフィグレーションファイルを受信して、起動時に自動的に DHCP クライアントになるように設定します。この方法を使用するためには、DHCP サーバは TFTP サーバに IP アドレスと DHCP リプライパケット内のコンフィグレーションファイル名情報を渡すように設定する必要があります。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構成ファイルを保管しておく必要があります。
Power Saving State	各物理ポートのリンクダウンの省電力モードを「Enabled」（有効）または「Disabled」（無効）にします。ポートが接続しない場合、スイッチポートはスリープモードに入ります。
Length Detection State	物理ポートにおける長さ検知の省電力モードを「Enabled」（有効）または「Disabled」（無効）にします。スイッチポートは、より短いケーブルへの電力送信を削減します。
Password Encryption State	パスワードの暗号化はコンフィグレーションファイル内のパスワード設定を暗号化します。初期値ではパスワードの暗号化は「Disabled」（無効）になっています。パスワードの暗号化を有効にするためには「Enabled」ボタンをクリックします。
Running Configuration	「Password Recovery」オプションにおける動作中のコンフィグレーションを「Enabled」（有効）または「Disabled」（無効）にすることができます。有効にすると、動作中のコンフィグレーションのパスワードリカバリの実行を可能とします。

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　D-Link グリーンテクノロジーに関する詳細については、http://green.dlink.com/ を参照してください。

Session Table（セッションテーブル）

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。

Management > Session 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 7.2-16　Session Table 画面

「Refresh」ボタンをクリックして、テーブルを更新し、新しいエントリを表示します。

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 4 台のスイッチ（番号：1-4）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。
- 複数の 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。

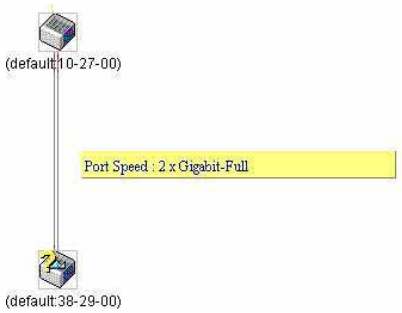
バージョン 1.61 へのアップグレード

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 **Management > 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。

図 7.2-17　Single IP Settings 画面（CaS 無効状態）

2. プルダウンメニューを使用して、「SIM State」を「Enabled」（有効）、「Role State」を「Commander」に変更し、次に「Group Name」欄を指定します。

図 7.2-18　Single IP Settings 画面（CS 有効状態）

3. 「Apply」ボタンをクリックして、設定を有効にします。

以下の項目が使用できます。

項目	説明
SIM State	プルダウンメニューから「Enabled」（有効）または「Disabled」（無効）を選択します。「Disabled」を選択すると、スイッチのすべての SIM 機能が無効になります。初期値は「Disabled」です。
Role State	プルダウンメニューからスイッチの SIM での役割を選択します。以下の 2 つから選択できます。 • Candidate - Candidate Switch（CaS）は SIM グループメンバではありませんが、Commander スイッチに接続しています。本スイッチの SIM 機能の初期設定です。 • Commander - Commander Switch（CS）。ユーザは CS に他のスイッチを参加させて SIM グループを作成します。このオプションを選択すると、本スイッチは SIM 機能対象のスイッチとして設定されます。
Group Name	SIM グループ名を入力します。
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。

Management > 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。

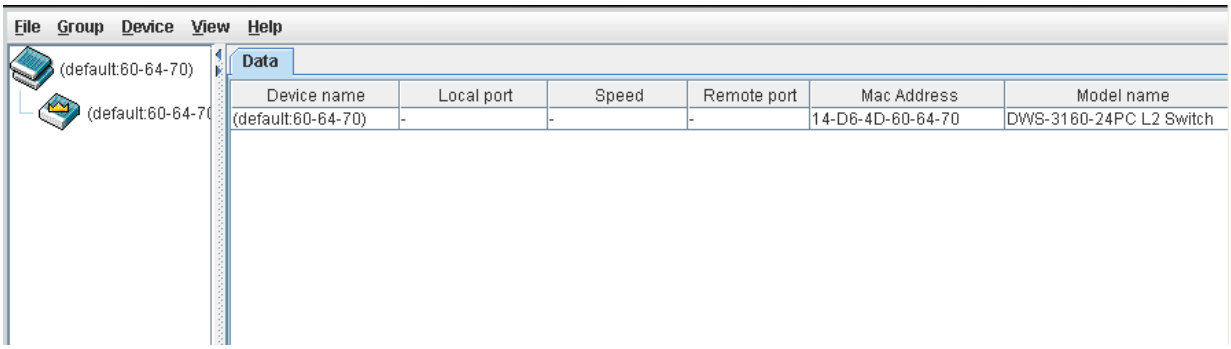


図 7.2-19　トポロジ画面

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。

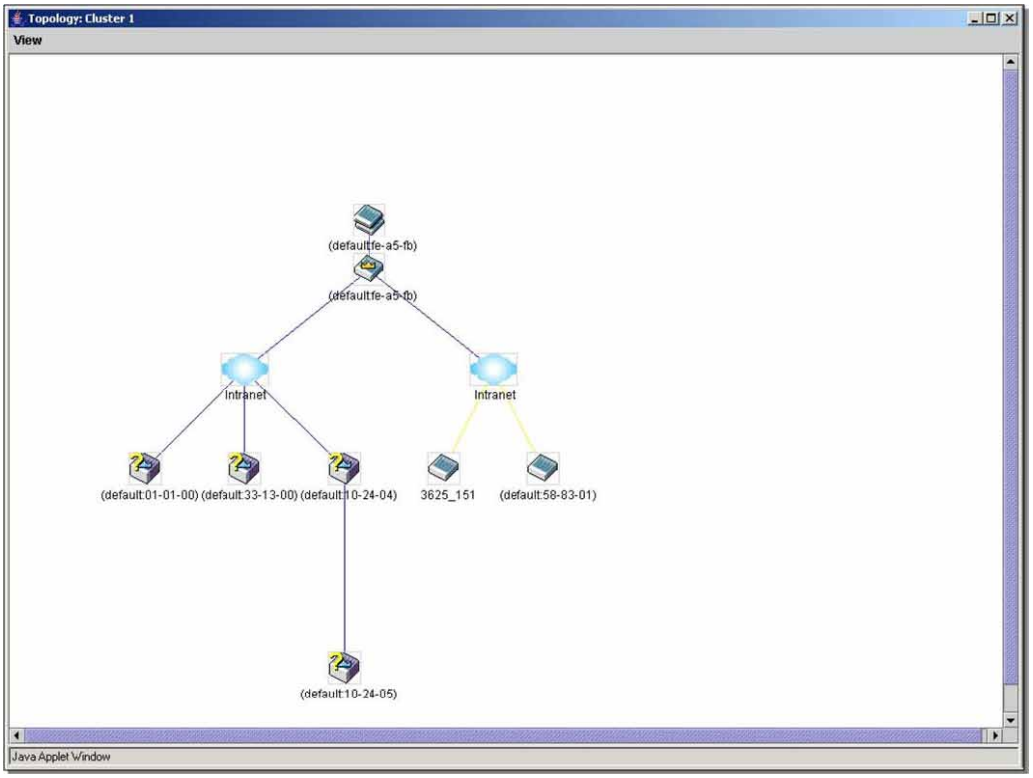
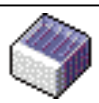


図 7.2-20　Topology 画面

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。

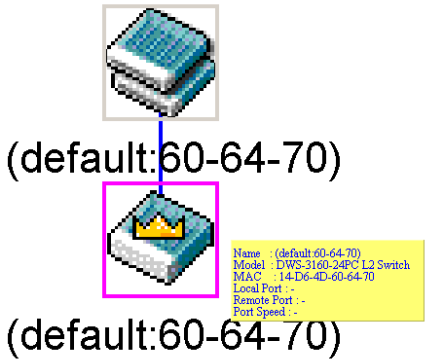


図 7.2-21　ツールヒントを利用したデバイス情報の表示

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

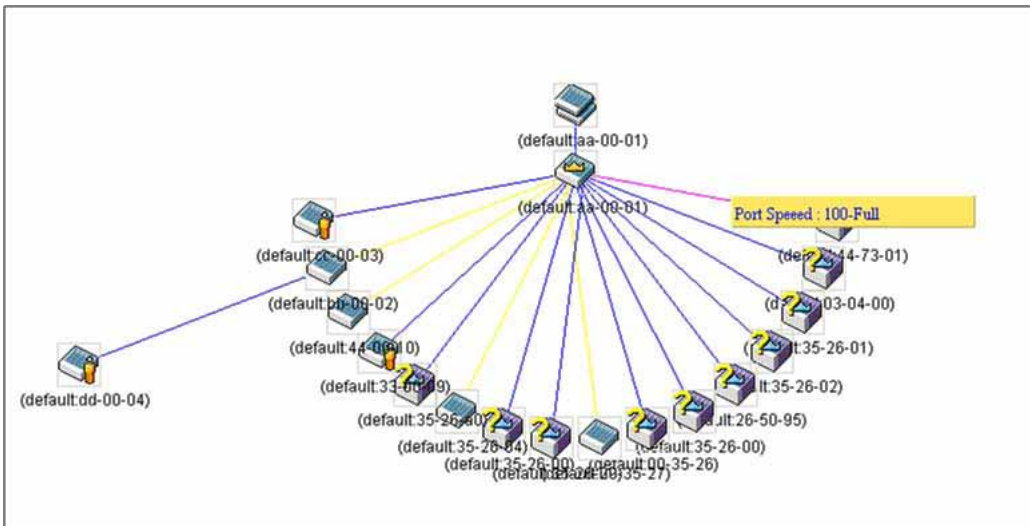


図 7.2-22　ツールヒントを利用したポート速度の表示

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

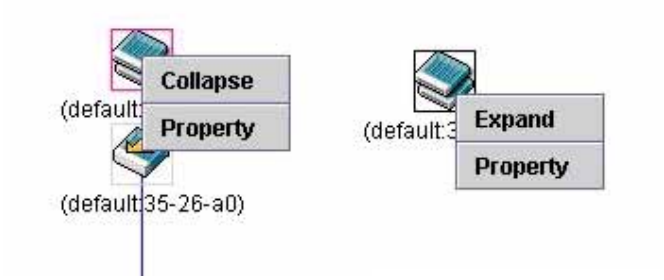


図 7.2-23　グループアイコン上での右クリック

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。

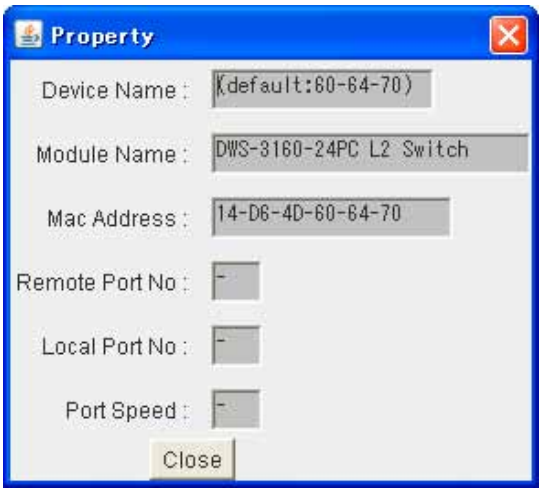


図 7.2-24　Property 画面

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

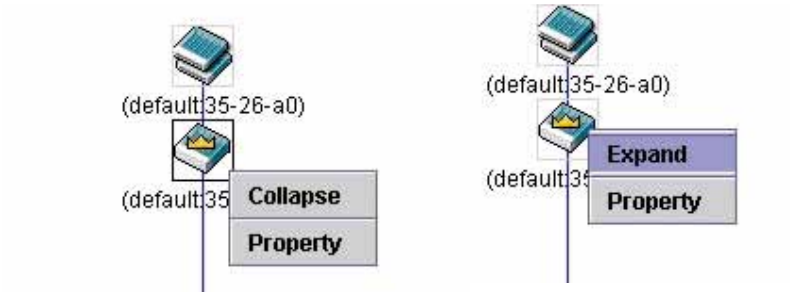


図 7.2-25　Commander スイッチアイコン上での右クリック

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

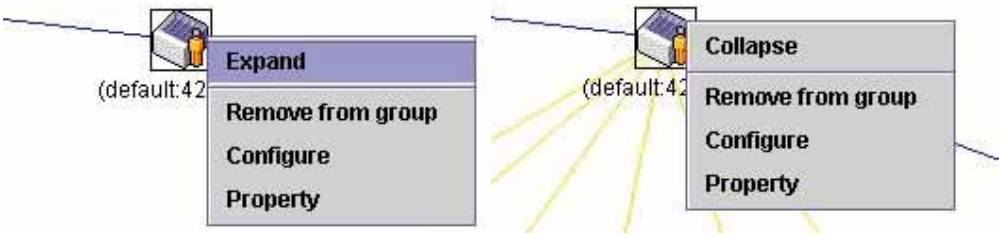


図 7.2-26　Member スイッチアイコン上での右クリック

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

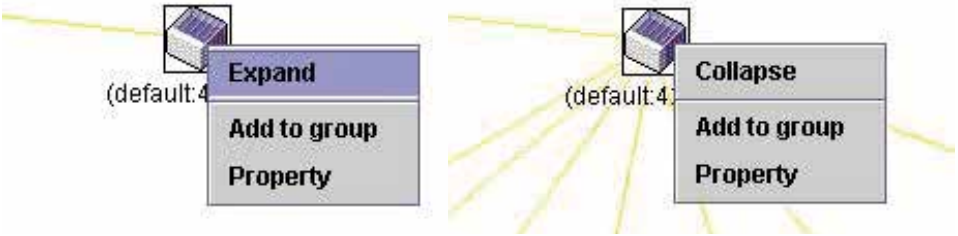


図 7.2-27　Candidate スイッチアイコン上での右クリック

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 7.2-28　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 7.2-29　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 7.2-30　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 7.2-31　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。

Management > 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 7.2-32　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。

Management > 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 7.2-33　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）

CS は、MS から指定したサーバに送信したログファイルを依頼することができます。

Management > 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 7.2-34　Upload Log File 画面

ログを格納する「Server IP Address」と MS のログファイルの「Path\Filename」を入力します。「Upload」ボタンをクリックすると TFTP サーバにログファイルを送信します。

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。

本スイッチシリーズは、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 v1 と SNMP v2c 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 v1 と SNMP v2c 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 V3」メニューから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 設定は、Web マネージャの「SNMP Settings」フォルダ下のメニューから行います。SNMP 権限を持ちスイッチへのアクセスを許されたワークステーションに制限を設けることも可能です。

SNMP Global Settings（SNMP グローバル設定）

SNMP グローバルステート設定を「Enabled」（有効）または「Disabled」（無効）にします。

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

図 7.2-35　SNMP Global Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
SNMP State	SNMP 機能を使用するためには本オプションを「Enabled」（有効）にします。

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

SNMP Trap Settings（SNMP トラップ設定）

スイッチの SNMP 機能のトラップ設定を「Enabled」（有効）または「Disabled」（無効）にします。

1. **Management > SNMP Settings > SNMP Trap 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 7.2-36　SNMP Traps Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
SNMP Traps	SNMP トラップ機能を使用するためには本オプションを「Enabled」（有効）にします。
SNMP Authentication Trap	SNMP 認証トラップ機能を使用するためには本オプションを「Enabled」（有効）にします。
Linkchange Traps	SNMP リンクチェンジトラップ機能を使用するためには本オプションを「Enabled」（有効）にします。
Coldstart Traps	SNMP コールドスタートトラップ機能を使用するためには本オプションを「Enabled」（有効）にします。
Warmstart Traps	SNMP ウォームスタートトラップ機能を使用するためには本オプションを「Enabled」（有効）にします。

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

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

SNMP リンクチェンジトラップを設定します。

1. **Management > SNMP Settings > SNMP Linkchange Traps 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。

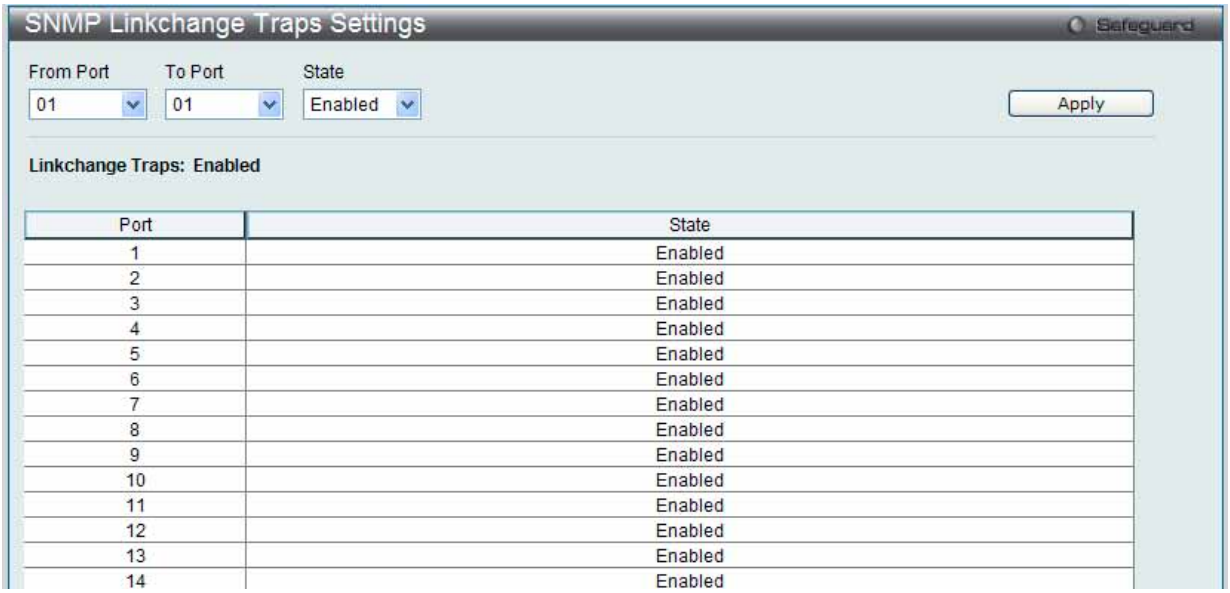


図 7.2-37　SNMP Linkchange Traps Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
From Port / To Port	使用する開始 / 終了ポートを選択します。
State	SNMP リンクチェンジトラップを「Enabled」（有効）または「Disabled」（無効）にします。

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

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

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

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

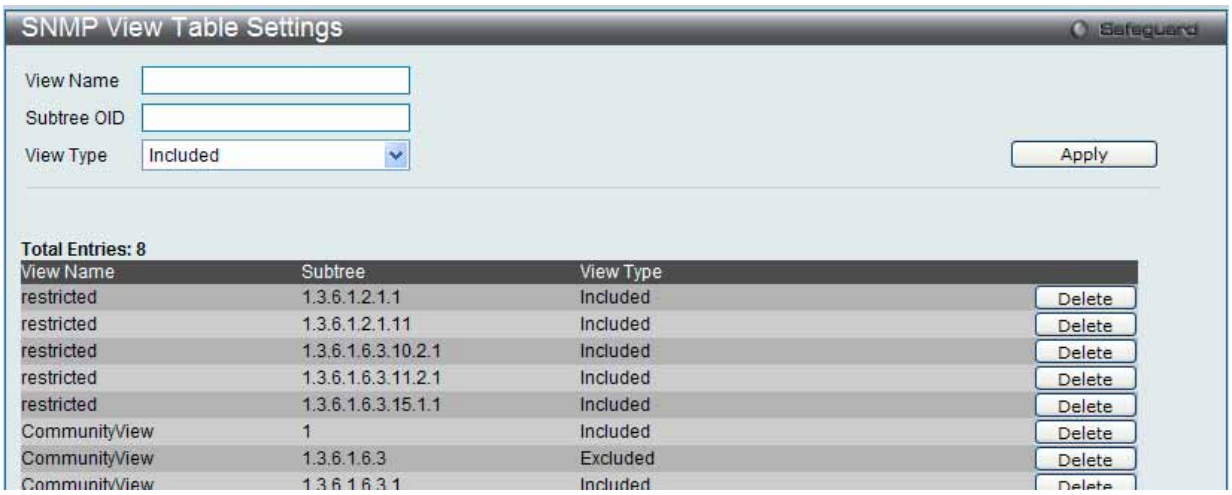


図 7.2-38　SNMP View Table Settings 画面

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。

2. 以下の項目を使用して設定および参照します。

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。

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。

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

SNMP Community Table Settings（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。

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

図 7.2-39　SNMP Community Table Settings 画面

2. 以下の項目を使用して設定および参照します。

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。

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。

エントリの設定
新しい SNMP コミュニティエントリを設定し、「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、エントリを削除します。

SNMP Group Table Settings（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。

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

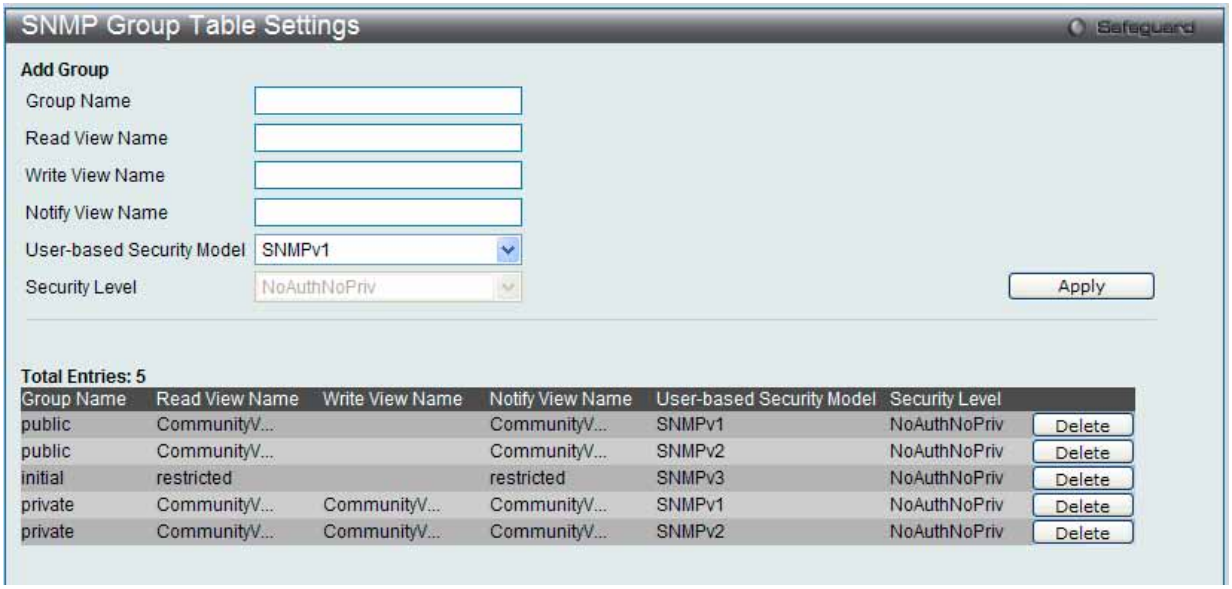


図 7.2-40　SNMP Group Table Settings 画面

2. 以下の項目を使用して設定および参照します。

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。

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。

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。

SNMP Engine ID Settings（SNMP エンジン ID 設定）

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

1. **Management > SNMP Settings > SNMP Engine ID Settings** の順にメニューをクリックし、以下の画面でスイッチの SNMP エンジン ID を表示します。

図 7.2-41　SNMP Engine ID Settings 画面

2. 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。

注意　エンジン ID 長は 10-64 で、0 ～ F の文字が許可されます。

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

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。

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

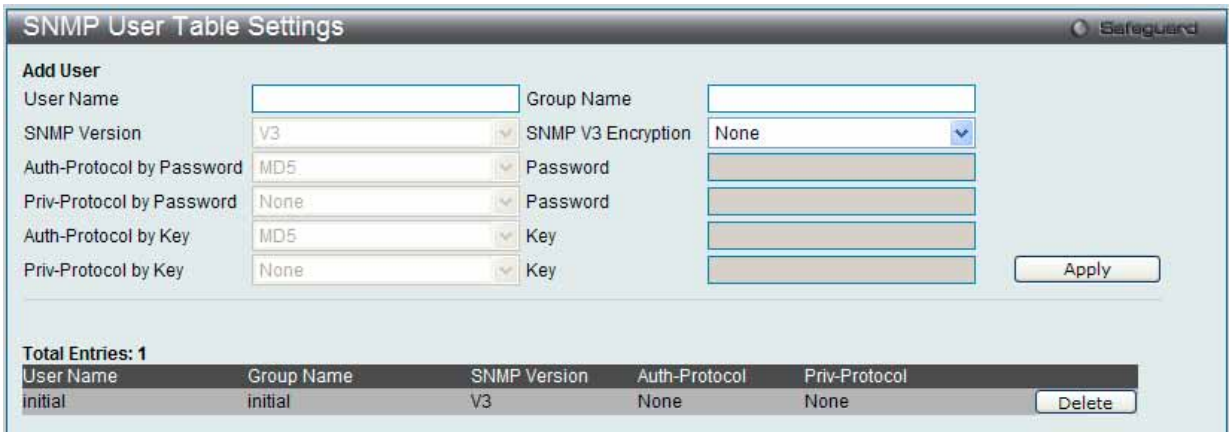


図 7.2-42　SNMP User Table Settings 画面

2. 以下の項目を使用して設定および参照します。

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。

項目	説明
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。

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。

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

IPv4 用の SNMP トラップの送信先を設定します。

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

図 7.2-43　SNMP Host Table Settings 画面

2. 以下の項目を使用して設定および参照します。

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。

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

SNMP v6Host Table Settings（SNMP v6 ホストテーブル設定）

IPv6 用の SNMP トラップの送信先を設定します。

1. **Management > SNMP Settings > SNMP v6Host Table Settings** の順にメニューをクリックし、以下の画面を表示します。

図 7.2-44　SNMP v6Host Table Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Host IPv6 Address	スイッチの SNMP ホストとなるリモート管理ステーション（トラップの送信先）の IPv6 アドレスを入力します。
User-based Security Model	• SNMPv1 - SNMP バージョン 1 が使用されます。 • SNMPv2c - SNMP バージョン 2c が使用されます。 • SNMPv3 - SNMP バージョン 3 が使用されます。
Security Level	• NoAuthNoPriv - NoAuth-NoPriv セキュリティレベルが使用されます。 • 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。

エントリの削除

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

RMON Settings（RMON 設定）

スイッチにおける SNMP 機能の上昇 / 下降アラームトラップに対するリモートモニタリング (RMON) を「Enabled」（有効）または「Disabled」（無効）にします。

1. **Management > SNMP Settings > RMON 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 7.2-45　RMON Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
RMON Rising Alarm Trap	RMON 上昇アラームトラップ機能を使用するためには「Enabled」（有効）にします。
RMON Falling Alarm Trap	RMON 下降アラームトラップ機能を使用するためには「Enabled」（有効）にします。

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

Telnet Settings（Telnet 設定）

スイッチに Telnet 設定をします。

1. **Management > 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 7.2-46　Telnet Settings 画面

2. 以下の項目を使用して設定および参照します。

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 管理に使用される 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。

Web Settings（Web 設定）

スイッチに Web ステータスを設定します。

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

図 7.2-47　Web Settings 画面

2. 以下の項目を使用して設定および参照します。

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。

7.3 L2 Features（レイヤ 2 機能の設定）

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

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

サブメニュー	説明	参照ページ
VLAN（VLAN 設定）	802.1Q スタティック VLAN 設定を行います。以下のメニューがあります。 802.1Q VLAN Settings（802.1Q VLAN 設定）、802.1v Protocol VLAN（802.1v プロトコル VLAN）、Asymmetric VLAN Settings（Asymmetric VLAN 設定）、GVRP（GVRP の設定）、MAC-based VLAN Settings（MAC ベース VLAN 設定）、Private VLAN Settings（プライベート VLAN 設定）、PVID Auto Assign Settings（PVID 自動割り当て設定）、Voice VLAN（音声 VLAN）、VLAN Trunk Settings（VLAN トランク設定）、Browse VLAN（VLAN の参照）、Show VLAN Ports（VLAN ポートの参照）	102
QinQ（QinQ 設定）	Q-in-Q 機能を「Enabled」（有効）または「Disabled」（無効）にします。次のメニューがあります。 QinQ Settings（QinQ 設定）、VLAN Translation Settings（VLAN 変換機能の設定）	118
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。以下のメニューがあります。 STP Bridge Global Settings（STP ブリッジグローバル設定）、STP Port Settings（STP ポートの設定）、MST Configuration Identification（MST の設定）、STP Instance Settings（STP インタンス設定）、MSTP Port Information（MSTP ポート情報）	121
Link Aggregation （ポート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。以下のメニューがあります。 Port Trunking Settings（ポートトランキング設定）、LACP Port Settings（LACP ポートの設定）	130
FDB（FDB 設定）	スタティック FDB、MAC アドレスエージングタイム、MAC アドレステーブルなどを設定します。以下のメニューがあります。 Static FDB Settings（スタティック FDB の設定）、MAC Notification Settings（MAC 通知設定）、MAC Address Aging Time Settings（MAC アドレスエージングタイムの設定）、MAC Address Table（MAC アドレステーブル）、ARP & FDB Table（ARP と FDB テーブル）	133
L2 Multicast Control （L2 マルチキャストコントロール）	IGMP Snooping、MLD Snooping の設定を行います。以下のメニューがあります。 IGMP Snooping（IGMP Snooping の設定）、IGMP Host Table（IGMP ホストテーブル）、MLD Snooping（MLD Snooping 設定）、MLD Host Table（MLD ホストテーブル）、Multicast VLAN（マルチキャスト VLAN）	138
Multicast Filtering （マルチキャストフィルタリング）	マルチキャストフィルタリングの設定を行います。以下のメニューがあります。 IPv4 Multicast Filtering（IPv4 マルチキャストフィルタリング）、IPv6 Multicast Filtering（IPv6 マルチキャストフィルタリング）、Multicast Filtering Mode（マルチキャストフィルタリングモード）	161
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。	170
LLDP（LLDP 設定）	LLDP 設定を行います。 LLDP Global Settings（LLDP グローバル設定）、LLDP Port Settings（LLDP ポート設定）、LLDP Management Address List（LLDP 管理アドレスリスト）、LLDP Basic TLVs Settings（LLDP ベーシック TLV 設定）、LLDP Dot1 TLVs Settings（LLDP Dot1 TLV 設定）、LLDP Dot3 TLVs Settings（LLDP Dot3 TLV 設定）、LLDP Statistics System（LLDP 統計情報システム）、LLDP Local Port Information（LLDP ローカルポート情報）、LLDP Remote Port Information（LLDP リモートポート情報）	173
NLB FDB Settings（NLB FDB 設定）	NLB 機能を設定します。	181

VLAN について

IEEE 802.1p プライオリティについて

IEEE 802.1p 標準規格において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で、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、タイムクリティカルなデータに依存するタイプのアプリケーションの品質は、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。

本スイッチでは、プライオリティタグ付きのパケットをご使用のネットワークでどのように扱うかを細かく調整することができます。プライオリティタグ付きのデータをキューの使用によって管理することにより、ご使用のネットワークのニーズに合わせて優先度を設定できます。1 つのキューに複数の異なるタグを使用したパケットを関連付ける方が効果のある場合もありますが、一般的には最高の優先度のキュー（キュー 7）には、プライオリティレベル 7 のパケットに割り当てることをお勧めします。プライオリティ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）機能をサポートし、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 とは

VLAN（Virtual Local Area Network : 仮想 LAN）とは、物理的なレイアウトではなく、論理的なスキームに従って構成されるネットワークトポロジです。VLAN 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、帯域を浪費しないでことにより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。

本スイッチシリーズにおける VLAN について

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。

本スイッチシリーズは IEEE 802.1Q 標準で規定する VLAN とポートベース VLAN をサポートします。ポートタグ取り機能は、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。必要性があれば、ポートベース VLAN のメンバポートの重複は許されています。

IEEE 802.1Q VLAN

用語の説明

- タグ付け - パケットのヘッダに 802.1Q VLAN 情報を挿入すること。
- タグ取り - パケットのヘッダから 802.1Q VLAN 情報を削除すること。
- イングレスポート - スイッチ上のパケットを受信するポート。VLAN の照合が行われます。
- イーグレスポート - 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つの種類のルールに基づいて決定されます。:
  イングレスルール - 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。
  イーグレスルール - パケットが送信される時にタグ付きかタグなしかを決定します。

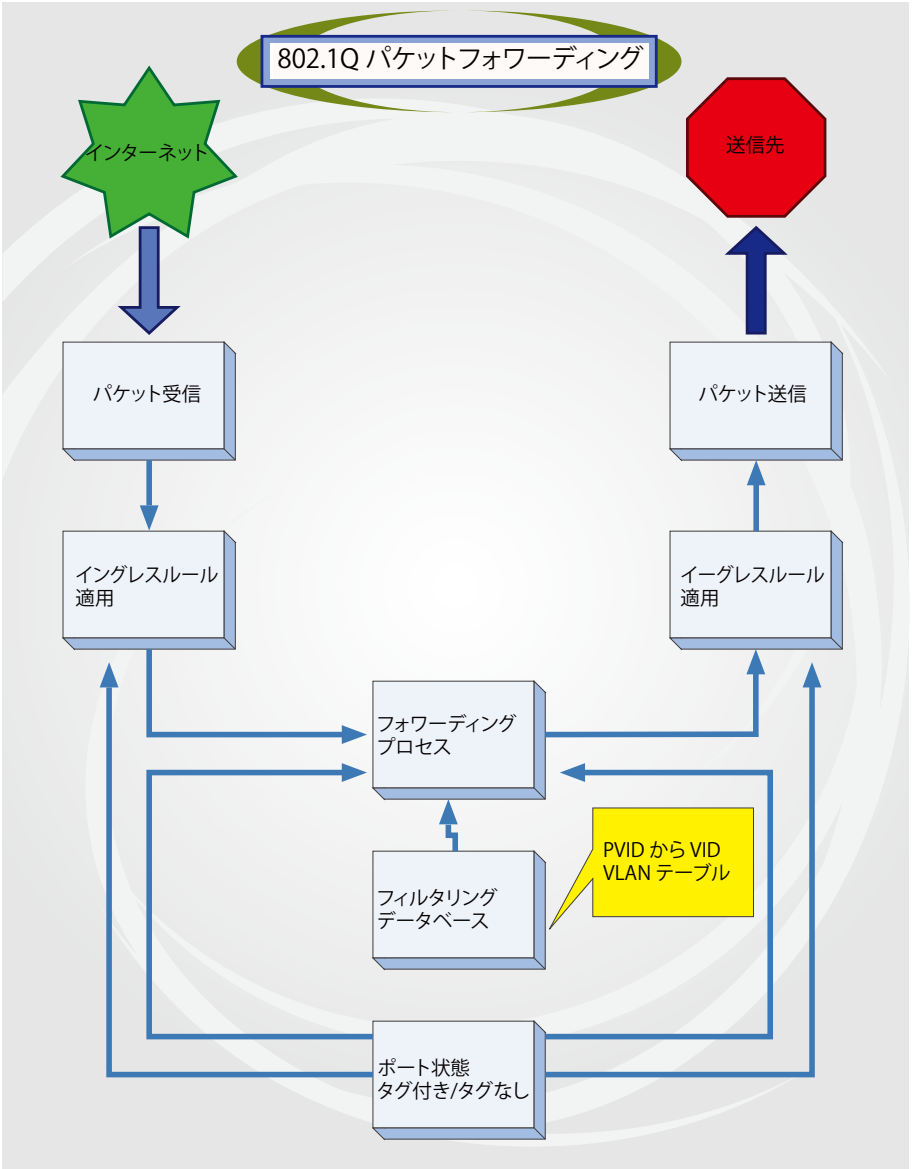


図 7.3-1　IEEE 802.1Q パケットフォワーディング

802.1Q VLAN タグ

次の図は 802.1Q VLAN のタグについて表示しています。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 0×8100 になります。つまり、パケットの EtherType フィールドが 0×8100 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 ビットから成ります。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 オクテット分長くなります。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。

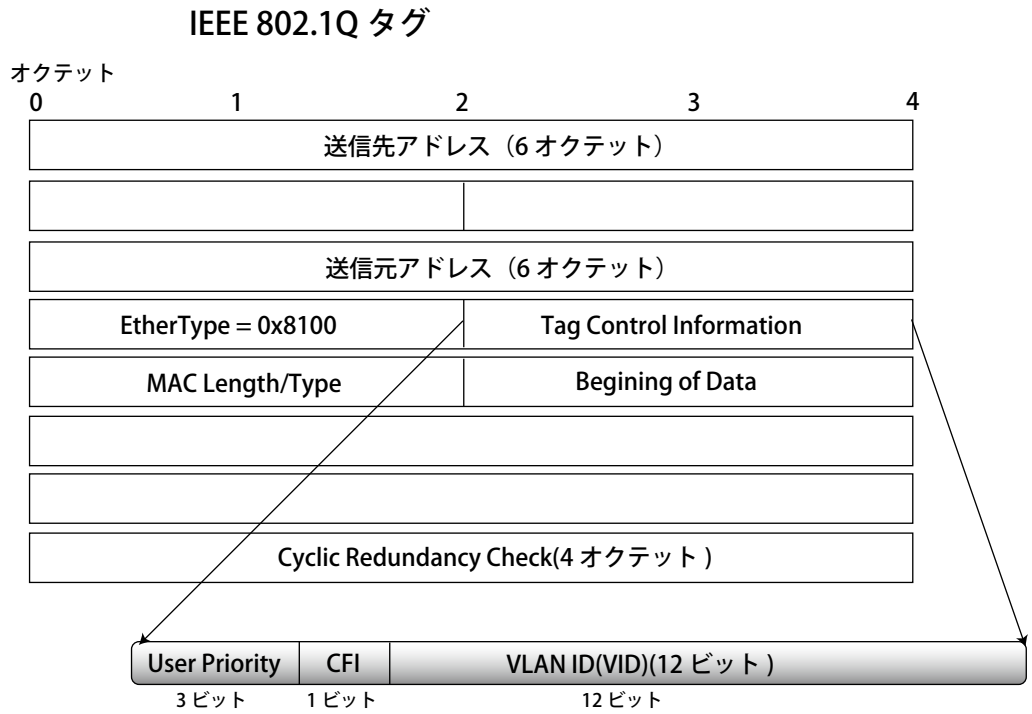


図 7.3-2　IEEE 802.1Q タグ

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

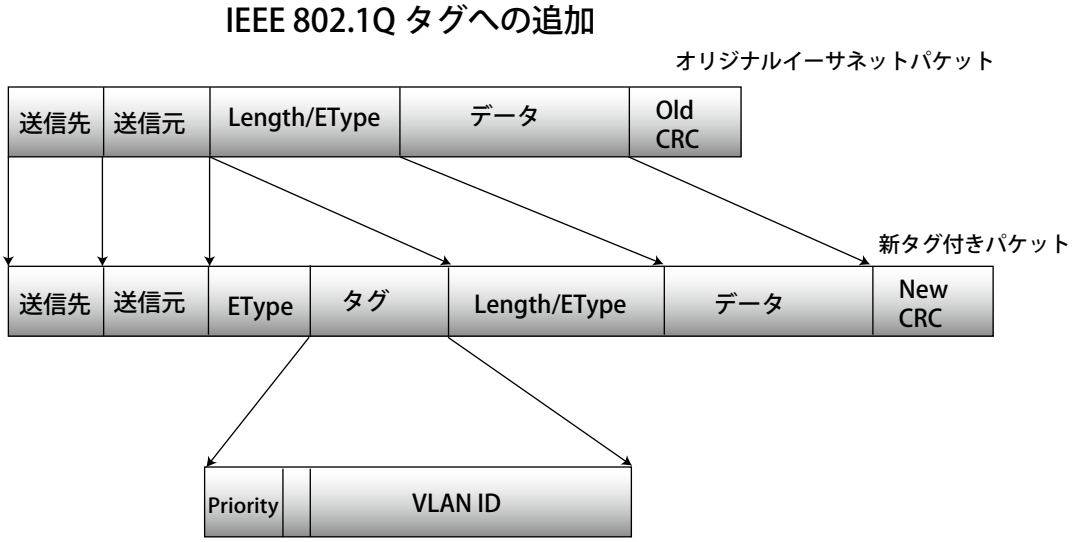


図 7.3-3　IEEE 802.1Q タグの挿入

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 がパケットの宛先のポートの 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 を元に決定されます。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。

タグ付きとタグなし

802.1Q に対応するスイッチのすべてのポートは、タグ付きかタグなしに設定できます。
タグ付きのポートは受信、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。

イングレスフィルタリング

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

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

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

本プロセスは、イングレスフィルタリングと呼ばれ、同じイングレスポートと同じ 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。新しい VLAN がポートベースモードで設定される時、そのポートは自動的に「default」VLAN から削除されます。

パケットは VLAN 間を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 1 つも 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。

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 VLAN 2 に所属しているか（つまり VLAN 2 パケットを受け取れるか）どうかを確認します。ポート 10 が VLAN 2 のメンバでない場合は、スイッチはそのパケットを廃棄します。メンバである場合、パケットは送信されます。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。

VLAN（VLAN 設定）

802.1Q VLAN Settings（802.1Q VLAN 設定）

802.1Q VLAN を設定します。

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

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。

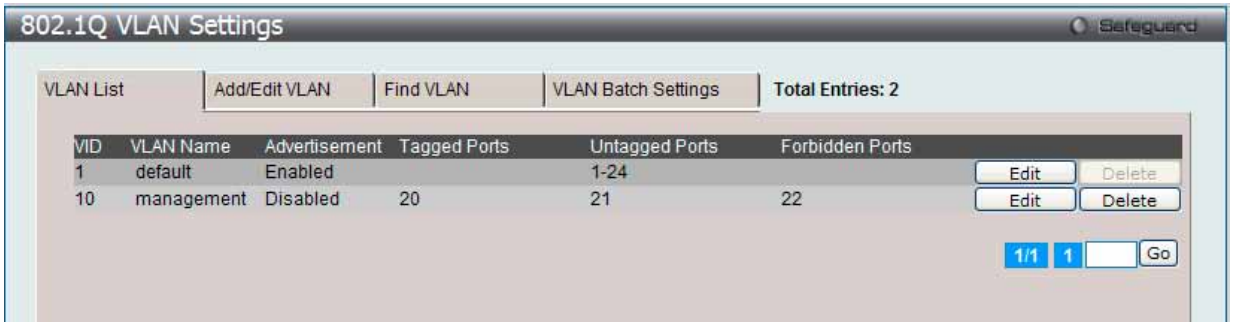


図 7.3-4　802.1Q VLAN Settings - VLAN List タブ画面

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

エントリの削除

対象のエントリの行の「Delete」ボタンをクリックします。

新規 / 既存の 802.1Q VLAN の登録

「Add/Edit VLAN」タブをクリックします。新しいタブが以下の通り表示され、ポートの設定、および新しい VLAN の固有名と番号を割り当てることができます。

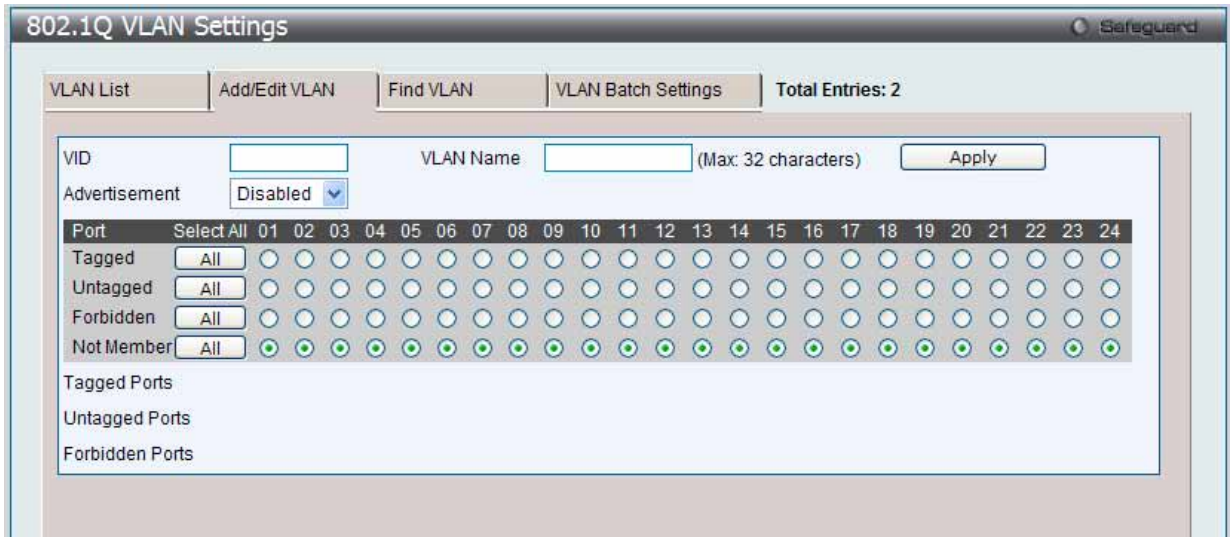


図 7.3-5　802.1Q VLAN Settings - Add/Edit VLAN タブ画面（Add）

802.1Q VLAN の編集

1. 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。

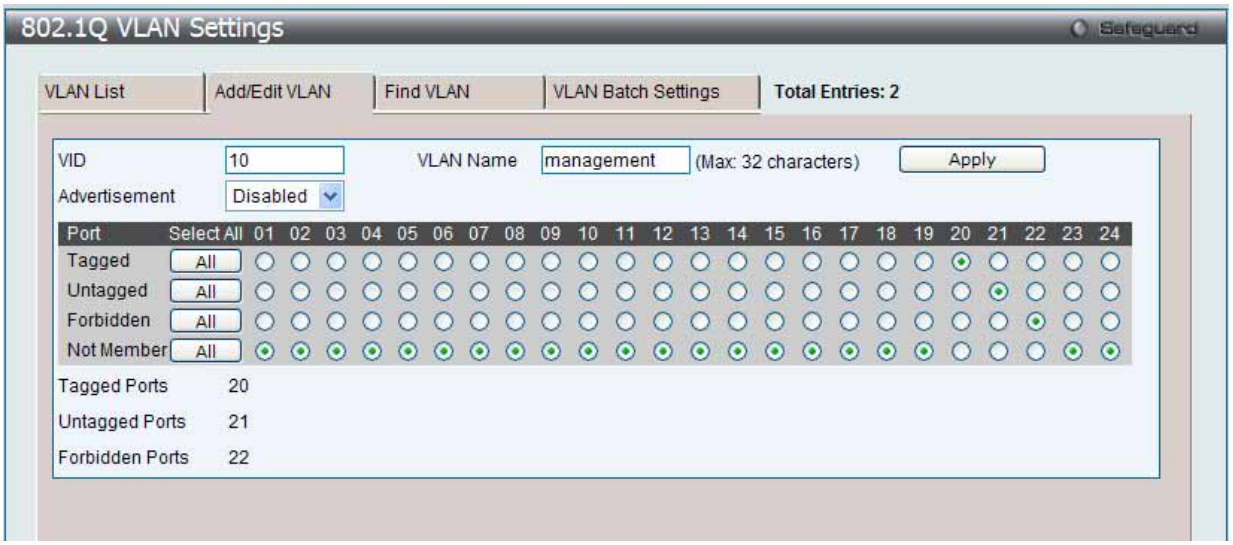


図 7.3-6　802.1Q VLAN Settings - Add/Edit VLAN タブ画面（Edit）

「802.1Q VLAN Settings」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。

「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

1. 「Find VLAN」タブをクリックします。以下の画面が表示されます。

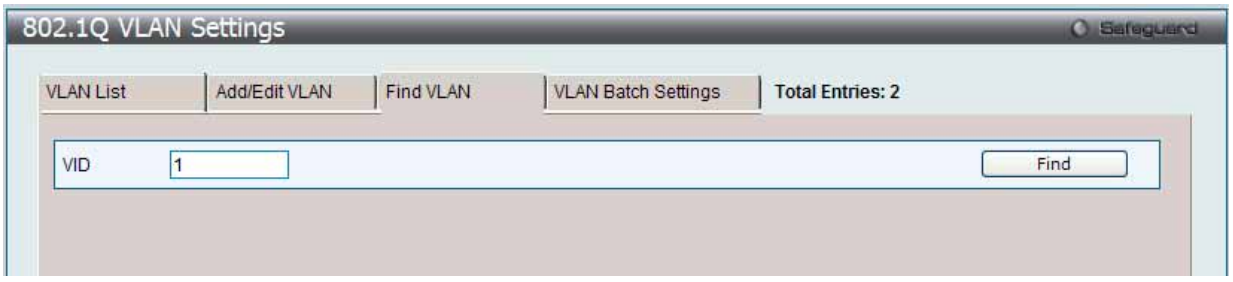


図 7.3-7　802.1Q VLAN Settings - Find VLAN タブ画面

2. 「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

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

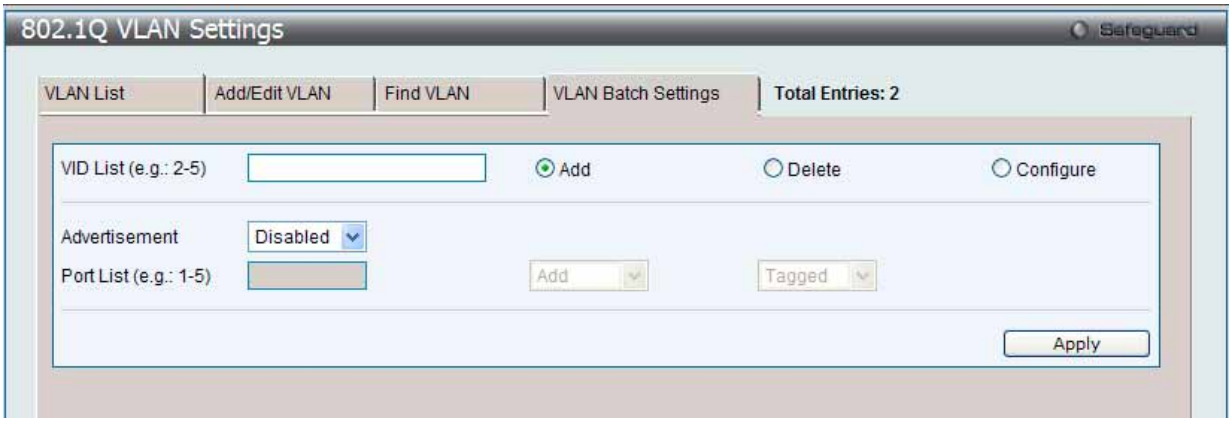


図 7.3-8　802.1Q VLAN Settings - VLAN Batch Settings タブ画面

2. 以下の項目を使用して設定および参照します。

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。 • Configure - 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。

注意　本スイッチは、最大 4K スタティック VLAN の設定をサポートしています。

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複数の 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。

1. **L2 Features > VLAN > 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。

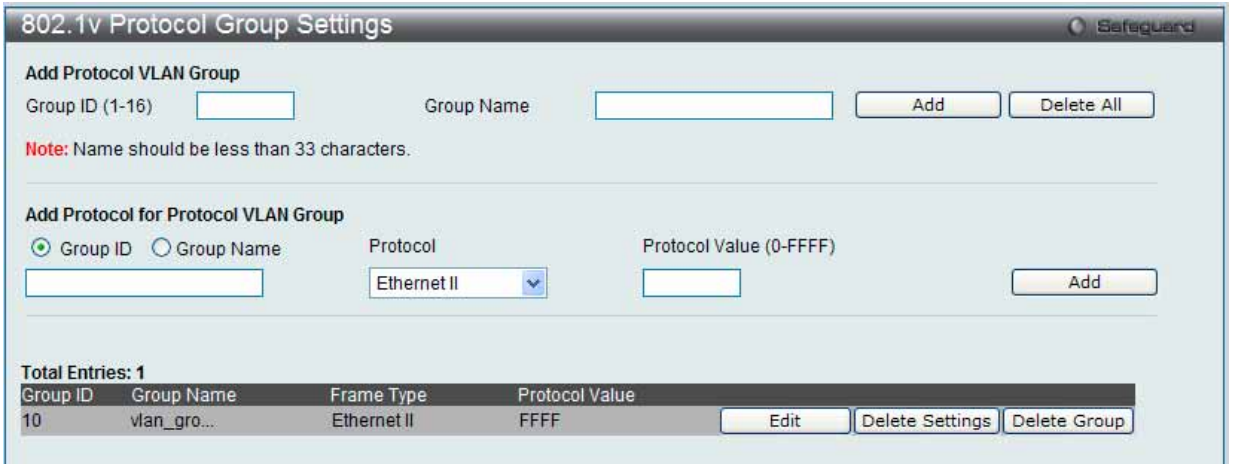


図 7.3-9　802.1v Protocol Group Settings 画面

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。

2. 以下の項目を使用して設定および参照します。

項目	説明
Add Protocol VLAN Group	
Group ID (1-16)	グループの ID 番号を 1-16 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 1-8 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、IEEE802.3 LLC および 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。入力形式は 0x0 から 0xffff です。オクテット文字列は、フレームタイプによって、以下に示す値の 1 つを持っています。 • Ethernet II - 16 ビット (2 オクテット) の 16 進数です。例えば、IPv4 は 800、IPv6 は 86dd、ARP は 806 などです。 • IEEE802.3 SNAP - 16 ビット (2 オクテット) の 16 進数です。 • IEEE802.3 LLC - 2 オクテットの IEEE 802.3 Link Service Access Point（LSAP）ペアです。はじめのオクテットは、Destination Service Access Point（DSAP）のための値であり、2 番目のオクテットは送信元のための値です。

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。

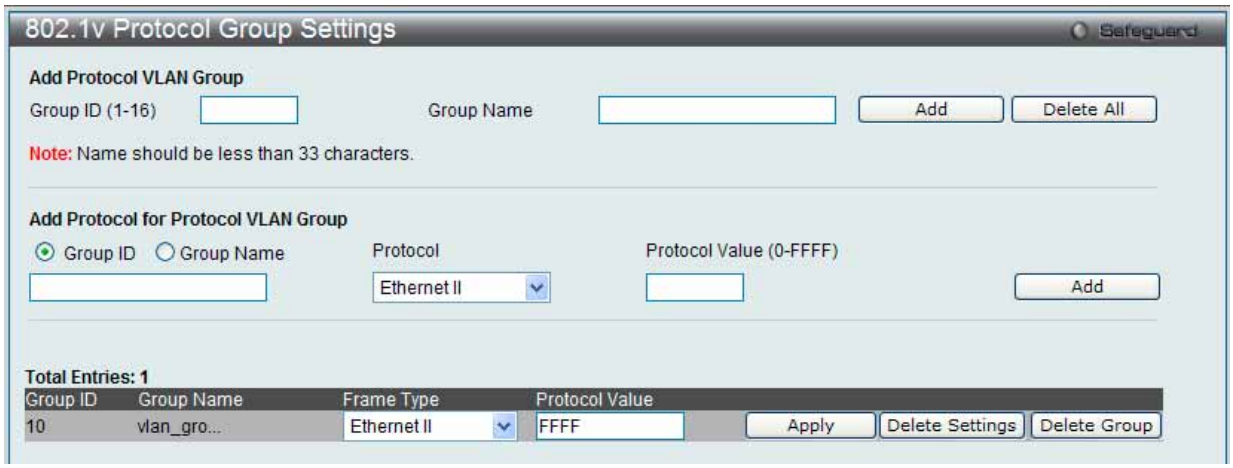


図 7.3-10　802.1v Protocol Group Settings 画面 - Edit

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 > VLAN > 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。

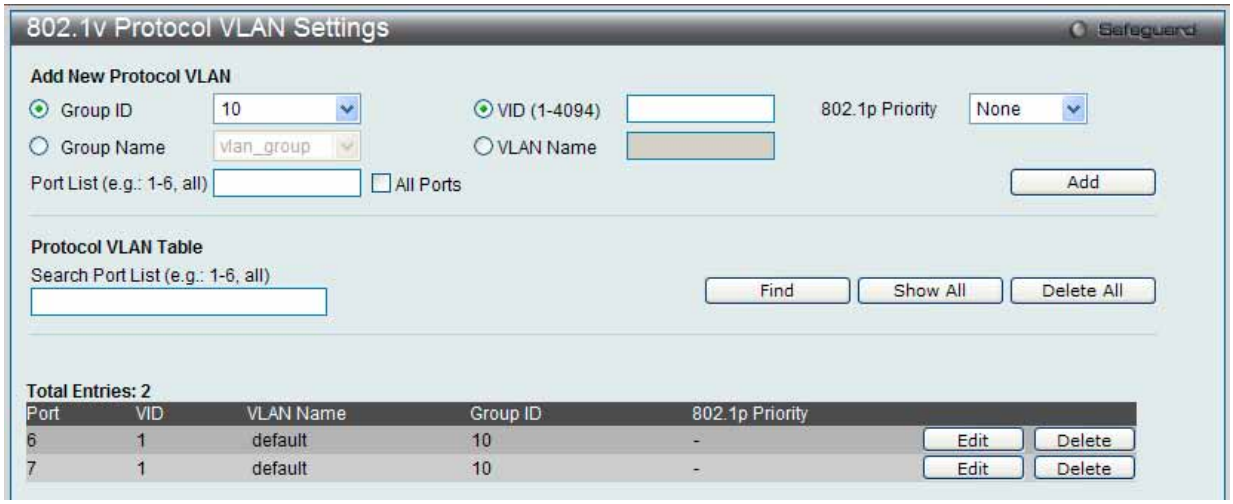


図 7.3-11　802.1v Protocol VLAN Settings 画面

以下の項目を使用して設定および参照します。

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「7.5 QoS（QoS 機能の設定）」（189 ページ）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。

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。

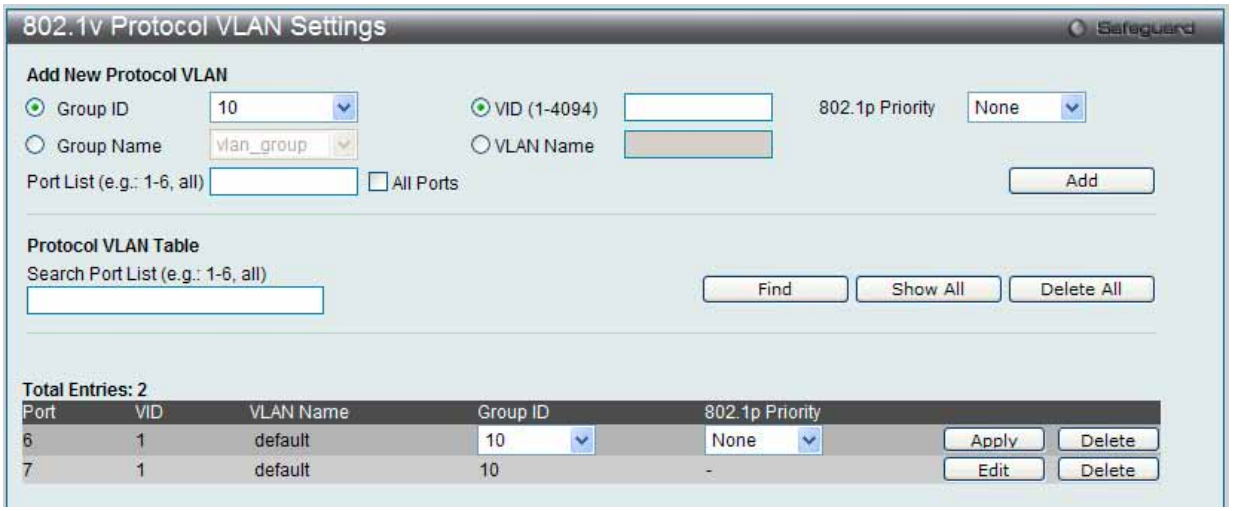


図 7.3-12　802.1v Protocol VLAN Settings 画面 - Edit

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 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。

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となる例です。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、または機密に関連する必要性があり、クライアント間のトラフィックを分ける場合です。

1. **L2 Features > VLAN > 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。

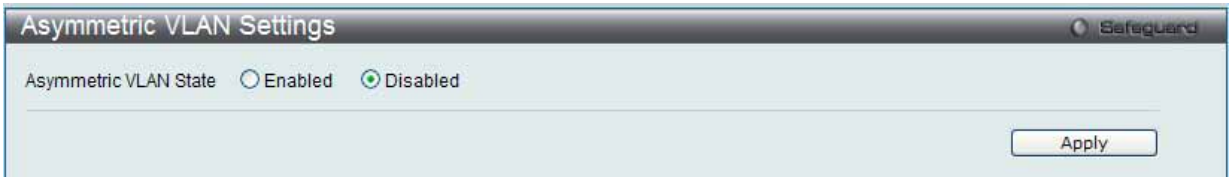


図 7.3-13　Asymmetric VLAN Settings 画面

2. 「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。

GVRP（GVRP の設定）

GVRP Global Settings（GVRP グローバル設定）

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。

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

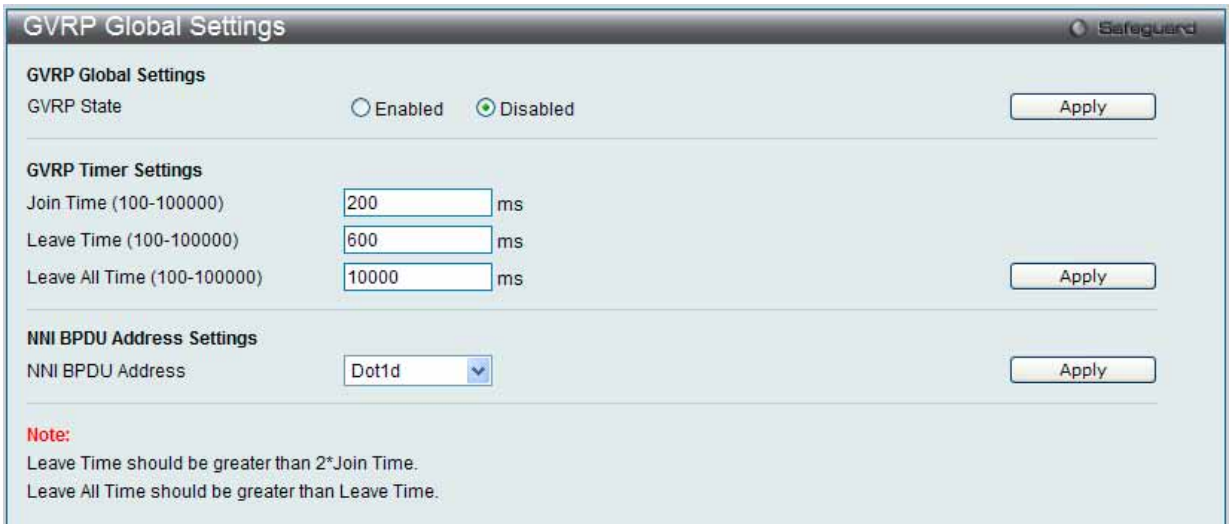


図 7.3-14　GVRP Global Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
GVRP Global Settings	
GVRP State	GVRP 状態を有効または無効にして「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）
GVRP Timer Settings	
Join Time (100-100000)	Join Time（ミリ秒）を入力します。
Leave Time (100-100000)	Leave Time（ミリ秒）を入力します。
Leave All Time (100-100000)	Leave All Time（ミリ秒）を入力します。
NNI BPDU Address Settings	
NNI BPDU Address (100-100000)	サービス提供サイトにおける GVRP の BPDU プロトコルアドレスを決定します。802.1d GVRP アドレス、802.1ad サービスプロバイダの GVRP アドレスまたはユーザ定義のマルチキャストを使用します。ユーザ定義アドレスの範囲は 0180C2000000-0180C2FFFFFF です。

「Apply」ボタンをクリックし、デバイスに GVRP 設定を適用します。

注意　「Leave time」は「Join time」の 2 倍以上である必要があります。「Leave All Time」は「Leave Time」より大きくする必要があります。

GVRP Port Settings（GVRP ポート設定）

GVRP ポートパラメータを設定します。

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

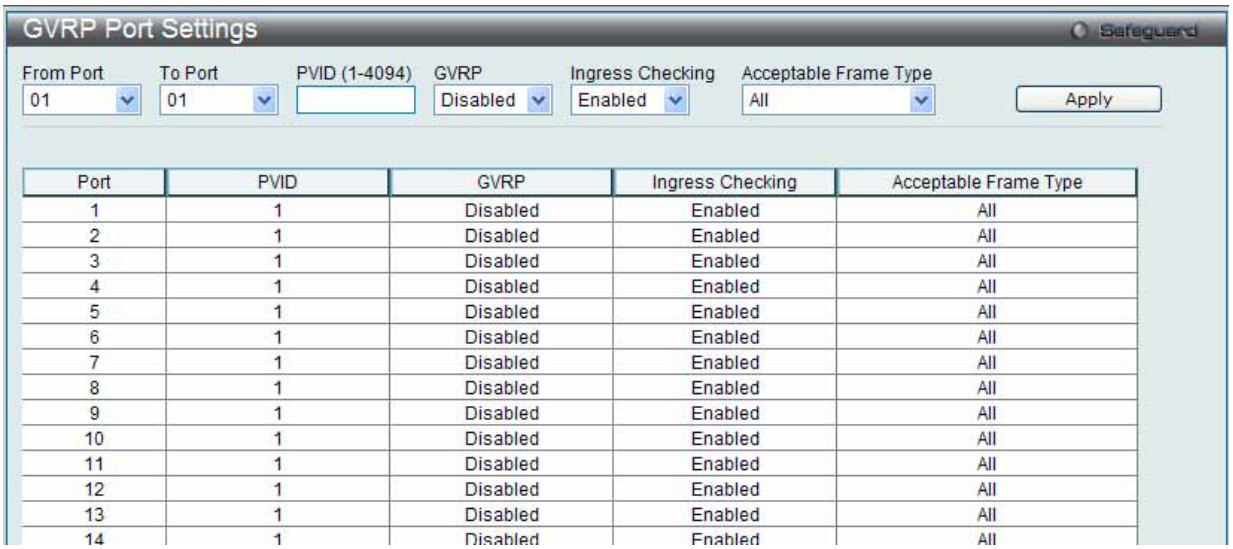


図 7.3-15　GVRP Port Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
From Port / To Port	ポートベース VLAN に含まれ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）に割り当てられています。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。 もし、ポートがタグ付きのフレームのみ受け付けるよう指定されていて（Tagging 指定）、タグなしのパケットがそのポートに送信されてきたら、ポートは PVID を使用してタグ内に VID を書き込み、802.1Q タグを追加します。パケットが宛先に届いた時、受信するデバイスは PVID を VLAN に送出するか否かを決定するために使用します。パケットを受信するポートの Ingress フィルタリングが有効である場合、ポートは到着したパケットの VID と自分の PVID を比較します。2 つが一致しないと、ポートはパケットを廃棄します。2 つが一致すると、ポートはパケットを受信します。
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	プルダウンメニューでポートを有効にすると、VLAN メンバシップを持つ入力パケット内の VID タグを比較します。イングレスチェックが有効であり、受信ポートがフレームの VLAN のメンバポートでないと、フレームは破棄されます。
Acceptable FrameType	ポートが受け入れるフレームの種類を設定します。 • Tagged Only - タグ付きフレームのみポートは受け入れます。 • All - タグ付き、タグなし両方のフレーム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。

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 の下で送信されます。

1. **L2 Features > VLAN > MAC-based 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。

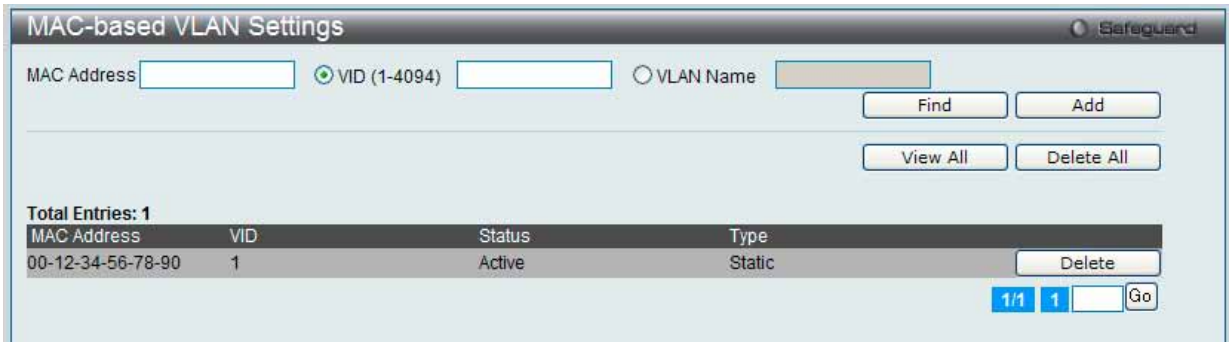


図 7.3-16　MAC-based VLAN Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
MAC Address	ユニキャスト MAC アドレスを入力します。
VLAN ID	VLAN ID 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。

エントリの参照

「View All」ボタンをクリックして、すべての定義済みエントリを表示します。

Private VLAN Settings（プライベート VLAN 設定）

プライベート VLAN はプライマリ VLAN、Isolated VLAN、および多くのコミュニティ VLAN から作成されます。プライベート VLAN ID はプライマリ VLAN の VLAN ID によって示されます。コマンドはセカンダリ VLAN をプライマリ VLAN と関連付けるため、または切り離すために使用されます。

セカンダリ VLAN は複数のプライマリ VLAN に関連付けることはできません。プライマリ VLAN のタグなしメンバポートはプロミスキャスポートとして名前をつけられます。プライマリ VLAN のタグ付きメンバポートはトランクポートとして名前をつけられます。プライベート VLAN のプロミスキャスポートは他のプライベート VLAN のプロミスキャスポートになることはできません。プライマリ VLAN メンバポートは、同時にセカンダリ VLAN メンバであることはできません。逆もまた同様です。セカンダリ VLAN は、タグなしのメンバポートのみを含むことができます。セカンダリ VLAN のメンバポートは、他のセカンダリ VLAN のメンバであることはできません。VLAN がセカンダリ VLAN としてプライマリ VLAN に関連付けされる場合、プライマリ VLAN のプロミスキャスポートはセカンダリ VLAN のタグなしメンバとして動作し、プライマリ VLAN のトランクポートはセカンダリ VLAN のタグ付きメンバとして動作します。通知を使用してセカンダリ VLAN を指定することはできません。プライマリ VLAN だけがレイヤ 3 インタフェースとして設定できます。プライベート VLAN メンバポートをトラフィックセグメンテーション機能に設定できません。

プライベート VLAN のパラメータを設定します。

1. **L2 Features > VLAN > Private 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。

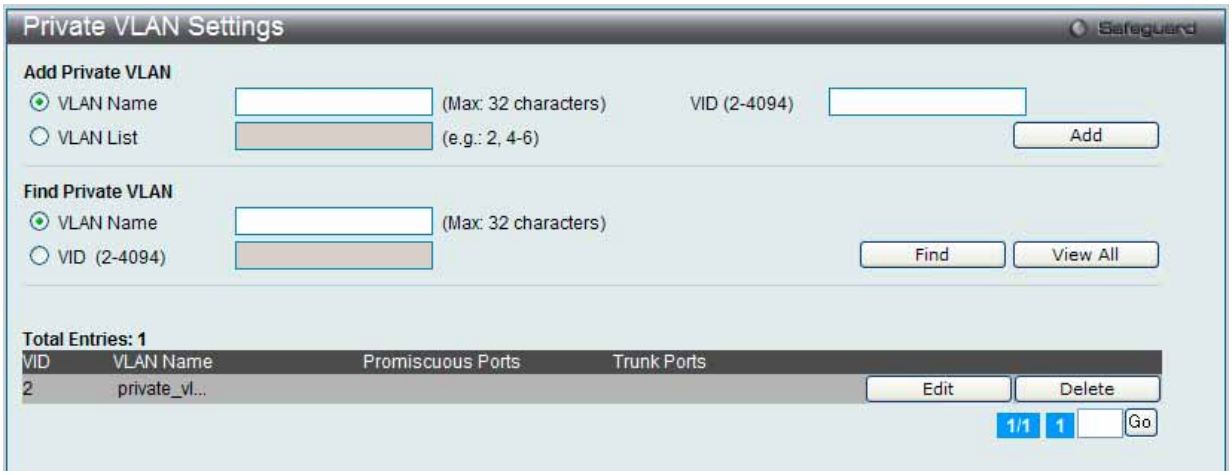


図 7.3-17　Private VLAN Settings 画面

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

2. 以下の項目を使用して設定および参照します。

項目	説明
VLAN Name	VLAN 名を入力します。
VID (2-4094)	VID 値を入力します。
VLAN List	VLAN ID を入力します。

エントリの新規登録

「Add Private VLAN」セクションでプライベート VLAN に登録する「VLAN Name」/「VID」または「VLAN List」を指定後、「Add」ボタンをクリックします。

エントリの検索

「Find Private VLAN」セクションで「VLAN Name」または「VID」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。「View All」ボタンをクリックすると、すべての定義済みエントリを表示します。

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 7.3-18　Private VLAN Settings 画面 - Edit

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

2. 以下の項目を使用して設定および参照します。

項目	説明
Secondary VLAN Type	プルダウンメニューを使用してセカンダリ VLAN のタイプ（「Isolated」または「Community」）を選択します。
Secondary VLAN Name	セカンダリ VLAN 名を入力します。
Secondary VLAN List	セカンダリ VLAN ID のリストを入力します。

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

View Private VLAN List リンクをクリックすると、すべてのプライベート VLAN を表示します。

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。

1. **L2 Features > VLAN > 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 7.3-19　PVID Auto Assign Settings 画面

2. 「Enabled」（有効）または「Disabled」（無効）を選択し、「Apply」ボタンをクリックして、デバイスに設定を適用します。

Voice VLAN（音声 VLAN）

Voice VLAN Global Settings（音声 VLAN グローバル設定）

音声 VLAN は、IP 電話からの音声トラフィックを送信するのに使用される VLAN です。不規則にデータを送信すると IP 電話の音の品質を低下させるため、音声トラフィックの QoS（Quality of Service）が音声パケットの伝送優先度を通常のトラフィックより確実に高くなるように設定する必要があります。

スイッチは、送信元 MAC アドレスをチェックすることで受信パケットが音声パケットであるかどうか判断します。パケットの送信元 MAC アドレスがシステムによって定義される OUI（Organizationally Unique Identifier : 組織で一意な識別子）アドレスを受諾すると、パケットは音声パケットとして判断されて、音声 VLAN に送信されます。

音声 VLAN をグローバルに有効 / 無効にします。

L2 Features > VLAN > Voice VLAN > Voice VLAN Global 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 7.3-20　Voice VLAN Global Settings 画面

3. 以下の項目を使用して設定および参照します。

項目	説明
Voice VLAN State	音声 VLAN の状態を「Enabled」（有効）または「Disabled」（無効）にします。
Voice VLAN Name	音声 VLAN 名を指定します。
Voice VID (1-4094)	音声 VLAN の VLAN ID を指定します。
Priority	音声 VLAN の優先度（0-7）を指定します。優先度の初期値は 5 です。
Aging Time (1-65535)	エージングタイム（1-65535 分）を指定します。初期値は 720（分）です。エージングタイムは、ポートが自動 VLAN メンバである場合に音声 VLAN からポートを削除するために使用されます。最後の音声デバイスが、トラフィックの送信を止めて、この音声デバイスの MAC アドレスがエージングタイムに到達すると、音声 VLAN エージングタイマが開始されます。ポートは音声 VLAN のエージングタイム経過後に音声 VLAN から削除されます。音声トラフィックがエージングタイム内に再開すると、エージングタイマは停止し、リセットされます。
Log State	音声 VLAN ログの送信を「Enabled」（有効）または「Disabled」（無効）にします。

音声 VLAN の有効化

「Voice VLAN State」を「Enabled」にして音声 VLAN を有効にする VLAN を「Voice VLAN Name」または「Voice VID」で指定後、「Apply」ボタンをクリックします。

音声 VLAN のパラメータ設定

音声 VLAN の有効後、「Priority」、「Aging Time」または「Log State」を設定後、「Apply」ボタンをクリックします。

Voice VLAN Port Settings（音声 VLAN のポート設定）

ポートの音声 VLAN 情報を表示します。

1. **L2 Features > VLAN > Voice VLAN > Voice VLAN 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。

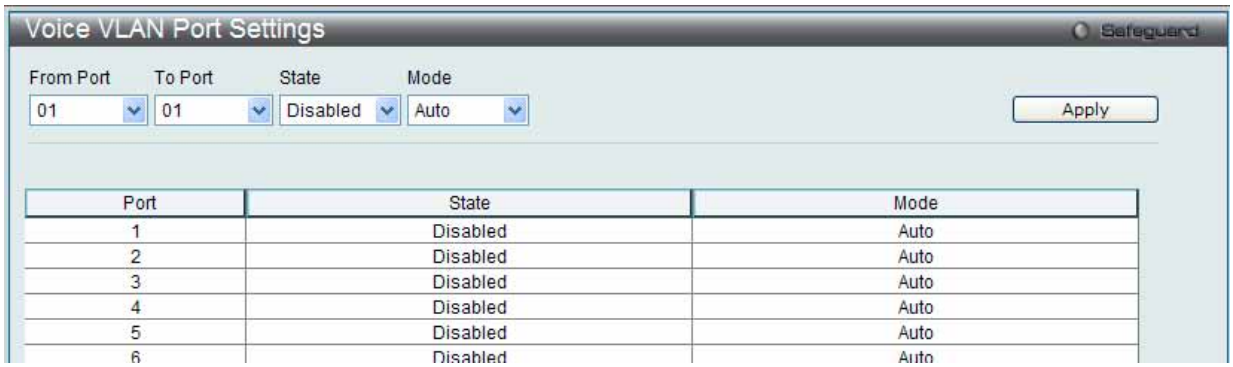


図 7.3-21　Voice VLAN Port Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
From Port / To Port	表示するポート範囲を選択します。
State	ポートの状態を「Enabled」（有効）/「Disabled」（無効）に設定します。
Mode	ポートのモード（Auto または Manual）を設定します。

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

Voice VLAN OUI Settings（音声 VLAN OUI 設定）

ユーザ定義の音声トラフィックの OUI を設定します。

OUI は音声トラフィックを識別するの使用されます。多くの定義済み OUI があり、必要に応じて、さらにユーザ定義の OUI を設定できます。
ユーザ定義 OUI は定義済みの OUI と同じとすることはできません。

1. **L2 Features > VLAN > Voice VLAN > Voice VLAN OUI 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。

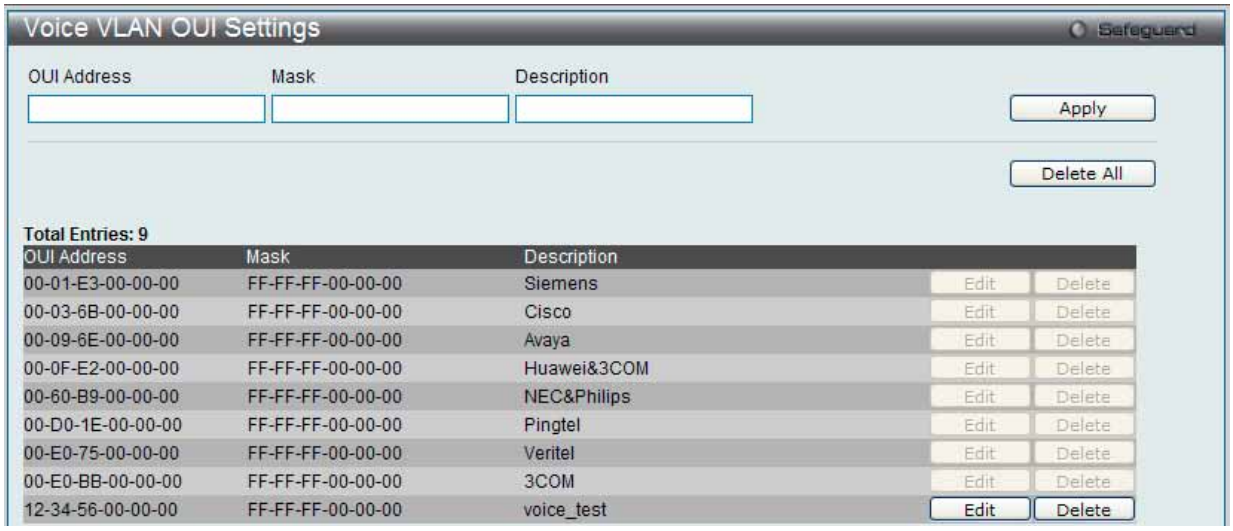


図 7.3-22　Voice VLAN OUI Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
OUI Address	ユーザ定義の OUI MAC アドレス。
Mask	ユーザ定義 OUI MAC アドレスマスク。
Description	ユーザ定義 OUI に関する説明文。

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

エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。または、「Delete All」ボタンをクリックして、表示されたユーザ定義の全エントリを削除します。

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。

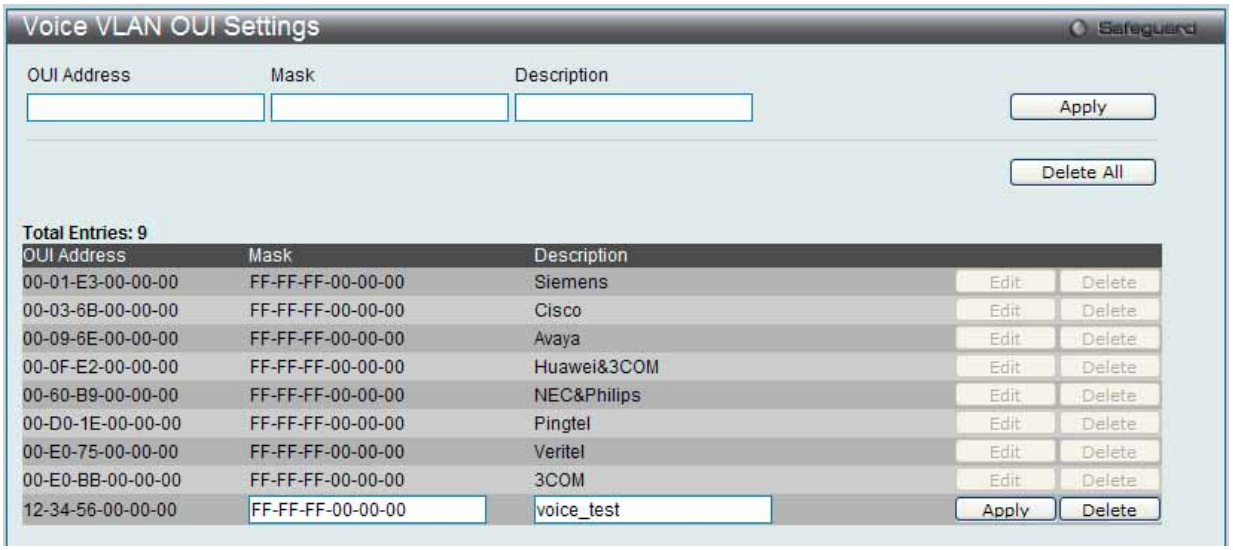


図 7.3-23　Voice VLAN OUI Settings 画面 - Edit

2. 項目を編集し、エントリの「Apply」ボタンをクリックします。

Voice VLAN Device（音声 VLAN デバイス）

ポートに接続する音声デバイスを表示します。開始時刻はデバイスがこのポートで検出される時間です。また、アクティベート時間はデバイスが一番最近トラフィックを送信した時間です。

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

図 7.3-24　Voice VLAN Device 画面

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。

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。

以下の図例を参照してください。

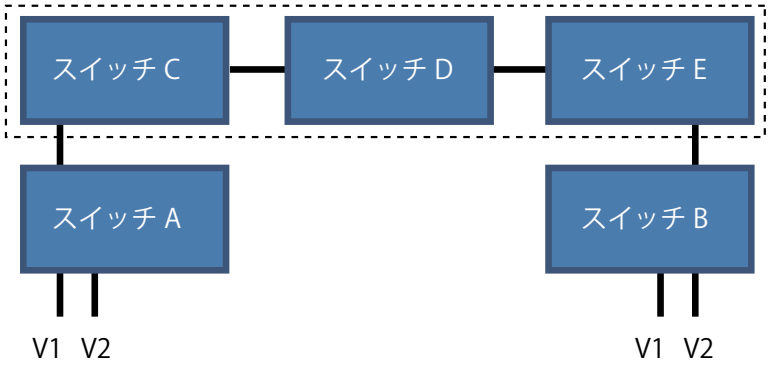


図 7.3-25　VLAN トランクの例題

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。

1. **L2 Features > VLAN > 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 7.3-26　VLAN Trunk Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
VLAN Trunk State	VLAN トランキングのグローバルな状態を「Enabled」（有効）または「Disabled」（無効）にします。
Port	設定するポートを指定します。 ・「Select All」ボタンをクリックすると、全ポートが設定に使用されます。 ・「Clear All」ボタンをクリックすると、全ポートの設定がクリアされます。

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。

Browse VLAN（VLAN の参照）

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。

1. **L2 Features > VLAN > Browse VLAN** メニューをクリックし、以下の画面を表示します。

図 7.3-27　Browse VLAN 画面

2. 画面上の「VID」に VLAN ID を入力し、「Find」ボタンをクリックします。

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

注意 本ページで使用される略記は、Tagged Port (T)、Untagged Port (U)、および Forbidden Port (F) です。

Show VLAN Ports（VLAN ポートの参照）

スイッチの VLAN ポートを VID ごとに表示します。

1. **L2 Features > VLAN > Show VLAN Ports** メニューをクリックし、以下の画面を表示します。

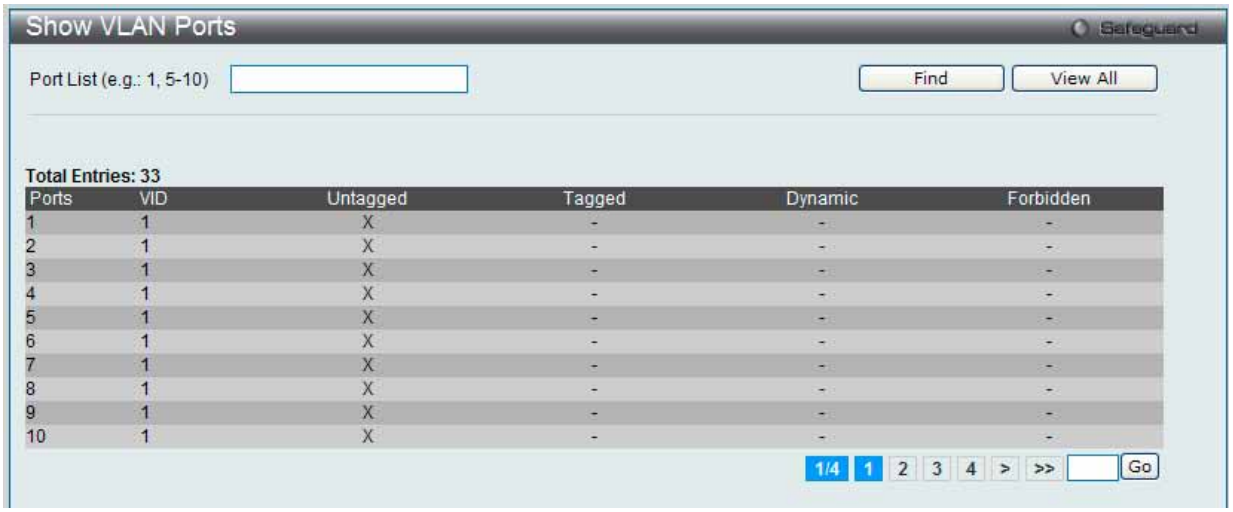


図 7.3-28　Show VLAN Ports 画面

2. 画面の上にある欄にポートまたはポート範囲を入力して、「Find」ボタンをクリックします。

「View All」ボタンをクリックして、すべての定義済みエントリを表示します。

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

QinQ（QinQ 設定）

ダブル VLAN または Q-in-Q 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。

ダブル 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。

以下にダブル VLAN 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 QinQ VLAN を使用した ISP ネットワークの例を示します。

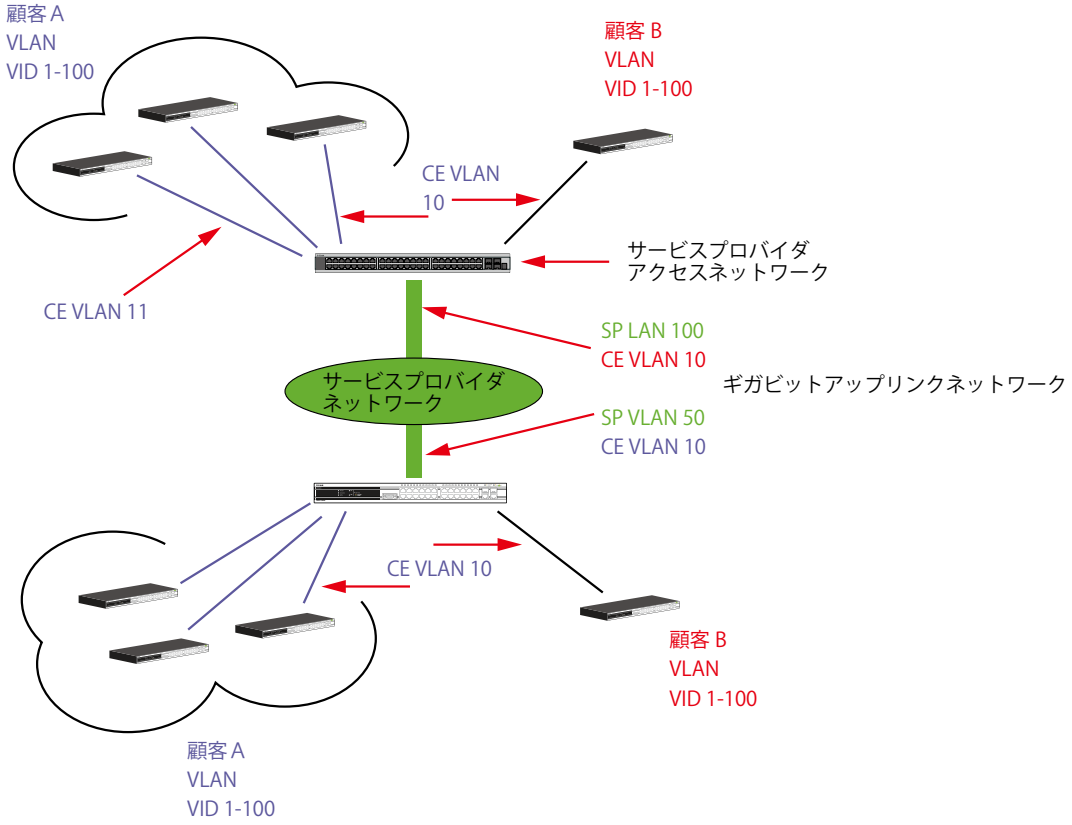


図 7.3-29　QinQ VLAN を使用したネットワーク例

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 QinQ 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 によって分割することができ、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調整します。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。

ダブル VLAN 使用時のルール

ダブル 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上の 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. スイッチにはダブル VLAN と通常の VLAN は混在できません。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、再設定が必要となります。
6. ダブル VLAN が有効とされると、GVRP を無効にする必要があります。
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取りされます。
8. スイッチがダブル VLAN モードにある場合、以下の機能は使用できなくなります。:
   - ゲスト VLAN
   - Web ベースのアクセス制御
   - IP マルチキャストルーティング
   - GVRP
   - 通常の 802.1Q VLAN 機能

QinQ Settings（QinQ 設定）

QinQ のパラメータを設定します。

1. **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。

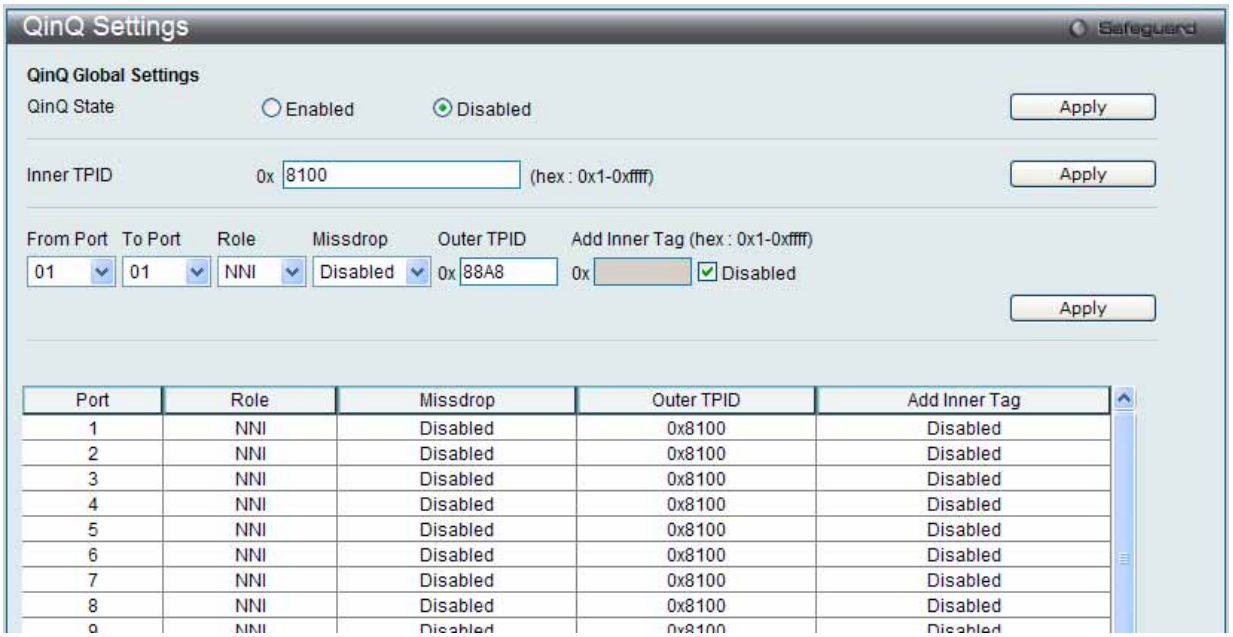


図 7.3-30　QinQ Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
QinQ State	QinQ 機能をグローバルに「Enabled」（有効）または「Disabled」（無効）にします。
Inner TPID	SP-VLAN タグに Inner TPID を入力します。
From Port/To Port	設定に使用するポート範囲を選択します。
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。
Missdrop	このオプションは、C-VLAN ベースの SP-VLAN 割り当ての Missdrop を「Enabled」（有効）または「Disabled」（無効）にします。 • Enabled - QinQ プロファイルにおけるどんな指定ルールにも一致しないパケットは廃棄されます。 • Disabled - パケットは転送され、受信ポートの PVID に割り当てられます。
Outer TPID	SP-VLAN タグに Outer TPID を入力します。
Add Inner Tag	「Disabled」のチェックを外して、「Inner Tag」が追加されるエントリを入力します。初期値では無効です。

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 Settings（VLAN 変換機能の設定）

C-VLAN と SP-VLAN 間の変換関係を追加します。

UNI ポートのイングレスでは、C-VLAN タグ付きパケットは、定義済みルールに従って追加または交換することで SP-VLAN のタグ付きパケットに変換されます。このポートのイーグレスでは、SP-VLAN タグは、C-VLAN タグに復元されるか、またはタグ取りされます。Inner 優先度フラグが受信ポートに対して無効になると、優先度は SP-VLAN タグの優先度となります。

1. **L2 Features > QinQ > VLAN Translation 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。

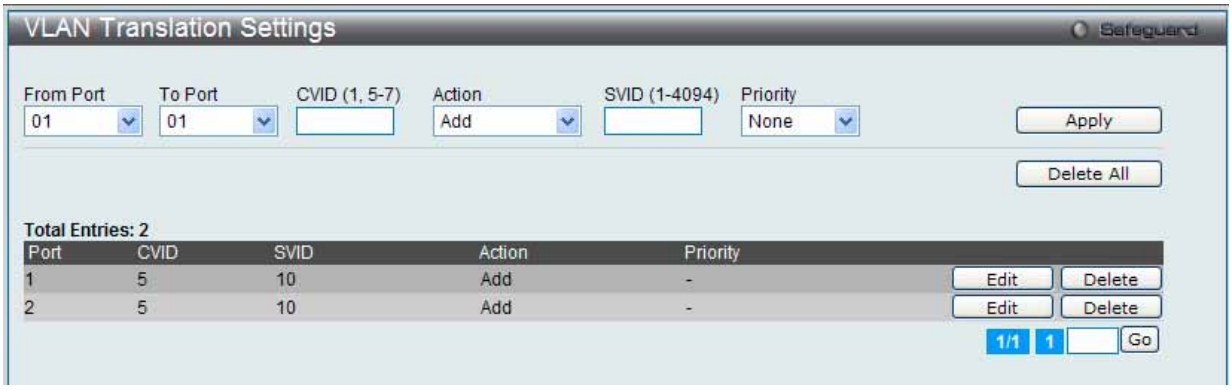


図 7.3-31　VLAN Translation Settings 画面

2. 以下の項目を使用して、設定および表示を行います。

項目	説明
From Port / To Port	設定に使用するポート範囲を選択します。
CVID (1, 5-7)	照合する C-VLAN ID を指定します。
Action	• Add - C- タグの前に S- タグを追加します。 • Replace - オリジナルの C- タグを S- タグに置き換えます。
SVID (1-4094)	SP-VLAN ID を入力します。
Priority	S- タグの優先度を選択します。

「Apply」ボタンをクリックし、新しいエントリを追加します。

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

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。

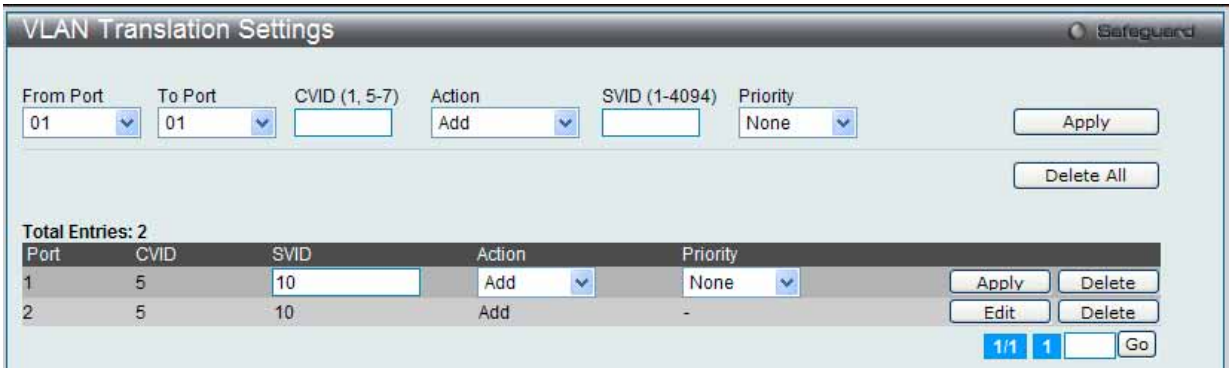


図 7.3-32　VLAN Translation Settings 画面 - Edit

2. エントリの編集後、「Apply」ボタンをクリックします。

エントリの削除

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

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（8802.1D-1998 STP、802.1D-2004 Rapid STP、および 802.1Q-2005 MSTP）をサポートしています。ネットワーキング管理者間では 802.1D-1998 STP が最も一般的なプロトコルとして認識されていると思います。しかし、D-Link のマネジメントスイッチにも 802.1D-2004 RSTP と 802.1Q-2005 MSTP は導入されており、それらの技術について、以下に簡単に紹介します。また、802.1D-1998 STP、802.1D-2004 RSTP および 802.1Q-2005 MSTP の設定方法についても記述します。

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. 4094 エレメントテーブル（「MST Configuration Identification」画面内の「VID List」）。スイッチがサポートする 4094 個までの 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。表にポートの状態遷移における 3 つのプロトコルの差を示しています。

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

ポート状態の比較

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

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

Edge Port

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

P2P Port

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

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

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

2 つのレベルで動作するスパニングツリープロトコル

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

STP Bridge Global Settings（STP ブリッジグローバル設定）

STP ブリッジグローバルパラメータを設定します。

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「Enabled」（有効）または「Disabled」（無効）にします。また、「STP Version」で STP の方式を選択します。

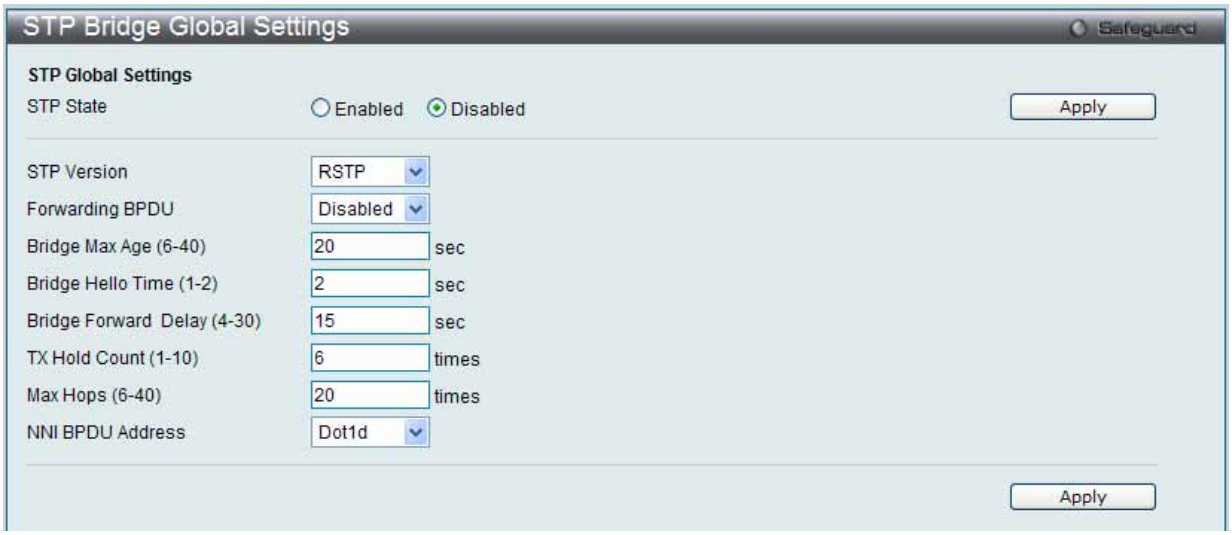


図 7.3-33　STP Bridge Global Settings 画面 : RSTP（初期値）

図 7.3-34　STP Bridge Global Settings 画面 : MSTP

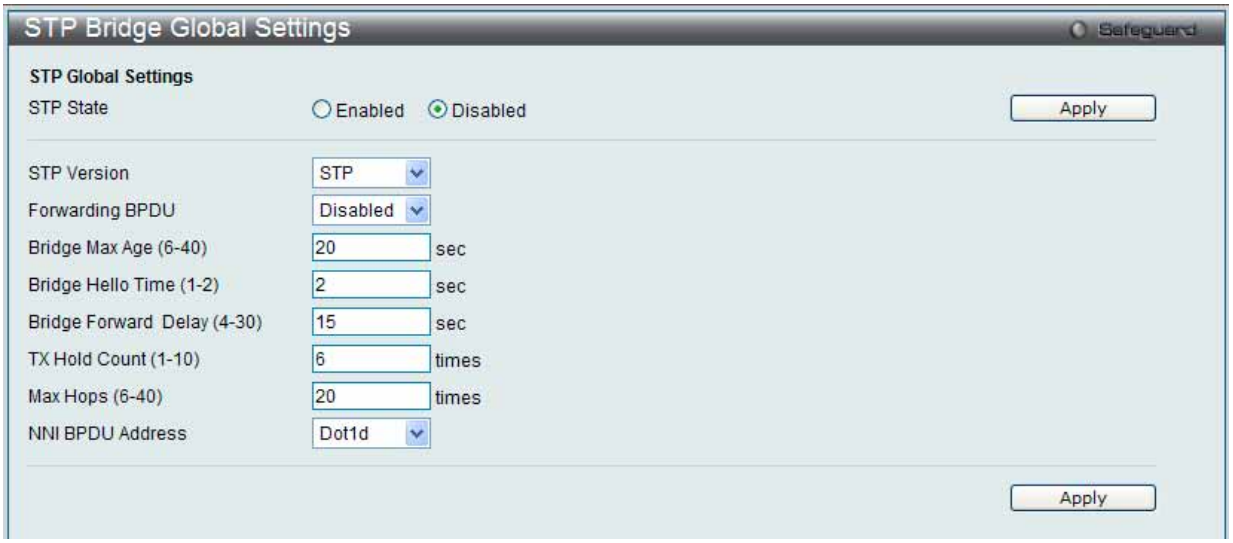


図 7.3-35　STP Bridge Global Settings 画面 : STP

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）

以下の項目を使用して設定および参照します。

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。初期値は 20（秒）です。

項目	説明
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 回目の送信の間隔です。STP または RSTP が「STP Version」で選択された場合に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 Port Settings（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。
NNI BPDU Address	サービス提供サイトにおける GVRP の BPDU プロトコルアドレスを決定します。「Dot1d」（802.1d GVRP アドレス）、「Dot1ad」（802.1ad サービスプロバイダの GVRP アドレス）、またはユーザ定義のマルチキャストアドレスを使用します。ユーザ定義アドレスの範囲は 0180C2000000-0180C2FFFFFF 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。

参照 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。

1. **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。

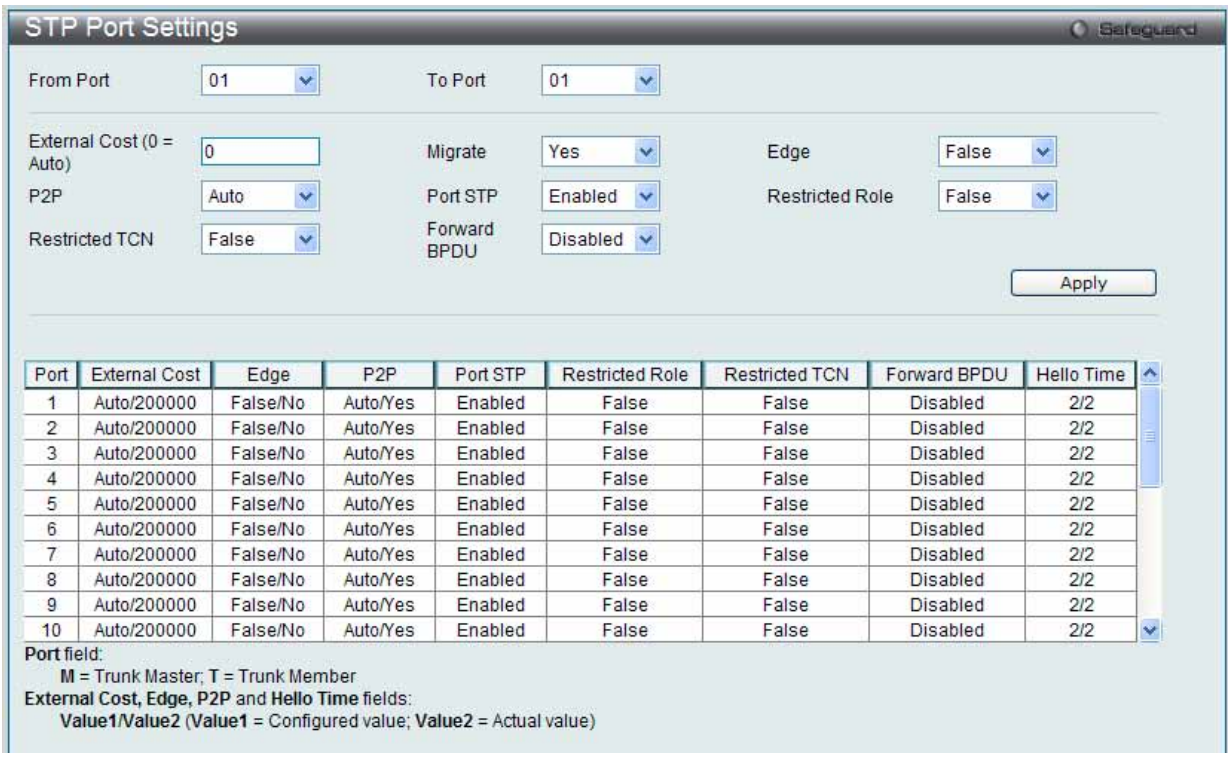


図 7.3-36　STP Port Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
From/ To Port	設定対象のポート範囲を指定します。
External Cost (0=Auto)	設定対象のポートに対し、パケット送信のためのコストを表すメトリックを定義します。ポートコストは、自動設定、あるいは手動でメトリック値を指定できます。初期値は 0（自動）です。 • 0 - 0 を指定すると、指定したポートに対して、最適なパケット送信スピードを自動的に設定します。デフォルトポートコスト : 100Mbps ポートの場合は 200000、ギガビットポートの場合は 20000。 • 1-200000000 の範囲から指定 - 小さい数字を指定すると、パケット送出ポートとして選定される確率が上がります。
Migrate	RSTP モードで動作中に、「Yes」を選択すると、選択されたポートは RSTP BPDU を送信します。
Edge	• True - 選択されたポートはエッジポートとして指定されます。エッジポートはループを発生しません。しかし、トポロジの変更によってループ発生の可能性が生じると、エッジポートはエッジポートとしての資格を失います。エッジポートは通常 BPDU パケットを受け取りません。しかし、BPDU パケットが受信されると、そのポートはエッジポートの資格を失います。 • False - そのポートにエッジポートの資格がないことを示しています。 •「Auto」オプションが利用可能です。
P2P	• True - 選択されたポートは P2P ポートとして指定されます。P2P ポートはエッジポートと似ていますが、全二重モードでのみ稼動する点で異なります。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）、自動的に False を指定した時と同様になります。（初期値）
Port STP	ポートの STP を「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Enabled」です。
Restricted Role	「True」と「False」を切り替えます。True に設定すると、ポートはルートポートになるように選択されることはありません。初期値は「False」です。
Restricted TCN	TCN（Topology Change Notification）は、ブリッジがトポロジ変更を合図するためにルートポートに送出する簡単な BPDU です。Restricted TCN は「True」と「False」間で切り変わります。「True」に設定すると、受信した TCN とトポロジ変更を他のポートへ伝搬することを停止します。初期値は「False」です。
Forward BPDU	プルダウンメニューから STP が無効の場合の BPDU パケットのフラッドを「Enabled」（有効）/「Disabled」（無効）にします。「Enabled」を選択すると、選択されたポートは他のネットワークデバイスから来る BPDU パケットの転送を行うようになります。

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。

注意 BPDU の送出をポートベースで有効とする場合は、はじめに以下の設定を行ってください。

1. STP をグローバルに無効とする。
2. BPDU の送出をグローバルに有効とする。

これらの設定は、前述の「STP Bridge Global Settings」（STP ブリッジグローバル設定）メニューで行います。

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。

1. **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。

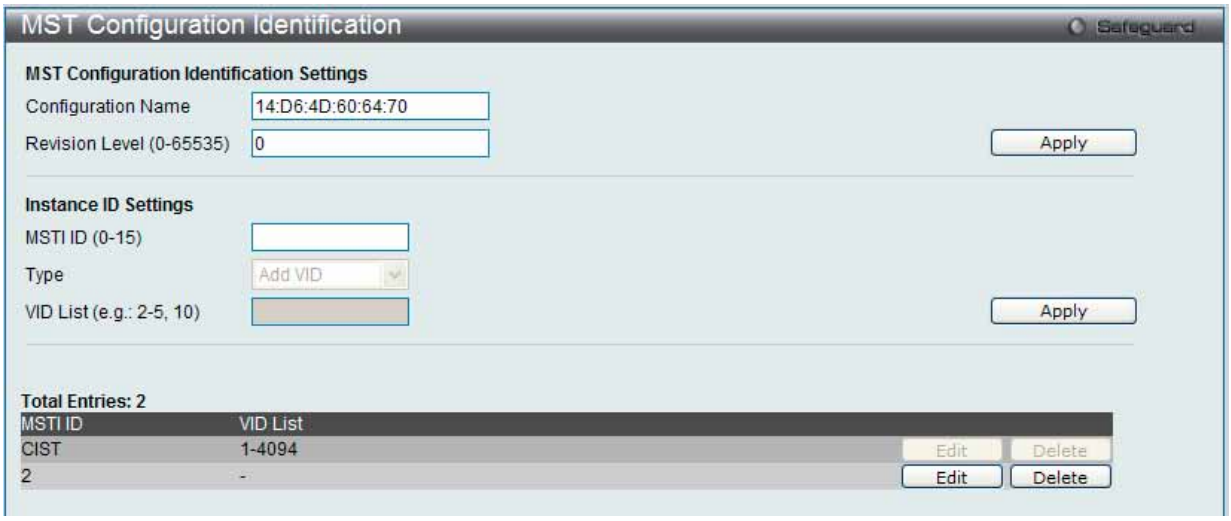


図 7.3-37　MST Configuration Identification 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Configuration Name	各 MSTI（Multiple Spanning Tree Instance）を識別するためにスイッチに名前を設定します。名前が設定されていない場合、MSTP が動作しているデバイスの MAC アドレスが表示されます。
Revision Level (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 (1-15)	新規の MSTI ID を 1-15 の範囲から指定します。
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	スイッチに登録済みの VLAN の中から 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 7.3-38　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）

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します。

1. **L2 Features > Spanning Tree > STP Instance Settings** をクリックし、以下の画面を表示します。

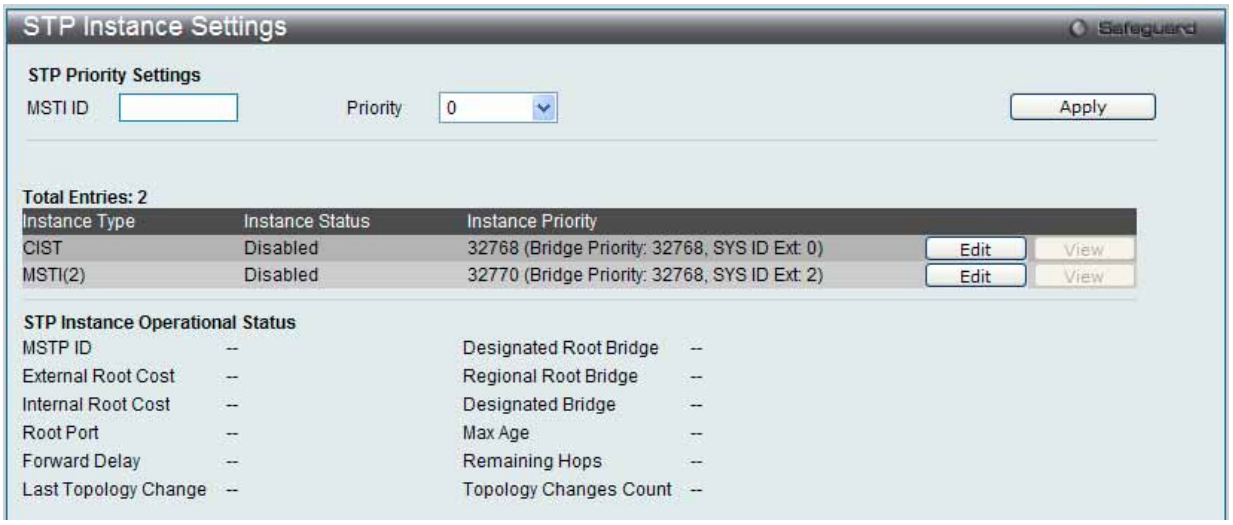


図 7.3-39　STP Instance Settings 画面

2. 以下の項目を使用して設定および参照します。

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。
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。

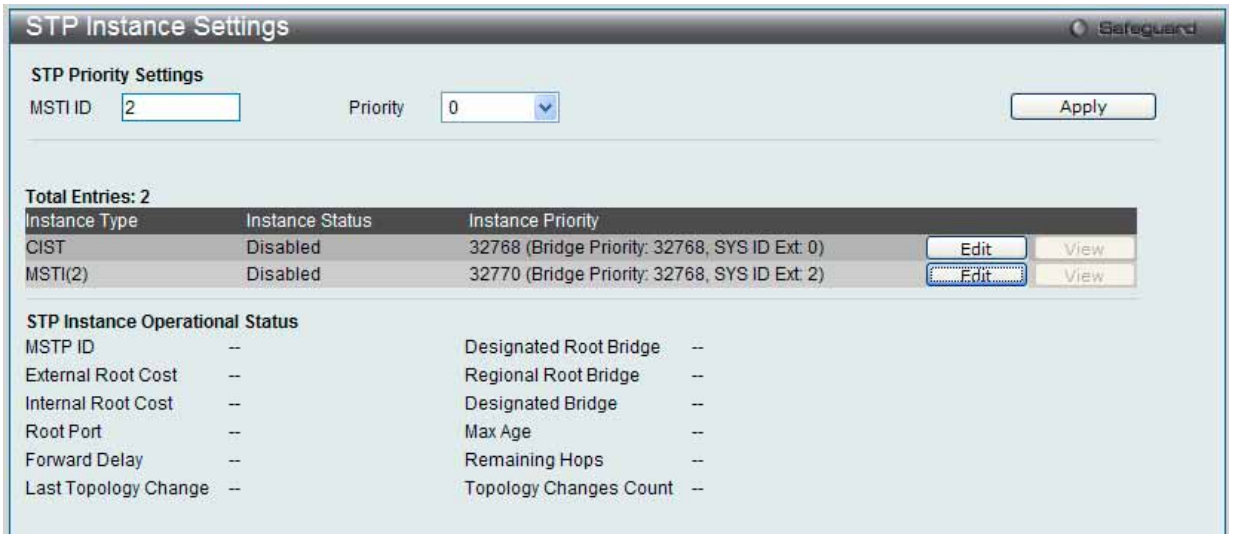


図 7.3-40　STP Instance Settings 画面 - Edit

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。

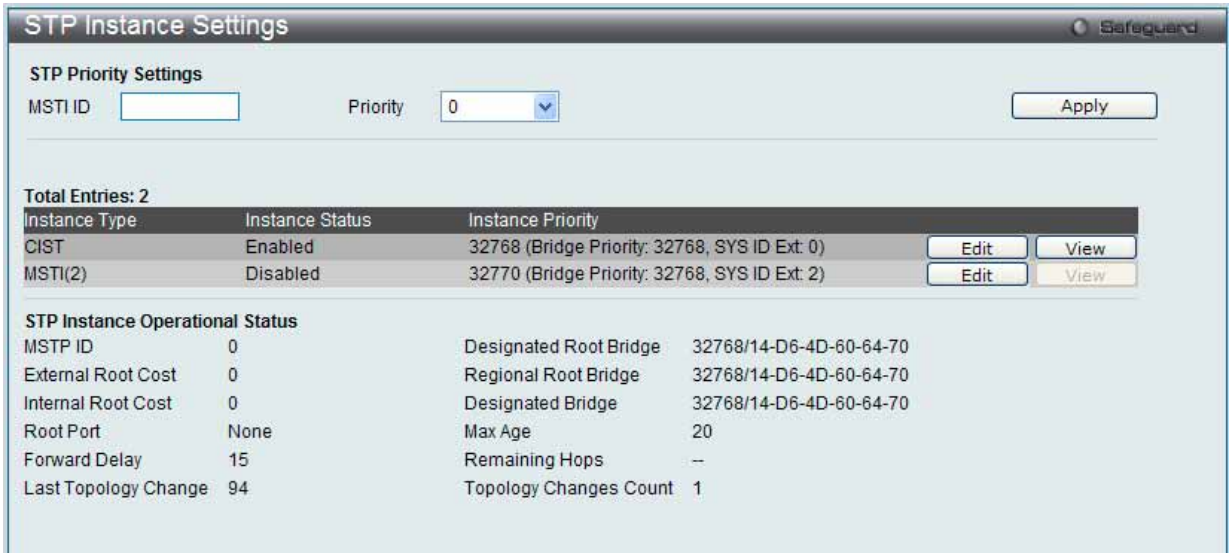


図 7.3-41　MST Configuration Identification 画面 - View

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います。ループが発生した場合に 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。

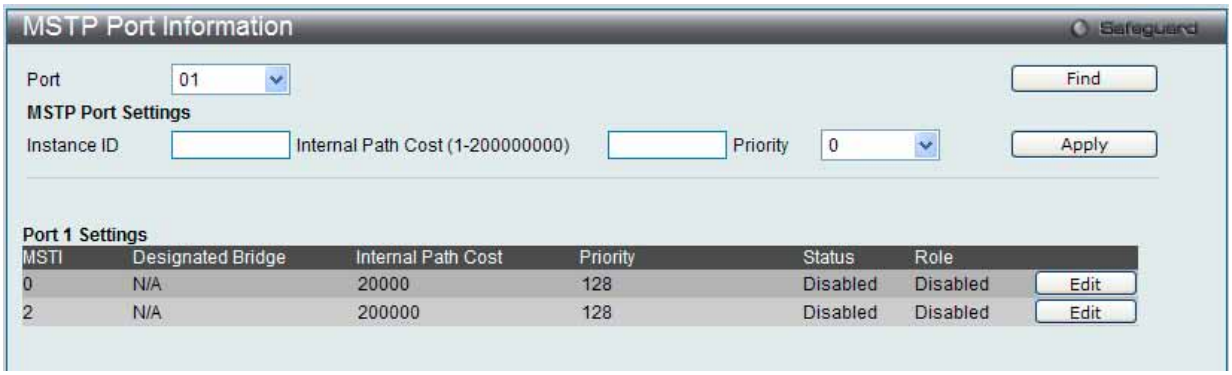


図 7.3-42　MSTP Port Information 画面

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。

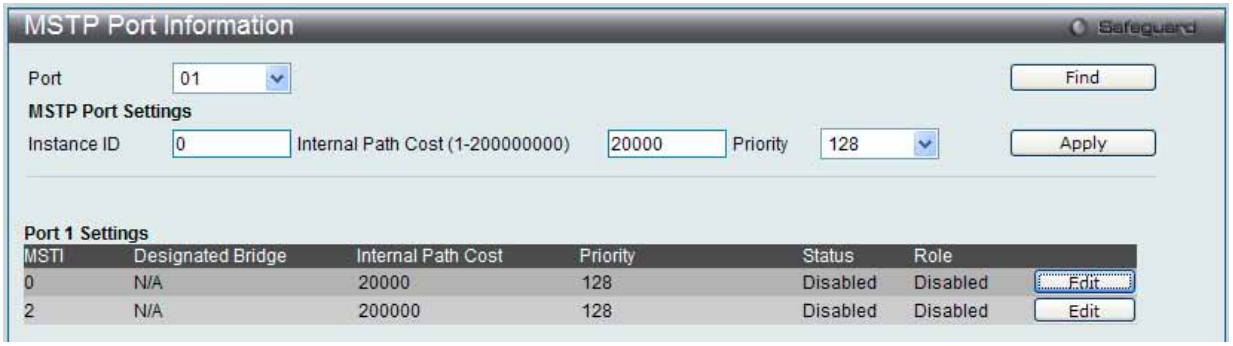


図 7.3-43　MSTP Port Information 画面 - Edit

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（0-15）。0 は CIST を意味します（初期値は MSTI）。
Internal Path Cost (1-200000000)	インタフェースを STP インスタンスで選択する場合、指定ポートにパケットを転送する相対的なコストを設定します。 • 0（Auto）- インタフェースに自動的で最適な最速のルートを設定します。（初期値） • 値 1-200000000 - ループが発生した場合、この範囲で指定した値を使用した最短のルートを設定します。コストが小さいほど高速で伝送されます。
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。

Link Aggregation（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 32 個のポートトランクグループをサポートしています。800Mbps のビットレートを実現する可能性があります。

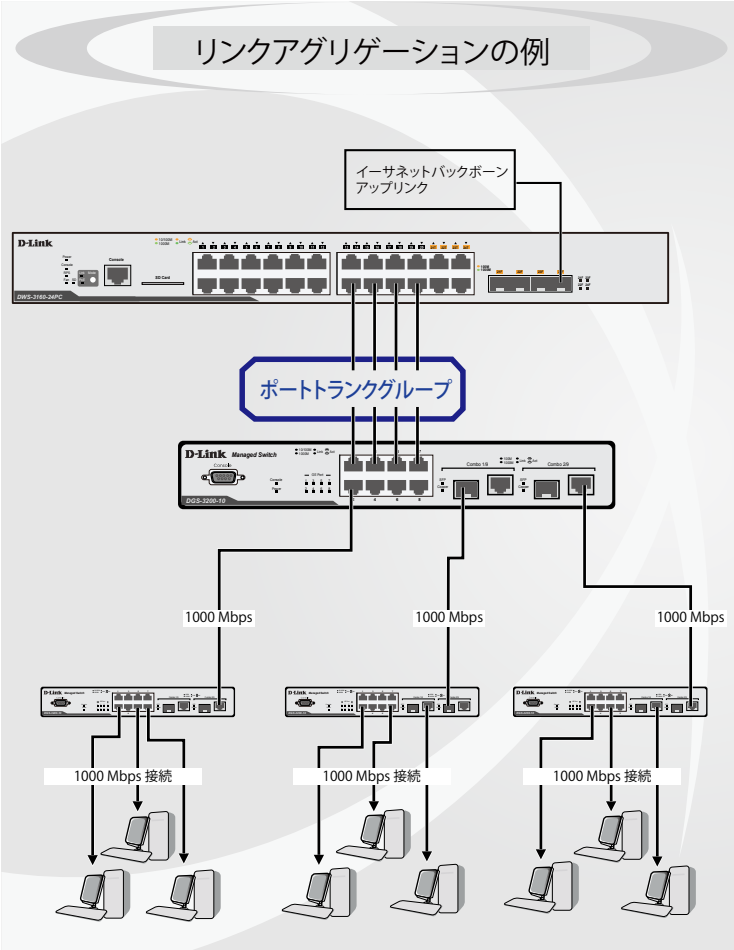


図 7.3-44　ポートトランクグループの例

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。

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 32 個のリンクアグリゲーショングループをサポートします。オプションのギガビットポートは 1 つのリンクアグリゲーショングループにだけ所属できます。

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。

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。

Port Trunking Settings（ポートトランキング設定）

スイッチにポートトランクを設定します。

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

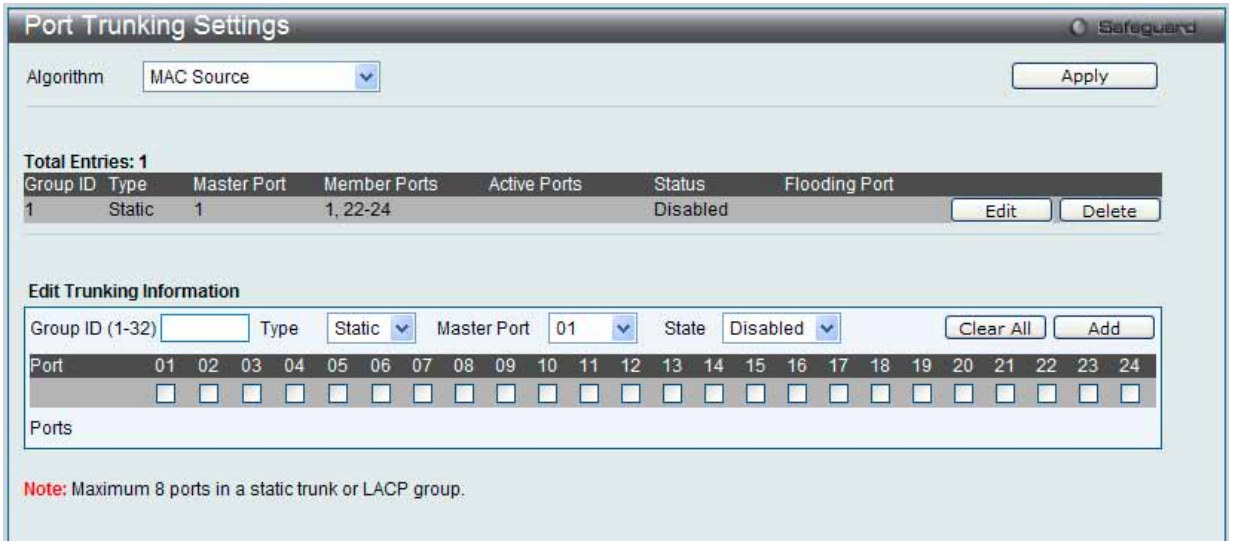


図 7.3-45　Port Trunking Settings 画面

以下の項目を使用して設定および参照します。

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 Dest」、「L4 Port Source」、「L4 Port Destination」、「L4 Source Dest」から指定してください。
Edit Trunking Information	
Group ID (1-32)	グループの ID 番号を 1-32 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」または「LACP」から選択します。LACP（Link Aggregation Control Protocol）を選択すると、ポートトランキンググループ内でのリンクの自動検出を行います。
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する場合、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。

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。

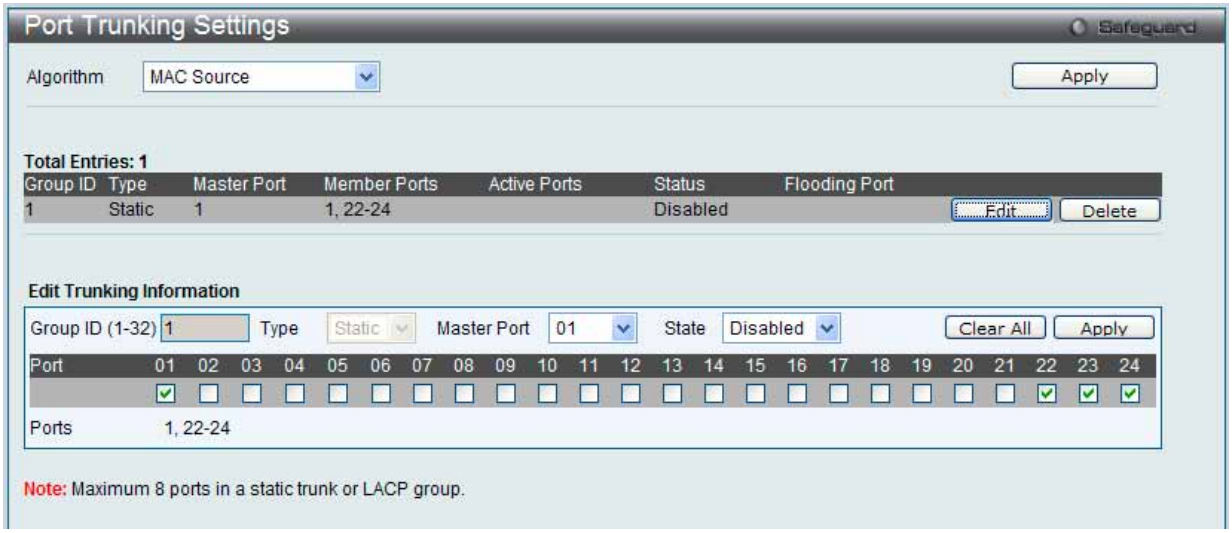


図 7.3-46　Port Trunking 画面 - Edit

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。「Clear All」ボタンをクリック

注意　スタティックなトランキングまたは LACP グループに設定されるポートの最大数は 8 です。

LACP Port Settings（LACP ポートの設定）

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。

1. **L2 Features > Link Aggregation > 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。

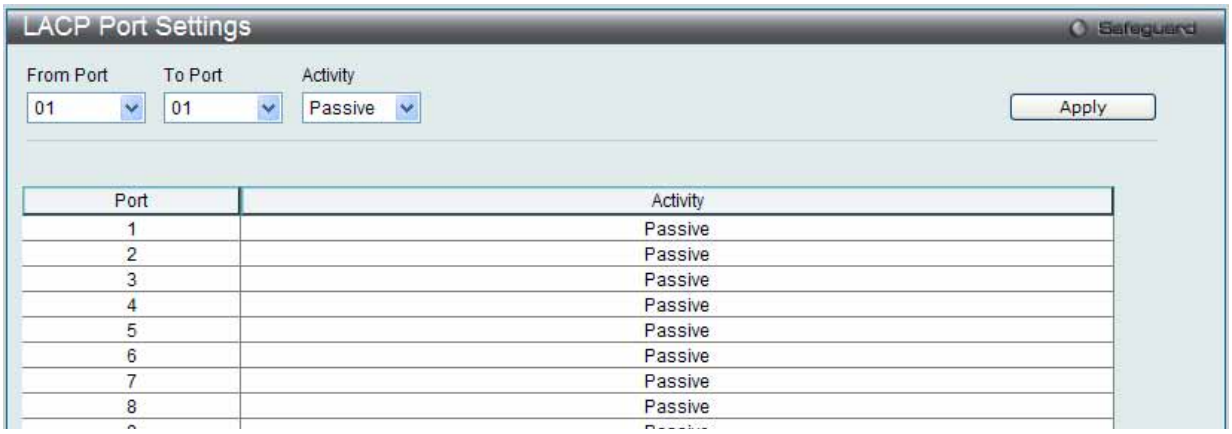


図 7.3-47　LACP Port Settings 画面

2. 以下の項目を使用して設定および参照します。

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。

FDB（FDB 設定）

Static FDB Settings（スタティック FDB の設定）

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

スイッチにスタティックなユニキャストフォワーディングを設定します。

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

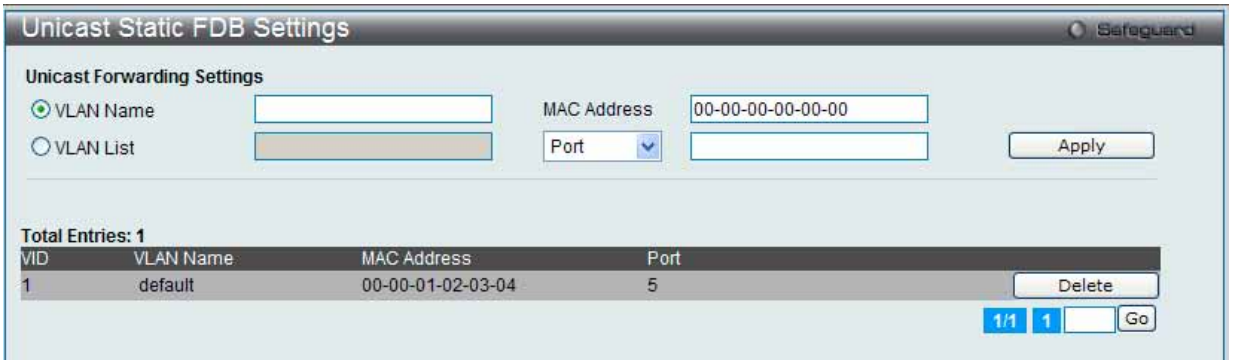


図 7.3-48　Unicast Static FDB Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
VLAN Name	ラジオボタンをクリックし、関連するユニキャスト MAC アドレスが存在する VLAN 名を入力します。
VLAN List	ラジオボタンをクリックし、関連するユニキャスト MAC アドレスが存在する VLAN リストを入力します。
MAC Address	パケットがスタティックに送信される宛先の MAC アドレス。ユニキャスト MAC アドレスを指定します。
Port/Drop	上記 MAC アドレスのあるポート番号を指定します。また、本オプションはユニキャストのスタティックな FDB から MAC アドレスを破棄します。 • Port - 上記 MAC アドレスのあるポート番号を指定します。 • drop - ユニキャストのスタティックな FDB から MAC アドレスを破棄します。

「Apply」ボタンをクリックして設定を適用します。

エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。

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

スイッチにスタティックなマルチキャストフォワーディングを設定します。

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

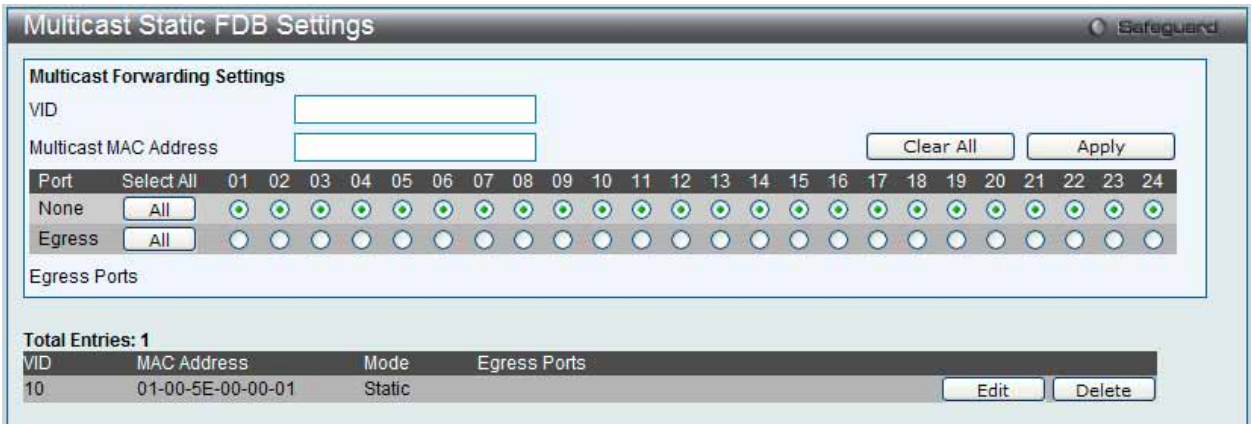


図 7.3-49　Multicast Static FDB Setting 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
VID	指定の Multicast MAC アドレスが属する VLAN の VLAN ID。
Multicast MAC Address	マルチキャストパケットの送信先 MAC アドレス。マルチキャスト MAC アドレスを指定します。
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、および GMRP によってダイナミックにグループに参加させるポート、参加させないポートを選択します。 • 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。「All」ボタンをクリックするとすべてのポートを選択します。 • 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。「All」ボタンをクリックするとすべてのポートを選択します。

「Apply」ボタンをクリックして設定を適用します。

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て以下の画面を表示します。

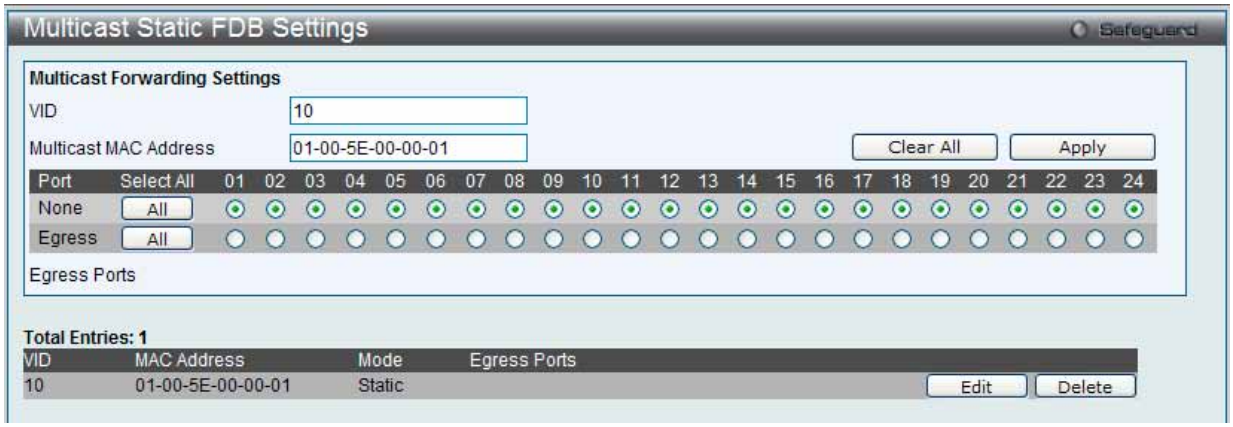


図 7.3-50　Multicast Static FDB Setting 画面

2. 項目を編集後「Apply」ボタンをクリックします。

エントリの削除

削除するエントリの「Delete」ボタンをクリックします。「Clear All」ボタンをクリックして、すべての情報エントリをクリアします。

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。スイッチの MAC 通知をグローバルに設定します。また、スイッチの各ポートに MAC 通知を設定します。

注意 本機能をご使用になる場合、NMS 側で、MAC Notification トラップを受信できる環境が必要になります。E-mail や Syslog における通知には対応しておりません。

1. **L2 Features > FDB > MAC Notification 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。

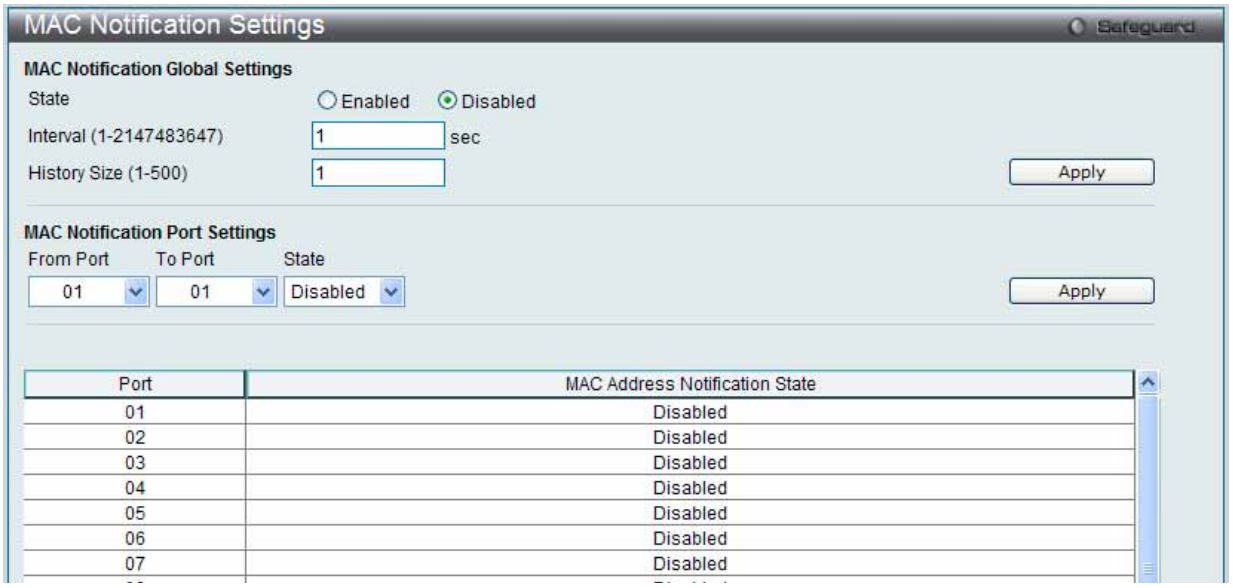


図 7.3-51　MAC Notification Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
MAC Notification Global Settings	
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)	通知に使用するヒストリログの最大エントリ数（最大 500 エントリ）。初期値 : 1
MAC Notification Port Settings	
From Port / To Port	プルダウンメニューを使用して MAC 通知を有効にするポート範囲を指定します。
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。

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

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

スイッチに MAC アドレスエージングタイムを設定します。

L2 Features > FDB > MAC Address Aging Time の順にクリックし、以下の画面を表示します。

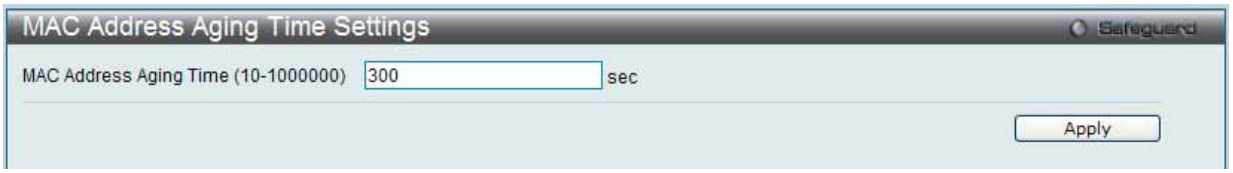


図 7.3-52　MAC Address Aging Time Settings 画面

以下の項目を使用して設定、表示を行います。

項目	説明
MAC Address Aging Time (10-1000000)	学習した MAC アドレスがアクセスされないままフォワーディングテーブルに保存される時間（学習した MAC アドレスがアイドル状態でいる時間）。 この値を変更するためには、MAC アドレスエージングタイム（秒）を示す別の値を入力します。10-1000000（秒）の範囲で値を入力します。初期値は 300（秒）です。

「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。

MAC Address Table（MAC アドレステーブル）

スイッチの MAC アドレスフォワーディングテーブルを参照します。スイッチが MAC アドレス、VLAN、およびポート番号間の関連性を学習するとテーブルに記載します。それらのエントリは、スイッチ経由でパケットを送信するのに使用されます。

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

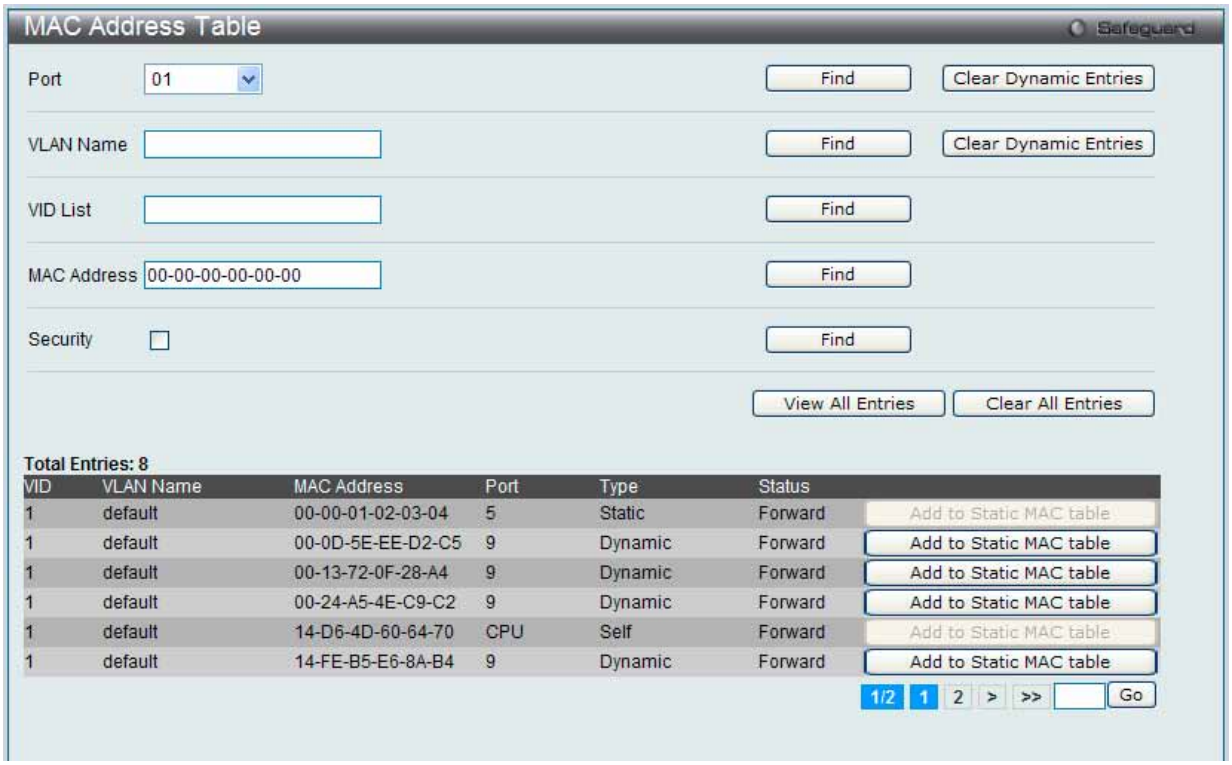


図 7.3-53　MAC Address Table 画面

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

2. 以下の項目を使用して設定および参照します。

項目	説明
Port	以下の MAC アドレスと関連付けられるポート。
VLAN Name	参照するフォワーディングテーブルの VLAN 名を入力します。
VID List	参照するフォワーディングテーブルの VLAN ID リストを入力します。
MAC Address	参照するフォワーディングテーブルの MAC アドレスを入力します。
Security	チェックすると、セキュリティモジュールによって作成される FDB エントリを表示します。
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 Entries	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 Entries	アドレステーブルのすべてのエントリを削除します。
Add to Static MAC table	スタティックテーブルに指定エントリを追加します。

ARP & FDB Table（ARP と FDB テーブル）

ARP と FDB テーブルのパラメータを検索します。

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

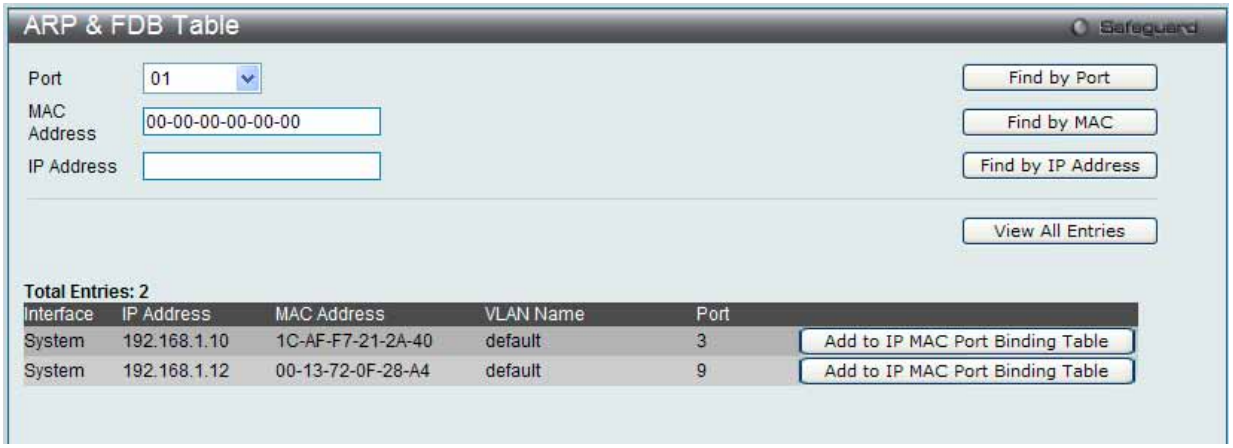


図 7.3-54　ARP & FDB Table 画面

2. 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	この設定に使用するポート番号を選択します。
MAC Address	本設定に使用する MAC アドレスを指定します。
IP Address	本設定に使用する IP アドレスを入力します。
Find by Port	選択したポート番号に基づく特定のエントリを検出します。
Find by MAC	入力した MAC アドレスに基づく特定のエントリを検出します。
Find by IP Address	入力した IP アドレスに基づく特定のエントリを検出します。
View All Entries	すべての既存エントリを表示します。
Add to IP MAC Port Binding Table	IP MAC ポートバインディングテーブルに指定エントリを追加します。

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

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。

IGMP Snooping Settings（IGMP Snooping 設定）

IGMP Snooping 設定をグローバルに「Enabled」（有効）または「Disabled」（無効）にします。

IGMP Snooping 機能を利用するためには、まず、画面上にある「IGMP Snooping Global Settings」でスイッチ全体を有効にする必要があります。その後、対応する「Edit」ボタンをクリックして、各 VLAN に詳細な設定を行います。

IGMP Snooping を有効にすると、スイッチはデバイスと IGMP ホスト間で送信される IGMP メッセージに基づいて、特定のマルチキャストグループメンバに接続するポートをオープンまたはクローズできるようになります。スイッチは IGMP メッセージをモニタして、マルチキャストパケットを要求しているホストがもう存在していないと判断すれば、マルチキャストパケットの送信を停止します。

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

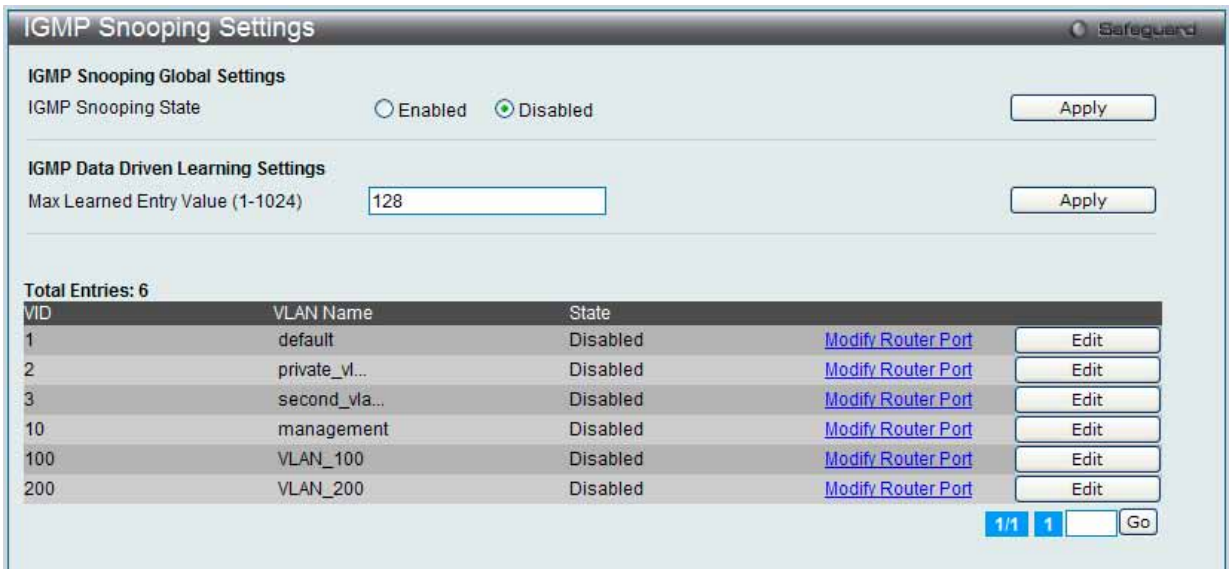


図 7.3-55　IGMP Snooping Settings 画面

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

2. 以下の項目を使用して設定および参照します。

項目	説明
IGMP Snooping Global Settings	
IGMP Snooping State	IGMP Snooping 状態を「Enabled」（有効）または「Disabled」（無効）にします。 • Enabled - デバイスで IGMP Snooping を有効にします。 • Disabled - デバイスで IGMP Snooping を無効に設定します。（初期値）
Max Learning Entry Value (1-1024)	学習する最大エントリ数を入力します。

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 Snooping 機能の詳細設定

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

図 7.3-56　IGMP Snooping Parameters Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
VID	VLAN ID を表示します。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します。
VLAN Name	IGMP Snooping クエリアを設定する VLAN 名を表示します。VLAN ID と共に、IGMP Snooping 設定を行う対象の VLAN を識別します。
Rate Limit	スイッチが特定のポート /VLAN で処理できる IGMP 制御パケットのレートを表示します。レートはパケット / 毎秒で指定されます。制限レートを超過したパケットは破棄されます。
Querier IP	ネットワークに IGMP クエリを送信するデバイスの IP アドレスを表示します。
Query Interval (1-65535)	一般的な IGMP クエリア送信間隔（秒）を指定します。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時間を 1-25（秒）で設定します。初期値は 10（秒）です。
Robustness Value (1-7)	予想されるサブネット上のパケットの損失に応じてこの変数を調整します。Robustness Variable は以下の IGMP メッセージ間隔を計算して使用されます。1-7 の範囲から指定します。初期値は 2 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。この間隔はルータがグループのラストメンバの損失を検出するためにかかる時間をより減少するように低くします。初期値は 1 です。
Data Drive Group Expiry Time (1-65535)	Data Driven グループの生存時間（秒）を指定します。
Querier State	クエリア状態を「Enabled」(有効) または「Disabled」(無効) にします。
Fast Leave	IGMP Snooping の Fast Leave 機能を「Enabled」(有効) /「Disabled」(無効) にします。有効にすると、システムが IGMP Leave メッセージを受信するとメンバはすぐにグループから削除されます。
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。 • Enabled - スイッチが IGMP クエリパケットを送信する IGMP クエリアとして選択されます。 • Disabled - スイッチは IGMP クエリアとしての役目を果たしません。 **注意** スイッチに接続するレイヤ 3 ルータが IGMP プロキシ機能だけを提供し、マルチキャストルーティング機能を提供しない場合、この状態は無効に設定されます。そうでない場合、レイヤ 3 ルータをクエリアとして選択しないと、IGMP クエリパケットを送信しません。また、マルチキャストルーティングプロトコルパケットを送信しないため、ポートはルータポートとしてタイムアウトになります。
Report Suppression	有効にされると、特定の (S、G) に対する複数の IGMP レポートまたはリーブがルータポートに送信される前に 1 つのレポートに統合されます。
Data Driven Learning State	Data Driven Learning 状態を「Enabled」(有効) /「Disabled」(無効) にします。
Data Drive Learning Aged Out	Data Driven Learning のエージングアウトオプションを「Enabled」(有効) /「Disabled」(無効) にします。
Version	このポートに送信される 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より高いバージョンを持つ場合、本パケットは破棄されます。

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。

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

1. 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。

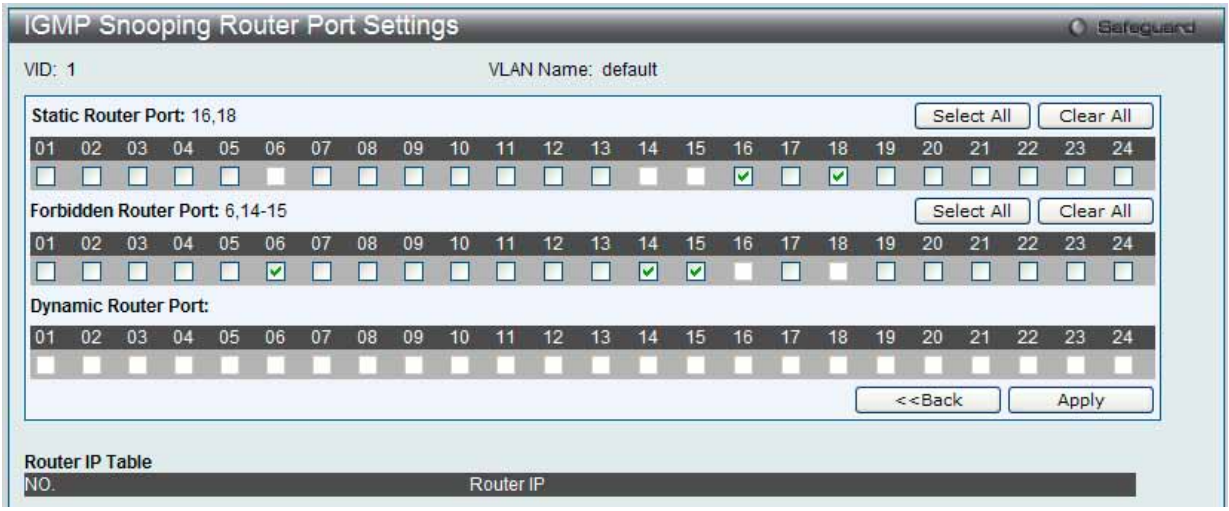


図 7.3-57　IGMP Snooping Router Ports Settings 画面

2. 以下の項目を設定または表示します。

項目	説明
Static Router Port	マルチキャストが有効なルータに接続するポート範囲を指定します。これは、宛先としてルータが持つすべてのパケットをプロトコルなどにかかわらず、マルチキャストが有効なルータに到達するように設定します。
Forbidden Router Port	マルチキャストが有効なルータに接続しないポート範囲を指定します。これは、禁止ポートがルーティングパケットを送信しないように設定します。
Dynamic Router Port	ダイナミックに設定されたルータポートを表示します。
Ports	個別に適切なポートを選択して、ルータポート設定に含めます。 • 「Select All」ボタンをクリックするとすべてのポートを選択します。 • 「Clear All」ボタンをクリックするとすべてのポートの選択を解除します。

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 Snooping Rate Limit Settings（IGMP Snooping レート制限設定）

IGMP Snooping レート制限パラメータを設定します。

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

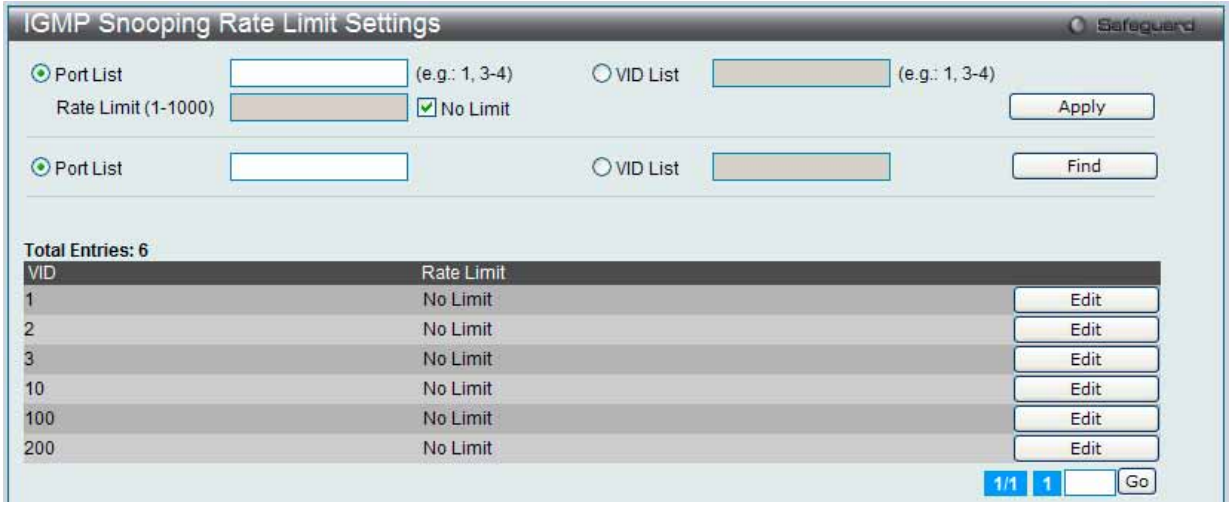


図 7.3-58　IGMP Snooping Rate Limit Settings 画面

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

2. 以下の項目を使用して設定および参照します。

項目	説明
Port List	本設定に使用するポートリストを指定します。
VID List	本設定に使用する VID リストを指定します。
Rate Limit (1-1000)	使用する IGMP Snooping レート制限を入力します。「No Limit」を選択すると、入力ポートのレート制限は無視されます。

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

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て、以下の画面を表示します。

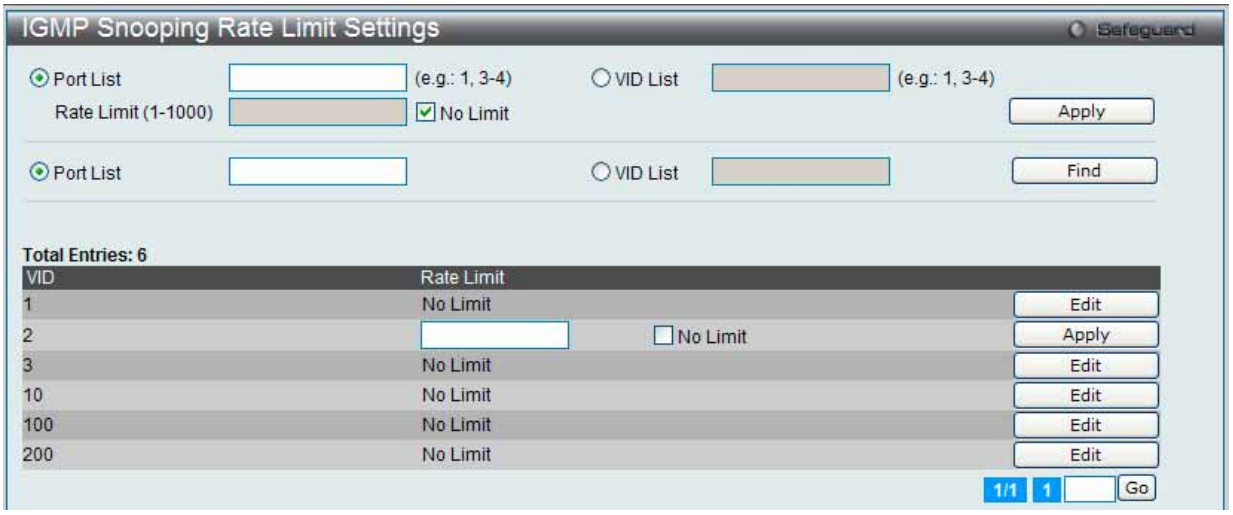


図 7.3-59　IGMP Snooping Rate Limit Settings 画面

2. 指定エントリを編集して「Apply」ボタンをクリックします。

エントリの参照

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

IGMP Snooping Static Group Settings（IGMP Snooping スタティックグループ設定）

スイッチの IGMP Snooping スタティック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 IP アドレスと対応する MAC アドレスを読み取ることができます。

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

図 7.3-60　IGMP Snooping Static Group Settings 画面

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

2. 以下の項目を設定または表示します。

項目	説明
VLAN Name	マルチキャストグループの VLAN 名を入力します。
VID List	マルチキャストグループの VID リストを入力します。
IPv4 Address	IPv4 アドレスを指定します。

エントリの参照

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

エントリの登録
「VLAN Name」または「VID List」、および「IPv4 Address」入力後、「Create」ボタンをクリックします。

エントリの削除
「Delete」ボタンをクリックして、入力した情報に基づいて指定エントリを削除します。

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

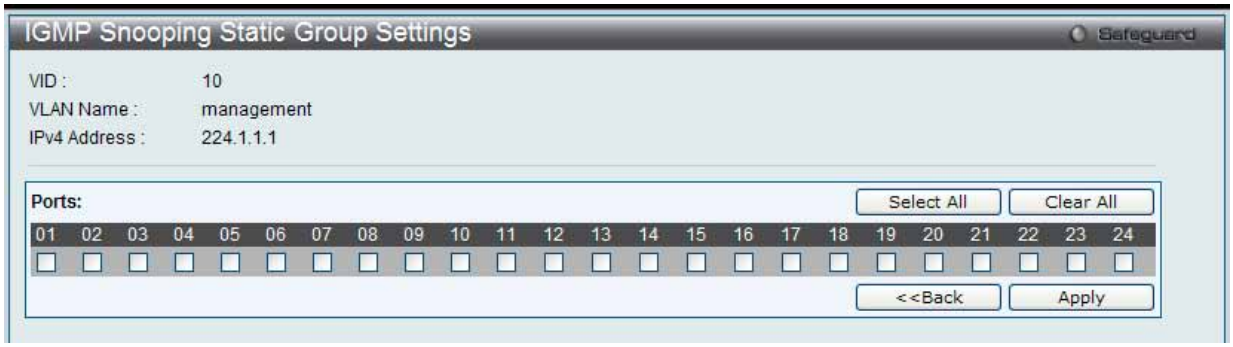


図 7.3-61　IGMP Snooping Static Group Settings 画面

2. 以下の項目を設定または表示します。

項目	説明
Ports	個別に適切なポートを選択して、IGMP Snooping スタティックグループ設定に含めます。 • 「Select All」ボタンをクリックするとすべてのポートを選択します。 • 「Clear All」ボタンをクリックするとすべてのポートの選択を解除します。

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

IGMP Router Port（ルータポート参照）

スイッチが現在ルータポートとして設定しているポートを表示します。

L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Router Port メニューをクリックして、以下の画面を表示します。

図 7.3-62　IGMP Router Port 画面

1. 画面上の VID (VLAN ID) を入力します。

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

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

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。

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。

1. **L2 Features > L2 Multicast Control > 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。

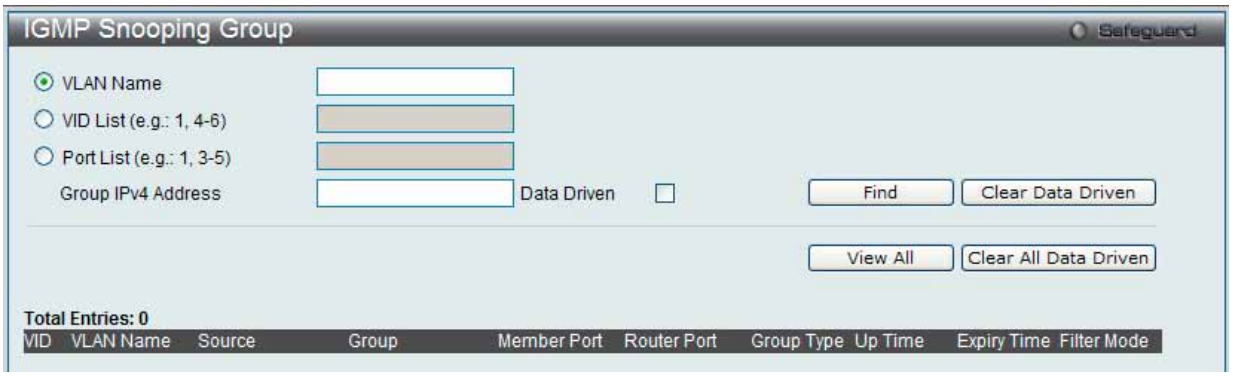


図 7.3-63　IGMP Snooping Group 画面

2. 以下の項目を使用して参照します。

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 ID リスト。
Port List (e.g.: 1, 3-5)	マルチキャストグループを検索するのに使用されるポート番号を指定します。
Group IPv4 Address	IPv4 アドレスを指定します。
Data Driven	選択すると、Data Driven グループだけが表示されます。

エントリの参照

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

エントリの削除

「Clear Data Driven」ボタンをクリックすると、指定 VLAN の Data Driven 機能が学習した IGMP Snooping グループを削除します。
「Clear All Data Driven」ボタンをクリックすると、指定 VLAN の Data Driven 機能が学習した IGMP Snooping グループをすべて削除します。

IGMP Snooping Forwarding Table（IGMP Snooping フォワーディングテーブル）

スイッチ上の現在の IGMP Snooping フォワーディングテーブルのエントリを表示します。

マルチキャストグループを送出するポートリストと転送される特定の送信元をチェックする簡単な方法を提供します。送信元 VLAN からのパケットをフォワーディング VLAN に転送します。さらに、IGMP Snooping はフォワーディングポートを制限できます。

L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping Forwarding 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。

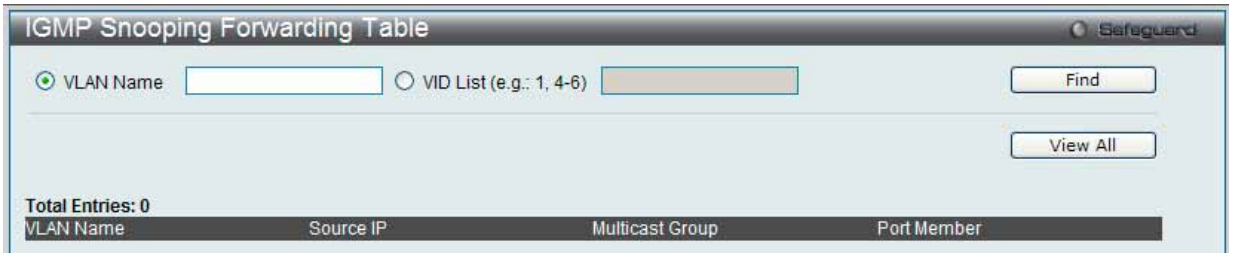


図 7.3-64　IGMP Snooping Forwarding Table 画面

3. 以下の項目を使用して参照します。

項目	説明
VLAN Name	マルチキャストグループの VLAN 名。
VID List	マルチキャストグループの VLAN ID リスト。

エントリの参照

画面左上の「VLAN Name」欄に VLAN 名を入力して「Find」ボタンをクリックすることにより、テーブル内を検索することができます。
「View All」ボタンをクリックして、すべての定義済みエントリを表示します。

IGMP Snooping Counter（IGMP Snooping カウンタ）

スイッチの IGMP Snooping カウンタテーブルを参照します。

1. **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP Snooping 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。

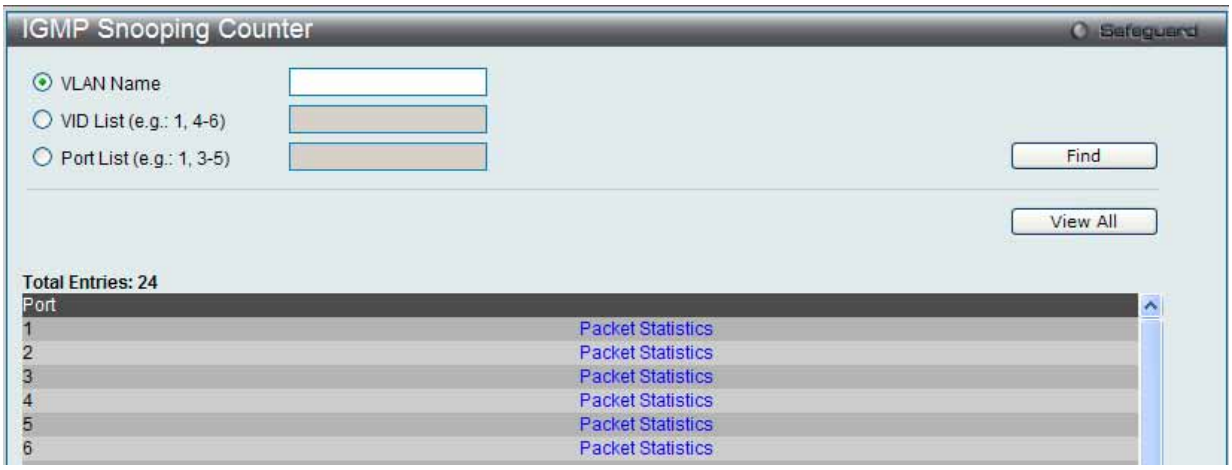


図 7.3-65　IGMP Snooping Counter 画面

2. 以下の項目を使用して参照します。

項目	説明
VLAN Name	マルチキャストグループの VLAN 名。
VID List	マルチキャストグループの VLAN ID リスト。
Port List	マルチキャストグループのポートリスト。

エントリの参照

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

IGMP Snooping カウンタテーブルの参照

「Packet Statistics」リンクをクリックすると、以下の画面が表示されます。

図 7.3-66　Browse IGMP Snooping Counter 画面

エントリの削除

「Clear Counter」ボタンをクリックして、本欄に表示したすべてのエントリをクリアします。
「Refresh」ボタンをクリックして、テーブルを更新して新しいエントリを表示します。

「<<Back」をボタンをクリックして前のページに戻ります。

IGMP Host Table（IGMP ホストテーブル）

IGMP ホストテーブルを参照します。

1. **L2 Features > L2 Multicast Control > IGMP Snooping > IGMP 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。

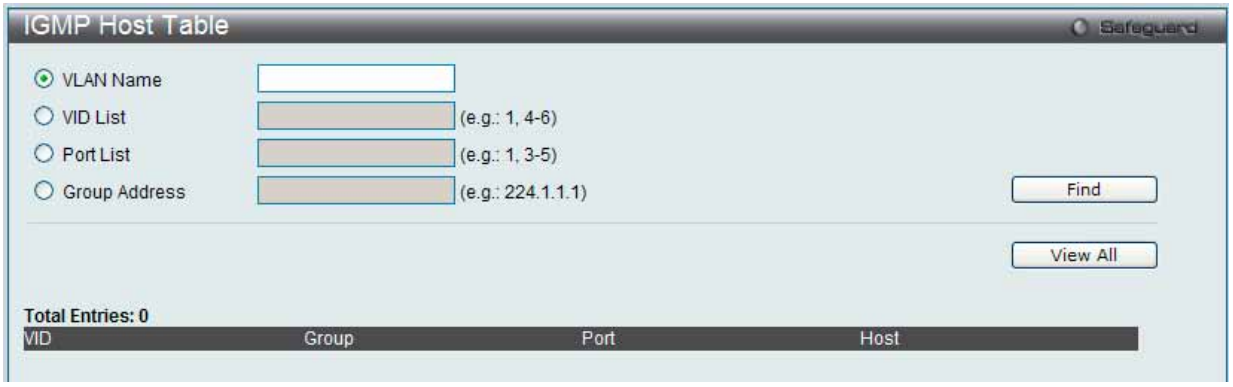


図 7.3-67　IGMP Host Table 画面

2. 以下の項目を使用して参照します。

項目	説明
VLAN Name	ラジオボタンをクリックして、表示する VLAN 名を入力します。
VID List	ラジオボタンをクリックして、表示する VLAN ID リストを入力します。
Port List	ラジオボタンをクリックして、表示するポートリストを入力します。
Group Address	ラジオボタンをクリックして、表示するグループアドレスを入力します。

エントリの参照

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

MLD Snooping（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。マルチキャストトラフィックを選択された VLAN のすべてのポートにフラッディングせずに、MLD スヌーピングは、マルチキャストトラフィックを要求しているポートと送信元によって生成されるクエリやレポートを介してデータを受信したいというポートにだけマルチキャストデータを転送します。

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

MLD コントロールメッセージ

MLD Snooping 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、132 および 143 にラベル付けされた ICMPv6 パケットヘッダによって定義されています。

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

2. Multicast Listener Report 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。

4. Multicast Listener Report、Version 2
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。

Data Driven Learning

MLD Snooping グループのために Data Driven Learning を実行できます。Dynamic IP Multicast Learning として知られる Data Driven Learning が VLAN に対して有効な場合、またはスイッチがこの VLAN で IP マルチキャストトラフィックを受信する場合、MLD Snooping グループが作成されます。エントリの学習は MLD メンバシップ登録ではなく、トラフィックによりアクティブになります。通常の MLD Snooping エントリのために、MLD プロトコルはエントリのエージングアウトを認めます。Data Driven エントリのために、エントリは、エージングアウトしないように指定されるか、またはタイマによってエージングアウトするように指定されます。

Data Driven Learning を有効にすると、すべてのポートのマルチキャストフィルタリングモードは無視されます。これは、マルチキャストパケットがフォワーディングテーブルとしてフラッドされることを意味します。

注意 Data Driven グループが作成され、MLD メンバポートが後で学習されると、エントリは、通常の MLD Snooping エントリになります。つまり、エージングアウトメカニズムは、通常、MLD Snooping エントリの状態に追従します。

Data Driven Learning は IP マルチキャストデータを記録して、送信するレイヤ 2 スイッチにビデオカメラが接続しているネットワークにおいて有益です。スイッチは、パケットを破棄せずに、またはパケットをフラッドせずにデータセンタに IP データを送信する必要があります。ビデオカメラには MLD プロトコルを実行する機能がないため、IP マルチキャストデータは通常の MLD Snooping 機能で破棄されます。

MLD Snooping Settings（MLD Snooping 設定）

スイッチの MLD Snooping を有効にして、MLD Snooping の設定を行います。

1. **L2 Features > L2 Multicast Control > MLD Snooping > 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。

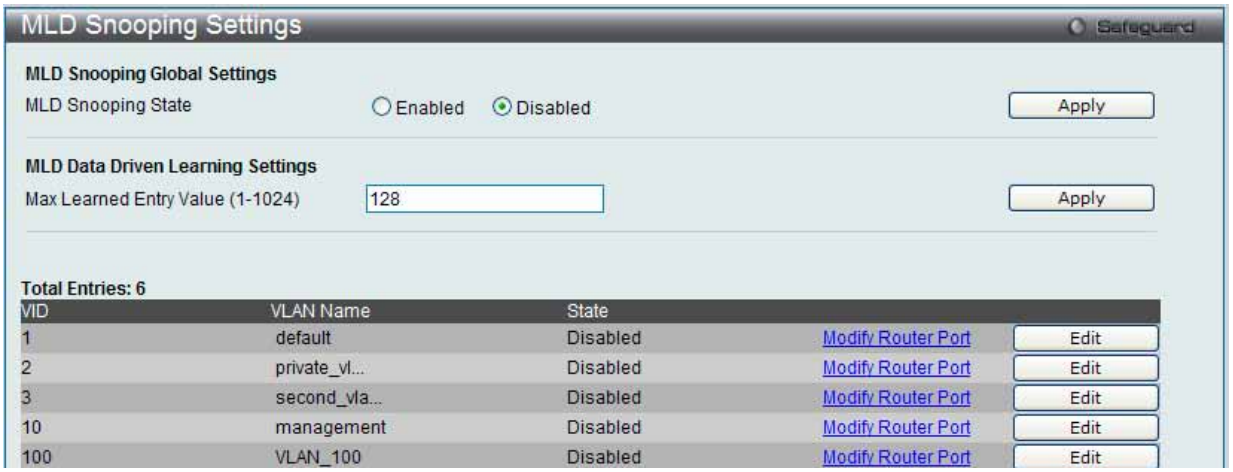


図 7.3-68　MLD Snooping Settings 画面

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。

2. 以下の項目を使用して設定および参照します。

項目	説明
MLD Snooping State	MLD Snooping 状態を「Enabled」(有効) または「Disabled」(無効) にします。
Max Learned Entry Value (1-1024)	学習する最大エントリ数を入力します。

「Apply」ボタンをクリックして各セクションで行った変更を適用します。

「Edit」ボタンをクリックして指定エントリの MLD Snooping 項目を設定します。
「Modify Router Port」リンクをクリックして、指定ポートに MLD Snooping ルータポート設定を行います。

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、「Apply」ボタンをクリックして変更を有効にします。

MLD Snooping に特定の VLAN を設定する

1. 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 7.3-69　MLD Snooping Parameters Settings 画面

2. 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
VID	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 MLD 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。
Rate Limit	スイッチが特定のポート /VLAN で処理できる MLD 制御パケットのレートを表示します。レートはパケット / 秒で指定されます。制限レートを超過したパケットは破棄されます。
Querier IP	ネットワークに MLD クエリを送信するデバイスの IP アドレスを表示します。
Querier Expiry Time	クエリアの有効時間を表示します。
Query Interval (1-65535)	一般的なクエリア送信間隔（秒）を指定します。初期値は 125（秒）です。
Max Response Time (1-25)	リスナーからの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。
Robustness Value (1-7)	予想されるサブネット上のパケットの損失に応じてこの変数を調整します。Robustness Variable は以下の MLD メッセージ間隔を計算して使用されます。1-7 の範囲から指定します。初期値は 2 です。 • Group Listener Interval - マルチキャストルータがネットワーク上のグループにリスナーがいないと判断するまでの時間。 • Other Querier Present Interval- マルチキャストルータがクエリアである他のマルチキャストルータがないと判断するまでの時間。 • Last Listener Query Count- ルータがグループにローカルリスナーがいないと見なす前に送信された Group-Specific Query 数。初期値は Robustness Variable の値です。 サブネットが失われたと予想する場合には、この値を増やすことができます。
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。この間隔はルータがグループのラストメンバの損失を検出するためにかかる時間をより減少するように低くします。
Data Driven Group Expiry Time (1-65535)	Data Driven グループの期限を入力します。
Querier State	有効または無効にして、スイッチを（MLD クエリパケットを送信する）MLD Querier または（MLD クエリパケットを送信しない）Non-Querier として指定します。初期値は無効です。
Fast Done	MLD Snooping の Fast Done 機能を「Enabled」（有効）または「Disabled」（無効）にします。有効にすると、システムが MLD Leave メッセージを受信するとメンバはすぐにグループから削除されます。
State	指定した VLAN への MLD Snooping 機能を「Enabled」（有効）/「Disabled」（無効）にします。初期値は無効です。 • Enabled - スイッチが MLD クエリパケットを送信する MLD クエリアとして選択されます。 • Disabled - スイッチは MLD クエリアとしての役目を果たしません。
Report Suppression	プルダウンメニューを使用して、レポート抑制機能を「Enabled」（有効）または「Disabled」（無効）にします。
Data Driven Learning State	MLD Snooping グループの Data Driven Learning を「Enabled」（有効）または「Disabled」（無効）にします。
Data Driven Learning Aged Out	Data Driven エントリのエージングアウト機能を「Enabled」（有効）または「Disabled」（無効）にします。
Version	このポートに送信される MLD 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 MLD パケットが指定のバージョンより高いバージョンを持つ場合、本パケットは破棄されます。
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います。 • Non-Querier - スイッチが MLD 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。

「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

MLD Snooping ルータポートの設定

1. 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。

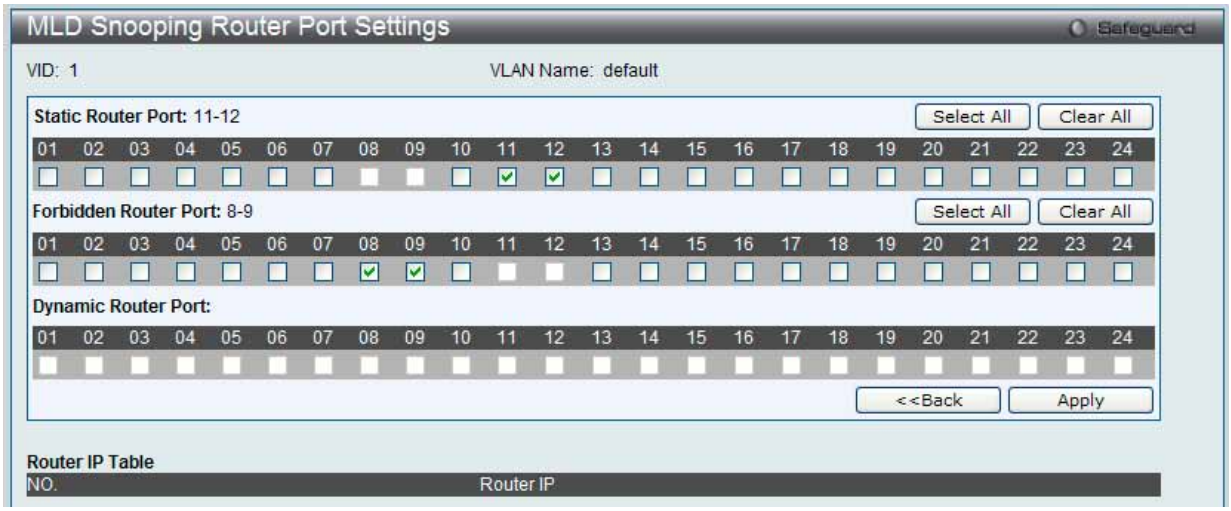


図 7.3-70　MLD Snooping Router Port Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Static Router Port	マルチキャストが有効なルータに接続するポート範囲を指定します。これは、宛先としてルータが持つすべてのパケットをプロトコルなどにかかわらず、マルチキャストが有効なルータに到達するように設定します。
Forbidden Router Port	マルチキャストが有効なルータに接続しないポート範囲を指定します。これは、禁止ポートがルーティングパケットを送信しないように設定します。
Dynamic Router Port	ダイナミックに設定されたルータポートを表示します。
Ports	個別に適切なポートを選択して、ルータポート設定に含めます。 • 「Select All」ボタンをクリックするとすべてのポートを選択します。 • 「Clear All」ボタンをクリックするとすべてのポートの選択を解除します。

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

「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

MLD Snooping Rate Limit Settings（MLD Snooping レート制限設定）

スイッチが特定のポート /VLAN で処理できる MLD 制御パケットのレート制限を設定します。この設定は、ポートまたは VLAN 内の最大パケット数 / 秒を制限するのに使用されます。

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

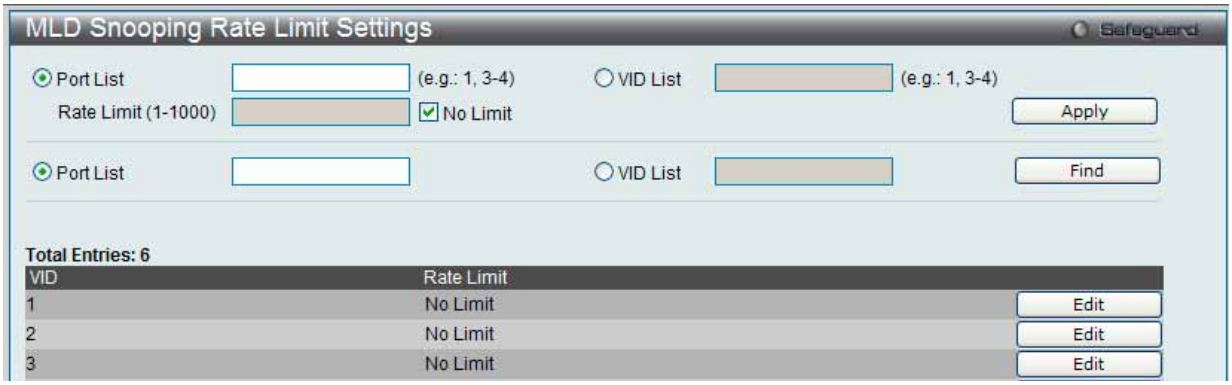


図 7.3-71　MLD Snooping Rate Limit Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Port List	本設定に使用するポートリストを指定します。
VID List	本設定に使用する VID リストを指定します。
Rate Limit (1-1000)	スイッチが特定のポート /VLAN で処理できる MLD 制御パケットのレート制限を設定します。レートはパケット / 秒で指定されます。制限を超過したパケットは破棄されます。「No Limit」オプションを選択すると、レート制限の要求は解除されます。

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。

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

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て、以下の画面を表示します。

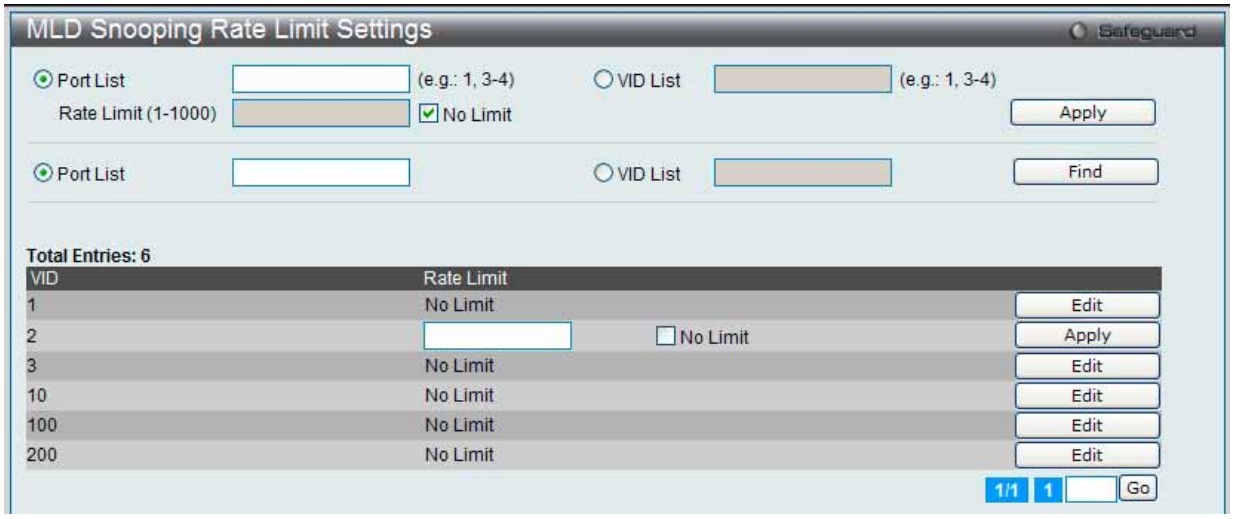


図 7.3-72　MLD Snooping Rate Limit Settings 画面 - Edit

2. 指定エントリを編集して「Apply」ボタンをクリックします。

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

MLD Snooping Static Group Settings（MLD Snooping スタティックグループ設定）

MLD Snooping マルチキャストグループのスタティックメンバポートを設定します。

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

図 7.3-73　MLD Snooping Static Group Settings 画面

2. 以下の項目を設定または表示します。

項目	説明
VLAN Name	スタティックグループのある VLAN 名を指定します。
VID List	スタティックグループのある VID リストを指定します。
IPv6 Address	マルチキャストグループの IPv6 アドレスを指定します。

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

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

エントリの削除
「Delete」ボタンをクリックして、入力した情報に基づいて指定エントリを削除します。

エントリの登録
「VLAN Name」または「VID List」、および「IPv6 Address」入力後、「Create」ボタンをクリックします。

エントリの編集

1. 「Edit」ボタンをクリックして、以下の画面を表示します。

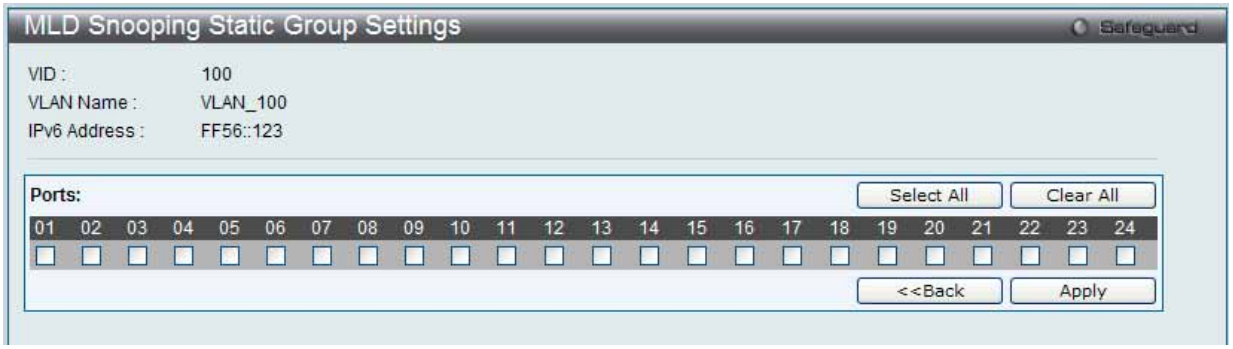


図 7.3-74　MLD Snooping Static Group Settings 画面

2. 以下の項目を設定または表示します。

項目	説明
Ports	ボックスをチェックして、設定するポートを選択します。 • 「Select All」ボタンをクリックするとすべてのポートを選択します。 • 「Clear All」ボタンをクリックするとすべてのポートの選択を解除します。

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

「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

MLD Router Port（ルータポート参照）

スイッチの現在 IPv6 におけるルータポートとして設定されているポートを表示します。

L2 Features > L2 Multicast Control > MLD Snooping > 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 7.3-75　MLD Router Port 画面

以下の項目を設定または表示します。

項目	説明
VID	VLAN ID を入力します。

ルータポートの参照

1. 画面上の VID（VLAN ID）を入力します。

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

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

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。

MLD Snooping Group（MLD Snooping グループ）

スイッチの MLD Snooping グループテーブルを参照します。MLD Snooping 機能では、スイッチを通過する MLD パケットからマルチキャストグループの 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。MLD Snooping は、IPv4 の IGMP Snooping に相当する IPv6 の機能です。

L2 Features > L2 Multicast Control > 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。

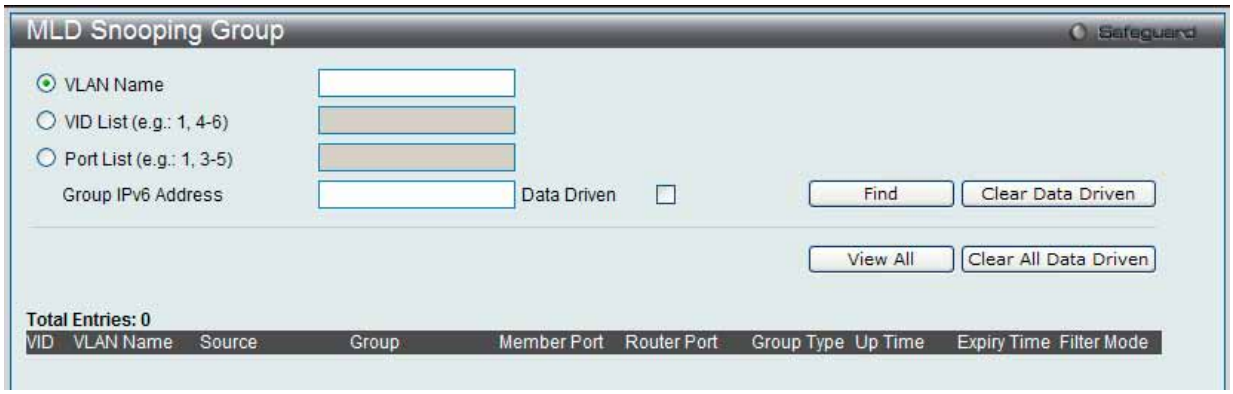


図 7.3-76　MLD Snooping Group 画面

MLD Snooping グループテーブルの参照

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 名を入力します。
VID List (e.g.: 1, 4-6)	マルチキャストグループの VLAN ID リストを入力します。
Port List (e.g.: 1, 3-5)	マルチキャストグループを検索するのに使用されるポート番号を指定します。
Group IPv6 Address	使用するグループ IPv6 アドレスを入力します。
Data Driven	「Data Driven」オプションを選択して、この MLD Snooping グループの Data Driven 機能を有効にします。選択すると、Data Driven グループだけが表示されます。

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」ボタンをクリックして、すべての定義済みエントリを表示します。

エントリの削除

「Clear Data Driven」ボタンをクリックすると、指定 VLAN の Data Driven 機能が学習した MLD Snooping グループを削除します。
「Clear All Data Driven」ボタンをクリックすると、指定 VLAN の Data Driven 機能が学習した MLD Snooping グループをすべて削除します。

MLD Snooping Forwarding Table（MLD Snooping フォワーディングテーブル）

スイッチ上の現在の MLD Snooping フォワーディングテーブルのエントリを表示します。

マルチキャストグループを送出するポートリストと転送される特定の送信元をチェックする簡単な方法を提供します。送信元VLANのパケットをフォワーディング VLAN に転送します。さらに、MLD Snooping はフォワーディングポートを制限します。

1. **L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping Forwarding 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。

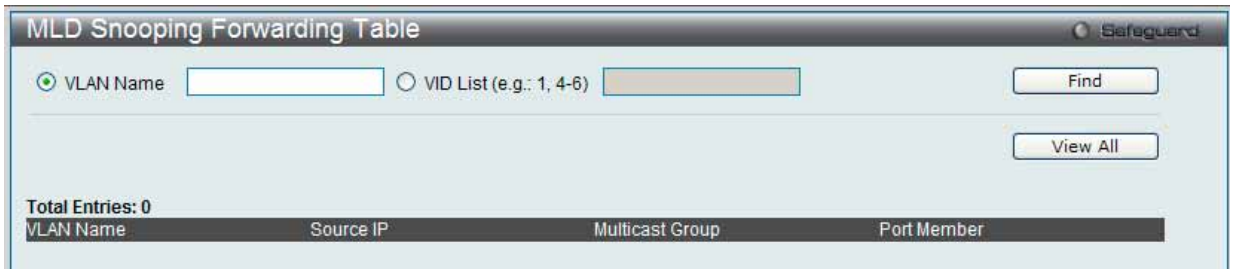


図 7.3-77　MLD Snooping Forwarding Table 画面

2. 以下の項目を使用して検索します。

項目	説明
VLAN Name	MLD Snooping フォワーディングテーブル情報を参照する VLAN 名。
VID List	MLD Snooping フォワーディングテーブル情報を参照するマルチキャストグループの VLAN ID リスト。

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

MLD Snooping Counter（MLD Snooping カウンタ）

MLD Snooping の有効後に、スイッチが受信した MLD プロトコルパケットの統計情報カウンタを表示します。

1. **L2 Features > L2 Multicast Control > MLD Snooping > MLD Snooping 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。

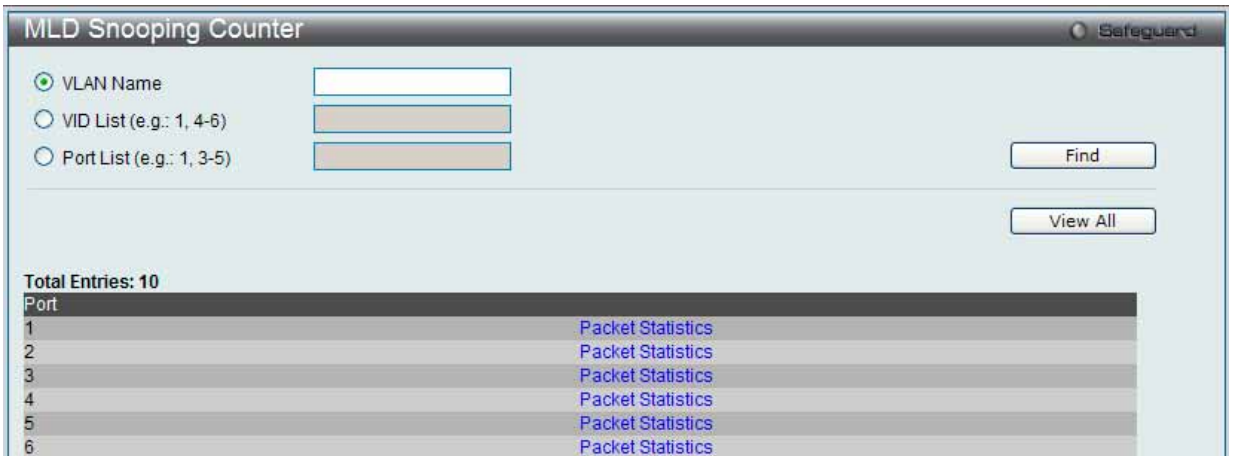


図 7.3-78　MLD Snooping Counter 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
VLAN Name	マルチキャストグループの VLAN 名。
VID List	マルチキャストグループの VLAN ID リスト。
Port List	マルチキャストグループのポートリスト。

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

MLD Snooping カウンタテーブルの参照

「Packet Statistics」リンクをクリックすると、以下の画面が表示されます。

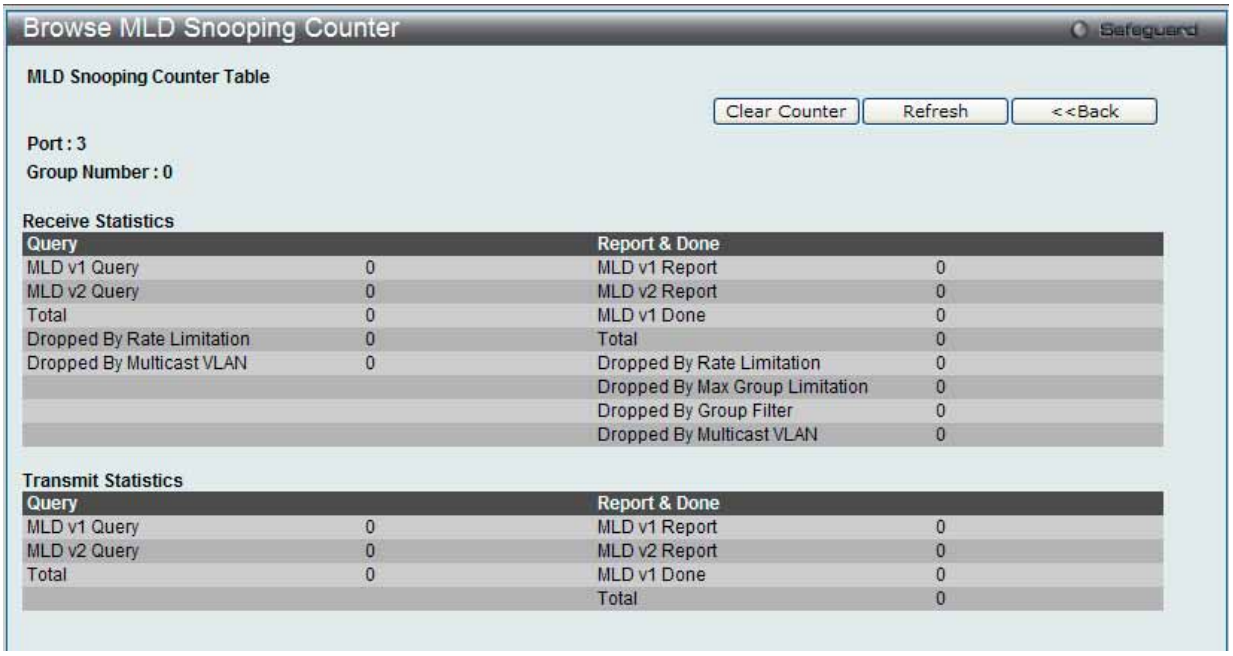


図 7.3-79　Browse MLD Snooping Counter 画面

「Refresh」ボタンをクリックして、テーブルを更新して新しいエントリを表示します。

エントリの削除

「Clear Counter」ボタンをクリックして、本欄に表示したすべてのエントリをクリアします。

「<<Back」をボタンをクリックして前のページに戻ります。

MLD Host Table（MLD ホストテーブル）

MLD ホストテーブルを参照します。

1. **L2 Features > L2 Multicast Control > MLD Snooping > MLD 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。

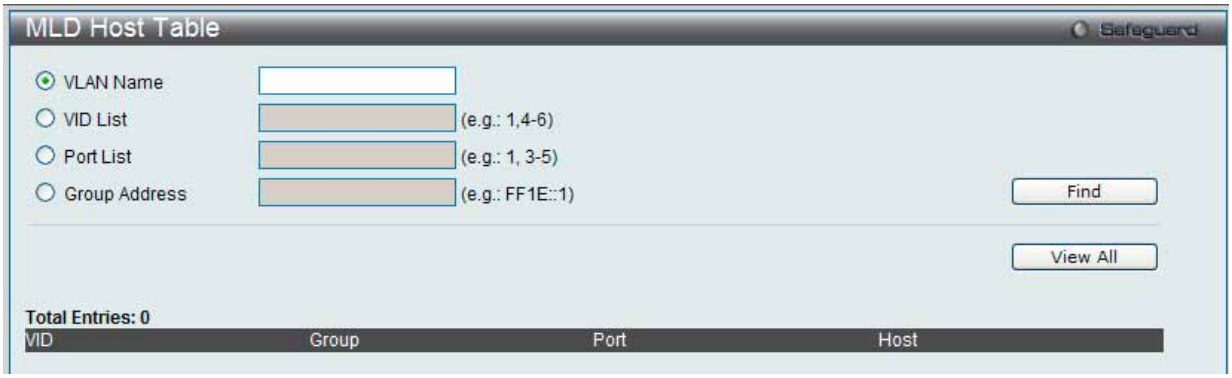


図 7.3-80　MLD Host Table 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
VLAN Name	ラジオボタンをクリックして、表示する VLAN 名を入力します。
VID List	ラジオボタンをクリックして、表示する VLAN ID リストを入力します。
Port List	ラジオボタンをクリックして、表示するポートリストを入力します。
Group Address	ラジオボタンをクリックして、表示するグループアドレスを入力します。

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

Multicast VLAN（マルチキャスト VLAN）

スイッチング環境には、複数の 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キャスト VLAN に対して任意のポートを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ってくるソースポートを設定した後、そのマルチキャストトラフィックを送信す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、指定すると、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。

本スイッチのマルチキャスト VLAN 機能には、以下のような制限があります。

制限と条件 :

1. マルチキャスト VLAN はエッジおよびエッジでないスイッチで実行することができます。

2. メンバポートとソースポートは複数の ISM VLAN で使用できます。しかし、特定の ISM VLAN では、メンバ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。

3. マルチキャスト VLAN はノーマルな 802.1Q VLAN とは排他的です。これは、802.1Q VLAN と ISM VLAN の VLAN ID(VID) と VLAN 名は同じにはできないことを意味します。VID または VLAN 名がどんな VLAN でも一度選択されると、別の VLAN に使用することはできません。

4. 設定された VLAN の通常の表示は設定されたマルチキャスト VLAN を表示しません。

5. 一度、ISM VLAN が有効になると、この VLAN に対応する IGMP Snooping 状態も有効になります。有効になった ISM VLAN の IGMP 機能を無効にすることはできません。

6. 1 つの IP マルチキャストアドレスを複数の ISM VLAN に追加することはできませんが、1 つの ISM VLAN に複数の範囲を追加することはできます。

IGMP Multicast Group Profile Settings（IGMP マルチキャストグループプロファイル設定）

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 マルチキャストアドレス /IP マルチキャストアドレス範囲を設定することができます。

1. **L2 Features > L2 Multicast Control > Multicast VLAN > IGMP Multicast Group 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。

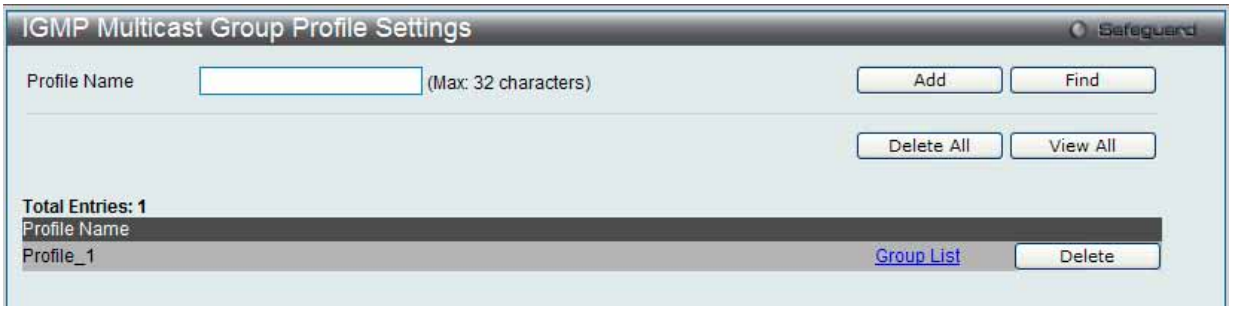


図 7.3-81　IGMP Multicast Group Profile Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Profile Name	IP マルチキャストプロファイル名を入力します。

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

エントリの追加
「Profile Name」を入力して「Add」ボタンをクリックして新しいエントリを追加します。

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

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 7.3-82　Multicast Group Profile Multicast Address Settings 画面

以下の項目を使用して設定および参照します。

項目	説明
Multicast Address List	マルチキャストアドレスリストの値を入力します。

2. 「Multicast Address 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。

「<<Back」をボタンをクリックし、前のページに戻ります。

IGMP Snooping Multicast VLAN Settings（IGMP Snooping マルチキャスト VLAN 設定）

IGMP Snooping マルチキャスト VLAN の作成と設定を行います。

1. **L2 Features > L2 Multicast Control >Multicast VLAN > 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。

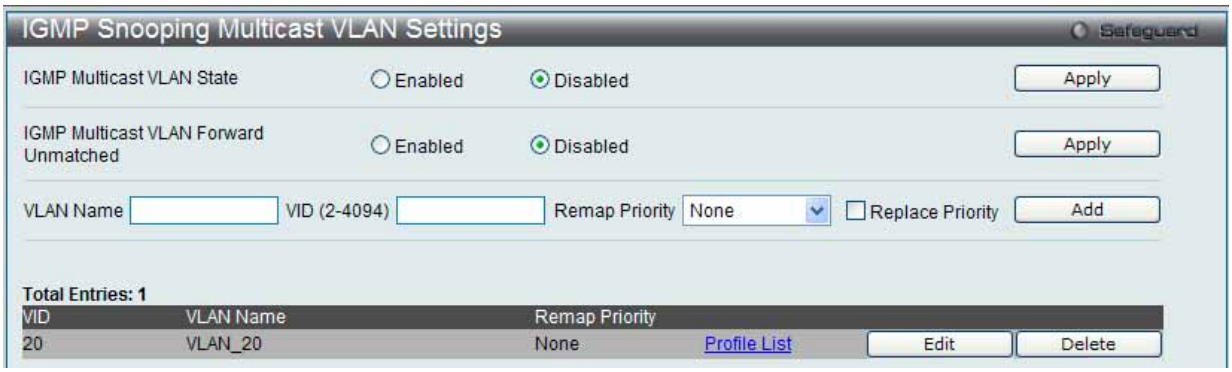


図 7.3-83　IGMP Snooping Multicast VLAN Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
IGMP Multicast VLAN State	IGMP マルチキャスト VLAN 状態を「Enabled」（有効）または「Disabled」（無効）にします。
IGMP Multicast VLAN Forward Unmatched	IGMP マルチキャスト VLAN フォワーディングの不一致の状態を「Enabled」（有効）または「Disabled」（無効）にします。
VLAN Name	使用する VLAN 名を入力します。
VID (2-4094)	使用する VID を指定します。
Remap Priority	• 0-7 - マルチキャスト VLAN に転送されるデータトラフィックに関連するリマップ優先度 (0-7)。 • None - パケットの元の優先度が使用されます。（初期値）
Replace Priority	スイッチはパケットの優先度をリマップ優先度に基づいて変更します。リマップ優先度が設定される場合だけ、このフラグは有効になります。

「Apply」ボタンをクリックして各セクションで行った変更を適用します。

マルチキャスト VLAN の登録

1. 「IGMP Multicast VLAN 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。

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。

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。

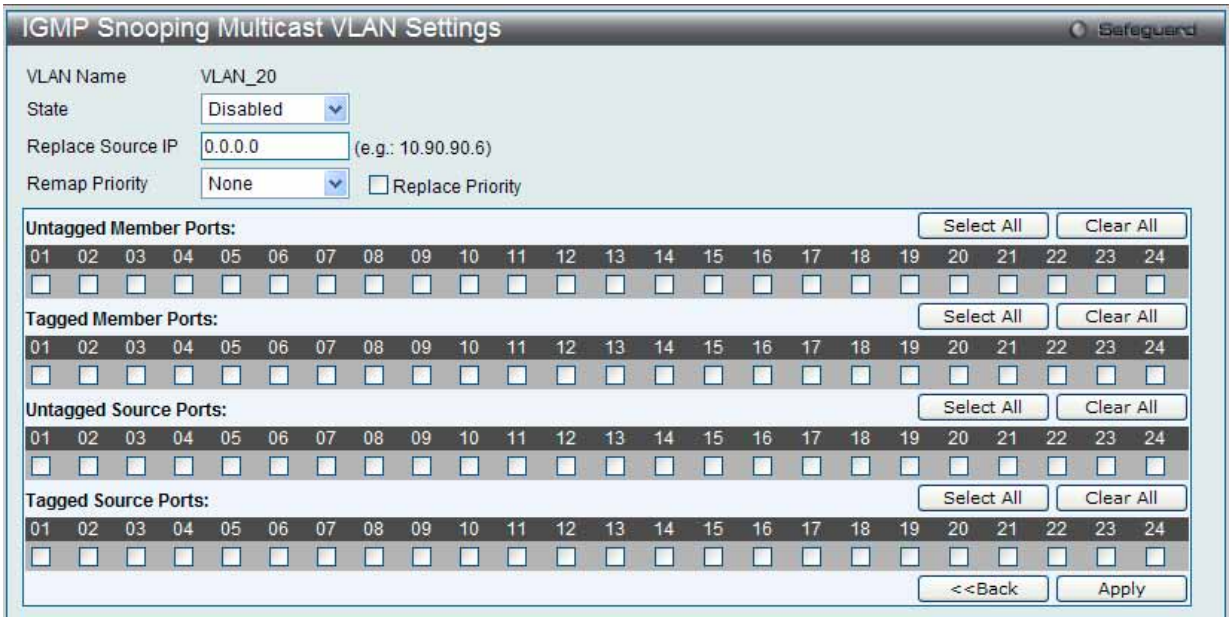


図 7.3-84　IGMP Snooping Multicast VLAN Settings 画面 - Edit

以下の項目を使用して設定および参照します。

項目	説明
VLAN Name	定義済みのマルチキャスト VLAN 名を表示します。
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 アドレスは交換されません。
Remap Priority	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。 • 0-7 - マルチキャスト VLAN に転送されるデータトラフィックに関連するリマップ優先度 (0-7)。 • None - パケットの元の優先度が使用されます。（初期値）
Replace Priority	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。
Untagged Member Ports	マルチキャスト VLAN のタグなしメンバポートを指定します。
Tagged Member Ports	マルチキャスト VLAN のタグ付きメンバポートを指定します。
Untagged Source Ports	マルチキャスト VLAN のタグなしメンバとしてソースポートまたはソースポートの範囲を指定します。タグなしソースポートの PVID は、自動的にマルチキャスト VLAN に対して変更されます。ソースポートは 1 つのマルチキャスト VLAN に対してタグ付けまたはタグなしのいずれかとなり、つまり、両方のタイプは同じマルチキャスト VLAN のメンバとなることができません。
Tagged Source Ports	マルチキャスト VLAN のタグ付きメンバとしてソースポートまたはソースポート範囲を指定します。

「Select All」ボタンをクリックするとすべてのポートを選択します。
「Clear All」ボタンをクリックするとすべてのポートの選択を解除します。

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

「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

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「Profile List」のリンクをクリックし、以下の画面を表示します。

図 7.3-85　IGMP Snooping Multicast VLAN Group List Settings 画面

以下の項目を使用して設定および参照します。

項目	説明
VID	VLAN ID を表示します。
VLAN Name	VLAN 名を表示します。
Profile Name	IGMP Snooping マルチキャスト VLAN グループプロファイル名を選択します。

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

2. プロファイル名を入力し、「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。

MLD Multicast Group Profile Settings（MLD マルチキャストグループプロファイル設定）

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。

1. **L2 Features > L2 Multicast Control > Multicast VLAN > MLD Multicast Group 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。

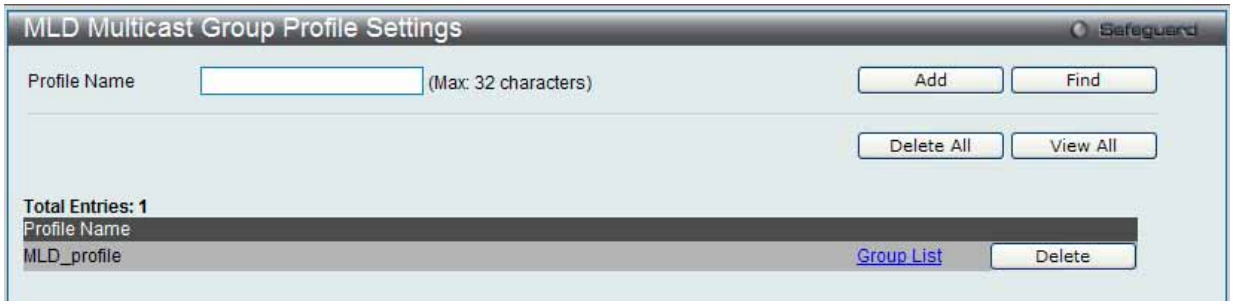


図 7.3-86　MLD Multicast Group Profile Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Profile Name	MLD マルチキャストプロファイル名を入力します。

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

エントリの追加
「Profile Name」を入力して「Add」ボタンをクリックして新しいエントリを追加します。

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

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 7.3-87　Multicast Group Profile Multicast Address Settings 画面 - Edit

以下の項目を使用して設定および参照します。

項目	説明
Multicast Address List	マルチキャストアドレスリストの値を入力します。

2. 「Multicast Address List」でマルチキャストアドレス範囲を入力し、「Add」ボタンをクリックします。

「<<Back」をボタンをクリックし、前のページに戻ります。

MLD Snooping Multicast VLAN Settings（MLD Snooping マルチキャスト VLAN 設定）

MLD Snooping マルチキャスト VLAN の作成と設定を行います。

1. **L2 Features > L2 Multicast Control > Multicast VLAN > MLD 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。

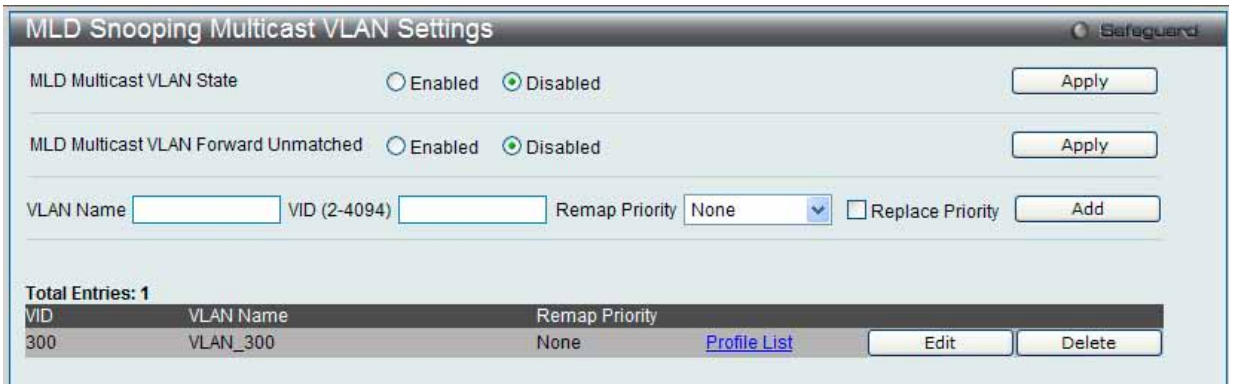


図 7.3-88　MLD Snooping Multicast VLAN Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
MLD Multicast VLAN State	MLD マルチキャスト VLAN 状態を「Enabled」（有効）または「Disabled」（無効）にします。
MLD Multicast VLAN Forward Unmatched	MLD マルチキャスト VLAN フォワーディングの不一致の状態を「Enabled」（有効）または「Disabled」（無効）にします。
VLAN Name	使用する VLAN 名を入力します。
VID (2-2094)	使用する VID を指定します。
Remap Priority	• 0-7 - マルチキャスト VLAN に転送されるデータトラフィックに関連するリマップ優先度 (0-7)。 • None - パケットの元の優先度が使用されます。（初期値）
Replace Priority	スイッチはパケットの優先度をリマップ優先度に基づいて変更します。リマップ優先度が設定される場合だけ、このフラグは有効になります。

「Apply」ボタンをクリックして各セクションで行った変更を適用します。

マルチキャスト VLAN の登録

1. 「MLD Multicast VLAN 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。

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。

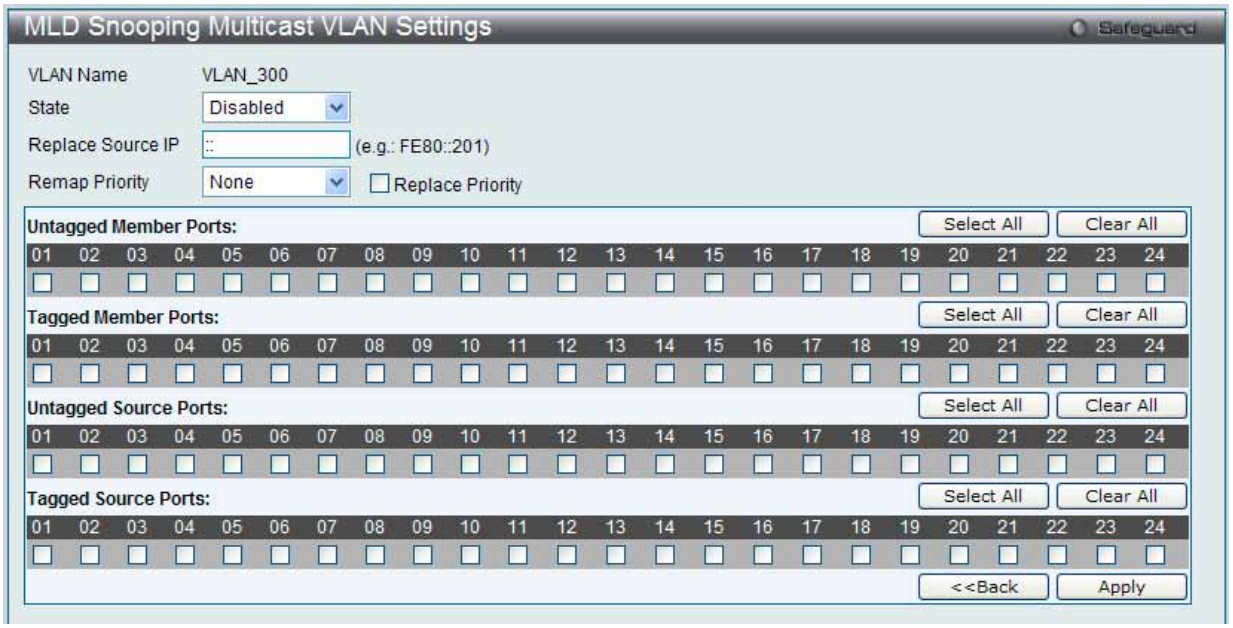


図 7.3-89　MLD Snooping Multicast VLAN Settings 画面 - Edit

以下の項目を使用して設定および参照します。

項目	説明
VLAN Name	定義済みのマルチキャスト VLAN 名を表示します。
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	MLD Snooping 機能を使用すると、ホストが送信した MLD 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 アドレスは交換されません。
Remap Priority	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。 • 0-7 - マルチキャスト VLAN に転送されるデータトラフィックに関連するリマップ優先度 (0-7)。 • None -「none」が指定されると、パケットの元の優先度が使用されます。（初期値）
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。
Untagged Member Ports	マルチキャスト VLAN のタグなしメンバポートを指定します。
Tagged Member Ports	マルチキャスト VLAN のタグ付きメンバポートを指定します。
Untagged Source Ports	マルチキャスト VLAN のタグなしメンバとしてソースポートまたはソースポートの範囲を指定します。タグなしソースポートの PVID は、自動的にマルチキャスト VLAN に対して変更されます。ソースポートは 1 つのマルチキャスト VLAN に対してタグ付けまたはタグなしのいずれかとなり、つまり、両方のタイプは同じマルチキャスト VLAN のメンバとなることができません。
Tagged Source Ports	マルチキャスト VLAN のタグ付きメンバとしてソースポートまたはソースポート範囲を指定します。

「Select All」ボタンをクリックするとすべてのポートを選択します。
「Clear All」ボタンをクリックするとすべてのポートの選択を解除します。
「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

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「Profile List」のリンクをクリックし、以下の画面を表示します。

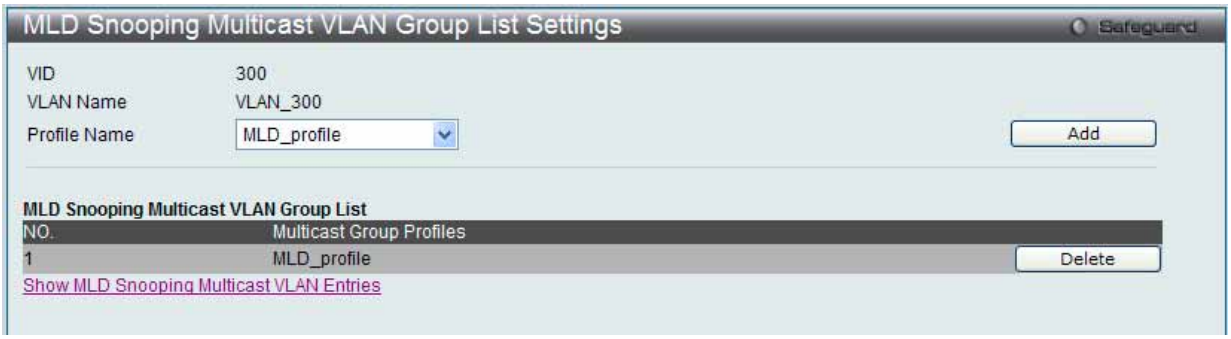


図 7.3-90　MLD Snooping Multicast VLAN Group List Settings 画面

以下の項目を使用して設定および参照します。

項目	説明
VID	VLAN ID が表示されます。
VLAN Name	VLAN 名が表示されます。
Profile Name	MLD Snooping マルチキャスト VLAN グループプロファイル名を選択します。

2. プロファイル名を入力し、「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

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。

「MLD Snooping VLAN Settings」画面に戻るためには、「Show MLD Snooping Multicast VLAN Entries」リンクをクリックします。

Multicast Filtering（マルチキャストフィルタリング）

IPv4 Multicast Filtering（IPv4 マルチキャストフィルタリング）

IPv4 Multicast Profile Settings（IPv4 マルチキャストプロファイル設定）

指定したスイッチポートにマルチキャストアドレスレポートを受信するプロファイルを追加します。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）IPv4 アドレス /IPv4 アドレス範囲を設定することができます。

1. **L2 Features > Multicast Filtering > IPv4 Multicast Filtering > IPv4 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。

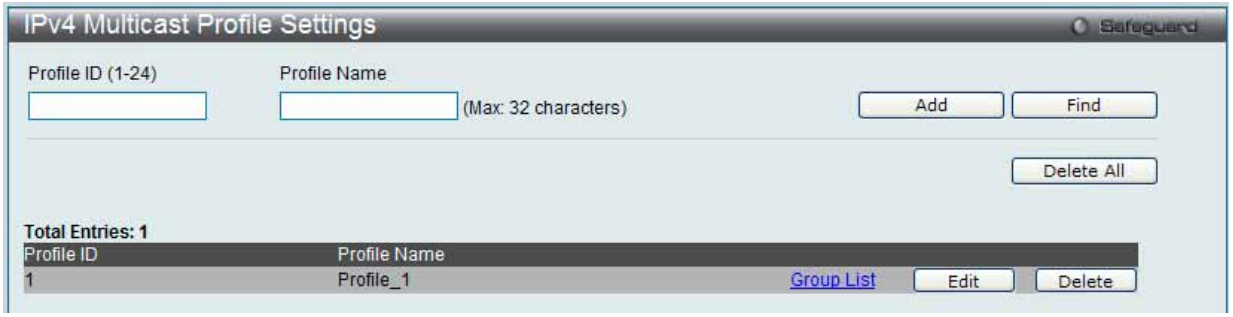


図 7.3-91　IPv4 Multicast Profile Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Profile ID (1-60)	プロファイル ID を入力します。
Profile Name	IP マルチキャストプロファイル名を入力します。

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

エントリの登録

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。

エントリの編集

1. 「Edit」ボタンをクリックして、以下の画面を表示します。

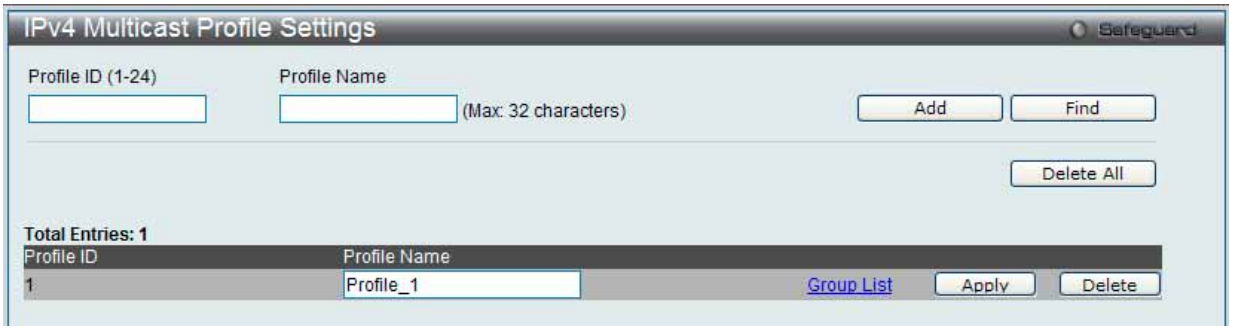


図 7.3-92　IPv4 Multicast Profile Settings 画面 - Edit

2. 指定エントリ名を編集し、「Apply」ボタンをクリックします。

エントリの削除

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

マルチキャストグループリストの設定

1. 「Group List」リンクをクリックすると、以下の画面が表示されます。

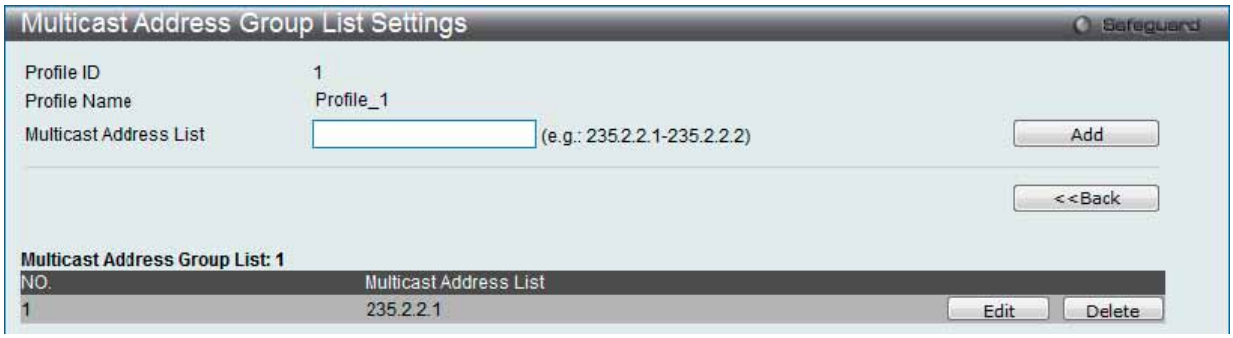


図 7.3-93　Multicast Address Group List Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Profile ID	プロファイル ID が表示されます。
Profile Name	プロファイル名が表示されます。
Multicast Address List	マルチキャストアドレスリストを入力します。

エントリの登録

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。

「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

エントリの編集

1. 「Edit」ボタンをクリックして、以下の画面を表示します。

図 7.3-94　IPv4 Multicast Profile Settings 画面 - Edit

2. 指定エントリを編集して「Apply」ボタンをクリックします。

エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。

IPv4 Limited Multicast Range Settings（IPv4 マルチキャスト範囲の限定設定）

IPv4 マルチキャスト範囲の制限設定を適用するスイッチのポートまたはVLANを設定します。送信元ポートごとに受信ポートに送信可能なマルチキャストアドレスの範囲を設定します。

1. **L2 Features > Multicast Filtering > IPv4 Multicast Filtering > IPv4 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。

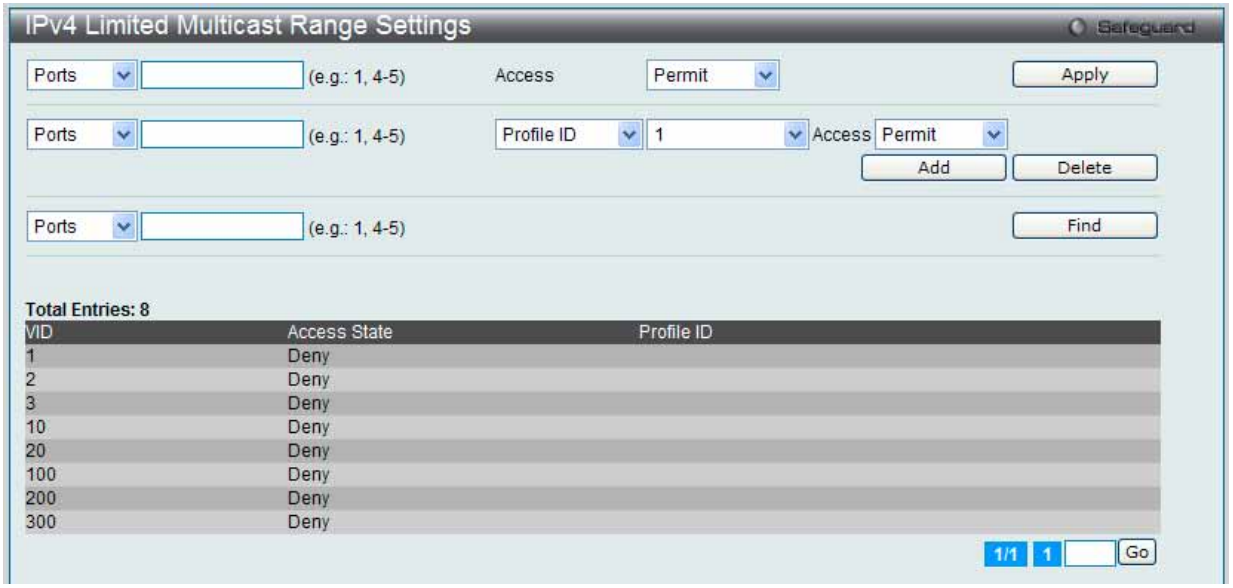


図 7.3-95　IPv4 Limited Multicast Range Settings 画面

2. 制限する IP マルチキャストの範囲に含まれるスイッチポートを設定します。

マルチキャストアドレスフィルタリング機能の設定

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
Ports / VID List	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または VLAN ID を指定します。
Access	以下のオプションの一つを選択します。 • Permit - 指定したポートまたは VID に一致するパケットを許可することを指定します。 • Deny - 指定したポートまたは VID 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。

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

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
Ports	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。

エントリの検索

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

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

IPv4 Max Multicast Group Settings（IPv4 マルチキャストグループの最大数の設定）

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。

1. **L2 Features > Multicast Filtering > IPv4 Multicast Filtering > IPv4 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。

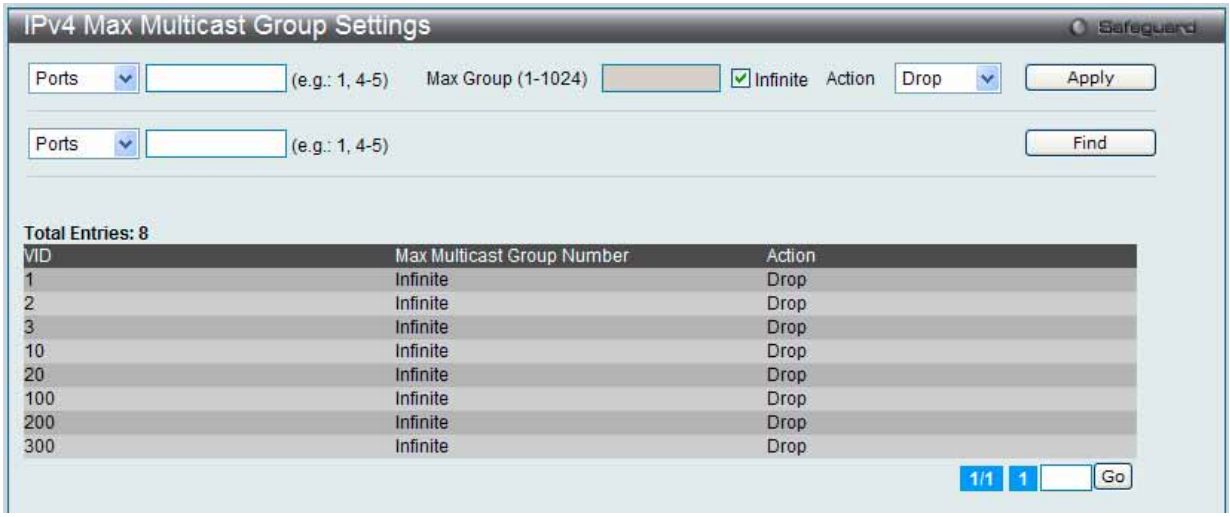


図 7.3-96　IPv4 Max Multicast Group Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Ports	本設定に使用される適切なポートまたは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。「Infinite」ボックスをチェックしない場合、最大グループ数を入力します。
Infinite	「Infinite」（制限なし）を「Enabled」（有効）または「Disabled」（無効）にします。
Action	ルールに適切な操作を選択します。 • Drop - 破棄の動作を行います。 • Replace - 交換の動作を行います。

エントリの追加

適切な情報を入力し「Apply」ボタンをクリックします。

エントリの参照

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

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

IPv6 Multicast Filtering（IPv6 マルチキャストフィルタリング）

指定したスイッチポートにマルチキャストアドレスレポートを受信するプロファイルを追加します。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）IPv6 アドレス /IPv6 アドレス範囲を設定することができます。

IPv6 Multicast Profile Settings（IPv6 マルチキャストプロファイル設定）

IPv6 マルチキャストプロファイルの追加、削除、または設定を行います。

1. **L2 Features > Multicast Filtering > IPv6 Multicast Filtering > IPv6 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。

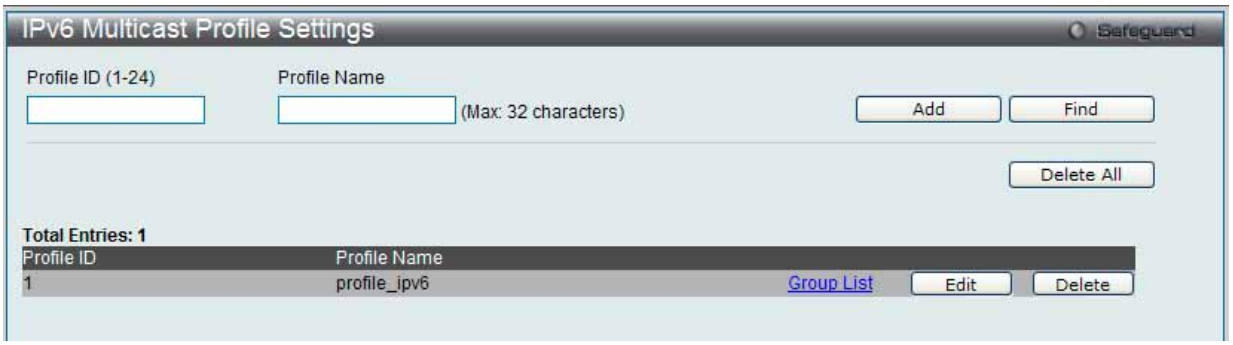


図 7.3-97　IPv6 Multicast Profile Settings 画面

2. 以下の項目を使用して設定および参照します。

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

エントリの登録

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

エントリの参照

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

エントリの編集

1. 「Edit」ボタンをクリックして、以下の画面を表示します。

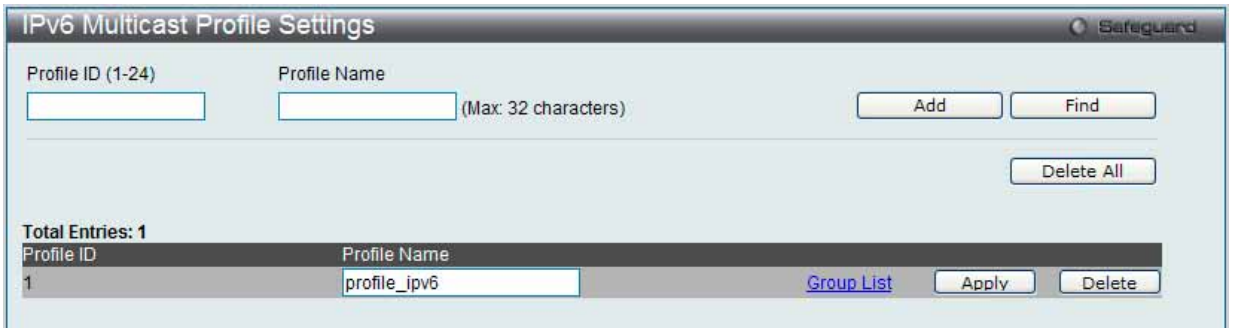


図 7.3-98　IPv6 Multicast Profile Settings 画面 - Edit

2. 指定エントリを編集して「Apply」ボタンをクリックします。

エントリの削除

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

マルチキャストグループリストの設定

1. 「Group List」リンクをクリックすると、以下の画面が表示されます。

図 7.3-99　Multicast Address Group List Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Profile ID	プロファイル ID が表示されます。
Profile Name	プロファイル名が表示されます。
Multicast Address List	マルチキャストアドレスリストを入力します。

エントリの登録

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

「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

エントリの編集

1. 「Edit」ボタンをクリックして、以下の画面を表示します。

図 7.3-100　Multicast Address Group List Settings 画面 - Edit

2. 指定エントリを編集して「Apply」ボタンをクリックします。

エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。

IPv6 Limited Multicast Range Settings（IPv6 マルチキャスト範囲の限定設定）

IPv6 マルチキャスト範囲の制限設定を適用するスイッチのポートまたはVLANを設定します。送信元ポートごとに受信ポートに送信可能なマルチキャストアドレスの範囲を設定します。

1. **L2 Features > Multicast Filtering > IPv6 Multicast Filtering > IPv6 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。

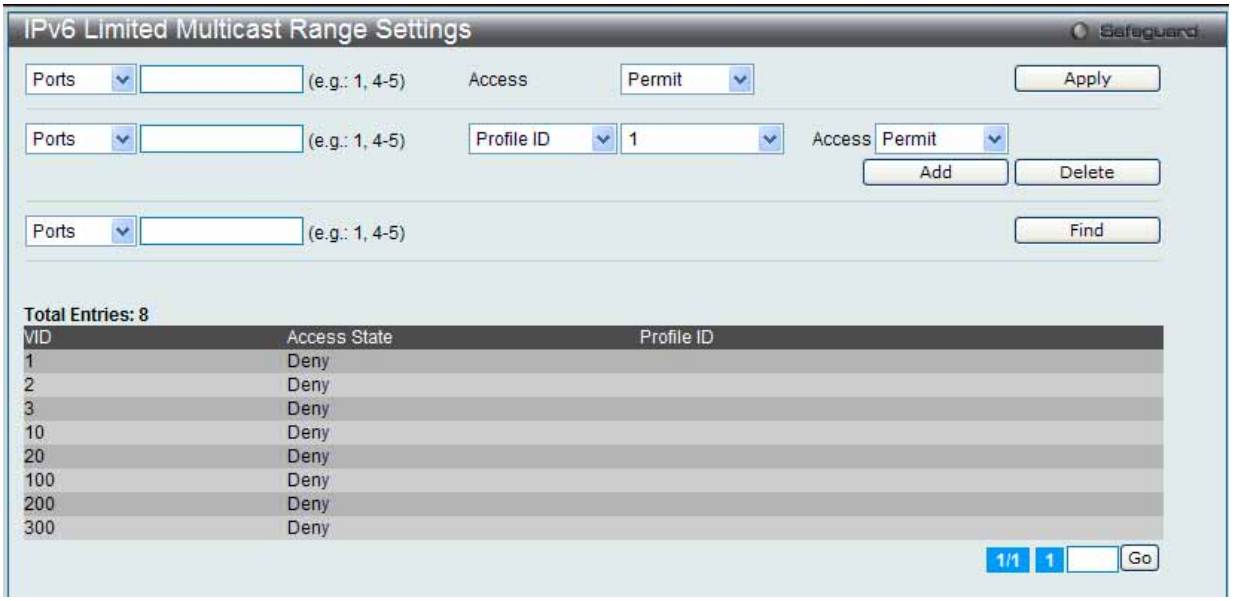


図 7.3-101　IPv6 Limited Multicast Range Settings 画面

2. 制限する IP マルチキャストの範囲に含まれるスイッチポートを設定します。

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

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
Ports/VID List	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または VID 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 - 指定したポートまたは VID に一致するパケットを許可することを指定します。 • Deny - 指定したポートまたは VID 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。

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

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
Ports / VID List	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または VID 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。

エントリの検索

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

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

IPv6 Max Multicast Group Settings（IPv6 マルチキャストグループの最大数の設定）

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。

1. **L2 Features > Multicast Filtering > IPv6 Multicast Filtering > IPv6 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。

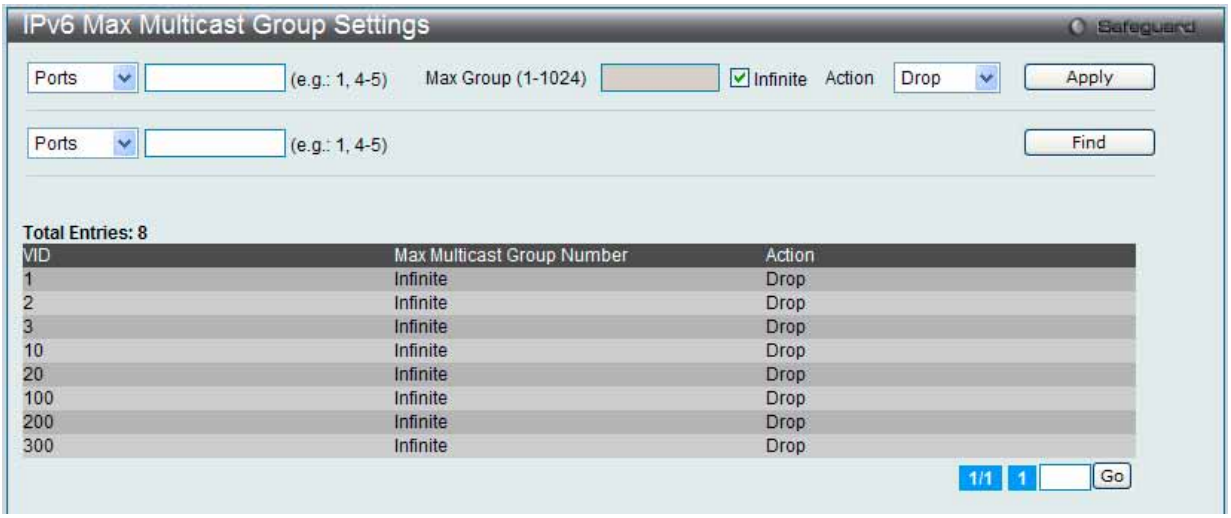


図 7.3-102　IPv6 Max Multicast Group Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Ports / VID List	本設定に使用される適切なポート範囲または VID 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。「Infinite」ボックスをチェックしない場合、最大グループ数を入力します。
Infinite	「Infinite」（制限なし）を「Enabled」（有効）または「Disabled」（無効）にします。
Action	ルールに適切な操作を選択します。「Drop」を選択すると破棄の動作を行い、「Replace」を選択すると交換の動作を行います。

エントリの登録

適切な情報を入力し「Apply」ボタンをクリックします。

エントリの検索

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

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

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

マルチキャストフィルタリングモードを設定します。

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

図 7.3-103　Multicast Filtering Mode 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
VLAN Name / VID List	フィルタリングが適用される VLAN を指定します。「All」をチェックするとすべての VLAN にフィルタリングが適用されます。
Multicast Filtering Mode	指定した VLAN 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 All Groups - 指定ポート VLAN にすべてのマルチキャストパケットを転送します。 • 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。

エントリの検索

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

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

ERPS Settings（イーサネットリングプロテクション設定）

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

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

G.8032 の用語と概念

用語	説明
RPL (Ring Protection Link)	ブリッジされたリングでループを防ぐためにアイドル状態でブロックされるメカニズムによって指定されるリンク。
RPL Owner	アイドル状態で RPL 上のトラフィックをブロックし、保護状態でブロックを解除する RPL に接続するノード。
R-APS (Ring - Automatic Protection Switching)	RAPS VLAN（R-APS チャンネル）経由でリング上の保護操作を調整するために使用する Y.1731 および G.8032 に定義されているプロトコルメッセージ。
RAPS VLAN (R-APS Channel)	R-APS メッセージ送信用の個別のリング範囲における VLAN。
Protected VLAN	通常のネットワークトラフィックの送信用サービストラフィック VLAN。

スイッチの ERPS 機能を有効にします。

注意 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 オーナの設定前に ERPS を有効にすることはできません。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のでご注意ください。

1. **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。

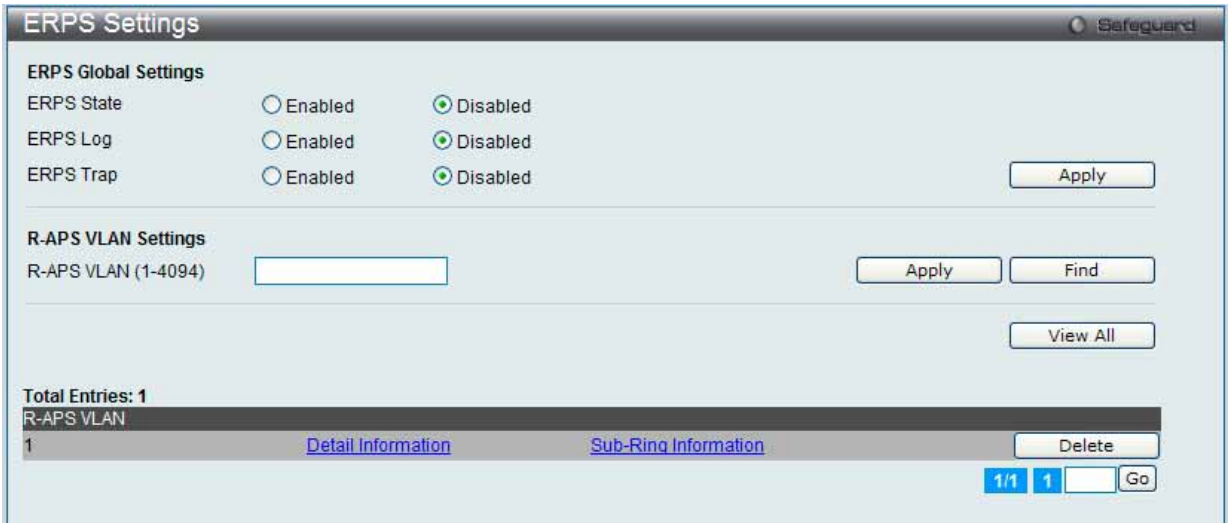


図 7.3-104　ERPS Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
ERPS Global Settings	
ERPS State	ERPS 状態を「Enabled」（有効）または「Disabled」（無効）にします。
ERPS Log	ERPS ログを「Enabled」（有効）または「Disabled」（無効）にします。
ERPS Trap	ERPS トラップを「Enabled」（有効）または「Disabled」（無効）にします。
R-APS VLAN Settings	
R-APS VLAN (1-4094)	R-APS VLAN とする VLAN を指定します。

各セクションの「Apply」ボタンをクリックして、設定を適用します。

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

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、「Apply」ボタンをクリックします。

詳細情報の参照

「Detail Information」リンクをクリックすると、以下の画面が表示されます。

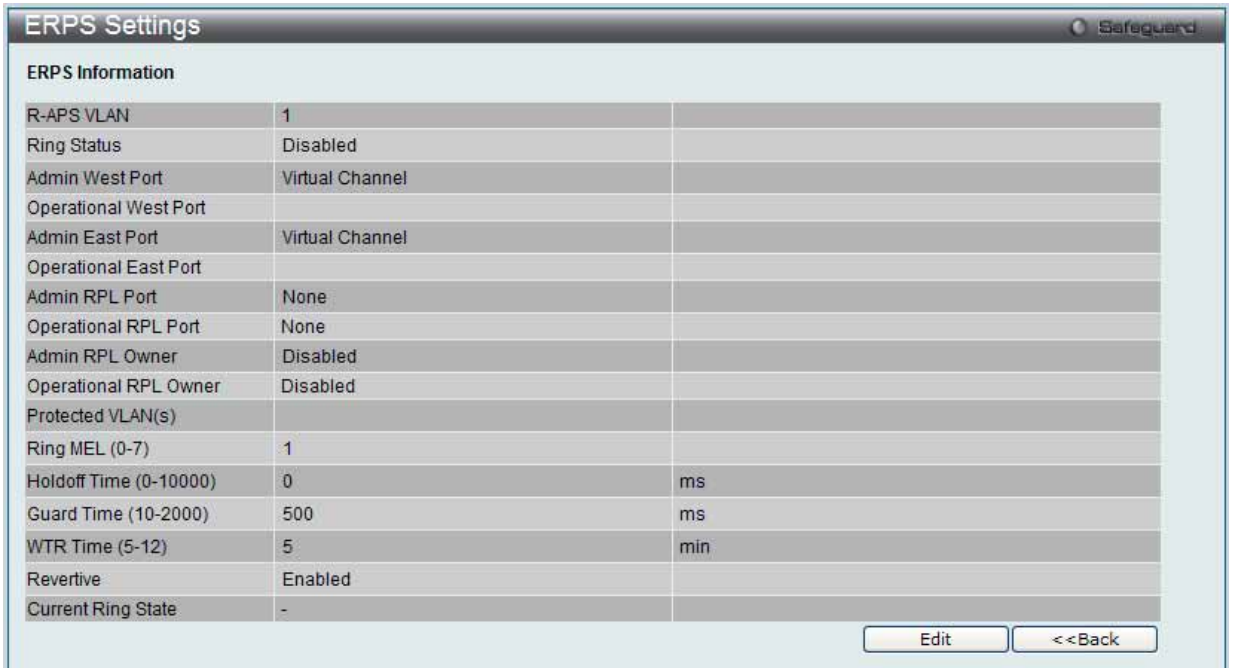


図 7.3-105　ERPS Settings 画面 - ERPS Information

エントリの編集

1. 「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。

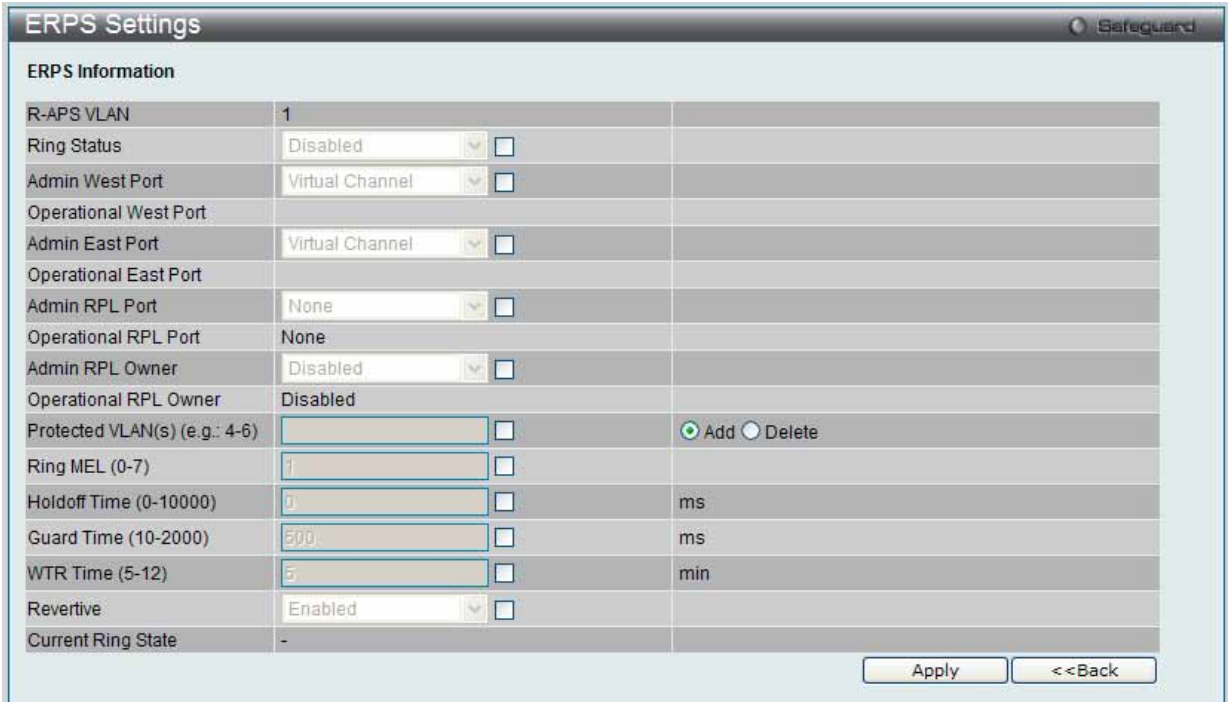


図 7.3-106　ERPS Settings 画面 - Edit

以下の項目を使用して設定および参照します。

項目	説明
R-APS VLAN	R-APS VLAN ID を表示します。
Ring Status	チェックし、プルダウンメニューを使用して、指定リングを「Enabled」（有効）/「Disabled」（無効）にします。
Admin West Port	チェックし、West リングポートとしてポートを指定します。また、使用する仮想ポートチャンネルも指定します。
Operational West Port	操作可能な West ポート値が表示されます。
Admin East Port	チェックし、East リングポートとしてポートを指定します。また、使用する仮想ポートチャンネルも指定します。
Operational East Port	操作可能な East ポート値が表示されます。
Admin RPL Port	チェックし、使用する RPL ポートを指定します。オプションを West Port、East Port、および None から選択します。
Operational RPL Port	操作可能な RPL ポートを表示します。
Admin RPL Owner	チェックを行い、プルダウンメニューを使用して、RPL オーナノードを「Enabled」（有効）/「Disabled」（無効）にします。
Operational RPL Owner	操作可能な RPL オーナを表示します。
Protected VLAN(s)	チェックを行い、「Add」または「Delete」を指定して、防御する VLAN グループを入力します。
Ring MEL (0-7)	チェックを行い、R-APS 機能のリングの MEL を入力します。リングの MEL の初期値は 1 です。
Holdoff Time (0-10000)	チェックを行い、R-APS 機能のホールドオフタイムを入力します。初期値は 0（ミリ秒）です。
Guard Time (10-2000)	チェックを行い、R-APS 機能のガードタイムを入力します。初期値は 500（ミリ秒）です。
WTR Time (5-12)	チェックを行い、R-APS 機能の WTR タイムを入力します。
Revertive	チェックを行い、プルダウンメニューを使用して、R-APS 復帰オプションを「Enabled」（有効）/「Disabled」（無効）にします。
Current Ring State	現在のリング状態を表示します。

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。

「<<Back」をボタンをクリックして前のページに戻ります。

サブリング情報の参照

1. 「Sub-Ring Information」リンクをクリックすると、以下の画面が表示されます。

図 7.3-107　ERPS Sub-Ring Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
R-APS VLAN	R-APS VLAN ID が表示されます。
Sub-Ring R-APS VLAN (1-4094)	使用するサブリングの R-APS VLAN ID を入力します。
State	チェックを行い、プルダウンメニューを使用して、ERPS のサブリングを追加または削除にします。
TC Propagation State	チェックを行い、プルダウンメニューを使用して、TC 伝搬の状態を「Enabled」（有効）/「Disabled」（無効）にします。

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。

「<<Back」をボタンをクリックして前のページに戻ります。

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。

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 ネットワークに接続する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）に格納されるため、SNMP（Simple Network Management Protocol）などの管理プロトコルを使用し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 グローバルパラメータを設定します。

1. **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。

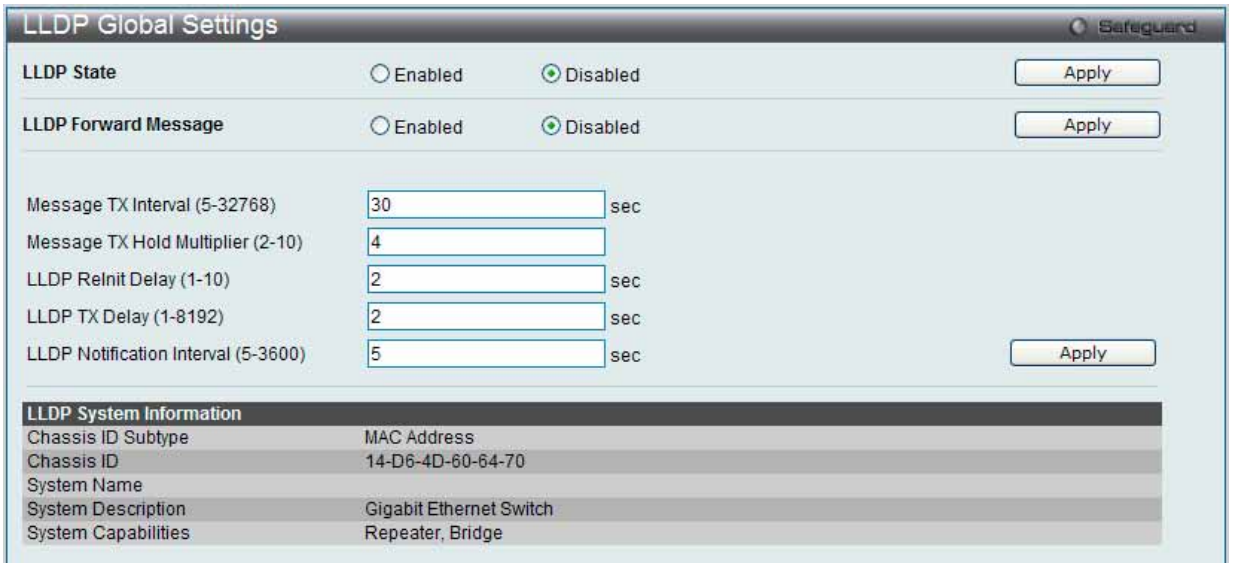


図 7.3-108　LLDP Global Settings 画面

2. 以下の項目を使用して設定および参照します。

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 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、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）

LLDP ポートパラメータを設定します。

1. **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。

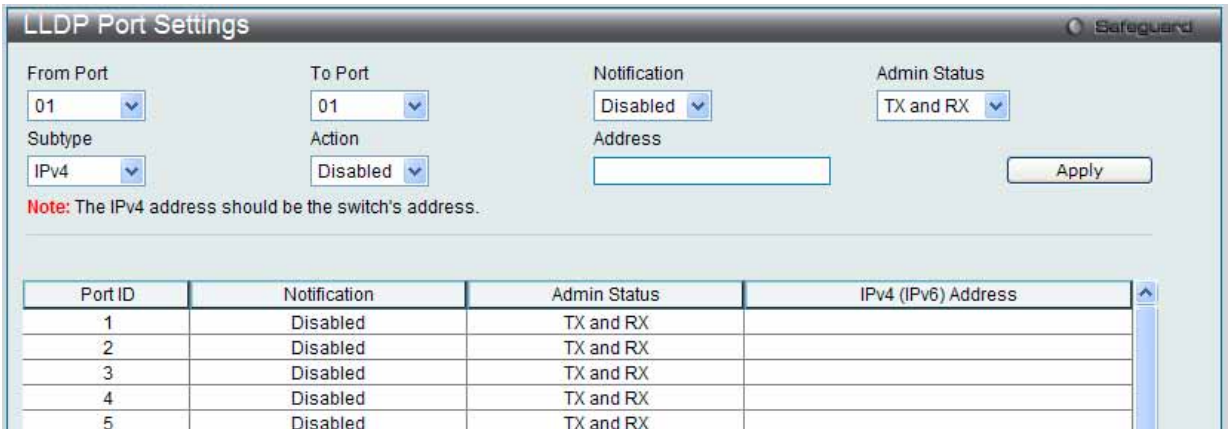


図 7.3-109　LLDP Port Settings 画面

2. 以下の項目を使用して設定および参照します。

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	送信される IP アドレス情報（IPv4 / IPv6）のタイプを選択します。
Action	ポートベースの管理アドレス機能を「Enabled」（有効）または「Disabled」（無効）にします。
Address	通知するエンティティの管理アドレスを入力します。

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

注意　ここに入力する IPv4 または IPv6 アドレスを既存の LLDP 管理 IP アドレスとする必要があります。

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

LLDP 管理アドレスを参照します。

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

図 7.3-110　LLDP Management Address List 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
IPv4 / IPv6	「IPv4」または「IPv6」を選択します。
Address	通知するエンティティの管理 IP アドレスを入力します。IPv4 アドレスは管理 IP アドレスであるため、IP 情報がフレームと共に送信されます。

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

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

TLV（Type-length-value）は、LLDP パケット内の TLV エレメントとして特定の送信情報を許可します。本スイッチにおけるベーシック TLV 設定を有効にします。

スイッチのアクティブな LLDP ポートは、通常その外向き通知にいつも必須データを含んでいます。外向き LLDP 通知からこれらのデータタイプの 1 個以上を除外するために、個別のポートまたはポートグループに設定できる 4 つのオプションデータがあり、必須データタイプには、4 つの基本的な情報タイプ（end of LLDPDU TLV、chassis ID TLV、port ID TLV および Time to Live TLV）があります。必須データタイプは無効にすることができません。さらに、オプションで選択可能な 4 つのデータタイプ（Port Description、System Name、System Description および System Capability）があります。

本スイッチにおけるベーシック TLV 設定を有効にします。

1. **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。

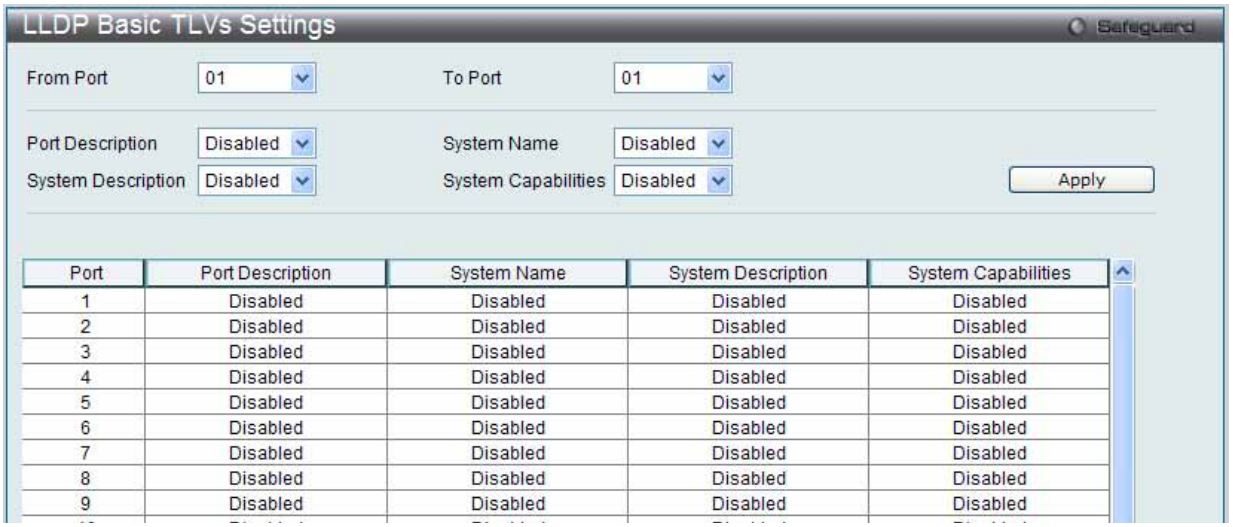


図 7.3-111　LLDP Basic TLVs Settings 画面

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。

2. 以下の項目を使用して設定および参照します。

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	システムケーパビリティを「Enabled」（有効）/「Disabled」（無効）にします。

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

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。

1. **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。

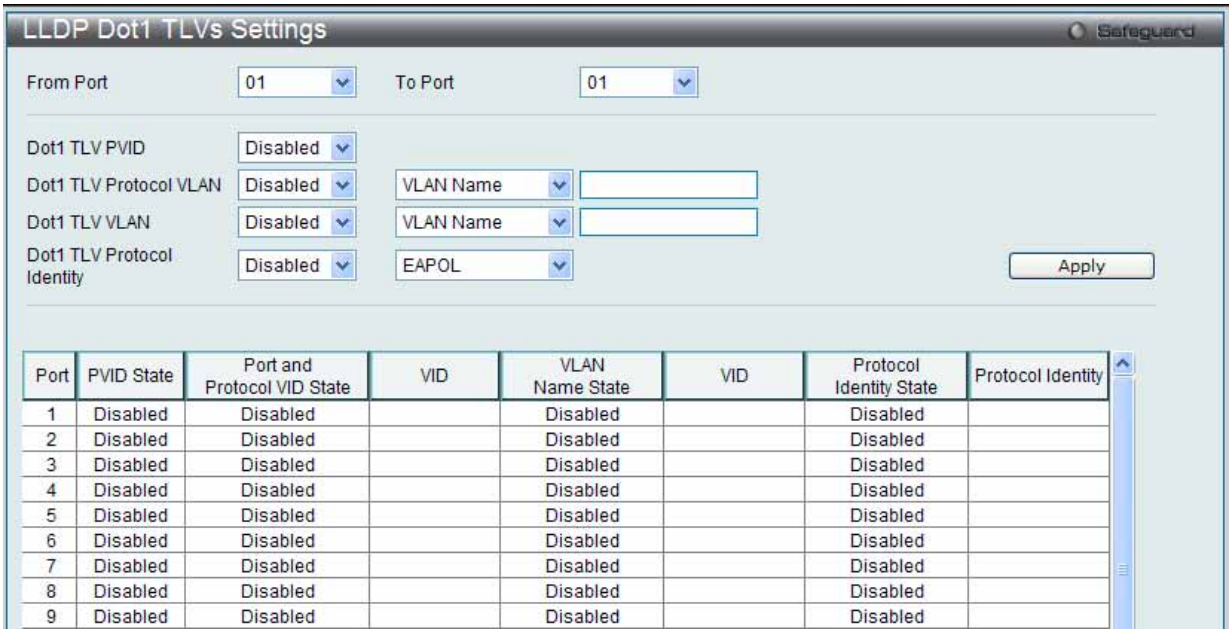


図 7.3-112　LLDP Dot1 TLVs Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
From Port/To Port	設定するポート範囲を指定します。
Dot1 TLV PVID	Dot1 TLV PVID の通知を「Enabled」（有効）/「Disabled」（無効）にします。
Dot1 TLV Protocol VLAN	プロトコル VLAN ID の通知を「Enabled」（有効）/「Disabled」（無効）にします。本オプションの有効後、次のプルダウンメニューで「VLAN Name」、「VID List」または「All」を選択することができます。これを選択後に、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。
Dot1 TLV VLAN	Dot1 TLV VLAN の「Enabled」（有効）/「Disabled」（無効）、および設定を行います。本オプションの有効後、次のプルダウンメニューで「VLAN Name」、「VID List」または「All」を選択することができます。これを選択後に、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。
Dot1 TLV 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。

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 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 IEEE802.3 で規定された特定の TLV データタイプを除外するように設定します。

1. **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。

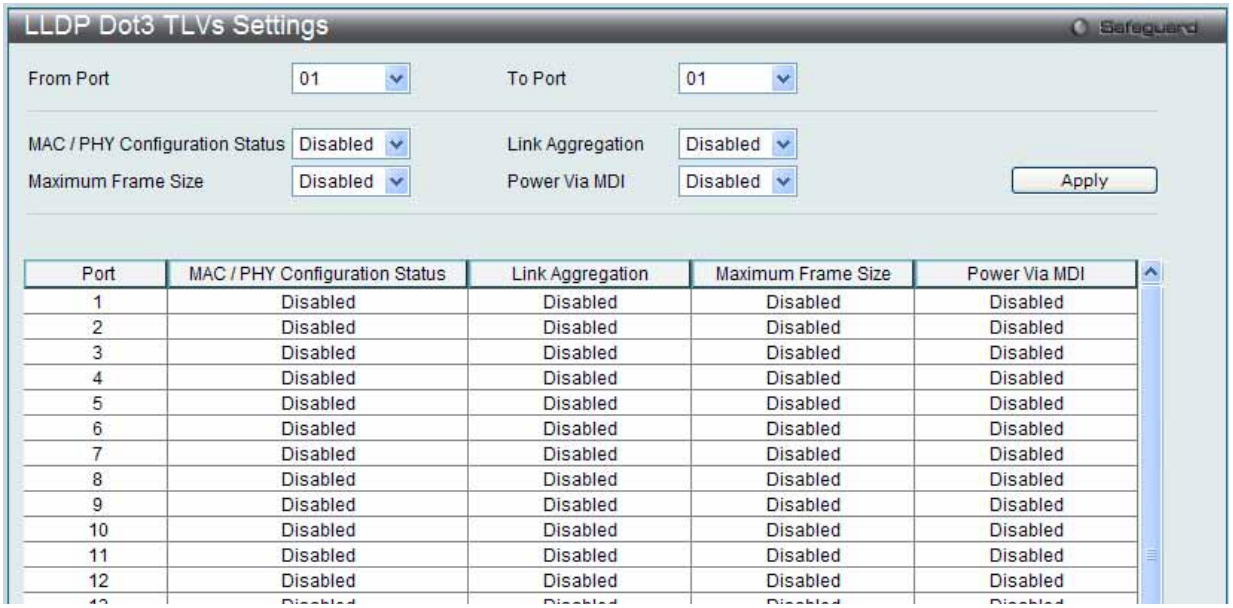


図 7.3-113　LLDP Dot3 TLVs Settings 画面

2. 以下の項目を使用して設定および参照します。

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 タイプが含まれます。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。
Power Via MDI	プルダウンメニューを使用して、MDI 経由の電力供給機能を「Enable」（有効）/「Disable」（無効）にします。 MDI TLV 経由の電力供給により、ネットワーク管理が通知を行い、送信する IEEE 802.3 LAN ステーション MDI 電力のサポート機能を検出します。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。

LLDP Statistics System（LLDP 統計情報システム）

スイッチの各ポートにおける Neighbor 検出アクティビティ、LLDP 統計情報および設定の概要を表示します。ポート番号を選択し、「Find」ボタンをクリックして、特定ポートの統計情報を参照します。

1. **L2 Features > 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。

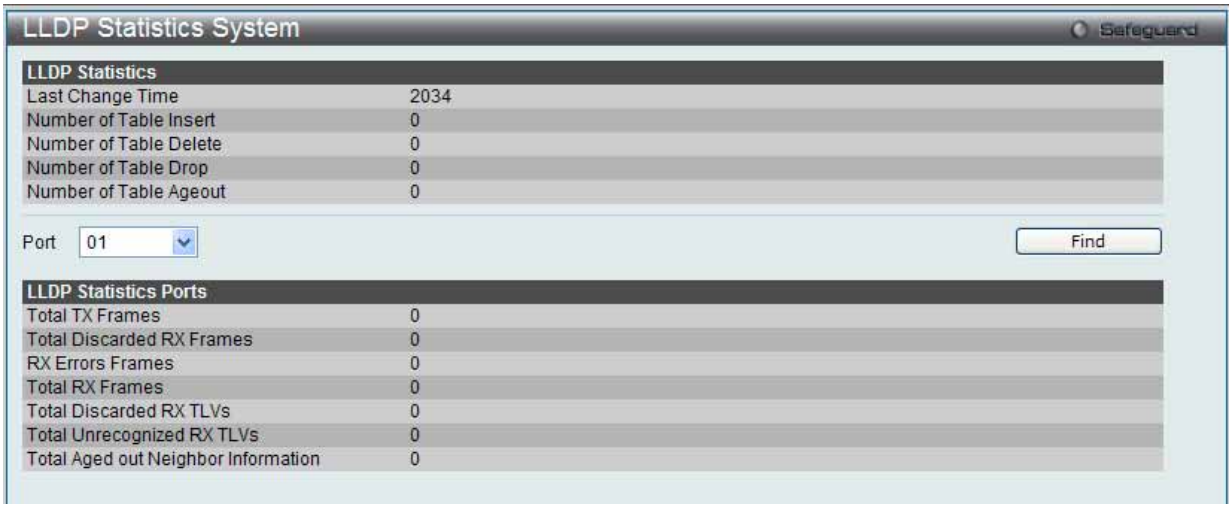


図 7.3-114　LLDP Statistics System 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Port	プルダウンメニューを使用してポートを指定します。

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

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

ローカルポートの要約テーブルに外向きの LLDP 通知を入力するために現在有効なポートごとの情報を表示します。

ポートごとに LLDP ローカルポート情報を参照するには、「Show Normal」ボタンをクリックします。
ポートごとに LLDP Local Port 情報の概要を参照するためには、「Show Brief」ボタンをクリックします。

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

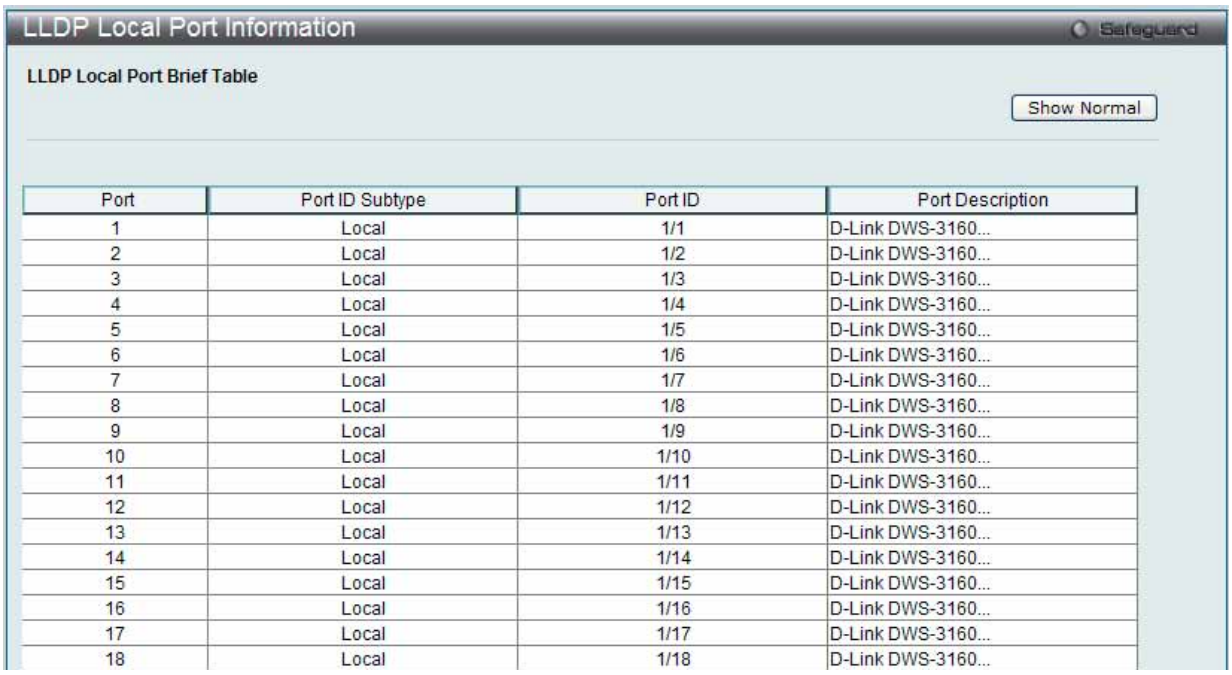


図 7.3-115　LLDP Local Port Information 画面 - Brief

図 7.3-116　LLDP Local Port Information 画面 - Normal

2.　以下の項目を使用して設定および参照します。

項目	説明
Port	プルダウンメニューを使用してポートを指定します。

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

詳細情報の表示

管理アドレスカウントに関してさらに詳細を参照するためには、「Management Address Count」の「Show Detail」リンクをクリックします。

図 7.3-117　LLDP Local Port Information 画面 - Detail

「<<Back」をボタンをクリックして前のページに戻ります。

LLDP Remote Port Information（LLDP リモートポート情報）

Neighbor から学習したポート情報を表示します。スイッチは、リモートステーションからのパケットを受信しますが、ローカルとして情報を保存することができます。

1. **L2 Features > 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 7.3-118　LLDP Remote Port Information 画面 - Brief

2. 以下の項目を使用して設定および参照します。

項目	説明
Port	プルダウンメニューを使用してポートを指定します。

ポート番号を選択し、「Find」ボタンをクリックして指定ポートの統計情報を表示します。

ポートごとに LLDP リモートポート情報を参照するには、「Show Normal」ボタンをクリックします。

図 7.3-119　LLDP Remote Port Information 画面 - Normal

「<<Back」をボタンをクリックして前のページに戻ります。

NLB FDB Settings（NLB FDB 設定）

本スイッチは、NLB（ネットワークロードバランシング）をサポートしています。これは、複数のサーバが同じ IP アドレスと MAC アドレスを共有できるマイクロソフト社のサーバロードバランシングアプリケーションをサポートするための MAC フォワーディングコントロールです。クライアントからのリクエストをすべてのサーバに送信しますが、それらの 1 つだけが処理します。マルチキャストモードでは、クライアントはサーバに到達するようにマルチキャスト MAC を宛先 MAC として使用します。モードに関係なく、宛先 MAC は共有 MAC です。サーバは応答パケットの送信元 MAC アドレスとして (共有 MAC よりむしろ) 自身の MAC アドレスを使用します。NLB マルチキャスト FDB エントリは L2 マルチキャストエントリと相互に排他的になっています。

1. **L2 Features > NLB FDB 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。

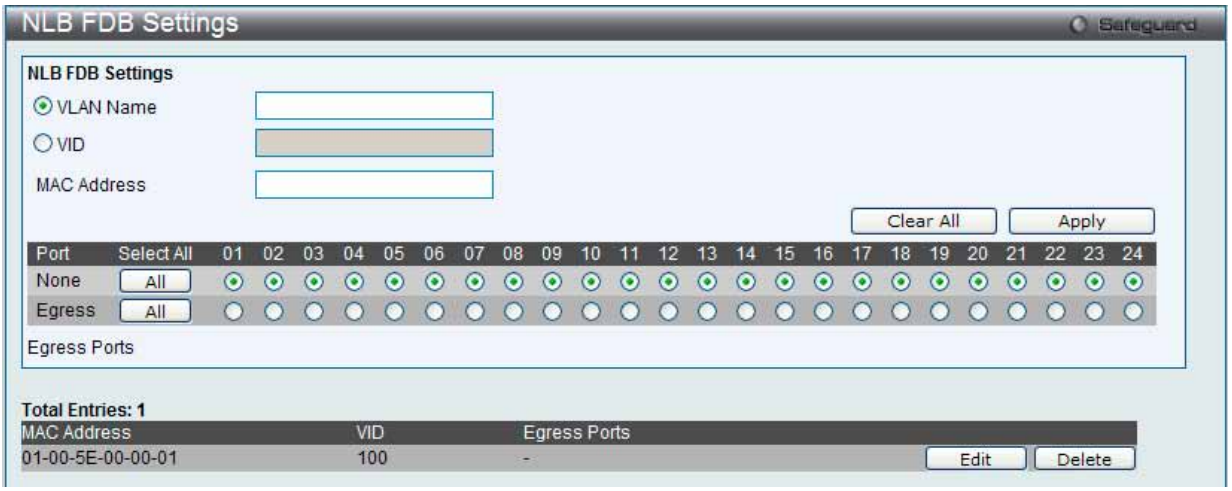


図 7.3-120　NLB FDB Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
VLAN Name	ラジオボタンをクリックして、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	ラジオボタンをクリックして、VLAN ID を入力します。
MAC Address	作成される NLB マルチキャスト FDB エントリの MAC アドレスを入力します。
Port	指定した NLB マルチキャスト 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。 • None - ポートはフォワーディングポートではありません。「All」ボタンをクリックするとすべてのポートを選択します。 • Egress - ポートはフォワーディングポートです。「All」ボタンをクリックするとすべての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。

エントリの編集

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

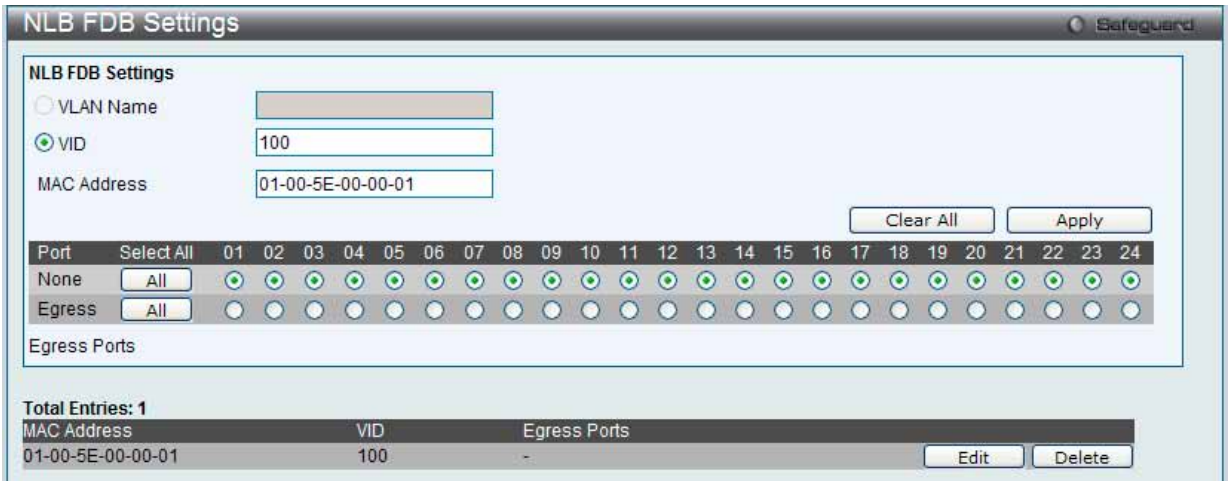


図 7.3-121　NLB FDB Settings 画面 - Edit

2. 画面上の「NLB FDB Settings」セクションの値を編集し、「Apply」ボタンをクリックします。

エントリの削除

削除するエントリの「Delete」ボタンをクリックします。「Clear All」ボタンをクリックして、すべての情報エントリをクリアします。

7.4 L3 Features（レイヤ 3 機能の設定）

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

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

サブメニュー	説明	参照ページ
IPv4 Static/Default Route Settings（IPv4 スタティック / デフォルトルート設定）	IPv4 スタティック / デフォルトルートの設定を行います。	182
IPv4 Route Table（IPv4 ルートテーブル）	IPv4 ルーティングテーブルの外部経路情報を参照します。	183
IPv6 Static/Default Route Settings（IPv6 スタティック / デフォルトルート設定）	IPv6 スタティック / デフォルトルートの設定を行います。	183
IP Forwarding Table（IP フォワーディングテーブル）	直接接続するすべての IP 情報を参照します。	184
VRRP（VRRP 設定）	VRRP リレーの設定を行います。次のメニューがあります。 VRRP Global Settings（VRRP グローバル設定）、VRRP Virtual Router Settings（VRRP 仮想ルータ設定）、VRRP Authentication Settings（VRRP 認証設定）	185

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

本スイッチは IPv4 アドレシングのためにスタティックルーティング機能をサポートしています。IPv4 には最大 512 個のスタティックルートエントリを作成することできます。

IPv4 スタティックルートのために、スタティックルートが一度設定されると、スイッチは設定されたネクストホップルータに ARP リクエストパケットを送信します。ARP の応答をネクストホップからスイッチが取得すると、ルートは有効になりますが、ARP エントリが既に存在している場合には と、ARP レスポンスは送信されません。

また、スイッチはフローティングスタティックルートをサポートしています。これは、同じネットワークにある異なるネクストホップデバイスに代替のスタティックルートを作成できるものです。この 2 個目のネクストホップデバイスのルートは、プライマリスタティックルートがダウンした場合のバックアップ用スタティックルートであると見なされます。プライマリルートをなくした場合、バックアップルートがリンクアップし、アクティブな状態になります。本スイッチのフォワーディングテーブル内へのエントリは IP アドレスのサブネットマスクとゲートウェイの両方を使用して行います。

1. **L3 Features > IPv4 Static/Default 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 7.4-1　IPv4 Static/Default Route Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
IP Address	スタティックルートに割り当てる IPv4 アドレスを入力します。「Default」をチェックすると、デフォルトルートに割り当てられます。
Netmask	対応するサブネットマスクを入力します。
Gateway	対応するゲートウェイ IP アドレスを入力します。
Metric (1-65535)	テーブルに入力した IP インタフェースのメトリック値を示します。1-65535 の範囲の値です。
Backup State	Primary、Backup、または Weight から選択します。 各 IP アドレスは 1 つのプライマリルートを持っており、一方、他のルートはバックアップ状態に割り当てられる必要があります。プライマリルートに障害が発生すると、スイッチはルートが回復するまでルーティングテーブルが学習した順番に従ってバックアップルートを試します。スタティックおよびデフォルトルートが設定されるバックアップ状態を示します。

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。

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

IPv4 Route Table（IPv4 ルートテーブル）

IP ルーティングテーブルはスイッチに関するすべての外部経路情報を保存します。ここではスイッチにおけるすべての外部経路情報を参照します。

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

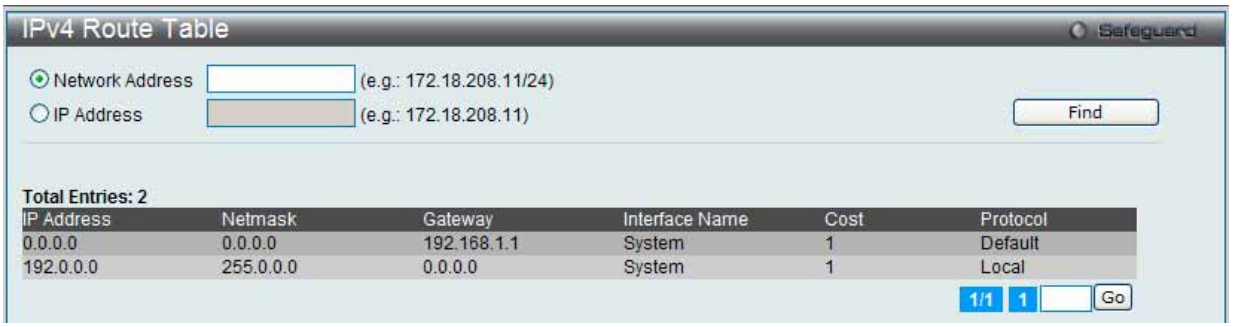


図 7.4-2　IPv4 Route Table 画面

2. 以下の項目を使用して参照します。

項目	説明
Network Address	表示するルートの宛先ネットワークアドレスを指定します。
IP Address	表示するルートの宛先 IP アドレスを指定します。ルートに最も長く一致するプレフィックスが表示されます。

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

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

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

IPv6 アドレスのスタティックエントリは IPv6 形式のアドレスで本スイッチのルーティングテーブルに入力します。

1. **L3 Features > IPv6 Static/Default 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 7.4-3　IPv6 Static/Default Route Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Interface Name	スタティック IPv6 ルートが作成される IP インタフェース名を指定します。
Nexthop Address	IPv6 形式におけるネクストホップゲートウェイアドレスに対応する IPv6 アドレスを指定します。
Metric (1-65535)	IPv6 インタフェースのメトリック値を指定します。スイッチと上記 IPv6 アドレス間のルータの数を表します。範囲は 1-65535 です。
Backup State	各 IP アドレスは 1 つのプライマリルートを持っており、一方、他のルートはバックアップ状態に割り当てられる必要があります。プライマリルートに障害が発生すると、スイッチはルートが回復するまでルーティングテーブルが学習した順番に従ってバックアップルートを試します。IPv6 が設定されるバックアップ状態を示します。「Primary」または「Backup」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。

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。

IP Forwarding Table（IP フォワーディングテーブル）

IP フォワーディングテーブルは直接接続するすべての IP 情報を保存しています。ここでは直接接続するすべての IP 情報を参照します。

1. **L3 Features > IP Forwarding Table** の順にメニューをクリックして以下の画面を表示します。

図 7.4-4　IP Forwarding Table 画面

2. 以下の項目を使用して参照します。

項目	説明
IP Address	ラジオボタンをクリックして、IP アドレスを入力します。
Interface Name	ラジオボタンをチェックして、インタフェース名を入力します。
Port	ラジオボタンをクリックして、ポートを入力します。

エントリの参照

「IP Address」、「Interface Name」または「Port」ラジオボタンをクリックして、情報を入力し、「Find」ボタンをクリックします。入力した情報に基づく特定のエントリを検出します。

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

VRRP（VRRP 設定）

VRRP（Virtual Routing Redundancy Protocol）は、LAN 上の VRRP ルータの 1 つに仮想ルータとしての役割を動的に割り当てる機能です。VRRP ルータのうち、仮想ルータと対向する IP アドレスの制御を行うものをマスタルータと呼び、このルータが本 IP アドレス向けのパケットを送出します。また、エンドホストは LAN 上の仮想ルータの IP アドレスをデフォルトのファーストホップとして使用できます。VRRP 機能を使用して、管理者はすべてのエンドホストにダイナミックルーティングやルート検出プロトコルの設定を行わなくても、デフォルトパスコストを取得することができます。

LAN 上に静的に設定されたデフォルトルートは、障害発生箇所となる傾向があります。VRRP 機能はこの障害を回避するために、選定プロトコルを使用して LAN 上の VRRP ルータの 1 つに仮想ルータとしての役割を割り当てるよう設計されています。仮想ルータがダウンすると、選定プロトコルが優先度の最も高い仮想ルータを選び、LAN 上のマスタルータに任命します。これによりダウンした箇所に関係なく、リンクとコネクションはその状態を保つことができます。

VRRP では、1 台の物理的ルータの代わりに、物理的ルータのグループから構成される仮想ルータを導入します。仮想ルータは 2 台以上の物理ルータから構成され、その中で実際に稼動するのは 1 台のみです。その仮想ルータの中で実際に稼動しているルータが停止した場合、自動的に別のルータに切り替わり稼動を開始します。実際に稼動している物理ルータをマスタルータと呼び、マスタルータ異常時に備えて待機している物理ルータをバックアップルータと呼びます。

スイッチに仮想ルータ用の VRRP 機能を設定するためには、IP インタフェースが存在し、その IP アドレスが VLAN に所属している必要があります。VRRP 用 IP インタフェースはスイッチの VLAN（IP インタフェース）ごとに設定します。VRRP 機能が正しく動作するために、同じ VRRP グループ内の VRRP ルータは、同じ設定内容を持つ必要があります。

VRRP Global Settings（VRRP グローバル設定）

スイッチの VRRP 機能をグローバルに有効にします。

3. **L3 Features > VRRP > VRRP Global Settings** の順にメニューをクリックし、以下の画面を表示します。

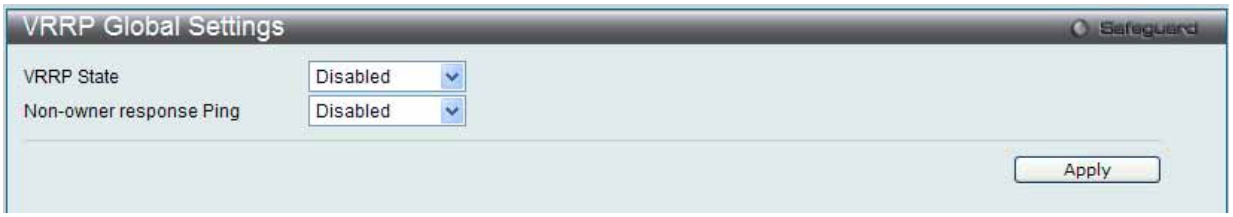


図 7.4-5　VRRP Global Settings 画面

4. 以下の項目を使用して設定を行います。

項目	説明
VRRP State	スイッチの VRRP 機能をグローバルに「Enabled」（有効）または「Disabled」（無効）にします。初期値は「Disabled」です。
Non-owner Response Ping	「Enabled」（有効）にすると、仮想 IP アドレスが他のホストエンドから ping を行い、接続性を確認することができます。初期値は「Disabled」（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。

VRRP Virtual Router Settings（VRRP 仮想ルータ設定）

VRRP 仮想ルータ設定を行います。

1. **L3 Features > VRRP > VRRP Virtual Router Settings** の順にメニューをクリックし、以下の画面でスイッチの仮想ルータの設定内容を参照します。

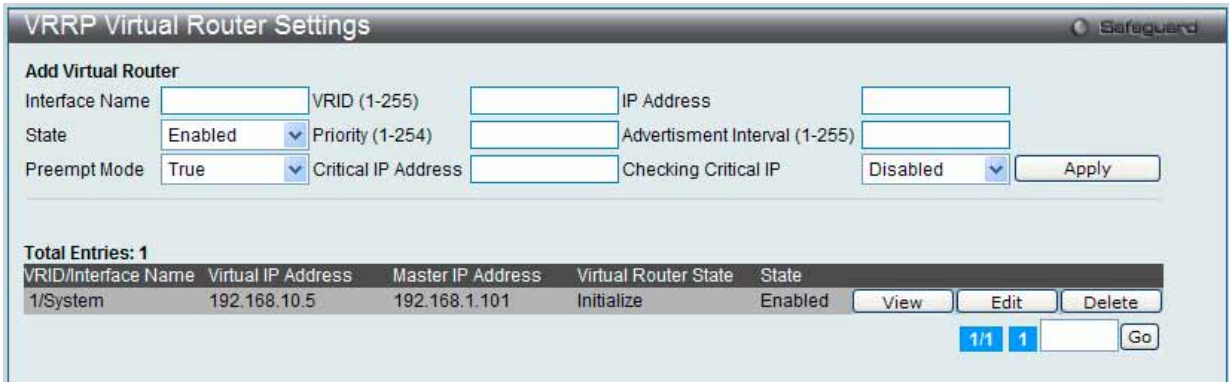


図 7.4-6　VRRP Virtual Router Settings 画面

2. インタフェースの仮想ルータの状態を指定します。

項目	説明
Interface Name	VRRP エントリを作成するのに使用する IP インタフェース名を指定します。
VRID (1-255)	使用する仮想ルータの ID を指定します。このグループに所属する全ルータには同じ VRID 値を割り当てる必要があります。この値はスイッチに設定されている他の VRRP グループと必ず異なる数値にします。
IP Address	仮想ルータの IP アドレスを入力します。この IP アドレスはまたエンドホストにスタティックに割り当てられるデフォルトゲートウェイで、本グループに所属する全ルータに設定される必要があります。
State	インタフェースの仮想ルータの状態を「Enabled」（有効）/「Disabled」（無効）にします。
Priority (1-254)	仮想ルータのマスタ選定プロセスで使用するプライオリティを入力します。VRRP プライオリティの値は、より高いプライオリティの VRRP ルータが低い VRRP ルータを無効にするかどうかを決定します。高いプライオリティほどこのルータがグループのマスタになる可能性を高め、プライオリティが低いほどルータがバックアップルータになる可能性を高めます。同じプライオリティ値を持つ VRRP ルータでは、最も高位の物理 IP アドレスを持つ VRRP ルータがマスタルータになるように選定されます。
Advertisement Interval (1-255)	Advertisement メッセージの送出間隔を入力します。
Preempt Mode	より高いプライオリティを持つバックアップルータがより低いプライオリティを持つマスタルータと置き替わるかどうかを制御することによって VRRP 内のバックアップルータの動作を決定します。 • True - バックアップルータのプライオリティがマスタの優先度よりも高く設定された場合、バックアップルータをマスタルータに設定します。 • False - バックアップルータをマスタルータにすることを無効にします。 本設定は VRRP グループに所属する全ルータで同じにする必要があります。
Critical IP Address	インターネットへの最も直接的な経路、またはこの仮想ルータからの他のクリティカルなネットワーク接続を提供する物理デバイスの IP アドレスを入力します。これはネットワークにある本物のデバイスの IP アドレスです。仮想ルータからこの IP アドレスへの接続に失敗するとが、仮想ルータは自動的に無効になります。新しいマスタは VRRP グループに所属するバックアップルータから選定されます。異なる Critical IP Address が VRRP グループに所属する異なるルータに割り当てられ、インターネットまたは他のクリティカルネットワーク接続に複数の経路を定義します。
Checking Critical IP	クリティカルな IP アドレスのステータス（Active または Inactive）をチェックする状態を指定します。「Enabled」または「Disabled」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。

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

エントリの編集

1. 「Edit」ボタンをクリックすると、以下の画面が表示されます。

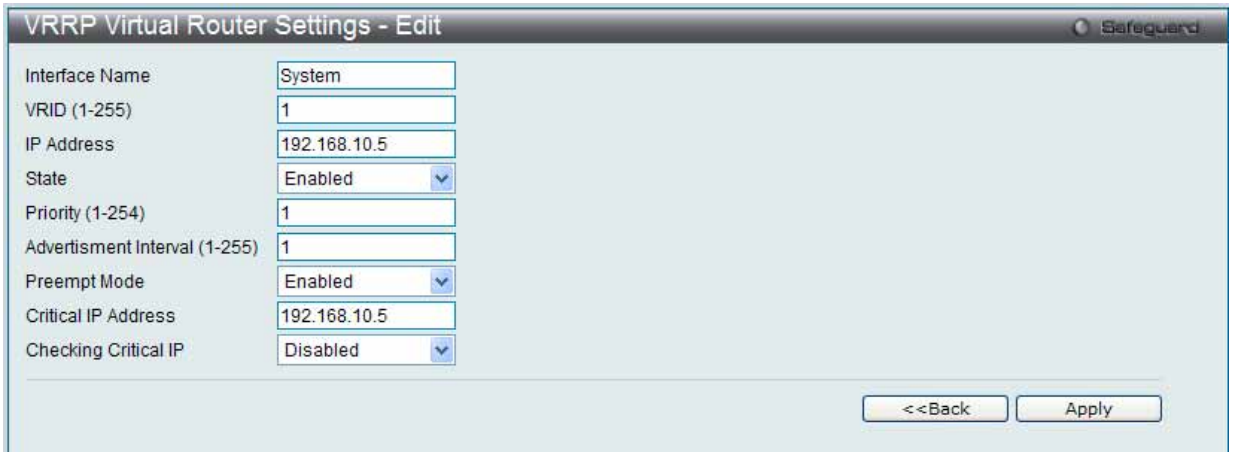


図 7.4-7　VRRP Virtual Router Settings – Edit 画面

2. 以下の項目を使用して設定を行います。

項目	説明
Interface Name	VRRP エントリを作成するのに使用する IP インタフェース名を入力します。
VRID (1-255)	仮想ルータの ID を入力します。このグループに所属する全ルータには同じ VRID 値を割り当てる必要があります。この値はスイッチに設定されている他の VRRP グループと必ず異なる数値にします。
IP Address	仮想ルータの IP アドレスを入力します。この IP アドレスはまたエンドホストに静的に割り当てられるデフォルトゲートウェイで、本グループに所属する全ルータに設定される必要があります。
State	インタフェースにおける仮想ルータ機能の状態を有効または無効にします。
Priority (1-254)	仮想ルータのマスタ選定プロセスで使用するプライオリティを入力します。VRRP プライオリティの値は、より高いプライオリティの VRRP ルータが低い VRRP ルータを無効にするかどうかを決定します。高いプライオリティほどこのルータがグループのマスタになる可能性を高め、プライオリティが低いほどルータがバックアップルータになる可能性を高めます。同じプライオリティ値を持つ VRRP ルータでは、最も高位の物理 IP アドレスを持つ VRRP ルータがマスタルータになるように選定されます。
Advertisement Interval (1-255)	Advertisement メッセージの送出間隔を入力します。
Preempt Mode	より高いプライオリティを持つバックアップルータがより低いプライオリティを持つマスタルータと置き替わるかどうかを制御することによって VRRP 内のバックアップルータの動作を決定します。 • True - バックアップルータのプライオリティがマスタの優先度よりも高く設定された場合、バックアップルータをマスタルータに設定します。 • False - バックアップルータをマスタルータにすることを無効にします。 本設定は VRRP グループに所属する全ルータで同じにする必要があります。
Critical IP Address	インターネットへの最も直接的な経路、またはこの仮想ルータから他のクリティカルなネットワークへの接続を提供する物理デバイスの IP アドレスを入力します。これはネットワークにある本物のデバイスの IP アドレスです。仮想ルータからこの IP アドレスへの接続に失敗するとが、仮想ルータは自動的に無効になります。新しいマスタは同じ VRRP グループに所属するバックアップルータから選定されます。異なる Critical IP Address が VRRP グループにある別のルータに割り当てられ、インターネットまたは他のクリティカルネットワーク接続に複数の経路を定義します。
Checking Critical IP	プルダウンメニューを使用して、Critical IP Address の状態を有効または無効にします。

3. エントリの編集を行い、「Apply」ボタンをクリックします。

エントリの削除

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

「<<Back」をボタンをクリックして前のページに戻ります。

エントリの参照

「View」ボタンをクリックすると、以下の画面が表示されます。

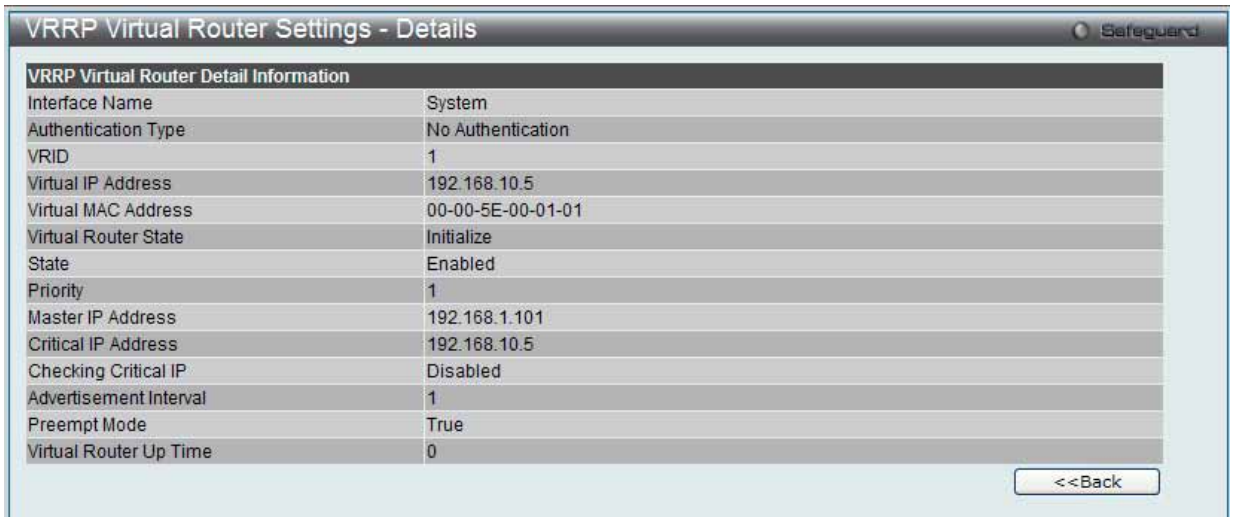


図 7.4-8　VRRP Virtual Router Settings - Details 画面

「<<Back」をボタンをクリックして前のページに戻ります。

VRRP Authentication Settings（VRRP 認証設定）

インタフェースにおける仮想ルータの認証設定を行います。

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

図 7.4-9　VRRP Authentication Settings 画面

エントリの編集

1. 「Edit」ボタンをクリックすると、以下の画面が表示されます。

図 7.4-10　VRRP Authentication Settings – Edit 画面

以下の項目を使用して設定および参照します。

項目	説明
Interface Name	VRRP 認証情報を設定する IP インタフェース。
Authentication Type	プルダウンメニューを使用して、VRRP の認証タイプを選択します。 • None - VRRP プロトコル交換は認証されません。 • Simple - ルータが受信した VRRP メッセージパケットを照合するために「Authentication Data」欄にシンプルパスワードを設定します。2 つのパスワードが正確に一致しない場合、パケットは破棄されます。 • IP - ルータが受信した VRRP メッセージを照合する認証のために IP を設定します。2 つのパスワードが一致しない場合、パケットは破棄されます。
Authentication Data	本欄は、「Authentication Type」欄で「Simple」または「IP」が指定されている場合に有効です。「Simple」と「IP」認証アルゴリズムで使用する認証データを指定します。同じ IP インタフェースに所属する全ルータが同じ設定を行う必要があります。 • Simple - ルータが受信した VRRP パケットを識別するために 8 文字以内の半角英数字を入力します。 • IP - ルータが受信した VRRP パケットを照合するために 16 文字以内の半角英数字を入力します。

2. エントリの編集を行い、「Apply」ボタンをクリックします。

7.5 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
802.1p Settings（802.1p 設定）	ポート単位にプライオリティを割り当てます。以下のメニューがあります。 802.1p Default Priority Settings（ポートへのパケットプライオリティの割り当て）、802.1p User Priority Settings（802.1p ユーザプライオリティ）	191
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。以下のメニューがあります。 Bandwidth Control Settings（帯域幅の設定）、Queue Bandwidth Control Settings（キュー帯域幅制御の設定）	192
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。	194
DSCP（DSCP 設定）	ポートの DSCP トラスト状態の設定および DSCP マッピング設定を行います。以下のメニューがあります。 DSCP Trust Settings（DSCP トラスト設定）、DSCP Map Settings（DSCP マップ設定）	196
HOL Blocking Prevention （HOL ブロッキング防止）	HOL ブロッキング防止機能を「Enabled」（有効）または「Disabled」（無効）にします。	197
Scheduling Settings （スケジュールの設定）	QoS スケジューリングを設定します。以下のメニューがあります。 Scheduling Profile Settings（スケジュールプロファイル設定）、Scheduling Group Settings（スケジューリンググループ設定）	198

本スイッチシリーズは、802.1p プライオリティキューイング QoS（Quality of Service）をサポートしています。以下の項では QoS の機能と、802.1 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。

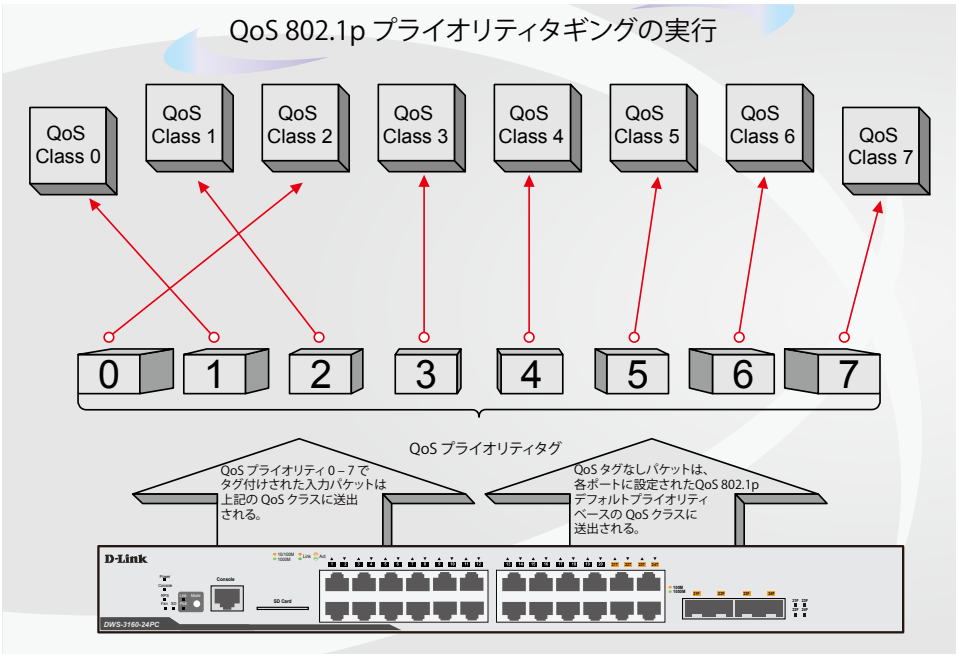


図 7.5-1　スイッチ上での QoS マッピングの例

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 -7 は、スイッチ上における 7 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。プライオリティキューには、最高レベルの 7 番（クラス 7）から最低レベルの 0 番（クラス 0）まであります。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 Q2 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 Q1 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 Q3 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 Q4 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 Q5 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 Q6 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 Q7 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 H までの 8 つある CoS キューに、8 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, E1, F1, G1, H1, A2, B2, C2, D2, E2, F2, G2, A3, B3, C3, D3, E3, F3, A4, B4, C4, D4, E4, A5, B5, C5, D5, A6, B6, C6, A7, B7, A8, A1, B1, C1, D1, E1, F1, G1, H1。

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。また、ある CoS の重み付けとして 0 を設定すると、その CoS から送信するパケットがなくなるまでパケットを処理します。0 以外の値を持つ他の CoS キューでは、重み付けラウンドロビンの規則により、重みに従って送信を行います。

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

注意 本スイッチは内部的にはポートに対して 8 つのサービスクラスを持っています。そのうち 1 つは最初からスイッチが使用するように予約されていて変更できません。以下のセクションでは、サービスクラスに関する説明はすべて管理者が使用および変更できる 8 つのサービスクラスについて行っています。

802.1p Settings（802.1p 設定）

802.1p Default Priority Settings（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。

本画面では、スイッチのそれぞれのポートにデフォルトの 802.1p プライオリティを割り当てて、受信したタグなしパケットに 802.1p プライオリティタグを挿入します。プライオリティ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。

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

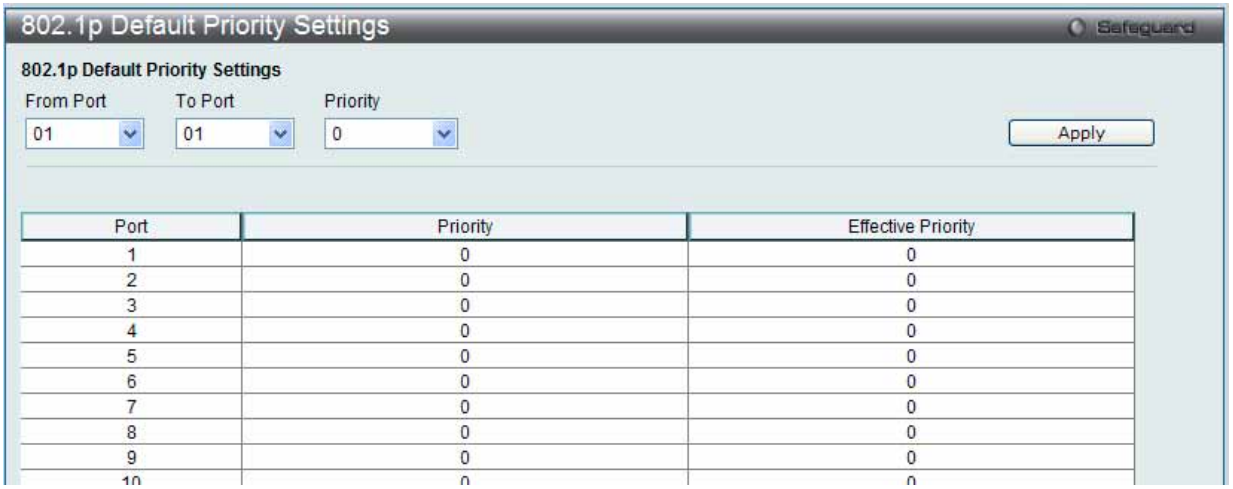


図 7.5-2　802.1p Default Priority Settings 画面

2. 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」、「To」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。

以下の項目を使用して設定および参照します。

項目	説明
From Port / To Port	使用する開始 / 終了ポートを選択します。
Priority	プルダウンメニューを使用して、0-7 の値を選択します。

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 Settings（802.1p ユーザプライオリティ）

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。

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

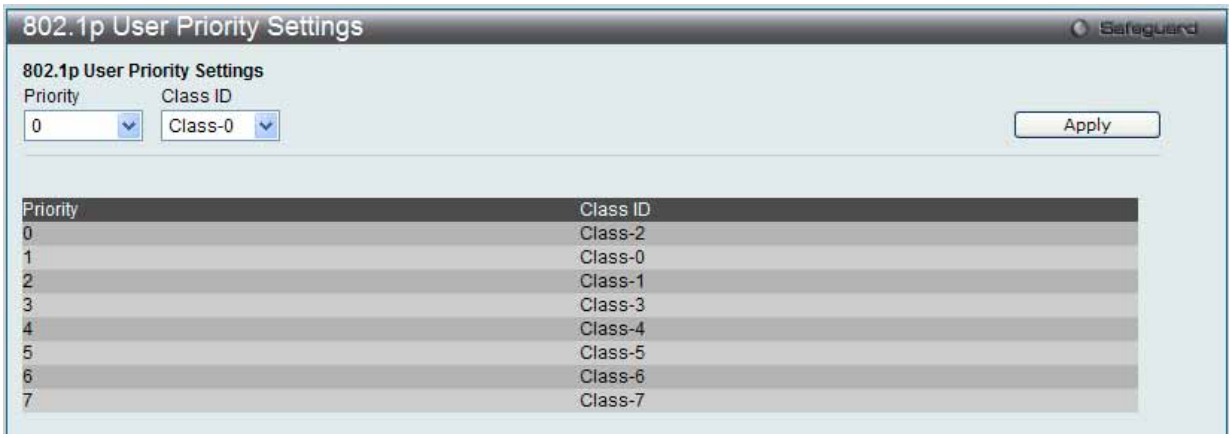


図 7.5-3　802.1P User Priority Settings 画面

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。ユーザプライオリティのマッピングは最後のページで設定したデフォルトプライオリティに対するだけではなく、802.1p タグを持つすべての入力パケットに対しても行われます。

2. 以下の項目を使用して設定および参照します。

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。

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。

Bandwidth Control Settings（帯域幅の設定）

「Effective RX Rate」は設定した速度に一致しない場合にスイッチポートの実際の帯域幅を表示します。これは、通常 RADIUS サーバをなどの高優先度を持つリソースが割り当てた速度を表示します。

1. **QoS > Bandwidth Control > 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。

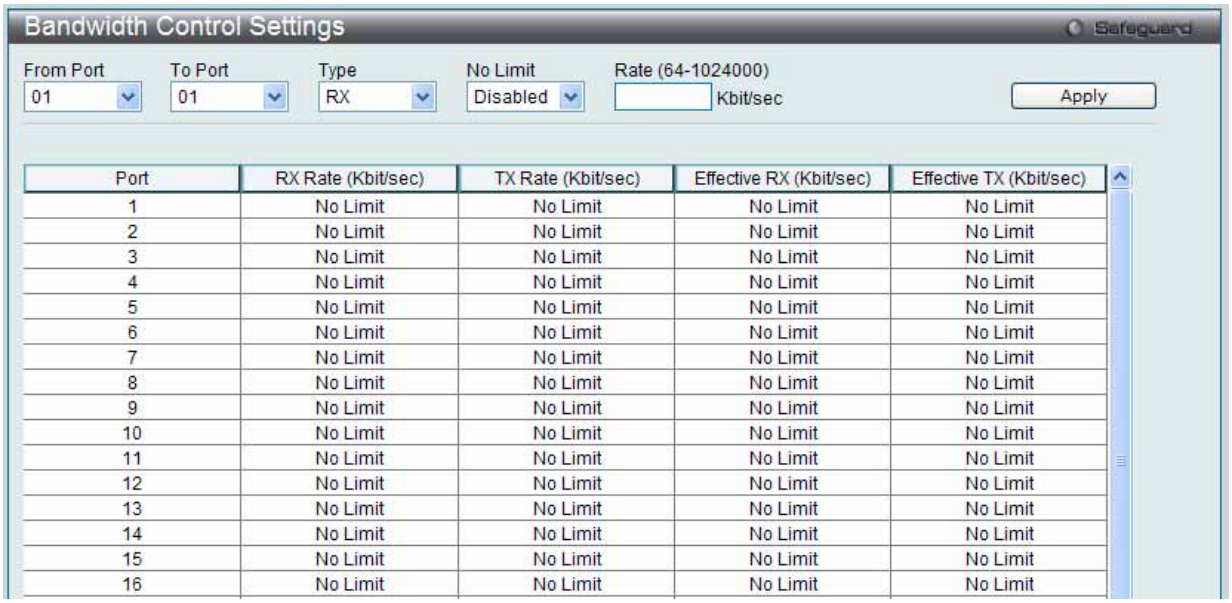


図 7.5-4　Bandwidth Control Settings 画面

2. 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） 注意 設定値がポート速度より大きいと、帯域幅制限の意味がなくなります。
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 の間で速度を指定します。
Effective RX	RADIUS サーバが RX の帯域幅を割り当てると、それは有効な RX 帯域幅となります。RADIUS サーバを使用した認証は、ポートごとかユーザごとに行われます。ユーザごとの認証のために、指定ポートに複数ユーザが割り当てられていると、割り当てられる RX 帯域幅が複数あります。最終的な RX 帯域幅は、これら複数の RX 帯域幅の中で最も大きいものとなります。
Effective TX	RADIUS サーバが TX の帯域幅を割り当てると、それは有効な TX 帯域幅となります。RADIUS サーバを使用した認証は、ポートごとかユーザごとに行われます。ユーザごとの認証のために、指定ポートに複数ユーザが割り当てられていると、割り当てられる TX 帯域幅が複数あります。最終的な TX 帯域幅は、これら複数の TX 帯域幅の中で最も大きいものとなります。

「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。

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

キューの帯域幅を設定します。

1. **QoS > Bandwidth Control > 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。

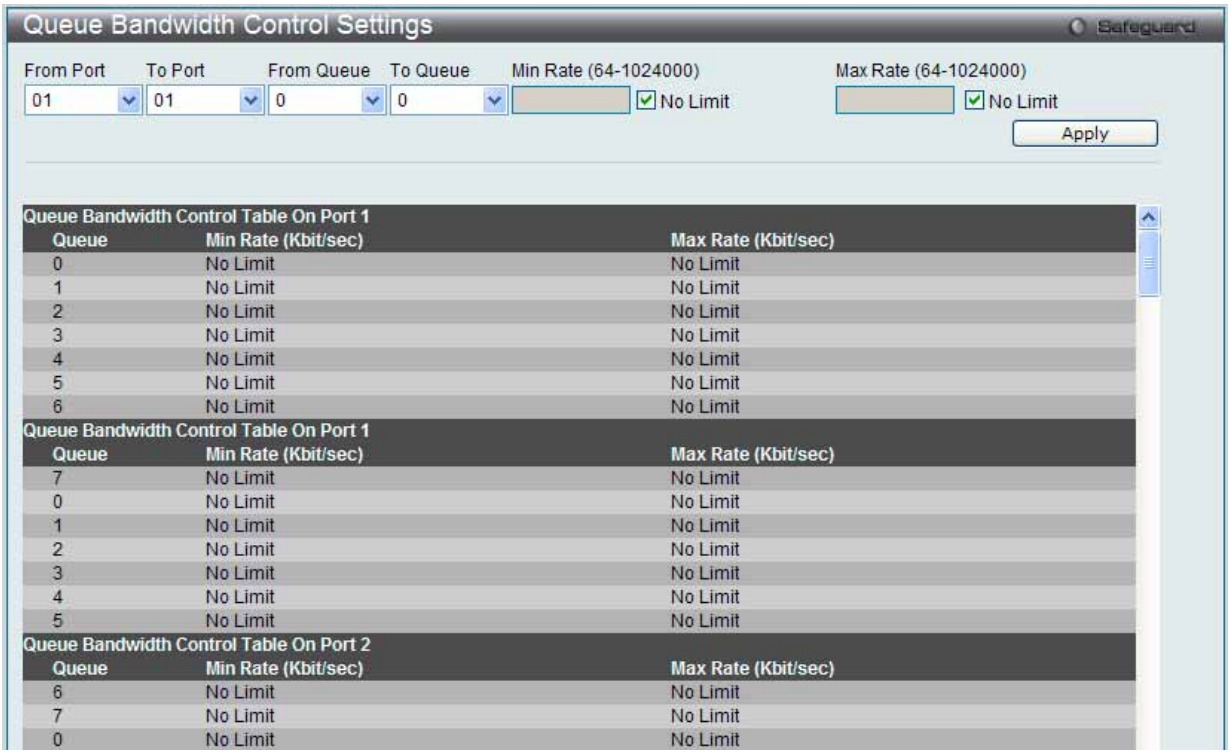


図 7.5-5　Queue Bandwidth Control Settings 画面

2. 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	この設定に使用するポート範囲を選択します。
From Queue / To Queue	この設定に使用するキュー範囲を選択します。
Min Rate (64-10240000)	ポートが受信できるパケット制限 (Kbps) を指定します。「No Limit」をチェックすると指定キューが受信するパケットにレート制限がなくなります。
Max Rate (64-10240000)	キューの最大レートを入力します。「No Limit」オプションを選択すると、レート制限はなくなります。

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。

注意 キュー帯域幅制御の最小グラニュラリティは 64Kbps です。システムは自動的に 64 倍の数に調整します。

Traffic Control Settings（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のように誤動作しているデバイスによって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レベルを基に非常に多くのパケットがネットワークであふれているどうかを判断します。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。

トラフィックコントロールに設定したポートで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 Forever」(永久シャットダウン) 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 Forever」モードに入ると、本ポートを回復する方法は、**System Configuration > Port Configuration > Port Settings** 画面で手動により有効状態に戻すか、または「Traffic Auto Recover Time」欄に設定した時間経過後自動的に回復します。無効なポートを選択して、「Status」を「Enabled」ステータスに戻します。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」フィールドで「Shutdown」オプションを選択してください。この画面を使用して、ストームコントロールの有効 / 無効や、マルチキャストおよびブロードキャストのしきい値の調整を行います。

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

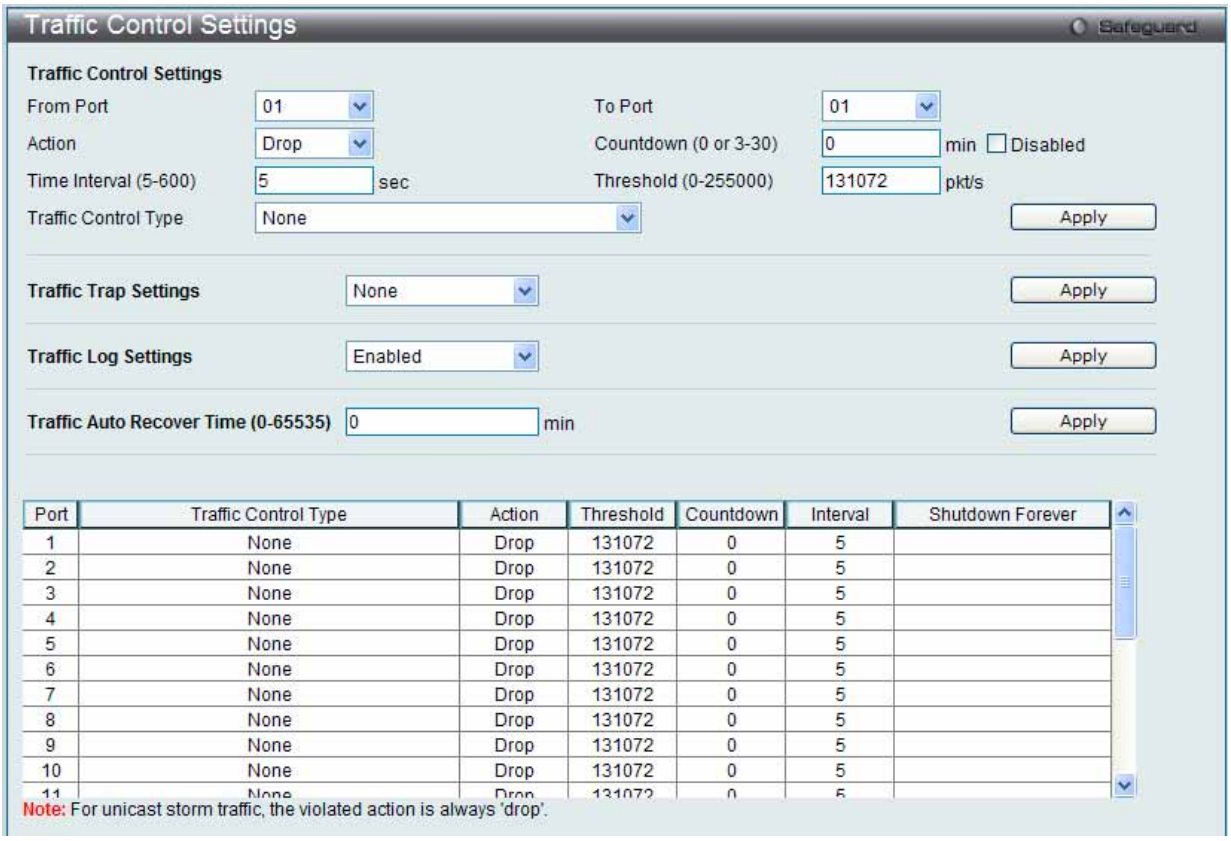


図 7.5-6　Traffic Control Settings 画面

2. 以下の項目を使用して設定および参照します。

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 – スイッチのハードウェアによるトラフィックコントロールを行います。選択すると、スイッチのハードウェアが指定したしきい値に基づくパケットストームの検知を行い、パケットストームが発生すると、状態が改善するまでパケットの廃棄を行います。 • Shutdown – スイッチのソフトウェアによるトラフィックコントロールにより、トラフィックストームの発生を検知します。ストームが検出されると、スイッチはスパニングツリーの保持に必要である 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、ポートをシャットダウンします。カウント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 Forever」(永久シャットダウン) モードに遷移し、5 分後自動的にポートが回復するまで操作できません。本ポートを通常の状態に戻すには、**System Configuration > Port Configuration> Port Settings** 画面で、無効になっているポートを手動で有効状態に戻します。本オプションを選択する際は、スイッチのチップからパケットカウントを受け取ってパケットストームの発生を検知するために必要な「Time Interval」の設定も必要となります。
Countdown (0 or 3-30)	本値はスイッチがトラフィックストームが発生中のポートをシャットダウンするまでに待機する時間（分）を表します。本値は、「Action」で「Shutdown」を指定し、ハードウェアによるトラフィックコントロールを行わない場合に有効です。0、3-30（分）が指定できます。「Disabled」をチェックすると、本設定は無効になります。
Time Interval (5-600)	スイッチのチップからトラフィックコントロール機能に送信する、マルチキャストおよびブロードキャストパケットカウントの送信間隔を指定します。このパケットカウントにより、いつ入力パケットがしきい値を超過したかの検出が行われます。値の範囲は 5-600 で、初期値は 5（秒）です。
Threshold (0-255000)	トラフィックコントロール機能を起動させるトリガーとなる、1 秒あたりの最大パケット数。設定可能なしきい値の範囲は 0-255000 です。初期値は 131072 パケット / 秒です。
Traffic 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 Settings	トラフィックコントロール機能によるトラフィックストームの扱いを指定します。 • None - トラフィックコントロールメカニズムの動作に関わらず、ストームトラップメッセージを送信しません。 • Storm Occurred - ストームトラップ発生時にストームトラップ警告メッセージを送信します。 • Storm Cleared - スイッチがストームトラップを消失させた時ストームトラップメッセージを送信します。 • Both - ストームトラップ発生時と消失時にストームトラップメッセージを送信します。 本機能は、ハードウェアモード中 (「Action」で「Drop」が選択された時) は実行できません。
Traffic Log Settings	プルダウンメニューを使用して、本機能を「Enabled」（有効）/「Disabled」（無効）にします。ログ状態が有効な場合、ストームが発生した場合やストームがクリアされた場合にトラフィックコントロール状態がログに出力されます。ログ状態が無効な場合、トラフィックコントロールイベントはログに出力されません。
Traffic Auto Recover Time (0-65535)	ポートがシャットダウンからの自動回復を許可する時間を入力します。初期値は 0 で、自動回復モードが無効で、永久にシャットダウンするということを意味します。ポートをフォワーディング状態に戻すためには、**System Configuration > Port Configuration > Port Settings** 画面で手動の設定が必要です。

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 Forever」モードのポートは、スイッチの CPU に BPDU 送信を行いますが、「Spanning Tree」画面では「Discarding」状態として表示されます。

注意 「Shutdown Forever」モードのポートは、ユーザがポートの復旧を行うまでの間はリンクダウン状態として表示されます。

注意 GE ポートの最小のストームコントロールのしきい値のグラニュラリティは 1pps です。

DSCP（DSCP 設定）

DSCP Trust Settings（DSCP トラスト設定）

ポートの DSCP トラスト状態を設定します。ポートが DSCP トラストモードにある場合、スイッチは、デフォルトポートプライオリティの代わりに DSCP マップ設定を使用して、タグなしパケットにプライオリティタグを挿入します。

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

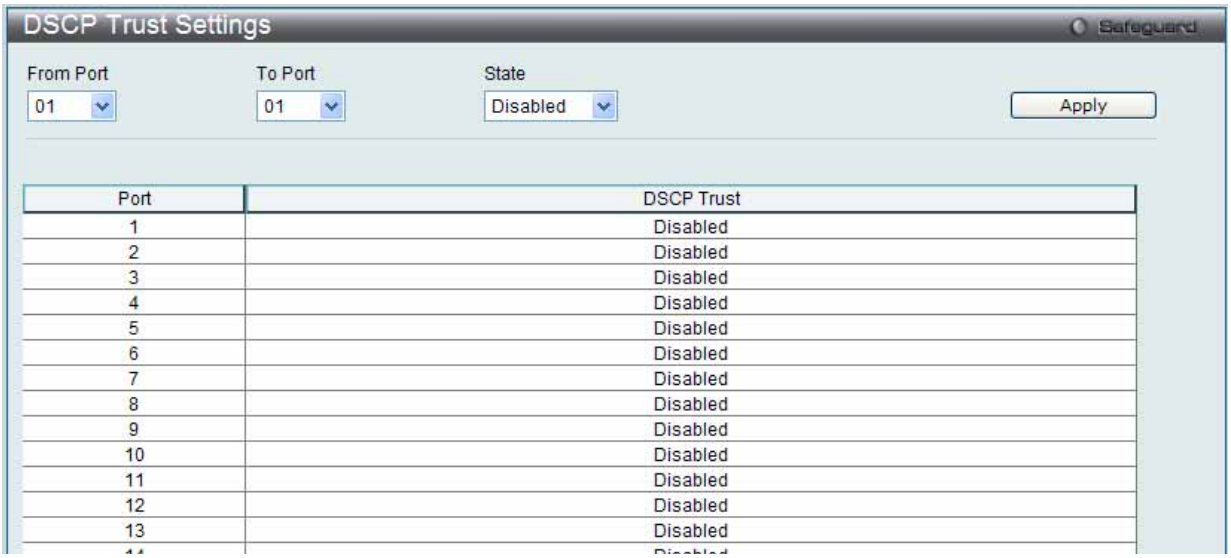


図 7.5-7　DSCP Trust Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
From Port / To Port	設定するポート範囲を選択します。
State	トラスト DSCP を「Enabled」（有効）または「Disabled」（無効）にします。初期値ではトラスト DSCP 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。

DSCP Map Settings（DSCP マップ設定）

キューに対する DSCP のマッピングは、ポートが DSCP トラスト状態にある場合、（次に、スケジューリングキューを決定するのに使用される）パケットのプライオリティを決定するために使用されます。パケットがポートへのイングレスである場合に、DSCP-to-DSCP マッピングはパケットの DSCP のスワップに使用されます。残りのパケットの処理は新しい DSCP に基づきます。初期値では、DSCP は同じ DSCP にマップされます。

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

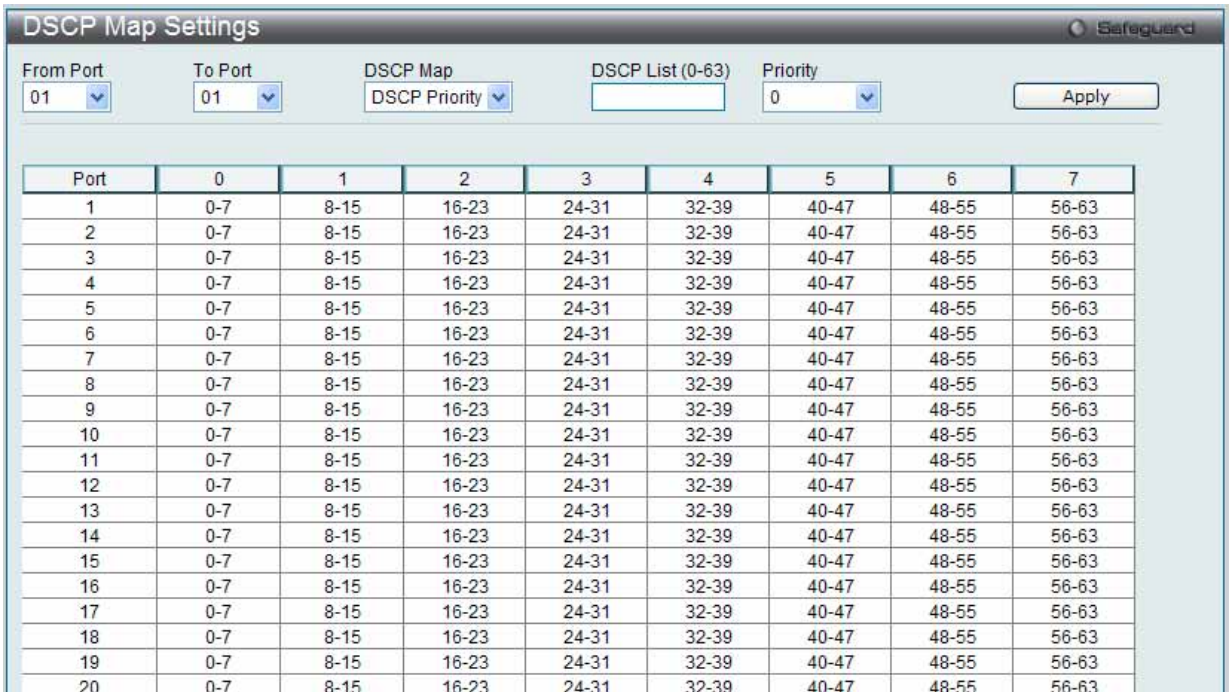


図 7.5-8　DSCP Map Settings - DSCP Priority 画面

QoS > DSCP > DSCP Map Settings の順にクリックし、「DSCP Map」メニューから「DSCP DSCP」を選択して以下の画面を表示します。

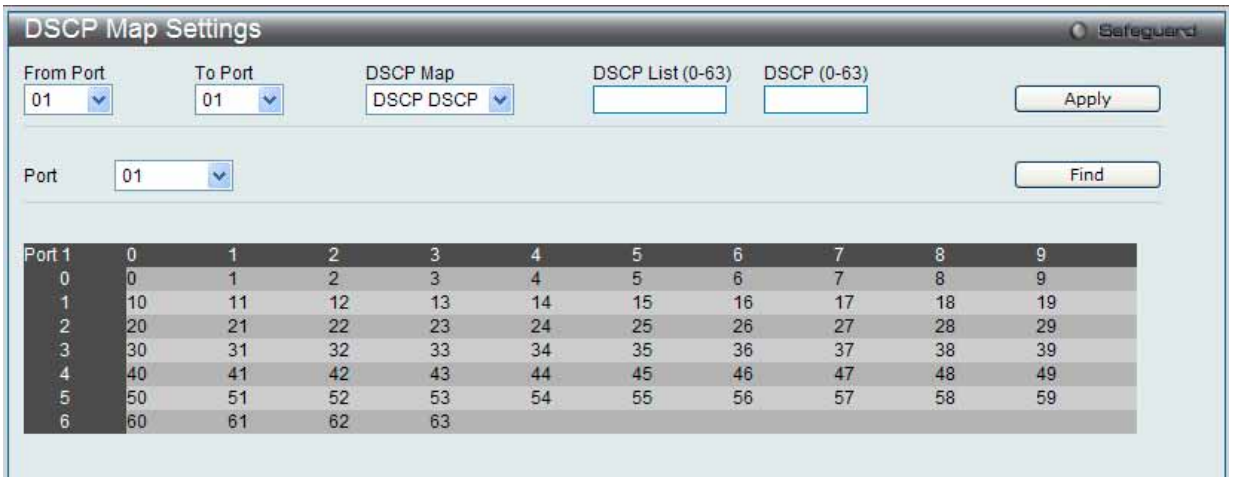


図 7.5-9　DSCP Map Settings - DSCP DSCP 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
From Port / To Port	プルダウンメニューを設定するポート範囲を指定します。
DSCP Map	プルダウンメニューを使用して以下のオプションから 1 つを選択します。 • DSCP Priority - 指定プライオリティにマップする DSCP 値のリストを指定します。 • DSCP DSCP - 指定した DSCP にマップする DSCP 値のリストを指定します。
DSCP List (0-63)	DSCP リストを入力します。
Priority	プライオリティ値を選択します。「DSCP Map」から「DSCP Priority」を選択すると、表示されます。
DSCP (0-63)	DSCP 値を入力します。「DSCP Map」プルダウンメニューで「DSCP DSCP」を選択すると表示されます。
Port	プルダウンメニューを使用してポートを指定します

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。

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

HOL Blocking Prevention（HOL ブロッキング防止）

ブロードキャストもしくはマルチキャストパケットの送信先ポートの一つが輻輳状態になった場合に HOL（Head of Line）ブロッキングが発生します。本スイッチは輻輳状態でない場合に他の送信先ポートがパケットを転送しない場合にでもバッファにこのパケットを保持します。HOL ブロッキング防止は、遅延を抑えより良いパフォーマンスを保つため、輻輳ポートを無視し、直接パケットを転送します。

この画面では HOL ブロッキング防止機能を有効化もしくは無効化します。

1. **QoS > HOL Blocking Prevention** の順にクリックし、以下の画面を表示します。

図 7.5-10　HOL Blocking Prevention 画面

2. HOL ブロッキング防止のグローバル設定を「Enabled」（有効）または「Disabled」（無効）にします。

以下の項目を使用して設定および参照します。

項目	説明
HOL Blocking Prevention State	HOL ブロッキング防止のグローバル設定を「Enabled」（有効）または「Disabled」（無効）にします。

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

Scheduling Settings（スケジュール設定）

QoS Scheduling（QoS スケジュール作成）

スイッチで利用可能な 8 個のハードウェアキューの 1 つに入力パケットの 802.1p ユーザプライオリティに基づいてポートごとに入力パケットを照合する方法を設定します。

1. **QoS > Scheduling Settings > QoS Scheduling** の順にメニューをクリックし、以下の画面を表示します。

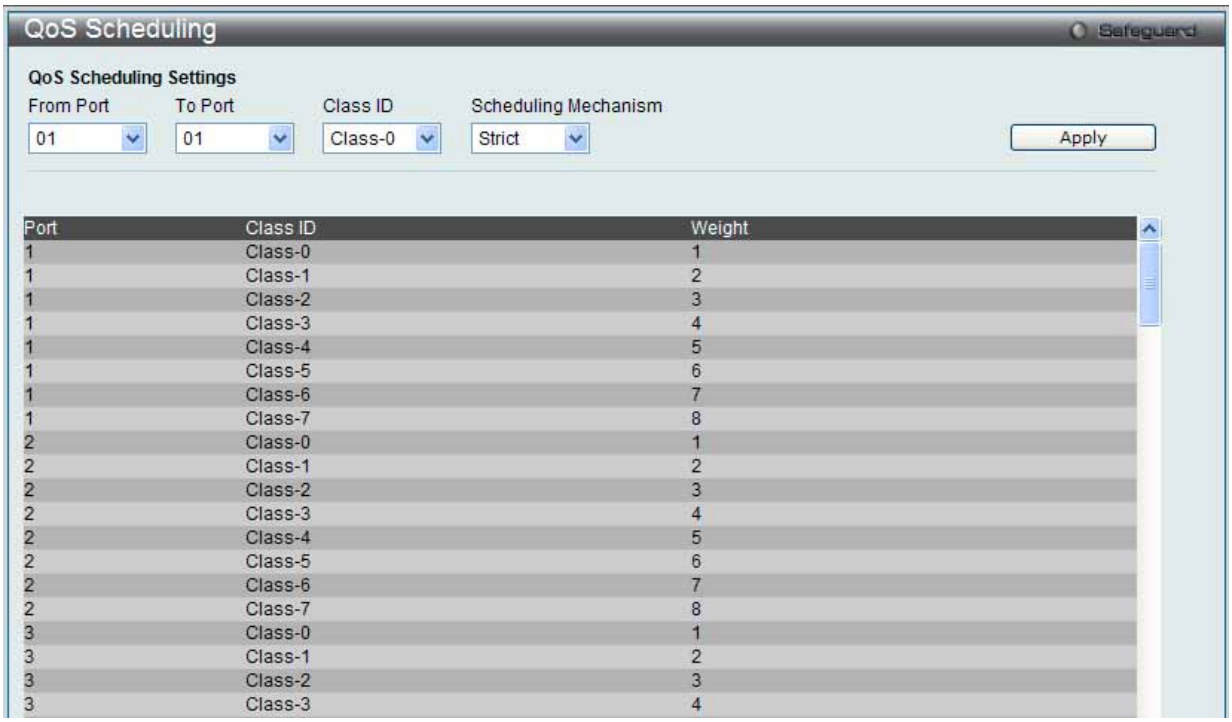


図 7.5-11　QoS Scheduling 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
From Port / To Port	設定対象のポート（範囲）を指定します。
Class ID	QoS パラメータに設定するクラス ID を 0 から 7 の範囲で指定します。
Scheduling Mechanism	• Strict - 上位の CoS キューからトラフィックを処理します。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 - 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。

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 Mechanism（QoS スケジュールメカニズム設定）

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。

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

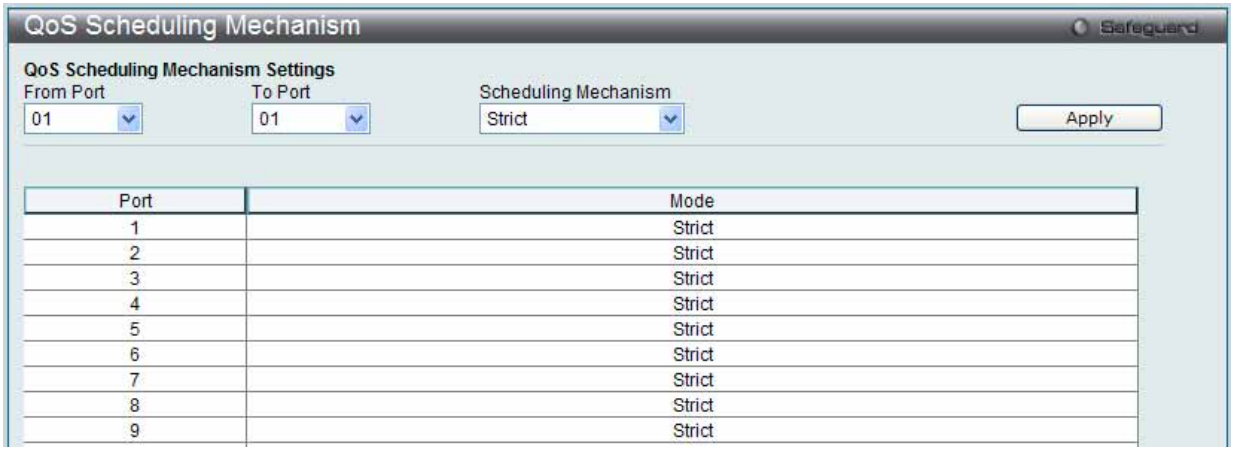


図 7.5-12　Scheduling Profile Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
From Port / To Port	設定対象のポート (範囲) を指定します。
Scheduling Mechanism	2 つのスケジューリングメカニズムの 1 つを選択します。 • Strict - 上位の CoS キューからトラフィックを処理します。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 Round Robin - プライオリティ CoS 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。

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 キューに割り当てる 0 から 7 の番号は IEEE 802.1p プライオリティタグの番号を表しています。ポート番号の指定ではない点にご注意ください。

7.6 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。	200
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。	202
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。	219
ACL Finder（ACL 検索）	ACL エントリを検索します。	235
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。	236
Egress Access Profile List（Egress アクセスプロファイルリスト）	フローごとのパケット処理を実行します。	240
Egress ACL Flow Meter（Egress ACL フローメータリング）	Egress アクセスプロファイルおよびルールに基づいてパケットフローベースのメータリングを設定します。	253

ACL Configuration Wizard（ACL 設定ウィザード）

ACL 設定ウィザードは、必要なアドレスやサービスタイプおよび操作を簡単に入力することで自動的にアクセスプロファイルと ACL ルールを作成します。管理者の多くの時間を節約します。

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。

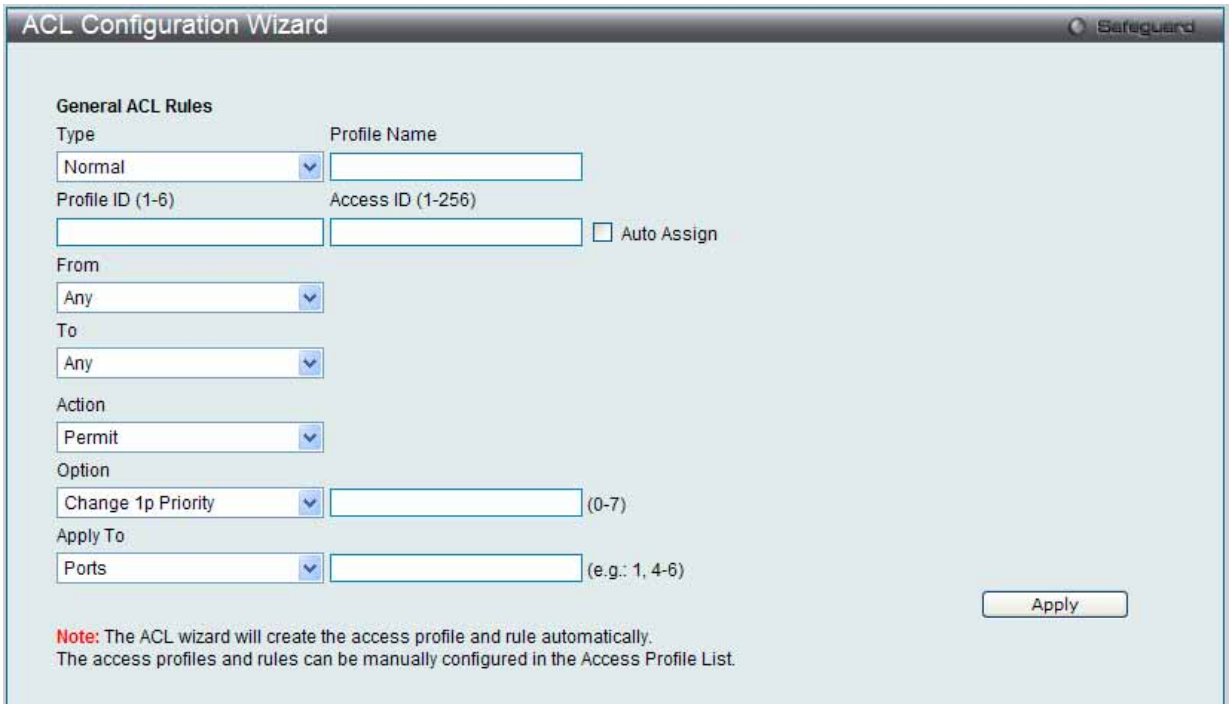


図 7.6-1　ACL Configuration Wizard 画面

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 (1-6) と Access ID (1-256) 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「Change 1p Priority」、「Replace DSCP」または「Replace ToS Precedence」から選択し、隣接している欄に「Change 1p Priority」または「Replace ToS Precedence」の場合は 0-7 の値を、「Replace DSCP」の場合は 0-63 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および参照します。

項目	説明
Type	プルダウンメニューを使用して以下の ACL ルールタイプを選択します。 • Normal - ノーマル ACL ルールを作成します。 • CPU - CPU ACL ルールを作成します。 • Egress - Egress ACL ルールを作成します。
Profile Name	「Normal」タイプルールを選択後、新しいルールに対するプロファイル名を入力します。
Profile ID (1-6)	新しいルールに対するプロファイル ID を入力します。
Access ID (1-256)	新しいルールに対するアクセス ID を入力します。「Auto Assign」オプションを選択すると、このルールに対して自動的に未使用のアクセス ID を割り当てます。
From / To	以下の 4 つの異なるカテゴリに適用するためにこのルールを作成します。 • Any - あらゆる開始カテゴリをこのルールに含めます。 • MAC Address - このルールに MAC アドレス範囲を入力します。 • IPv4 Address - このルールに IPv4 アドレス範囲を入力します。 • IPv6 - このルールに IPv6 アドレス範囲を入力します。
Service Type	「From / To」欄でサブジェクトを選択した後、以下のサービスの 1 つを選択することができます。 • 「IPv4 Address」を選択した場合 - Any - このルールをすべてのサービスタイプに適用します。 - ICMP All - このルールにすべての ICMP トラフィックを適用します。 - IGMP - このルールに ICMP トラフィックを適用します。 - TCP All - このルールにすべての TCP トラフィックを適用します。 - TCP Source Port - このルールに TCP トラフィックを適用します。 - TCP Destination Port - このルールに送信先ポートからの TCP トラフィックだけを適用します。 - UDP All - このルールにすべての UDP トラフィックを適用します。 - UDP Source Port - このルールに送信元ポートからのすべての UDP トラフィックを適用します。 - UDP Destination Port - このルールに送信先ポートからのすべての UDP トラフィックを適用します。 - VLAN Mask (Name) - このルールに VLAN 名を適用します。 • 「IPv6」を選択した場合 - Any - このルールをすべてのサービスタイプに適用します。 - Flow Label - このルールにフローラベルを適用します。 - Class - このルールに IPv6 クラスを適用します。 - TCP All - このルールにすべての TCP トラフィックを適用します。 - TCP Source Port - このルールに TCP トラフィックを適用します。 - TCP Destination Port - このルールに送信先ポートからの TCP トラフィックだけを適用します。 - UDP All - このルールにすべての UDP トラフィックを適用します。 - UDP Source Port - このルールに送信元ポートからのすべての UDP トラフィックを適用します。 - UDP Destination Port - このルールに送信先ポートからのすべての UDP トラフィックを適用します。 - ICMP All - このルールにすべての ICMP トラフィックを適用します。 • 「MAC Address」を選択した場合 - Any - このルールをすべてのサービスタイプに適用します。 - 802.1p - このルールに 802.1p プライオリティ値を適用します。 - VLAN Mask (Name) - このルールに VLAN 名を適用します。 - Ethernet Type - このルールにイーサネットタイプを適用します。
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、以下のフィールド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ミラーポートセクション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	「Permit」アクション選択後、以下のオプションの 1 つを選択します。 • Change 1p Priority - 802.1p プライオリティ値を入力します。 • Replace DSCP - DSCP 値を入力します。 • Replace ToS Precedence - ToS 優先度値を入力します。
Apply To	このルールに適用するオブジェクトの選択または入力を行います。 • Ports - ポート番号またはポート範囲を入力します。 • VLAN Name - VLAN 名を入力します。 • VLAN ID - VID 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。

注意 スイッチはユーザが 入力するすべての項目をカバーするために最小限のマスクを使用しますが、余分なのビットまで同時にマスクする可能性があります。ACL プロファイルとルールを最適化するためには、手動設定を行ってください。

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。

スイッチに現在定義済みのアクセスプロファイルを表示できます。

1. **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。

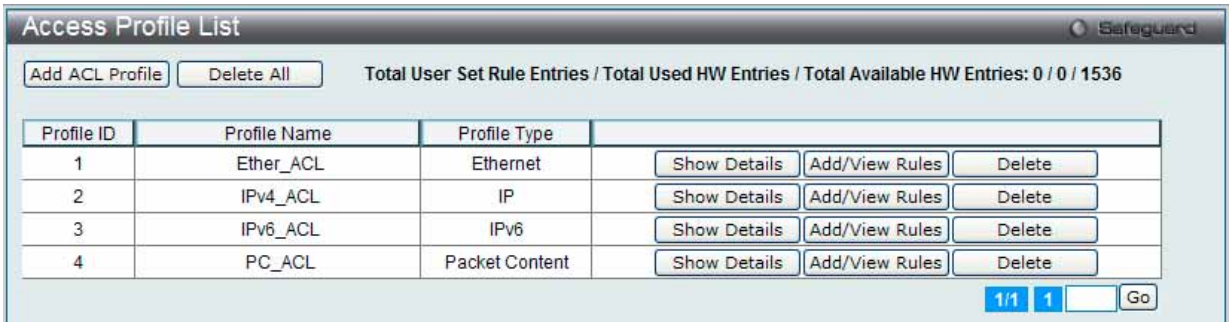


図 7.6-2　Access Profile List 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Add ACL Profile	アクセスプロファイルリストにエントリを追加します。
Delete All	テーブルからすべてのアクセスプロファイルを削除します。
Show Details	指定プロファイル ID エントリに関する情報を表示します。
Add/View Rules	指定プロファイル ID の ACL ルールの参照または追加を行います。
Delete	指定エントリを削除します。
Go	複数ページが存在する場合は、ページ番号を入力後、クリックして、特定のページへ移動します。

「Add Access Profile」画面には 4 種類あります。:
イーサネット (MAC アドレスベース) プロファイル設定用、IPv6 アドレスベースプロファイル設定用、IPv4 アドレスベースプロファイル設定用およびパケットコンテンツマスクプロファイル設定用です。

アクセスプロファイルリストの作成（Ethernet）

イーサネット用の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。

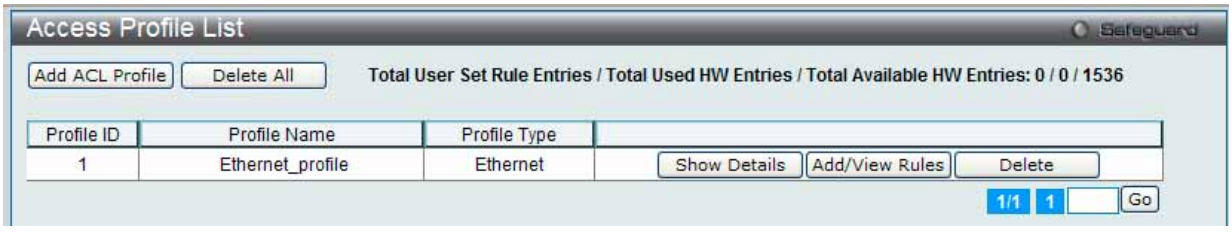


図 7.6-3　Access Profile List 画面

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

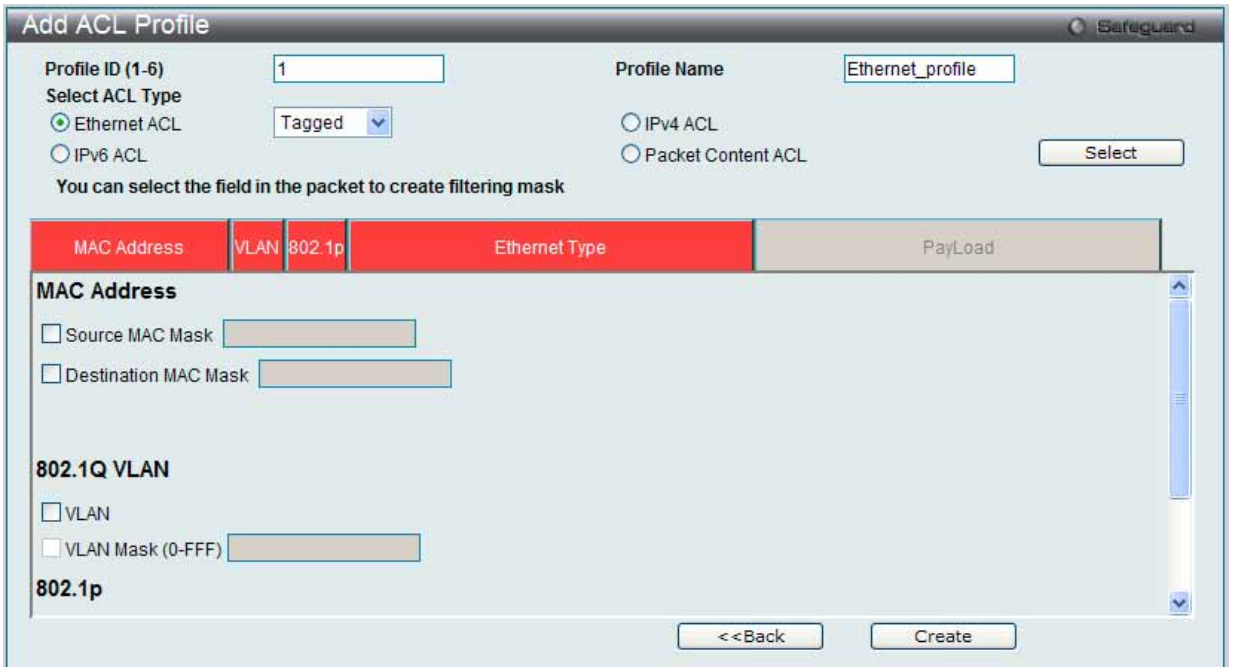


図 7.6-4　Add ACL Profile - Ethernet ACL 画面

「Profile ID」でプロファイル番号を 1-1024 から選択し、「Select ACL Type」で「Ethernet ACL」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
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 6 が指定できます。
Profile Name	作成したプロファイルにプロファイル名を入力します。
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。例 : FF-FF-FF-FF-FF-FF • 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。例 : FF-FF-FF-FF-FF-FF
802.1Q VLAN	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	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	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。

「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

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。

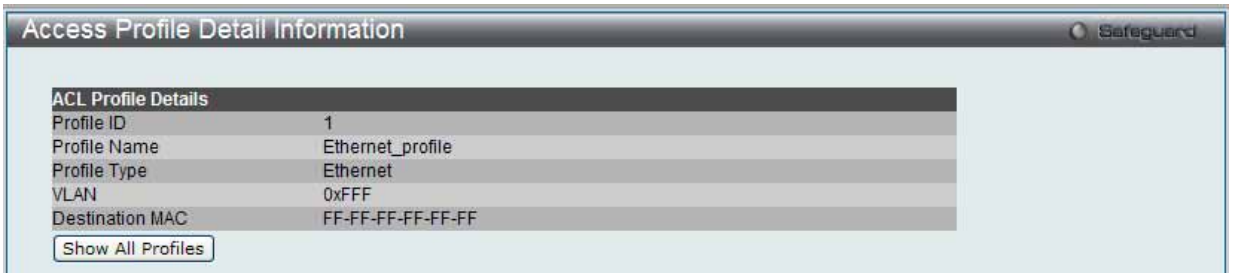


図 7.6-5　Access Profile Detail Information - Ethernet 画面

「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 7.6-6　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 7.6-7　Access Rule List - Ethernet 画面

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

「<<Back」をボタンをクリックし、前のページに戻ります。

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

1. 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。

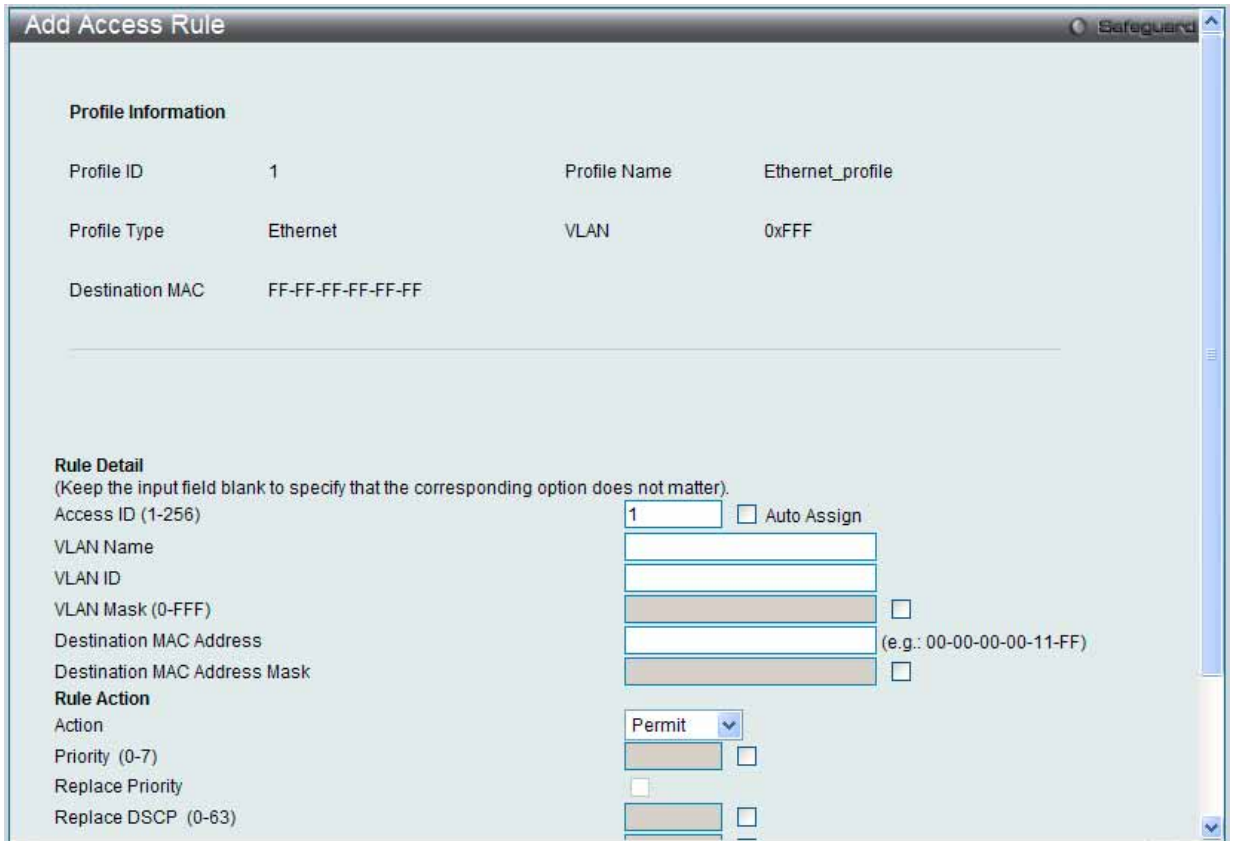


図 7.6-8　Add Access Rule - Ethernet 画面

2. 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 (1-256)	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 256 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	VLAN ID 番号を指定します。
VLAN Mask (0-FFF)	VLAN マスクを指定します。
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 Address 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 Address 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。）
Rule Action	
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、以下のフィールド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。
Priority (0-7)	スイッチにより設定された 802.1p デフォルトプライオリティを上書きしたい場合に指定します。このプライオリティにより転送されたパケットがどの CoS キューを使用するかが決まります。この欄を指定するとパケットはこのプライオリティを割り当てられ、対応した CoS キューに転送されます。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「7.5　QoS（QoS 機能の設定）」（189 ページ）を参照してください。
Replace Priority	条件に合ったパケットの DSCP 値は指定した値に入れ替わります。
Replace DSCP (0-63)	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フィールド内に指定した値に書き換えます。ACL ルールがプライオリティと IPv4 パケットの両方を変更するために追加されても、チップの制限のためそれらの一方しか変更できません。プライオリティと DSCP の両方が変更されるように設定されている場合は、現在のプライオリティを変更します。
Replace ToS Precedence (0-7)	出力パケットの IP 優先度が新しい値に変更されます。操作の優先度なしで使用すると、デフォルト TC にパケットは送信されます。
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 / VLAN Name / VLAN ID	• Ports - ポートの範囲を指定する際には、本画面中の「Access ID」フィールドの「Auto assign」チェックボックスを選択しておく必要があります。選択しないと、エラーメッセージが表示され、アクセスルールの設定が行われません。「All Ports」をチェックすると、スイッチのすべてのポートを選択できます。 • VLAN Name - アクセスルールに適用する VLAN 名を指定します。 • VLAN ID - アクセスルールに適用する VLAN ID 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。

「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

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。

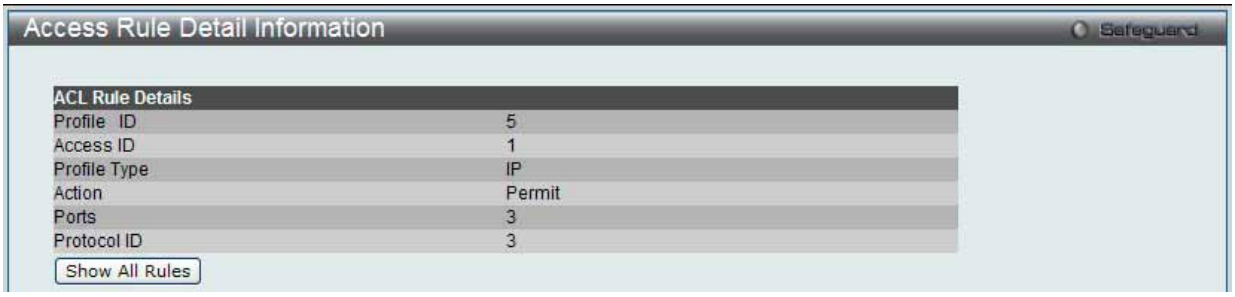


図 7.6-9　Access Rule Detail Information - Ethernet 画面

「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。

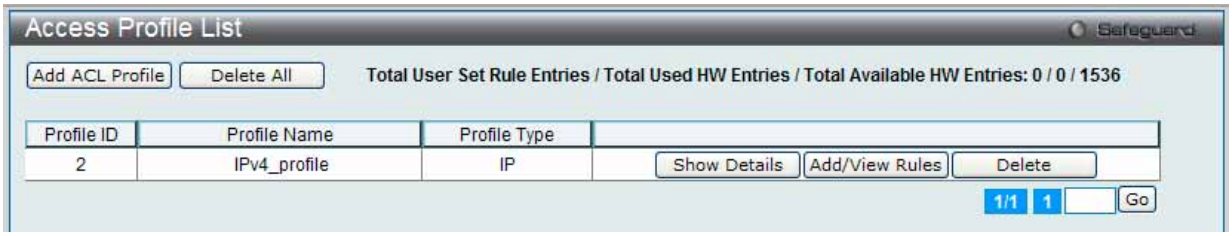


図 7.6-10　Access Profile List 画面

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

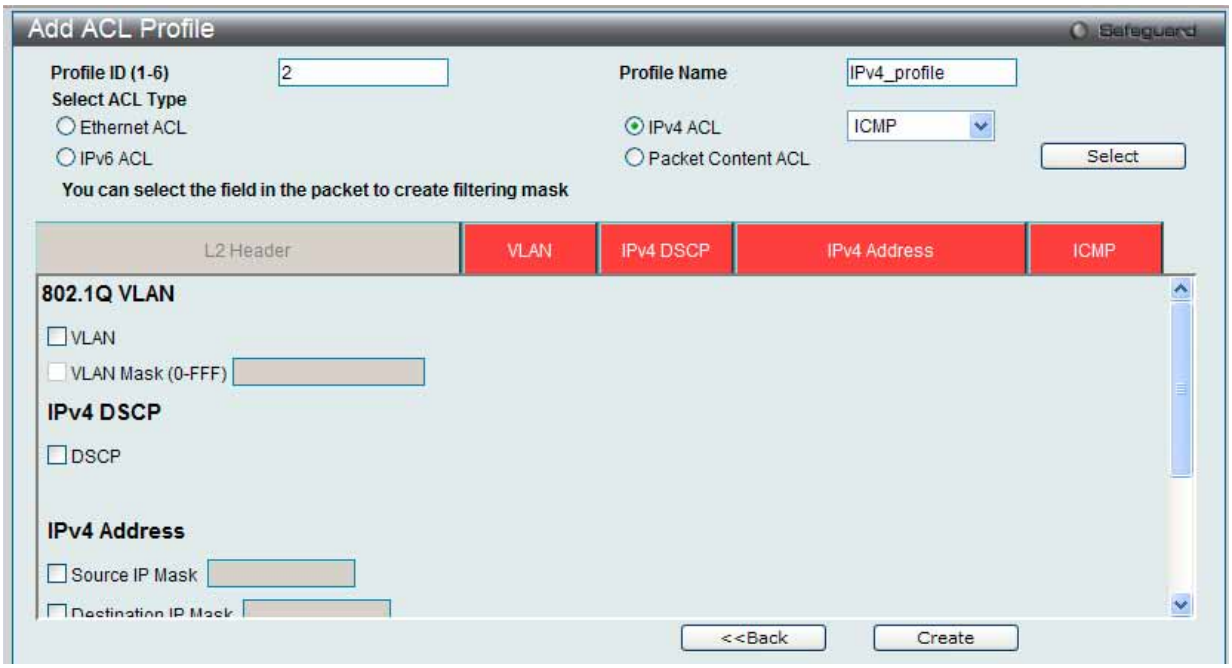


図 7.6-11　Add ACL Profile - IPv4 ACL 画面

「Profile ID」でプロファイル番号を 1-6 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
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 6 が指定できます。
Profile Name	作成したプロファイルにプロファイル名を入力します。
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	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。
IPv4 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。
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。
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。例 : 255.255.255.255 - 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。例 : 255.255.255.255
Protocol ID	マスクしたいパケットヘッダの Protocol ID Mask（0-FF）を指定します。「User Define」マスクは 16 進数（0-FFFFFFFF）で指定します。

「Create」ボタンをクリックし、設定を適用します。
「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

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。

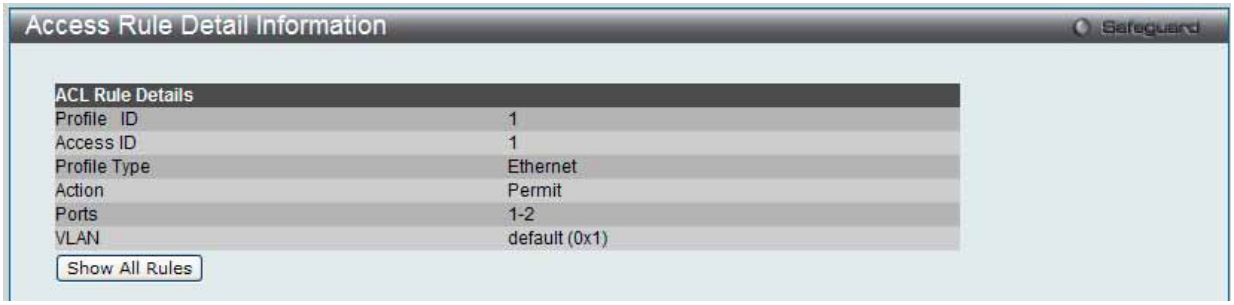


図 7.6-12　Access Profile Detail Information - IPv4 画面

「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。

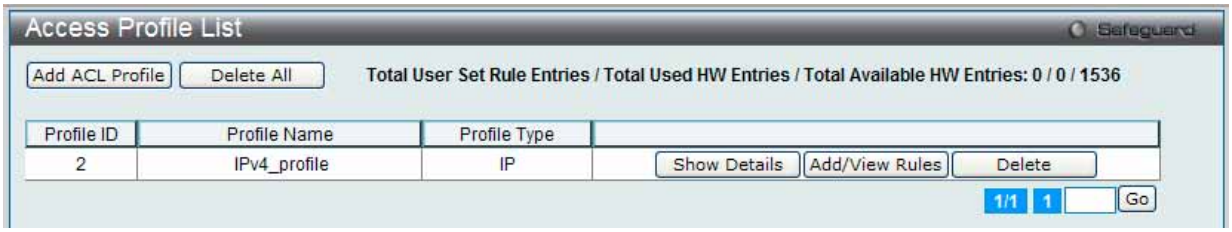


図 7.6-13　Access Profile List 画面

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 7.6-14　Access Rule List - IPv4 画面

「<<Back」をボタンをクリックして前のページに戻ります。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、指定ページへ移動します。

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。

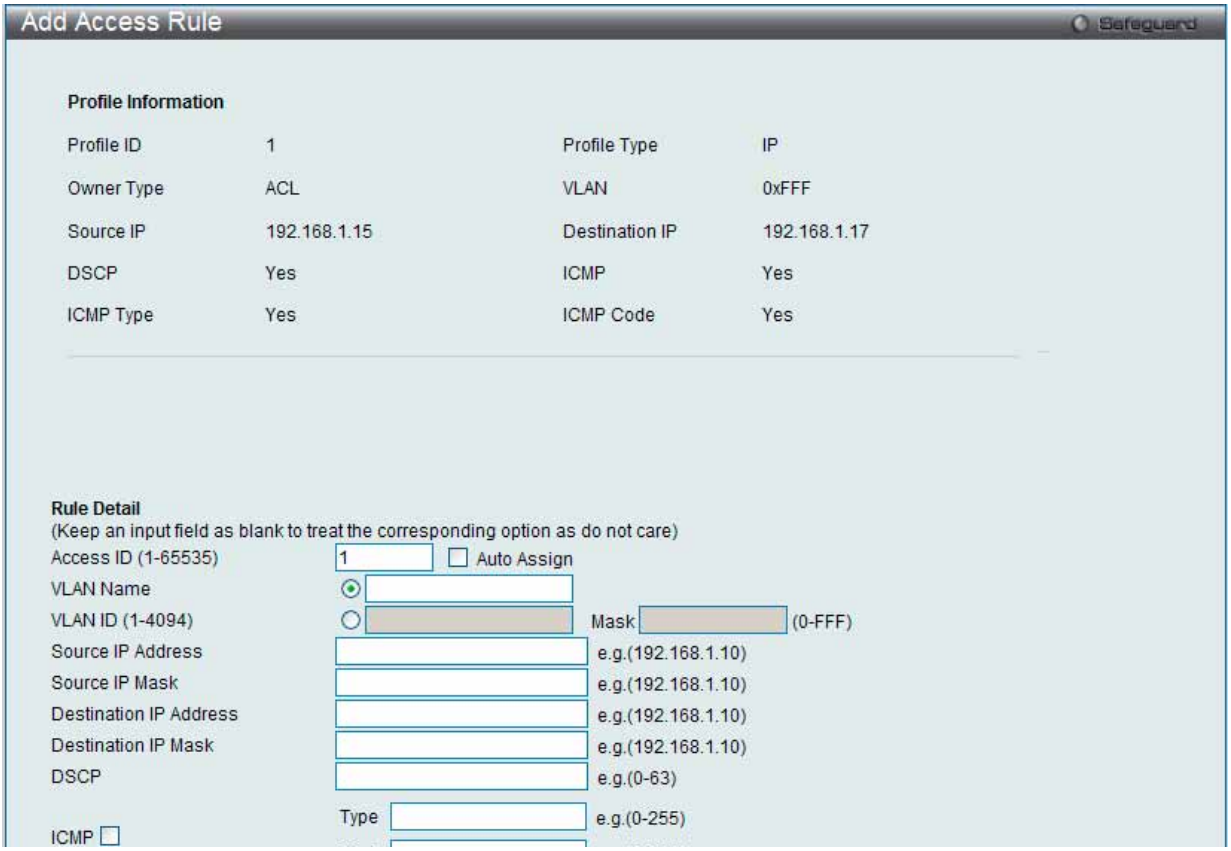


図 7.6-15　Add Access Rule - IPv4 画面

以下の項目を使用して設定および参照します。

項目	説明
Rule Detail	
Access ID (1-256)	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 256 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 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 Address 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 Address 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)	スイッチにより設定された 802.1p デフォルトプライオリティを上書きしたい場合に指定します。このプライオリティにより転送されたパケットがどの CoS キューを使用するかが決まります。この欄を指定するとパケットはこのプライオリティを割り当てられ、対応した CoS キューに転送されます。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「7.5　QoS（QoS 機能の設定）」（189 ページ）を参照してください。
Replace Priority	条件に合ったパケットの DSCP 値は指定した値に入れ替わります。
Replace DSCP (0-63)	スイッチはここで指定した基準に一致するパケットの DSCP をボックスの右側の欄内に指定した値に書き換えます。ACL ルールがプライオリティと IPv4 パケットの両方を変更するのに追加されても、チップの制限のためそれらの一方しか変更できません。プライオリティと DSCP の両方を変更するように設定している場合は、現在のプライオリティを変更します。
Replace ToS Precedence (0-7)	出力パケットの IP 優先度が新しい値に変更されます。操作の優先度なしで使用すると、デフォルト TC にパケットは送信されます。
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。

項目	説明
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 / VLAN Name / VLAN ID	• Ports - ポートの範囲を指定する際には、本画面中の「Access ID」フィールドの「Auto assign」チェックボックスを選択しておく必要があります。選択しないと、エラーメッセージが表示され、アクセスルールの設定が行われません。「All Ports」をチェックすると、スイッチのすべてのポートを選択できます。 • VLAN Name - アクセスルールに適用する VLAN 名を指定します。 • VLAN ID - アクセスルールに適用する VLAN ID 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。
「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

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 7.6-16　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。

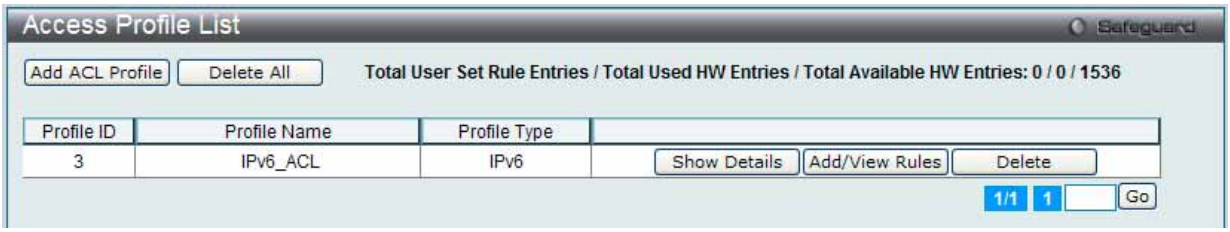


図 7.6-17　Access Profile List 画面

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 7.6-18　Add ACL Profile - IPv6 ACL 画面

「Profile ID」でプロファイル番号を 1-6 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
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 6 を指定できます。
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。
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。

項目	説明
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。
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。
IPv6 Address	• IPv6 Source Address - 対応するボックスをチェックして、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。 • IPv6 Destination Address - 対応するボックスをチェックして、送信先 IPv6 アドレスをマスクする IP アドレスを指定します。

「Create」ボタンをクリックし、設定を適用します。
「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

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。

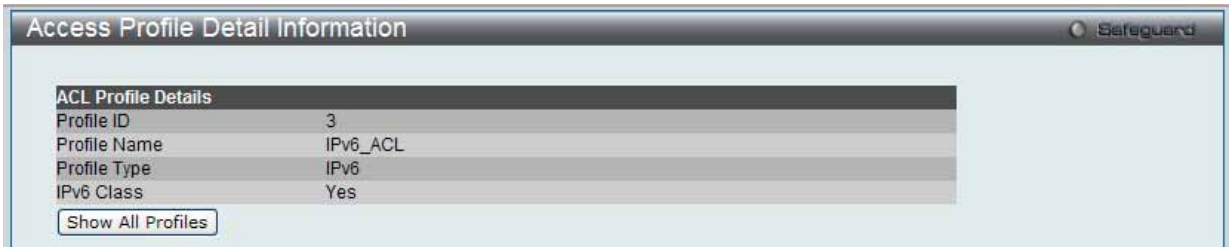


図 7.6-19　Access Profile Detail Information - IPv6 ACL 画面

「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。

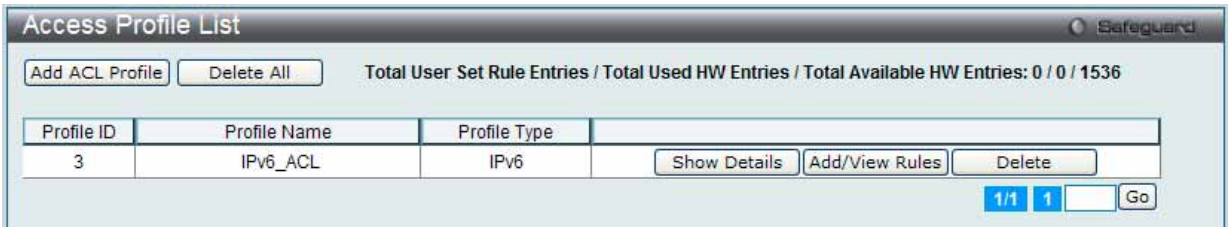


図 7.6-20　Access Profile List 画面

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 7.6-21　Access Rule List - IPv6 画面

「<<Back」をボタンをクリックして前のページに戻ります。

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

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

1. 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。

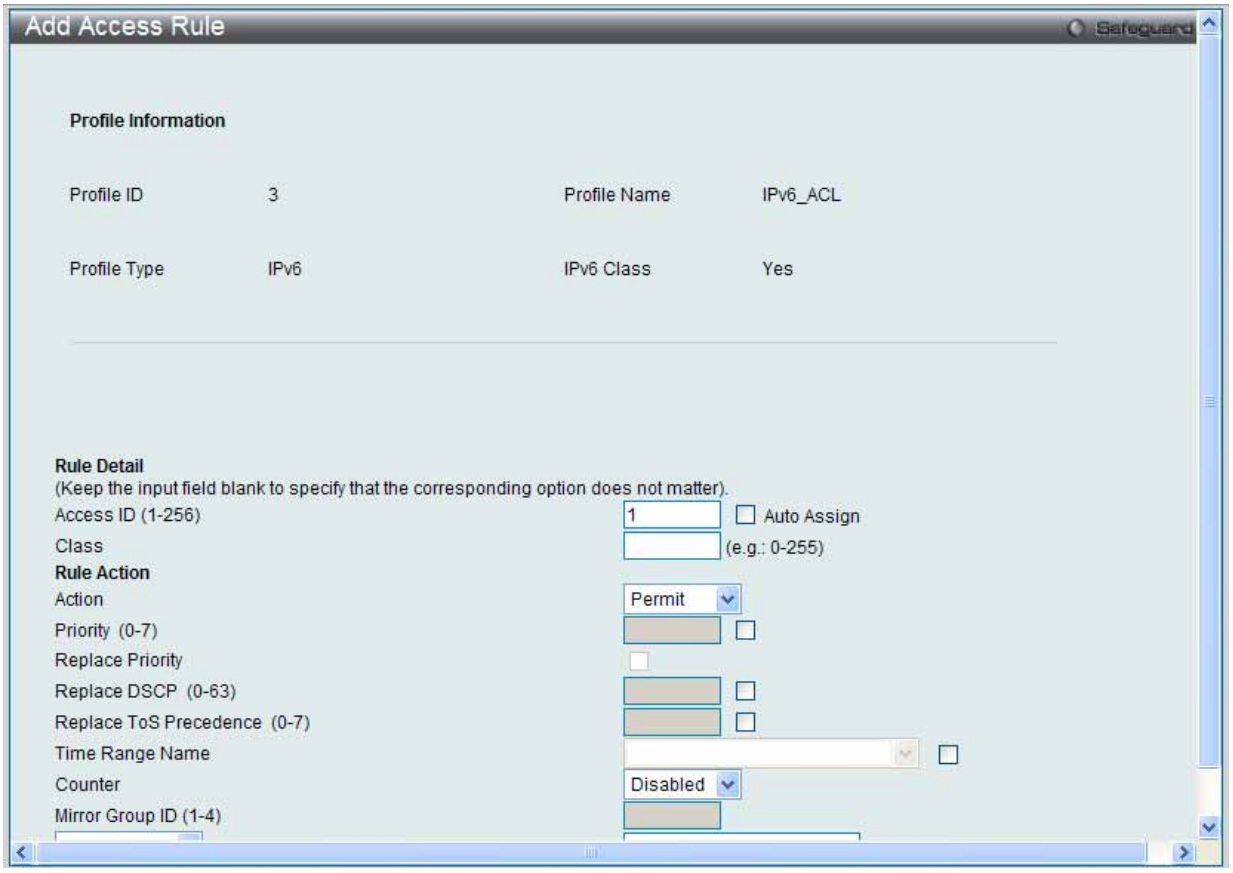


図 7.6-22　Add Access Rule - IPv6 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Rule Detail	
Access ID (1-256)	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 256 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 Address 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。
IPv6 Destination Address	IPv6 送信元アドレスの IPv6 アドレスを入力します。
IPv6 Destination Address 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。
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。
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。

項目	説明
Priority (0-7)	スイッチにより設定された 802.1p デフォルトプライオリティを上書きしたい場合に指定します。このプライオリティにより転送されたパケットがどの CoS キューを使用するかが決まります。この欄を指定するとパケットはこのプライオリティを割り当てられ、対応した CoS キューに転送されます。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「7.5　QoS（QoS 機能の設定）」（189 ページ）を参照してください。
Replace Priority	条件に合ったパケットの DSCP 値は指定した値に入れ替わります。
Replace DSCP (0-63)	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フィールド内に指定した値に書き換えます。ACL ルールがプライオリティと IPv4 パケットの両方を変更するために追加されても、チップの制限のためそれらの一方しか変更できません。プライオリティと DSCP の両方が変更されるように設定されている場合は、現在のプライオリティを変更します。
Replace ToS Precedence (0-7)	出力パケットの IP 優先度が新しい値に変更されます。操作の優先度なしで使用すると、デフォルト TC にパケットは送信されます。
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 / VLAN Name / VLAN ID	• Ports - ポートの範囲を指定する際には、本画面中の「Access ID」フィールドの「Auto assign」チェックボックスを選択しておく必要があります。選択しないと、エラーメッセージが表示され、アクセスルールの設定が行われません。「All Ports」をチェックすると、スイッチのすべてのポートを選択できます。 • VLAN Name - アクセスルールに適用する VLAN 名を指定します。 • VLAN ID - アクセスルールに適用する VLAN ID 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。
「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

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。

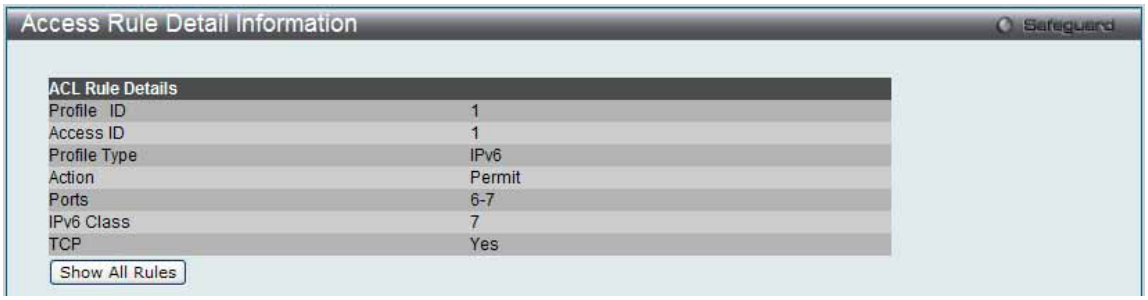


図 7.6-23　Access Rule Detail Information - IPv6 画面

「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。

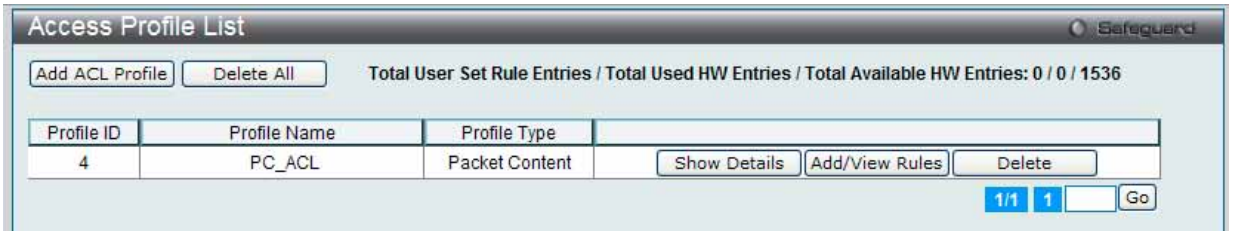


図 7.6-24　Access Profile List 画面

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

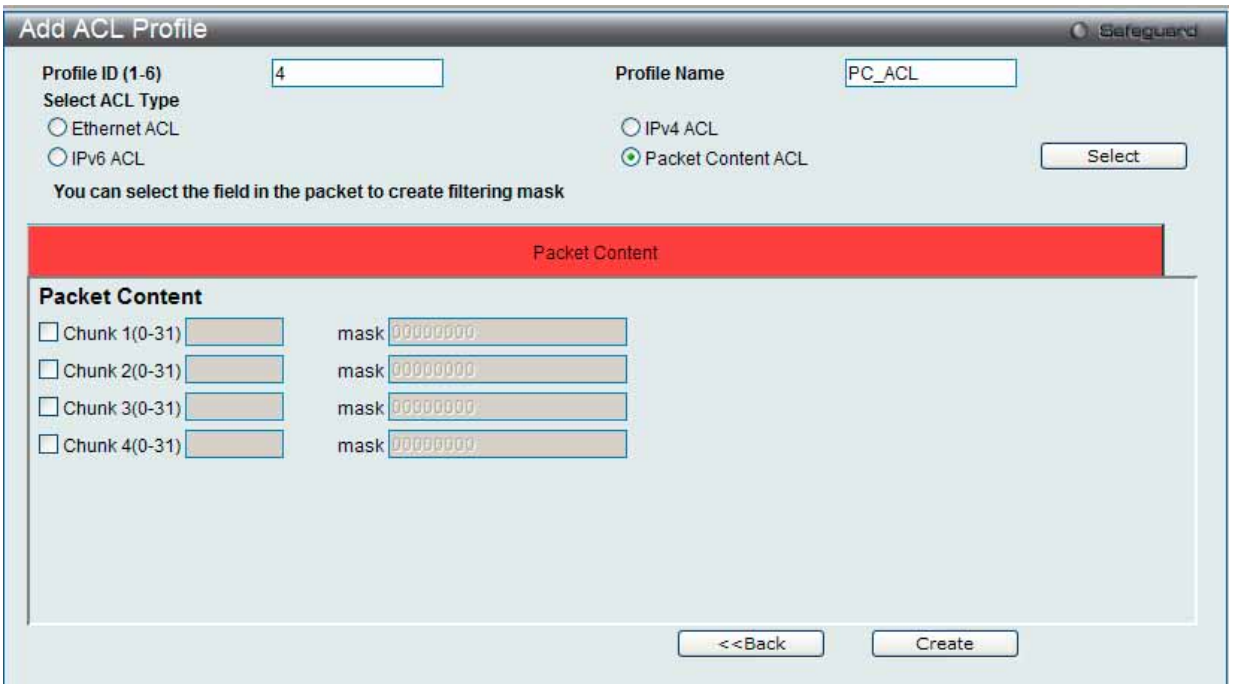


図 7.6-25　Add ACL Profile 画面 - パケットコンテンツ

「Profile ID」でプロファイル番号を 1-6 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。

<table>
<tr><th>項目</th><th>説明</th></tr>
<tr><td>Profile ID</td><td>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 6 を指定できます。</td></tr>
<tr><td>Select ACL Type</td><td>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。
• 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。</td></tr>
<tr><td>Packet Content</td><td>パケットコンテンツは、同時にパケット内の 4 個のオフセットチャンクと、そのフレームコンテンツとオフセットを検証できます。設定可能な 4 個のチャンクオフセットとマスクがあります。チャンクマスクは 4 バイトを示します。

以下で説明するように、32 個の定義済みオフセットチャンクから 4 つのオフセットチャンクを選択することができます。
offset_chunk_1、offset_chunk_2、offset_chunk_3、offset_chunk_4
<table>
<tr><td>chunk0</td><td>chunk1</td><td>chunk2</td><td>……</td><td>chunk29</td><td>chunk30</td><td>chunk31</td></tr>
<tr><td>B126, B127,
B0, B1</td><td>B2, B3,
B4, B5</td><td>B6, B7,
B8, B9</td><td>……</td><td>B114, B115,
B116, B117</td><td>B118, B119,
B120, B121</td><td>B122, B123,
B124, B125</td></tr>
</table>
例題：
offset_chunk_1 0 0xffffffff はパケットバイトオフセット 126,127,0,0,1 に一致します。
offset_chunk_1 0 0x0000ffff はパケットバイトオフセット 0,1 に一致します。

注意 一度に、1 個のパケットコンテンツマスクプロファイルしか作成できません。

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。</td></tr>
</table>

「Select」ボタンをクリックし、ACL タイプを選択します。
「Create」ボタンをクリックし、プロファイルを追加します。

「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

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 7.6-26　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。

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最後にある「付録 B パスワードのリカバリ手順」（534 ページ）を参照してください。

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。

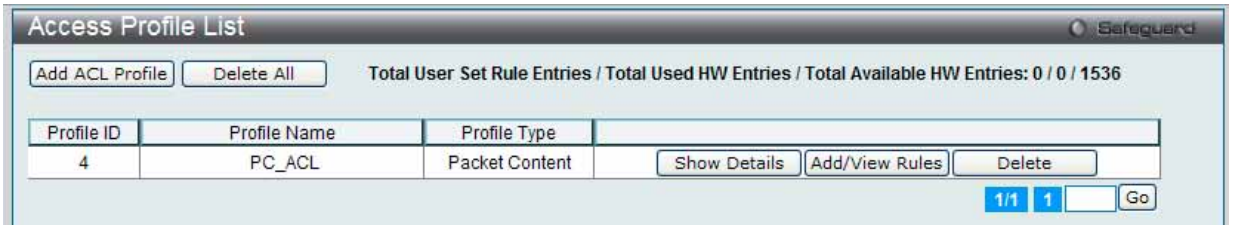


図 7.6-27　Access Profile List 画面

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。

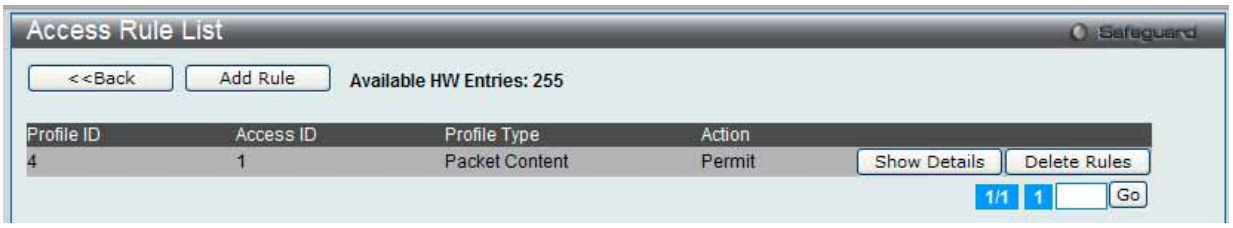


図 7.6-28　Access Rule List 画面 - パケットコンテンツ

「<<Back」をボタンをクリックして前のページに戻ります。

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

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。

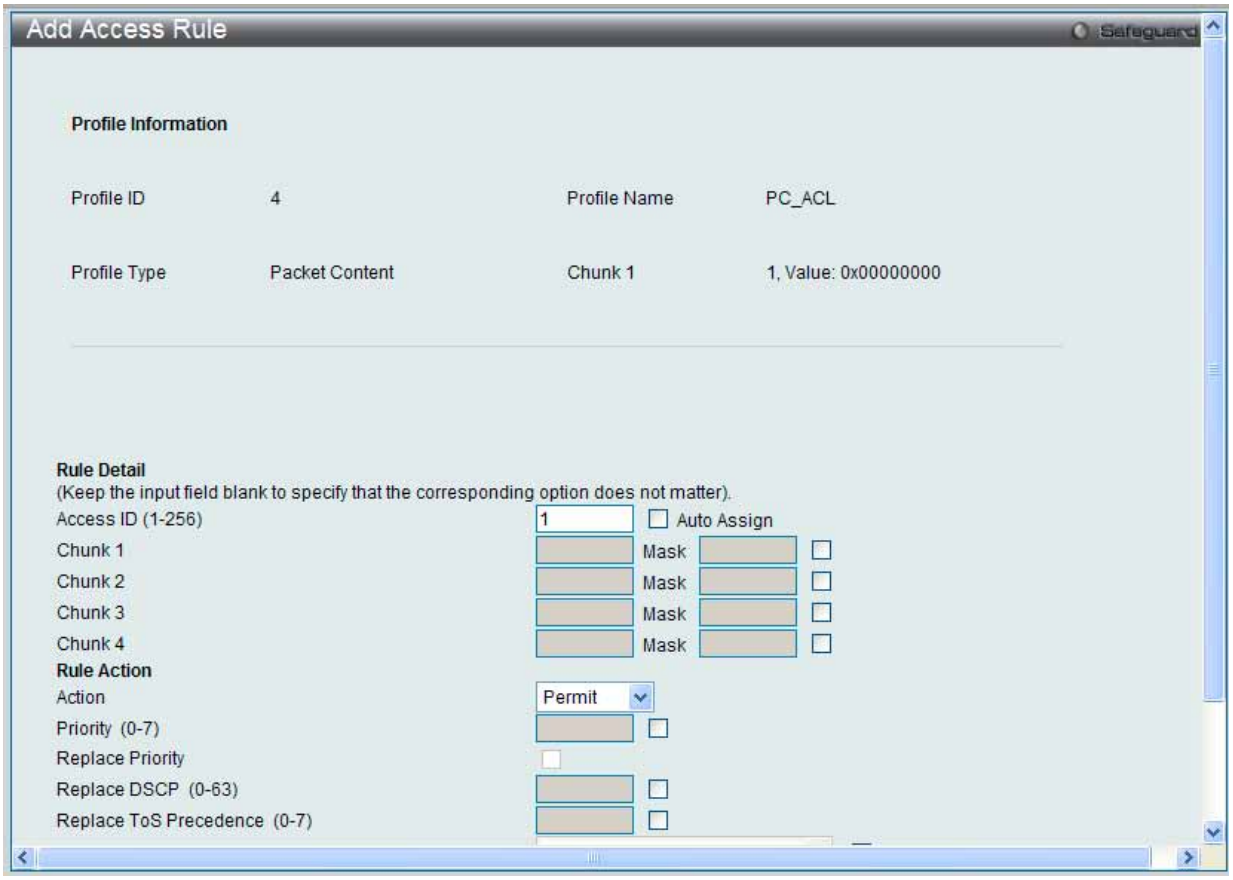


図 7.6-29　Add Access Rule 画面 - パケットコンテンツ

以下の項目を使用して設定および参照します。

項目	説明
Rule Detail	
Access ID (1-256)	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 256 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。
Chunk	本項目の設定により、スイッチは指定したオフセット値で始まるパケットヘッダをマスクします。
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)	スイッチにより設定された 802.1p デフォルトプライオリティを上書きしたい場合に指定します。このプライオリティにより転送されたパケットがどの CoS キューを使用するかが決まります。この欄を指定するとパケットはこのプライオリティを割り当てられ、対応した CoS キューに転送されます。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「7.5　QoS（QoS 機能の設定）」（189 ページ）を参照してください。
Replace Priority	条件に合ったパケットの DSCP 値は指定した値に入れ替わります。
Replace DSCP (0-63)	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フィールド内に指定した値に書き換えます。ACL ルールがプライオリティと IPv4 パケットの両方を変更するために追加されても、チップの制限のためそれらの一方しか変更できません。プライオリティと DSCP の両方が変更されるように設定されている場合は、現在のプライオリティを変更します。
Replace ToS Precedence (0-7)	出力パケットの IP 優先度が新しい値に変更されます。操作の優先度なしで使用すると、デフォルト TC にパケットは送信されます。
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 / VLAN Name / VLAN ID	このルールに適用するオブジェクトの選択または入力を行います。 • Ports - ポート番号またはポート範囲を入力します。ポートの範囲を指定する際には、本画面中の「Access ID」フィールドの「Auto Assign」チェックボックスを選択しておく必要があります。選択しないと、エラーメッセージが表示され、アクセスルールの設定が行われません。 • VLAN Name - VLAN 名を入力します。 • VLAN ID - VID を入力します。

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。

「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

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 7.6-30　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。

CPU Access Profile List（CPU アクセスプロファイルリスト）

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。

注意 CPU インタフェースフィルタリングは、プロトコル変換または管理アクセスなど直接スイッチへのトラフィックアクセスを制御するのに使用されます。CPU インタフェースフィルタリングルールは正常な L2/3 トラフィックの送信には影響ありません。しかし、不適当な CPU インタフェースフィルタリングルールによって、ネットワークは不安定になる可能性があります。

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。

動作状態を変更するためには、ラジオボタンを使用して、CPU インタフェースフィルタリング機能をグローバルに「Enabled」（有効）または「Disabled」（無効）にします。
「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。「Disabled」にするとこの動作は行われません。

ACL > CPU 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。

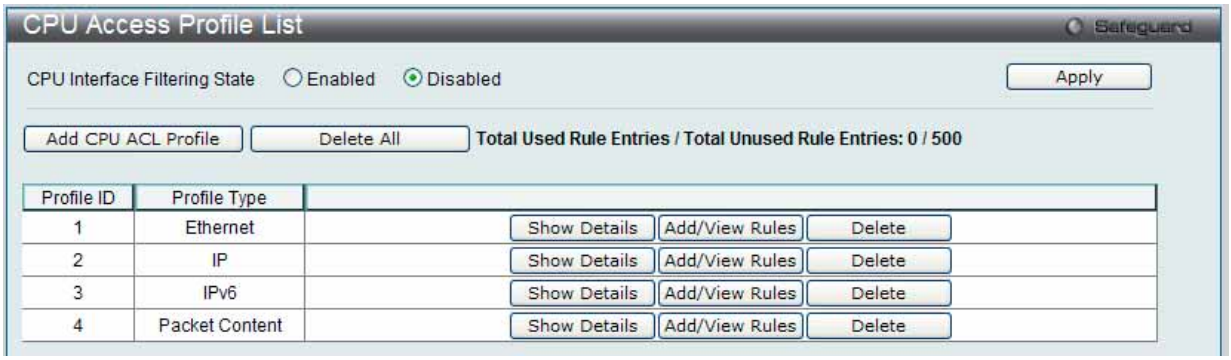


図 7.6-31　CPU Access Profile List 画面

以下の項目を使用して設定および参照します。

項目	説明
CPU Interface Filtering State	CPU インタフェースフィルタリング状態を「Enabled」（有効）または「Disabled」（無効）にします。設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
Add CPU ACL Profile	CPU ACL リストにエントリを追加します。
Delete All	テーブルからすべてのアクセスプロファイルを削除します。
Show Details	指定プロファイル ID エントリに関する情報を表示します。
Add/View Rules	指定プロファイル ID 内の CPU ACL ルールの参照または追加を行います。
Delete	指定エントリを削除します。

「Add CPU ACL Profile」画面には 4 種類あります。:
イーサネット (MAC アドレスベース) プロファイル設定用、IPv6 アドレスベースプロファイル設定用、IPv4 アドレスベースプロファイル設定用およびパケットコンテンツマスクプロファイル設定用です。

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 7.6-32　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

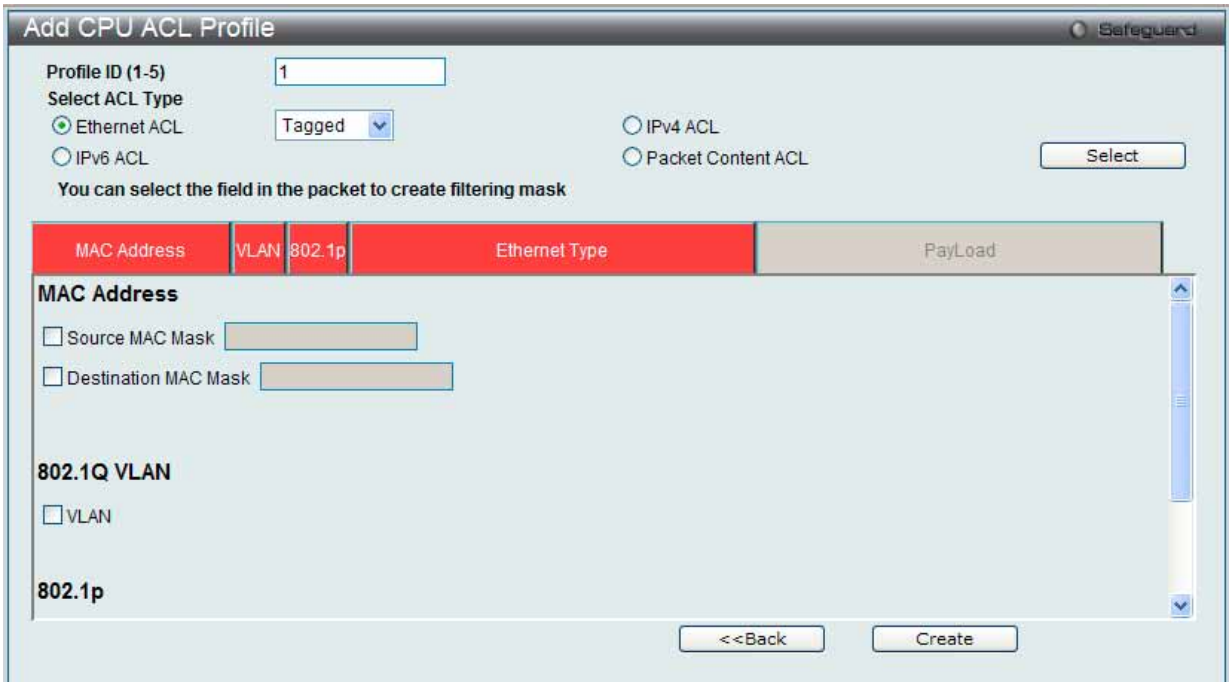


図 7.6-33　Add CPU ACL Profile - Ethernet 画面

「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。

以下の項目を使用して設定および参照します。

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 5 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 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 Mask (0-FFF) - VLAN マスクを指定します。
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 7.6-34　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 7.6-35　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。

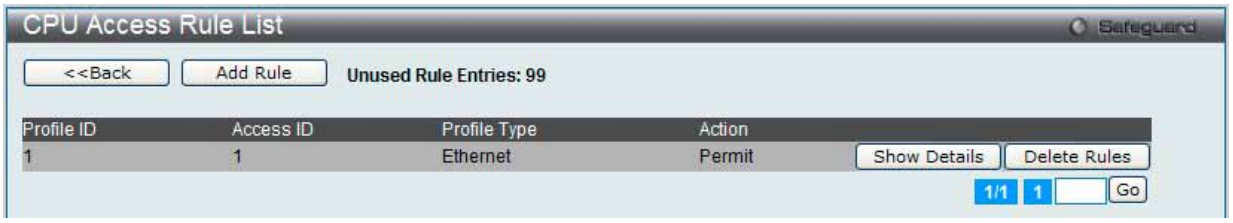


図 7.6-36　CPU Access Rule List - Ethernet 画面

「Show Details」ボタンをクリックし、作成した指定ルールに関する詳しい情報を表示します。
「Delete Rules」ボタンをクリックして、指定エントリを削除します。

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

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。

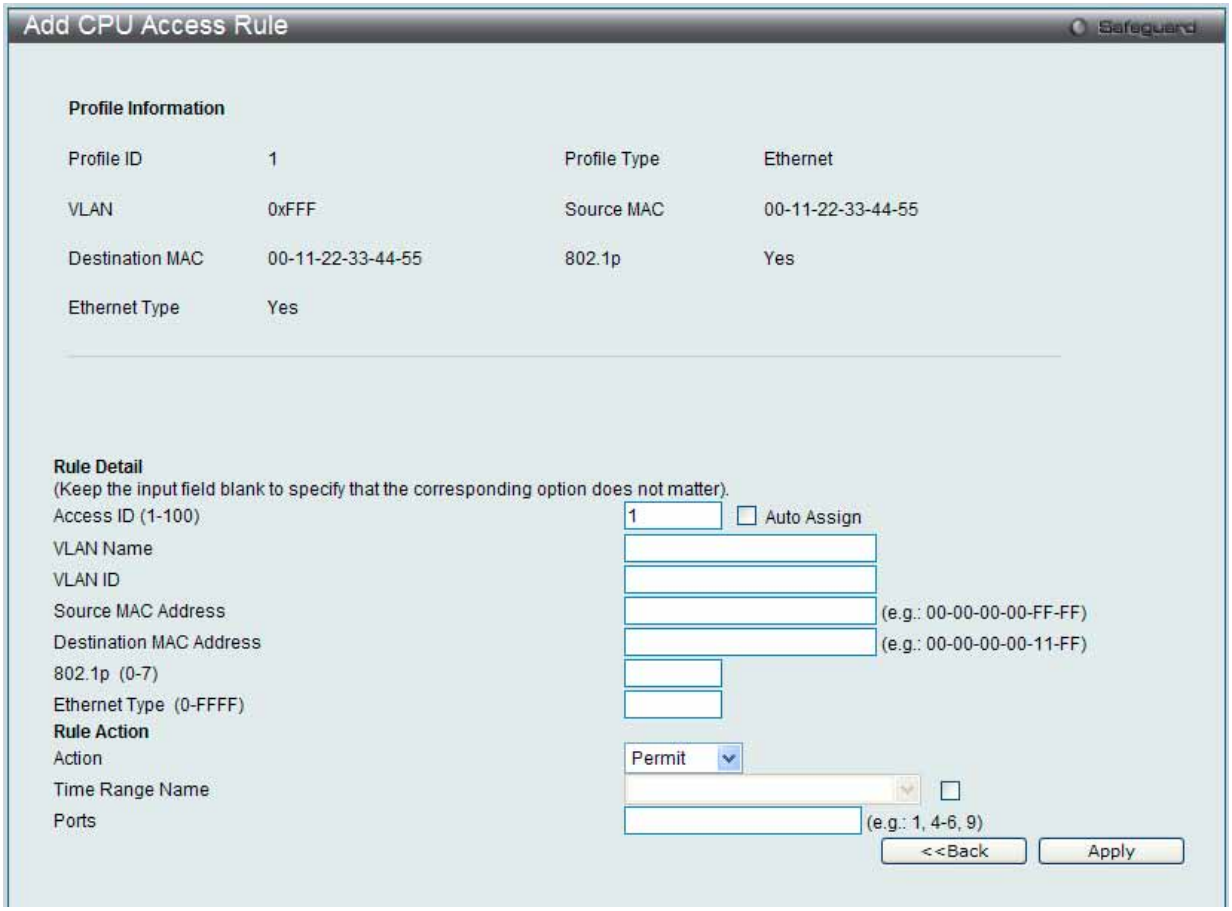


図 7.6-37　Add Access Rule - Ethernet 画面

以下の項目を使用して設定および参照します。

項目	説明
Rule Action	
Access ID (1-100)	それぞれのルールに固有の番号を指定します。1 から 100 が指定できます。 • Auto Assign - 選択すると、作成中のルールに自動で 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。
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。
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。
「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

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。

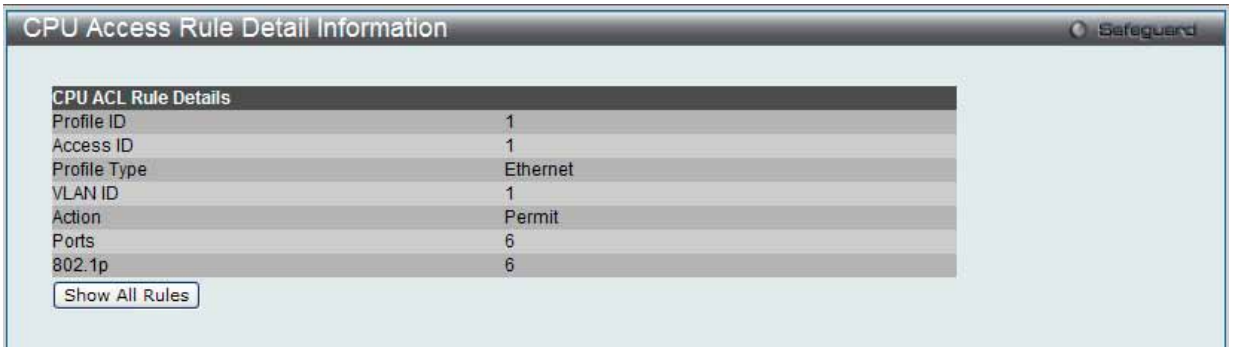


図 7.6-38　CPU Access Rule Detail Information - Ethernet 画面

「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。

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 7.6-39　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

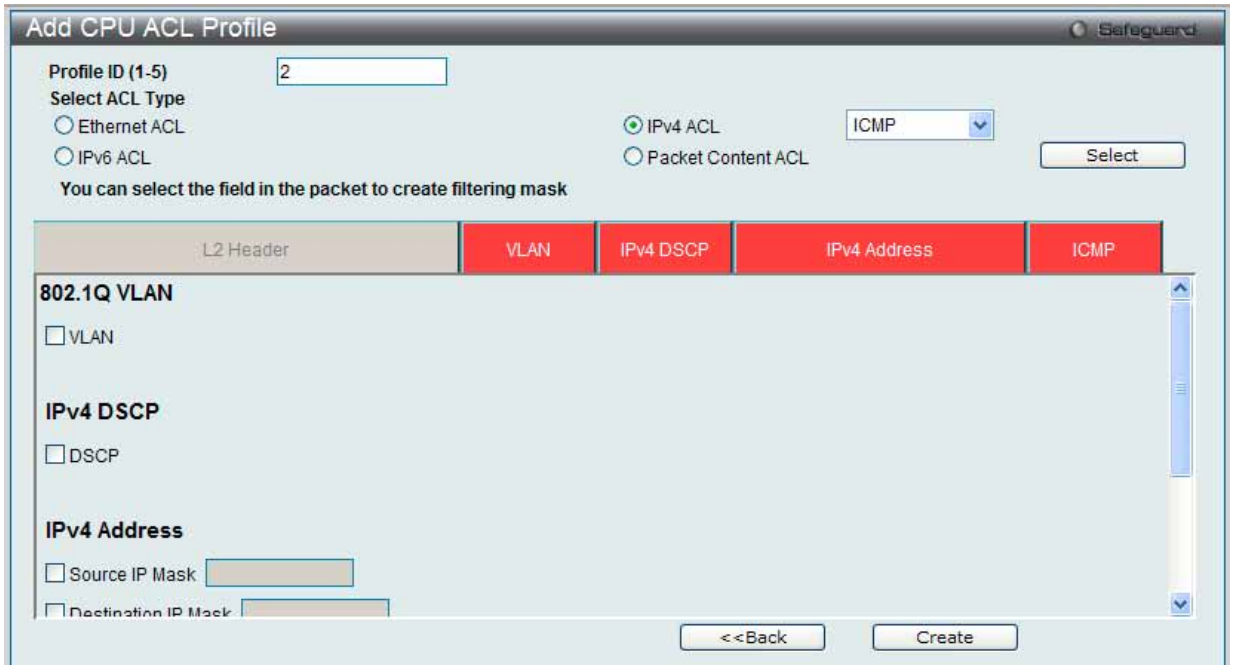


図 10-38　Add CPU ACL Profile - IPv4 画面

「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 5 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。	
802.1Q VLAN	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。
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。例 : 255.255.255.255 • 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。例 : 255.255.255.255
Protocol: 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。	
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。
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。

項目	説明
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 (0-FFFF) - 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 (0-FFFF) - 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) - ユーザ定義のレイヤ 4 パートマスク値を指定します。

「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。

「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

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 7.6-40　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 7.6-41　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 7.6-42　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。

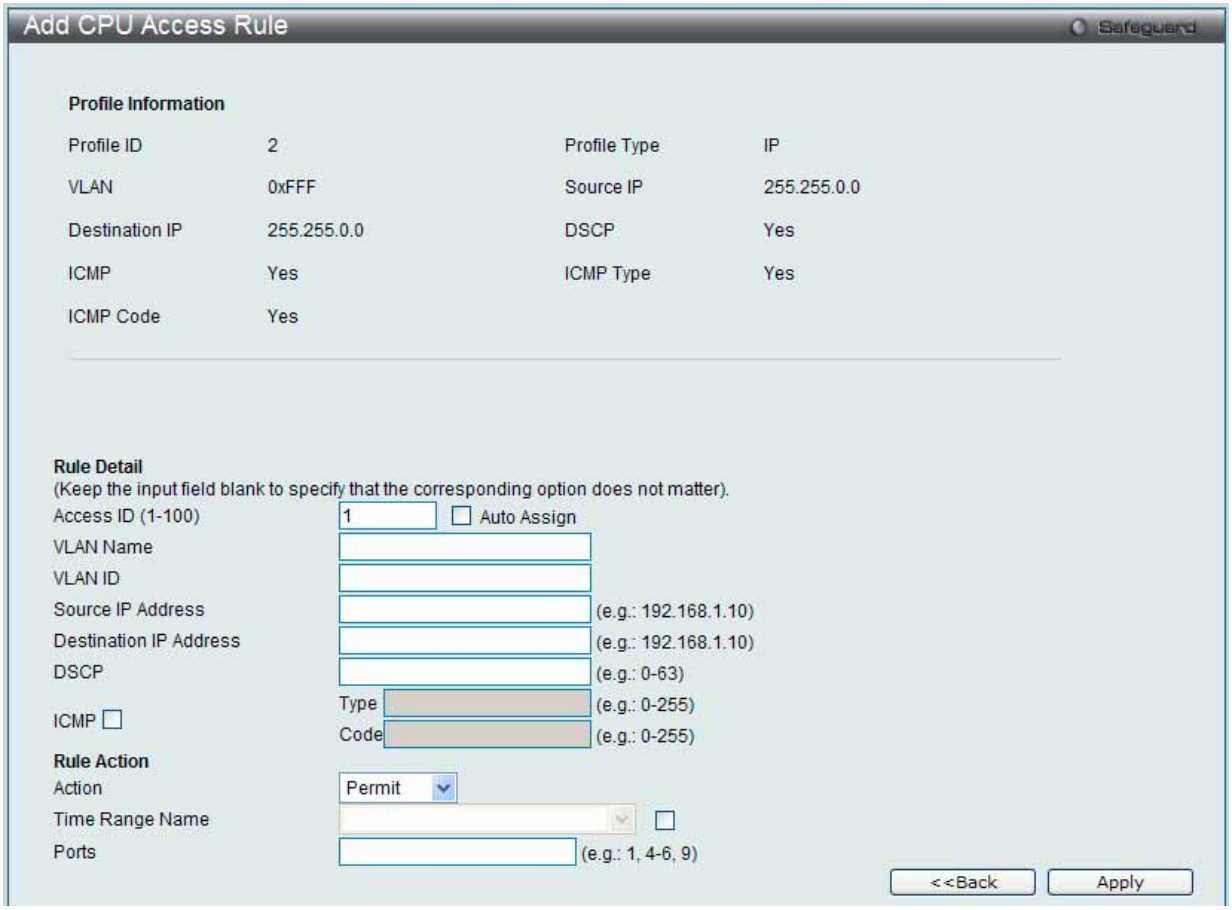


図 7.6-43　Add Access Rule - IP 画面

以下の項目を使用して設定および参照します。

項目	説明
Rule Detail	
Access ID (1-100)	それぞれのルールに固有の番号を指定します。1 から 100 が指定できます。 • Auto Assign - 選択すると、作成中のルールに自動で Access ID を割り当てます。
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	定義済みの 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。
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。

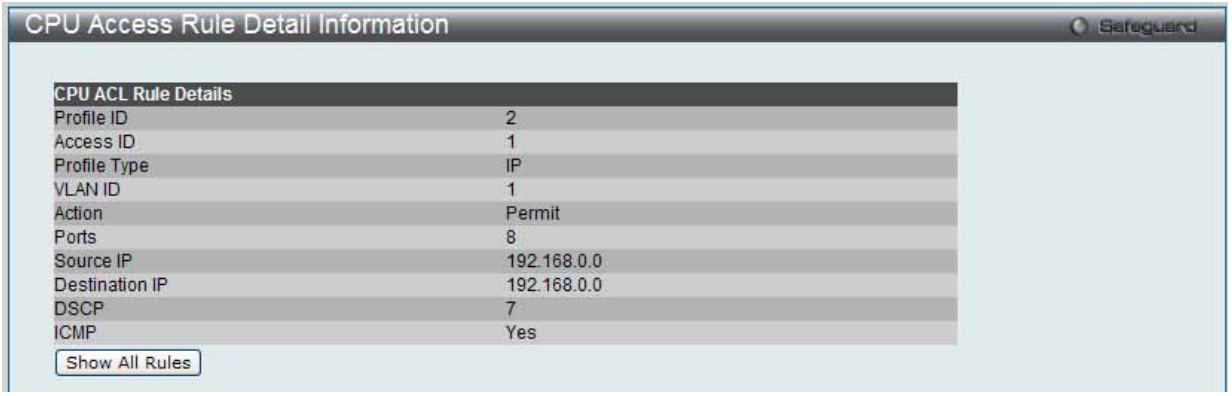


図 7.6-44　CPU Access Rule Detail Information - IP 画面

「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 7.6-45　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

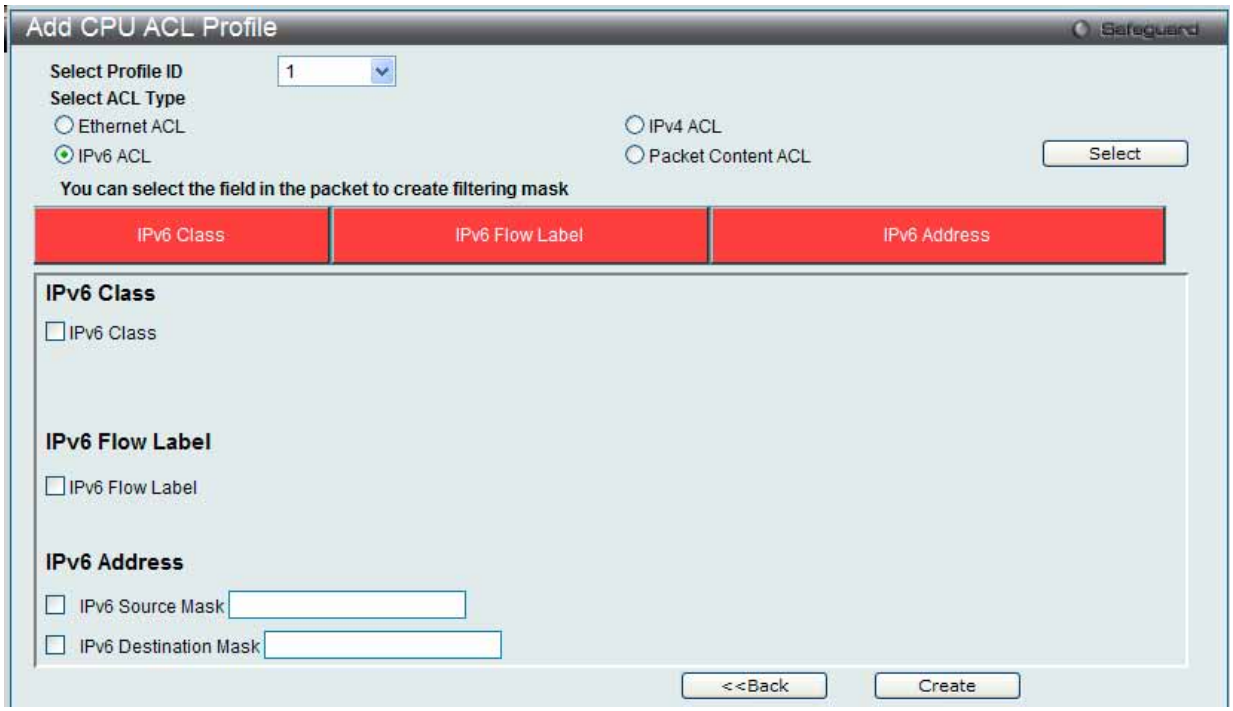


図 7.6-46　Add CPU ACL Profile - IPv6 画面

「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 5 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 Mask - 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 Mask - 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。
TCP	• Source Port Mask (0-FFFF) - IPv6 L4 TCP 送信元ポートサブマスクを指定します。 • Destination Port Mask (0-FFFF) - IPv6 L4 TCP 送信先ポートサブマスクを指定します。
UDP	• Source Port Mask (0-FFFF) - IPv6 L4 UDP 送信元ポートサブマスクを指定します。 • Destination Port Mask (0-FFFF) - IPv6 L4 UDP 送信先ポートサブマスクを指定します。

「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 7.6-47　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 7.6-48　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 7.6-49　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。

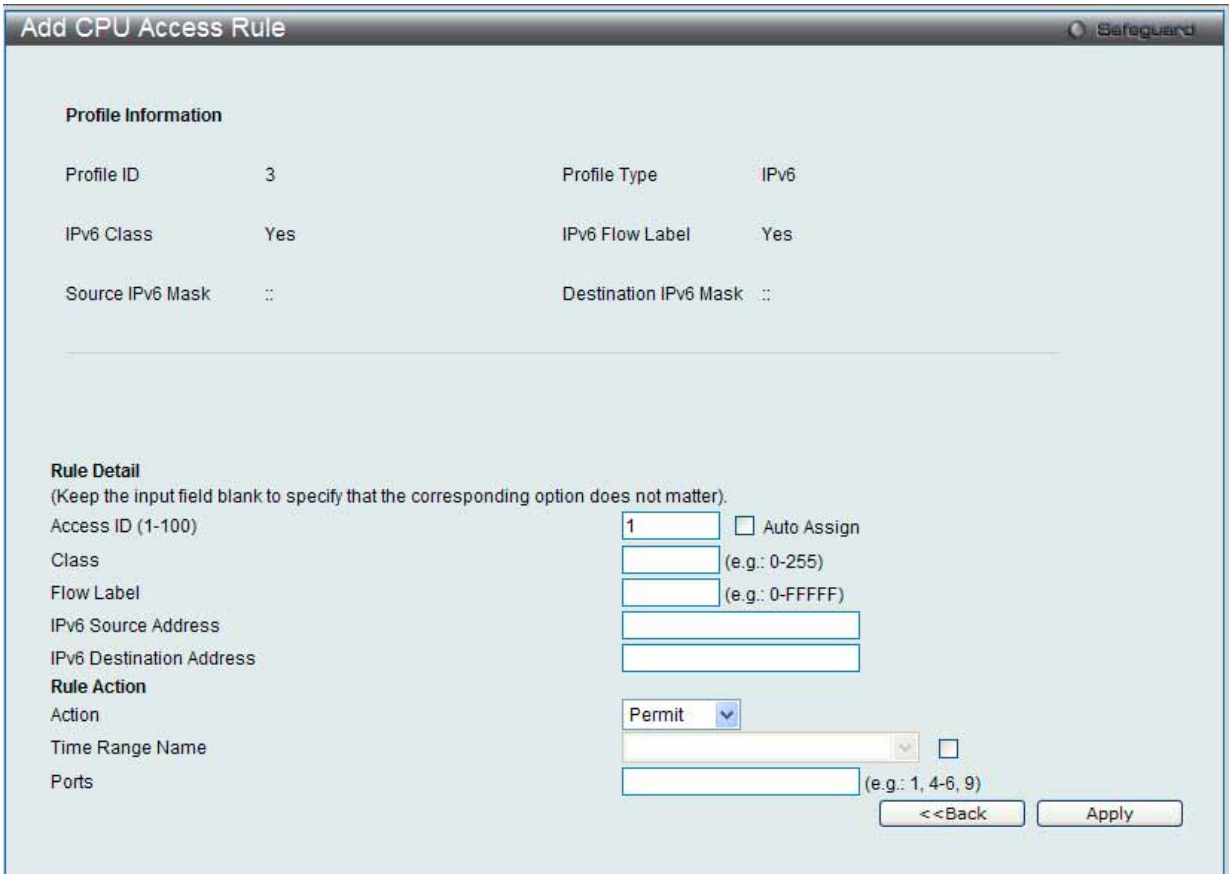


図 7.6-50　Add Access Rule - IPv6 画面

以下の項目を使用して設定および参照します。

項目	説明
Rule Detail	
Access ID (1-100)	それぞれのルールに固有の番号を指定します。1 から 100 が指定できます。 • Auto Assign - 選択すると、作成中のルールに自動で 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	16 進数で指定して IPv6 ヘッダの「Flow Label」フィールドを調べます。本フィールド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フィールドです。
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。
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。

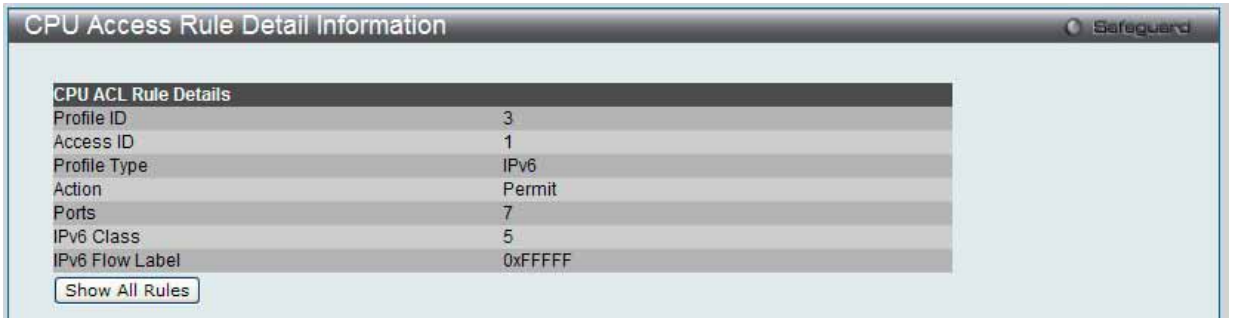


図 7.6-51　CPU Access Rule Detail Information - IPv6 画面

「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 7.6-52　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

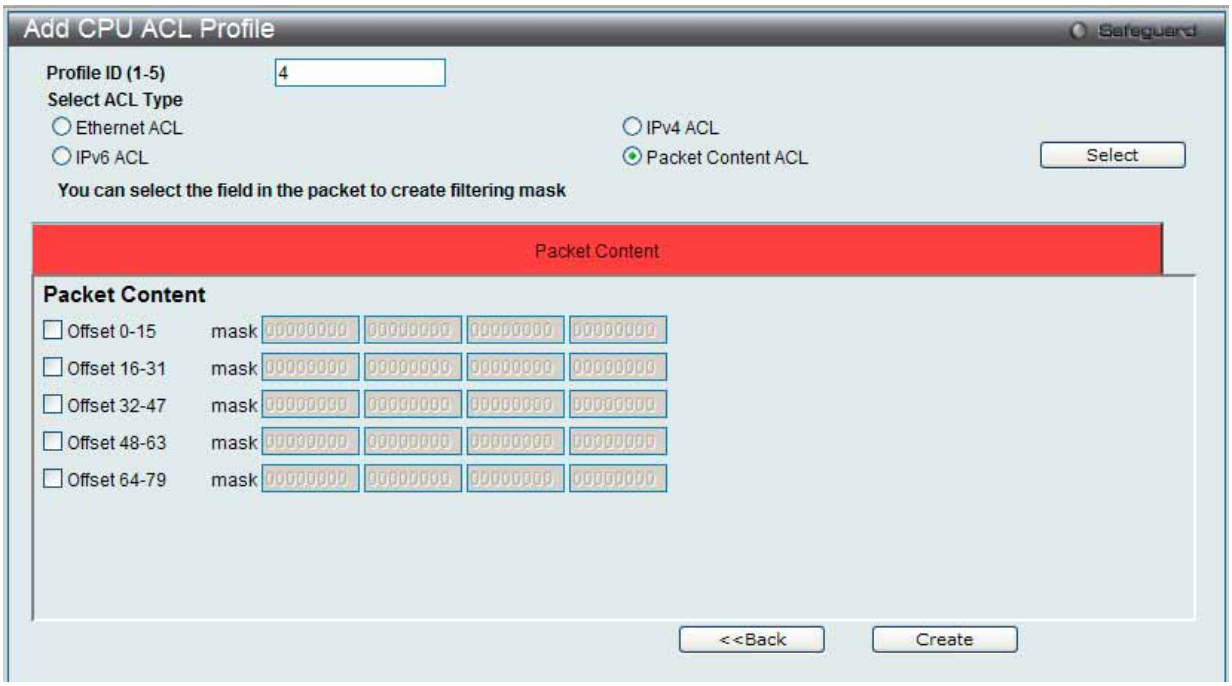


図 7.6-53　Add CPU ACL Profile - Packet Content 画面

「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 5 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。

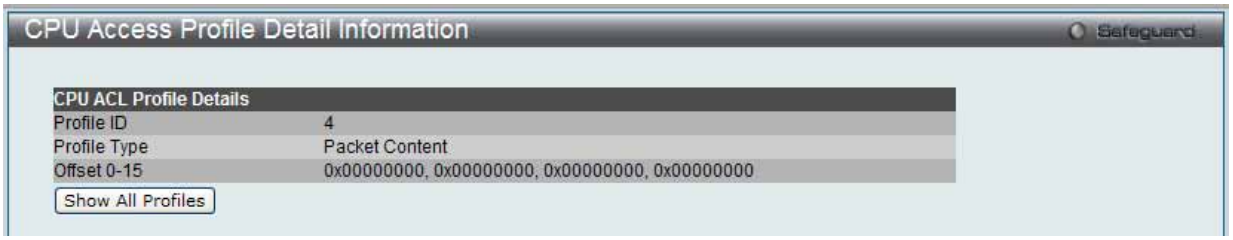


図 7.6-54　CPU Access Profile Detail Information - Packet Content 画面

「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 7.6-55　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。

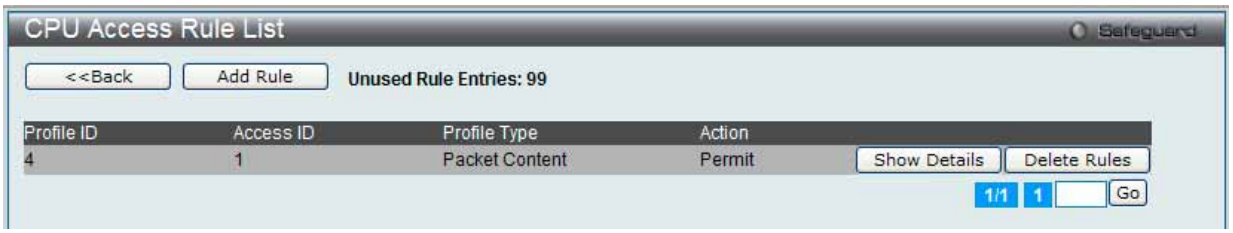


図 7.6-56　CPU Access Rule List - Packet Content 画面

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。

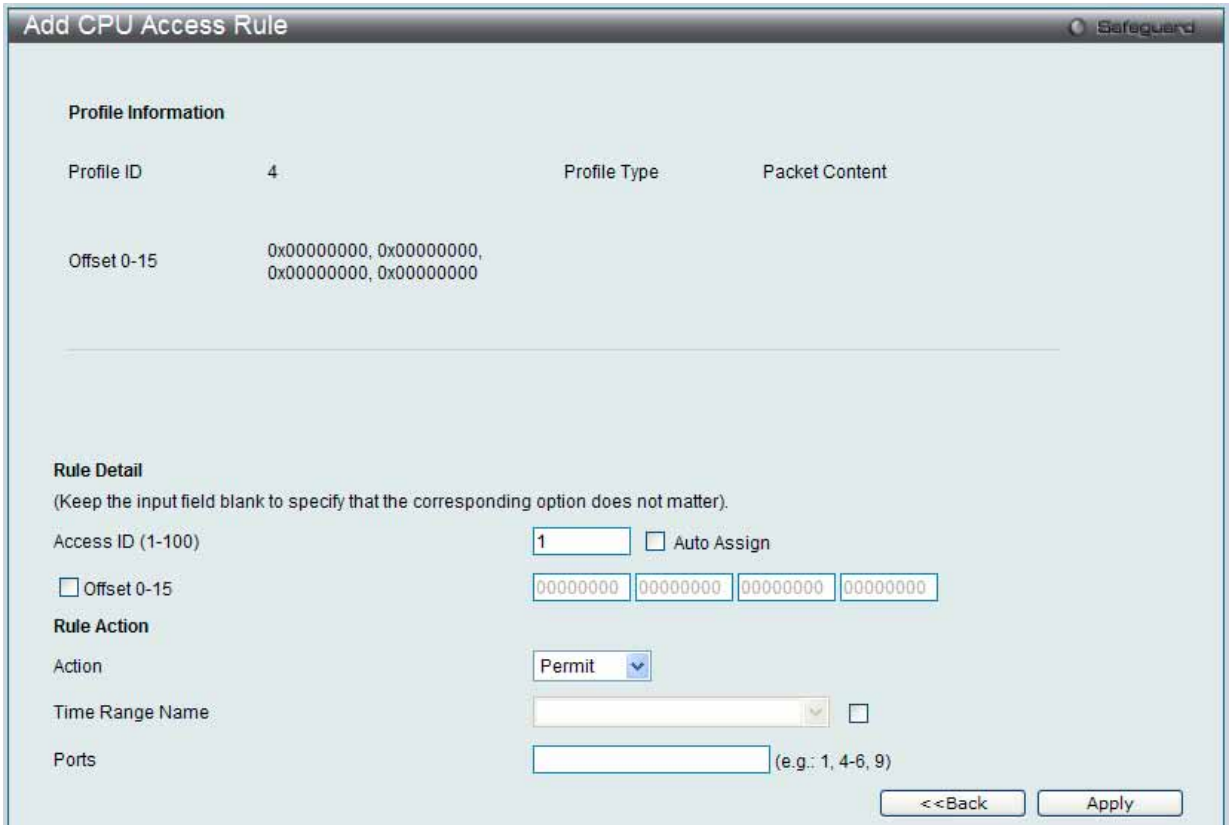


図 7.6-57　Add Access Rule - Packet Content 画面

項目	説明
Rule Detail	
Access ID (1-100)	それぞれのルールに固有の番号を指定します。1 から 100 が指定できます。 • Auto Assign - 選択すると、作成中のルールに自動で Access ID を割り当てます。
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。
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 7.6-58　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。

「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

ACL Finder（ACL 検索）

ACL ルール検索を使用して、特定のポートに割り当てられたすべてのルールを確認し、すばやく既存のルールを編集します。

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。

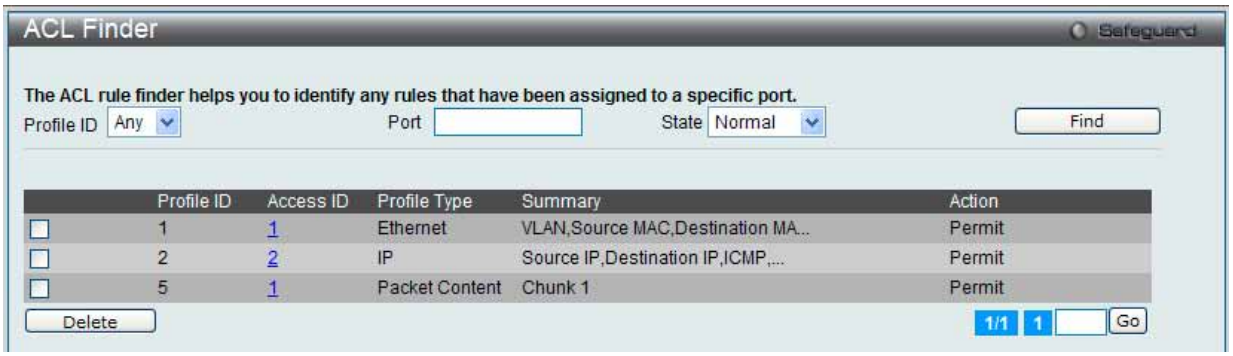


図 7.6-59　ACL Finder 画面

以下の項目を使用して設定および参照します。

項目	説明
Profile ID	ルールの特定のために ACL ルール検索でプロファイル ID を選択します。
Port	ルールの特定のために ACL ルール検索でポート番号を入力します。
State	プルダウンメニューを使用して状態を選択します。 • Normal - 通常の ACL ルールを検索します。 • CPU - CPU ACL ルールを検索します。 • Egress - Egress ACL ルールを検索します。

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」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。

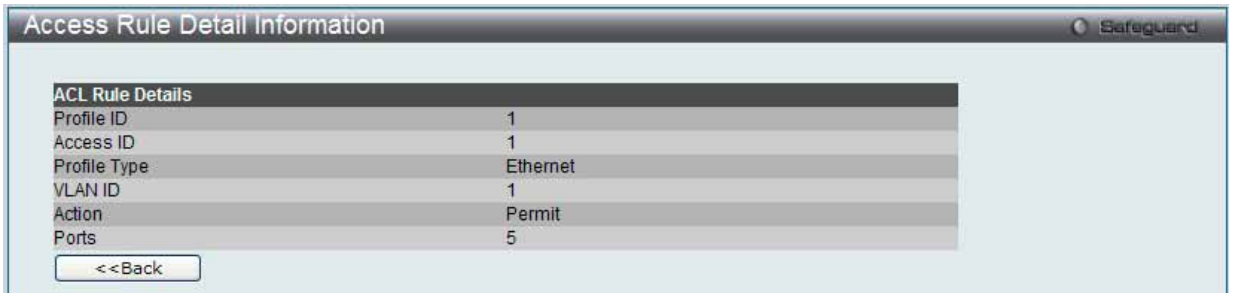


図 7.6-60　Access Rule Detail Information 画面

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

ACL Flow Meter（ACL フローメータ）

ACL フローメータを設定する前に、ユーザが知っておく必要がある頭文字語および項目のリストは次の通りです。

trTCM - Two Rate Three Color Marker。これは、srTCM と共にメータリングおよびパケットフローをマーキングするためにスイッチで可能な 2 つの方式です。trTCM が IP フローを計測し、2 つのレート（CIR および PIR）に基づいて、色でマークします。

CIR - Committed Information Rate。trTCM と srTCM の両方に共通で、CIR は IP パケットのバイト数を計測します。IP パケットのバイト数は、リンクする特定のヘッダではなく、IP ヘッダのサイズを取得することで計測します。trTCM に関しては、パケットフローは、CIR を超過していない場合に緑色でマークされ、CIR を超過している場合に黄色でマークされます。設定される CIR のレートは PIR のレートを超過してはなりません。また、CBS および PBS フィールドを使用して予期しないパケットバーストのために CIR を設定することができます。

- **CBS** - Committed Burst Size。バイト数を計測する場合、CBS は、CIR に関連して、パケットサイズの正常な境界を越えているパケットを特定するために使用されます。IP フローで予想される最も大きい IP パケットを受け入れるために、CBS を設定する必要があります。

PIR - Peak Information Rate。このレートは IP パケットのバイト数で計測されます。IP パケットのバイト数は、リンクする特定のヘッダではなく、IP ヘッダのサイズを取得することで計測します。パケットフローが PIR を超過すると、そのパケットフローは赤でマークされます。CIR のレートと同じかそれ以上になるように PIR を設定する必要があります。

- **PBS** - Peak Burst Size。バイト数を計測する場合、PBS は、PIR に関連して、パケットサイズの正常な境界を越えているパケットを特定するために使用されます。IP フローで予想される最も大きい IP パケットを受け入れるために、PBS を設定する必要があります。

srTCM - Single Rate Three Color Marker。これは、trTTCM と共にメータリングおよびパケットフローをマーキングするためにスイッチで可能な 2 つの方式です。srTCM は、設定された CBS と EBS に基づいて IP パケットフローをマークします。CBS に到達しないパケットフローは、緑色にマークされ、EBS ではなく CBS を超過している場合、黄色にマークされ、EBS を超過している場合、赤色にマークされます。

CBS - Committed Burst Size。バイト数を計測する場合、CBS は、CIR に関連して、パケットサイズの正常な境界を越えているパケットを特定するために使用されます。IP フローで予想される最も大きい IP パケットを受け入れるために、CBS を設定する必要があります。

EBS - Excess Burst Size。バイト数を計測する場合、EBS は、CIR に関連して、パケットサイズの正常な境界を越えているパケットを特定するために使用されます。EBS は、CBS と同じかさらに大きいレートに設定されます。

DSCP - Differentiated Services Code Point。色が追加されるパケットヘッダの部分。入力パケットの「DSCP」フィールドを変更することが可能です。ACL フローメータ機能により、入力パケットのレートに基づいて IP パケットフローにカラーコードを付加することができます。以前に説明した通り、２つのフローメータリングのタイプ（trTCM および srTCM）を選択することができます。パケットフローがカラーコードに置かれる時、その色分けされたレートを超過したパケットで何をするべきかを決めることができます。

緑 - IP フローが緑色のモードである時、設定可能なパラメータは、パケットがその「DSCP」フィールドを変更できる「Conform」フィールドにて設定されます。これは ACL フローメータ機能で許容できるフローレートです。

黄 - IP フローが黄色のモードである時、設定可能なパラメータは、「Exceed」フィールドにて設定されます。超過したパケットを「Permit」（許可）または「Drop」（廃棄）するかを選択します。パケットの「DSCP」フィールドを変更ために選択します。

赤 - IP フローが赤色のモードである時、設定可能なパラメータは、「Violate」フィールドにて設定されます。

超過したパケットを「Permit」（許可）または「Drop」（廃棄）するかを選択します。パケットの「DSCP」フィールドを変更ために選択します。
また、「Counter」を指定することによって超過パケットをカウントできるように選択することができます。
「Counter」を有効にすると、アクセスプロファイル内のカウンタ設定は無効になります。どんな指定時間においても 1 つのフローメータに対して 2 つのカウンタのみ有効になります。

1. **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。

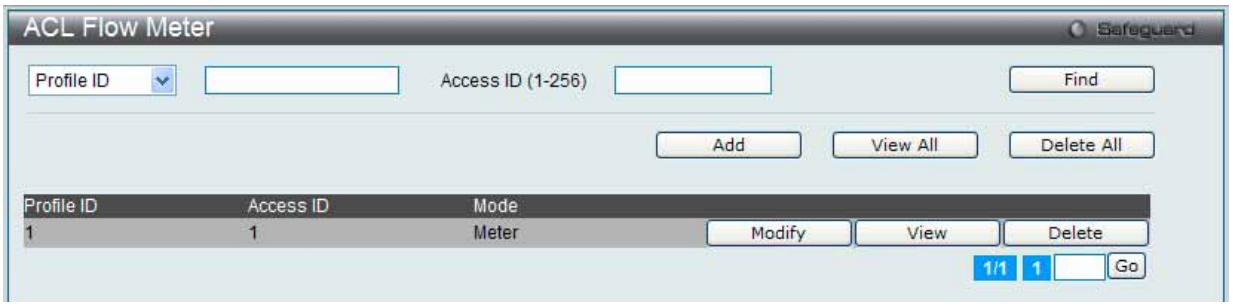


図 7.6-61　ACL Flow Meter 画面

2. 以下の項目を使用して設定および参照します。

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

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。

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

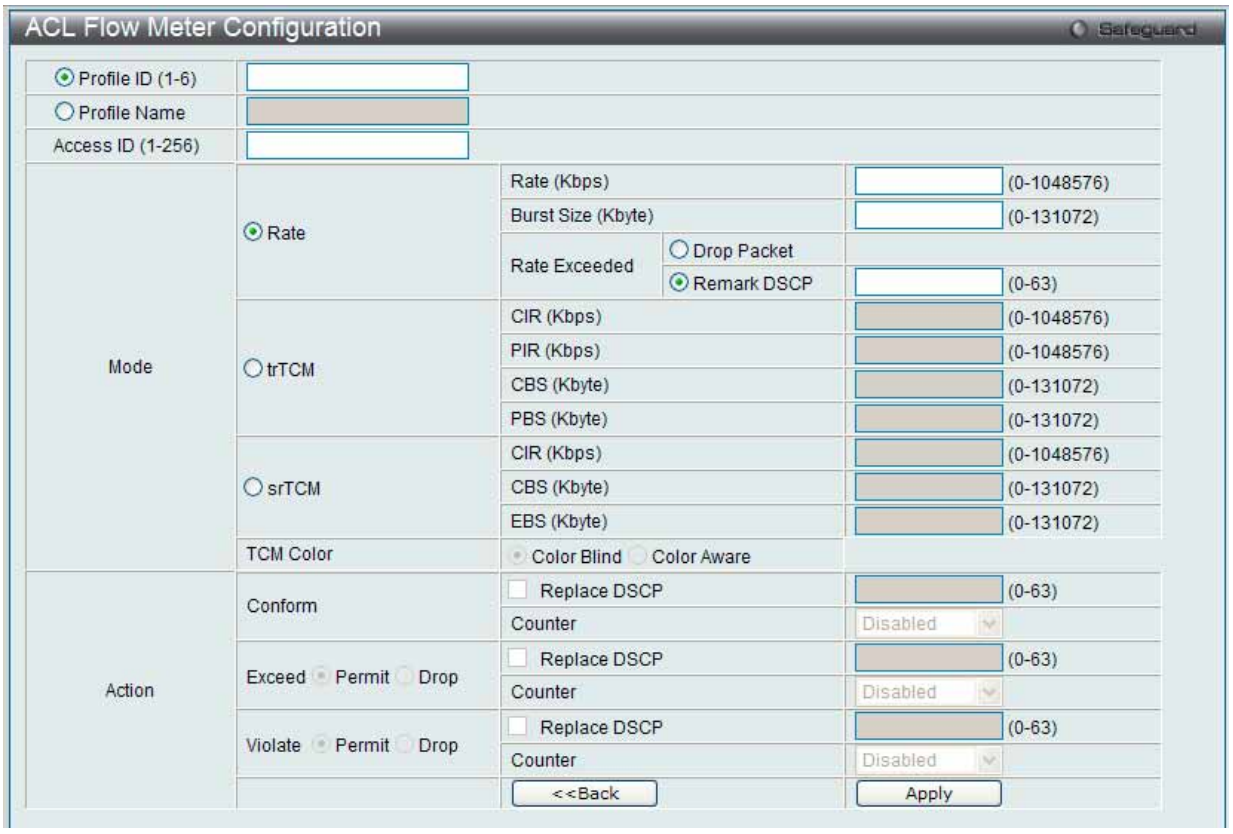


図 7.6-62　ACL Flow Meter Configuration 画面 - Add

2. 以下の項目を使用して設定および参照します。

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。
Profile Name	フローメータに対するプロファイル名を入力します。
Access ID (1-256)	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 1-256 の範囲で指定します。
Mode	Rate - シングルレート 2 カラーモードのレートを指定します。 • Rate - フローに規定する帯域幅を Kbps 単位で指定します。 • Burst Size - シングルレート 2 カラーモードにバーストサイズを指定します。単位は Kbps です。 • Rate Exceeded - シングルレート 2 カラーモードでコミットレートを超過したパケットへの操作を指定します。以下の一つの動作が行われます。: - Drop Packet - パケットを直ちに破棄します。 - Remark DSCP - 特定の DSCP をパケットにマークをつけます。高い優先度を持つパケットが破棄されるように設定されます。 trTCM -「2 レート 3 カラーモード」を指定します。 • CIR - コミット情報レートの値を入力します。単位は Kbps です。CIR は PIR 以下である必要があります。 • PIR - ピーク情報レートを指定します。単位は Kbps です。PIR は CIR 以上である必要があります。 • CBS -「コミットバーストサイズ」の値を入力します。単位は Kbps です。 • PBS - ピークバーストサイズの値を入力します。単位は Kbps です。 srTCM -「シングルレート 3 カラーモード」を指定します。 • CIR - コミット情報レートの値を入力します。単位は Kbps です。 • CBS -「コミットバーストサイズ」の値を入力します。単位は Kbps です。 • EBS -「超過バーストサイズ」を指定します。単位は Kbps です。
Action	Conform - 本フィールドは緑色のパケットフローを表します。緑色のパケットフローは、DSCP フィールドを本フィールドで指定された値に書き換える可能性があります。また、「Counter」パラメータを使用することで緑色のパケットをカウントするように選択することができます。 • Replace DSCP - 緑色のフローにあるパケットが本パラメータを使用し、DSCP 値を入力することで、DSCP 値を書き換えることが可能です。 • Counter - 緑色のフローにおいて指定された ACL エントリのパケットカウンタを「Enabled」（有効）または「Disabled」（無効）にします。 Un-conform - 不適合 (黄色または赤) パケットの DSCP を変更します。 • Replace DSCP - 赤色のフローにあるパケットが本パラメータを使用し、DSCP 値を入力することで、DSCP 値を書き換えることが可能です。 Exceed - 本フィールドは黄色のパケットフローを表します。黄色のパケットフローは超過パケットを許可または廃棄します。これらのパケットの「DSCP」フィールドを割り当てられたフィールドに新しい DSCP 値を入れることで交換することができます。 • Counter - 黄色のフローにおいて指定された ACL エントリのパケットカウンタを「Enabled」（有効）または「Disabled」（無効）にします。 Violate - 本フィールドは赤色のパケットフローを表します。赤色のパケットフローは超過パケットを許可または廃棄します。これらのパケットの「DSCP」フィールドを割り当てられたフィールドに新しい DSCP 値を入れることで交換することができます。 • Counter - 赤色のフローにおいて指定された ACL エントリのパケットカウンタを「Enabled」（有効）または「Disabled」（無効）にします。

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

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

エントリの変更

1. 対応する「Modify」ボタンをクリックし、以下の画面を表示します。

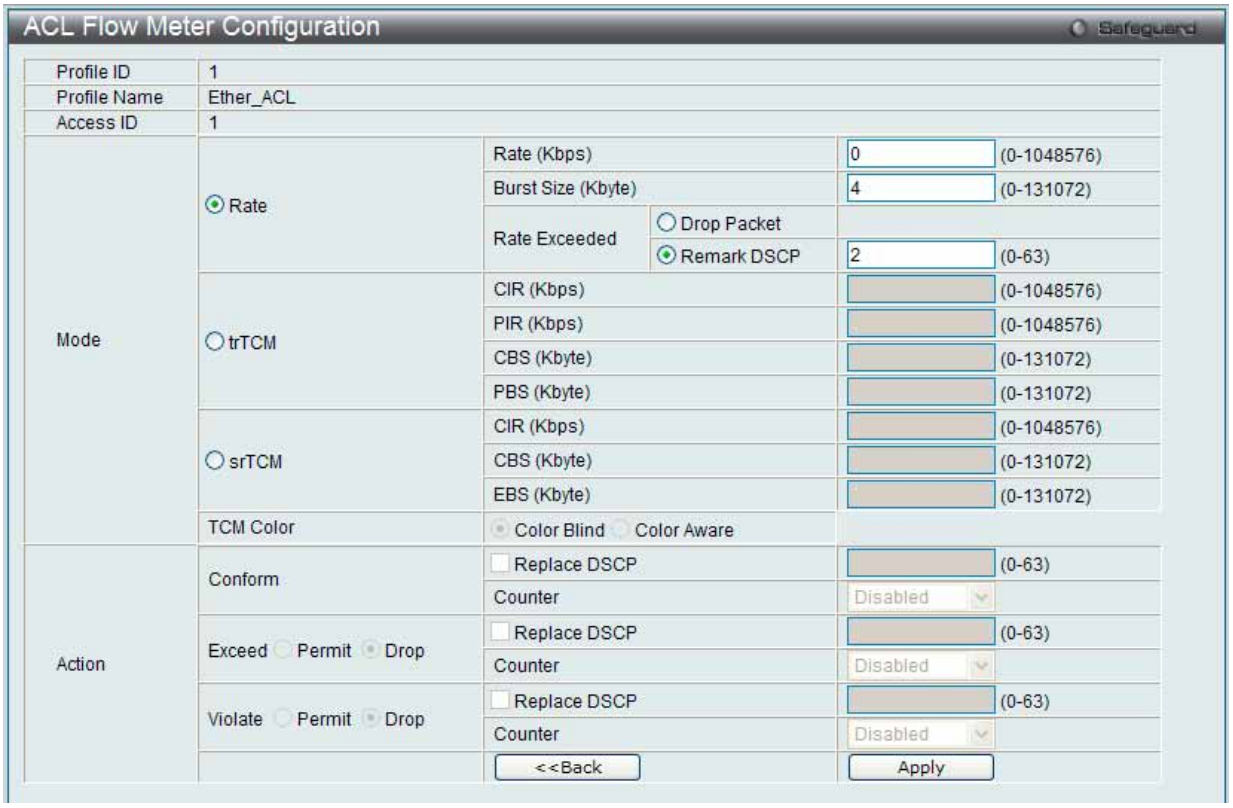


図 7.6-63　ACL Flow Meter Configuration 画面 - Modify

2. 以下の項目を使用して設定および参照します。

項目	説明
Mode	Rate - シングルレート 2 カラーモードのレートを指定します。 • Rate - フローに規定する帯域幅を Kbps 単位で指定します。 • Burst Size - シングルレート 2 カラーモードにバーストサイズを指定します。単位は Kbps です。 • Rate Exceeded - シングルレート 2 カラーモードでコミットレートを超過したパケットへの操作を指定します。以下の一つの動作が行われます。: - Drop Packet - パケットを直ちに破棄します。 - Remark DSCP - 特定の DSCP をパケットにマークをつけます。高い優先度を持つパケットが破棄されるように設定されます。

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

「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。

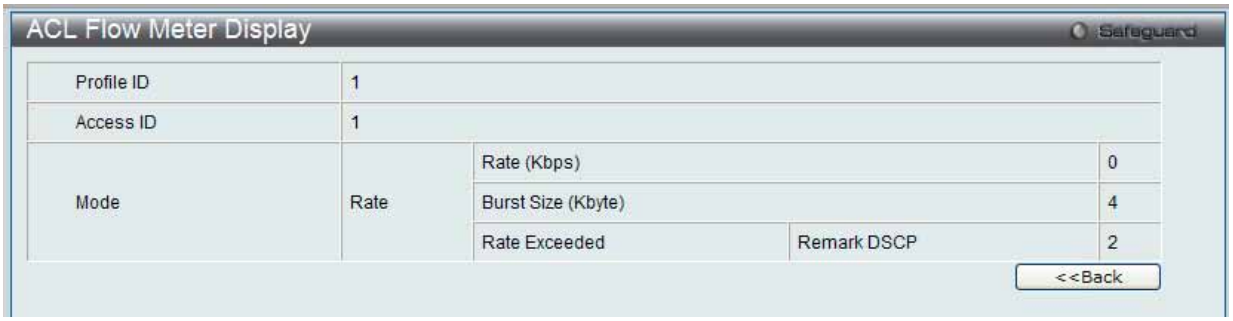


図 7.6-64　ACL Flow Meter Display 画面

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

Egress Access Profile List（Egress アクセスプロファイルリスト）

Egress ACL は、スイッチから送出される場合に、フローごとのパケット処理を実行します。スイッチは、3 つのプロファイルタイプ（イーサネット ACL、IPv4 ACL、および IPv6 ACL）をサポートしています。

1. **ACL > Egress 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。

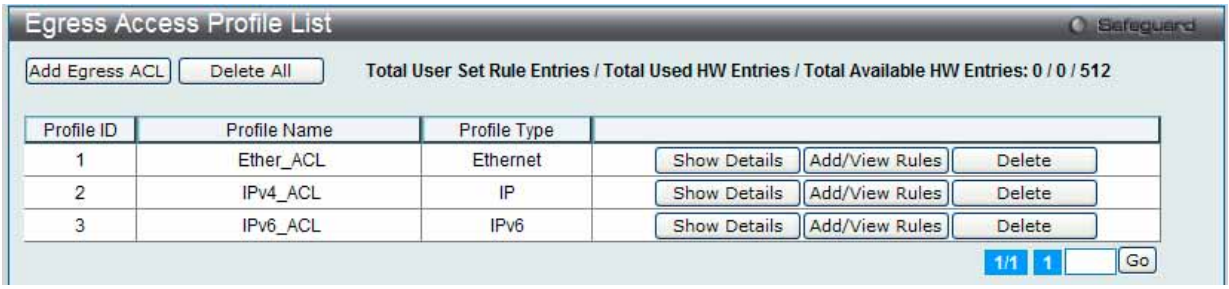


図 7.6-65　Egress Access Profile List 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Add Egress Profile	Egress アクセスプロファイルリストにエントリを追加します。
Delete All	テーブルからすべてのアクセスプロファイルを削除します。
Show Details	指定プロファイル ID エントリに関する情報を表示します。
Add/View Rules	指定プロファイル ID の ACL ルールの参照または追加を行います。
Delete	指定エントリを削除します。
Go	複数ページが存在する場合は、ページ番号を入力後、クリックして、特定のページへ移動します。

以下の 3 つの「Add Egress ACL」画面があります。
- イーサネットプロファイル設定
- IPv6 アドレスベースのプロファイル設定
- IPv4 アドレスベースのプロファイル設定

アクセスプロファイルリストの作成（Ethernet）

イーサネット用の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 > Egress 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。

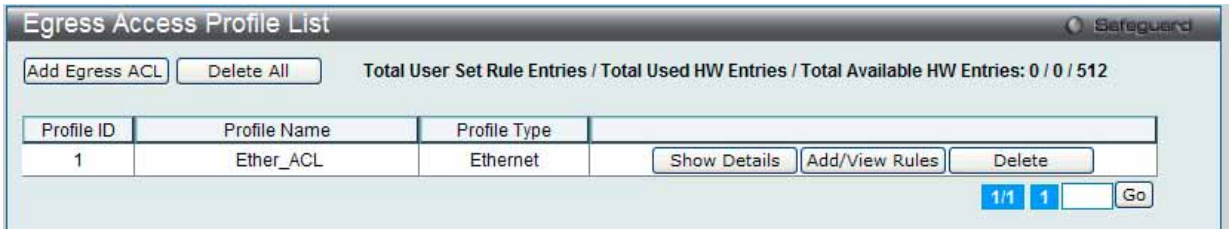


図 7.6-66　Egress Access Profile List 画面

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 Egress ACL」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

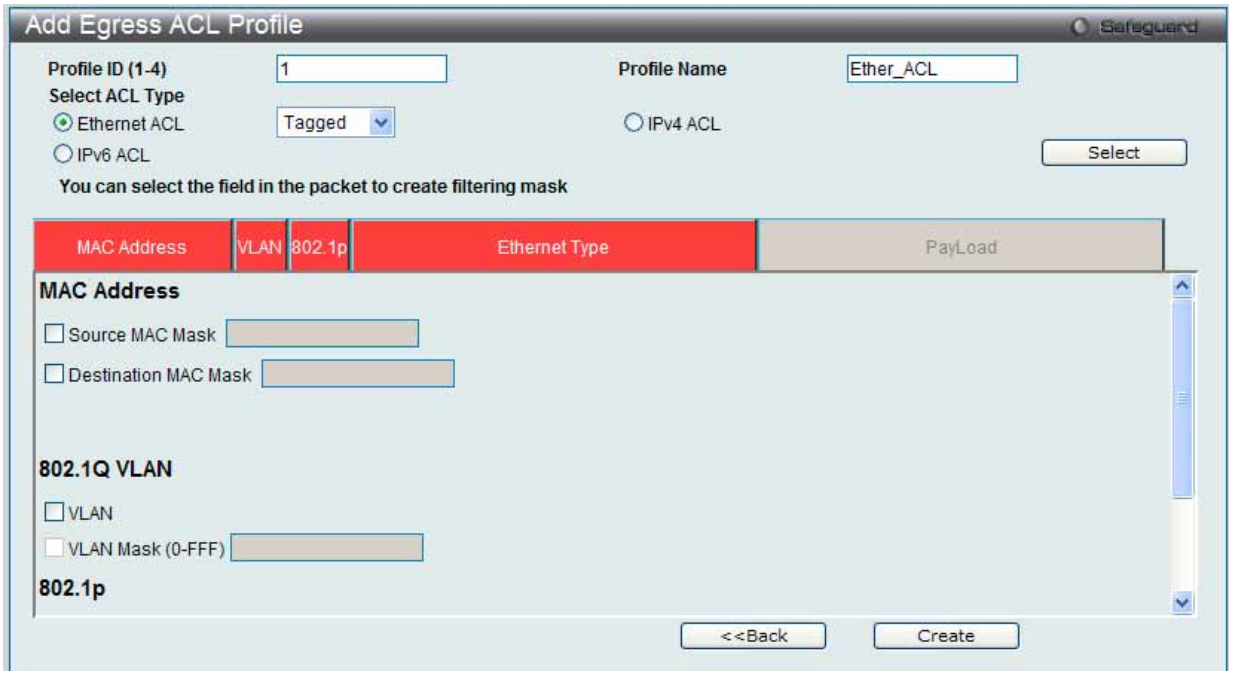


図 7.6-67　Add Egress ACL Profile - Ethernet ACL 画面

「Profile ID」でプロファイル番号を 1-4 から選択し、「Select ACL Type」で「Ethernet ACL」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
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 4 が指定できます。
Profile Name	作成したプロファイルにプロファイル名を入力します。
Select ACL Type	Ethernet（MAC アドレス）、IPv4 アドレス、または IPv6 アドレス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。例 : FF-FF-FF-FF-FF-FF • 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。例 : FF-FF-FF-FF-FF-FF
802.1Q VLAN	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	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	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。

「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

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 7.6-68　Egress Access Profile Detail Information - Ethernet 画面

「Show All Profiles」ボタンをクリックすると、「Egress 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。

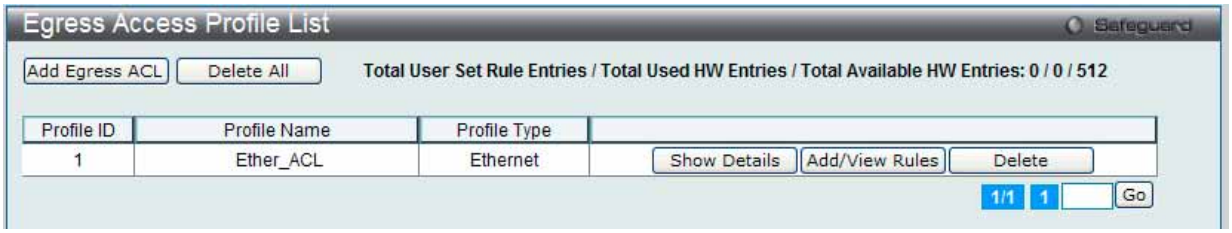


図 7.6-69　Egress Access Profile List 画面

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。

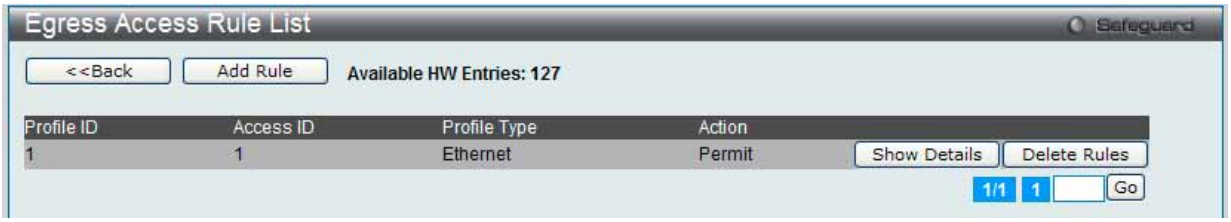


図 7.6-70　Egress Access Rule List - Ethernet 画面

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

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。

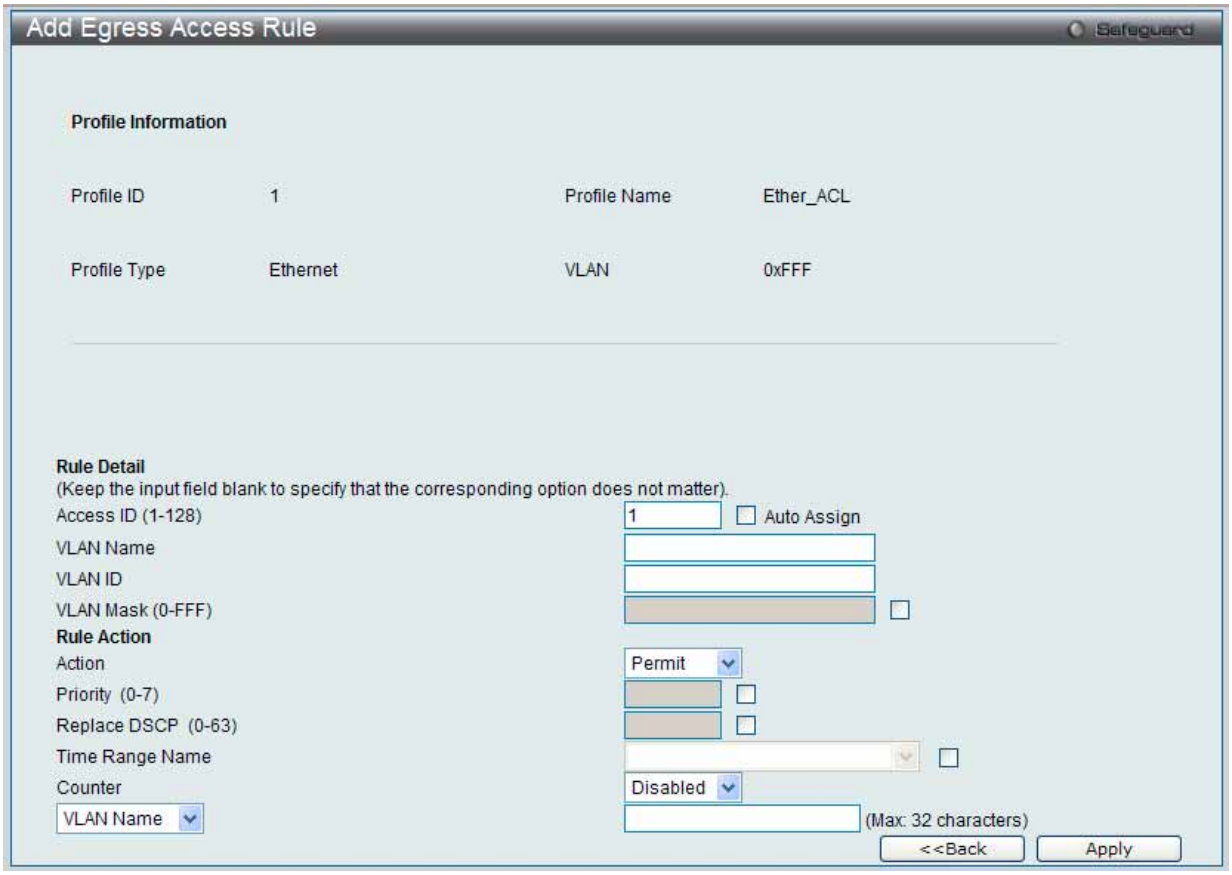


図 7.6-71　Add Access Rule - Ethernet 画面

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 (1-128)	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 128 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	VLAN ID 番号を指定します。
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。）
Rule Action	
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、以下のフィールド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を送信せずにフィルタリングします。
Priority (0-7)	スイッチが設定した 802.1p デフォルトプライオリティを上書きしたい場合に指定します。このプライオリティにより転送されたパケットがどの CoS キューを使用するかが決まります。この欄を指定するとパケットはこのプライオリティを割り当てられ、対応した CoS キューに転送されます。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「7.5　QoS（QoS 機能の設定）」（189 ページ）を参照してください。
Replace Priority	条件に合ったパケットの DSCP 値は指定した値に入れ替わります。
Replace DSCP (0-63)	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フィールド内に指定した値に書き換えます。ACL ルールがプライオリティと IPv4 パケットの両方を変更するために追加されても、チップの制限のためそれらの一方しか変更できません。プライオリティと DSCP の両方が変更されるように設定されている場合は、現在のプライオリティを変更します。
Replace ToS Precedence (0-7)	出力パケットの IP 優先度が新しい値に変更されます。操作の優先度なしで使用すると、デフォルト TC にパケットは送信されます。
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。
Port	アクセスルールに適用するポート番号を指定します。
Port Group ID	アクセスルールに適用するポートグループ ID を指定します。
Port Group Name	アクセスルールに適用するグループ名を指定します。
VLAN Name	アクセスルールに適用する VLAN 名を指定します。
VLAN ID	アクセスルールに適用する VLAN ID を指定します。

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

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。

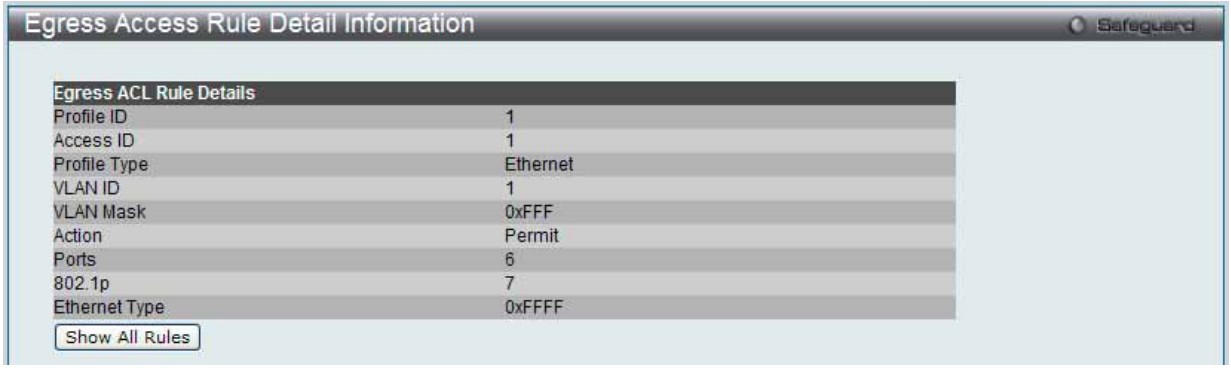


図 7.6-72　Egress Access Profile Detail Information - Ethernet 画面

「Show All Profiles」ボタンをクリックすると、「Access Profile List」画面に戻ります。

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 > Egress 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。

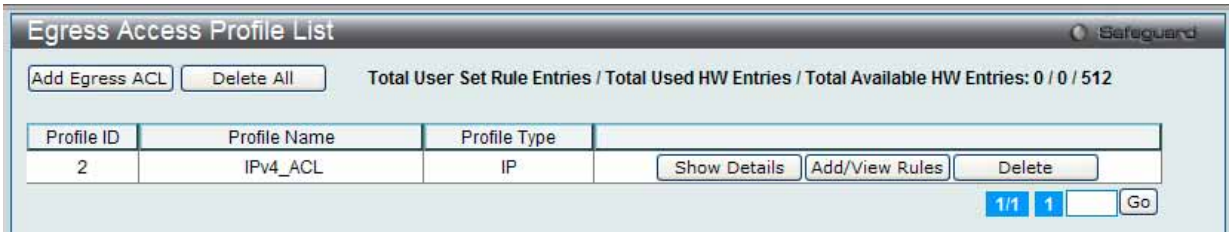


図 7.6-73　Egress Access Profile List 画面

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 7.6-74　Add Egress ACL Profile - IPv4 ACL 画面

「Profile ID」でプロファイル番号を 1-4 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
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 4 が指定できます。
Profile Name	作成したプロファイルにプロファイル名を入力します。
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	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。
IPv4 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。
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。
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。例 : 255.255.255.255 - 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。例 : 255.255.255.255
Protocol ID	マスクしたいパケットヘッダの Protocol ID Mask（0-FF）を指定します。 • User Define - レイヤ 4 パ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。

「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

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、「Egress 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 7.6-75　Egress Access Profile Detail Information - IPv4 画面

「Show All Profiles」ボタンをクリックすると、「Egress 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. 「Egress Access Profile List」画面を表示します。

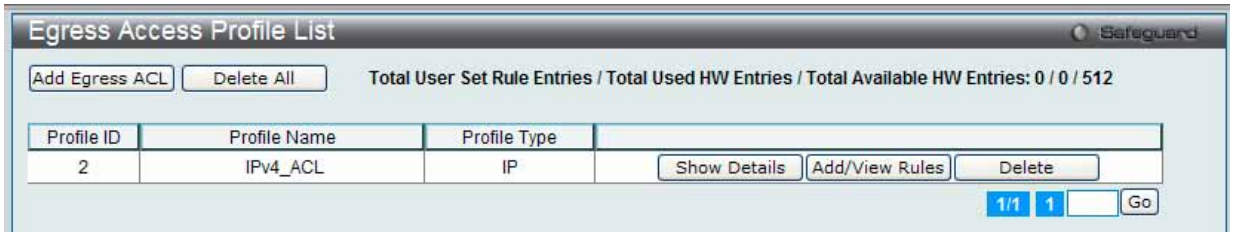


図 7.6-76　Egress Access Profile List 画面

2. 「Egress 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。

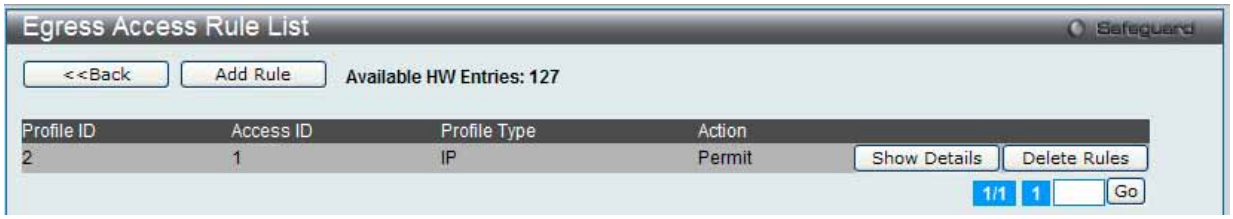


図 7.6-77　Egress Access Rule List - IPv4 画面

「<<Back」をボタンをクリックして前のページに戻ります。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、指定ページへ移動します。

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。

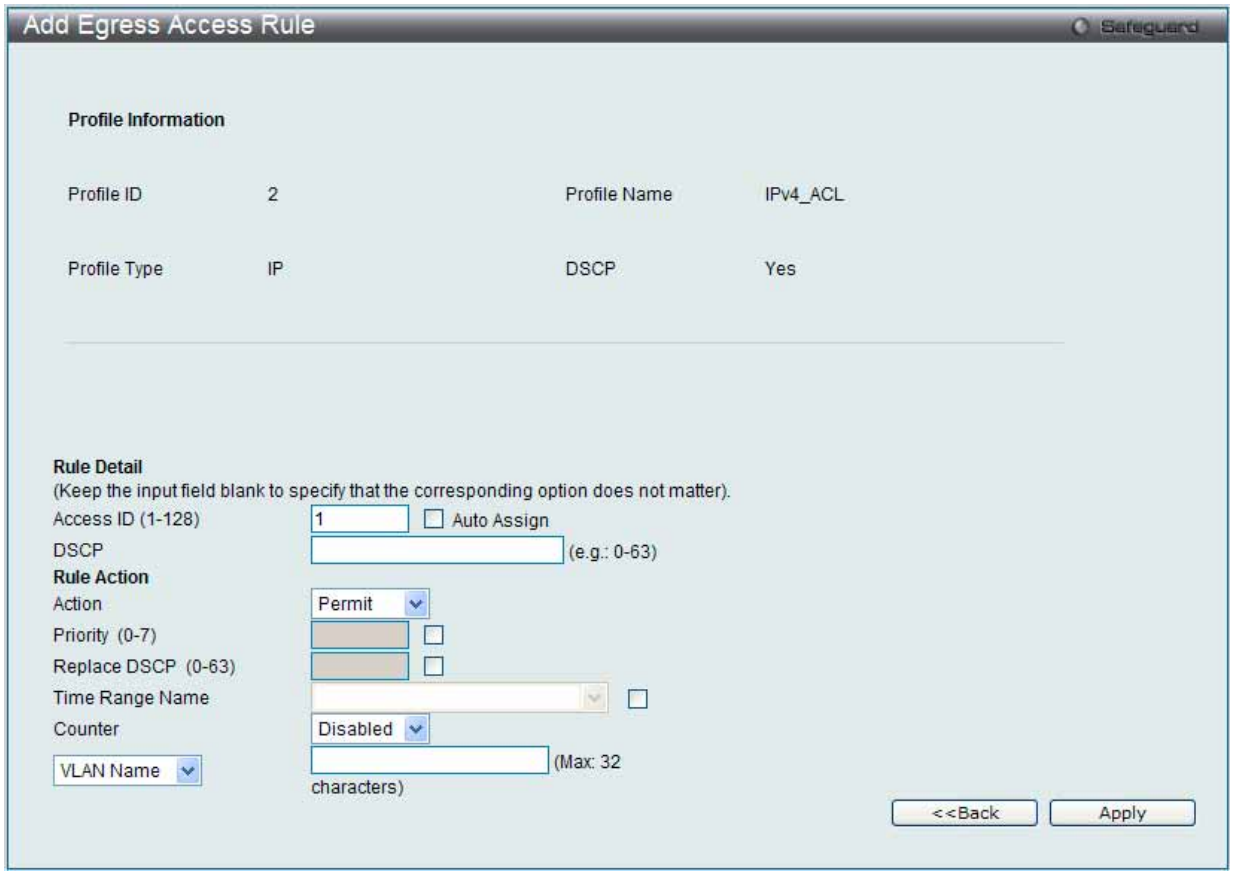


図 7.6-78　Add Egress Access Rule - IPv4 画面

以下の項目を使用して設定および参照します。

項目	説明
Rule Detail	
Access ID (1-128)	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 128 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 を入力します。
VLAN Mask (FFF)	VLAN 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 Address 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 Address 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。
Priority (0-7)	スイッチにより設定された 802.1p デフォルトプライオリティを上書きしたい場合に指定します。このプライオリティにより転送されたパケットがどの CoS キューを使用するかが決まります。この欄を指定するとパケットはこのプライオリティを割り当てられ、対応した CoS キューに転送されます。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「7.5　QoS（QoS 機能の設定）」（189 ページ）を参照してください。
Replace Priority	条件に合ったパケットの DSCP 値は指定した値に入れ替わります。
Replace DSCP (0-63)	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フィールド内に指定した値に書き換えます。ACL ルールがプライオリティと IPv4 パケットの両方を変更するために追加されても、チップの制限のためそれらの一方しか変更できません。プライオリティと DSCP の両方が変更されるように設定されている場合は、現在のプライオリティを変更します。
Replace ToS Precedence (0-7)	出力パケットの IP 優先度が新しい値に変更されます。操作の優先度なしで使用すると、デフォルト TC にパケットは送信されます。
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。

項目	説明
Port	アクセスルールに適用するポート番号を指定します。
Port Group ID	アクセスルールに適用するポートグループ ID を指定します。
Port Group Name	アクセスルールに適用するグループ名を指定します。
VLAN Name	アクセスルールに適用する VLAN 名を指定します。
VLAN ID	アクセスルールに適用する VLAN ID 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。
「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

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。

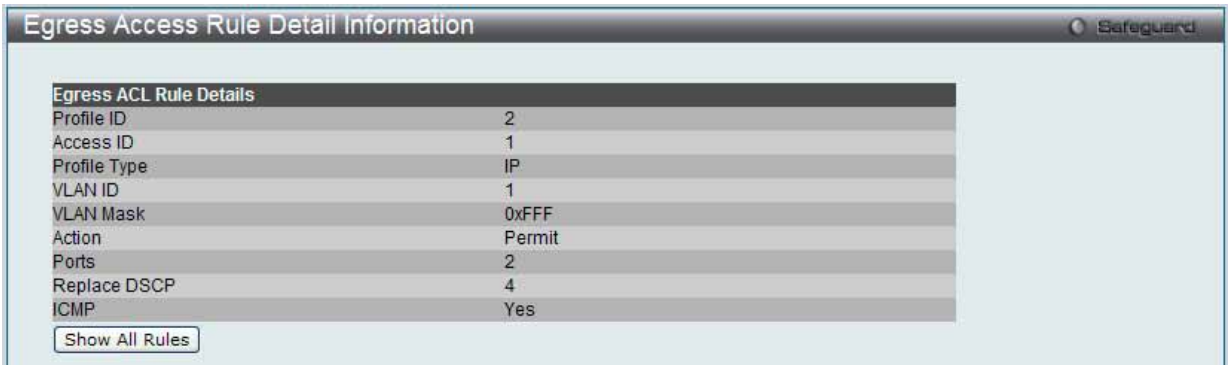


図 7.6-79　Egress Access Rule Detail Information - IP 画面

「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 > Egress 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。

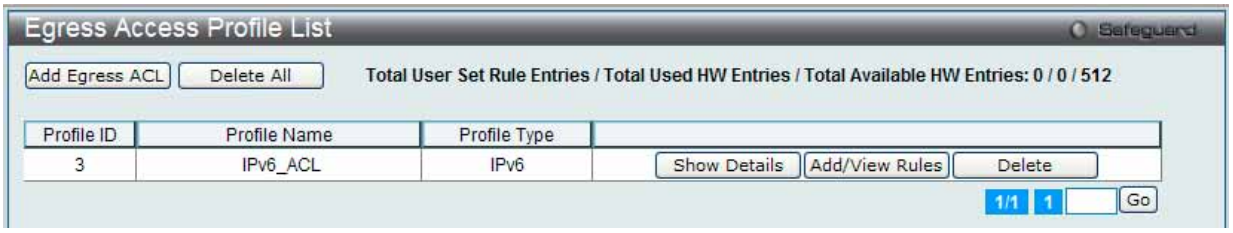


図 7.6-80　Egress Access Profile List 画面

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

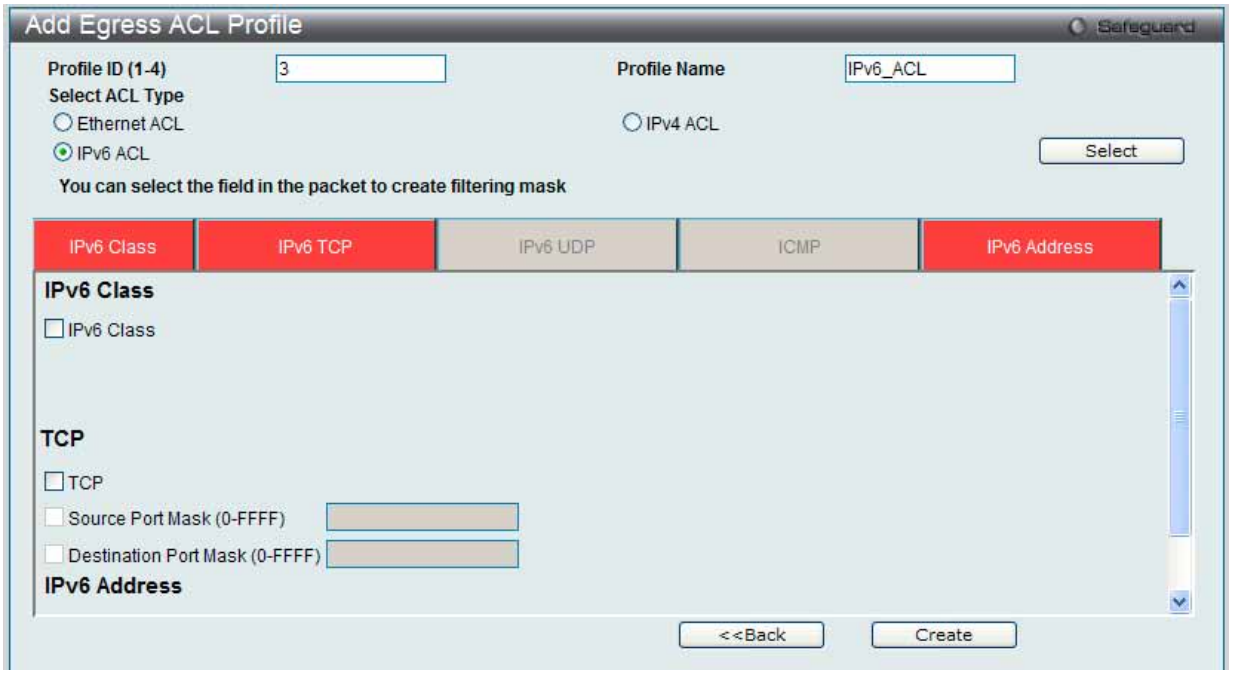


図 7.6-81　Add Egress ACL Profile - IPv6 ACL 画面

「Profile ID」でプロファイル番号を 1-6 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
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 4 を指定できます。
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。
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。
IPv6 Address	• IPv6 Source Address - 対応するボックスをチェックして、IP アドレスマスク（例 255.255.255.255）を入力することで送信元 IPv6 アドレスのマスクアドレスを指定します。 • IPv6 Destination Address - 対応するボックスをチェックして、IP アドレスマスク（例 255.255.255.255）を入力することで送信先 IPv6 アドレスのマスクアドレスを指定します。

「Create」ボタンをクリックし、設定を適用します。
「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

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 7.6-82　Egress 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. 「Egress Access Profile List」画面を表示します。

図 7.6-83　Egress　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 7.6-84　Egress Access Rule List - IPv6 画面

「<<Back」をボタンをクリックして前のページに戻ります。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、指定ページへ移動します。

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。

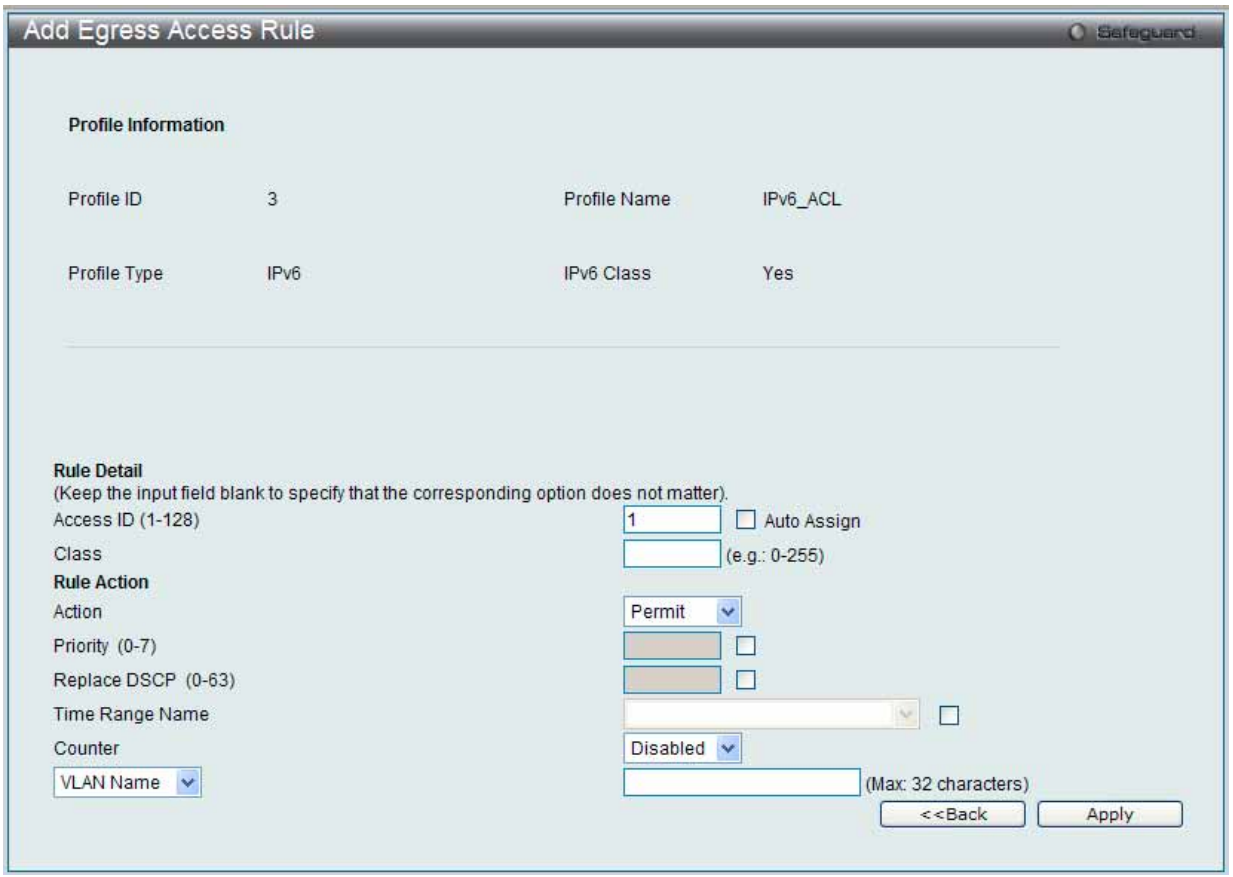


図 7.6-85　Add Egress Access Rule - IPv6 画面

以下の項目を使用して設定および参照します。

項目	説明
Rule Detail	
Access ID (1-128)	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 128 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。
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。
Priority (0-7)	スイッチにより設定された 802.1p デフォルトプライオリティを上書きしたい場合に指定します。このプライオリティにより転送されたパケットがどの CoS キューを使用するかが決まります。この欄を指定するとパケットはこのプライオリティを割り当てられ、対応した CoS キューに転送されます。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「7.5　QoS（QoS 機能の設定）」（189 ページ）を参照してください。
Replace Priority	条件に合ったパケットの DSCP 値は指定した値に入れ替わります。
Replace DSCP (0-63)	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 をボックスの右側の欄に指定した値に書き換えます。ACL ルールがプライオリティと IPv4 パケットの両方を変更するために追加されても、チップの制限のためそれらの一方しか変更できません。プライオリティと DSCP の両方が変更されるように設定されている場合は、現在のプライオリティを変更します。
Replace ToS Precedence (0-7)	出力パケットの IP 優先度が新しい値に変更されます。操作の優先度なしで使用すると、デフォルト TC にパケットは送信されます。
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。
Port	アクセスルールに適用するポート番号を指定します。
Port Group ID	アクセスルールに適用するポートグループ ID を指定します。
Port Group Name	アクセスルールに適用するグループ名を指定します。
VLAN Name	アクセスルールに適用する VLAN 名を指定します。
VLAN ID	アクセスルールに適用する VLAN ID 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。
「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

作成したルールの詳細の参照

「Egress 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。

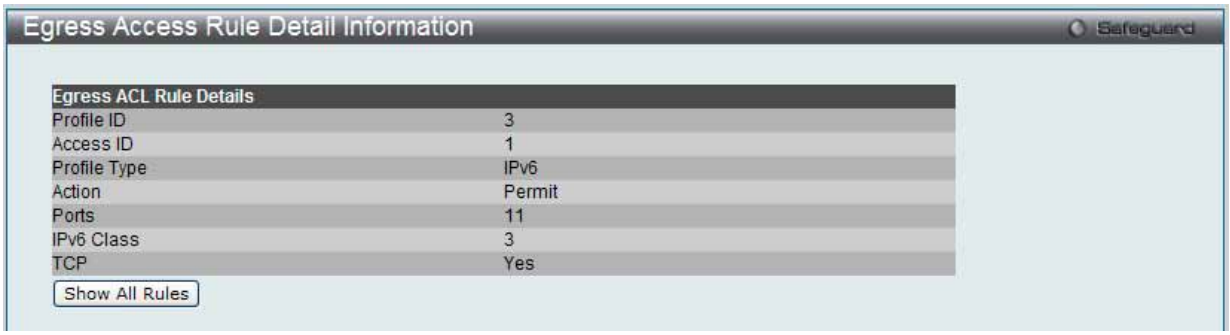


図 7.6-86　Egress Access Rule Detail Information - IPv6 画面

「Show All Rules」ボタンをクリックすると、「Egress Access Rule List」画面に戻ります。

Egress ACL Flow Meter（Egress ACL フローメータリング）

Egress アクセスプロファイルおよびルールに基づいてパケットフローベースのメータリングを設定します。

ACL > Egress 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。

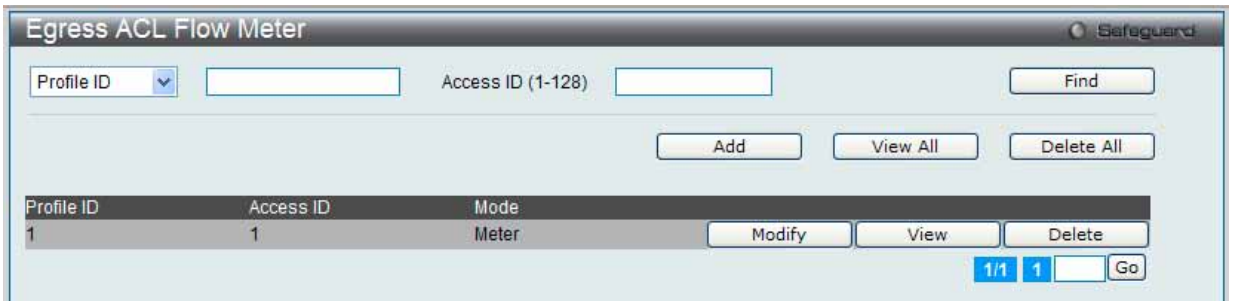


図 7.6-87　Egress ACL Flow Meter 画面

以下の項目を使用して設定および参照します。

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。
Profile Name	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名を指定します。
Access ID (1-128)	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。

エントリの追加

「Add」ボタンをクリックし、以下の画面を表示します。

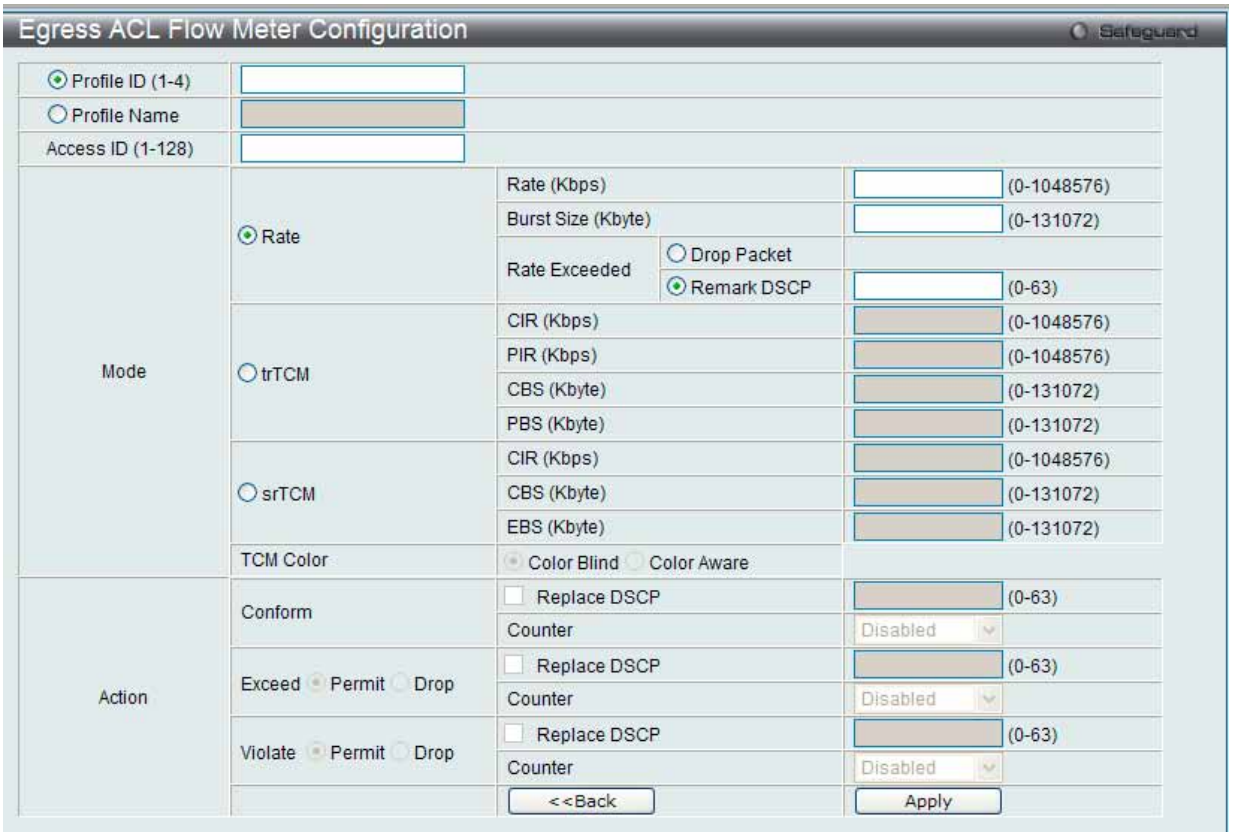


図 7.6-88　Egress　ACL Flow Meter Configuration 画面 - Add

以下の項目を使用して設定および参照します。

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。
Profile Name	フローメータに対するプロファイル名を入力します。
Access ID (1-128)	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 1-128 の範囲で指定します。
Mode	Rate - シングルレート 2 カラーモードのレートを指定します。 • Rate - フローに規定する帯域幅を Kbps 単位で指定します。 • Burst Size - シングルレート 2 カラーモードにバーストサイズを指定します。単位は Kbps です。 • Rate Exceeded - シングルレート 2 カラーモードでコミットレートを超過したパケットへの操作を指定します。以下の一つの動作が行われます。: - Drop Packet - パケットを直ちに破棄します。 - Remark DSCP - 特定の DSCP をパケットにマークをつけます。高い優先度を持つパケットが破棄されるように設定されます。 trTCM -「2 レート 3 カラーモード」を指定します。 • CIR - コミット情報レートの値を入力します。単位は Kbps です。CIR は PIR 以下である必要があります。 • PIR - ピーク情報レートを指定します。単位は Kbps です。PIR は CIR 以上である必要があります。 • CBS -「コミットバーストサイズ」の値を入力します。単位は Kbps です。 • PBS - ピークバーストサイズの値を入力します。単位は Kbps です。 srTCM -「シングルレート 3 カラーモード」を指定します。 • CIR - コミット情報レートの値を入力します。単位は Kbps です。 • CBS -「コミットバーストサイズ」の値を入力します。単位は Kbps です。 • EBS -「超過バーストサイズ」を指定します。単位は Kbps です。
Action	Conform - 本フィールドは緑色のパケットフローを表します。緑色のパケットフローは、DSCP フィールドを本フィールドで指定された値に書き換える可能性があります。また、「Counter」パラメータを使用することで緑色のパケットをカウントするように選択することができます。 • Replace DSCP - 緑色のフローにあるパケットが本パラメータを使用し、DSCP 値を入力することで、DSCP 値を書き換えることが可能です。 • Counter - 緑色のフローにおいて指定された ACL エントリのパケットカウンタを「Enabled」（有効）または「Disabled」（無効）にします。 Un-conform - 不適合 (黄色または赤) パケットの DSCP を変更します。 • Replace DSCP - 赤色のフローにあるパケットが本パラメータを使用し、DSCP 値を入力することで、DSCP 値を書き換えることが可能です。 Exceed - 本フィールドは黄色のパケットフローを表します。黄色のパケットフローは超過パケットを許可または廃棄します。これらのパケットの「DSCP」フィールドを割り当てられたフィールドに新しい DSCP 値を入れることで交換することができます。 • Counter - 黄色のフローにおいて指定された ACL エントリのパケットカウンタを「Enabled」（有効）または「Disabled」（無効）にします。 Violate - 本フィールドは赤色のパケットフローを表します。赤色のパケットフローは超過パケットを許可または廃棄します。これらのパケットの「DSCP」フィールドを割り当てられたフィールドに新しい DSCP 値を入れることで交換することができます。 • Counter - 赤色のフローにおいて指定された ACL エントリのパケットカウンタを「Enabled」（有効）または「Disabled」（無効）にします。

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

「Egress ACL Flow Meter」画面に戻るためには、「<<Back」ボタンをクリックします。

エントリの変更

1. 対応する「Modify」ボタンをクリックし、以下の画面を表示します。

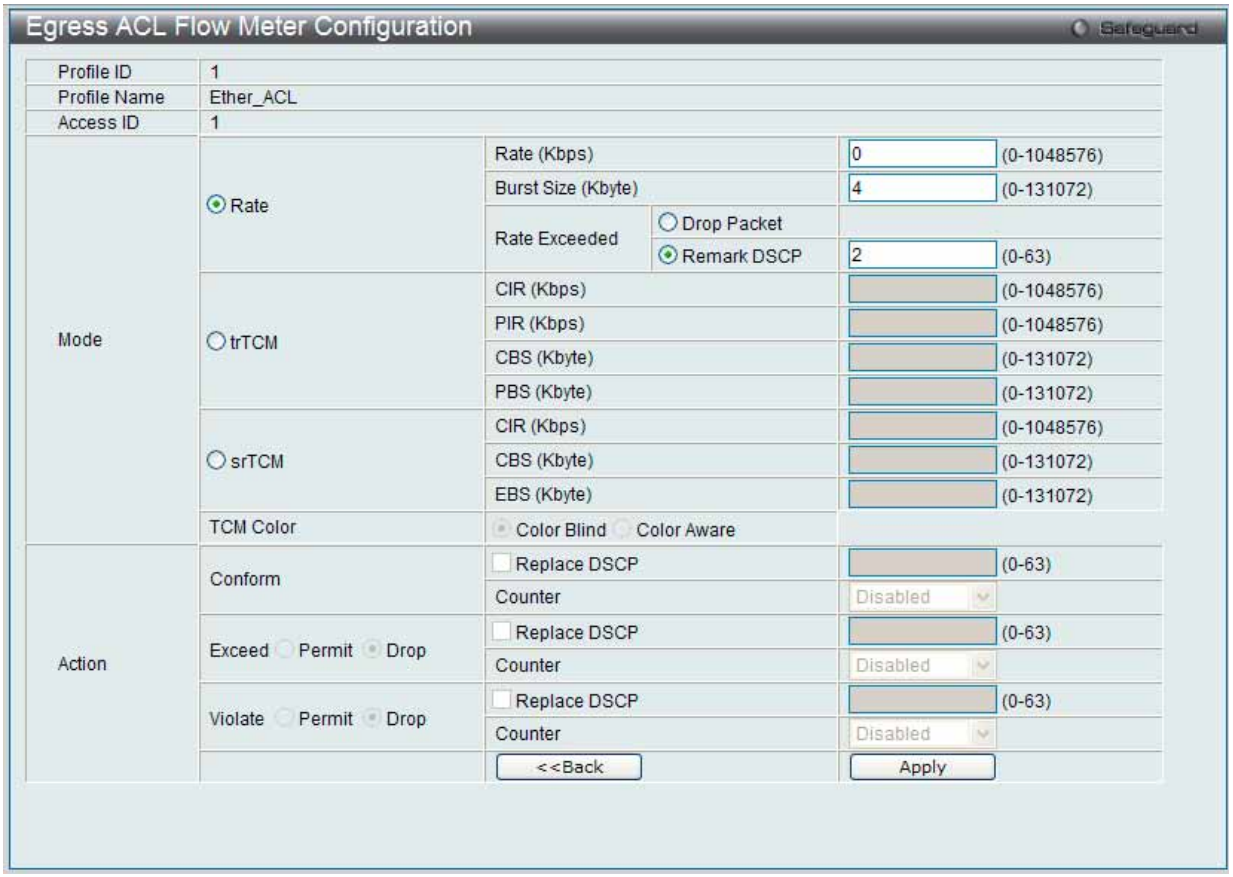


図 7.6-89　Egress ACL Flow Meter Configuration 画面 - Modify

2. 以下の項目を使用して設定および参照します。

項目	説明
Mode	Rate - シングルレート 2 カラーモードのレートを指定します。 • Rate - フローに規定する帯域幅を Kbps 単位で指定します。 • Burst Size - シングルレート 2 カラーモードにバーストサイズを指定します。単位は Kbps です。 • Rate Exceeded - シングルレート 2 カラーモードでコミットレートを超過したパケットへの操作を指定します。以下の一つの動作が行われます。: - Drop Packet - パケットを直ちに破棄します。 - Remark DSCP - 特定の DSCP をパケットにマークをつけます。高い優先度を持つパケットが破棄されるように設定されます。

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

「Egress 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。

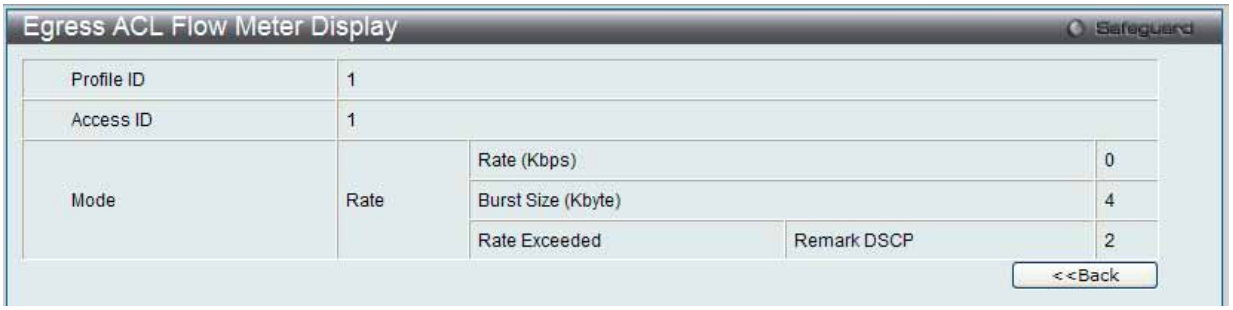


図 7.6-90　Egress ACL Flow Meter Display 画面

「Egress ACL Flow Meter」画面に戻るためには、「<<Back」ボタンをクリックします。

7.7 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
802.1X（802.1X 設定）	802.1X 認証を設定します。以下のメニューがあります。: 802.1X Global Settings（802.1X グローバル設定）、802.1X Port Settings（802.1X ポート設定）、802.1X User Settings（802.1X ユーザ設定）、Guest VLAN（ゲスト VLAN の設定）、Authenticator State（オーセンティケータの状態）、Authenticator Statistics（オーセンティケータ統計情報）、Authenticator Session Statistics（オーセンティケータセッション統計情報）、Authenticator Diagnostics（オーセンティケータ診断）、Initialize Port(s)（初期化ポート）、Reauthenticate Port(s)（再認証ポート）	257
RADIUS（RADIUS 設定）	RADIUS サーバの設定を行います。以下のメニューがあります。 Authentication RADIUS Server Settings（認証 RADIUS サーバ設定）、RADIUS Accounting Setting（RADIUS アカウンティング設定）、RADIUS Authentication（RADIUS 認証）、RADIUS Account Client（RADIUS アカウンティングクライアント）	270
IP-MAC-Port Binding（IMPB : IP-MAC- ポートバインディング）	IP アドレス、MAC アドレスおよびポートを結合し、レイヤ間通信を行います。以下のメニューがあります。 IMPB Global Settings（IMPB グローバル設定）、IMPB Port Settings（IMPB ポート設定）、IMPB Entry Settings（IMPB エントリ設定）、MAC Block List（MAC ブロックリスト）、DHCP Snooping（DHCP Snooping 設定）、DHCP Snooping Entries（DHCP Snooping エントリ）	274
MAC Based Access Control（MAC ベースアクセスコントロール）	MAC アドレス認証機能を設定します。以下のメニューがあります。 MAC-based Access Control Settings（MAC ベースアクセスコントロール設定）、MAC-based Access Control Local Settings（MAC ベースアクセスコントロール ローカル設定）、MAC-based Access Control Authentication State（MAC ベースアクセスコントロールの認証状態）	279
Compound Authentication（コンパウンド認証）	コンパウンド認証方式を設定します。以下のメニューがあります。 Compound Authentication Settings（コンパウンド認証設定）、Compound Authentication Guest VLAN Settings（コンパウンド認証ゲスト VLAN の設定）	283
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。以下のメニューがあります。 Port Security Settings（ポートセキュリティの設定）、Port Security VLAN Settings（ポートセキュリティ VLAN 設定）、Port Security Entries（ポートセキュリティエントリ）	285
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。	289
BPDU Attack Protection（BPDU アタック防止設定）	ポートに BPDU 防止機能を設定します。	290
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。	291
Traffic Segmentation Settings（トラフィックセグメンテーション設定）	ポートのトラフィックフローを制限します。	292
NetBIOS Filtering Setting（NetBIOS フィルタリング設定）	NetBIOS フィルタ設定を行います。	293
DHCP Server Screening（DHCP サーバスクリーニング）	不正な DHCP サーバへのアクセスを拒否します。以下のメニューがあります。 DHCP Server Screening Port Settings（DHCP サーバスクリーニング設定）、DHCP Offer Permit Entry Settings（DHCP オファー許可エントリ設定）	294
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。以下のメニューがあります。 Enable Admin（管理者レベルの認証）、Authentication Policy Settings（認証ポリシー設定）、Application Authentication Settings（アプリケーションの認証設定）、Authentication Server Group Settings（認証サーバグループ設定）、Authentication Server Settings（認証サーバ設定）、Login Method Lists Settings（ログインメソッドリスト）、Enable Method Lists Settings（メソッドリストの有効化）、Local Enable Password Settings（ローカルユーザパスワード設定）	296
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。	304
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。以下のメニューがあります。: SSH Settings（SSH サーバ設定）、SSH Authentication Method and Algorithm Settings（SSH 認証モードとアルゴリズム設定）、SSH User Authentication Lists（SSH ユーザ認証リスト）	306
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。	309
Safeguard Engine Setting（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。	310
Captive Portal (CP)	有線 / 無線ユーザ両方についてネットワークへの接続性を制御します。以下のメニューがあります。: CP Configuration（CP 設定）、CP Web ページのカスタマイズ、Local User（ローカルユーザ）、Interface Association（インタフェースアソシエーション）、CP Status（CP 状態）、Interface Status（インタフェース状態）、Client Connection Status（クライアントの接続状態）、SNMP Trap Configuration（SNMP トラップ設定）	312

802.1X（802.1X 設定）

Port Access Entity（ポートアクセスエンティティ）

802.1X ポートベースおよび MAC ベースの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。

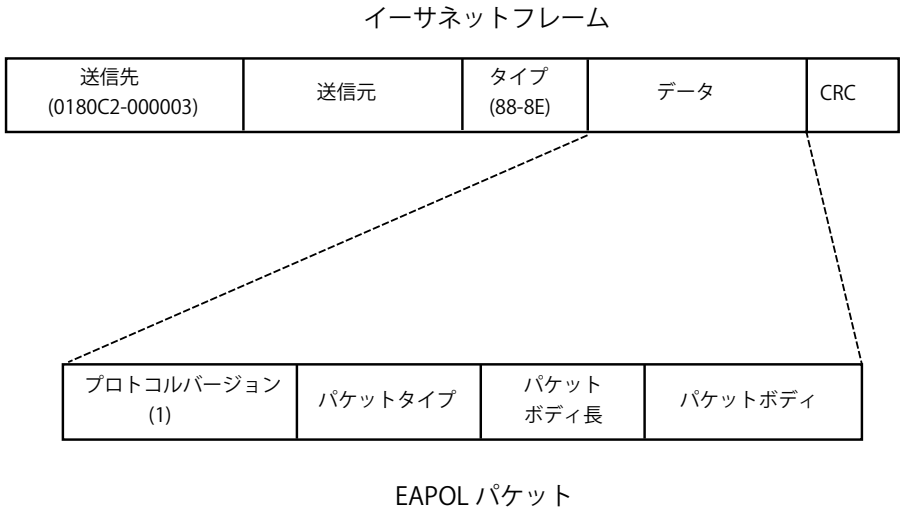


図 7.7-1　EAPOL パケット

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。

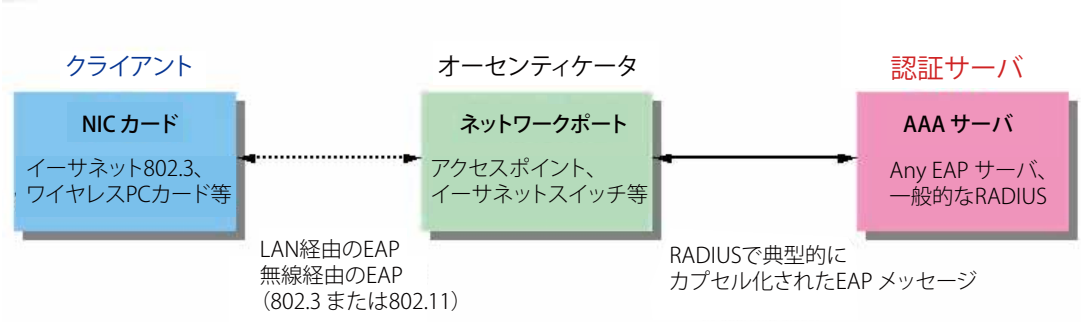


図 7.7-2　802.1X の 3 つの要素

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。

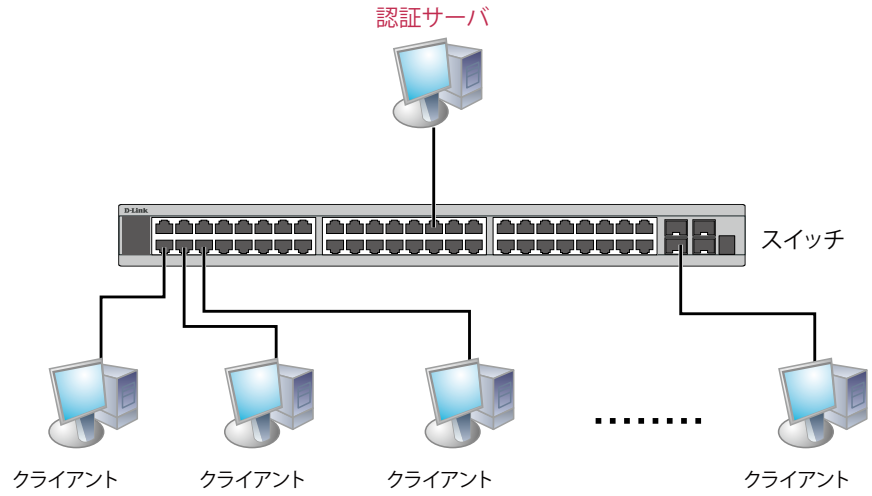


図 7.7-3　認証サーバ

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。（**DWS-3160 Web Management Tool**）
2. 対象ポートに 802.1X の設定を行います。（**Security > 802.1X > 802.1X Port Settings**）
3. スイッチに RADIUS サーバの設定を行います。（**Security > RADIUS > Authentication RADIUS Server Settings**）

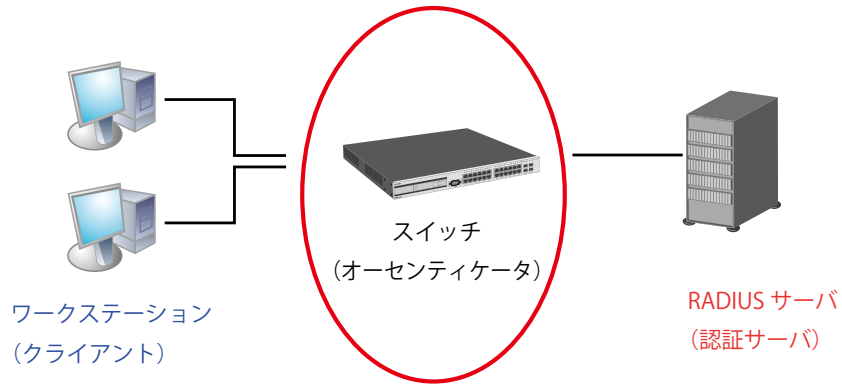


図 7.7-4　オーセンティケータ

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。

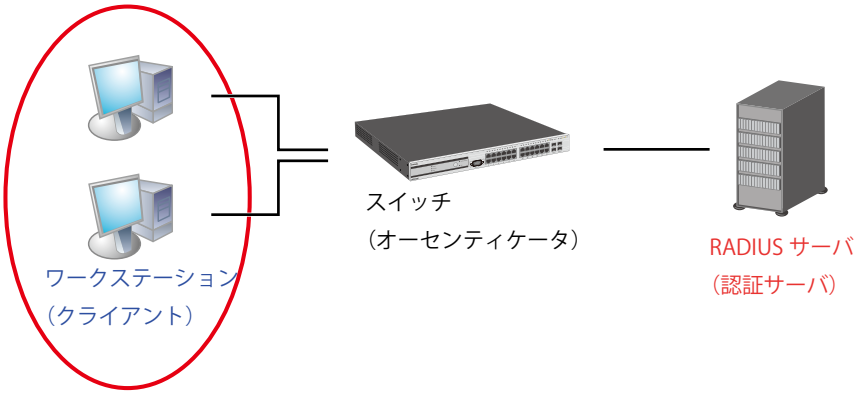


図 7.7-5　クライアント

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 アドレスも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。

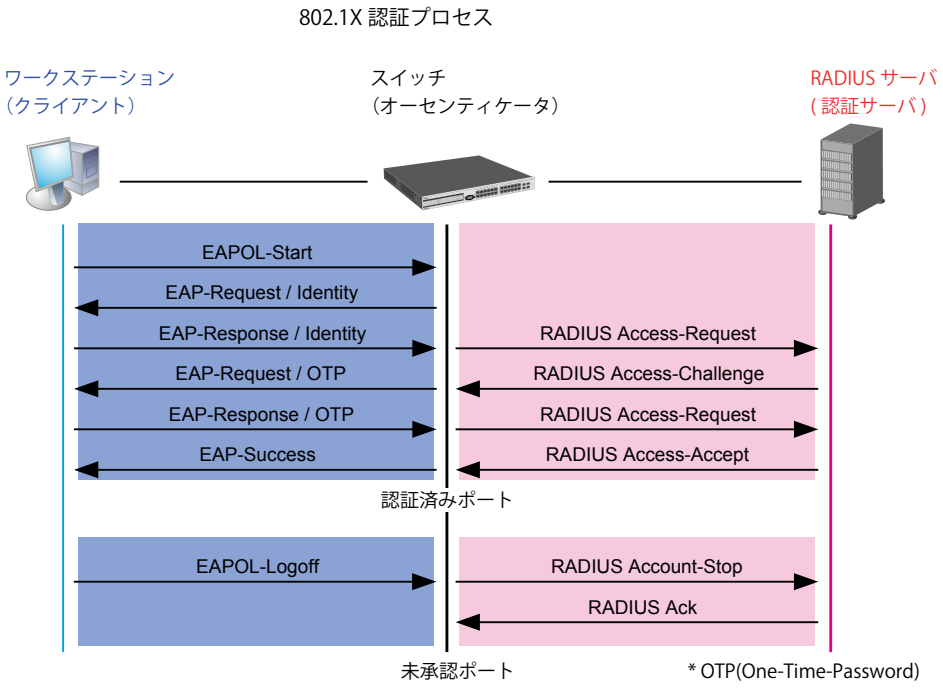


図 7.7-6　802.1X 認証プロセス

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 448 件までの MAC アドレスを自動的に学習してリストに追加します。スイッチはリモート RADIUS サーバを使用して、ネットワークへのアクセスを許可する前に各 MAC アドレスの認証を行います。

ポートベースのネットワークアクセスコントロール

802.1X 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。

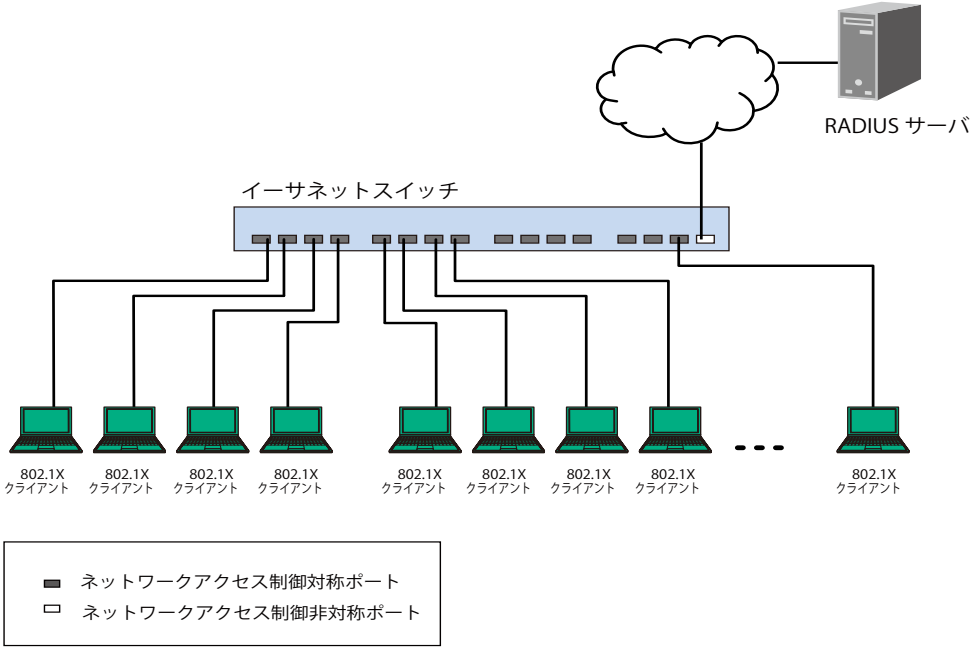


図 7.7-7　典型的なポートベースアクセスコントロールのネットワーク構成例

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。

ホストベースのネットワークアクセスコントロール

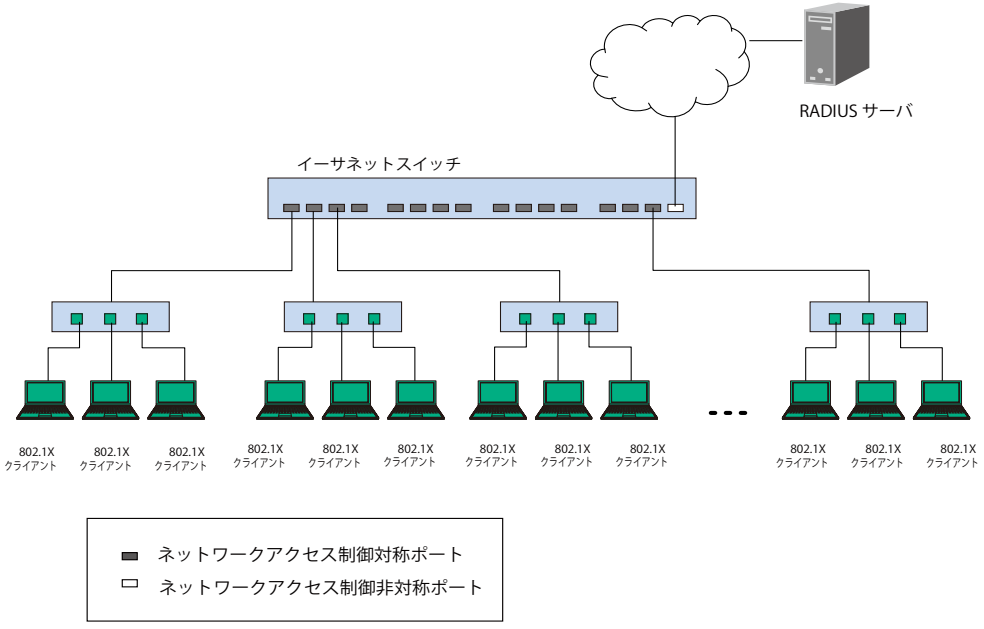


図 7.7-8　典型的な MAC ベースアクセスコントロールのネットワーク構成例

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 Global Settings（802.1X グローバル設定）

802.1X グローバルパラメータを設定します。

1. **Security > 802.1X > 802.1X 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 7.7-9　802.1X Global Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Authentication Mode	80.1X 認証モードを「Disabled」、「Port-based」または「MAC-based」から選択します。
Authentication Protocol	認証プロトコルを「Local」または「RADIUS EAP」から選択します。
Forward EAPOL PDU	これは、EAPOL PDU の転送を制御するグローバル設定です。802.1X 機能をグローバルまたはポートに無効とした場合に、802.1X forward PDU がグローバルおよびポートに有効にされると、ポートに受信した EAPOL パケットは同じ VLAN 内で（グローバルまたはそのポートに対して）802.1X forward PDU が有効で 802.1X が無効であるポートにフラッドします。初期値は無効です。
Max Users (1-448)	ユーザの最大数を指定します。最大ユーザ数は 448 です。「No Limit」をチェックすると、ユーザ制限はなくなります。
RADIUS Authorization	認可設定の受け入れを「Enabled」（有効）/「Disabled」（無効）にします。802.1X の RADIUS における許可を有効にする場合、グローバルな認可ネットワークが有効になると、RADUIS サーバに割り当てられる認可データが許可されます。

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。

802.1X Port Settings（802.1X ポート設定）

802.1X のオーセンティケータ設定を行います。

1. **Security > 802.1X > 802.1X 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。

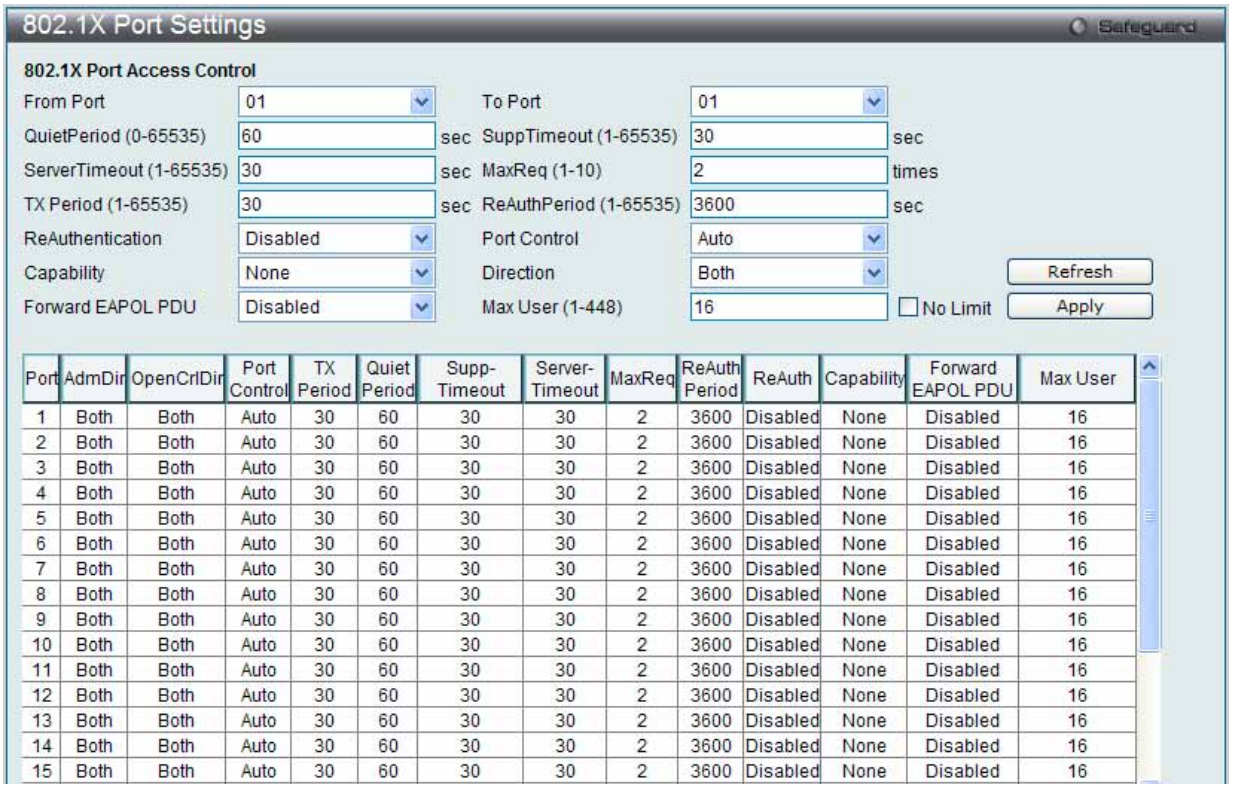


図 7.7-10　802.1X Port Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
From Port / To Port	設定するポート範囲を指定します。
QuietPeriod	クライアントの認証交換に失敗した後、スイッチが静止状態のままクライアントとの通信を拒否する期間（秒）。初期値は 60（秒）です。
SuppTimeout	オーセンティケータとクライアント間の交換でクライアントに EAP-Request を送信した後、応答を待つ時間（1-65535 秒）を指定します。これは、IEEE-802.1X-2001 P47 の SuppTimeout で定義されているものであり、サプリカントがタイムアウトになった際に aWhile タイマを初期化する値です。しかし、現在の認証交換に関連するチャレンジのタイプが異なるタイムアウト値を要求する場合（例えば、チャレンジがユーザ側の操作を必要とする場合）、タイムアウト値はそれに基づいて調整されます。初期値は 30（秒）です。
ServerTimeout	オーセンティケータが認証サーバ間の交換でオーセンティケータが Access-Request を送信した後、応答を待つ時間。初期値は 30（秒）です。
MaxReq	認証セッションのタイムアウト前にスイッチからクライアントへの EAPOL-Request パケットの最大再送回数（1-10）を指定します。IEEE-802.1X-2001 P47 の MaxReq で定義されているものであり、認証セッションのタイムアウト前にスイッチからクライアントへの EAPOL-Request パケットの最大再送回数です。初期値は 2 です。
TxPeriod	オーセンティケータ PAE 状態マシンの TxPeriod の時間を指定します。本値がクライアントへの EAP Request/Identity パケットの送信間隔となります。初期値は 30（秒）です。
ReAuthPeriod	クライアントの再認証間隔を定義する 0（秒）以外の定数。初期値は 3600（秒）です。
ReAuthentication	このポート上で通常の再認証を行うかどうか指定します。初期値は「Disabled」です。
Port Control	ポートの認証状態を制御できます。 • forceAuthorized - 802.1X を無効にし、認証情報の交換を要求せずにポートを Authorized 状態にします。この時ポートではクライアントの 802.1X ベースの認証を行うことなく、通常のトラフィックの送受信が可能になります。 • forceUnauthorized - 対象ポートは Unauthorized 状態を貫き、すべてのクライアントからの認証要求を無視します。スイッチはインタフェースを通したクライアントの認証サービスを行いません。 • Auto - 802.1X を有効にし、Unauthorized 状態を開始し、ポートにおいて EAPOL フレームのみの送受信を許可します。認証プロセスは、ポートのリンク状態が Down から Up に遷移した時、または EAPOL-start フレームが受信された時に開始されます。スイッチはクライアントの ID を要求し、クライアントと認証サーバとの間で認証メッセージの中継を開始します。（初期値）
Capability	ポートに 802.1X オーセンティケータの設定を適用するために使用します。Authenticator が設定をポートに適用するのを選択してください。 • Authenticator - ユーザは認証プロセスを通過するとネットワークにアクセス可能になります。 • None - 指定ポートは 802.1X 認証機能によって制御されません。
Direction	管理制御するトラフィックの方向 を指定します。 • Both - 指定したポートでの入力、出力トラフィックの両方が制御対象となります。 • In - 最初の欄に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。
Forward EAPOL PDU	EAPOL PDU の転送をポートベースで制御します。802.1X 機能をグローバルまたはポートに無効とした場合に、802.1X forward PDU がグローバルおよびポートに有効にされると、ポートに受信した EAPOL パケットは同じ VLAN 内で（グローバルまたはそのポートに対して）802.1X forward PDU が有効で 802.1X が無効であるポートにフラッドします。初期値は無効です。
Max Users	ユーザの最大数を指定します。最大ユーザ数は 448 です。初期値は 16 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。

「Refresh」ボタンをクリックして、テーブルを更新して新しいエントリを表示します。

802.1X User Settings（802.1X ユーザ設定）

スイッチのローカルデータベースに様々な 802.1X ユーザを設定します。

1. **Security > 802.1X > 802.1X User Settings** の順にメニューをクリックし、以下の画面を表示します。

図 7.7-11　802.1X User Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
802.1X User	802.1X ユーザのユーザ名を入力します。
Password	802.1X ユーザのパスワードを入力します。
Confirm Password	802.1X ユーザのパスワードを再度入力します。

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

「Delete」ボタンをクリックして、指定エントリを削除します。

注意　802.1X ユーザ名とパスワードは 16 文字以内とします。

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。

ゲスト 802.1X 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ます。

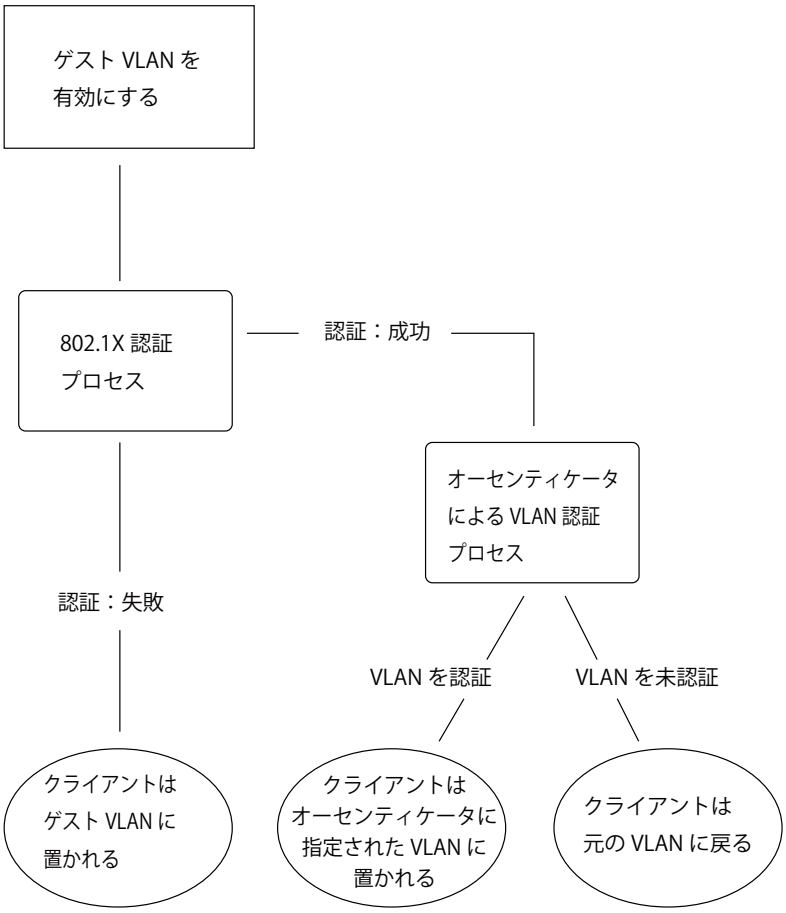


図 7.7-12　ゲスト VLAN 認証プロセス画面

ゲスト VLAN を使用する場合の制限事項

1. ゲスト VLAN はポートベースの VLAN にのみ対応しています。MAC ベースの VLAN では、本プロセスは行われません。
2. ゲスト VLAN をサポートするポートで GVRP を有効化することはできません。また、GVRP が有効であるポートでゲスト VLAN はサポートできません。
3. ポートはゲスト VLAN とスタティック VLAN の両方に所属することはできません。
4. クライアントがターゲット VLAN に所属を許可されると、ゲスト VLAN にはアクセスできなくなります。
5. ポートが複数の VLAN に所属している場合、ゲスト VLAN には所属できません。

ゲスト VLAN 設定

ゲスト VLAN を設定します。

注意 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。

1. **Security > 802.1X > Guest VLAN** の順にクリックし、以下の画面を表示します。

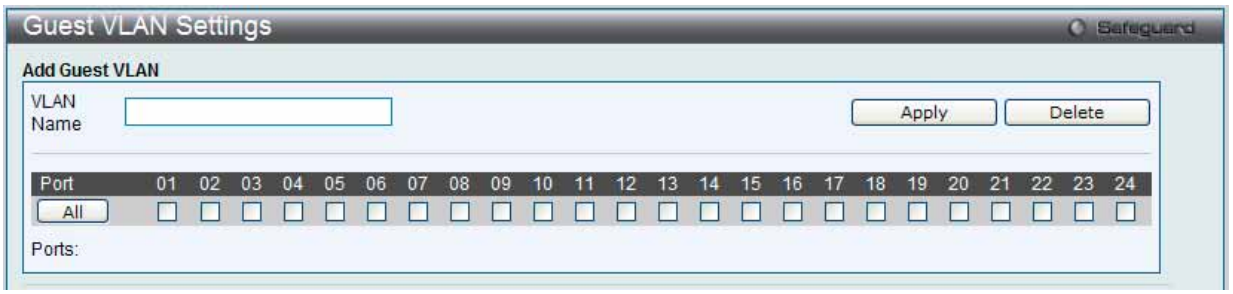


図 7.7-13　Guest VLAN Settings 画面

2. 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	ゲスト 802.1X VLAN にする定義済みの VLAN 名を入力します。
Port List	ゲスト 802.1X 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。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

「Delete」ボタンをクリックして、入力した情報に基づいて指定エントリを削除します。

Authenticator State（オーセンティケータの状態）

オーセンティケータの状態を表示します。「Authentication State」が「802.1X Global Settings」画面で有効な場合に表示されます。

1. **Security > 802.1X > Authenticator 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。

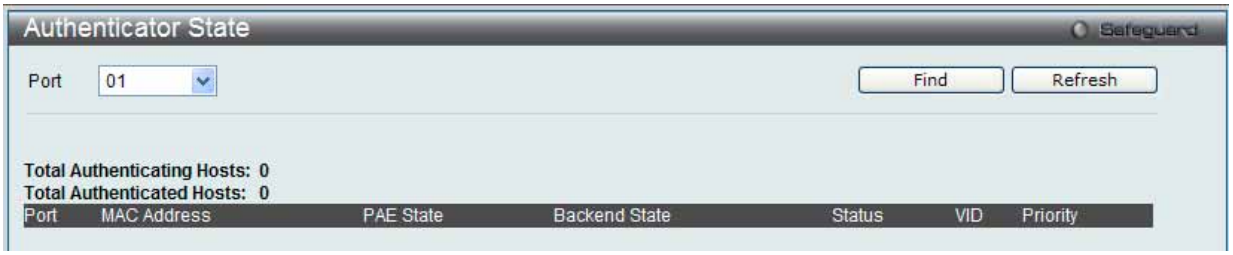


図 7.7-14　Authenticator State 画面

2. 以下の項目を使用して参照します。

項目	説明
Port	プルダウンメニューを使用して表示するポート範囲を指定します。

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
「Refresh」ボタンをクリックして、テーブルを更新して新しいエントリを表示します。

注意 ポートを初期化する前に、まず「802.1X Global Settings」画面で「Authentication Mode」をグローバルに有効とする必要があります。本画面の情報は、「Port-based」または「MAC-based」のいずれかの認証モードを有効にしないと表示されません。

Authenticator Statistics（オーセンティケータ統計情報）

オーセンティケータの統計情報を表示します。「Authentication State」が「802.1X Global Settings」画面で有効な場合に表示されます。

1. **Security > 802.1X > Authenticator Statistics** の順にメニューをクリックし、以下の画面を表示します。

図 7.7-15　Authenticator Statics 画面

2. 以下の項目を使用して参照します。

項目	説明
Port	プルダウンメニューを使用して表示するポート範囲を指定します。
Time Interval	プルダウンメニューを使用して統計情報を更新する間隔を選択します。

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。

注意　ポートを初期化する前に、まず「802.1X Global Settings」画面で「Authentication Mode」をグローバルに有効とする必要があります。本画面の情報は、「Port-based」または「MAC-based」のいずれかの認証モードを有効にしないと表示されません。

Authenticator Session Statistics（オーセンティケータセッション統計情報）

オーセンティケータセッションの統計情報を表示します。「Authentication State」が「802.1X Global Settings」画面で有効な場合に表示されます。

1. **Security > 802.1X > Authenticator Session Statistics** の順にメニューをクリックし、以下の画面を表示します。

図 7.7-16　Authenticator Session Statistics 画面

2. 以下の項目を使用して参照します。

項目	説明
Port	プルダウンメニューを使用して表示するポート範囲を指定します。
Time Interval	プルダウンメニューを使用して統計情報を更新する間隔を選択します。

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。

注意 ポートを初期化する前に、まず「802.1X Global Settings」画面で「Authentication Mode」をグローバルに有効とする必要があります。本画面の情報は、「Port-based」または「MAC-based」のいずれかの認証モードを有効にしないと表示されません。

Authenticator Diagnostics（オーセンティケータ診断）

オーセンティケータ診断情報を表示します。「Authentication State」が「802.1X Global Settings」画面で有効な場合に表示されます。

1. **Security > 802.1X > Authenticator Diagnostics** の順にメニューをクリックし、以下の画面を表示します。

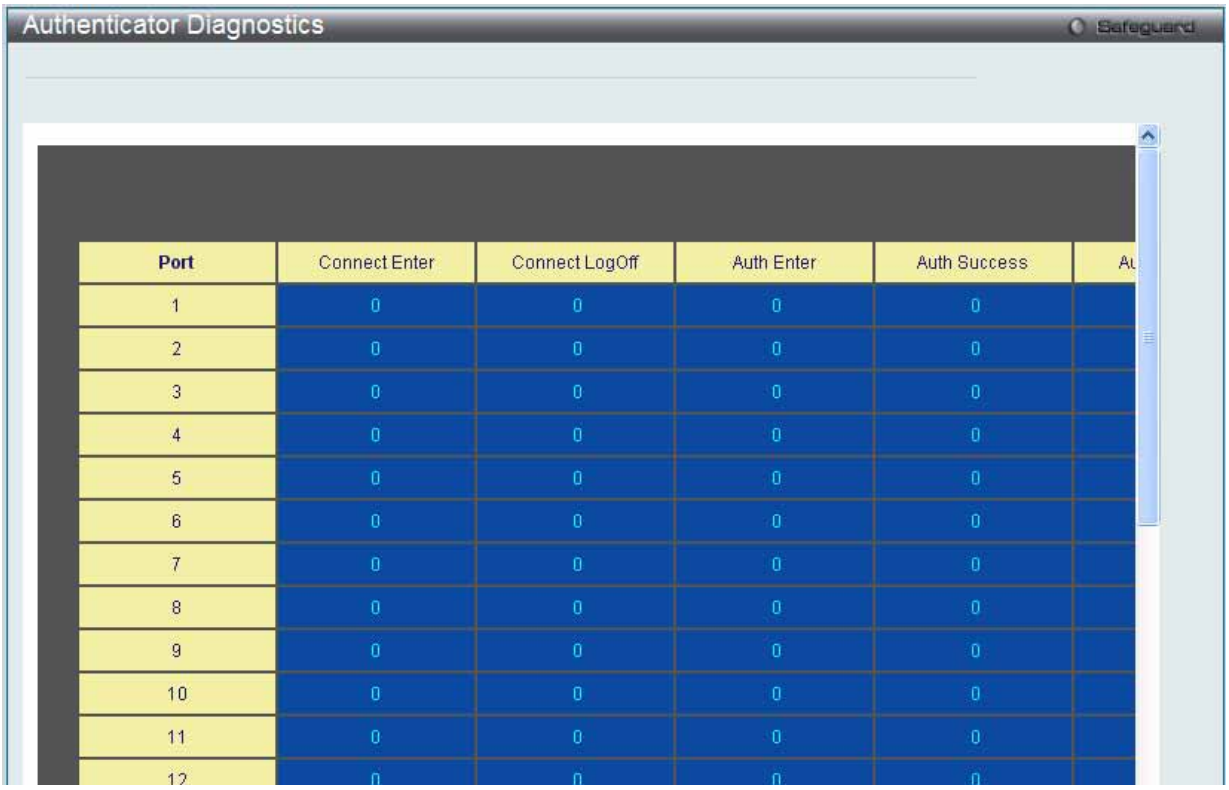


図 7.7-17　Authenticator Diagnostics 画面

2. 以下の項目を使用して参照します。

項目	説明
Port	プルダウンメニューを使用して表示するポート範囲を指定します。
Time Interval	プルダウンメニューを使用して統計情報を更新する間隔を選択します。

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。

注意　ポートを初期化する前に、まず「802.1X Global Settings」画面で「Authentication Mode」をグローバルに有効とする必要があります。本画面の情報は、「Port-based」または「MAC-based」のいずれかの認証モードを有効にしないと表示されません。

Initialize Port(s)（初期化ポート）

ポートベース

現在の初期化されているポート（ポートベース）を表示します。「Authentication State」が「802.1X Global Settings」画面で有効な場合に表示されます。

1. **Security > 802.1X > Initialize Port(s)** の順にメニューをクリックし、以下の画面を表示します：

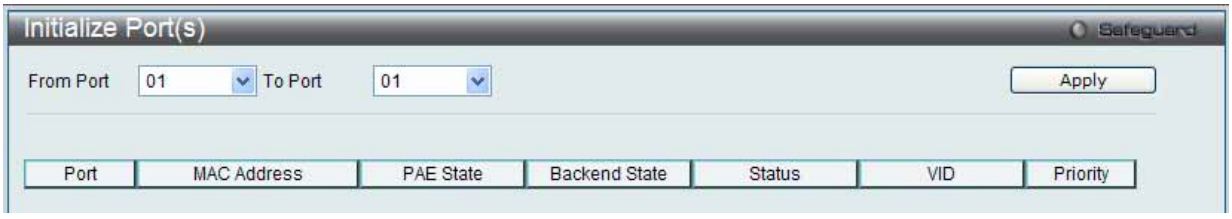


図 7.7-18　Initialize Port-based Port(s) 画面

2. 以下の項目を使用して参照します。

項目	説明
Port	プルダウンメニューを使用して表示するポート範囲を指定します。

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　ポートを初期化する前に、まず「802.1X Global Settings」画面で「Authentication Mode」をグローバルに有効とする必要があります。本画面の情報は、「Port-based」または「MAC-based」のいずれかの認証モードを有効にしないと表示されません。

ホストベース

現在の初期化されているポート（ホストベース）を表示します。「Authentication State」が「802.1X Global Settings」画面で有効な場合に表示されます。

1. **Security > 802.1X > Initialize Port(s)** の順にメニューをクリックし、以下の画面を表示します。

図 7.7-19　Initialize Host-based Port(s) 画面

2. 以下の項目を使用して参照します。

項目	説明
Port	プルダウンメニューを使用して表示するポート範囲を指定します。
MAC Address	チェックして、対応するポートに接続するクライアントの認証 MAC アドレスを入力します。

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

注意 ポートを初期化する前に、まず「802.1X Global Settings」画面で「Authentication Mode」をグローバルに有効とする必要があります。本画面の情報は、「Port-based」または「MAC-based」のいずれかの認証モードを有効にしないと表示されません。

Reauthenticate Port(s)（再認証ポート）

ポートベース

現在の再認証ポート（ポートベース）を表示します。「Authentication State」が「802.1X Global Settings」画面で有効な場合に表示されます。

1. **Security > 802.1X > Reauthenticate Port(s)** の順にメニューをクリックし、以下の画面を表示します。

図 7.7-20　Reauthenticate Port-based Port(s) 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Port	プルダウンメニューを使用して表示するポート範囲を指定します。

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 ポートを初期化する前に、まず「802.1X Global Settings」画面で「Authentication Mode」をグローバルに有効とする必要があります。本画面の情報は、「Port-based」または「MAC-based」のいずれかの認証モードを有効にしないと表示されません。

ホストベース

現在の再認証ポート（ホストベース）を表示します。「Authentication State」が「802.1X Global Settings」画面で有効な場合に表示されます。

1. **Security > 802.1X > Reauthenticate Port(s)** の順にメニューをクリックし、以下の画面を表示します。

図 7.7-21　Reauthenticate Host-based Port(s)

2. 以下の項目を使用して設定および参照します。

項目	説明
Port	プルダウンメニューを使用して表示するポート範囲を指定します。
MAC Address	チェックを行い、対応するポートに接続するクライアントの認証 MAC アドレスを入力します。

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

注意 ポートを初期化する前に、まず「802.1X Global Settings」画面で「Authentication Mode」をグローバルに有効とする必要があります。本画面の情報は、「Port-based」または「MAC-based」のいずれかの認証モードを有効にしないと表示されません。

RADIUS（RADIUS 設定）

Authentication RADIUS Server Settings（認証 RADIUS サーバ設定）

スイッチの RADIUS 機能は中央集中型のユーザ管理を容易にし、またスニッフィングやハッカーからの攻撃から保護します。

1. **Security > RADIUS > Authentication RADIUS 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。

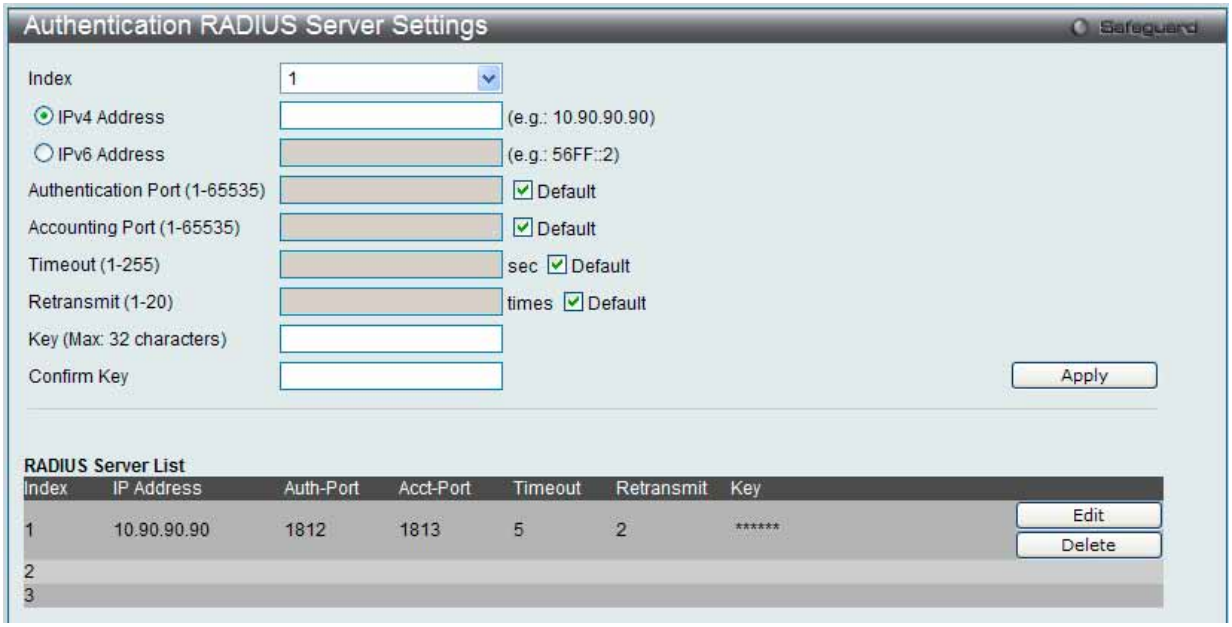


図 7.7-22　Authentic RADIUS Server Settings 画面

本画面は 2 つのメインセクションに分かれています。上のセクションでは、管理者が RADIUS サーバ設定を行い、下のセクションではシステムに現在設定されている RADIUS サーバの設定を表示します。

2. 以下の項目を使用して設定および参照します。

項目	説明
Index	「1」、「2」、「3」、「select the IPv4 Address」から設定を行う RADIUS サーバを選択します。
IPv4 Address	RADIUS サーバの IP アドレスを入力します。
IPv6 Address	RADIUS サーバの IPv6 アドレスを入力します。
Authentication Port (1-65535)	スイッチと RADIUS サーバ間で RADIUS 認証データを送信するために使用される RADIUS 認証サーバの UDP ポート番号を指定します。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送信するために使用される RADIUS 認証サーバの UDP ポート番号を指定します。初期値は 1813 です。
Timeout (1-255)	RADIUS サーバのエージングタイム（秒）を設定します。
Retransmit (1-20)	RADIUS サーバの送信回数を設定します。
Key	RADIUS サーバと同じキーを入力します。
Confirm Key	RADIUS サーバと同じキーを確認のために再度入力します。

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。

エントリの編集

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

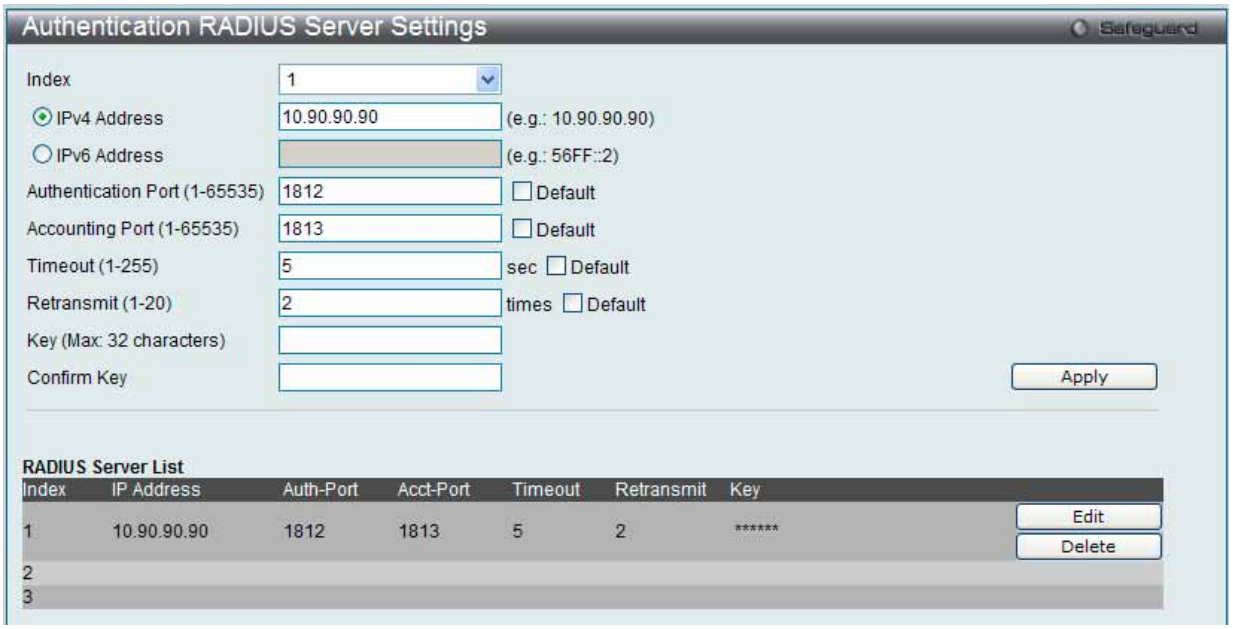


図 7.7-23　Authentic RADIUS Server Settings 画面 - Edit

2. エントリの編集後、「Apply」ボタンをクリックします。

エントリの削除

削除するエントリの「Delete」ボタンをクリックします。

RADIUS Accounting Setting（RADIUS アカウンティング設定）

指定した RADIUS アカウンティングサービスの状態を設定します。

1. **Security > RADIUS > Authentication RADIUS 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。

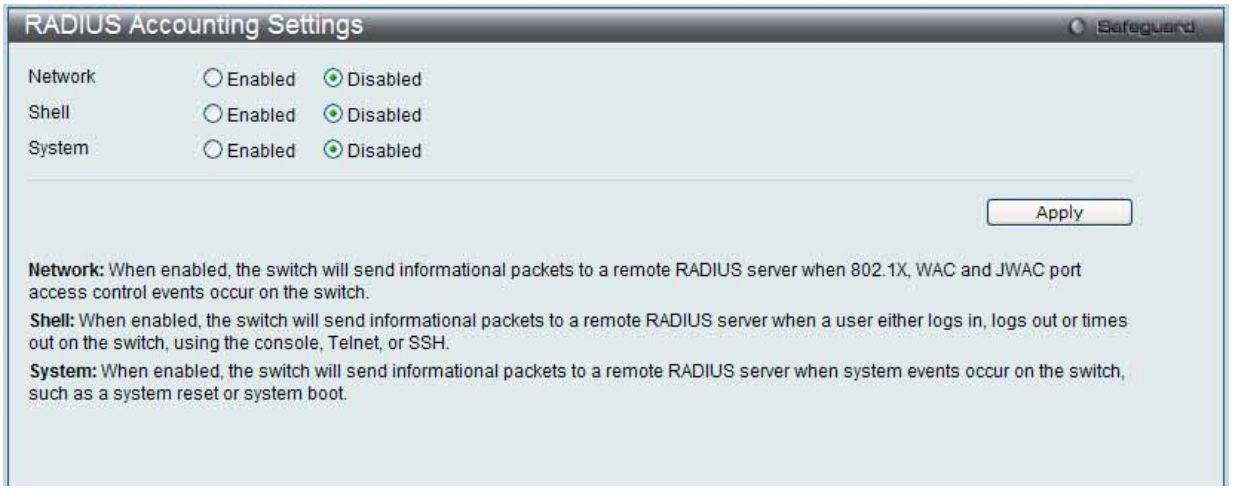


図 7.7-24　RADIUS Accounting Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Network	「Enabled」（有効）にすると、スイッチは、スイッチに 802.1X および WAC にポートアクセスコントロールイベントが発生した場合にリモート RADIUS サーバに情報パケットを送信します。
Shell	「Enabled」（有効）にすると、スイッチは、コンソール、Telnet、または SSH を使用してスイッチにログイン、ログアウトまたはタイムアウトの場合にリモート RADIUS サーバに情報パケットを送信します。
System	「Enabled」（有効）にすると、スイッチは、システムリセットやシステムリブートなどのシステムイベントがスイッチに発生した場合にリモート RADIUS サーバに情報パケットを送信します。

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

RADIUS Authentication（RADIUS 認証）

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。

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

図 7.7-25　RADIUS Authentication 画面

「Time Interval」から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（「Enabled」（有効）/「Disabled」（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（「Enabled」（有効）/「Disabled」（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（「Enabled」（有効）/「Disabled」（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）

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。

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

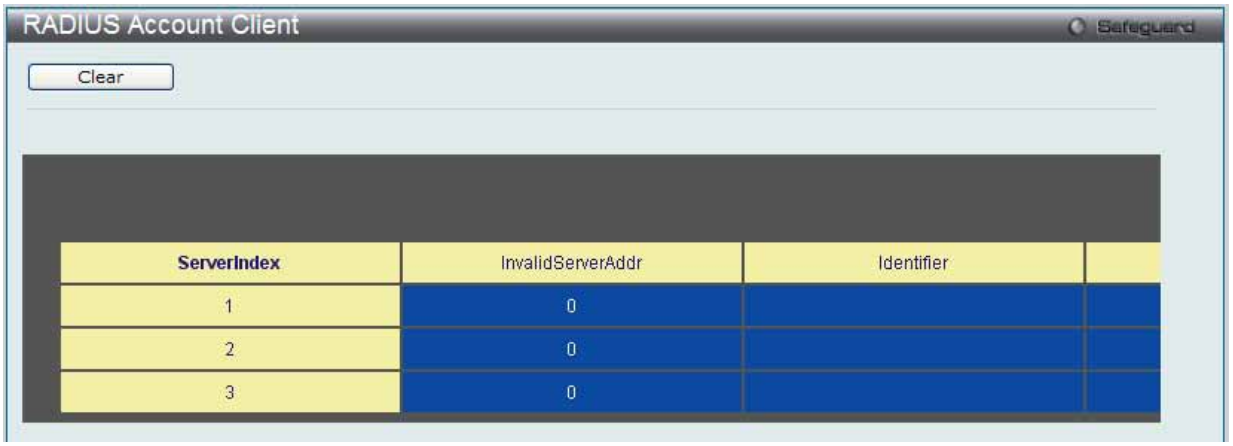


図 7.7-26　RADIUS Accounting Client 画面

「Time Interval」から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。）
ServerAddress	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。
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。

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 バイトのアドレスを使用し、イーサネットリンクレイヤ（データリンクレベル）では 6 バイトの MAC アドレスを使用します。これらの 2 つのアドレスタイプを結合させることにより、レイヤ間のデータ転送を可能にします。

IP-MAC- 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認可ユーザ数を制限することです。IP/MAC アドレスのペアを、事前に設定したデータベースと比較を行うことで、認証クライアントはスイッチのポートアクセスできるようになります。

また、DHCP Snooping を有効にすると、スイッチは、DHCP パケットを検索し、IMPB ホワイトリストにそれらを保存することで自動的に IP/MAC アドレスのペアを学習します。未認証ユーザが IP-MAC バインディングが有効なポートにアクセスしようとすると、システムはアクセスをブロックして、パケットを廃棄します。

本スイッチシリーズでは、アクティブ、インアクティブエントリは共に同じデータベースを使用します。IPv4/IPv6 最大エントリ数は 510 で、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「Enabled」（有効）/「Disabled」（無効）にすることができます。

IMPB Global Settings（IMPB グローバル設定）

IP-MAC- ポートバインディング設定（Trap / Log ステータスおよび DHCP Snoop ステータス）をグローバルに有効または無効にするのに使用します。

1. **Security > IP-MAC-Port Binding (IMPB) > IMPB 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 7.7-27　IMPB Global Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Trap/Log	IP-MAC- ポートバインディングのトラップ / ログメッセージ送信を「Enabled」（有効）/「Disabled」（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。初期値は「Disabled」です。
DHCP Snoop	IP-MAC- ポートバインディングの DHCP Snooping を「Enabled」（有効）または「Disabled」（無効）にします。初期値は「Disabled」です。
Recover Learning Ports	学習状態を回復するポート番号を選択します。「All」をチェックすると、学習ポートすべてをリカバリします。

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。

IMPB Port Settings（IMPB ポート設定）

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。

1. **Security > IP-MAC-Port Binding (IMPB) > IMPB 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。

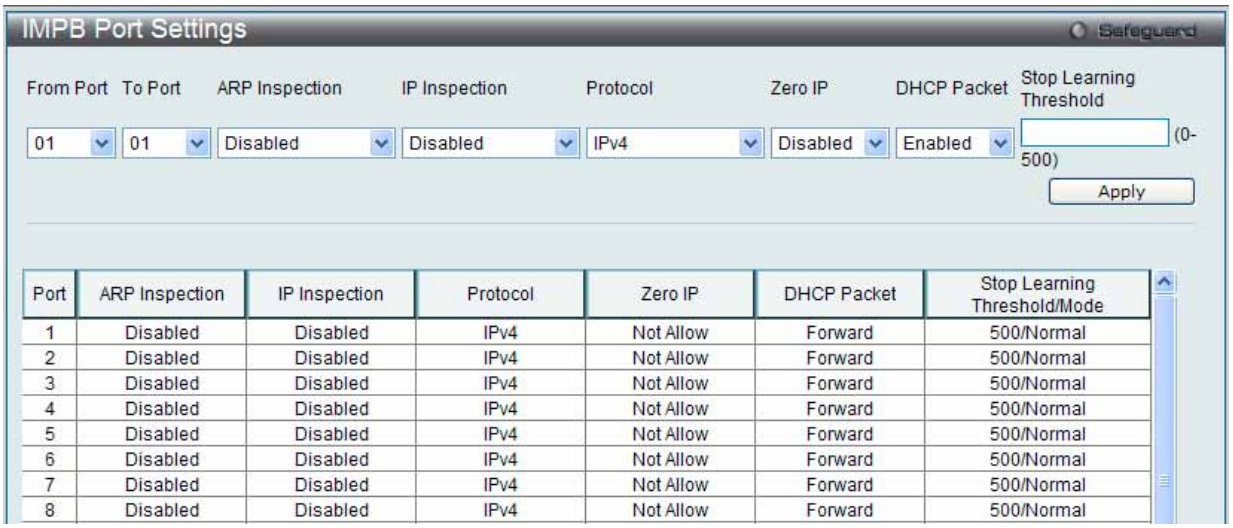


図 7.7-28　IMPB Port Settings 画面

2. 以下の項目を使用して設定および参照します。

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。
ARP Inspection	ARP 検証機能が有効な場合、正しい ARP パケットは転送され、一方不正なパケットは破棄されます。 • Disabled - ARP 検証機能を無効にします。 • Enabled (Strict) - 本モードはハードウェアによる MAC アドレスの学習を無効にします。本モードでは、正しい ARP または IP パケットが検出されるまで、すべてのパケットが初期値で破棄されます。本モードを有効にすると、スイッチはポートの破棄 FDB エントリの記載を停止します。正しいパケットを検出した場合は、スイッチは FDB エントリを記載する必要があります。 • Enabled (Loose) - 本モードでは、不正な ARP パケットが検出されるまで、初期値ですべてのパケットを転送します。初期値は「Disabled」（無効）です。
IP Inspection	ARP と IP 検証の両方を有効にすると、すべての IP パケットがチェックされます。正しい IP パケットは転送され、一方不正なパケットは破棄されます。IP 検証が有効で、ARP 検証が無効である場合、IP でない全パケット（例 L2 パケット、または ARP）が初期値で送信されます。初期値は「Disabled」（無効）です。
Protocol	プルダウンメニューを使用してプロトコルを選択します。「IPv4」のみ選択します。
Zero IP	プルダウンメニューを使用して、本機能を「Enabled」（有効）/「Disabled」（無効）にします。「Allow zero IP」を設定すると、ステートが 0.0.0.0 送信元 IP の ARP パケットを許容します。
DHCP Packet	• Enabled - ブロードキャスト DA の DHCP パケットをフラッドします。（初期値） • Disabled - 指定ポートが受信したブロードキャスト DHCP パケットは、「strict」モードでは転送されません。 本設定は、CPU がトラップした DHCP パケットをソフトウェアが転送する必要がある時、DHCP Snooping で有効である場合に効果があります。本設定はこの状況における転送の実行を制御します。
Stop Learning Threshold	ポートにおいてブロックされるエントリ数を表示します。初期値は 500 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。

IMPB Entry Settings（IMPB 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。

1. **Security > IP-MAC-Port Binding (IMPB) > IMPB 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。

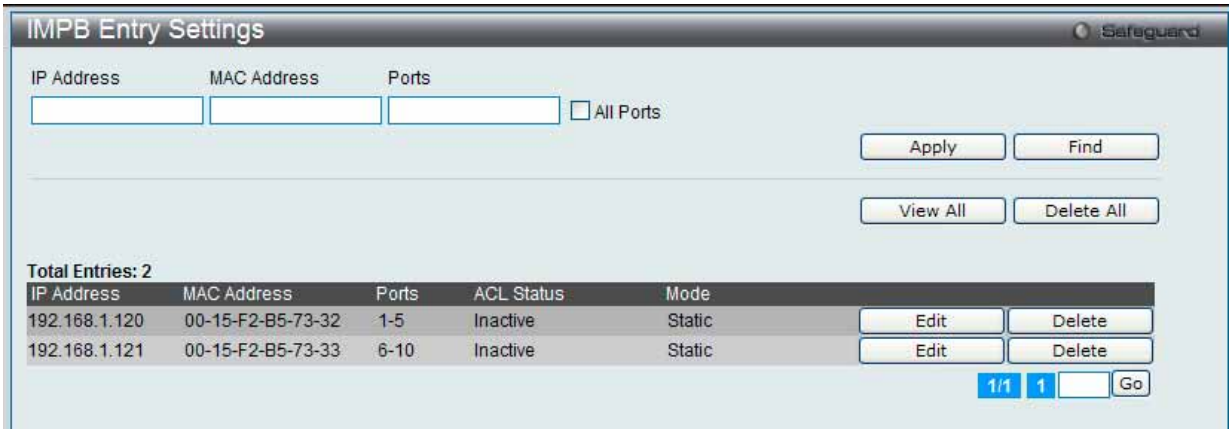


図 7.7-29　IMPB Entry Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
IP Address	チェックして 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。
Ports	本IP-MACバインディングエントリ(IPアドレス+MACアドレス)を設定する対象のポートを指定します。「All Ports」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. 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。

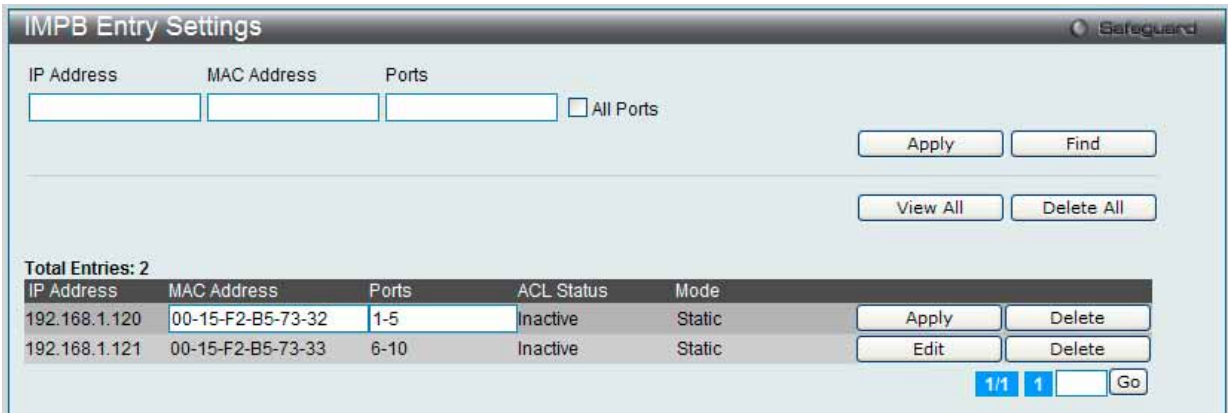


図 7.7-30　IMPB Entry Settings 画面 - Edit

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。

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。

1. **Security > IP-MAC-Port Binding (IMPB) > 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。

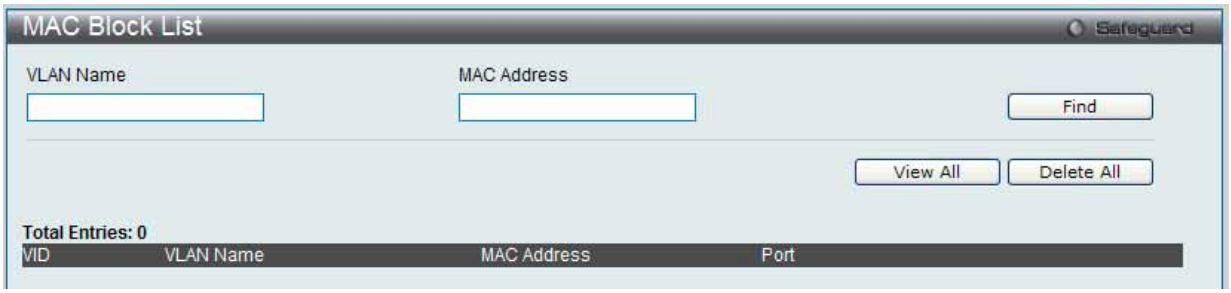


図 7.7-31　MAC Block List 画面

2. 以下の項目を使用して参照します。

項目	説明
VLAN Name	検出または削除する VLAN の VLAN 名を入力します。
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。

DHCP Snooping（DHCP Snooping 設定）

DHCP Snooping Maximum Entry Settings（DHCP Snooping 最大エントリ設定）

DHCP Snooping の最大エントリをポートに設定します。

1. **Security > IP-MAC-Port Binding (IMPB) > DHCP Snooping > DHCP Snooping Maximum Entries** の順にクリックして、以下の画面を表示します。

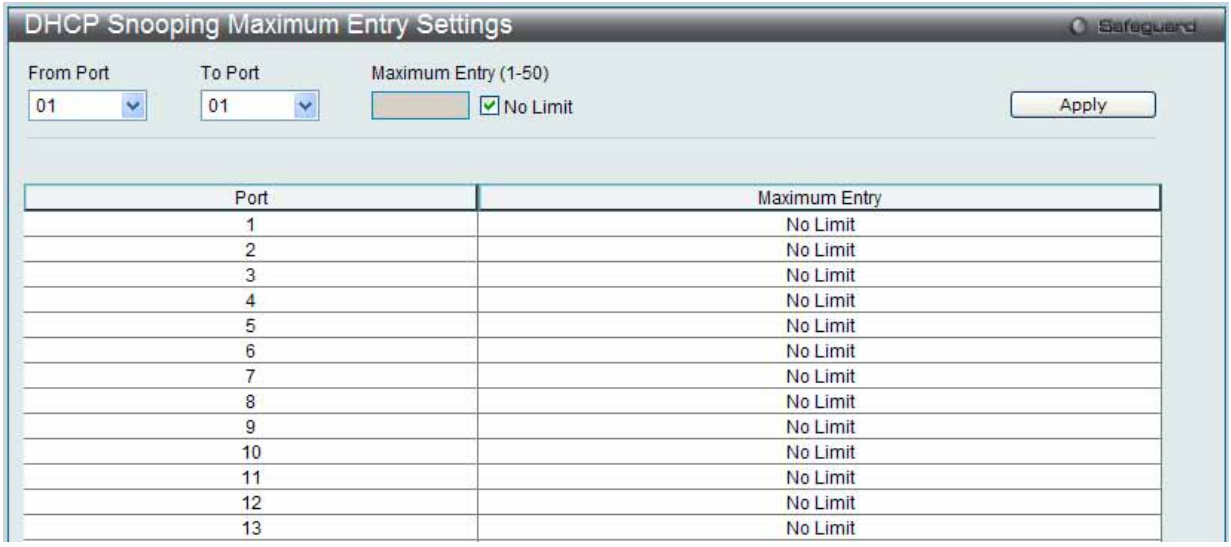


図 7.7-32　DHCP Snooping Maximum Entry Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
From Port / To Port	使用するポート範囲を選択します。
Maximum Entry (1-50)	最大エントリ数を入力します。「No limit」をチェックすると学習するエントリの最大数に制限がなくなります。

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。

DHCP Snooping Entry（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。

1. **Security > IP-MAC-Port Binding (IMPB) > DHCP Snooping > DHCP Snooping Entry** の順にクリックして、以下の画面を表示します。

図 7.7-33　DHCP Snooping Entry 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Port	プルダウンメニューで希望するポートを選択します。
Ports	DHCP Snooping エントリを表示するポートを指定します。 • All - すべてのポートの全エントリを選択します。

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-Based Access Control（MAC ベースアクセスコントロール）

MAC ベースアクセスコントロールは、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。本方式では、ポートベースの MAC にはポートアクセス権を決定し、一方ホストベースの 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 ベースアクセスコントロールでは、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 ベースアクセスコントロールに関する注意

MAC ベースアクセスコントロールに関するいくつかの制限と規則があります。

1. 本機能がポートで有効になると、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. リンクアグリゲーション、およびポートセキュリティが有効なポートは、MAC ベースアクセスコントロールを有効にすることはできません。
4. GVRP 認証が有効なポートをゲスト VLAN で有効にすることはできません。

MAC-based Access Control Settings（MAC ベースアクセスコントロール設定）

スイッチの MAC ベースアクセスコントロール機能にパラメータを設定します。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 ベースアクセスコントロール機能に関連するゲスト VLAN 設定の参照を行います。また、ポートの MAC ベースアクセスコントロール機能を「Enabled」（有効）/「Disabled」（無効）にします。以前に記述した他の機能で有効とされているポートは、MAC ベースアクセスコントロールを使用できないことにご注意ください。

1. **Security > MAC-based Access Control (MAC) > 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。

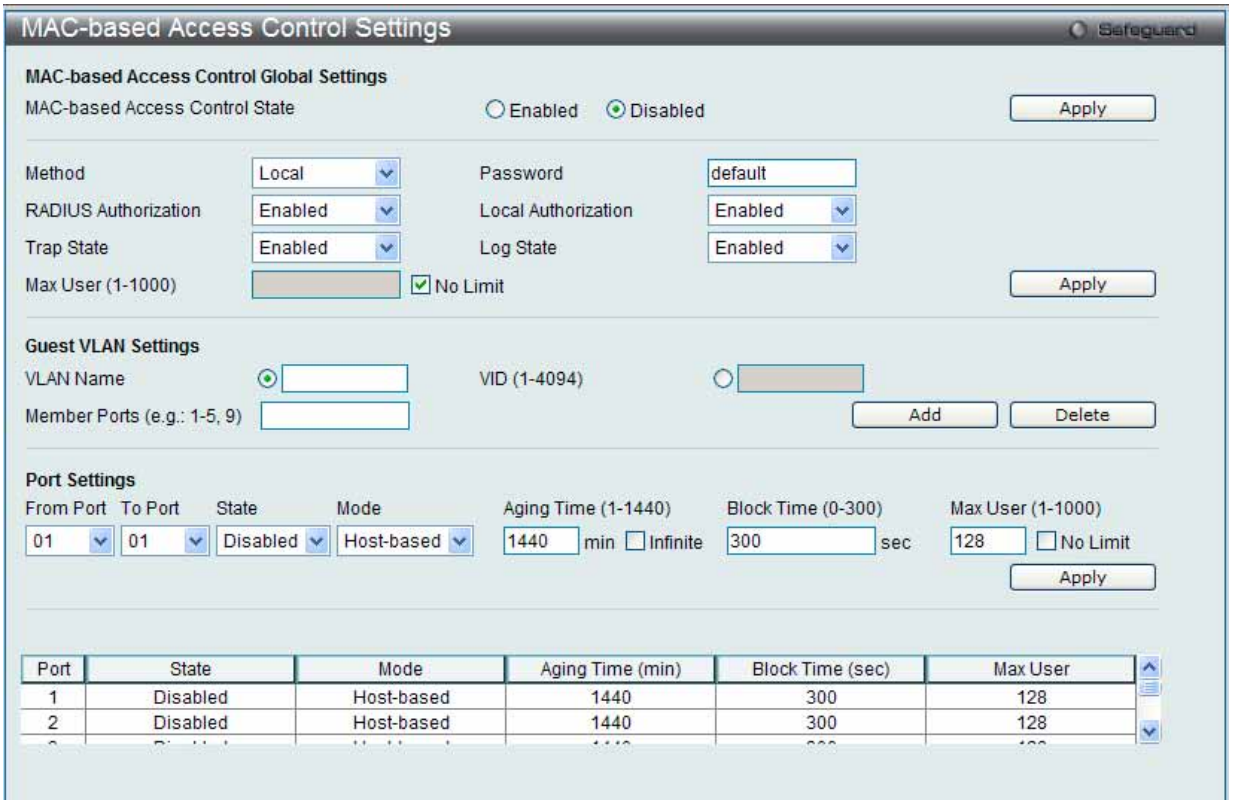


図 7.7-34　MAC-based Access Control Settings 画面

以下の項目を使用して設定および参照します。

項目	説明
MAC-based Access Control Global Settings	
MAC-based Access Control State	「Enabled」（有効）または「Disabled」（無効）を選択し、スイッチの MAC ベースアクセスコントロールをグローバルに設定します。
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 ベースアクセスコントロール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 ベースアクセスコントロール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。
RADIUS Authorization	RADIUS 認証を「Enabled」（有効）/「Disabled」（無効）にします。
Local Authorization	ローカル認証を「Enabled」（有効）/「Disabled」（無効）にします。
Trap State	プルダウンメニューから MAC ベースアクセスコントロール用のトラップの送信を「Enabled」（有効）または「Disabled」（無効）にします。
Log State	プルダウンメニューを使用して、ログの状態を「Enabled」（有効）/「Disabled」（無効）にします。
Max User (1-1000)	スイッチの最大ユーザ数を指定します。「No Limit」を選択すると、ユーザの最大数の設定を行いません。
Guest VLAN Settings	
VLAN Name	本機能に使用される設定済みのゲスト VLAN 名を入力します。
VID (1-4094)	先頭のラジオボタンをクリックしてゲスト VLAN ID を入力します。
Member Ports	ゲスト VLAN に設定するポートリストを入力します。
Port Settings	
From Port / To Port	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設定するポート範囲を指定します。
State	本画面の「Port Settings」セクションで選択したポートまたはポート範囲の MAC ベースアクセスコントロール「Enabled」（有効）/「Disabled」（無効）にします。
Mode	「Port-based」または「Host-based」を選択します。
Aging Time (1-1440)	1-1440（分）の範囲で指定します。初期値は 1440 です。エージングタイムを無効にするためには、「Infinite」オプションを選択します。
Block Time (0-300)	1-300（秒）の範囲で指定します。初期値は 300 です。
Max User (1-1000)	本設定に使用する最大ユーザ数を指定します。「No Limit」を選択すると、本ルールにユーザの制限はなくなります。

「Apply」ボタンをクリックして各セクションで行った変更を適用します。

エントリの追加

「Add」ボタンをクリックすると、入力情報に基づいて新しいエントリを追加します。

エントリの削除

「Delete」ボタンをクリックして、入力した情報に基づいて指定エントリを削除します。

MAC-based Access Control Local Settings（MAC ベースアクセスコントロール ローカル設定）

スイッチに対して認証されるターゲット VLAN と 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。

1. **Security > MAC-based Access Control (MAC) > MAC-based Access Control Local Settings** をクリックし、以下の画面を表示します。

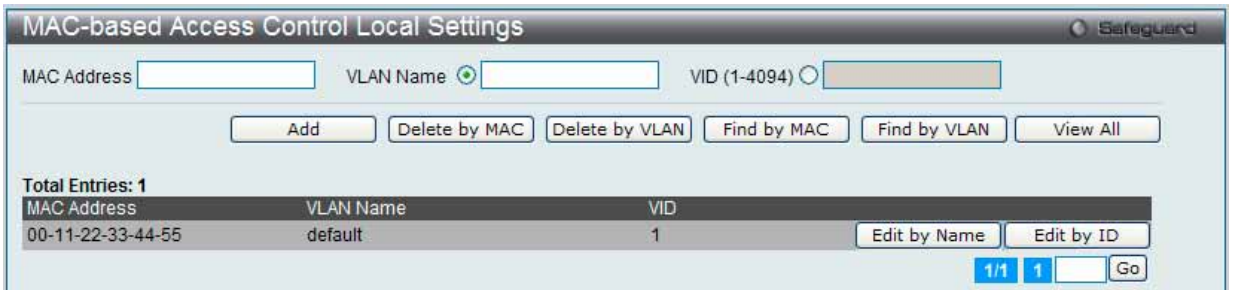


図 7.7-35　MAC-based Access Control Local Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
MAC Address	ローカル認証リストに追加する MAC アドレスを入力します。
VLAN Name	MAC アドレスに対応する VLAN 名を入力します。
VID (1-4094)	MAC アドレスに対応する VLAN ID を入力します。

MAC アドレスリストへの新規登録

MAC アドレスをローカル認証リストに追加するためには、「MAC Address」と「VLAN Name」/「VID」に MAC アドレスとターゲット VLAN 名 / VLAN ID をそれぞれ入力し、「Add」ボタンをクリックします。

MAC アドレスリストの検出

「Find by MAC」ボタンをクリックして、入力した MAC アドレスに基づく特定のエントリを検出します。また、「Find by VLAN」ボタンをクリックして、入力した VLAN 名または VLAN ID に基づく特定のエントリを検出します。

MAC アドレスリストの参照

「View All」ボタンをクリックして、すべての定義済みエントリを表示します。

MAC アドレスエントリの削除

「Delete by MAC」ボタンをクリックして、入力した MAC アドレスに基づいて指定エントリを削除します。または、「Delete by VLAN」ボタンをクリックして、入力した VLAN 名または VLAN ID に基づいて指定エントリを削除します。

MAC アドレスリストの変更

選択した MAC アドレスの VLAN 名を変更するためには、「Edit by Name」ボタンをクリックし、以下の画面を表示します。

図 7.7-36　Edit by VLAN Name 画面

選択した MAC アドレスの VID 変更するためには、「Edit by ID」ボタンをクリックします。

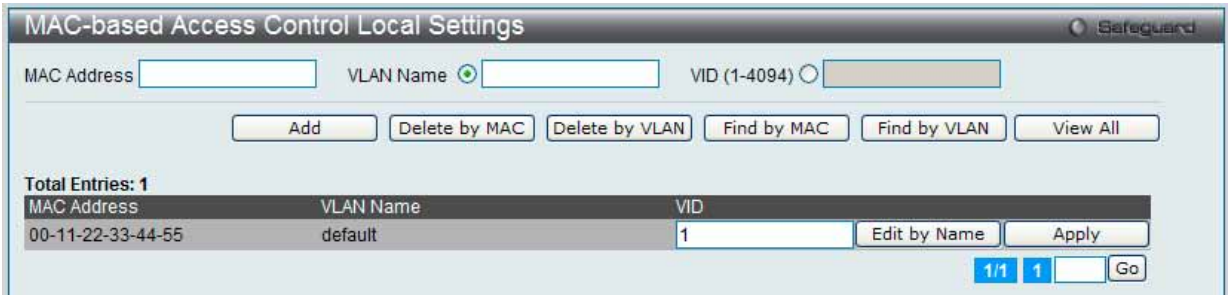


図 7.7-37　Edit by VID 画面

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

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

MAC-based Access Control Authentication State（MAC ベースアクセスコントロールの認証状態）

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。

1. **Security > MAC-based Access Control (MAC) > MAC-based Access Control Authentication State** をクリックし、以下の画面を表示します。

図 7.7-38　MAC-based Access Control Authentication State 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Port List	本設定に使用するポートリストを指定します。

エントリの参照

MAC ベースアクセスコントロールの認証状態の情報を表示するためには、ポート番号を入力し、「Find」ボタンをクリックします。
「View All Hosts」ボタンをクリックして、すべての定義済みホストを表示します。

エントリの削除

「Clear by Port」ボタンをクリックして、入力したポートにリンクするすべての情報をクリアします。
「Clear All Hosts」ボタンをクリックして、すべての定義済みホストをクリアします。

Compound Authentication（コンパウンド認証）

新しいネットワークでは多くの認証方式を採用しています。

Compound Authentication Settings（コンパウンド認証設定）

スイッチポートに認可ネットワーク状態の設定およびコンパウンド認証方式の設定を行います。

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

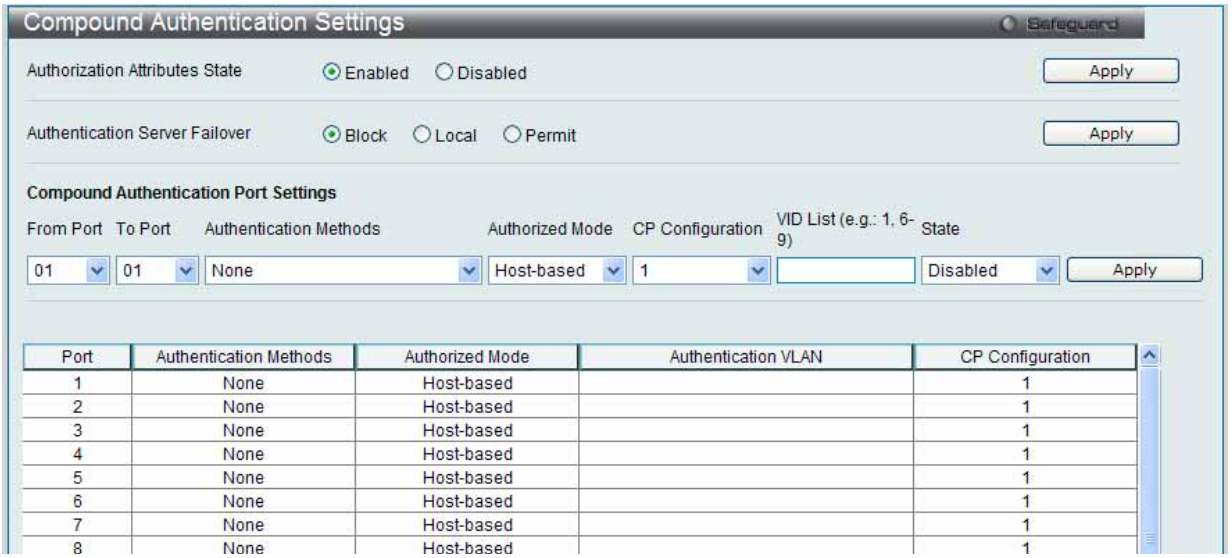


図 7.7-39　Compound Authentication Settings 画面

2. スイッチの各ポートにコンパウンド認証を設定するには、以下の項目を指定します。

項目	説明
Authorization Attributes State	認可ネットワーク状態を「Enabled」（有効）/「Disabled」（無効）にします。
Authentication Server Failover	認証サーバのフェイルオーバ機能を設定します。 • Local - スイッチは、クライアントを認証するためにローカルデータベースを使用します。クライアントがローカル認証に失敗すると、クライアントは認証されなかったとみなされます。 • Permit - クライアントは、通常認証されたものとして見なされます。ゲスト VLAN が有効であると、クライアントはゲスト VLAN にとどまり、そうでない場合、オリジナルの VLAN にとどまります。 • Block - クライアントは通常認証されないものとして見なされます。（初期値）
From Port / To Port	コンパウンド認証ポートとして設定するポート範囲を指定します。
Authentication Methods	コンパウンド認証方式のオプションを指定します。 • None - すべてのコンパウンド認証方式を無効とします。 • Any (MAC, 802.1X or CP) - 認証方式のどれかを通過するとアクセスは許可されます。このモードでは、MAC、802.1X、および CP が同時にポートで有効とされます。また、システム状態によって各セキュリティモジュールがアクティブまたは非アクティブになります。 • 802.1X+IMPB - はじめに 802.1X 認証を行い、次に IMPB 認証を行います。両方の認証が通過のために必要です。 • MAC+IMPB - はじめに MAC 認証を行い、次に IMPB 認証を行います。両方の認証が通過のために必要です。 IMPB+CP - IMPB が最初に検証され、次に CP が検証されます。両方の認証が通過のために必要です。
Authorized Mode	「Host-based」または「Port-based」を選択します。 • Port-based - 対応するホストの 1 つが認証を通過すると、同じポート上のホストはすべてネットワークへの接続が許可されます。認証に失敗するとこのポートは続いて次の認証方式を実行します。 • Host-based - ユーザは個別に認証されます。
CP Configuration	キャプティブポータルの設定 ID（1-10）を選択します。
VID List	VLAN ID リストを指定します。
State	認証 VLAN の状態（「Enabled」（特定の VID リストを割り当て）/「Disabled」（削除））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。

Compound Authentication Guest VLAN Settings（コンパウンド認証ゲスト VLAN の設定）

ポートをゲスト VLAN に割り当て、または削除することができます。

1. **Security > Compound Authentication > Compound Authentication Guest 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 7.7-40　Compound Authentication Guest VLAN Settings 画面

2. 以下の項目を使用して、ゲスト VLAN の設定をします。

項目	説明
VLAN Name	VLAN をゲスト VLAN として割り当てます。定義済みのスタティック VLAN を割り当てます。
VLAN ID (1-4094)	VLAN ID をゲスト VLAN に割り当てます。定義済みのスタティック VLAN を割り当てます。
Port List (e.g : 1,6-9)	設定するポート範囲を指定します。または、「All Ports」のチェックボタンをチェックしてすべてのポートを一度に設定します。
Action	実行する機能を選択します。 • Create VLAN - VLAN を作成します。 • Add Ports - ポートを追加します。 • Delete Ports - ポートを削除します。

「Apply」ボタンをクリックし、ゲスト 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

「Delete」ボタンをクリックして、指定エントリを削除します。

Port Security（ポートセキュリティ）

Port Security 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。

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

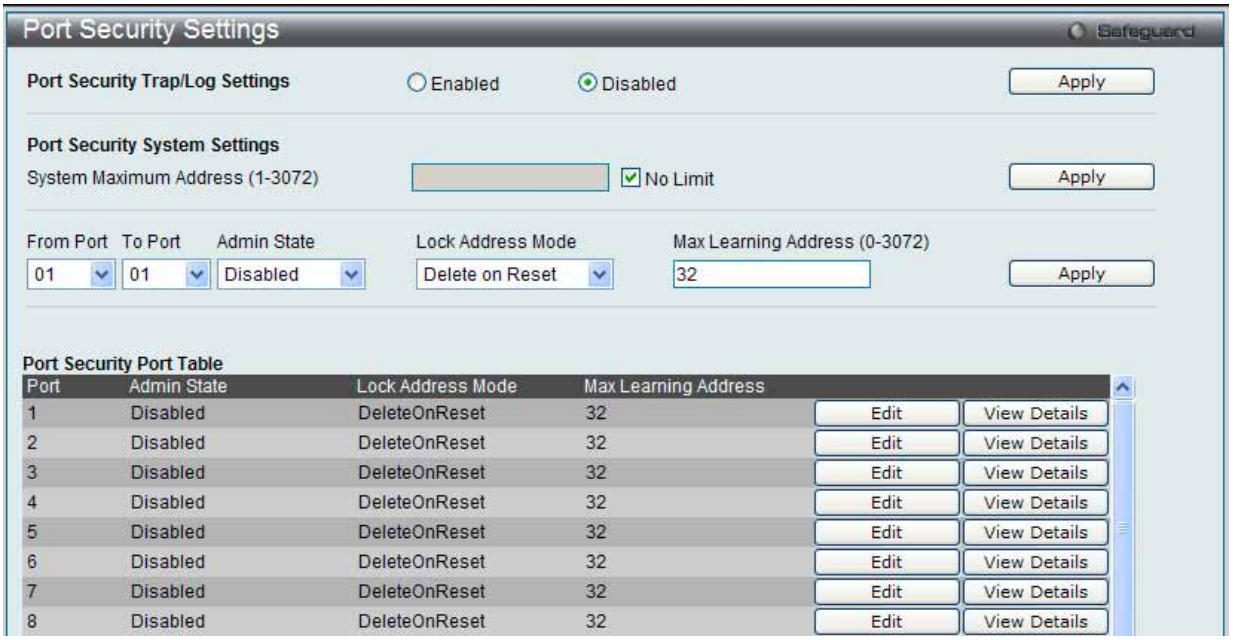


図 7.7-41　Port Security Settings 画面

以下の項目を使用して設定および参照します。

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。
System Maximum Address (1-3072)	システムの最大アドレス数を入力します。「No Limit」をチェックすると、システムのアドレス数は制限されなくなります。
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選択します。
Admin State	ポートセキュリティの「Enabled」（有効）/「Disabled」（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。
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。
Max Learning Address (0-3072)	本ポートが学習できるポートセキュリティエントリの最大数を指定します。

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

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て、以下の画面を表示します。

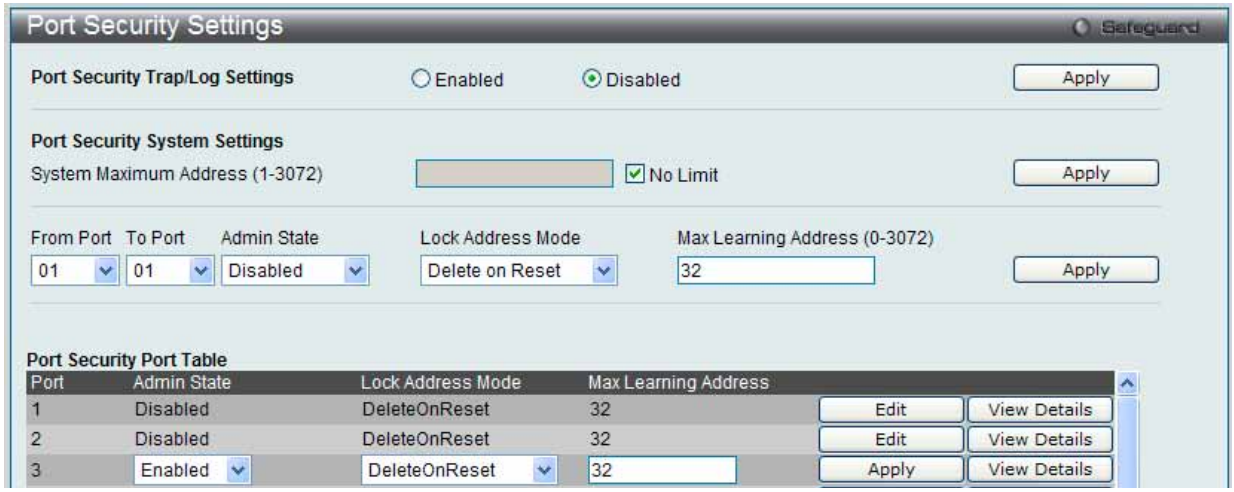


図 7.7-42　Port Security Settings 画面 - Edit

2. 指定エントリを編集して「Apply」ボタンをクリックします。

指定エントリの参照

「View Detail」ボタンをクリックし、以下の画面を表示します。

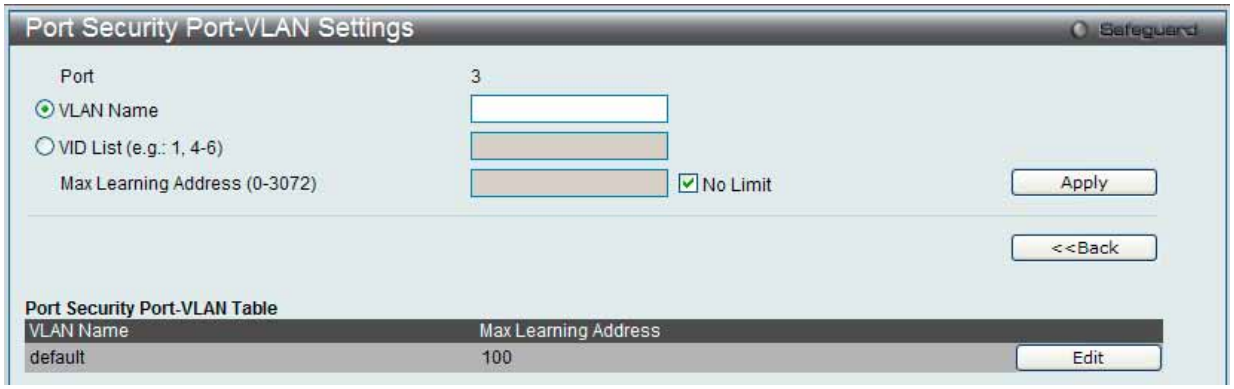


図 7.7-43　Port Security Port-VLAN Settings 画面

以下の項目を使用して設定および参照します。

項目	説明
VLAN Name	チェックして VLAN 名を入力します。
VID List	チェックして VLAN ID リストを入力します。
Max Learning Address (0-3072)	VLAN が学習できるポートセキュリティエントリの最大数を指定します。「0」は本 VLAN でユーザの認証は行わないことを意味します。設定が VLAN ポートで現在学習したエントリ数より小さいと、コマンドは拒否されます。「No Limit」をチェックすると、VLAN が学習できるポートセキュリティエントリの最大数を制限しません。初期値は「No Limit」です。

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て、以下の画面を表示します。

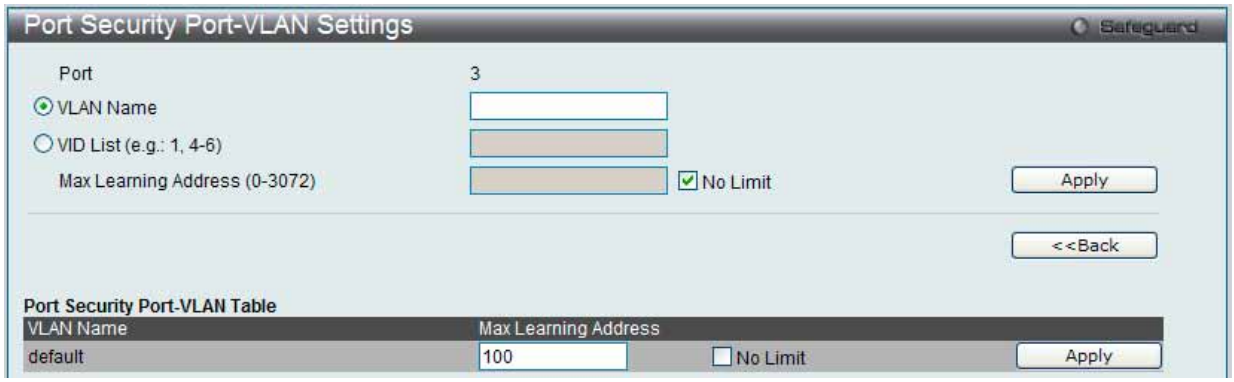


図 7.7-44　Port Security Port-VLAN Settings 画面 - Edit

2. 指定エントリを編集して「Apply」ボタンをクリックします。

「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

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

指定 VLAN で学習されるポートセキュリティエントリの最大数を指定します。

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

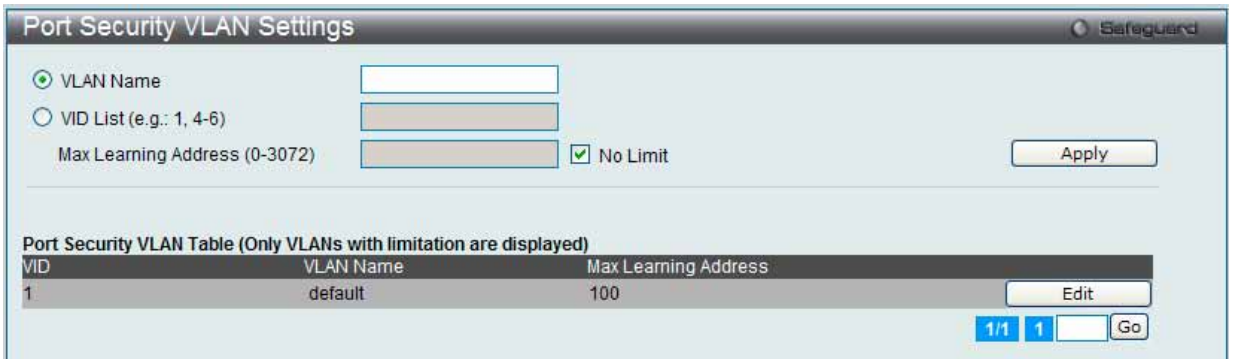


図 7.7-45　Port Security VLAN Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
VLAN Name	VLAN 名を入力します。
VID List	VLAN ID リストを指定します。
Max Learning Address (0-3072)	VLAN が学習できるポートセキュリティエントリの最大数を指定します。「No Limit」をチェックすると、VLAN が学習できるポートセキュリティエントリの最大数を制限しません。

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

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て、以下の画面を表示します。

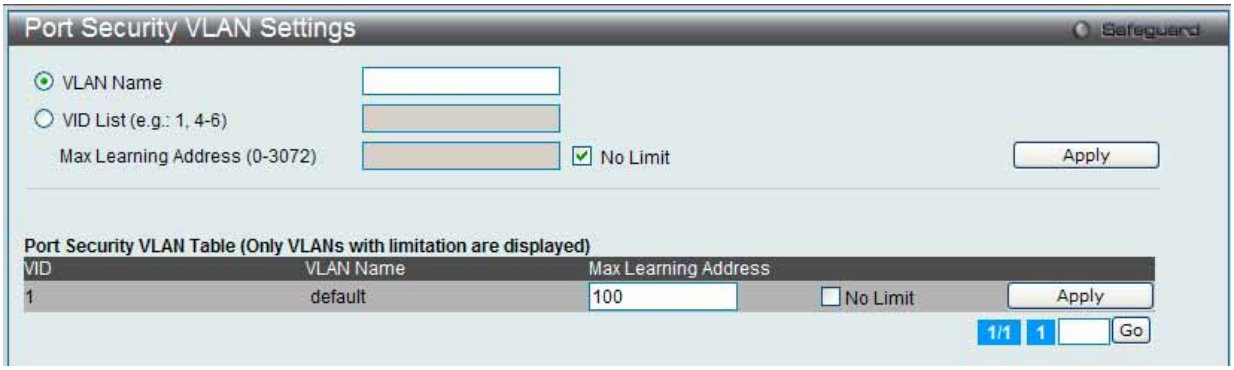


図 7.7-46　Port Security VLAN Settings 画面 - Edit

2. 指定エントリを編集して「Apply」ボタンをクリックします。

Port Security Entries（ポートセキュリティエントリ）

スイッチが学習して転送データベースに登録したポートセキュリティエントリからエントリを削除します。

1. **Security > Port Security > Port Security 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 7.7-47　Port Security Entries 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
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 名を指定します。
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 を指定します。
Port List	ポートセキュリティエントリ検索に使用するポート番号（リスト）を入力します。「All」を選択すると、設定されているすべてのポートを表示します。
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 アドレスを表示します。
Lock Mode	MAC アドレステーブルのロックモードを表示します。

エントリの参照

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

エントリのクリア

「Clear」ボタンをクリックして、入力した情報に基づいてすべてのエントリを削除します。
「Clear All」ボタンをクリックして、表示されたすべてのエントリを削除します。

エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。

ARP Spoofing Prevention Settings（ARP Spoofing 防止設定）

保護されたゲートウェイに対する MAC のなりすましを防止するためにスプーフィング防止エントリを設定します。エントリが作成されると、送信側 IP がエントリのゲートウェイ IP に一致するが、送信側 MAC フィールドまたは送信元 MAC フィールドがエントリのゲートウェイ MAC に一致しない ARP パケットは、システムによって破棄されます。

1. **Security > 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。

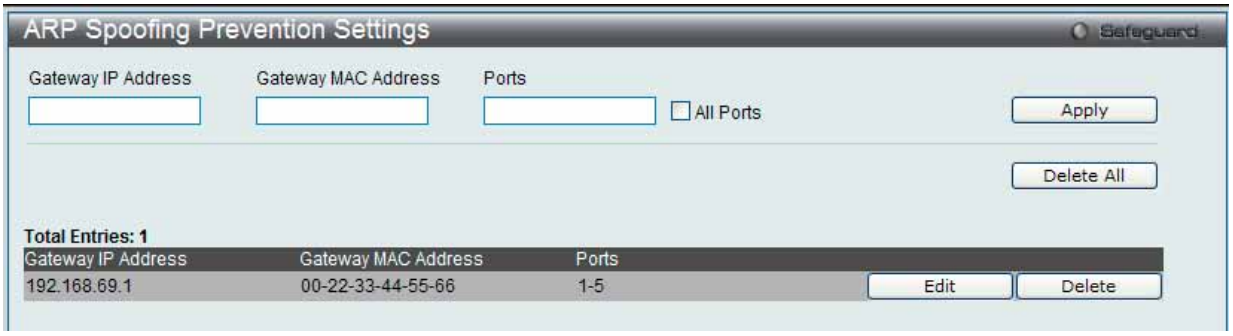


図 7.7-48　ARP Spoofing Prevention Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Gateway IP Address	ARP Spoofing を防止するのに使用するゲートウェイ IP アドレスを入力します。
Gateway MAC Address	ARP Spoofing を防止するのに使用する MAC アドレスを指定します。
Ports	機能を適用するポート番号を選択します。また、「All Ports」を選択するとスイッチのすべてのポートに本機能が適用されます。

3. 「Gateway IP Address」（ゲートウェイの IP アドレス）、「Gateway MAC Address」（ゲートウェイの MAC アドレス）および「Ports」（ポートリスト）を入力し、「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て、以下の画面を表示します。

図 7.7-49　ARP Spoofing Prevention Settings 画面 - Edit

2. 指定エントリを編集して「Apply」ボタンをクリックします。

エントリの削除

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

BPDU Attack Protection（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 > Layer2 Protocol Tunneling 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。

1. **Security > BPDU Attack Protection** の順にメニューをクリックし、以下の画面を表示します。

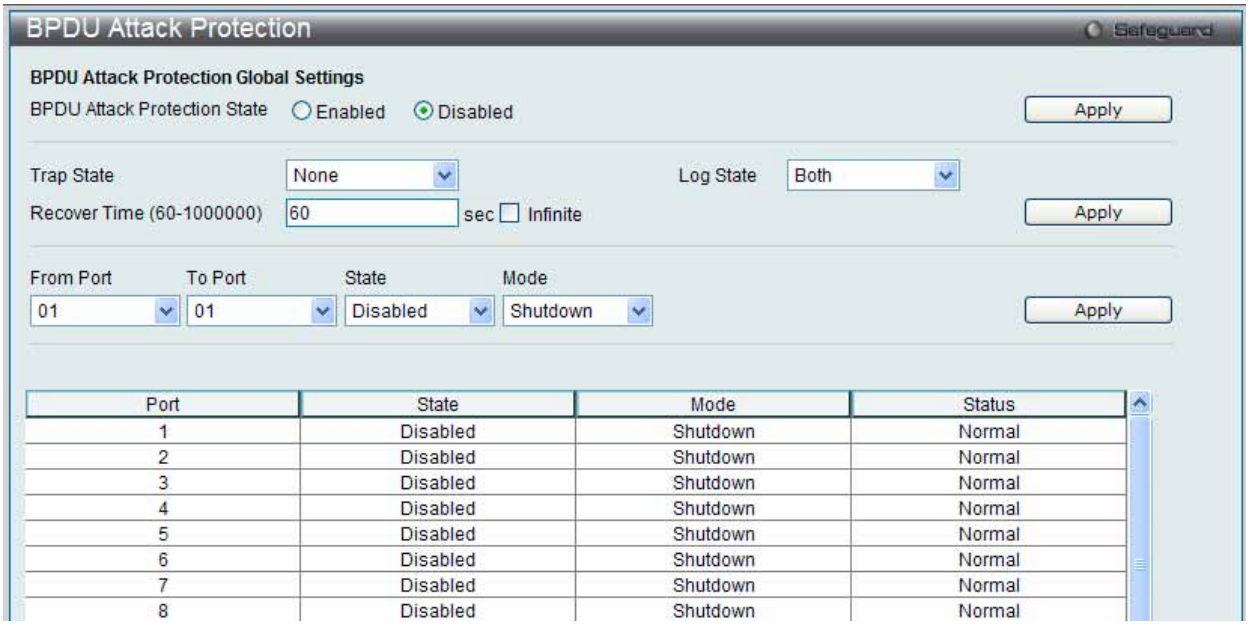


図 7.7-50　BPDU Attack Protection 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
BPDU Attack Protection State	BPDU アタック防止機能をグローバルに「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Disabled」です。
Trap State	トラップをいつ送信するか指定します。「None」、「Attack Detected」、「Attack Cleared」、または「Both」を選択します。初期値は「None」（なし）です。
Log State	ログエントリをいつ送信するか指定します。「None」、「Attack Detected」、「Attack Cleared」、または「Both」を選択します。初期値は「Both」です。
Recover Time (60-1000000)	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（秒）です。「Infinite」をチェックすると、ポートは自動復帰はしなくなります。
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「Enabled」（有効）/「Disabled」（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）

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。

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。本機能は、CTP（Configuration Testing Protocol）パケットがスイッチにループバックすると、スイッチのポートを一時的にシャットダウンします。スイッチが CTP パケットをポートまたは VLAN から受信したことを検知すると、ネットワークにループバックが発生していると認識します。スイッチは、自動的にポートまたは VLAN をブロックして管理者にアラートを送信します。「Loopback Detection Recover Time」がタイムアウトになると、ループバック検知ポートは再起動（Discarding 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。

1. **Security > 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。

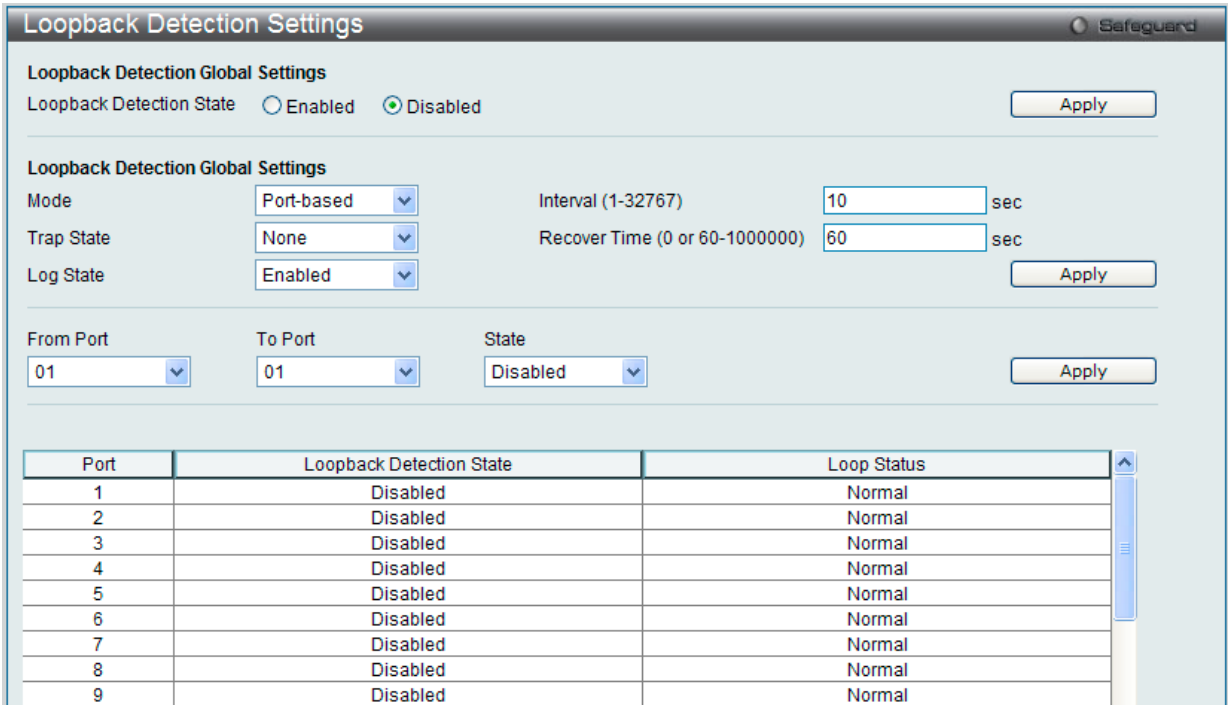


図 7.7-51　Loopback Detection Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Loopback Detection State	ループバック検知機能を「Enabled」（有効）または「Disabled」（無効）にします。初期値は「Disabled」です。
Mode	プルダウンメニューを使用して、「Port-based」と「VLAN-based」を切り替えます。
Trap State	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。
Log State	プルダウンメニューを使用して、ループバック検知のログ状態を「Enabled」（有効）/「Disabled」（無効）にします。
Interval (1-32767)	デバイスがループバックイベントを検出するためにすべての CTP（Configuration Test Protocol）パケットを送信する間隔（秒）。有効な範囲は 1-32767（秒）です。初期値 :10（秒）。
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。

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。

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

トラフィックセグメンテーション機能は、（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。

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

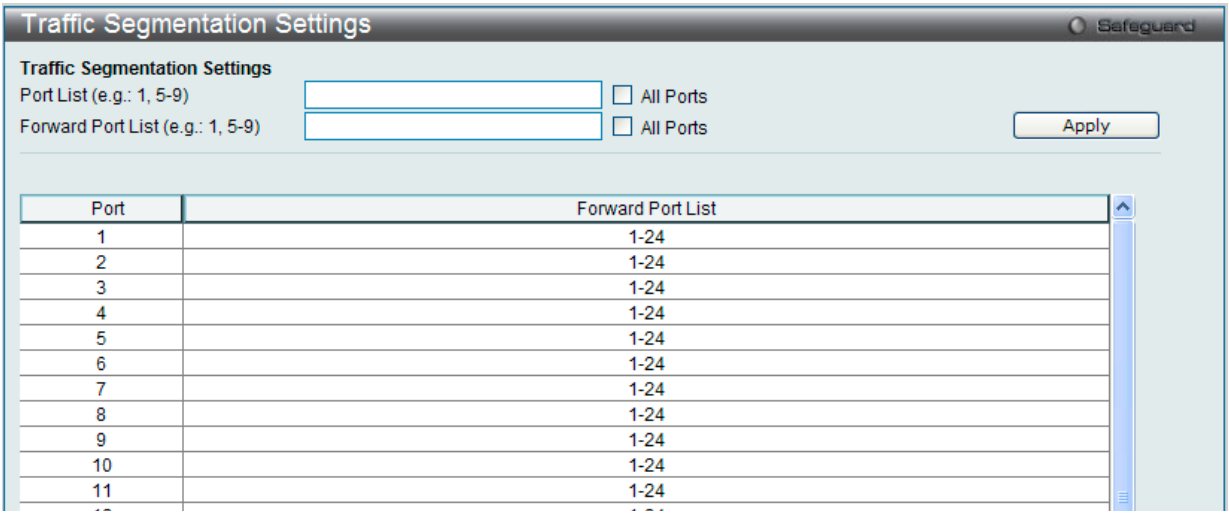


図 7.7-52　Traffic Segmentation Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Port List	トラフィックセグメンテーションを設定するポートを入力します。「All Ports」ボタンをクリックすると設定用にすべてのポートを選択します。
Forward Port List	トラフィックセグメンテーション設定に含めるポートを入力します。「All Ports」ボタンをクリックすると設定用にすべてのポートを選択します。
Port	トラフィックセグメンテーション設定に含めたポートを表示します。

「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。

NetBIOS Filtering Setting（NetBIOS フィルタリング設定）

ネットワークをまたいで通信するために、NetBIOS はインタフェースをプログラミングするアプリケーションで、アプリケーションが使用する多くの機能を提供します。NetBEUI（NetBIOS Enhanced User Interface）は、NetBIOS のためのデータリンク層フレーム構造として作成されました。NetBIOS トラフィックを送信するためのシンプルなメカニズムである NetBEUI は小規模の MS-DOS や Windows ベースのワークグループのために選択するプロトコルです。NetBIOS は、厳密には NetBEUI プロトコル内には含まれません。マイクロソフトは、RFC1001 と RFC1002 に NetBIOS over TCP/IP（NBT）を記述した国際規格を作成するために取り組みました。

NetBUEI プロトコルを使用する 2 台以上のコンピュータのネットワーク通信をブロックする場合、これらの種類のパケットをフィルタするために NetBIOS フィルタリングを使用することができます。

NetBIOS フィルタを有効にすると、スイッチは自動的に 1 つのアクセスプロファイルと 3 つのアクセスルールを作成します。ユーザが広範囲に NetBIOS フィルタを有効にすると、スイッチはもう 1 つずつアクセスプロファイルとアクセスルールを作成します。

1. **Security > NetBIOS Filtering 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。

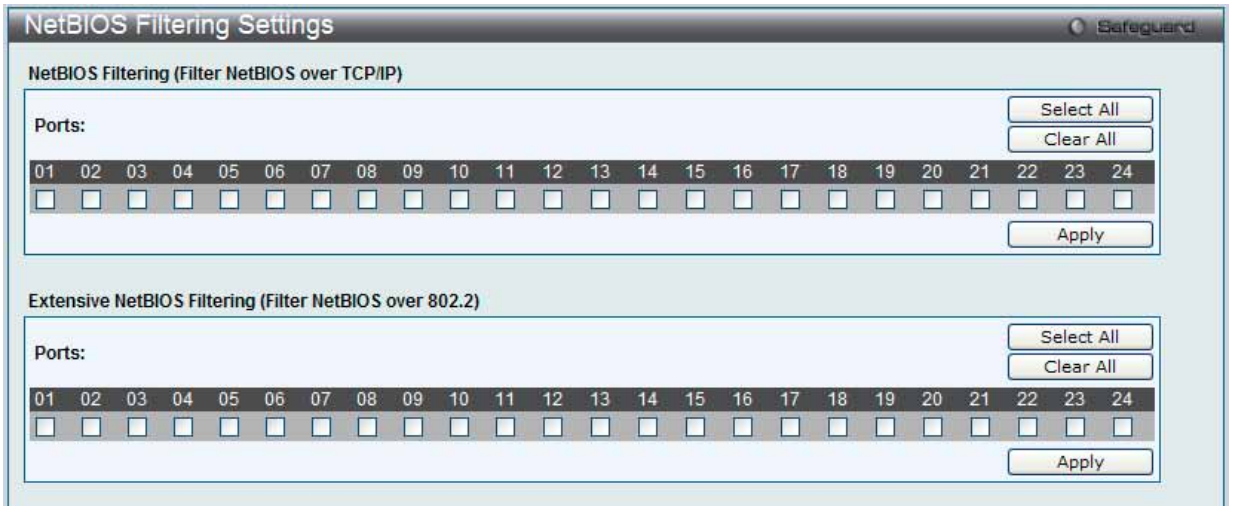


図 7.7-53　NetBIOS Filtering Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
NetBIOS Filtering	
NetBIOS フィルタリング設定に含める適切なポートを選択します。	
Ports	NetBIOS フィルタリング設定に含める適切なポートを簡単にチェックできます。
Extensive NetBIOS Filtering	
Extensive NetBIOS フィルタリング設定に含める適切なポートを選択します。Extensive NetBIOS は 802.3（TCP/IP）における NetBIOS です。スイッチはこれが有効なポートでは 802.3 における NetBIOS フレームを拒否します。	
Ports	Extensive NetBIOS フィルタリング設定に含める適切なポートを簡単にチェックできます。

「Apply」ボタンをクリックして各セクションで行った変更を適用します。

「Select All」ボタンをクリックすると設定用にすべてのポートを選択します。
「Clear All」ボタンをクリックして、すべてのポートを削除します。

DHCP Server Screening（DHCP サーバスクリーニング）

本機能では、ユーザはすべての DHCP サーバパケットを制限できるだけでなく、指定したどの DHCP クライアントからの DHCP サーバパケットも受信することが可能になります。この機能は 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と区別するのに役に立ちます。

初めて DHCP フィルタを有効にした時にアクセスプロファイルエントリとポートエントリごとのアクセスルールとその他のアクセスルールが作成されます。これらのルールは、すべての DHCP サーバパケットをブロックするのに使用します。さらに、DHCP エントリの許可のために、初めて DHCP クライアント MAC アドレスがクライアント MAC アドレスとして使用される時に、1 つのアクセスプロファイルと 1 つのアクセスルールエントリが作成されます。送信元 IP アドレスは DHCP サーバの IP アドレスと同じになります（UDP ポート番号は 67 です）。これらのルールは、ユーザが設定した特定のフィールドを持つ DHCP サーバパケットを許可するのに使用します。

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されます。

DHCP Server Screening Port Settings（DHCP サーバスクリーニング設定）

DHCP サーバスクリーニングは不正な DHCP サーバへのアクセスを拒否する機能です。この DHCP サーバフィルタ機能が有効になると指定ポートからのすべての DHCP サーバパケットはフィルタされます。

1. **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。

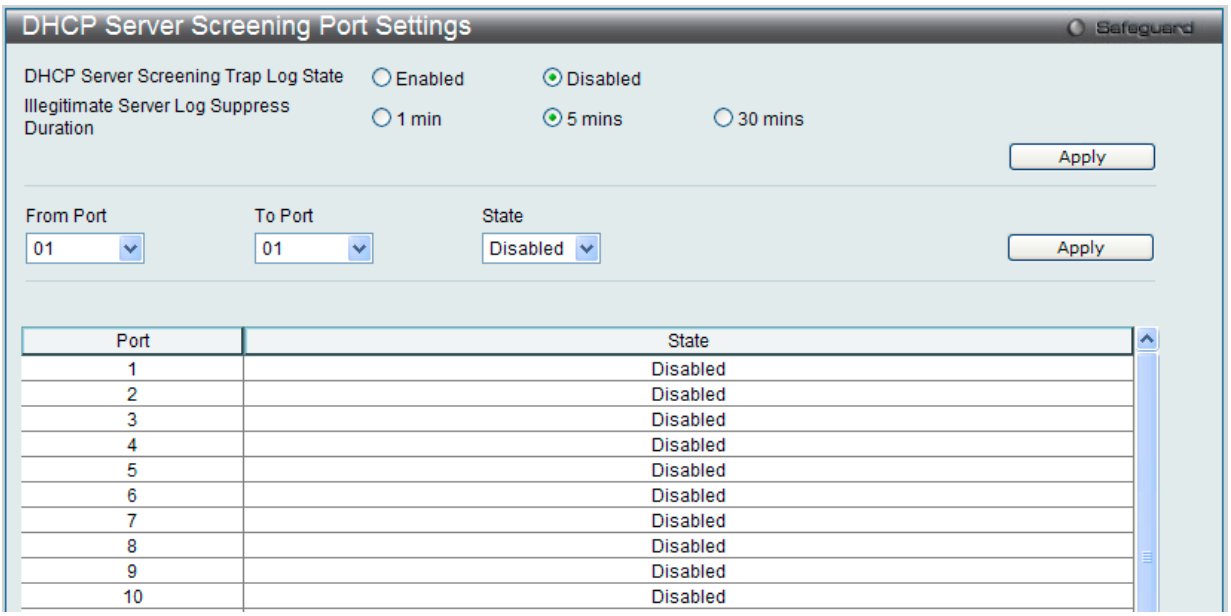


図 7.7-54　DHCP Screening Port Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
DHCP Server Screening Trap Log State	DHCP サーバのトラップとログのフィルタを「Enabled」（有効）または「Disabled」（無効）にします。
Illegitimate Server Log Suppress Duration	不正なサーバログの抑制時間を 1、5、または 30 分から選択します。
From Port/To Port	設定の対象となるポートを指定します。
State	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 Offer Permit Entry Settings（DHCP オファー許可エントリ設定）

許可エントリの追加または削除を行います。

1. **Security > DHCP Server Screening > DHCP Offer Permit Entry Settings** の順にクリックし、画面を表示します。

図 7.7-55　DHCP Offer Permit Entry Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Server IP Address	フィルタを通過させる DHCP サーバを指定します。
Client's MAC Address	DHCP クライアントの MAC アドレスを指定します。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	フィルタする DHCP サーバのポート番号を入力します。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。

エントリの削除

「Delete」ボタンをクリックして、入力した情報に基づいて指定エントリを削除します。

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。

TACACS/XTACACS/TACACS+ または non（認証なし）のメソッド経由でユーザがデバイスへのログインに成功すると、「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に更新したい場合、「enable admin」コマンドを実行し、権限レベルを昇格させる必要があります。しかし、ユーザが RADIUS サーバまたはローカルな方法を経由してデバイスへのログインに成功すると、3 種類の権限レベルをユーザに割り当てることが可能であり、ユーザは「enable admin」コマンドを使用して、権限レベルを昇格させることはできません。

スイッチへのアクセス権を取得したユーザは、スイッチに通常ユーザのアクセス権を与えられています。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。）

Enable Admin（管理者レベルの認証）

本画面は、通常のユーザレベルとしてスイッチにログインした後、管理者レベルに昇格したい場合に使用します。スイッチにログインした後のユーザにはユーザレベルの権限のみが与えられています。管理者レベルの権限を取得するためには、本画面を開き、認証用パスワードを入力します。本機能における認証方法は、TACACS/XTACACS/TACACS+/RADIUS、ユーザ定義のサーバグループ、local enable（スイッチ上のローカルアカウント）または、認証なし（none）から選択できます。XTACACS と TACACS は Enable の機能をサポートしていないため、ユーザはサーバホスト上に特別なアカウントを作成し、ユーザ名「enable」、および管理者が設定するパスワードを登録する必要があります。本機能は認証ポリシーが「Disabled」（無効）である場合には実行できません。

1. **Security > Access Authentication Control > Enable Admin** の順にメニューをクリックし、以下の画面を表示します。

図 7.7-56　Enable Admin 画面

2. 「Enable Admin」ボタンをクリックして以下のダイアログボックスを表示します。

図 7.7-57　ユーザ名とパスワード入力ダイアログボックス

3. 「ユーザー名」と「パスワード」を入力して「OK」ボタンをクリックします。「ユーザー名」と「パスワード」が承認されると、ユーザ権限は管理者特権レベルに変更されます。

Authentication Policy Settings（認証ポリシー設定）

スイッチにアクセスするユーザのために管理者が定義した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。

1. **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 7.7-58　Authentication Policy Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Authentication Policy	スイッチの認証ポリシーを「Enabled」（有効）または「Disabled」（無効）に設定します。
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。

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、HTTP）を設定します。

1. **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。

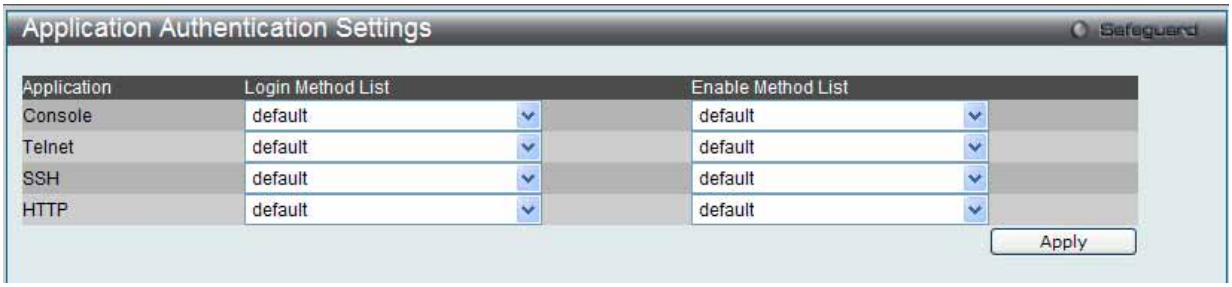


図 7.7-59　Application Authentication Settings 画面

2. 以下の項目を使用して設定および参照します。

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 Settings」画面を参照してください。
Enable Method List	プルダウンメニューにより、登録済みのメソッドリストを使用してユーザレベルを管理者レベルに昇格させるアプリケーションを選択します。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 Settings」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 Settings（認証サーバグループ設定）

スイッチ上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。

1. **Security > Access Authentication Control > Authentication Server 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。

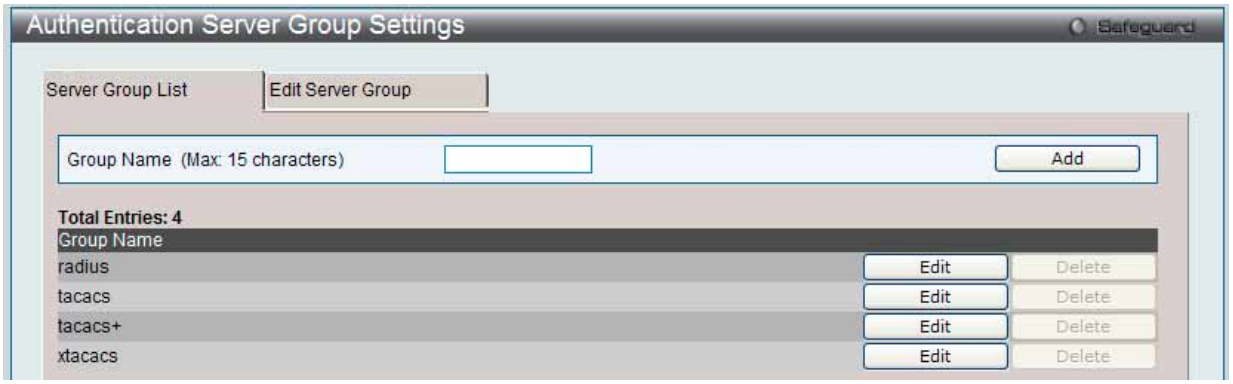


図 7.7-60　Authentication Server Group Settings 画面 - Server Group List タブ

スイッチの認証サーバグループを表示します。スイッチには 4 つの認証サーバグループが組み込まれています。これらは削除できませんが、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。

2. 以下の項目を使用して設定および参照します。

項目	説明
Group Name	新規サーバグループ名を指定します。

新しいサーバグループの作成

「Group Name」欄に名前を入力し、「Add」ボタンをクリックします。

サーバグループの編集

1. 対応する「Edit」ボタンをクリックするか、またはこの画面の上の「Edit Server Group」タブをクリックし、以下の画面を表示します。

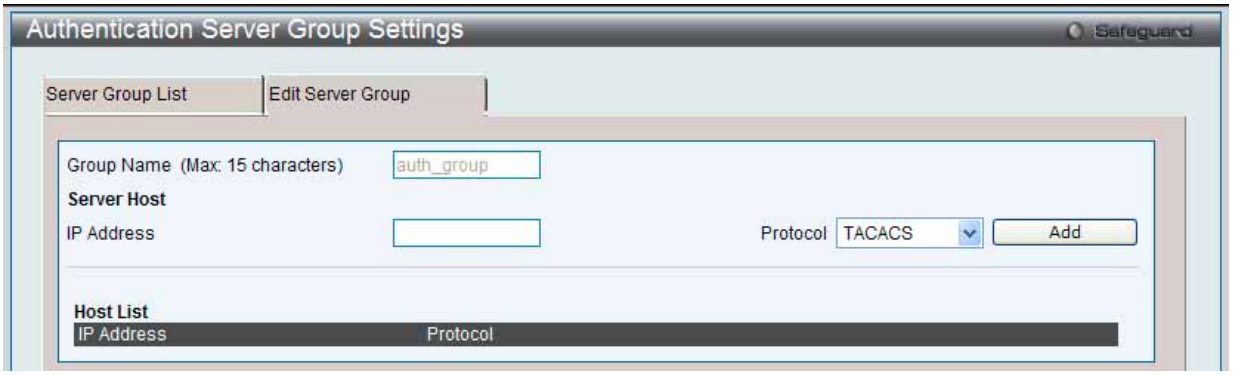


図 7.7-61　Authentication Server Group Settings 画面 - Edit Server Group タブ

2. 以下の項目を使用して設定および参照します。

項目	説明
Group Name	サーバグループ名を指定します。
IP Address	サーバホストの IP アドレスを入力します。
Protocol	プルダウンメニューを使用して、認証サーバホストの IP アドレスに割り当てるプロトコルを選択します。

リストに認証サーバホストを追加するためには、「Group Name」欄にホストの名称、「IP Address」フィールドにホストの IP アドレスを入力し、プルダウンメニューから認証サーバホストの IP アドレスに関連付けるプロトコルを指定します。その後「Add」ボタンをクリックすると、本認証サーバホストがグループに登録されます。エントリはこのタブの「Host List」に表示されます。

注意　認証サーバホストをリストに追加する前に、「Authentication Server Settings」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 Settings（認証サーバ設定）

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。

1. **Security > Access Authentication Control > Authentication Server Settings** の順にメニューをクリックし、以下の画面を表示します。

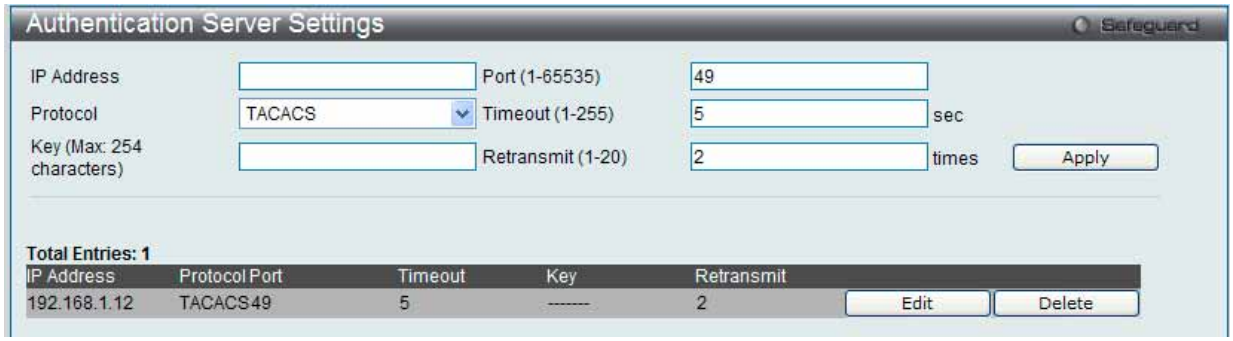


図 7.7-62　Authentication Server Settings 画面

2. 以下の項目を使用して設定および参照します。

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。
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（1-65535）。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。
Protocol	サーバホストが使用するプロトコルを選択します。 • 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。 • 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	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。
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）を指定します。初期値は 5（秒）です。
Retransmit (1-20)	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を入力します。TACACS+ に設定しても効果はありません。初期値は 2 です。

「Apply」ボタンをクリックし、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。

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て、以下の画面を表示します。

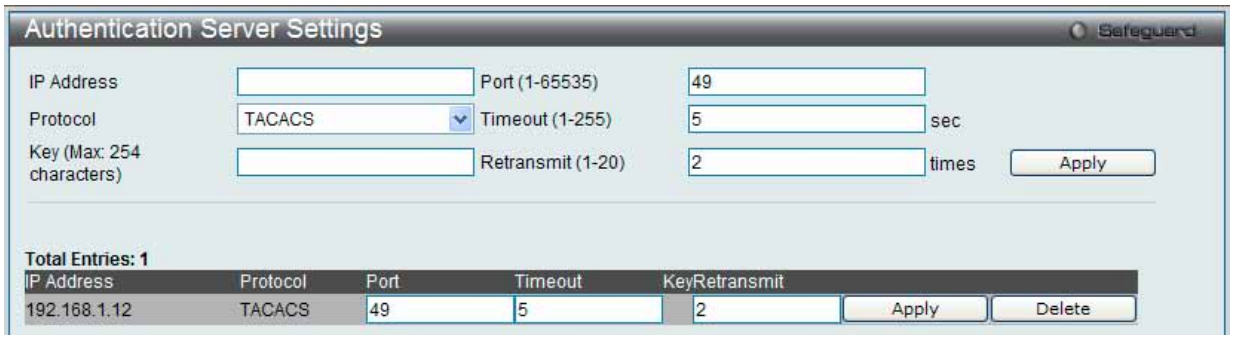


図 7.7-63　Authentication Server Settings 画面 - Edit

2. 指定エントリを編集して「Apply」ボタンをクリックします。

エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。

Login Method Lists Settings（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。本メニュー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。

Security > Access Authentication Control > Login Method Lists 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 7.7-64　Login Method Lists Settings 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。

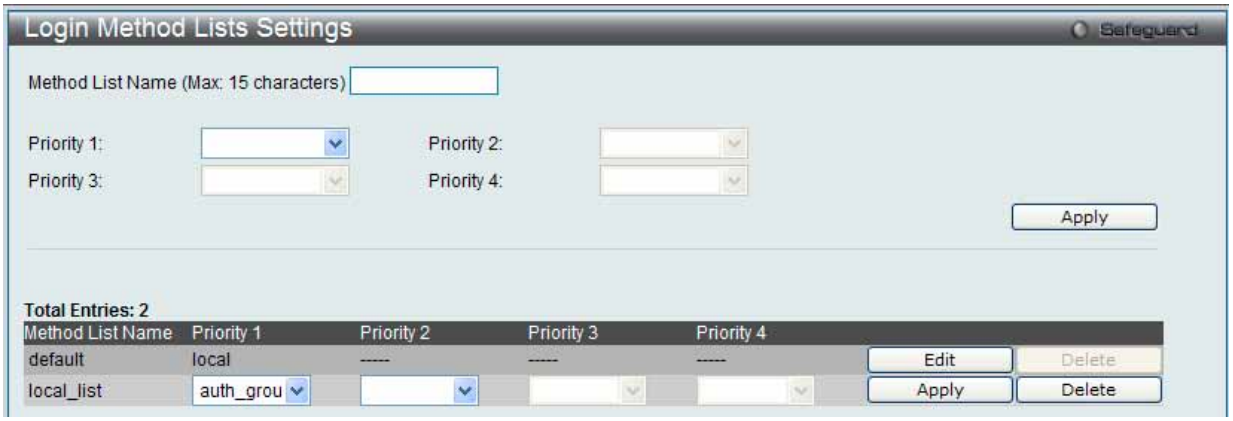


図 7.7-65　Login Method Lists 画面 - Edit

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

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 Settings（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「Local Enable Password Settings（ローカルユーザパスワード設定）」（303 ページ）の項を参照してください。

1. **Security > Access Authentication Control > Enable Method Lists 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。

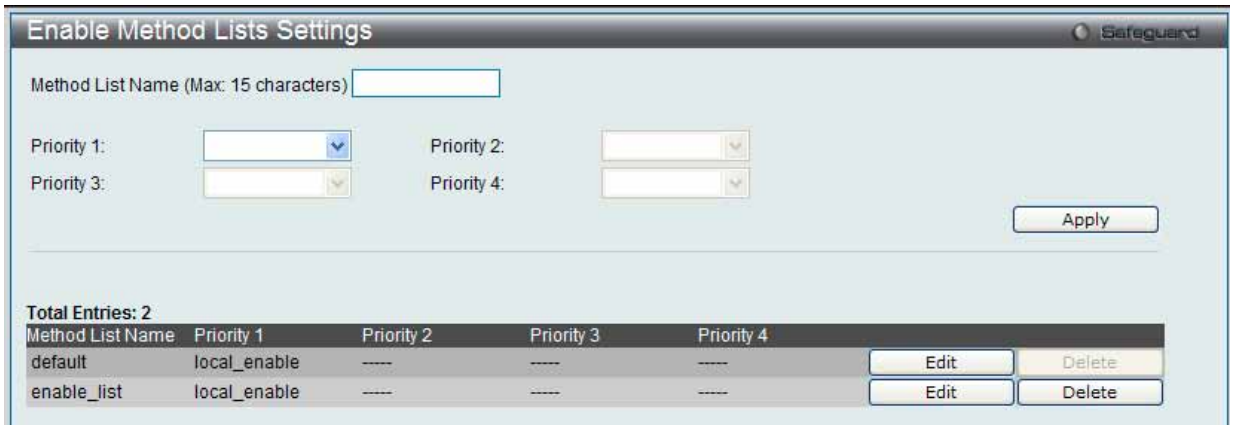


図 7.7-66　Enable Method Lists Settings 画面

2. 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「Local Enable Password Settings（ローカルユーザパスワード設定）」（303 ページ）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。

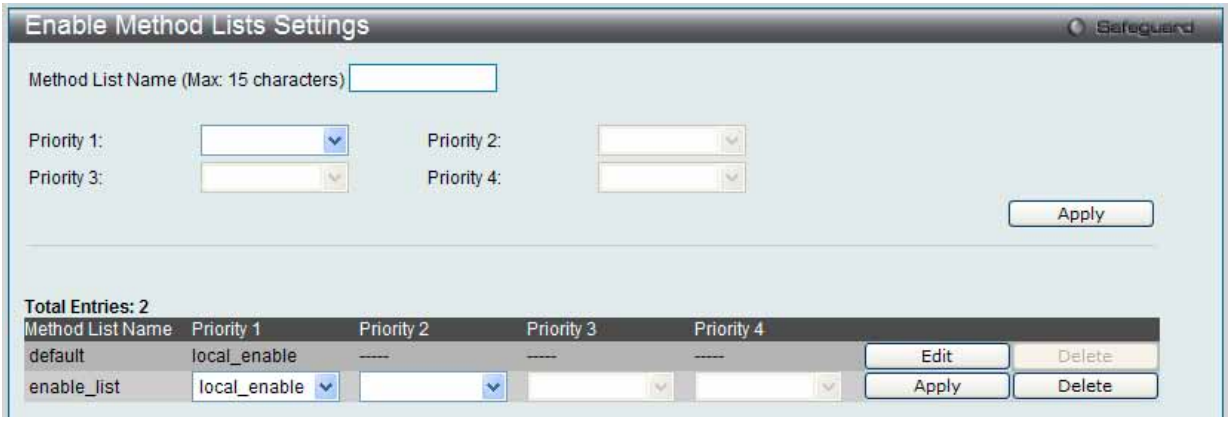


図 7.7-67　Enable Method Lists 画面 - Edit

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。

1. **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 7.7-68　Local Enable Password Settings 画面

2. 以下の項目を使用して、Local Enable Password を設定します。

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。

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。

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。

「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。

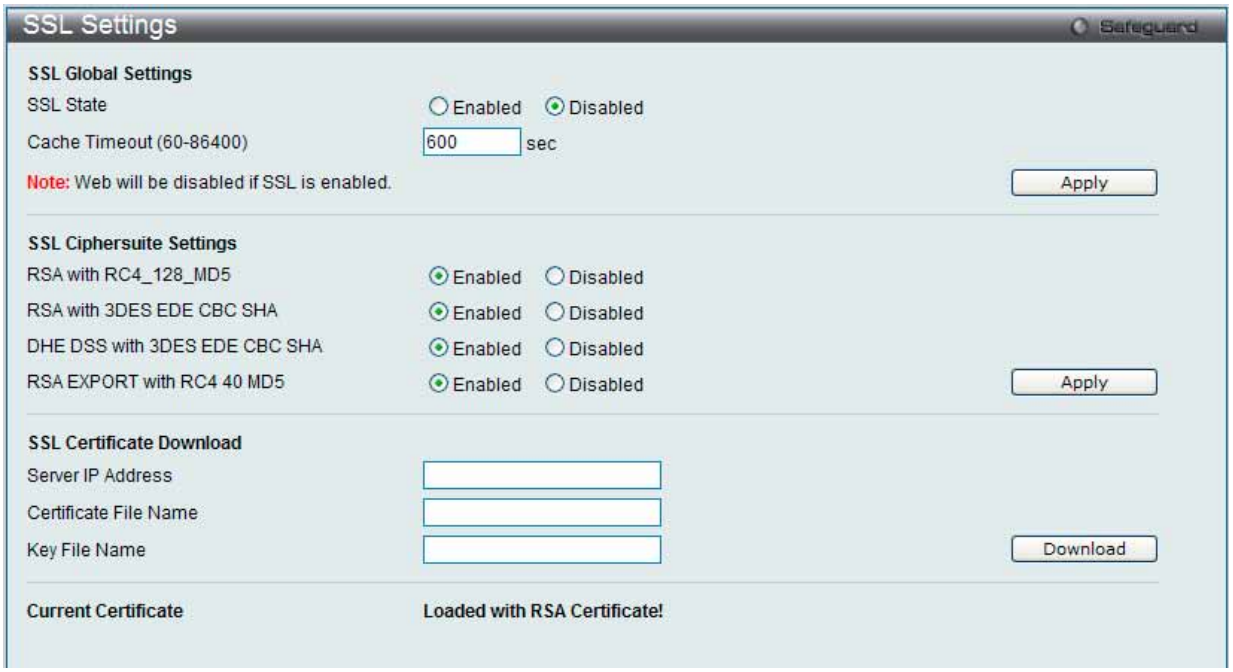


図 7.7-69　SSL Settings 画面

SSL 機能の設定

「SSL Global 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 Global 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 の機能と構成に関するいくつかの機能は本スイッチの Web ベースマネジメントでは利用できません。コマンドラインインタフェースを使用して設定します。

注意　SSL 機能が有効になると Web ベースマネ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 Web ブラウザのアドレスフィーウドに URL の最初が https:// で始まるアドレスを指定してください。他のアドレスを入力するとエラーとなり、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. **System 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 Lists」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 Authentication Method 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 Settings」画面で、SSH を有効にします。

これらの手順が完了後、安全な帯域内の接続でスイッチの管理を行うために、リモート PC 上の SSH クライアントの設定を行います。

SSH 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。

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

図 7.7-70　SSH Settings 画面

2. 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。
TCP Port Number (1-65535)	SSH に使用する TCP 番号を入力します。初期値は 22 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 Authentication Method 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。

1. **Security > SSH > SSH Authentication Method 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。

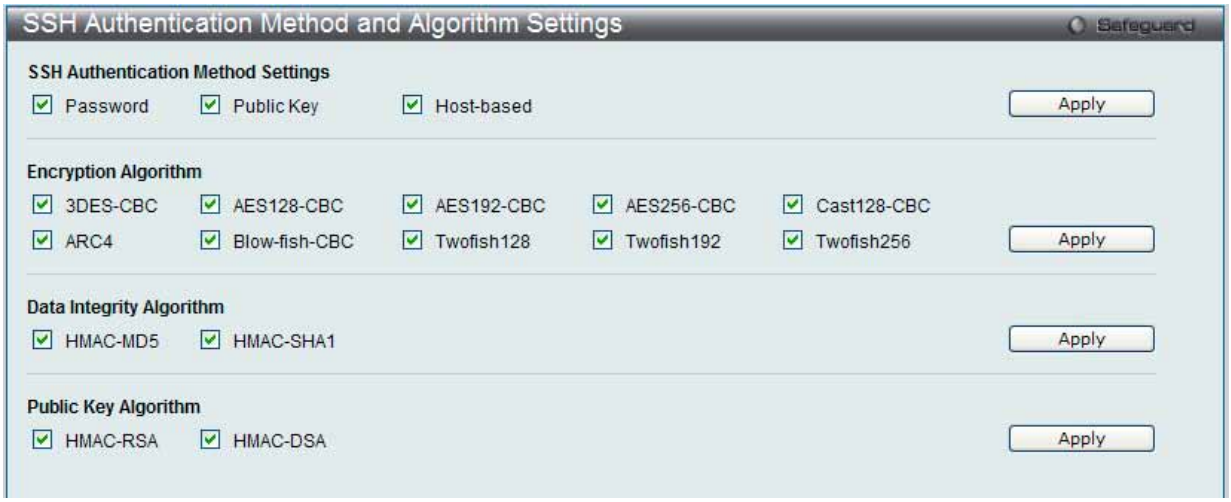


図 7.7-71　SSH Authentication Method and Algorithm Settings 画面

2. 以下のアルゴリズムが設定できます。

項目	説明
SSH Authentication Method 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 ユーザ認証リスト）

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 7.7-72　SSH User Authentication List 画面

上記画面例のユーザアカウントは **System 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

1. 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。

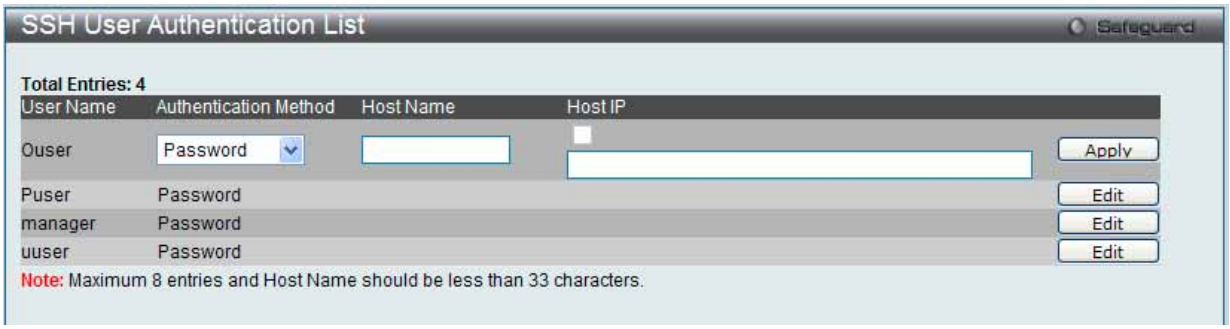


図 7.7-73　SSH User Authentication Lists 画面 - Edit

2. 以下の項目を使用して設定および参照します。

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。
Authentication Method	スイッチにアクセスを試みるユーザの認証モードを以下から指定します。 • Host-Based - 認証用にリモート SSH サーバを使用する場合に選択します。本項目を選択すると、SSH ユーザ識別のために以下の情報を入力することが必要になります。 - 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 32 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「Authentication Mode」欄で「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「User Accounts Settings（ユーザアカウントの設定）」（63 ページ）を参照してください。

Trusted Host（トラストホスト）

最大 30 個までのトラストホストのセキュアな IP アドレスが、リモートのスイッチ管理のために設定され、使用できます。1 個以上のトラストホストが使用可能な状態にあると、スイッチは直ちに指定 IP アドレスからのリモートアクセスのみ許可することにご注意ください。この機能を有効にする場合、はじめに現在使用している IP アドレスを入力してください。

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

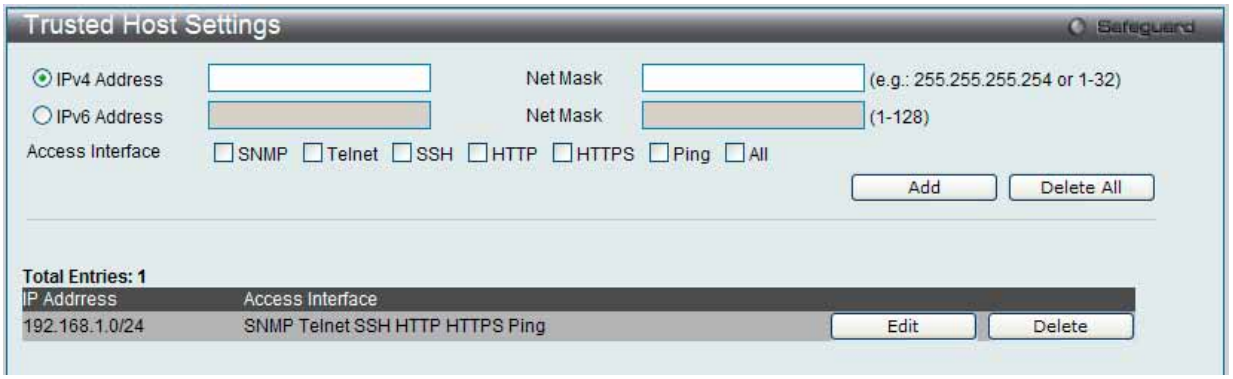


図 7.7-74　Trusted Host 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
IPv4 Address	IPv4 アドレスを入力してトラストホストリストに追加します。
IPv6 Address	IPv6 アドレスを入力してトラストホストリストに追加します。
Net Mask	ネットマスクを入力してトラストホストリストに追加します。
Access Interface	トラストホストに許可するサービスを選択します。

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

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て、以下の画面を表示します。

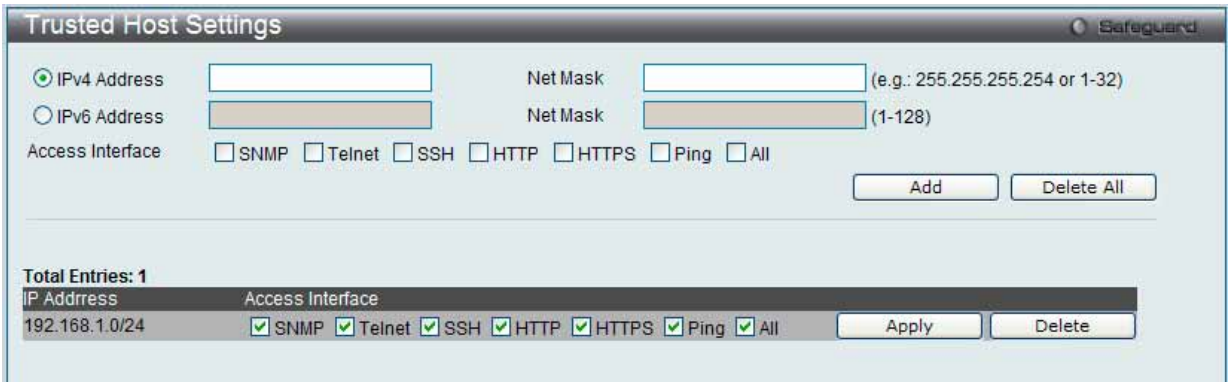


図 7.7-75　Trusted Host Settings 画面 - Edit

2. 指定エントリを編集して「Apply」ボタンをクリックします。

エントリの削除

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

Safeguard Engine Settings（セーフガードエンジン設定）

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。これらの攻撃はスイッチに能力以上の負荷を加え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、限られたリソース内で必要不可欠なパケットの送受信を可能にします。セーフガードエンジンには、Strict と Fuzzy の 2 つの操作モードがあります。「Strict」モードでは、スイッチが (a) 処理能力を超えた量のパケットを受信した場合、または (b) メモリ使用率が高すぎる場合には、「Exhausted」モードに遷移します。本モードでは、スイッチは算出された間隔で、すべての ARP と IP ブロードキャストパケットを廃棄します。スイッチは 5 秒おきにパケットフラッディングが発生していないかチェックをします。パケット数がしきい値を超えると、スイッチはまず、すべての入力 ARP および IP ブローキャストパケットを 5 秒間停止させます。その 5 秒後に、スイッチは再びパケットの入力フローをチェックします。フラッディングが解消されていれば、スイッチは再びすべてのパケットを受信し始めます。逆に、まだフラッディングが認められれば、前回の 2 倍の時間（10 秒）、すべての入力 ARP および IP ブローキャストパケットを停止させます。パケットの停止時間は、最大時間（320 秒）に達するまで倍増していき、それ以降は、通常の入力フローに戻るまで 320 秒で行われます。このしくみを以下に例示します。

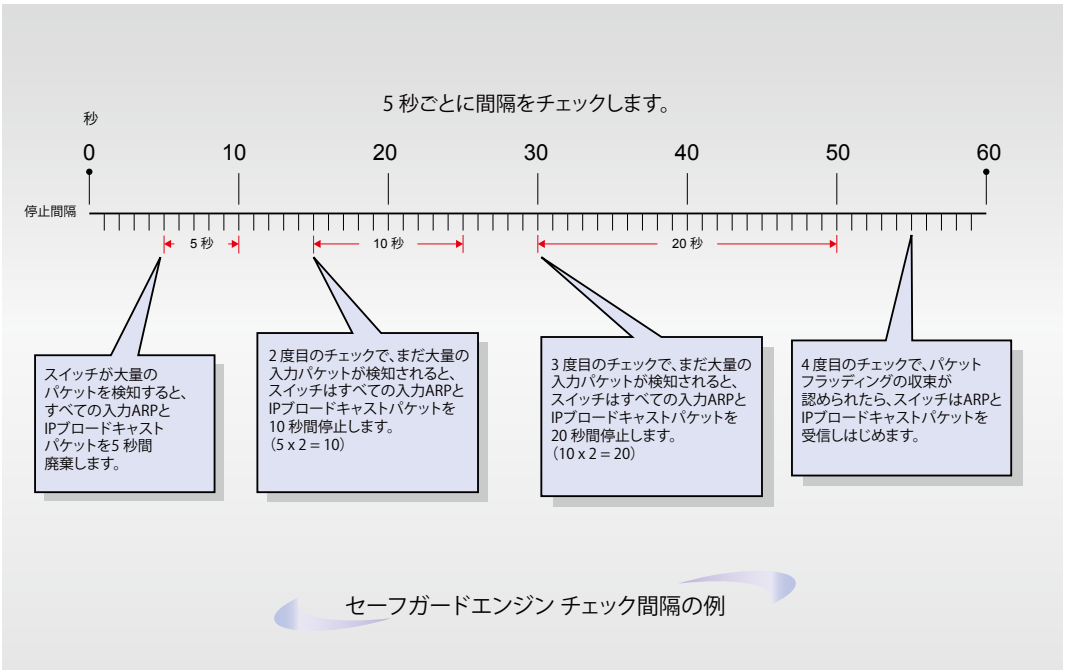


図 7.7-76　セーフガードエンジンの例

パケットのフラッディングの問題を軽減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、信頼できない IP アドレスからの受信 ARP および IP ブロードキャストパケットを破棄す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 および IP ブロードキャスト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 および IP ブロードキャストパケットを破棄する間隔を 5 秒に戻してプロセスを再開します。

Fuzzy モードでは、一度セーフガードエンジンは Exhausted モードになると、パケットフローは本モード開始時の半分のレベルまで減少させます。Normal モードに戻ると、パケットを 25%ずつ増加させます。スイッチは、その後間隔をチェックし、スイッチのオーバロードを避けるように動的に通常のパケットフローに戻します。

注意　セーフガードエンジンが有効の場合、本スイッチは FFP（Fast Filter Processor）メータリングテーブルを使用し、各トラフィックフロー（ARP、IP）に帯域を割り当て、CPU 使用率を制御することでトラフィックを制限します。これは、ネットワーク上のトラフィックのルーティング速度を制限します。

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 Settings の順にクリックし、以下の画面を表示します。

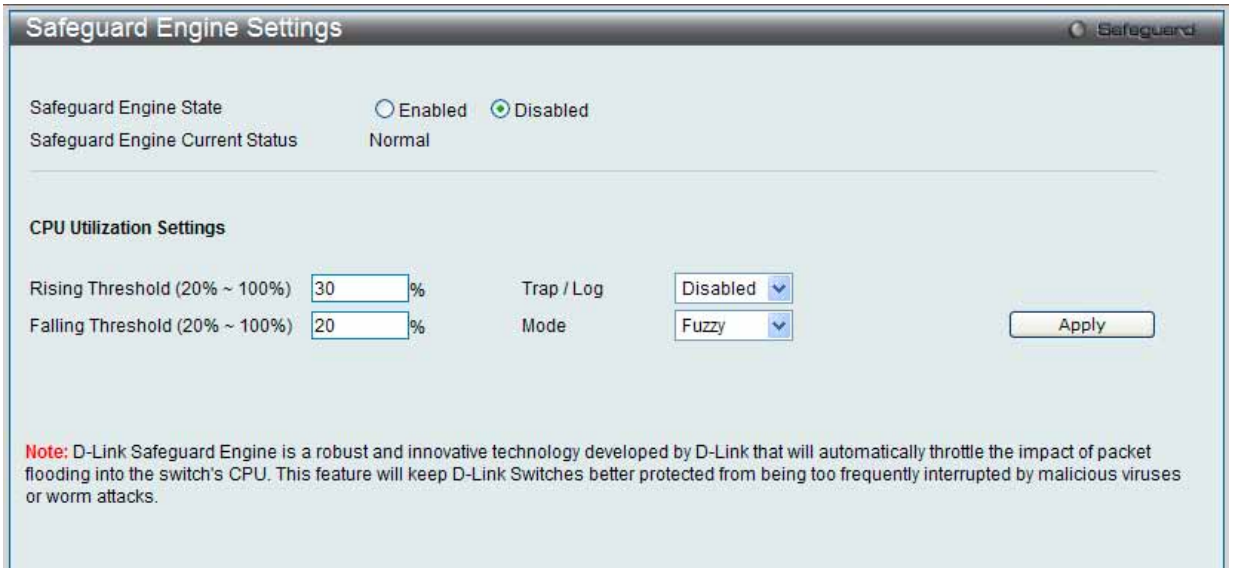


図 7.7-77　Safeguard Engine Settings 画面

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。

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て設定および参照します。

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 Safeguard Engine 状態から 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。

Captive Portal（キャプティブポータル）

Captive Portal（CP）は、有線 / 無線ユーザ両方についてネットワークへの接続性を制御する機能です。ここでは、ゲストと認証ユーザーにアクセスを許可するための検証を設定します。

注意 「Captive Portal (CP)」フォルダはナビゲーション画面の「WLAN」タブからもアクセスできます。本フォルダ内のどの設定も「WLAN」タブの「Captive Portal (CP)」フォルダと全く同じです。

Global Configuration（グローバル設定）

グローバルに CP 設定を行います。

1. **Security > Captive Portal (CP) > Global 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。

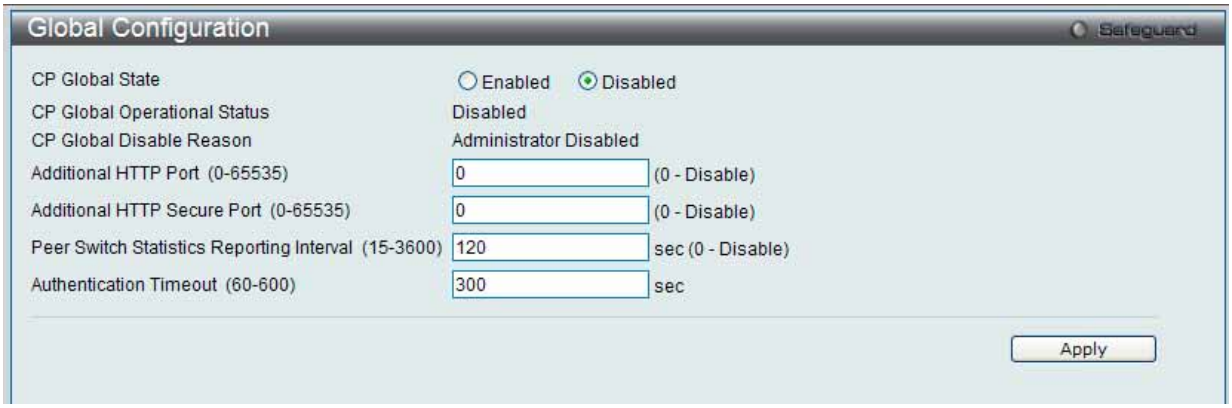


図 7.7-78　Global Configuration 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
CP Global State	CP のグローバル状態を「Enabled」（有効）/「Disabled」（無効）にします。
CP Global Operational Status	CP の操作状態を表示します。
CP Global Disable Reason	キャプティブポータルが無効にされた場合に、本欄ではその理由を表示します。 表示可能な理由は以下の通りです。: • Administrator Disabled（管理者が無効にした） • IP Address Not Configured（IP アドレスが未設定） • No IP Routing Interface and Routing Disabled（IP ルーティングインタフェースがなく、ルーティングは無効）
Additional HTTP Port (0-65535)	追加 HTTP ポート番号（0-65535 の範囲、80 と 443 は除く）を入力します。80 は HTTP デフォルトポート、および 443 は HTTPS デフォルトポートに予約されています。初期値は 0 で、これは追加ポートは使用されていないことを示しています。
Additional HTTP Secure Port (0-65535)	追加 HTTP ポート番号（0-65535 の範囲、80 と 443 は除く）を入力します。80 は HTTP デフォルトポート、および 443 は HTTPS デフォルトポートに予約されています。初期値は 0 で、これは追加ポートは使用されていないことを示しています。
Peer Switch Statistics Reporting Interval (15-3600)	クラスタリングがスイッチにサポートされている場合は、ピアスイッチが認証済みクライアントの統計情報をクラスタコントローラに送信する頻度を入力します。レポート間隔は 0 および 15-3600（秒）です。値 0 は機能を無効にすることを意味します。初期値は 120 です。
Authentication Timeout (60-600)	認証時間を入力します。CP ユーザは時間内に有効な証明書を入力しないと、クライアントがネットワークへのアクセスを獲得するために、再度認証ページを表示する必要があります。値は 60-600（秒）です。

「Apply」ボタンをクリックして各セクションで行った変更を適用します。

CP Configuration（CP 設定）

CP コンフィグレーションを作成します。

1. **Security > Captive Portal (CP) > CP 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 7.7-79　CP configuration - CP Summary タブ画面

以下の項目を使用して設定および参照します。

項目	説明
CP Configuration	CP コンフィグレーション名を入力します。
Configuration	CP ID と名前を表示します。
Mode	CP が有効か否かを表示します。
Protocol	ポータルが HTTP または HTTPS のどちらを使用するかを表示します。
Verification	実行するユーザ検証のタイプを表示します。 • Guest - ユーザはデータベースに認証される必要がありません。 • Local - スイッチは認証ユーザに対してローカルデータベースを使用します。 • RADIUS - スイッチはユーザを認証するためにリモート RADIUS サーバのデータベースを使用します。
Languages	このキャプティブポータルに設定される言語の数を表示します。

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

エントリの追加

「CP Configuration」を入力し、「Add」ボタンをクリックして新しいエントリを追加します。指定した名前で新しくタブが表示されます。

エントリの削除

特定エントリのボックスをチェック後、「Delete」ボタンをクリックして指定エントリを削除します。

CP コンフィグレーションの詳細情報設定

1. テーブル内の「Configuration」下のリンク、または設定する CP コンフィグレーション名のタブをクリックして、以下の画面を表示します。

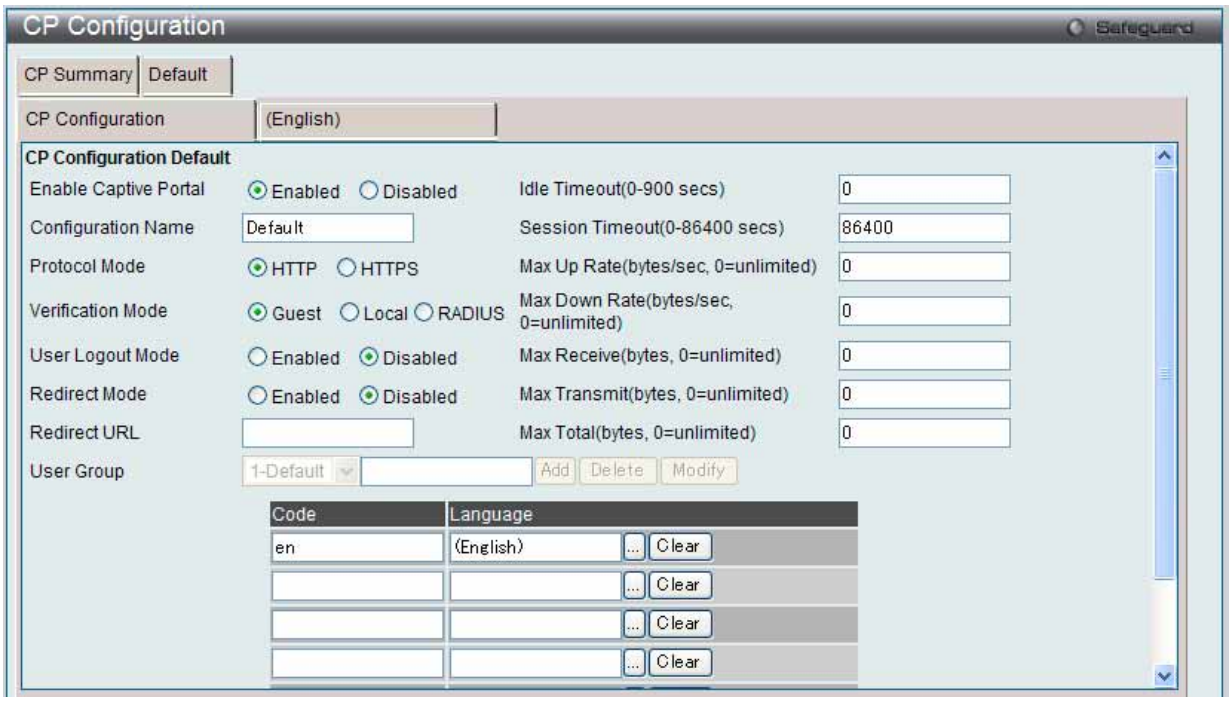


図 7.7-80　CP Configuration - Edit 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Enable Captive Portal	ラジオボタンを使用して CP コンフィグレーションを「Enabled」（有効）/「Disabled」（無効）にします。
Configuration Name	編集するコンフィグレーション名を入力します。
Protocol Mode	検証処理で CP コンフィグレーションを使用するプロトコル（HTTP または HTTPS）のラジオボタンをクリックします。
Verification Mode	ラジオボタンをクリックして、クライアントを検証するモードを選択します。 • Guest - ユーザはデータベースに認証される必要がありません。 • Local - スイッチは認証ユーザに対してローカルデータベースを使用します。 • RADIUS - スイッチはユーザを認証するためにリモート RADIUS サーバのデータベースを使用します。
User Logout Mode	ラジオボタンをクリックして、認証ユーザがネットワークから認証解除を行うことを「Enabled」（有効）/「Disabled」（無効）にします。
Redirect Mode	ラジオボタンを使用して CP コンフィグレーションのリダイレクトモードを「Enabled」（有効）/「Disabled」（無効）にします。
Redirect URL	「Redirect Mode」が有効である場合、新たに認証されたクライアントがリダイレクトされる URL を入力します。
Idle Time	自動的にログアウトされるまでユーザが待機できる時間（秒）を入力します。値 0 はタイムアウトが行われないことを示します。初期値は 0 です。
Session Timeout	セッション終了までの待ち時間を入力します。セッションタイムアウトになると、ユーザはログアウトされます。値 0 はタイムアウトが行われないことを示します。
Max Up Rate	CP の使用時にクライアントがデータを送信できる最高速度（バイト / 秒）を入力します。速度の範囲は 0-536870911 です。
Max Down Rate	CP の使用時にクライアントがデータを受信できる最高速度（バイト / 秒）を入力します。速度の範囲は 0-536870911 です。
Max Receive	CP の使用時にクライアントが受信できる最大バイト数を入力します。この制限に到達すると、ユーザは切断されます。
Max Transmit	CP の使用時にクライアントが送信できる最大バイト数を入力します。この制限に到達すると、ユーザは切断されます。
Max Total	クライアントが送受信できる最大バイト数の合計を入力します。この制限に到達すると、ユーザは切断されます。
User Group	「Verification Mode」に「Local」または「RADIUS」を選択した場合、ユーザグループを割り当てる必要があります。グループに所属するすべてのユーザが、このポータル経由でネットワークにアクセスすることが許可されます。CP すべてにユーザグループを作成、削除、または編集することができます。 • プルダウンメニューから CP に割り当てる定義済みユーザグループを選択します。 • 新しいユーザグループを作成するためには、本欄に名前を入力し、「Add」ボタンをクリックします。 • 既存のユーザグループ名を変更するためには、プルダウンメニューから変更する名前を選択し、新しい名前をフィールドに入力して、「Modify」ボタンをクリックします。
Code	言語に対して IANA 言語サブタグコードを入力します。すべてのコードが IANA 言語サブタグレジストリに表示されます。スイッチが言語をサポートしている場合、言語を選択すると自動的に入力されます。
Language	「…」ボタンをクリックして、CP に使用する言語を選択します。「Clear」ボタンをクリックして、リストから言語を削除します。

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

設定のクリア

「Clear」ボタンをクリックして、すべてのコンフィグレーションを一掃し、初期設定に戻します。

CP Web ページのカスタマイズ

言語タブをクリックして、CP Web ページをカスタマイズします。

例えば、キャプティブポータルページの英語版をカスタマイズするためには、（English）タブをクリックします。Web ページは無線クライアントがアクセスポイントに接続している場合に表示します。プルダウンメニューを使用して、CP Web 用に別の Web ページをカスタマイズします。

Global Parameters（グローバルパラメータ）

1. 画面上部のプルダウンメニューから「Global Parameters」を選択して、以下の画面を表示します。

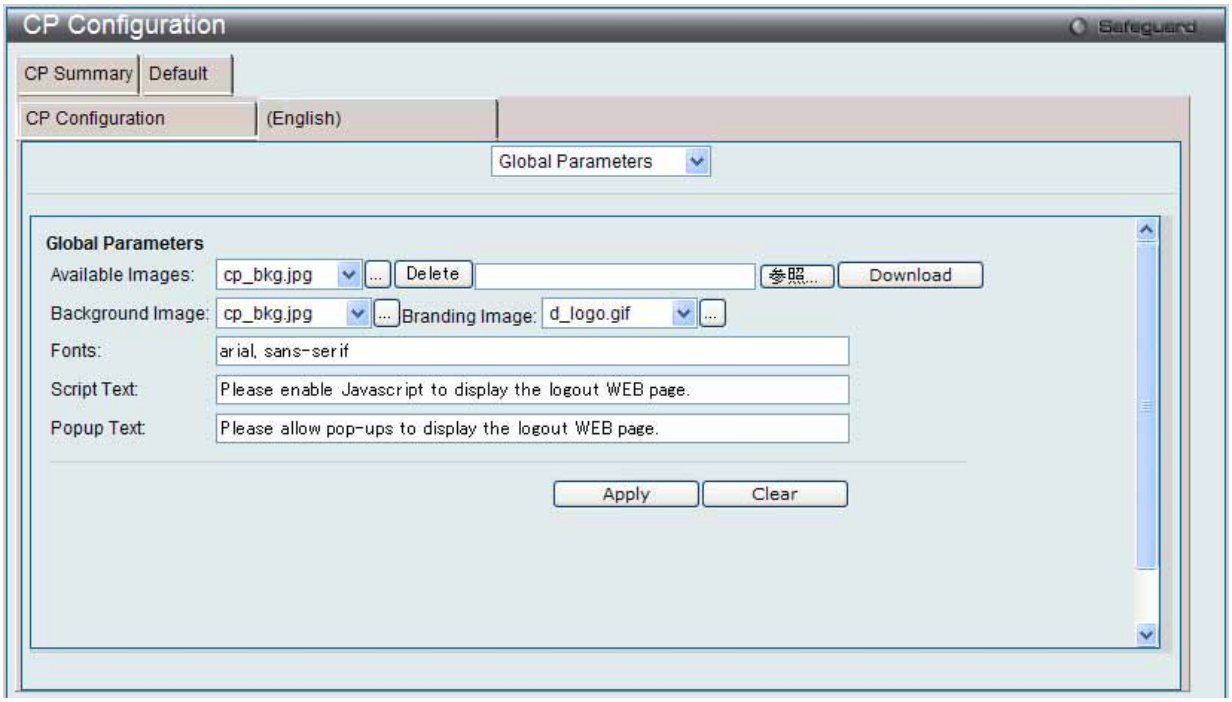


図 7.7-81　CP Configuration - Customize（Global Parameters）画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Available Images	プルダウンメニューにはページ背景、画面タイトルおよびアカウント画像に使用できる画像が表示されます。「…」ボタンをクリックして、画像を参照します。新しい画像を追加するためには、「参照」ボタンをクリックして、ローカルシステムにあるイメージを選択し、「Download」ボタンをクリックして画像をスイッチにダウンロードします。リストから画像を削除する場合は、プルダウンメニューからそのファイル名を選択して「Delete」ボタンをクリックします。削除できるのはダウンロードした画像のみです。
Background Image	プルダウンメニューを使用して、画面背景として表示する画像名を選択します。「…」ボタンをクリックして、利用可能な画像を表示することもできます。選択する画像をクリックします。背景画像を使用しないように設定するためには、プルダウンメニューから <No Selection> を選択します。
Branding Image	プルダウンメニューから画像ファイル名を選択すると、画面左上に表示されます。この画像は会社のロゴなどのようなブランド表示の目的に使用します。「…」ボタンをクリックして、利用可能な画像を表示することもできます。選択する画像をクリックします。ブランド表示を使用しないように設定するためには、プルダウンメニューから <No Selection> を選択します。
Fonts	CP Web ページに使用するフォント名を入力します。
Script Text	ユーザがログアウト Web 画面を表示するために、JavaScript が有効でなければならないことを示すテキストを入力します。「User Logout Mode」が有効である時にだけ、本欄は適用できます。
Popup Text	ユーザがログアウト Web 画面を表示するためには、ポップアップ画面を許可する必要があることを示す情報を入力します。User Logout Mode モードが有効である時にだけ、本欄は適用できます。

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

設定のクリア

「Clear」ボタンをクリックして、すべてのコンフィグレーションを初期設定にリセットします。

Authentication Page（認証ページ）

1. 画面の上部のプルダウンメニューから「Authentication Page」を選択して、以下の画面を表示します。

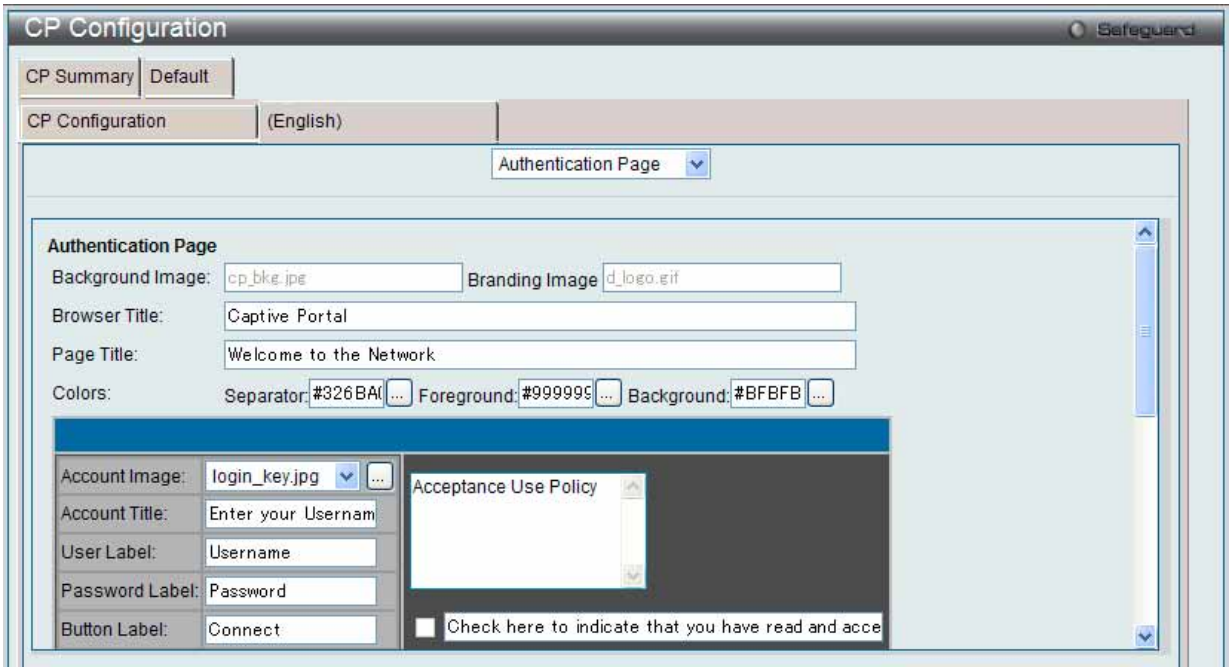


図 7.7-82　CP Configuration - Customize（Authentication Page）画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Background Image	「Authentication」画面に現在の背景画像の名称を表示します。
Branding Image	「Authentication」画面の現在の画面タイトル画像の名称を表示します。
Browser Title	クライアントの Web ブラウザのタイトルバーやタブに表示するテキストを入力します。
Page Title	ページタイトルとして使用するテキストを入力します。
Colors	CP ページの各エリアのカラーを指定します。フィールドにカラーコードを入力するか、または「…」ボタンをクリックして、カラーを選択します。
Account Image	プルダウンメニューを使用して、ログインフィールド上の CP Web ページに表示する画像を選択します。「…」ボタンをクリックして、利用可能な画像を表示することもできます。選択する画像をクリックします。
Account Title	ユーザに認証を行うよう指示するテキストを入力します。
User Label	ユーザ名テキストボックス横に表示するテキストを入力します。
Password Label	パスワードテキストボックスの横に表示するテキストを入力します。
Button Label	ネットワークに接続する時にクリックするボタンに表示するテキストを入力します。
Acceptance Use Policy Text Box	「Acceptance Use Policy」欄に表示するテキストを入力します。「Acceptance Use Policy」は、ユーザがネットワークへの接続を許可される時にその状況を示します。
Acceptance Use Policy Check Box	ユーザが使用条件を承諾すべきこと示すために、ボタンの横に表示するテキストを入力します。
Instructional Text	ユーザに認証を行うよう指示する詳細情報を入力します。このテキストはボタンの下に表示されます。
Denied message	ユーザが有効な認証情報を提供しない場合に表示するメッセージを入力します。
Resource Message	システムリソースの制限のために、システムが認証を拒否した場合に表示するメッセージを入力します。
Timeout Message	認証トランザクションに時間がかかりすぎたことによりシステムが認証を拒否した場合に表示されるメッセージを入力します。
Busy Message	CP 機能が認証リクエストを処理している時に表示されるメッセージを入力します。
No Accept Message	ユーザが「Acceptance Use Policy」をチェックしなかった場合に表示するメッセージを入力します。

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。

設定のクリア

「Clear」ボタンをクリックして、すべてのコンフィグレーションを初期設定にリセットします。

結果の参照

「Preview」ボタンをクリックして、Web ページの結果を参照します。

Welcome Page（ウエルカムページ）

1. 画面の上部のプルダウンメニューから「Welcome Page」を選択して、以下の画面を表示します。:

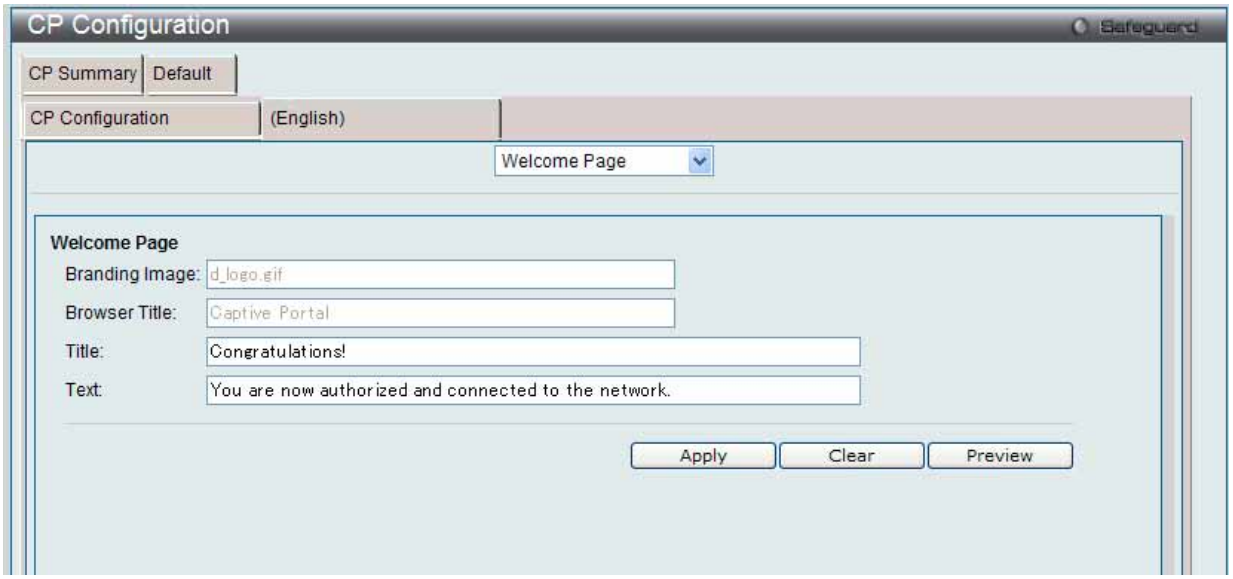


図 7.7-83　CP Configuration - Customize（Welcome Page）画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Branding Image	「Welcome Page」画面における現在の画面タイトル画像の名称を表示します。
Browser Title	クライアントの Web ブラウザのタイトルバーまたはタブに表示するテキストを入力します。
Title	ネットワークへの接続に成功した後に表示するユーザへの挨拶のタイトルを入力します。
Text	CP ユーザがアクセスするネットワークをさらに確認するオプションテキストを入力します。

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

設定のクリア

「Clear」ボタンをクリックして、すべてのコンフィグレーションを初期設定にリセットします。

結果の参照

「Preview」ボタンをクリックして、Web ページの結果を参照します。

Logout Page（ログアウトページ）

1. 画面の上部のプルダウンメニューから「Logout Page」を選択して、以下の画面を表示します。

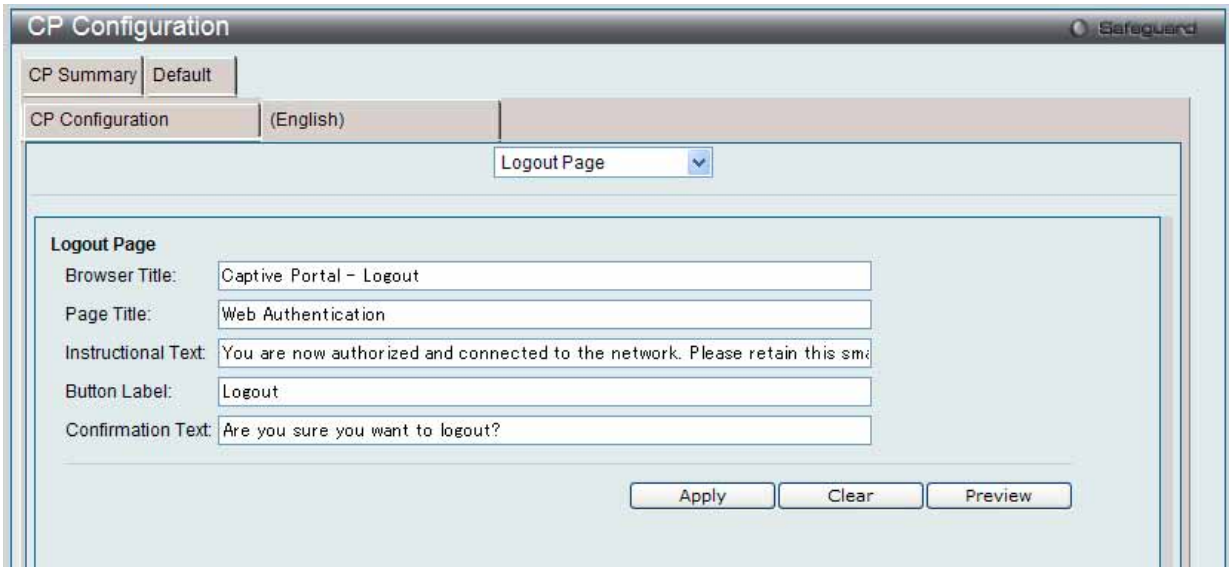


図 7.7-84　CP Configuration - Customize（Logout Page）画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Browser Title	「Logout」画面のタイトルバーに表示するためにテキストを入力します。
Page Title	画面タイトルとして使用するテキストを入力します。
Instruction Text	ユーザが認証されていることを確認し、ユーザに認証解除する方法を指示する詳細情報を入力します。
Button Label	認証を解除するボタンに表示するテキストを入力します。
Confirmation Text	認証の解除処理を確認するメッセージを入力します。

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。

設定のクリア

「Clear」ボタンをクリックして、すべてのコンフィグレーションを初期設定にリセットします。

結果の参照

「Preview」ボタンをクリックして、Web ページの結果を参照します。

Logout Success Page（ログアウト成功ページ）

画面の上部のプルダウンメニューから「Logout Success Page」を選択して、以下の画面を表示します。

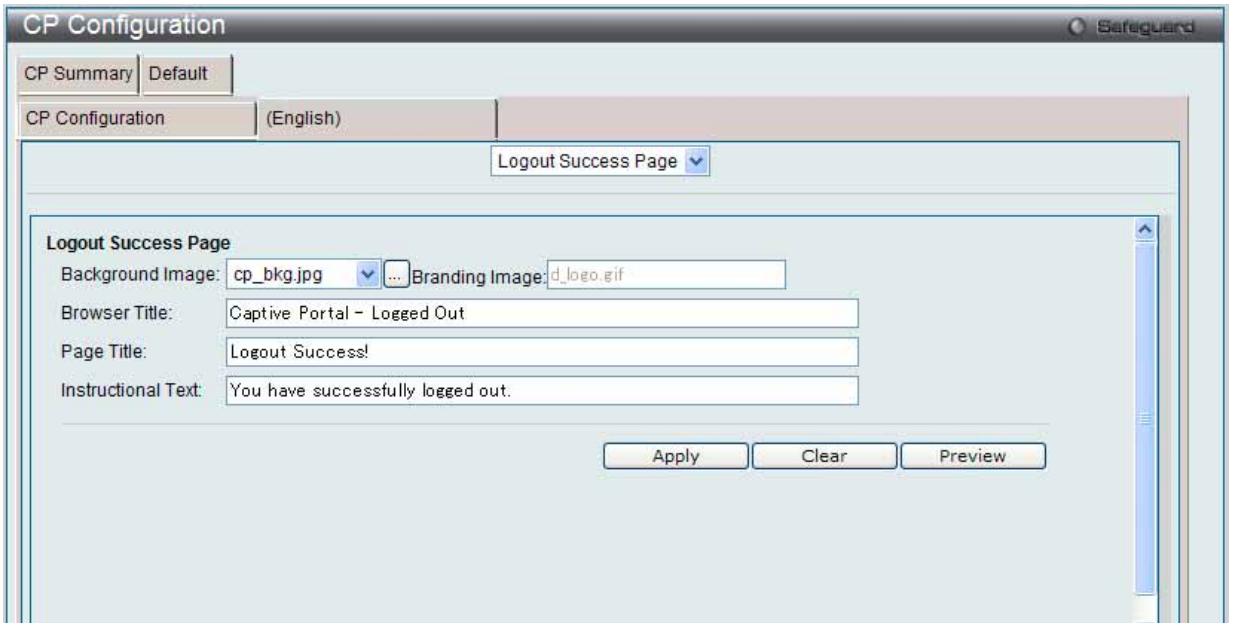


図 7.7-85　CP Configuration - Customize（Logout Success Page）画面

以下の項目を使用して設定および参照します。

項目	説明
Background Image	「Logout Success」画面における現在の背景画像の名称を表示します。
Branding Image	「Logout Success」画面における現在の画面タイトルの名称を表示します。
Browser Title	「Logout Success」画面のタイトルバーに表示するテキストを入力します。
Page Title	画面タイトルとして使用するテキストを入力します。
Instructional Text	ユーザの認証解除を確認する詳細なメッセージを入力します。

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。

設定のクリア

「Clear」ボタンをクリックして、すべてのコンフィグレーションを初期設定にリセットします。

結果の参照

「Preview」ボタンをクリックして、Web ページの結果を参照します。

Local User（ローカルユーザ）

ローカルデータベースに対する認可ユーザの作成、編集、または削除を行います。

Security > Captive Portal (CP) > Local User の順にメニューをクリックし、以下の画面を表示します。

図 7.7-86　Local User - Summary 画面

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

エントリの削除

対応するボックスをチェック後、「Delete」ボタンをクリックして指定エントリを削除します。「Delete All」ボタンをクリックして、表示されたすべてのエントリを削除します。

ユーザの新規登録

新しいユーザを「Local User」データベースに追加します。

1. 「Add」ボタンをクリックして、以下の画面を表示します。

図 7.7-87　Local User - Configuration 画面（Add）画面

2. 以下の項目を使用して設定および参照します。

項目	説明
User Name	ユーザ名を入力します。
Password	ユーザのパスワードを入力します。
User Group	少なくとも 1 つのユーザグループにユーザを割り当てます。複数のグループにユーザを割り当てるためには、「Ctrl」キーを押して、各グループをクリックします。
Session Timeout (secs)	ユーザがネットワークに接続可能な時間（秒）を入力します。「Session Timeout」値に到達すると、ユーザは自動的にログアウトされます。
Idle Timeout (secs)	自動的にログアウトされるまでユーザが待機できる時間（秒）を入力します。
Max Up Rate (bytes/sec)	CP 使用時にトラフィックを送信する最大速度（バイト / 秒）入力します。
Max Down Rate (bytes/sec)	CP 使用時にトラフィックを受信する最大速度（バイト / 秒）を入力します。
Max Receive (bytes)	CP の使用時にユーザが受信できる最大バイト数を入力します。この制限に到達すると、ユーザは切断されます。
Max Transmit (bytes)	CP の使用時にユーザが送信できる最大バイト数を入力します。この制限に到達すると、ユーザは切断されます。
Max Total (bytes)	ユーザが送受信できる最大バイト数を入力します。この制限に到達すると、ユーザは切断されます。

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

エントリの編集

1. 情報を編集する「User」のハイパーリンクをクリックし、以下の画面を表示します。

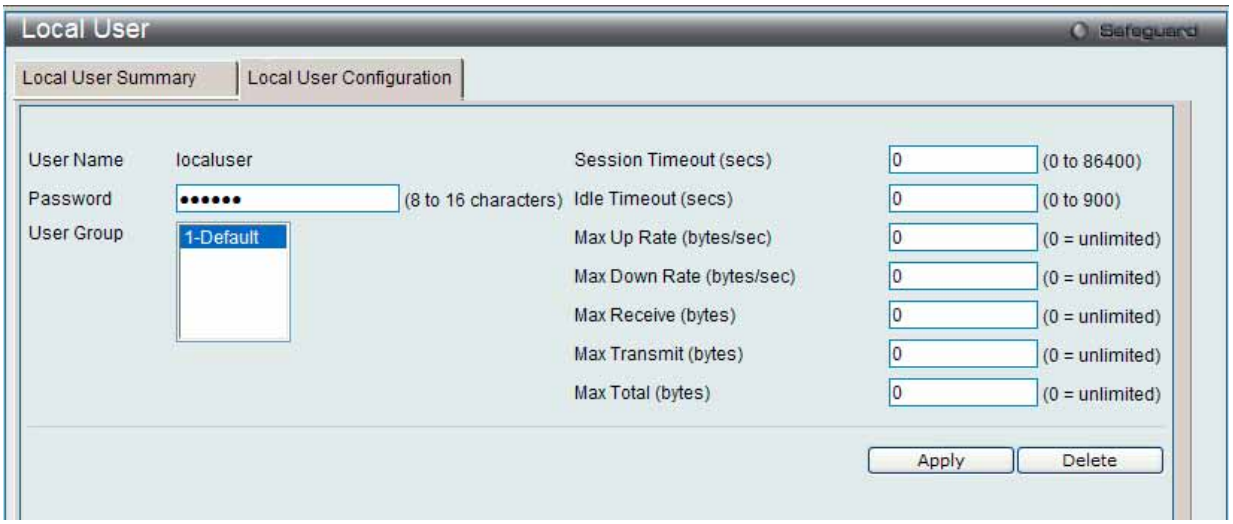


図 7.7-88　Local User - Configuration 画面（Edit）画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Password	ユーザのパスワードを入力します。
User Group	少なくとも 1 つのユーザグループにユーザを割り当てます。複数のグループにユーザを割り当てるためには、「Ctrl」キーを押して、各グループをクリックします。
Session Timeout (secs)	ユーザがネットワークに接続可能な時間（秒）を入力します。「Session Timeout」値に到達すると、ユーザは自動的にログアウトされます。
Idle Timeout (secs)	自動的にログアウトされるまでユーザが待機できる時間（秒）を入力します。
Max Up Rate (bytes/sec)	CP 使用時にトラフィックを送信する最高速度（バイト / 秒）入力します。
Max Down Rate (bytes/sec)	CP 使用時にトラフィックを受信する最高速度（バイト / 秒）を入力します。
Max Receive (bytes)	CP の使用時にユーザが受信できる最大バイト数を入力します。この制限に到達すると、ユーザは切断されます。
Max Transmit (bytes)	CP の使用時にユーザが送信できる最大バイト数を入力します。この制限に到達すると、ユーザは切断されます。
Max Total (bytes)	ユーザが送受信できる最大バイト数を入力します。この制限に到達すると、ユーザは切断されます。

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。

エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。

Interface Association（インタフェースアソシエーション）

設定済み CP をインタフェースに関連付けます。インタフェースは、物理ポートまたは無線ネットワーク（SSID）とすることができます。

1. **Security > Captive Portal (CP) > Interface Association** の順にメニューをクリックし、以下の画面を表示します。

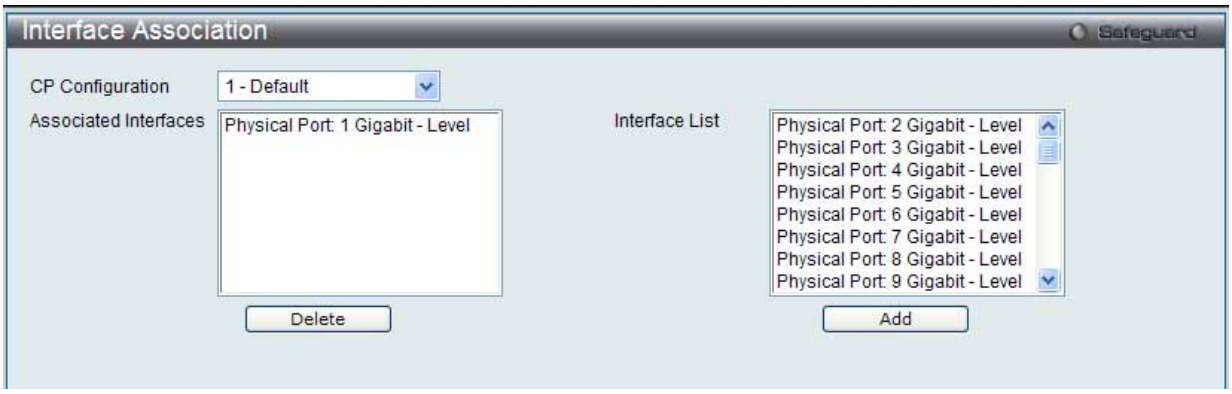


図 7.7-89　Interface Association 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
CP Configuration	プルダウンメニューを使用して、設定する CP を指定します。
Associated Interfaces	CP に関連するすべてのインタフェースを表示します。複数のインタフェースを選択するためには、「Ctrl」キーを押したまま、各インタフェースをクリックします。
Interface List	選択可能なすべてのインタフェースを表示します。複数のインタフェースを選択するためには、「Ctrl」キーを押したまま、各インタフェースをクリックします。

「Add」ボタンをクリックして、「Interface List」ボックス内で選択したインタフェースを「Associated Interfaces」に追加します。

エントリの削除

「Delete」ボタンをクリックして、「Associated Interfaces」ボックスから選択したインタフェースを削除します。

CP Status（CP 状態）

本画面では CP 状態を表示します。

Global Status（グローバル状態）

1. **Security > Captive Portal (CP) > CP Status > Global Status タブ**の順にメニューをクリックし、以下の画面を表示します。

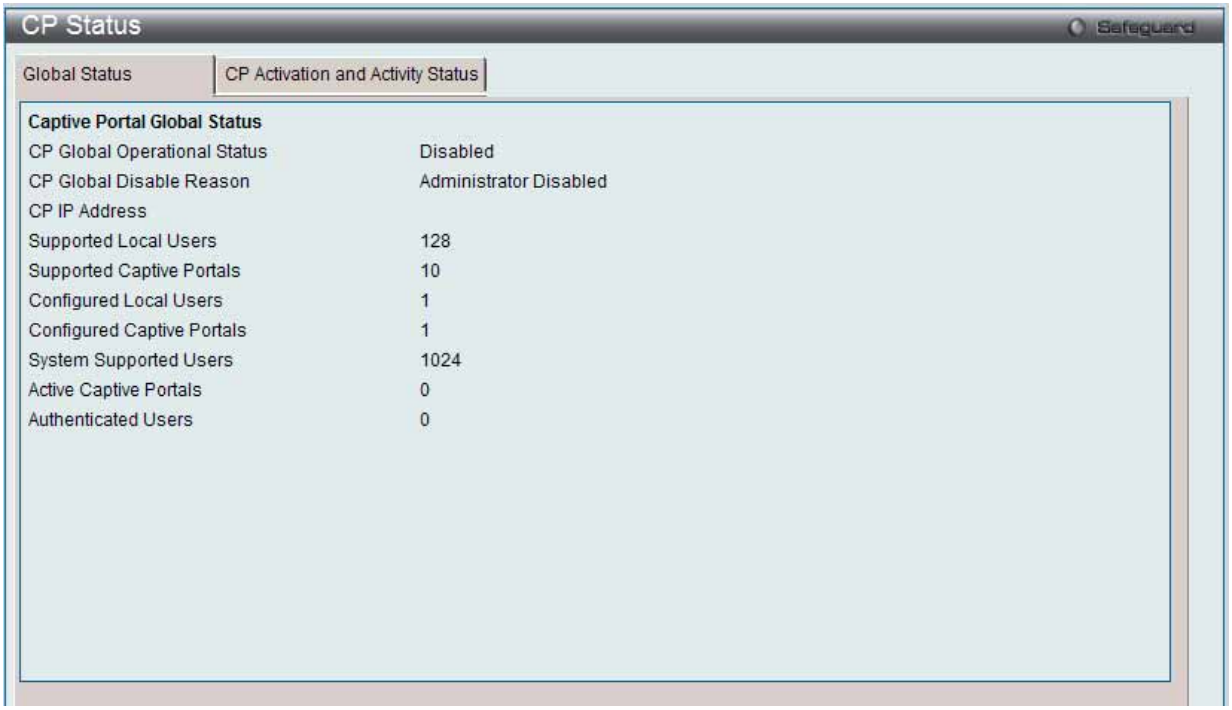


図 7.7-90　CP Global Status 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
CP Global Operational Status	CP の操作状態を表示します。
CP Global Disable Reason	CP が無効にされた場合に、本欄ではその理由を表示します。 表示可能な理由は以下の通りです。 • Administrator Disabled（管理者が無効にした） • IP Address Not Configured（IP アドレスが未設定） • No IP Routing Interface and Routing Disabled（IP ルーティングインタフェースがなく、ルーティングは無効）
CP IP Address	CP の IP アドレスを表示します。
Supported Local Users	ローカルユーザデータベースがサポートするエントリ数を表示します。
Supported Captive Portals	システムのサポートしている CP の数を表示します。
Configured Local Users	システムに設定されているユーザ数を表示します。
Configured Captive Portals	スイッチに設定された CP 数を表示します。
System Supported Users	システムがサポートしている認証ユーザの数を表示します。
Active Captive Portals	操作上有効である CP インスタンスの数を表示します。
Authenticated Users	本スイッチにおけるすべての CP インスタンスに対して現在認証されているユーザ数を表示します。

CP Activation and Activity Status（CP アクティベーションとアクティビティ状態）

アクティベーションとアクティビティの状態を参照します。

1. **Security > Captive Portal (CP) > CP Status > CP Activation and Activity Status タブ**の順にメニューをクリックし、以下の画面を表示します。

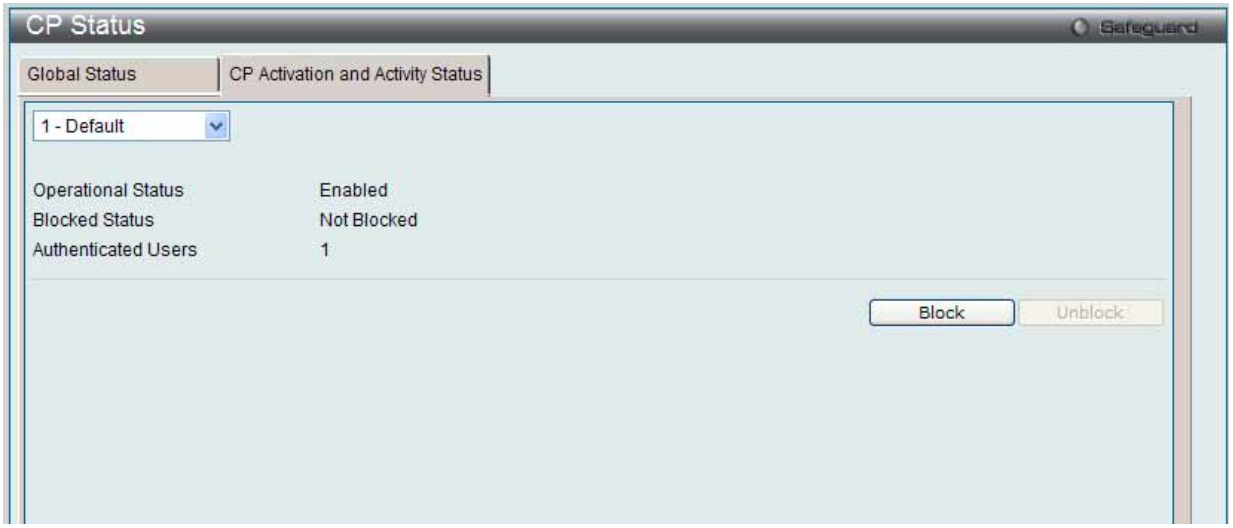


図 7.7-91　CP Activation and Activity Status 画面

2. プルダウンメニューを使用して、アクティベーションとアクティビティの状態を参照する CP を選択します。

アクセスのブロック
「Block」ボタンをクリックすると、ユーザが、選択したキャプティブポータルを経由してネットワークへのアクセス権を取得することを防ぎます。

アクセスの許可
選択したキャプティブポータルの「Blocked Status」が「Blocked」の場合、「Unblock」ボタンをクリックすると、キャプティブポータルを経由したネットワークへのアクセスを許可します。

Interface Status（インタフェース状態）

CP インタフェース状態を表示します。

Interface Activation Status（インタフェースアクティベーション状態）

1. **Security > Captive Portal (CP) > Interface Status > Interface Activation Status** タブの順にメニューをクリックし、以下の画面を表示します。

図 7.7-92　Interface Activation Status 画面

2. 最初のプルダウンメニューでポータルを、2 番目のプルダウンメニューで情報を参照するインタフェースを選択します。

Interface Capability Status（インタフェースケイパビリティ状態）

1. **Security > Captive Portal (CP) > Interface Status > Interface Capability Status** タブの順にメニューをクリックし、以下の画面を表示します。

図 7.7-93　Interface Capability Status 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Bytes Received Counter	インタフェースが各クライアントから受信したバイト数の表示をサポートするかどうかを表示します。
Bytes Transmitted Counter	インタフェースが各クライアントに送信したバイト数の表示をサポートするかどうかを表示します。
Packets Received Counter	インタフェースが各クライアントから受信したパケット数の表示をサポートするかどうかを表示します。
Packets Transmitted Counter	インタフェースが各クライアントに送信したパケット数の表示をサポートするかどうかを表示します。
Session Timeout	インタフェースがクライアントセッションのタイムアウトをサポートするかどうかを表示します。本属性はすべてのインタフェースでサポートされます。
Idle Timeout	ユーザが何もトラフィックを送受信しない場合のタイムアウトをインタフェースがサポートするかどうかを表示します。
Roaming Support	インタフェースがクライアントのローミングをサポートするかどうかを表示します。無線インタフェースだけがクライアントローミングをサポートします。

プルダウンメニューを使用して、詳細情報を表示するインタフェースを選択します。

Client Connection Status（クライアントの接続状態）

キャプティブポータル経由でスイッチに接続するクライアントに関する詳細情報を表示します。

Client Summary（クライアントに関するサマリ情報の参照）

1. **Security > Captive Portal (CP) > Client Connection Status > Client Summary タブ**の順にメニューをクリックし、以下の画面を表示します。

図 7.7-94　Client Summary 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
MAC Address	（該当する場合）クライアントの MAC アドレスを表示します。MAC アドレスが（*）でマークされている場合、クライアントはピアコントローラに認証されています。つまり、クラスタコントローラはオーセンティケータではありませんでした。
IP Address	（該当する場合）クライアントの IP アドレスを表示します。
User	接続するクライアントのユーザ名（またはゲスト ID）を表示します。
Protocol	現在の接続プロトコル（HTTP または HTTPS）を表示します。
Verification	現在のアカウントタイプ（Guest、Local または RADIUS）を表示します。

クライアントの切断

キャプティブポータルが認証クライアントを切断するためには、そのクライアントの MAC アドレス横にある対応するチェックボックスを選択して「Delete」ボタンをクリックします。すべてのキャプティブポータルからすべてのクライアントを切断するには、「Delete All」ボタンをクリックします。

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

「MAC Address」のリンクをクリックすると、「Client Detail」タブにリンクします。

Client Detail（クライアント詳細情報の参照）

キャプティブポータル経由でネットワークに接続する各クライアントの詳細情報を表示します。

1. **Security > Captive Portal (CP) > Client Connection Status > Client Detail タブ**の順にメニューをクリックし、以下の画面を表示します。

図 7.7-95　Client Detail 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Client IP Address	（該当する場合）クライアントの IP アドレスを表示します。
User Name	接続するクライアントのユーザ名 (またはゲスト ID) を表示します。
CP Configuration	クライアントが使用している CP 設定を表示します。
Interface	クライアントが使用しているインタフェースを表示します。
Protocol	現在の接続プロトコル（HTTP または HTTPS）を表示します。
Verification	現在のアカウントタイプ（Guest、Local または RADIUS）を表示します。
Session Time	クライアントが認証されてから経過した時間を表示します。
Switch MAC Address	このクライアントの認証を行うスイッチの MAC アドレスを表示します。クラスタリングがサポートされる場合、本欄はクラスタ内のピアスイッチの MAC アドレスを表示します。
Switch Type	このクライアントの認証を行うスイッチが、ローカルスイッチであるか、またはクラスタ内のピアスイッチであるかを示しています。
Switch IP Address	このクライアントの認証を行うスイッチの IP アドレスを表示します。クラスタリングがサポートされる場合、本欄はクラスタ内のピアスイッチの IP アドレスを表示します。

プルダウンメニューを使用して、詳細情報を参照する接続クライアントの MAC アドレスを選択します。:

Client Statistics（クライアント統計情報の参照）

クライアントが送信または受信したトラフィックに関する情報を参照します。

1. **Security > Captive Portal (CP) > Client Connection Status > Client Statistics タブ**の順にメニューをクリックし、以下の画面を表示します。

図 7.7-96　Client Statistics 画面

2. プルダウンメニューを使用して、詳細情報を参照する接続クライアントの MAC アドレスを選択します。

Interface - Client Status（クライアントインタフェース関連ステータスの参照）

指定インタフェースに認証されているクライアントを参照します。

1. **Security > Captive Portal (CP) > Client Connection Status > Interface - Client Status タブ**の順にメニューをクリックし、以下の画面を表示します。

図 7.7-97　Interface - Client Status 画面

2. プルダウンメニューを使用して、本インタフェースの CP に接続するクライアントに関する情報を参照するインタフェースを選択します。

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

CP-Client Status（クライアント CP 関連ステータスの参照）

指定 CP 設定に認証されているクライアントを参照します。

1. **Security > Captive Portal (CP) > Client Connection Status > CP - Client Status タブ**の順にメニューをクリックし、以下の画面を表示します。

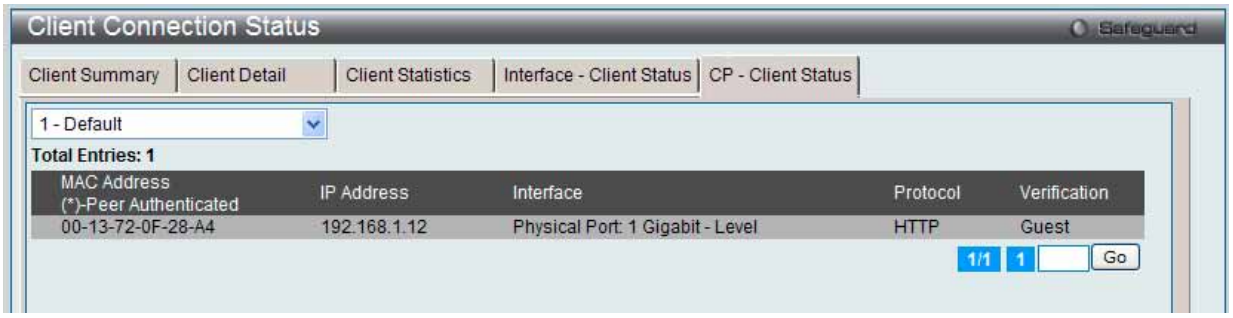


図 7.7-98　CP-Client Status 画面

2. プルダウンメニューを使用して、CP に接続するクライアントに関する情報を参照するインタフェースを選択します。

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

SNMP Trap Configuration（SNMP トラップ設定）

SNMP トラップをキャプティブポータルから送信するかどうかを設定し、トラップを生成するキャプティブポータルのイベントを指定します。

1. **Security > Captive Portal (CP) > SNMP Trap 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 7.7-99　SNMP Trap Configuration 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Client Authentication Failure Traps	プルダウンメニューを使用して、クライアントがキャプティブポータルに認証を試みて失敗した場合、SNMP エージェントがトラップを送信するかどうかを設定します。
Client Connection Traps	プルダウンメニューを使用して、クライアントがキャプティブポータルに認証され、接続した場合、SNMP エージェントがトラップを送信するかどうかを設定します。
Client Database Full Traps	プルダウンメニューを使用して、エントリがフル状態のためクライアントデータベースに追加されない場合に SNMP エージェントのトラップを送信するかどうかを設定します。
Client Disconnection Traps	プルダウンメニューを使用して、クライアントがキャプティブポータルとの接続を解除された場合、SNMP エージェントがトラップを送信するかどうかを設定します。

「Apply」ボタンをクリックして各セクションで行った変更を適用します。

7.8 Network Application（ネットワークアプリケーション）

以下は Network Application 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
DHCP（DHCP 設定）	DHCP リレーの設定を行います。以下のメニューがあります。 DHCP Relay（DHCP リレー）、DHCP Local Relay Settings（DHCP ローカルリレー設定）	329
SNTP（SNTP 設定）	本製品に時刻設定をします。以下のメニューがあります。 SNTP Settings（SNTP 設定）、Time Zone Settings（タイムゾーン設定）	336
Flash File System Settings （フラッシュファイルシステム設定）	フラッシュファイルシステムを利用したファイル操作を行います。	338

DHCP（DHCP 設定）

DHCP Relay（DHCP リレー）

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

DHCP リレーグローバル設定の有効化および設定を行うことができます。

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。パケット内のホップカウントが、このホップカウント制限以上になると破棄されます。「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」フィールドの値が「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。

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

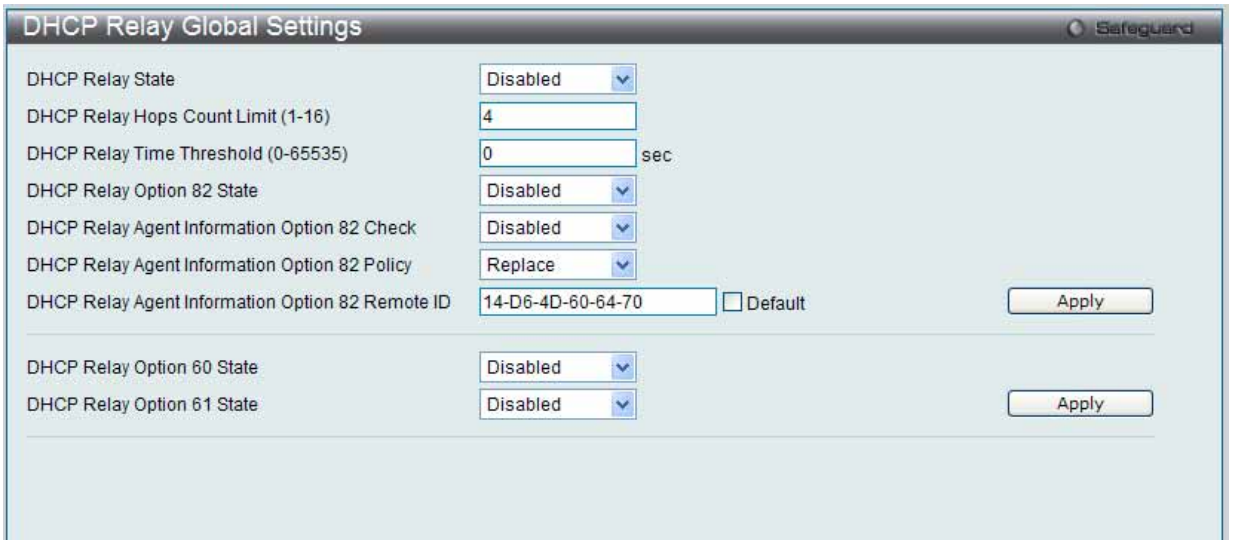


図 7.8-1　DHCP Relay Global Settings 画面

「DHCP Relay State」で DHCP リレーをグローバルに有効にして、その他項目の設定を行います。

2. 以下の項目を使用して設定および参照します。

項目	説明
DHCP Relay State	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 0-65535（秒）で定義します。0 を指定すると、スイッチは DHCP パケットの「Seconds」フィールド内の値の処理を行いません。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 Option 82 State	スイッチにおける 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。また、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 情報が挿入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。
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。 • 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。（初期値） • 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。
DHCP Relay Option 60 State	DHCP Relay Option 60 State 機能を「Enabled」（有効）または「Disabled」（無効）にします。 パケットが有効なオプション 60 を持たないと、リレーサーバをオプション 60 に基づいて決定できません。この場合、リレーサーバは、オプション 61 または IP インタフェースに従って設定したサーバに基づいて決定されます。リレーサーバをオプション 60 またはオプション 61 に基づいて決定すると、IP インタフェースに従って設定したサーバは無視されます。リレーサーバをオプション 60 またはオプション 61 で決定しないと、IP インタフェースに従って設定したサーバがリレーサーバを決定するのに使用されます。
DHCP Relay Option 61 State	DHCP Relay Option 61 State 機能を「Enabled」（有効）または「Disabled」（無効）にします。 オプション 61 が有効な場合、パケットがオプション 61 を持たないと、リレーサーバをオプション 61 に基づいて決定できません。リレーサーバをオプション 60 またはオプション 61 に基づいて決定すると、IP インタフェースに従って設定したサーバは無視されます。リレーサーバをオプション 60 またはオプション 61 で決定しないと、IP インタフェースに従って設定したサーバは、リレーサーバを決定するのに使用されます。

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

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から Option-82 欄を削除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 Relay Agent 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

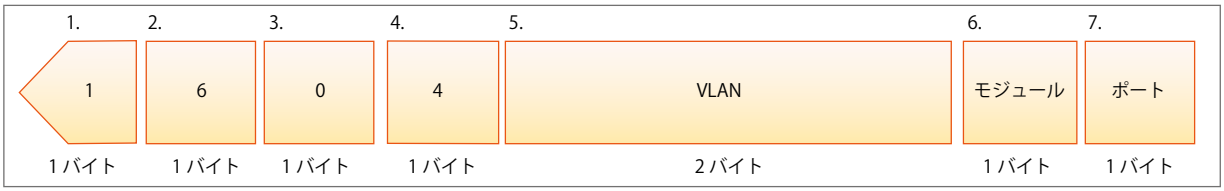


図 7.8-2　サーキット ID サブオプション形式

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）

図 7.8-3　リモート ID サブオプション形式

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

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

DHCP 情報をスイッチに中継するために、IP アドレスでサーバを設定します。以下の画面を使用して、DHCP サーバに直接接続するスイッチ上に定義済みの IP インタフェースを入力します。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。

1. **Network Application > DHCP > 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 7.8-4　DHCP Relay Interface Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Interface Name	DHCP サーバに直接接続するスイッチの IP インタフェース名を入力します。
Server IP Address	DHCP サーバの IP アドレスを入力します。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。

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 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 Relay Option 60 Server Settings（DHCP リレーオプション 60 サーバ設定）

DHCP リレーオプション 60 サーバのパラメータを設定します。

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。

1. **Network Application > DHCP > DHCP Relay > DHCP Relay Option 60 Server Settings** の順にメニューをクリックし、以下の画面を表示します。

図 7.8-5　DHCP Relay Option 60 Server Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Server IP Address	DHCP リレーオプション 60 サーバのリレー IP アドレスを指定します。「Add」ボタンをクリックして、入力した情報に基づいて新しいエントリを追加します。
Mode	DHCP リレーオプション 60 サーバのモードを選択します。「Apply」ボタンをクリックして行った変更を適用します。

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

注意　オプション 60 に基づくパケットに一致しないサーバが発見された場合、リレーサーバはデフォルトリレーサーバによって判断されます。

DHCP Relay Option 60 Settings（DHCP リレーオプション 60 設定）

DHCP リレーが DHCP オプション 60 を処理するかどうか決定します。

1. **Network Application > DHCP > DHCP Relay > DHCP Relay Option 60 Settings** の順にメニューをクリックし、以下の画面を表示します。

図 7.8-6　DHCP Relay Option 60 Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
String	DHCP リレーオプション 60 文字列を入力します。 同じリレーサーバに異なる文字列を指定でき、複数のリレーサーバに同じ文字列を指定できます。システムはすべてが一致しているサーバにパケットをリレーします。
Server IP	DHCP リレーオプション 60 サーバの IP アドレスを入力します。
Match Type	DHCP リレーオプション 60 サーバの一致タイプを入力します。 • Exact Match - パケットにおけるオプション 60 の文字列が指定した文字列に完全に一致する必要があります。 • Partial Match - パケットにおけるオプション 60 の文字列が指定した文字列に部分的にだけ一致する必要があります。
IP Address	DHCP リレーオプション 60 の IP アドレスを入力します。

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

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

エントリの削除
「Delete」ボタンをクリックして、入力した情報に基づいて指定エントリを削除します。
「Delete All」ボタンをクリックして、表示されたすべてのエントリを削除します。

DHCP Relay Option 61 Settings（DHCP リレーオプション 61 設定）

DHCP リレーオプション 61 のパラメータを設定します。

1. **Network Application > DHCP > DHCP Relay > DHCP Relay Option 61 Settings** の順にメニューをクリックし、以下の画面を表示します。

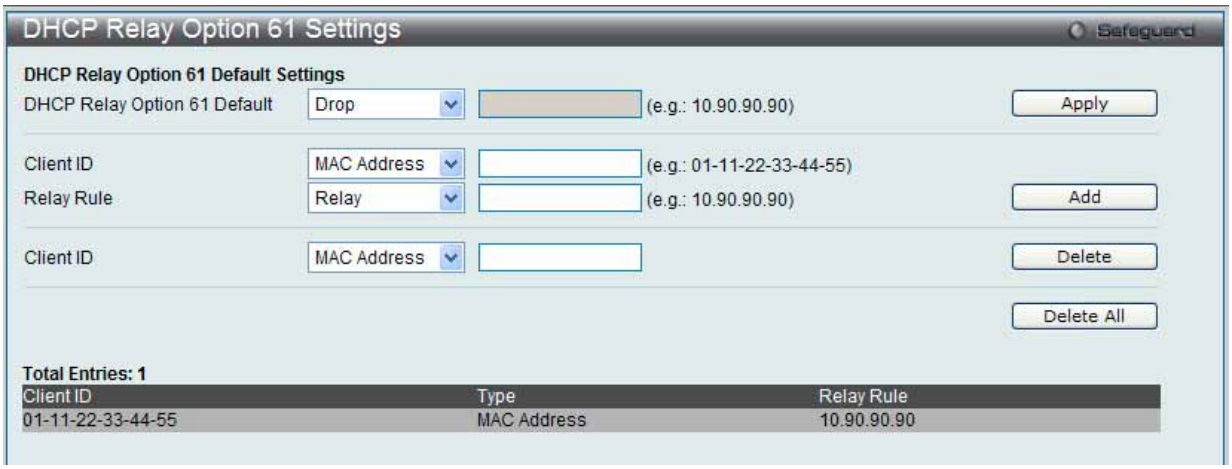


図 7.8-7　DHCP Relay Option 61 Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
DHCP Relay Option 61 Default	DHCP リレーオプション 61 デフォルトオプションを選択します。 • Drop - パケットを破棄します。 • Relay - IP アドレスにパケットをリレーします。デフォルトリレーサーバの IP アドレスを入力します。オプション 61 に基づくパケットに一致しないサーバが発見された場合、リレーサーバはデフォルトリレーサーバ設定によって判断されます。
Client ID	• MAC Address - クライアントのハードウェアアドレスであるクライアント ID。 • String - 管理者によって指定されるクライアント ID。
Relay Rule	• Drop - パケットを破棄します。 • Relay - IP アドレスにパケットをリレーします。

「Apply」ボタンをクリックして行った変更を適用します。

エントリの追加

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

エントリの削除

「Delete」ボタンをクリックして、入力した情報に基づいて指定エントリを削除します。
「Delete All」ボタンをクリックして、表示されたすべてのエントリを削除します。

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

DHCP クライアントが同じ VLAN から IP アドレスを取得する場合、DHCP ローカルリレー設定では、DHCP リクエストパケットにオプション 82 を追加できます。DHCP ローカルリレー設定をしないと、スイッチは VLAN にパケットをフラッドします。DHCP リクエストパケットにオプション 82 を追加するためには、DHCP ローカルリレー設定と Global VLAN の状態を有効にする必要があります。

1. **Network Application > DHCP Server > 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 7.8-8　DHCP Local Relay Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
DHCP Local Relay State	DHCP ローカルリレー設定を「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Disabled」です。
VLAN Name	DHCP ローカルリレー操作に適用する VLAN を識別するために使用する VLAN 名です。
State	VLAN に対する DHCP ローカルリレー設定を「Enabled」（有効）/「Disabled」（無効）にします。

「Apply」ボタンをクリックして各セクションで行った変更を適用します。

SNTP（SNTP 設定）

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

SNTP Settings（SNTP 設定）

スイッチに時刻を設定します。

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

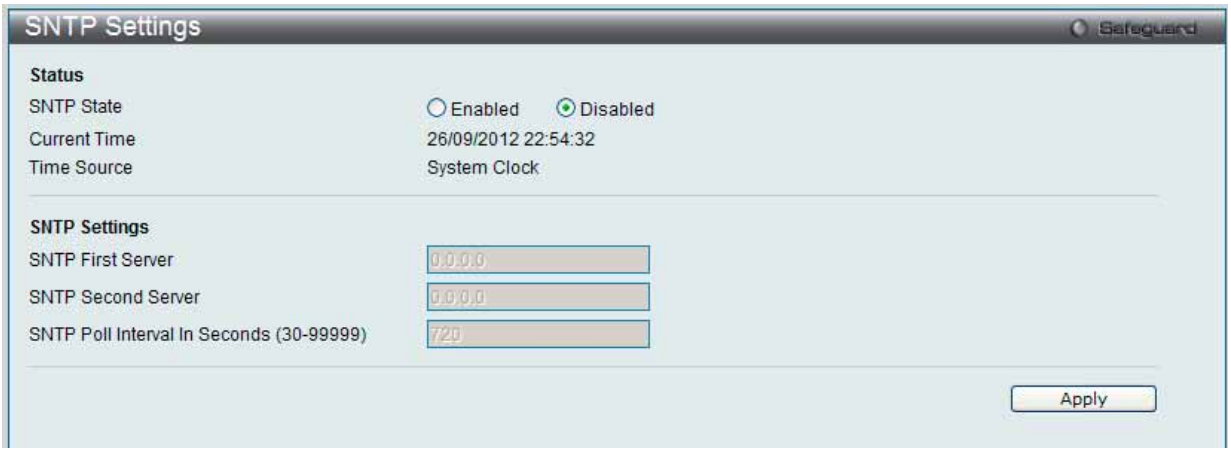


図 7.8-9　SNTP Settings 画面

2. 以下の項目を使用して設定および参照します。

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表示します。
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 情報の更新リクエストの送信間隔（秒）を設定します。

「Apply」ボタンをクリックし、デバイスに SNTP 設定を適用します。

Time Zone Settings（タイムゾーン設定）

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。

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

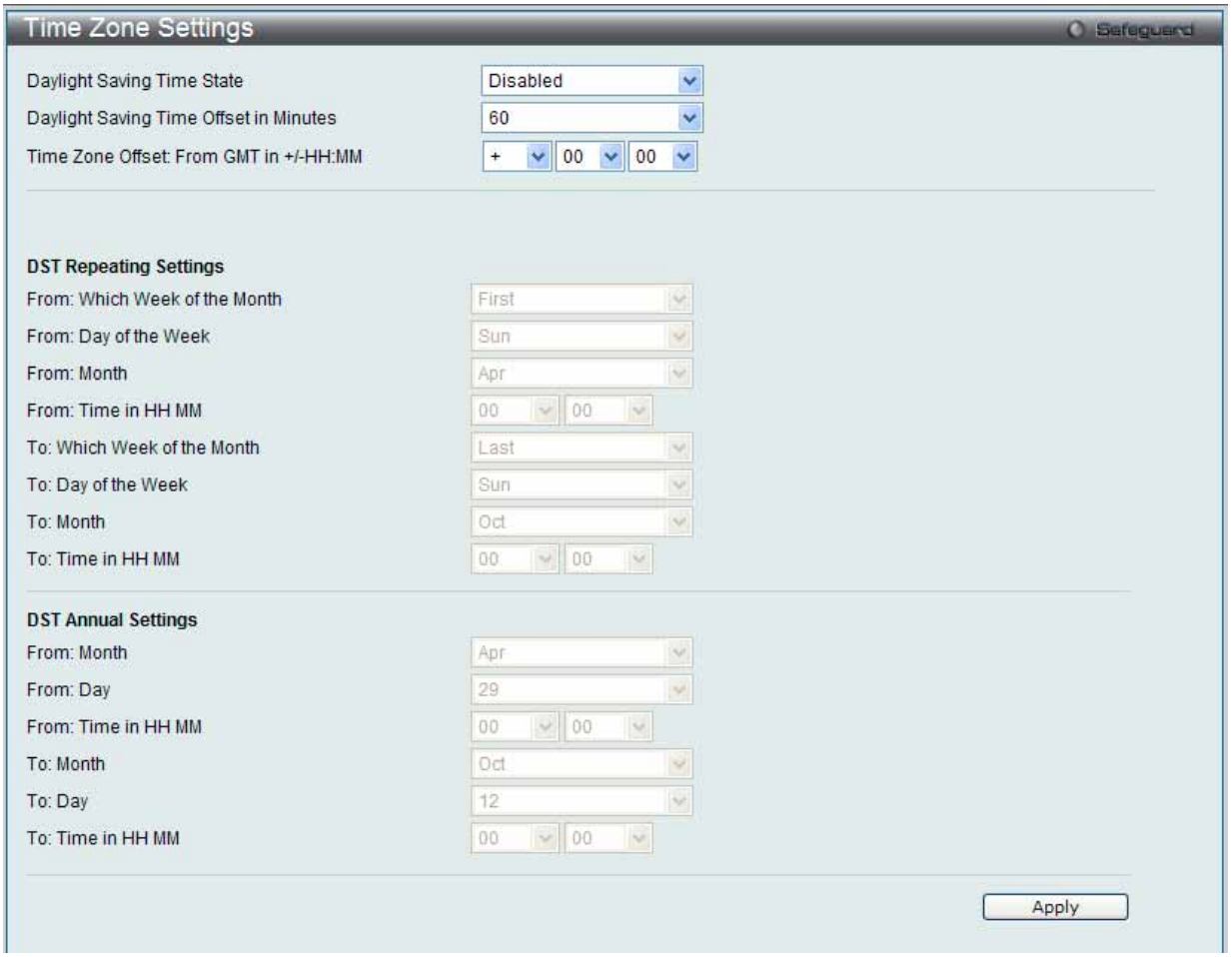


図 7.8-10　TimeZone Settings 画面

2. 以下の項目を使用して設定および参照します。

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。本モードでは、法則に従って指定される DST（サマータイム）の開始日と終了日が必要です。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。本モードを使用すると、DST（サマータイム）の開始日と終了日を簡潔に指定することが必要です。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。

Flash File System Settings（フラッシュファイルシステム設定）

フラッシュファイルシステムを使用する理由

古いスイッチシステムでは、ファームウェア、コンフィグレーション、およびログ情報は固定アドレスとサイズを持つフラッシュに保存されます。これは、最大のコンフィグレーションファイルが 2M バイトだけであり、現在のコンフィグレーションが 40K バイトにすぎなくても、フラッシュストレージスペースの 2M バイトを消費することを意味します。

また、コンフィグレーションファイル番号とファームウェア番号は固定されています。コンフィグレーションファイルまたはファームウェアサイズが元々設計されたサイズを超えている場合、互換性の問題が発生します。

使用するシステムにおけるフラッシュファイルシステム

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

ファイルシステムに不具合がある場合、Z- モデムを使用して直接システムにバックアップファイルをダウンロードすることができます。

1. **Network Application > Flash File System Settings** の順にメニューをクリックし、以下の画面を表示します。

図 7.8-11　Flash File System Settings 画面

「Current Path」に現在のパスを入力し、「Go」ボタンをクリックすると入力したパスに遷移します。

2. 「C:」リンクをクリックすると、以下の画面が表示されます。

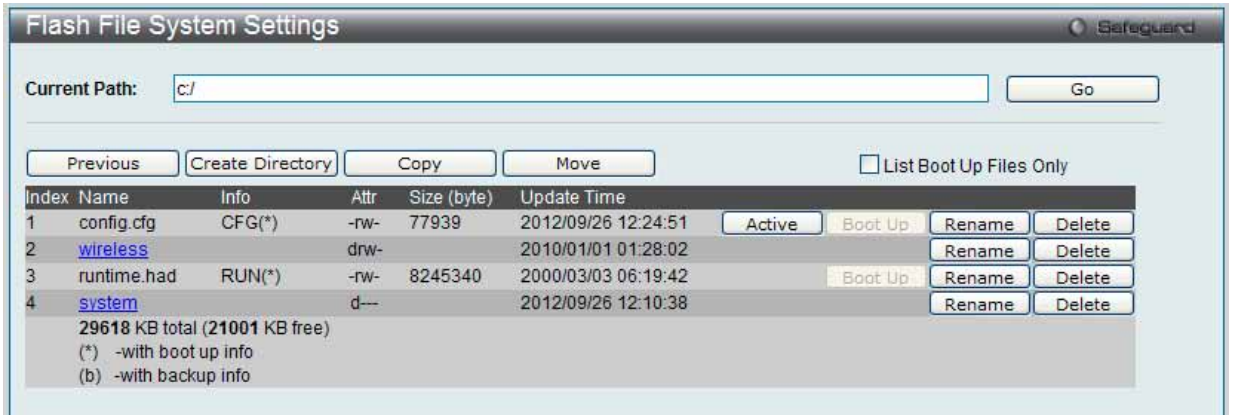


図 7.8-12　Flash File System Settings 画面

3. 以下の項目を使用して設定および参照します。

項目	説明
Previous	前のページに戻ります。
Create Directory	スイッチのファイルシステムに新しいディレクトリを作成します。
Copy	指定ファイルをスイッチにコピーします。
Move	指定ファイルをスイッチに移動します。
List Boot Up Files Only	チェックすると起動ファイルだけを表示します。
Active	アクティブなランタイムコンフィグレーションとして指定したコンフィグファイルを設定します。
Boot Up	起動用のブートアップイメージとして指定したランタイムイメージを設定します。
Rename	指定ファイルを変更します。
Delete	ファイルシステムから指定ファイルを削除します。

ファイルのコピー

1. 「Copy」ボタンをクリックすると、以下の画面が表示されます。

図 7.8-13　Flash File System Settings 画面 - Copy

2. このスイッチのファイルシステムにファイルをコピーする場合、送信元と送信先のパスを入力します。

3. 「Apply」ボタンをクリックして、コピーを開始します。「Cancel」ボタンをクリックすると処理は破棄されます。

ファイルの移動

1. 「Move」ボタンをクリックすると、以下の画面が表示されます。

図 7.8-14　Flash File System Settings - Move 画面

2. ファイルを別の場所に移動する場合、「Source」（送信元）と「Destination」（送信先）のパスを入力する必要があります。

3. 「Apply」ボタンをクリックして、コピーを開始します。「Cancel」ボタンをクリックすると処理は破棄されます。

ファイル名の変更

1. 「Rename」ボタンをクリックすると、以下の画面が表示されます。

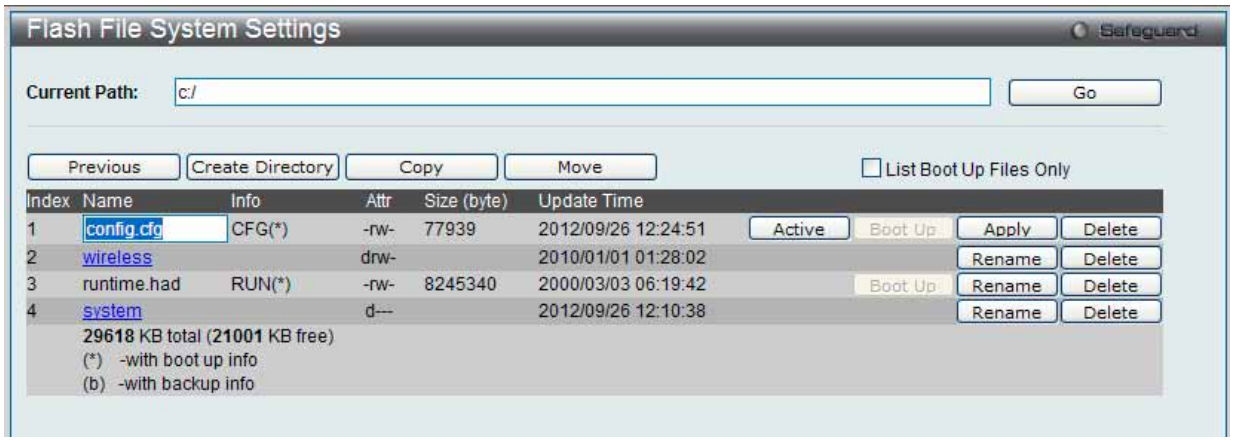


図 7.8-15　Flash File System Settings 画面 - Rename

2. ファイル名を変更して「Apply」ボタンをクリックします。

7.9 OAM（Object Access Method : オブジェクトアクセス方式）

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

サブメニュー	説明	参照ページ
CFM（Connectivity Fault Management : 接続性障害管理）	CFM 機能を設定します。以下のメニューがあります。CFM Settings（CFM 設定）、CFM Port Settings（CFM ポート設定）、CFM MIPCCM Table（CFM MIPCCM テーブル）、CFM Loopback Settings（CFM ループバック設定）、CFM Linktrace Settings（CFM リンクトレース設定）、CFM Packet Counter（CFM パケットカウンタ）、CFM Fault Table（CFM 障害テーブル）、CFM MP Table（CFM MP テーブル）	341
Ethernet OAM（イーサネット OAM）	ポートにイーサネット OAM モード、イベント、ログを設定します。以下のメニューがあります。Ethernet OAM Settings（イーサネット OAM 設定）、Ethernet OAM Configuration Settings（イーサネット OAM コンフィグレーション設定）、Ethernet OAM Event Log（イーサネット OAM イベントログ）、Ethernet OAM Statistics（イーサネット OAM 統計情報）	353
Cable Diagnostics（ケーブル診断機能）	ケーブル診断を行います。	356

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

CFM Settings（CFM 設定）

CFM 機能を設定します。

1. **OAM > 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 7.9-1　CFM Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
CFM Global Settings	
CFM State	CFM 機能を「Enabled」（有効）/「Disabled」（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 MP（メンテナンスポイント）を「Enabled」（有効）/「Disabled」（無効）にします。
CFM MD Settings	
MD	メンテナンスドメインの名称を入力します。22 文字内で指定します。
MD Index	使用するメンテナンスドメインインデックスを入力します。
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	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 - 次に存在する低いレベルのポートに設定済みの MEP がなく、ポートがこの MD の MEP に設定されないと、MIP がこの MD のどのポートにも作成されません。

項目	説明
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。

「Apply」ボタンをクリックして各セクションで行った変更を適用します。

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て、以下の画面を表示します。

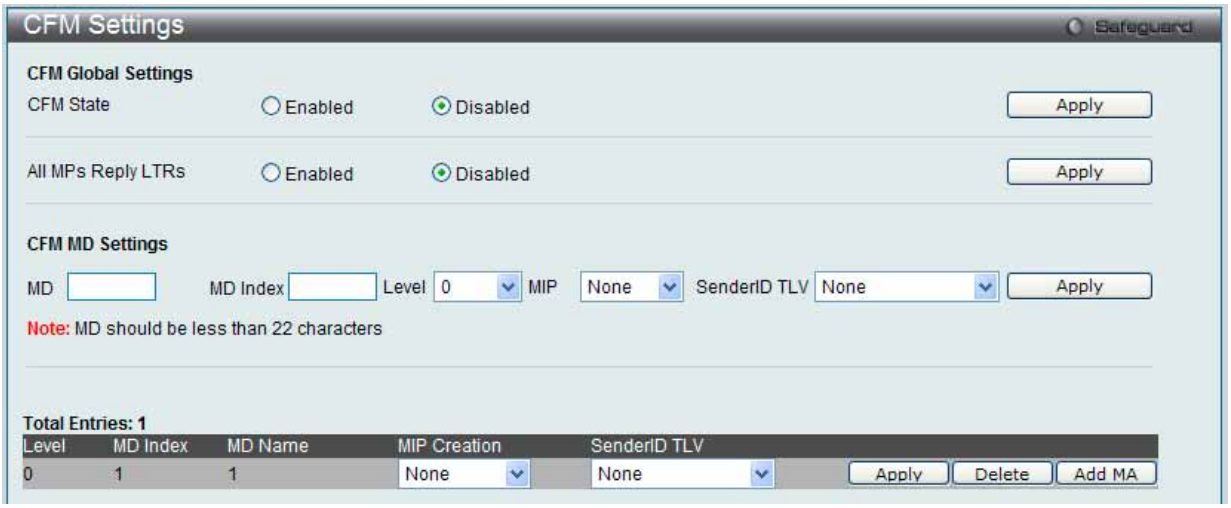


図 7.9-2　CFM Settings 画面 - Edit

2. 指定エントリを編集して「Apply」ボタンをクリックします。

エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。

注意　グループ名は 22 文字未満とします。

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。

1. **OAM > 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。

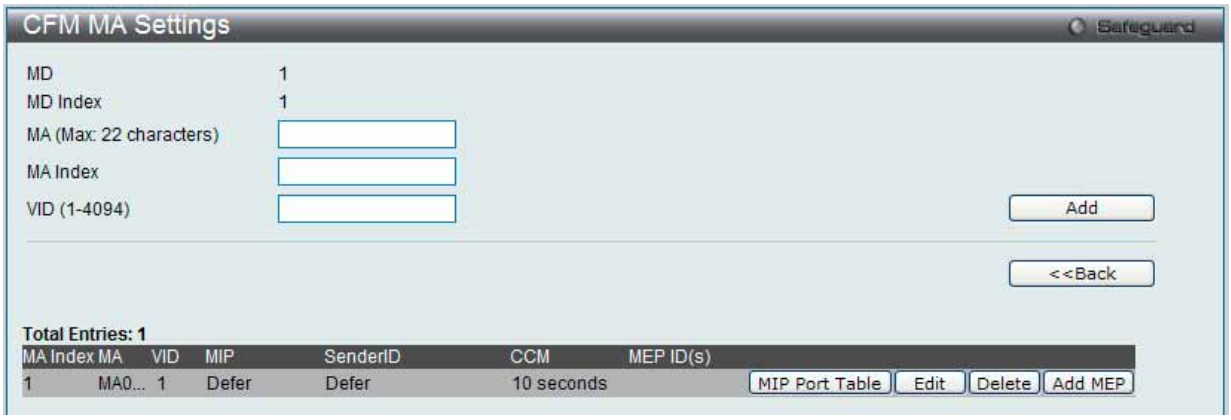


図 7.9-3　CFM MA Settings 画面

2. 以下の項目を使用して設定および参照します。

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。
MA Index	メンテナンスアソシエーションのインデックスを入力します。
VID (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。

「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

CFM MIP テーブルの参照

「MIP Port Table」ボタンをクリックして、CFM MIP Table を参照します。

MEP エントリの追加

「Add MEP」ボタンをクリックして、MEP（Maintenance End Point）エントリを追加します。

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」ボタンをクリックして以下の画面を表示します。

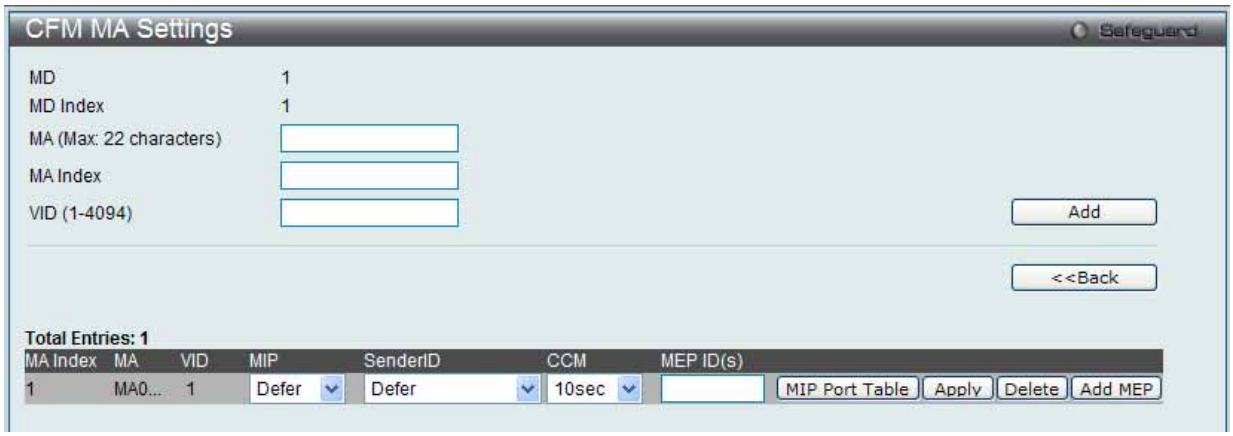


図 7.9-4　CFM MA Settings 画面 - Edit

2. 以下の項目を使用して設定および参照します。

項目	説明
MA	メンテナンスアソシエーションの名称を表示します。
VID (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。
MIP	MIP の作成を制御します。 • None - MIP を作成しません。 • 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。 • 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 - 次に存在する低いレベルのポートに設定済みの MEP がなく、ポートがこの MD の MEP に設定されないと、MIP がこの MD のどのポートにも作成されません。
SenderID	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	CCM 送信間隔を指定します。 • 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（1-8191）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。

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。

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

図 7.9-5　CFM MIP Table 画面

CFM MEP 設定

MEP を追加します。

1. **OAM > 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 7.9-6　CFM MEP Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
MEP Name	MEP 名を入力します。デバイスに設定されたすべての MEP 内で固有です。
MEP ID (1-8191)	MA の MEP ID リストに設定される MEP ID を入力します。
Port	プルダウンメニューを使用してポート番号を指定します。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。

「<<Back」をボタンをクリックし、変更を破棄してと前のページに戻ります。

エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。

注意　MEP 名は 32 文字未満とします。

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 7.9-7　CFM MEP Information 画面

MEP の編集

1. 「Edit」ボタンをクリックし、以下の画面を表示します。

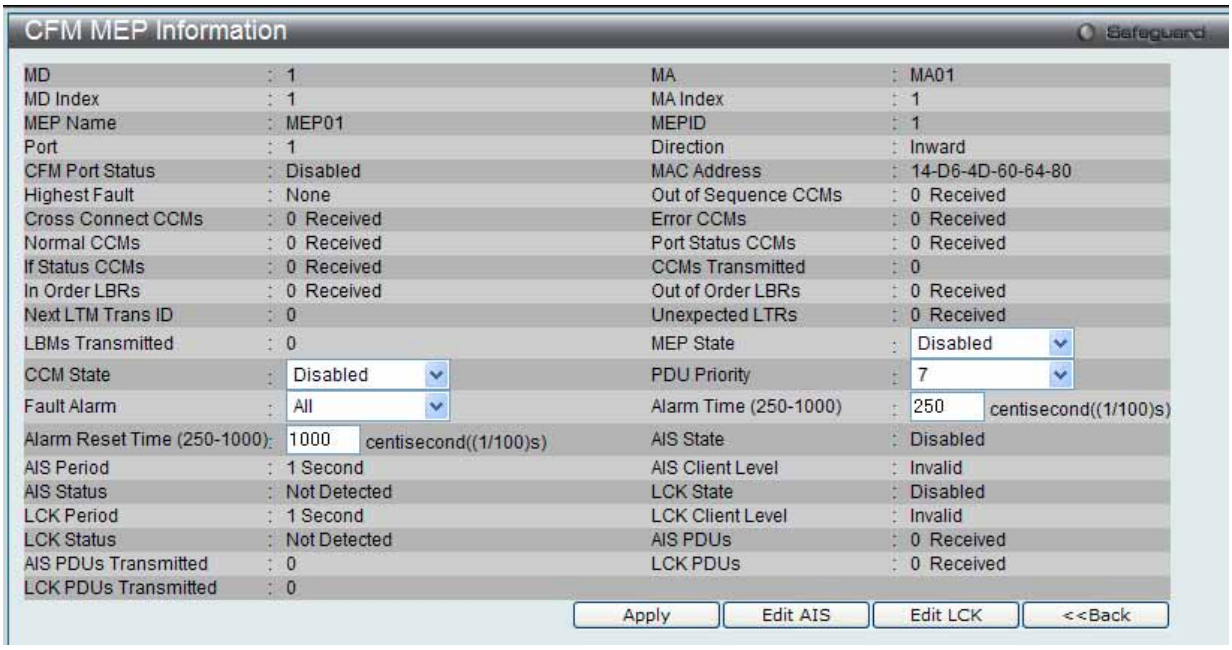


図 7.9-8　CFM MEP Information 画面 - Edit

2. 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)	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。

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

「<<Back」をボタンをクリックし、変更を破棄してと前のページに戻ります。

「Edit AIS」ボタンをクリックして AIS を設定します。
「Edit LCK」ボタンをクリックして LCK を設定します。

Extension AIS 設定

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

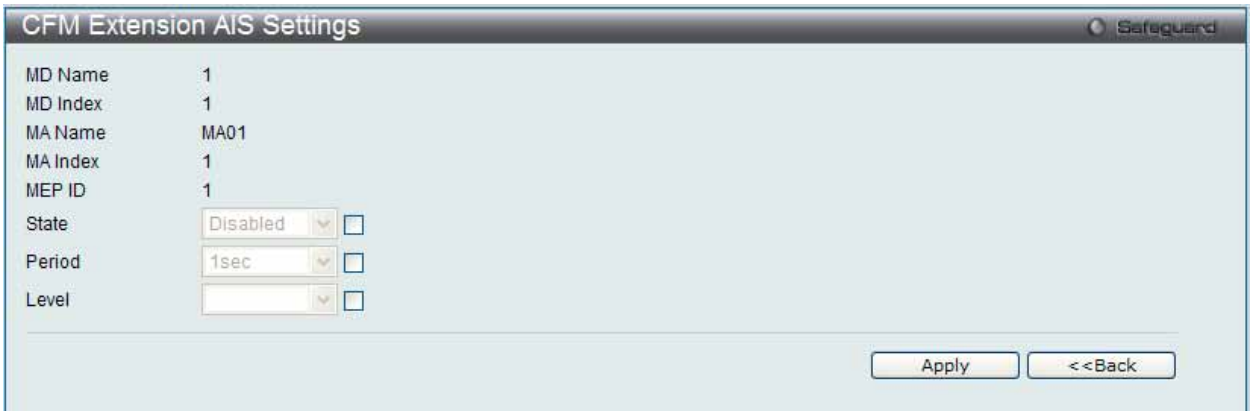


図 7.9-9　CFM Extension AIS (Edit) 画面

以下の項目を設定または表示できます。

項目	説明
State	チェックし、プルダウンメニューを使用して、AIS 機能を「Enabled」(有効) /「Disabled」(無効) にします。
Period	チェックし、プルダウンメニューを使用して、AIS PDU 送信間隔を選択します。 • 1sec - 送信間隔を 1 秒に設定します。（初期値） • 1min - 送信間隔を 1 分に設定します。
Level	チェックし、プルダウンメニューを使用して、MEP が AIS PDU を送信するクライアントレベル ID を選択します。クライアント MD レベルの初期値は最も近いクライアントレイヤの MIP と MEP が存在する MD レベルです。オプションを 0-7 からを選択します。

2. エントリの編集を行い、「Apply」ボタンをクリックします。

「<<Back」をボタンをクリックし、変更を破棄してと前のページに戻ります。

Extension LCK 設定

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

図 7.9-10　CFM Extension LCK Settings (Edit) 画面

以下の項目を設定または表示できます。

項目	説明
State	チェックし、プルダウンメニューを使用して、LCK 機能を「Enabled」（有効）/「Disabled」（無効）にします。
Period	チェックし、プルダウンメニューを使用して、LCK PDU 送信間隔を選択します。 • 1sec - 送信間隔を 1 秒に設定します。（初期値） • 1min - 送信間隔を 1 分に設定します。
Level	チェックし、プルダウンメニューを使用して、MEP が LCK PDU を送信するクライアントレベル ID を選択します。クライアント MD レベルの初期値は最も近いクライアントレイヤの MIP と MEP が存在する MD レベルです。オプションを 0-7 からを選択します。

2. エントリの編集を行い、「Apply」ボタンをクリックします。

「<<Back」をボタンをクリックし、変更を破棄してと前のページに戻ります。

CFM Port Settings（CFM ポート設定）

ポートベースで CFM ポート状態を「Enabled」（有効）/「Disabled」（無効）にします。

1. **OAM > 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。

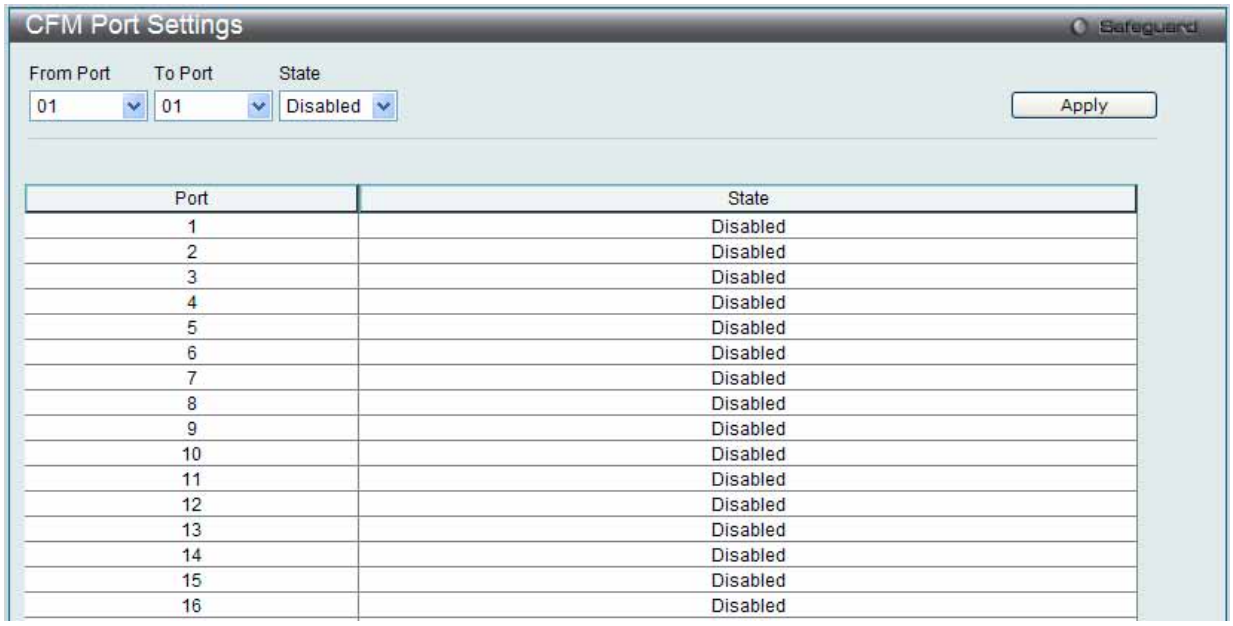


図 7.9-11　CFM Port Settings 画面

2. 以下の項目を使用して設定および参照します。

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「Enabled」（有効）/「Disabled」（無効）にします。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。

CFM MIPCCM Table（CFM MIPCCM テーブル）

CFM MIPCCM データベースエントリを表示します。

OAM > 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 7.9-12　CFM MIPCCM Table 画面

CFM Loopback Settings（CFM ループバック設定）

CFM ループバックテストを設定します。

1. **OAM > 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。

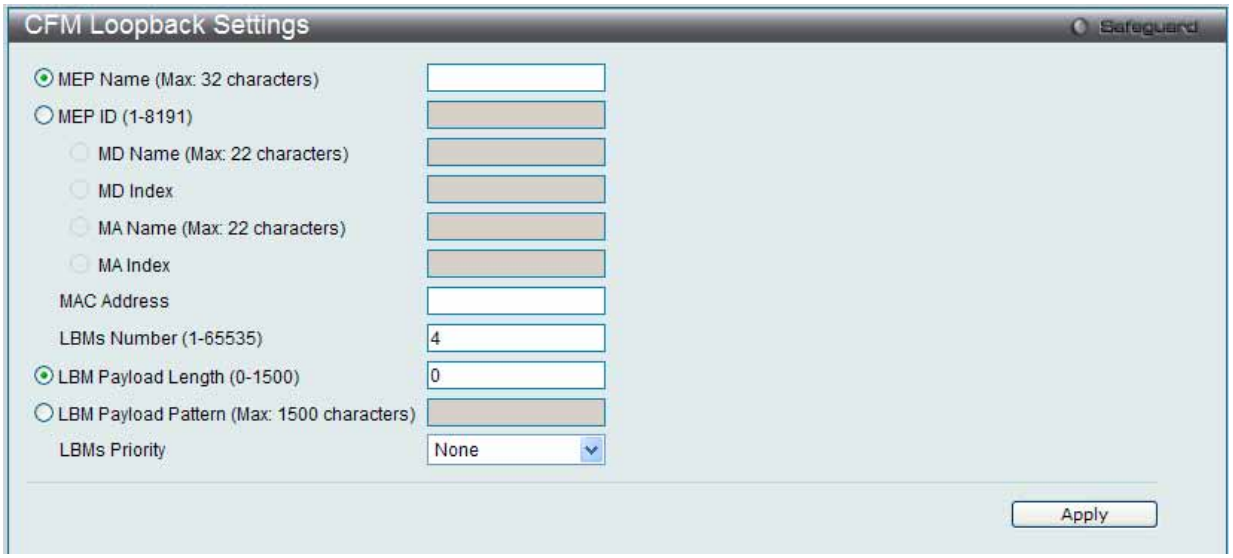


図 7.9-13　CFM Loopback Settings 画面

2. 以下の項目を使用して設定および参照します。

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 Name	使用するメンテナンスドメイン名を指定します。
MD Index	使用するメンテナンスドメインのインデックスを指定します。
MA Name	使用するメンテナンスアソシエーション名を指定します。
MA Index	使用するメンテナンスアソシエーションのインデックスを指定します。
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。

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。

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の発行、表示、リンクトレース応答の削除します。

1. **OAM > 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。

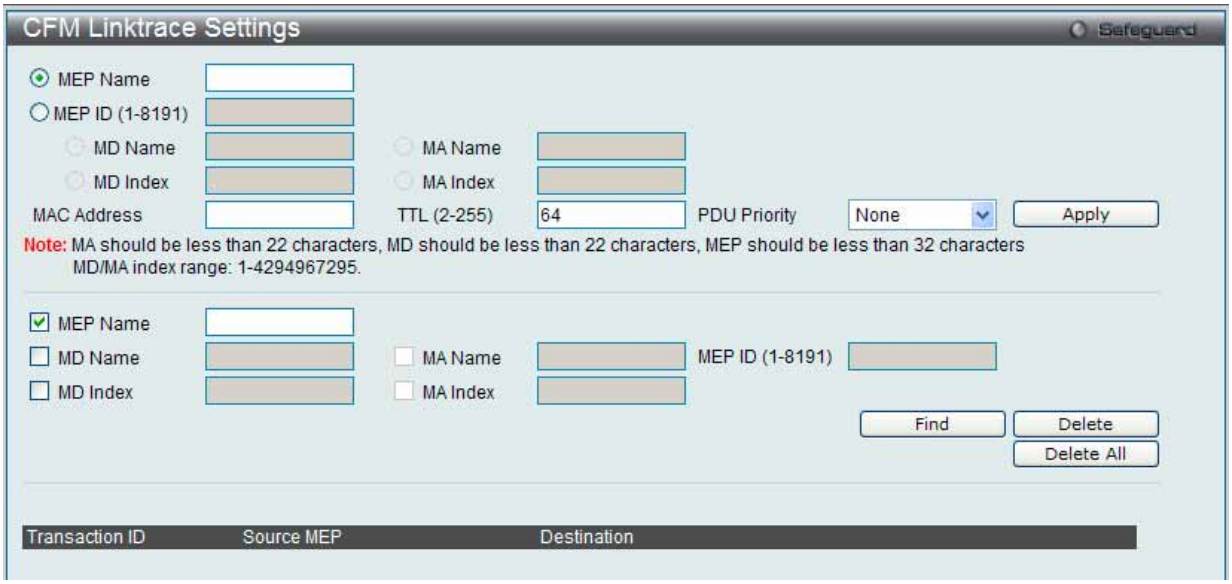


図 7.9-14　CFM Linktrace Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
MEP Name	使用するメンテナンスエンドポイントを指定します。
MEP ID (1-8191)	使用するエンドポイント ID を指定します。
MD Name	使用するメンテナンスドメイン名を指定します。
MD Index	使用するメンテナンスドメインのインデックスを指定します。
MA Name	使用するメンテナンスアソシエーション名を指定します。
MA Index	使用するメンテナンスアソシエーションのインデックスを指定します。
MAC Address	送信先 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。

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。

エントリの参照

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。
検出後、「View Detail」リンクをクリックすると、CFM リンクトレースの詳細情報が表示されます。

図 7.9-15　CFM Linktrace Settings 画面

エントリの削除

「Delete」ボタンをクリックして、入力した情報に基づいて指定エントリを削除します。
「Delete All」ボタンをクリックして、表示されたすべてのエントリを削除します。

CFM Packet Counter（CFM パケットカウンタ）

CPF パケットカウンタの RX/TX カウンタ情報を表示します。

1. **OAM > 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。

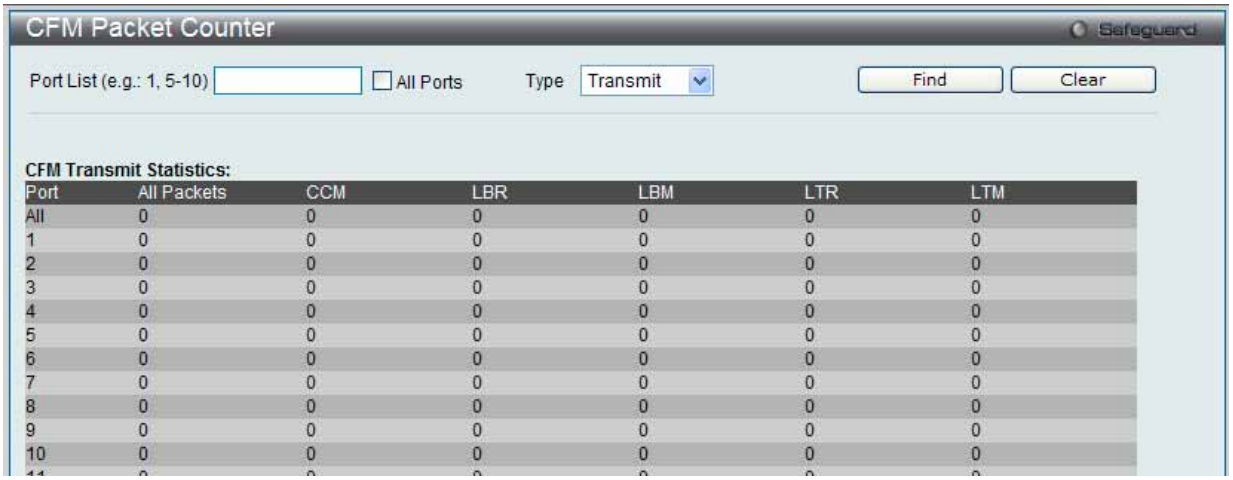


図 7.9-16　CFM Packet Counter 画面

2. 以下の項目を使用して参照します。

項目	説明
Port List	参照するポートを選択します。「All Ports」を選択すると、すべてのポートを表示します。
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。
「Clear」ボタンをクリックして、本欄に入力したすべてのエントリをクリアします。

CFM Fault Table（CFM 障害テーブル）

障害を持つ MEP 情報を表示します。

1. **OAM > 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。

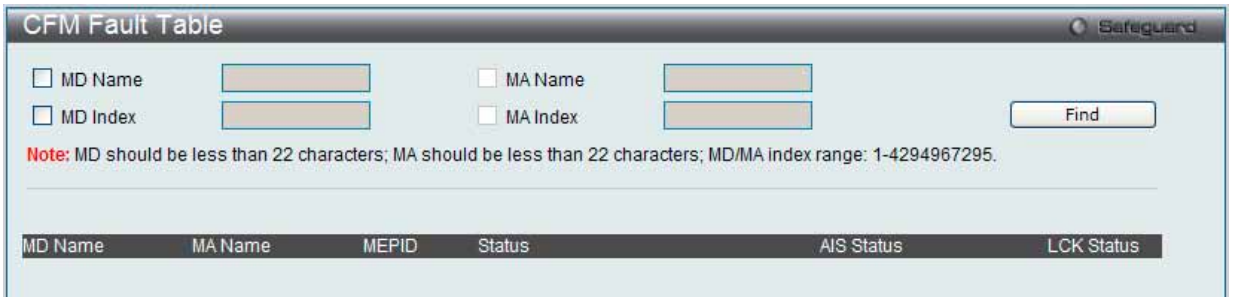


図 7.9-17　CFM Fault MEP 画面

2. 以下の項目を使用して参照します。

項目	説明
MD Name	表示するメンテナンスドメイン名を指定します。
MD Index	表示するメンテナンスドメインのインデックスを指定します。
MA Name	表示するメンテナンスアソシエーション名を指定します。
MA Index	表示するメンテナンスアソシエーションのインデックスを指定します。

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 MP Table（CFM MP テーブル）

CFM MP 情報を表示します。

1. **OAM > 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 7.9-18　CFM MP Table 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Port	参照するユニット ID とポート番号を選択します。
Level (0-7)	参照するレベルを指定します。
Direction	プルダウンメニューを使用して参照する方向を選択します。 • Any - 内向き / 外向き MP を示します。（初期値） • Inward - 内向き MP を示します。 • Outward - 外向き MP を示します。
VID (1-4094)	参照するエントリの VLAN ID を指定します。

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。

Ethernet OAM（イーサネット OAM）

Ethernet OAM Settings（イーサネット OAM 設定）

ポートにイーサネット OAM モードを設定します。

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

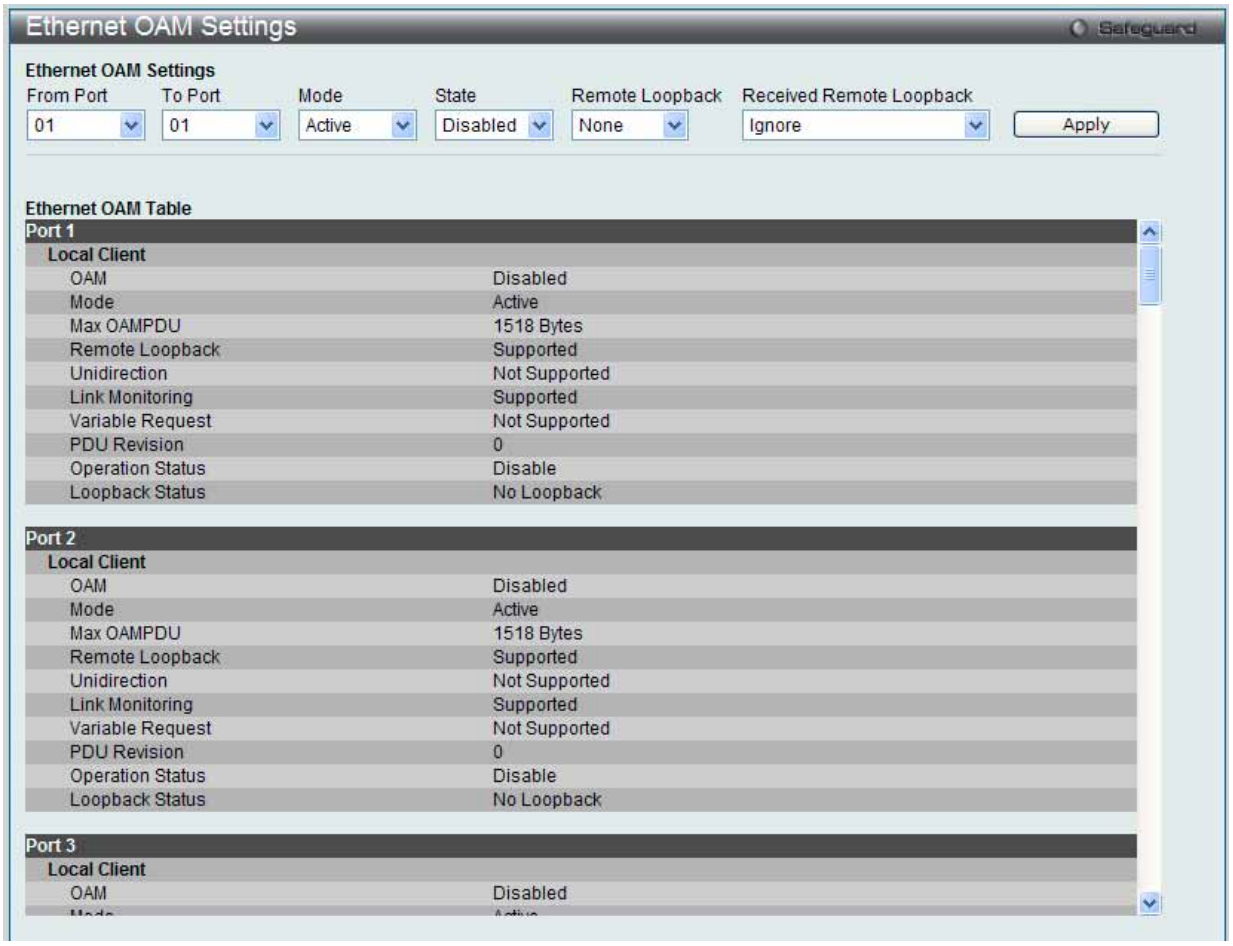


図 7.9-19　Ethernet OAM Settings 画面

2. 以下の項目を使用して設定および参照します。

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「Enabled」（有効）/「Disabled」（無効）にします。初期値は「Disabled」です。
Remote Loopback	• None - リモートループバックを行いません。（初期値） • Start - 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 - 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	クライアントが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 - 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を処理します。 • Ignore - 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を無視します。（初期値）

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。

Ethernet OAM Configuration Settings（イーサネット OAM コンフィグレーション設定）

ポートにイーサネット OAM のイベントを設定します。

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

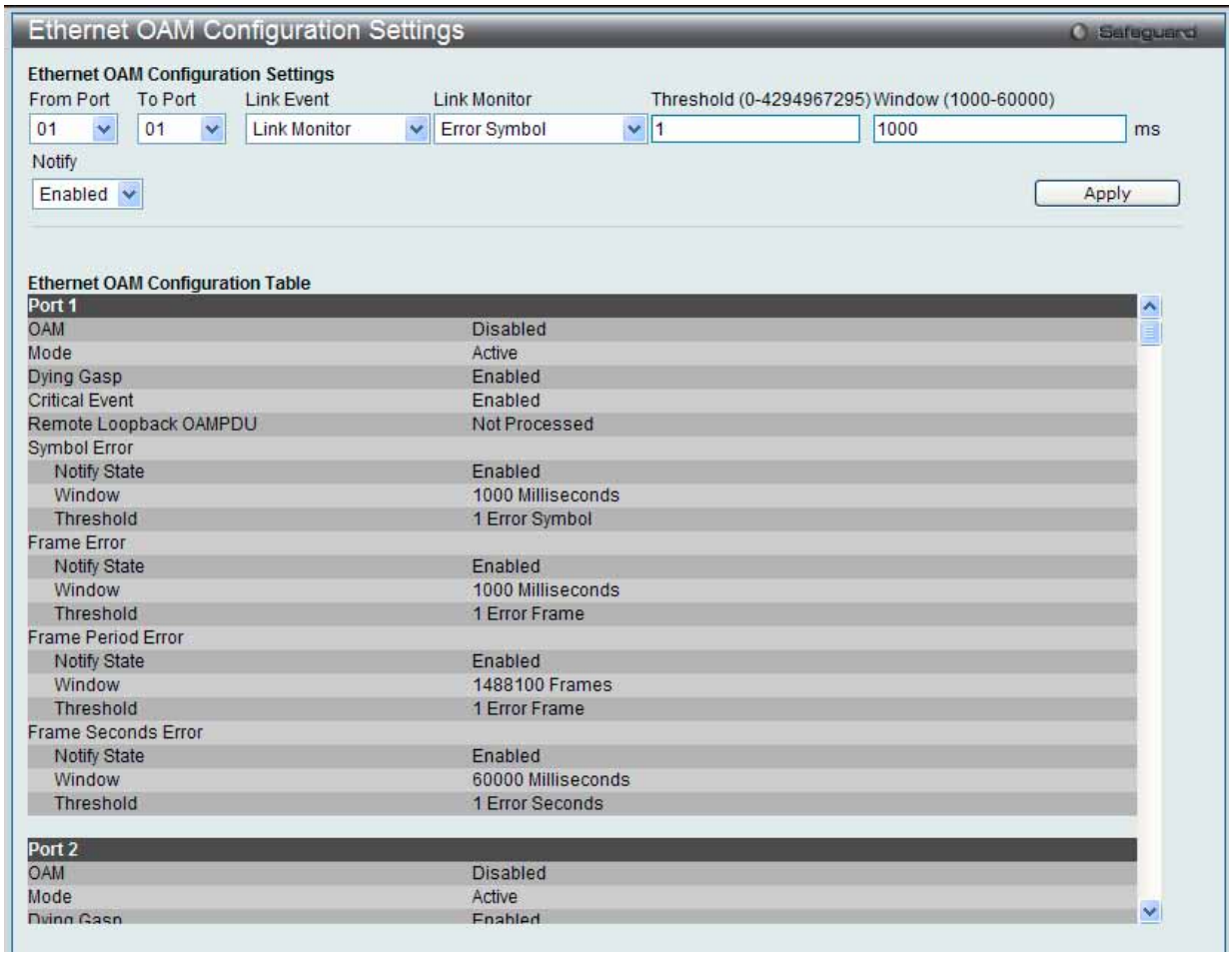


図 7.9-20　Ethernet OAM Configuration Settings 画面

2. 以下の項目を使用して設定および参照します。

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	イーサネット OAM のクリティカルなリンクイベント機能（「Link Monitor」または「Critical Link Event」）を設定します。イベント機能を無効にすると、ポートは対応するクリティカルなリンクイベントを送信しません。
Link Monitor	ポートにイーサネット OAM リンクモニタリング (Error Symbol) を設定します。リンクモニタリング機能は、さまざまな条件のもと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共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。シンボルエラー数が、期間内に定義したしきい値以上になる場合およびイベント通知状態 (Notify) が有効になる場合、リモート OAM ピアに通知するエラーシンボル期間のイベントを生成します。使用可能オプションは、Error Symbol、Error Frame、Error Frame Period、および Error Frame Second です。
Critical Link Event	イーサネット OAM のクリティカルなリンクイベント機能を設定します。イベント機能が無効になると、ポートは対応するクリティカルなリンクイベントを送信しません。 • 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)	期間内のエラーフレームまたはシンボルエラー数を指定します。これ以上になるとイベントが生成されます。
Window (1000-6000)	エラーフレームまたはシンボルのサマリイベントの期間（ミリ秒）を入力します。
Notify	イベント通知を「Enabled」（有効）/「Disabled」（無効）にします。初期値は有効です。

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。

Ethernet OAM Event Log（イーサネット OAM イベントログ）

ポートのイーサネット OAM イベントログ情報を表示します。

1. **OAM > Ethernet OAM > 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。

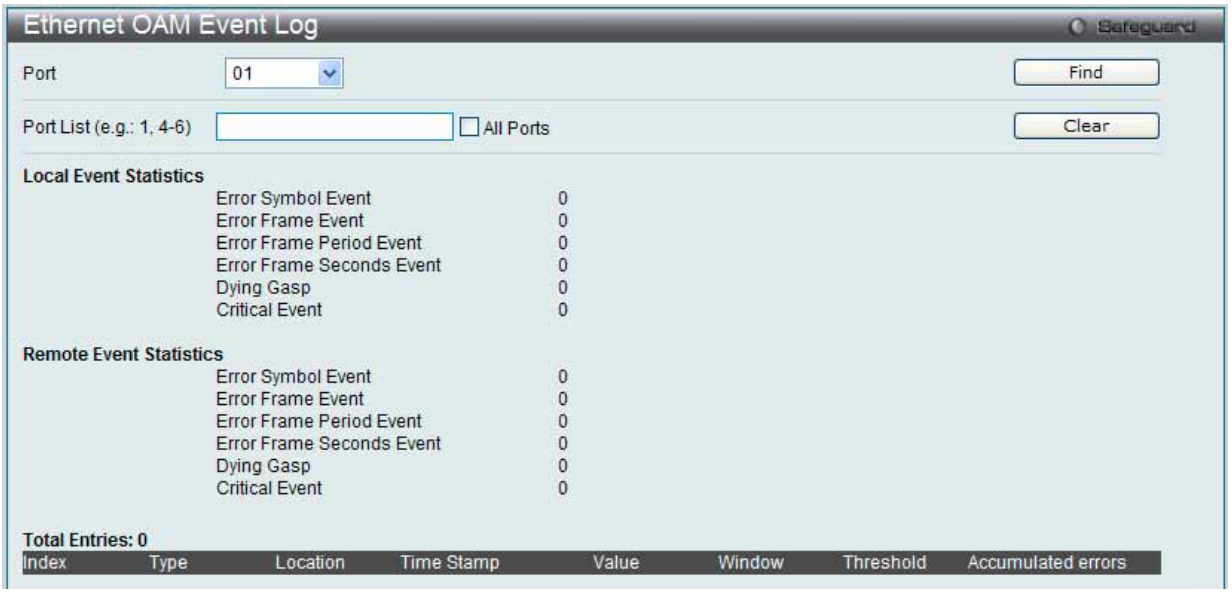


図 7.9-21　Ethernet OAM Event Log 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Port	参照するポート番号を選択します。
Port List	本設定に使用するポートリストを指定します。「All Ports」を選択すると、すべてのポートを選択します。

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。また、「All Port」を選択するとスイッチの全ポートの情報を表示します。

エントリの削除

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。

Ethernet OAM Statistics（イーサネット OAM 統計情報）

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。

1. **OAM > Ethernet OAM > 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。

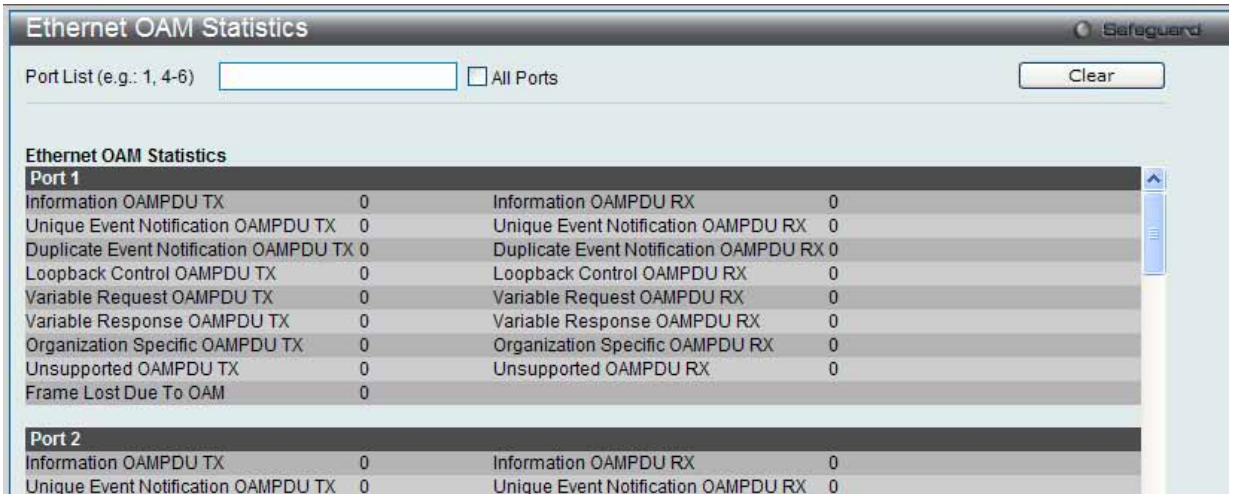


図 7.9-22　Ethernet OAM Statistics 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Port List	本設定に使用するポートリストを指定します。「All Ports」を選択すると、すべてのポートを選択します。

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。また、「All Port」を選択するとスイッチの全ポートの情報をクリアします。

Cable Diagnostics（ケーブル診断機能）

スイッチの特定のポートに接続する UTP ケーブルの詳細について表示します。ケーブルにエラーがある場合、エラーのタイプと発生箇所を判断します。ケーブル診断機能は主に管理者とカスタマサービス担当者が UTP ケーブルを検証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。

1. **Monitoring > Cable Diagnostics** の順にメニューをクリックし、以下の画面を表示します。

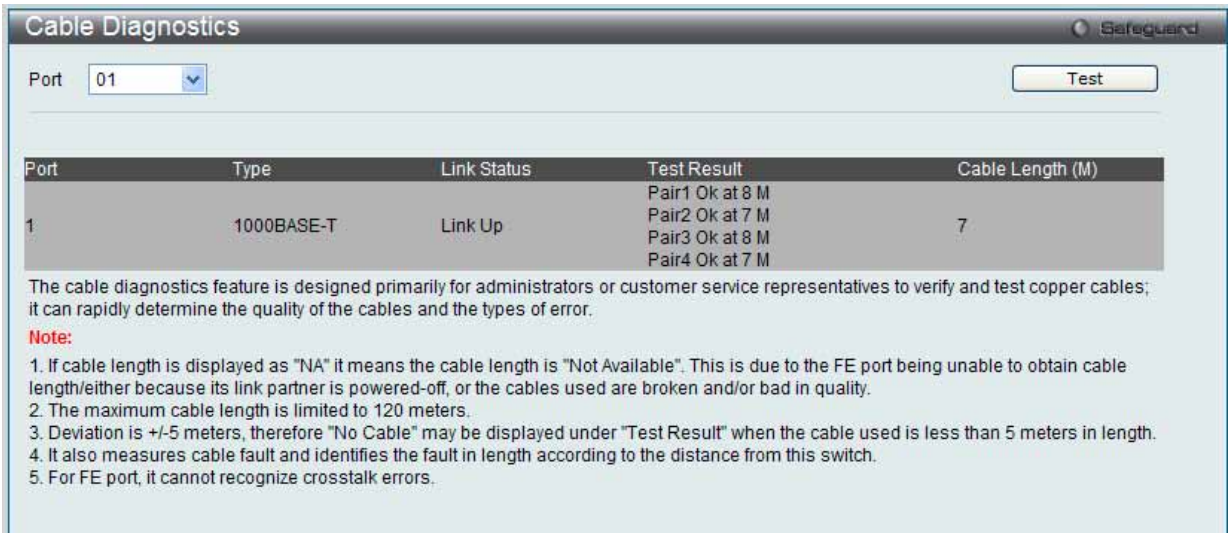


図 7.9-23　Cable Diagnostics 画面

2. 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。

エラーメッセージは以下の通りです。

項目	説明
Open	このペアはオープン状態です。
Short	このペアの 2 つのラインがショートしています。
CrossTalk	このペアのラインは共にショートしています。
Unknown	診断によりケーブルステータスを取得しませんでした。再度実行してください。
NA	ケーブルが見つかりません。ケーブルが診断の仕様外であるか品質が非常に悪い可能性があります。

注意　ケーブル診断機能の制限

ケーブル長検出は GE ポートでのみサポートされています。ポートは 1000M の速度でリンクおよび動作する必要があります。クロストークエラー検出は FE ポートではサポートされていません。

注意　ケーブルが挿入されていないポートでは診断結果が誤った値になる場合があります。

注意　有効なケーブル診断の長さは 5-120m です。

注意　ケーブル長検出の誤差は GE ポートで +/-5m です。

7.10 Monitoring（スイッチのモニタリング）

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

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

サブメニュー	説明	参照ページ
Utilization（CPU 使用率）	CPU 使用率、ポートの帯域使用率を表示します。次のメニューがあります。 CPU Utilization（CPU 使用率）、DRAM & Flash Utilization（DRAM とフラッシュ利用率）、Port Utilization（ポート使用率）	357
Statistics（統計情報）	パケット統計情報とエラー統計情報を表示します。次のメニューがあります。 Packets（パケット統計情報）、Errors（パケットエラー）、Packet Size（パケットサイズ）	359
Mirror（ポートミラーリング）	ポートミラーリングの設定を行います。次のメニューがあります。 Port Mirror Settings（ポートミラーリング設定）、RSPAN Settings（RSPAN 設定）	368
sFlow（sFlow 設定）	sFlow 機能の設定を行います。次のメニューがあります。 sFlow Global Settings（sFlow グローバル設定）、sFlow Analyzer Server Settings（sFlow アナライザ設定）、sFlow Flow Sampler Settings（sFlow サンプラ設定）、sFlow Counter Poller Settings（sFlow カウンタポーラ設定）	370
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。	374
Trace Route（トレースルート）	ネットワーク上のスイッチとホスト間の経路をトレースします。	375
Peripheral（周辺機器）	デバイス環境機能はスイッチの内部温度ステータスを表示します。	376

Utilization（使用率）

CPU Utilization（CPU 使用率）

現在の CPU 使用率をパーセント表示し、また指定した間隔で計算した平均値も表示します。

1. **Monitoring > Utilization > CPU Utilization** メニューをクリックし、以下の画面を表示します。

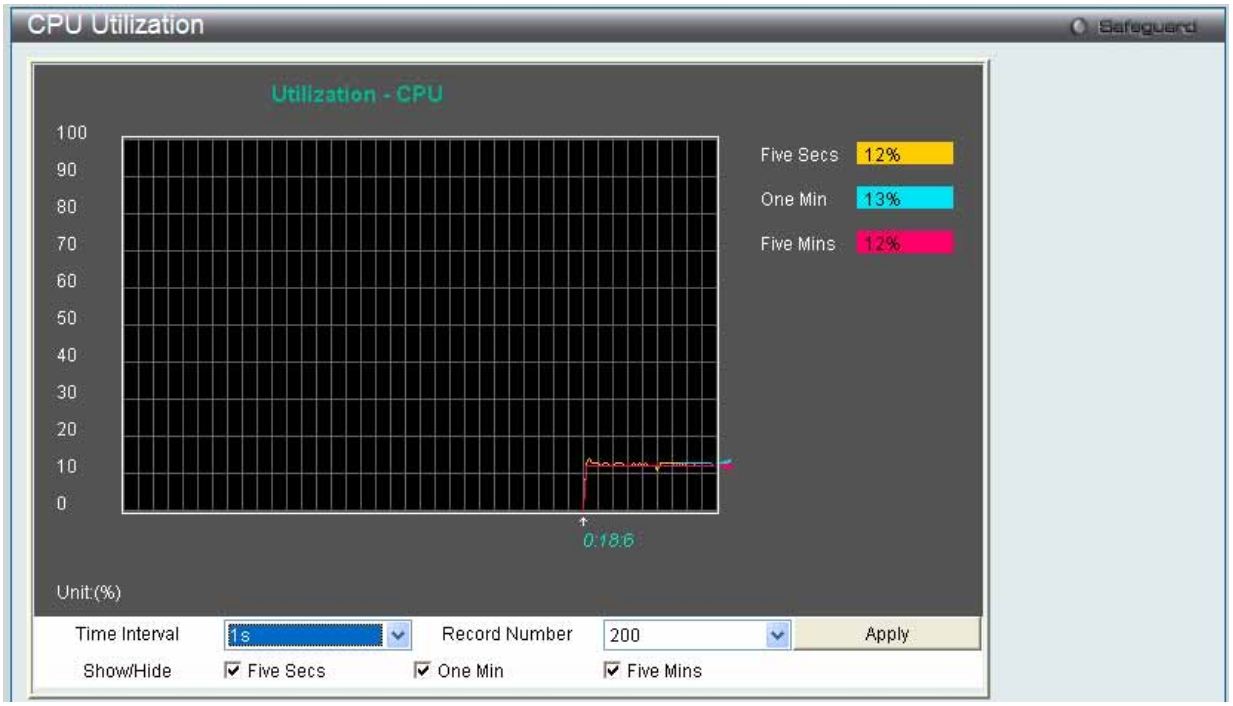


図 7.10-1 CPU Utilization 画面

2. 以下の設定項目を使用して表示を変更します。

項目	説明
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	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。

DRAM & Flash Utilization（DRAM とフラッシュ利用率）

DRAM とフラッシュ利用率に関する情報を参照します。

Monitoring > Utilization > DRAM & Flash Utilization メニューをクリックし、以下の画面を表示します。

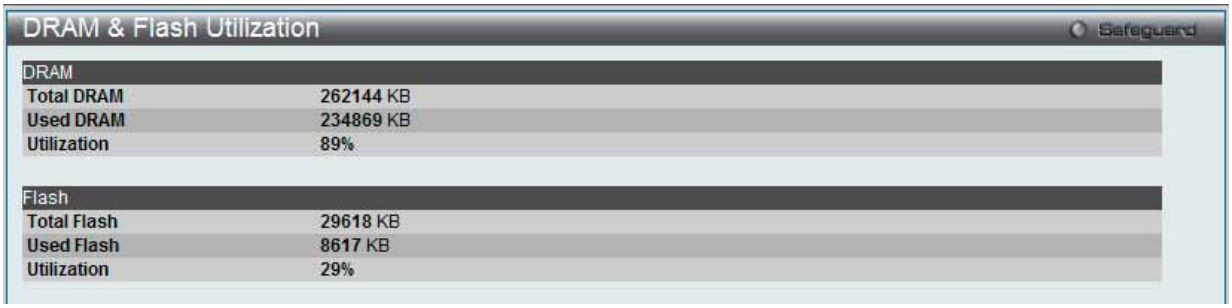


図 7.10-2　DRAM & Flash Utilization 画面

Port Utilization（ポート使用率）

ポートの帯域使用率を表示します。

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

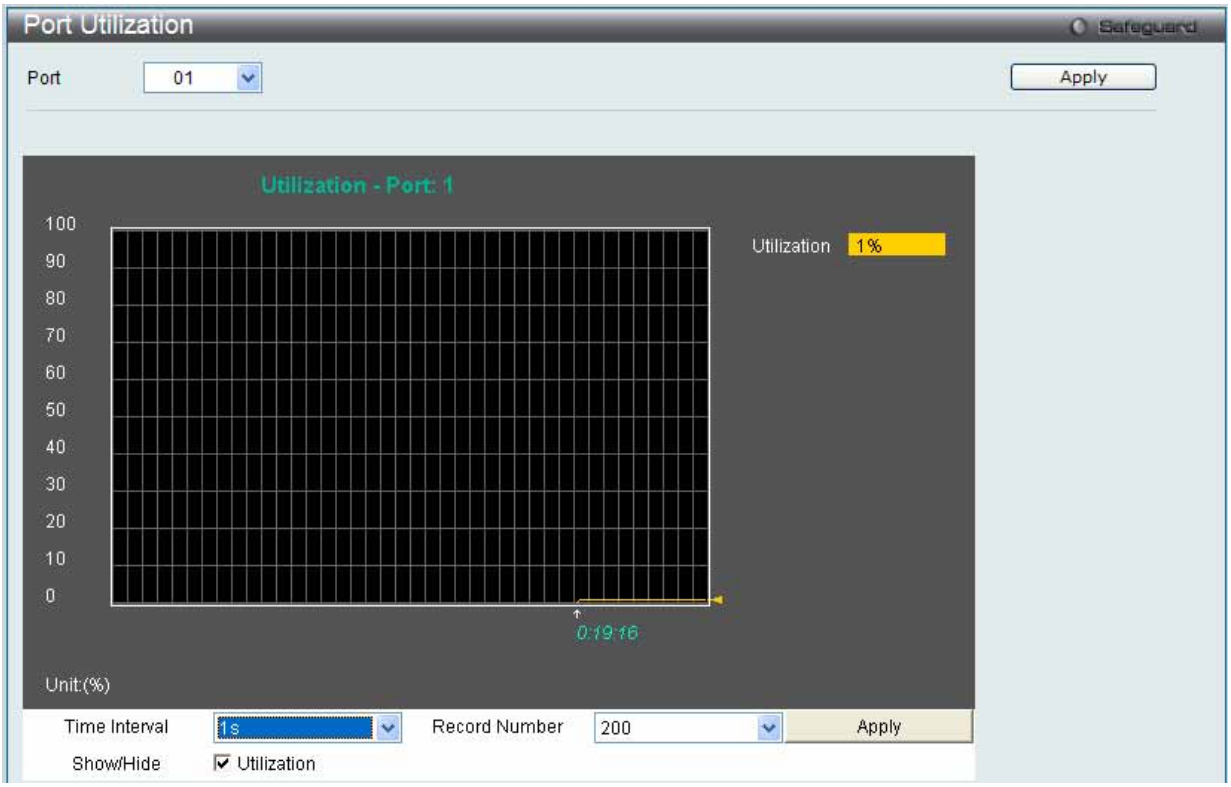


図 7.10-3　Port Utilization 画面

2. 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 ページ上部にあるスイッチ上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。

3. 以下の設定項目を使用して表示を変更します。

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	「Utilization」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。

Statistics（統計情報）

Packets（パケット統計情報）

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。

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 ページ上部にあるスイッチ上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 > Statistics > 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。

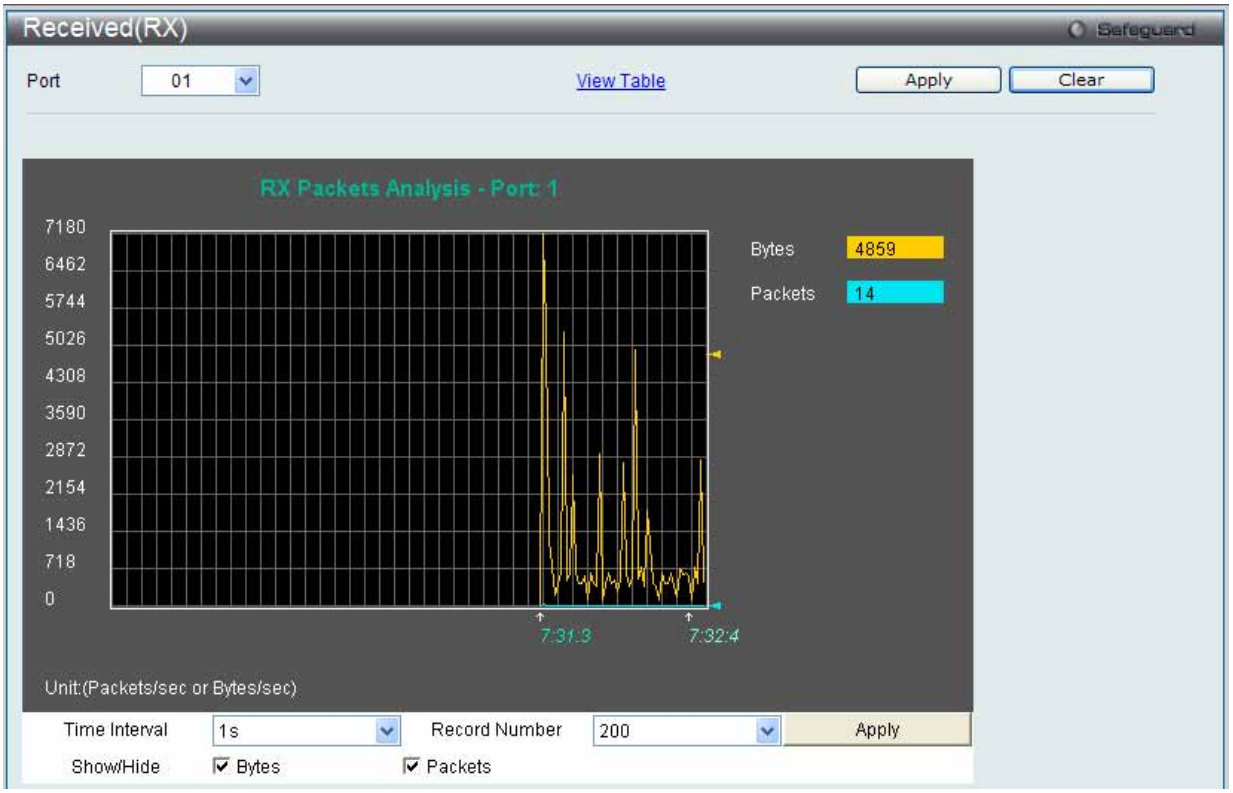


図 7.10-4　Received（RX）画面（バイトとパケットの折れ線グラフ）

「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 7.10-5　Received（RX）Table 画面（バイトとパケットの表）

以下の項目を使用して設定および参照します。

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）をカウントします。
Packets	ポートに受信したパケット数をカウントします。
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 ページ上部にあるスイッチ上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 > Statistics > 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。

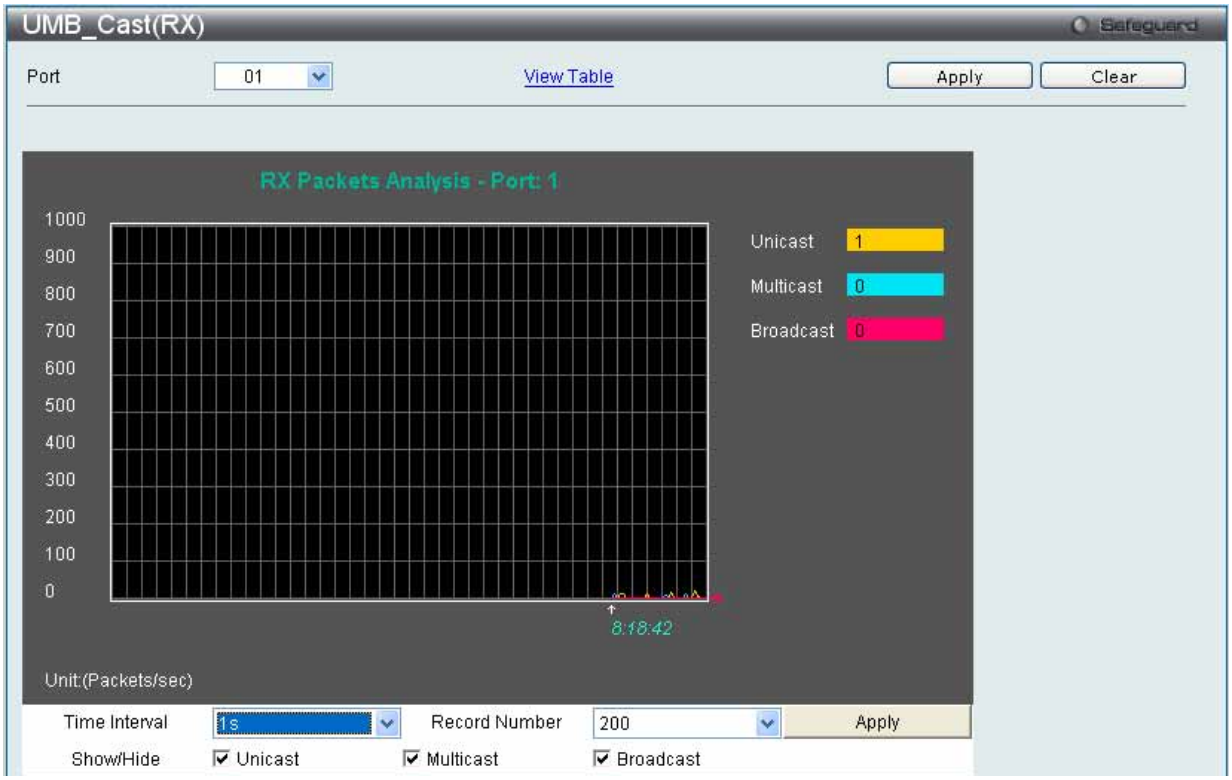


図 7.10-6　UMB_Cast（RX）画面（ユニキャスト、マルチキャスト、ブロードキャスト情報の折れ線グラフ）

「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 7.10-7　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）

以下の項目を使用して設定および参照します。

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 ページ上部にあるスイッチ上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 > Statistics > 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。

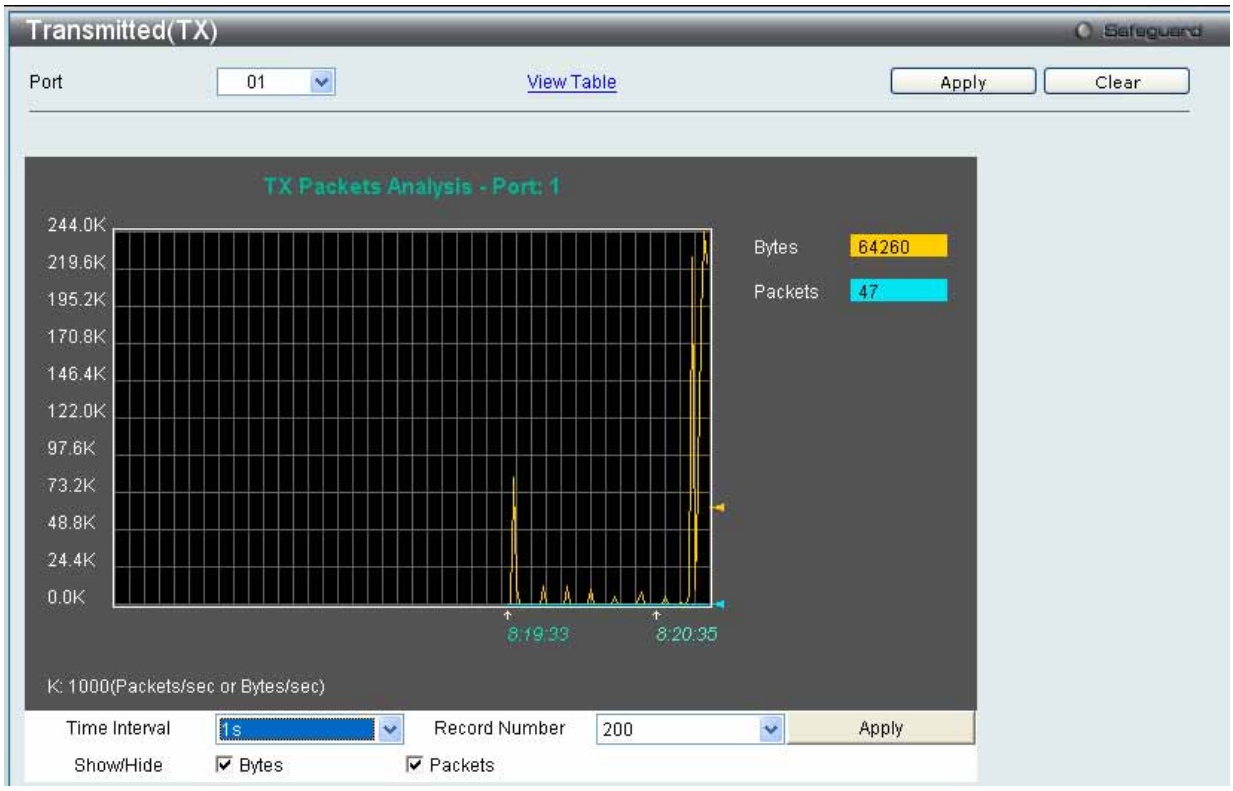


図 7.10-8　Transmitted（TX）画面（パケットサイズ、パケット数の折れ線グラフ表示）

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 7.10-9　Transmitted（TX）Table 画面（パケットサイズ、パケット数の表示）

以下の項目を使用して設定および参照します。

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 ページ上部にあるスイッチ上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 > Statistics > 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。

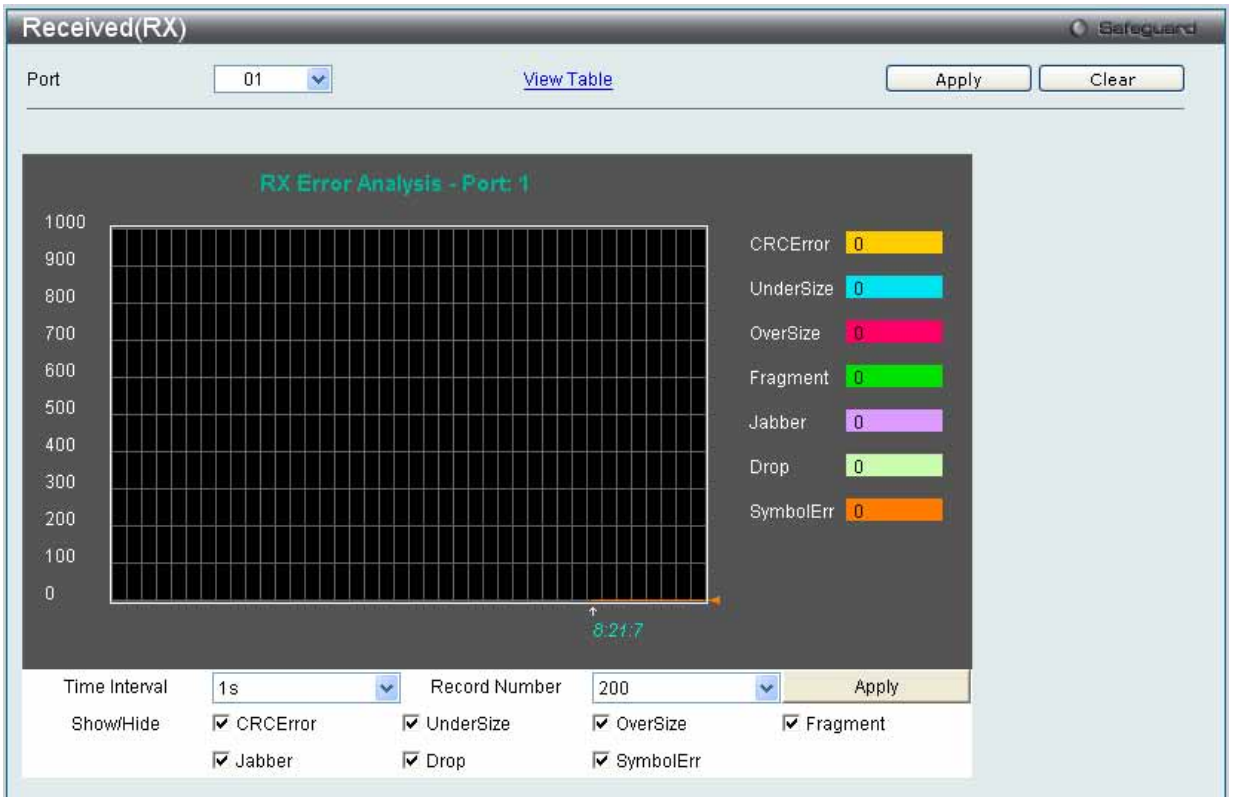


図 7.10-10　Received（RX）- Error 画面（折れ線グラフ形式）

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。

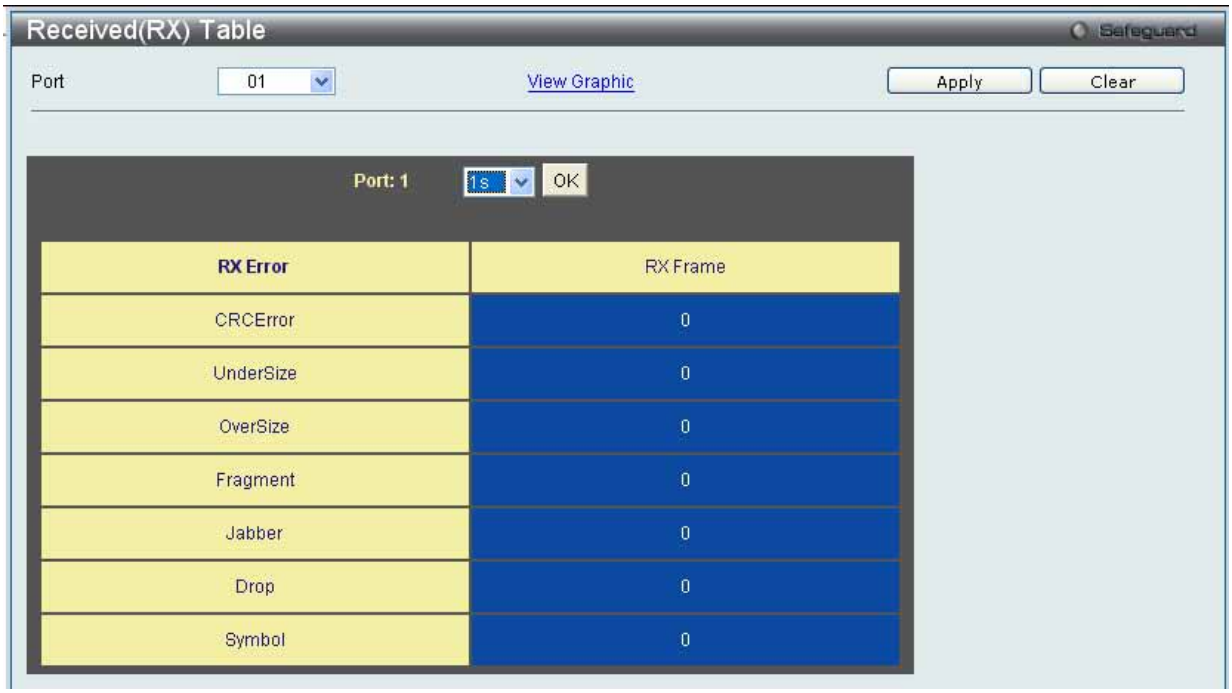


図 11-14　Received（RX）Table - Error 画面（表形式）

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 ページ上部にあるスイッチ上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 > Statistics > 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。

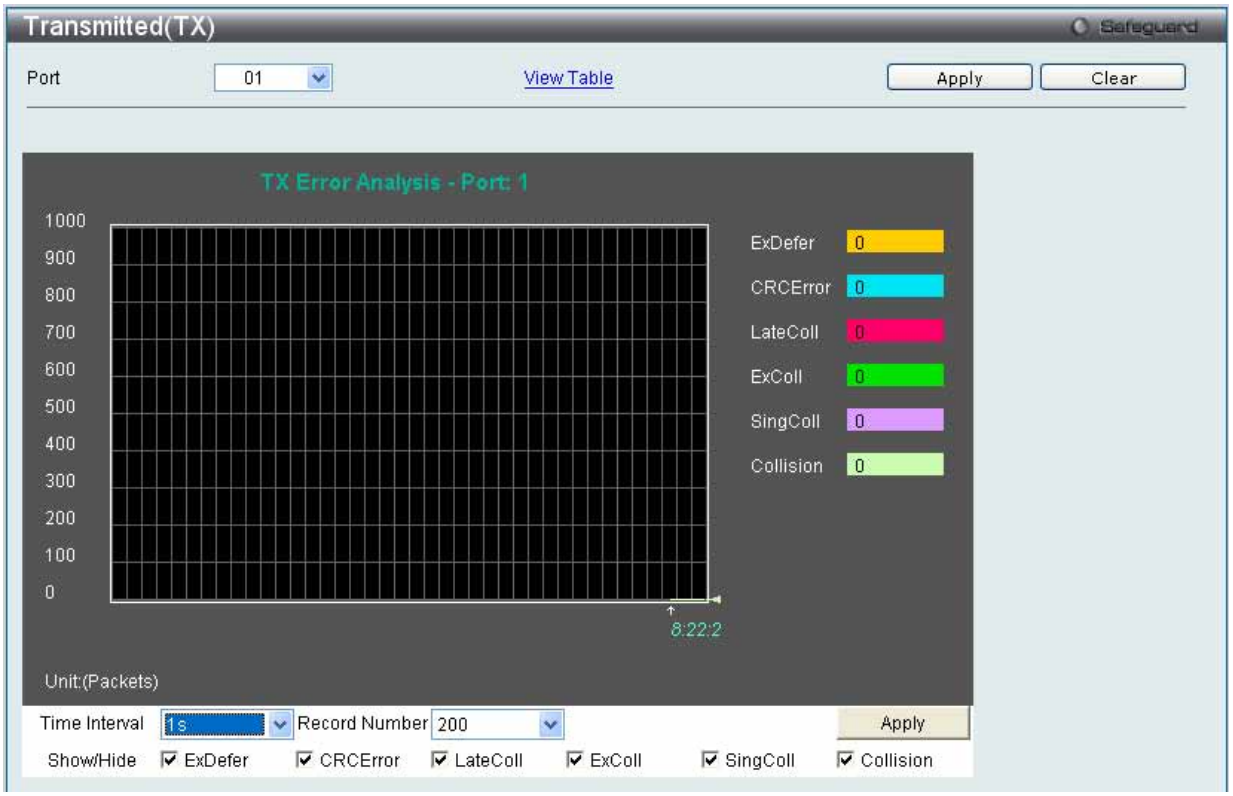


図 11-15　Transmitted（TX）- Error 画面（折れ線グラフ形式）

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 7.10-11　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。

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 ページ上部にあるスイッチ上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 > Statistics > 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。

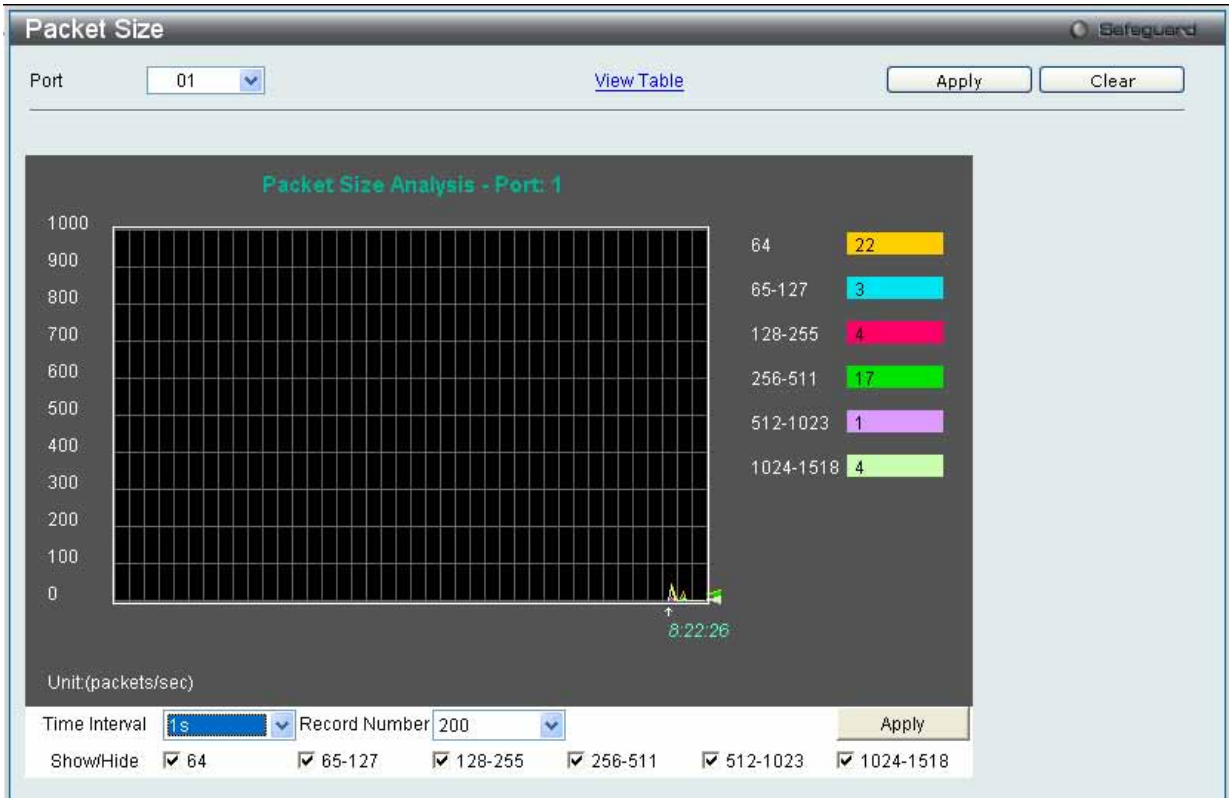


図 7.10-12　Packet Size 画面（折れ線グラフ）

「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 7.10-13　Packet Size Table 画面（表形式）

以下の項目を使用して設定および参照します。

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 および 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。

Mirror（ポートミラーリング）

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。

Port Mirror Settings（ポートミラーリング設定）

ポートミラーリング機能を設定します。

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

図 7.10-14　　Port Mirror Settings 画面

ミラーポートの設定手順：

1. 「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。また、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。

以下の項目を使用して設定および参照します。

項目	説明
Target Port Setting	
State	ポートミラーリング機能を「Enabled」（有効）/「Disabled」（無効）にします。
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	ポートが外向きトラフィックを含むかどうかを選択します。
RX	ポートが内向きトラフィックを含むかどうかを選択します。
Both	ポートが内向きおよび外向きの両方のトラフィックを含むかどうかを選択します。
None	ポートがどのトラフィックも含まないかどうかを選択します。

RSPAN Settings（RSPAN 設定）

RSPAN機能をコントロールします。RSPAN機能の目的は、パケットをリモートスイッチにミラーリングすることです。パケットは、ミラーされるパケットを受信したスイッチから、中間スイッチを通過し、スニファーが接続するスイッチに送信します。最初のスイッチはソーススイッチと言われます。

RSPAN 機能を動作するためには、ソーススイッチに RSPAN VLAN ソース設定を行います。中間スイッチと最後のスイッチに関しては、RSPAN VLAN のリダイレクト設定を行います。

注意 RSPAN が有効な場合だけ (1 つの RSPAN VLAN がソースポートに設定されている場合)、RSPAN VLAN ミラーリングは動作します。RSPAN が有効になり、少なくとも 1 つの RSPAN VLAN がリダイレクトポートに設定されると、RSPAN リダイレクト機能は動作します。

1. **Monitoring > Mirror > RSPAN Settings** の順にメニューをクリックし、以下の画面を表示します。

図 7.10-15　RSPAN Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
RSPAN State	RSPAN 機能を「Enabled」（有効）/「Disabled」（無効）にします。
VLAN Name	VLAN 名により RSPAN VLAN を指定します。
VID (1-4094)	VLAN ID により RSPAN VLAN を指定します。

「RSPAN State」を「Enabled」または「Disabled」にして「Apply」ボタンをクリックして、RSPAN 機能を「Enabled」（有効）/「Disabled」（無効）にします。

エントリの追加

「VLAN Name」または「VID」を指定後、「Add」ボタンをクリックして、入力した情報に基づいて新しいエントリを追加します。

エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。

RSPAN 設定の編集

1. 「Modify」ボタンをクリックして、以下の画面を表示します。

図 7.10-16　RSPAN Settings (Modify) 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
VID	VLAN ID により RSPAN VLAN を表示します。
VLAN Name	VLAN 名により RSPAN VLAN を表示します。
Source Ports	ポートがこのオプションで指定されないと、RSPAN のソースは「mirror」コマンドによって指定されるソースまたは ACL によって指定されたフローベースのソースとなります。ソースにパラメータが指定されないと、設定されたソースパラメータは削除されます。パケットをモニタする方向（RX、TX、Both）を選択します。「Add」または「Delete」ボタンをクリックしてソースポートを追加または削除します。
Redirect Port List	RSPAN VLAN パケットに出力ポートリストを指定します。リダイレクトポートがリンクアグリゲーションポートであると、RSPAN パケットにリンクアグリゲーションの動作を行います。「Add」または「Delete」ボタンをクリックしてリダイレクトポートを追加または削除します。

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

「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

sFlow（sFlow 設定）

sFlow（RFC3176）はスイッチとルータを含むデータネットワークのトラフィックをモニタリングする技術です。sFlow モニタリングシステムは、（スイッチまたはルータに組み込まれている、またはスタンドアロンの検査装置にある）sFlow エージェントと中央の sFlow コレクタから成っています。sFlow モニタリングシステムで使用されるアーキテクチャとサンプリング手法は、高速でスイッチされて、ルートを決定されるネットワークに対して連続したサイト全体（企業全体）のトラフィックモニタリングを提供するように設計されています。

sFlow Global Settings（sFlow グローバル設定）

sFlow 機能を「Enabled」（有効）/「Disabled」（無効）にします。

1. **Monitoring > sFlow > sFlow 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 7.10-17　sFlow Global Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
sFlow State	sFlow 機能を「Enabled」（有効）/「Disabled」（無効）にします。

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。

sFlow Analyzer Server Settings（sFlow アナライザ設定）

スイッチは、同時に 4 個の異なるアナライザサーバをサポートすることができ、各サンプラまたはポーラはコレクタを選択してサンプルを送信します。異なるサンプラまたはポーラから異なるコレクタに異なるサンプルを送信できます。

1. **Monitoring > sFlow > sFlow Analyzer Server Settings** の順にメニューをクリックし、以下の画面を表示します。

図 7.10-18　sFlow Analyzer Server Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Analyzer Server ID (1-4)	パケットが転送されるアナライザサーバの ID を指定します。
Owner Name	この sFlow アナライザサーバを利用するエンティティ。オーナが設定または変更される場合、タイムアウト値は自動で 400 になります。
Timeout (1-2000000)	サーバがタイムアウトになるまでの時間。アナライザサーバがタイムアウトになると、すべての sFlow サンプラとこのアナライザサーバに関連するカウンタポーラは削除されます。初期値は 400 です。「Infinite」をチェックすると制限はなくなります。
Collector Address	アナライザサーバの IP アドレスを指定します。指定しないか、0 のアドレスを設定すると、エントリは非アクティブになります。
Collector Port (1-65535)	sFlow データが送信される宛先 UDP ポート。初期値は 6343 です。
Max Datagram Size (300-1400)	1 つのサンプルデータにパックされるデータの最大数（バイト）。初期値は 1400 です。

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

エントリの編集

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

図 7.10-19　sFlow Analyzer Server Settings 画面 - Edit

2. 指定エントリを編集して「Apply」ボタンをクリックします。

エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。

sFlow Flow Sampler Settings（sFlow サンプラ設定）

sFlow アナライザサーバのパラメータを設定します。ポートにサンプリング機能を設定することによって、このポートが受信したサンプルパケットはカプセル化されて指定間隔でアナライザサーバに転送されます。

注意　アナライザサーバ ID を変更するためには、フローサンプラの削除後に、新規に作成する必要があります。

1. **Monitoring > sFlow > sFlow Flow Sampler Settings** の順にメニューをクリックし、以下の画面を表示します。

図 7.10-20　sFlow Flow Sampler Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
From Port / To Port	設定するポートリストを指定します。
Analyzer Server ID (1-4)	パケットが転送されるアナライザサーバの ID を指定します。
Rate (0-65535)	受信パケットサンプリングのためのサンプリングレート。256 の倍数で設定されたレートが実効レートです。例えば、レートが 20 であれば、実効レートは 5120 です。あるパケットが 5120 のパケットごとに抽出されます。0 に設定されると、サンプラは無効になります。レートを指定しないと、初期値は 0 です。
Max Header Size (18-256)	カプセル化してサーバに送信するサンプリングパケットのヘッダの最大バイト数。初期設定は 128 です。

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

エントリの編集

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

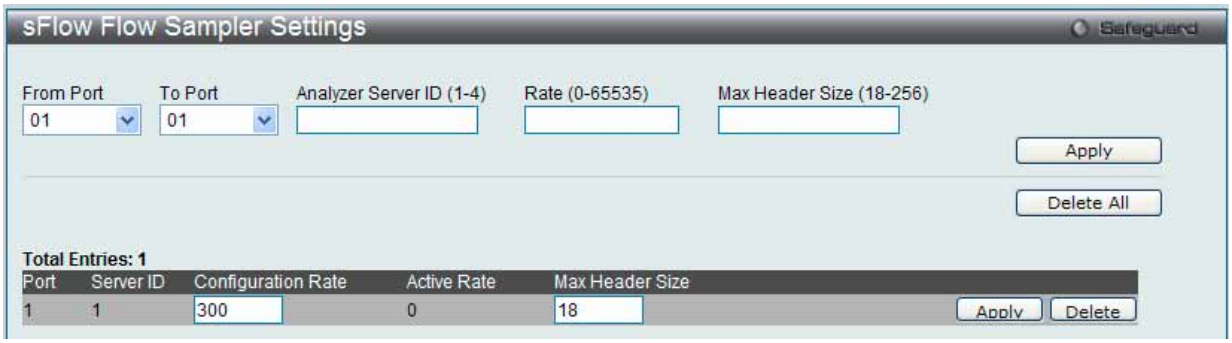


図 7.10-21　sFlow Flow Sampler Settings 画面 - Edit

2. 指定エントリを編集して「Apply」ボタンをクリックします。

エントリの削除

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

sFlow Counter Poller Settings（sFlow カウンタポーラ設定）

sFlow カウンタポーラのパラメータを設定します。アナライザサーバ ID を変更するためには、カウンタポーラの削除後に、新規に作成する必要があります。

1. **Monitoring > sFlow > sFlow Counter Poller Settings** の順にメニューをクリックし、以下の画面を表示します。

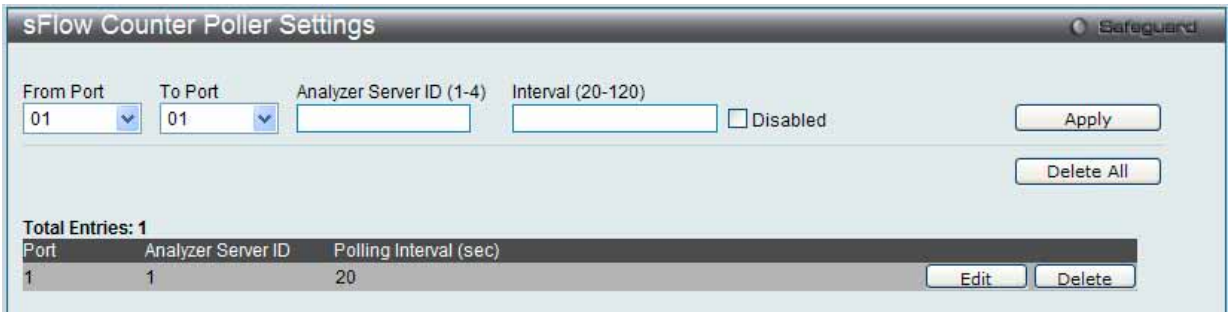


図 7.10-22　sFlow Counter Poller Settings 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
From Port / To Port	設定するポートリストを指定します。
Analyzer Server ID (1-4)	パケットが転送されるアナライザサーバの ID を指定します。
Interval (20-120)	カウンタの連続するサンプルの間隔（秒）。

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

エントリの編集

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

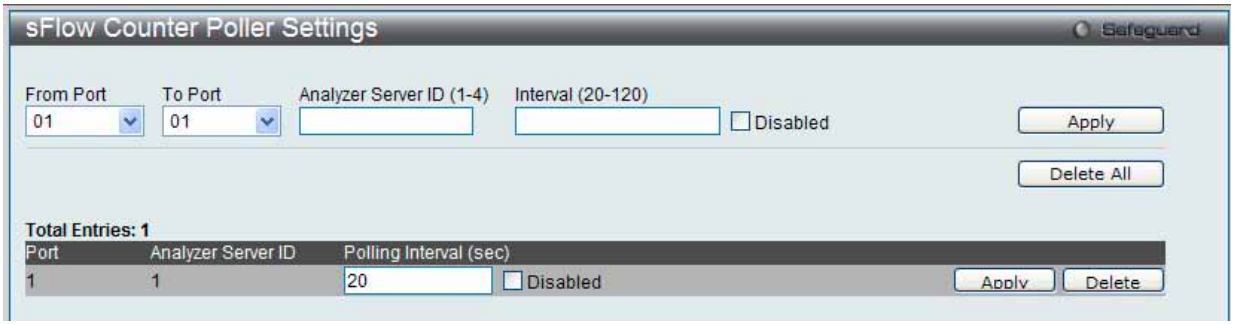


図 7.10-23　sFlow Counter Poller Settings 画面 - Edit

2. 指定エントリを編集して「Apply」ボタンをクリックします。

エントリの削除

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

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。

1. **Monitoring > 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。

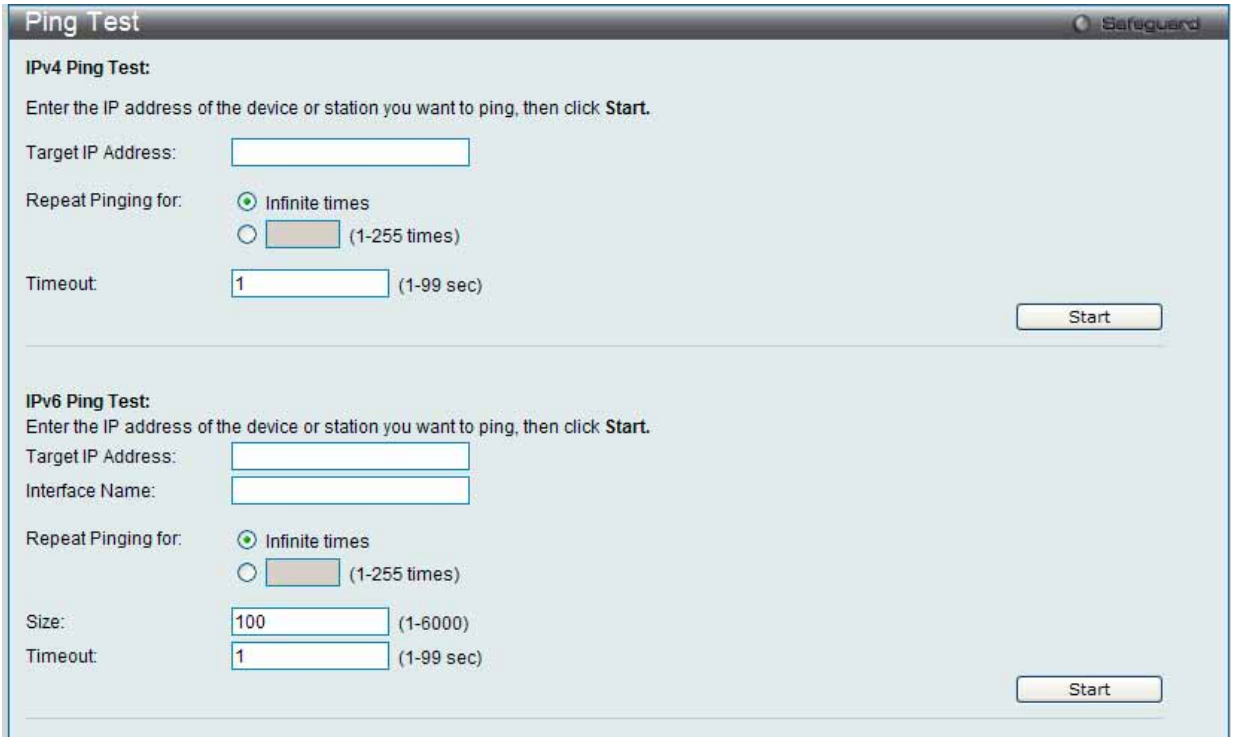


図 7.10-24　Ping Test 画面

2. 「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および参照します。

項目	説明
IPv4 Ping Test	
Target IP Address	Ping する IP アドレスを入力します。
Repeat Pinging for	送信先 IPv4 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。
Timeout	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。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。
IPv6 Ping Test	
Target IPv6 Address	Ping する IPv6 アドレスを入力します。
Interface Name	Ping するインタフェースの名前を入力します。
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 の場合のみ、1-6000 の値を入力します。初期値は 100 です。
Timeout	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。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。

以下の結果画面が表示されます。

図 7.10-25　Ping Test Result 画面

「Stop」ボタンをクリックして、Ping テストを停止します。
「Resume」ボタンをクリックして、Ping テストを再開します。

Trace Route（トレースルート）

ネットワーク上のスイッチとホスト間の経路をトレースします。

1. **Monitoring > Trace Route** の順にメニューをクリックし、以下の画面を表示します。

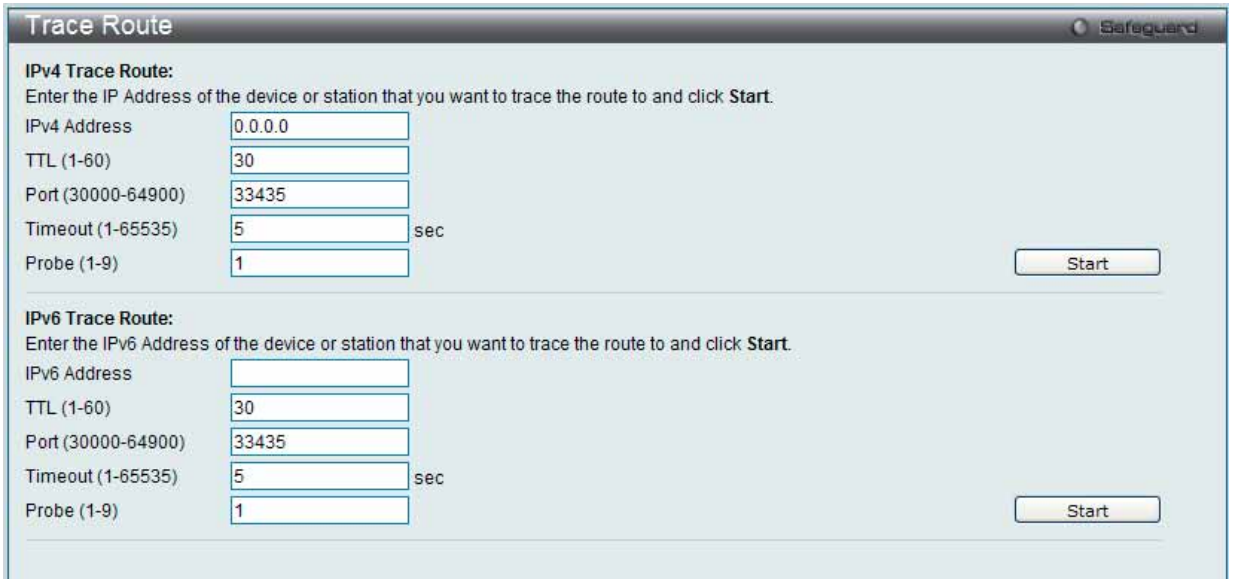


図 7.10-26　Trace Route 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
IPv4 Address	宛先ステーションの IP アドレス。
IPv6 Address	宛先ステーションの IPv6 アドレス。
TTL (1-60)	トレースルートリクエストの有効時間。これは、トレースルートパケットが経由するルータの最大数です。トレースルートは、2 つのデバイス間のネットワーク経路を検索する間に経由します。TTL の範囲は 1-60 ホップです。
Port (3000-64900)	ポート番号。値の範囲は 30000-64900 です。
Timeout (1-65535)	リモートデバイスからの応答を待つ時間を定義します。1-65535（秒）を指定します。初期値は 5（秒）です。
Probe (1-9)	プローブ数。範囲は 1-9 です。初期値は 1 です。

「Start」ボタンをクリックして、トレースルートを開始します。

以下の結果画面が表示されます。

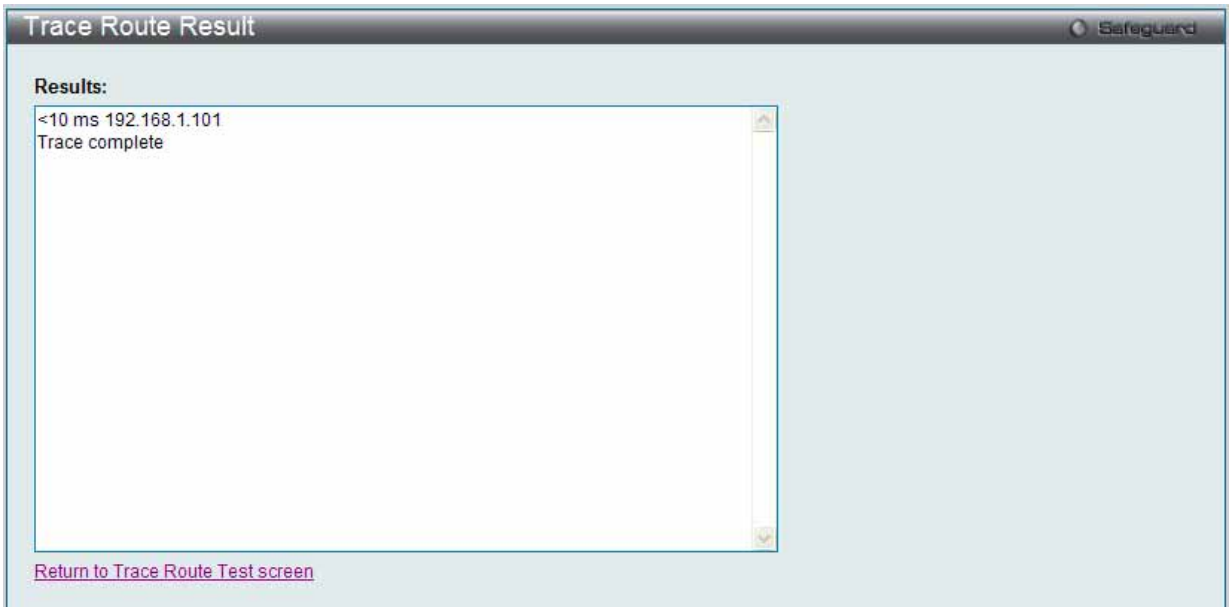


図 7.10-27　Trace Route Result 画面

「Stop」ボタンをクリックして、トレースルートを停止します。
「Resume」ボタンをクリックして、トレースルートを再開します。

「Return to True Route Test screen」リンクをクリックして「Trace Route」画面に戻ります。

Peripheral（周辺機器）

Device Environment（デバイス環境の参照）

デバイス環境機能はスイッチの内部温度ステータスを表示します。

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

図 7.10-28　Device Environment 画面

「Refresh」ボタンをクリックし、テーブルを更新して新しいエントリを表示します。

第 8 章 WAN タブ （WAN の設定）

8.1 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
Captive Portal（キャプティブポータル）	有線 / 無線ユーザ両方についてネットワークへの接続性を制御します。以下のメニューがあります。 CP Configuration（CP 設定）、CP Web ページのカスタマイズ、Local User（ローカルユーザ）、Interface Association（インタフェースアソシエーション）、CP Status（CP 状態）、Interface Status（インタフェース状態）、Client Connection Status（クライアントの接続状態）、SNMP Trap Configuration（SNMP トラップ設定）	378

Captive Portal（キャプティブポータル）

Captive Portal（CP）は、有線 / 無線ユーザ両方についてネットワークへの接続性を制御する機能です。ここでは、ゲストと認証ユーザにアクセスを許可するための検証を設定します。

注意 「Captive Portal (CP)」フォルダはナビゲーション画面の「LAN」タブからもアクセスできます。本フォルダ内のどの設定も「WLAN」タブの「Captive Portal (CP)」フォルダと全く同じです。

Global Configuration（グローバル設定）

グローバルに CP 設定を行います。

1. **Security > Captive Portal (CP) > Global 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。

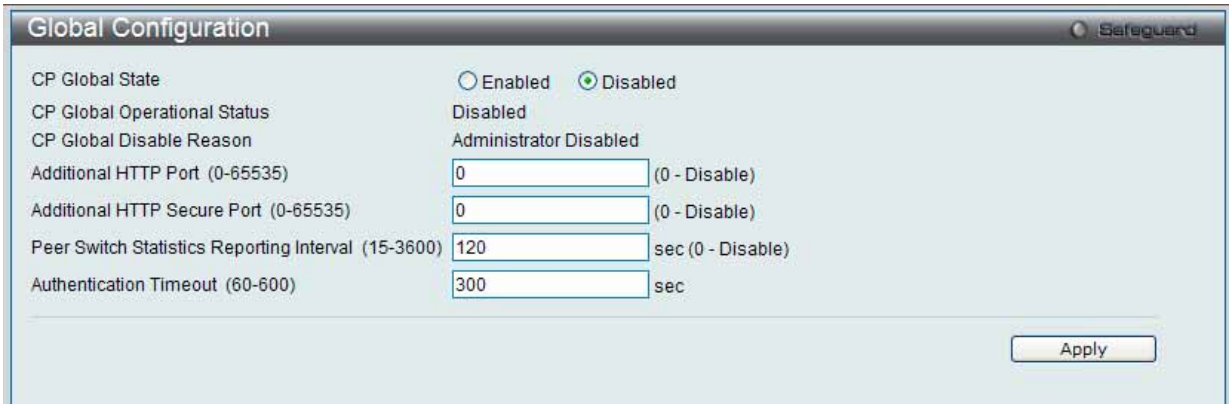


図 8.1-29 Global Configuration 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
CP Global State	CP のグローバル状態を「Enabled」(有効) /「Disabled」(無効) にします。
CP Global Operational Status	CP の操作状態を表示します。
CP Global Disable Reason	キャプティブポータルが無効にされた場合に、本欄ではその理由を表示します。 表示可能な理由は以下の通りです。: • Administrator Disabled（管理者が無効にした） • IP Address Not Configured（IP アドレスが未設定） • No IP Routing Interface and Routing Disabled（IP ルーティングインタフェースがなく、ルーティングは無効）
Additional HTTP Port (0-65535)	追加 HTTP ポート番号（0-65535 の範囲、80 と 443 は除く）を入力します。80 は HTTP デフォルトポート、および 443 は HTTPS デフォルトポートに予約されています。初期値は 0 で、これは追加ポートは使用されていないことを示しています。
Additional HTTP Secure Port (0-65535)	追加 HTTP ポート番号（0-65535 の範囲、80 と 443 は除く）を入力します。80 は HTTP デフォルトポート、および 443 は HTTPS デフォルトポートに予約されています。初期値は 0 で、これは追加ポートは使用されていないことを示しています。
Peer Switch Statistics Reporting Interval (15-3600)	クラスタリングがスイッチにサポートされている場合は、ピアスイッチが認証済みクライアントの統計情報をクラスタコントローラに送信する頻度を入力します。レポート間隔は 0 および 15-3600（秒）です。値 0 は機能を無効にすることを意味します。初期値は 120 です。
Authentication Timeout (60-600)	認証時間を入力します。CP ユーザは時間内に有効な証明書を入力しないと、クライアントがネットワークへのアクセスを獲得するために、再度認証ページを表示する必要があります。値は 60-600（秒）です。

「Apply」ボタンをクリックして各セクションで行った変更を適用します。

CP Configuration（CP 設定）

CP コンフィグレーションを作成します。

1. **Security > Captive Portal (CP) > CP 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 8.1-30　CP configuration - CP Summary タブ画面

以下の項目を使用して設定および参照します。

項目	説明
CP Configuration	CP コンフィグレーション名を入力します。
Configuration	CP ID と名前を表示します。
Mode	CP が有効か否かを表示します。
Protocol	ポータルが HTTP または HTTPS のどちらを使用するかを表示します。
Verification	実行するユーザ検証のタイプを表示します。 • Guest - ユーザはデータベースに認証される必要がありません。 • Local - スイッチは認証ユーザに対してローカルデータベースを使用します。 • RADIUS - スイッチはユーザを認証するためにリモート RADIUS サーバのデータベースを使用します。
Languages	このキャプティブポータルに設定される言語の数を表示します。

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

エントリの追加

「CP Configuration」を入力し、「Add」ボタンをクリックして新しいエントリを追加します。指定した名前で新しくタブが表示されます。

エントリの削除

特定エントリのボックスをチェック後、「Delete」ボタンをクリックして指定エントリを削除します。

CP コンフィグレーションの詳細情報設定

1. テーブル内の「Configuration」下のリンク、または設定する CP コンフィグレーション名のタブをクリックして、以下の画面を表示します。

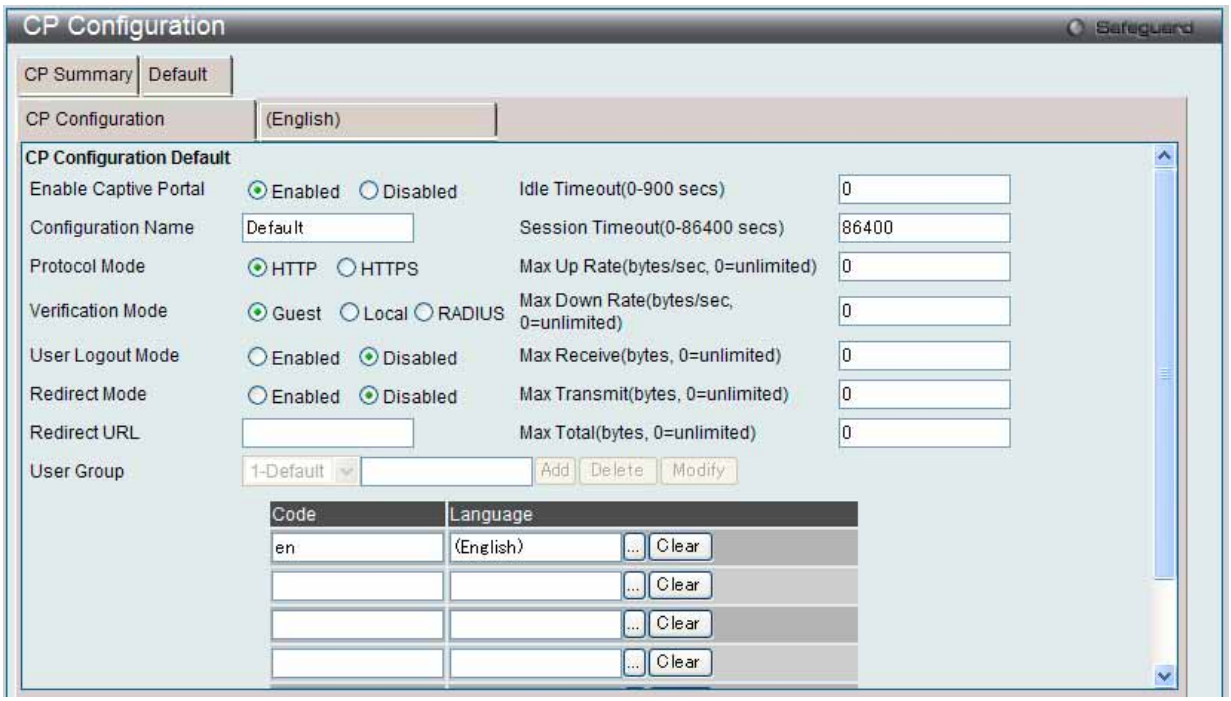


図 8.1-31　CP Configuration - Edit 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Enable Captive Portal	ラジオボタンを使用して CP コンフィグレーションを「Enabled」（有効）/「Disabled」（無効）にします。
Configuration Name	編集するコンフィグレーション名を入力します。
Protocol Mode	検証処理で CP コンフィグレーションを使用するプロトコル（HTTP または HTTPS）のラジオボタンをクリックします。
Verification Mode	ラジオボタンをクリックして、クライアントを検証するモードを選択します。 • Guest - ユーザはデータベースに認証される必要がありません。 • Local - スイッチは認証ユーザに対してローカルデータベースを使用します。 • RADIUS - スイッチはユーザを認証するためにリモート RADIUS サーバのデータベースを使用します。
User Logout Mode	ラジオボタンをクリックして、認証ユーザがネットワークから認証解除を行うことを「Enabled」（有効）/「Disabled」（無効）にします。
Redirect Mode	ラジオボタンを使用して CP コンフィグレーションのリダイレクトモードを「Enabled」（有効）/「Disabled」（無効）にします。
Redirect URL	「Redirect Mode」が有効である場合、新たに認証されたクライアントがリダイレクトされる URL を入力します。
Idle Time	自動的にログアウトされるまでユーザが待機できる時間（秒）を入力します。値 0 はタイムアウトが行われないことを示します。初期値は 0 です。
Session Timeout	セッション終了までの待ち時間を入力します。セッションタイムアウトになると、ユーザはログアウトされます。値 0 はタイムアウトが行われないことを示します。
Max Up Rate	CP の使用時にクライアントがデータを送信できる最高速度（バイト / 秒）を入力します。速度の範囲は 0-536870911 です。
Max Down Rate	CP の使用時にクライアントがデータを受信できる最高速度（バイト / 秒）を入力します。速度の範囲は 0-536870911 です。
Max Receive	CP の使用時にクライアントが受信できる最大バイト数を入力します。この制限に到達すると、ユーザは切断されます。
Max Transmit	CP の使用時にクライアントが送信できる最大バイト数を入力します。この制限に到達すると、ユーザは切断されます。
Max Total	クライアントが送受信できる最大バイト数の合計を入力します。この制限に到達すると、ユーザは切断されます。
User Group	「Verification Mode」に「Local」または「RADIUS」を選択した場合、ユーザグループを割り当てる必要があります。グループに所属するすべてのユーザが、このポータル経由でネットワークにアクセスすることが許可されます。CP すべてにユーザグループを作成、削除、または編集することができます。 • プルダウンメニューから CP に割り当てる定義済みユーザグループを選択します。 • 新しいユーザグループを作成するためには、本欄に名前を入力し、「Add」ボタンをクリックします。 • 既存のユーザグループ名を変更するためには、プルダウンメニューから変更する名前を選択し、新しい名前をフィールドに入力して、「Modify」ボタンをクリックします。
Code	言語に対して IANA 言語サブタグコードを入力します。すべてのコードが IANA 言語サブタグレジストリに表示されます。スイッチが言語をサポートしている場合、言語を選択すると自動的に入力されます。
Language	「…」ボタンをクリックして、CP に使用する言語を選択します。「Clear」ボタンをクリックして、リストから言語を削除します。

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

設定のクリア

「Clear」ボタンをクリックして、すべてのコンフィグレーションを一掃し、初期設定に戻します。

CP Web ページのカスタマイズ

言語タブをクリックして、CP Web ページをカスタマイズします。

例えば、キャプティブポータルページの英語版をカスタマイズするためには、（English）タブをクリックします。Web ページは無線クライアントがアクセスポイントに接続している場合に表示します。プルダウンメニューを使用して、CP Web 用に別の Web ページをカスタマイズします。

Global Parameters（グローバルパラメータ）

1. 画面上部のプルダウンメニューから「Global Parameters」を選択して、以下の画面を表示します。

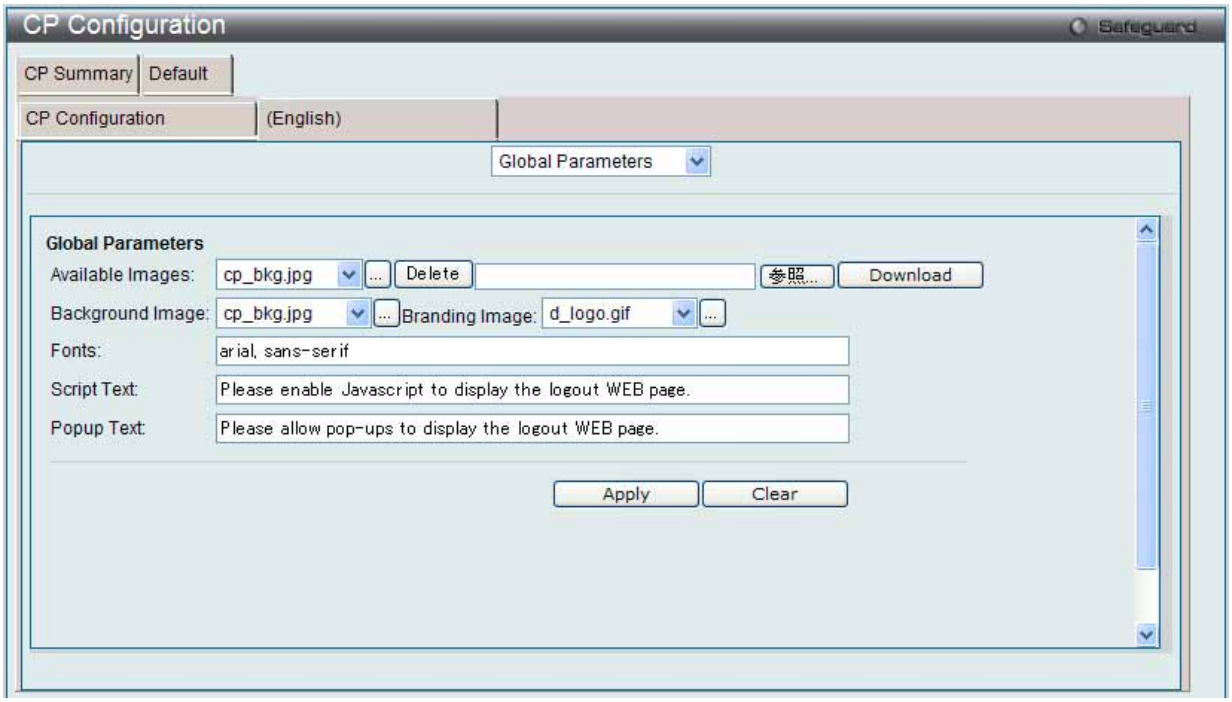


図 8.1-32　CP Configuration - Customize（Global Parameters）画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Available Images	プルダウンメニューにはページ背景、画面タイトルおよびアカウント画像に使用できる画像が表示されます。「…」ボタンをクリックして、画像を参照します。新しい画像を追加するためには、「参照」ボタンをクリックして、ローカルシステムにあるイメージを選択し、「Download」ボタンをクリックして画像をスイッチにダウンロードします。リストから画像を削除する場合は、プルダウンメニューからそのファイル名を選択して「Delete」ボタンをクリックします。削除できるのはダウンロードした画像のみです。
Background Image	プルダウンメニューを使用して、画面背景として表示する画像名を選択します。「…」ボタンをクリックして、利用可能な画像を表示することもできます。選択する画像をクリックします。背景画像を使用しないように設定するためには、プルダウンメニューから <No Selection> を選択します。
Branding Image	プルダウンメニューから画像ファイル名を選択すると、画面左上に表示されます。この画像は会社のロゴなどのようなブランド表示の目的に使用します。「…」ボタンをクリックして、利用可能な画像を表示することもできます。選択する画像をクリックします。ブランド表示を使用しないように設定するためには、プルダウンメニューから <No Selection> を選択します。
Fonts	CP Web ページに使用するフォント名を入力します。
Script Text	ユーザがログアウト Web 画面を表示するために、JavaScript が有効でなければならないことを示すテキストを入力します。「User Logout Mode」が有効である時にだけ、本欄は適用できます。
Popup Text	ユーザがログアウト Web 画面を表示するためには、ポップアップ画面を許可する必要があることを示す情報を入力します。User Logout Mode モードが有効である時にだけ、本欄は適用できます。

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

設定のクリア

「Clear」ボタンをクリックして、すべてのコンフィグレーションを初期設定にリセットします。

Authentication Page（認証ページ）

1. 画面の上部のプルダウンメニューから「Authentication Page」を選択して、以下の画面を表示します。

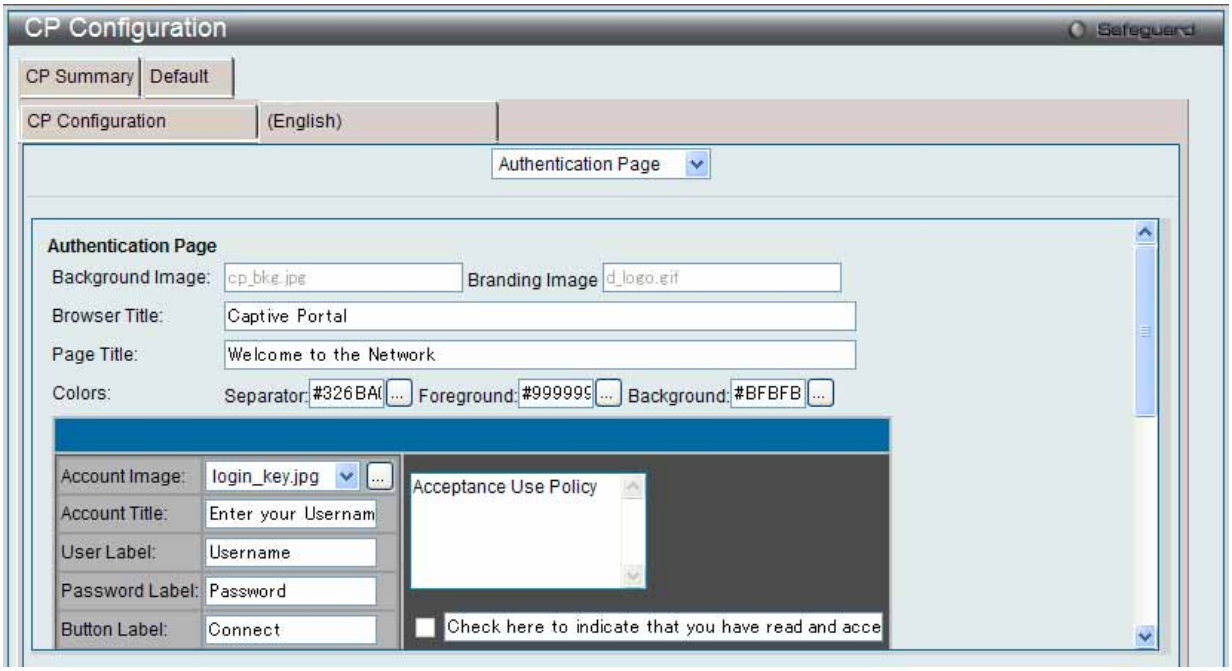


図 8.1-33　CP Configuration - Customize（Authentication Page）画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Background Image	「Authentication」画面に現在の背景画像の名称を表示します。
Branding Image	「Authentication」画面の現在の画面タイトル画像の名称を表示します。
Browser Title	クライアントの Web ブラウザのタイトルバーやタブに表示するテキストを入力します。
Page Title	ページタイトルとして使用するテキストを入力します。
Colors	CP ページの各エリアのカラーを指定します。フィールドにカラーコードを入力するか、または「…」ボタンをクリックして、カラーを選択します。
Account Image	プルダウンメニューを使用して、ログインフィールド上の CP Web ページに表示する画像を選択します。「…」ボタンをクリックして、利用可能な画像を表示することもできます。選択する画像をクリックします。
Account Title	ユーザに認証を行うよう指示するテキストを入力します。
User Label	ユーザ名テキストボックス横に表示するテキストを入力します。
Password Label	パスワードテキストボックスの横に表示するテキストを入力します。
Button Label	ネットワークに接続する時にクリックするボタンに表示するテキストを入力します。
Acceptance Use Policy Text Box	「Acceptance Use Policy」欄に表示するテキストを入力します。「Acceptance Use Policy」は、ユーザがネットワークへの接続を許可される時にその状況を示します。
Acceptance Use Policy Check Box	ユーザが使用条件を承諾すべきこと示すために、ボタンの横に表示するテキストを入力します。
Instructional Text	ユーザに認証を行うよう指示する詳細情報を入力します。このテキストはボタンの下に表示されます。
Denied message	ユーザが有効な認証情報を提供しない場合に表示するメッセージを入力します。
Resource Message	システムリソースの制限のために、システムが認証を拒否した場合に表示するメッセージを入力します。
Timeout Message	認証トランザクションに時間がかかりすぎたことによりシステムが認証を拒否した場合に表示されるメッセージを入力します。
Busy Message	CP 機能が認証リクエストを処理している時に表示されるメッセージを入力します。
No Accept Message	ユーザが「Acceptance Use Policy」をチェックしなかった場合に表示するメッセージを入力します。

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。

設定のクリア

「Clear」ボタンをクリックして、すべてのコンフィグレーションを初期設定にリセットします。

結果の参照

「Preview」ボタンをクリックして、Web ページの結果を参照します。

Welcome Page（ウエルカムページ）

1. 画面の上部のプルダウンメニューから「Welcome Page」を選択して、以下の画面を表示します。:

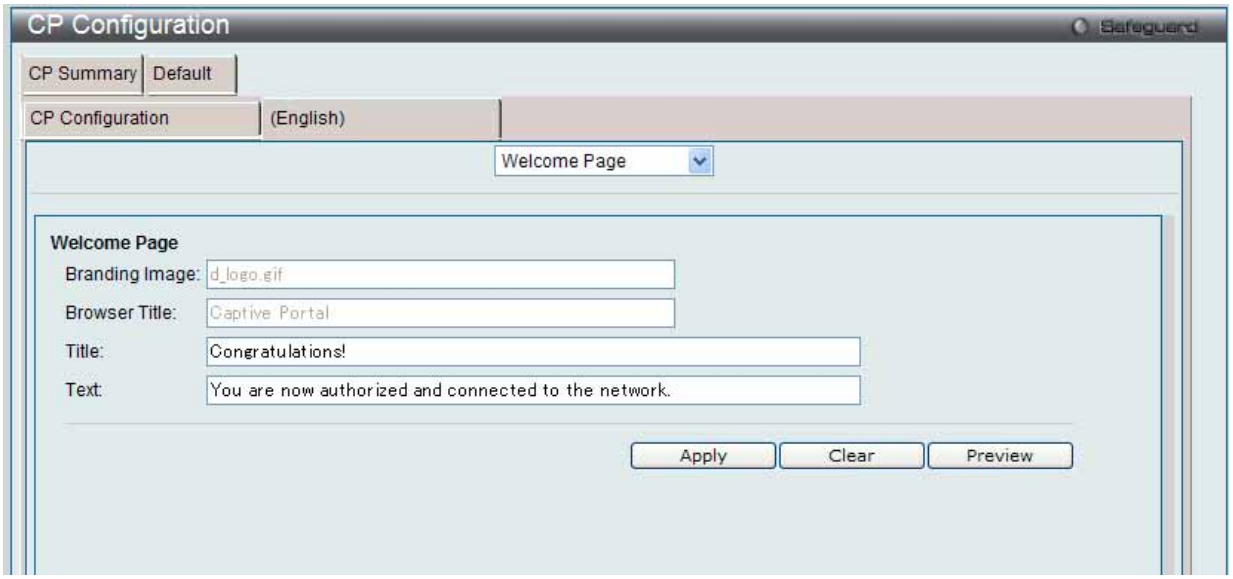


図 8.1-34　CP Configuration - Customize（Welcome Page）画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Branding Image	「Welcome Page」画面における現在の画面タイトル画像の名称を表示します。
Browser Title	クライアントの Web ブラウザのタイトルバーまたはタブに表示するテキストを入力します。
Title	ネットワークへの接続に成功した後に表示するユーザへの挨拶のタイトルを入力します。
Text	CP ユーザがアクセスするネットワークをさらに確認するオプションテキストを入力します。

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

設定のクリア

「Clear」ボタンをクリックして、すべてのコンフィグレーションを初期設定にリセットします。

結果の参照

「Preview」ボタンをクリックして、Web ページの結果を参照します。

Logout Page（ログアウトページ）

1. 画面の上部のプルダウンメニューから「Logout Page」を選択して、以下の画面を表示します。

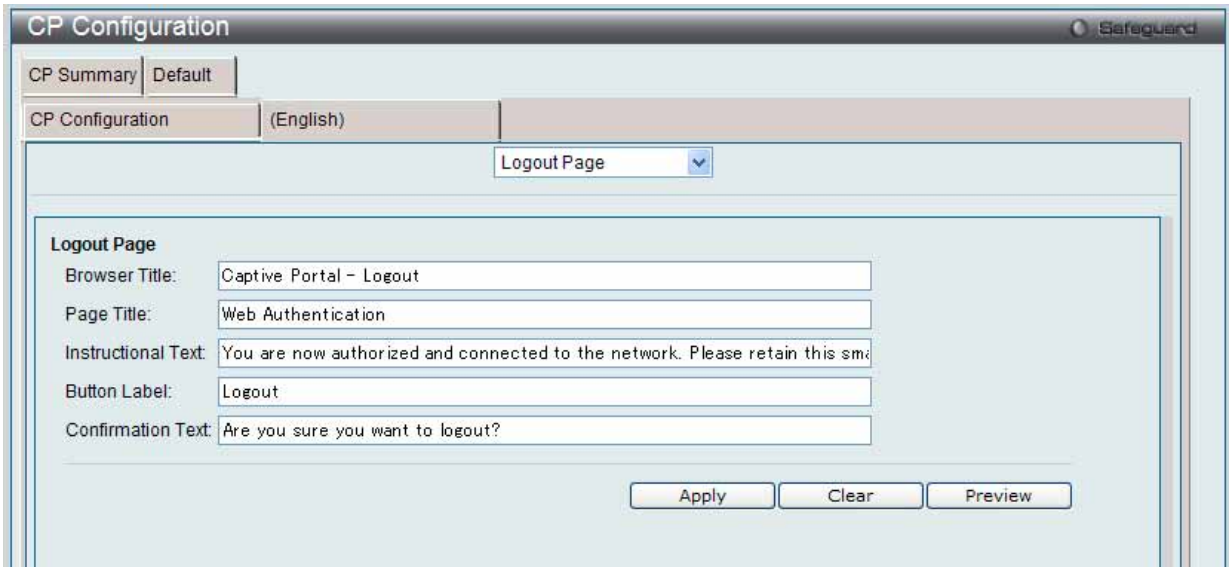


図 8.1-35　CP Configuration - Customize（Logout Page）画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Browser Title	「Logout」画面のタイトルバーに表示するためにテキストを入力します。
Page Title	画面タイトルとして使用するテキストを入力します。
Instruction Text	ユーザが認証されていることを確認し、ユーザに認証解除する方法を指示する詳細情報を入力します。
Button Label	認証を解除するボタンに表示するテキストを入力します。
Confirmation Text	認証の解除処理を確認するメッセージを入力します。

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。

設定のクリア

「Clear」ボタンをクリックして、すべてのコンフィグレーションを初期設定にリセットします。

結果の参照

「Preview」ボタンをクリックして、Web ページの結果を参照します。

Logout Success Page（ログアウト成功ページ）

画面の上部のプルダウンメニューから「Logout Success Page」を選択して、以下の画面を表示します。

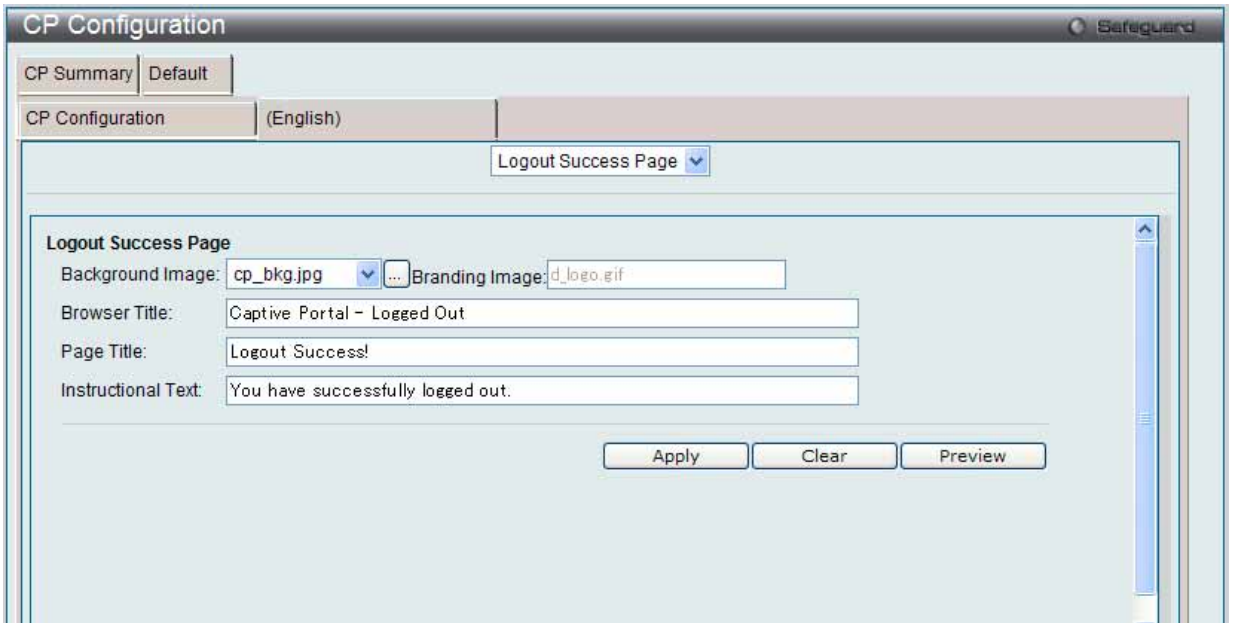


図 8.1-36　CP Configuration - Customize（Logout Success Page）画面

以下の項目を使用して設定および参照します。

項目	説明
Background Image	「Logout Success」画面における現在の背景画像の名称を表示します。
Branding Image	「Logout Success」画面における現在の画面タイトルの名称を表示します。
Browser Title	「Logout Success」画面のタイトルバーに表示するテキストを入力します。
Page Title	画面タイトルとして使用するテキストを入力します。
Instructional Text	ユーザの認証解除を確認する詳細なメッセージを入力します。

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。

設定のクリア

「Clear」ボタンをクリックして、すべてのコンフィグレーションを初期設定にリセットします。

結果の参照

「Preview」ボタンをクリックして、Web ページの結果を参照します。

Local User（ローカルユーザ）

ローカルデータベースに対する認可ユーザの作成、編集、または削除を行います。

Security > Captive Portal (CP) > Local User の順にメニューをクリックし、以下の画面を表示します。

図 8.1-37　Local User - Summary 画面

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

エントリの削除

対応するボックスをチェック後、「Delete」ボタンをクリックして指定エントリを削除します。「Delete All」ボタンをクリックして、表示されたすべてのエントリを削除します。

ユーザの新規登録

新しいユーザを「Local User」データベースに追加します。

1. 「Add」ボタンをクリックして、以下の画面を表示します。

図 8.1-38　Local User - Configuration 画面（Add）画面

2. 以下の項目を使用して設定および参照します。

項目	説明
User Name	ユーザ名を入力します。
Password	ユーザのパスワードを入力します。
User Group	少なくとも 1 つのユーザグループにユーザを割り当てます。複数のグループにユーザを割り当てるためには、「Ctrl」キーを押して、各グループをクリックします。
Session Timeout (secs)	ユーザがネットワークに接続可能な時間（秒）を入力します。「Session Timeout」値に到達すると、ユーザは自動的にログアウトされます。
Idle Timeout (secs)	自動的にログアウトされるまでユーザが待機できる時間（秒）を入力します。
Max Up Rate (bytes/sec)	CP 使用時にトラフィックを送信する最大速度（バイト / 秒）入力します。
Max Down Rate (bytes/sec)	CP 使用時にトラフィックを受信する最大速度（バイト / 秒）を入力します。
Max Receive (bytes)	CP の使用時にユーザが受信できる最大バイト数を入力します。この制限に到達すると、ユーザは切断されます。
Max Transmit (bytes)	CP の使用時にユーザが送信できる最大バイト数を入力します。この制限に到達すると、ユーザは切断されます。
Max Total (bytes)	ユーザが送受信できる最大バイト数を入力します。この制限に到達すると、ユーザは切断されます。

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

エントリの編集

1. 情報を編集する「User」のハイパーリンクをクリックし、以下の画面を表示します。

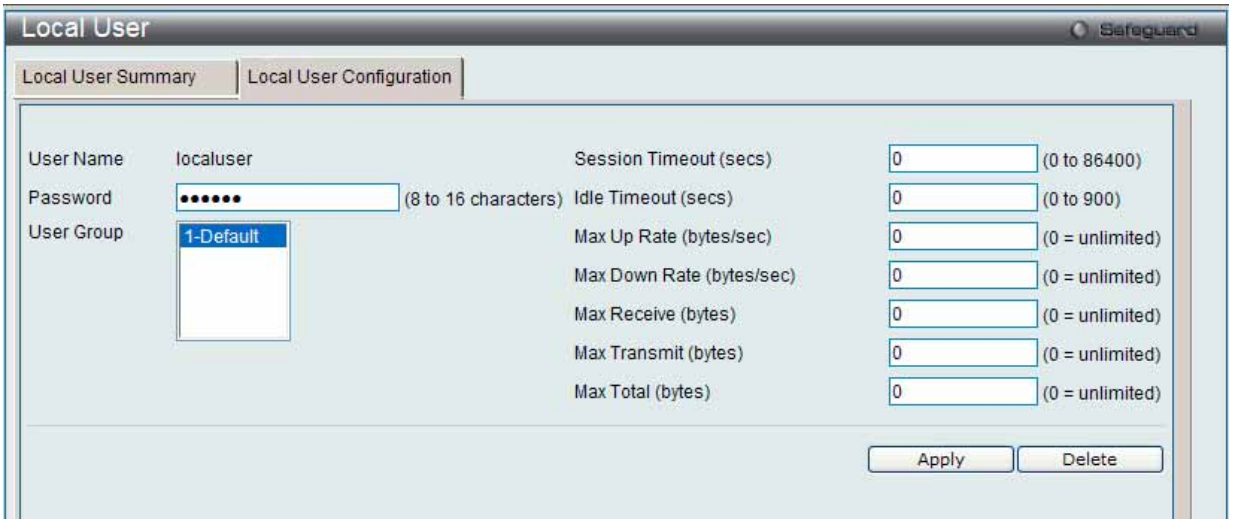


図 8.1-39　Local User - Configuration 画面（Edit）画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Password	ユーザーのパスワードを入力します。
User Group	少なくとも 1 つのユーザグループにユーザを割り当てます。複数のグループにユーザを割り当てるためには、「Ctrl」キーを押して、各グループをクリックします。
Session Timeout (secs)	ユーザがネットワークに接続可能な時間（秒）を入力します。「Session Timeout」値に到達すると、ユーザは自動的にログアウトされます。
Idle Timeout (secs)	自動的にログアウトされるまでユーザが待機できる時間（秒）を入力します。
Max Up Rate (bytes/sec)	CP 使用時にトラフィックを送信する最高速度（バイト / 秒）入力します。
Max Down Rate (bytes/sec)	CP 使用時にトラフィックを受信する最高速度（バイト / 秒）を入力します。
Max Receive (bytes)	CP の使用時にユーザが受信できる最大バイト数を入力します。この制限に到達すると、ユーザは切断されます。
Max Transmit (bytes)	CP の使用時にユーザが送信できる最大バイト数を入力します。この制限に到達すると、ユーザは切断されます。
Max Total (bytes)	ユーザが送受信できる最大バイト数を入力します。この制限に到達すると、ユーザは切断されます。

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。

エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。

Interface Association（インタフェースアソシエーション）

設定済み CP をインタフェースに関連付けます。インタフェースは、物理ポートまたは無線ネットワーク（SSID）とすることができます。

1. **Security > Captive Portal (CP) > Interface Association** の順にメニューをクリックし、以下の画面を表示します。

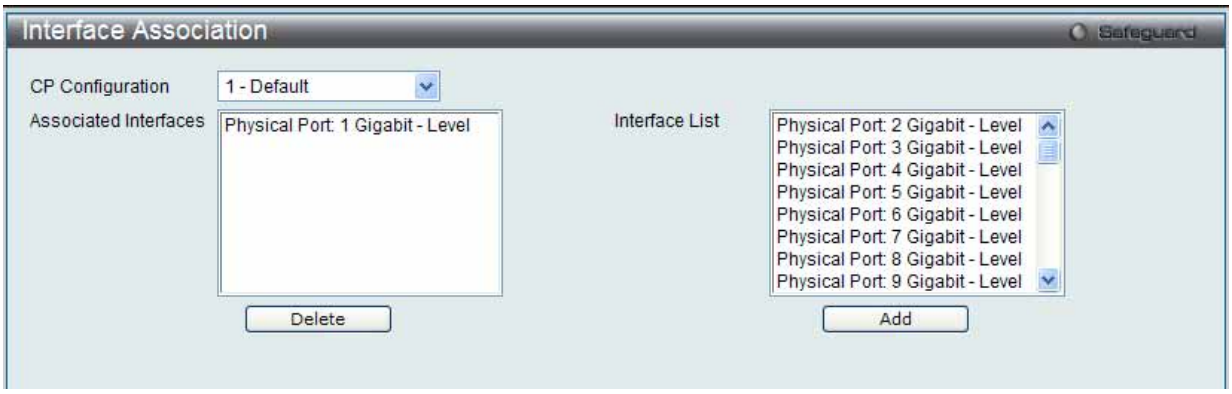


図 8.1-40　Interface Association 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
CP Configuration	プルダウンメニューを使用して、設定する CP を指定します。
Associated Interfaces	CP に関連するすべてのインタフェースを表示します。複数のインタフェースを選択するためには、「Ctrl」キーを押したまま、各インタフェースをクリックします。
Interface List	選択可能なすべてのインタフェースを表示します。複数のインタフェースを選択するためには、「Ctrl」キーを押したまま、各インタフェースをクリックします。

「Add」ボタンをクリックして、「Interface List」ボックス内で選択したインタフェースを「Associated Interfaces」に追加します。

エントリの削除

「Delete」ボタンをクリックして、「Associated Interfaces」ボックスから選択したインタフェースを削除します。

CP Status（CP 状態）

本画面では CP 状態を表示します。

Global Status（グローバル状態）

1. **Security > Captive Portal (CP) > CP Status > Global Status タブ**の順にメニューをクリックし、以下の画面を表示します。

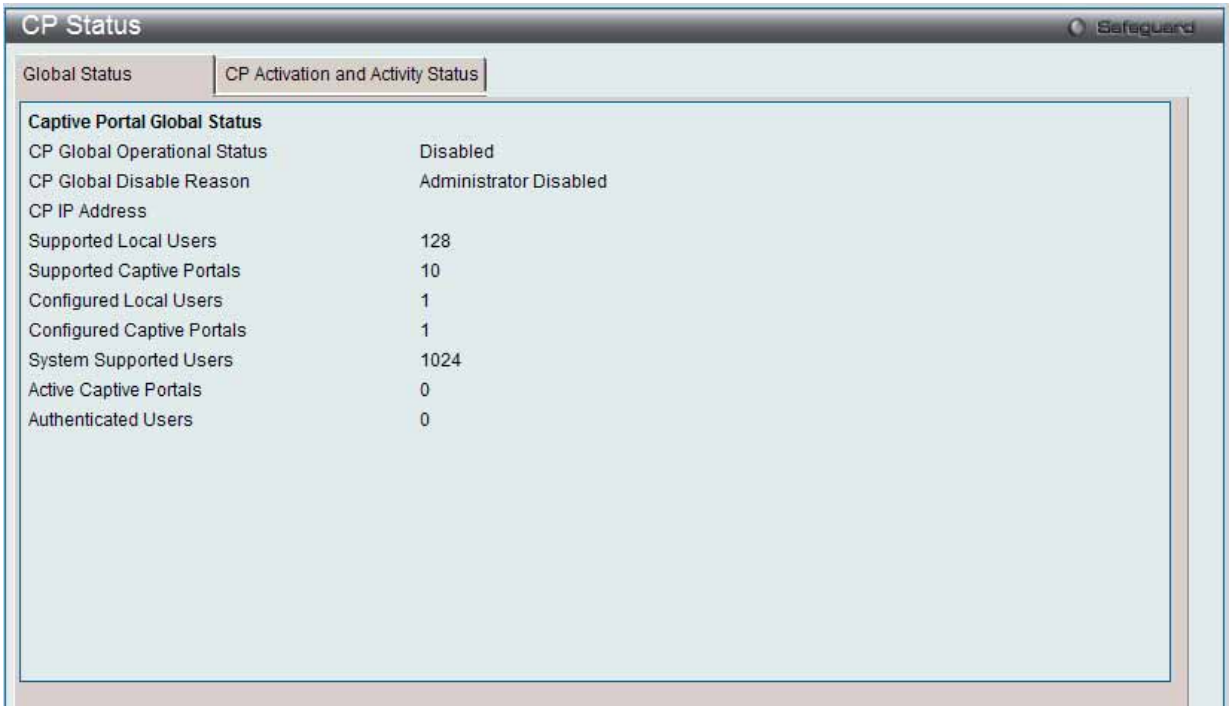


図 8.1-41　CP Global Status 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
CP Global Operational Status	CP の操作状態を表示します。
CP Global Disable Reason	CP が無効にされた場合に、本欄ではその理由を表示します。 表示可能な理由は以下の通りです。 • Administrator Disabled（管理者が無効にした） • IP Address Not Configured（IP アドレスが未設定） • No IP Routing Interface and Routing Disabled（IP ルーティングインタフェースがなく、ルーティングは無効）
CP IP Address	CP の IP アドレスを表示します。
Supported Local Users	ローカルユーザデータベースがサポートするエントリ数を表示します。
Supported Captive Portals	システムのサポートしている CP の数を表示します。
Configured Local Users	システムに設定されているユーザ数を表示します。
Configured Captive Portals	スイッチに設定された CP 数を表示します。
System Supported Users	システムがサポートしている認証ユーザの数を表示します。
Active Captive Portals	操作上有効である CP インスタンスの数を表示します。
Authenticated Users	本スイッチにおけるすべての CP インスタンスに対して現在認証されているユーザ数を表示します。

CP Activation and Activity Status（CP アクティベーションとアクティビティ状態）

アクティベーションとアクティビティの状態を参照します。

1. **Security > Captive Portal (CP) > CP Status > CP Activation and Activity Status タブ**の順にメニューをクリックし、以下の画面を表示します。

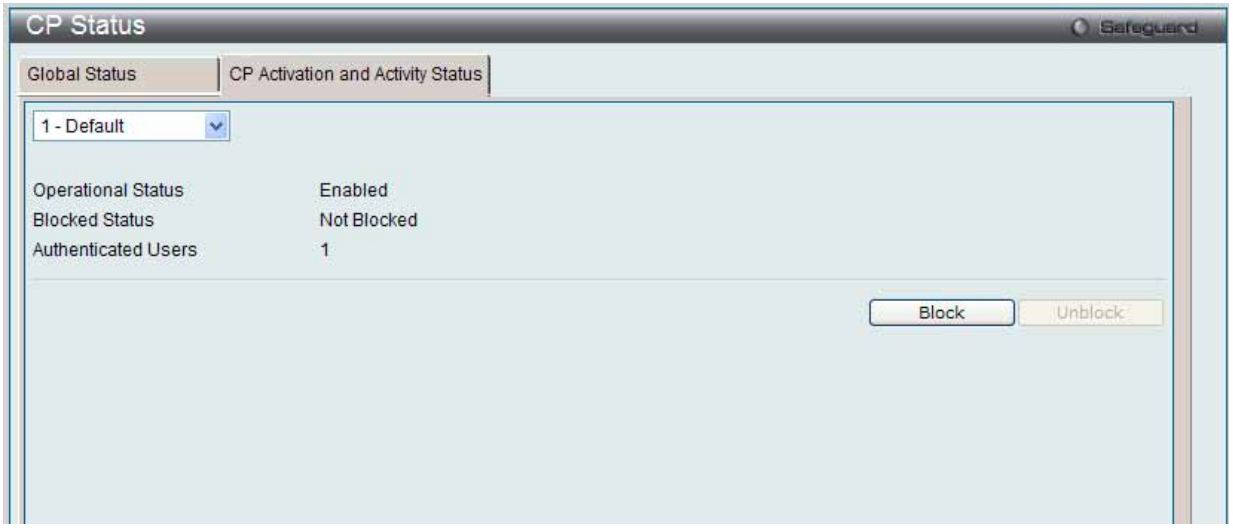


図 8.1-42　CP Activation and Activity Status 画面

2. プルダウンメニューを使用して、アクティベーションとアクティビティの状態を参照する CP を選択します。

アクセスのブロック
「Block」ボタンをクリックすると、ユーザが、選択したキャプティブポータルを経由してネットワークへのアクセス権を取得することを防ぎます。

アクセスの許可
選択したキャプティブポータルの「Blocked Status」が「Blocked」の場合、「Unblock」ボタンをクリックすると、キャプティブポータルを経由したネットワークへのアクセスを許可します。

Interface Status（インタフェース状態）

CP インタフェース状態を表示します。

Interface Activation Status（インタフェースアクティベーション状態）

1. **Security > Captive Portal (CP) > Interface Status > Interface Activation Status** タブの順にメニューをクリックし、以下の画面を表示します。

図 8.1-43　Interface Activation Status 画面

2. 最初のプルダウンメニューでポータルを、2 番目のプルダウンメニューで情報を参照するインタフェースを選択します。

Interface Capability Status（インタフェースケイパビリティ状態）

1. **Security > Captive Portal (CP) > Interface Status > Interface Capability Status** タブの順にメニューをクリックし、以下の画面を表示します。

図 8.1-44　Interface Capability Status 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Bytes Received Counter	インタフェースが各クライアントから受信したバイト数の表示をサポートするかどうかを表示します。
Bytes Transmitted Counter	インタフェースが各クライアントに送信したバイト数の表示をサポートするかどうかを表示します。
Packets Received Counter	インタフェースが各クライアントから受信したパケット数の表示をサポートするかどうかを表示します。
Packets Transmitted Counter	インタフェースが各クライアントに送信したパケット数の表示をサポートするかどうかを表示します。
Session Timeout	インタフェースがクライアントセッションのタイムアウトをサポートするかどうかを表示します。本属性はすべてのインタフェースでサポートされます。
Idle Timeout	ユーザが何もトラフィックを送受信しない場合のタイムアウトをインタフェースがサポートするかどうかを表示します。
Roaming Support	インタフェースがクライアントのローミングをサポートするかどうかを表示します。無線インタフェースだけがクライアントローミングをサポートします。

プルダウンメニューを使用して、詳細情報を表示するインタフェースを選択します。

Client Connection Status（クライアントの接続状態）

キャプティブポータル経由でスイッチに接続するクライアントに関する詳細情報を表示します。

Client Summary（クライアントに関するサマリ情報の参照）

1. **Security > Captive Portal (CP) > Client Connection Status > Client Summary タブ**の順にメニューをクリックし、以下の画面を表示します。

図 8.1-45　Client Summary 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
MAC Address	（該当する場合）クライアントの MAC アドレスを表示します。MAC アドレスが（*）でマークされている場合、クライアントはピアコントローラに認証されています。つまり、クラスタコントローラはオーセンティケータではありませんでした。
IP Address	（該当する場合）クライアントの IP アドレスを表示します。
User	接続するクライアントのユーザ名（またはゲスト ID）を表示します。
Protocol	現在の接続プロトコル（HTTP または HTTPS）を表示します。
Verification	現在のアカウントタイプ（Guest、Local または RADIUS）を表示します。

クライアントの切断

キャプティブポータルが認証クライアントを切断するためには、そのクライアントの MAC アドレス横にある対応するチェックボックスを選択して「Delete」ボタンをクリックします。すべてのキャプティブポータルからすべてのクライアントを切断するには、「Delete All」ボタンをクリックします。

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

「MAC Address」のリンクをクリックすると、「Client Detail」タブにリンクします。

Client Detail（クライアント詳細情報の参照）

キャプティブポータル経由でネットワークに接続する各クライアントの詳細情報を表示します。

1. **Security > Captive Portal (CP) > Client Connection Status > Client Detail タブ**の順にメニューをクリックし、以下の画面を表示します。

図 8.1-46　Client Detail 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Client IP Address	（該当する場合）クライアントの IP アドレスを表示します。
User Name	接続するクライアントのユーザ名 (またはゲスト ID) を表示します。
CP Configuration	クライアントが使用している CP 設定を表示します。
Interface	クライアントが使用しているインタフェースを表示します。
Protocol	現在の接続プロトコル（HTTP または HTTPS）を表示します。
Verification	現在のアカウントタイプ（Guest、Local または RADIUS）を表示します。
Session Time	クライアントが認証されてから経過した時間を表示します。
Switch MAC Address	このクライアントの認証を行うスイッチの MAC アドレスを表示します。クラスタリングがサポートされる場合、本欄はクラスタ内のピアスイッチの MAC アドレスを表示します。
Switch Type	このクライアントの認証を行うスイッチが、ローカルスイッチであるか、またはクラスタ内のピアスイッチであるかを示しています。
Switch IP Address	このクライアントの認証を行うスイッチの IP アドレスを表示します。クラスタリングがサポートされる場合、本欄はクラスタ内のピアスイッチの IP アドレスを表示します。

プルダウンメニューを使用して、詳細情報を参照する接続クライアントの MAC アドレスを選択します。:

Client Statistics（クライアント統計情報の参照）

クライアントが送信または受信したトラフィックに関する情報を参照します。

1. **Security > Captive Portal (CP) > Client Connection Status > Client Statistics タブ**の順にメニューをクリックし、以下の画面を表示します。

図 8.1-47　Client Statistics 画面

2. プルダウンメニューを使用して、詳細情報を参照する接続クライアントの MAC アドレスを選択します。

Interface - Client Status（クライアントインタフェース関連ステータスの参照）

指定インタフェースに認証されているクライアントを参照します。

1. **Security > Captive Portal (CP) > Client Connection Status > Interface - Client Status タブ**の順にメニューをクリックし、以下の画面を表示します。

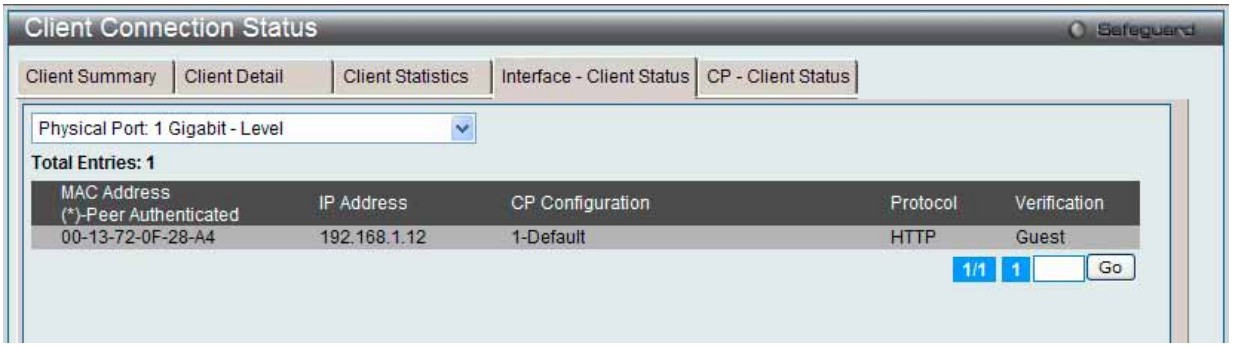


図 8.1-48　Interface - Client Status 画面

2. プルダウンメニューを使用して、本インタフェースの CP に接続するクライアントに関する情報を参照するインタフェースを選択します。

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

CP-Client Status（クライアント CP 関連ステータスの参照）

指定 CP 設定に認証されているクライアントを参照します。

1. **Security > Captive Portal (CP) > Client Connection Status > CP - Client Status タブ**の順にメニューをクリックし、以下の画面を表示します。

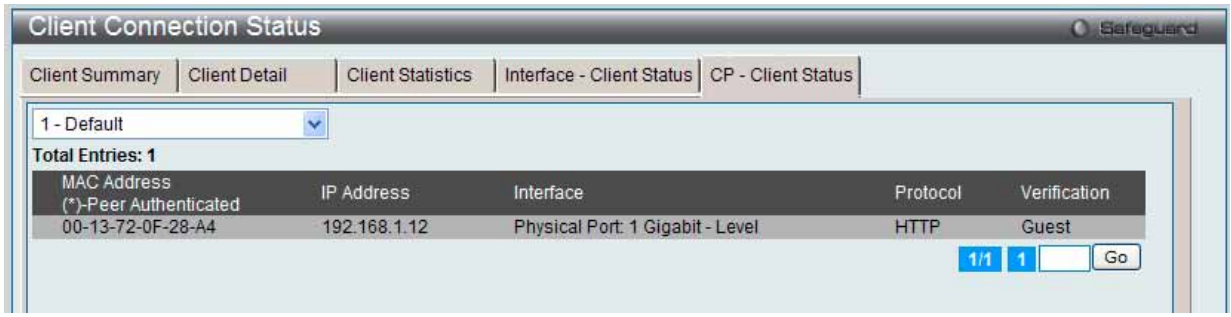


図 8.1-49　CP-Client Status 画面

2. プルダウンメニューを使用して、CP に接続するクライアントに関する情報を参照するインタフェースを選択します。

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

SNMP Trap Configuration（SNMP トラップ設定）

SNMP トラップをキャプティブポータルから送信するかどうかを設定し、トラップを生成するキャプティブポータルのイベントを指定します。

1. **Security > Captive Portal (CP) > SNMP Trap 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 8.1-50　SNMP Trap Configuration 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Client Authentication Failure Traps	プルダウンメニューを使用して、クライアントがキャプティブポータルに認証を試みて失敗した場合、SNMP エージェントがトラップを送信するかどうかを設定します。
Client Connection Traps	プルダウンメニューを使用して、クライアントがキャプティブポータルに認証され、接続した場合、SNMP エージェントがトラップを送信するかどうかを設定します。
Client Database Full Traps	プルダウンメニューを使用して、エントリがフル状態のためクライアントデータベースに追加されない場合に SNMP エージェントのトラップを送信するかどうかを設定します。
Client Disconnection Traps	プルダウンメニューを使用して、クライアントがキャプティブポータルとの接続を解除された場合、SNMP エージェントがトラップを送信するかどうかを設定します。

「Apply」ボタンをクリックして各セクションで行った変更を適用します。

8.2 Monitoring（無線のモニタリング）

本章は以下の項で構成され、D-Link 統合アクセスシステムネットワークの状態および統計情報のモニタに役立つ情報を提供します。

項目	説明	参照ページ
Global（無線グローバル情報）	スイッチや接続するデバイスの状況や統計情報をモニタします。	395
Peer Switch（ピアスイッチ）	ネットワーク上の他の D-Link 統合スイッチの情報を参照します。次のメニューがあります。 Status（ピアスイッチの状態）、Configuration（コンフィグレーション状態）、Managed AP（管理対象アクセスポイント）	403
Access Point（アクセスポイントのモニタ）	検出したすべてのアクセスポイントの状態（管理下、接続失敗、不正等）を確認します。 次のメニューがあります。 All AP Status（全アクセスポイントの状態）、Managed AP Status（管理対象アクセスポイントの状態）、AP Authentication Failure Status（アクセスポイント認証エラー状態）、AP RF Scan Status（アクセスポイントの RF スキャン状態）、AP De-Authentication Attack Status（アクセスポイント認証解除攻撃状態）	406
Client（クライアント）	スイッチ管理対象のアクセスポイントが接続中の無線クライアントについて、さまざまな情報を参照します。次のメニューがあります。: Associated Clients（接続中のクライアント）、Detected Clients（検出クライアント）、Ad Hoc Clients（アドホッククライアント）	427
QoS（QoS 設定）	アクセスコントロールリストおよび DiffServ に関する情報を表示します。次のメニューがあります。 Access Control Lists（アクセスコントロールリスト）、Differentiated Services（DiffServ: ディフサーブ）	445

CLI を使用して、WLAN の状態と統計情報を確認するコマンドの詳細については、「D-Link CLI MANUAL」を参照してください。

Global（無線グローバル情報）

統合スイッチは、接続中のアクセスポイントや関連するピアスイッチの情報を定期的に収集しています。ここでは、スイッチやスイッチに接続するオブジェクトの状況や統計情報を参照できます。

Global（全般）

グローバル情報を表示します。

1. **Monitoring > Global > Global タブ**の順にメニューをクリックし、以下の画面を表示します。

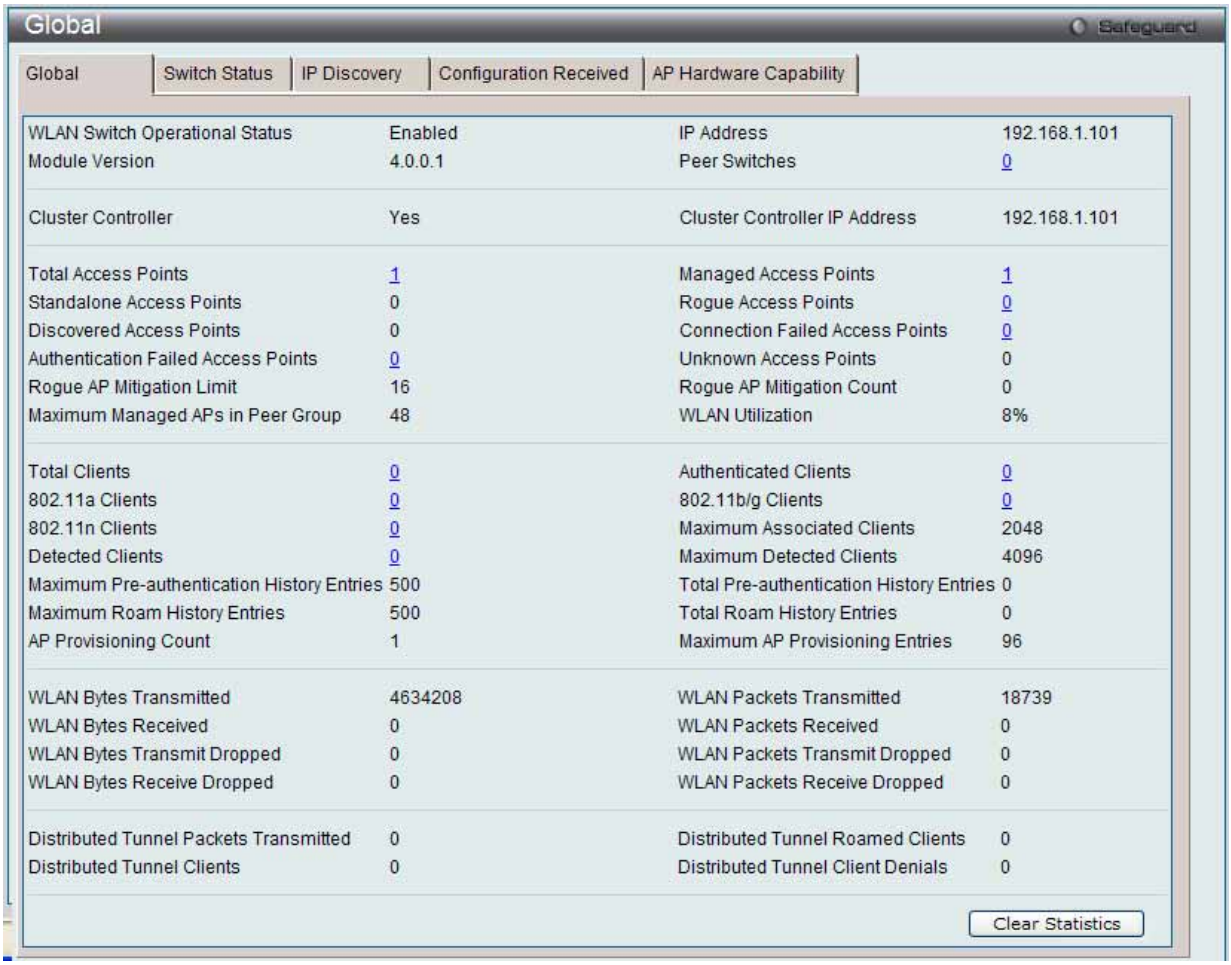


図 8.2-1　Global 画面

2. 以下の項目が表示されます。

項目	説明
WLAN Switch Operational Status	WLAN スイッチの動作状態が表示されます。WLAN スイッチが設定上有効になっていても、コンフィグレーション上の従属関係により、非稼働状態にある場合があります。稼働状態が無効である場合、その原因が続く「status」欄に表示されます。 WLAN スイッチは複数のコンポーネントで構成されています。システムの各コンポーネントが、それぞれ WLAN スイッチの動作状態（動作中 / 停止中）を認識する必要があります。動作状態の移行期間中には、動作状態は保留中と表示される場合があります。
IP Address	スイッチの IP アドレス。
Module Version	WLAN バージョンを表示します。
Peer Switches	ネットワーク上で検出されたピア WLAN スイッチの数。
Cluster Controller	このスイッチがクラスタにおけるクラスタコントローラはどうかを表示します。ピアスイッチのグループでは、スイッチの 1 つが、自動的に選定されるかクラスタコントローラになるように設定されます。クラスタコントローラは、ピアグループ内のすべてのアクセスポイントとクライアントに関するステータスと統計情報を収集します。 **注意** クラスタコントローラスイッチだけが、全クラスタにおける管理下のアクセスポイント、クライアント、統計情報および RF スキャンデータベースを表示することができます。クラスタコントローラではないスイッチは、ローカルに接続するデバイスに関する情報だけを表示できます。
Cluster Controller IP Address	クラスタコントローラであるピアスイッチの IP アドレス。
Total Access Points	データベース中の管理対象のアクセスポイントの総数。この値は常に「Managed Access Points」と「Connection Failed Access Points」と「Discovered Access Points」の値の和と等しくなります。
Managed Access Points	管理下の AP データベース中のアクセスポイントの数。これは、認証、設定がされており、統合スイッチとの間でアクティブな接続が確立されているアクセスポイントです。
Standalone Access Points	Standalone モードのトラストアクセスポイント数。Standalone モードのアクセスポイントは、スイッチで管理されません。
Rogue Access Points	現在 WLAN 上で検出されているローグ（不正）アクセスポイントの数。アクセスポイントが RF スキャンする時、認知されていないアクセスポイントを検出する場合があります。このようなアクセスポイントをローグ（不正）として報告します。
Discovered Access Points	スイッチと接続していますが、完全に設定されていないアクセスポイント。この値には管理下で「Discovered」（検出）または「Authenticated」（認証）状態のすべてのアクセスポイントが含まれます。
Connection Failed Access Points	以前に認証され、スイッチの管理下にあったが、現在は無線スイッチとの間に接続が確立されていないアクセスポイントの数。
Authentication Failed Access Points	統合スイッチとのリンクの確立に失敗したアクセスポイント数。
Unknown Access Points	現在 WLAN 上で検出されてい Unknown（未知）のアクセスポイントの数。統合スイッチが管理するように設定済みのアクセスポイントが、アクティブに管理されていない時に RF スキャンを通じて検出されると、Unknown（未知）のアクセスポイントとして分類されます。
Rogue AP Mitigation Limit	システムが認証解除フレームを送信できるアクセスポイントの最大数。
Rogue AP Mitigation Count	無線システムが現在不正なアクセスポイントの数を減少させるために現在認証解除メッセージを送信しているアクセスポイント数。範囲は以下の通りです。0 の値は、軽減が行われていないことを示します。
Maximum Managed APs in Peer Group	クラスタが管理するアクセスポイントの最大数。
WLAN Utilization	本スイッチの管理下にあるすべてのアクセスポイントのネットワーク使用率。本値はグローバル統計値を基にしています。
Total Clients	データベース中のクライアントの総数。この値は「Associated」、「Authenticated」、「Disassociated」の状態のクライアントを含みます。
Authenticated Clients	クライアントデータベース中のクライアントで、「Authenticated」状態のクライアントの数。
802.11a Clients	認証された IEEE 802.11a クライアントの数。
802.11b/g Clients	認証された IEEE 802.11b/g クライアントの数。
802.11n Clients	認証された IEEE 802.11n クライアントの数。これらには、IEEE 802.11a/n、IEEE 802.11b/g/n、5GHz IEEE 802.11n、2.4GHz IEEE 802.11n が含まれます。
Maximum Associated Clients	無線システムに接続できるクライアントの最大数。これは Associated Client データベースで許可されているエントリの最大数。
Detected Clients	WLAN に検出された無線クライアントの数。
Maximum Detected Clients	スイッチが検出したクライアントの最大数。この数値は Detected Client データベースのサイズによって制限されます。

項目	説明
Maximum Pre-authentication History Entries	システムが記録できる Client Pre-Authentication イベントの最大数。
Total Pre-authentication History Entries	システムで使用中の Pre-Authentication ヒストリエントリの現在の数。
Maximum Roam History Entries	すべての検出クライアントに対してローミングヒストリに定義できるエントリの最大数。
Total Roam History Entries	システムで使用中のローミングヒストリエントリの現在の数。
AP Provisioning Count	システムに設定したアクセスポイントのプロビジョニングエントリの現在の数。
Maximum AP Provisioning Entries	システムが保存できるアクセスポイントのプロビジョニングエントリ数。
WLAN Bytes Transmitted	本スイッチの管理下にあるすべてのアクセスポイントが送信した総データ量（バイト）。
WLAN Packets Transmitted	本スイッチの管理下にあるすべてのアクセスポイントが送信したパケット数。
WLAN Bytes Received	本スイッチの管理下にあるすべてのアクセスポイントが受信した総データ量（バイト）。
WLAN Packets Received	本スイッチの管理下にあるすべてのアクセスポイントが受信したパケット数。
WLAN Bytes Transmit Dropped	本スイッチの管理下にあるすべてのアクセスポイントが送信し、破棄された総データ量（バイト）。
WLAN Packets Transmit Dropped	本スイッチの管理下にあるすべてのアクセスポイントが送信し、破棄された総パケット数。
WLAN Bytes Received Dropped	本スイッチの管理下にあるすべてのアクセスポイントが受信し、破棄された総データ量（バイト）。
WLAN Packets Receive Dropped	本スイッチの管理下にあるすべてのアクセスポイントが受信し、破棄された総パケット数。
Distributed Tunnel Packets Transmitted	すべての AP ピアが分配型トンネル経由で送信したパケットの総数。
Distributed Tunnel Roamed Clients	分配型トンネリングを使用してホーム AP からの移動に成功したクライアントの数。
Distributed Tunnel Clients	分配型トンネリングを使用しているアクセスポイントに接続するクライアントの総数。
Distributed Tunnel Client Denials	クライアントがローミングする際に、システムが分配型トンネルを設定できなかったクライアントの総数。

「Refresh」ボタンをクリックすると、画面を最新の情報に更新します。

エントリの削除

「Clear Statistics」ボタンをクリックして、画面の全統計情報を削除します。

Switch Status（スイッチ状態）

スイッチの状態を表示します。

1. **Monitoring > Global > Switch Status タブ**の順にメニューをクリックし、以下の画面を表示します。

図 8.2-2　Switch Status 画面

2. プルダウンメニューを使用して、情報を参照するスイッチを指定します。

3. 以下の項目が表示されます。

項目	説明
Total Access Points	データベース中の管理対象のアクセスポイントの総数。この値は常に「Managed Access Points」、「Connection Failed Access Points」、「Discovered Access Points」の値の和と等しくなります。
Total Clients	データベース中のクライアントの総数。この値には「Associated」、「Authenticated」、「Disassociated」の状態のクライアントを含みます。
Managed Access Points	管理 AP データベース中のアクセスポイントの数。認証、設定がされており、無線スイッチとの間でアクティブな接続が確立されているアクセスポイントです。
Authenticated Clients	クライアントデータベース中のクライアントで、「Authenticated」状態のクライアントの総数。
Discovered Access Points	スイッチと接続していますが、完全に設定されていないアクセスポイント。この値には「Discovered」（検出）または「Authenticated」（認証）状態のすべての管理アクセスポイントが含まれます。
IP Address	スイッチの IP アドレス。
Connection Failed Access Points	以前に認証され、スイッチの管理下にあったが、現在は無線スイッチとの間に接続が確立されていないアクセスポイントの数。
Cluster Priority	スイッチのクラスタ優先度値。クラスタ内で最も高い優先度を持つスイッチがクラスタコントローラになります。優先度が同じである場合、最も低い IP アドレスを持つスイッチがクラスタコントローラになります。優先度 0 は、スイッチがクラスタコントローラになれないことを意味します。
Maximum Managed Access Points	スイッチが管理するアクセスポイントの最大数。
Distributed Tunnel Clients	分配型トンネリングを使用しているアクセスポイントに接続するクライアントの総数。
WLAN Utilization	本スイッチの管理下にあるすべてのアクセスポイントのネットワーク使用率。本値はグローバル統計値を基にしています。
WLAN Bytes Transmitted	本スイッチの管理下にあるすべてのアクセスポイントが送信した総データ量（バイト）。
WLAN Packets Transmitted	本スイッチの管理下にあるすべてのアクセスポイントが送信したパケット数。
WLAN Bytes Received	本スイッチの管理下にあるすべてのアクセスポイントが受信した総データ量（バイト）。
WLAN Packets Received	本スイッチの管理下にあるすべてのアクセスポイントが受信したパケット数。
WLAN Bytes Transmit Dropped	本スイッチの管理下にあるすべてのアクセスポイントが送信し、破棄された総データ量（バイト）。
WLAN Packets Transmit Dropped	本スイッチの管理下にあるすべてのアクセスポイントが送信し、破棄された総パケット数。
WLAN Bytes Received Dropped	本スイッチの管理下にあるすべてのアクセスポイントが受信し、破棄された総データ量（バイト）。
WLAN Packets Receive Dropped	本スイッチの管理下にあるすべてのアクセスポイントが受信し、破棄された総パケット数。

IP Discovery（IP 検出状態）

Administration > Basic Setup > Discovery タブの「IP List」にあるデバイスとの通信情報を確認できます。

1. **Monitoring > Global > IP Discovery タブ**をクリックして、以下の画面を表示します。

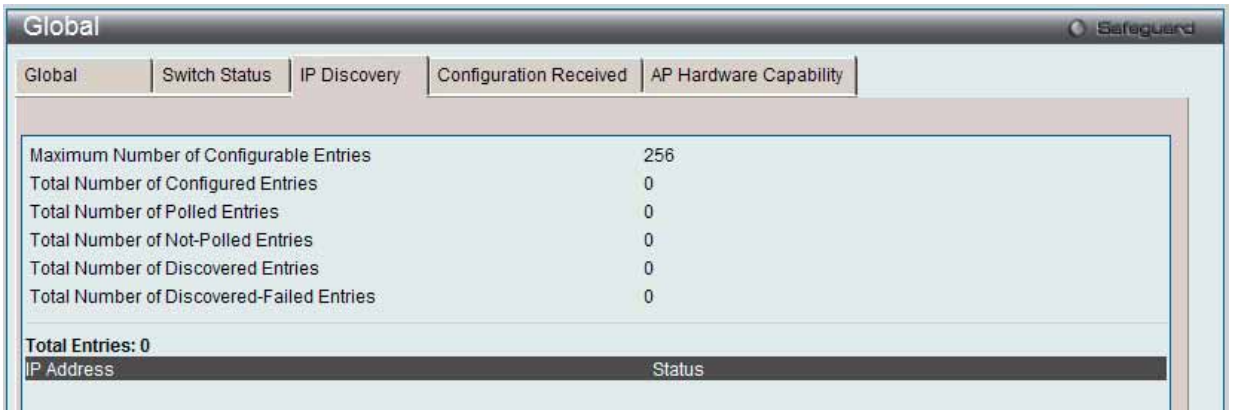


図 8.2-3　IP Discovery 画面

2. 以下の項目が表示されます。

項目	説明
Maximum Number of Configurable Entries	「IP Discovery」リストに設定できる IP アドレスの最大数を表示します。
Total Number of Configured Entries	「IP Discovery」リストに設定された IP アドレス数を表示します。
Total Number of Polled Entries	スイッチがコンタクトを試みた「IP Discovery」リスト内の IP アドレス数を表示します。
Total Number of Not-Polled Entries	スイッチがコンタクトを試みなかった「IP Discovery」リスト内の IP アドレス数を表示します。
Total Number of Discovered Entries	スイッチがディスカバリに成功し、認証されて、「IP Discovery」リストに設定された IP アドレスをポーリングすることで有効となったデバイス（ピアスイッチまたはアクセスポイント）数を表示します。
Total Number of Discovered-Failed Entries	「IP Discovery」リスト内に設定された IP アドレスで、スイッチがコンタクトを試みて、認証エラーとなったか有効になった IP アドレスを持つデバイス数を表示します。
Total Entries	以下のテーブルに表示されるエントリの合計数。
IP Address	「IP Discovery」リストに設定したデバイスの IP アドレスを表示します。
Status	以下の状態の 1 つが表示されます。 • Not Polled - スイッチは「L3/IP Discovery」リスト中の本 IP アドレスに接続を試みていません。 • Polled - スイッチは本 IP アドレスに接続を試みました。 • Discovered - スイッチは「L3/IP Discovery」リスト中のピアスイッチまたはアクセスポイントに接続し、認証または有効にしました。 • Discovered - Failed - スイッチは「L3/IP Discovery」リスト中の本 IP アドレスを持つデバイスに接続したが、認証または有効化に失敗しました。 デバイスがアクセスポイントであった場合は、そのエントリは失敗原因とともに「Authentication Failed Access Points」リストに表示されます。

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

Configuration Received（コンフィグレーションの保存状態）

1. **Monitoring > Global > Configuration Received タブ**をクリックして、以下の画面を表示します。

図 8.2-4　Configuration Received 画面

2. 以下の項目が表示されます。

項目	説明
Current Receive Status	ピアスイッチから無線設定を受信する場合のグローバルステータスを表示します。 • Not Started（開始していません。） • Receiving Configuration（設定を受信中です。） • Saving Configuration（コンフィグレーションを保存中です。） • Applying AP Profile Configuration（AP プロファイルの設定を適用中です。） • Success（成功） • Failure-Invalid Code Version（不正なコードバージョン） • Failure-Invalid Hardware Version（不正なハードウェアバージョン） • Failure-Invalid Configuration（不正なコンフィグレーション）
Peer Switch IP Address	無線コンフィグレーションデータを受信した最後のスイッチを表示します。
Configuration	コンフィグレーションのどの部分が最後にピアスイッチから受信したかを表示します。以下に示す 1 つ以上の項目が表示されます。 • Global - 基本および高度なグローバル設定を受信。 • Discovery - VLAN と IP リストを含む L2/L3 ディスカバリ情報を受信。 • Channel/Power - RF マネジメント設定の受信。 • AP Database - AP データベース設定の受信。 • AP Profiles - AP プロファイル設定の受信。 • Known Client - Known Client データベース設定の受信。 • Captive Portal - キャプティブポータル情報の受信。 • RADIUS Client - RADIUS 情報を受信。 • QoS ACL - QoS アクセスコントロールリストの設定受信。 • QoS DiffServ - Differentiated クラス、サービス、およびポリシーの受信。 スイッチが別のスイッチの設定を受信していない場合、値は「None」です。
Timestamp	このスイッチがピアスイッチからコンフィグレーションデータを受信した最後の時間を表示します。

AP Hardware Capability（アクセスポイントのハードウェアケイパビリティ状態）

Monitoring > Global > AP Hardware Capability タブをクリックすると、いくつかのサブタブが表示されます。

Summary（サマリ情報）

1. 「Summary」タブをクリックすると、以下の画面が表示されます。

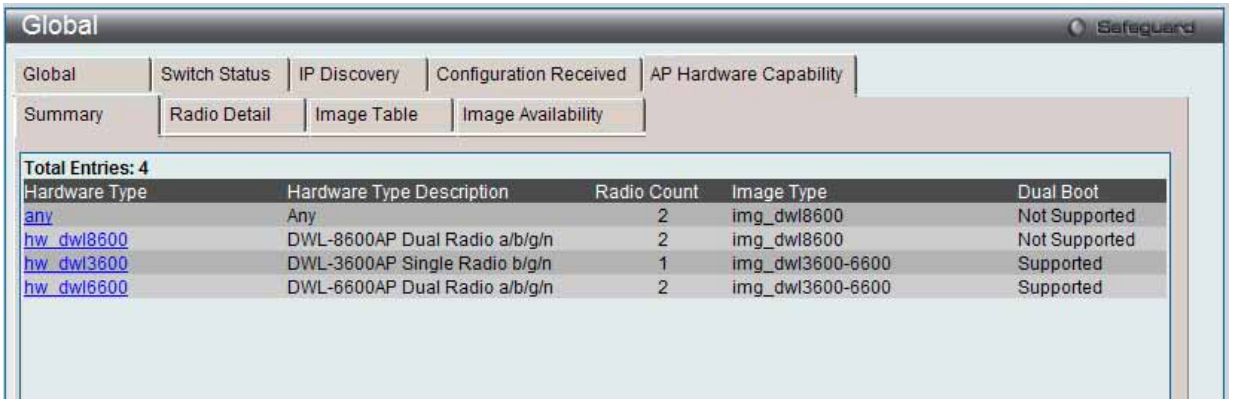


図 8.2-5　AP Hardware Capability - Summary 画面

2. 以下の項目が表示されます。

項目	説明
Total Entries	以下のテーブルに表示されるエントリの合計数。
Hardware Type	アクセスポイントのハードウェアタイプを表示します。
Hardware Type Description	プラットフォームに関する説明文とサポートしている IEEE 802.11 モードを表示します。
Radio Count	ハードウェアが 1 個または 2 個の周波数帯域をサポートするかどうか表示します。
Image Type	ハードウェアが要求するソフトウェアのタイプを表示します。
Dual Boot	このアクセスポイントのハードウェアタイプがデュアルブートをサポートしているかどうかを表示します。デュアルブートのアクセスポイントでは停電か予期しないアクセスポイントの再起動のためにソフトウェアアップグレード処理中に、アクセスポイントのソフトウェアが壊れると、アクセスポイントは古いイメージを使用して NVRAM に書き込みを行い、起動することができます。

Radio Detail（無線電波詳細）

1. 「Hardware Type」ハイパーリンクまたは「AP Hardware Capability」タブの「Radio Detail」サブタブをクリックすると、以下の画面が表示されます。

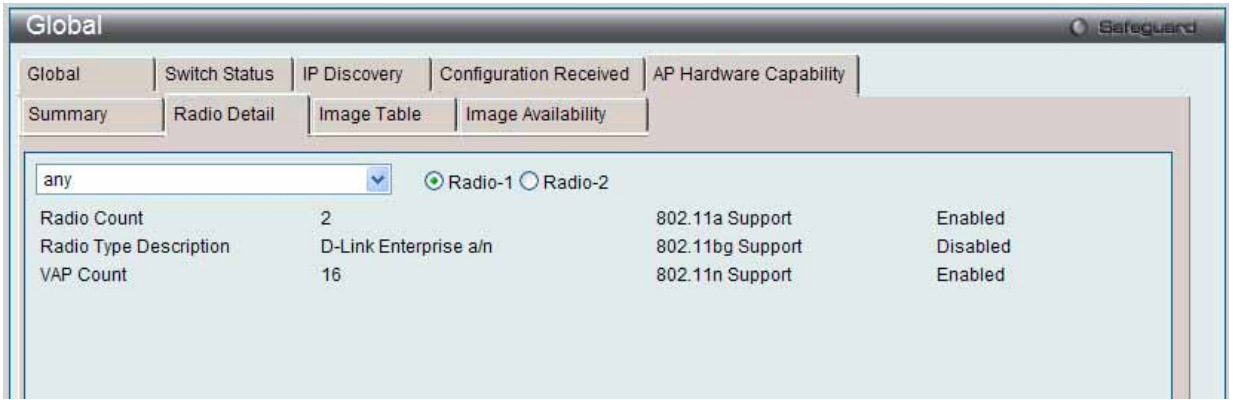


図 8.2-6　AP Hardware Capability - Radio Detail 画面

2. プルダウンメニューを使用してハードウェアタイプを選択し、ラジオボタンをクリックして、無線電波を選択します。

3. 以下の項目が表示されます。

項目	説明
Radio Count	ハードウェアプラットフォームでサポートされる無線帯域番号（1 または 2）を表示します。
Radio Type Description	メーカ名やサポートする IEEE 802.11 モードなどの情報を含む無線帯域のタイプを表示します。
VAP Count	無線インタフェースがサポートする VAP 番号を表示します。
802.11a Support	IEEE 802.11a モードのサポートが有効かどうかを表示します。
802.11bg Support	IEEE 802.11bg モードのサポートが有効かどうかを表示します。
802.11n Support	IEEE 802.11n モードのサポートが有効かどうかを表示します。

Image Table（画像テーブル）

「AP Hardware Capability」タブの「Image Table」サブタブをクリックすると、以下の画面が表示されます。

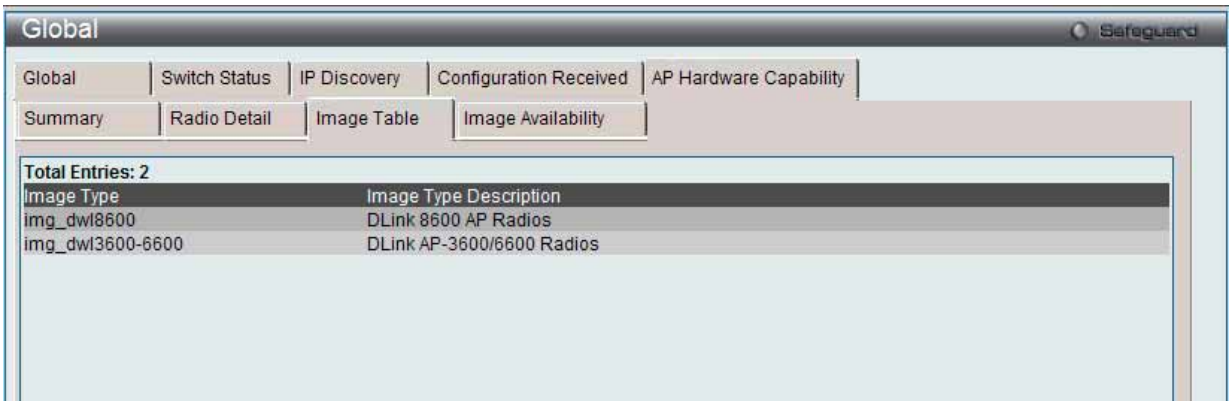


図 8.2-7　AP Hardware Capability - Image Table 画面

Image Availability

「AP Hardware Capability」タブの「Image Availability」サブタブをクリックすると、以下の画面が表示されます。

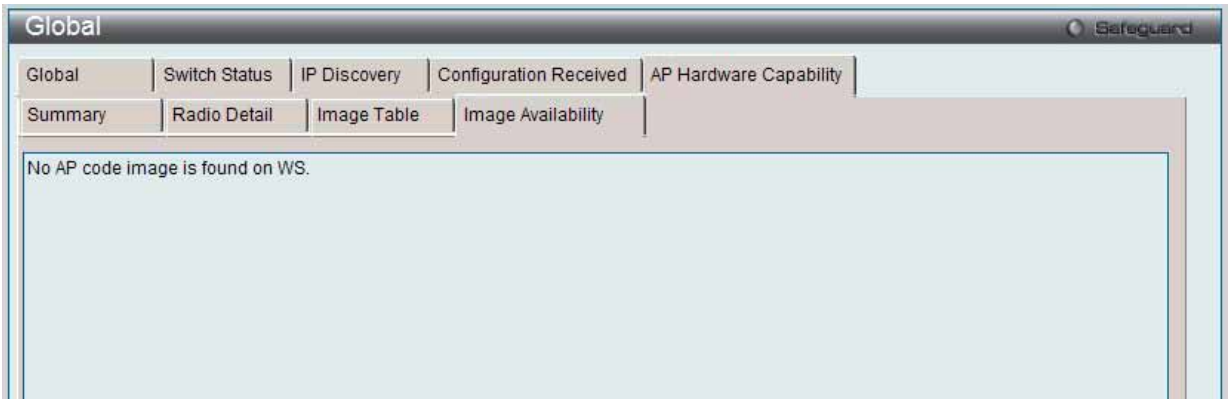


図 8.2-8　AP Hardware Capability - Image Availability 画面

Peer Switch（ピアスイッチ）

ネットワークにおける統合無線スイッチについて情報を提供します。同一クラスタ内のピア無線スイッチ同士は、スイッチ、スイッチ配下のアクセスポイントおよびクライアントの情報を交換します。スイッチはそのデータをデータベースに保持するため、IP アドレスやソフトウェアバージョンなどのピア情報を確認することができます。1 つのスイッチがクラスタコントローラとして選定されます。クラスタコントローラは、クラスタ内の他のスイッチすべてからステータスと統計情報を収集します。これには、ペアスイッチが管理するアクセスポイントおよびアクセスポイントに接続するクライアントに関する情報も含まれます。

Status（ピアスイッチの状態）

ピアスイッチの状態を表示します。

1. **Monitoring > Peer Switch > Status タブ**の順にメニューをクリックし、以下の画面を表示します。

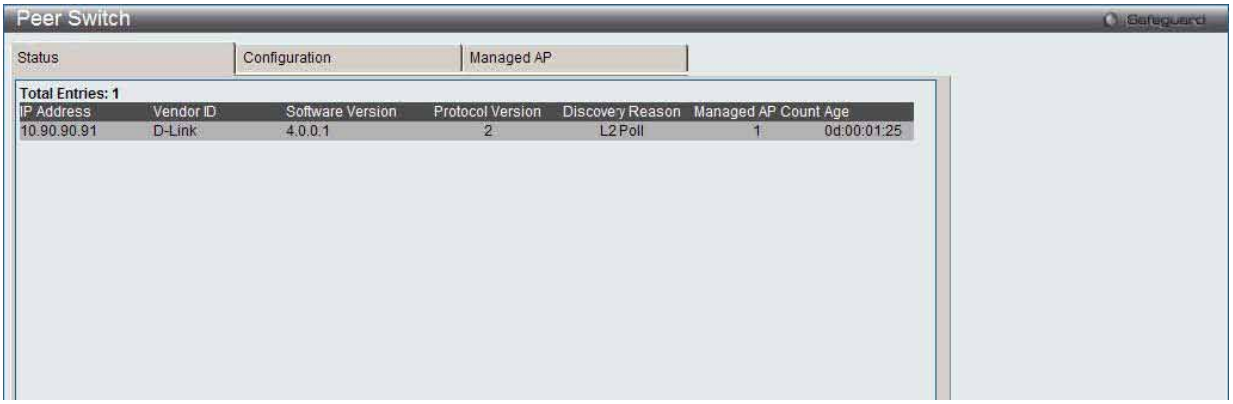


図 8.2-9　Peer Switch - Status 画面

2. 以下の項目が表示されます。

項目	説明
Total Entries	以下のテーブルに表示されるエントリの合計数。
IP Address	クラスタ内の無線スイッチの IP アドレス。
Vendor ID	ピアスイッチのソフトウェアのベンダ ID。
Software Version	ピアスイッチのソフトウェアバージョン。
Protocol Version	ピアスイッチのソフトウェアがサポートするプロトコルのバージョン。
Discovery Reason	ピアスイッチの検出方法。L2 ポーリングまたは IP ポーリング。
Managed AP Count	スイッチが現在管理するアクセスポイントの数。
Age	前回のスイッチとの通信から経過した時間（時間 : 分 : 秒）。

Configuration（コンフィグレーション状態）

ピアスイッチのコンフィグレーションの状態を表示します。

1. **Monitoring > Peer Switch > Configuration タブ**の順にメニューをクリックし、以下の画面を表示します。

図 8.2-10　Peer Switch - Configuration 画面

2. 以下の項目が表示されます。

項目	説明
Total Entries	以下のテーブルに表示されるエントリの合計数。
Failure Count	設定情報を受信したクラスタ内の各ピアスイッチの IP アドレス。
Configuration Switch IP Address	設定情報を送信したクラスタ内のスイッチの IP アドレス。
Configuration	スイッチがピアスイッチから受信した設定の一部を表示します。 以下に示す 1 つ以上の設定エレメントが表示されます。 • Global - 基本および高度なグローバル設定を受信。 • Discovery - VLAN と IP リストを含む L2/L3 ディスカバリ情報を受信。 • Channel/Power - RF マネジメント設定の受信。 • AP Database - AP データベース設定の受信。 • AP Profiles - AP プロファイル設定の受信。 • Known Client - Known Client データベース設定の受信。 • Captive Portal - キャプティブポータル情報の受信。 • RADIUS Client - RADIUS 情報を受信。 • QoS ACL - QoS アクセスコントロールリストの設定受信。 • QoS DiffServ - Differentiated クラス、サービス、およびポリシーの受信。 スイッチが別のスイッチの設定を受信していない場合、値は「None」です。
Timestamp	設定がスイッチに適用された日時を表示します。管理者が NTP を使用するために各ピアスイッチを設定した場合にだけ、時間は UTC で表示されます。

Managed AP（管理対象アクセスポイント）

ピアスイッチが管理するアクセスポイントに関する情報を表示します。

1. **Monitoring > Peer Switch > Managed AP タブ**の順にメニューをクリックし、以下の画面を表示します。

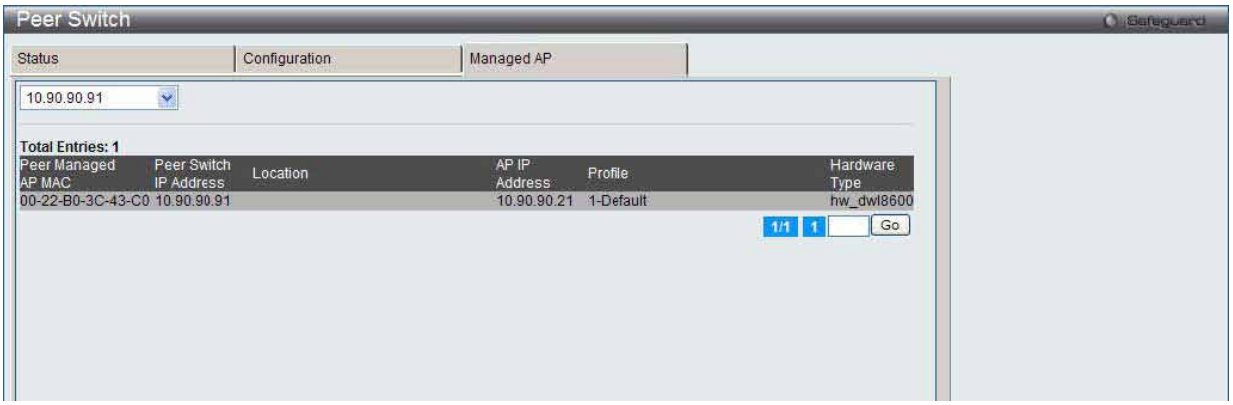


図 8.2-11　Peer Switch - Managed AP 画面

2. プルダウンメニューを使用して、ピアスイッチの IP アドレスを選択します。

3. 以下の項目が表示されます。

項目	説明
Total Entries	以下のテーブルに表示されるエントリの合計数。
Peer Managed AP MAC	ピアスイッチが管理する各アクセスポイントの MAC アドレス。
Peer Switch IP Address	アクセスポイントを管理するピアスイッチの IP アドレス。
Location	管理下のアクセスポイントの場所。
AP IP Address	アクセスポイントの IP アドレス。
Profile	スイッチがアクセスポイントに適用した AP プロファイル。
Hardware Type	アクセスポイントのハードウェアプラットフォームに割り当てられているハードウェア ID。

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

Access Point（アクセスポイントのモニタ）

All AP Status（全アクセスポイントの状態）

スイッチが発見または削除したアクセスポイントに関するサマリ情報を表示します。

1. **Monitoring > Access Point > All AP Status** の順にメニューをクリックし、以下の画面を表示します。

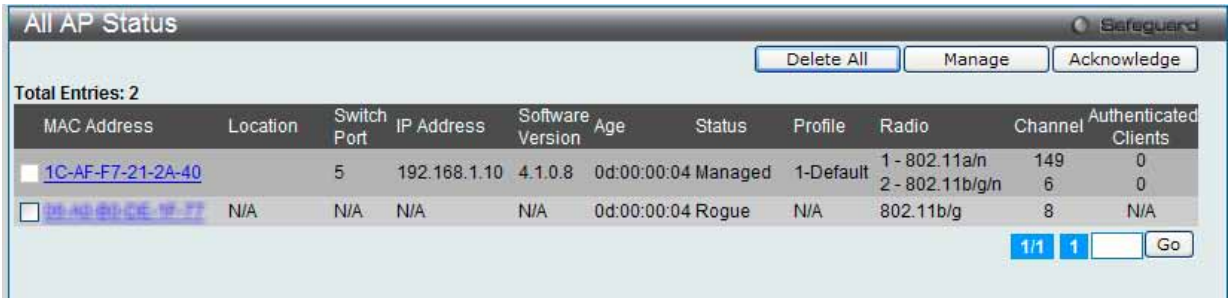


図 8.2-12　All AP Status 画面

2. 以下の項目が表示されます。

項目	説明
MAC Address	アクセスポイントの MAC アドレス。
Location	アクセスポイントの位置。Valid AP データベース（ローカルまたは RADIUS サーバ内）に登録されている値です。
Switch Port	同じ L3 ドメインにアクセスポイントが直接的または間接的に接続しているスイッチ上の物理ポート（スロット / ポートの形式）。アクセスポイントが L3 ネットワークの境界を越えている場合、「Unknown」が表示されます。
IP Address	アクセスポイントのネットワーク IP アドレス。
Software Version	アクセスポイントのソフトウェアバージョン。
Age	アクセスポイントの最後の検出および情報の更新から経過した時間。
Status	アクセスポイントの状態を示します。 • Managed - AP プロファイル設定が適用され、「Managed」モードで動作中です。 • No Database Entry - MAC アドレスがローカルまたは RADIUS サーバ内の Valid AP データベース中に存在しません。 • Authentication (Failed AP) - 統合スイッチまたは RADIUS サーバによる認証に失敗しました。 • Failed - 統合スイッチとの接続が失われました。エントリは管理者が削除するまでは管理 AP データベースに残ります。管理下のアクセスポイントは再起動中に一般的に「Failed」と表示されることがあります。 • Rogue - スイッチに接続を試みていません。またその MAC アドレスは Valid AP データベース内に存在しません。
Profile	管理下のアクセスポイントに現在適用している AP プロファイル。プロファイルは Valid AP データベース内のアクセスポイントに適用されています。 **注意** 一度アクセスポイントが検出されて統合スイッチの管理下に入ると、その後プロファイルが Valid AP データベース内（ローカルまたは RADIUS サーバ）で変更され、その新しいプロファイルが適用される場合、アクセスポイントは自動的に再起動します。
Radio	アクセスポイントが使用中の無線帯域モードを表示します。
Channel	無線インタフェースで運用中のチャンネル。
Authenticated Clients	アクセスポイントのインタフェースに接続し、認証されたクライアント数。

エントリの削除

「Delete All」ボタンをクリックして、Managed アクセスポイントを除いて、リストからすべてのエントリを削除します。

エントリの状態の変更

対応するボックスをチェックし、「Manage」ボタンをクリックして、「Authentication Failed AP」（認証に失敗したアクセスポイント）を次回検出時にスイッチが管理するように設定します。

対応するボックスをチェックして、「Acknowledge」ボタンをクリックして、アクセスポイントを「Acknowledged Rogue」として識別します。

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

Managed AP Status（管理対象アクセスポイントの状態）

スイッチの管理下にある各アクセスポイントの各種情報を表示します。画面には 2 つのメインタブ（Status および Statistics）があります。

- 「Status」タブ - 管理下のアクセスポイントと隣接するアクセスポイントの設定情報や接続情報を表示できます。
- 「Statistics」タブ - 各インタフェースにおいて送受信されたパケット数やデータ量に関する情報を表示できます。

Status タブ

Monitoring > Access Point > Managed AP Status > Status タブの順にメニューをクリックし、以下の画面を表示します。

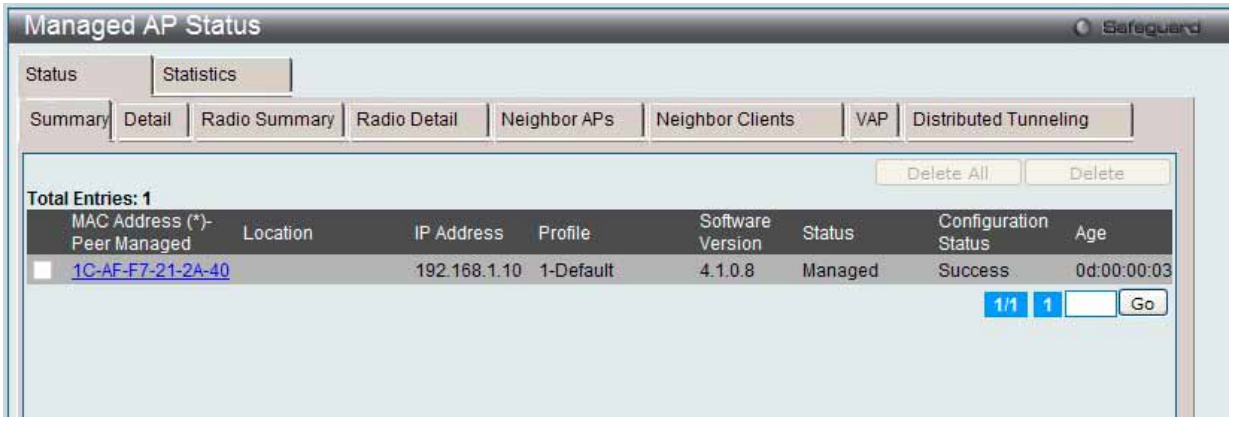


図 8.2-13　Managed AP Status > Status タブ > Summary サブタブ画面

「Managed AP Status」画面の「Status」タブには以下のサブタブがあります。

タブ	説明
Summary	スイッチの管理下にあるアクセスポイントとそのサマリ情報を表示します。
Detail	アクセスポイントから収集した詳細情報を表示します。
Radio Summary	管理下にあるアクセスポイントの使用チャンネル、送信電力、および接続中のクライアント数を表示します。
Radio Detail	「Radio Summary」画面で、アクセスポイントの MAC アドレスをクリックすると無線インタフェースの詳細情報を参照できます。ラジオボタンをクリックすることにより、2 つの無線インタフェースから選択できます。
Neighbor APs	指定したアクセスポイントが、選択した無線インタフェース上で周期的な RF スキャンを行って検出した隣接アクセスポイントを表示します。
Neighbor Clients	アクセスポイントに接続中、またはアクセスポイントのこの無線インタフェースが検出したクライアントの情報を表示します。
VAP	選択したアクセスポイント上の仮想アクセスポイント（VAP）や、管理対象のアクセスポイントの無線インタフェースに関するサマリ情報を表示します。
Distributed Tunneling	分配型トンネルモードを使用してこのアクセスポイントに接続するアクセスポイントおよびクライアントに関する情報を表示します。

Summary サブタブ

「Summary」サブタブ内の各項目について説明します。

項目	説明
MAC Address	統合スイッチの管理下にあるアクセスポイントの MAC アドレス。アクセスポイントの MAC アドレスの後に (*) が続いている場合、ピアスイッチによって管理されます。
Location	アクセスポイントの位置の説明。Valid AP データベース（ローカルまたは RADIUS サーバ内）に登録されている値です。
IP Address	管理下にあるアクセスポイントのネットワーク IP アドレス。
Profile	管理下のアクセスポイントに現在適用されている AP プロファイル。プロファイルは Valid AP データベース中においてアクセスポイントに適用されています。 **注意** 一度アクセスポイントが検出されて統合スイッチの管理下に入ると、その後プロファイルが Valid AP データベース内（ローカルまたは RADIUS サーバ）で変更され、その新しいプロファイルが適用される場合、アクセスポイントは自動的に再起動します。
Software Version	管理下にあるアクセスポイント上で運用中のソフトウェアのバージョン。

項目	説明
Status	アクセスポイントの現在の管理状態を示します。以下のいずれかの状態が表示されます。 • Discovered - スイッチにより検出されましたが、認証はされていません。 • Authenticated - スイッチにより認可、認証されました（認証を有効に設定している場合）が、AP プロファイル設定が適用されていません。 • Managed - AP プロファイル設定が適用され、「Managed」モードで動作中。 • Failed - 統合スイッチとの接続が失われました。エントリは管理者が削除するまでは管理 AP データベースに残ります。管理下のアクセスポイントは再起動中に「Failed」と表示されることがあります。 注意 管理の接続性が管理で喪失している場合、アクセスポイントの両方のインタフェースはダウンします。アクセスポイントに関連しているすべてのクライアントの接続が解除されます。そのアクセスポイントが再びスイッチによって再度管理されると、無線インタフェースは動作状態になります。
Configuration Status	アクセスポイントに対してプロファイルの設定が成功したかどうかを確認できます。以下の状態の 1 つが表示されます。 • Not Configured - アクセスポイントにプロファイルがまだ送信されていません。アクセスポイントが検出された可能性がありますが、まだ認証されていません。 • In Progress - スイッチからアクセスポイントに AP プロファイル・コンフィグレーションパケットを送信中です。 • Success - プロファイルがアクセスポイントに送信され、コンフィグレーションエラーは認められませんでした。 • Partial Success - AP プロファイルがアクセスポイントに送信されましたが、コンフィグレーションエラーが発生しました（例 : コンフィグレーションパラメータが受け入れられない等）。ただし、アクセスポイントは運用可能です。 • Failure - AP プロファイルがアクセスポイントに送信されましたが、コンフィグレーションエラーが発生しました。アクセスポイントは運用不可です。
Age	統合スイッチとアクセスポイント間の最後の通信から経過した時間。

詳細情報の参照
「MAC Address」のハイパーリンクをクリックして、アクセスポイントの詳細を参照します。

エントリの削除
対応するボックスをチェック後、「Delete」ボタンをクリックして指定エントリを削除します。
「Delete All」ボタンをクリックして、表示されたすべてのエントリを削除します。

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

Detail サブタブ

1. 「Status」タブの「Detail」サブタブをクリックすると、以下の画面が表示されます。

図 8.2-14　Managed AP Status > Status タブ > Detail サブタブ画面

2. プルダウンメニューを使用して、詳細情報を参照するアクセスポイントの MAC アドレスを選択します。

「Managed AP Status」の「Status」タブの「Detail」サブタブ内の各項目について説明します。

項目	説明
IP Address	管理下のアクセスポイントのネットワーク IP アドレス。
IP Subnet Mask	管理下のアクセスポイントのサブネットマスク
Status	アクセスポイントの現在の管理状態を示します。以下の状態の 1 つが表示されます。 • Discovered - スイッチにより検出されましたが、認証されていません。 • Authenticated - スイッチにより認可・認証されました（認証を有効に設定している場合）が、AP プロファイル設定が適用されていません。 • Managed - AP プロファイル設定が適用され、「Managed」モードで動作中。 • Failed - 統合スイッチとの接続が失われました。エントリは管理者が削除するまでは管理 AP データベースに残ります。管理下のアクセスポイントは再起動中に「Failed」と表示されることがあります。 **注意** 管理の接続性が管理で喪失している場合、アクセスポイントの両方のインタフェースはダウンします。アクセスポイントに関連しているすべてのクライアントの接続が解除されます。そのアクセスポイントが再びスイッチによって再度管理されると、無線インタフェースは動作状態になります。
Software Version	アクセスポイントのソフトウェアバージョン。アクセスポイントの検出の際に学習される情報です。
Code Download Status	アクセスポイントに対するソフトウェアのダウンロードリクエストの状態を示します。 • Not Started - ダウンロードは開始していません。 • Requested - このアクセスポイントにダウンロードが計画されていますが、アクセスポイントが現在のダウンロードグループにないため、まだダウンロードの開始が伝えられていません。 • Code-Transfer-In-Progress - アクセスポイントはソフトウェアのダウンロードを通知しました。 • Failure - アクセスポイントはソフトウェアのダウンロードの失敗を報告しました。 • Aborted - アクセスポイントが TFTP サーバからソフトウェアをロードする前にダウンロードは中止されました。 • Waiting-For-APs-To-Download - ダウンロードはこのアクセスポイント上で終了し、他のアクセスポイントがダウンロードを終了するのを待っています。Reset コマンドはこの状態ではアクセスポイントに送信されません。 • NVRAM-Update-In-Progress - ダウンロードに成功しました。Reset コマンドがアクセスポイントに送信されました。 • Timed-Out - アクセスポイントは所定の時間統合スイッチに再接続されませんでした。
Configuration Status	アクセスポイントに対してプロファイルの設定が成功したかどうかを確認できます。以下の状態の 1 つが表示されます。 • Not Configured - アクセスポイントにプロファイルがまだ送信されていません。アクセスポイントが検出された可能性がありますが、まだ認証されていません。 • In Progress - スイッチからアクセスポイントに AP プロファイル・コンフィグレーションパケットを送信中です。 • Success - プロファイルがアクセスポイントに送信され、コンフィグレーションエラーは認められませんでした。 • Partial Success - AP プロファイルがアクセスポイントに送信されましたが、コンフィグレーションエラーが発生しました（例 : コンフィグレーションパラメータが受け入れられない等）。ただし、アクセスポイントは運用可能です。 • Failure - AP プロファイルがアクセスポイントに送信されましたが、コンフィグレーションエラーが発生しました。アクセスポイントは運用不可です。
Vendor ID	アクセスポイントのソフトウェアのベンダ。アクセスポイントの検出の際に学習されます。
Part Number	アクセスポイントのハードウェアパート番号。アクセスポイントの検出の際に学習されます。
Hardware Type	アクセスポイントのハードウェアプラットフォーム。アクセスポイントの検出の際に学習されます。
Managing Switch	アクセスポイントがローカルスイッチまたはピアスイッチによって管理されるかどうか表示します。
Switch MAC Address	アクセスポイントを管理しているスイッチのの MAC アドレス。
Switch IP Address	アクセスポイントを管理しているスイッチの IP アドレス。
Profile	管理下のアクセスポイントに現在適用されている AP プロファイル。プロファイルは Valid AP データベース内のアクセスポイントに適用されています。 **注意** 一度アクセスポイントが検出され、統合スイッチの管理下に入ると、その後プロファイルが Valid AP データベース内（ローカルまたは RADIUS サーバ）で変更され、その新しいプロファイルが適用される時、アクセスポイントは自動的に再起動します。
Discovery Reason	アクセスポイントを検出した方法を表示します。以下の 1 つが表示されます。 • IP Poll Received - 統合スイッチからの IP ポーリングにより検出。その IP アドレスは IP ポーリングリスト内に設定されています。 • Peer Redirect - ピアスイッチからのリダイレクトにより検出。アクセスポイントは他のピアスイッチへの接続を試みたが、そのピアスイッチから現在接続中の統合スイッチの IP アドレスを取得した（アクセスポイントを認可する時、ピアは統合スイッチ IP アドレスを RADIUS サーバからの応答により取得）。 • Switch IP Configured - アクセスポイントに統合スイッチの IP アドレスが設定されていた。 • Switch IP DHCP - アクセスポイントは統合スイッチの IP アドレスを DHCP オプション 43 から取得した。 • L2 Poll Received - D-Link 無線デバイス検出プロトコルにより検出された。

項目	説明
Protocol Version	アクセスポイントのソフトウェアがサポートするプロトコルのバージョン。ディスカバリの際に学習されます。
Authenticated Clients	アクセスポイントに接続し、認証されたクライアントの数。この値は、アクセスポイント上で動作中のすべての VAP に認証されたクライアントの和です。
System Up Time	前回のアクセスポイントのパワーオンリセットからの経過時間（秒）。
Age	統合スイッチとアクセスポイント間の最後の通信から経過した時間。

「Reboot」ボタンをクリックすると、Managed スイッチが再起動します。
「Disassociate Clients」ボタンをクリックすると、アクセスポイントから接続するすべてのクライアントを切断します。

スイッチの管理下にあるアクセスポイントの詳細な情報を得るには、「Detail」画面の上部にあるプルダウンメニューから、目的のアクセスポイントの MAC アドレスを選択します。アクセスポイントを再起動するためには、「Reset」ボタンをクリックします。再起動を本当に行うかを確認するポップアップ画面が表示されます。再起動する場合は、「OK」ボタンをクリックします。

再起動を行うと、アクセスポイントに接続中のクライアントはすべて切断されます。アクセスポイントの状態データを更新するためには「Refresh」ボタンをクリックします。

Radio Summary サブタブ

「Status」タブの「Radio Summary」サブタブをクリックすると、以下の画面が表示されます。

図 8.2-15　Managed AP Status > Status タブ > Radio Summary サブタブ画面

「Managed AP Status」の「Status」タブの「Radio Summary」サブタブ内の各項目について説明します。

項目	説明
MAC Address	統合スイッチ管理下にあるアクセスポイントのイーサネットアドレス。アクセスポイントの MAC アドレスの後に (*) が続いている場合、それはピアスイッチによって管理されます。
Location	アクセスポイントの位置。Valid AP データベース（ローカルまたは RADIUS サーバ内）に設定されている値です。
Radio	無線帯域インタフェースを表示します。
Channel	無線帯域で現在運用中のチャンネル。
Transmit Power	無線帯域の現在の送信電力。
Authenticated Clients	物理無線帯域にあるアクセスポイントが認証したクライアントの合計数。これは、指定した無線モードで有効な VAP に認証されたクライアントの総数。
Authenticated Clients	アクセスポイントに接続し、認証されたクライアントの数。指定した無線モードで有効な VAP に認証されたクライアントの総数。

「MAC Address」または「Radio」のハイパーリンクをクリックして、無線帯域の詳細情報を参照します。

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

Radio Detail サブタブ

1. 「Status」タブの「Radio Detail」サブタブをクリックすると、以下の画面が表示されます。

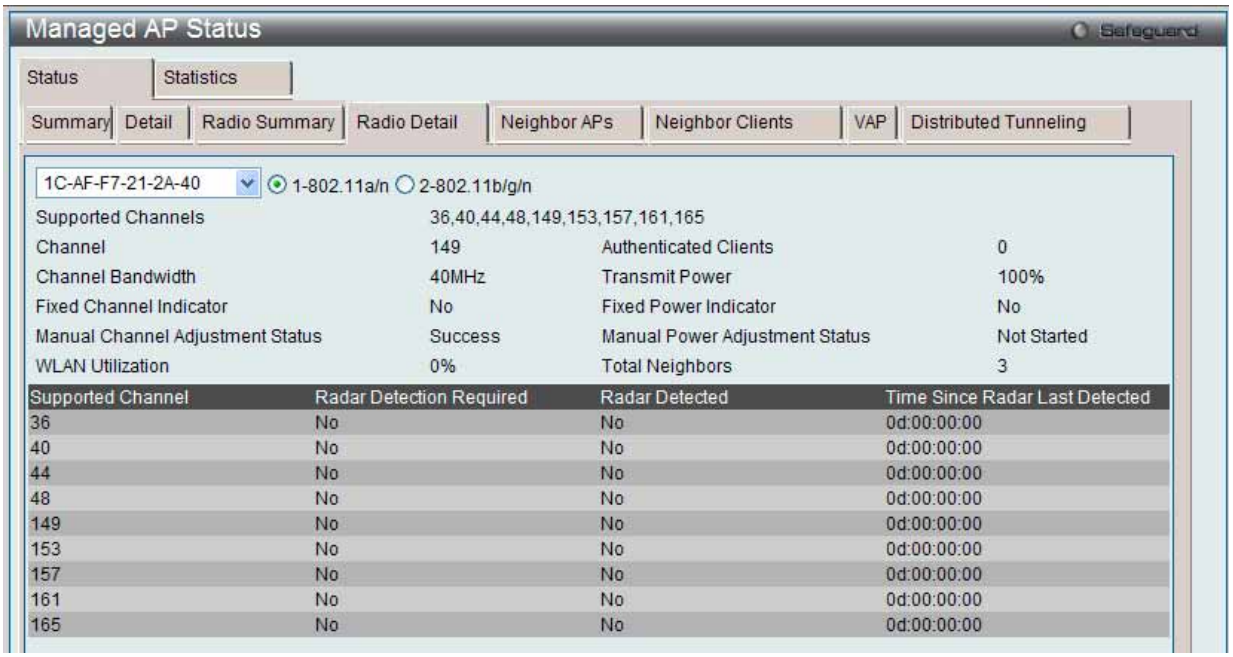


図 8.2-16　Managed AP Status > Status タブ > Radio Detail サブタブ画面

2. プルダウンメニューを使用して、詳細情報を参照するアクセスポイントの MAC アドレスと無線周波数のタイプを選択します。

「Managed AP Status」の「Status」タブの「Radio Detail」サブタブ内の各項目について説明します。

項目	説明
Supported Channels	アクセスポイントがスイッチに報告する、チャンネル割り当ての候補となるチャンネル。リスト中のエントリは国コード、ハードウェアの性能、および設定によるチャンネル制限により異なります。
Channel	無線帯域で現在運用中のチャンネル。
Channel Bandwidth	チャンネル帯域幅が 20MHz または 40MHz のいずれかであるかを表示します。
Fixed Channel Indicator	本フラグは固定チャンネルが設定され、無線インタフェースに割り当てられているかを示しています。固定チャンネルは Valid AP データベース（ローカルまたは RADIUS サーバ）において設定できます。
Manual Channel Adjustment Status	チャンネル変更する手動リクエストの現在の状況を示しています。以下の 1 つが表示されます。 • Not Started - チャンネル変更のリクエストは発行されていません。 • Requested - ユーザによりチャンネル変更のリクエストが発行されたが、スイッチはまだ処理をしていません。 • In Progress - スイッチはチャンネル変更リクエストを処理中です。 • Success - チャンネル変更リクエストは完了しました。 • Failure - チャンネル変更リクエストは失敗しました。
WLAN Utilization	物理無線帯域のネットワーク利用量の合計。本値は無線帯域の統計情報に基づきます。
Authenticated Clients	物理無線帯域にあるアクセスポイントが認証したクライアントの合計数。無線インタフェースで有効な各 VAP に対してアクセスポイントが認証したクライアントの総数。
Transmit Power	無線帯域の現在の送信電力。
Fixed Power Indicator	本フラグは固定送信電力が設定され、無線インタフェースに割り当てられているかを示しています。固定送信電力は Valid AP データベース（ローカルまたは RADIUS サーバ）において設定できます。
Manual Power Adjustment Status	送信電力を変更する手動リクエストの現在の状況を示しています。以下のいずれかが表示されます。 • Not Started - 電力変更のリクエストは発行されていません。 • Requested - ユーザにより電力変更のリクエストが発行されたが、スイッチはまだ処理をしていません。 • In Progress - スイッチは電力変更リクエストを処理中です。 • Success - 電力変更リクエストは完了しました。 • Failure - 電力変更リクエストは失敗しました。
Total Neighbors	RF エリア内の指定帯域内で隣接するデバイス（アクセスポイントとクライアントの両方）の数。
Supported Channel	トラフィックの送受信に使用される無線チャンネルを表示します。
Radar Detection Required	いくつかの規制範囲では、5GHz 帯域のチャンネルで無線モードの検出が必要です。チャンネルで無線モードの検出が必要な場合、アクセスポイントは、他の無線機器の混信を避けるために 802.11h 仕様を使用します。
Radar Detected	他の 802.11 デバイスがそのチャンネルで検出されたかどうかを表示します。
Time Since Radar Last Detected	デバイスが最後にチャンネルで検出されてから経過した時間を表示します。

Neighbor APs サブタブ

1. 「Status」タブの「Neighbor APs」サブタブをクリックして、以下の画面を表示します。

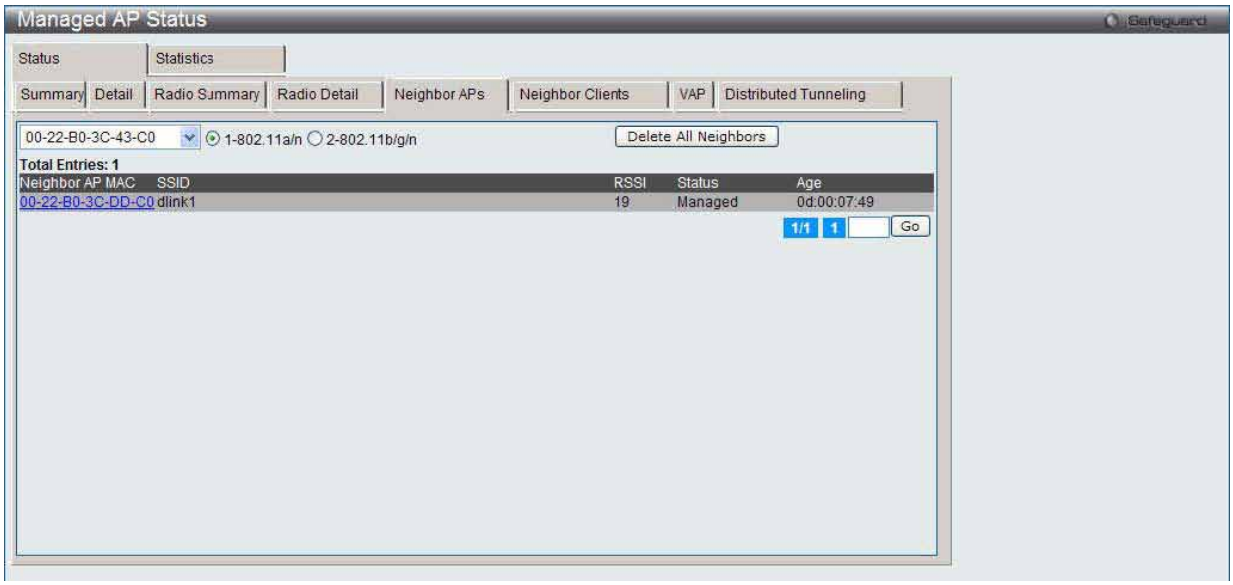


図 8.2-17　Managed AP Status > Status タブ > Neighbor APs サブタブ画面

2. RF スキャンを使用してその無線帯域で検出した隣接アクセスポイントを参照するためには、プルダウンメニューを使用して、アクセスポイントの MAC アドレスを選択し、ラジオボタンを使用して、無線帯域を選択します。

「Managed AP Status」の「Status」タブの「Neighbor APs」サブタブ内の各項目について説明します。

項目	説明
Neighbor AP MAC	隣接アクセスポイントネットワークの MAC アドレス。物理的な無線インタフェースまたは VAP の MAC アドレス。D-Link アクセスポイントの場合は常に VAP の MAC アドレスです。隣接アクセスポイントの MAC アドレスは、RF スキャン状態の内容と相互参照できます。
SSID	隣接アクセスポイントネットワークの SSID。
RSSI	Received Signal Strength Indication（受信信号強度）。隣接アクセスポイントからの信号強度を示します。これにより、管理下のアクセスポイントと隣接アクセスポイント間の距離が推測できる場合があります。範囲は 1-100 で、1 が最も弱い信号強度です。
Status	隣接アクセスポイントの管理状況を示します。スイッチに認識されている有効なアクセスポイントであるか、またはローグ（不正）と見なされるかなどの情報を得ることができます。以下のいずれかが表示されます。 • Managed - 本隣接アクセスポイントは、無線システムにより管理されています。 • Standalone - アクセスポイントは、スタンドアロンモードで管理され、Valid AP エントリ (ローカルまたは RADIUS) として設定されます。 • Rogue - 不正なアクセスポイントは脅威検出アルゴリズムの 1 つによって脅威として分類されます。 • Unknown - アクセスポイントは、ネットワークで検出されますが、脅威検出アルゴリズムは脅威として分類しません。
Age	無線帯域で、本アクセスポイントが RF スキャンによって最後に報告されてから経過した時間。

詳細情報の参照

「Neighbor AP MAC」ハイパーリンクをクリックして、アクセスポイントの RF スキャン状態に関する詳細情報を参照します。

隣接エントリの削除

「Delete All Neighbors」ボタンをクリックして、すべての隣接エントリを削除します。

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

Neighbor Clients サブタブ

1. 「Status」タブの「Neighbor Clients」サブタブをクリックして、以下の画面を表示します。

図 8.2-18　Managed AP Status > Status タブ > Neighbor Clients サブタブ画面

2. RF スキャンを使用してその無線帯域で検出した隣接クライアントを参照するためには、プルダウンメニューを使用して、アクセスポイントの MAC アドレスを選択し、ラジオボタンを使用して、無線帯域を選択します。

「Managed AP Status」の「Status」タブの「Neighbor Clients」サブタブ内の各項目について説明します。

項目	説明
Neighbor Client MAC	隣接クライアントの MAC アドレス。
RSSI	Received Signal Strength Indication（受信信号強度）。隣接クライアントからの信号強度を示します。これにより、管理下のアクセスポイントと隣接クライアント間の距離が推測できる場合があります。
Channel	クライアントからのフレームを受信した管理下のアクセスポイントのチャンネル。本インタフェースの運用チャンネルとは異なる場合があります。
Discovery Reason	隣接クライアントの検出原因。複数の原因が表示される場合があります。 • RF Scan - 本隣接クライアントは、RF スキャンにより報告されました。RF スキャンによるクライアント検出は困難なため、通常は本原因以外が表示されます。 • Probe Request - 管理対象のアクセスポイントが本隣接クライアントからプローブリクエストを受信しました。 • Associated to Managed AP - 本隣接クライアントは、当スイッチ管理下の他のアクセスポイントと接続しています。 • Associated to this AP - 本隣接クライアントは、当アクセスポイントと接続しています。 • Associated to Peer AP - 本隣接クライアントは、ピアスイッチ管理下のアクセスポイントと接続しています。 • Ad Hoc Rogue - 本隣接クライアントはアドホックネットワークに参加していることが検知されました。
Age	無線インタフェースで本クライアントが RF スキャンにより最後に報告されてから経過した時間。

詳細情報の参照

「Neighbor Client MAC」ハイパーリンクをクリックして、検出されたクライアントに関する詳細情報を参照します。

隣接エントリの削除

「Delete All Neighbors」ボタンをクリックして、すべての隣接エントリを削除します。

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

VAP サブタブ

1. 「Status」タブの「VAP」サブタブをクリックして、以下の画面を表示します。

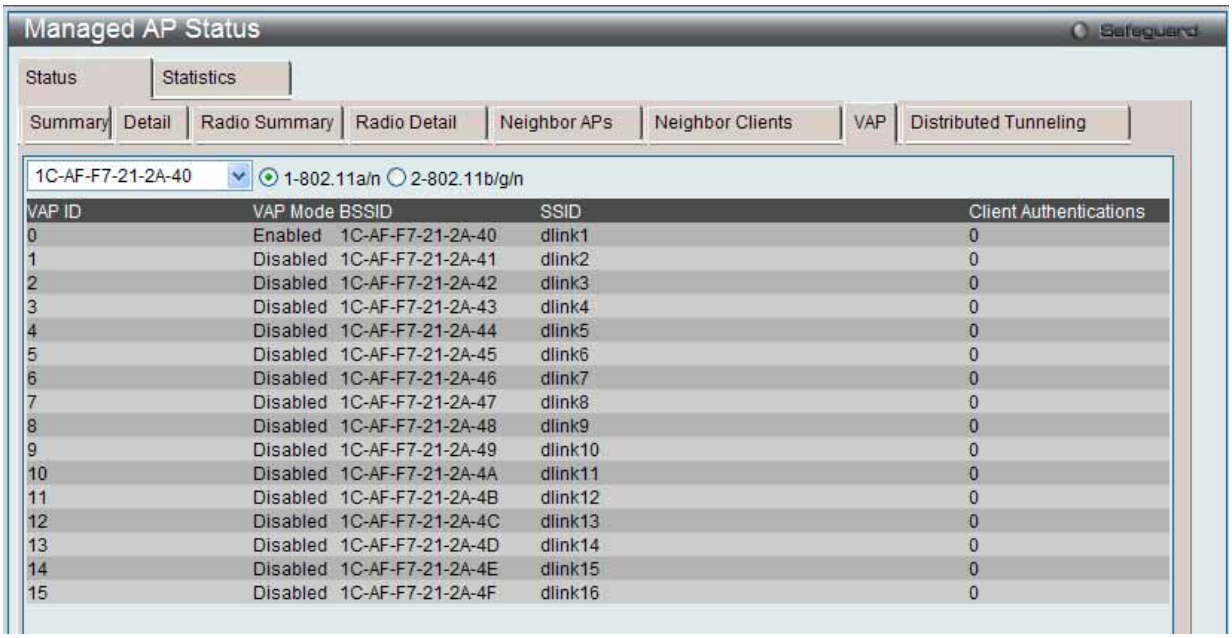


図 8.2-19　Managed AP Status > Status タブ > VAP サブタブ画面

2. その無線帯域の VAP に関する詳細を参照するためには、プルダウンメニューを使用して、アクセスポイントの MAC アドレスを選択し、ラジオボタンを使用して、無線帯域を選択します。

「Managed AP Status」の「Status」タブの「VAP」サブタブ内の各項目について説明します。

項目	説明
VAP ID	VAP を識別する ID 番号（0~7）。CLI または SNMP 経由の VAP 設定に対して VAP を識別するために使用します。
VAP Mode	VAP の「Enabled」（有効）または「Disabled」（無効）を表示します。VAP の設定後、有効にした VAP のみが、ビーコンの送信やクライアントと接続することができます。
BSSID	VAP のイーサネットアドレス。
SSID	VAP に割り当てたネットワーク。各 VAP のネットワークは AP プロファイル内で設定され、SSID はネットワークコンフィグレーションに基づいています。
Client Authentications	現在 VAP の認証を受けているクライアントの総数。

Distributed Tunneling サブタブ

1. 「Status」タブの「Distributed Tunneling」サブタブをクリックして、以下の画面を表示します。

図 8.2-20　Managed AP Status > Status タブ > Distributed Tunneling サブタブ画面

2. プルダウンメニューを使用してアクセスポイントの MAC アドレスを選択し、分配型トンネル情報を参照します。

「Managed AP Status」の「Status」タブの「Distributed Tunneling」サブタブ内の各項目について説明します。

項目	説明
Clients using AP as Home	分配型トンネルモードを使用してこのアクセスポイントからローミングし、このアクセスポイントにトンネル経由でデータを返しているクライアントの数。
Clients using AP as Associate	分配型トンネルモードを使用してこのアクセスポイントにローミングし、ホーム AP にトンネル経由でデータを送信するクライアントの数。
Distributed Tunnels	このアクセスポイントとの分配型 L2 トンネルを持っているアクセスポイントの数。アクセスポイントは、トンネルを使用することで、クライアントに対してホーム AP またはアソシエーション AP として機能します。
Multicast Replications	同じ VLAN のメンバであるホーム AP の最大トンネル数。
VLAN with Max Multicast Replications	分配型トンネルにマルチキャストを送信するためにアクセスポイントが最も多くの回数複製を行った VLAN ID。

Statistics（アクセスポイントの統計情報）タブ

1. **Monitoring > Access Point > Managed Access Points** サブタブをクリックして、以下の画面を表示します。

図 8.2-21　Managed AP Status > Statistics タブ > WLAN Summary サブタブ画面

「Managed AP Status」画面の「Statistics」タブには、以下のサブタブがあります。

項目	説明
WLAN Summary	スイッチが管理する各アクセスポイント上の無線インタフェースについてのサマリ情報を表示します。
Ethernet Summary	スイッチが管理する各アクセスポイント上のイーサネット（有線）インタフェースについてのサマリ情報を表示します。
Detail	指定するアクセスポイントが送受信したパケット数と種類を表示します。
Radio	アクセスポイントが送受信したパケット数と種類を無線インタフェースごとに表示します。
VAP	アクセスポイントが送受信したパケット数と種類、および接続に失敗したクライアントの数を VAP ごとに表示します。
Distributed Tunneling	スイッチが管理するアクセスポイントと分配型 L2 トンネルを通じてクライアントが送受信したパケット数を表示します。

WLAN Summary サブタブ

「WLAN Summary」タブで MAC アドレスをクリックすると、そのアクセスポイントの詳細な統計情報が確認できます。

「Managed AP Status」の「Statistics」タブの「WLAN Summary」サブタブ内の各項目について説明します。

項目	説明
MAC Address	統合スイッチが管理するアクセスポイントの MAC アドレス。
Packets Received	無線ネットワーク上でアクセスポイントが受信した総パケット数。
Bytes Received	無線ネットワーク上でアクセスポイントが受信した総データ量（バイト）。
Packets Transmitted	無線ネットワーク上でアクセスポイントが送信した総パケット数。
Bytes Transmitted	無線ネットワーク上でアクセスポイントが送信した総データ量（バイト）。

「MAC Address」のハイパーリンクをクリックして、アクセスポイントの詳細な統計情報を参照します。

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

Ethernet Summary サブタブ

「Managed AP Status」の「Statistics」タブの「Ethernet Summary」サブタブをクリックして、以下の画面を表示します。

図 8.2-22　Managed AP Status > Statistics タブ > Ethernet Summary サブタブ画面

「Managed AP Status」の「Statistics」タブの「Ethernet Summary」サブタブ内の各項目について説明します。

項目	説明
MAC Address	統合スイッチ管理下にあるアクセスポイントの MAC アドレス。
Packets Received	有線ネットワーク上でアクセスポイントが受信した総パケット数。
Bytes Received	有線ネットワーク上でアクセスポイントが受信した総データ量（バイト）。
Packets Transmitted	有線ネットワーク上でアクセスポイントが送信した総パケット数。
Bytes Transmitted	有線ネットワーク上でアクセスポイントが送信した総データ量（バイト）。

詳細情報の参照

「MAC Address」のハイパーリンクをクリックして、アクセスポイントの詳細な統計情報を参照します。

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

Detail サブタブ

1. 「Managed AP Status」の「Statistics」タブの「Detail」サブタブをクリックして、以下の画面を表示します。

図 8.2-23　Managed AP Status > Statistics タブ > Detail サブタブ画面

2. プルダウンメニューを使用して、統計情報を参照するスイッチ管理下のアクセスポイントの MAC アドレスを選択します。

「Managed AP Status」の「Statistics」タブの「Detail」サブタブ内の各項目について説明します。

項目	説明
WLAN Packets Received	無線ネットワーク上でアクセスポイントが受信した総パケット数。
WLAN Bytes Received	無線ネットワーク上でアクセスポイントが受信した総データ量（バイト）。
WLAN Packets Transmitted	無線ネットワーク上でアクセスポイントが送信した総パケット数。
WLAN Bytes Transmitted	無線ネットワーク上でアクセスポイントが送信した総データ量（バイト）。
WLAN Packets Received Dropped	無線ネットワーク上でアクセスポイントが受信し、破棄された総パケット数。
WLAN Bytes Received Dropped	無線ネットワーク上でアクセスポイントが受信し、破棄された総データ量（バイト）。
WLAN Packets Transmit Dropped	無線ネットワーク上でアクセスポイントが送信し、破棄された総パケット数。
WLAN Bytes Transmit Dropped	無線ネットワーク上でアクセスポイントが送信し、破棄された総データ量（バイト）。
Ethernet Packets Received	有線ネットワーク上でアクセスポイントが受信した総パケット数。
Ethernet Bytes Received	有線ネットワーク上でアクセスポイントが受信した総データ量（バイト）。
Ethernet Packets Transmitted	有線ネットワーク上でアクセスポイントが送信した総パケット数。
Ethernet Bytes Transmitted	有線ネットワーク上でアクセスポイントが送信した総データ量（バイト）。
Multicast Packets Received	有線ネットワーク上でアクセスポイントが受信したマルチキャストパケット数。
Total Receive Errors	有線ネットワーク上で検知した受信エラーの数。
Total Transmit Errors	有線ネットワーク上で検知した送信エラーの数。
ARP Reqs Converted from Bcast to Ucast	アクセスポイントが無線リンクに送信する前にブロードキャストパケットをユニキャストパケットに変換した ARP リクエストの数。
Filtered ARP Reqs	無線リンクで送信する代わりにアクセスポイントが破棄できた ARP リクエストの数。
Broadcasted ARP Requests	VAP にブロードキャストとして送信された ARP リクエストの数。このカウンタは WDS リンクを含みません。それが複数の VAP にブロードキャストされると、同じ ARP フレームが複数のカウントされる可能性があります。ARP の抑止が無効にされても、本カウンタは利用可能です。

「Refresh」ボタンをクリックすると、画面を最新の情報に更新します。

Radio サブタブ

1. 「Managed AP Status」の「Statistics」タブの「Radio」サブタブをクリックして、以下の画面を表示します。

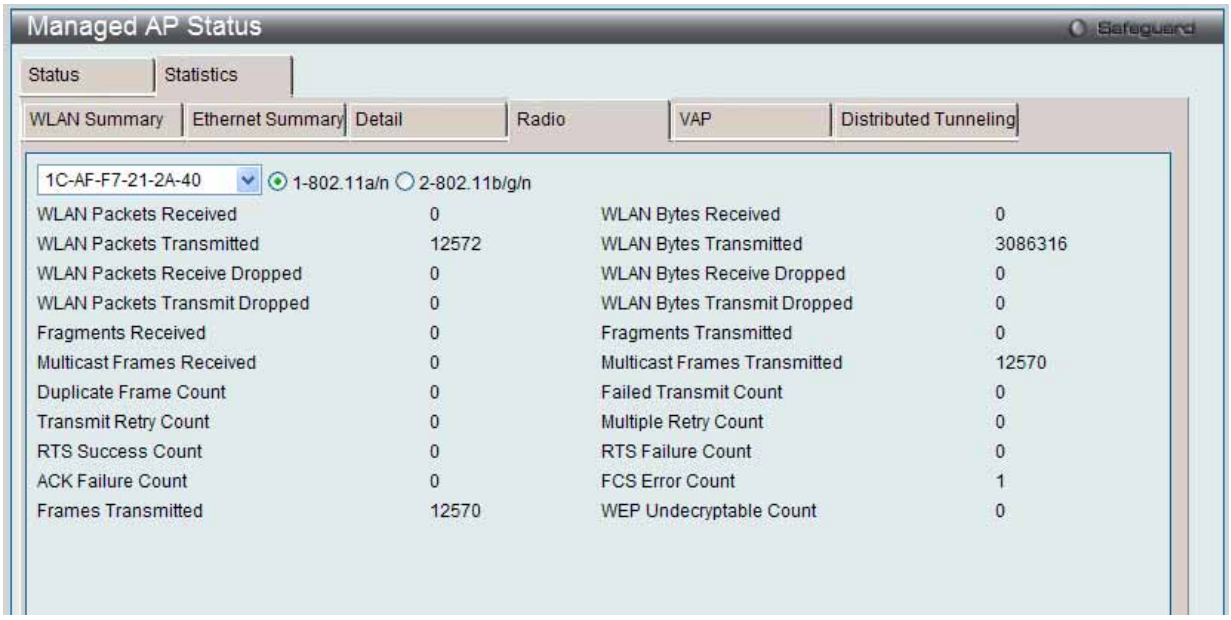


図 8.2-24　Managed AP Status > Statistics タブ > Detail サブタブ画面

2. プルダウンメニューを使用してアクセスポイントの MAC アドレスを選択し、ラジオボタンで無線帯域を選択して、スイッチが管理する特定のアクセスポイントの無線帯域インタフェースで送受信したパケット数およびデータ量（バイト）に関する詳しい情報を表示します。

「Managed AP Status」の「Statistics」タブの「Radio」サブタブ内の各項目について説明します。

項目	説明
WLAN Packets Received	無線インタフェース上でアクセスポイントが受信した総パケット数。
WLAN Bytes Received	無線インタフェース上でアクセスポイントが受信した総データ量（バイト）。
WLAN Packets Transmitted	無線インタフェース上でアクセスポイントが送信した総パケット数。
WLAN Bytes Transmitted	無線インタフェース上でアクセスポイントが送信した総データ量（バイト）。
WLAN Packets Received Dropped	無線インタフェース上でアクセスポイントが受信し、破棄されたパケット数。
WLAN Bytes Received Dropped	無線インタフェース上でアクセスポイントが受信し、破棄されたデータ量（バイト）。
WLAN Packets Transmit Dropped	無線インタフェース上でアクセスポイントが送信し、破棄されたパケット数。
WLAN Bytes Transmit Dropped	無線インタフェース上でアクセスポイントが送信し、破棄されたデータ量（バイト）。
Bytes Transmit Dropped	正しく受信したタイプがデータまたは管理の MPDU フレーム数。
Fragments Transmitted	送信したタイプがデータまたは管理で、個別アドレスまたはマルチキャストアドレスを含む MPDU フレーム数。
Multicast Frames Received	受信した宛先 MAC アドレス中にマルチキャストビットが設定されている MSDU フレーム数。
Multicast Frames Transmitted	正しく送信した宛先 MAC アドレス中にマルチキャストビットが設定されている MSDU 数。
Duplicate Frame Count	シーケンス制御フィールドで duplicate(冗長) と示されているフレームを受信した回数。
Failed Transmit Count	Short retry limit/Long retry limit 超過により、MSDU が正しく送信されなかった回数。
Transmit Retry Count	1 度以上のリトライ後に MSDU が正しく送信された回数。
Multiple Retry Count	2 度以上のリトライ後に MSDU が正しく送信された回数。
RTS Success Count	RTS フレームの応答として受信された CTS フレームの数。
RTS Failure Count	RTS フレームの応答として受信されなかった CTS フレームの数。
ACK Failure Count	想定していた ACK フレームが受信されなった数。
FCS Error Count	受信した MPDU により検知した FCS エラー数。
Frames Transmitted	送信に成功した MSDU の数。
WEP Undecryptable Count	暗号化されたフレームのうち、暗号化の必要なしと示されているもの、または受信デバイスがプライバシーオプションを使用していないために廃棄されたフレームの数。

「Refresh」ボタンをクリックすると、画面を最新の情報に更新します。

VAP サブタブ

1. 「Managed AP Status」の「Statistics」タブの「VAP」サブタブをクリックして、以下の画面を表示します。

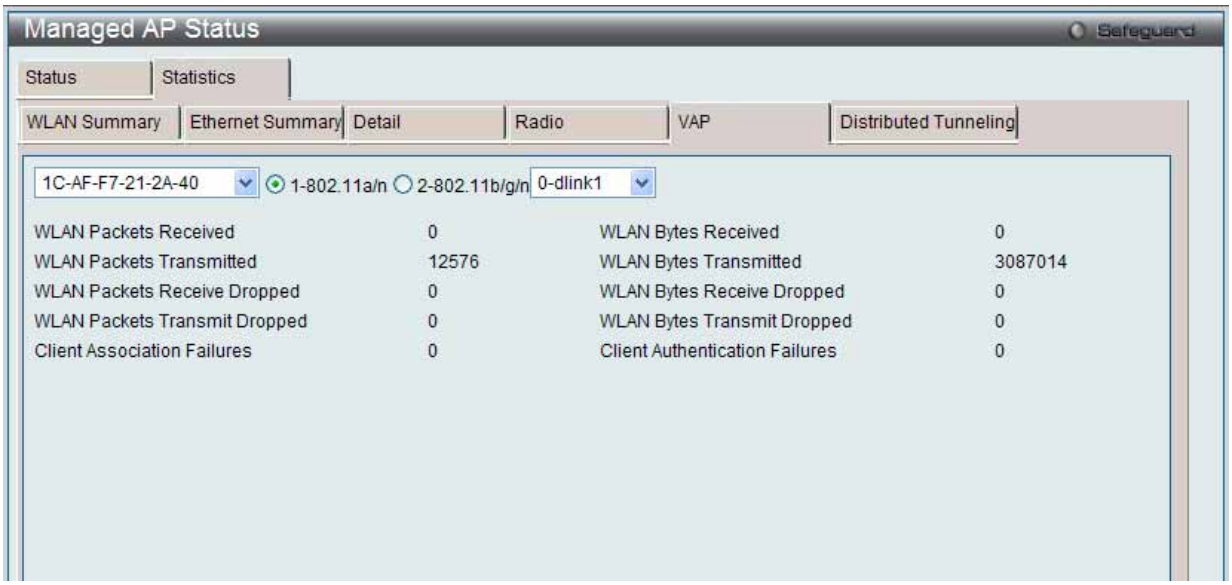


図 8.2-25　Managed AP Status > Statistics タブ > VAP サブタブ画面

2. プルダウンメニューを使用してアクセスポイントの MAC アドレスと VAP ID を選択し、ラジオボタンで無線帯域を選択して、スイッチが管理する特定のアクセスポイントの無線帯域におけるクライアントエラーの情報および各 VAP が送受信したパケット数およびデータ量（バイト）に関する情報を表示します。

「Managed AP Status」の「Statistics」タブの「Distributed Tunneling」サブタブ内の各項目について説明します。

項目	説明
WLAN Packets Received	指定した VAP が受信した総パケット数。
WLAN Bytes Received	指定した VAP が受信した総データ量（バイト）。
WLAN Packets Transmitted	指定した VAP が送信した総パケット数。
WLAN Bytes Transmitted	指定した VAP が送信した総データ量（バイト）。
WLAN Packets Received Dropped	この VAP 上でアクセスポイントが受信し、破棄されたパケット数。
WLAN Bytes Received Dropped	この VAP 上でアクセスポイントが受信し、破棄されたバイト数。
WLAN Packets Transmit Dropped	この VAP 上でアクセスポイントが送信し、破棄されたパケット数。
WLAN Bytes Transmit Dropped	この VAP 上でアクセスポイントが送信し、破棄されたバイト数。
Client Association Failures	VAP により接続を拒否されたクライアント数。
Client Authentication Failures	VAP への認証に失敗したクライアント数。

「Refresh」ボタンをクリックすると、画面を最新の情報に更新します。

Distributed Tunneling サブタブ

「Managed AP Status」の「Statistics」タブの「Distributed Tunneling」サブタブをクリックして、以下の画面を表示します。

図 8.2-26　Managed AP Status > Statistics タブ > Distributed Tunneling サブタブ画面

プルダウンメニューを使用して、スイッチが管理するアクセスポイントにおける L2 Distributed トンネルを使用するクライアントが送受信したパケットおよびバイト数に関する情報を表示するアクセスポイントの MAC アドレスを選択します。

AP Authentication Failure Status（アクセスポイント認証エラー状態）

スイッチへの接続に失敗したアクセスポイントを表示します。

1. **Monitoring > Access Point > AP Authentication Failure Status** の順にメニューをクリックし、以下の画面を表示します。

図 8.2-27　AP Authentication Failure Status 画面

2. 以下の項目が表示されます。

項目	説明
MAC Address	アクセスポイントの MAC アドレス。
IP Address	アクセスポイントのネットワーク IP アドレス。
Last Failure Type	前回の認証失敗の原因。
Age	失敗発生からの経過時間。

エントリの状態変更

対応するボックスをチェックし、「Manage」ボタンをクリックして、アクセスポイントをスイッチに関連付けします。

エントリの削除

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

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

詳細情報の表示

「MAC Address」ハイパーリンクをクリックすると、以下の画面が表示されます。

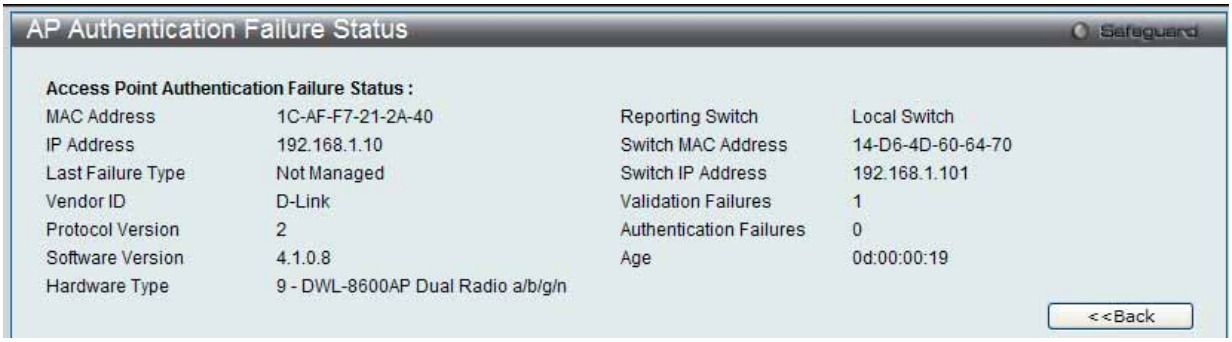


図 8.2-28　AP Authentication Failure Status - Detail 画面

「<<Back」をボタンをクリックして前のページに戻ります。

AP RF Scan Status（アクセスポイントの RF スキャン状態）

「Rogue」（不正）として報告されたものを含む RF スキャンで検出されたすべてのアクセスポイントに関する情報を表示します。

1. **Monitoring > Access Point > AP RF Scan Status** の順にメニューをクリックし、以下の画面を表示します。

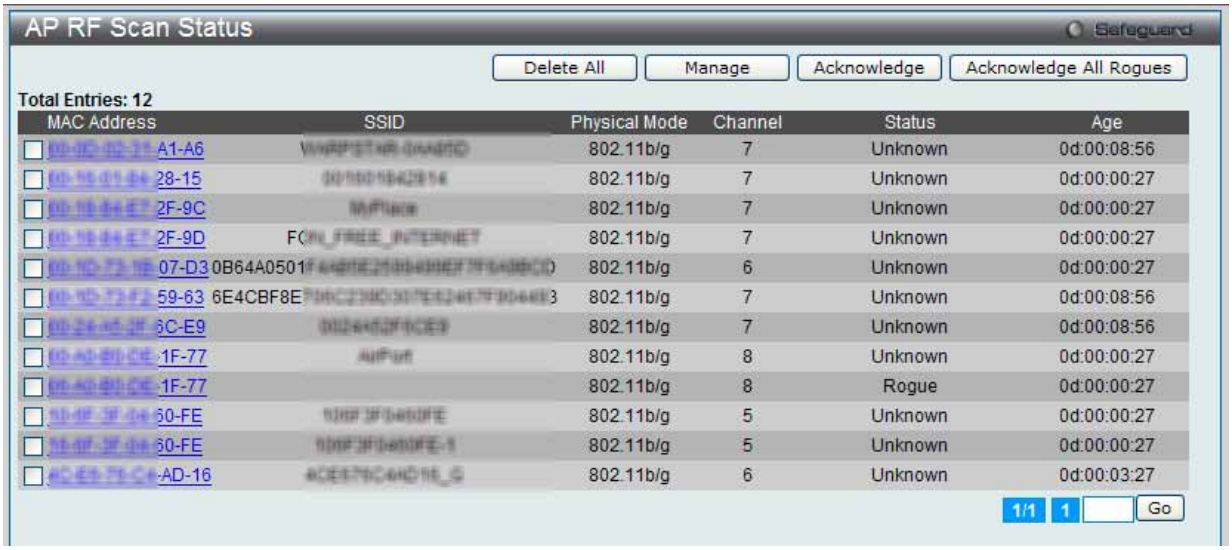


図 8.2-29　AP RF Scan Status 画面

2. 以下の項目が表示されます。

項目	説明
MAC Address	検出されたアクセスポイントの MAC アドレス。これは、物理的な無線インタフェースまたは VAP の MAC アドレスです。D-Link アクセスポイントの場合は常に VAP の MAC アドレスとなります。
SSID	ネットワークの SSID。ブロードキャストされたビーコンフレームから検出します。
Physical Mode	アクセスポイントで使用している 802.11 のモードを表示します。
Channel	アクセスポイントの通信チャンネル。
Status	隣接アクセスポイントの管理状況を示します。スイッチに認識されている有効なアクセスポイントであるか、または Rogue（不正）と見なされるかなどの情報を得ることができます。以下の 1 つが表示されます。 • Managed - 本隣接アクセスポイントは、無線システムにより管理されています。 • Standalone - アクセスポイントは、スタンドアロンモードで管理され、Valid AP エントリ（ローカルまたは RADIUS）として設定されます。 • Rogue - 不正なアクセスポイントは脅威検出アルゴリズムの 1 つによって脅威として分類されます。 • Unknown - アクセスポイントは、ネットワークで検出されますが、脅威検出アルゴリズムは脅威として分類しません。
Age	本アクセスポイントが最後に RF スキャンで検出されてから経過した時間。

エントリの状態変更

特定のボックスをチェックし、「Manage」ボタンをクリックして、「Rogue AP」を次回検出時にスイッチが管理するように設定します。
特定のボックスをチェックし、「Acknowledge」ボタンをクリックして、「RF Scan」データベースにアクセスポイントの不正状態をクリアします。
「Acknowledge All Rogues」ボタンをクリックして、ローグ状態であるすべてのアクセスポイントを承認します。

エントリの削除

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

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

詳細情報の表示

「MAC Address」ハイパーリンクをクリックすると、以下の画面が表示されます。

AP RF Scan Status タブ

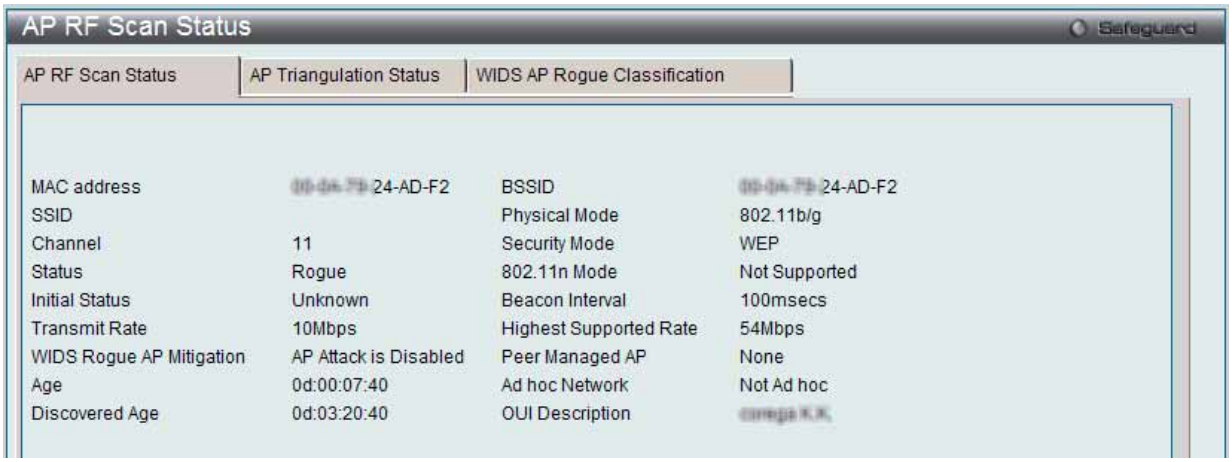


図 8.2-30　AP RF Scan Status - Detail 画面

以下の項目が表示されます。

項目	説明
MAC Address	検出されたアクセスポイントの MAC アドレス。これは、物理的な無線インタフェースまたは VAP の MAC アドレスです。D-Link アクセスポイントの場合は常に VAP の MAC アドレスとなります。
SSID	ネットワークの SSID。ブロードキャストされたビーコンフレームから検出します。
Channel	アクセスポイントの通信チャンネル。
Status	隣接アクセスポイントの管理状況を示します。スイッチに認識されている有効なアクセスポイントであるか、またはローグ（不正）と見なされるかなどの情報を得ることができます。以下の 1 つが表示されます。 • Managed - 本隣接アクセスポイントは、無線システムにより管理されています。 • Standalone - アクセスポイントは、スタンドアロンモードで管理され、Valid AP エントリ (ローカルまたは RADIUS) として設定されます。 • Rogue - 不正なアクセスポイントは脅威検出アルゴリズムの 1 つによって脅威として分類されます。 • Unknown - アクセスポイントは、ネットワークで検出されますが、脅威検出アルゴリズムは脅威として分類しません。
Initial Status	アクセスポイントが不正でなければ、初期状態は「Managed」、「Standalone」、または「Unknown」となります。不正なアクセスポイントの初期状態はこのアクセスポイントが不正になる前の分類となります。
Transmit Rate	アクセスポイントの現在の送信速度を表示します。
WIDS Rogue AP Mitigation	不正なアクセスポイントの移行がこのアクセスポイントで進行しているかどうかを示す状況。移行が進んでいない場合、以下の原因から 1 つが表示されます。 • Not Required（アクセスポイントは不正ではありません。） • Already mitigating too many APs.（既に、非常にに多くのアクセスポイント AP を移行しています。） • AP Is operating on an illegal channel.（アクセスポイントは不正なチャンネルで動作中です。） • AP is spoofing valid managed AP MAC address.（アクセスポイントは、有効な管理アクセスポイントの MAC アドレスをスプーフィングしています。） • AP is Ad hoc.（アクセスポイントは Ad hoc モードです。）
Age	本アクセスポイントが最後に RF スキャンで検出されてから経過した時間。
Discovered Age	本アクセスポイントが最初に RF スキャンで検出されてから経過した時間。
BSSID	アクセスポイントから通知されたビーコンフレーム内のアクセスポイントの識別名。
Physical Mode	アクセスポイントで使用している 802.11 のモードを表示します。
Security Mode	アクセスポイントが使用するセキュリティモード。
802.11n Mode	本アクセスポイントが IEEE 802.11n モードをサポートするかどうかを表示します。
Beacon Interval	隣接アクセスポイントネットワークへのビーコン間隔。
Highest Supported Rate	ビーコンフレームの中で本アクセスポイントは通知した最も高いサポートレート。レートは、1Mbps ずつ増加して表示されます。
Peer Managed AP	本アクセスポイントがクラスタ内でスイッチに管理されているかどうかを表示します。
Ad hoc Network	ad hoc ネットワークからビーコンフレームを受信したかどうかを表示します。
OUI Description	スイッチにおける OUI データベースの情報に基づいて、アクセスポイントまたは無線クライアントアダプタのメーカを表示します。

AP Triangulation Status タブ

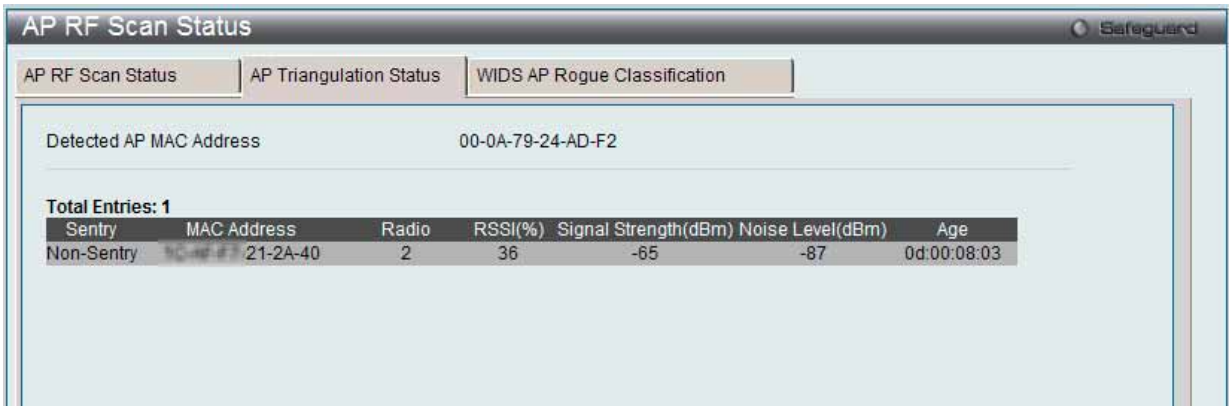


図 8.2-31　AP RF Scan Status - AP Triangulation Status 画面

以下の項目があります。

項目	説明
Detected AP MAC Address	検出されたアクセスポイントの MAC アドレス。これは、物理的な無線インタフェースまたは VAP の MAC アドレスです。D-Link アクセスポイントの場合は常に VAP の MAC アドレスです。
Sentry	エントリを検出したアクセスポイントのモード（Sentry または Non-Sentry）を表示します。
MAC Address	RF スキャンエントリを検出したアクセスポイントの MAC アドレスを表示します。 アドレスは、Valid AP データベースにリンクしています。
Radio	RF スキャンエントリを検出したアクセスポイントの無線電波を表示します。
RSSI (%)	Non-Sentry AP の受信信号強度 (%) を表示します。範囲は 0-100% です。0 の値は、AP が検出されないことを示します。
Signal Strength(dBm)	Non-Sentry AP のための受信信号強度。範囲は -127 dBm ～ 127 dBm ですが、大抵の値は -95 dBm ～ -10 dBm の範囲に入ります。
Noise Level(dBm)	Non-Sentry AP がチャンネルについて報告したノイズ。
Age	本アクセスポイントが最後に RF スキャンで検出されてから経過した時間。

WIDS AP Rogue Classification タブ

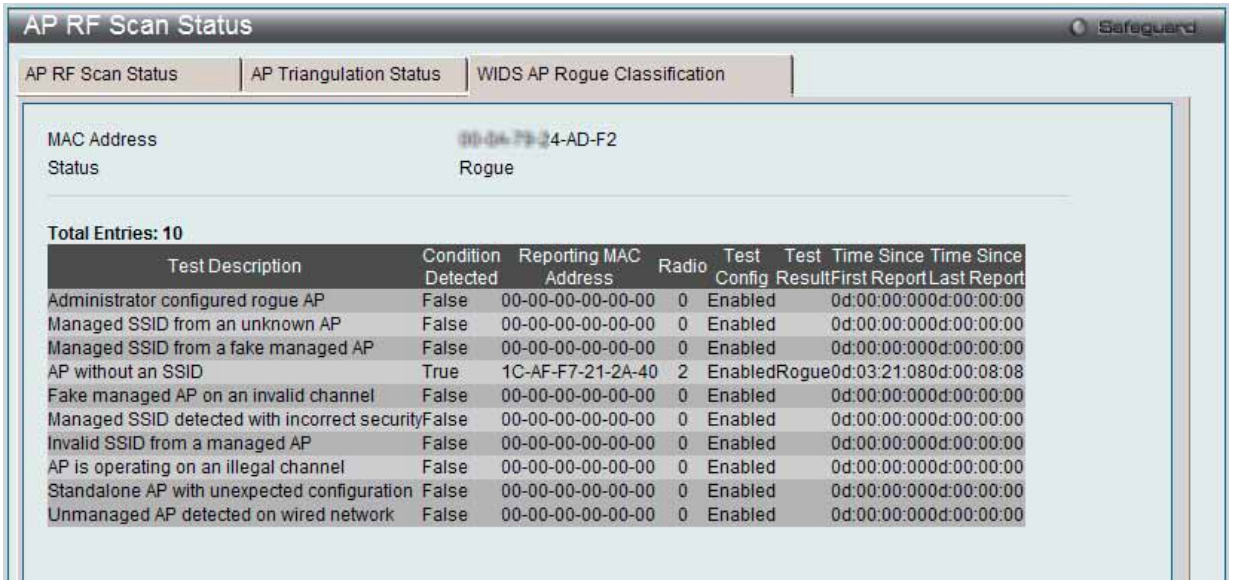


図 8.2-32　AP RF Scan Status - WIDS AP Rogue Classification 画面

以下の項目が表示されます。

項目	説明
MAC Address	検出されたアクセスポイントの MAC アドレス。これは、物理的な無線電インタフェースまたは VAP の MAC アドレスです。D-Link アクセスポイントの場合は常に VAP の MAC アドレスです。
Status	隣接アクセスポイントの管理状況を示します。ネットワークにおいてスイッチに認識されている Valid AP であるか、または Rogue（不正）かどうかを表示します。以下の 1 つが表示されます。 • Managed - 本隣接アクセスポイントは、無線システムにより管理されています。 • Standalone - アクセスポイントは、スタンドアロンモードで管理され、Valid AP エントリ (ローカルまたは RADIUS) として設定されます。 • Rogue - 不正なアクセスポイントは脅威検出アルゴリズムの 1 つによって脅威として分類されます。 • Unknown - アクセスポイントは、ネットワークで検出されますが、脅威検出アルゴリズムは脅威として分類しません。
Test Description	実行されたテストを表示します。以下のテストがあります。 • Administrator-Configured rogue AP（管理者が設定した不正アクセスポイント） • Managed SSID received from an unknown AP（不明なアクセスポイントから受信した管理 SSID） • Managed SSID from a fake managed AP（偽の管理下のアクセスポイントから受信した管理 SSID） • Fake managed AP on an invalid channel（不正チャンネルにおける偽の管理対象アクセスポイント） • AP without an SSID（SSID を持たないアクセスポイント） • Managed SSID detected with incorrect security configuration（不正なセキュリティ設定を持つことを検出された管理 SSID） • Invalid SSID received from managed AP（管理対象アクセスポイントから受信した不正な SSID） • AP is operating on an illegal channel（アクセスポイントが不正なチャンネルで動作中） • Standalone AP is operating with unexpected configuration（スタンドアロンモードのアクセスポイントが予期しない設定を使用して動作中） • Unmanaged AP detected on wired network（管理下にないアクセスポイントが有線ネットワークで検出）
Condition Detected	テストの結果が正しいかどうかを表示します。
Reporting MAC Address	テスト結果を報告したアクセスポイントの MAC アドレスを表示します。
Radio	報告されたアクセスポイントのどの物理無線帯域がテスト結果の原因となったかを表示します。
Test Config	このテストが不正を報告するように設定されているかどうかを表示します。不正として確実に結果を報告するために、各テストをグローバルに「Enabled」（有効）または「Disabled」（無効）にします。
Test Result	このテストが、デバイスを不正であると報告したかどうかを表示します。デバイスはこのモードで動作を許可されているため、いくつかの場合、テストは肯定的な結果を報告し、有効であり、不正なものとしてレポートしないかもしれません。
Time Since First Report	このテストが最初にこの条件を検出した時期を示すタイムスタンプ。
Time Since Last Report	このテストが最後にこの条件を検出した時期を示すタイムスタンプ。

AP De-Authentication Attack Status（アクセスポイント認証解除攻撃状態）

認証解除攻撃機能を使用してクラスタコントローラが攻撃を行った不正アクセスポイントに関する情報を表示します。無線スイッチは、認証解除メッセージを不正なアクセスポイントに送信することで、不正なアクセスポイントから防御できます。無線システムが本機能を動作するためには、認証解除攻撃機能をグローバルに有効にする必要があります。攻撃機能を有効にする前には、認知されないアクセスポイントは「Rogue」（不正）として分類されないことにご注意ください。本機能は初期値では「Disabled」（無効）になっています。

無線システムは、同時に 16 個のアクセスポイントに対して認証解除攻撃を行うことができます。この攻撃の目的は、不正なアクセスポイントが検出され、無効になるまでの一時的な方法として動作することです。

1. **Monitoring > Access Point > AP De-Authentication Attack Status** の順にメニューをクリックし、以下の画面を表示します。

図 8.2-33　AP De-Authentication Attack Status 画面

2. 以下の項目が表示されます。

項目	説明
BSSD	攻撃を開始するアクセスポイントの BSSID を表示します。BSSID は MAC アドレスです。
Channel	不正なアクセスポイントが動作しているチャンネルを表示します。
Time Since Attack Started	攻撃がアクセスポイントに開始してから経過した時間を表示します。
RF Scan Report Age	RF スキャンがこのアクセスポイントを報告してから経過した時間を表示します。

Client（クライアント）

Associated Clients（接続中のクライアント）

スイッチが管理するアクセスポイントに接続中の無線クライアントについて、さまざまな情報を表示します。

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

図 8.2-34　Associated Clients - Status - Summary 画面

本画面では以下のタブが利用可能です。

項目	説明
Status	スイッチ管理対象のアクセスポイントと接続中のクライアントの状態。以下の情報が表示されます。 • Summary - 接続中のクライアントの基本的な情報。 • Detail - 接続中のクライアントの詳細情報（例 : クライアントが接続している VLAN。クライアントが非アクティブである時間など）。 • Client QoS - 接続中のクライアントの QoS ステータスを表示します。 • Neighbor APs - クライアントの通信範囲内にある管理対象のアクセスポイントを表示します。接続中のクライアントがローミングに使用するアクセスポイントを決定する場合に役立てることができます。 • Distributed Tunneling - クライアントの分配型トンネリングに関する情報を表示します。
SSID Status	SSID と、そのネットワークに接続するクライアントの MAC アドレス。
VAP Status	D-Link アクセスポイント上の指定した VAP に接続中のクライアントを表示します。
Switch Status	各無線クライアントが接続したスイッチの情報を表示します。
Statistics	アクセスポイントに接続中のクライアントについて、以下の統計情報を表示します。 • Summary - 1 台のアクセスポイントと接続中のクライアントの統計情報。 • Session Summary - クライアントが、異なるアクセスポイント間でローミングする際のセッション全体についての統計情報。 • Association Detail - 1 台のアクセスポイントと接続中のクライアントが送受信するパケットの詳細情報。 • Session Detail - 1 台、またはローミング時には複数のアクセスポイントと接続中のクライアントが送受信するパケットの詳細情報。

Status タブ

Summary サブタブ

「Associated Clients」の「Status」タブの「Summary」サブタブをクリックします。

「Status」タブの「Summary」サブタブ内の各項目について説明します。

項目	説明
MAC Address	クライアントステーションの MAC アドレス。MAC アドレスの後に (*) が続いている場合、クライアントはピアスイッチに管理されているアクセスポイントに接続します。
Detected IP Address	クライアントの IPv4 アドレスを表示します。
NetBIOS Name	無線クライアントの NetBIOS 名。マイクロソフト Windows における NetBIOS 名は、通常クライアントのホスト名とに同じか、またはホスト名に基づいています。
SSID	クライアントが接続中のネットワーク。
BSSID	クライアントが接続中の VAP におけるアクセスポイントの MAC アドレス。
Channel	クライアントの接続に使用されているチャンネル。
Status	クライアントが接続中であるか、認証されているかを示しています。以下のいずれかが表示されます。 • Associated - クライアントは現在管理対象のアクセスポイントと接続中です。 • Authenticated - クライアントは現在接続中で、アクセスポイントに認証されています。 • Disassociated - クライアントはアクセスポイントと接続していません。タイムアウト時間内に他の管理対象アクセスポイントとローミングを開始しない場合は削除されます。
Network Time	最初にクライアントがネットワークに認証されてから経過した時間を表示します。

クライアントの切断

特定のボックスをチェックし、「Disassociate」ボタンをクリックして、管理するアクセスポイントからクライアントを切断します。
「Disassociate All」ボタンをクリックして、管理下のアクセスポイントからすべてのクライアントを切断します。

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

Detail サブタブ

「Associated Clients」の「Status」タブの「Detail」サブタブをクリックして、以下の画面を表示します。

図 8.2-35　Associated Clients - Status - Detail 画面

「Status」タブの「Detail」サブタブ内の各項目について説明します。

項目	説明
MAC Address	クライアントの MAC アドレス。プルダウンメニューから MAC アドレスを選択すると、そのクライアントについての詳細情報が表示されます。
SSID	クライアントが接続中のネットワークを表示します。
BSSID	クライアントが接続中のアクセスポイントにおける VAP の MAC アドレスを表示します。
AP MAC Address	管理下にあるベースアクセスポイントのイーサネット MAC アドレスを示します。
Status	クライアントが接続中であるか、認証されているかを示しています。以下の 1 つが表示されます。 • Associated - クライアントは現在管理対象のアクセスポイントと接続中です。 • Authenticated - クライアントは現在接続中で、アクセスポイントに認証されています。 • Disassociated - クライアントはアクセスポイントと接続していません。タイムアウト時間内に他の管理対象アクセスポイントとローミングを開始しない場合は削除されます。
Channel	クライアントの接続に使用されているチャンネルを表示します。
User Name	802.1X により認証されているクライアントのユーザ名。他のセキュリティモードを使用しているクライアントはユーザ名の表示はありません。
Inactive Period	クライアントから最後にデータパケットを受信してから経過した時間を表示します。
Age	スイッチが、このクライアントの新しい状態および統計情報の更新を受信してから経過した時間を表示します。
Dot11n Capable	接続するクライアントが IEEE 802.11n 標準をサポートするかどうかを表示します。
NetBIOS Name	無線クライアントの NetBIOS 名を表示します。マイクロソフト Windows ホストにおける NetBIOS 名は、通常ホスト名と同じか、またはホスト名に基づいています。
Tunnel IP Address	クライアントがトンネルを使用している場合、割り当てられたトンネル IP アドレスが表示されます。トンネルを使用しないクライアントの場合、表示はありません。
Associating Switch	無線クライアントが接続するアクセスポイントがローカルスイッチまたはピアスイッチによって管理されるかどうか示します。
Reporting Switch	無線クライアントが接続するアクセスポイントを管理するスイッチの MAC アドレスを表示します。
Switch IP Address	無線クライアントが接続するアクセスポイントを管理するスイッチの IP アドレスを表示します。
Location	管理下のアクセスポイントの設置場所について表示します。
Radio	クライアントが接続中のアクセスポイントの無線インタフェースと無線モードを表示します。
VLAN	クライアントが VAP にあり、VLAN データ送信モードを使用している場合、現在割り当てられている VLAN を表示します。
Transmit Data Rate	クライアントステーションの現在のデータ送信速度を表示します。
Network Time	最初にクライアントがネットワークに認証されてから経過した時間を表示します。
STBC Capable	クライアントの Space Time Block Code（STBC）モードを表示します。
Detected IP Address	クライアントの IPv4 アドレスを表示します。

プルダウンメニューを使用して、アクセスポイントに接続するクライアントとそのアソシエーションに関する詳細状態の情報を参照するクライアントの MAC アドレスを選択します。

クライアントの切断

「Disassociate」ボタンをクリックして、管理下のアクセスポイントからクライアントを切断します。

Client QoS サブタブ

1. 「Associated Clients」の「Status」タブの「Client QoS」サブタブをクリックして、以下の画面を表示します。

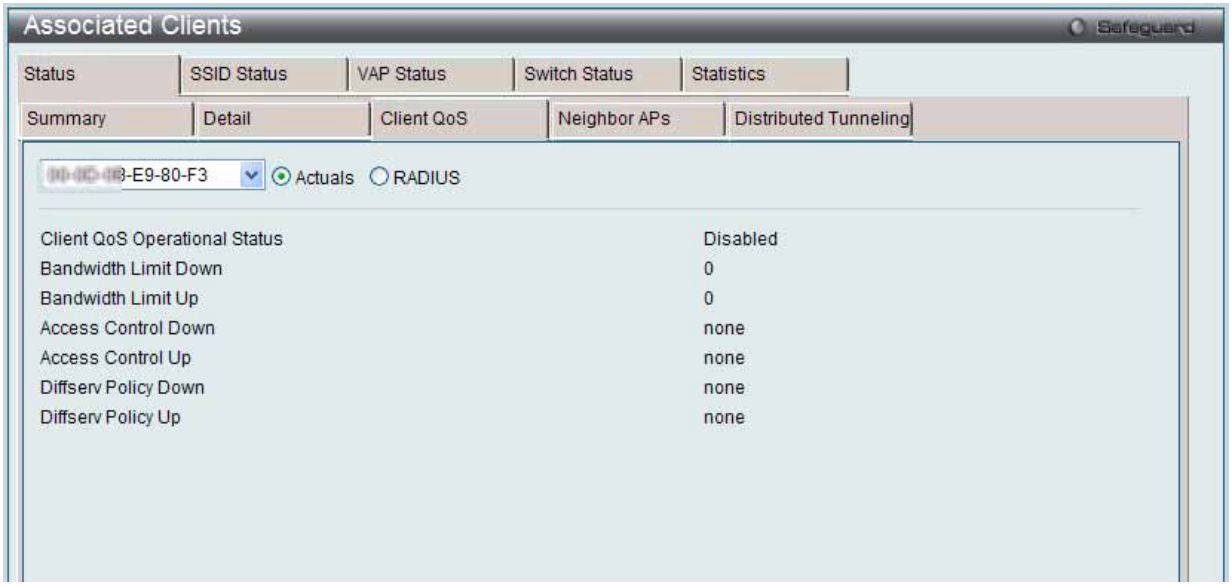


図 8.2-36　Associated Clients - Status - Client QoS 画面

2. プルダウンメニューを使用して、情報を参照するクライアントの MAC アドレスを選択します。

「Status」タブの「Client QoS」サブタブ内の各項目について説明します。

項目	説明
Actuals / RADIUS	• Actuals - アクセスポイントに設定した実際のステータスパラメータを表示します。 • RADIUS - 802.1X 認証を使用した際に、RADIUS サーバからクライアントに取得したクライアントの QoS パラメータを表示します。
Client QoS Operational Status	QoS がクライアントに実施されるかどうかを表示します。
Bandwidth Limit Down	クライアントがアクセスポイントからトラフィックを受信する最大レート (bps) を表示します。本欄に表示されるレートは、64Kbps に最も近づくように丸められた設定値です。0 の値は、この方向に帯域幅の制限がないことを意味します。
Bandwidth Limit Up	クライアントがアクセスポイントにトラフィックを送信する最大レート (bps) を表示します。本欄に表示されるレートは、64Kbps に最も近づくように丸められた設定値です。0 の値は、この方向に帯域幅の制限がないことを意味します。
Access Control Down	もしあれば、アクセスポイントからクライアントまでのトラフィックに適用される ACL を表示します。
Access Control Up	もしあれば、クライアントからアクセスポイントまでのトラフィックに適用される ACL を表示します。
Diffserv Policy Down	もしあれば、アクセスポイントからクライアントまでのトラフィックに適用される DiffServ ポリシーを表示します。
Diffserv Policy Up	もしあれば、クライアントからアクセスポイントまでのトラフィックに適用される DiffServ ポリシーを表示します。

Neighbor APs サブタブ

1. 「Associated Clients」の「Status」タブの「Neighbor APs」サブタブをクリックして、以下の画面を表示します。

図 8.2-37　Associated Clients - Status - Neighbor APs 画面

2. プルダウンメニューを使用して、情報を参照するクライアントの MAC アドレスを選択します。

「Status」タブの「Neighbor APs」サブタブ内の各項目について説明します。

項目	説明
MAC Address	クライアントの MAC アドレス。プルダウンメニューから MAC アドレスを選択すると、そのクライアントについての詳細情報が表示されます。
AP MAC Address	統合スイッチ管理下にあるアクセスポイントのイーサネットアドレス。
Location	管理下のアクセスポイントの設定場所の説明。
Radio	本クライアントを隣接クライアントとして検出した無線インタフェースと無線モード。
Discovery Reason	隣接クライアントの検出原因。複数の原因が表示される場合があります。 • RF Scan - 本隣接クライアントは、RF スキャンにより報告されました。RF スキャンによるクライアント検出は困難なため、通常は本原因以外が表示されます。 • Probe Request - 管理対象のアクセスポイントが本隣接クライアントからプローブリクエストを受信しました。 • Associated to Managed AP - 本隣接クライアントは、当スイッチ管理下の他のアクセスポイントと接続しています。 • Associated to This AP - 本隣接クライアントは、当アクセスポイントと接続しています。 • Associated to Peer AP - 本隣接クライアントは、ピアスイッチの管理下のアクセスポイントと接続しています。 • Ad Hoc Rogue - 本隣接クライアントはアドホックネットワークに参加していることが検知されました。

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

Distributed Tunneling サブタブ

1. 「Associated Clients」の「Status」タブの「Distributed Tunneling」サブタブをクリックして、以下の画面を表示します。

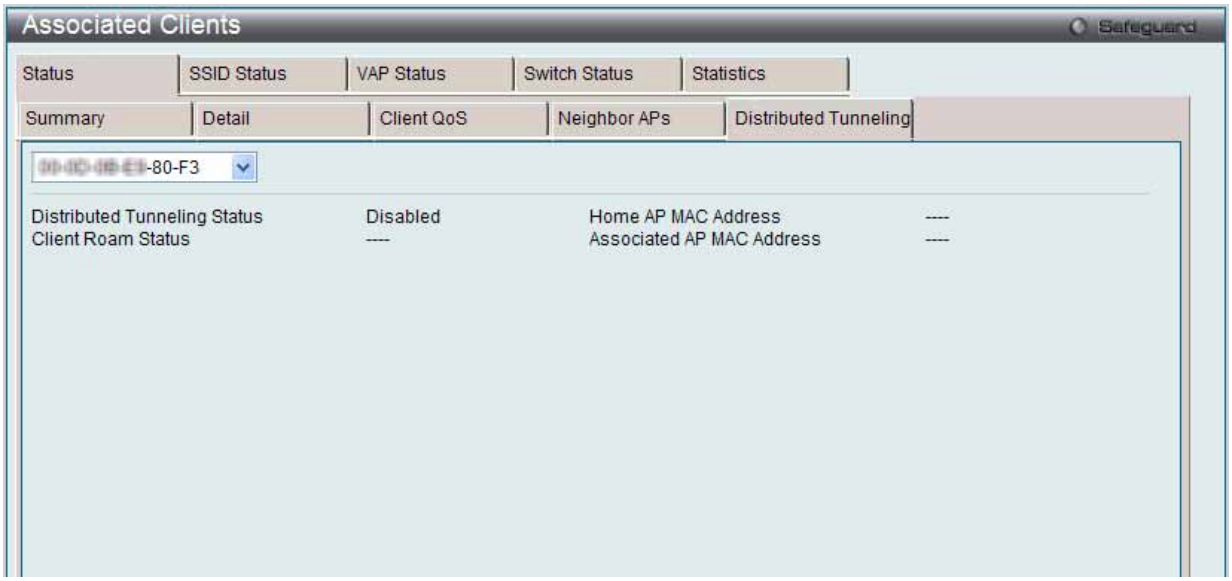


図 8.2-38　Associated Clients - Status - Distributed Tunneling 画面

2. プルダウンメニューを使用して、情報を参照するクライアントの MAC アドレスを選択します。

「Status」タブの「Distributed Tunneling」サブタブ内の各項目について説明します。

項目	説明
Distributed Tunneling Status	このクライアントが L2 分配型トンネリングをサポートするネットワークに接続中かどうかを表示します。
Client Roam Status	クライアントがホーム AP 上にあるか、または別のアクセスポイントに移動して、トンネルを使用中であるかどうかを表示します。本欄には以下のいずれかの値が表示されます。 • Home - クライアントはトンネルを使用していません。 • Roaming - クライアントはトンネルを使用しています。
Home AP MAC Address	クライアント対するホーム AP の MAC アドレスを表示します。この値は、分配型トンネリングが有効なネットワークに接続するクライアントだけに意味があります。
Associated AP MAC Address	クライアントが分配型トンネリングプロトコルを通じてローミングしたアクセスポイントの MAC アドレスを表示します。

SSID Status タブ

1. 「SSID Status」タブをクリックすると、以下の画面が表示されます。

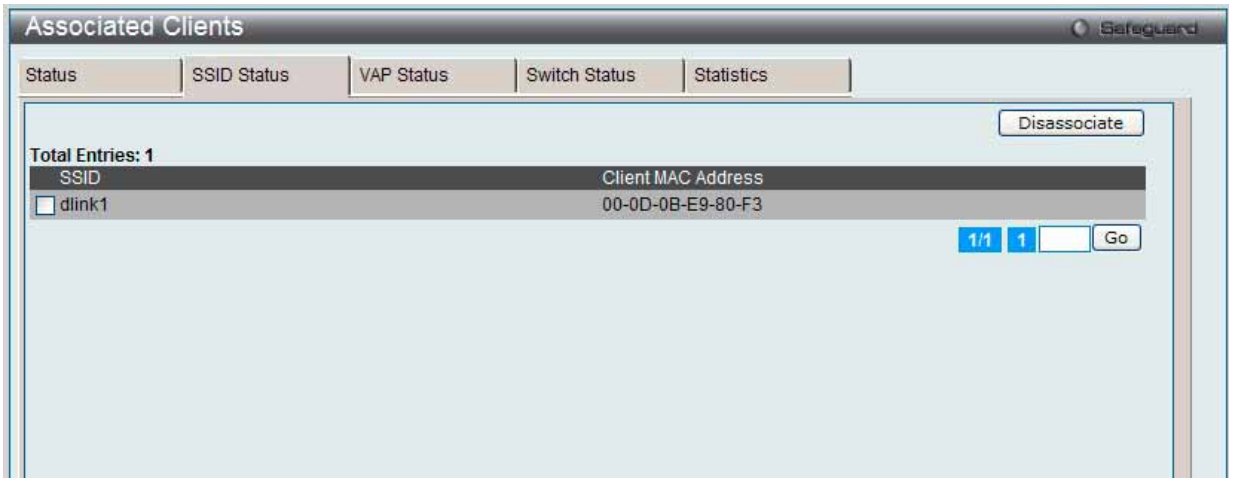


図 8.2-39　Associated Clients - SSID Status 画面

2. 各クライアントが接続しているネットワークの SSID を表示します。

項目	説明
SSID	クライアントが接続中のネットワーク。
Client MAC Address	クライアントステーションの MAC アドレス。

クライアントの切断
ボックスをチェックし、「Disassociate」ボタンをクリックして、管理するアクセスポイントからクライアントを切断します。

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

VAP Status タブ

1. 「VAP Status」タブをクリックすると、以下の画面が表示されます。

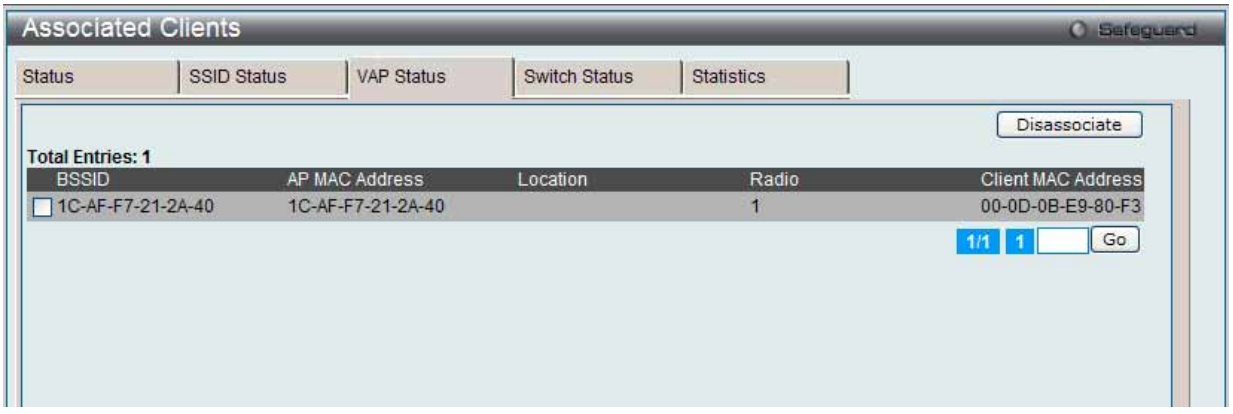


図 8.2-40　Associated Clients - VAP Status 画面

2. 以下の項目が表示されます。

項目	説明
BSSID	クライアントが接続中の VAP におけるアクセスポイントの MAC アドレス。
AP MAC Address	管理下にあるベースアクセスポイントのイーサネット MAC アドレス。
Location	管理下にあるアクセスポイントの場所。
Radio	クライアントが接続中のアクセスポイントの無線インタフェースと無線モードを表示します。
Client MAC Address	クライアントステーションの MAC アドレス。

クライアントの切断
ボックスをチェックし、「Disassociate」ボタンをクリックして、管理するアクセスポイントからクライアントを切断します。

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

Switch Status タブ

1. 「Switch Status」タブをクリックすると、以下の画面が表示されます。

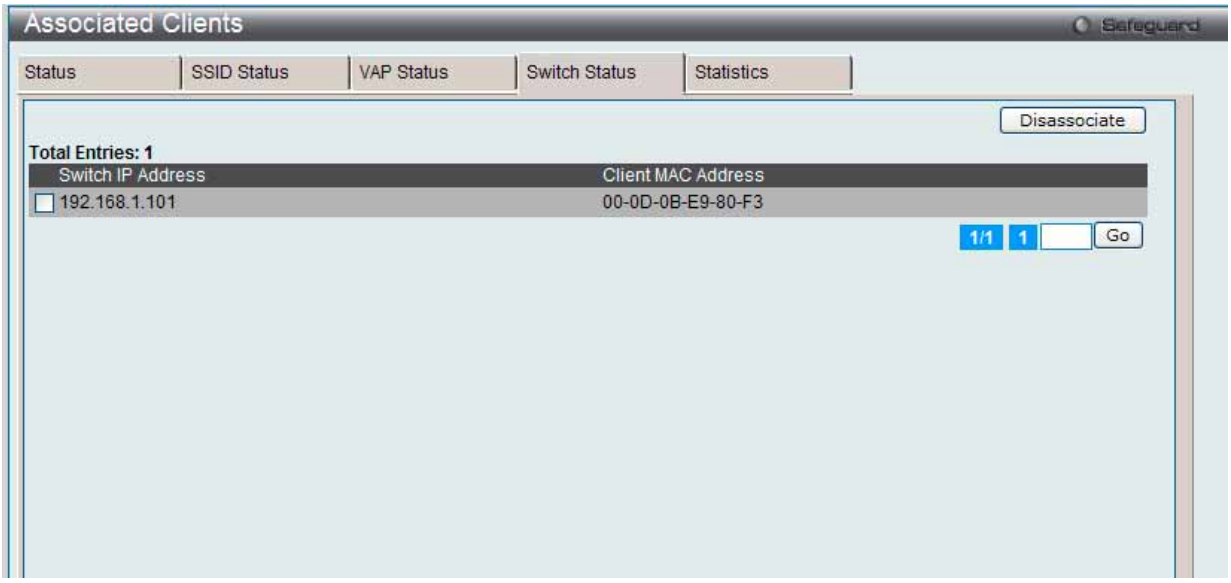


図 8.2-41　Associated Clients - Switch Status 画面

2. 以下の項目が表示されます。

項目	説明
Switch IP Address	クライアントが接続するアクセスポイントを管理するスイッチの IP アドレス。
Client MAC Address	接続する無線クライアントの MAC アドレス。

クライアントの切断

ボックスをチェックし、「Disassociate」ボタンをクリックして、管理するアクセスポイントからクライアントを切断します。

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

Statistics タブ

「Statistics」タブをクリックすると、以下の画面が表示されます。

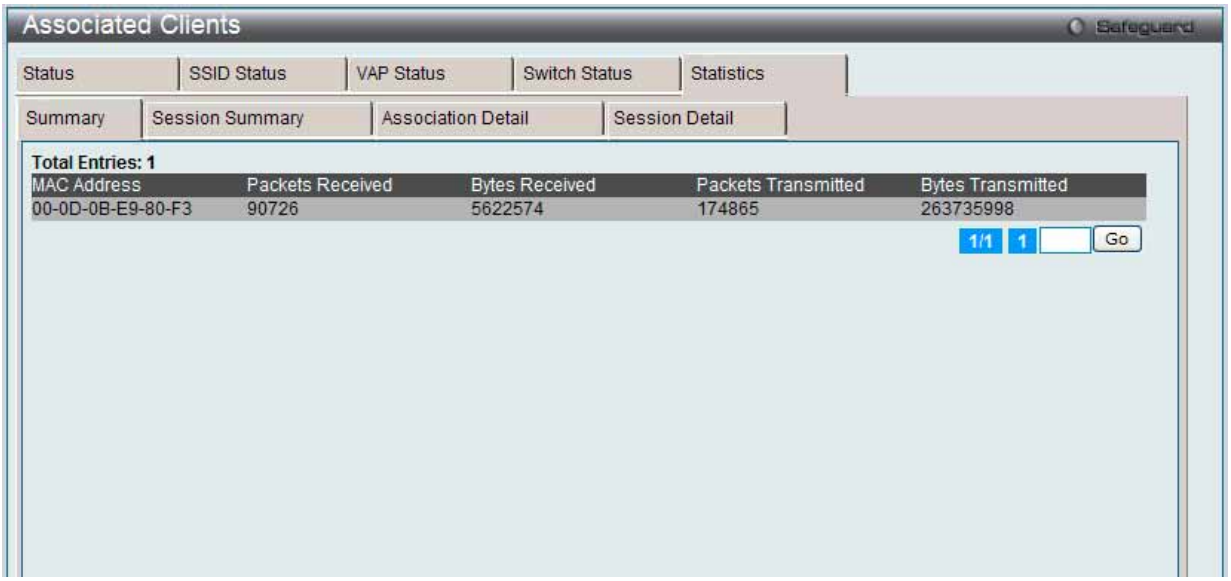


図 8.2-42　Associated Clients - Statistics - Summary 画面

Summary サブタブ

1. 「Statistics」タブの「Summary」サブタブをクリックします。

2. 以下の項目が表示されます。

項目	説明
MAC Address	クライアントステーションの MAC アドレス。
Packets Received	クライアントから受信したパケット数。
Bytes Received	クライアントから受信したデータ量（バイト）。
Packets Transmitted	クライアントに送信したパケット数
Bytes Transmitted	クライアントに送信したデータ量（バイト）。

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

Session Summary サブタブ

1. 「Statistics」タブの「Session Summary」サブタブをクリックすると、以下の画面が表示されます。

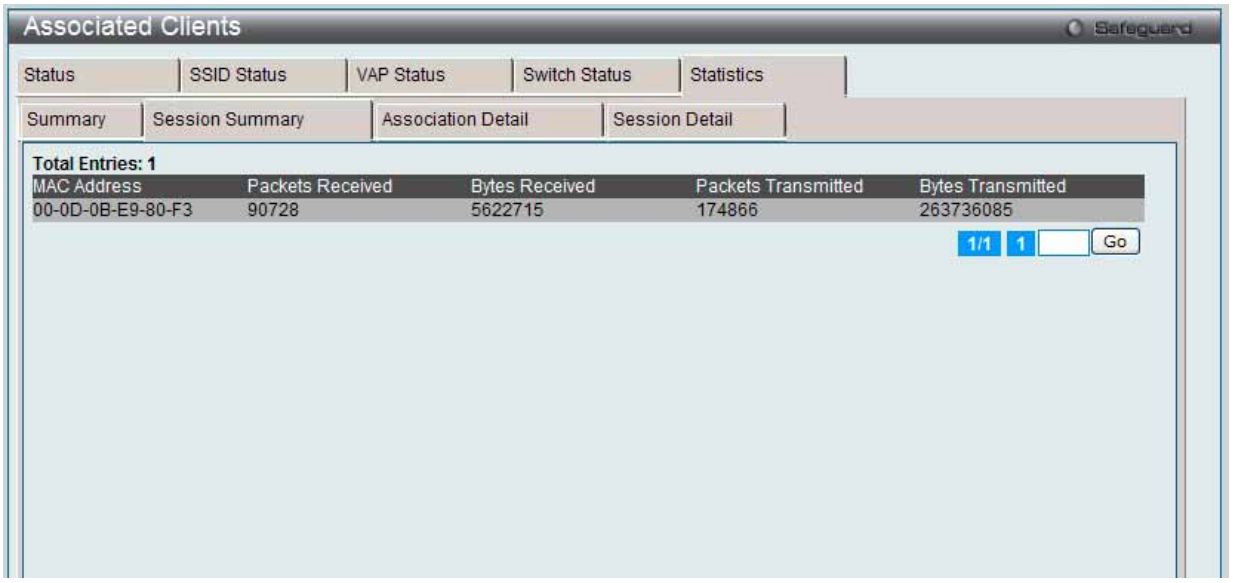


図 8.2-43　Associated Clients - Statistics - Session Summary 画面

あるクライアントがアクセスポイントから他のアクセスポイントへローミングする時、それが同じネットワーク内であれば、そのセッションは継続していると見なされ、セッションの統計情報は累積されます。クライアントが無線通信を終了した場合、またはスイッチ管理下のアクセスポイントの通信範囲を出た場合、そのセッションは終了したものと見なされます。

2. 以下の項目が表示されます。

項目	説明
MAC Address	クライアントステーションの MAC アドレス。
Packets Received	クライアントから受信した総パケット数。
Bytes Received	クライアントから受信した総データ量（バイト）。
Packets Transmitted	クライアントに送信した総パケット数。
Bytes Transmitted	クライアントに送信した総データ量（バイト）。

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

Association Detail サブタブ

無線クライアントが 1 台のアクセスポイントに接続中に送受信したトラフィックの情報を表示します。各クライアントは MAC アドレスで識別されます。

1. 「Statistics」タブの「Association Detail」サブタブをクリックすると、以下の画面が表示されます。

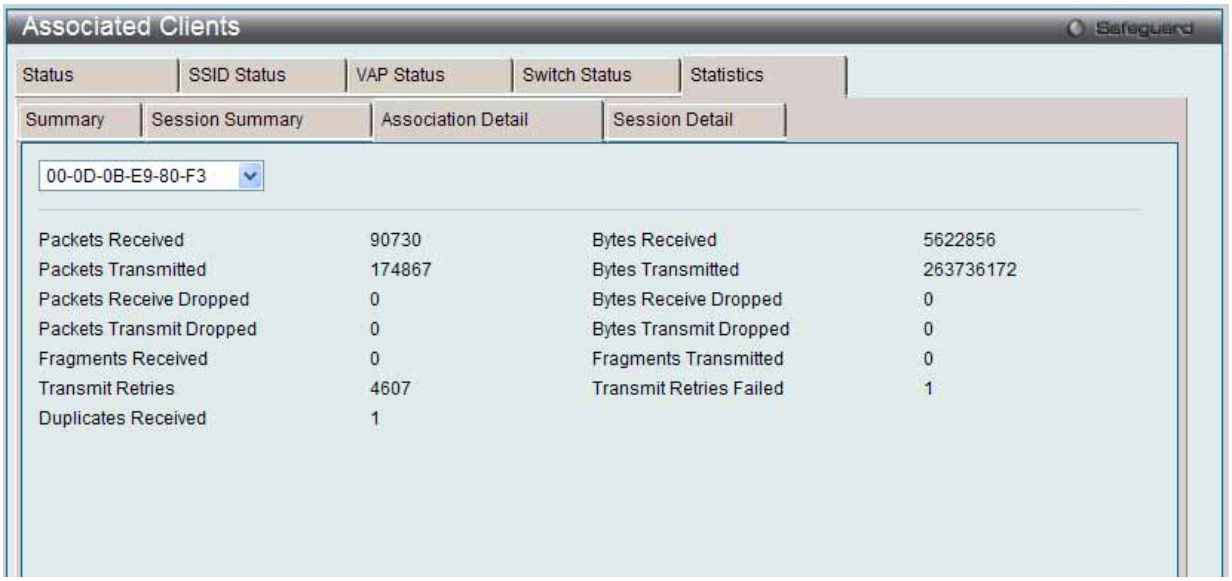


図 8.2-44　Associated Clients - Statistics - Association Detail 画面

2. プルダウンメニューを使用して、情報を参照するクライアントの MAC アドレスを選択します。

3. 以下の項目が表示されます。

項目	説明
MAC Address（メニュー）	クライアントの MAC アドレス。メニューで MAC アドレスを選択し、詳細情報を表示します。
Packets Received	クライアントから受信した総パケット数。
Bytes Received	クライアントから受信した総データ量（バイト）。
Packets Transmitted	クライアントに送信した総パケット数。
Bytes Transmitted	クライアントに送信した総データ量（バイト）。
Packets Received Dropped	クライアントから受信し、破棄されたパケット数。
Bytes Received Dropped	クライアントから受信し、破棄されたデータ量（バイト）。
Packets Transmit Dropped	クライアントから送信し、破棄されたパケット数。
Bytes Transmit Dropped	クライアントから受信し、破棄されたデータ量（バイト）。
Fragments Received	クライアントから受信したフラグメント化されたパケット総数。
Fragments Transmitted	クライアントに送信したフラグメント化されたパケット総数。
Transmit Retries	1 回以上のリトライの後、クライアントに送信成功した回数。
Transmit Retries Failed	1 回以上のリトライの後、クライアントに送信失敗した回数。
Duplicates Received	クライアントから受信した冗長パケットの総数。

Session Detail サブタブ

クライアントが、スイッチ管理下のアクセスポイントが共有する同一の WLAN ネットワークに接続している間に送受信するトラフィックに関する情報を表示します。各クライアントは MAC アドレスで識別されます。

1. 「Statistics」タブの「Session Detail」サブタブをクリックすると、以下の画面が表示されます。

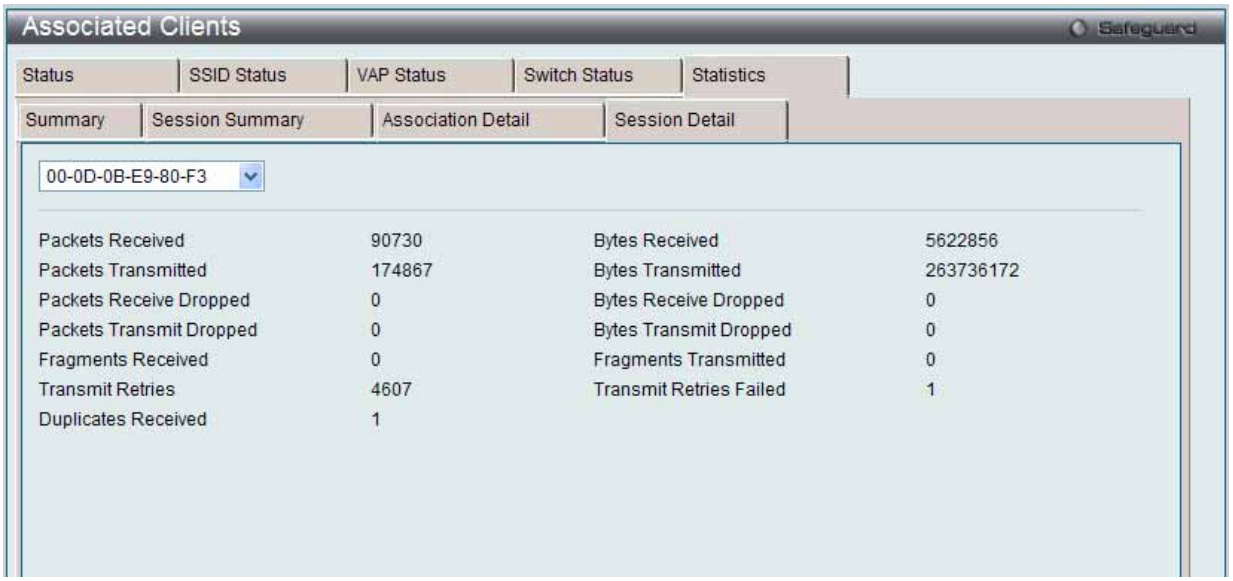


図 8.2-45　Associated Clients - Statistics - Session Detail 画面

2. プルダウンメニューを使用して、情報を参照するクライアントの MAC アドレスを選択します。

3. 以下の項目が表示されます。

項目	説明
MAC Address（メニュー）	クライアントの MAC アドレス。メニューで MAC アドレスを選択し、詳細情報を表示します。
Packets Received	クライアントから受信した総パケット数。
Bytes Received	クライアントから受信した総データ量（バイト）。
Packets Transmitted	クライアントに送信した総パケット数。
Bytes Transmitted	クライアントに送信した総データ量（バイト）。
Packets Received Dropped	クライアントから受信し、破棄されたパケット数。
Bytes Received Dropped	クライアントから受信し、破棄されたデータ量（バイト）。
Packets Transmit Dropped	クライアントから送信し、破棄されたパケット数。
Bytes Transmit Dropped	クライアントから受信し、破棄されたデータ量（バイト）。
Fragments Received	クライアントから受信したフラグメント化されたパケット総数。
Fragments Transmitted	クライアントに送信したフラグメント化されたパケット総数。
Transmit Retries	1 回以上のリトライの後、クライアントに送信成功した回数。
Transmit Retries Failed	1 回以上のリトライの後、クライアントに送信失敗した回数。
Duplicates Received	クライアントから受信した冗長パケットの総数。

Detected Clients（検出クライアント）

離脱して、システムに接続していないクライアントに関する情報などアクセスポイントで認証を行ったクライアントに関する情報を表示します。

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

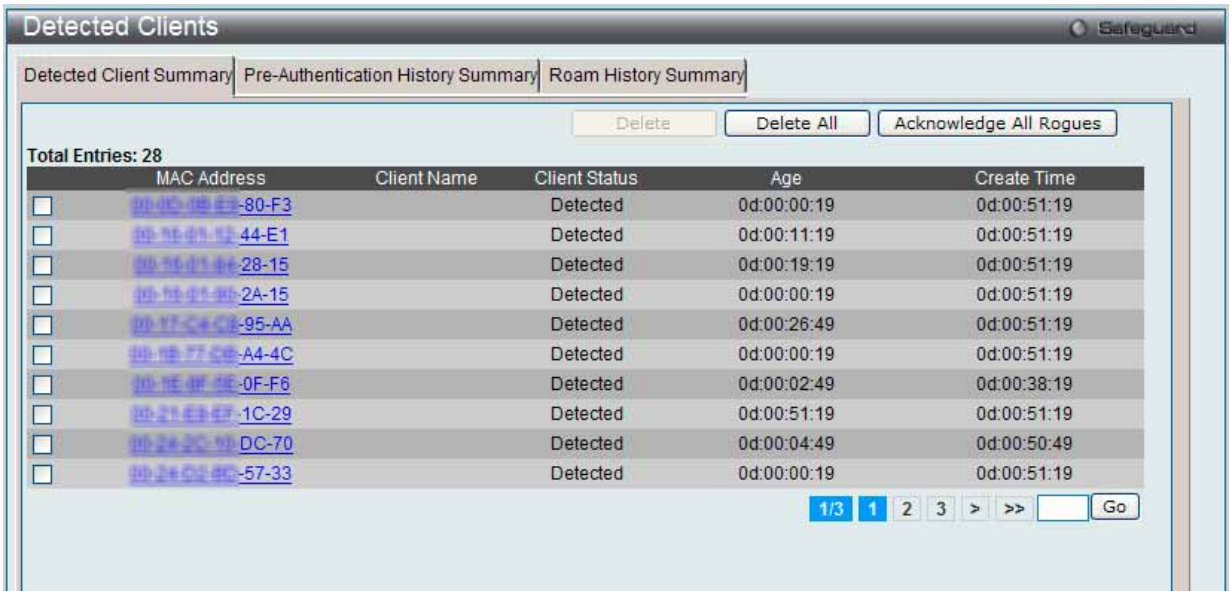


図 8.2-46　Detected Client - Summary 画面

Detected Client Summary タブ

以下の項目が表示されます。

項目	説明
MAC Address	クライアントの MAC アドレス。
Client Name	「Known Client」データベースからクライアント名を表示します。データベースにクライアントがない場合、このフィールドは空白です。
Client Status	クライアントの状態を表示します。以下のいずれかが表示されます。 • Authenticated - 無線クライアントは無線システムで認証済みです。 • Detected - 無線クライアントは無線システムで検出されていますが、セキュリティの脅威ではありません。 • Black-Listed - この MAC アドレスを持つクライアントは、MAC 認証経由で明確にアクセスを拒否されます。 • Rogue - 不正なアクセスポイントは脅威検出アルゴリズムの 1 つによって脅威として分類されます。
Age	クライアントのイベントを受信し、クライアントのデータベースエントリを更新してから経過した時間。
Create Time	クライアントを検出し、クライアントデータベースに最初に追加されてから経過した時間。

詳細情報の表示

「MAC Address」ハイパーリンクをクリックすることにより、クライアントの詳しい情報を参照します。

エントリの削除

対応するボックスをチェック後、「Delete」ボタンをクリックしてエントリを削除します。
「Delete All」ボタンをクリックして、すべてのエントリを削除します。

エントリの状態変更

「Acknowledge All Rogues」ボタンをクリックして、すべてのクライアントの不正状態をクリアします。

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

クライアントの詳細情報の表示

「MAC Address」ハイパーリンクをクリックすると、以下の画面が表示されます。

Detected Client Status サブタブ

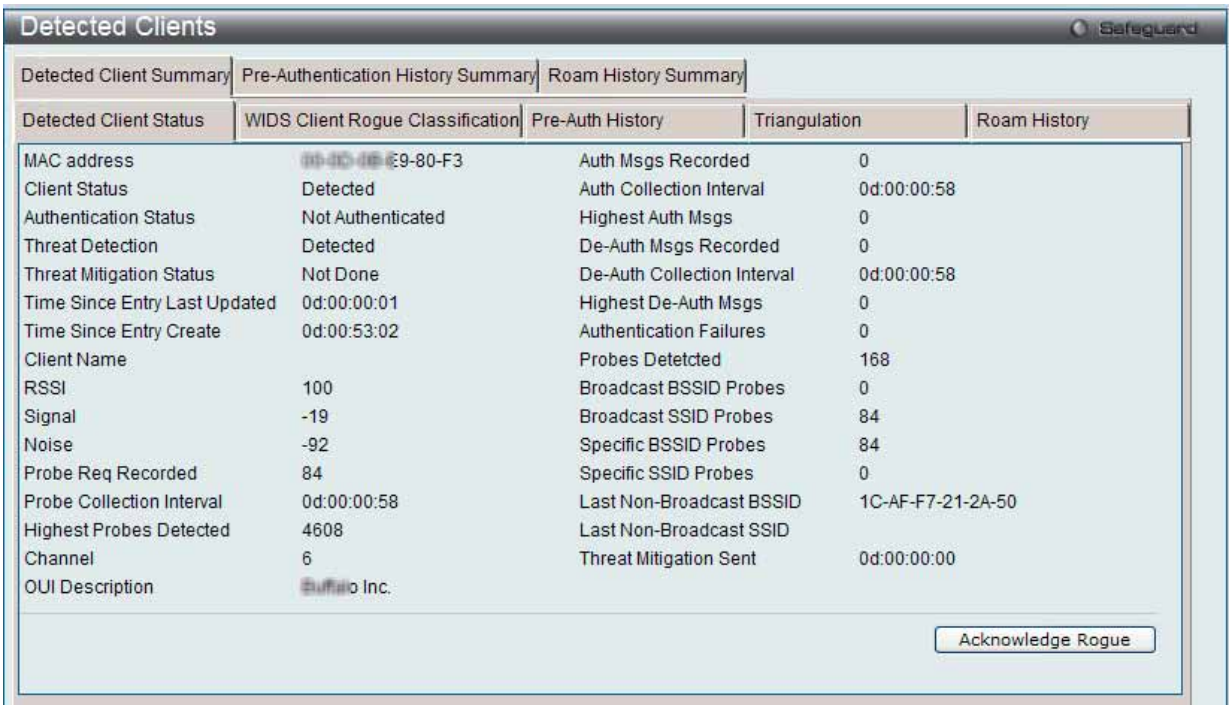


図 8.2-47　Detected Client Summary - Detected Client Status 画面

以下の項目が表示されます。

項目	説明
MAC Address	クライアントの MAC アドレス。
Client Status	クライアントの状態を表示します。以下のいずれかが表示されます。 • Authenticated - 無線クライアントは無線システムで認証済みですが、Rogue（不正）ではありません。 • Detected - クライアントは検出されていますが、未認証です。また、Rogue ではなく、Known Clients データベースで未検出です。 • Known - クライアントは、Known Clients データベースで検出済みですが、未認証です。 • Black-Listed - クライアントは、システムに接続しようとしましたが、MAC 認証で拒否されました。 • Rogue - クライアントは使用可能な脅威テストでエラーになりました。
Authentication Status	このクライアントの認証状態を表示します。 注意 「Client Status」が「Rogue」であっても、本ステータスがまだ「Authenticated」であることもあります。
Threat Detection	脅威検出テストの 1 つがこのクライアントに始動したかどうかを表示します。テストが無効にされると、クライアントは「Rogue」としてマークされませんが、脅威が引き起こされた理由を調査することはできます。
Threat Mitigation Status	このクライアントに脅威の軽減を行ったどうかを表示します。
Time Since Entry Last Updated	クライアントのイベントを受信し、クライアントのデータベースエントリを更新してから経過した時間。
Time Since Entry Create	クライアントを検出し、クライアントデータベースに最初に追加されてから経過した時間。
Client Name	「Known Client」データベースからクライアント名を表示します。データベースにクライアントがない場合、このフィールドは空白です。
RSSI	クライアントが管理下のアクセスポイントに認証されると、本項目はクライアントを認証するアクセスポイントが報告した最後の RSSI 値を表示します。RSSI の範囲は 1-100% です。0 の値は、アクセスポイントが検出されないことを意味します。
Signal	クライアントを認証する管理下のアクセスポイントが報告した最後の信号強度。有効な範囲は -128 ～ 128 dBm です。
Noise	クライアントを認証する管理下のアクセスポイントが報告した最後のチャンネルノイズ。有効な範囲は -128 ～ 128 dBm です。
Probe Req Recorded	Probe Collection Interval の間、記録したプローブリクエスト数。
Probe Collection Interval	各 Probe Collection Interval（プローブ収集間隔）の経過時間。プローブ収集は、クライアントが脅威であるかどうかをスイッチが判断するために役立ちます。
Highest Probes Detected	スイッチが Probe Collection Interval（プローブ収集間隔）に検出したプローブの最大数を表示します。
Channel	クライアントが使用しているチャンネルを表示します。

項目	説明
OUI Description	無線クライアントの Organization Unique Identifier（メーカ識別子）を表示します。
Auth Msgs Recorded	「Auth Collection Interval」に記録した IEEE 802.11 Authentication メッセージ数を表示します。
Auth Collection Interval	各 Authentication Collection 期間の経過時間を表示します。認証収集は、クライアントが脅威であるかどうかをスイッチが判断するために役立ちます。
Highest Auth Msgs	スイッチが認証収集期間に検出した Authentication メッセージの最大数を表示します。
De-Auth Msgs Recorded	認証収集期間に記録した IEEE 802.11 De-Authentication メッセージ数を表示します。
De-Auth Collection Interval	各認証解除の収集期間の経過時間を参照します。De-Authentication の収集は、クライアントが脅威であるかどうかをスイッチが判断するために役立ちます。
Highest De-Authe Msgs	スイッチが認証解除の収集期間に検出した De-Authentication メッセージの最大数を表示します。
Authentication Failures	クライアントに検出された 802.1X 認証エラー数を表示します。
Probes Detected	最後の RF スキャンで検出したプローブ数を表示します。
Broadcast BSSID Probes	最後の RF スキャンで検出したブロードキャスト BSSID に対するプローブ数を表示します。
Broadcast SSID Probes	最後の RF スキャンで検出したブロードキャスト SSID に対するプローブ数を表示します。
Specific BSSID Probes	最後の RF スキャンで検出した特定の BSSID に対するプローブ数を表示します。
Specific SSID Probes	最後の RF スキャンで検出した特定の SSID に対するプローブ数を表示します。
Last Non-Broadcast BSSID	RF スキャンで検出した最後のノンブロードキャスト BSSID を表示します。これは MAC アドレスです。
Last Non-Broadcast SSID	RF スキャンで検出した最後のノンブロードキャスト SSID を表示します。
Threat Mitigation Sent	このクライアントに脅威の軽減を行ったどうかを表示します。

「Acknowledge Rogues」ボタンをクリックして、クライアントの不正状態をクリアします。

WIDS Client Rogue Classification サブタブ

1. 「Detected Client Summary」タブの「WIDS Client Rogue Classification」サブタブをクリックすると、以下の画面が表示されます。

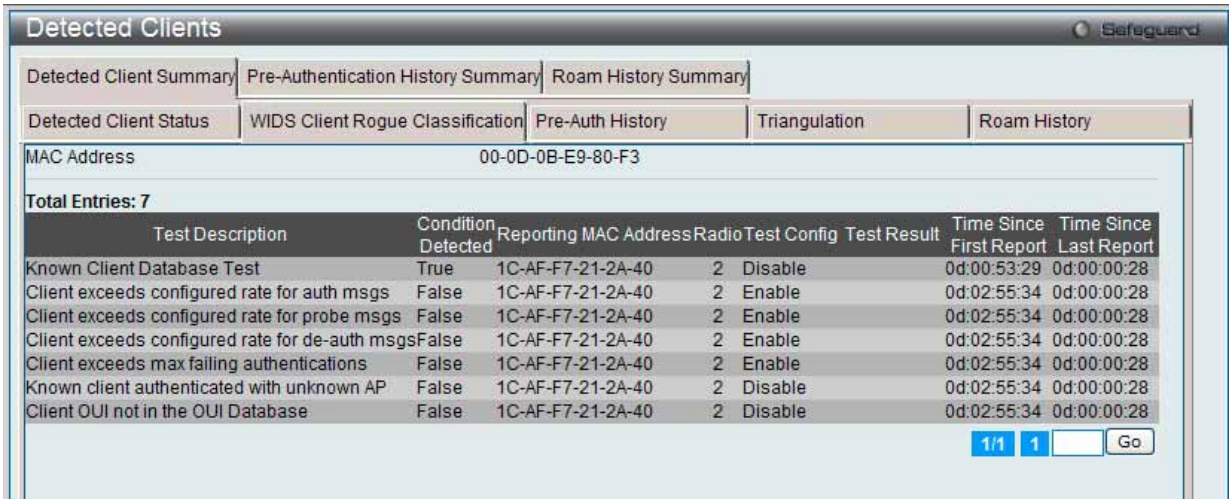


図 8.2-48　Detected Client Summary - WIDS Client Rogue Classification 画面

2. 以下の項目が表示されます。

項目	説明
MAC Address	検出されたアクセスポイントの MAC アドレス。
Test Description	実行されたテストを表示します。以下のテストがあります。 • Known Clients database Test • Client exceeds configured rate for auth msgs • Client exceeds configured reate for probe msgs • Client exceeds configured rate for de-auth msgs • Client exceeds max failing authentications • Known client authenticated with unknown AP • Client OUI not in the OUI Database
Condition Detection	テストの結果が正しいかどうかを表示します。
Reporting MAC Address	テスト結果を報告したアクセスポイントの MAC アドレスを表示します。
Radio	報告されたアクセスポイントのどの物理無線帯域がテスト結果の原因となったかを表示します。
Test Config	このテストが「Rogue」（不正）を報告するように設定されているかどうかを表示します。不正として確実に結果を報告するために、各テストをグローバルに「Enabled」（有効）または「Disabled」（無効）にします。
Test Result	本のテストが、デバイスを「Rogue」（不正）であると報告したかどうかを表示します。デバイスはこのモードで動作を許可されているため、いくつかの場合、テストは肯定的な結果を報告し、有効であり、「Rogue」（不正）なものとしてレポートしないかもしれません。
Time Since First Report	このテストが最初にこの条件を検出した時期を示すタイムスタンプ。
Time Since Last Report	このテストが最後にこの条件を検出した時期を示すタイムスタンプ。

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

Pre-Auth History サブタブ

1. 「Detected Client Summary」タブの「Pre-Auth History」サブタブをクリックすると、以下の画面が表示されます。

図 8.2-49　Detected Client Summary - Pre-Auth History 画面

2. 以下の項目が表示されます。

項目	説明
MAC Address	クライアントの MAC アドレス。
AP MAC Address	クライアントを事前認証する管理下のアクセスポイントの MAC アドレス。
Radio Interface Number	クライアントが認証される無線インタフェースの番号（Radio1 または Radio2）。
VAP MAC Address	クライアントがローミングを行った VAP の MAC アドレス。
SSID	VAP が使用される SSID 名。
Age	ヒストリエントリが追加されてから経過した時間。
User Name	802.1X で認証されたクライアントのユーザ名を表示します。
Pre-Authentication Status	クライアント認証の結果を表示します。 • Success - 成功 • Failure - 失敗

Triangulation サブタブ

1. 「Detected Client Summary」タブの「Triangulation」サブタブをクリックすると、以下の画面が表示されます。

図 8.2-50　Detected Client Summary - Triangulation 画面

2. 以下の項目が表示されます。

項目	説明
MAC Address	クライアントの MAC アドレス。
AP Function	クライアントを検出した無線インタフェースのモード（Sentry または Non-Sentry）を表示します。 • Non-Sentry - クライアントを検出した無線帯域は、Sentry モードで設定されません。これは、無線インタフェースが、無線クライアントからの接続を受け入れ、トラフィックの送受信を行うことができることを意味します。 • Sentry - クライアントを検出した無線帯域が Sentry モードで設定されます。Sentry AP を配置するネットワークまたは無線インタフェースは、ネットワーク上のデバイスをより迅速に検出して、より徹底的なセキュリティ分析を行うことができます。
AP MAC Address	クライアントを検出した管理下のアクセスポイントの MAC アドレス。
Radio	クライアントが認証される無線インタフェースの番号 (Radio1 または Radio2)。
RSSI (%)	Non-Sentry AP の受信信号強度 (%)。範囲は 0-100 です。最大値は 100 です。0 の値はクライアントが検出されないことを示します。
Signal (dBm)	受信信号強度 (dBm)。有効な範囲は -127 ～ 127(dBm) です。しかし、現実的な範囲は -95 ～ -10 です。
Noise (dBm)	Non-Sentry AP がチャンネルについて報告したノイズ。有効な範囲は -127 ～ 127(dBm) です。
Age	このアクセスポイントが信号を検出してから経過した時間。

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

Roam History サブタブ

1. 「Detected Client Summary」タブの「Roam History」サブタブをクリックすると、以下の画面が表示されます。

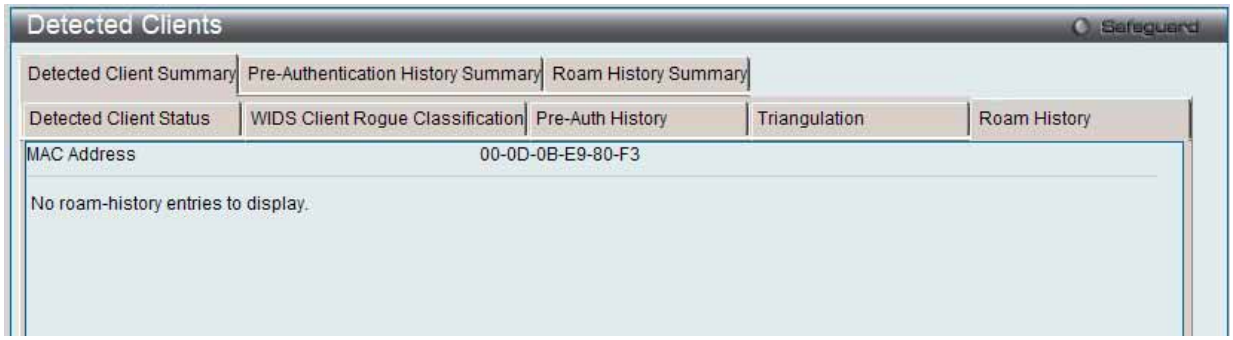


図 8.2-51　Detected Client Summary - Roam History 画面

2. 以下の項目が表示されます。

項目	説明
MAC Address	検出されたクライアントの MAC アドレス。
AP MAC Address	クライアントを認証した管理下のアクセスポイントの MAC アドレス。
Radio Interface Number	クライアントが認証される無線インタフェースの番号。
VAP MAC Address	クライアントがローミングを行った VAP の MAC アドレス。
SSID	VAP が使用される SSID 名。
New Authentication	ヒストリエントリが新しい認証またはローミングイベントを示しているかどうか示すフラグ。
Age	ヒストリエントリが追加されてから経過した時間。

Pre-Authentication History Summary タブ

1. 「Pre-Authentication History Summary」タブをクリックすると、以下の画面が表示されます。

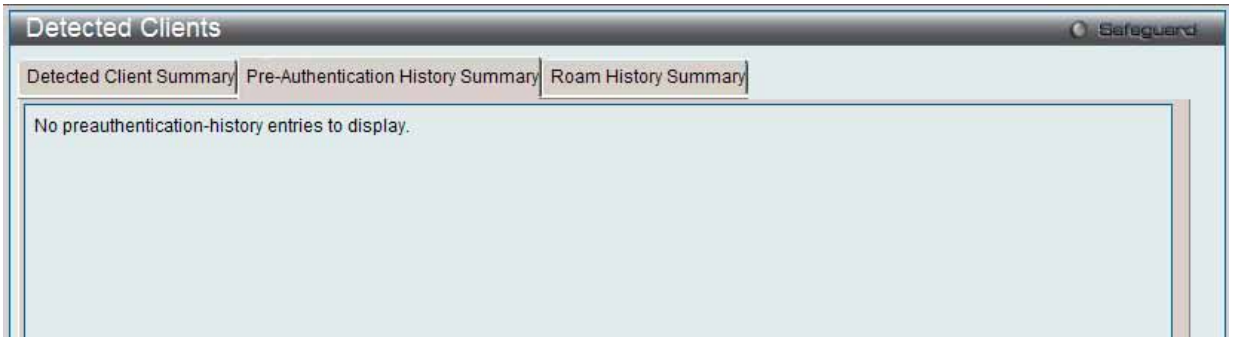


図 8.2-52　Detected Client – Pre-Authentication History Summary 画面

2. 以下の項目が表示されます。

項目	説明
MAC Address	検出されたクライアントの MAC アドレス。
AP MAC Address	クライアントを事前認証する管理下のアクセスポイントの MAC アドレス。各クライアントに最大 10 個の事前認証のヒストリを表示します。

Roam History Summary タブ

1. 「Roam History Summary」タブをクリックすると、以下の画面が表示されます。

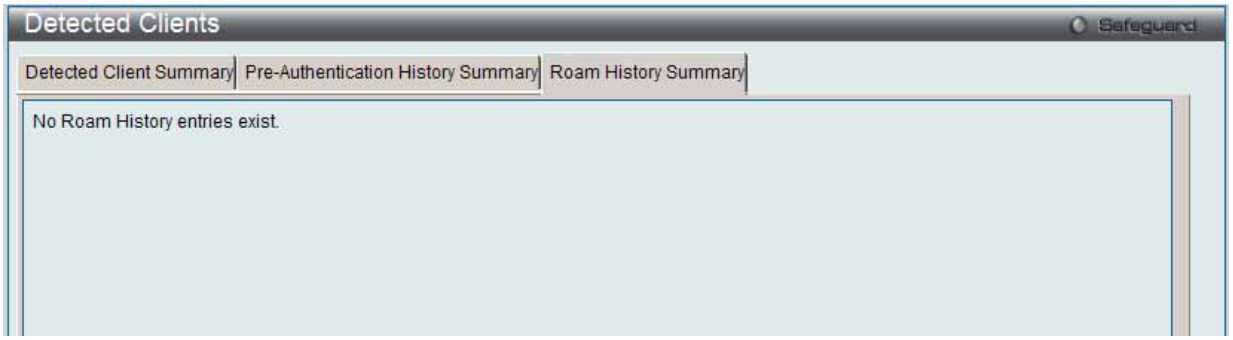


図 8.2-53　Detected Client – Detected Client Roam History Summary 画面

2. 以下の項目が表示されます。

項目	説明
MAC Address	検出されたクライアントの MAC アドレス。
AP MAC Address	クライアントを認証した管理下のアクセスポイントの MAC アドレス。クライアントがローミングし、認証を行った最後から 10 個分のアクセスポイントの MAC アドレスを表示します。

Ad Hoc Clients（アドホッククライアント）

Ad Hoc クライアントを表示します。

アドホッククライアントとは、アクセスポイントに接続しているクライアントを経由して WLAN に接続するクライアントです。アドホッククライアントは、直接アクセスポイントと通信を行いません。アドホックネットワークは、RF 帯域を消費し、セキュリティ上のリスクを招く可能性を含んでいるため、特に注意が必要です。

1. **Monitoring > Client > Ad Hoc Clients** の順にメニューをクリックし、以下の画面を表示します。

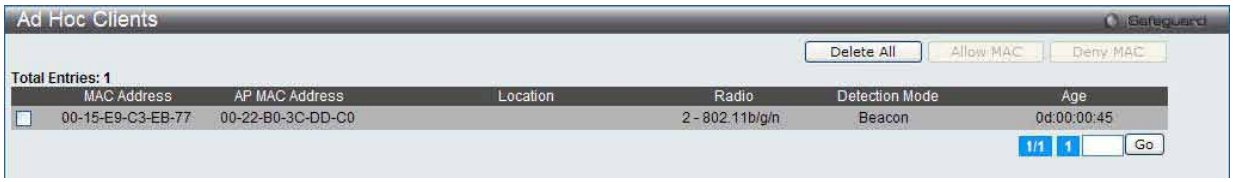


図 8.2-54　Ad Hoc Clients 画面

2. 以下の項目が表示されます。

項目	説明
MAC Address	クライアントの MAC アドレス。「Detection Mode」が「Beacon」の場合、「RF Scan」データベースや「Neighbor AP List」には、クライアントはアクセスポイントとして表示されます。「Detection Mode」が「Data」の場合、クライアント情報は「Neighbor Client List」に表示されます。
AP MAC Address	クライアントを検出した管理対象アクセスポイントのベースイーサネット MAC アドレス。
Location	管理下のアクセスポイントの設置場所の説明。
Radio	アドホッククライアントが検出された無線帯域とその設定モード。
Detection Mode	アドホックデバイスの検出方式。有効な値は「Beacon Frame」または「Data」です。
Age	アドホックネットワークが最後に検出されてから経過した時間。

アドホッククライアントの許可 / 拒否

MAC アドレスを追加するボックスをチェックし、「Allow MAC」ボタンをクリックします。これによって、初期アクションは「Known Clients」画面に対する許可となり、クライアントは WLAN へのアクセスを許可されます。

MAC アドレスを追加するボックスをチェックし、「Deny MAC」ボタンをクリックします。これによって、初期アクションは「Known Clients」画面に対する拒否となり、アドホッククライアントは WLAN へのアクセスをブロックされます。

エントリの削除

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

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

QoS（QoS 設定）

Access Control Lists（アクセスコントロールリスト）

IP Access Control Lists（IP アクセスコントロールリスト）

IP ACL（Access Control Lists）を表示します。

Monitoring > QoS > Access Control Lists > IP Access Control 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 8.2-55　IP Access Control Lists 画面

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

「Type Select」プルダウンメニューを使用して、IP ACL の各種タイプの表示します。
「Rules ID」ハイパーリンクをクリックして、ルールに関する詳細情報を表示します。

ルールに関する詳細情報の表示
「Rules ID」ハイパーリンクをクリックして、以下の画面を表示します。

Standard IP ACL

図 8.2-56　IP Access Control Lists - Rule ID 画面（Standard IP ACL）

以下の項目が表示されます。

項目	説明
IP ACL ID	IP ACL の ID。
Rule ID	IP ACL に定義される各ルールの識別子。
Action	各ルールに関連するアクション。「Permit」（許可）または「Deny」（拒否）です。
Match Every	すべてのパケットに対する本アクセスリストの適用の有無を表示します。 • True - 適用する。 • False - 適用しない。
Source IP Address	本ルールの送信元 IP アドレス。
Source IP Mask	本ルールの送信元 IP マスク。

「<<Back」をボタンをクリックして前のページに戻ります。

Extended IP ACL

図 8.2-57　IP Access Control Lists - Rule ID 画面 (Extended IP ACL)

以下の項目が表示されます。

項目	説明
IP ACL Name	IP ACL の ID。
Rule ID	IP ACL に定義される各ルールの識別子。
Action	各ルールに関連するアクション。「Permit」（許可）または「Deny」（拒否）です。
Match Every	すべてのパケットに対する本アクセスリストの適用の有無を表示します。 • True - 適用する。 • False - 適用しない。
Protocol	本ルールをフィルタするプロトコル。
Source IP Address	本ルールの送信元 IP アドレス。
Source IP Mask	本ルールの送信元 IP マスク。
Source L4 Port	本ルールの送信元ポート。
Destination IP Address	本ルールの送信先 IP アドレス。
Destination IP Mask	本ルールの送信先 IP マスク。
Destination L4 Port	本ルールの送信先ポート。
Service Type	拡張 IP ACL ルールに対して 3 つの Match 条件（IP DSCP、IP Precedence または IP ToS）のうち 1 つを表示します。

「<<Back」をボタンをクリックして前のページに戻ります。

Named IP ACL

図 8.2-58　IP Access Control Lists - Rule ID 画面 (Named IP ACL)

以下の項目が表示されます。

項目	説明
IP ACL Name	IP ACL の名前。
Rule ID	IP ACL に定義される各ルールの識別子。
Action	各ルールに関連するアクション。「Permit」（許可）または「Deny」（拒否）です。
Match Every	すべてのパケットに対する本アクセスリストの適用の有無を表示します。 • True - 適用する。 • False - 適用しない。
Protocol	本ルールをフィルタするプロトコル。
Source IP Address	本ルールの送信元 IP アドレス。
Source IP Mask	本ルールの送信元 IP マスク。
Source L4 Port	本ルールの送信元ポート。
Destination IP Address	本ルールの送信先 IP アドレス。
Destination L4 Port	本ルールの送信先 IP マスク。
Service Type	拡張 IP ACL ルールに対して 3 つの Match 条件 (IP DSCP、IP Precedence または IP ToS) のうち 1 つを表示します。

「<<Back」をボタンをクリックして前のページに戻ります。

IPv6 Access Control Lists（IPv6 アクセスコントロールリスト）

IPv6 ACL（Access Control Lists）を表示します。

Monitoring > QoS > Access Control Lists > IPv6 Access Control 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 8.2-59　IPv6 Access Control Lists 画面

「Rules ID」ハイパーリンクをクリックして、ルールに関する詳細情報を表示します。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、指定ページへ移動します。

ルールに関する詳細情報の表示

1. 「Rules ID」ハイパーリンクをクリックして、以下の画面を表示します。

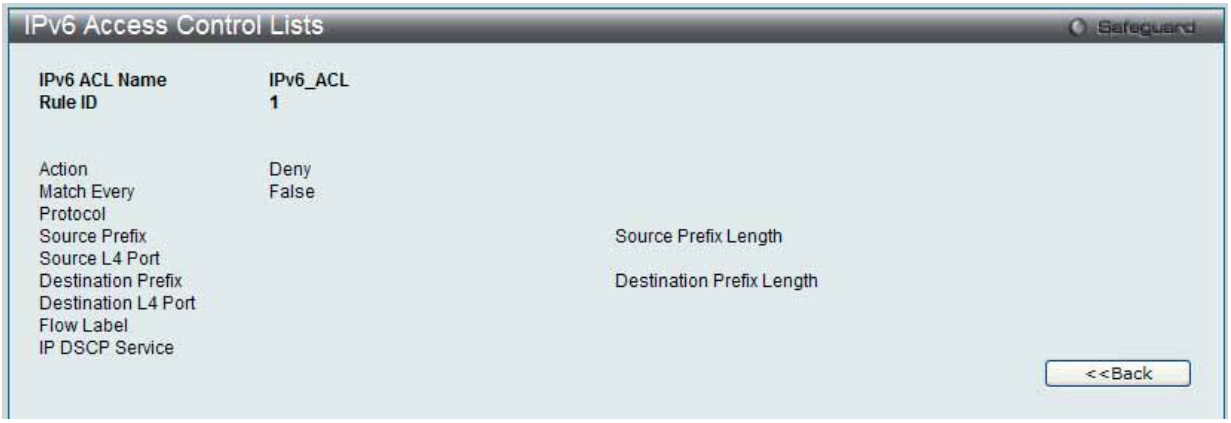


図 8.2-60　IPv6 Access Control Lists - Rule ID 画面

2. 以下の項目が表示されます。

項目	説明
IPv6 ACL Name	IPv6ACL 識別子。
Rule ID	IPv6 ACL 内に定義されている各ルール番号の識別子。
Action	各ルールに関連するアクション。「Permit」（許可）または「Deny」（拒否）です。
Match Every	すべてのパケットに対する本アクセスリストの適用の有無を表示します。 • True - 適用する。 • False - 適用しない。
Protocol	本ルールをフィルタするプロトコル。
Source Prefix	本ルールの送信元 IPv6 アドレス。
Source L4 Port	本ルールの送信元ポート。
Destination Prefix	本ルールの送信先 IPv6 アドレス。
Destination L4 Port	本ルールの送信先ポート。
Flow Label	IPv6 フローラベルの値。
IP DSCP Service	DSCP キーワードの値。

「<<Back」をボタンをクリックして前のページに戻ります。

MAC Access Control Lists（MAC アクセスコントロールリスト）

MAC ACL(Access Control Lists) を表示します。

Monitoring > QoS > Access Control Lists > MAC Access Control 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 8.2-61　MAC Access Control Lists 画面

「Rules ID」ハイパーリンクをクリックして、ルールに関する詳細情報を表示します。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、指定ページへ移動します。

ルールに関する詳細情報の表示

1. 「Rules ID」ハイパーリンクをクリックして、以下の画面を表示します。

図 8.2-62　MAC Access Control Lists - Rule ID 画面

2. 以下の項目が表示されます。

項目	説明
MAC ACL Name	MAC ACL の識別子。
Rule ID	IPv6 ACL 内に定義されている各ルール番号の識別子。
Action	各ルールに関連するアクション。「Permit」（許可）または「Deny」（拒否）です。
Match Every	すべてのパケットに対する本アクセスリストの適用の有無を表示します。 • True - 適用する。 • False - 適用しない。
CoS	本ルールの 802.1p ユーザプライオリティを表示します。
Destination MAC	本ルールの送信先 MAC アドレス。
Destination MAC Mask	Ethernet フレームに対して比較する送信先 MAC のビットを表示します。
EtherType Key	本ルールの「Ethertype」キーワードまたはカスタム値。
Source MAC	本ルールの送信元 IP アドレス。
Source MAC Mask	Ethernet フレームに対して比較する送信元 MAC のビットを表示します。
VLAN	本ルールの VLAN 識別子の値。

「<<Back」をボタンをクリックして前のページに戻ります。

Differentiated Services（DiffServ: ディフサーブ）

Class Summary（クラスのサマリ）

DiffServ クラスを表示します。

1. **Monitoring > QoS > Differentiated Services > Class Summary** の順にメニューをクリックし、以下の画面を表示します。

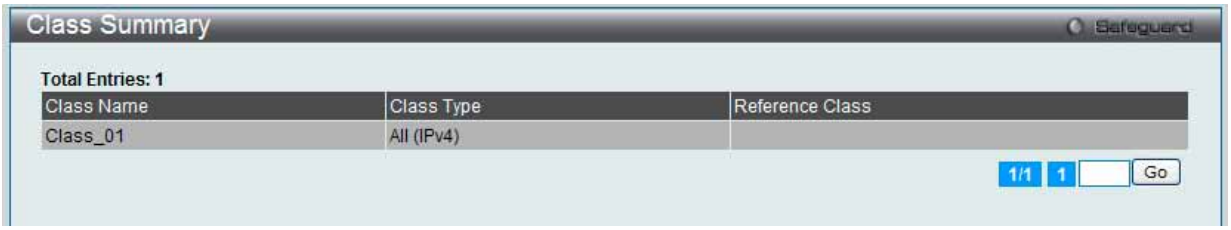


図 8.2-63　Class Summary 画面

2. 以下の項目が表示されます。

項目	説明
Class Name	クラス名。
Class Type	「All」クラスタイプは、クラスに定義されたすべての一致基準が同時に評価され、すべてのクラスが正確に一致する必要があることを意味します。
Reference Class	条件と照合する既存の DiffServ クラス名は特定のクラス定義によって参照されます。

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

Policy Summary（ポリシーサマリ）

DiffServ ポリシーを表示します。

1. **Monitoring > QoS > Differentiated Services > Policy Summary** の順にメニューをクリックし、以下の画面を表示します :

図 8.2-64　Policy Summary 画面

2. 以下の項目が表示されます。

項目	説明
Policy Name	ポリシー名。
Policy Type	ポリシータイプ。
Member Classes	このポリシーに割り当てられているすべてのクラス名リスト。

詳細情報の表示

「Member Classes」ハイパーリンクをクリックして、照合されるクラスに関する詳細情報を表示します。

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

クラスに関する詳細情報の表示

1. 「Member Classes」ハイパーリンクをクリックすると、以下の画面が表示されます。

図 8.2-65　Policy Summary - Class Configuration 画面

2. 以下の項目が表示されます。

項目	説明
Class Name	クラス名。
Class Type	「All」クラスタイプは、クラスに定義されたすべての一致基準が同時に評価され、すべてのクラスが正確に一致する必要があることを意味します。
Class Layer 3 Protocol	このクラスのレイヤ 3 プロトコル（「IPv4」および「IPv6」）。
Match Criteria	本欄は設定されている場合にだけユーザが入力した順に表示されます。また、クラスタイプに従って、本欄は検証されます。次の項目が表示されます。: Destination IP Address、Destination Layer 4 Port、Destination MAC Address、Ethertype、Source MAC Address、VLAN、Class of Service、Any、IP DSCP、IP Precedence、IP TOS、Protocol Keyword、Reference Class、Source IP Address、および Source Layer 4 Port
Values	照合基準の値。

「<<Back」をボタンをクリックして前のページに戻ります。

Policy Attribute Summary（ポリシー属性のサマリ）

DiffServ ポリシーの属性を表示します。

1. **Monitoring > QoS > Differentiated Services > Policy Attribute Summary** の順にメニューをクリックし、以下の画面を表示します。

図 8.2-66　Policy Attribute Summary 画面

2. 以下の項目が表示されます。

項目	説明
Policy Name	ポリシー名。
Policy Type	ポリシータイプ。
Class Name	このクラスの名前。
Attribute	ポリシークラスインスタンスに関連付けられている属性を表示します。
Attribute Details	割り当てられている属性の設定値を表示します。

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

8.3 Administration（アクセスポイントの設定）

スイッチと接続する D-Link アクセスポイントを認定後、スイッチはそのアクセスポイントの管理を行います。認定の前または後に、すべてのアクセスポイントの設定をスイッチから直接行うことができます。D-Link 統合アクセスシステムは D-Link Wireless AP Protocol（DWAPP）を利用して、AP の検出、設定、管理およびモニタを行います。ここでは、アクセスポイントの設定と、D-Link 統合スイッチによるアクセスポイントの管理方法について説明します。

本章は、以下の項で構成されています。

項目	説明	参照ページ
Basic Setup（基本設定）	D-Link 統合スイッチに設定するアクセスポイントプロファイル、無線ネットワーク、およびローカルアクセスポイント・データベースについて説明します。次のメニューがあります。 Global タブ（無線グローバル基本設定）、Discovery タブ（無線ディスカバリの設定）、Profile タブ（プロファイル）、Radio タブ（周波数帯域）、SSID タブ（SSID 設定）、Valid AP タブ（Valid アクセスポイントの設定）、OUI タブ（OUI データベース）	452
AP Management（アクセスポイント管理）	無線インタフェースを設定します。次のメニューがあります。 AP Reboot（アクセスポイント再起動）、RF Management（RF 管理）、Software Downloads（アクセスポイントソフトウェアのダウンロード）、Advanced Settings（管理アクセスポイントの詳細設定）、AP Provisioning（アクセスポイントプロビジョニング）	464
Advanced Configuration（高度な設定）	各アクセスポイントにチャンネルや RF 信号送信電力レベルを指定します。また、AP モード、ローカル認証パスワード、アクセスポイントが使用するプロファイルを設定します。次のメニューがあります。 Global（グローバル設定）、Networks（ネットワーク）、AP Profiles（AP プロファイル）、Peer Switch（ピアスイッチ）、WIDS Security（WIDS セキュリティ）、Clients（クライアント）、Switch Provisioning（スイッチのプロビジョニング）	473

Basic Setup（基本設定）

無線の基本的な設定を行います。

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

- 無線グローバル基本設定（Global タブ）
- 無線ディスカバリの設定（Discovery タブ）
- プロファイル（Profile タブ）
- 周波数帯域（Radio タブ）
- SSID 設定（SSID Configuration タブ）
- Valid アクセスポイントの設定（Valid AP タブ）
- ローカルの OUI データベース概要（OUI タブ）

Global タブ（無線グローバル基本設定）

統合スイッチがアクセスポイントの検出と管理を行うためには、WLAN スイッチ機能とその操作ステータスを共に有効にする必要があります。

スイッチのユーザインタフェースに接続する場合、スイッチに正しい国コードが設定されていることを確認します。アクセスポイントが本製品を日本で許可されるモードで動作できるように、WLAN スイッチ機能を有効にする前に、まず国コードを「JP」（日本）に変更します。国コードの初期値は「US」（アメリカ合衆国）となっています。

Web インタフェースを使用して、国コードを「JP」に変更します。

1. **Administration > Basic Setup > Global** タブをクリックして、以下の画面を表示します。

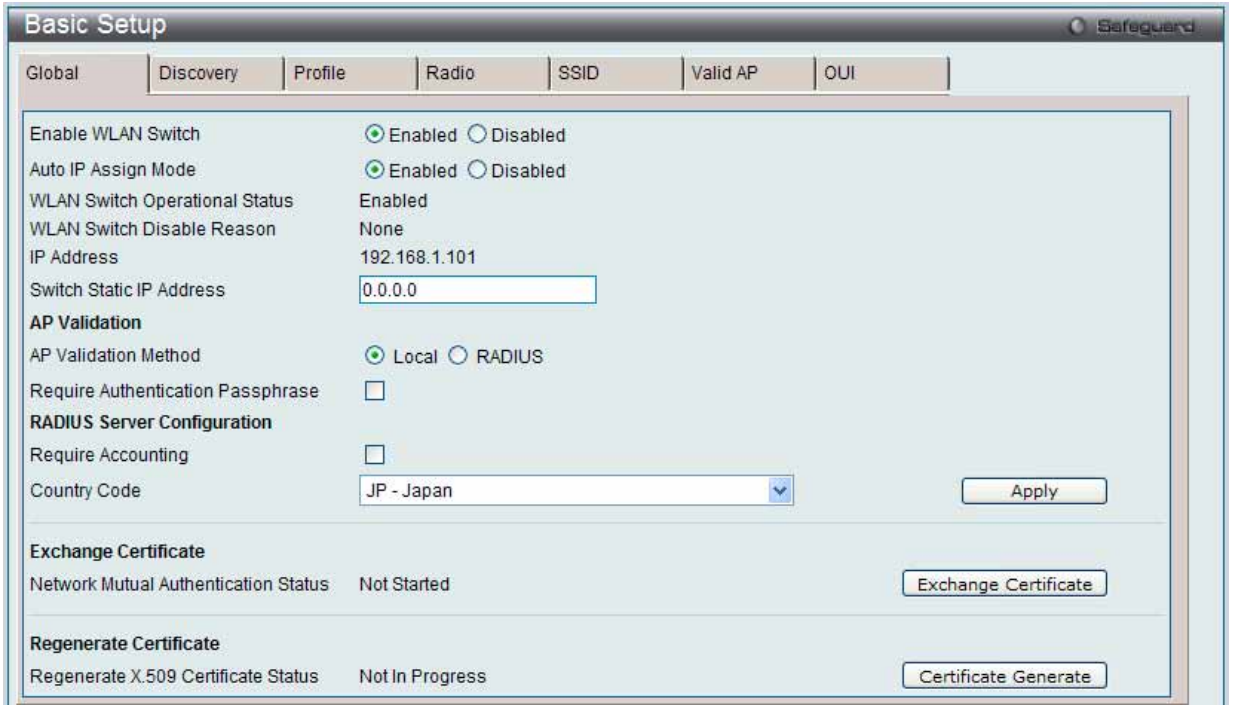


図 8.3-1　Basic Setup > Global 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Enable WLAN Switch	クリックして、WLAN スイッチ機能を「Enabled」（有効）または「Disabled」（無効）にします。
Auto IP Assign Mode	クリックして、無線スイッチが自動的に IP アドレスを自身に割り当てることを「Enabled」（有効）または「Disabled」（無効）にします。
WLAN Switch Operational Status	スイッチの稼動状況を表示します。
WLAN Switch Disable Reason	WLAN スイッチ機能が無効である場合、本項目が現れて原因が表示されます。
IP Address	スイッチの WLAN インタフェースの IP アドレスが表示されます。
Switch Static IP Address	「Auto IP Assign Mode」が「Disabled」（無効）である場合、手動でスイッチのスタティック IP アドレスを割り当てる必要があります。
AP Validation	
AP Validation Method	AP Validation の方法を指定します。 • Local - AP Validation に「Valid AP」に追加されたエントリを使用します。 • RADIUS - AP Validation に外部 RADIUS サーバのデータベースを使用します。
Require Authentication Passphrase	スイッチと接続する前に「Local」または「RADIUS」データベースによるパスフレーズを使用してアクセスポイントの認証が必要とされる場合は、ボックスにチェックを入れます。
RADIUS Server Configuration	
Require Accounting	無線クライアントのために RADIUS アカウンティングを有効にします。
Country Code	ご使用のスイッチとアクセスポイントを操作する国を示す国コードを選択します。 注意　無線通信に関する規則は国ごとに異なります。正しい国コードを選択し、WLAN システムが運用する国の規則を遵守するようにしてください。国コードの変更により、スイッチは有効または無効に切り替えられます。チャンネルおよび、無線モードの設定のうち、その地域の規則に対して妥当でないものは、初期値にリセットされます。

項目	説明
Exchange Certificate	
Network Authentication Server Status	ネットワークの認証サーバが設定状況を示します。
Regenerate Certificate	
Regenerate X.509 Certificate Status	X.509 証明書の再生成状態を示します。

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。

X.509 証明書の要求

「Exchange Certificate」ボタンをクリックして、クラスタコントローラから X.509 証明書を要求します。

X.509 証明書と RSA キーの生成

「Certificate Generate」ボタンをクリックして、スイッチに X.509 証明書と RSA キーを生成します。

Discovery タブ（無線ディスカバリの設定）

スイッチをアクセスポイントと他のスイッチを検出するように設定します。

1. **Administration > Basic Setup > Discovery** タブをクリックして、以下の画面を表示します。

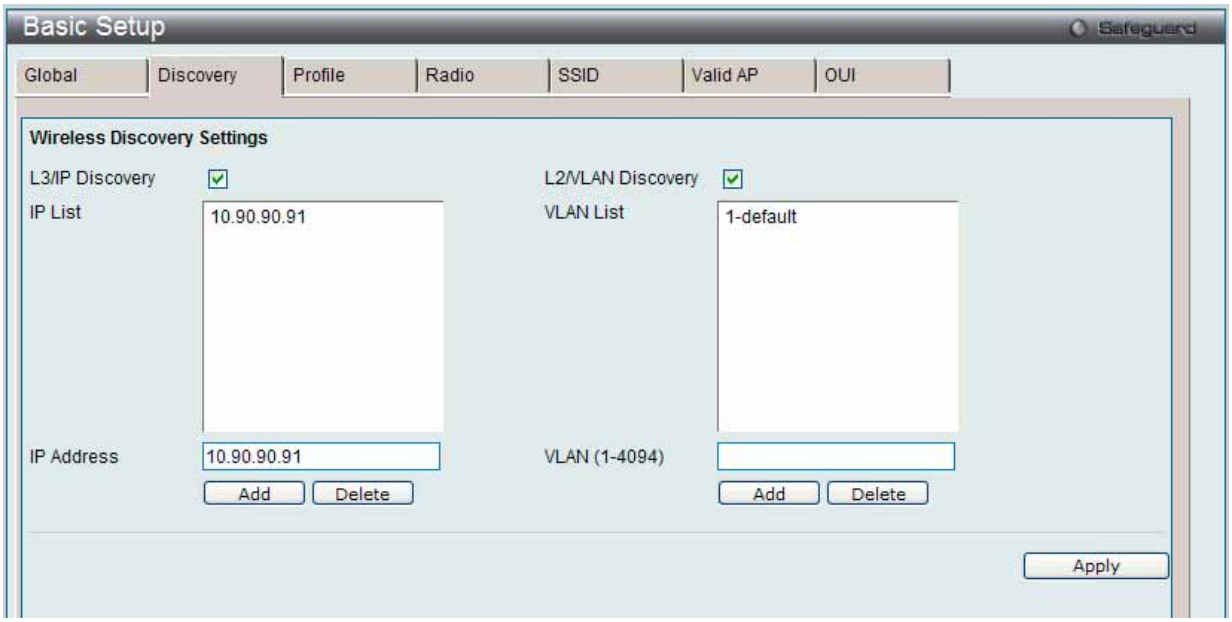


図 8.3-2　Basic Setup > Discovery 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
L3/IP Discovery	チェックボックスを使用して、アクセスポイントおよびピアスイッチの IP ベースのディスカバリを有効 または無効 にします。チェックを外して、機能を無効にします。初期値は有効です。
IP List	ディスカバリ用に設定されている IP アドレスのリストを表示します。 リストからエントリを削除するためには、対応するエントリを選択して「Delete」ボタンをクリックします。
IP Address	IP アドレスを入力して、「IP List」に IP アドレスを追加します。入力可能な最大エントリ数は 256 です。
L2/VLAN Discovery	ボックスをチェックして、L2/VLAN ディスカバリを有効にします。チェックを外して、機能を無効にします。入力可能な最大エントリ数は 16 です。
VLAN List	ディスカバリ用の VLAN リストを表示します。
VLAN (1-4094)	VLAN ID を入力して、「VLAN List」に VLAN を追加します。

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

IP アドレスまたは VLAN 情報を入力して、対応する「Add」ボタンをクリックして、エントリをリストに追加します。

エントリの削除

「IP List」または「VLAN List」から 1 つ以上のエントリを選択し、対応する「Delete」ボタンをクリックして、リストからエントリを削除します。

Profile タブ（プロファイル）

無線のデフォルトプロファイルの設定を行います。

1. **Administration > Basic Setup > Profile** タブをクリックして、以下の画面を表示します。

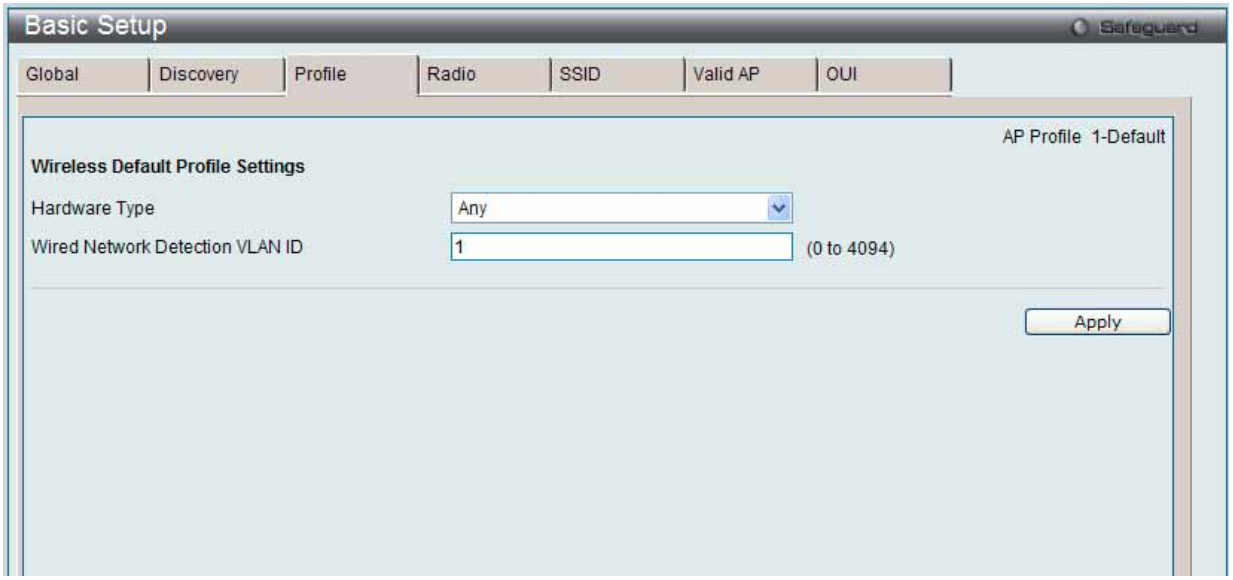


図 8.3-3　Basic Setup > Profile タブ画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Hardware Type	このプロファイルを使用するアクセスポイントのハードウェアタイプを選択します。
Wired Network Discovery VLAN ID	アクセスポイントの無線ネットワークへの接続を検出するためにスイッチがトレーサパケットの送信時に使用する VLAN ID を入力します。 トレーサパケットは、D-Link 統合アクセスシステムに未所属で有線ネットワークに接続している未認証アクセスポイントをスイッチが識別するのに役立ちます。

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。

Radio タブ（周波数帯域）

デフォルト帯域設定を行います。

1. **Administration > Basic Setup > Radio** タブをクリックして、以下の画面を表示します。

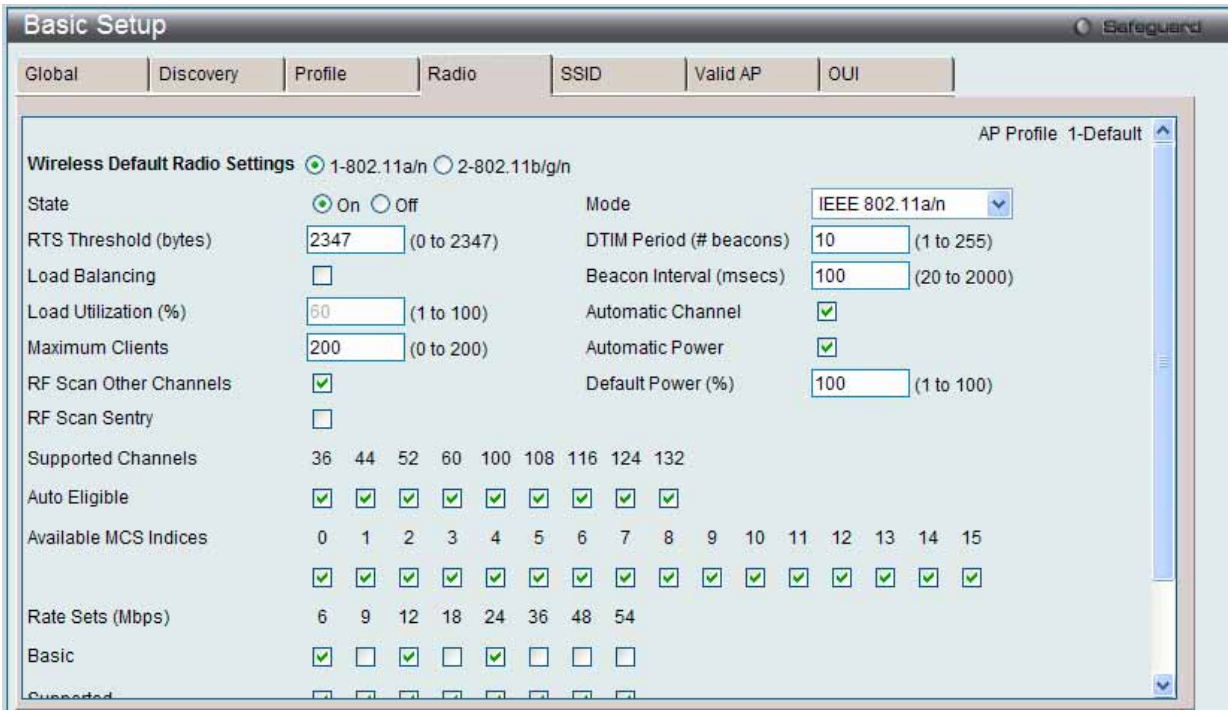


図 8.3-4　Basic Setup > Radio 画面

2. 本画面の設定を変更するためには、最初に設定する無線電波（802.11a/n および 802.11b/g/n）を選択します。

3. 以下の項目を使用して設定および参照します。

項目	説明
Wireless Default Radio Settings	ラジオボタンをクリックして、無線帯域（802.11a/n および 802.11b/g/n）を選択します。
State	「On」または「Off」ボタンを選択して、無線帯域をオンまたはオフにします。
Mode	無線帯域が使用する物理レイヤの標準を選択します。 • 「Wireless Default Radio Settings」で「1-802.11a/n」を選択した場合、利用可能なオプションは、「IEEE 802.11a」と「IEEE 802.11a/n」、および「5GHz IEEE 802.11n」です。 • 「Wireless Default Radio Settings」で「2-802.11b/g/n」を選択した場合、利用可能なオプションは、「IEEE 802.11b/g」と「IEEE 802.11b/g/n」、および「2.4GHz IEEE 802.11n」です。
RTS Threshold (bytes)	Request to Send (RTS) しきい値を 0-2347 の範囲で指定します。RTS しきい値は、MPDU 内のオクテット数を示します。 設定値より低いと RTS/CTS ハンドシェークは実行されません。この値を変更することで、特に多数のクライアントを抱えるアクセスポイントを通過するトラフィックフローの制御をすることができます。低い値を指定すると、RTS パケットは頻繁に送信されるようになります。これにより消費する帯域幅は増大し、パケットのスループットは低下します。一方、RTS パケットの送信数を増やす、混雑したネットワーク内で起こり得る干渉や衝突からの回避や、電磁波による干渉を軽減できるようになります。
DTIM Period (# beacons)	本アクセスポイントの配下にあるクライアントが、送信待ちしているアクセスポイントにバッファされているデータを確認する Delivery Traffic Information Map (DTIM) 間隔（1-255）を指定します。 DTIM メッセージはビーコンフレームに含まれる要素です。DTIM は省電力モード中の無線クライアント向けのデータがアクセスポイントに送信待ちとしてバッファされていることを示しています。ここで指定する DTIM Period（DTIM 間隔）は、本アクセスポイントの配下にあるクライアントが、アクセスポイントにバッファされているデータを確認する間隔を示します。数字はビーコンの数で表します。例えば、本欄に「1」と入力した場合、バッファされたデータの確認は、ビーコンフレーム送信ごとにアクセスポイントで行われます。「10」と入力した場合は 10 回のビーコンフレーム送信に 1 度の確認となります。
Beacon Interval (msecs)	無線ネットワークの存在を通知するために、アクセスポイントがビーコンフレームを送信する間隔（20-2000）を指定します。初期状態では、ビーコンフレームは 100（ミリ秒）に 1 度（1 秒に 10 回）送信されます。単位はミリ秒です。
Load Balancing	チェックボックスを使用して、ロードバランシングを有効にします。有効にすると、アクセスポイントに許可するトラフィック量を制御することができます。
Local Utilization (%)	その無線帯域に許可されるネットワーク帯域使用率 (%) のしきい値を入力します。レベルがしきい値に到達すると、アクセスポイントは新しいクライアントとの接続を停止します。
Maximum Clients	本アクセスポイントに接続できるステーションの最大数を指定します。
Automatic Channel	ボックスをチェックすると、本プロファイルを割り当てたアクセスポイントの無線帯域では、自動チャンネル選択が可能になります。
Automatic Power	ボックスをチェックすると、RF 信号を正しい距離にブロードキャストするように自動的に調整します。
Default Power (%)	RF 信号の最大送信電力（%）を入力します。「Automatic Power」ボックスを選択すると、RF 信号電力の初期設定が使用されます。または、固定の RF 信号電力設定が使用されます。自動 RF 信号電力調整アルゴリズムは、本欄で設定した数値以下に電力を下げることはありません。初期値は 100% です。
RF Scan Other Channels	チェックボックスを選択すると、無線帯域が定期的に操作チャンネルから移動し、他のチャンネルのスキャンを行うことができます。
RF Scan Sentry	チェックボックスを選択すると、無線帯域は Sentry（監視）モードで動作することができます。
Supported Channels	無線帯域でサポートしているチャンネルを表示します。「Basic Setup > Global」画面で選択した「Country Code」に基づいて有効なチャンネルが変わります。
Auto Eligible	各チャンネル下のチェックボックスを選択すると、自動チャンネル割り当てプロセスにそのチャンネルを含めます。
Available MSC Indices	チェックボックスを選択して、802.11n モードで動作する際の MCS Index を追加します。
Rate Sets (Mbps)	通信速度設定を表示します。
Basic	チェックボックスを選択して、アクセスポイントに接続するすべてのステーションがサポートすべきデータ速度を示します。
Supported	チェックボックスを選択して、アクセスポイントがサポートする速度を示します。エラー率やアクセスポイントとクライアントとの距離などの要素をもとに、アクセスポイントは最も効率の良い速度を自動的に選択します。

設定内容を変更した後は、「Apply」ボタンをクリックして設定を適用してください。設定変更は選択した帯域だけに適用されます。

「Clear」をボタンをクリックし、変更を破棄して初期設定に戻します。

SSID タブ（SSID 設定）

SSID タブでは、デフォルト IP プロファイルに関連する仮想アクセスポイント（VAP）設定を示します。各 VAP に対し 1 つのネットワークが接続しており、ネットワーク番号や SSID により識別します。各物理アクセスポイントの無線インタフェースごとに VAP を定義できます。

1. **Administration > Basic Setup > SSID** タブをクリックして、以下の画面を表示します。

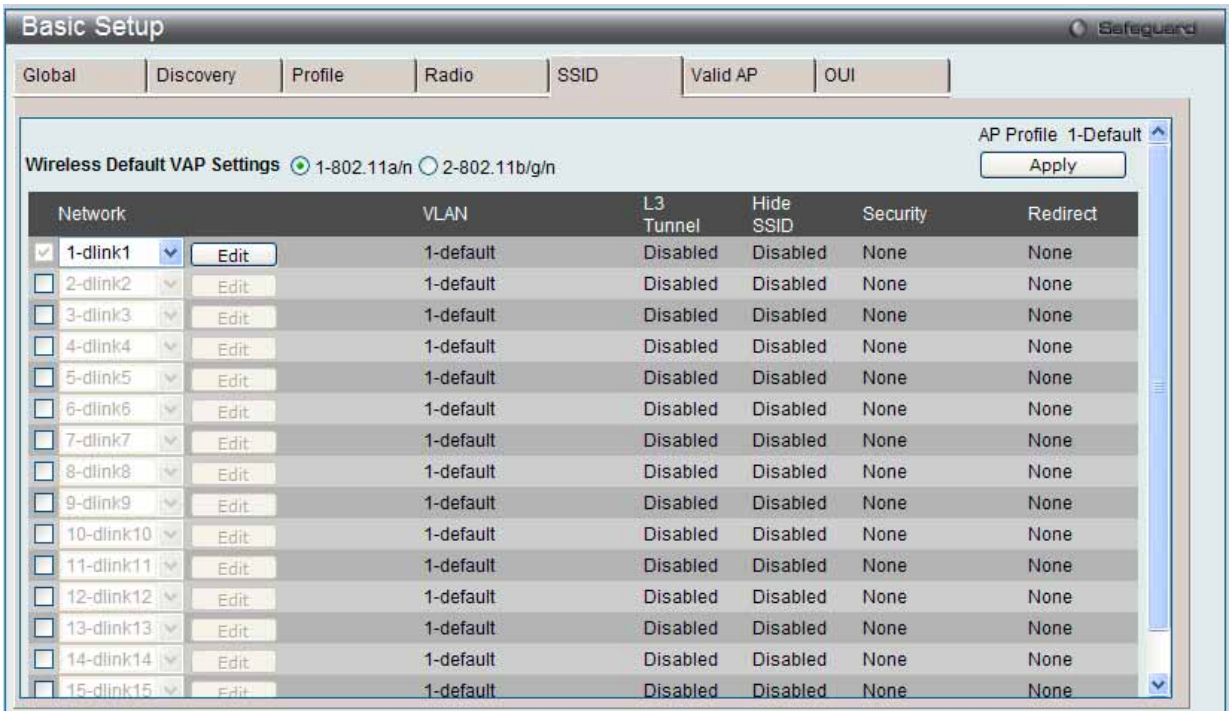


図 8.3-5　Basic Setup > SSID 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Wireless Default VAP Settings	VAP を有効にする前に、設定する無線帯域を選択します。
Network	ボックスをチェックして、選択した無線帯域に対応する VAP を有効にします。プルダウンメニューを使用して、VAP に割り当てるネットワークを選択します。
VLAN	VAP の VLAN ID を表示します。
L3 Tunnel	VAP において L3 トンネリングが「Enabled」（有効）または「Disabled」（無効）であるかを表示します。
Hide SSID	VAP が SSID をブロードキャストするかどうかを表示します。「Enabled」と表示されている時、そのネットワークの SSID は AP ビーコンフレームに含まれません。
Security	VAP の現在のセキュリティ設定を表示します。
Redirect	HTTP リダイレクトが有効かどうかを表示します。 • HTTP - HTTP リダイレクトは有効です。 • None - HTTP リダイレクトは無効です。

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。

「Edit」ボタンをクリックして、対応するネットワークの設定を編集します。

ネットワークの設定の編集

1. 「Edit」ボタンをクリックして、以下の画面を表示します。

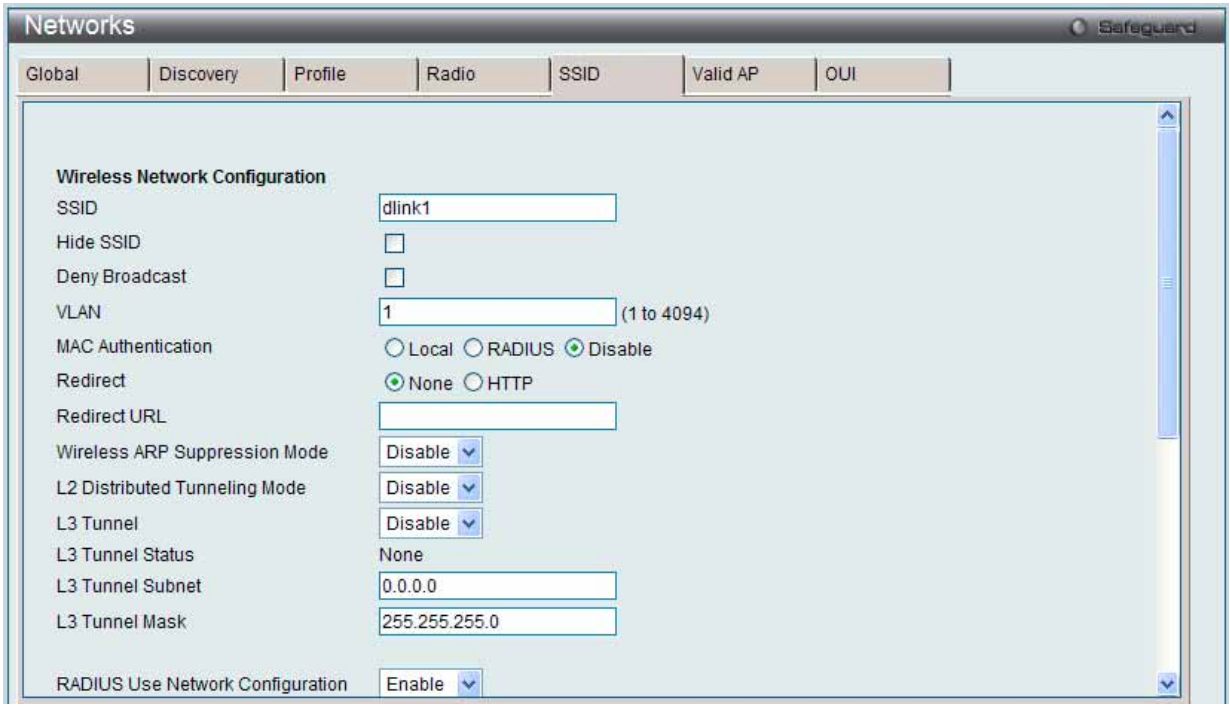


図 8.3-6　Basic Setup > SSID - Edit 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
SSID	ネットワークの SSID（Service Set Identifier）を入力します。これは、英数字のキーで無線 LAN を識別します。
Hide SSID	ボックスをチェックして、SSID のブロードキャストを無効にすることにより、ステーションによるアクセスポイントの自動ディスカバリを阻止します。
Deny Broadcast	ボックスをチェックして、アクセスポイントがクライアントプローブ要求に応答することを禁止します。
VLAN	VLAN ID を入力します。
MAC Authentication	「Local」または「RADIUS」をクリックして、MAC 認証を有効にします。ローカルスイッチまたは外部 RADIUS サーバでクライアントの MAC アドレスを設定する必要があります。
Redirect	「HTTP」ボタンをクリックして、カスタム Web 画面に無線クライアントをリダイレクトします。
Redirect URL	すべての初期の HTTP アクセスがリダイレクトされる URL を入力します。HTTP をリダイレクトタイプとして選択した場合にのみ、本欄は表示されます。
Wireless ARP Suppression Mode	無線 ARP パケット抑制モードを「Enable」（有効）または「Disable」（無効）にします。本モードを有効にすると、アクセスポイントは、無線インタフェース上でブロードキャストされた ARP 要求数を削減することができます。ブロードキャストの削減は、無線インタフェースの電力の節約に役立ちます。省電力モードを使用する無線クライアントは、ブロードキャストフレームを検出した時に必ず起動するので、より電力を使用します。 **注意** 本機能を有効にすると、DHCP パケットを検出するためにフィルタリングする余分なパケットや、ARP 要求や返答パケットの処理のために、アクセスポイントのパケット転送性能は少し低下します。IPv4 を使用しないネットワークでは、本機能を有効にするべきではありません。

項目	説明	
L2 Distributed Tunneling Mode	Distributed L2 トンネリングモードでは、データトラフィックを統合スイッチに送信することなく、無線クライアントの L3 ローミングをサポートします。メニューを使用して、「Enable」（有効）または「Disable」（無効）にします。 本機能は、統合スイッチがハードウェアの送信アクセラレーションまたはハードウェアベースの L2 トンネルをサポートしない場合に推奨されます。 **注意** **1.** すべてのアクセスポイントを管理するスイッチが 1 つだけで、そのスイッチがダウンした場合、すべてのアクセスポイントは接続する無線帯域でシャットダウンし、トンネルを切断します。スイッチが回復し、アクセスポイントが再び管理状態になった後に、以前にトラフィックをトンネルしていたクライアントは再接続され、現在位置するネットワークで IP アドレスを取得します。この IP アドレスは以前にトンネルしていた時に使用していた IP アドレスとは異なり、トラフィックはトンネルされません。 **2.** ピアスイッチを持つネットワークで、そのピアスイッチが管理するアクセスポイント間でトンネルが確立されれば、ホーム AP を管理するスイッチが故障した場合、アソシエーション AP を管理するスイッチは故障を検知してトンネルを切断します。この時点でクライアントは接続を切断されます。クライアントは、再接続した際に新たに IP アドレスを取得します。 **3.** アソシエーション AP を管理するスイッチが故障すると、上記 1 と同様なシナリオになります。アクセスポイントは、すべての無線帯域をダウンさせ、クライアントを切断します。	
L3 Tunnel	L3 トンネル機能を「Enable」（有効）または「Disable」（無効）にします。L3 トンネル機能では、モバイルステーションが 1 つのアクセスポイントから他のアクセスポイントにローミングする際に、これらのアクセスポイントが異なる IP サブネットに属している場合でも IP 接続を維持することができます。 **注意** L3 トンネルが有効である時､VLAN ID は使用されません。実際の運用ではスイッチはトンネリングするパケットに管理用 VLAN ID を記載しています。 **注意** L3 トンネリング機能が使用中に統合スイッチが再起動するなど無線ネットワークトポロジが変更された場合、トンネルされているネットワークへの接続性を再確立する処理を直ちに行うために有線クライアントに対して ARP リフレッシュを実行する必要があります。	
L3 Tunnel Status	L3 トンネリングの状態を表示します。	
L3 Tunnel Subnet	L3 トンネルサブネット。本項目に入力するネットワーク IP アドレスは、スイッチに定義した WLAN 用ルーティングインタフェースと同一サブネット内で指定します。	
L3 Tunnel Mask	L3 トンネルサブネット上のネットワーク IP アドレス用サブネットマスクを入力します。	
RADIUS Use Network Configuration	VAP がネットワークの RADIUS 設定とグローバル RADIUS アカウンティング設定のどちらを使用するかを制御します。 • Enable -「Wireless Network Configuration」画面で設定した RADIUS アカウンティングを使用します。 • Disable -「Wireless Global Configuration」画面で設定した RADIUS アカウンティングを使用します。	
RADIUS Accounting	選択すると無線クライアントの RADIUS アカウンティング機能を有効にします。	
Security	無線接続のセキュリティメカニズムを選択して、ネットワークを保護します。	
	None	選択すると、ネットワークにセキュリティはなくなります。また、詳しいオプションをアクセスポイントに設定する必要はありません。
	WEP	WEP（Wired Equivalent Privacy）は 802.11 無線ネットワーク用のデータ暗号化プロトコルです。このセキュリティメカニズムを選択すると、ネットワークのすべての無線クライアントとアクセスポイントにはデータ暗号化のために 64 ビット または 128 ビットの共有鍵も設定します。「WEP」を選択すると、以下のオプションが表示されます。 • Static WEP - スタティックキーの管理設定を行います。以下のオプションが表示されます。 - Authentication - ボックスをチェックして、認証タイプを選択します。利用可能なオプションは「Open System」および「Shared Key」です。 - WEP Key Type - ラジオボタンをクリックして、キータイプを選択します。利用可能なオプションは「ASCII」と「HEX」です。ASCII キーはアルファベットの大文字、小文字、数字、および @# などの記号を含みます。Hex キーは数字（0~9）と文字（A~F）を含みます。 - WEP Key Length (bits) - ラジオボタンをクリックして、キー長（64 ビットまたは 128 ビット）を選択します。 - WEP Keys - ラジオボタンをクリックして、特定の変換キーを選択します。テキスト欄には最大 4 つの WEP キーを入力します。キーの文字数は「WEP Key Type」と「WEP Key Length」によって異なります。 • WEP IEEE 802.1X - 以下のオプションが表示されます。: - Bcast Key Refresh Rate - この VAP に接続するクライアントが使用するブロードキャストキーの更新間隔を入力します。 - Session Key Refresh Rate - ユニキャストセッションキーの更新間隔を入力します。

項目	説明	
Security	WPA/WPA2	WPA と WPA2 は、AES-CCMP および TKIP メカニズムを含む Wi-Fi Alliance の IEEE802.11i 標準に準拠しています。「WPA/WPA2」を選択すると、以下のオプションが表示されます。 • WPA Personal - これを選択して、スタティックなキー管理を設定します。 - WPA Versions - ボックスをチェックして、サポートするクライアントステーションのタイプを選択します。利用可能なオプションは WPA および WPA2 です。 - WPA Ciphers - ボックスをチェックして、使用する暗号スイートを選択します。利用可能なオプションは TKIP および CCMP (AES) です。 - WPA Key Type - キータイプは ASCII で、アルファベットの大文字、小文字、数字、および @# などの記号を含みます。 - WPA Key - WPA パーソナルで使用する WPA キーは共有秘密鍵です。8-63 文字の文字列に入力します。アルファベットの大文字、小文字、数字、および @# などの記号が入力できます。 - Bcast Key Refresh Rate - この VAP に接続するクライアントが使用するブロードキャストキーの更新間隔を入力します。 • WPA Enterprise - これを選択して、アクセスポイントはグローバル RADIUS サーバまたは無線ネットワークに指定した RADIUS サーバを使用します。 - WPA Versions - ボックスをチェックして、サポートするクライアントステーションのタイプ（WPA および WPA2）を選択します。 - WPA Ciphers - ボックスをチェックして、使用する暗号スイートを選択します。利用可能なオプションは TKIP および CCMP (AES) です。 - Pre-Authentication - ボックスをチェックして、WPA2 無線クライアントによる事前認証パケットの送信を許可します。事前認証情報はアクセスポイントからリレーされます。クライアントは現在ターゲットのアクセスポイントに使用しています。本機能を有効にすると、ローミングするために複数のアクセスポイントと接続するクライアントの認証を高速化することができます。本機能は WPA2 を使用して接続するクライアントのみが利用できます。WPA ではサポートされていません。 - Pre-Authentication Limit - アクセスポイントが同時に扱う事前認証数を入力します。このように制限することにより、RADIUS サーバへの過負荷を防ぐことができます。負荷が軽い状態では、事前認証が再度送信されても制限されません。0 は制限しないことを示しています。 - Key Caching Hold Time - アクセスポイントが PMK を保持している時間（1-1440 分）を指定します。この設定は、RADIUS サーバが生成し、事前認証からアクセスポイントに送信される PMK に適用されます。この時間の制限は、RADIUS サーバがある特定のユーザ用としてここで指定する値よりも大きな値を Session-Timeout に返してきた場合は、その値が優先されますのでご注意ください。値を設定しない場合、無線クライアントがローミングすることを想定して、アクセスポイントは無線クライアントの PMK を他のアクセスポイントに送信しません。 - Bcast Key Refresh Rate - この VAP に接続するクライアントが使用するブロードキャスト（グループ）キーの更新間隔を入力します。 - Session Key Refresh Rate - ユニキャストセッションキーの更新間隔を入力します。
Client QoS	ボックスをチェックして、前の欄の SSID を使用して AP に接続する無線クライアントのクライアント QoS の動作を有効にします。	
Client QoS Bandwidth Limit Down	無線クライアントがアクセスポイントからトラフィックを受信する最大値 (bps) を入力します。	
Client QoS Bandwidth Limit Up	クライアントがアクセスポイントにトラフィックを送信する最大値 (bps) を入力します。	
Client QoS Access Control Down	プルダウンメニューを使用して、外向き（ダウン）方向のトラフィックに適用するアクセスリスト名を選択します。	
Client QoS Access Control Up	プルダウンメニューを使用して、内向き（アップ）方向のトラフィックに適用するアクセスリスト名を選択します。	
Client QoS DiffServ Policy Down	プルダウンメニューを使用して、外向き（ダウン）にアクセスポイントから送信されるトラフィックに適用する DiffServ ポリシー名を選択します。	
Client QoS DiffServ Policy Up	プルダウンメニューを使用して、内向き（アップ）にアクセスポイントから送信されるトラフィックに適用する DiffServ ポリシー名を選択します。	

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

「<<Back」をボタンをクリックし、変更を破棄してと前のページに戻ります。

「Clear」をボタンをクリックし、変更を破棄して初期設定に戻します。

Valid AP タブ（Valid アクセスポイントの設定）

アクセスポイント認証に使用するデータベースを指定します。「Valid Access Point Summary」画面には、ローカルデータベースに設定したアクセスポイントの情報が表示されます。

1. **Administration > Basic Setup > Valid AP** タブをクリックして、以下の画面を表示します。

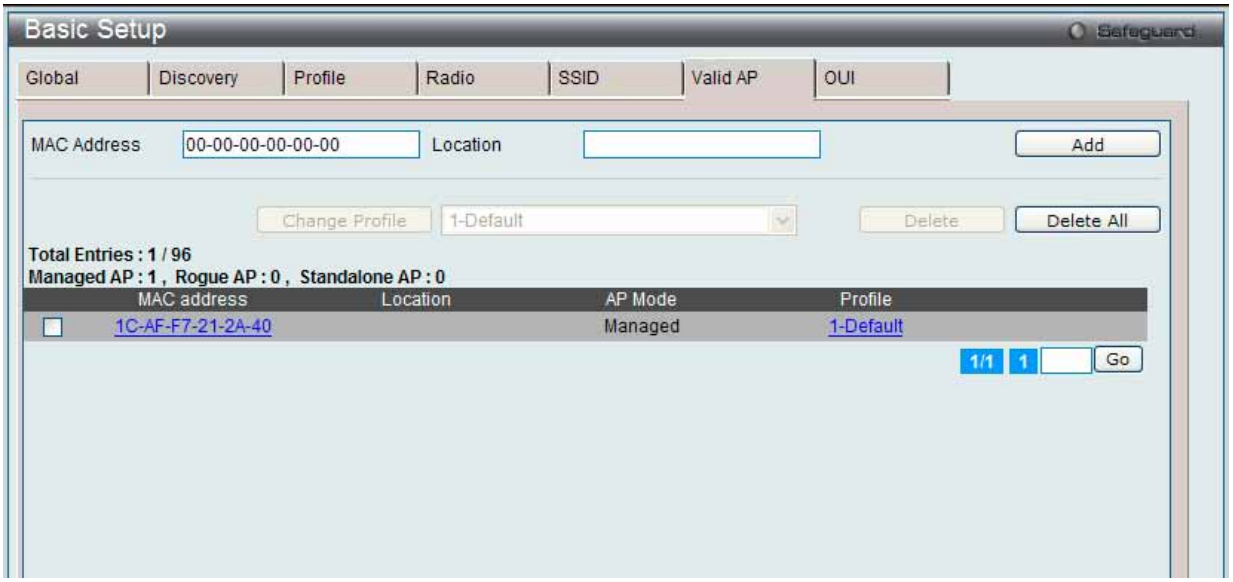


図 8.3-7　Basic Setup > Valid AP 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Total Entries	アクセスポイントデータベースに登録されているアクセスポイントの総数。
Managed AP	データベース内でアクセスポイントモードが「Managed」に設定されているアクセスポイントの数。
Rogue AP	データベース内で、アクセスポイントモードが「Rouge」に設定されているアクセスポイントの数。
Standalone AP	データベース内でアクセスポイントモードが「Standalone」に設定されているアクセスポイントの数。
MAC Address	アクセスポイントの MAC アドレスを入力します。
Location	アクセスポイントを識別しやすいように場所を入力します。
AP Mode	現在のアクセスポイントのモードを表示します。
Profile	アクセスポイントに適用されている AP プロファイルが表示されます。

エントリの追加

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

プロファイルの変更

選択アクセスポイントに割り当てられているプロファイルを変更するためには、1 つ以上の MAC アドレスをチェックし、プルダウンメニューから AP プロファイルを選択して「Change Profile」ボタンをクリックします。

エントリの削除

MAC アドレスをチェックし、「Delete」ボタンをクリックして、エントリを削除します。

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

詳しい Valid AP 設定の参照

「MAC Address」ハイパーリンクをクリックして、詳しい Valid AP 設定を参照します。

「Profile」ハイパーリンクをクリックして、「AP Profiles」画面に遷移します。

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

Valid AP 設定

1. 「MAC Address」ハイパーリンクをクリックすると、以下の画面が表示されます。

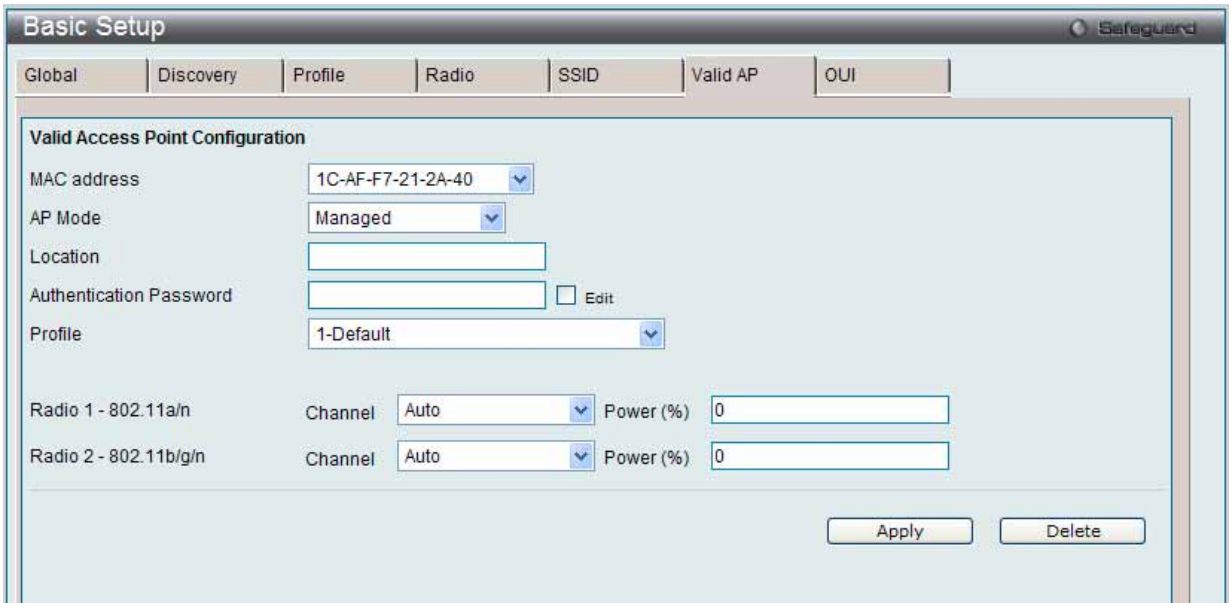


図 8.3-8　Basic Setup > Valid AP - Valid Access Point Configuration 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
MAC address	アクセスポイントの MAC アドレスを選択します。
AP Mode	プルダウンメニューを使用して 3 つのオプションから 1 つを選択します。 • Managed - アクセスポイントは D-Link 統合スイッチの一部となり、統合スイッチが管理を行います。「Managed」を選択すると、画面の下半分に以下のオプションが表示されます。 - Authentication Password -「Edit」ボックスをチェックして、スイッチがディスカバリした際に認証するアクセスポイントのパスワードを入力します。 - Profile - プルダウンメニューを使用して、AP に割り当てる AP プロファイルを選択します。 - Channel - プルダウンメニューを使用して、無線帯域がデータの送受信に使用するチャンネルを選択します。 - Auto - 使用する利用可能な RF 信号を自動的にスキャンします。 - Power - 送信電力を設定します。これはアクセスポイントがどれだけ遠くまで RF 信号をブロードキャストできるかということに影響する電力レベル（%）です。 • Standalone - アクセスポイントはネットワークにおいて個別のアクセスポイントとして機能します。「Standalone」を選択すると、画面の下半分に以下のオプションが表示されます。 - Expected SSID - Standalone モードのアクセスポイントのみ無線ネットワークを識別する SSID を入力します。 - Expected Channel - プルダウンメニューを使用して、Standalone モードのアクセスポイントが使用するチャンネルを選択します。アクセスポイントがチャンネルを自動選択するように設定されている場合、あるいはチャンネルを指定しない場合は、「Any」を選択します。 - Expected Security Mode - アクセスポイントが使用するセキュリティのタイプを選択します。: • Any - すべてのセキュリティモード。 • Open - セキュリティなし。 • WEP - Static WEP または WEP IEEE 802.1X。 • WPA/WAP2 - WPA および / または WPA2(パーソナル、エンタープライズ)。 - Expected Wired Network Mode - 有線ネットワークで Standalone モードのアクセスポイントが許可されていない場合は「Allowed」を選択します。有線ネットワークでアクセスポイントが許可されていない場合は、「Not Allowed」を選択します。 • Rogue - このアクセスポイントをネットワーク内で検出した時に（SNMP トラップが有効の場合、SNMP トラップを通じて）通知します。
Location	アクセスポイントを識別しやすいように場所を入力します。

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

「Delete」ボタンをクリックして、エントリを削除します。

OUI タブ（OUI データベース）

無線ネットワークで検出したアクセスポイントと無線クライアントのメーカを識別するために、無線スイッチにはあらかじめ登録された OUI（Organizationally Unique Identifiers）のデータベースがあります。ここでは OUI を登録します。

1. **Administration > Basic Setup > OUI** タブをクリックして、以下の画面を表示します。

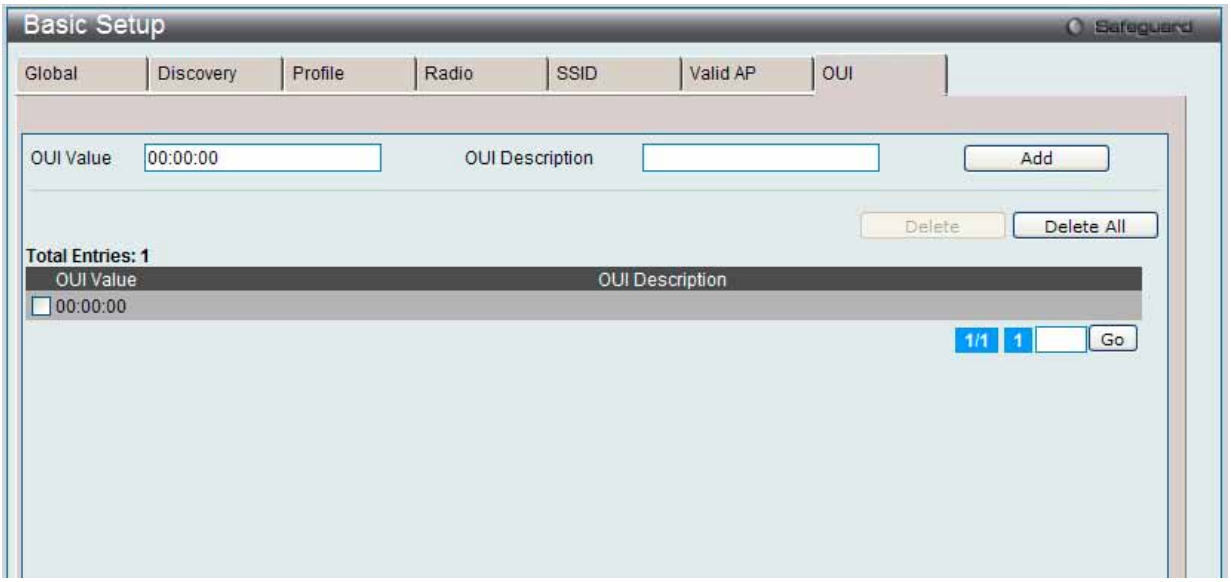


図 8.3-9　Basic Setup > OUI 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
OUI Value	会社番号を表す OUI を「XX:XX:XX」形式で入力します。（XX は 00-FF の 16 進数） MAC アドレスの最初の 3 バイトは会社の ID の割り当てを示しています。
OUI Description	OUI に関連付けされる組織名。

エントリの追加

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

エントリの削除

1 つ以上の OUI 値をチェックし、「Delete」ボタンをクリックして、エントリを削除します。

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

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

AP Management（アクセスポイント管理）

AP Reboot（アクセスポイント再起動）

統合スイッチから 1 つまたはすべてのアクセスポイントを再起動します。

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

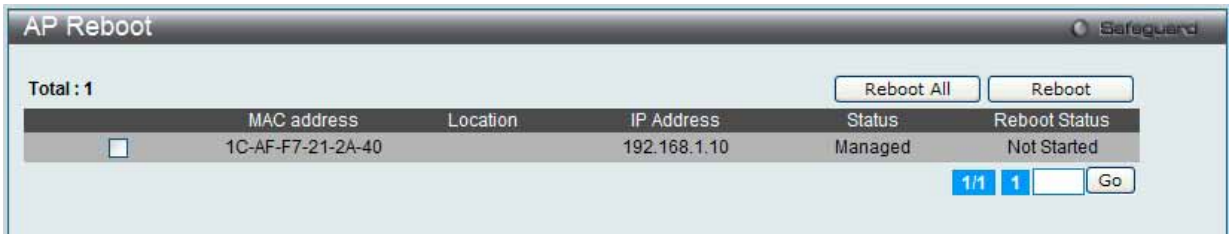


図 8.3-10　AP Reboot 画面

1 つ以上の MAC アドレスを選択し、「Reboot」ボタンをクリックして、指定したアクセスポイントを再起動します。
「Reboot All」ボタンをクリックすると、すべてのスイッチが再起動します。

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

RF Management（RF 管理）

Configuration タブ

無線電波の周波数を設定します。

1. **Administration > AP Management > RF Management > Configuration タブ**の順にメニューをクリックし、以下の画面を表示します。

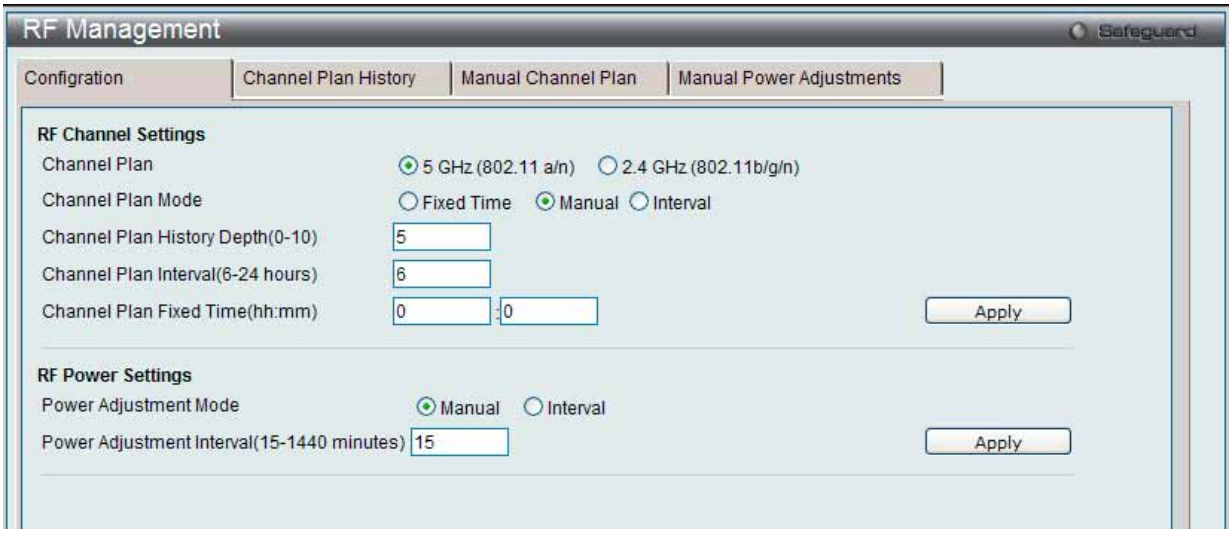


図 8.3-11　RF Management > Configuration 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
RF Channel Settings	
Channel Plan	2.4 GHz (802.11b/g/n) および 5 GHz (802.11 a/n) 帯域は異なるチャンネルプランを使用します。ラジオボタンをクリックして、無線帯域を選択します。
Channel Plan Mode	チャンネル割当てモードを選択します。 • Fixed Time - チャンネルプランとチャンネル割り付けの時間を指定します。 • Manual - 手動でチャンネルプランアルゴリズムを実行し、アクセスポイントにチャンネルプランを適用します。（初期値） • Interval - スイッチは定期的に計算して、チャンネルプランを適用します。
Channel Plan History Depth (0-10)	チャンネルプランのヒストリの反復数を入力します。初期値は 5 です。チャンネルプランヒストリには、チャンネルプラン適用後にスイッチが各アクセスポイントに割り当てたチャンネルが記録されています。エントリは実行間隔、時間、またはチャンネルプランモードにかかわらず、ヒストリに追加されます。本フィールドで指定した数字により、チャンネル割り当ての反復回数が制御されます。 **注意** チャンネルを変更をしたアクセスポイントは、次回のサイクルではチャンネルは変更されません。本ヒストリにより同じアクセスポイントのチャンネルが何度も変更されることを防止します。

項目	説明
Channel Plan Interval (6-24 hours)	「Channel Plan Mode」で「Interval」を選択すると、チャンネルプランの計算と割り当てを行う間隔（6-24 時間）を入力します。初期値は 6 です。
Channel Plan Fixed Time (hh:mm)	「Channel Plan Mode」で「Fixed Time」を指定した場合、チャンネルプランの計算と割り当てを実行する時刻を指定します。チャンネルプランの計算は、24 時間ごとに 1 回指定した時刻に実行されます。
RF Power Settings	
Power Adjustment Mode	「Manual」または「Interval」をクリックして、手動または定期的にアクセスポイント無線電波周波数の送信電力を調整します。 • Manual -「Manual Power Adjustments」ページから手動で提案した電力調整を実行します。（初期値） • Interval - スイッチが定期的に電力調整を計算し、すべてのアクセスポイントに電力を適用します。実行間隔は、「Submit」ボタンをクリックした時からカウントされます。
Power Adjustment Interval (15-1440 minutes)	スイッチが電力調整アルゴリズムを実行する間隔を指定します。「Power Adjustment Mode」で「Interval」が選択した場合に、値は適用されます。初期値は 15 です。

「Apply」ボタンをクリックして各セクションで行った変更を適用します。

Channel Plan History タブ（チャンネルプランヒストリの表示）

1. **Administration > AP Management > RF Management > Channel Plan History タブ**の順にメニューをクリックし、以下の画面を表示します。

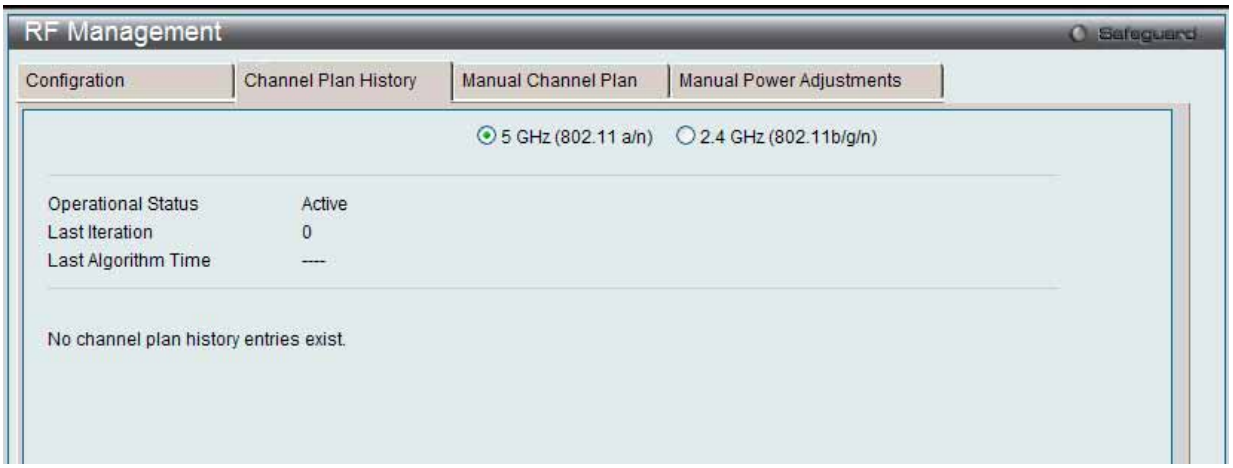


図 8.3-12　RF Management Channel Plan History 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
5GHz (802.11a/n) 2.4GHz (802.11b/g/n)	5 GHz と 2.4 GHz モードでは異なるチャンネルプランを使用します。そのためスイッチは別々にチャンネルヒストリを記録します。指定した無線帯域のチャンネル情報のみ表示します。
Operational Status	スイッチがアクセスポイントの無線帯域で自動チャンネル調整アルゴリズムを使用しているか否かを表示します。
Last Iteration	チャンネルプラン調整の最新の反復を表示します。チャンネルを変更したアクセスポイントは、次回の反復サイクルではチャンネルは変更されません。これにより、同じアクセスポイントのチャンネルが何度も変更されることを防止します。 **AP Management > RF Management > Configuration** タブを選択し、「History Depth」を設定することにより、チャンネルプランヒストリに記録、表示する最大反復サイクル回数を制御します。
Last Algorithm Time	最後にチャンネルプランアルゴリズムが実行された日時を表示します。 **注意** システム時間を設定するためには、初期値では無効である SNTP の使用が必要になります。Web インタフェースを使用して、**LAN タブ > Network Application > SNTP** の順にメニューをクリックし、SNTP 設定を行います。
AP MAC Address	統合無線スイッチの管理下にあるアクセスポイントのイーサネットアドレス。アクセスポイントの MAC アドレスのあとに (*) が続いている場合、それはピアスイッチによって管理されます。
Location	アクセスポイントの位置で、Valid AP データベース (ローカルまたは RADIUS サーバ内) に設定されている値です。
Radio	無線帯域および設定された無線モードを表示します。無線帯域が無効に設定されていれば、無線モードには、設定されているモードの代わりに「Off」と表示されます。
Iteration	チャンネルプラン調整の反復を表示します。
Channel	無線帯域が有効な場合、現在動作状態にあるチャンネルが表示されます。

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

注意 以下のような条件下では、アクセスポイントへのチャンネルの割り当てはできません。

- アクセスポイントがダウンしている。
- プロファイルのアップデートにより、アクセスポイントの無線モードが無効になっている。
- 無線モードにおいて無効なチャンネルが指定されている。
- チャンネルプランの計算後にアクセスポイントが再起動され、ローカルデータベースにスタティックに設定されたスタティックチャンネルを取得した。
- 「Advanced」ページによりチャンネルが手動で設定されている。
- アクセスポイントのプロファイルに自動チャンネルモードが無効に設定されている。

Manual Channel Plan タブ（手動チャンネルプランの起動）

1. **Administration > AP Management > RF Management > Manual Channel Plan タブ**の順にメニューをクリックし、以下の画面を表示します。

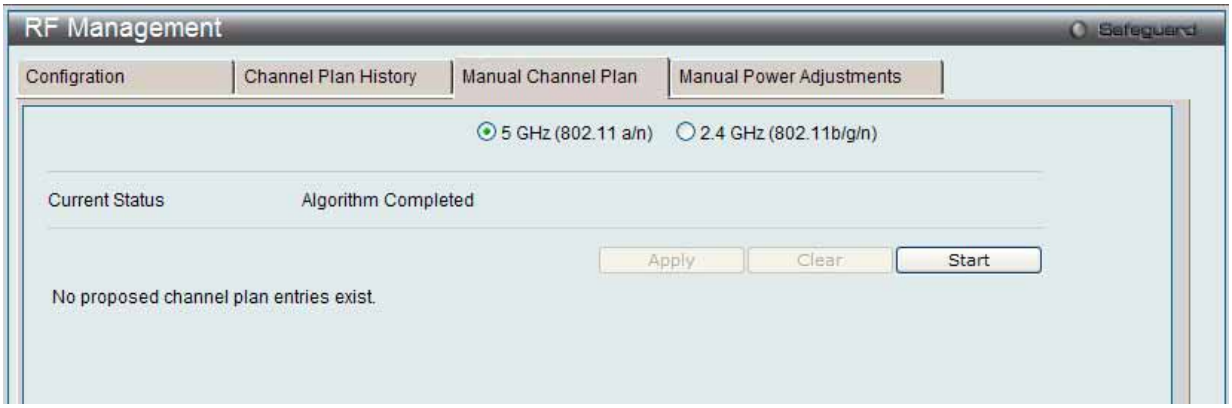


図 8.3-13　RF Management > Manual Channel Plan 画面

2. ラジオボタンをクリックして、チャンネルプランを参照する無線帯域の周波数を選択します。

3. 以下の項目を使用して設定および参照します。

項目	説明
5GHz (802.11a/n) 2.4GHz (802.11b/g/n)	5 GHz と 2.4 GHz モードでは異なるチャンネルプランを使用します。そのためスイッチは別々にチャンネルヒストリを記録します。指定した無線帯域のチャンネル情報のみ表示します。
Current Status	以下の状態から 1 つを表示します。 • None - 前回のスイッチの再起動からチャンネルプランアルゴリズムの手動による実行はありません。 • Algorithm In Progress - チャンネルプランアルゴリズムを実行中です。 • Algorithm Complete - チャンネルプランアルゴリズムは実行を完了しました。表中にチャンネル割り当て案が表示されます。エントリにはアクセスポイントの現在のチャンネルおよび変更案が表示されます。変更案に同意し、変更を適用するためには「Apply」ボタンをクリックします。変更案の適用は手動で行います。 • Apply In Progress - スイッチは提供されたチャンネルプランを適用し、テーブルに表示されているアクセスポイントのチャンネル調整を行っています。 • Apply Complete - アルゴリズムの実行およびチャンネル調整は完了しました。
AP MAC Address	統合無線スイッチの管理下にあるアクセスポイントのイーサネットアドレス。AP の MAC アドレスの後に (*) が続いている場合、それはピアスイッチによって管理されます。
Location	アクセスポイントの位置。Valid AP データベース (ローカルまたは RADIUS サーバ内) に設定されている値です。
Radio	無線インタフェースおよび設定した無線帯域のモードを表示します。無線帯域が無効に設定されていれば、無線帯域モードには、設定モードの代わりに「Off」と表示されます。
Current Channel	アルゴリズムが新しいチャンネル割り当てを推奨するアクセスポイントの現在の操作チャンネルを表示します。
New Channel	アクセスポイントに対する操作チャンネル案を表示します。

「Start」ボタンをクリックして、手動で電力調整機能を開始します。

「Apply」ボタンをクリックして行ったチャンネル変更案を適用します。

エントリの削除
「Clear」ボタンをクリックして、エントリを削除します。

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

Manual Power Adjustments タブ（手動電力調整の起動）

「Configuration」タブ上で「Power Adjustment Mode」を「Manual」に指定している場合、「Manual Power Adjustments」タブ画面を使用して、送信電力調整アルゴリズムを手動で起動することができます。

1. **Administration > AP Management > RF Management > Manual Power Adjustments タブ**の順にメニューをクリックし、以下の画面を表示します。

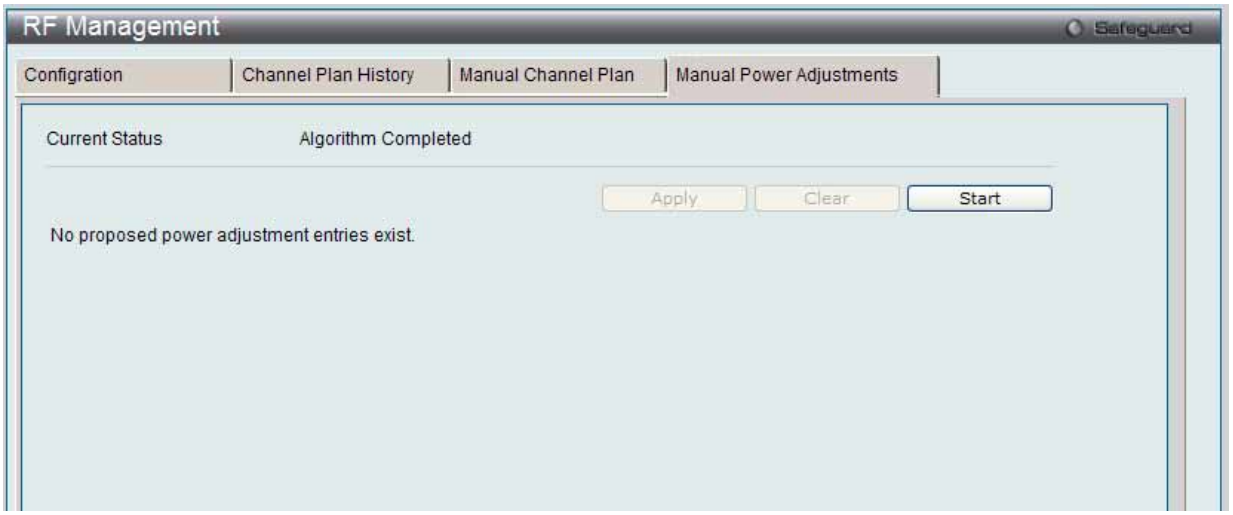


図 8.3-14　RF Management > Manual Power Adjustments 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Current Status	プランの現在の状態を表示します。 • None - 前回のスイッチの再起動から電力調整アルゴリズムの手動による実行はありません。 • Algorithm In Progress - 電力調整アルゴリズムを実行中です。 • Algorithm Complete - 電力調整アルゴリズムは実行を完了しました。 表に電力調整案が表示されます。エントリにはアクセスポイントの現在の電力レベルおよび変更案が表示されます。変更案に同意し、変更を適用するためには「Apply」ボタンをクリックします。変更案の適用は手動で行います。 • Apply In Progress - スイッチはアクセスポイントが使用する電力レベルを調整しています。 • Apply Complete - アルゴリズムの実行および電力調整は完了しました。
AP MAC Address	アクセスポイントの MAC アドレスを表示します。
Location	アクセスポイントの場所を表示します。これは Valid AP データベースに設定されています。
Radio	無線帯域を表示します。
Current Power	アクセスポイントの現在の電力レベルを表示します。
New Power	アクセスポイントの電力レベル案を表示します。

「Start」ボタンをクリックして、手動で電力調整機能を開始します。

「Apply」ボタンをクリックして行った電力変更案を適用します。

エントリの削除

「Clear」ボタンをクリックして、エントリを削除します。

Software Downloads（アクセスポイントソフトウェアのダウンロード）

AP Software Download タブ

スイッチが管理するアクセスポイントのソフトウェアをアップグレードします。クラスタコントローラはピア無線スイッチに管理されたアクセスポイントのプログラムを更新することができます。

1. **Administration > AP Management > Software Download > AP Software Download タブ**の順にメニューをクリックし、以下の画面を表示します。

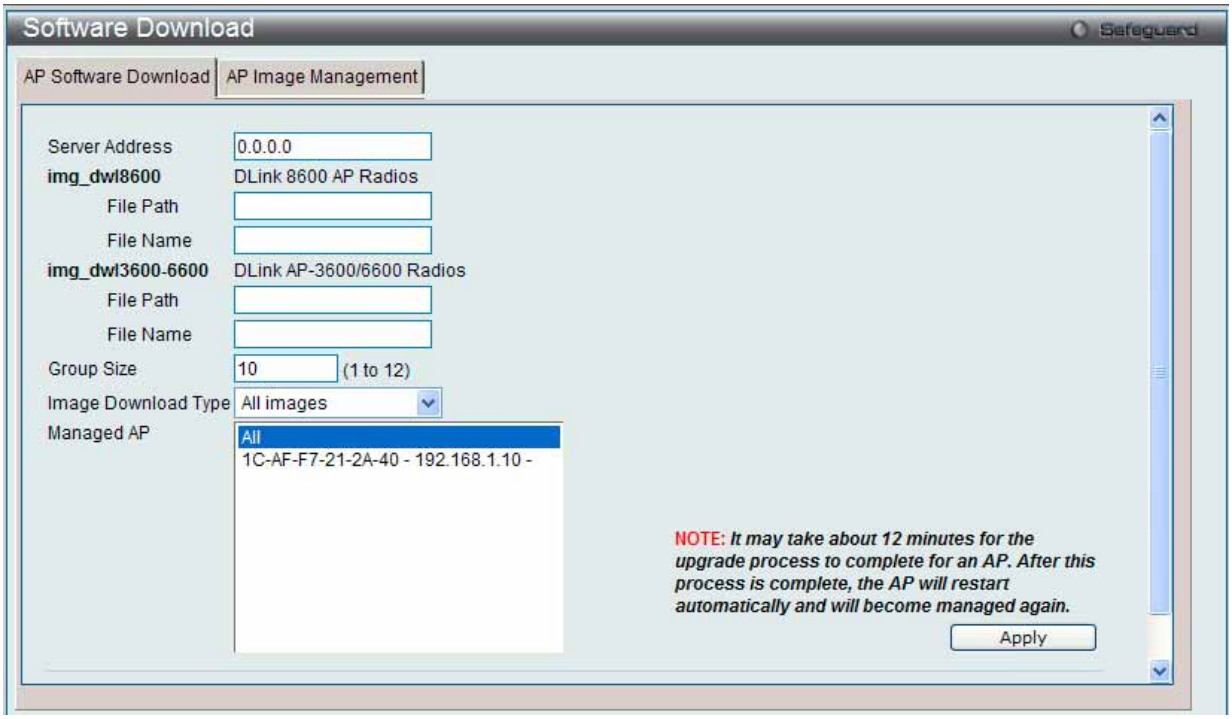


図 8.3-15　Software Download > AP Software Download 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Server Address	アップグレード用ファイルが格納されているホストの IP アドレスを入力します。
File Path	選択ファイルが位置する TFTP サーバのパスを入力します。 **注意** ファイルのパスを指定する場合、前にスラッシュ「/」を入力する必要があります。例「/<filepath>」
File Name	アップグレードするファイルの名称を入力します。
Group Size	アップグレードするアクセスポイント数を入力します。これにより、一度にアップグレードするアクセスポイント数を制限します。
Image Download Type	アクセスポイントプルダウンメニューを使用して、ダウンロードするイメージファイルのタイプを選択します。
Managed AP	管理下にある全アクセスポイントを表示します。管理下にあるすべてのアクセスポイントをアップグレードする場合は、リストから「All」を選択します。 1 台のアクセスポイントをアップグレードする場合、リストからアクセスポイントを選択します。複数のアクセスポイントをアップグレードするためには、「CTRL」キーを押したまま複数のアクセスポイントを選択します。

「Apply」ボタンをクリックして、処理を開始します。

注意 アクセスポイントのアップグレード処理が完了するには 12 分ほどかかります。処理が完了すると、アクセスポイントは、自動的に再起動して、再び管理下のアクセスポイントになります。

AP Image Managements タブ

ファイルが指定した AP コードイメージである場合に、無線スイッチへのファイルのダウンロード処理を行います。

1. **Administration > AP Management > Software Download > AP Image Management タブ**の順にメニューをクリックし、以下の画面を表示します。

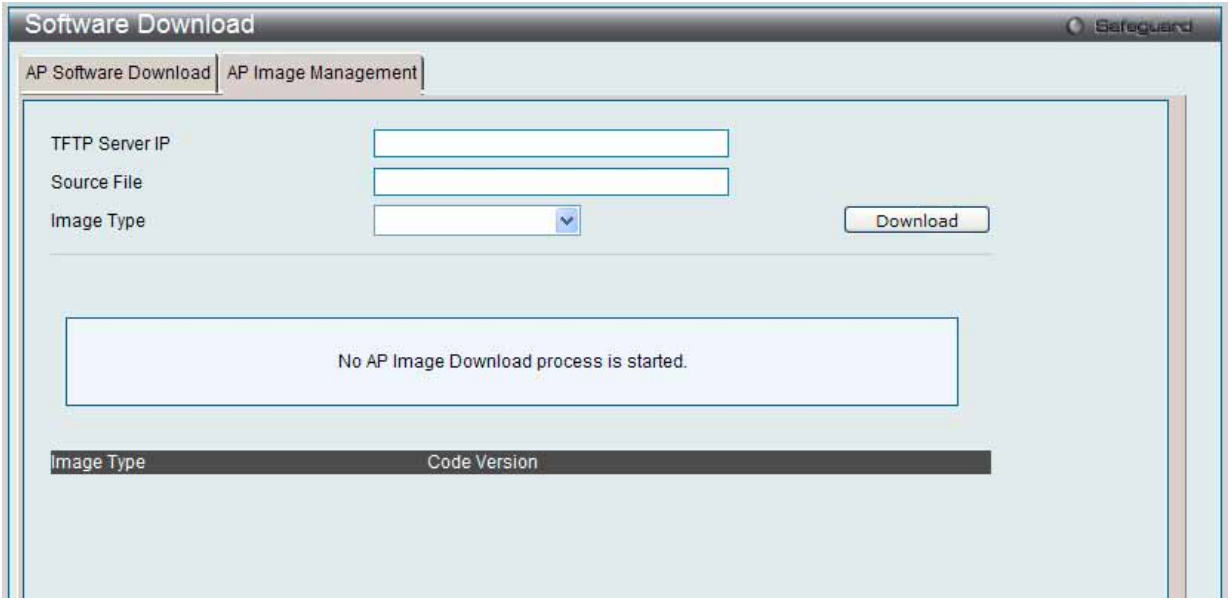


図 8.3-16　Software Download > AP Image Management 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
TFTP Server IP	TFTP サーバの IP アドレスを入力します。
Source File	ファイル名を入力します。
Image Type	プルダウンメニューを使用して、ダウンロードするイメージファイルのタイプを選択します。

「Download」ボタンをクリックして、無線スイッチに対してファイルダウンロード処理を開始します。

Advanced Settings（管理アクセスポイントの詳細設定）

リモート Telnet アクセス、および無線帯域の周波数チャンネル / 電力を設定します。

1. **Administration > AP Management > Advanced 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 8.3-17　Advanced Settings 画面

2. 「Debug」、「Channel」または「Power」のハイパーリンクをクリックして、詳細情報を設定します。

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

Debug リンク（アクセスポイントのデバッグ）

1. 「Debug」ハイパーリンクをクリックすると、以下の画面が表示されます。

図 8.3-18　Advanced Settings > Debug 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
MAC address	アクセスポイントの MAC アドレスを示します。
Location	Valid AP データベースに登録されたアクセスポイントの場所を表示します。
IP Address	アクセスポイントの IP アドレスを表示します。
Status	デバッグ機能の状態を表示します。
Password	アクセスポイントの管理パスワードを入力します。
Confirm Password	確認のためにパスワードを再度入力します。
Enable Debug	デバッグ機能を「Enabled」（有効）または「Disabled」（無効）にします。

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

「<<Back」をボタンをクリックし、変更を破棄してと前のページに戻ります。

Channel または Power リンク（チャンネルと電力の調整）

1. 「Channel」または「Power」ハイパーリンクをクリックすると、以下の画面が表示されます。

図 8.3-19　Advanced Settings - Channel/Power 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
AP MAC Address	アクセスポイントの MAC アドレスを表示します。
Radio	無線帯域を表示します。
Channel Status	チャンネルの状態を表示します。
Channel	プルダウンメニューを使用して、無線帯域が送受信に使用するチャンネルを定義します。
Power Status	電力状態を表示します。
Power	送信電力を設定します。これはアクセスポイントがどれだけ遠くまで RF 信号をブロードキャストできるかということに影響する電力レベル（%）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。

「<<Back」をボタンをクリックし、変更を破棄してと前のページに戻ります。

AP Provisioning（アクセスポイントプロビジョニング）

アクセスポイントにプロビジョニング機能を設定します。

Summary タブ

1. **Administration > AP Management > AP Provisioning** の順にメニューをクリックし、以下の画面を表示します。

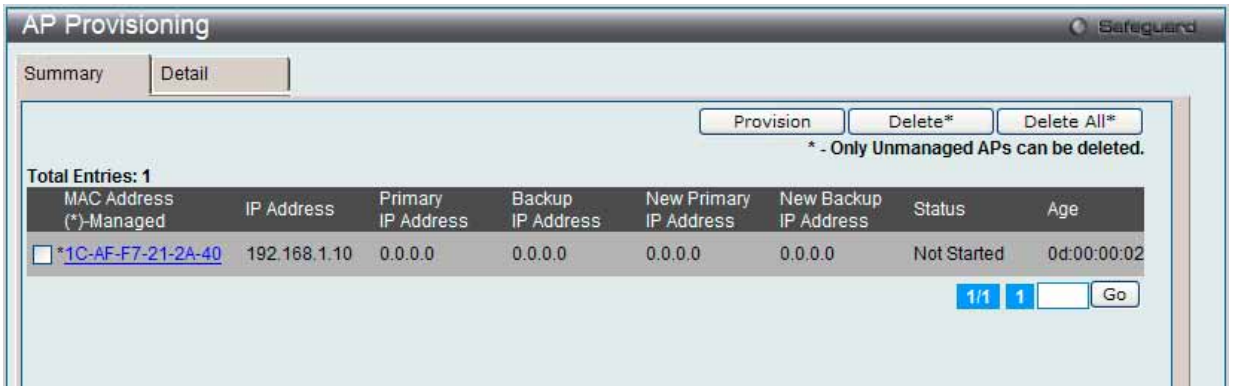


図 8.3-20　AP Provisioning > Summary 画面

2. 特定の MAC アドレスをチェックし、「Provision」ボタンをクリックして、プロビジョニングを実行します。

エントリの削除

特定の MAC アドレスをチェック後、「Delete」ボタンをクリックしてエントリを削除します。
「Delete All」ボタンをクリックして、管理下にないアクセスポイントを削除します。

詳細情報の表示

「MAC Address」のハイパーリンクをクリックするか、または「Detail」タブをクリックして、詳しい情報を参照します。

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

Detail タブ

1. 「MAC Address」ハイパーリンクまたは「Detail」タブをクリックすると、以下の画面が表示されます。

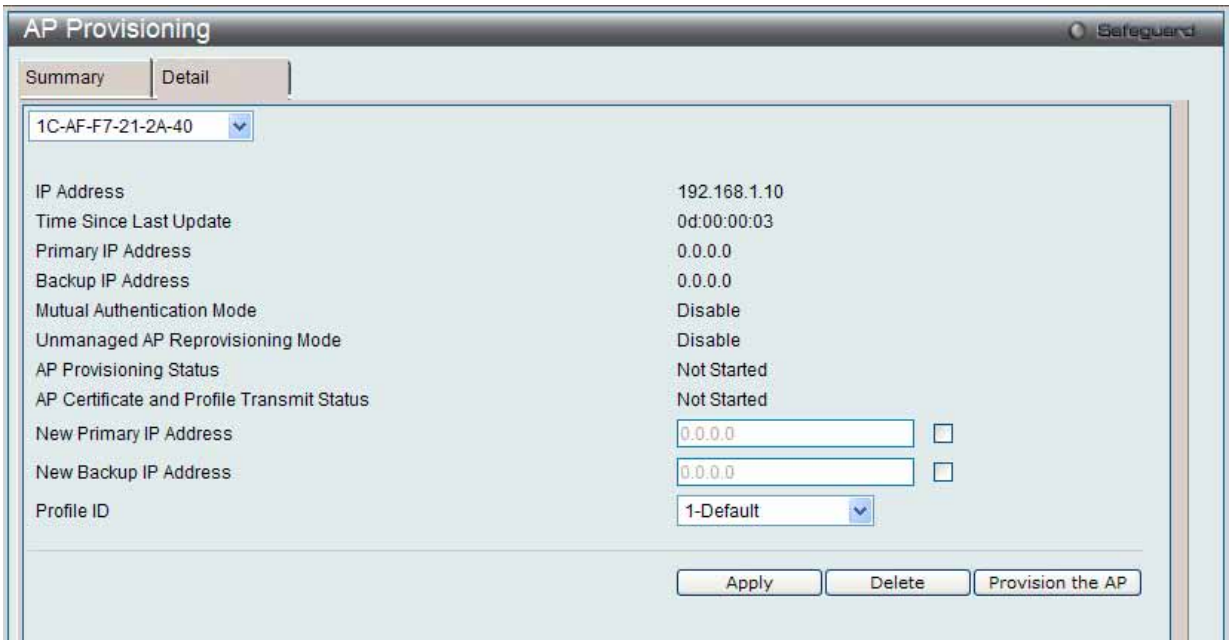


図 8.3-21　AP Provisioning > Detail 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
MAC Address	プルダウンメニューを使用して、アクセスポイントの MAC アドレスを選択します。
New Primary IP Address	ボックスをチェックして、アクセスポイントにプロビジョニングが行われるプライマリの IP アドレスを入力します。
New Backup IP Address	ボックスをチェックして、アクセスポイントにプロビジョニングが行われるバックアップスイッチの IP アドレスを入力します。
Profile ID	プルダウンメニューを使用して、プロビジョニング時に使用されるプロファイル ID を選択します。

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

エントリの削除

「Delete」ボタンをクリックして、エントリを削除します。

プロビジョニングの実行

「Provision the AP」ボタンをクリックして、プロビジョニングを実行します。

Advanced Configuration（高度な設定）

Global（グローバル設定）

無線の詳細的な設定を行います。

General タブ

1. **Administration > Advanced Configuration > Global > General タブ**の順にメニューをクリックし、以下の画面を表示します。

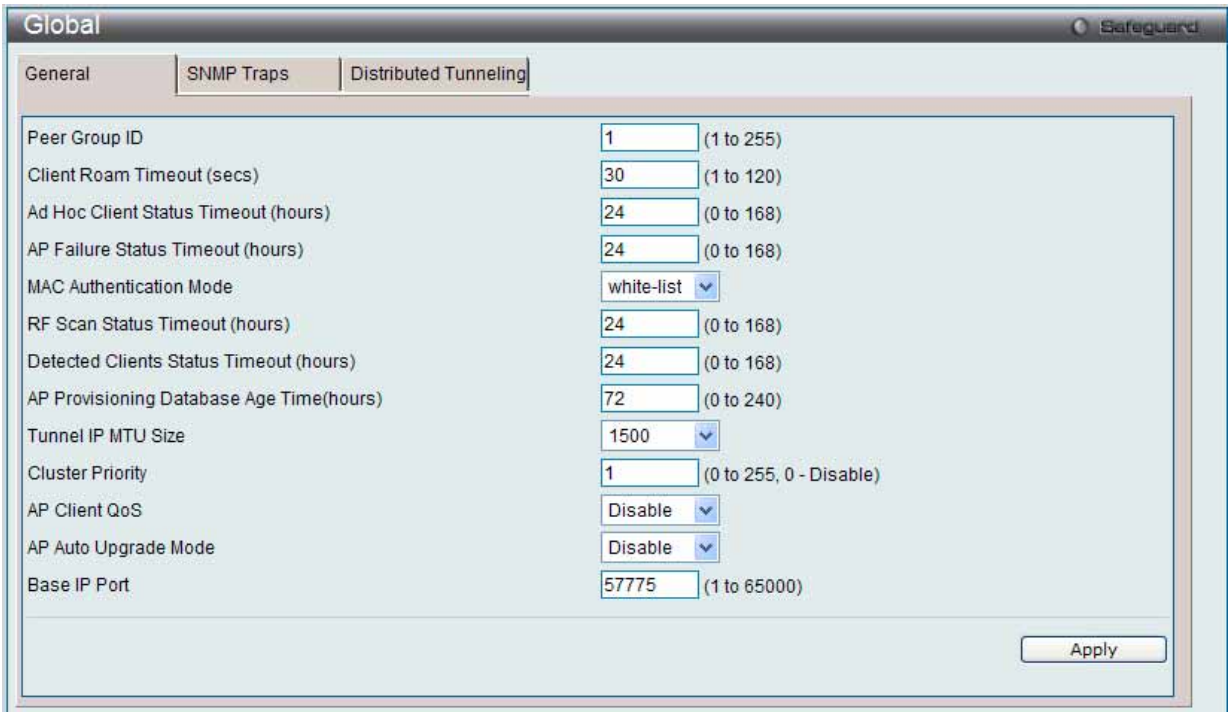


図 8.3-22　Global > General 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Peer Group ID	ピアグループ ID を入力して、無線スイッチをピアと設定します。ピアスイッチ同士はアクセスポイントに関する情報の一部を共有することにより L3 ローミングを実現します。
Client Roam Timeout (secs)	クライアントの切断後、エントリが「Associated Client Status」リストから削除されるまでの時間を指定します。
Ad Hoc Client Status Timeout (hours)	「Ad Hoc Client Status」リストにエントリを保持する時間を決定します。
AP Failure Status Timeout (hours)	「AP Authentication Failure Status」リストにエントリを保持する時間を決定します。
MAC Authentication Mode	ホワイトリストまたはブラックリストにある無線クライアントに行うグローバルなアクションを選択します。 • white-list - Known Client データベースに記載され、明確にアクセスを拒否されていない MAC アドレスを持つ無線クライアントを指定し、アクセスを許可します。データベースに MAC アドレスがない場合、クライアントへのアクセスは拒否されます。 • black-list - Known Client データベースに記載され、明確にアクセスを許可されていない MAC アドレスを持つ無線クライアントを指定し、アクセスを拒否します。データベースに MAC アドレスがない場合、クライアントへのアクセスは許可されます。
RF Scan Status Timeout (hours)	「RF Scan Status」リストにエントリを保持しておく時間を指定します。
Detected Clients Status Timeout (hours)	「Detected Client Status」リストにエントリを保持しておく時間を指定します。
AP Provisioning Database Age Time (hours)	「AP provisioning」データベースにエントリを保持しておく時間を指定します。

項目	説明
Tunnel IP MTU Size	ネットワークに処理される IP パケットの最大サイズを指定します。MTU はトンネル VAP 上だけで実施されます。 IP パケットがアクセスポイントと統合スイッチ間をトンネリングする場合、トンネルを通過中のパケットサイズは 20 バイトごとに増加します。これは、1500 バイトの IP MTU サイズに設定されている無線クライアントが、スイッチに 1518（1522 のタグ付き）バイトのフレームを設定し、切り換える場合に既存のネットワークインフラの最大 MTU サイズを超える可能性があることを意味します。トンネル IP MTU サイズを増やすと、トラフィックがフローするポートの物理的な MTU を増やす必要があります。 **注意** 以下の条件を満たす場合、トンネル IP の MTU サイズを増やす必要はありません。 • 無線ネットワークは L3 トンネリングを使用しません。 • トンネリングモードは、通常小さいパケットを持つ音声トラフィックにだけ使用されます。 • トンネリングモードは、HTTP などの TCP ベースのプロトコルにだけ使用されます。これはすべての TCP 接続がトンネルに合うようにアクセスポイントが自動的に最大セグメントサイズを減少させるためです。
Cluster Priority	クラスタコントローラの選定のために本スイッチの優先度を指定します。 クラスタ内で最も高い優先度を持つスイッチがクラスタコントローラになります。優先度がすべてのスイッチで同じである場合、最も低い IP アドレス値を持つスイッチがクラスタコントローラになります。優先度 0 は、スイッチがクラスタコントローラになれないことを意味します。最も高い優先度は 255 です。
AP Client QoS	クライアント QoS 機能を「Enable」（有効）または「Disable」（無効）にします。
AP Auto Upgrade Mode	アクセスポイントの自動アップグレードモードを「Enable」（有効）または「Disable」（無効）にします 。
Basic IP Port	IP 制御データの通信ポートを入力します。

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

SNMP Traps タブ（無線 SNMP トラップ設定）

統合スイッチの管理に SNMP（Simple Network Management Protocol）を使用する場合、スイッチに SNMP エージェントを設定して、ネットワーク内の SNMP マネージャにトラップ送信をする必要があります。

1. **Administration > Advanced Configuration > Global > SNMP Traps タブ**の順にメニューをクリックし、以下の画面を表示します。

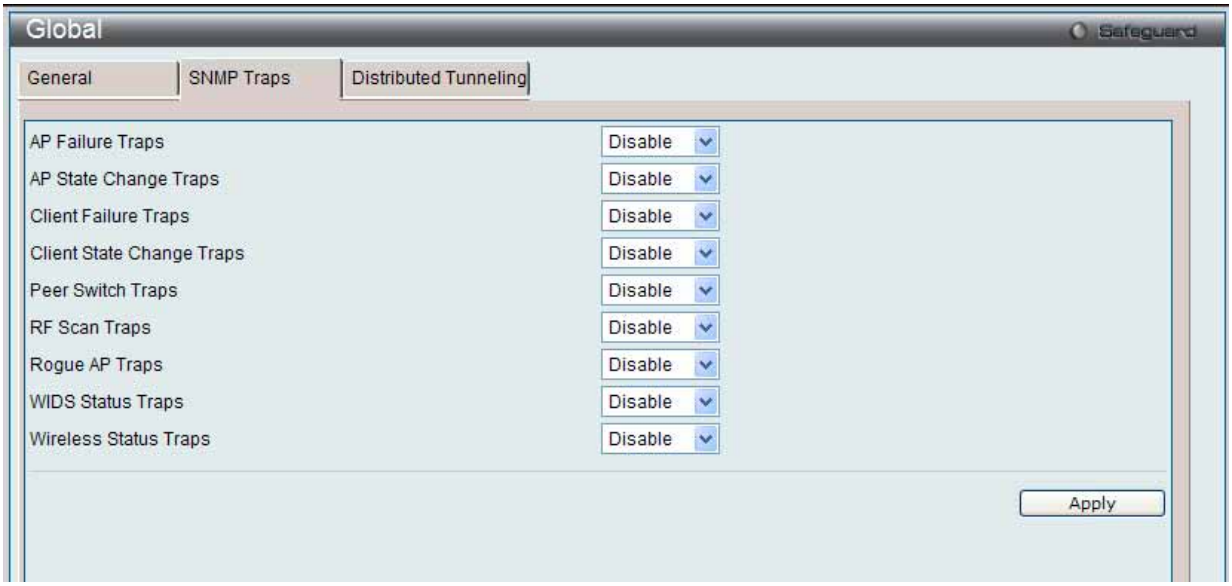


図 8.3-23　Global > SNMP Traps 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
AP Failure Traps	「Enable」を選択すると、アクセスポイントがスイッチとの接続または認証に失敗した時に SNMP エージェントがトラップを送信します。
AP State Change Traps	「Enable」を選択すると、以下の場合、SNMP エージェントがトラップを送信します。 • 管理対象のアクセスポイントの検出 • 管理対象のアクセスポイント異常 • 管理対象のアクセスポイントから不明なプロトコルの検出 • 管理対象のアクセスポイントのロードバランス使用率超過
Client Failure Traps	「Enable」を選択すると、無線クライアントがアクセスポイントとの接続または認証に失敗した時に SNMP エージェントがトラップを送信します。

項目	説明
Client State Change Traps	「Enable」を選択すると、クライアントに関連する以下のいずれかの原因により、SNMP エージェントがトラップを送信します。 • クライアントの接続検出 • クライアントの切断検出 • クライアントのローミング検出
Peer Switch Traps	「Enable」を選択すると、ピアスイッチに関連する以下のいずれかの原因により、SNMP エージェントがトラップを送信します。 • ピアスイッチの検出 • ピアスイッチの異常 • ピアスイッチから不明なプロトコルの検出 • Configuration コマンドがピアスイッチから受信されました。（スイッチは、このトラップを生成するためにクラスタコントローラを必要としません。）
RF Scan Traps	「Enable」を選択すると、RF スキャンが新しいアクセスポイント、クライアント、またはアドホッククライアントを検出した時に SNMP エージェントがトラップを送信します。
Rogue AP Traps	「Enable」を選択すると、スイッチがローグ（不正）アクセスポイントを検出した場合、SNMP エージェントがトラップを送信します。また、何らかの不正なアクセスポイントがネットワークに存在していると、エージェントは「Rogue Detected Trap Interval」（秒）ごとにトラップを送信します。
WIDS Status Traps	「Enable」を選択すると、以下のいずれか原因により SNMP エージェントがトラップを送信します。 • このスイッチがクラスタスコントローラになりました。 • 不正なクライアントを検出しました。 • 「Rogue Detected Trap Interval」（秒）後も不正なクライアントが存在しています。 • ピアグループにおける管理アクセスポイントの最大数を超過しました。
Wireless Status Traps	「Enable」を選択すると、統合スイッチ（このトラップではクラスタコントローラである必要はありません）の動作ステータスが変更されると、SNMP エージェントはトラップを送信します。Channel Algorithm または Power Algorithm が実行されるとトラップを送信します。また、以下のデータベース中のリストのエントリ数が最大値を超えた時に SNMP エージェントがトラップを送信します。 • Managed AP データベース • AP Neighbor リスト • Client Neighbor リスト • AP Authentication Failure リスト • RF Scan AP リスト • Client Association データベース • Ad Hoc クライアントリスト • 検出されたクライアントリスト

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。

Distributed Tunneling タブ（Distributed トンネリング設定）

1. **WLAN タブ > Administration > Advanced Configuration > Global > Distributed Tunneling タブ**の順にメニューをクリックし、以下の画面を表示します。

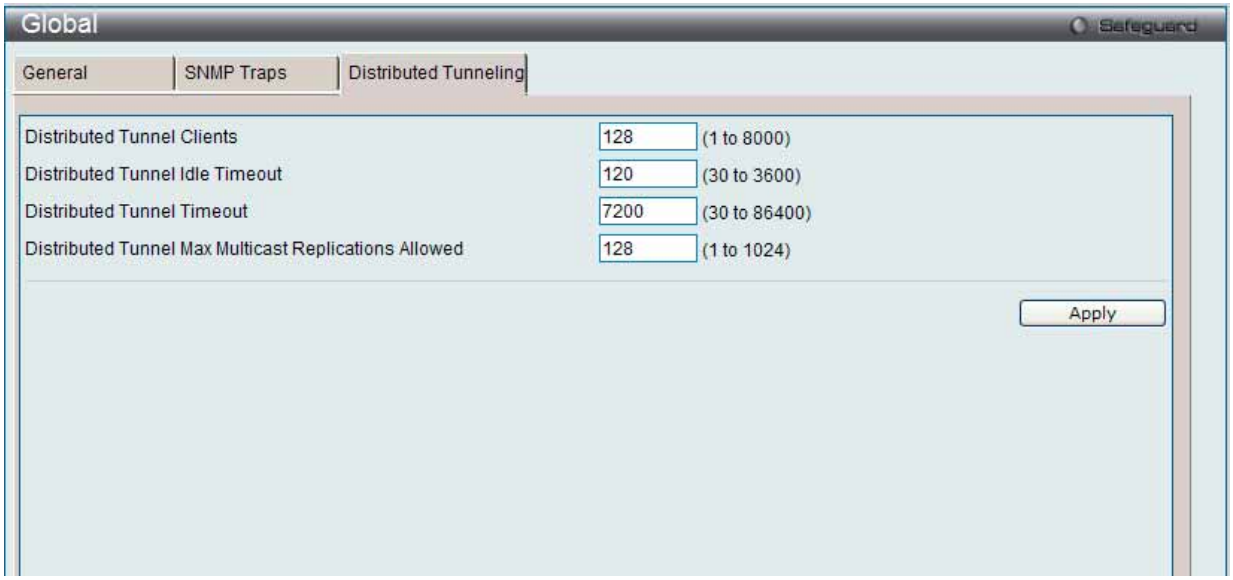


図 8.3-24　Global > Distributed Tunneling 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Distributed Tunnel Clients	ホーム AP から同時に移動できる分散型トンネリングを行うクライアントの最大数を指定します。
Distributed Tunnel Idle Timeout	クライアントへのトンネルが終了し、クライアントが強制的に IP アドレスを変更される前のクライアントの無通信時間（秒）を指定します。
Distributed Tunnel Timeout	ローミングクライアントへのトンネルが終了し、クライアントが強制的に IP アドレスを変更されるまでの時間（秒）を指定します。
Distributed Tunnel Max Multicast Replications Allowed	マルチキャストフレームがホーム AP にコピーされるトンネルの最大数を指定します。

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

Networks（ネットワーク）

スイッチに設定済みの無線ネットワークをすべて表示します。

1. **Administration > Advanced Configuration > Networks** の順にメニューをクリックし、以下の画面を表示します。

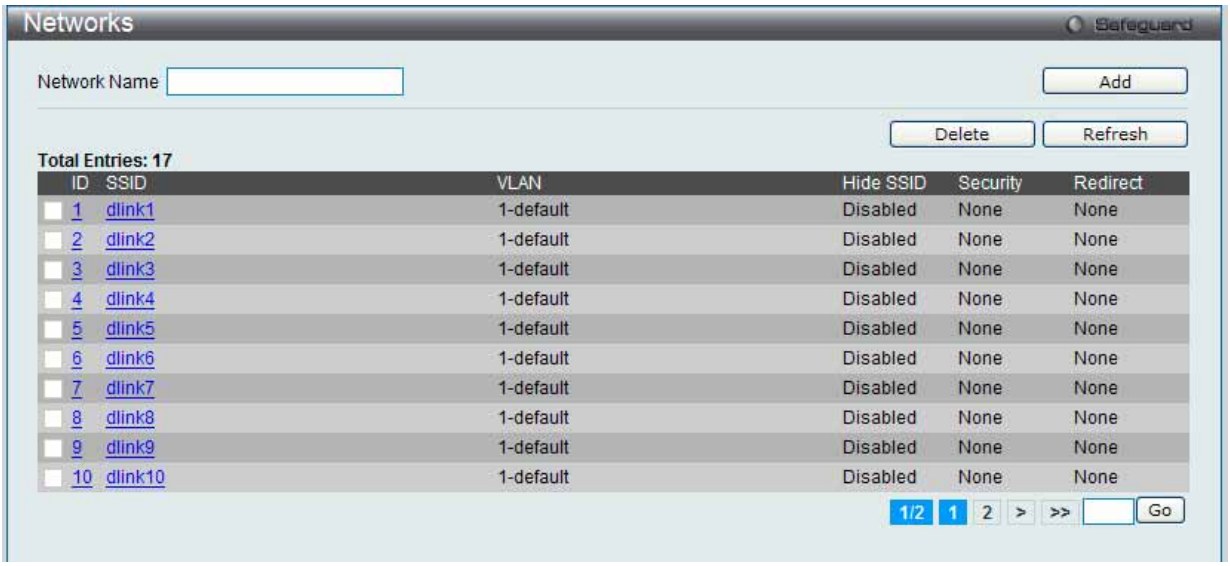


図 8.3-25　Networks 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Network Name	SSID を入力します。

エントリの追加

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

エントリの削除

特定の SSID のボックスをチェック後、「Delete」ボタンをクリックしてエントリを削除します。

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

ネットワークの編集

1. 「ID」または「SSID」ハイパーリンクをクリックして、以下の画面を表示します。

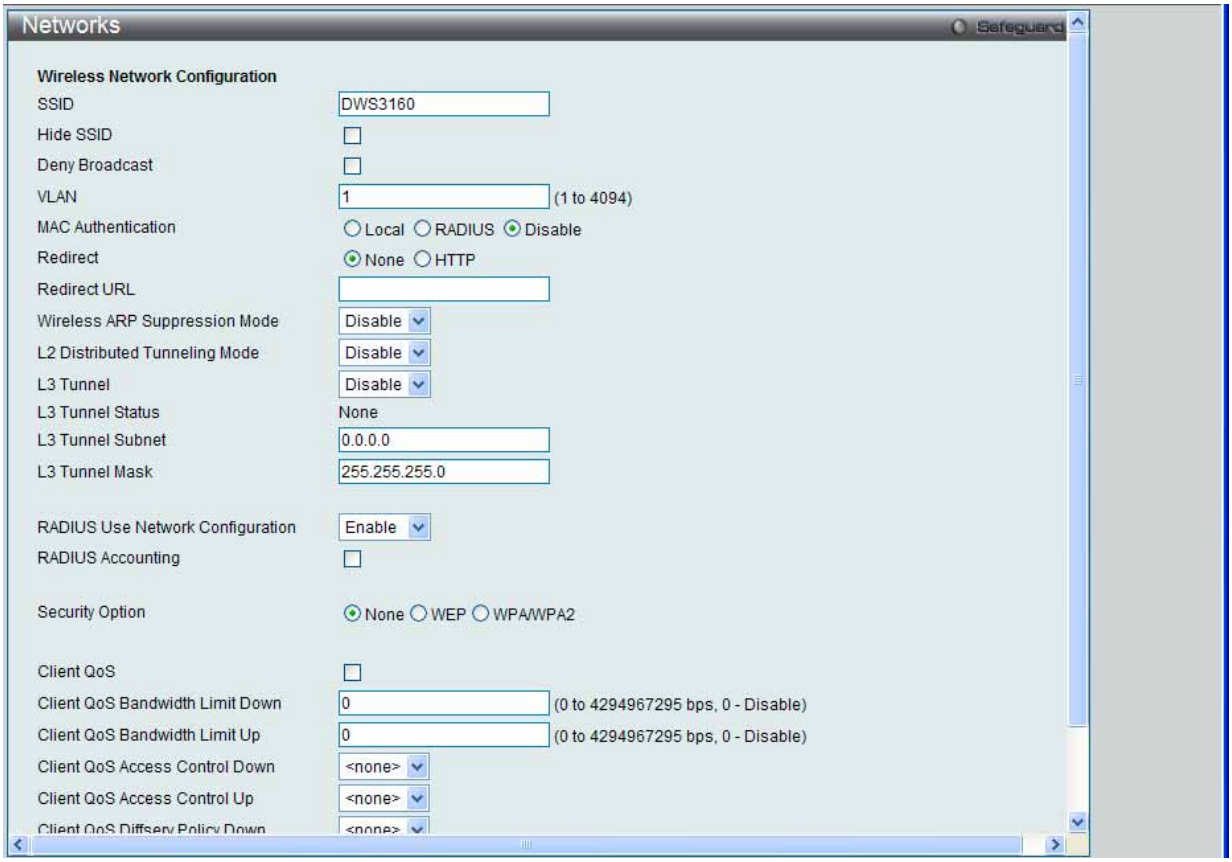


図 8.3-26　Networks - Edit 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
SSID	ネットワークの SSID（Service Set Identifier）を入力します。これは、英数字のキーで無線 LAN を識別します。
Hide SSID	ボックスをチェックして、SSID のブロードキャストを無効にすることにより、ステーションによるアクセスポイントの自動ディスカバリを阻止します。
Deny Broadcast	ボックスをチェックして、アクセスポイントがクライアントプローブ要求に応答することを禁止します。
VLAN	VLAN ID を入力します。
MAC Authentication	「Local」または「RADIUS」をクリックして、MAC 認証を有効にします。ローカルスイッチまたは外部 RADIUS サーバでクライアントの MAC アドレスを設定する必要があります。
Redirect	「HTTP」ボタンをクリックして、カスタム Web 画面に無線クライアントをリダイレクトします。
Redirect URL	すべての初期の HTTP アクセスがリダイレクトされる URL を入力します。HTTP をリダイレクトタイプとして選択した場合にのみ、本欄は表示されます。
Wireless ARP Suppression Mode	本モードを有効にすると、アクセスポイントは、無線インタフェース上でブロードキャストされた ARP 要求数を削減することができます。ブロードキャストの削減は、無線インタフェースの電力の節約に役立ちます。省電力モードを使用する無線クライアントは、ブロードキャストフレームを検出した時に必ず起動するので、より電力を使用します。 **注意** 本機能を有効にすると、DHCP パケットを検出するためにフィルタリングする余分なパケットや、ARP 要求や返答パケットの処理のために、アクセスポイントのパケット転送性能は少し低下します。IPv4 を使用しないネットワークでは、本機能を有効にするべきではありません。

項目	説明	
L2 Distributed Tunneling Mode	分散型 L2 トンネリングモードでは、データトラフィックを統合スイッチに送信することなく、無線クライアントの L3 ローミングをサポートします。メニューを使用して、「Enable」（有効）または「Disable」（無効）にします。 本機能は、統合スイッチがハードウェアの送信アクセラレーションまたはハードウェアベースの L2 トンネルをサポートしない場合に推奨されます。 **注意** **1.** すべてのアクセスポイントを管理するスイッチが 1 つだけで、そのスイッチがダウンした場合、すべてのアクセスポイントは接続する無線電波でシャットダウンし、トンネルを切断します。スイッチが回復し、アクセスポイントが再び管理状態になった後に、以前にトラフィックをトンネルしていたクライアントは再接続され、現在位置するネットワークで IP アドレスを取得します。この IP アドレスは以前にトンネルしていた時に使用していた IP アドレスとは異なり、トラフィックはトンネルされません。 **2.** ピアスイッチを持つネットワークで、そのピアスイッチが管理するアクセスポイント間でトンネルが確立されれば、ホーム AP を管理するスイッチが故障した場合、アソシエーション AP を管理するスイッチは故障を検知してトンネルを切断します。この時点でクライアントは接続を切断されます。クライアントは、再接続した際に新たに IP アドレスを取得します。 **3.** アソシエーション AP を管理するスイッチが故障すると、上記 1 と同様なシナリオになります。アクセスポイントは、すべての無無線電波をダウンさせ、クライアントを切断します。	
L3 Tunnel	L3 トンネル機能を「Enable」（有効）または「Disable」（無効）にします。L3 トンネル機能では、モバイルステーションが 1 つのアクセスポイントから他のアクセスポイントにローミングする際に、これらのアクセスポイントが異なる IP サブネットに属している場合でも IP 接続を維持することができます。 **注意** L3 トンネルが有効である時､VLAN ID は使用されません。実際の運用ではスイッチはトンネリングするパケットに管理用 VLAN ID を記載しています。 **注意** L3 トンネリング機能が使用中に統合スイッチが再起動するなど無線ネットワークトポロジが変更された場合、トンネルされているネットワークへの接続性を再確立する処理を直ちに行うために有線クライアントに対して ARP リフレッシュを実行する必要があります。	
L3 Tunnel Status	L3 トンネリングの状態を表示します。	
L3 Tunnel Subnet	L3 トンネルサブネット。本項目に入力するネットワーク IP アドレスは、スイッチに定義した WLAN 用ルーティングインタフェースと同一サブネット内で指定します。	
L3 Tunnel Mask	L3 トンネルサブネット上のネットワーク IP アドレス用サブネットマスクを入力します。	
RADIUS Use Network Configuration	VAP がネットワークの RADIUS 設定とグローバル RADIUS アカウンティング設定のどちらを使用するかをコントロールします。 • Enable -「Wireless Network Configuration」画面で設定した RADIUS アカウンティングを使用します。 • Disable -「Wireless Global Configuration」画面で設定した RADIUS アカウンティングを使用します。	
RADIUS Accounting	選択すると無線クライアントの RADIUS アカウンティング機能を有効にします。	
Security Option	無線接続のセキュリティメカニズムを選択して、ネットワークを保護します。	
	None	選択すると、ネットワークにセキュリティはなくなります。また、詳しいオプションをアクセスポイントに設定する必要はありません。
	WEP	WEP（Wired Equivalent Privacy）は 802.11 無線ネットワーク用のデータ暗号化プロトコルです。このセキュリティメカニズムを選択すると、ネットワークのすべての無線クライアントとアクセスポイントにはデータ暗号化のために 64 ビット または 128 ビットの共有鍵も設定します。「WEP」を選択すると、以下のオプションが表示されます。 • Static WEP - スタティックキーの管理設定を行います。以下のオプションが表示されます。 - Authentication - ボックスをチェックして、認証タイプを選択します。利用可能なオプションは「Open System」および「Shared Key」です。 - WEP Key Type - ラジオボタンをクリックして、キータイプを選択します。利用可能なオプションは「ASCII」と「HEX」です。ASCII キーはアルファベットの大文字、小文字、数字、および @# などの記号を含みます。Hex キーは数字（0~9）と文字（A~F）を含みます。 - WEP Key Length (bits) - ラジオボタンをクリックして、キー長（64 ビットまたは 128 ビット）を選択します。 - WEP Keys - ラジオボタンをクリックして、特定の変換キーを選択します。テキスト欄には最大 4 つの WEP キーを入力します。キーの文字数は「WEP Key Type」と「WEP Key Length」によって異なります。 • WEP IEEE 802.1X - 以下のオプションが表示されます。: - Bcast Key Refresh Rate - この VAP に接続するクライアントが使用するブロードキャストキーの更新間隔を入力します。 - Session Key Refresh Rate - ユニキャストセッションキーの更新間隔を入力します。

項目	説明	
Security Option	WPA/WPA2	WPA と WPA2 は、AES-CCMP および TKIP メカニズムを含む Wi-Fi Alliance の IEEE802.11i 標準に準拠しています。「WPA/WPA2」を選択すると、以下のオプションが表示されます。 • WPA Personal - これを選択して、スタティックなキー管理を設定します。 - WPA Versions - ボックスをチェックして、サポートするクライアントステーションのタイプを選択します。利用可能なオプションは WPA および WPA2 です。 - WPA Ciphers - ボックスをチェックして、使用する暗号スイートを選択します。利用可能なオプションは TKIP および CCMP(AES) です。 - WPA Key Type - キータイプは ASCII で、アルファベットの大文字、小文字、数字、および @# などの記号を含みます。 - WPA Key - WPA パーソナルで使用する WPA キーは共有秘密鍵です。8-63 文字の文字列に入力します。アルファベットの大文字、小文字、数字、および @# などの記号が入力できます。 - Bcast Key Refresh Rate - この VAP に接続するクライアントが使用するブロードキャストキーの更新間隔を入力します。 • WPA Enterprise - これを選択して、アクセスポイントはグローバル RADIUS サーバまたは無線ネットワークに指定した RADIUS サーバを使用します。 - WPA Versions - ボックスをチェックして、サポートするクライアントステーションのタイプを選択します。利用可能なオプションは WPA および WPA2 です。 - WPA Ciphers - ボックスをチェックして、使用する暗号スイートを選択します。利用可能なオプションは TKIP および CCMP (AES) です。 - Pre-Authentication - ボックスをチェックして、WPA2 無線クライアントによる事前認証パケットの送信を許可します。事前認証情報はアクセスポイントからリレーされます。クライアントは現在ターゲットのアクセスポイントに使用しています。本機能を有効にすると、ローミングするために複数のアクセスポイントと接続するクライアントの認証を高速化することができます。本機能は WPA2 を使用して接続するクライアントのみが利用できます。WPA ではサポートされていません。 - Pre-Authentication Limit - アクセスポイントが同時に扱う事前認証数を入力します。このように制限することにより、RADIUS サーバへの過負荷を防ぐことができます。負荷が軽い状態では、事前認証が再度送信されても制限されません。0 は制限しないことを示しています。 - Key Caching Hold Time - アクセスポイントが PMK を保持している時間（1-1440 分）を指定します。この設定は、RADIUS サーバが生成し、事前認証からアクセスポイントに送信される PMK に適用されます。この時間の制限は、RADIUS サーバがある特定のユーザ用としてここで指定する値よりも大きな値を Session-Timeout に返してきた場合は、その値が優先されますのでご注意ください。値を設定しない場合、無線クライアントがローミングすることを想定して、アクセスポイントは無線クライアントの PMK を他のアクセスポイントに送信しません。 - Bcast Key Refresh Rate - この VAP に接続するクライアントが使用するブロードキャスト（グループ）キーの更新間隔を入力します。 - Session Key Refresh Rate - ユニキャストセッションキーの更新間隔を入力します。
Client QoS	ボックスをチェックして、前の欄の SSID を使用して AP に接続する無線クライアントのクライアント QoS の動作を有効にします。	
Client QoS Bandwidth Limit Down	無線クライアントがアクセスポイントからトラフィックを受信する最大値 (bps) を入力します。	
Client QoS Bandwidth Limit Up	クライアントがアクセスポイントにトラフィックを送信する最大値 (bps) を入力します。	
Client QoS Access Control Down	プルダウンメニューを使用して、外向き（ダウン）方向のトラフィックに適用するアクセスリスト名を選択します。	
Client QoS Access Control Up	プルダウンメニューを使用して、内向き（アップ）方向のトラフィックに適用するアクセスリスト名を選択します。	
Client QoS DiffServ Policy Down	プルダウンメニューを使用して、外向き（ダウン）にアクセスポイントから送信されるトラフィックに適用する DiffServ ポリシー名を選択します。	
Client QoS DiffServ Policy Up	プルダウンメニューを使用して、内向き（アップ）にアクセスポイントから送信されるトラフィックに適用する DiffServ ポリシー名を選択します。	

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

「<<Back」をボタンをクリックし、変更を破棄してと前のページに戻ります。

エントリのクリア

「Clear」をボタンをクリックし、変更を破棄して初期設定に戻します。

AP Profiles（AP プロファイル）

AP プロファイルの作成、設定および削除を行います。

AP プロファイルとはテンプレートのようなもので、作成した AP プロファイルは統合スイッチ管理下のアクセスポイントに適用することができます。

1. **Administration > Advanced Configuration > AP Profiles** の順にメニューをクリックし、以下の画面を表示します。

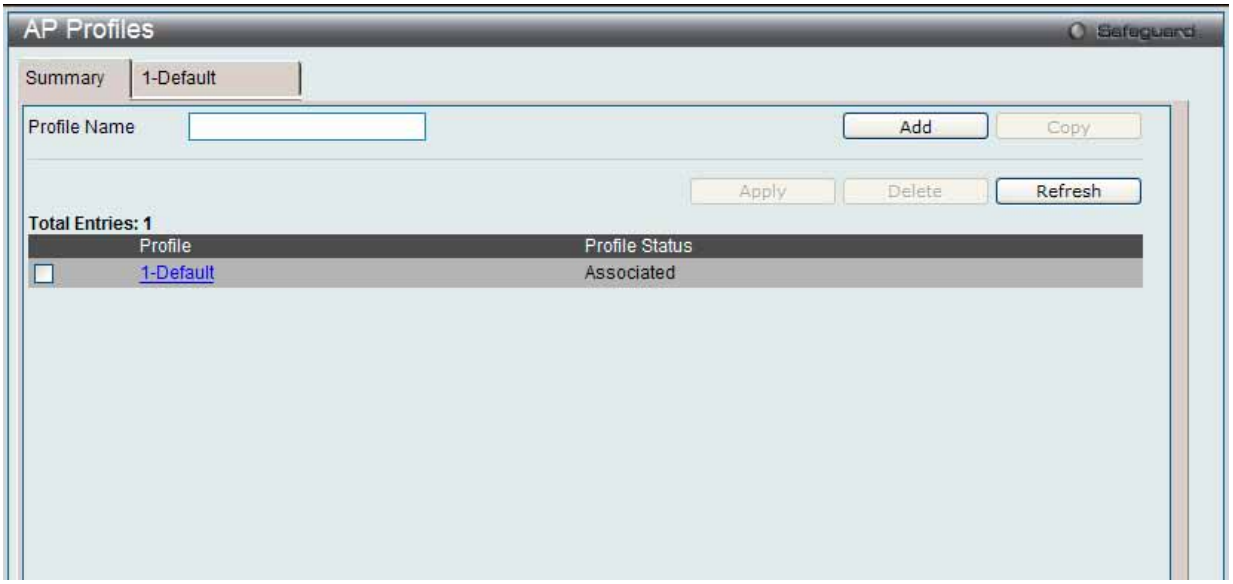


図 8.3-27　AP Profile > Summary 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Profile Name	プロファイル名を入力します。

プロファイルのボックスをチェックし、「Apply」ボタンをクリックして、そのプロファイルを使用するすべてのアクセスポイントにプロファイルを適用します。

エントリの追加

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

プロファイルのコピー

プロファイルのボックスをチェックし、「Copy」ボタンをクリックして、既存のプロファイルの設定を新しいプロファイルにコピーします。

プロファイルの削除

プロファイルのボックスをチェックし、「Delete」ボタンをクリックして、エントリを削除します。

「Refresh」ボタンをクリックしてと、情報を更新します。
「Profile」ハイパーリンクをクリックして、詳細情報を参照します。

Global サブタブ（AP プロファイルの詳細情報の参照）

1. 「Profile」ハイパーリンクまたはプロファイル名を持つタブをクリックすると、以下の画面が表示されます。

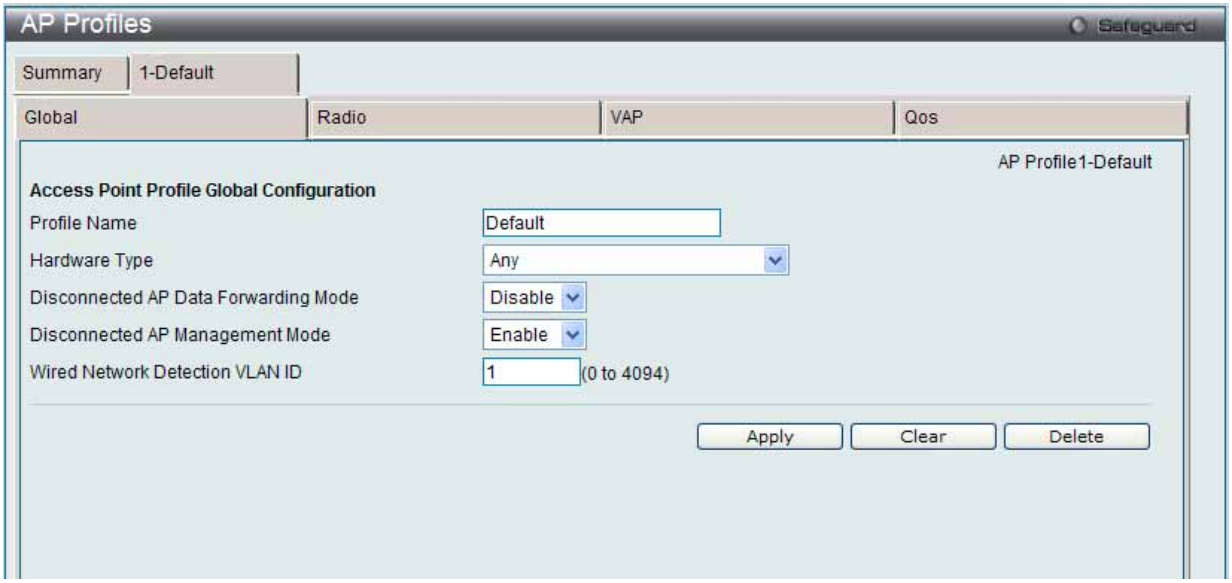


図 8.3-28　AP プロファイル設定 - Global 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Profile Name	アクセスポイントのプロファイル名を入力します。
Hardware Type	プルダウンメニューを使用して、このプロファイルを使用するアクセスポイントに対するハードウェアタイプを選択します。
Disconnected AP Data Forwarding Mode	「Disconnected AP Data Forwarding Mode」（切断時のアクセスポイントデータ転送モード）を「Enabled」（有効）または「Disabled」（無効）にします。モードが有効である場合、管理下のアクセスポイントは、アクセスポイントが無線スイッチとの接続を喪失した場合に既に接続中のクライアントのトラフィックの送信を継続するようにできます。
Disconnected AP Management Mode	「Disconnected AP Management Mode」（切断時のアクセスポイント管理モード）を「Enabled」（有効）または「Disabled」（無効）にします。モードが有効である場合、管理下のアクセスポイントは、アクセスポイントが無線スイッチとの接続を喪失した場合にスタンドアロンの管理機能を有効にします。
Wired Network Detection VLAN ID	スイッチが有線ネットワークに接続するアクセスポイントを検出するためにトレーサパケットを送信するのに使用する VLAN ID を入力します。トレーサパケットは、D-Link 統合アクセスシステムに未所属で有線ネットワークに接続している未認証アクセスポイントをスイッチが識別するのに役立ちます。

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。

エントリのクリア

「Clear」をボタンをクリックし、変更を破棄して初期設定に戻します。

エントリの削除

「Delete」ボタンをクリックして、エントリを削除します。

Radio サブタブ

1. プロファイル名タブの「Radio」サブタブをクリックして、以下の画面を表示します。

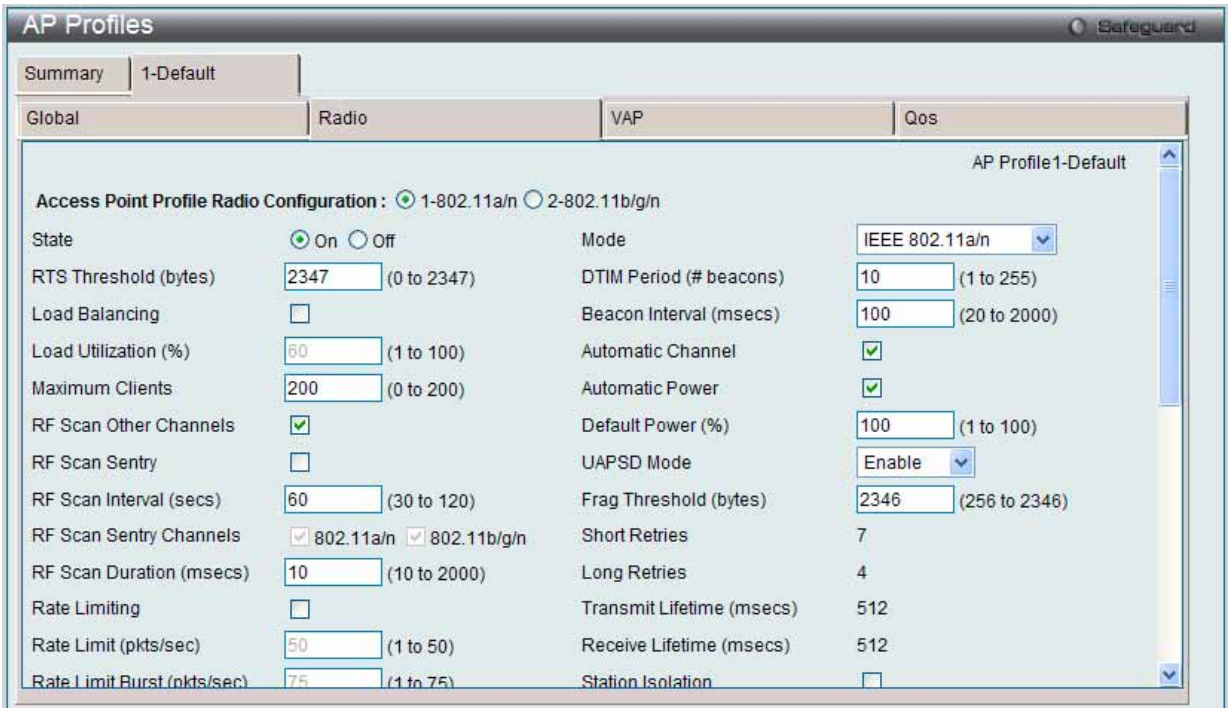


図 8.3-29　AP プロファイル設定 - - Radio 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Access Point Profile Radio Configuration	ラジオボタンをクリックして、無線帯域（802.11a/n および 802.11b/g/n）を選択します。
State	「On」または「Off」ボタンを選択して、無線帯域をオンまたはオフにします。
Mode	無線帯域が使用する物理レイヤの標準を選択します。「Access Point Profile Radio Configuration」で「1-802.11a/n」を選択すると、利用可能なオプションは、「IEEE 802.11a」と「IEEE 802.11a/n」、および「5GHz IEEE 802.11n」です。「Access Point Profile Radio Configuration」で「2-802.11b/g/n」を選択すると、利用可能なオプションは、「IEEE 802.11b/g」と「IEEE 802.11b/g/n」、および「2.4GHz IEEE 802.11n」です。
RTS Threshold (bytes)	Request to Send (RTS) しきい値を 0-2347 の範囲で指定します。RTS しきい値は、MPDU 内のオクテット数を示します。設定値より低いと RTS/CTS ハンドシェークは実行されません。この値を変更することで、特に多数のクライアントを抱えるアクセスポイントを通過するトラフィックフローの制御をすることができます。低い値を指定すると、RTS パケットは頻繁に送信されるようになります。これにより消費する帯域幅は増大し、パケットのスループットは低下します。一方、RTS パケットの送信数を増やす、混雑したネットワーク内で起こり得る干渉や衝突からの回避や、電磁波による干渉を軽減できるようになります。
DTIM Period (# beacons)	本アクセスポイントの配下にあるクライアントが、送信待ちしているアクセスポイントにバッファされているデータを確認する Delivery Traffic Information Map (DTIM) 間隔（1-255）を指定します。DTIM メッセージはビーコンフレームに含まれる要素です。DTIM は省電力モード中の無線クライアント向けのデータがアクセスポイントに送信待ちとしてバッファされていることを示しています。ここで指定する DTIM Period（DTIM 間隔）は、本アクセスポイントの配下にあるクライアントが、アクセスポイントにバッファされているデータを確認する間隔を示します。数字はビーコンの数で表します。例えば、本欄に「1」と入力した場合、バッファされたデータの確認は、ビーコンフレーム送信ごとにアクセスポイントで行われます。「10」と入力した場合は 10 回のビーコンフレーム送信に 1 度の確認となります。
Beacon Interval (msecs)	無線ネットワークの存在を通知するために、アクセスポイントがビーコンフレームを送信する間隔（20-2000）を指定します。初期状態では、ビーコンフレームは 100（ミリ秒）に 1 度（1 秒に 10 回）送信されます。単位はミリ秒です。
Load Balancing	チェックボックスを使用して、ロードバランシングを有効にします。有効にすると、アクセスポイントに許可するトラフィック量を制御することができます。
Local Utilization (%)	その無線帯域に許可されるネットワーク帯域使用率 (%) のしきい値を入力します。レベルがしきい値に到達すると、アクセスポイントは新しいクライアントとの接続を停止します。
Maximum Clients	本アクセスポイントに接続できるステーションの最大数を指定します。
Automatic Channel	ボックスをチェックすると、本プロファイルを割り当てたアクセスポイントの無線帯域では、自動チャンネル選択が可能になります。
Automatic Power	ボックスをチェックすると、RF 信号を正しい距離にブロードキャストするように自動的に調整します。

項目	説明
Default Power (%)	RF 信号の最大送信電力（%）を入力します。「Automatic Power」ボックスを選択すると、RF 信号電力の初期設定が使用されます。または、固定の RF 信号電力設定が使用されます。自動 RF 信号電力調整アルゴリズムは、本欄で設定した数値以下に電力を下げることはありません。初期値は 100% です。
RF Scan Other Channels	チェックボックスを選択すると、無線帯域が定期的に操作チャンネルから移動し、他のチャンネルのスキャンを行うことができます。
RF Scan Sentry	チェックボックスを選択すると、無線帯域は Sentry（監視）モードで動作することができます。
RF Scan Interval (secs)	RF スキャン中のチャンネル変更の間隔を入力します。
RF Scan Sentry Channels	無線帯域は 802.11b/g/n（2.4 GHz）と 802.11a/n（5 GHz）または両無線電波が使用する周波数内のチャンネルのスキャンを行います。スキャンの対象となる無線電波のチャンネルを選択します。
RF Scan Duration (msecs)	RF スキャン時に他のチャンネルのスキャンに無線帯域が要する時間（ミリ秒）を指定します。
Rate Limiting	マルチキャストとブロードキャスト速度制限を有効にすると、ネットワークを経由して送信されるパケット数を制限することによって、全体的なネットワーク性能を改善することができます。
Rate Limit (pkts/sec)	マルチキャストとブロードキャストトラフィックに設定する速度制限を入力します。
Rate Limit Burst (pkts/sec)	速度を制限するバースト値を設定すると、すべてのトラフィックが速度制限を超える前のトラフィックバーストの量を決定します。
Channel Bandwidth	プルダウンメニューを使用して、チャンネル帯域幅の使用を 20MHz または 40MHz に制限します。
Protection	「Auto」を選択すると、802.11 の伝送がレガシーステーションまたはアプリケーションで干渉を起こさないことを保証します。「Off」を選択すると、保護メカニズムを無効にします。
Space Time Block Code	「Enable」を選択すると、同時に、複数アンテナに同じデータストリームを転送します。
No ACK	「Enable」を選択して、アクセスポイントがサービスクラス値として QosNoAck を持つフレームを承認するべきでないことを指定します。
UAPSD Mode	「Enable」を選択して、電源管理方法である自動省電力機能 (APSD) を有効にします。
Frag Threshold (bytes)	ネットワーク上で伝送されるパケットサイズを制限します。入力したサイズ以下のパケットはフラグメント化されません。2346 の入力は、パケットはフラグメント化されないことを示します。
Short Retries	RTS Threshold と同じか、またはそれより小さいサイズのフレーム送信の最大リトライ回数を示します。
Long Retries	RTS Threshold より大きいサイズのフレーム送信の最大リトライ回数を示します。
Transmit Lifetime (msecs)	最初の MSDU 送信から送信リトライを終了までの時間（ミリ秒）を指定します。
Receive Lifetime (msecs)	最初にフラグメント化された MMPDU または MSDU を受信してから、MMPDU または MSDU 再構築のリトライを終了するまでの時間（ミリ秒）を指定します。
Station Isolation	ボックスをチェックすると、アクセスポイントが無線クライアント間の通信をブロックします。
Primary Channel	40MHz 帯域の上位または下位 20MHz のチャンネルとして Primary Channel を設定します。本オプションは「Channel Bandwidth」が「40MHz」に設定されている場合のみ利用可能です。
Short Guard Interval	802.11n モードで動作時のショートガードインターバルを「Enabled」（有効）または「Disabled」（無効）にします。
Multicast Tx Rate (Mbps)	帯域がマルチキャストフレームを転送するのに 802.11 レートを選択します。
Supported Channels	無線帯域でサポートしているチャンネルを表示します。「Basic Setup > Global」画面で選択した「Country Code」に基づいて有効なチャンネルが変わります。
Auto Eligible	各チャンネル下のチェックボックスを選択すると、自動チャンネル割り当てプロセスにそのチャンネルを含めます。
Available MSC Indices	チェックボックスを選択して、802.11n モードで動作する際の MCS Index を追加します。
Rate Sets (Mbps)	通信速度設定を表示します。
Basic	チェックボックスを選択して、アクセスポイントに接続するすべてのステーションがサポートすべきデータ速度を示します。
Supported	チェックボックスを選択して、アクセスポイントがサポートする速度を示します。エラー率やアクセスポイントとクライアントとの距離などの要素をもとに、アクセスポイントは最も効率の良い速度を自動的に選択します。

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。

エントリのクリア

「Clear」をボタンをクリックし、変更を破棄して初期設定に戻します。

VAP サブタブ

1. プロファイル名タブの「VAP」サブタブをクリックすると、以下の画面が表示されます。

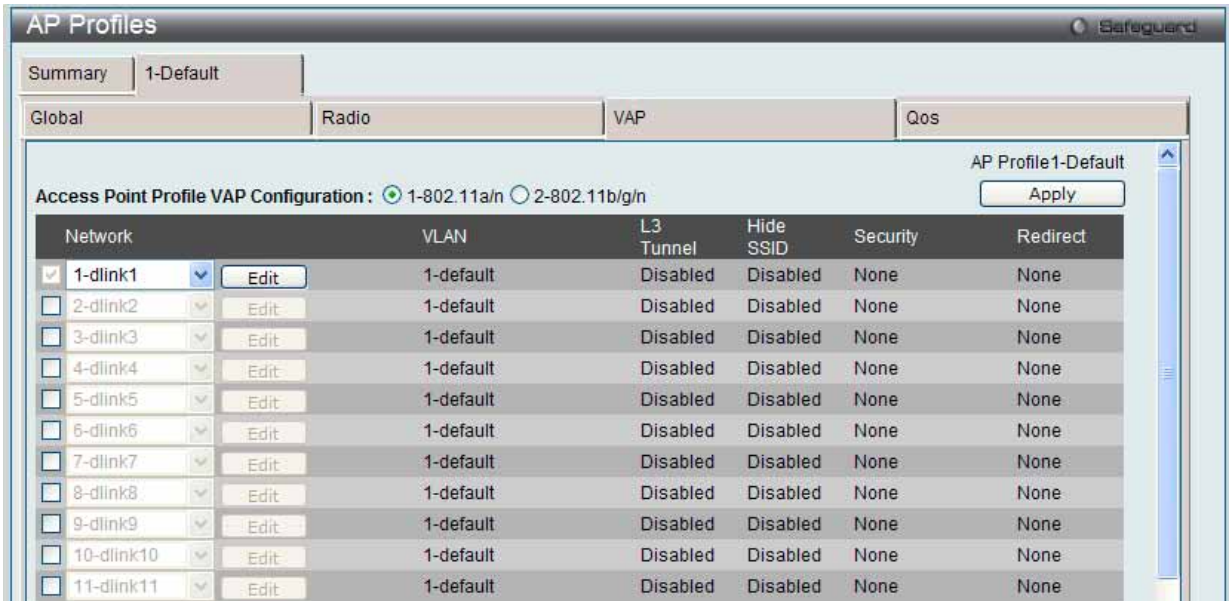


図 8.3-30　AP プロファイル名 - VAP 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Access Point Profile VAP Configuration	VAP を有効にする前に、設定する無線帯域を選択します。
Network	ボックスをチェックして、選択した無線帯域に対応する VAP を有効にします。プルダウンメニューを使用して、VAP に割り当てるネットワークを選択します。

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。

「Edit」ボタンをクリックして、対応するネットワークの設定を編集します。

VAP の編集

1. 「Edit」ボタンをクリックすると、以下の画面が表示されます。

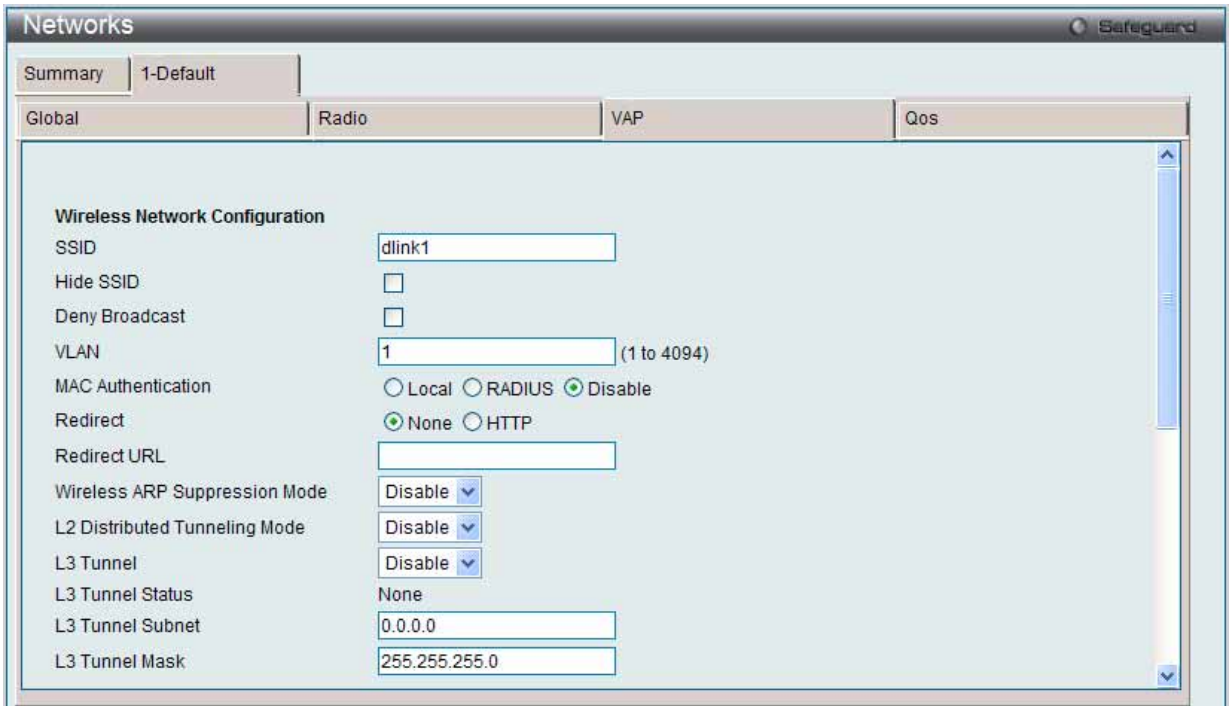


図 8.3-31　AP プロファイル設定 - VAP (Edit) 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
SSID	ネットワークの SSID（Service Set Identifier）を入力します。これは、英数字のキーで無線 LAN を識別します。
Hide SSID	ボックスをチェックして、SSID のブロードキャストを無効にすることにより、ステーションによるアクセスポイントの自動ディスカバリを阻止します。
Deny Broadcast	ボックスをチェックして、アクセスポイントがクライアントプローブ要求に応答することを禁止します。
VLAN	VLAN ID を入力します。
MAC Authentication	「Local」または「RADIUS」をクリックして、MAC 認証を有効にします。ローカルスイッチまたは外部 RADIUS サーバでクライアントの MAC アドレスを設定する必要があります。
Redirect	「HTTP」ボタンをクリックして、カスタム Web 画面に無線クライアントをリダイレクトします。
Redirect URL	すべての初期の HTTP アクセスがリダイレクトされる URL を入力します。HTTP をリダイレクトタイプとして選択した場合にのみ、本欄は表示されます。
Wireless ARP Suppression Mode	本モードを有効にすると、アクセスポイントは、無線インタフェース上でブロードキャストされた ARP 要求数を削減することができます。ブロードキャストの削減は、無線インタフェースの電力の節約に役立ちます。省電力モードを使用する無線クライアントは、ブロードキャストフレームを検出した時に必ず起動するので、より電力を使用します。 **注意** 本機能を有効にすると、DHCP パケットを検出するためにフィルタリングする余分なパケットや、ARP 要求や返答パケットの処理のために、アクセスポイントのパケット転送性能は少し低下します。IPv4 を使用しないネットワークでは、本機能を有効にするべきではありません。
L2 Distributed Tunneling Mode	Distributed L2 トンネリングモードでは、データトラフィックを統合スイッチに送信することなく、無線クライアントの L3 ローミングをサポートします。メニューを使用して、「Enabled」（有効）または「Disabled」（無効）にします。 本機能は、統合スイッチがハードウェアの送信アクセラレーションまたはハードウェアベースの L2 トンネルをサポートしない場合に推奨されます。 **注意** **1.** すべてのアクセスポイントを管理するスイッチが 1 つだけで、そのスイッチがダウンした場合、すべてのアクセスポイントは接続する無線帯域でシャットダウンし、トンネルを切断します。スイッチが回復し、アクセスポイントが再び管理状態になった後に、以前にトラフィックをトンネルしていたクライアントは再接続され、現在位置するネットワークで IP アドレスを取得します。この IP アドレスは以前にトンネルしていた時に使用していた IP アドレスとは異なり、トラフィックはトンネルされません。 **2.** ピアスイッチを持つネットワークで、そのピアスイッチが管理するアクセスポイント間でトンネルが確立されれば、ホーム AP を管理するスイッチが故障した場合、アソシエーション AP を管理するスイッチは故障を検知してトンネルを切断します。この時点でクライアントは接続を切断されます。クライアントは、再接続した際に新たに IP アドレスを取得します。 **3.** アソシエーション AP を管理するスイッチが故障すると、上記 1 と同様なシナリオになります。アクセスポイントは、すべての無線帯域をダウンさせ、クライアントを切断します。
L3 Tunnel	L3 トンネル機能を「Enable」（有効）または「Disable」（無効）にします。L3 トンネル機能では、モバイルステーションが 1 つのアクセスポイントから他のアクセスポイントにローミングする際に、これらのアクセスポイントが異なる IP サブネットに属している場合でも IP 接続を維持することができます。 **注意** L3 トンネルが有効である時、VLAN ID は使用されません。実際の運用ではスイッチはトンネリングするパケットに管理用 VLAN ID を記載しています。 **注意** L3 トンネリング機能が使用中に統合スイッチが再起動するなど無線ネットワークトポロジが変更された場合、トンネルされているネットワークへの接続性を再確立する処理を直ちに行うために有線クライアントに対して ARP リフレッシュを実行する必要があります。
L3 Tunnel Status	L3 トンネリングの状態を表示します。
L3 Tunnel Subnet	L3 トンネルサブネット。本項目に入力するネットワーク IP アドレスは、スイッチに定義した WLAN 用ルーティングインタフェースと同一サブネット内で指定します。
L3 Tunnel Mask	L3 トンネルサブネット上のネットワーク IP アドレス用サブネットマスクを入力します。
RADIUS Use Network Configuration	VAP がネットワークの RADIUS 設定とグローバル RADIUS アカウンティング設定のどちらを使用するかをコントロールします。 • Enable -「Wireless Network Configuration」画面で設定した RADIUS アカウンティングを使用します。 • Disable -「Wireless Global Configuration」画面で設定した RADIUS アカウンティングを使用します。
RADIUS Accounting	選択すると無線クライアントの RADIUS アカウンティング機能を有効にします。

項目	説明	
Security	無線接続のセキュリティメカニズムを選択して、ネットワークを保護します。	
	None	選択すると、ネットワークにセキュリティはなくなります。また、詳しいオプションをアクセスポイントに設定する必要はありません。
	WEP	WEP（Wired Equivalent Privacy）は 802.11 無線ネットワーク用のデータ暗号化プロトコルです。このセキュリティメカニズムを選択すると、ネットワークのすべての無線クライアントとアクセスポイントにはデータ暗号化のために 64 ビット または 128 ビットの共有鍵も設定します。「WEP」を選択すると、以下のオプションが表示されます。 • Static WEP - スタティックキーの管理設定を行います。以下のオプションが表示されます。 - Authentication - ボックスをチェックして、認証タイプを選択します。利用可能なオプションは「Open System」および「Shared Key」です。 - WEP Key Type - ラジオボタンをクリックして、キータイプを選択します。利用可能なオプションは「ASCII」と「HEX」です。ASCII キーはアルファベットの大文字、小文字、数字、および @# などの記号を含みます。Hex キーは数字（0~9）と文字（A~F）を含みます。 - WEP Key Length (bits) - ラジオボタンをクリックして、キー長（64 ビットまたは 128 ビット）を選択します。 - WEP Keys - ラジオボタンをクリックして、特定の変換キーを選択します。テキスト欄には最大 4 つの WEP キーを入力します。キーの文字数は「WEP Key Type」と「WEP Key Length」によって異なります。 • WEP IEEE 802.1X - 以下のオプションが表示されます。: - Bcast Key Refresh Rate - この VAP に接続するクライアントが使用するブロードキャストキーの更新間隔を入力します。 - Session Key Refresh Rate - ユニキャストセッションキーの更新間隔を入力します。
	WPA/ WPA2	WPA と WPA2 は、AES-CCMP および TKIP メカニズムを含む Wi-Fi Alliance の IEEE802.11i 標準に準拠しています。「WPA/WPA2」を選択すると、以下のオプションが表示されます。 • WPA Personal - これを選択して、スタティックなキー管理を設定します。 - WPA Versions - ボックスをチェックして、サポートするクライアントステーションのタイプを選択します。利用可能なオプションは WPA および WPA2 です。 - WPA Ciphers - ボックスをチェックして、使用する暗号スイートを選択します。利用可能なオプションは TKIP および CCMP(AES) です。 - WPA Key Type - キータイプは ASCII で、アルファベットの大文字、小文字、数字、および @# などの記号を含みます。 - WPA Key - WPA パーソナルで使用する WPA キーは共有秘密鍵です。8-63 文字の文字列に入力します。アルファベットの大文字、小文字、数字、および @# などの記号が入力できます。 - Bcast Key Refresh Rate - この VAP に接続するクライアントが使用するブロードキャストキーの更新間隔を入力します。 • WPA Enterprise - これを選択して、アクセスポイントはグローバル RADIUS サーバまたは無線ネットワークに指定した RADIUS サーバを使用します。 - WPA Versions - ボックスをチェックして、サポートするクライアントステーションのタイプを選択します。利用可能なオプションは WPA および WPA2 です。 - WPA Ciphers - ボックスをチェックして、使用する暗号スイートを選択します。利用可能なオプションは TKIP および CCMP(AES) です。 - Pre-Authentication - ボックスをチェックして、WPA2 無線クライアントによる事前認証パケットの送信を許可します。事前認証情報はアクセスポイントからリレーされます。クライアントは現在ターゲットのアクセスポイントに使用しています。本機能を有効にすると、ローミングするために複数のアクセスポイントと接続するクライアントの認証を高速化することができます。本機能は WPA2 を使用して接続するクライアントのみが利用できます。WPA ではサポートされていません。 - Pre-Authentication Limit - アクセスポイントが同時に扱う事前認証数を入力します。このように制限することにより、RADIUS サーバへの過負荷を防ぐことができます。負荷が軽い状態では、事前認証が再度送信されても制限されません。0 は制限しないことを示しています。 - Key Caching Hold Time - アクセスポイントが PMK を保持している時間（分）を指定します。この設定は、RADIUS サーバが生成し、事前認証からアクセスポイントに送信される PMK に適用されます。この時間の制限は、RADIUS サーバがある特定のユーザ用としてここで指定する値よりも大きな値を Session-Timeout に返してきた場合は、その値が優先されますのでご注意ください。1-1440（分）以上で設定します。値を設定しない場合、無線クライアントがローミングすることを想定して、アクセスポイントは無線クライアントの PMK を他のアクセスポイントに送信しません。 - Bcast Key Refresh Rate - このVAPに接続するクライアントが使用するブロードキャスト(グループ)キーの更新間隔を入力します。 - Session Key Refresh Rate - ユニキャストセッションキーの更新間隔を入力します。

項目	説明
Client QoS	ボックスをチェックして、前の欄の SSID を使用して AP に接続する無線クライアントのクライアント QoS の動作を有効にします。
Client QoS Bandwidth Limit Down	無線クライアントがアクセスポイントからトラフィックを受信する最大値 (bps) を入力します。
Client QoS Bandwidth Limit Up	クライアントがアクセスポイントにトラフィックを送信する最大値 (bps) を入力します。
Client QoS Access Control Down	プルダウンメニューを使用して、外向き（ダウン）方向のトラフィックに適用するアクセスリスト名を選択します。
Client QoS Access Control Up	プルダウンメニューを使用して、内向き（アップ）方向のトラフィックに適用するアクセスリスト名を選択します。
Client QoS DiffServ Policy Down	プルダウンメニューを使用して、外向き（ダウン）にアクセスポイントから送信されるトラフィックに適用する DiffServ ポリシー名を選択します。
Client QoS DiffServ Policy Up	プルダウンメニューを使用して、内向き（アップ）にアクセスポイントから送信されるトラフィックに適用する DiffServ ポリシー名を選択します。

QoS サブタブ

プロファイル名タブの「QoS」サブタブをクリックして、以下の画面を表示します。

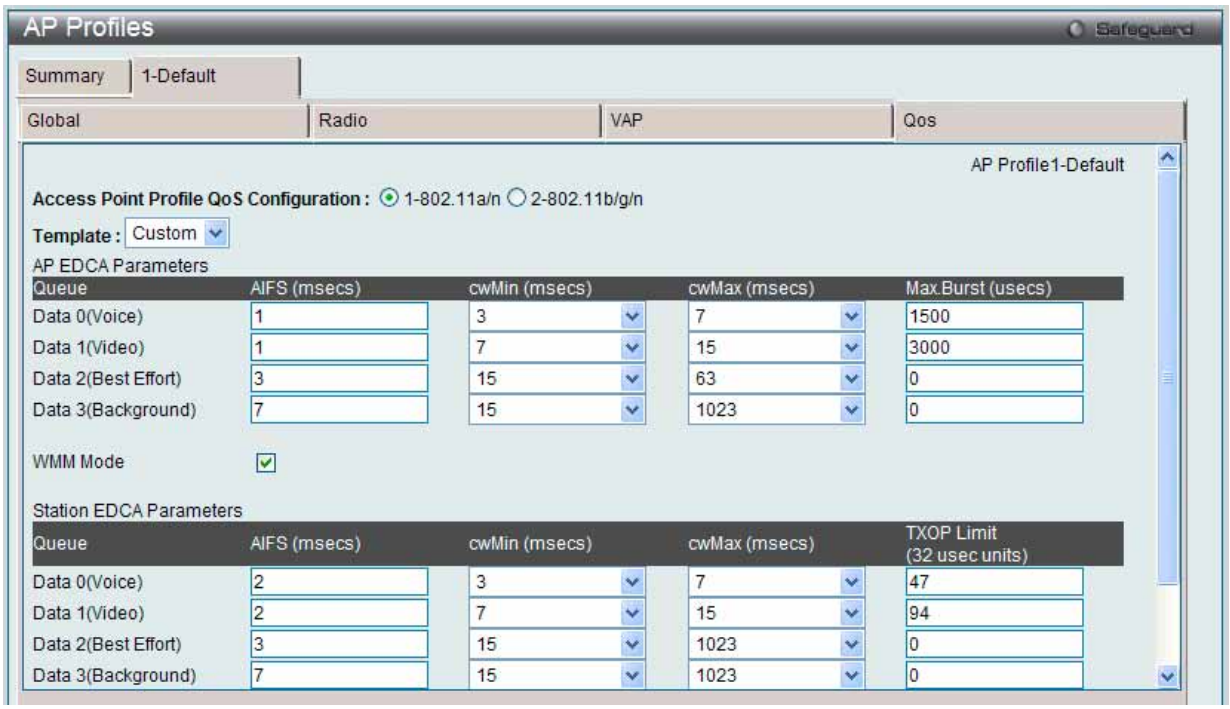


図 8.3-32　AP プロファイル設定 - QoS 画面

以下の表では、QoS の設定項目について説明します。

項目	説明
Access Point Profile QoS Configuration	ラジオボタンをクリックして、無線帯域 (802.11a/n および 802.11b/g/n) を選択します。
Template	プルダウンメニューを使用して QoS のテンプレートを選択します。 利用可能なオプションは、Custom、Default および Voice です。自身の QoS がメカニズムを作成するためには「Custom」を選択します。
AP EDCA Parameters / Station EDCA Parameters	
Queue	アクセスポイントからステーション (AP EDCA Parameters) まで、またはステーションからアクセスポイント (Station EDCA Parameters) まで送信される各データのタイプを表示します。
AIFS (msecs)	データフレームの待ち時間を入力します。
cwMin (msecs)	伝送リトライの「初回ランダムバックオフ待ち時間」（画面）を決定するアルゴリズムを入力します。
cwMax (msecs)	上限（ミリ秒）を入力します。ランダムバックオフ値の 2 倍にします。
Max.Burst (usecs)	無線ネットワークでのパケットバーストに許可される最大バースト長（ミリ秒）を入力します。
TXOP Limit (32 usec units)	WMM クライアントステーションが無線ネットワークで伝送を開始する間隔を入力します。
WMM Mode	チェックして、WMM モードを有効にします。

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

Peer Switch（ピアスイッチ）

1 つのスイッチから他のすべてのスイッチに様々な設定情報を送信します。スイッチの同期を維持することに加え、本機能は 1 つのスイッチからクラスタ内のすべての無線スイッチを管理することができます。

Configuration Request タブ

1. **Administration > Advanced Configuration > Peer Switch > Configuration Request タブ**の順にメニューをクリックし、以下の画面を表示します。

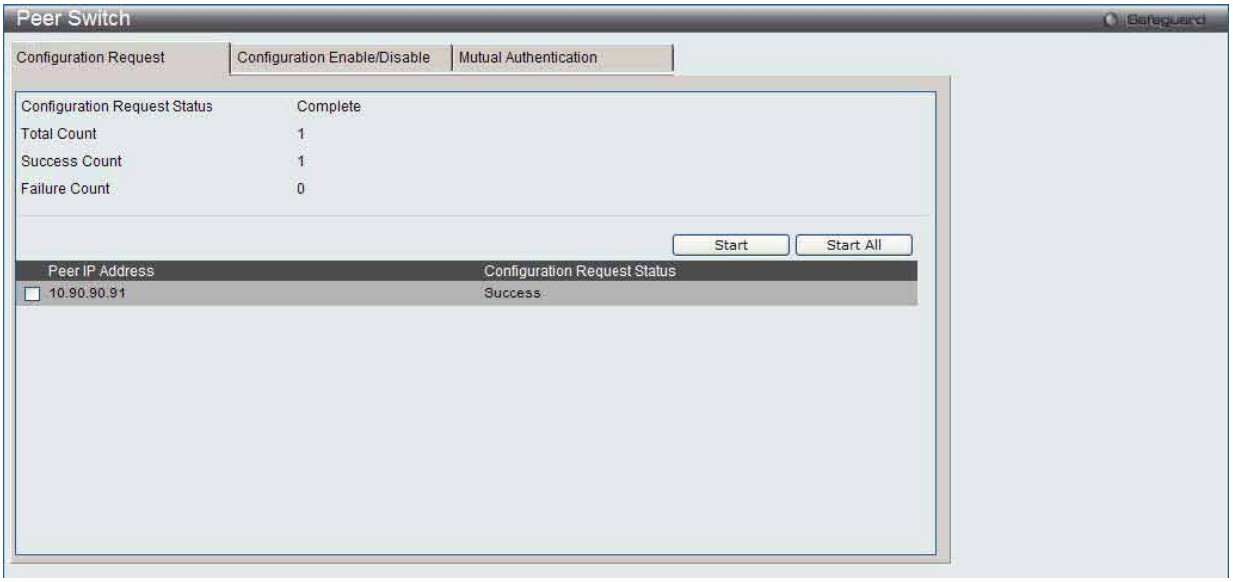


図 8.3-33　Peer Switch > Configuration Request 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Configuration Request Status	複数のピアスイッチにコンフィグレーションの書き込みを実施している時のグローバルなステータスを表示します。以下のいずれかのステータスが表示されます。 • Not Started - 開始していません。 • Receiving Configuration - コンフィグレーションを受信中です。 • Saving Configuration - コンフィグレーションを保存中です。 • Success - 成功 • Failure - Invalid Code Version - 不正なコードバージョン • Failure - Invalid Hardware Version - 不正なハードウェアバージョン • Failure - Invalid Configuration - 不正なコンフィグレーション
Total Count	コンフィグレーションのダウンロードリクエストが開始された場合に含まれるピアスイッチ数を表示します。ダウンロードリクエストが 1 つのスイッチに行われた場合、値は 1 です。
Success Count	コンフィグレーションのダウンロードに成功したピアスイッチの総数を表示します。
Failure Count	コンフィグレーションのダウンロードに失敗したピアスイッチの総数を表示します。
Peer IP Address	クラスタ内の各スイッチの IP アドレスを表示します。
Configuration Request Status	クラスタ内のスイッチのコンフィグレーションリクエストのステータスを表示します。

指定ピアスイッチにコンフィグレーション更新を開始するために、更新するピアスイッチの IP アドレスの横のボックスを選択し、「Start」ボタンをクリックします。すべてのピアスイッチを更新するために、「Start All」ボタンをクリックします。

Configuration Enable/Disable タブ

1. **Administration > Advanced Configuration > Peer Switch > Configuration Enable/Disable タブ**の順にメニューをクリックし、以下の画面を表示します。

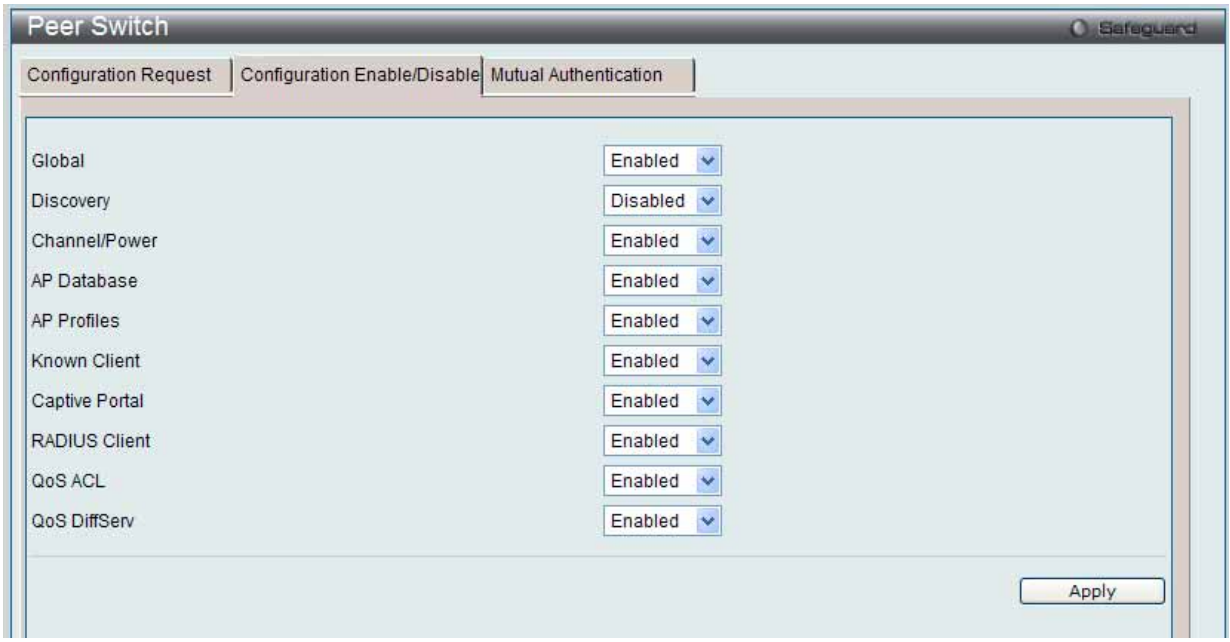


図 8.3-34　Peer Switch > Configuration Enable/Disable 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Global	「Enabled」を選択すると、スイッチがピアに設定するコンフィグレーションに基本および高度なグローバル設定を含めます。
Discovery	「Enabled」を選択すると、スイッチがピアに設定するコンフィグレーションに VLAN リストおよび IP リストを含む L2/L3 ディスカバリ情報を含めます。
Channel/Power	「Enabled」を選択すると、スイッチがピアに設定するコンフィグレーションに RF 管理情報を含めます。
AP Database	「Enabled」を選択すると、スイッチがピアに設定するコンフィグレーションにアクセスポイントデータベースを含めます。
AP Profiles	「Enabled」を選択すると、スイッチがピアに設定するコンフィグレーションにすべての AP プロファイルを含めます。
Known Client	「Enabled」を選択すると、スイッチがピアに設定するコンフィグレーションに Known Client データベースを含めます。
Captive Portal	「Enabled」を選択すると、スイッチがピアに設定するコンフィグレーションにキャプティブポータル情報を含めます。
RADIUS Client	「Enabled」を選択すると、スイッチがピアに設定するコンフィグレーションに Client RADIUS 情報を含めます。
QoS ACL	「Enabled」を選択すると、スイッチがピアに設定するコンフィグレーションに QoS ACL を含めます。
QoS DiffServ	「Enabled」を選択すると、スイッチがピアに設定するコンフィグレーションに Diffserv クラス、サービス、およびポリシーを含めます。

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。

Mutual Authentication タブ

1. **Administration > Advanced Configuration > Peer Switch > Mutual Authentication タブ**の順にメニューをクリックし、以下の画面を表示します。

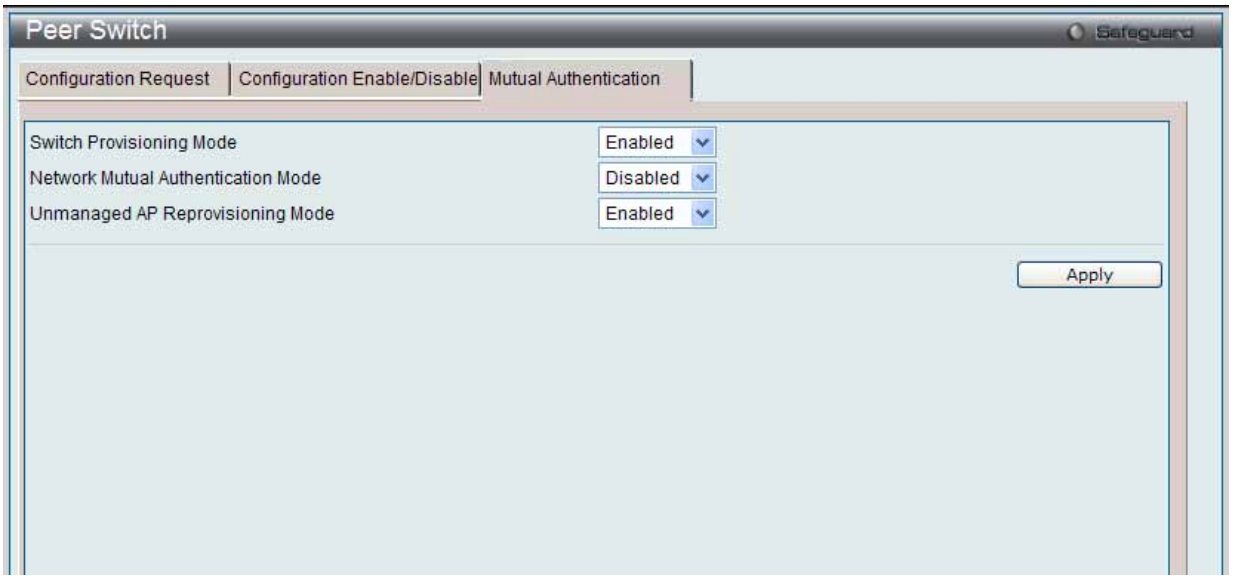


図 8.3-35　Peer Switch Mutual Authentication 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Switch Provisioning Mode	「Enabled」を選択すると、スイッチのプロビジョニングモードを有効にします。
Network Mutual Authentication Mode	「Enabled」を選択すると、すべてのネットワークの相互認証を有効にします。
Unmanaged AP Reprovisioning Mode	「Enabled」を選択すると、管理されていないアクセスポイントのリプロビジョニングを有効にします。

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

WIDS Security（WIDS セキュリティ）

D-Link 統合スイッチの Wireless Intrusion Detection System（WIDS）は、無線ネットワークへの侵入の試みを検出するのを補助し、ネットワークを保護するために自動的にアクションを実行することができます。

AP Configuration タブ（WIDS AP 設定）

1. **Administration > Advanced Configuration > WIDS Security > AP Configuration タブ**の順にメニューをクリックし、以下の画面を表示します。

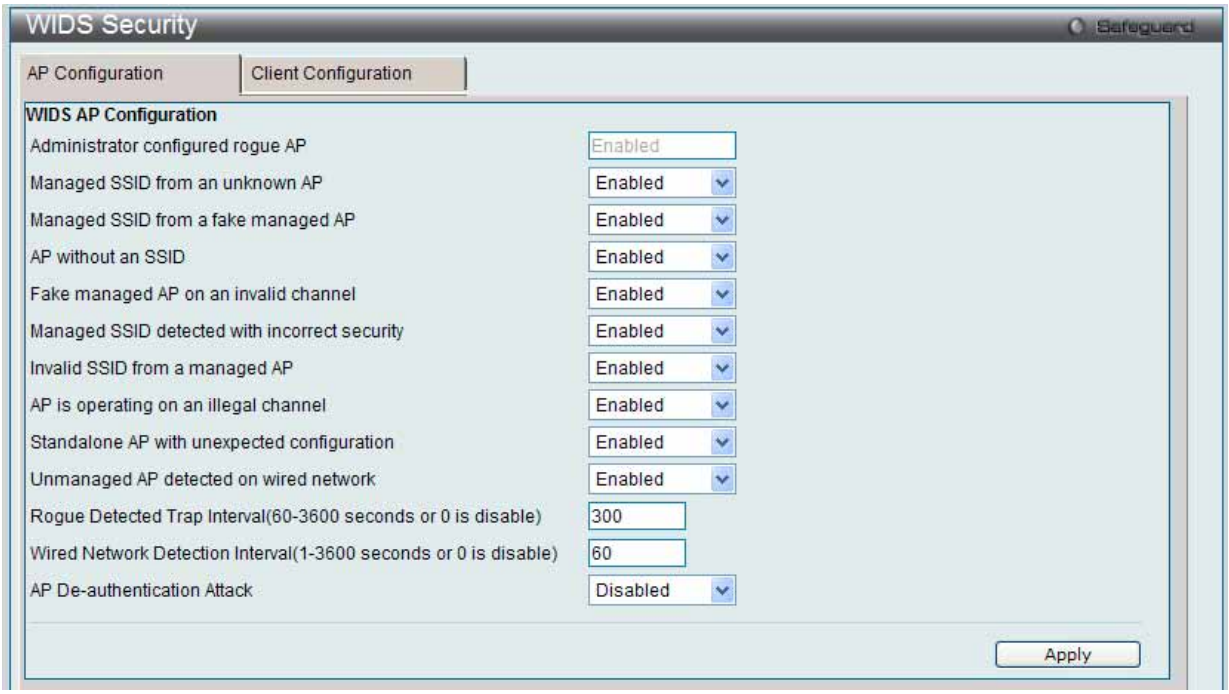


図 8.3-36　WIDS Security > AP Configuration 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Administrator configured rogue AP	送信元 MAC アドレスが、スイッチまたは RADIUS サーバにおける Valid-AP データベースにあり、AP タイプが「Rogue」としてマークされる場合、AP ステートは「不正」です。
Managed SSID from an unknown AP	未知のアクセスポイントが管理されたネットワーク SSID を使用しているかどうかをチェックします。ハッカーは、管理 SSID を持つアクセスポイントを設定することでユーザをだましてアクセスポイントへの接続、パスワードや他のセキュアな情報の開示を行うかもしれません。 複数のクラスタを使用している大規模ネットワークの管理者は、各クラスタで異なるネットワーク名を使用するか、またはこのテストを無効にするべきです。そうでないと、最初のクラスタが 2 番目のクラスタに最初のクラスタ内のアクセスポイントと同じ SSID を送信するアクセスポイントを検出すると、これらのアクセスポイントは Rogue として報告されます。
Managed SSID from a fake managed AP	ハッカーは、管理アクセスポイントの 1 つと同じ MAC アドレスでアクセスポイントを設定し、また、その管理 SSID の 1 つを送信するように設定します。このテストは、管理アクセスポイントが通常送信するビーコンのベンダフィールドをチェックします。ベンダフィールドが存在しない場合、アクセスポイントはにせのアクセスポイントとして確認されます。
AP without an SSID	SSID はビーコンフレームのオプションフィールドです。検出を回避するために、ハッカーは管理されたネットワークの SSID をアクセスポイントに設定するかもしれませんが、ビーコンフレームの SSID 伝送を無効にします。アクセスポイントは、まだクライアントがハッカーのアクセスポイントに接続するようにだましている管理SSIDに対してプローブ要求を送信するクライアントにプローブ応答を送信します。 このテストでは、SSID フィールドのないビーコンを送信するアクセスポイントを検出して、フラグを付けます。プロファイル内の無線インタフェースのどれかが「SSID」を送信しないように設定されていると、このテストは自動的に無効になります。これは、実際にはセキュリティを提供しないで、本テストを無効にするため推奨されません。
Fake managed AP on an invalid channel	管理されたアクセスポイントの 1 つの送信元 MAC アドレスからビーコンを送信する不正なアクセスポイントを検出しますが、アクセスポイントが動作していると思われるチャンネルとは違うチャンネルで検出されます。
Managed SSID detected with incorrect security	RF スキャン中に、アクセスポイントは、他のアクセスポイントから受信したビーコンフレームを検証して、検出されたアクセスポイントがオープン中のネットワーク、WEP、または WPA を通知しているかどうか判断します。 RF スキャンで報告された SSID が、管理されたネットワークの 1 つであり、セキュリティ設定が検出されたセキュリティと一致していないと、本テストは、アクセスポイントが Rogue（不正）であるとマークします。

項目	説明
Invalid SSID from a managed AP	「Enabled」を選択すると、既知の管理アクセスポイントが予期しない SSID を送信しているかどうかをチェックします。RF スキャンで報告された SSID は、管理アクセスポイントに割り当てられたプロファイルが使用するすべて SSID 設定のリストと比較されます。検出された SSID が設定済みのどの SSID にも一致しないと、アクセスポイントは Rogue（不正）であるとマークします。
AP is operating on an illegal channel	「Enabled」を選択すると、ハッカーまたは無線システムが設定される国では合法でないチャンネルで動作する不正に設定されたデバイスを検出します。 **注意** 無線システムでこの脅威を検出するためには、無線ネットワークは Sentry モードで動作する 1 個以上の周波数帯域を持つ必要があります。
Standalone AP with unexpected configuration	アクセスポイントが既知のスタンドアロンアクセスポイントとして分類される場合、スイッチは、アクセスポイントが予期された設定パラメータを使用して動作しているかどうかチェックします。ローカルまたは RADIUS Valid AP データベースにスタンドアロンアクセスポイントのために予期されるパラメータを設定します。
Unexpected WDS device detected on network	アクセスポイントが、「Managed AP」または「Unknown AP」として分類され、WDS（Wireless Distribution System）トラフィックがアクセスポイントに検出される場合、アクセスポイントは「Rogue」（不正）と見なされます。 WDS モードで明らかに動作を許可されているスタンドアロンのアクセスポイントだけが、このテストにより Rogue（不正）として報告されません。
Unmanaged AP detected on wired network	アクセスポイントが有線ネットワークに検出されるかどうかチェックします。アクセスポイントのステータスが「Unknown」であれば、テストはこれを「Rogue」（不正）に変更します。アクセスポイントが有線ネットワークに検出されるかどうかを示すフラグは、RF スキャンレポートの一部として報告されます。アクセスポイントが管理されていて、ネットワークに検出されると、スイッチは、単にこの事実を報告して、アクセスポイントのステータスを「Rogue」（不正）に変更しません。 無線システムでこの脅威を検出するためには、無線ネットワークは Sentry モードで動作する 1 個以上の周波数帯域を持つ必要があります。
Rogue Detected Trap Interval (seconds)	不正なアクセスポイントが RF スキャンデータベースに存在していると管理者に通知する SNMP トラップの伝送間隔（秒）を指定します。0 を設定すると機能は無効になります。
Wired Network Detection Interval (seconds)	新しい有線ネットワーク検出サイクルを開始するまで、アクセスポイントが待機する時間（秒）を指定します。0 を設定すると機能は無効になります。
AP De-Authentication Attack	アクセスポイント認証解除攻撃を「Enabled」（有効）または「Disabled」（無効）にします。 無線スイッチは、認証解除メッセージを不正なアクセスポイントに送信することで、不正なアクセスポイントを防御します。無線システムが本機能を動作するためには、認証解除攻撃機能をグローバルに有効にする必要があります。攻撃機能を有効にするまで認知されないアクセスポイントは「Rogue」として分類されないことにご注意ください。本機能は初期値では「Disable」（無効）になっています。

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

Client Configuration タブ（WIDS クライアントの設定）

Administration > Advanced Configuration > WIDS Security > Client Configuration タブの順にメニューをクリックし、以下の画面を表示します。

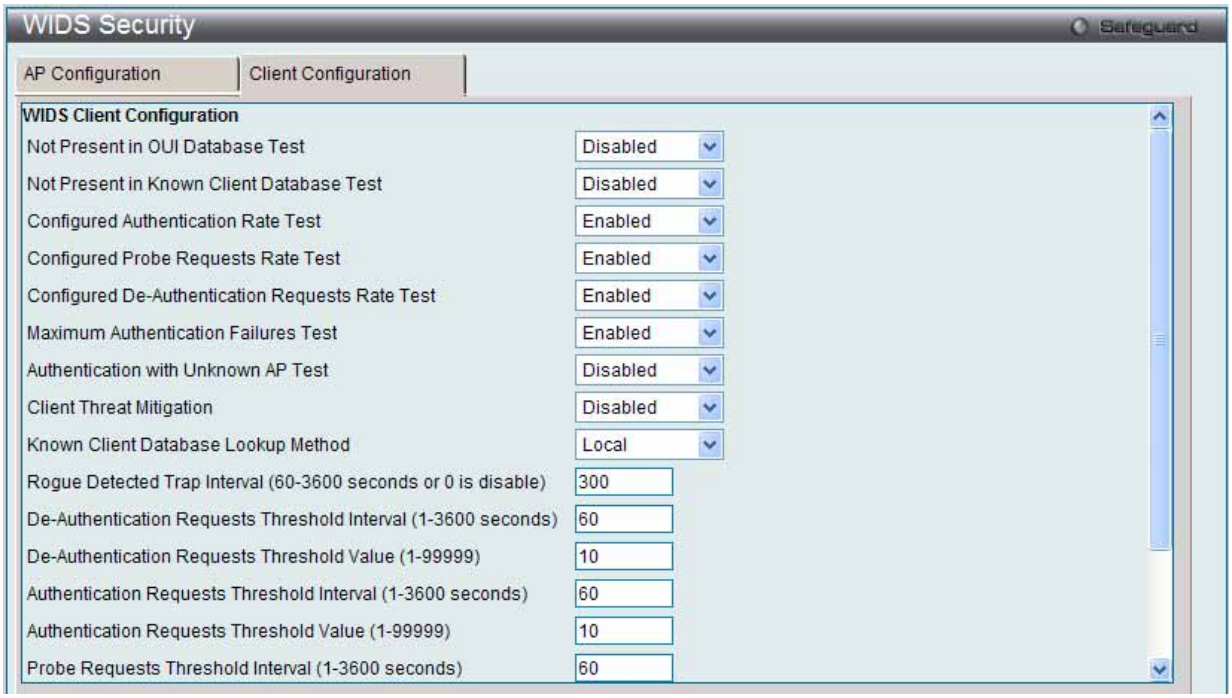


図 8.3-37　WIDS Security > Client Configuration 画面

3. 以下の項目を使用して設定および参照します。

項目	説明
Not Present in OUI Database Test	「Enabled」を選択すると、OUI DB Test にクライアントが存在するかどうかチェックします。
Not Present in Known Client Database Test	「Enabled」を選択すると、MAC アドレスによって特定されるクライアントが、Known Client データベースに表示され、Authentication Action の Grant、または、ホワイトリストの Global Action のいずれかを通じてアクセスポイントへのアクセスを許可されるかどうかをチェックします。 クライアントが Known Client データベースにあり、Deny の機能を持つ場合、または、動作が Global Action であり、またはそれがブラックリストにグローバルに設定される場合、クライアントはこのテストに失敗します。
Configured Authentication Rate Test	「Enabled」を選択すると、クライアントが 802.11 の認証要求の送信のために設定レートを超えているかどうかチェックします。
Configured Probe Requests Rate Test	「Enabled」を選択すると、クライアントがプローブ要求の送信のために設定レートを超えているかどうかチェックします。
Configured De-Authentication Requests Rate Test	「Enabled」を選択すると、クライアントが認証解除要求の送信のために設定レートを超えているかどうかチェックします。
Maximum Authentication Failures Test	「Enabled」を選択すると、クライアントがプローブ要求の送信のために設定レートを超えているかどうかチェックします。
Authentication with Unknown AP Test	「Enabled」を選択すると、Known Client データベースのクライアントが Unknown（未知）のアクセスポイントで認証されるかどうかをチェックします。
Client Threat Mitigation	• Enable - Known Clients データベースにあるが、未知のアクセスポイントに接続していないクライアントに認証解除メッセージを送信します。Unknown AP テストを使用する認証を、緩和が行われるために有効にする必要があります。 • Disable - Known Clients データベース内のクライアントは、Unknown（未知）のアクセスポイントで認証されたまま残ります。
Known Client Database Lookup Method	スイッチがネットワークにクライアントを検出する場合、それは Known Client データベースの検索を実行します。スイッチがこれらの検索にローカルまたは RADIUS データベースを使用するべきかどうか指定します。
Rogue Detected Trap Interval (seconds)	不正なアクセスポイントが RF スキャンデータベースに存在していると管理者に通知する SNMP トラップの伝送間隔（秒）を指定します。0 を入力すると機能は無効になります。
De-Authentication Requests Threshold Interval (seconds)	無線クライアントが送信した認証解除メッセージをカウントするのにアクセスポイントが使う時間（秒）を指定します。
De-Authentication Requests Threshold Value	しきい値を入力します。しきい値内で、スイッチが指定メッセージよりも多く受信すると、テストを始動します。
Authentication Requests Threshold Interval (seconds)	無線クライアントが送信した認証メッセージをカウントするのにアクセスポイントが使う時間（秒）を指定します。

項目	説明
Authentication Requests Threshold Value	しきい値を入力します。しきい値内で、スイッチが指定メッセージよりも多く受信すると、テストを始動します。
Probe Requests Threshold Interval (seconds)	無線クライアントが送信したプローブメッセージをカウントするのにアクセスポイントが使う時間（秒）を指定します。
Probe Requests Threshold Value	イベントが脅威として報告される前に無線クライアントがしきい値の間に送信を許可されるプローブ要求数を指定します。
Authentication Failure Threshold Value	イベントが脅威として報告される前に無線クライアントがしきい値の間に許可される 802.1X 認証エラー数を指定します。

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

Clients（クライアント）

Known Clients（既知のクライアント）

現在 Known Client データベースにある無線クライアントを表示します。

1. **Administration > Advanced Configuration > Client > Known Client** の順にメニューをクリックし、以下の画面を表示します。

図 8.3-38　Known Clients 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
MAC Address	クライアントの MAC アドレスを表示します。
Name	「Known Client」データベースに追加される場合にクライアントに設定された記述名を表示します。
Authentication Action	MAC 認証がネットワークで有効な場合、無線クライアントで行われるアクションを表示します。

エントリの削除

特定の MAC アドレスをチェック後、「Delete」ボタンをクリックしてエントリを削除します。
「Delete All」ボタンをクリックして、リストからすべてのエントリを削除します。

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

エントリの追加

1. 「Add」ボタンまたは「MAC Address」ハイパーリンクをクリックすると、以下の画面が表示されます。

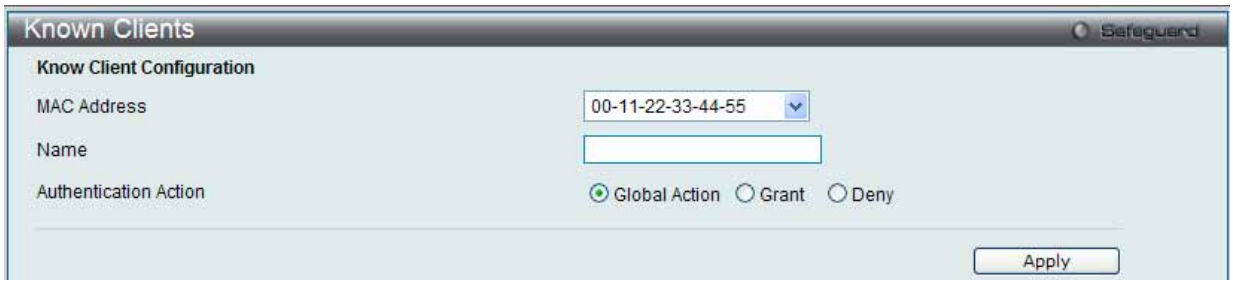


図 8.3-39　Known Clients - Add 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
MAC Address	プルダウンメニューを使用して、クライアントの MAC アドレスを選択します。
Name	クライアントの記述名を入力します。
Authentication Action	MAC 認証がネットワークで有効な場合、無線クライアントに行うアクションを指定します。 • Grant - 指定した MAC アドレスを持つクライアントにネットワークへのアクセスを許可します。 • Deny - 指定した MAC アドレスを持つクライアントにネットワークへのアクセスを禁止します。 • Global Action - **Advanced Configuration > Global** の「Advanced Global Configuration」画面で設定されたグローバルなホワイトリストまたはブラックリストを使用して、クライアントの処理方法を決定します。

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。

Switch Provisioning（スイッチのプロビジョニング）

スイッチのプロビジョニングを設定します。

Switch Certificate Request タブ

1. **Administration > Advanced Configuration > Switch Provisioning > Switch Certificate Request** タブの順にメニューをクリックし、以下の画面を表示します。

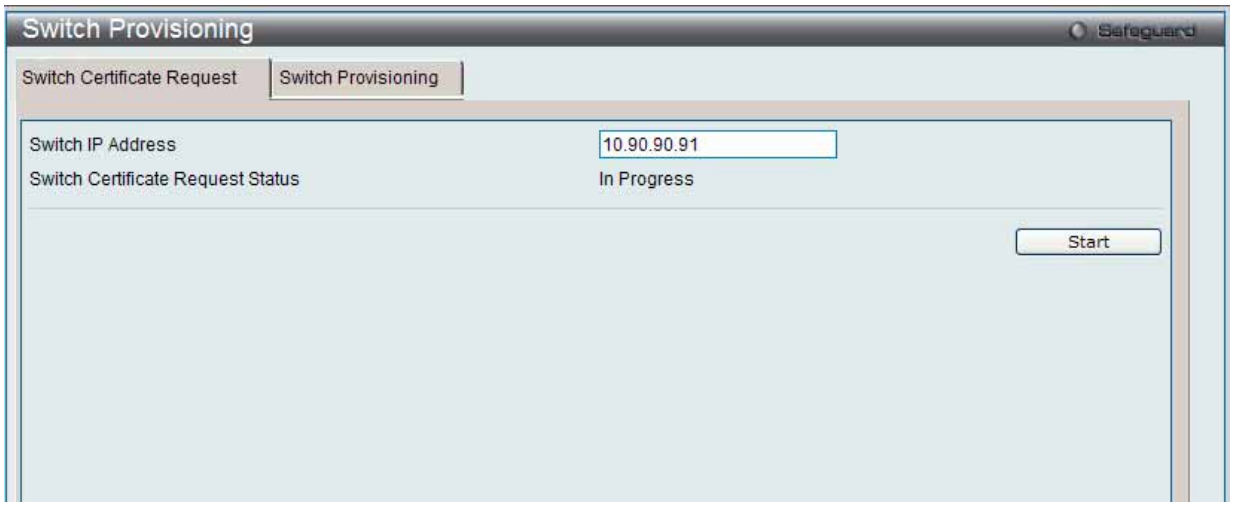


図 8.3-40　Switch Certificate Request 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Switch IP Address	ピアスイッチの IP アドレスを入力します。

「Start」ボタンをクリックして、スイッチの証明書要求を実行します。

Switch Provisioning タブ

1. **Administration** > **Advanced Configuration** > **Switch Provisioning** > **Switch Provisioning** タブの順にメニューをクリックし、以下の画面を表示します。

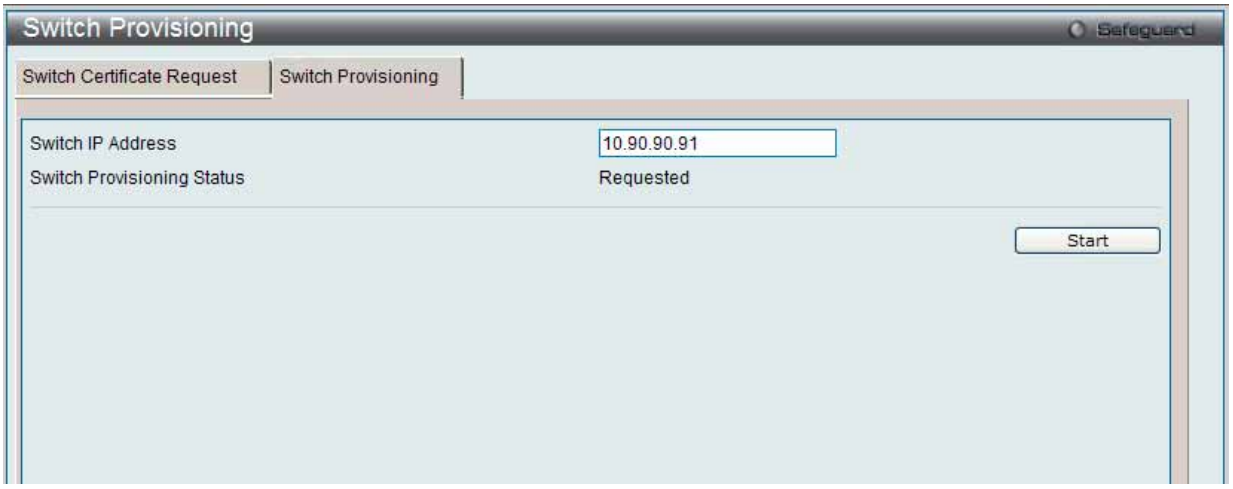


図 8.3-41　Switch Provisioning 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Switch IP Address	ピアスイッチの IP アドレスを入力します。

「Start」ボタンをクリックして、スイッチのプロビジョニングを実行します。

8.4 QoS（QoS 機能の設定）

本セクションでは、QoS に関する概要を提供し、「Quality of Service」メニューで可能な QoS 機能について記述しています。本セクションでは以下のサブセクションを含んでいます。

設定項目	説明	参照ページ
Access Control Lists（アクセスコントロールリスト）	トラフィックを定義済みのホップ単位の動作に基づいてストリームに分類して、特定の QoS 処理を行います。次のメニューがあります。 IP Access Control Lists（IP アクセスコントロールリスト）、IPv6 Access Control Lists（IPv6 アクセスコントロールリスト）、MAC Access Control Lists（MAC アクセスコントロールリスト）	498
Differentiated Services（クラス別サービス）	CoS 設定を行います。次のメニューがあります。 Diffserv Configuration（Diffserv 設定）、Class Configuration（クラス設定）、Policy Configuration（ポリシー設定）、Policy Class Definition（ポリシークラス定義）	511

Access Control Lists（アクセスコントロールリスト）

IP Access Control Lists（IP アクセスコントロールリスト）

ネットワーク管理者は、IP アクセスコントロールリスト (ACL) により無線ネットワークに分類のアクションとルールを定義することができます。

QoS > Access Control Lists > IP Access Control 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。

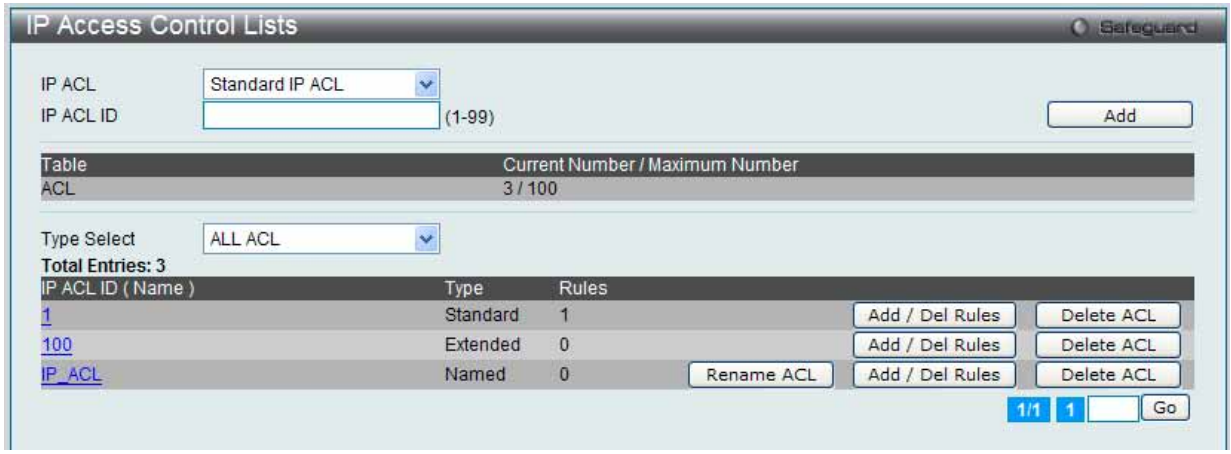


図 8.4-1 IP Access Control Lists 画面

1. 以下の項目を使用して設定および参照します。

項目	説明
IP ACL	プルダウンメニューを使用して、IP ACL タイプを選択します。 • Standard IP ACL - 送信元 IP アドレスからのトラフィックを許可または拒否します。 • Extended IP ACL - 指定した送信元 IP アドレスからの送信先 IP アドレスからへのレイヤ 3 またはレイヤ 4 のトラフィックタイプを許可または拒否します。この ACL タイプは、標準の IP ACL より、詳細で高いフィルタリング性能を提供します。 • Named IP ACL - 番号より名称で指定される Extended IP ACL を作成することができます。これらの ACL は、サポートする照合の基準およびアクションについて Extended IP ACL と同じ性能を持っています。
IP ACL ID/Name	IP ACL の ID または名前を入力します。
Type Select	プルダウンメニューを使用して、IP ACL タイプを選択し、テーブル下に表示される情報を参照します。

「Add」ボタンをクリックして、入力した情報に基づいて新しいエントリを追加します。
「Rename ACL」ボタンをクリックして、指定した ACL 名を変更します。

エントリの削除

「Add / Delete Rules」をクリックして、ACL ルールを設定します。
「Delete ACL」ボタンをクリックして、リストからエントリを削除します。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

ACL 名の変更

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

図 8.4-2　IP Access Control Lists - Rename 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
New IP ACL Name	新しい IP ACL 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。
「Cancel」ボタンをクリックすると設定は破棄されます。

ACL ルールの設定

「Add / Delete Rules」または特定の IP ACL ID (Name) ハイパーリンクをクリックして、以下の画面を表示します。

図 8.4-3　IP Access Control Lists - Add / Delete Rules 画面

「Add Rule」ボタンをクリックし、新しいルールを作成します。
「<<Back」をボタンをクリックして前のページに戻ります。
対応するボックスをチェック後、「Delete」ボタンをクリックして指定ルールを削除します。
「Refresh」ボタンをクリックして、リストを更新します。
「Rule ID」ハイパーリンクまたは「Edit」ボタンをクリックして、指定ルールを編集します。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

IP ACL のタイプの違いにより、ルール設定は異なります。

Standard IP ACL にルールを追加する

1. 「IP ACL」で「Standard IP ACL」を選択し、「Add Rule」ボタンをクリックして、以下の画面を表示します。

図 8.4-4　IP Access Control Lists - Add Rule (Standard IP ACL) 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Rule ID	ルール ID を入力します。
Action	プルダウンメニューを使用して、パケットがルールの基準に一致する際にアクションを進める ACL を選択します。
Match Every	プルダウンメニューを使用して、「True」または「False」を選択します。 • True - すべてのパケットが選択した IP ACL およびルールに一致し、許可または拒否されること意味します。「True」を選択すると、すべてのパケットをルールに照合するため、他の照合基準を設定するオプションは提供されません。 • False - ルールに特定の照合基準を設定して、他の照合基準を設定します。
Source IP Address	IP アドレスを入力します。パケットの送信元 IP アドレスは入力したアドレスと一致する必要があります。
Source IP Mask	送信元 IP マスクを指定します。

「Create」ルールボタンをクリックして、新しいルールを追加します。
「Cancel」ボタンをクリックすると設定は破棄されます。

Extended IP ACL にルールを追加する

1. 「IP ACL」で「Extended IP ACL」を選択し、「Add Rule」ボタンをクリックして、以下の画面を表示します。

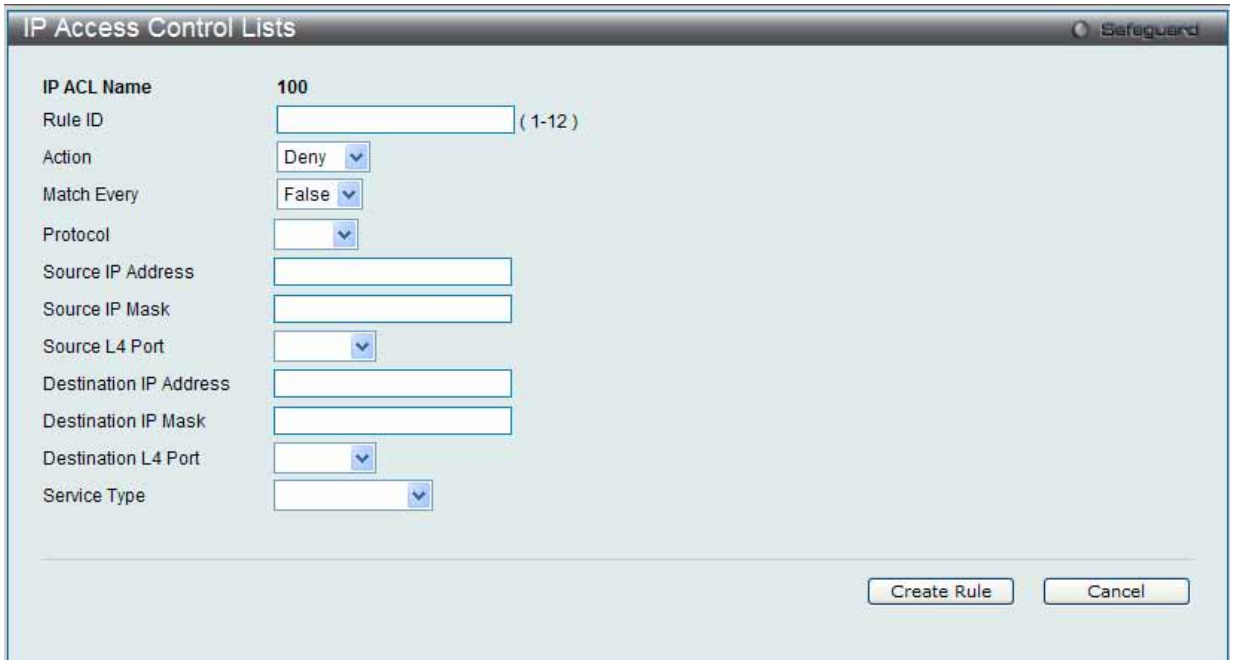


図 8.4-5　IP Access Control Lists - Add Rule (Extended IP ACL) 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Rule ID	ルール ID を入力します。
Action	プルダウンメニューを使用して、パケットがルールの基準に一致する際にアクションを進める ACL を選択します。
Match Every	プルダウンメニューを使用して、「True」または「False」を選択します。 • True - すべてのパケットが選択した IP ACL およびルールに一致し、許可または拒否されること意味します。「True」を選択すると、すべてのパケットをルールに照合するため、他の照合基準を設定するオプションは提供されません。 • False - ルールに特定の照合基準を設定して、他の照合基準を設定します。
Protocol	プルダウンメニューを使用して、選択した IP ACL ルールの条件に照合するパケットの IP プロトコルを選択します。「Other」を選択すると、「Protocol Value」欄が表示されますので、ここに値を入力します。
Source IP Address	IP アドレスを入力します。パケットの送信元 IP アドレスは入力したアドレスと一致する必要があります。
Source IP Mask	送信元 IP マスクを指定します。
Source L4 Port	プルダウンメニューを使用して、パケットの TCP/UDP 送信元ポートを照合する送信元ポートの L4 キーワードを選択します。「Other」を選択すると、「Source Port Value」欄が表示されますので、ここに値を入力します。
Destination IP Address	IP アドレスを入力します。パケットの送信先 IP アドレスは入力したアドレスと一致する必要があります。
Destination IP Mask	送信先 IP マスクを入力します。
Destination L4 Port	プルダウンメニューを使用して、パケットの TCP/UDP 送信先ポートを照合する送信先ポートの L4 キーワードを選択します。「Other」を選択すると、「Destination Port Value」欄が表示されますので、ここに値を入力します。
Service Type	extended IP ACL ルールに対する以下の 3 つの「Match」条件から 1 つを選択します。 • IP DSCP - IP DSCP プルダウンメニューから DSCP キーワードの 1 つを選択します。「Other」を選択すると、「IP DSCP Value」欄が表示されますので、ここに値を入力します。 • IP Precedence -「IP Precedence」欄に 0-7 の値を入力します。 • IP ToS -「IP ToS Bits」および「IP ToS Mask」欄に 00-FF の 16 進数を入力します。

「Create」ルールボタンをクリックして、新しいルールを追加します。
「Cancel」ボタンをクリックすると設定は破棄されます。

Named IP ACL にルールを追加する

1. 「IP ACL」で「Named IP ACL」を選択し、「Add Rule」ボタンをクリックして、以下の画面を表示します。

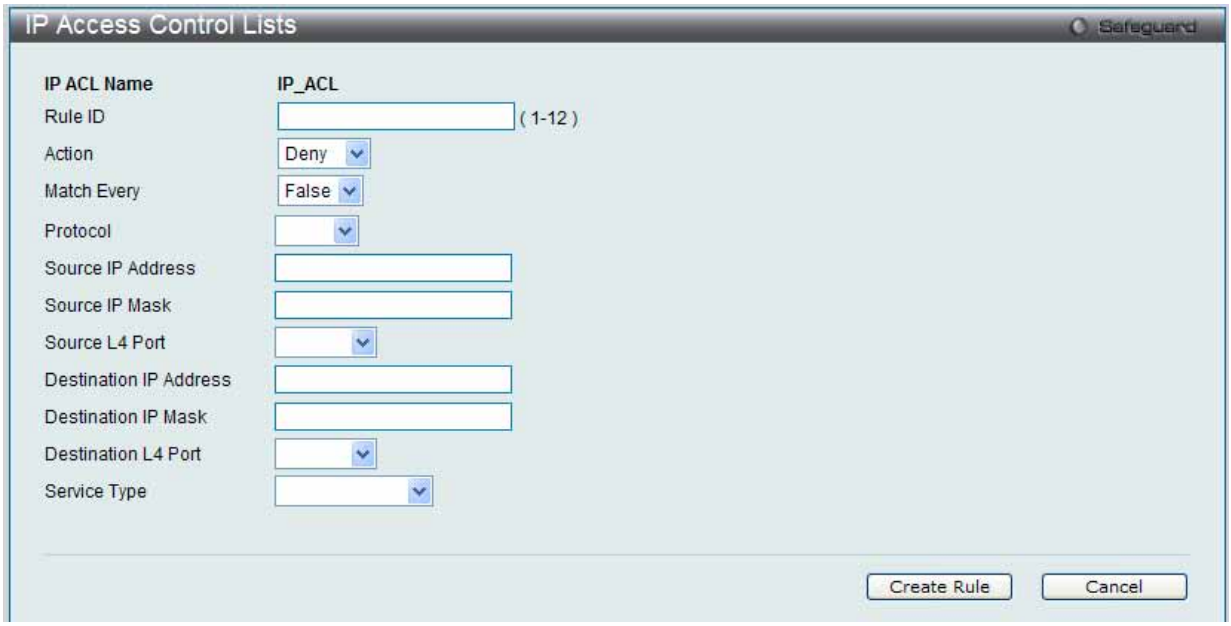


図 8.4-6　IP Access Control Lists - Add Rule (Named IP ACL) 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Rule ID	ルール ID を入力します。
Action	プルダウンメニューを使用して、パケットがルールの基準に一致する際にアクションを進める ACL を選択します。
Match Every	プルダウンメニューを使用して、「True」または「False」を選択します。 • True - すべてのパケットが選択した IP ACL およびルールに一致し、許可または拒否されること意味します。「True」を選択すると、すべてのパケットをルールに照合するため、他の照合基準を設定するオプションは提供されません。 • False - ルールに特定の照合基準を設定して、他の照合基準を設定します。
Protocol	プルダウンメニューを使用して、選択した IP ACL ルールの条件に照合するパケットの IP プロトコルを選択します。「Other」を選択すると、「Protocol Value」欄が表示されますので、ここに値を入力します。
Source IP Address	IP アドレスを入力します。パケットの送信元 IP アドレスは入力したアドレスと一致する必要があります。
Source IP Mask	送信元 IP マスクを指定します。
Source L4 Port	プルダウンメニューを使用して、パケットの TCP/UDP 送信元ポートを照合する送信元ポートの L4 キーワードを選択します。「Other」を選択すると、「Source Port Value」欄が表示されますので、ここに値を入力します。
Destination IP Address	IP アドレスを入力します。パケットの送信先 IP アドレスは入力したアドレスと一致する必要があります。
Destination IP Mask	送信先 IP マスクを入力します。
Destination L4 Port	プルダウンメニューを使用して、パケットの TCP/UDP 送信先ポートを照合する送信先ポートの L4 キーワードを選択します。「Other」を選択すると、「Destination Port Value」欄が表示されますので、ここに値を入力します。
Service Type	extended IP ACL ルールに対する以下の 3 つの「Match」条件から 1 つを選択します。 • IP DSCP - IP DSCP プルダウンメニューから DSCP キーワードの 1 つを選択します。「Other」を選択すると、「IP DSCP Value」欄が表示されますので、ここに値を入力します。 • IP Precedence -「IP Precedence」欄に 0-7 の値を入力します。 • IP ToS -「IP ToS Bits」および「IP ToS Mask」欄に 00-FF の 16 進数を入力します。

「Create」ルールボタンをクリックして、新しいルールを追加します。
「Cancel」ボタンをクリックすると設定は破棄されます。

ACL のルール編集

Standard IP ACL のルール編集

1. 「Standard IP ACL」のルールを編集するためには「Rule ID」ハイパーリンクまたは「Edit」ボタンをクリックして、以下の画面を表示します。

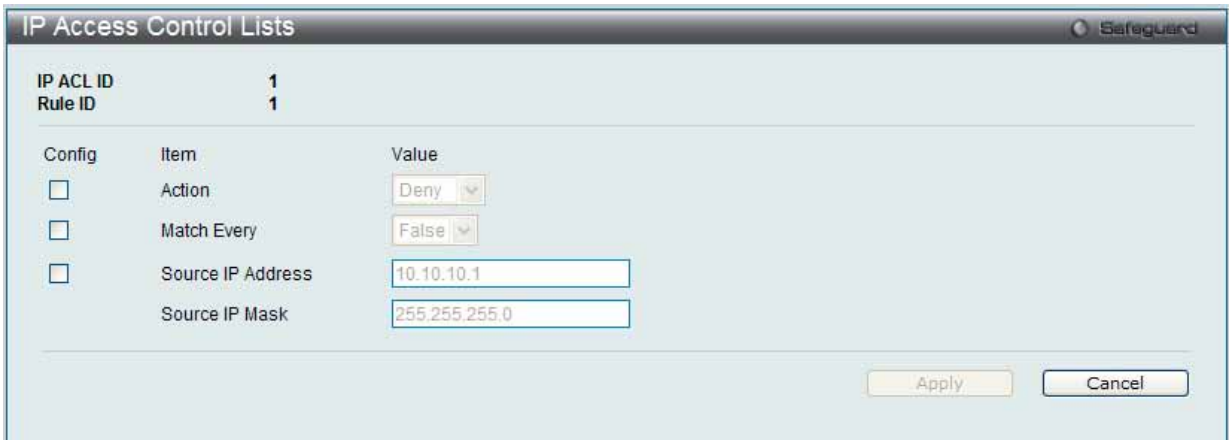


図 8.4-7 IP Access Control Lists - Edit Rule (Standard IP ACL) 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Action	ボックスをチェックし、プルダウンメニューを使用して、ACL 送信アクションを選択します。
Match Every	プルダウンメニューを使用して、「True」または「False」を選択します。 • True - すべてのパケットが選択した IP ACL およびルールに一致し、許可または拒否されること意味します。「True」を選択すると、すべてのパケットをルールに照合するため、他の照合基準を設定するオプションは提供されません。 • False - ルールに特定の照合基準を設定して、他の照合基準を設定します。
Source IP Address	ボックスをチェックして、IP アドレスを入力します。パケットの送信元 IP アドレスは入力したアドレスと一致する必要があります。
Source IP Mask	「Source IP Address」ボックスをチェックした場合に、送信元 IP マスクを入力します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Cancel」ボタンをクリックすると設定は破棄されます。

Extended IP ACL のルール編集

1. 「Extended IP ACL」のルールを編集するためには「Rule ID」ハイパーリンクまたは「Edit」ボタンをクリックして、以下の画面を表示します。

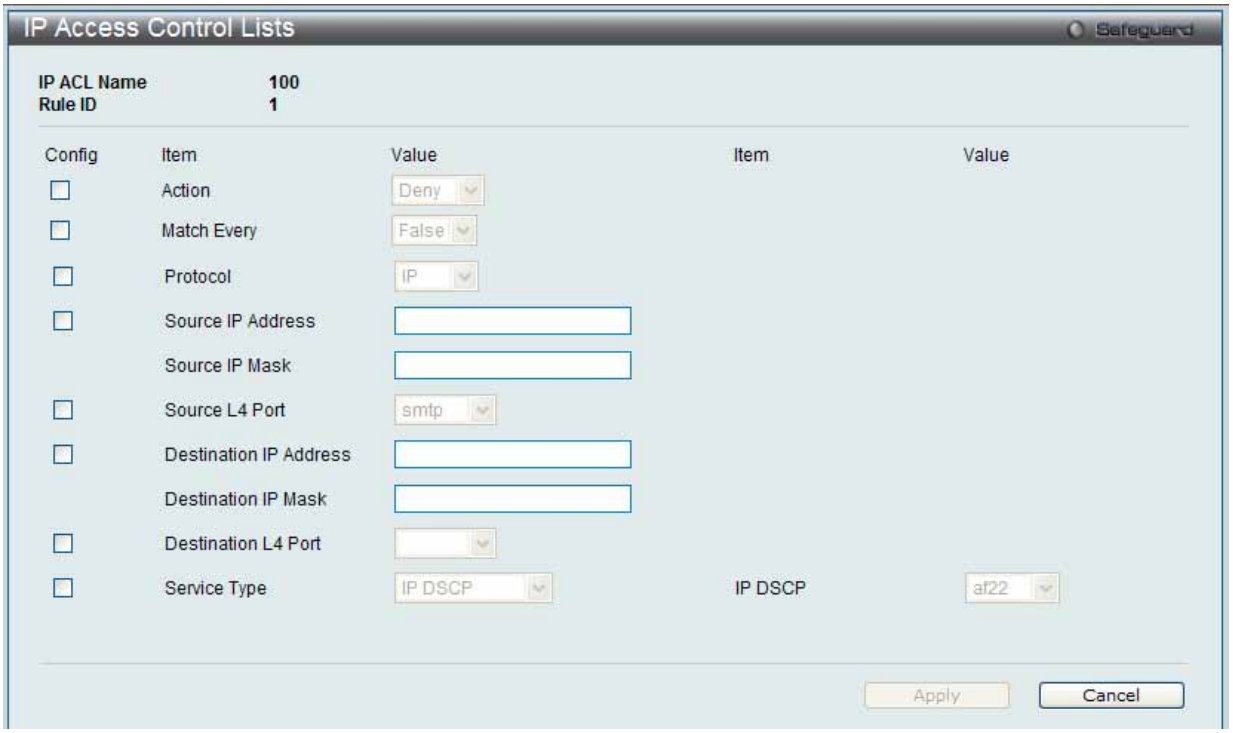


図 8.4-8　IP Access Control Lists - Edit Rule (Extended IP ACL) 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Action	ボックスをチェックし、プルダウンメニューを使用して、ACL 送信アクションを選択します。
Match Every	プルダウンメニューを使用して、「True」または「False」を選択します。 • True - すべてのパケットが選択した IP ACL およびルールに一致し、許可または拒否されること意味します。「True」を選択すると、すべてのパケットをルールに照合するため、他の照合基準を設定するオプションは提供されません。 • False - ルールに特定の照合基準を設定して、他の照合基準を設定します。
Protocol	ボックスをチェックし、プルダウンメニューを使用して、選択した IP ACL ルールの条件に照合するパケットの IP プロトコルを選択します。「Other」を選択すると、「Protocol Value」欄が表示されますので、ここに値を入力します。
Source IP Address	ボックスをチェックして、IP アドレスを入力します。パケットの送信元 IP アドレスは入力したアドレスと一致する必要があります。
Source IP Mask	「Source IP Address」ボックスをチェックした場合に、送信元 IP マスクを入力します。
Source L4 Port	ボックスをチェックし、プルダウンメニューを使用して、パケットの TCP/UDP 送信元ポートを照合する送信元ポートの L4 キーワードを選択します。「Other」を選択すると、「Source Port Value」欄が表示されますので、ここに値を入力します。
Destination IP Address	ボックスをチェックして、IP アドレスを入力します。パケットの送信先 IP アドレスは入力したアドレスと一致する必要があります。
Destination IP Mask	「Destination IP Address」ボックスをチェックした場合に、送信先 IP マスクを入力します。
Destination L4 Port	ボックスをチェックし、プルダウンメニューを使用して、パケットの TCP/UDP 送信先ポートを照合する送信先ポートの L4 キーワードを選択します。「Other」を選択すると、「Destination Port Value」欄が表示されますので、ここに値を入力します。
Service Type	ボックスをチェックし、extended IP ACL ルールに対する以下の 3 つの「Match」条件から 1 つを選択します。 • IP DSCP - IP DSCP プルダウンメニューから DSCP キーワードの 1 つを選択します。「Other」を選択すると、「IP DSCP Value」欄が表示されますので、ここに値を入力します。 • IP Precedence -「IP Precedence」欄に 0-7 の値を入力します。 • IP ToS -「IP ToS Bits」および「IP ToS Mask」欄に 00-FF の 16 進数を入力します。

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。
「Cancel」ボタンをクリックすると設定は破棄されます。

Named IP ACL のルール編集

1. 「Named IP ACL」のルールを編集するためには「Rule ID」ハイパーリンクまたは「Edit」ボタンをクリックして、以下の画面を表示します。

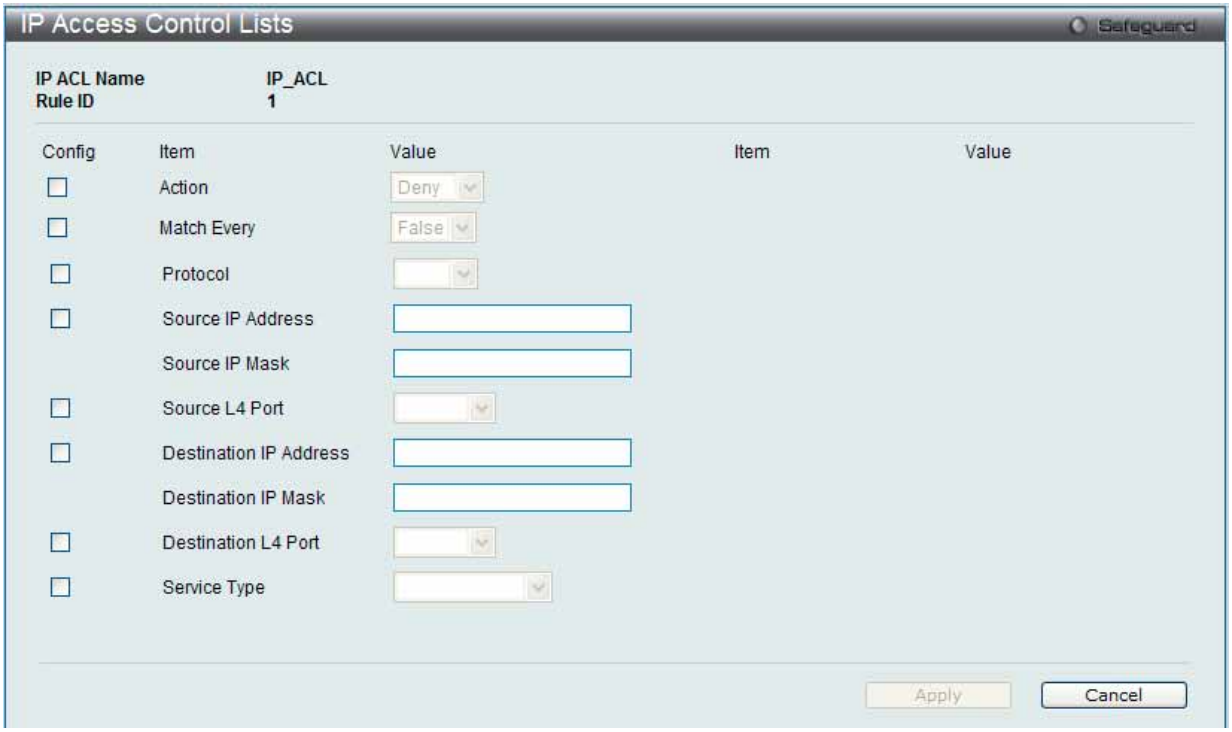


図 8.4-9　IP Access Control Lists - Edit Rule (Named IP ACL) 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Action	ボックスをチェックし、プルダウンメニューを使用して、ACL 送信アクションを選択します。
Match Every	プルダウンメニューを使用して、「True」または「False」を選択します。 • True - すべてのパケットが選択した IP ACL およびルールに一致し、許可または拒否されること意味します。「True」を選択すると、すべてのパケットをルールに照合するため、他の照合基準を設定するオプションは提供されません。 • False - ルールに特定の照合基準を設定して、他の照合基準を設定します。
Protocol	ボックスをチェックし、プルダウンメニューを使用して、選択した IP ACL ルールの条件に照合するパケットの IP プロトコルを選択します。「Other」を選択すると、「Protocol Value」欄が表示されますので、ここに値を入力します。
Source IP Address	ボックスをチェックして、IP アドレスを入力します。パケットの送信元 IP アドレスは入力したアドレスと一致する必要があります。
Source IP Mask	「Source IP Address」ボックスをチェックした場合に、送信元 IP マスクを入力します。
Source L4 Port	ボックスをチェックし、プルダウンメニューを使用して、パケットの TCP/UDP 送信元ポートを照合する送信元ポートの L4 キーワードを選択します。「Other」を選択すると、「Source Port Value」欄が表示されますので、ここに値を入力します。
Destination IP Address	ボックスをチェックして、IP アドレスを入力します。パケットの送信先 IP アドレスは入力したアドレスと一致する必要があります。
Destination IP Mask	「Destination IP Address」ボックスをチェックした場合に、送信先 IP マスクを入力します。
Destination L4 Port	ボックスをチェックし、プルダウンメニューを使用して、パケットの TCP/UDP 送信先ポートを照合する送信先ポートの L4 キーワードを選択します。「Other」を選択すると、「Destination Port Value」欄が表示されますので、ここに値を入力します。
Service Type	ボックスをチェックし、extended IP ACL ルールに対する以下の 3 つの「Match」条件から 1 つを選択します。 • IP DSCP - IP DSCP プルダウンメニューから DSCP キーワードの 1 つを選択します。「Other」を選択すると、「IP DSCP Value」欄が表示されますので、ここに値を入力します。 • IP Precedence -「IP Precedence」欄に 0-7 の値を入力します。 • IP ToS -「IP ToS Bits」および「IP ToS Mask」欄に 00-FF の 16 進数を入力します。

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。
「Cancel」ボタンをクリックすると設定は破棄されます。

IPv6 Access Control Lists（IPv6 アクセスコントロールリスト）

IPv6 ACL（Access Control Lists）を設定します。

1. **QoS > Access Control Lists > IPv6 Access Control 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。

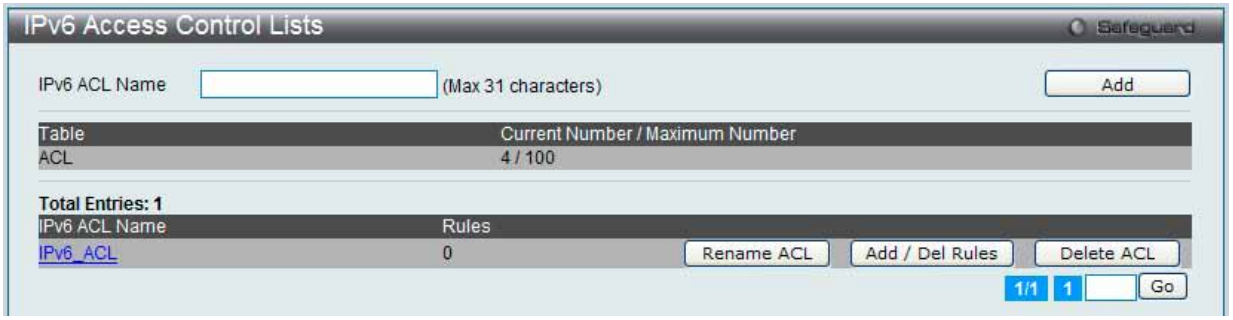


図 8.4-10　IPv6 Access Control Lists 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
IPv6 ACL Name	IPv6 ACL の ID または名前を入力します。

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

「Rename ACL」ボタンをクリックして、指定した ACL 名を変更します。
「Add/Delete Rules」をクリックして、ACL ルールを設定します。
「Delete ACL」ボタンをクリックして、リストからエントリを削除します。

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

ACL 名の変更

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

図 8.4-11　IPv6 Access Control Lists - Rename 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
New IPv6 ACL Name	新しい IPv6 ACL 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。
「Cancel」ボタンをクリックすると設定は破棄されます。

ACL ルールの設定

1. 「Add/Delete Rules」ボタンまたは特定の IPv6 ACL ID (Name) ハイパーリンクをクリックして、以下の画面を表示します。

図 8.4-12　IPv6 Access Control Lists - Add / Delete Rules 画面

2. 「Add Rule」ボタンをクリックし、新しいルールを作成します。

「<<Back」をボタンをクリックして前のページに戻ります。

エントリの削除
対応するボックスをチェック後、「Delete」ボタンをクリックして指定ルールを削除します。

「Refresh」ボタンをクリックして、リストを更新します。
「Rule ID」ハイパーリンクまたは「Edit」ボタンをクリックして、指定ルールを編集します。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

ルールの追加
1. 「Add Rule」ボタンをクリックすると、以下の画面が表示されます。

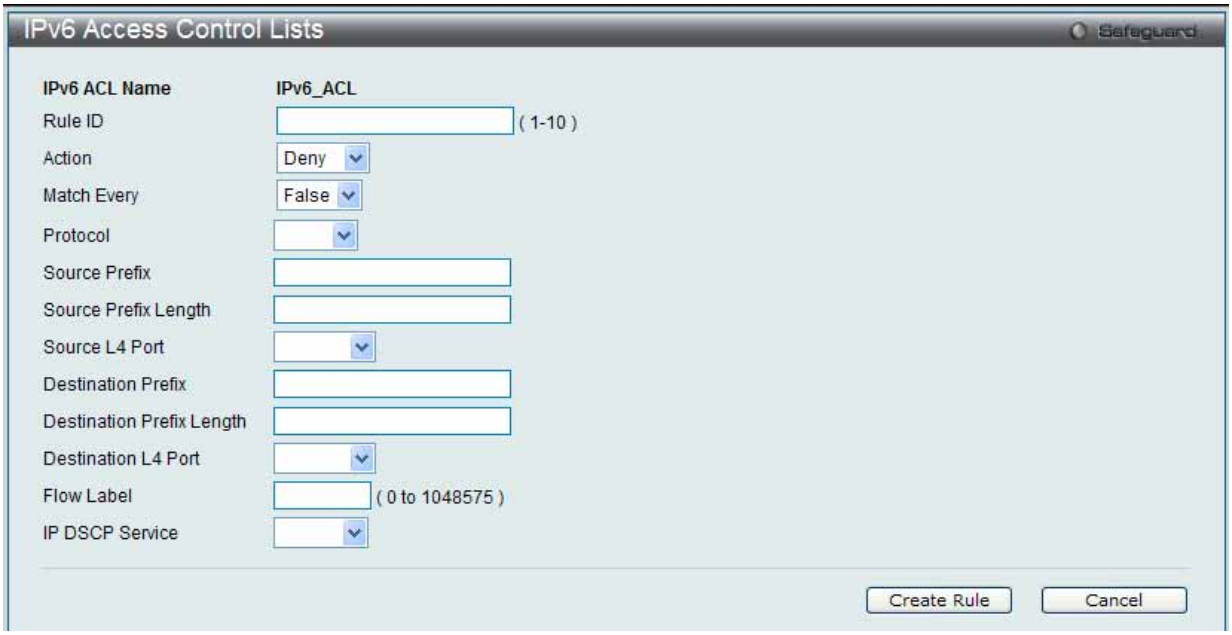


図 8.4-13　IPv6 Access Control Lists - Add Rule 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Rule ID	ルール ID を入力します。
Action	プルダウンメニューを使用して、パケットがルールの基準に一致する際にアクションを進める ACL を選択します。
Match Every	プルダウンメニューを使用して、「True」または「False」を選択します。 • True - すべてのパケットが選択した IP ACL およびルールに一致し、許可または拒否されること意味します。「True」を選択すると、すべてのパケットをルールに照合するため、他の照合基準を設定するオプションは提供されません。 • False - ルールに特定の照合基準を設定して、他の照合基準を設定します。
Protocol	プルダウンメニューを使用して、選択した IP ACL ルールの条件に照合するパケットの IP プロトコルを選択します。「Other」を選択すると、「Protocol Value」欄が表示されますので、ここに値を入力します。
Source Prefix	IPv6 プレフィックスを入力します。パケットの送信元 IPv6 プレフィックスは入力したアドレスと一致する必要があります。
Source Prefix Length	送信元 IPv6 マスクを入力します。

項目	説明
Source L4 Port	プルダウンメニューを使用して、パケットの TCP/UDP 送信元ポートを照合する送信元ポートの L4 キーワードを選択します。「Other」を選択すると、「Source Port Value」欄が表示されますので、ここに値を入力します。
Destination Prefix	IPv6 プレフィックスを入力します。パケットの送信先 IPv6 プレフィックスは入力したアドレスと一致する必要があります。
Destination Prefix Length	送信先 IPv6 マスクを入力します。
Destination L4 Port	プルダウンメニューを使用して、パケットの TCP/UDP 送信先ポートを照合する送信先ポートの L4 キーワードを選択します。「Other」を選択すると、「Destination Port Value」欄が表示されますので、ここに値を入力します。
Flow Label	IPv6 フローラベルの値を入力します。
IP DSCP Service	IP DSCP プルダウンメニューから DSCP キーワードの 1 つを選択します。「Other」を選択すると、「IP DSCP Value」欄が表示されますので、ここに値を入力します。

「Create」ルールボタンをクリックして、新しいルールを追加します。
「Cancel」ボタンをクリックすると設定は破棄されます。

ルールの編集

1. 「Rule ID」ハイパーリンクまたは「Edit」ボタンをクリックして、以下の画面を表示します。

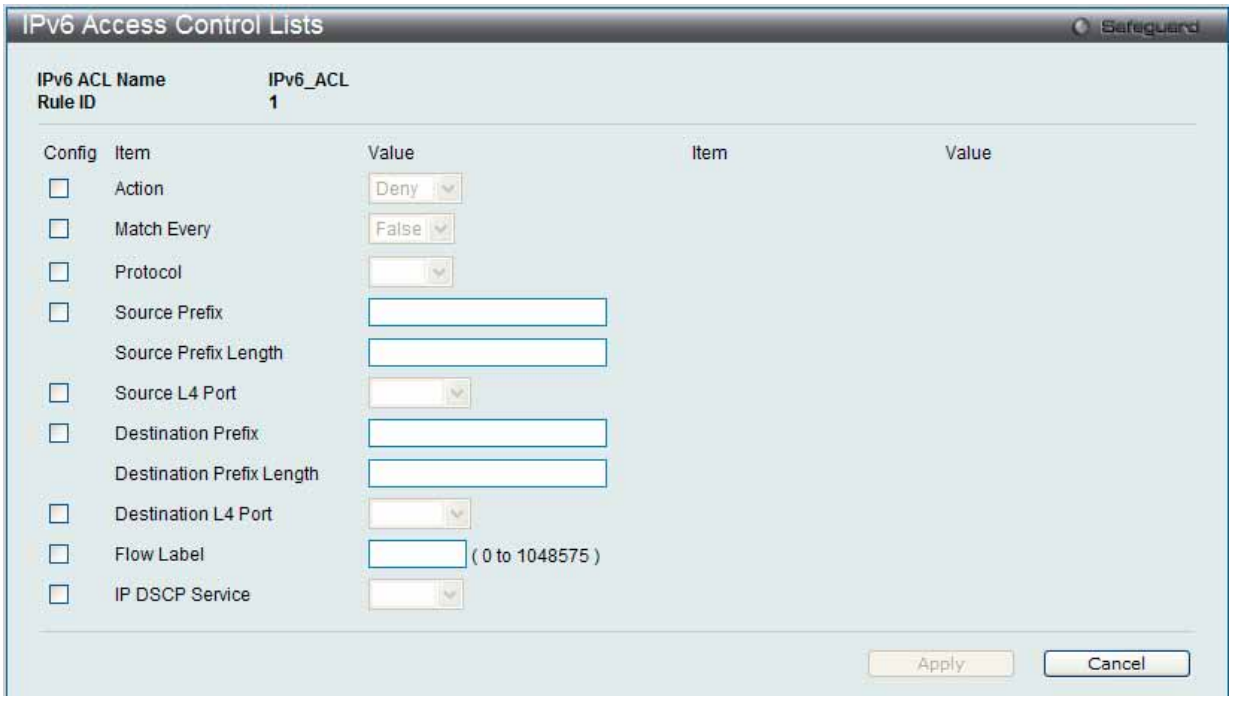


図 8.4-14　IPv6 Access Control Lists - IPv6 Access Control Lists - Edit Rule 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Action	ボックスをチェックし、プルダウンメニューを使用して、ACL 送信アクションを選択します。
Match Every	プルダウンメニューを使用して、「True」または「False」を選択します。 • True - すべてのパケットが選択した IP ACL およびルールに一致し、許可または拒否されること意味します。「True」を選択すると、すべてのパケットをルールに照合するため、他の照合基準を設定するオプションは提供されません。 • False - ルールに特定の照合基準を設定して、他の照合基準を設定します。
Protocol	ボックスをチェックし、プルダウンメニューを使用して、選択した IP ACL ルールの条件に照合するパケットの IP プロトコルを選択します。「Other」を選択すると、「Protocol Value」欄が表示されますので、ここに値を入力します。
Source Prefix	ボックスをチェックし、IPv6 プレフィックスを入力します。パケットの送信元 IPv6 プレフィックスは入力したアドレスと一致する必要があります。
Source Prefix Length	「Source Prefix」ボックスをチェックした場合に、送信元 IPv6 マスクを入力します。
Source L4 Port	ボックスをチェックし、プルダウンメニューを使用して、パケットの TCP/UDP 送信元ポートを照合する送信元ポートの L4 キーワードを選択します。「Other」を選択すると、「Source Port Value」欄が表示されますので、ここに値を入力します。
Destination Prefix	ボックスをチェックし、IPv6 プレフィックスを入力します。パケットの送信先 IPv6 プレフィックスは入力したアドレスと一致する必要があります。
Destination Prefix Length	「Destination Prefix」ボックスを選択した場合に、送信先 IPv6 マスクを入力します。

項目	説明
Destination L4 Port	ボックスをチェックし、プルダウンメニューを使用して、パケットの TCP/UDP 送信先ポートを照合する送信先ポートの L4 キーワードを選択します。「Other」を選択すると、「Destination Port Value」欄が表示されますので、ここに値を入力します。
Flow Label	ボックスをチェックし、IPv6 フローラベルの値を入力します。
IP DSCP Service	ボックスをチェックし、「IP DSCP」プルダウンメニューから DSCP キーワードの 1 つを選択します。「Other」を選択すると、「IP DSCP Value」欄が表示されますので、ここに値を入力します。

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。
「Cancel」ボタンをクリックすると設定は破棄されます。

MAC Access Control Lists（MAC アクセスコントロールリスト）

MAC ACL（Access Control Lists）を設定します。

1. **QoS > Access Control Lists > MAC Access Control 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。

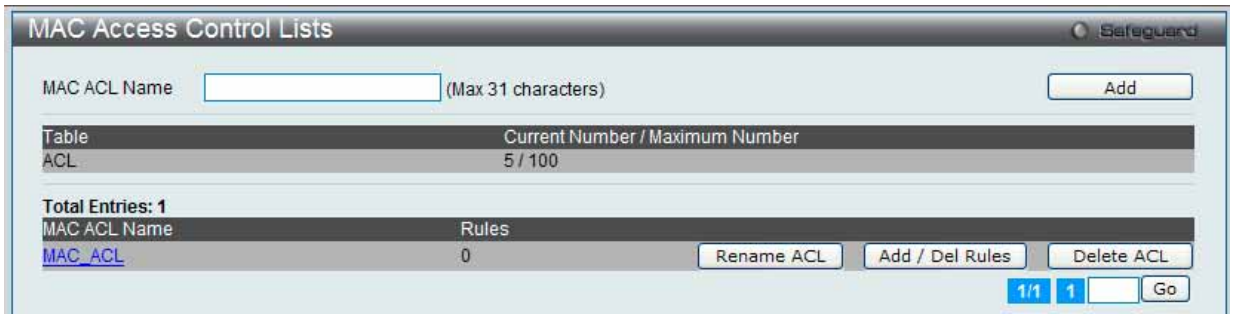


図 8.4-15　MAC Access Control Lists 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
MAC ACL Name	MAC ACL の ID または名前を入力します。

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

「Rename ACL」ボタンをクリックして、指定した ACL 名を変更します。
「Add/Delete Rules」をクリックして、ACL ルールを設定します。

エントリの削除

「Delete ACL」ボタンをクリックして、リストからエントリを削除します。

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

ACL 名の変更

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

図 8.4-16　MAC Access Control Lists - Rename 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
New MAC ACL Name	新しい MAC ACL の名前を入力します。

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。
「Cancel」ボタンをクリックすると設定は破棄されます。

ACL ルールの設定

1. 「Add/Delete Rules」ボタンまたは特定の MAC ACL ID 名のハイパーリンクをクリックして、以下の画面を表示します。

図 8.4-17　MAC Access Control Lists - Add / Delete Rules 画面

2. 「Add Rule」ボタンをクリックし、新しいルールを作成します。

「<<Back」をボタンをクリックして前のページに戻ります。

エントリの削除

対応するボックスをチェック後、「Delete」ボタンをクリックして指定ルールを削除します。

「Refresh」ボタンをクリックして、リストを更新します。
「Rule ID」ハイパーリンクまたは「Edit」ボタンをクリックして、指定ルールを編集します。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

ルールの追加

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

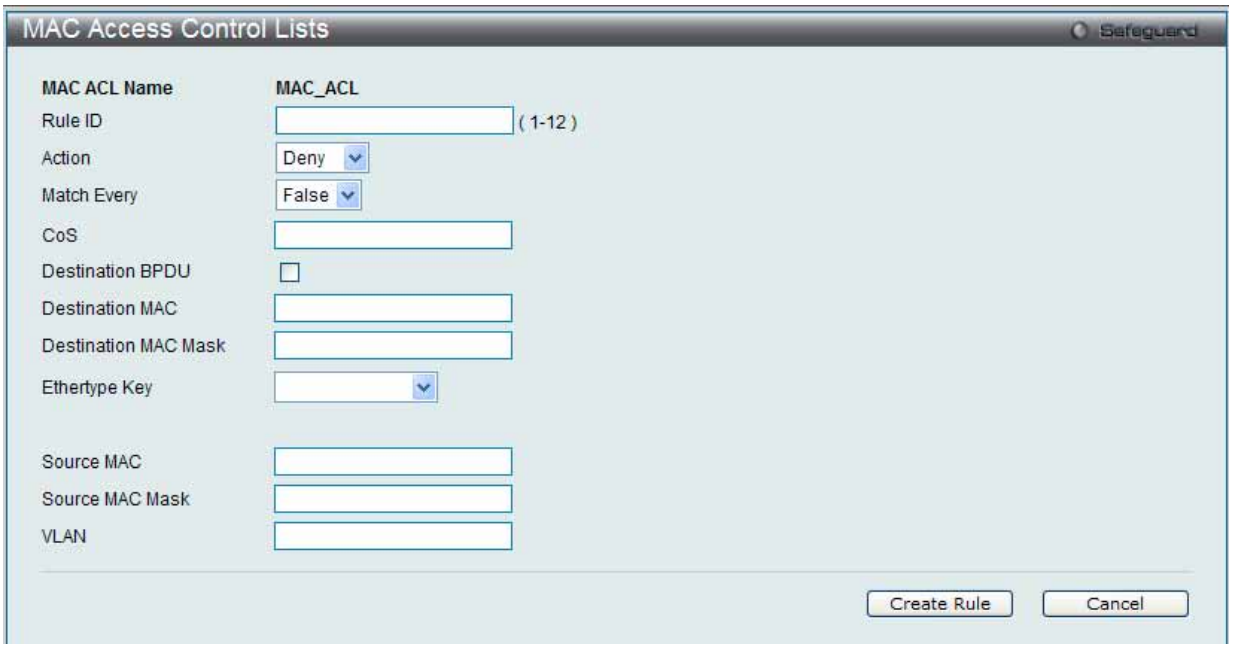


図 8.4-18　MAC Access Control Lists - Add Rule 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Rule ID	ルール ID を入力します。
Action	プルダウンメニューを使用して、パケットがルールの基準に一致する際にアクションを進める ACL を選択します。
Match Every	プルダウンメニューを使用して、「True」または「False」を選択します。 • True - すべてのパケットが選択した IP ACL およびルールに一致し、許可または拒否されること意味します。「True」を選択すると、すべてのパケットをルールに照合するため、他の照合基準を設定するオプションは提供されません。 • False - ルールに特定の照合基準を設定して、他の照合基準を設定します。
CoS	イーサネットフレームと照合する 802.1p ユーザプライオリティを入力します。
Destination BPDU	ボックスをチェックし、送信先 MAC としてマルチキャストアドレス「01:80:C2:00:00:00」を使用します。マスクは「FF:FF:FF:00:00:00」です。
Destination MAC	MAC アドレスを入力します。イーサネットフレームの送信先 MAC アドレスはこのアドレスに一致する必要があります。
Destination MAC Mask	送信先 MAC のマスクを入力します。
Ethertype Key	プルダウンメニューを使用して「EtherType」を選択します。パケットの EtherType がここで示す EtherType に一致する必要があります。「User Value」を選択すると、「Ethertype Value」欄が表示されます。この欄にカスタム値を入力します。
Source MAC	MAC アドレスを入力します。イーサネットフレームの送信元 MAC アドレスはこのアドレスに一致する必要があります。
Source MAC Mask	送信元 MAC のマスクを入力します。
VLAN	VLAN の ID を入力します。パケットの VLAN ID はここで入力した ID に一致する必要があります。

「Create」ルールボタンをクリックして、新しいルールを追加します。
「Cancel」ボタンをクリックすると設定は破棄されます。

ルールの編集

1. 「Rule ID」ハイパーリンクまたは「Edit」ボタンをクリックして、以下の画面を表示します。

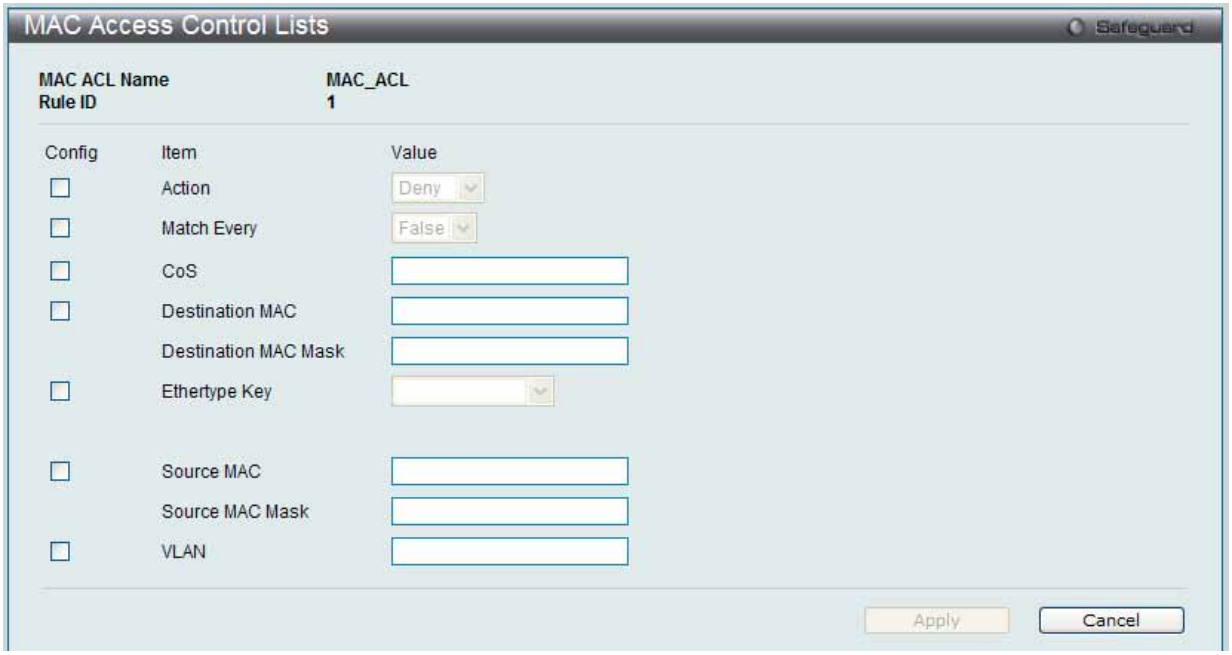


図 8.4-19　MAC Access Control Lists - Edit Rule 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Action	ボックスをチェックし、プルダウンメニューを使用して、ACL 送信アクションを選択します。
Match Every	プルダウンメニューを使用して、「True」または「False」を選択します。 • True - すべてのパケットが選択した IP ACL およびルールに一致し、許可または拒否されること意味します。「True」を選択すると、すべてのパケットをルールに照合するため、他の照合基準を設定するオプションは提供されません。 • False - ルールに特定の照合基準を設定して、他の照合基準を設定します。
CoS	ボックスをチェックし、イーサネットフレームと照合する 802.1p ユーザプライオリティを入力します。
Destination BPDU	ボックスをチェックし、送信先 MAC としてマルチキャストアドレス「01:80:C2:00:00:00」を使用します。マスクは「FF:FF:FF:00:00:00」です。
Destination MAC	ボックスをチェックし、MAC アドレスを入力します。イーサネットフレームの送信先 MAC アドレスはこのアドレスに一致する必要があります。
Destination MAC Mask	「Destination MAC」ボックスを選択した場合に、送信先 MAC を入力します。

項目	説明
EtherType Key	ボックスをチェックし、プルダウンメニューを使用して、EtherType を選択します。パケットの EtherType がここで示す EtherType に一致する必要があります。「User Value」を選択すると、「Ethertype Value」欄が表示されます。この欄にカスタム値を入力します。
Source MAC	ボックスをチェックし、MAC アドレスを入力します。イーサネットフレームの送信元 MAC アドレスはこのアドレスに一致する必要があります。
Source MAC Mask	「Source MAC」ボックスをチェックした場合に、送信元 MAC を入力します。
VLAN	ボックスをチェックし、VLAN ID を入力します。パケットの VLAN ID はここで入力した ID に一致する必要があります。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Cancel」ボタンをクリックすると設定は破棄されます。

Differentiated Services（クラス別サービス）

QoS 機能は Differentiated Services（DiffServ）をサポートしており、トラフィックを定義済みのホップ単位の動作に基づいてストリームに分類し、特定の QoS 処理を行うことができます。

Diffserv Configuration（Diffserv 設定）

Diffserv の一般的な状態情報を表示します。これには、主な DiffServ プライベート MIB テーブルの現在値と最大行および現在の管理モード設定が含まれます。

QoS > Differentiated Services > Diffserv 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。

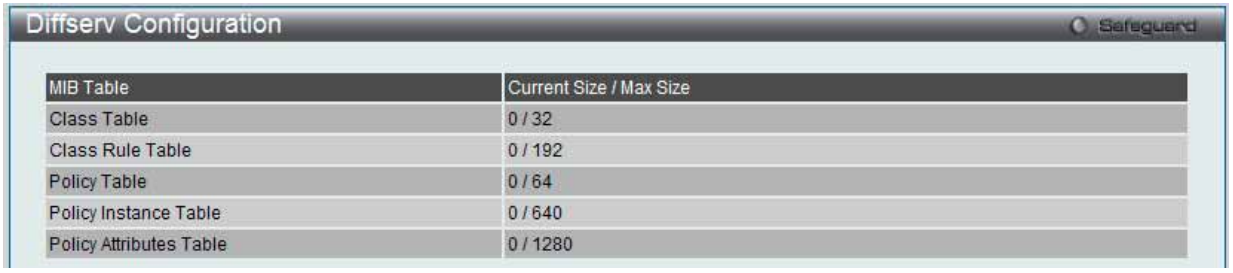


図 8.4-20　Diffserv Configuration 画面

Class Configuration（クラス設定）

新しい Diffserv クラス名の追加、既存のクラス名の変更または削除を行います。

1. **QoS > Differentiated Services > Class Summary** の順にメニューをクリックし、以下の画面を表示します。

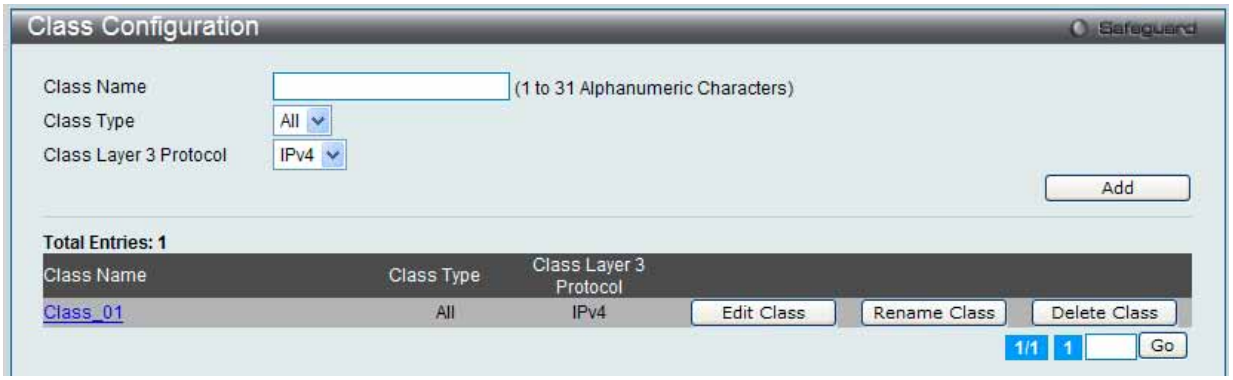


図 8.4-21　Class Configuration 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Class Name	クラス名を入力します。
Class Type	クラスタイプを選択します。
Class Layer 3 Protocol	クラスレイヤ 3 プロトコル（IPv4 または IPv6）を選択します。

「Add」ボタンをクリックして、入力した情報に基づいて新しいエントリを追加します。
「Edit Class」ボタンをクリックして、エントリを設定します。
「Rename Class」ボタンをクリックして、指定したクラス名を変更します。

エントリの削除
「Delete Class」ボタンをクリックして、リストからエントリを削除します。

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

クラス名の変更
1. 「Class ACL」ボタンをクリックすると、以下の画面が表示されます。

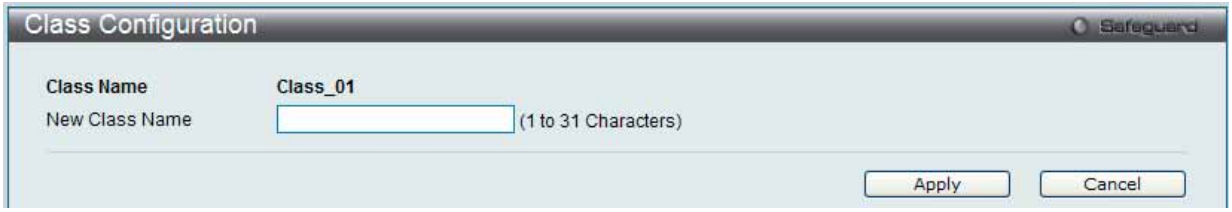


図 8.4-22　Class Configuration - Rename 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
New Class Name	新しいクラス名を入力します。

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「Cancel」ボタンをクリックすると設定は破棄されます。

エントリの設定
1. 「Edit Class」ボタンをクリックすると、以下の画面が表示されます。

図 8.4-23　Class Configuration - Edit Class 画面

2. 「Class Match Selector」から照合する要素を選択すると、選択した項目ごとに以下のような画面が表示されます。

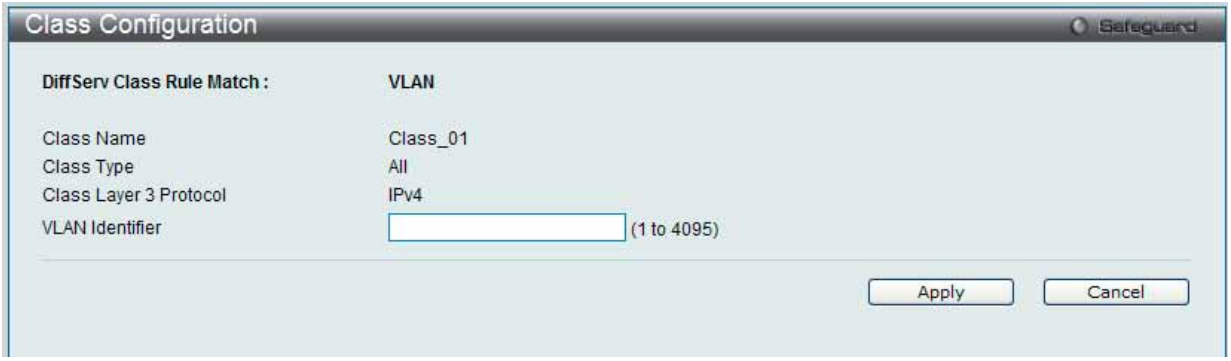


図 8.4-24　Class Configuration - Class Match Selector 画面

「Class Match Selector」には次の項目があります。

項目	説明
Class Match Selector	プルダウンメニューを使用して、特定のクラスに対する照合基準を選択します。「Add Match Criteria」ボタンをクリックして、そのクラスの基準設定を参照します。「Class Layer 3 Protocol」が「IPv4」である場合、プルダウンメニューに以下の項目選択が表示されます。 • Class of Service - これを選択し、次の画面で「Class of Service」の値 (0-7) を選択します。 • Destination IP Address - これを選択し、次の画面で IP アドレスとそのマスクを入力します。パケットの送信先 IP アドレスは入力したアドレスと一致する必要があります。 • Destination Layer4 Port - これを選択し、次の画面でプロトコルキーワードを選択します。パケットの TCP/UDP 宛先ポートがここで選択したポートに一致する必要があります。「Other」を選択し、「Protocol Value」欄にパケットがルールに一致するユーザ定義の Port ID を入力します。 • Destination MAC Address - これを選択して、次の画面で MAC アドレスとそのマスクを入力します。パケットの送信元 IP アドレスは入力したアドレスと一致する必要があります。 • Ethertype - これを選択して、次の画面で「Ethertype Key」を選択します。フレームの EtherType がここで選択した EtherType に一致する必要があります。「User Value」を選択し、本欄にユーザ定義の Ethertype を入力します。 • any - すべてのパケットが指定クラスに一致すると見なされ、追加入力情報は必要とされません。 • IP DSCP- これを選択して、次の画面で IP DSCP Keyword を選択します。パケットの DSCP は選択したキーワードと一致する必要があります。 • IP Precedence - これを選択して、次の画面で「Precedence Value」を選択します。パケットの DSCP は選択値に一致する必要があります。 • IP ToS - これを選択して、次の画面で ToS ビットとそのマスクを入力します。パケットの IP ヘッダにおける Type of Service ビットは、ここで入力した値に一致する必要があります。 • Protocol - これを選択して、次の画面でプロトコルを選択します。パケットのレイヤ 4 プロトコルが選択したプロトコルに一致する必要があります。 • Reference Class - これを選択して、基準の参照を開始するクラスを選択します。 • Source IP Address - これを選択して、次の画面で IP アドレスとそのマスクを入力します。パケットの送信元 IP アドレスは、ここで入力した IP アドレスとそのマスクに一致する必要があります。 • Source Layer4 Port - これを選択して、次の画面でプロトコルキーワードを選択します。パケットの TCP/UDP 送信元ポートが、ここで選択したポートに一致する必要があります。 • Source MAC Address - これを選択して、次の画面で MAC アドレスとそのマスクを入力します。パケットの送信元ポートの MAC アドレスが、ここで選択したアドレスに一致する必要があります。 • VLAN - これを選択して、次の画面で VLAN ID を入力します。Class Layer 3 Protocol が IPv6 である場合、以下の選択がプルダウンメニューに表示されます。 • Destination IPv6 Address - これを選択して、次の画面で IPv6 プレフィックスとプレフィックス長を入力します。パケットの送信先 IPv6 プレフィックスは入力したアドレスと一致する必要があります。 • Destination Layer4 Port - これを選択して、次の画面でプロトコルキーワードを選択します。パケットの TCP/UDP 宛先ポートがここで選択したポートに一致する必要があります。 • Any - すべてのパケットが指定クラスに一致すると見なされ、追加入力情報は必要とされません。 • Flow Label - これを選択して、次の画面でフローラベル値を入力します。 • IP DSCP - これを選択して、次の画面で IP DSCP Keyword を選択します。パケットの DSCP は選択したキーワードに一致する必要があります。 • Protocol - これを選択して、次の画面でプロトコルを選択します。パケットのレイヤ 4 プロトコルは選択したプロトコルに一致する必要があります。 • Reference Class - 次の画面で基準の参照を開始するクラスを選択します。 • Source IPv6 Address - これを選択して、次の画面で IPv6 プレフィックスとプレフィックス長を入力します。パケットの送信元 IPv6 プレフィックスは入力したアドレスと一致する必要があります。 • Source Layer4 Port - これを選択して、次の画面でプロトコルキーワードを選択します。パケットの TCP/UDP 送信元ポートがここで選択したポートに一致する必要があります。「Add Match Criteria」ボタンをクリックして、クラスの基準設定を参照します。

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。
「Cancel」ボタンをクリックすると設定は破棄されます。

Policy Configuration（ポリシー設定）

クラスのコレクションを 1 つ以上のポリシーステートメントと関連付けます。

1. **QoS > Differentiated Services > Policy 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。

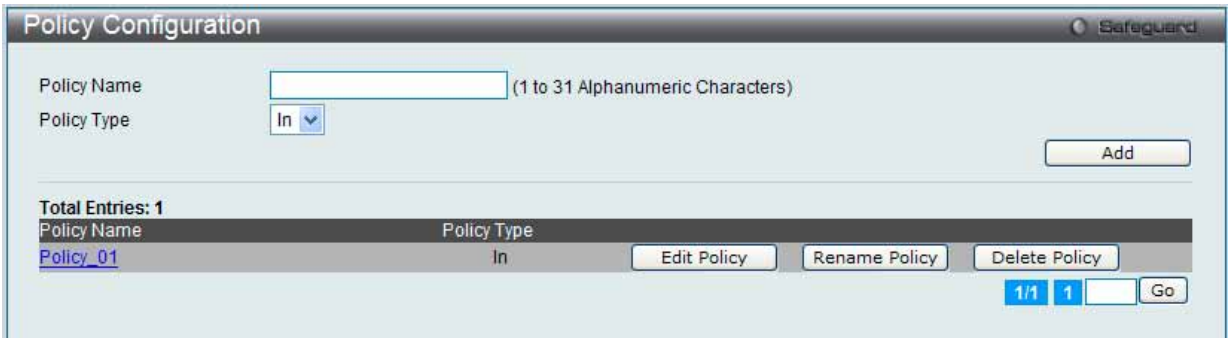


図 8.4-25　Policy Configuration 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Policy Name	ポリシー名を入力します。
Policy Type	ポリシータイプを選択します。

「Add」ボタンをクリックして、入力した情報に基づいて新しいエントリを追加します。
「Edit Policy」ボタンをクリックして、エントリを設定します。
「Rename Policy」ボタンをクリックして、指定したポリシー名を変更します。
「Delete Policy」ボタンをクリックして、リストからエントリを削除します。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

ポリシー名の変更

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

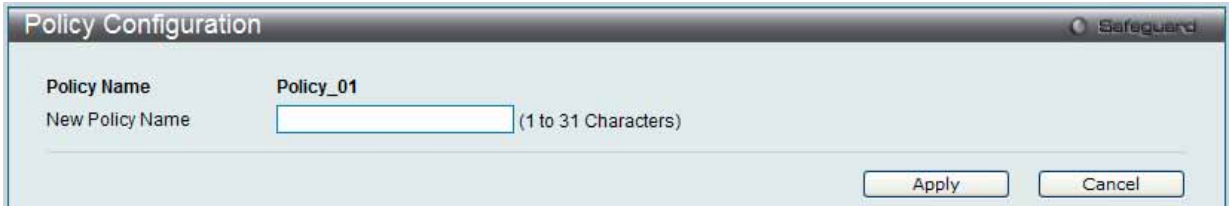


図 8.4-26　Policy Configuration - Rename 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
New Policy Name	新しいポリシー名を入力します。

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。
「Cancel」ボタンをクリックすると設定は破棄されます。

エントリの設定

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

図 8.4-27　Policy Configuration - Edit Policy 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Policy Type	利用可能なポリシータイプを選択します。
Available Class List	既存の DiffServ クラス名を選択します。「Class Configuration」画面で新しいクラスの追加または削除を行うと、自動的にリストは更新されます。
Member Class List	ポリシーに追加されている DiffServ クラスを選択します。

「Add Selected Class」ボタンをクリックして、「Member Class List」プルダウンメニューに既存の DiffServ クラスを追加します。
「Remove Selected Class」ボタンをクリックして、「Member Class List」プルダウンメニューから既存の DiffServ クラスを削除します。
「<<Back」をボタンをクリックして前のページに戻ります。

Policy Class Definition（ポリシークラス定義）

ポリシーにクラスを関連付けて、そのポリシークラスインスタンスに属性を定義します。

1. **QoS > Differentiated Services > Policy Class Definition** の順にメニューをクリックし、以下の画面を表示します。

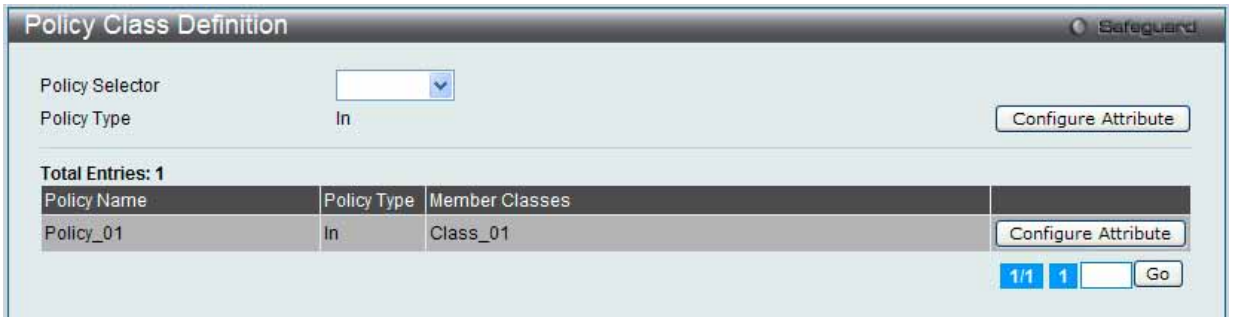


図 8.4-28　Policy Class Definition 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Policy Selector	設定するポリシーを選択します。

「Configuration Attribute」ボタンをクリックして、指定ポリシーを設定します。
複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

ポリシー設定

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

図 8.4-29　Policy Class Definition 画面

2. 「Policy Attribute Selector」から選択した項目ごとに以下のような画面が表示されます。

図 8.4-30　Policy Class - Policy Attribute Selector 画面

3. 以下の項目を使用して設定および参照します。

項目	説明
Member Class List	このポリシー名に関連付けるメンバクラスを選択します。
Policy Attribute Selector	プルダウンメニューを使用してこのポリシータイプにサポートする属性を選択します。「Configure Selected Attribute」ボタンをクリックして、そのポリシーに対する属性設定を参照します。 • Drop - これを選択すると、このポリシークラスのパケットが破棄されます。 • Mark CoS - 本欄を選択し、特定の Class of Service キュー番号を入力すると、802.1p ヘッダの優先度フィールドに指定したサービスクラスに関連するトラフィックストリームに対するパケットのすべてにマークを付けます。 • Mark IP DSCP - これを選択して、次の画面で IP DSCP Keyword を選択します。これは、選択した IP DSCP 値を持つトラフィックストリームの全パケットをマークします。 • Mark IP Precedence - これを選択して、次の画面で「 IP Precedence Value」を選択します。これは、指定した IP Precedence 値を持つトラフィックストリームの全パケットをマークします。 • Police Simple - これを選択して、次の画面で指定クラスにトラフィックポリシングスタイルを設定します。 - Committed Rate (bps) - このクラスへの入力パケットの到着レートをモニタリングするためにコミットレートを入力します。 - Committed Burst Size (KB) - コミットバーストサイズを入力して、許可される適合トラフィック量を決定します。 - Conform Action Selector - パケットが適合すると思われた場合のアクションを選択します。 • Drop - パケットは直ちに破棄されます。 • Mark CoS - パケットは、システムのフォワーディングエレメントに提供される前に DiffServ によって指定済みの CoS 値でマークされます。 •「Conform CoS Value」欄に値（0-7）を入力します。 • Mark IP DSCP - パケットは、システムのフォワーディングエレメントに提供される前に DiffServ によって指定済みの DSCP 値にマークされます。 • プルダウンメニューから Conform DSCP Keyword を選択します。 • Mark IP Precedence - パケットは、システムのフォワーディングエレメントに提供される前に DiffServ によって指定済みの IP Precedence 値にマークされます。「Conform IP Precedence Value」欄に値（0-7）を入力します。 • Send - パケットは DiffServ によってシステムのフォワーディングエレメントに変更されずに提供されます。 「Configure Selected Attribute」ボタンをクリックして、そのポリシーに関する属性設定を参照します。

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

8.5 Network Visualization（無線ネットワークの視覚化）

WLAN 視覚化コンポーネントは無線ネットワークの情報を図式化して表示するためのオプション機能です。本機能では Java アプレットを使用して、D-Link 統合スイッチ、D-Link アクセスポイント、他社のアクセスポイント、および接続する無線クライアントを表示します。本機能によって、建物の中でのデバイスの位置等をビジュアル化して確認できます。

まず、用意したカスタムイメージをアップロードして図の背景を作成します。そして、スイッチにより検出された WLAN を構成するデバイスを図中に配置し、ご使用の無線ネットワークをリアルに表現します。視覚化された WLAN 図上の各デバイスから、そのデバイスについての情報を取得したり、Web インタフェースの設定ページへリンクすることもできます。

本章は以下の項で構成され、D-Link 統合アクセスシステムの WLAN 視覚化コンポーネントの操作、管理方法について説明します。

項目	説明	参照ページ
Download Image（イメージのダウンロード）	WLAN 視覚化グラフ用画像をダウンロードします。	517
Launch…（起動）	WLAN 視覚化アプリケーションの起動、メニューバーについて説明します。	518

Download Image（イメージのダウンロード）

ネットワーク可視化のためにイメージをダウンロードします。

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

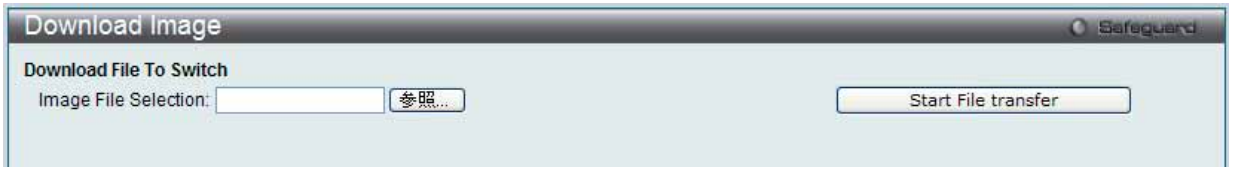


図 8.5-1　Download Image 画面

「参照」ボタンをクリックして、画像ファイルを参照します。画像ファイルは GIF または JPG 形式とします。

「Start File transfer」ボタンをクリックすると、スイッチに画像をダウンロードします。

Launch…（起動）

D-Link WLAN Visualization を表示します。

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

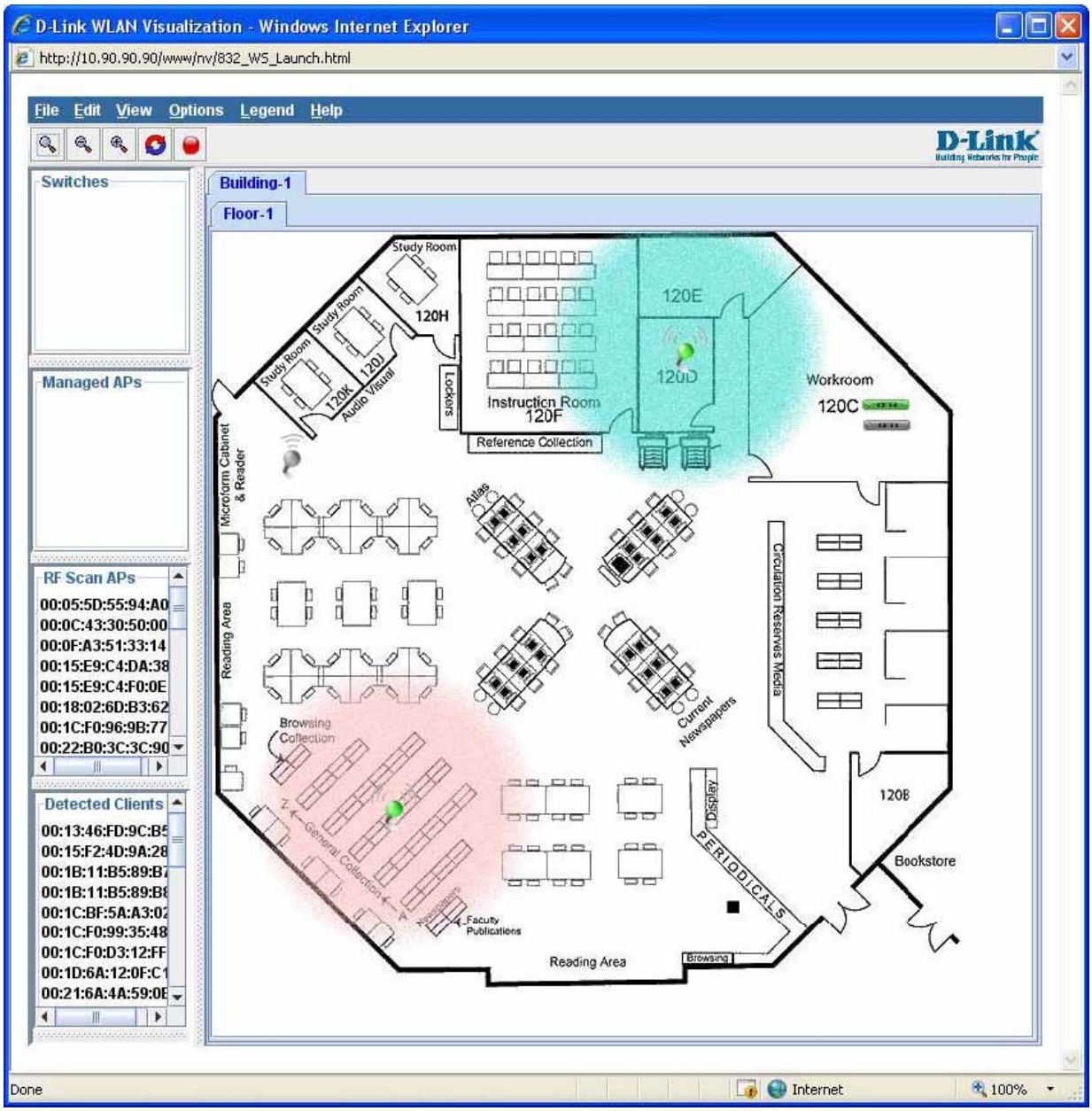


図 8.5-2　D-Link WLAN Visualization 画面

右のウィンドウに複数の画像をインポートし、左の画面にあるスイッチ、アクセスポイントまたはクライアントを右にドラッグして、仮想無線ネットワーク環境を作成することができます。

メニューバー

図 8.5-3　D-Link WLAN 可視化用のメニューバー

以下の表では、WLAN 視覚化ツールで使用できるメニューの概要を示します。

WLAN 視覚化ツールのメニューバー

メニュー項目		説明
File	Force refresh	手動更新。Java クライアントアプリケーションの再同期します。グラフの編集後、本メニューを実行して、画面を更新します。
	Reconnect and Refresh	クライアントアプリケーションを一旦スイッチから切断して、再接続します。
	Exit	WLAN 視覚化アプリケーションを終了します。
Edit	New Graph	新規のグラフを作成し、グラフ名、背景画像、縮尺を設定するための画面を開きます。
	Edit Graph	作成済みのグラフを開きます。背景画像と縮尺は変更可能ですが、グラフ名を変更するためには、新規のグラフを作成する必要があります。
	Delete Graph	作成済みのグラフを削除します。本項目を選択すると、本当に削除を実行するかどうか確認するダイアログボックスが表示されます。
	Image Management	使用可能な背景画像のリストを表示します。また画像の削除も本項目から行います。
View	Ungraphed Components	左区画の図示化されていないコンポーネント群の表示方法を選択します。 • Tab View - 1 種類のコンポーネントのみを表示し、他の種類をタブにまとめて表示します。 • List View - すべての種類のコンポーネントを表示します。
	AP Power Display	アクセスポイントの出力エリアイメージを選択します。 • Disable Power Display - 出力エリアイメージの表示を行いません。 • Show 5GHz Band - 802.11a または 5GHz 802.11n モードで動作している無線インタフェースの出力エリアイメージを表示します。 • Show 2.4GHz Band - 802.11b/g または 2.4GHz 802.11n モードで動作している無線インタフェースの出力エリアイメージを表示します。 出力エリアイメージのサイズは、無線インタフェースの送信電力に基づき、3 種類（低、中、高）のが用意されています。またそのサイズは現在使用している背景画像の倍率にも依存します。 1 つのモードがアクセスポイントの 2 つの無線インタフェースに設定されている場合は、2 つの出力エリアイメージが表示されます。 **注意** 出力エリアイメージの色は、接続に使用するチャンネルによって異なります。 もし、2 台のアクセスポイントが、お互いの伝送範囲内において同じチャンネル（または近隣のチャンネル）を使用していれば、アクセスポイント同士が干渉し合い、無線クライアントの通信品質は悪くなります。そのような干渉を防ぐために、以下のいずれかを実行してください。 • アクセスポイントの送信電力を低く設定する • アクセスポイント同士を物理的に離して設置する • アクセスポイント上で自動チャンネル調整アルゴリズムを使用する。または干渉を起こさないように手動でチャンネルを調整する。 **警告** 出力エリアイメージは例示を目的としており、あくまでもイメージです。実際の電力分布は、オフィスの壁などの伝播特性やバックグラウンドの RF ノイズなどにより異なります。
Options	Show Managed APs	選択すると管理下のアクセスポイントを表示します。
	Show RF Scan APs	選択すると RF スキャンにより検出されたアクセスポイントを表示します。
	Show Managed AP Clients	選択すると管理下のアクセスポイントと接続中のクライアントを表示します。
	Show Detected Clients	選択すると検出された無線クライアントを表示します。
Legend	Images	WLAN コンポーネントとアイコンの対応を表示します。
	Channel Color	伝送に使用されているチャンネルと、出力エリアイメージで使用する色の対応を表示します。
Help	WLAN Visualization	新しい HTML 画面を表示し、WLAN オンラインヘルプを表示します

「Legend」メニューについて

「Legend（凡例）」メニューを選択すると、グラフ上に表示されるアイコンと、それらの色についての情報を確認することができます。
「Images」を選択すると、グラフ上で各 WLAN コンポーネントを表すアイコンを表示します。

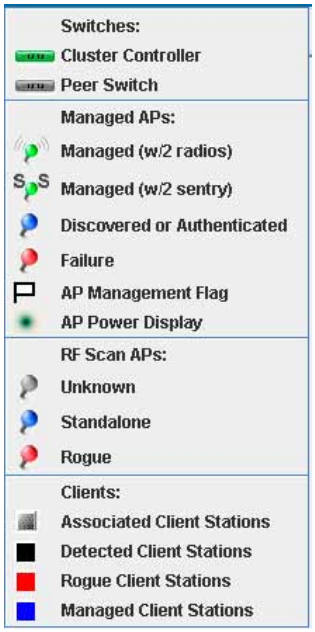


図 8.5-4　アイコンの凡例

凡例が示すように、スイッチ配下のアクセスポイントは、その状態によって色分けして表示されます。

- 青 -（Discovered or Authenticated）アクセスポイントはスイッチにより検出されましたが、状態遷移中です。アクセスポイントは認証待ちであるか、または認可・認証はされたが設定がなされていない状態です。
- 緑 -（Managed）AP プロファイルが適用されており、「Managed」モードで動作中です。
- 赤 -（Failure）スイッチとの通信が切断されました。アクセスポイントが再起動中であるか、または認証に失敗しました。

「Sentry」モードでの動作中は、以下の通りアクセスポイントのアイコンのアンテナが「S」という文字に変わって表示されます。

図 8.5-5　「Sentry」モード - 詳細図

「Sentry」モード中は、アクセスポイント周囲の出力イメージはグレーで表示されます。
チャンネルカラーの凡例では、出力イメージと各チャンネルを表す色の対応を示します。無線インタフェースが通信に使用している各チャンネルはそれぞれ色が割り当てられています。利用できるチャンネルは、無線モードおよび国によって異なります。

図 8.5-6　チャンネルの色

使用中のチャンネルを表示するためには、管理対象のアクセスポイント上にマウスをポイントして、ポップアップ画面を表示させます。画面中に使用中のチャンネルを含む、アクセスポイントの諸情報が確認できます。

第 9 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 / Log（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	521
Tools（ツールメニュー）		
License Management（ライセンス管理）	ライセンスのアクティベーションコードをインストールします。	522
Download Firmware（ファームウェアのダウンロード）	コンフィグレーションファイルをアップロードします。	522
Upload Firmware（ファームウェアのアップロード）	ファームウェアファイルをアップロードします。	523
Download Configuration（コンフィグレーションのダウンロード）	コンフィグレーションファイルをダウンロードします。	524
Upload Configuration（コンフィグレーションファイルのアップロード）	コンフィグレーションファイルをアップロードします。	525
Upload Log File（ログファイルのアップロード）	ログファイルをアップロードします。	526
Reset（リセット）	工場出荷時設定に戻し、メモリに保存します。	527
Reboot System（システムの再起動）	スイッチの再起動を行います。	527

Save Configuration / Log（コンフィグレーションとログの保存）

「Save Configuration」により、コンピュータでのフォルダにスイッチのコンフィグレーションをバックアップすることができます。「Type」欄から「Configuration」を選択し、提供されたスペースにファイルパスを入力して「Apply」ボタンをクリックします。

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

コンフィグレーションの保存
スイッチのコンフィグレーションファイルをバックアップすることができます。「Type」欄から「Configuration」を選択して、「Apply」ボタンをクリックします。

図 9-1　Save 画面 - Configuration

ログの保存
スイッチに関するログファイルをバックアップすることができます。「Type」欄から「Log」を選択して、「Apply」ボタンをクリックします。

図 9-2　Save 画面 - Log

すべての保存
コンフィグレーションに行った変更を永続的に保存します。本オプションを使用すると、スイッチの再起動後も変更は維持されます。「Type」欄から「All」を選択して、「Apply」ボタンをクリックします。

図 9-3　Save 画面 - All

Tools（ツールメニュー）

Web マネージャ先頭の **Tools** をクリックして、以下のメニューからオプションを選択します。

License Management（ライセンス管理）

D-Link License Management System (DLMS) のアクティベーションコードをインストールして、表示します。

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

図 9-4　License Management 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
Activation Code Installation	アクティベーションコードを入力します。

「Install」ボタンをクリックすると、DLMS アクティベーションコードをインストールします。
「Find」ボタンをクリックして、選択に基づいて表示セクションにログを表示します。

Download Firmware（ファームウェアのダウンロード）

スイッチにファームウェアをダウンロードします。

Download Firmware From TFTP（TFTP からファームウェアをダウンロード）

TFTP サーバからスイッチにファームウェアをダウンロードして、スイッチを更新することができます。

1. Web マネージャ先頭の **Tools > Download Firmware** を選択して以下の画面を表示します。

図 9-5　Download Firmware From TFTP 画面

2. 「Download Firmware From TFTP」をチェックします。

3. 以下の項目を使用して設定および参照します。

項目	説明
TFTP Server IP	使用する TFTP サーバの IP アドレスを指定します。 • IPv4 - ラジオボタンをクリックして、使用する TFTP サーバの IP アドレスを指定します。 • IPv6 - ラジオボタンをクリックして、使用する TFTP サーバの IPv6 アドレスを指定します。
Source File	送信元ファイルの位置と名前を入力します。
Destination File	送信先ファイルの位置と名前を入力します。

「Download」ボタンをクリックすると、ダウンロードが開始されます。

Download Firmware From HTTP（HTTP からファームウェアをダウンロード）

コンピュータからスイッチにファームウェアをダウンロードして、スイッチを更新することができます。

1. Web マネージャ先頭の **Tools > Download Firmware** を選択して以下の画面を表示します。

図 9-6　Download Firmware From HTTP 画面

2. 「Download Firmware From HTTP」をチェックします。

3. 以下の項目を使用して設定および参照します。

項目	説明
Source File	送信元ファイルの位置と名前を入力するか、または「参照」ボタンをクリックして、ダウンロード用のファームウェアファイルを参照します。
Destination File	送信先ファイルの位置と名前を入力します。

「参照」ボタンをクリックすると、ダウンロードのためのファームウェアファイルを参照することができます。
「Download」ボタンをクリックすると、ダウンロードが開始されます。

Upload Firmware（ファームウェアのアップロード）

スイッチにファームウェアをアップロードします。

Upload Firmware To TFTP（ファームウェアを TFTP にアップロードする）

スイッチから TFTP サーバにファームウェアをアップロードすることができます。

1. Web マネージャ先頭の **Tools > Upload Firmware** を選択して以下の画面を表示します。

図 9-7　Upload Firmware To TFTP 画面

2. 以下の項目を使用して設定および参照します。

項目	説明
TFTP Server IP	使用する TFTP サーバの IP アドレスを指定します。 • IPv4 - ラジオボタンをクリックして、使用する TFTP サーバの IP アドレスを指定します。 • IPv6 - ラジオボタンをクリックして、使用する TFTP サーバの IPv6 アドレスを指定します。
Destination File	送信先ファイルの位置と名前を入力します。
Source File	送信元ファイルの位置と名前を入力します。

「Upload」ボタンをクリックすると、アップロードが開始されます。

Download Configuration（コンフィグレーションのダウンロード）

スイッチにコンフィグレーションをダウンロードするために以下の画面を使用します。

Download Configuration From TFTP（TFTP サーバからコンフィグレーションファイルをダウンロードする）

TFTP サーバからスイッチにコンフィグレーションをダウンロードして、スイッチを更新することができます。

1. Web マネージャ先頭の **Tools > Download Configuration** を選択して以下の画面を表示します。

図 9-8　Download Configuration From TFTP 画面

2. 「Download Configuration From TFTP」をチェックします。

3. 以下の項目を使用して設定および参照します。

項目	説明
TFTP Server IP	使用する TFTP サーバの IP アドレスを指定します。 • IPv4 - ラジオボタンをクリックして、使用する TFTP サーバの IP アドレスを指定します。 • IPv6 - ラジオボタンをクリックして、使用する TFTP サーバの IPv6 アドレスを指定します。
Source File	送信元ファイルの位置と名前を入力します。
Destination File	送信先ファイルの位置と名前を入力します。

「Download」ボタンをクリックすると、ダウンロードが開始されます。

Download Configuration From HTTP（HTTP からコンフィグレーションファイルをダウンロードする）

コンピュータからスイッチにコンフィグレーションをダウンロードして、スイッチを更新することができます。

1. Web マネージャ先頭の **Tools > Download Configuration** を選択して以下の画面を表示します。

図 9-9　Download Configuration From HTTP 画面

2. 「Download Configuration From HTTP」をチェックします。

3. 以下の項目を使用して設定および参照します。

項目	説明
Destination File	送信先ファイルの位置と名前を入力します。
Source File	送信元ファイルの位置と名前を入力します。

「参照」ボタンをクリックすると、ダウンロードのためのコンフィグレーションファイルを参照することができます。
「Download」ボタンをクリックすると、ダウンロードが開始されます。

Upload Configuration（コンフィグレーションファイルのアップロード）

スイッチからコンフィグレーションをアップロードするために以下の画面を使用します。

Upload Configuration To TFTP（TFTP サーバにコンフィグレーションをアップロードする）

スイッチから TFTP サーバにコンフィグレーションファイルをアップロードすることができます。

1. Web マネージャ先頭の **Tools > Upload Configuration** を選択して以下の画面を表示します。

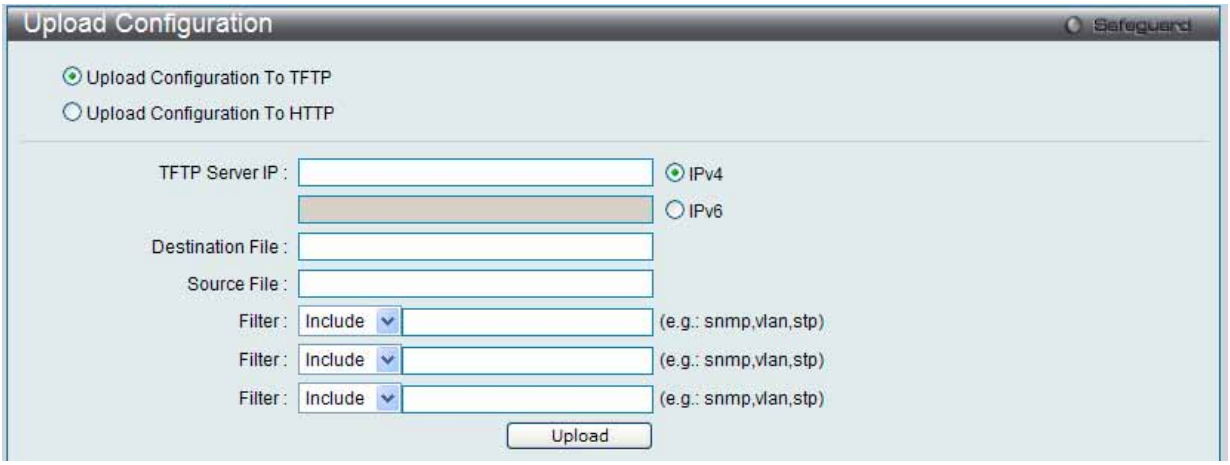


図 9-10　Upload Configuration To TFTP 画面

2. 「Upload Configuration From TFTP」をチェックします。

3. 以下の項目を使用して設定および参照します。

項目	説明
TFTP Server IP	使用する TFTP サーバの IP アドレスを指定します。 • IPv4 - ラジオボタンをクリックして、使用する TFTP サーバの IP アドレスを指定します。 • IPv6 - ラジオボタンをクリックして、使用する TFTP サーバの IPv6 アドレスを指定します。
Source File	送信元ファイルの位置と名前を入力します。
Destination File	送信先ファイルの位置と名前を入力します。
Filter	SNMP、VLAN または STP のようなフィルタを「Include」（含む）、「Exclude」（除外する）、または「Begin」（開始する）ように指定できます。適切な「Filter」アクションを選択し、提供されたスペースにファイル名を入力します。

「Upload」ボタンをクリックすると、アップロードが開始されます。

Upload Configuration To HTTP（コンフィグレーションを HTTP にアップロードする）

スイッチからコンピュータにコンフィグレーションファイルをアップロードすることができます。

1. Web マネージャ先頭の **Tools > Upload Configuration** を選択して以下の画面を表示します。

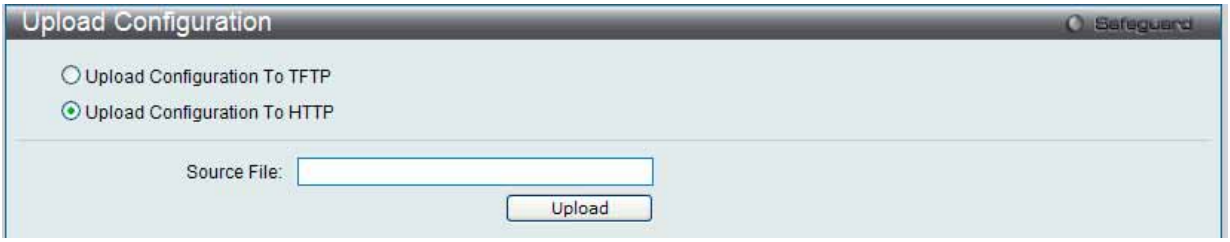


図 9-11　Upload Configuration To HTTP 画面

2. 「Upload Configuration From HTTP」をチェックします。

3. 以下の項目を使用して設定および参照します。

項目	説明
Destination File	送信先ファイルの位置と名前を入力します。

「Upload」ボタンをクリックすると、アップロードが開始されます。

Upload Log File（ログファイルのアップロード）

スイッチのログファイルをアップロードします。

Upload Log To TFTP（TFTP サーバにログをアップロードする）

スイッチから TFTP サーバにログファイルをアップロードすることができます。

1. Web マネージャ先頭の **Tools > Upload Log File** を選択して以下の画面を表示します。

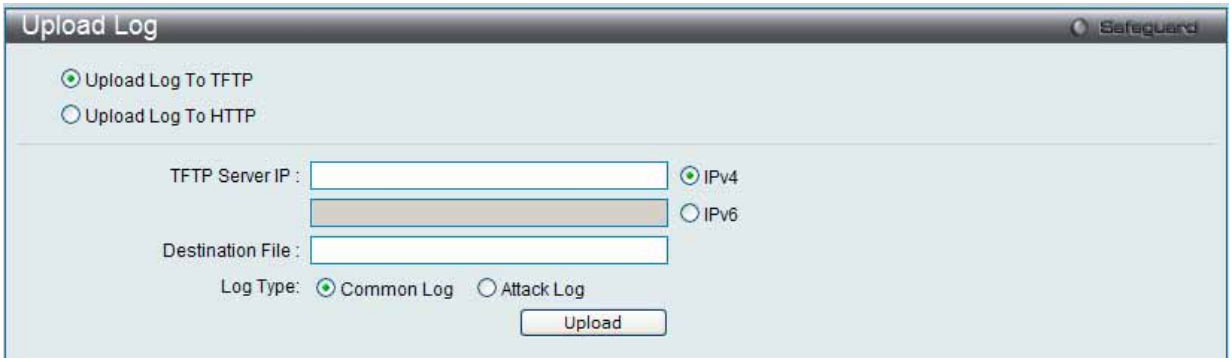


図 9-12　Upload Log To TFTP 画面

2. 「Upload Log From TFTP」をチェックします。

3. 以下の項目を使用して設定および参照します。

項目	説明
TFTP Server IP	使用する TFTP サーバの IP アドレスを指定します。 • IPv4 - ラジオボタンをクリックして、使用する TFTP サーバの IP アドレスを指定します。 • IPv6 - ラジオボタンをクリックして、使用する TFTP サーバの IPv6 アドレスを指定します。
Destination File	送信先ファイルの位置と名前を入力します。
Log Type	転送されるログのタイプを選択します。 • Common Log - 一般的なログエントリをアップロードします。 • Attack Log - 攻撃に関するログをアップロードします。

「Upload」ボタンをクリックすると、アップロードが開始されます。

Upload Log To HTTP（HTTP にログをアップロードする）

スイッチからコンピュータにログファイルをアップロードすることができます。

1. Web マネージャ先頭の **Tools > Upload Log File** を選択して以下の画面を表示します。

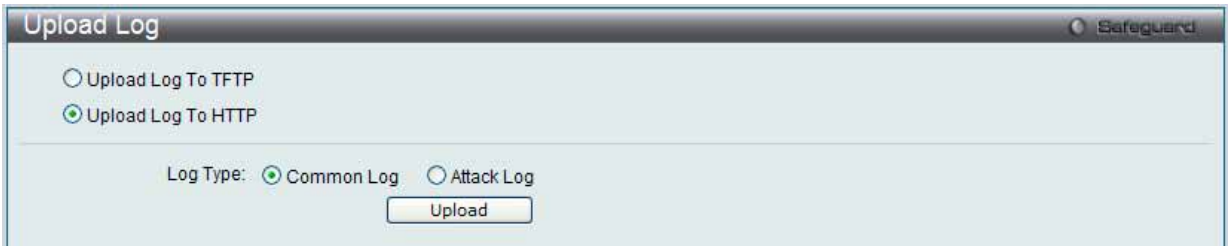


図 9-13　Upload Log To HTTP 画面

2. 「Upload Log From HTTP」をチェックします。

3. 以下の項目を使用して設定および参照します。

項目	説明
Log Type	転送されるログのタイプを選択します。 • Common Log - 一般的なログエントリをアップロードします。 • Attack Log - 攻撃に関するログをアップロードします。

「Upload」ボタンをクリックすると、アップロードが開始されます。

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用意されています。いくつかのパラメータの設定内容を保持したままで、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。

注意 「Reset System」オプションだけは工場出荷時設定をスイッチの NV-RAM に書き込み、スイッチを再起動します。他のすべてのオプションは現在の設定を出荷時設定に戻しますが、この設定は保存されません。「Reset System」はスイッチのコンフィグレーションを工場出荷状態まで戻します。

「Reset」はスイッチのユーザアカウント、ヒストリログを除いて他のすべての設定を工場出荷時の初期設定に戻します。スイッチは、本画面を使用してリセットされ、「Save Changes」が実行されないと、スイッチは再起動時に最後に保存されたコンフィグレーションに戻ります。

Web マネージャ先頭の **Tools > Reset** を選択し、以下の画面を表示します。

図 9-14　Reset System 画面

項目	説明
Reset	IP アドレス、ユーザアカウントおよびバナーを除いてスイッチを工場出荷時の初期設定に戻します。
Reset Config	スイッチを工場出荷時設定にリセットしますが、再起動は行いません。
Reset System	スイッチを工場出荷時設定にリセットして、再起動を実行します。

「Apply」ボタンをクリックして、リセット操作を開始します。

Reboot System（システムの再起動）

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。

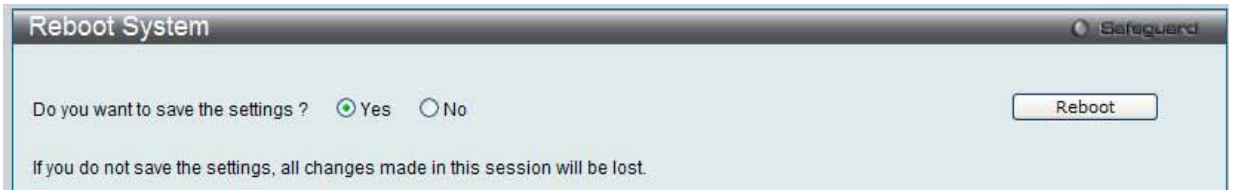


図 9-15　Reboot System 画面

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。

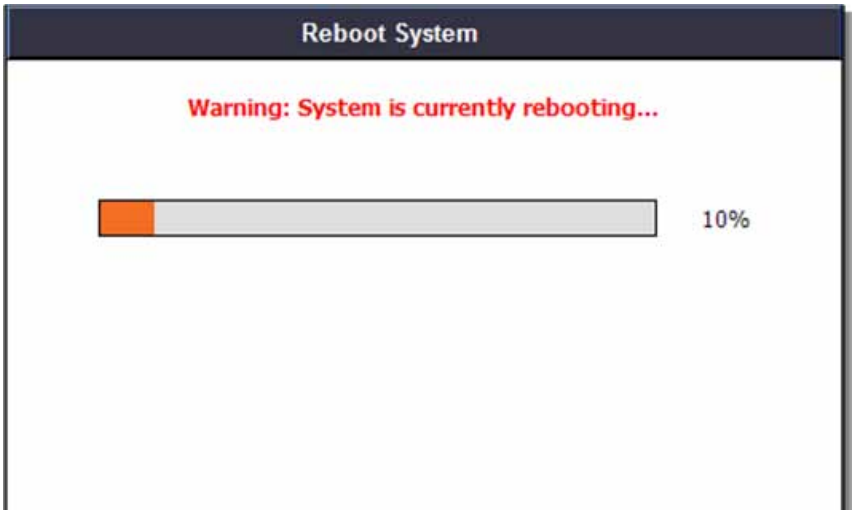


図 9-16　System Reboot 画面

付録 A パケットコンテンツ ACL を使用した ARP スプーフィング攻撃の軽減

ARP を動作させる方法

ARP（Address Resolution Protocol）は、IP アドレスだけがわかっている場合に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的な方法です。しかし、クラッカーが ARP パケット内の IP および MAC 情報を偽造して LAN への攻撃（ARP スプーフィングとして、知られている）を行うために、このプロトコルは被害を受けやすいと言えます。ここでは ARP プロトコル、ARP スプーフィング攻撃、および D-Link スイッチが提供する ARP スプーフィング攻撃を防御する対策について紹介します。

ARP 処理中に、PC-A は、はじめに、PC-B の MAC アドレスを問い合わせする ARP リクエストを発行します。そのネットワーク構造は図 A-1 の通りです。

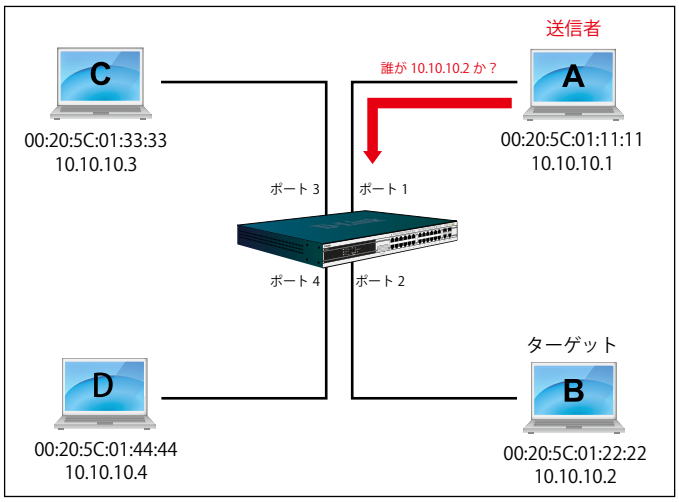


図 A-1　ARP の動作方法

その間、PC-A の MAC アドレスは「送信側 H/W アドレス」に書かれ、その IP アドレスは ARP ペイロードの「送信側プロトコルアドレス」に書かれます。PC-B の MAC アドレスが未知である場合、「ターゲット H/W アドレス」は「00-00-00-00-00-00」であり、PC-B の IP アドレスは図 A-2 に示された「ターゲットプロトコルアドレス」に書かれます。

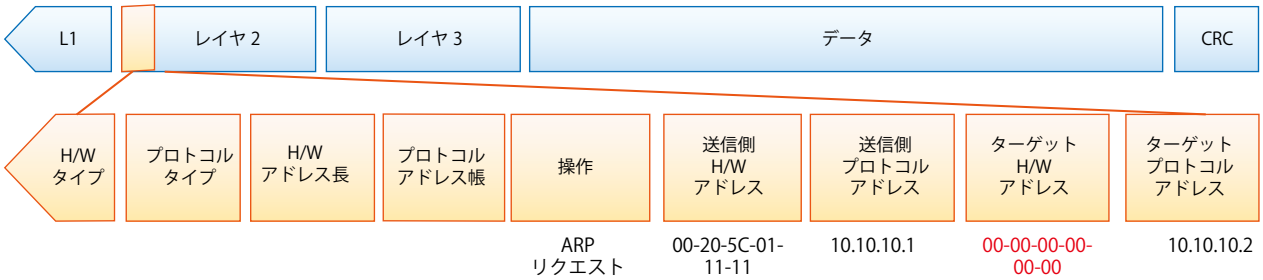


図 A-2　ARP ペイロード

ARP リクエストはイーサネットフレームにカプセル化されて送信されます。図 A-3 の通り、イーサネットフレーム内の「送信元アドレス」は、PC-A の MAC アドレスとなります。ARP リクエストは、ブロードキャスト経由で送信されるため、イーサネットのブロードキャスト（FF-FF-FF-FF-FF-FF）のフォーマットには「宛先アドレス」があります。

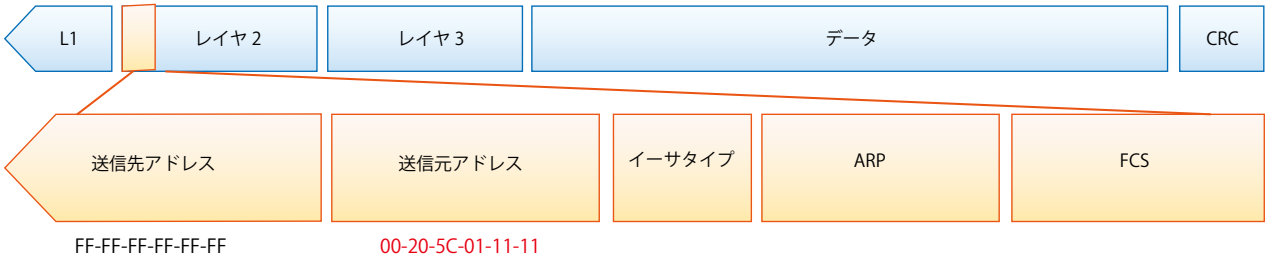


図 A-3　イーサネットフレームフォーマット

スイッチがフレームを受信すると、イーサネットフレームヘッダの「送信元アドレス」をチェックします。アドレスがフォワーディングテーブルにないと、スイッチは学習して PC-A の MAC アドレスと関連ポートをフォワーディングテーブルに追加します。

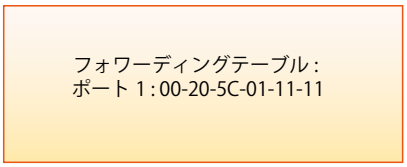


図 A-4　フォワーディングテーブル

さらに、スイッチがブロードキャストされた ARP リクエストを受信すると、送信元ポート（図 A-5 ではポート 1）を除くすべてのポートにフレームをフラッドします。

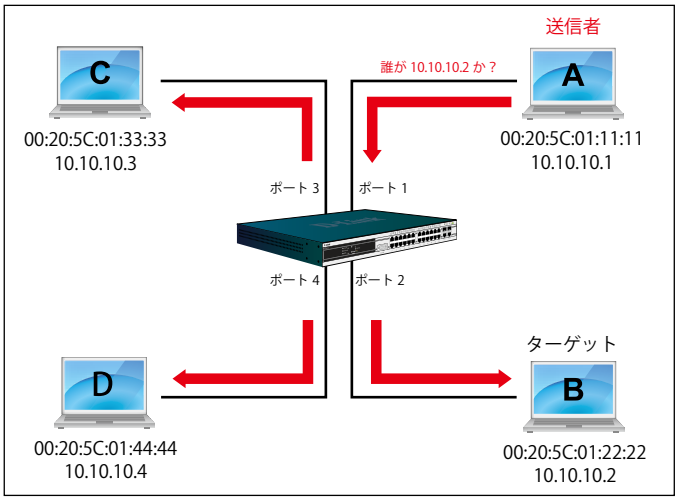


図 A-5　ポートフラッド画面

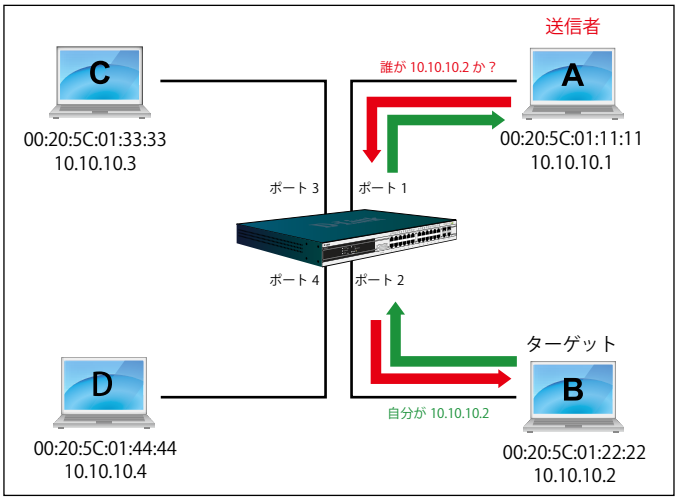


図 A-6　パケットコンテンツ ACL 画面

スイッチが ARP リクエストのフレームをネットワークにフラッドする場合、すべての PC が、フレームを受信し、検証を行いますが、PC-B だけが宛先 IP に一致するためにクエリに応答します（図 A-6 参照）。

PC-B が ARP リクエストに応答すると、その MAC アドレスは図 A-7 に示されている ARP ペイロード内の「ターゲット H/W アドレス」に書かれます。ARP リプライは、次に、再びイーサネットフレームにカプセル化されて、送信側に返送されます。ARP リプライはユニキャスト通信の形式です。

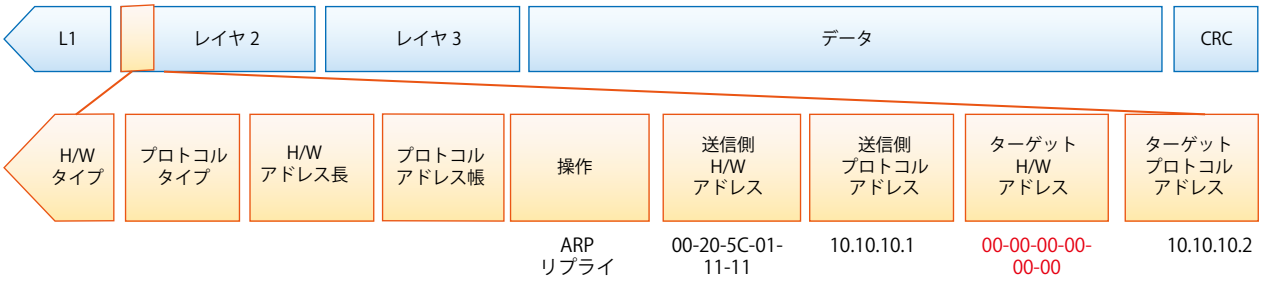


図 A-7　ARP ペイロード

PC-B がクエリに応答する場合、イーサネットフレーム内の「宛先アドレス」は、PC-A の MAC アドレスに変更されます。「送信元アドレス」は PC-B の MAC アドレスに変更されます（図 A-8 参照）。

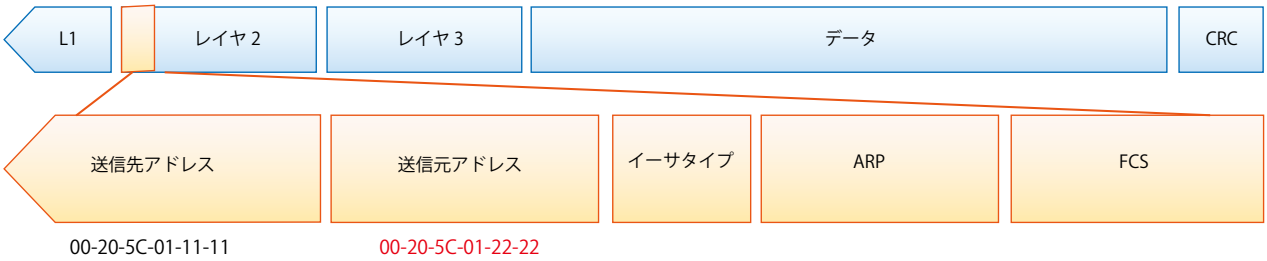


図 A-8　イーサネットフレームフォーマット

スイッチは、また、イーサネットフレームの「送信元アドレス」を調べて、フォワーディングテーブルにはアドレスがないことを見つけます。スイッチは PC の MAC アドレスを学習してフォワーディングテーブルを更新します。

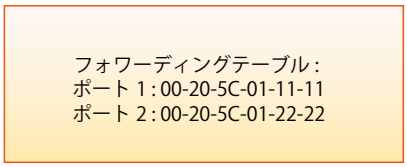


図 A-9　フォワーディングテーブル

ARP スプーフィングでネットワークを攻撃する方法

また、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、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。一般的に、目的は、デフォルトゲートウェイなどの別のノードの IP アドレスに攻撃者の MAC アドレスかでたらめの 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ます。

IP スプーフィング攻撃は、ホストが自身の IP アドレスを解決するため ARP リクエストを送信する場合に発生する Gratuitous ARP によって引き起こされます。図 A-10 は、LAN のハッカーによる ARP スプーフィング攻撃の開始を示しています。

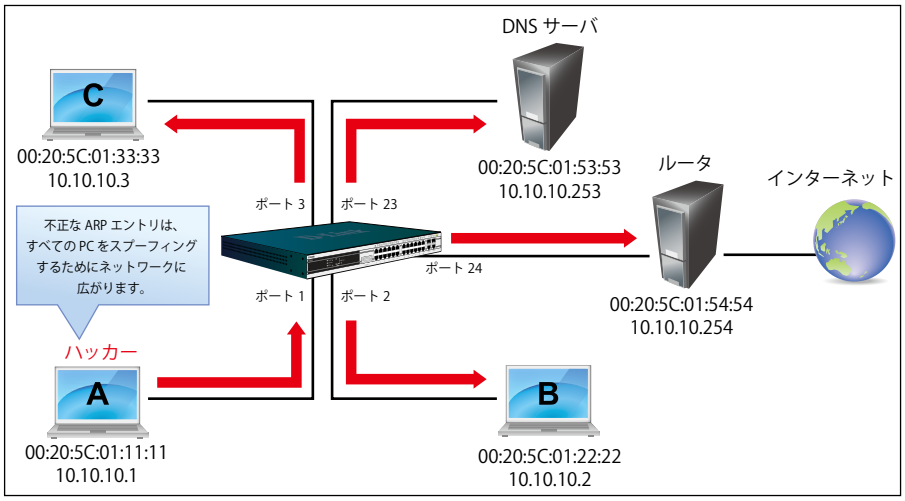


図 A-10　IP スプーフィング攻撃

Gratuitous ARP パケットでは、「送信側プロトコルアドレス」と「ターゲットプロトコルアドレス」は同じ送信元 IP アドレスとなります。「送信側 H/W アドレス」と「ターゲット H/W アドレス」は同じ送信元 MAC アドレスとなります。宛先の MAC アドレスは、イーサネットブロードキャストアドレス（FF-FF-FF-FF-FF-FF）となります。ネットワーク内のすべてのノードは、送信側の MAC アドレスおよび IP アドレスに従って、直ちに自身の ARP テーブルを更新します。Gratuitous ARP の書式は以下の表の通りです。

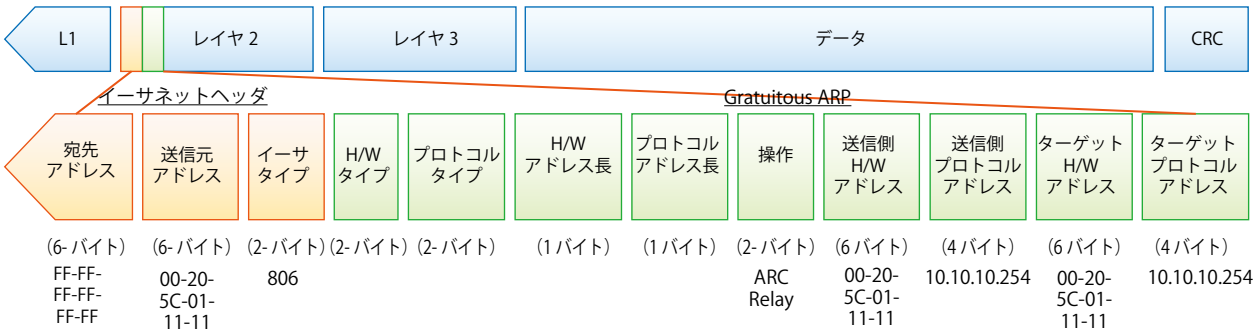


図 A-11　イーサネットフレームフォーマット

一般的な DoS 攻撃は、実在しない MAC アドレスやあらゆる指定 MAC アドレスをネットワークのデフォルトゲートウェイの IP アドレスに関連させることで行われます。悪意がある攻撃者は、1 つの Gratuitous ARP をゲートウェイであると言っているネットワークに対してブロードキャストする必要があるだけであり、これによりすべてのネットワーク操作は、インターネットへの全パケットが間違ったノードに向けられるためにダウンさせられてしまいます。

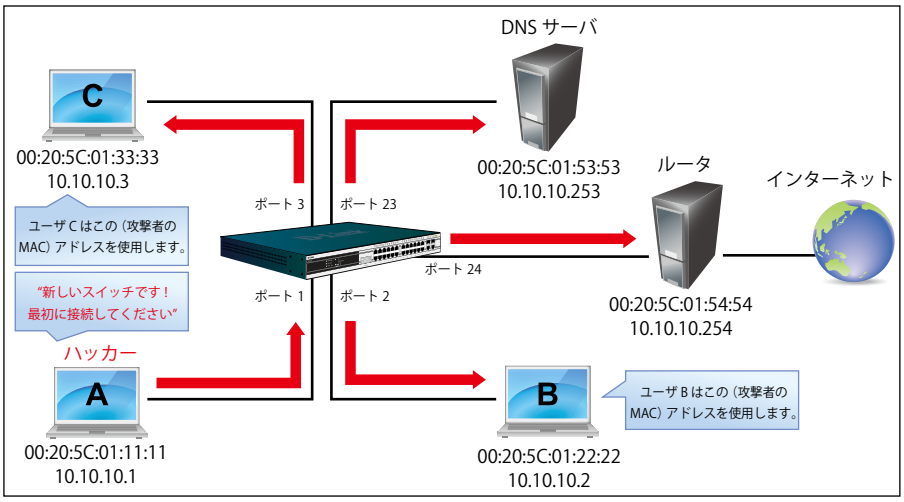


図 A-11　IP スプーフィング攻撃

同様に、攻撃者は、実際のデフォルトゲートウェイにトラフィックを転送する（パッシブスニッフィング）か、またはそれを転送する前にデータを更新する（man-in-the-middle 攻撃）を選択することが可能です。ハッカーは PC をだまし、犠牲者であるルータをだまします。図 A-11 で参照されるように、すべてのトラフィックはハッカーにスニッフィングされますが、ユーザはそれを発見できません。

パケットコンテンツ ACL 経由で ARP スプーフィング攻撃を防止する

D-Link マネージドスイッチは、独自のパケットコンテンツ ACL 経由で ARP スプーフィングが引き起こした一般的な DoS を効果的に軽減することができます。基本的な ACL は、パケットタイプ、VLAN ID、送信元および送信先 MAC 情報に基づいて ARP パケットをフィルタするだけであるため、より詳細な ARP パケットの検証が必要となります。

ARP スプーフィング攻撃を防ぐために、スイッチでパケットコンテンツ ACL を使用し、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。

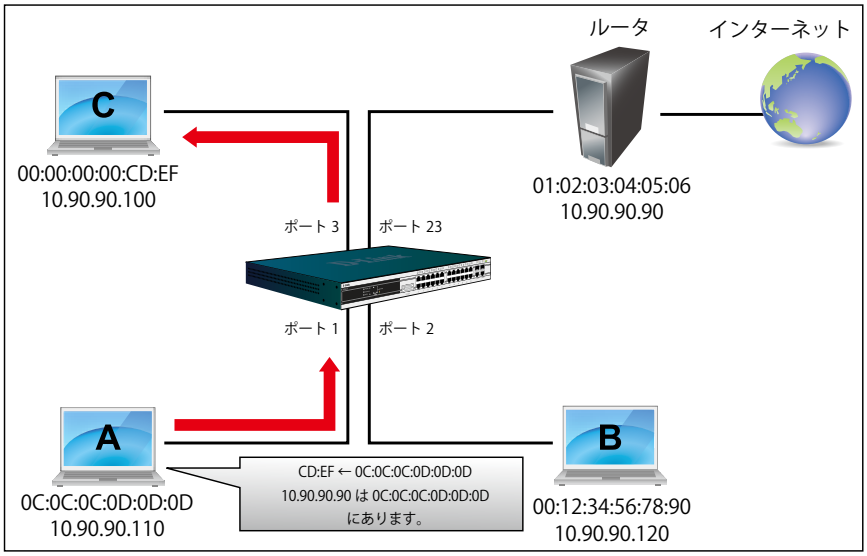


図 A-12　パケットコンテンツ ACL 経由の ARP スプーフィング防止

設定

設定のロジックは以下の通りです。

1. ARP がイーサネットにおける送信元 MAC アドレスに一致する場合にだけ、ARP プロトコルの送信者の MAC アドレスと送信者の IP アドレスはスイッチを通過することができます。（この例では、ゲートウェイの ARP です。）
2. スイッチはゲートウェイの IP アドレスから来ていると言う他のすべての ARP パケットを拒否します。

スイッチのパケットコンテンツ ACL の設計により、ユーザはどんなオフセットチャンクも検証することができます。オフセットチャンクは 16 進数形式の 4 バイトのブロックであり、イーサネットフレーム内の各項目に一致させるために利用されます。各プロファイルは、最大 4 つのオフセットチャンクを持つことができます。その上、パケットコンテンツ ACL に 1 個のプロファイルだけがスイッチごとサポートされます。つまり、最大 16 バイトのオフセットチャンクが各プロファイルとスイッチに適用されます。そのため、有効なオフセットチャンクの計画と設定が必要とされます。

表 A-1 で、Offset_Chunk0 が 127 バイト目から開始し、128 バイト目で終了することにご注意ください。されに、オフセットチャンクが 0 ではなく、1 から抽出されることがわかります。

表 A-1　チャンクとパケットオフセット

Offset Chunk	Offset Chunk0	Offset Chunk1	Offset Chunk2	Offset Chunk3	Offset Chunk4	Offset Chunk5	Offset Chunk6	Offset Chunk7	Offset Chunk8	Offset Chunk9	Offset Chunk10	Offset Chunk11	Offset Chunk12	Offset Chunk13	Offset Chunk14	Offset Chunk15
バイト	127	3	7	11	15	19	23	27	31	35	39	43	47	51	55	59
バイト	128	4	8	12	16	20	24	28	32	36	40	44	48	52	56	60
バイト	1	5	9	13	17	21	25	29	33	37	41	45	49	53	57	61
バイト	2	6	10	14	18	22	26	30	34	38	42	46	50	54	58	62

Offset Chunk	Offset Chunk15	Offset Chunk16	Offset Chunk17	Offset Chunk18	Offset Chunk19	Offset Chunk20	Offset Chunk21	Offset Chunk22	Offset Chunk23	Offset Chunk24	Offset Chunk25	Offset Chunk26	Offset Chunk27	Offset Chunk28	Offset Chunk29	Offset Chunk30
バイト	63	67	71	75	79	83	87	91	95	99	103	107	111	115	119	123
バイト	64	68	72	76	80	84	88	92	96	100	104	108	112	116	120	124
バイト	65	69	73	77	81	85	89	93	97	101	105	109	113	117	121	125
バイト	66	70	74	78	82	86	90	94	98	102	106	110	114	118	122	126

以下の表は、パケットオフセットの計算のためのパターンであるイーサネットフレームに含まれる完全な ARP パケットを示しています。

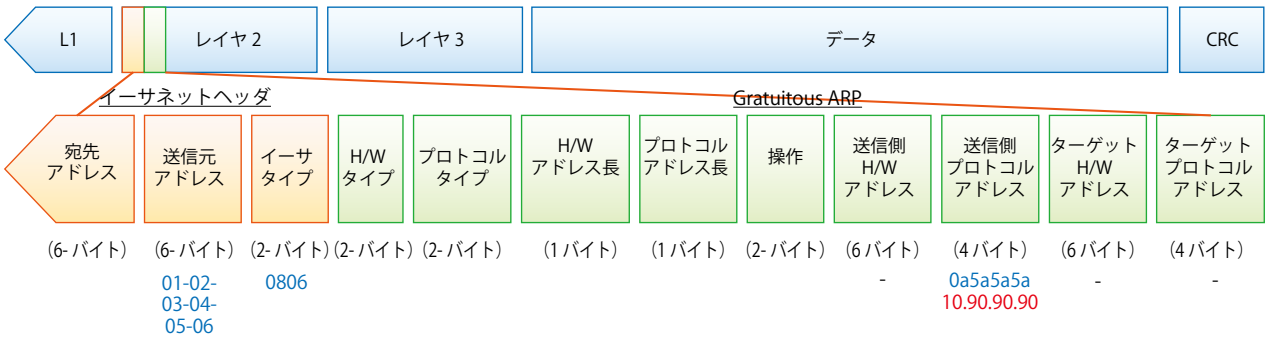


図 A-13　イーサネットフレームに含まれる完全な ARP パケット

	コマンド	記述
手順 1	create access_profile_id 1 ethernet source_mac FF-FF-FF-FF-FF-FF ethernet_type	• 「イーサネットタイプ」と「送信元 MAC アドレス」を一致させるアクセスプロファイル 1 を作成します。
手順 2	config access_profile profile_id 1 add access_id1 ethernet source_mac 01-02-03-04-04-06 ethernet_type 0x806 port 1-12 permit	• アクセスプロファイル 1 を設定します。 • ゲートウェイの ARP パケットがイーサネットフレームに正しい「送信元 MAC」を持っている場合だけスイッチを通過できます。
手順 3	create access_profile profile_id 2 profile_name 2 packet_content_mask offset_chunk_1 3 0xFFFF offset_chunk_2 7 0xFFFF offset_chunk_3 8 0xFFFF0000	• アクセスプロファイル 2 を作成します。 • ２つ目のチャンクは Chunk7 から開始します。 :「イーサネットタイプ」のマスク（表 A-1 : 13/14 バイト目の青色部分） • 1 つ目のチャンクは Chunk3 から開始します。 : ARP パケットの「Sender IP」（始め 2 バイト）のマスク（表 A-1 : 29/30 バイト目の緑色部分） • 1 つ目のチャンクは Chunk8 から開始します。 : ARP パケットの「Sender IP」（最後 2 バイト）のマスク（表 A-1 : 31/32 バイト目の茶色部分）
手順 4	config access_profile profile_id 2 add access_id 1 packet_content offset_chunk_1 0x806 offset_chunk_2 0xA5A offset_chunk_3 0x5A5A0000	• アクセスプロファイル 2 を設定します。 • 「Sender IP」がゲートウェイの IP であると言う残りの ARP パケットは廃棄されます。
手順 5	save	• 設定を保存します。

付録 B パスワードのリカバリ手順

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。「UART init」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「 ^ 」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                                          V1.00.001
--------------------------------------------------------------------------------

  Power On Self Test ....................................  100%

  MAC Address    : 01-01-02-03-04-05-00
  H/W Version    : A1

  Please Wait, Loading V1.00.029 Runtime Image ..............  100 %
  UART init .................................................  100 %
```

```
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 {force_agree}	リセットし、全設定を工場出荷時設定に戻します。オプション「force_agree」は、ユーザの同意なしで全コンフィグレーションをリセットすることを意味します。
reboot {force_agree}	「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。オプション「force_agree」は、ユーザの同意なしで全コンフィグレーションをリセットすることを意味します。
reset account	作成済みのアカウントのすべてを削除します。
reset password {< ユーザ名 >}	指定ユーザのパスワードをリセットします。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 C ログエントリ

スイッチのシステムログに表示される可能性のあるログエントリとそれらの意味を以下に示します。

Critical（重大）、Warning（警告）、Informational（報告）

カテゴリ	イベントの説明	ログの内容	緊急度	摘要
システム	システムスタート	System started up	Critical	
	システムのウォームスタート	System warm start	Critical	
	システムのコールドスタート	System cold start	Critical	
	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。	Configuration saved to flash by console (Username: < ユーザ名 >, IP: <IP アドレス >)	Informational	"console" と "IP: <IP アドレス >" は XOR（排他的論理和）です。これはコンソールでログインした場合、IP 情報は表示されません。
	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。	System log saved to flash by console (Username: < ユーザ名 > IP: <IP アドレス >)	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。	Configuration and log saved to flash by console(Username: < ユーザ名 > IP: <IP アドレス >)	Informational	
	内部電源が故障しました。	Internal Power failed	Critical	
	内部電源が故障から回復しました。	Internal Power is recovered	Critical	
	リダンダント電源異常	Redundant Power failed	Critical	
	リダンダント電源使用中	Redundant Power is working	Critical	
	側面のファンが故障しました。	Side Fan failed	Critical	
	側面のファンの故障から回復しました。	Side Fan recovered	Critical	
アップロード / ダウンロード	ファームウェアの更新成功。	Firmware upgraded by console successfully (Username: < ユーザ名 >, IP: <IP アドレス >)	Informational	"console" と "IP: <IP アドレス >" は XOR（排他的論理和）です。これはコンソールでログインした場合、IP 情報は表示されません。
	ファームウェアの更新失敗。	Firmware upgrade by console 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成功。	Configuration successfully downloaded by console (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失敗。	Configuration download by console 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成功。	Configuration successfully uploaded by console (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失敗。	Configuration upload by console 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成功。	Log message successfully uploaded by console (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失敗。	Log message upload by console was unsuccessful! (Username: < ユーザ名 >, IP: <IP アドレス >)	Warning	
	ファームウェアのアップロード成功。	Firmware successfully uploaded by console (Username: < ユーザ名 >, IP: <IP アドレス >)	Informational	
	ファームウェアのアップロード失敗。	Firmware upload by console was unsuccessful! (Username: < ユーザ名 >, IP: <IP アドレス >)	Warning	
インタフェース	ポートリンクアップ	Port < ポート番号 > link up, < リンク状態 >	Informational	ポートリンク状態（例 : 100Mbps 全二重）
	ポートリンクダウン	Port < ポート番号 > link down	Informational	
コンソール	コンソール経由のログイン成功	Successful login through Console (Username: < ユーザ名 >)	Informational	コンソール経由でログインをしている場合は、IP や MAC アドレス情報は表示されません。
	コンソール経由のログイン失敗	Login failed through Console (Username: < ユーザ名 >)	Warning	
	コンソール経由でログアウト	Logout through Console (Username: < ユーザ名 >)	Informational	
	コンソールセッション、タイムアウト	Console session timed out (Username: < ユーザ名 >)	Informational	

カテゴリ	イベントの説明	ログの内容	緊急度	摘要
Web	Web 経由のログイン成功	Successful login through Web (Username: < ユーザ名 >, IP: <IP アドレス >)	Informational	
	Web 経由のログイン失敗	Login failed through Web (Username: < ユーザ名 >, IP: <IP アドレス >)	Warning	
	Web 経由でログアウト	Logout through Web (Username: < ユーザ名 >, IP: <IP アドレス >)	Informational	
	Web セッションタイムアウト	Web session timed out (Username: < ユーザ名 >, IP:<IP アドレス >)	Informational	
	Web(SSL) 経由のログイン成功	Successful login through Web(SSL) (Username: < ユーザ名 >, IP: <IP アドレス >)	Informational	
	Web(SSL) 経由のログイン失敗	Login failed through Web(SSL) (Username: < ユーザ名 >, IP: <IP アドレス >)	Warning	
	Web(SSL) 経由でログアウト	Logout through Web(SSL) (Username: < ユーザ名 >, IP: <IP アドレス >)	Informational	
	Web(SSL) セッションタイムアウト	Web(SSL) session timed out (Username: < ユーザ名 >, IP:<IP アドレス >)	Informational	
Telnet	Telnet 経由のログイン成功	Successful login through Telnet (Username: < ユーザ名 >, IP: <IP アドレス >)	Informational	
	Telnet 経由のログイン失敗	Login failed through Telnet (Username: < ユーザ名 >, IP: <IP アドレス >)	Warning	
	Telnet 経由でログアウト	Logout through Telnet (Username: < ユーザ名 >, IP: <IP アドレス >)	Informational	
	Telnet セッションタイムアウト	Telnet session timed out (Username: < ユーザ名 >, IP: <IP アドレス >)	Informational	
SNMP	無効なコミュニティ名を含む SNMP request 受信	SNMP request received from < IP アドレス > with invalid community string !	Informational	
STP	トポロジ変更	Topology changed (Instance:< インスタンス ID> port< ポート番号 >)	notice	
	新規ルートを選択	[CIST | CIST Regional | MSTI Regional] New Root bridge selected([Instance: < インスタンス ID>]MAC: <MAC アドレス > Priority :< プライオリティ値 >)	Informational	
	スパニングツリープロトコル有効化	Spanning Tree Protocol is enabled	Informational	
	スパニングツリープロトコル無効化	Spanning Tree Protocol is disabled	Informational	
	新規ルートポートを選択	New root port selected (Instance:< インスタンス >, Port:< ポート番号 >)	notice	
	スパニングツリーポート状態の変更	Spanning Tree port status changed (Instance:< インスタンス >, Port:< ポート番号 >) <old_status> -> < 新しい状態 >	notice	
	スパニングツリーポートのロール変更	Spanning Tree port role changed (Instance:< インスタンス >, Port:< ポート番号 >) <old_role> -> < 新規ロール >	Informational	
	スパニングツリーインスタンスの作成	Spanning Tree instance created (Instance:< インスタンス ID>)	Informational	
	スパニングツリーインスタンスの削除	Spanning Tree instance deleted (Instance:< インスタンス ID>)	Informational	
	スパニングツリーバージョンの変更	Spanning Tree version changed (new version:< 新バージョン >)	Informational	
	スパニングツリー MST コンフィグレーション ID 名とリビジョンレベルの変更	Spanning Tree MST configuration ID name and revision level changed (name:< 名前 > ,revision level < リビジョンレベル >)	Informational	
	スパニングツリー MST コンフィグレーション ID が VLAN マッピングテーブルから削除	Spanning Tree MST configuration ID VLAN mapping table changed (instance: < インスタンス ID> delete vlan < 開始 VLANID> [- < 終了 VLANID>])	Informational	
	スパニングツリー MST コンフィグレーション ID が VLAN マッピングテーブルに追加	Spanning Tree MST configuration ID VLAN mapping table changed (instance: < インスタンス ID> add vlan < 開始 VLANID> [- < 終了 VLANID>])	Informational	

カテゴリ	イベントの説明	ログの内容	緊急度	摘要
DoS	スプーフィング攻撃 **1.** 送信元 IP は、送信元 MAC アドレスが異なるのにもかかわらず、スイッチのインタフェース IP と同じです。 **2.** 送信元 IP が ARP パケット内のスイッチの IP と同じです。 **3.** 自身の IP パケットが検出されました。	Possible spoofing attack from (IP: <IP アドレス > MAC: <MAC アドレス > Port: < ポート番号 >)	Critical	
SSH	SSH 経由のログイン成功	Successful login through SSH (Username: < ユーザ名 >, IP: <IP アドレス >)	Informational	
	SSH 経由のログイン失敗	Login failed through SSH (Username: < ユーザ名 >, IP: <IP アドレス >)	Warning	
	SSH 経由のログアウト	Logout through SSH (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 session timed out (Username: < ユーザ名 >, IP: <IP アドレス >)	Informational	
	SSH サーバ有効化	SSH server is enabled	Informational	
	SSH サーバ無効化	SSH server is disabled	Informational	
AAA	認証ポリシー有効化	Authentication Policy is enabled (Module: AAA)	Informational	
	認証ポリシー無効化	Authentication Policy is disabled (Module: AAA)	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	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失敗	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 Web 経由のログイン認証成功	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失敗	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 (SSL) 経由のログイン認証成功	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失敗	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 Telnet 経由のログイン認証成功	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失敗	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 SSH 経由のログイン認証成功	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失敗	Login failed through SSH from < ユーザ IP> authenticated by AAA local method (Username: < ユーザ名 >)	Warning	
	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 Console 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 from < ユーザ IP> authenticated by AAA none method (Username: < ユーザ名 >)	Informational	

カテゴリ	イベントの説明	ログの内容	緊急度	摘要
AAA	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 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 Telnet 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 SSH 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 サーバによるコンソール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	コンソール経由でログインをしている場合は、IP や MAC アドレス情報は表示されません。
	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 authenticated by AAA server< サーバ IP> (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	Login failed through Console due to AAA server timeout or improper configuration (Username: < ユーザ名 >)	Warning	
	AAA サーバによる Web 経由のログイン認証成功	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失敗	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	Login failed through Web from < ユーザ IP> due to AAA server timeout or improper configuration (Username: < ユーザ名 >)	Warning	
	AAA サーバによる Web (SSL) 経由のログイン認証成功	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失敗	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	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 サーバによる Telnet 経由のログイン認証成功	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失敗	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	Login failed through Telnet from < ユーザ IP> due to AAA server timeout or improper configuration (Username: < ユーザ名 >)	Warning	
	AAA サーバによる SSH 経由のログイン認証成功	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失敗	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	Login failed through SSH from < ユーザ IP> due to AAA server timeout or improper configuration (Username: < ユーザ名 >)	Warning	
	AAA local_enable メソッド認証によるコンソール経由の Admin レベル遷移成功	Successful Enable Admin through Console authenticated by AAA local_enable method (Username: < ユーザ名 >)	Informational	
	AAA local_enable メソッド認証によるコンソール経由の Admin レベル遷移失敗	Enable Admin failed through Console authenticated by AAA local_enable method (Username: < ユーザ名 >)	Warning	
	AAA local_enable メソッド認証による Web 経由の Admin レベル遷移成功	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 メソッド認証による Web 経由の Admin レベル遷移失敗	Enable Admin failed through Web from < ユ ー ザ IP> authenticated by AAA local_enable method (Username: < ユーザ名 >)	Warning	

カテゴリ	イベントの説明	ログの内容	緊急度	摘要
AAA	AAA local_enable メソッド認証による Web(SSL) 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 local_enable method (Username: < ユーザ名 >)	Informational	
	AAA local_enable メソッド認証による Web(SSL) 経由の Admin レベル遷移失敗	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 メソッド認証による Telnet 経由の Admin レベル遷移成功	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 メソッド認証による Telnet 経由の Admin レベル遷移失敗	Enable Admin failed through Telnet from < ユーザ IP> authenticated by AAA local_enable method (Username: < ユーザ名 >)	Warning	
	AAA local_enable メソッド認証による SSH 経由の Admin レベル遷移成功	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 メソッド認証による SSH 経由の Admin レベル遷移失敗	Enable Admin failed through <Telnet、Web または SSH> from < ユーザ IP> authenticated by AAA local_enable method (Username: < ユーザ名 >)	Warning	
	AAA none メソッド認証によるコンソール経由の Admin レベル遷移成功	Successful Enable Admin through Console authenticated by AAA none method (Username: < ユーザ名 >)	Informational	
	AAA none メソッド認証による Web 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 メソッド認証による Web(SSL) 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 メソッド認証による Telnet 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 メソッド認証による SSH 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 サーバの認証によるコンソール経由の 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 サーバの認証によるコンソール経由の Admin レベル遷移失敗	Enable Admin failed through Console authenticated by AAA server < サーバ IP> (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	Enable Admin failed through Console due to AAA server timeout or improper configuration (Username: < ユーザ名 >)	Warning	
	AAA サーバによる Web 経由の Admin レベル遷移成功	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 レベル遷移失敗	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	Enable Admin failed through Web due to AAA server timeout or improper configuration (Username: < ユーザ名 >)	Warning	
	AAA サーバによる Web(SSL) 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 server < サーバ IP> (Username: < ユーザ名 >)	Informational	
	AAA サーバによる Web(SSL) 経由の Admin レベル遷移失敗	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	

カテゴリ	イベントの説明	ログの内容	緊急度	摘要
AAA	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 Admin レベル遷移失敗	Enable Admin failed through Web(SSL) due to AAA server timeout or improper configuration (Username: < ユーザ名 >)	Warning	
	AAA サーバによる Telnet 経由の Admin レベル遷移成功	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 レベル遷移失敗	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	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 サーバによる SSH 経由の Admin レベル遷移成功	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 レベル遷移失敗	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	Enable Admin failed through SSH from < ユーザ IP> due to AAA server timeout or improper configuration (Username: < ユーザ名 >)	Warning	
ポートセキュリティ	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。	Port security violation (MAC address:<MAC アドレス > on port:< ポート番号 >)	Warning	
MBAC	ホストは認証通過に失敗しました。	MAC-based Access Control unauthenticated host (MAC: <MAC アドレス >, Port < ポート番号 >, VID: <VID>)	Information	
	ポートにおける認可ユーザ数が最大ユーザの制限に到達しました。	Port < ポート番号 > enters MAC-based Access Control stop learning state	Warning	各ポート
	ポートにおける認可ユーザ数が時間内の最大ユーザの制限に到達しました。	Port < ポート番号 > recovers from MAC-based Access Control stop learning state	Warning	各ポート
	デバイス全体の認可ユーザ数が最大ユーザの制限に到達しました。	MAC-based Access Control enters stop learning state	Warning	各システム
	デバイス全体の認可ユーザ数が時間内の最大ユーザの制限に到達しました。	MAC-based Access Control recovers from stop learning state	Warning	各システム
	ホストは認証に成功しました。	MAC-based Access Control host login successful (MAC: <MAC アドレス >, port: < ポート番号 >, VID: <VLAN ID>)	Information	
	ホストはエージングされました。	MAC-based Access Control host aged out (MAC: <MAC アドレス >, port: < ポート番号 >, VID: <VLAN ID>)	Information	

カテゴリ	イベントの説明	ログの内容	緊急度	摘要
IP-MAC ポートバインディング	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。	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	
	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 ARP(IP: <IP アドレス >, MAC: <MAC アドレス >, Port: < 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 FDB(IP: <IP アドレス >, MAC: <MAC アドレス >, Port: < 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。	Dynamic IMPB entry is conflicting with static IMPB: 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。	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	
IP とパスワード変更	IP アドレスが変更されました。	Management IP address was changed by (Username: < ユーザ名 >,IP:<IP アドレス >)	Informational	"console" と "IP: <IP アドレス >" は XOR（排他的論理和）です。これはコンソールでログインした場合、IP 情報は表示されません。
	パスワードが変更されました。	Password was changed by (Username: < ユーザ名 >,IP:<IP アドレス >)	Informational	
セーフガードエンジン	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 NORMAL mode	Informational	
	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。	Safeguard Engine enters EXHAUSTED mode	Warning	
パケットストーム	ブロードキャストストーム発生中。	Port < ポート番号 > Broadcast storm is occurring	Warning	
	ブロードキャストストーム停止。	Port < ポート番号 > Broadcast storm has cleared	Informational	
	マルチキャストストーム発生中。	Port < ポート番号 > Multicast storm is occurring	Warning	
	マルチキャストストーム停止。	Port < ポート番号 > Multicast storm has cleared	Informational	
	パケットストームのためにポートはシャットダウン。	Port < ポート番号 > is currently shut down due to a packet storm	Warning	
ループバック検知	ポートでループが発生	Port < ポート番号 > LBD loop occurred. Port blocked	Critical	
	ポートでループが発生し、タイプアウト後にポートループ検知は再起動しました。	Port < ポート番号 > LBD port recovered. Loop detection restarted	Informational	
	ポートで VID ループが発生。	Port < ポート番号 > VID <VLAN ID> LBD loop occurred. Packet discard begun	Critical	
	ポートで VID ループが発生し、タイプアウト後にポートループ検知は再起動しました。	Port < ポート番号 > VID <VLAN ID> LBD recovered. Loop detection restarted	Informational	
	ループバックが発生した VLAN 数が指定数に到達しました。	Loop VLAN number overflow	Informational	
Gratuitous ARP	Gratuitous ARP は重複 IP アドレスを検出しました。	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	
DHCP	信頼性の低い DHCP サーバの IP アドレスを検出。	Detected untrusted DHCP server(IP: <IP アドレス >, Port: < ポート番号 >)	Informational	

カテゴリ	イベントの説明	ログの内容	緊急度	摘要
BPDU 保護	BPDU アタックが発生	Port < ポート番号 > enter BPDU under attacking state (mode: drop / block / shutdown)	Informational	
	BPDU アタックは自動的に回復	Port < ポート番号 > recover from BPDU under attacking state automatically	Informational	
	BPDU アタックは手動で回復	Port < ポート番号 > recover from BPDU under attacking state manually	Informational	
モニタ	温度が信頼レベルを超えています。	Temperature Sensor < センサー ID> enter alarm state. (current temperature: < 温度 >)	Warning	
	温度が通常の値に戻りました。	Temperature Sensor < センサー ID> recovers to normal state. (current temperature: < 温度 >)	Informational	
CFM	クロスコネクトを検出	CFM cross-connect. VLAN:<VLAN ID>, Local (MD Level:<MD レベル >, Port < ポート番号 >, Direction: <MEP ディレクション >) Remote (MEPID:<MEP ID>, MAC: <MAC アドレス >)	Critical	
	エラー CFM CCM パケットを検出	CFM error ccm. MD Level:<MD レベル >, VLAN:<VLAN ID>, Local(Port < ポート番号 >, Direction:<MEP ディレクション >) Remote(MEPID:<mepid>, MAC:<MAC アドレス >)	Warning	
	リモート MEP の CCM パケットを受信できません	CFM remote down. MD Level:<MD レベル >, VLAN:<VLAN ID>, Local (Port < ポート番号 >, Direction:<MEP ディレクション >)	Warning	
	リモート MEP の MAC がエラー状態をレポートしています。	CFM remote MAC error. MD Level:<MD レベル >, VLAN:<VLAN ID>, Local (Port < ポート番号 >, Direction:<MEP ディレクション >)	Warning	
	リモートの MEP が CFM の欠陥を検出しました。	CFM remote detects a defect. MD Level:<MD レベル >, VLAN:<VLAN ID>, Local (Port < ポート番号 >, Direction:<MEP ディレクション >)	Informational	
CFM 拡張	AIS 状態を検出	AIS condition detected. MD Level:<mdlevel>, VLAN:<VLAN ID>, Local(Port < ポート番号 >, Direction:<MEP ディレクション >, MEPID:<mepid>)	Notice	
	AIS 状態が解消	AIS condition cleared. MD Level:<mdlevel>, VLAN:<VLAN ID>, Local(Port < ポート番号 >, Direction:<MEP ディレクション >, MEPID:<mepid>)	Notice	
	LCK 状態を検出	LCK condition detected. MD Level:<mdlevel>, VLAN:<VLAN ID>, Local(Port < ポート番号 >, Direction:<MEP ディレクション >, MEPID:<mepid>)	Notice	
	LCK 状態が解消	LCK condition cleared. MD Level:<mdlevel>, VLAN:<VLAN ID>, Local(Port < ポート番号 >, Direction:<MEP ディレクション >, MEPID:<mepid>)	Notice	
音声 VLAN	新しい音声 VLAN をポートに検出	New voice device detected (MAC:<MAC アドレス >,Port: ポート番号 >)	Informational	
	自動音声 VLAN モードのポートを音声 VLAN に追加しました。	Port < ポート番号 > add into voice VLAN <VLAN ID>	Informational	
	ポートが音声 VLAN から離脱し、同時にそのポートのエージングタイム内に音声 VLAN が見つからないとログメッセージを送信します。	Port < ポート番号 > remove from voice VLAN <VLAN ID>	Informational	
ERPS	エラー信号を検出	Signal failure detected on node <MAC アドレス >	Notice	
	エラー信号のクリア	Signal failure cleared on node <MAC アドレス >	Notice	
	RPL オーナの重複	RPL owner conflicted on the ring <MAC アドレス >	Warning	
コマンドログ出力	コマンドログ	< ユーザ名 >: execute command "< 文字列 >".	Informational	

カテゴリ	イベントの説明	ログの内容	緊急度	摘要
無線状態	無線スイッチの有効化	Wireless switch enabled	Informational	
	無線スイッチの無効化	Wireless switch disabled	Informational	
	管理下にあるローカルなアクセスポイントの制限を超えました。	Wireless Local Managed AP Exceeded MAC: <MAC アドレス >	Warning	
	無線 AP のハードウェアタイプをサポートしていません。	Wireless AP Hardware Type Failure MAC: <MAC アドレス > Hardware Type: <int>	Warning	
テーブルフル	管理下にある無線 AP のデータベースがいっぱいです。	Wireless managed AP database full AP MAC: <MAC アドレス > dropped	Warning	
	管理下にある無線 AP- AP Neighbor リストがいっぱいです。	Wireless managed AP-AP neighbor list full	Warning	
	管理下にある無線 AP- クライアントのリストがいっぱいです。	Wireless managed AP-Client neighbor list full	Warning	
	無線 AP エラーリストがいっぱいです。	Wireless AP failure list full	Warning	
	無線 RF スキャン AP リストがいっぱいです。	Wireless RF scan AP list full	Warning	
	無線クライアントアソシエーションデータベースがいっぱいです。	Wireless client association database full client MAC: <MAC アドレス > dropped	Warning	
	無線 Ad Hoc クライアントのリストがいっぱいです。	Wireless Ad Hoc client list full	Warning	
	無線ピアの管理下にある AP データベースがいっぱいです。	Wireless peer switch <IP アドレス > managed AP database full AP MAC: <MAC アドレス > dropped	Warning	
	Wireless peer Switch client 無線ピアスイッチのクライアントデータベースがいっぱいです。	Wireless peer switch <IP アドレス > client database full client MAC: <MAC アドレス > dropped	Warning	
ピアスイッチ	無線ピアスイッチを検出しました。	Wireless peer switch: <ipaddr> discovered	Informational	
	無線ピアスイッチエラー。	Wireless peer switch: <ipaddr> failed	Warning	
	無線ピアスイッチのプロトコルバージョンが不明です。	Wireless peer switch: <ipaddr> protocol version: < バージョン > unknown	Warning	
	無線ピアスイッチの管 Managed AP データベースの制限を超えました。	Wireless peer switch <ipaddr> managed AP database full AP MAC: <MAC アドレス > dropped	Warning	
Managed AP	管理下にある AP を検出しました。	Wireless managed AP MAC: <MAC アドレス > discovered	Informational	
	管理下にある AP のエラー。	Wireless managed AP MAC: <MAC アドレス > failed	Warning	
	管理下にある AP のプロトコルバージョンが不明です。	Wireless managed AP MAC: <MAC アドレス > protocol version:<string> unknown	Warning	
	管理下にある AP のアソシエーションエラー。	Wireless managed AP MAC: <MAC アドレス > Association failed	Warning	
	理下にある AP の認証エラー。	Wireless managed AP MAC: <MACアドレス> Authentication failed	Warning	

カテゴリ	イベントの説明	ログの内容	緊急度	摘要
RF スキャン	RF スキャンで不正な AP を検出しました。	Wireless RF scan rogue-AP MAC: <MAC アドレス > AP MAC: <MAC アドレス > Radio If: <int> SSID: <SSID> detected	Informational	
	RF スキャンで新しく Neighbor AP を検出しました。	Wireless RF scan new Neighbor AP MAC: <MAC アドレス > AP MAC: <MAC アドレス > Radio If: <int> SSID: <SSID> detected	Informational	
	RF スキャンで新しくクライアントを検出しました。	Wireless RF scan new Client MAC: <MAC アドレス > AP MAC: <MAC アドレス > Radio If: <int> detected	Informational	
	無線クライアントの接続を検出しました。	Wireless Client Association MAC: <MAC アドレス > VAP MAC: <MAC アドレス > AP MAC: <MAC アドレス > SSID: <SSID> Security Mode: < 文字列 > detected	Informational	
	無線クライアントの接続解除を検出しました。	Wireless Client Disassociation MAC: <MAC アドレス > VAP MAC: <MAC アドレス >AP MAC: <MAC アドレス > detected	Informational	
	無線クライアントのローミングを検出しました。	Wireless Client Roam MAC: <MAC アドレス > VAP MAC: <MAC アドレス > AP MAC: <MAC アドレス >detected	Informational	
	無線クライアントの接続エラーを検出しました。	Wireless Client MAC: <MAC アドレス > Association Failure detected	Warning	
	無線クライアントの認証エラーを検出しました。	Wireless Client MAC: <MAC アドレス > Authentication Failure detected	Warning	
	RF スキャンで新しく Ad-Hoc クライアントを検出しました。	Wireless RF scan new Ad-Hoc Client MAC: <MAC アドレス > AP MAC: <MAC アドレス > Radio If: <int> detected	Informational	
ロードバランシング	無線のロードバランシングの利用のオーバフロー	Wireless load balancing utilization overflow: AP MAC: <MAC アドレス > Radio If: <int> Radio MAC: <MAC アドレス > Utilization: <int>	Warning	
コンフィグレーションのプッシュ	無線ピアスイッチの「config push 」コマンドを受信しました。	Wireless peer switch config push command with mask <int> from switch: <IP アドレス > received	Informational	
WIDS	ローカルスイッチが WIDS コントローラに選定されました。	Local Switch is elected as WIDS Controller	Informational	
	無線ネットワークの管理対象 AP が WIDS コントローラの最大数を超えました。	Wireless Network Managed AP Max AP exceeded on WIDS Controller <IP アドレス > when AP MAC: <MAC アドレス > with IP address <IP アドレス > connected to Wireless Switch <IP アドレス >	Warning	
	不正な AP(s) がネットワークに存在します。	Wireless rogue-AP(s) present in the network	Informational	
	無線クライアントの検出リストがいっぱいになりました。	Wireless Detected client list full	Warning	
	不正なクライアント (s) がネットワークに存在します。	Wireless rogue-Client(s) present in the network	Informational	
自動チャンネル & 電力	無線チャンネルアルゴリズムの完了。	Wireless Channel Algorithm is complete	Informational	
	無線チ電力アルゴリズムの完了。	Wireless Power Algorithm is complete	Informational	
キャプティブポータル	CP クライアントを接続しました。	CP Client Connected: MAC: <MAC アドレス > IP: <ipaddr> SwMAC: <MAC アドレス > CPID: <int> Interface: <int>	Informational	
	CP クライアントを切断しました。	CP Client Disconnected: MAC: <MAC アドレス > IP: <ipaddr> SwMAC: <MAC アドレス > CPID: <int> Interface: <int>	Informational	
	CP クライアントの認証エラー。	CP Client Auth Failure: MAC: <MAC アドレス > IP: <ipaddr> SwMAC: <MAC アドレス > CPID: <int> Interface: <int> User: <username>	Warning	
	CP クライアント認証データベースがいっぱいになりました。	CP Client Authentication Database Full	Informational	

付録 D トラップログ

本製品では、以下のトラップログが検出されます。

トラップ名	説明	OID
swL2macNotification	アドレステーブル内の MAC アドレスの変化を示します。	1.3.6.1.4.1.171.11.101.1.2.100.1.2.0.1
swL2PortSecurityViolationTrap	ポートセキュリティトラップが有効な場合、定義済みのポートセキュリティ設定に違反する新しい MAC アドレスがあると、トラップメッセージを送信します。	1.3.6.1.4.1.171.11.101.1.2.100.1.2.0.2
PortLoopOccurred	ポートにループが発生すると、本トラップを送信します。	1.3.6.1.4.1.171.12.41.10.0.1
PortLoopRestart	ポートにループが一定間隔後に再度発生すると、本トラップを送信します。	1.3.6.1.4.1.171.12.41.10.0.2
VlanLoopOccurred	VLAN に所属するポートにループが発生すると、本トラップを送信します。	1.3.6.1.4.1.171.12.41.10.0.3
VlanLoopRestart	VLAN に所属するポートにループが一定間隔後に再度発生すると、本トラップを送信します。	1.3.6.1.4.1.171.12.41.10.0.4
SafeGuardChgToExhausted	システムが「normal」から「exhausted」に操作モードを変更したことを示します。	1.3.6.1.4.1.171.12.19.4.1.0.1
SafeGuardChgToNormal	システムが「exhausted」から「normal」に操作モードを変更したことを示します。	1.3.6.1.4.1.171.12.19.4.1.0.2
MacBasedAuthLoggedSuccess	MAC ベースアクセスコントロールホストがログインに成功した場合、本トラップを送信します。	1.3.6.1.4.1.171.12.35.11.1.0.1
MacBasedAuthLoggedFail	MAC ベースアクセスコントロールホストがログインに失敗した場合、本トラップを送信します。	1.3.6.1.4.1.171.12.35.11.1.0.2
MacBasedAuthAgesOut	MAC ベースアクセスコントロールホストがエージングを行った場合、本トラップを送信します。	1.3.6.1.4.1.171.12.35.11.1.0.3
FilterDetectedTrap	不正な DHCP サーバが検出された時、送信されます。ログが認証を止めている期間は、同じ不正な DHCP サーバの IP アドレスが検出されても、送信されるのは一度のみです。	1.3.6.1.4.1.171.12.37.100.0.1
SingleIPMSColdStart	Comander スイッチは、メンバがコールドスタート通知を生成する場合に指定ホストに swSingleIPMSColdStart 通知を送信します。	1.3.6.1.4.1.171.12.8.6.0.11
SingleIPMSWarmStart	Comander スイッチは、メンバがウォームスタート通知を生成する場合に指定ホストに swSingleIPMSWarmStart 通知を送信します。	1.3.6.1.4.1.171.12.8.6.0.12
swSingleIPMSLinkDown	Commander スイッチは、メンバがリンクダウン通知を生成する場合に指定ホストに swSingleIPMSLinkDown 通知を送信します。	1.3.6.1.4.1.171.12.8.6.0.13
swSingleIPMSLinkUp	Commander スイッチは、メンバがリンクアップ通知を生成する場合に指定ホストに swSingleIPMSLinkUp 通知を送信します。	1.3.6.1.4.1.171.12.8.6.0.14
swSingleIPMSAuthFail	Commander スイッチは、メンバが認証エラー通知を生成する場合に指定ホストに swSingleIPMSAuthFail 通知を送信します。	1.3.6.1.4.1.171.12.8.6.0.15
swSingleIPMSnewRoot	Commander スイッチは、メンバが新しいルート通知を生成する場合に指定ホストに swSingleIPMSnewRoot 通知を送信します。	1.3.6.1.4.1.171.12.8.6.0.16
swSingleIPMSTopologyChange	Commander スイッチは、メンバがトポロジの変更通知を生成する場合に指定ホストに swSingleIPMSTopologyChange 通知を送信します。	1.3.6.1.4.1.171.12.8.6.0.17
coldStart	coldStart トラップは、送信側のプロトコルエンティティがエージェントの設定またはプロトコルエンティティの実行を変更するように再初期化することを意味します。	1.3.6.1.6.3.1.1.5.1
warmStart	warmStart トラップは、送信側のプロトコルエンティティがエージェントの設定またはプロトコルエンティティのどちらの実行も変更しないように再初期化することを意味します。	1.3.6.1.6.3.1.1.5.2
linkDown	linkDown トラップは、送信側のプロトコルエンティティがエージェントの設定内にある通信リンクの 1 つに発生したエラーを認識したことを意味します。	1.3.6.1.6.3.1.1.5.3
linkUp	linkUp トラップは、送信側のプロトコルエンティティがエージェントの設定内にある通信リンクの 1 つのリンクアップを認識したことを意味します。 authenticationFailure トラップは、送信側のプロトコルエンティティが適切に認証されていないプロトコルメッセージのアドレスであることを意味します。	1.3.6.1.6.3.1.1.5.4

トラップ名	説明	OID
authenticationFailure	SNMPv2 の実行が本トラップを生成する必要がある間、実行用の特定のメカニズム経由でそのようなトラップの送信を抑制できる必要があります。 本トラップは、高性能のアラームエントリがしきい値の上限を超えて、SNMP トラップを送信するために設定されているイベントを生成する場合に生成される SNMP 通知です。	1.3.6.1.6.3.1.1.5.5
risingAlarm	本トラップは SNMP トラップ送信で設定されたしきい値の上限を超えるイベントが発生した時に、高レベルの容量警告として SNMP 通知されます。	1.3.6.1.2.1.16.29.2.0.1
fallingAlarm	本トラップは SNMP トラップ送信で設定されたしきい値の下限を超えるイベントが発生した時に、高レベルの容量警告として SNMP 通知されます。	1.3.6.1.2.1.16.29.2.0.2
newRoot	トラップは、新しいルートとしての選定後すぐにブリッジによって送信され、その選定に続いてすぐに Topology Change Timer のアクションの起動などを行います。本トラップの実行はオプションです。	1.3.6.1.2.1.17.0.1
topologyChange	topologyChange トラップは、構成するいずれかのポートが Learning 状態から Forwarding 状態に、Forwarding 状態から Blocking 状態に、または Forwarding 状態から Blocking 状態に遷移する場合にブリッジによって送信されます。本トラップは、newRoot トラップが同様の変更に対して送信される場合には送信されません。本トラップの実行はオプションです。	1.3.6.1.2.1.17.0.2
wsModeEnabled	wsModeEnabled トラップは、エージェントロールで動作する SNMP エンティティがデバイスの無線機能が有効となったことを検出したことを示します。	1.3.6.1.4.1.171.12.96.11.0.1
wsModeDisabled	A wsModeDisabled トラップは、エージェントロールで動作する SNMP エンティティがデバイスの無線機能が無効となったことを検出したことを示します。	1.3.6.1.4.1.171.12.96.11.0.2
wsManagedAPDatabaseFull	wsAPDatabaseFull トラップは、エージェントロールで動作する SNMP エンティティが AP データベースのフルを検出したことを示します。	1.3.6.1.4.1.171.12.96.11.0.3
wsManagedAPNeighborAPListFull	wsManagedAPNeighborAPListFull トラップは、エージェントロールで動作する SNMP エンティティが Managed AP Neighbor AP リストのフルを検出したことを示します。	1.3.6.1.4.1.171.12.96.11.0.4
wsManagedAPNeighborClientListFull	wsManagedAPNeighborClientListFull トラップは、エージェントロールで動作する SNMP エンティティが Managed AP Neighbor クライアントリストのフルを検出したことを示します。	1.3.6.1.4.1.171.12.96.11.0.5
wsAPFailureListFull	wsAPFailureListFull トラップは、エージェントロールで動作する SNMP エンティティが AP エラーリストのフルを検出したことを示します。	1.3.6.1.4.1.171.12.96.11.0.6
wsRFScanAPListFull	wsRFScanAPListFull トラップは、エージェントロールで動作する SNMP エンティティが RF スキャン AP リストのフルを検出したことを示します。	1.3.6.1.4.1.171.12.96.11.0.7
wsClientAssociationDatabaseFull	wsClientAssociationDatabaseFull トラップは、エージェントロールで動作する SNMP エンティティがクライアントアソシエーションデータベースのフルを検出したことを示します。	1.3.6.1.4.1.171.12.96.11.0.8
wsPeerSwitchDiscovered	wsPeerSwitchDiscovered トラップは、エージェントロールで動作する SNMP エンティティがネットワークにピアスイッチを検出したことを示します。	1.3.6.1.4.1.171.12.96.11.0.9
wsPeerSwitchFailed	wsPeerSwitchFailed トラップは、エージェントロールで動作する SNMP エンティティがピアスイッチの接続エラーを検出したことを示します。	1.3.6.1.4.1.171.12.96.11.0.10
wsPeerSwitchUnknownProtocol	wsPeerSwitchUnknownProtocol トラップは、エージェントロールで動作する SNMP エンティティが無線スイッチとピアスイッチの通信で不明なプロトコルを検出したことを示します。	1.3.6.1.4.1.171.12.96.11.0.11
wsManagedAPDiscovered	wsManagedAPDiscovered トラップは、エージェントロールで動作する SNMP エンティティが Managed AP を検出したことを示します。	1.3.6.1.4.1.171.12.96.11.0.12
wsManagedAPFailed	wsManagedAPFailed トラップは、エージェントロールで動作する SNMP エンティティが Failed AP を検出したことを示します。	1.3.6.1.4.1.171.12.96.11.0.13

トラップ名	説明	OID
wsManagedAPUnknownProtocol	wsManagedAPUnknownProtocol トラップは、エージェントロールで動作する SNMP エンティティが無線スイッチと Managed AP 間の通信で不明なプロトコルを検出したことを示します。	1.3.6.1.4.1.171.12.96.11.0.14
wsAPAssociationFailure	wsAPAssociationFailure トラップは、エージェントロールで動作する SNMP エンティティが AP アソシエーションエラーを検出したことを示します。	1.3.6.1.4.1.171.12.96.11.0.15
wsAPAuthenticationFailure	wsAPAuthenticationFailure トラップは、エージェントロールで動作する SNMP エンティティが AP 認証エラーを検出したことを示します。	1.3.6.1.4.1.171.12.96.11.0.16
wsRFScanRogueAPDetected	wsRFScanRogueAPDetected トラップは、エージェントロールで動作する SNMP エンティティが RF スキャンを通じて不正な AP を検出したことを示します。	1.3.6.1.4.1.171.12.96.11.0.17
wsRFScanAPDetected	wsRFScanAPDetected トラップは、エージェントロールで動作する SNMP エンティティが RF スキャンを通じて AP を検出したことを示します。	1.3.6.1.4.1.171.12.96.11.0.18
wsRFScanNewClientDetected	wsRFScanNewClientDetected トラップは、エージェントロールで動作する SNMP エンティティが RF スキャンを通じて新しくクライアントを検出したことを示します。	1.3.6.1.4.1.171.12.96.11.0.19
wsClientAssociationDetected	wsClientAssociationDetected トラップは、エージェントロールで動作する SNMP エンティティがクライアントアソシエーションを検出したことを示します。	1.3.6.1.4.1.171.12.96.11.0.20
wsClientDisassociationDetected	wsClientDisassociationDetected トラップは、エージェントロールで動作する SNMP エンティティがクライアントアソシエーション解除を検出したことを示します。	1.3.6.1.4.1.171.12.96.11.0.21
wsClientRoamDetected	wsClientRoamDetected トラップは、エージェントロールで動作する SNMP エンティティがクライアントのローミングを検出したことを示します。	1.3.6.1.4.1.171.12.96.11.0.22
wsClientAssociationFailure	wsClientAssociationFailure トラップは、エージェントロールで動作する SNMP エンティティがクライアントアソシエーションのエラーを検出したことを示します。	1.3.6.1.4.1.171.12.96.11.0.23
wsClientAuthenticationFailure	wsClientAuthenticationFailure トラップは、エージェントロールで動作する SNMP エンティティがクライアントの認証エラーを検出したことを示します。	1.3.6.1.4.1.171.12.96.11.0.24
wsAdHocClientDetected	wsAdHocClientDetected トラップは、エージェントロールで動作する SNMP エンティティが Ad hoc クライアントを検出したことを示します。	1.3.6.1.4.1.171.12.96.11.0.25
wsWLANBandwidthUtilizationExceeded	wsWLANBandwidthUtilizationExceeded トラップは、エージェントロールで動作する SNMP エンティティが WLAN 帯域制限を超過を検出したことを示します。	1.3.6.1.4.1.171.12.96.11.0.26
wsAdHocClientListFull	wsAdHocClientListFull トラップは、エージェントロールで動作する SNMP エンティティが Ad hoc クライアントデータベースのフルを検出したことを示します。	1.3.6.1.4.1.171.12.96.11.0.27
wsPeerSwitchConfigurationCommandReceived	wsPeerSwitchConfigurationCommandReceived トラップは、エージェントロールで動作する SNMP エンティティがネットワークにおいてピアスイッチから「Configuration」コマンドを受信したことを示します。 また、受信したコンフィグマスクをトラップに返します。	1.3.6.1.4.1.171.12.96.11.0.28
wsPeerSwitchManagedAPLimitExceeded	wsPeerSwitchManagedAPLimitExceeded トラップは、エージェントロールで動作する SNMP エンティティが Peer Switch Managed AP データベースの制限の超過を検出したことを示します。	1.3.6.1.4.1.171.12.96.11.0.29
wsClusterControllerElected	wsClusterControllerElected トラップは、エージェントロールで動作する SNMP エンティティがピアグループのクラスタコントローラとして自身を選定したことを示します。	1.3.6.1.4.1.171.12.96.11.0.32
wsClusterMaxAPExceeded	wsClusterMaxAPExceeded トラップは、エージェントロールで動作する SNMP エンティティがネットワーク内の Managed AP の超過を検出したことを示します。	1.3.6.1.4.1.171.12.96.11.0.33
wsRoguesPresent	wsRoguesPresent トラップは、エージェントロールで動作する SNMP エンティティがネットワーク内に 1 つ以上の不正な存在を検出したことを示します。	1.3.6.1.4.1.171.12.96.11.0.34
wsDetectedClientListFull	wsDetectedClientListFull トラップは、エージェントロールで動作する SNMP エンティティが検出済みクライアントデータベースのフルを検出したことを示します。	1.3.6.1.4.1.171.12.96.11.0.35

トラップ名	説明	OID
wsRogueClientsPresent	wsRogueClientsPresent トラップは、エージェントロールで動作する SNMP エンティティがネットワーク内に 1 つ以上の不正クライアントの存在を検出したことを示します。	1.3.6.1.4.1.171.12.96.11.0.36
wsChannelPlanAlgoComplete	wsChannelPlanAlgoComplete トラップは、エージェントロールで動作する SNMP エンティティがチャンネルアルゴリズムの完了イベントを検出したことを示します。	1.3.6.1.4.1.171.12.96.11.0.37
wsPowerPlanAlgoComplete	wsPowerPlanAlgoComplete トラップは、エージェントロールで動作する SNMP エンティティが電力アルゴリズムの完了イベントを検出したことを示します。	1.3.6.1.4.1.171.12.96.11.0.38
wsLocallyManagedAPLimitExceeded	wsLocallyManagedAPLimitExceeded トラップは、エージェントロールで動作する SNMP エンティティが WS のローカルな Managed AP データベースの制限の超過を検出したことを示します。	1.3.6.1.4.1.171.12.96.11.0.41
wsAPHardwareTypeFailure	wsAPHardwareTypeFailure トラップは、エージェントロールで動作する SNMP エンティティが未サポートの AP ハードウェアタイプを検出したことを示します。	1.3.6.1.4.1.171.12.96.11.0.100
cpClientAuthenticationFailure	cpClientAuthenticationFailure トラップは、エージェントロールで動作する SNMP エンティティがクライアントの認証エラーを検出したことを示します。	1.3.6.1.4.1.171.12.97.4.0.1
cpClientConnect	cpClientConnect トラップは、エージェントロールで動作する SNMP エンティティがクライアントの接続を検出したことを示します。	1.3.6.1.4.1.171.12.97.4.0.2
cpClientDatabaseFull	cpClientDatabaseFull トラップは、エージェントロールで動作する SNMP エンティティがクライアントアソシエーションデータベースのフルを検出したことを示します。	1.3.6.1.4.1.171.12.97.4.0.3
cpClientDisconnect	cpClientDisconnect トラップは、エージェントロールで動作する SNMP エンティティがクライアントの切断を検出したことを示します。	1.3.6.1.4.1.171.12.97.4.0.4

付録 E RADIUS 属性の割り当て指定

スイッチにおける 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
- キャプティブポータル（CP）

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

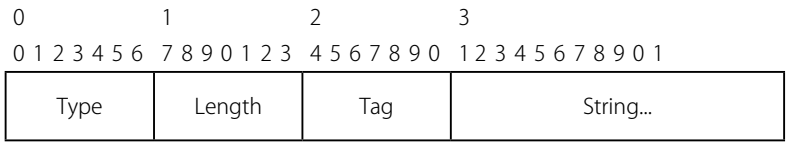
RADIUS サーバの 802.1p プライオリティ属性（例 : プライオリティ 7）を設定し、802.1X またはホストベース認証に成功すると、RADIUS サーバに従ってデバイスは 802.1p デフォルトプライオリティをポートに割り当てます。しかし、プライオリティ属性を設定せずに認証に成功しても、デバイスはプライオリティをポートに割り当てません。RADIUS サーバに設定されたプライオリティ属性が範囲外（7 より大きい）であると、そのデバイスには設定されません。

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
Tunnel-Type	本属性はトンネルの開始に使用されるトンネリングプロトコルまたはトンネルの終了に使用されるトンネリングプロトコルを示します。	13 (VLAN)	必須
Tunnel-Medium-Type	本属性は使用されている伝送の媒体を示します。	6 (802)	必須
Tunnel-Private-Group-ID	本属性は特定のトンネルセッションのグループ ID を示します。	文字列（VID）	必須

「Tunnel-Private-Group-ID」属性フォーマットのサマリは次のようになります。



タグフィールドの定義は次の通りです。（RFC 2868 とは異なります）

タグフィールド値	文字列フィールドのフォーマット	備考
0x01	VLAN 名 (ASCII)	0x1F よりも大きいタグフィールドは続くフィールドの最初のオクテットとして認識されます。
0x02	VLAN ID (ASCII)	
その他 (0x00、0x03 ~ 0x1F、>0x1F)	**1.** スイッチが VLAN 設定の文字列を受信した場合、最初は VLAN ID として認識します。つまりスイッチは既存の VLAN ID をチェックし、合致するものがあるか調べます。 **2.** スイッチが合致する VLAN ID を発見した場合、その VLAN へ移動します。 **3.** スイッチが合致する VLAN ID を発見できなかった場合、VLAN 設定の文字列は VLAN 名として認識されます。 **4.** そして合致する VLAN 名を発見します。	

RADIUS サーバの VLAN 属性（例 : VID 3）を設定し、802.1X または MAC ベースアクセスコントロール認証に成功すると、ポートは VLAN 3 に追加されます。しかし、VLAN 属性を設定せずに認証に成功しても、ポートは元の VLAN に置かれます。RADIUS サーバに設定された VLAN 属性が存在しないと、ポートは要求された VLAN に割り当てられません。

RADIUS サーバが ACL を割り当てるためには、適切な項目を RADIUS サーバに設定する必要があります。以下の表では ACL の項目を示しています。RADIUS ACL の割り当ては、MAC ベースアクセスコントロールにて使用されるだけです。

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、「アクセスコントロールリスト（ACL）コマンド」を参照してください。

アクセスポイントの RADIUS 属性

アクセスポイントは物理 MAC アドレスによって識別されるため、管理者は各アクセスポイントのに対して MAC アドレスに対する User-Name 属

性のセット共に RADIUS エントリを追加します。以下の表は RADIUS サーバエントリに設定される属性を示しています。ベンダー指定の属性は、D-Link ベンダー ID（171）を使用することで追加されます。

属性	説明	範囲	摘要	初期値
User-Name (1)	アクセスポイントの MAC アドレス。	有効なイーサネット MAC アドレス。	必須	なし
User-Password (2)	AP エントリ検索に使用するパスワード。	8-63 文字の英数字。初期値は「NOPASSWORD」。	必須	なし
Vendor-Specific (26), D-Link (171), Location (101)	アクセスポイントの場所。	0-32 文字。	オプション	""
Vendor-Specifc (26), D-Link (171), Mode (102)	本アクセスポイントがスイッチまたは管理者の管理下にあるか、または不正 AP であるかを示します。	Managed (1), Standalone (2), Rogue (3)	必須	なし
Vendor-Specifc (26), D-Link (171), Profile-ID (103)	アクセスポイントがスイッチの管理下にあるときの、本アクセスポイント用のコンフィグレーションプロファイルの ID。	1-16	モードが「WS-Managed」の場合、必須。	なし
Vendor-Specifc (26), D-Link (171), Switch-IP (104)	本 RADIUS サーバを複数台のスイッチで共有している場合に、本アクセスポイントを管理するスイッチの IP アドレス。	有効な IP アドレス	オプション	なし
Vendor-Specifc (26), D-Link (171), Radio-1-Chan (105)	無線帯域の固定チャンネル。	0, 1-13, 36, 40, 44, 48, 52,56, 60, 64, 104, 108, 112,116, 120, 124, 128, 132,140, 149, 153, 157, 161,165。「0」は自動チャンネル割り当てを示します。	オプション。定義されたチャンネルが有効であるならば、自動チャンネル割り当てによる設定は上書きされます。	0
Vendor-Specifc (26), D-Link (171), Radio-2-Chan (106)	無線帯域の固定チャンネル。	0, 1-13, 36, 40, 44, 48, 52,56, 60, 64, 104, 108, 112,116, 120, 124, 128, 132,140, 149, 153, 157, 161,165。「0」は自動チャンネル割り当てを示します。	オプション。定義されたチャンネルが有効であるならば、自動チャンネル割り当てによる設定は上書きされます。	0
Vendor-Specifc (26), D-Link (171), Radio-1-Power (107)	無線帯域の固定電力設定を示します。	0、1-100%。0 は自動送信電力調整を示します。	オプション。定義された値が有効であれば自動電力設定は上書きされます。	0
Vendor-Specifc (26), D-Link (171), Radio-2-Power (108)	無線帯域の固定チャンネル。	0、1-100 パーセント。0 は自動送信電力調整を示します。	オプション。定義された値が有効であれば自動電力設定は上書きされます。	0
Vendor-Specifc (26), D-Link (171), Expected-Channel (112)	スタンドアロンのアクセスポイントのための Expected-Channel。	0, 1-165。0 は本アクセスポイントがどのチャンネルでも動作することを示します。	オプション	0
Vendor-Specifc (26), D-Link (171), Expected-AP-Security (110)	スタンドアロンのアクセスポイントのための Expected Security Mode。	• 0 - すべてのモード • 1- Open • 2 - WEP • 3 - WPA または WPA2	オプション	0
Vendor-Specifc (26), D-Link (171), Expected-SSID (109)	スタンドアロンアクセスポイントのための Expected SSID。	0-32 バイトの文字列。入力しないと、デバイスはあらゆる SSID を使用する可能性があります。	オプション	""
Vendor-Specifc (26), D-Link (171), Allowed-On-Wired-Network (113)	本スタンドアロンアクセスポイントが有線ネットワークに許可されているかどうかを示すフラグ。	• 0 - アクセスポイントは有線ネットワークに許可されています。 • 1 - アクセスポイントは有線ネットワークで許可されていません。	オプション	0

クライアントの 802.1X RADIUS 属性

アクセスポイントは、RADIUS を通じて 802.1X 認証を使用することで、クライアントステーションの特定ユーザに対して無線ネットワークへのアクセスを許可または禁止でできます。802.1X 認証は使用されている場合（および 802.1X 認証のみ使用されている場合）、無線クライアントの QoS パラメータは取得されます。これは、ユーザ名とパスワードの識別証明に基づいています。ここで定義される各 QoS パラメータはオプションです。これは、有効な 802.1X 認証がクライアントで行われても、QoS パラメータがクライアントの RADIUS サーバエントリには存在しない可能性があることを意味します。無線クライアントが 802.1X を使用した認証に成功すると仮定すると、クライアントに存在する各 QoS RADIUS 属性は処理のためにアクセスポイントに送信されます。

それ以外の場合、次のいずれかとなります。

- 802.1X 認証を使用しない。
- 使用するが認証に失敗する。
- 認証に成功するが、特定の QoS RADIUS 属性がクライアントに設定されていないか有効ではない。

対応する AP ネットワーククライアント QoS デフォルトパラメータが代わりにクライアント用として使用されます。これらの個々の RADIUS 属性はこのようにその場その場で評価されます。

属性	説明	範囲	摘要
Vendor-Specific (26), D-Link (171), Client-ACL-Dn (120)	外向き（down）の 802.1X 認証済み無線クライアントトラフィックに適用されるアクセスリストの ID。この属性が存在しないと、「Network Configuration」で定義した「Client QoS」の ACL Down Type および Name パラメータの初期値が代わりに使用されます。この属性が存在し、システムに未定義のアクセスリスト名を示すと、ACL が定義されるまで、このクライアントに対する全パケットが破棄されます。	Type: 5-36 文字の文字列（ヌル終端なし） 文字列は以下の通り、「type:name」形式になります。: • type = ACL タイプ識別子 :IPV4, IPV6, MAC •「:」は区切り文字として必要です。 • name = 英数字（1-31 文字）で ACL 番号（IPv4）または名称（IPv6、MAC）を示します。	オプション
Vendor-Specific (26), D-Link (171), Client-ACL-Up (121)	内向き（up）の 802.1X 認証済み無線クライアントトラフィックに適用されるアクセスリストの ID。この属性が存在しないと、「Network Configuration」で定義した「Client QoS」の ACL Up Type および Name パラメータの初期値が代わりに使用されます。この属性が存在し、システムに未定義のアクセスリスト名を示すと、ACL が定義されるまで、このクライアントに対する全パケットが破棄されます。	Type: 5-36 文字の文字列（ヌル終端なし） 文字列は以下の通り、「type:name」形式になります。: • type = ACL タイプ識別子 :IPV4, IPV6, MAC •「:」は区切り文字として必要です。 • name= 英数字 (1-31 文字) で ACL 番号 (IPv4) または名称 (IPv6,MAC) を示します。	オプション
Vendor-Specific (26), D-Link (171), Client-Policy-Dn (122)	外向き（down）の 802.1X 認証済み無線クライアントトラフィックに適用される DiffServ ポリシー名。この属性が存在しないと、「Network Configuration」で定義した「Client QoS」の「Default Policy Down」パラメータが代わりに使用されます。この属性が存在し、システムに未定義のアクセスリスト名を示すと、DiffServ ポリシーが定義されるまで、このクライアントに対する全パケットが破棄されます。	Type: 1-31 文字の文字列（ヌル終端なし）	オプション
Vendor-Specific (26), D-Link (171), Client-Policy-Up (123)	内向き（up）の 802.1X 認証済み無線クライアントトラフィックに適用される DiffServ ポリシー名。この属性が存在しないと、「Network Configuration」で定義した「Client QoS」の「Default Policy Up」パラメータが代わりに使用されます。この属性が存在し、システムに未定義のアクセスリスト名を示すと、DiffServ ポリシーが定義されるまで、このクライアントに対する全パケットが破棄されます。	Type: 1-31 文字の文字列 (ヌル終端なし)	オプション
Tunnel-Type (64)	ダイナミック VLAN 用。	VLAN (13)	オプション
Tunnel-Medium-Type (65)	ダイナミック VLAN 用。	802	オプション
Tunnel-Private-Group-ID (81)	ダイナミック VLAN 用。	VLANID	オプション

Known Client と MAC 認証の RADIUS 属性

データベースは、MAC 認証の実行や RADIUS サーバからクライアントの記述名を取得するために使用されます。アクセスポイントは、RADIUS を通じて MAC 認証を使用することで、特定のクライアントステーションのに対して無線ネットワークへのアクセスを許可または禁止できます。これをそれほど安全ではありませんが、802.1X をサポートしないクライアントステーションに使用できます。

以下の表に RADIUS サーバに設定する属性を示します。

属性	説明	範囲	摘要	初期値
Default User-Name (1)	クライアントステーションのイーサネットアドレス。	有効なイーサネット MAC アドレス。	必須	なし
User-Password (2)	クライアントの MAC エントリ検索用の固定パスワード。	"NOPASSWORD"	必須	なし
Vendor-Specific (26), D-Link (171), MAC-Authentication-Action (114)	MAC 認証がネットワークで有効である場合に適用する操作を示すフラグ。	• 0 - Global Action • 1 - アクセスを許可する • 2 - アクセスを拒否する	オプション	0
Vendor-Specifc (26), D-Link (171), Client-Nickname (115)	クライアントを説明する名。	0-32 文字の文字列	オプション	""
Tunnel-Type (64)	ダイナミック VLAN 用	VLAN (13)	オプション	
Tunnel-Medium-Type (65)	ダイナミック VLAN 用	802	オプション	
Tunnel-Private-Group-ID (81)	ダイナミック VLAN 用	VLANID	オプション	

グローバル MAC 認証の動作が、「White List」として設定されると、リストに指定されていて、明示的にアクセスを拒否されていないアドレスを持つ無線クライアントはすべてアクセスを許可されます。リストに MAC アドレスがない場合、クライアントへのアクセスは拒否されます。

グローバル MAC 認証の動作が、「Black List」として設定されると、リストに指定されていて、明示的にアクセスを許可されていないアドレスを持つ無線クライアントはすべてアクセスを拒否されます。リストに MAC アドレスがない場合、クライアントへのアクセスは許可されます。

キャプティブポータル RADIUS 属性

以下のテーブルではキャプティブポータルユーザを設定するのに使用される RADIUS 属性を示します。本テーブルはキャプティブポータルを設定するのに使用される RADIUS 属性とベンダー特有の属性 (VSA) の両方を示しています。

属性	説明	範囲	摘要	初期値
User-Name (1)	認証されるユーザ名	1-32 文字	必須	なし
User-Password (2)	ユーザパスワード	8-64 文字	必須	なし
Session-Timeout (27)	アイドルタイムアウト（秒）に到達するとログアウトします。属性が 0 または表示されていない場合、キャプティブポータルに設定された値を使用します。	整数（秒）	オプション	86400
Idle-Timeout (28)	アイドルタイムアウト（秒）に到達するとログアウトします。属性が 0 または表示されていない場合、キャプティブポータルに設定された値を使用します。	整数（秒）	オプション	0
Vendor-Specific (26), WISPr (14122), WISPr-Bandwidth-Max-Down (8)	クライアントの最大受信レート（b/s）。クライアントがネットワークにデータを受信できる帯域幅を制限します。属性が 0 または表示されていない場合、キャプティブポータルに設定された値を使用します。	整数	オプション	0
Vendor-Specific (26), WISPr (14122), WISPr-Bandwidth-Max-Up (7)	クライアントの最大送信レート（b/s）。クライアントがネットワークにデータを送信できる帯域幅を制限します。属性が 0 または表示されていない場合、キャプティブポータルに設定された値を使用します。	整数	オプション	0
Vendor-Specific (26), D-Link (171), LVL7-Max-Input-Octets (124)	ユーザが送信できる最大オクテット数。この制限に到達すると、ユーザは切断されます。属性が 0 または表示されていない場合、キャプティブポータルに設定された値を使用します。	整数	オプション	0
Vendor-Specific (26), D-Link (171), LVL7-Max-Output-Octets (125)	ユーザが受信できる最大オクテット数。この制限に到達すると、ユーザは切断されます。属性が 0 または表示されていない場合、キャプティブポータルに設定された値を使用します。	整数	オプション	0
Vendor-Specific (26), D-Link (171), LVL7-Max-Total-Octets (126)	ユーザクライアントが転送できる最大オクテット数（送受信オクテットの合計）。この制限に到達すると、ユーザは切断されます。属性が 0 または表示されていない場合、キャプティブポータルに設定された値を使用します。	整数	オプション	0
Vendor-Specific (26), D-Link (171), LVL7-Captive-Portal-Groups (127)	設定した「CP instance configuration」に対応するグループ名をコンマで区切っているリスト。	文字列	オプション	なし。指定しない場合は、初期設定が使用されます。

付録 F　無線スイッチ仕様

キャプティブポータルガイドライン

認証ローミングとクラスタリング

一般的なインプリメンテーションに加えて、キャプティブポータルは「認証ローミング」と「クラスタリング」と呼ばれる無線ネットワーク用の 2 つの重要な機能を提供します。

1. 認証ローミングでは、クライアントは認証中であれば、シームレスを形成するアクセスポイント間をローミングできます。

2. クラスタリングにより、異なるスイッチに接続するアクセスポイント間のローミングとクラスタコントローラからスイッチすべてのキャプティブポータル状態のモニタリングを行うことができます。

クラスタ内のスイッチは同じキャプティブポータル設定（キャプティブポータル設定のインスタンス、接続インタフェース、ローカルユーザデータベース、および RADIUS サーバ設定など）を共有する必要があります。データベースは、クライアントの認証ローミングをサポートするために 1 つのクラスタ内で同期されるべきです。

クラスタコントローラ選定

ピアグループの各スイッチはどれがクラスタコントローラであるかを個別に決定します。スイッチが 1 つのピアスイッチも持たない場合、自身をクラスタコントローラに任命します。

2 つのスイッチがディスカバリプロセスを通じて相互に検出した場合、クラスタ優先度フィールドの値を比較します。高い優先度を持つスイッチがクラスタコントローラになります。優先度が同じである場合、低い IP アドレスを持つスイッチがクラスタコントローラになります。クラスタ優先度は初期の識別メッセージで送信されます。

クラスタ優先度の範囲は 0-255 です。優先度を 0 に設定すると、スイッチクラスタコントローラ機能は無効になります。上位スイッチまたはネットワークアプライアンスだけでも十分クラスタコントローラのように機能できる大規模なネットワークを展開する場合、下位のスイッチをクラスタコントローラにしないよう機能を無効にしたい場合があるかもしれません。

スイッチがピアグループに参加した後に、管理者はスイッチのクラスタ優先度値を変更する可能性があります。また、クラスタ優先度は keep-alive メッセージで伝搬され、これによりピアスイッチがスイッチの新しいクラスタ優先度を学習できます。

スイッチは再起動後、現在のクラスタコントローラとの接続を喪失した後、および別のスイッチから初期識別メッセージまたは keep-alive メッセージを受信するたびに選定処理を実行します。スイッチは、各ピアスイッチ用のクラスタ優先度と IP アドレスのリストを保持しており、上で記述した基準に基づいてクラスタコントローラを選定します。

クラスタコントローラスイッチが、より高位のクラスタ優先度または低位の IP アドレスを持つ別のスイッチからのメッセージを受信したため、自身がもうコントローラでないと判断すると、いくつかのデータベースを削除します。

クラスタコントローラ状態の移行の決定は直ちに行われます。スイッチが自身をクラスタコントローラとして選定する場合も直ちに行われます。スイッチが別のスイッチをクラスタコントローラとして選定すると、keep-alive タイマの遅延によりそのスイッチをクラスタコントローラとして宣言する決定が行われます。別のクラスタコントローラがこの間に検出されると、遅延タイマは再度開始します。管理者が遅延期間にスイッチ状態を確認すると、スイッチがクラスタコントローラでなく、クラスタコントローラアドレスが「0.0.0.0」であることがわかります。本リリースでは keep-alive の間隔は 120 秒に固定されています。

各ピアスイッチは個別に他のピアスイッチとの接続を確立します。一時的な場合、別のスイッチと接続を確立しているだけのスイッチの 1 つは、2 つのスイッチが違うクラスタコントローラを選択できるように、別のスイッチが参照するスイッチのすべてを参照しないようにすることができます。スイッチがクラスタコントローラであることにピアスイッチが同意しない場合、WIDS セキュリティ機能は正しく動作しませんが、この条件はネットワークを通じたデータ転送には影響せず、通常の操作はピアグループ内のすべてのスイッチが相互にディスカバリするとすぐに復元されます。

クラスタ優先度を 0 に設定することでクラスタコントローラ機能を無効にしてから、ネットワークにおけるすべての無線スイッチのクラスタコントローラ機能を無効に、ネットワークがクラスタコントローラなしで動作するように設定できます。

クラスタ優先度はグローバルなスイッチのコンフィグレーション設定です。グローバルなコンフィグレーションが 1 つのピアスイッチから別のピアスイッチまでプッシュされる場合、目的が各スイッチのクラスタコントローラ機能に対して優先度レベルを区別することであるため、クラスタ優先度はこのコンフィグレーションには含まれません。

クラスタコントローラ選定プロセスの結果を反映する 2 つのスイッチステータスパラメータがあります。このステータスパラメータは、本スイッチがクラスタコントローラであるかどうかを示す選定済みクラスタコントローラの「IP アドレス」と「Boolean フラグ」です。フラグは、クラスタアドレスとスイッチの IP アドレスとの比較により取得するため、特別な情報を提供しませんが、管理者がローカルスイッチがクラスタコントローラであるかどうかを知ると迅速な方法を提供します。

スイッチは自身がクラスタコントローラであると判断した後に、SNMP トラップを送信します。

X.509 Certification Mutual Authentication（X.509 証明書相互認証）

X.509 Certification Mutual Authentication（X.509 証明書相互認証）

無線システムが X.509 Mutual Certificate 交換を実行するために設定されると、スイッチとアクセスポイントは、互いの X.509 証明書交換を実行するために TLS 接続を設定します。各デバイスはリモートデバイスの証明書のローカルコピーとリモートエンドポイントから受信した証明書を比較します。証明書が一致しないと、TLS 接続は破棄されます。

X.509 証明書はスイッチとアクセスポイントで自動生成されるため、デバイスがどんな信頼できる認証局とも通信せずに、管理者は証明書維持費用を支払う必要はありません。各スイッチは他のすべてのスイッチとそれが管理するアクセスポイント用に X.509 証明書のコピーを持っています。各アクセスポイントはアクセスポイントが接続を確立する可能性のあるスイッチの X.509 証明書のコピーを持っています。相互認証機能がアクセスポイントとスイッチのプロビジョニング中に有効であり、管理者コマンドで起動される場合、証明書は配布されます。

スイッチはパスフレーズ認証をサポートしないため、X.509 相互証明書交換はピアスイッチが相互に認証を行う唯一のメカニズムです。クラスタコントローラが無線スイッチを現在管理している場合、本スイッチに向かうどのプロビジョニング要求もエラーとなることにご注意ください。

X.509 相互認証が有効である場合、アクセスポイントとピアスイッチディスカバリは、TLS 接続設定中に証明書を交換するため、本機能が無効な場合より遅くなります。

無線システムにおける証明書の概要と利用法

TLS 接続には、次の 2 つの側面があります。: クライアント側が接続を開始し、サーバ側が接続を受け付けます。無線システムでは、アクセスポイントは単に TLS クライアントとして機能し、スイッチは TLS クライアントまたは TLS サーバのどちらかとして機能します。スイッチは、ピアスイッチとの接続を確立すると、TLS クライアントとして機能します。

TLS プロトコルはサーバ証明書と相互証明書のクライアント照合をサポートします。相互認証モードが有効である場合、無線システムは相互証明書照合を使用するために TLS セッションを設定します。相互認証モードが無効である場合、無線システムは、Anonymous Cipher を使用して、証明書交換と照合を無効にします。

証明書を検証するためには、各デバイスは秘密鍵と X.509 証明書を生成します。秘密鍵は、デバイスに保持されており、他のスイッチまたはアクセスポイントに配布されません。証明書には照合する公開鍵があります。無線システムにおける他のデバイスにデバイス証明書を付与します。デバイスの証明書を使用して公開鍵で暗号化されたデータは、デバイスの秘密鍵で復号化することができます。

証明書は Base64 でコード化されている PEM 形式を使用してコード化されます。Base64 コード化は、2 進数データを表すのに印刷可能な ASCII 文字を使用します。証明書ファイルが証明書検証に使用可能となる前に、OpenSSL ライブラリにロードされます。

各無線デバイスには、通信する必要があるデバイスの証明書のコピーがあります。TLS 接続の確立中、無線デバイスは他の無線デバイスにロードされている利用可能な証明書のすべてを使用して接続設定時に受信した証明書と比較します。一致する証明書を見つけると、証明書の照合は成功します。照合機能は証明書を持つデバイスの IP アドレスを関連付けたり、証明書の有効期限をチェックしません。

TLS 接続は、初期の接続設定時にだけ証明書を検証するために設定されます。接続の再認証は新しい証明書検証を起動しません。

アクセスポイントにおける証明書生成

アクセスポイントは起動時に X.509 証明書を自動生成します。アクセスポイントは、起動時にキーファイルと証明書ファイルが既に存在しているかどうかをチェックします。アクセスポイントはファイルが存在するとそれらを使用し、存在しないとファイルを生成します。「/etc/uwskey.pem」ファイルは 1024 ビットの秘密鍵を含んでいます。「/etc/uwscert.pem」ファイルは X.509 証明書を含んでいます。

AP 証明書を再作成するためには、管理者はアクセスポイントで「factory-reset」コマンドを実行するか、ファイルシステムから 2 個のファイルを削除するか、またはアクセスポイントを再起動します。

スイッチにおける証明書生成

スイッチは起動時に X.509 証明書と他のキーファイルを自動生成します。スイッチは起動時にキーファイルと証明書ファイルが存在しているかどうかをチェックし、存在しないとファイルを生成します。

管理者は無線コンポーネントが使用する X.509 証明書を再生成できます。Diffie-Hellman キーが再生成されないことにご注意ください。キーの再生成中に無線機能を無効にするべきです。相互認証が有効である場合、クラスタに参加する前にスイッチに再プロビジョニングを行う必要があります。

IP アドレスの割り当て

管理者によって無線スイッチは IP アドレスを割り当てられます。ルーティングパッケージは製品に含められおり、ルーティングは初期値で有効です。既存のシステムインタフェースに加え、管理者はオプションでルーティングインタフェースを作成できます。無線のソフトウェアは自動的に最も低位のインタフェースインデックスの IP アドレスを選択します。システムインタフェースは最も低位のインデックス「1」を持つインタフェースです。システムインタフェースが削除されると、ソフトウェアは自動的に最も低位のインデックスを持つルーティングインタフェースの IP アドレスを選択します。インタフェースが何も定義されないと、無線機能は無効になります。

インタフェースを無効にするか、またはインタフェースの IP アドレスを変更すると、無線機能は無効になります。別のインタフェースが存在する場合、無線機能は自動的にそれの使用を開始します。

一度、インタフェースが選択されると、無線機能はインタフェースがダウンするまで、そのインタフェースの使用を継続します。

ネットワークインタフェースの IP アドレスを変更すると、自動的に無線機能が一旦無効になり、その後有効になります。

管理者には、無線機能のための自動 IP アドレス割り当てを無効にして、スタティックな IPv4 アドレスを入力するオプションがあります。無線機能が正常に動作するためには、IP アドレスはアクティブなルーティングインタフェースのアドレスと同じである必要があります。特定アドレスを持つインタフェースが存在していないか、またはアクティブでないと、無線機能は無効にされます。また、WLAN Switch Disable Reason（無線スイッチの無効化の理由）は「No Active Interface for Statically Configured IP Address」（スタティックに設定した IP アドレス用のアクティブなインタフェースはありません）に設定されます。

無線機能が既に有効である時にスタティック IP アドレスが設定され、定義済みのスタティック IP アドレスが無線機能に使用される現在の IP アドレスと異なる場合、無線機能は新しい IP アドレスで自動的に無効化および再有効化されます。定義済みのスタティック IP アドレスが無線機能に既に使用されている場合、無線機能は無効にされません。また、無線クライアントに対するサービスは中止されません。

MBA および IMPB に対する IP トンネル

無線スイッチが無線クライアントに対する IP トンネルを有効にすると、無線トンネルクライアントの MAC が最も高い優先度を持ちます。MBA と IMPB は、無線トンネルクライアントの MAC を制限するために動作しません。さらに、無線トンネルクライアントが無線スイッチによって追加されると、無線スイッチは MAC を追加した場合に、そのクライアント MAC を削除するように MBA モジュールに通知します。つまり、MAC がトンネルクライアントに所属する時、MBA と IMPB は動作しません。

IP-in-IP トンネルフォワーディングを実行するためには、トンネル配下のデバイスの MAC アドレスは学習され、無線スイッチの「スタティック」FDB エントリとしてマークされます。これらの「スタティック」エントリは「clear fdb all」コマンドを使用して削除されません。また、「delete fdb <vlan_name> <macaddr>」コマンドを使用しても削除されます。また、デバイスがまだオンラインである限り、FDB テーブルからエージングアウトされません。

付録 G　D-Link 統合アクセスシステムの初期設定

本章では、D-Link 統合スイッチ用設定の初期値、およびスイッチがアクセスポイントを検出・認証後に適用するデフォルト AP プロファイルに設定されている値を示します。

G.1 DWS-3160 の初期設定

本製品の初期設定を示します。

スイッチの初期設定

設定項目		初期値
システム情報	ユーザ名	なし
	Password	なし
ネットワーク情報	DHCP クライアント	無効
	ネットワークコンフィグレーションプロトコル	なし
	IP アドレス	10.90.90.90
	サブネットマスク	255.0.0.0
	802.1Q	有効
	管理用 VLAN ID	1
	タグなし VLAN ID	1
	スパニングツリープロトコル	有効
WLAN 情報	無線スイッチモード	有効
	AP 認証	無効
	AP 認知	ローカル
	国コード	US
	デフォルトプロファイル名	Default
	ピアスイッチグループ ID	1
	L2（VLAN）/L3（IP）検出	有効
	SNMP トラップ	無効
	Client Roam Timeout	30 秒
	Ad Hoc Client Status	24 時間
	AP Failure Status	24 時間
	Detected Clients Status	24 時間
	RF Scan Status	24 時間

G.2 D-Link アクセスポイントプロファイルの初期設定

デフォルト AP プロファイルの設定内容を示します。初期設定では、D-Link アクセスポイントがスイッチと接続する時、アクセスポイントが認知されると同時に本表中の設定内容が適用されます。

デフォルト AP プロファイル設定

	設定項目	初期値
システム情報	ユーザ名	admin
	パスワード	admin
ネットワーク情報	DHCP クライアント	有効
	管理用 IP アドレス	10.90.90.91（DHCP による割り当てがない場合）
	サブネットマスク	255.0.0.0（DHCP による割り当てがない場合）
	DNS 名	なし
	管理用 VLAN ID	1
	タグなし VLAN ID	1
	IPv6 Admin モード	有効
	IPv6 Auto Config Admin モード	有効
無線設定	無線インタフェース（1 と 2）	On
	無線 1 IEEE 802.11 モード	802.11a/n
	無線 2 IEEE 802.11 モード	802.11b/g/n
	802.11b/g/n チャンネル	自動
	無線 1 チャンネル帯域	40 MHz
	無線 2 チャンネル帯域	20 MHz
	802.11a/n チャンネル	自動
	プライマリチャンネル	Lower
	Protection	Auto
	無線クライアント数	200
	Transmit Power	100 %
	ブロードキャスト / マルチキャストレート制限	無効
	Fixed Multicast Rate	自動
	Beacon Interval	100 ミリ秒
	DTIM Period	2 ビーコン
	Fragmentation Threshold	2346 バイト
	RTS Threshold	2347 バイト
	Rate Sets Supported(Mbps)	IEEE 802.11a : 54, 48, 36, 24, 18, 12, 9, 6 IEEE 802.11b : 11, 5.5, 2, 1 IEEE 802.11g : 54, 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2, 1 IEEE 5-GHz 802.11n : 54, 48, 36, 24, 18, 12, 9, 6 IEEE 2.4 GHz 802.11g : 54, 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2, 1
	Rate Sets(Mbps) (Basic/Advertised)	IEEE 802.11a : 24, 12, 6 IEEE 802.11b : 2, 1 IEEE 802.11g : 11, 5.5, 2, 1 EEE 5-GHz 802.11n : 24, 12, 6 IEEE 2.4 GHz 802.11n : 11, 5.5, 2, 1
仮想アクセスポイントとネットワーク設定	Status	双方の無線インタフェースにおいて VAP0 が有効。他の VAP は無効。
	ネットワーク名 (SSID)	dlink1 から dlink16
	VLAN ID	1
	Broadcast SSID	許可
	セキュリティモード	None（プレーンテキスト）
	認証タイプ	None
	RADIUS IP アドレス	10.90.90.1
	RADIUS キー	secret
	RADIUS アカウンティング	無効
	HTTP Redirect	なし

設定項目		初期値
その他の設定	WDS	None
	STP	無効
	MAC 認証	リスト内にステーションの記載なし。
	Load Balancing	無効
	SNMP	有効
	RO SNMP Community Name	Public
	Managed AP Mode	無効
	認証（802.1X サプリカント）	無効
	Management ACL	無効
	HTTP Access	有効、「Managed Mode」では無効。
	HTTPS Access	有効、「Managed Mode」では無効。
	SNMP Agent Port	161
	SNMP Set Requests	無効
	Console Port Access	有効
	Telnet Access	有効、「Managed Mode」では無効。
	SSH Access	有効、「Managed Mode」では無効。
	WMM	有効
	Network Time Protocol (NTP)	有効
	Clustering	停止
	Client QoS Global Admin Mode	無効
	VAP QoS Mode	無効

G.3 キャプティブポータル設定の初期値

キャプティブポータル設定の初期値を示します。

キャプティブポータル設定の初期値

設定項目		初期値
Global Configuration	Operational Status	Enabled
	Additional HTTP Port	None
	Peer Switch Statistics Reporting Interval	120 seconds
	Authentication Session Timeout	600 seconds
CP Configuration	Status	Enabled
	Configuration Name	None
	Protocol Mode	HTTP
	Verification Mode	Guest
	User Group	None
	URL Redirect Mode	Disabled
	Session Timeout	0（無制限）
	Idle Timeout	0（無制限）
	Languages	English

付録 H ケーブルとコネクタ

イーサネットケーブル

スイッチを別のスイッチ、ブリッジまたはハブに接続する場合、ノーマルケーブルが必要です。ケーブルピンアサインに合うことを再確認してください。

以下の図と表は標準の RJ-45 プラグ / コネクタとピンアサインです。

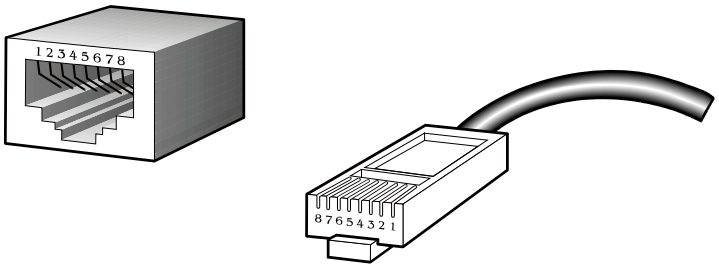


図 H-1　標準的な RJ-45 プラグとコネクタ

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

コンソールケーブル

スイッチを PC に接続する場合、付属のコンソールケーブルが必要です。以下の図と表は標準のコンソール -RJ45 へのソケット / コネクタとそれらのピンアサインです。

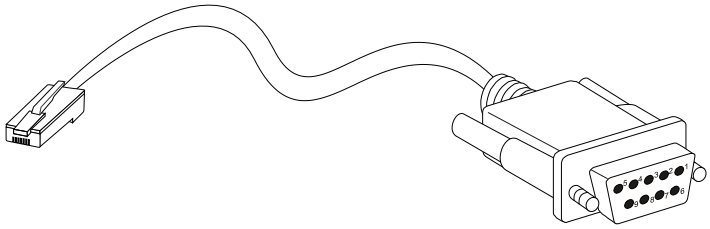


図 H-2　標準的なコンソール -RJ-45 ケーブル

コンソール -RJ-45 ピンアサイン		
ピン番号	コンソール（D-Sub9 / RS232）	RJ-45
1	未使用	未使用
2	RXD	未使用
3	TXD	TXD
4	未使用	GND
5	GND（共有）	GND
6	未使用	RXD
7	未使用	未使用
8	未使用	未使用

リダンダント電源（RPS）ケーブル

スイッチをリダンダント電源に接続する場合、RPS ケーブルが必要です。製品がケーブルのピンアサインに一致することを確認してください。以下の図と表は標準の RPS のソケット / コネクタとそれらのピンアサインです。

注意 DWS-3160-24PC は RPS-200 ではなく RPS-700 を使用します。どちらもパッケージに自身のケーブルが同梱されています。

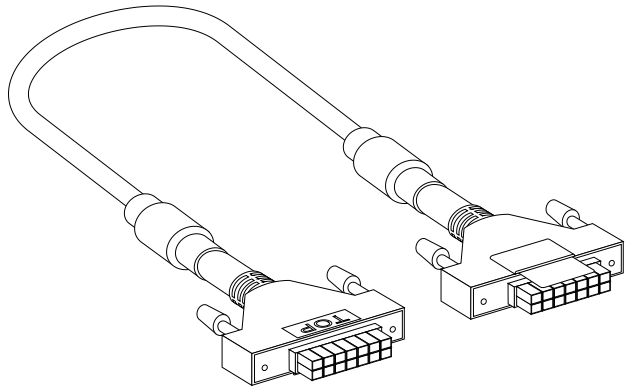


図 H-3　リダンダント電源ケーブル

RPS ケーブルピンアサイン		
ピン番号	デバイス	DPS-500
1	GND	GND
2	NC	NC
3	+12V	+12V
4	+12V	+12V
5	+12V	+12V
6	+12V	+12V
7	GND	GND
8	GND	GND
9	NC	電力良好
10	NC	電力供給
11	電力良好	NC
12	電力供給	NC
13	GND	GND
14	GND	GND

RPS ケーブルピンアサイン		
ピン番号	デバイス	DPS-700
1	-54Vrtn	-54Vrtn
2	-54V	-54V
3	+12V	+12V
4	+12V	+12V
5	+12V	+12V
6	+12V	+12V
7	NC/GND	NC/GND
8	+12vsen	+12Ven
9	LS-54v	LS-54V
10	-54V	-54V
11	-54Vrtn	-54Vrtn
12	GND	GND
13	GND/NC	GND/NC
14	RPS Present	RPS Present
15	Status_1	RPS PG
16	Status_2	GND
17	RPS PG	Status_1
18	GND	Status_2
19	+12VRTNsen	+12VRTNsen
20	LS+12V	LS+12V
21	-54Vsen	-54Vsen

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。

ケーブル長

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