D-Link DWS-4026
DWL-8600AP
Unified Wired & Wireless Access System

ユーザマニュアル

D-Link
Building Networks for People

安全にお使いいただくために

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

安全上のご注意　必ずお守りください

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

⚠警告	この表示を無視し、まちがった使いかたをすると、火災や感電などにより人身事故になるおそれがあります。
⚠注意	この表示を無視し、まちがった使いかたをすると、傷害または物損損害が発生するおそれがあります。

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

⚠警告

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

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

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

ぬれ手禁止
ぬれた手でさわらない
感電のおそれがあります。

水ぬれ禁止
水をかけたり、ぬらしたりしない
内部に水が入ると、火災、感電、または故障のおそれがあります。

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

禁止
内部に金属物や燃えやすいものを入れない
火災、感電、または故障のおそれがあります。

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

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

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

禁止
雷鳴が聞こえたら、ケーブル / コード類にはさわらない
感電のおそれがあります。

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

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

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

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

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

⚠注意

❗
静電気注意
コネクタやプラグの金属端子に触れたり、帯電したものを近づけますと故障の原因となります。

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

❗
振動が発生する場所では使用しない
接触不良や動作不良の原因となります。

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

電波障害自主規制について

DWS-4026 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。

DWL-8600AP 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 B 情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。
本書の記載に従って正しい取り扱いをしてください。

無線に関するご注意

電波に関するご注意

DWL-8600AP 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、W56 以外の 5GHz 帯 (IEEE 802.11a) 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 帯の 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

DWL-8600AP 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。

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。
また、テクニカルサポートご提供のためにはユーザ登録が必要となります。
http://www.dlink-jp.com/

目次

はじめに

DWS-4026/DWL-8600AP ユーザマニュアルは、本製品のインストールおよび操作方法を例題と共に記述しています。

第 1 章 本製品のご利用にあたって

- 本製品の概要とその機能について説明します。また、前面、背面の各パネルと LED 表示について説明します。

第 2 章 スイッチ管理の導入

- 製品の起動と、ユーザインターフェースへのアクセス方法について説明します。

第 3 章 システム管理

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

第 4 章 L2 機能の設定

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

第 5 章 L3 機能の設定

- スイッチは、ルート再配送設定、ルート優先度設定、ARP 設定、ルーティングテーブル、RIP などスイッチの L3 機能について説明します。

第 6 章 QoS 機能の設定

- スイッチの QoS の概要と設定について説明します。

第 7 章 アクセスコントロールリスト機能の設定

- アクセスコントロールの設定について説明します。

第 8 章 セキュリティ機能の設定

- 802.1X 認証、アクセス認証コントロールなどスイッチのセキュリティ機能について説明します。

第 9 章 無線機能の設定

- 無線デバイスの管理方法について説明します。

第 10 章　統合スイッチのログメッセージ

- 統合スイッチが提供する一般的なログメッセージを各メッセージの原因に関する情報と共に記述します。

付録 A 設定例

- VLAN 設定、ルーティングの設定、ネットワークアクセスコントロールなどの設定例について説明します。

付録 B D-Link 統合アクセスシステムの初期設定

- 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。

本マニュアルの対象者

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

表記規則について

本項では、本マニュアル中での表記方法について説明します。

注意 注意では、特長や技術についての詳細情報を記述します。

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

表 1 に、本マニュアル中での字体、・記号についての表記規則を表します。

表 1　字体・記号の表記規則

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

第 1 章　本製品のご利用にあたって

本項では、スイッチの前面、背面、および側面パネルと、LED 表示について説明します。

前面パネル

スイッチの前面パネルには、電源、コンソール、RPS（冗長電源システム）、PoE（Power over Ethernet）用 LED、PoE の切り替えを行うボタン、および各ポート用の Link/Act/Speed を示す LED、さらにオプションのモジュール実装時用の 10GE ポートと SPF ポート用の LED があります。

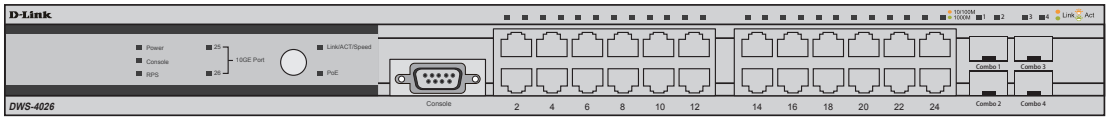


図 1-1　DWS-4026 の前面パネル図

LED 表示

本スイッチは電源、コンソール、RPS、PoE 用 LED、各ポートおよびオプションモジュール搭載時の 10GE ポート用 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 の状態を表す意味を示します。

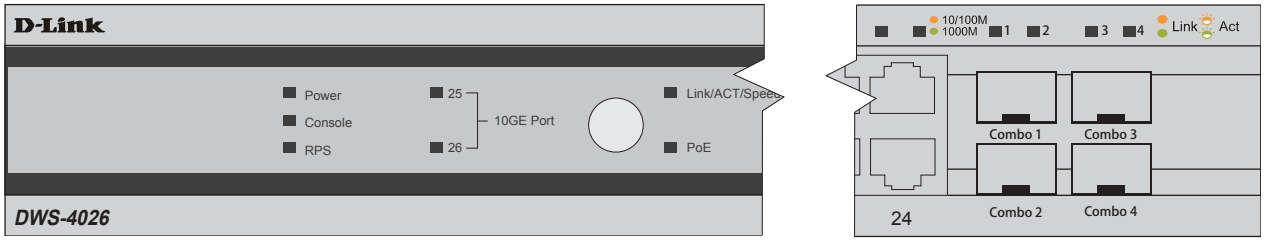


図 1-2　DWS-4026 の LED 表示

以下の表では、各スイッチの前面パネル上の LED およびモード選択ボタンについて説明します。

LED 表示		色	ステータス	説明
Power		緑	点灯	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（電源オフ時）。
Console		緑	点滅	電源投入後の Power ON Self Test（POST）中点滅し、終了すると消灯します。
		緑	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。
		ー	消灯	リダンダント電源ユニットは動作していません。
Link/Act/Speed モード		緑	点灯	ポート LED でリンク、動作、速度を示します。Link/Act/Speed モードから PoE モードへ変更する時は、LED モード選択ボタンを押下します。
PoE モード		緑	点灯	ポートに接続されたデバイスによる 802.3af PoE（Power over Ethernet）電源供給状態を示すモードです。PoE モードから Link/Act/Speed モードへ変更する時は、LED モード選択ボタンを押下します。
ポート LED	前面パネルの 2 列のポートの上に 1 列のポート LED が配置されています。ポートの左上に位置する LED は、その直下の上段のポートの状態を示します。またポートの右上に位置する LED は、下段のポートの状態を示します。 ポート LED は、各ポートのリンク / 動作 / 速度を示す場合と、PoE の使用状態を示す場合があり、LED モード選択ボタンで切り替えます。			
	Link/Act/Speed モード	緑	点灯	ポートに 1000Mbps のリンクが確立されていることを示します。
		緑	点滅	ポート上でデータ転送中であることを示します（伝送速度 : 1000Mbps）。
		橙	点灯	ポートに 10Mbps または 100Mbps のリンクが確立されていることを示します。
		橙	点滅	ポート上でデータ転送中であることを示します（伝送速度 : 100Mbps）。
		ー	消灯	リンク / 動作のないことを示します。
	PoE モード	緑	点灯	給電中（802.3af 対応の受電デバイス検出）。
		橙	点滅	PoE ポートエラー。 IEEE 802.3af 非対応の受電デバイスの接続、IEEE 802.3af 低電流状態（電流 Imin 以下）、IEEE 802.3af 過電流状態（電流 I cut 以上）、ハードウェアエラーによりポート動作不能、供給可能電力超過、ショート検出、低電流・過電流の反復によるポートシャットダウン（受電デバイスの DC/DC エラーによるもの）等。
		ー	消灯	給電なし（受電デバイスの検出なし、または接続なし）。
10GE ポート LED		緑	点灯	ポートにリンクが確立されていることを示します。
		緑	点滅	ポート上の動作（データ転送）を示します。
		ー	消灯	リンク / 動作のないことを示します。
Combo SFP LED		コンボポート用の LED はポート上部に位置し、Combo 1、Combo 2、Combo 3、Combo 4 と番号が振られています。		
		緑	点灯	リンクが確立しています。
		緑	点滅	ポート上の動作（データ転送）を示します。
		ー	消灯	リンク / 動作のないことを示します。

背面パネル

電源コネクタは、標準の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、電源プラグをコンセントに接続します。スイッチは供給電圧が 100~240VAC、50~60Hz の間であれば自動的に電源設定を調整します。

背面パネルには、電源コネクタ、システムファン通気口、リダンダント電源コネクタ、さらにオプションの 10GE モジュール挿入用の 2 つの空きスロットがあります。電源に異常が発生した際には、オプションの外付けリダンダント電源システムがリダンダント電源コネクタに接続されていれば、瞬時かつ自動的にスイッチへの電源供給を開始します。

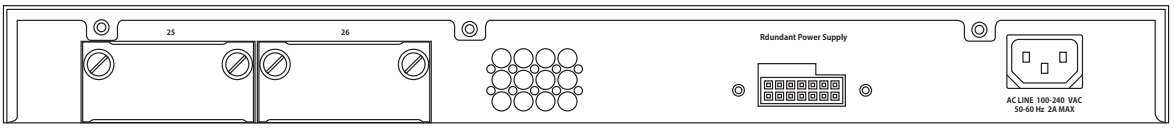


図 1-3　DWS-4026 背面パネル図

側面パネル

スイッチの両側に位置するシステムファンと排熱用通気口によって熱を放出するため、通気口を塞がないように注意してください。十分な通気のためには、装置の背面と側面には最低でも 15 センチ以上の空間を保つようにしてください。適切な熱放出、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可能性があります。

第 2 章　スイッチ管理の導入

本章では、製品の起動と、ユーザインタフェースへのアクセス方法について説明します。以下の項で構成されています。

- スイッチのネットワークへの接続
- 端末をコンソールポートに接続する
- ユーザインタフェースについて

スイッチのネットワークへの接続

物理的なハードウェアの設置の完了後、SSH、Telnet、Web ブラウザ、または SNMP を経由したスイッチのリモート管理を有効にするためには、スイッチをネットワークに接続する必要があります。
スイッチの管理インタフェースの IP アドレスとサブネットの初期値は「10.90.90.90/255.0.0.0」で、DHCP は無効になっています。DHCP を有効にしたい場合や、違う固定 IP アドレスを割り当てる場合は、スイッチに接続して、初期設定を変更する必要があります。

スイッチへの接続は、Telnet 経由や、「10.90.90.90/255.0.0.0」と同一のネットワークにあるホストの Web ブラウザを経由して行います。またはスイッチのコンソールポート（RS-232C DCE）を使用する方法もあります。スイッチと接続し、ネットワーク情報の設定や、DHCP クライアントの設定が可能です。

10.0.0.0 ネットワーク上のホストからスイッチに接続するためには、スイッチの IP アドレスの初期値「10.90.90.90」を Web ブラウザまたは Telnet クライアントのアドレスフィールドに入力します。

端末をコンソールに接続する

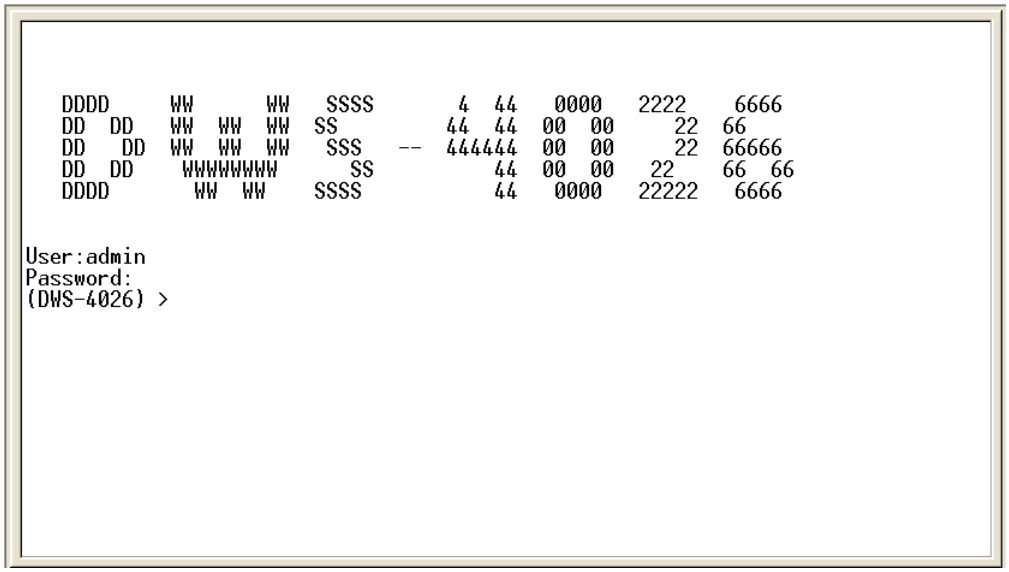
コンソールポートを使用したネットワーク情報の設定は、以下の手順で行います。

1. モデムケーブルを使用して、VT100/ANSI 端末かワークステーションをコンソール（シリアル）ポートに接続します。
PC、Apple や UNIX のワークステーションと接続する場合は、ハイパーターミナルなどの端末エミュレーションプログラムを起動してください。

2. 端末エミュレーションプログラムの設定を以下に合わせてください。
- データ速度 : 115,200bps
- データビット : 8
- パリティ : なし
- ストップビット : 1
- フロー制御 : なし

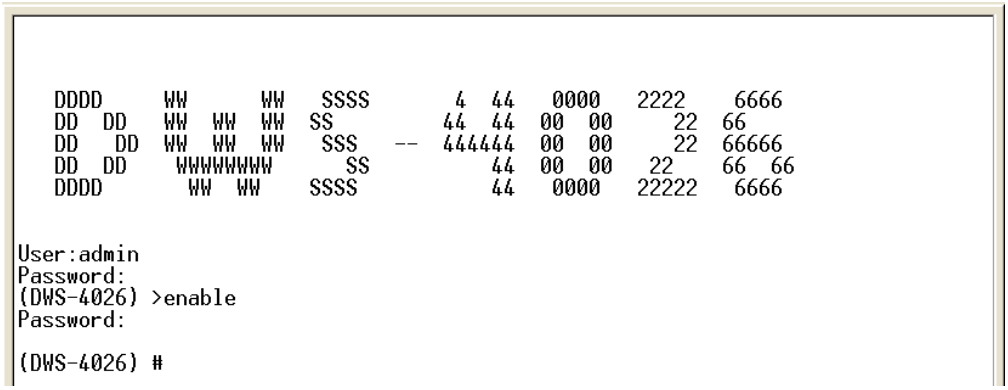
3. 「Enter」キーを押すと「User:」プロンプトが表示されます。
ユーザ名に「**admin**」と入力してください。パスワードの初期設定はありません。パスワードの設定を行わない場合は、パスワードプロンプトが表示されたら「Enter」キーを押してください。

ログインに成功すると、画面のプロンプトが 「(DWS-4026)>」に変わります。



4. Privilege EXEC コマンドモードに遷移するために、「(DWS-4026)>」プロンプトの後に「**enable**」と入力します。Privilege EXEC コマンドモード用のパスワードの初期設定はありません。パスワードを変更しない場合は、パスワードプロンプトで「Enter」キーを押してください。

コマンドプロンプトは「(DWS-4026)#」に変わります。

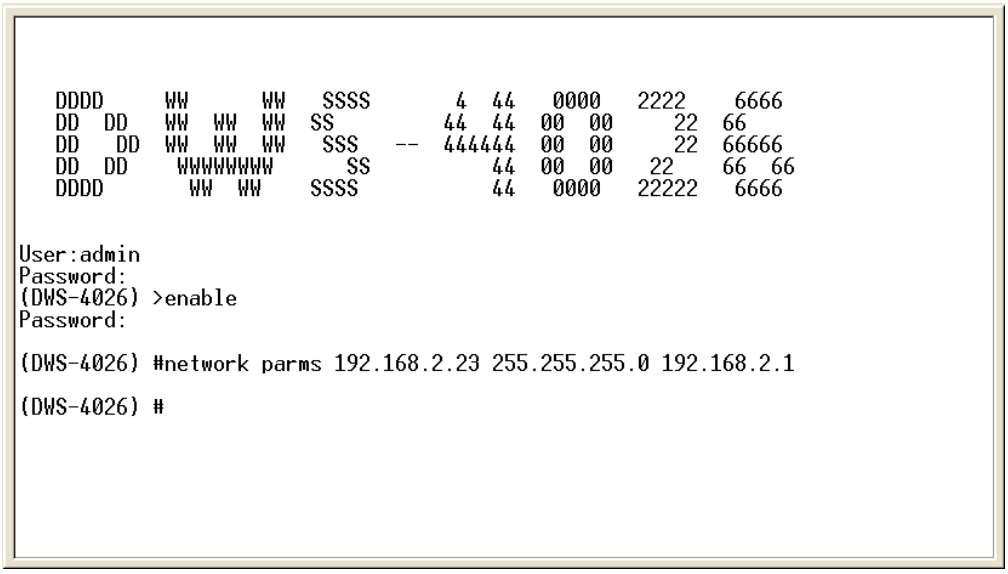


5. ネットワーク情報を登録します。

- DHCP サーバを使用して、IP アドレス、サブネットマスク、デフォルトゲートウェイ情報を取得するためには「**network protocol dhcp**」と入力します。
- BootP サーバを使用して、IP アドレス、サブネットマスク、デフォルトゲートウェイ（オプション）情報を取得するためには「**network protocol bootp**」と入力します。
- IP アドレス、サブネットマスク、デフォルトゲートウェイ情報を手動で登録するためには、「**network parms** <IP アドレス > < サブネットマスク > [< ゲートウェイ >]」の順で入力します。

例

```
network parms 192.168.2.23 255.255.255.0 192.168.2.1
```



- IPv6 アドレス、サブネットマスク、デフォルトゲートウェイ（オプション）情報を手動で登録するためには、「**network ipv6 address** < アドレス >< プレフィックス長 >**[eui64] network ipv6 gateway** < ゲートウェイ >」の順で入力します。

デフォルトゲートウェイ情報は任意のパラメータなので、デフォルトゲートウェイアドレスは省略可能です。

ネットワーク情報を確認するためには「**show network**」と入力します。

```
(DWS-4026) #show network

Interface Status.............................. Always Up
IP Address.................................... 192.168.2.23
Subnet Mask................................... 255.255.255.0
Default Gateway............................... 192.168.2.1
IPv6 Administrative Mode...................... Enabled
IPv6 Prefix is ............................... FE80::217:9AFF:FE95:2A7C/64
Burned In MAC Address......................... 00:17:9A:95:2A:7C
Locally Administered MAC address.............. 00:00:00:00:00:00
MAC Address Type.............................. Burned In
Network Configuration Protocol Current........ None
Management VLAN ID............................ 1

(DWS-4026) #_
```

6. これらの設定を保存し、スイッチのリセット時も保持されるようにするためには、以下のコマンドを入力します。

```
copy system:running-config nvram:startup-config
```

または、以下のコマンドを入力します。

```
write memory
```

一度スイッチがネットワークに接続すると、IP アドレスを使用して、Web ブラウザ、または Telnet、SSH を経由してスイッチにリモートアクセスが可能になります。

ユーザインタフェースについて

本システムでは、以下の 3 つの方法を使用して、システムを設定および監視するために包括的な管理を行います。

- Web ユーザインタフェース
- コマンドラインインタフェース（CLI）
- 簡易ネットワーク管理プロトコル（SNMP）

標準に準拠した各管理方法により、D-Link ソフトウェアの設定および管理を行うことができます。システムの管理方法については、ネットワークの規模や要件、およびご希望により選択してください。

ここでは、Web ベースのインタフェースを使用してシステムの管理および監視を行う方法について説明します。CLI を使用してシステムの保守管理をする方法についての情報は「D-Link CLI MANUAL」を参照してください。

Web ベースの管理について

本スイッチのすべてのソフトウェア機能は、実装されている Web ベース（HTML）インタフェース（以降、Web マネージャと記載）経由で管理、設定およびモニタできます。ブラウザを使用してネットワーク上のリモートステーションから本スイッチを管理できます。

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

Web ブラウザから本スイッチにアクセスするためには、操作をする PC に以下のソフトウェアが必要です。

- HTML バージョン 4.0 以上
- HTTP バージョン 1.1 以上
- JavaScriptTM バージョン 1.5 以上

Web マネージャへのログイン

Web ブラウザからスイッチにアクセスするためには、操作をする PC に以下のソフトウェアが必要です。

- Internet Explorer 6.0 以降

以下の手順で Web インタフェースにログインしてください。

1. Web ブラウザを起動し、「アドレス」欄にスイッチの IP 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。

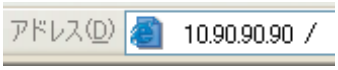


図 2-1　アドレス入力

2. 表示されたダイアログボックスに、「User Name」（ユーザ名）および「Password」（パスワード）を入力し、「Login」ボタンをクリックします。

図 2-2　ログイン

参照　ユーザ名とパスワードはコマンドライン・インタフェースにログインする際に使用するものと同じです。初期値ではユーザ名が「admin」、パスワードは設定されていません。パスワードの大文字、小文字は区別されます。

3. システムから認証を受けると、「System Description」画面が表示されます。

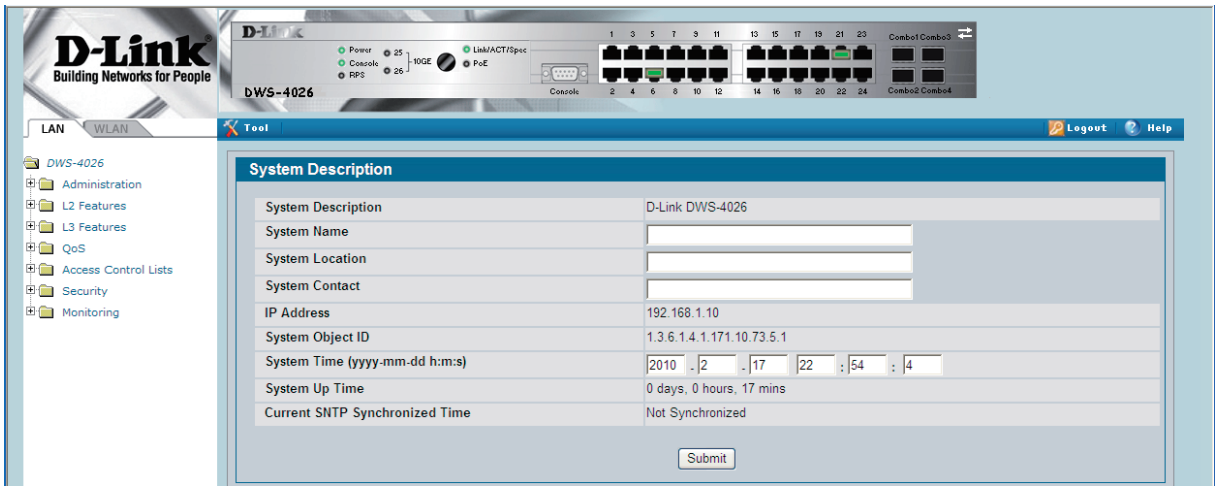


図 2-3　初期画面

図 2-4 に D-Link 統合スイッチの Web インタフェースのレイアウト例を示します。ページは「インタフェース構成図」、「ナビゲーションツリー」、「設定状況・オプション」の 3 つのメインエリアから構成されています。

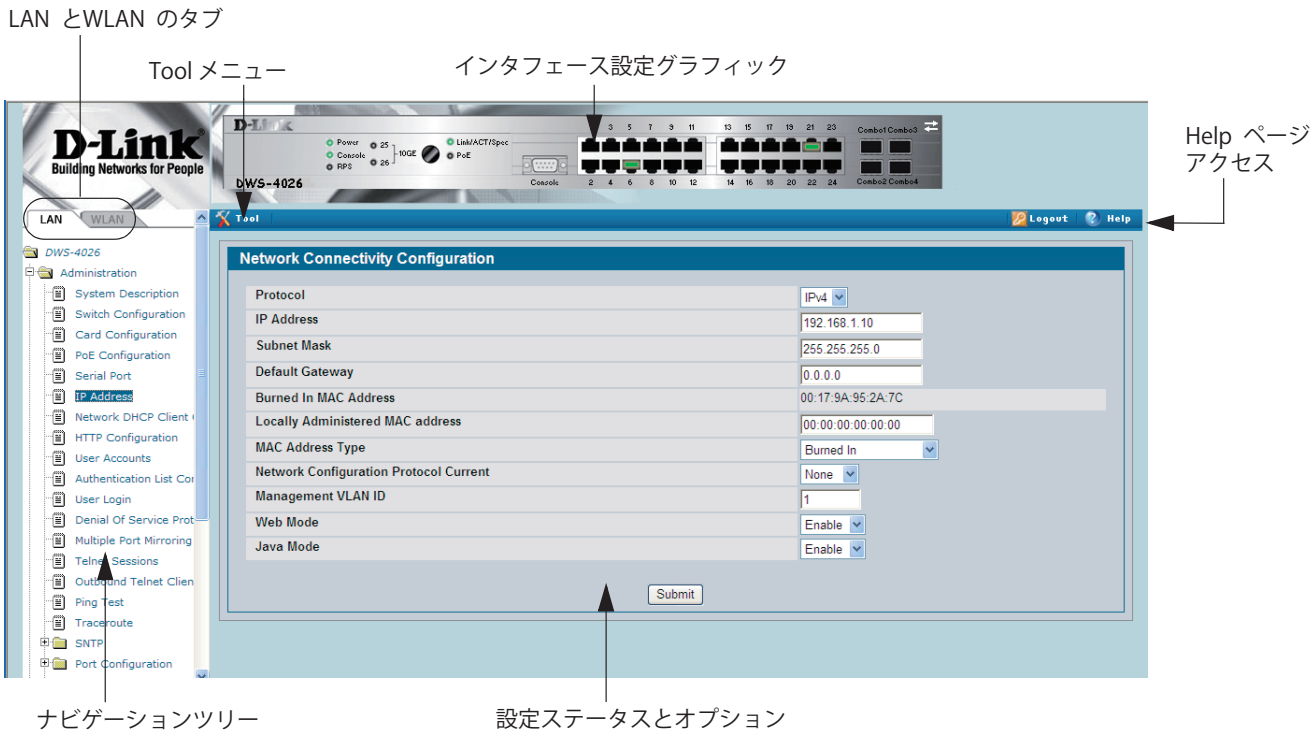


図 2-4　Web インタフェースのレイアウト

インタフェース設定グラフィック

「インタフェース設定グラフィック」は Java™ アプレットで、D-Link 統合スイッチ上のポートを図示します。この図は各ページの上部に表示され、ここからも設定およびモニタリングオプションへと移行できるように設計されています。

確認や設定を行いたいポートをクリックすると、統計や設定オプションなどのメニューが表示されます。目的のメニューをクリックし、設定やモニタリングをするページへと移行します。

「Logout」ボタンをクリックし、スイッチの Web インタフェースからログアウトします。Logout プロンプトで「OK」をクリックして、変更を保存して、適用します。変更を保存しない場合は「Cancel」をクリックして、Web インタフェースをクローズします。

グラフィック部分の、ポート以外の場所をクリックすると、メインメニューが表示されます。このメニューの内容は、ページ左側に表示される、ナビゲーションメニューと同じです。

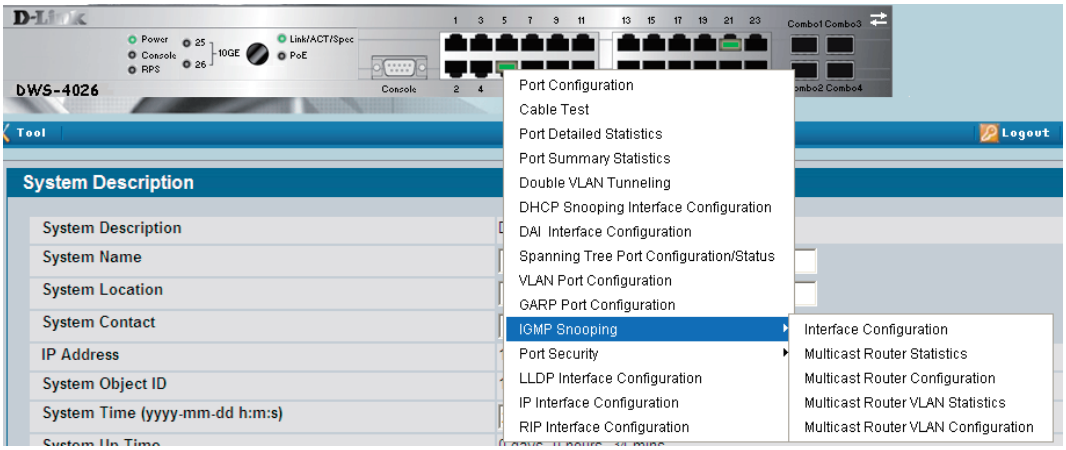


図 2-5　カスケード形式のナビゲーションメニュー

ナビゲーションメニュー

画面左側に階層型のツリー構造が表示されます。ツリー構造はフォルダ、サブフォルダ、および設定と状態表示をする HTML ページで構成されます。フォルダをクリックするとフォルダの内部が表示されます。各フォルダはサブフォルダまたは HTML ページ、またはその両方を格納しています。

図 2-6 にナビゲーションメニュー内のフォルダ、サブフォルダ、HTML ページの例を示します。左側に「+」マークのあるフォルダまたはサブフォルダをクリックすると、フォルダの内容が表示されます。HTML ページをクリックすると、メインフレーム内に新しいページが表示されます。フォルダやサブフォルダをクリックしても新しいページは表示されません。

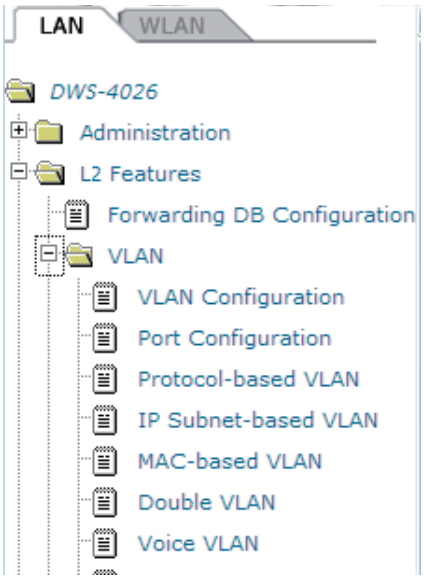


図 2-6　階層型ツリー構造のナビゲーションメニュー

設定・モニタリングオプション

画面中、インタフェース構成図の下、ナビゲーションメニューの右側には、選択したページの設定情報または現在の状況が表示されます。設定オプションが表示されるページでは、フィールド内に入力したり、プルダウンメニューを選択するなどの操作を行います。

各ページには HTML ベースのヘルプが用意されており、フィールドや設定オプションの詳細などを確認することができます。多くのページにはコマンドボタンも用意されています。

以下のコマンドボタンは、Web インタフェースのどのページにも表示されます。

項目	説明
Submit	更新した設定内容がスイッチに送信されます。設定の変更は直ちに行われますが、設定事項の中には電源をオフにすると失われてしまうものがあります。そのような設定は事前にシステムコンフィグレーションファイルに保存しておく必要があります。
Save	現在の設定内容をシステムコンフィグレーションファイルに保存します。このボタンを押すと、スイッチに送信した変更内容は、システムのリブートを行った後にも保存されます。設定の保存には「Tool」メニュー中の「Save Changes」を使用することもできます。
Refresh	画面上のデータを更新します。

「WLAN」タブ

WLAN フォルダのページには、操作を簡単にし、共通の機能をグループ化するためにタブが用意されています。タブをクリックして目的のページにアクセスします。

ツールメニュー

「Tool」アイコンをマウスでクリックすると、以下の便利なシステムツールが表示されます。

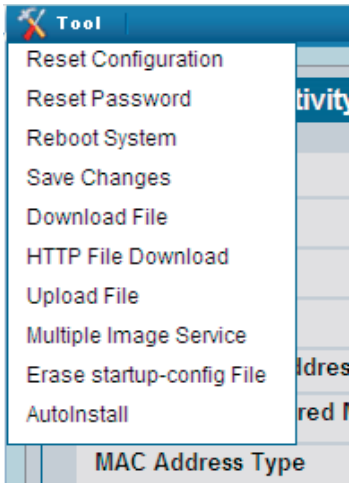


図 2-7　ツールメニュー

項目	説明
Reset Configuration	工場出荷時設定に戻します。
Reset Password	パスワードをリセットします。
Reboot System	本製品をリブートします。
Save Changes	設定を本製品に保存します。
Download File	設定内容のバックアップをします。
Upload File	設定内容をリストアします。
Multiple Image Service	設定ファイルを変更します。
Erase startup-config File	不揮発性メモリに保存されているテキストベースのコンフィグレーションファイルを削除します。
Autoinstall	本製品起動時にメモリにコンフィグレーションファイルがない場合に、スイッチのコンフィグレーションを自動的に有効にします。

リスト表示されている各ツールをクリックすると、それぞれの操作をする Web ページに移動します。

コマンドラインインタフェースを使用する

コマンドラインインタフェース（CLI）とは、テキストベースのコマンドを入力することにより、システムの管理と監視をする方法です。CLI はダイレクトシリアル接続、または Telnet や SSH を経由してリモートから論理接続することができます。

CLI では、コマンドを機能によってモードで分類しています。コマンドモードによりサポートするコマンドが異なります。つまり、あるコマンドは、ある特定のモードに遷移した状態でないと実行することができません。ただし、User EXEC モードのコマンドはすべて Privilege EXEC モードで実行することができます。

現在のモードで使用可能なコマンドを確認するためには、コマンドプロンプトの後に、クエスチョンマーク「?」を入力します。使用可能なコマンドのキーワードやパラメータを確認するためには、コマンドプロンプトの後にタイプしたテキストの後に、クエスチョンマーク「?」を入力します。追加するコマンドキーワードやパラメータがない場合、または追加のパラメータが任意である場合、以下のメッセージが表示されます。

```
<cr>            Press Enter to execute the command
```

CLI についての詳細は、本製品付属の CD-ROM に収録の「D-Link CLI MANUAL」をご参照ください。

「D-Link CLI MANUAL」には CLI で使用するコマンドがリスト形式で掲載されています。リストには、コマンド名ごとの簡単な説明と以下の情報が記されています。

- コマンドキーワードと必須および任意のパラメータ
- コマンドを実行するモード
- 初期値（設定されている場合）

show コマンドで表示する情報の内容は、「D-Link CLI MANUAL」中の show コマンドのページで参照することができます。

SNMP を使用する

D-Link 統合スイッチのソフトウェアは SNMP モジュールを実装し、SNMP グループやユーザの設定を行い、SNMP エージェントが送信するトラップの管理をすることができます。

D-Link 統合スイッチは、標準的な機能をカバーするパブリック MIB と、さらにスイッチが提供する追加機能を実現させるプライベート MIB の両方をサポートしています。すべてのプライベート MIB はプレフィックス「DLINK-」で始まります。インタフェースコンフィグレーションのメインオブジェクトはプライベート MIB である、「DLINK-SWITCHING-MIB」に存在します。パブリック MIB や IF-MIB のオブジェクトにもインタフェースコンフィグレーションは含まれます。

SNMP は初期状態で有効になっています。スイッチにアクセスする SNMP マネージャの設定をするために必要な情報は、Web インタフェースにログインすると最初に表示される「System Description」画面と、「show sysinfo」コマンドで参照することができます。

すべてのユーザは SNMPv3 プロトコルを利用してスイッチに接続することができます。しかし、認証および暗号化の設定のために、新規にユーザプロファイルの作成をする必要があります。CLI を使用してプロファイルを作成するためには、「D-Link CLI MANUAL」の SNMP の項を参照してください。Web インタフェースを用いる場合には、以下の手順に従い行ってください。

第 3 章　システム管理

スイッチ情報へのアクセス、IP アドレス、ユーザアカウント、システムログ、システム時刻、SNMP などの本製品のシステム設定について説明します。

設定項目	説明	参照ページ
ARP キャッシュの参照	本製品が学習した ARP キャッシュを参照します。	23 ページ
搭載資源の参照	不揮発性メモリに保存されている製品データを表示します。	23 ページ
デュアルイメージ状態の参照	デバイスのシステムイメージに関する情報を表示します。	24 ページ
システム説明の設定	一般的なデバイス情報の設定と参照を行います。	25 ページ
スイッチの設定	ブロードキャスト、マルチキャスト、ユニキャストストームリカバリ機能、および IEEE 802.3x フローコントロールなどの機能を設定します。	26 ページ
カードの設定	スロットに挿入したカード情報を表示します。	27 ページ
PoE 設定	Power over Ethernet（PoE）機能を設定します。	28 ページ
PoE ステータス	PoE のステータスを表示します。	29 ページ
シリアルポートの設定	スイッチのシリアルポート設定を変更します。	29 ページ
IP アドレス設定	IP 情報を変更します。	30 ページ
DHCP クライアントオプション	リースをリクエストする場合にスイッチの DHCP クライアントが DHCP サーバに送信するベンダのクラス識別子情報を設定、および有効にします。	31 ページ
HTTP 設定	HTTP サーバを設定します。	32 ページ
ユーザアカウントの設定	ユーザアカウントの追加、編集を行います。	33 ページ
認証リストの設定	ログインリストを設定します。	36 ページ
認証リストのサマリ	システム上の認証リスト、または 802.1X ポートセキュリティユーザに関する情報を表示します。	38 ページ
ログインセッション	スイッチにログインしているユーザに関する情報を参照します。	38 ページ
ユーザログイン	スイッチのログインリストにユーザを割り当てます。	39 ページ
DoS 設定	DoS の制御を設定します。	40 ページ
フォワーディングデータベースの設定と検索	フォワーディングデータベースの設定と検索を行います。	41 ページ
ログの管理	ログの参照、またはログの管理ステータスと動作の設定を行います。	42 ページ
Telnet セッション	内向きの Telnet 設定を行います。	49 ページ
アウトバウンド Telnet クライアント設定	アウトバウンド Telnet クライアント設定を使用して、リモートシステムに接続する Telnet セッションを制御します。	50 ページ
Ping テスト	指定した IP アドレスに Ping 要求を送信します。	50 ページ
SNTP 設定	SNTP サーバ、タイムゾーン、サマータイムを設定します。	51 ページ
デバイススロット情報の設定と参照	スイッチのスロットにインストールされたカード情報の表示、スロットに関する情報の設定を行います。	59 ページ
デバイスポート情報の設定と参照	スイッチで有効なポートの物理ポート情報を参照またはモニタします。	61 ページ
マルチプルポートミラーリング	ポートミラーリングセッションを定義します。	66 ページ
sFlow の設定	sFlow の設定を行います。	69 ページ
SNMP パラメータの定義	SNMP パラメータの定義を行います。	73 ページ
システム統計情報の参照	スイッチが送受信したトラフィック量とタイプに関する様々な情報を表示します。	77 ページ
システムのユーティリティの使用	スイッチの管理を補助するユーティリティを設定します。	84 ページ
DHCP サーバの管理	DHCP パラメータとデータを定義します。	94 ページ
DNS クライアントの設定	DNS サーバの情報の設定、およびスイッチ / ルータが DNS クライアントとして動作する方法を設定します。	101 ページ
ISDP 情報の設定と参照	ISDP 情報の設定と参照を行います。	104 ページ

ARP キャッシュの参照

ARP キャッシュは、ネットワークの各ステーション内にローカルに保持されているテーブルです。ARP キャッシュエントリは、ARP リクエストまたは ARP 応答に関わらず、ARP パケットペイロードフィールドの送信元情報を検証することによって学習されます。そのため、ARP リクエストが LAN セグメントまたは仮想 LAN（VLAN）上のすべてのステーションにブロードキャストされる場合、すべての受信者には、それぞれの ARP キャッシュにある送信元の IP および MAC アドレスを保存する機会があります。ユニキャストである ARP の応答は、通常、ARP キャッシュにある送信元情報を保存するリクエストを行った送信者にだけ参照されます。新しい情報は、常に ARP キャッシュにある既存のコンテンツと置き換えられます。

ARP キャッシュは 1024 個のエントリをサポートしており、このサイズは 1024 未満の任意の値に設定することができます。ルータなどのようにデバイスが複数のネットワークインタフェースをサポートしている場合、単一の ARP キャッシュがすべてのインタフェースに使用されるか、または個別のキャッシュがインタフェース単位で維持されます。後者の手法は、ネットワークのアドレス指定がインタフェースごとにユニークでない場合に役に立ちますが、単一の ARP キャッシュを採用しているようなイーサネットの MAC アドレス指定には適当ではありません。

LAN タブ > Monitoring > ARP Cache の順にメニューをクリックし、システムの ARP キャッシュを表示します。

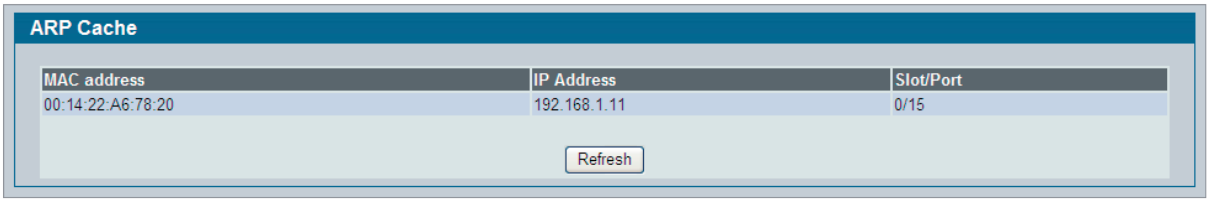


図 3-1　ARP Cache 画面

本画面には次の項目があります。

項目	説明
MAC address	ARP キャッシュ内のシステムの物理（MAC）アドレスを表示します。
IP address	システムの MAC アドレスに割り当てられる IP アドレスを表示します。
Slot/Port	接続に使用されているスロット、およびポート番号を表示します。

「Refresh」ボタンをクリックして、ページを再読み込みして、本画面を更新します。

搭載資源の参照

本画面を使用して、工場出荷時に不揮発性メモリに保存されているスイッチに不可欠な製品データを表示します。

LAN タブ > Monitoring > Inventory Information の順にメニューをクリックし、搭載資源情報を表示します。

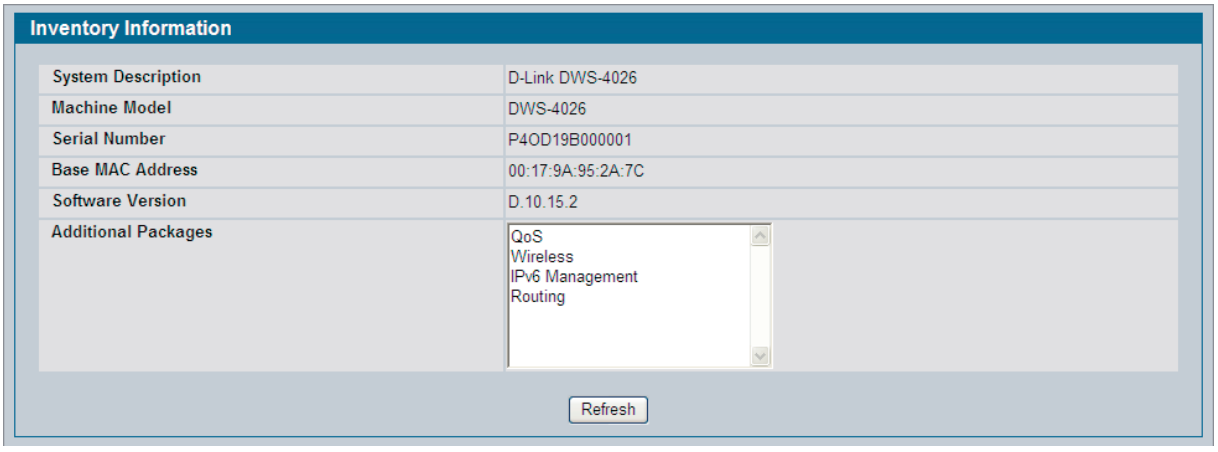


図 3-2　Inventory Information 画面

デュアルイメージ状態の参照

デュアルイメージ機能により、スイッチは不揮発性記憶装置に 2 つの D-Link ソフトウェアイメージを持つことができます。1 つのイメージがアクティブなイメージで、2 つ目のイメージはバックアップです。本機能はアップグレードとダウングレードの間のシステムダウン時間を短縮します。「Dual Image Status」画面を使用して、デバイスのシステムイメージに関する情報を参照することができます。

LAN タブ > Monitoring > Dual Image 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。

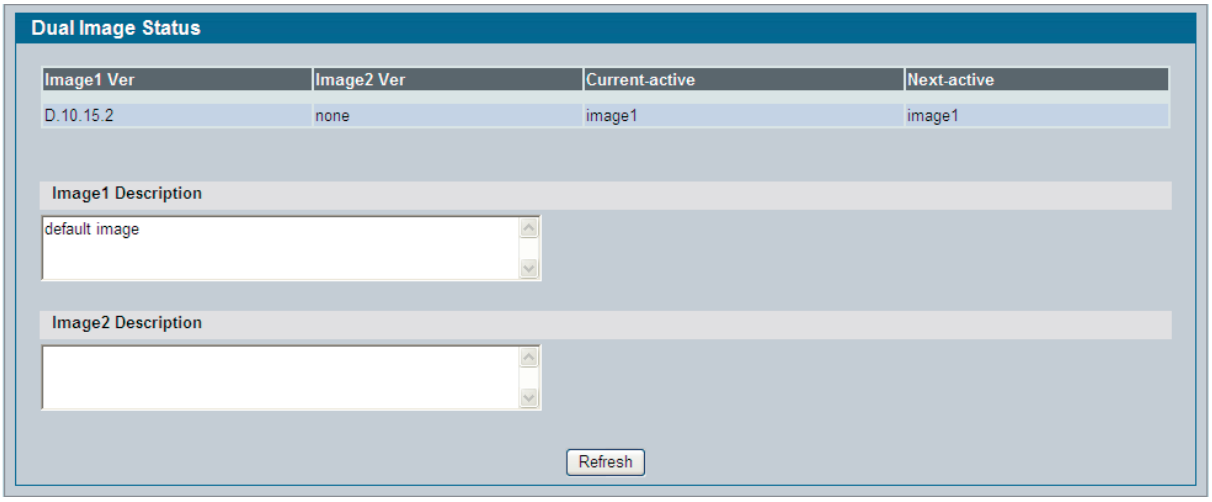


図 3-3　Dual Image Status 画面

本画面には次の項目があります。

項目	説明
Unit	スイッチのユニット番号を表示します。
Image1 Ver	image1 のソフトウェアファイルのバージョンを表示します。
Image2 Ver	image2 のソフトウェアファイルのバージョンを表示します。
Current-active	本ユニットにおける現在のアクティブなイメージを表示します。
Next-active	このユニットの次の再起同時に使用されるイメージを表示します。
Image1 Description	image1 のソフトウェアファイルに関連する説明を表示します。
Image2 Description	image2 のソフトウェアファイルに関連する説明を表示します。

「Refresh」ボタンをクリックし、システムの情報を最新に更新します。

システム説明の設定

ログイン成功後に、システム説明画面を表示します。本画面を使用して一般的なデバイス情報の設定と参照を行います。

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

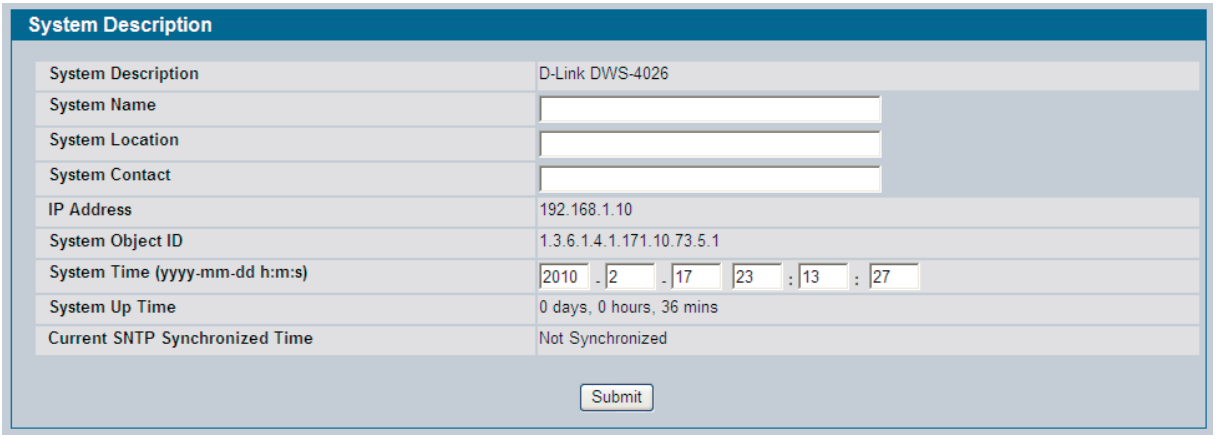


図 3-4　System Description 画面

本画面には次の項目があります。

項目	説明
System Description	本スイッチの製品名。
System Name	本スイッチを特定する識別名を入力します。半角英数字 31 文字以内。初期値では空白です。
System Location	スイッチの場所を入力します。半角英数字 31 文字以内。初期値では空白です。
System Contact	本スイッチ管理用の連絡窓口を入力します。半角英数字 31 文字以内。初期値では空白です。
IP Address	ネットワークインタフェースに割り当てられている IP アドレス。 IP アドレスを変更するためには、「シリアルポートの設定」（29 ページ）を参照してください。
System Object ID	スイッチのエンタプライズ MIB 用のオブジェクト ID。
System Time (yyyy-mm-dd h:m:s)	システム搭載のリアルタイムクロックを使用することでスイッチの現在の日時を指定します。
System Up Time	スイッチの最後の再起動からの時間（日、時間、分）を表示します。
Current SNTP Synchronized Time	現在同期している UTC の SNTP 時間を表示します。SNTP サーバが設定されておらず、時間が同期していない場合、本欄は「Not Synchronized」と表示されます。SNTP サーバを指定するためには、「SNTP の設定」（51 ページ）を参照してください。

システム情報の定義

1. 「System Description」画面を表示します。
2. 「System Name」、「System Contact」、「System Location」欄を定義します。
3. 「Submit」ボタンをクリックします。システム設定は適用され、デバイスは更新されます。

注意　再起動後も新しい値をスイッチに保持する場合、保存を行う必要がありますが、システム時間は保存する必要はありません。

スイッチの設定

スイッチにブロードキャスト、マルチキャスト、ユニキャストストームリカバリ機能、および IEEE 802.3x フローコントロール機能を設定します。

IEEE 802.3x フローコントロールは、ポート参照の申し込みが超過するようになるとポートを一時停止して、輻輳状態におけるわずかなバースト時間のトラフィックをすべて廃棄することで行われます。これにより高い優先度および(または)ネットワーク制御トラフィックの損失を引き起こします。802.3x フローコントロールが有効な場合、高速のスイッチがパケットの送信を控えるように要求されることで、低速のスイッチは、高速のスイッチと通信できるようになります。伝送は、バッファオーバフローを防止するために一時停止されます。

LAN タブ > Administration > System 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。

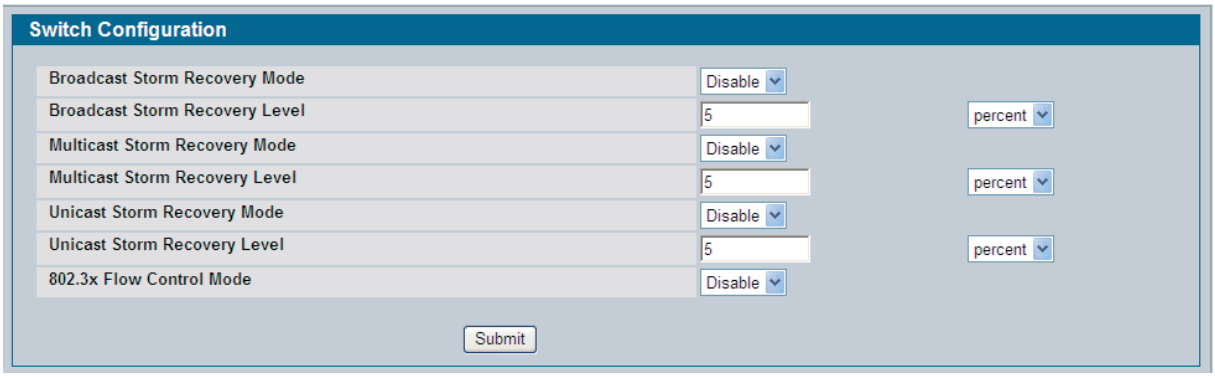


図 3-5　Switch Configuration 画面

本画面には次の項目があります。

項目	説明
Broadcast Storm Recovery Mode	以下の 1 つを選択し、本オプションを有効または無効にします。 • Enable - イーサネットポートにおいてブロードキャストトラフィックが、設定したしきい値を超過した場合、スイッチはブロードキャストトラフィックを防御（廃棄）します。 • Disable - イーサネットポートにおいてブロードキャストトラフィックが、設定したしきい値を超過しても、スイッチはブロードキャストトラフィックを防御しません。工場出荷時設定は「Disable」（無効）です。
Broadcast Storm Recovery Level	ストーム制御がアクティブになるデータ速度を指定します。値は、ポートスピードの割合であり、0-100 で指定します。初期値はポートスピードの 5% です。
Multicast Storm Recovery Mode	以下の 1 つを選択し、本オプションを有効または無効にします。 • Enable - イーサネットポートにおいてマルチキャストトラフィックが設定したしきい値を超過した場合、スイッチはマルチキャストトラフィックを防御（廃棄）します。 • Disable - イーサネットポートにおいてマルチキャストトラフィックが設定したしきい値を超過しても、スイッチはマルチキャストトラフィックを防御しません。工場出荷時設定は「Disable」(無効) です。
Multicast Storm Recovery Level	ストーム制御がアクティブになるデータ速度を指定します。値は、ポートスピードの割合であり、0-100 で指定します。初期値はポートスピードの 5% です。
Unicast Storm Recovery Mode	以下の 1 つを選択し、本オプションを有効または無効にします。 • Enable - イーサネットポートにおいてユニキャストトラフィックが、設定したしきい値を超過した場合、スイッチはユニキャストトラフィックを防御（廃棄）します。 • Disable - イーサネットポートにおいてユニキャストトラフィックが、設定したしきい値を超過しても、スイッチはユニキャストトラフィックを防御しません。工場出荷時設定は「Disable」(無効) です。
Unicast Storm Recovery Level	ストーム制御がアクティブになるデータ速度を指定します。値は、ポートスピードの割合であり、0-100 で指定します。初期値はポートスピードの 5% です。
802.3x Flow Control Mode	システムにおける IEEE 802.3x フローコントロールを有効または無効にします。工場出荷時設定は「Disable」(無効) です。 • Enable - フローコントロールを有効にすると、スイッチは、より高速のスイッチと通信できるようになります。 • Disable - フローコントロールを無効にすると、スイッチは、ポートバッファがフル状態になるとポーズパケットを送信しません。

設定を変更した場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。再起動後も新しい値をスイッチに保持する場合、保存を行う必要があります。

カードの設定

スイッチに設定済みのカードの情報を参照します。

LAN タブ > Administration > System Card の順にメニューをクリックし、以下の画面を表示します。ここでは、スロットに挿入したカード情報について表示します。

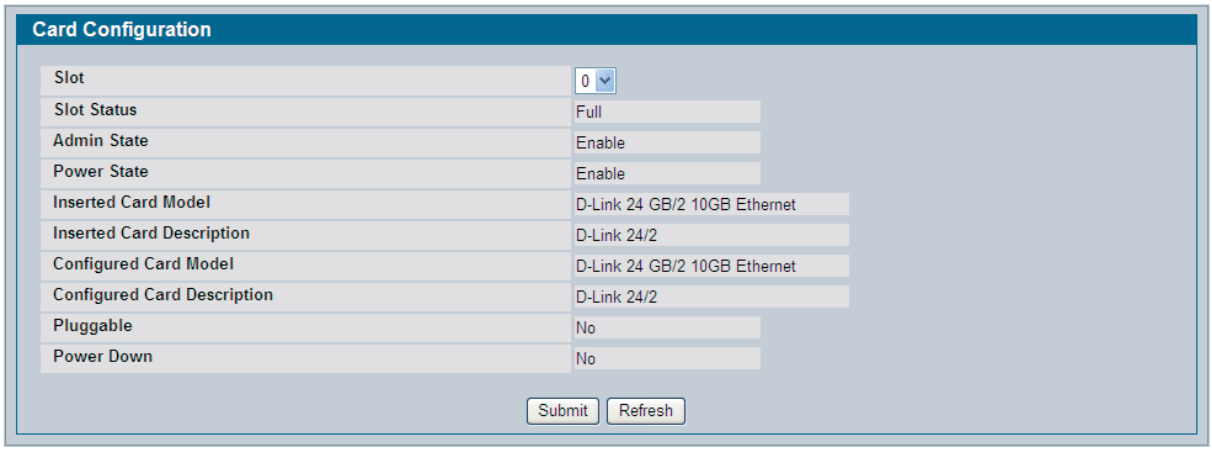


図 3-6　Card Configuration 画面

本画面には次の項目があります。

項目	説明
Slot	データを表示する選択ユニットのスロットを選択します。
Slot Status	カードがスロットにあるか否かを表示します。「Full」（挿入済み）、「Empty」（空）。
Admin State	スロットが管理上有効または無効であるかを表示します。読取専用ユーザは、本項目を設定することはできません。
Power State	スロットの電源状態「Enable」（オン）または「Disable」（オフ）を表示します。読取専用ユーザは、本項目を設定することはできません。
Card Type	スロットに挿入可能なサポートするカードの種類を表示します。これは、カードが挿入されておらず、まだ設定をしていないスロットに対してだけ参照することができます。読取専用ユーザは、本項目を参照することはできません。
Inserted Card Model	選択スロットに挿入されているカードのモデル識別子を表示します。カードが挿入されていないと、本項目は表示されません。
Inserted Card Description	選択スロットに挿入されているカードの説明文を表示します。カードが挿入されていないと、本項目は表示されません。
Configured Card Model	選択スロットに設定済みのカードモデルの識別子を表示します。事前に設定したカードがないと、本項目は表示されません。
Configured Card Description	選択スロットに設定済みのカードの説明文を表示します。事前に設定したカードがないと、本項目は表示されません。
Pluggable	指定スロットの挿入可能状態を表示します。
Power Down	指定スロットの電源状態を表示します。

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。

PoE 設定

Power over Ethernet（PoE）機能を設定します。

LAN タブ > Administration > PoE 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。

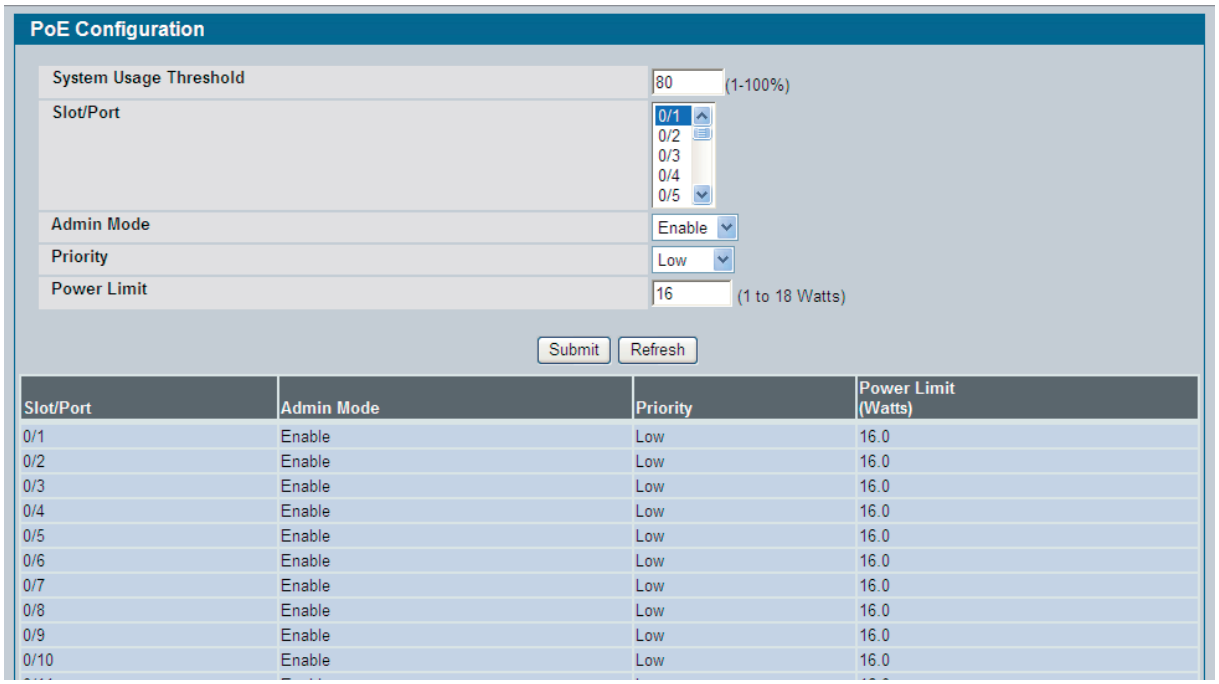


図 3-7　PoE Configuration 画面

本画面には次の項目があります。

項目	説明
System Usage Threshold	総消費電力が利用可能な総電力値の指定の割合以上である場合にトラップが送信されるしきい値レベルを設定します。
Slot/Port	情報を設定するスロットとポートを選択します。
Admin Mode	ポートの電力供給を有効または無効にします。
Priority	スイッチはすべての接続デバイスに電力を供給することはできません。そのため、優先度を使用し、電力を供給するポートを決定します。同じ優先度を持つポートの場合、低い番号のポートが高い優先度を持ちます。
Power Limit	ポートが提供できる最大電力を定義します。

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。

PoE ステータス

PoE 技術を使用することで、IP 電話、無線 LAN アクセスポイント、Web カメラ、および他の多くの装置は、既存のイーサネットインフラを変更せずに、既存の LAN ケーブルを経由してデータと共に電力を受信することができます。

PoE のステータスを表示します。

LAN タブ > Monitoring> PoE 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。

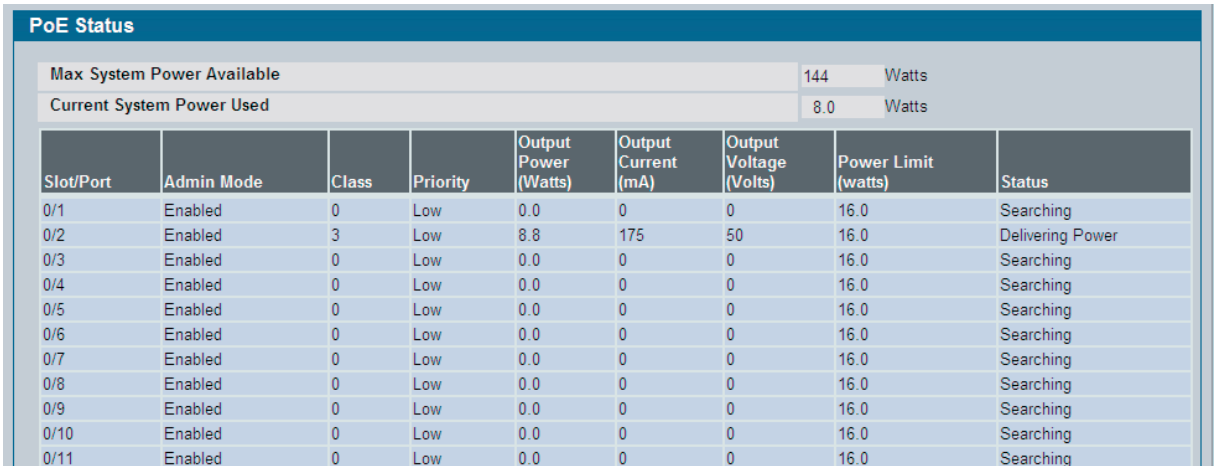


図 3-8　PoE Status 画面

シリアルポートの設定

スイッチのシリアルポート設定を変更します。端末または端末エミュレータがスイッチと通信するためには、両方のデバイスのシリアルポート設定は同じである必要があります。

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

図 3-9　Serial Port Configuration 画面

本画面には次の項目があります。

項目	説明
Serial Port Login Timeout (minutes)	スイッチが接続を終了する前にシリアルポート接続に起こる無通信の時間を指定します。0-160（分）で値を指定します。初期値は 5（分）です。0 を入力するとタイムアウトは発生しません。
Baud Rate (bps)	スイッチのシリアルポートのボーレートを指定します。初期値は 115200 です。
Character Size (bits)	データビット数。常に 8 です。
Flow Control	ハードウェアのフローコントロールを有効または無効にします。常に「Disabled」（無効）です。
Stop Bits	1 文字あたりのストップビット数。常に 1 です。
Parity	シリアルポートで使用されるパリティ方式。常に「None」です。

データを変更した場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。再起動後も新しい値をスイッチに保持する場合、保存を行う必要があります。

IP アドレス設定

ネットワークインタフェースは、スイッチの前面パネルにあるポートのいずれかを経由してスイッチとのインバンド接続に使用される論理インタフェースです。スイッチのネットワークインタフェースに関連する設定項目は、トラフィックがスイッチまたは送信される前面パネルポートの設定に影響しません。ここでは、Web インタフェースを使用して IP 情報を変更することができます。

LAN タブ > Administration> IP Address の順にメニューをクリックし、以下の画面を表示します。選択した IP プロトコルバージョンによって異なる画面が表示されます。

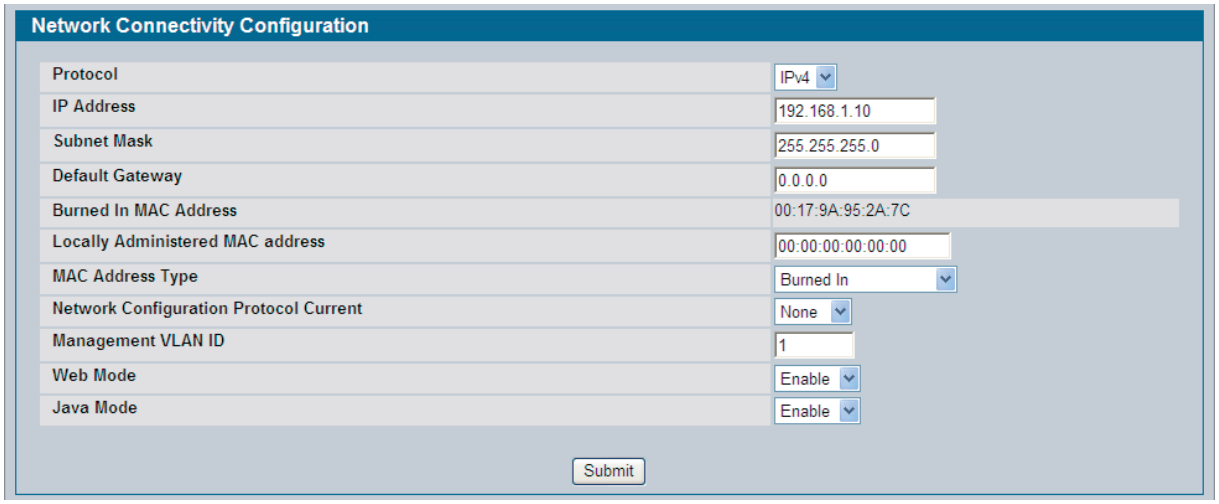


図 3-10　Network Connectivity Configuration - IPv4 画面

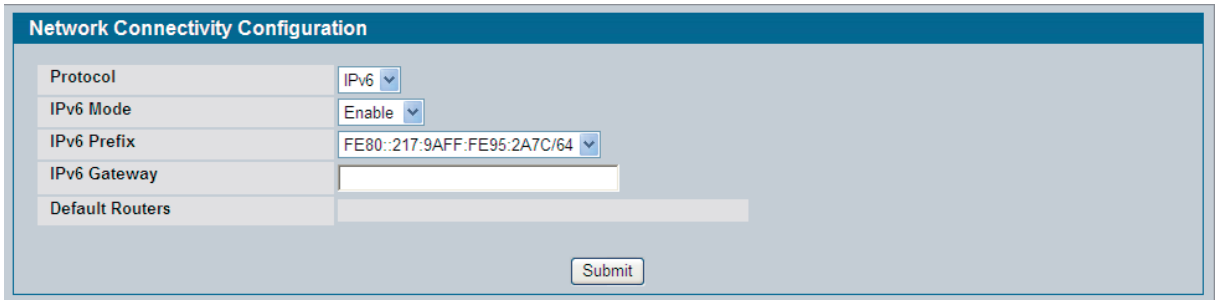


図 3-11　Network Connectivity Configuration - IPv6 画面

「Protocol」欄でインタフェースに設定する IP プロトコルバージョン（IPv4 または IPv6）を選択します。選択により異なる項目が表示されます。

IPv4 アドレス

IPv4 をプロトコルとして選択した場合に以下の項目が表示されます。

項目	説明
Protocol	IPv4 を選択します。
IP Address	ネットワークインタフェースの IP アドレス。初期値は 10.90.90.90 です。 **注意** IP アドレスは 0 以外の数で始まる必要があります。例えば、IP アドレス 001.100.192.6 と 192.001.10.3 は無効です。
Subnet Mask	インタフェースの IP サブネットマスク。初期値は 255.0.0.0 です。
Default Gateway	インタフェースのデフォルトゲートウェイ。初期値は 0.0.0.0 です。
Burned In MAC Address	各ポートのアップリンク状況（「Enabled」または「Disabled」）を表示します。
Locally Administered MAC address	ローカルな MAC アドレスを入力します。
MAC Address Type	インバンド接続に使用する MAC アドレスを選択します。工場出荷時設定は、「Burned In」です。 • Burned In - 工場出荷時設定の MAC アドレスを使用します。 • Locally Administered -「Locally Administered MAC Address」に入力した MAC アドレスを使用します。
Network Configuration Protocol Current	電源投入後、スイッチの動作を指定します。オプションは以下の通りです。 • BootP - Bootp リクエストを送信します。 • DHCP - DHCP リクエストを送信します。 • None - 電源投入後にリクエストを送信しません。（初期値）

項目	説明
Management VLAN ID	スイッチの管理 VLAN ID を指定します。1-3965 の範囲で指定します。管理 VLAN は、スイッチ管理に使用されます。本項目は、管理者ユーザにのみ設定可能で、他のユーザは参照だけ可能です。
Web Mode	スイッチのユーザインタフェースに Web ブラウザからアクセスできるかどうかを制御します。初期値は「Enable」(有効)です。 • Enable - スイッチの Web ベース管理を許可します。 • Disable - スイッチの Web ベース管理を禁止します。本モードが無効の場合、SNMP または CLI を使用してスイッチを管理する必要があります。
Java Mode	画面の右上にあるスイッチ画像を示す Java アプレットを表示するかどうかを制御します。初期値は「Enable」(有効)です。 • Enable - アプレットの表示を許可します。Java アプレットは、画面左側にあるナビゲーションツリーを使用する代わりにスイッチの画像の上をクリックして設定画面を選択することができます。 • Disable - Java アプレットの表示を許可しません。アプレットは空白のエリアに置き換えられます。

IPv6 アドレス

IPv6 をプロトコルとして選択した場合に以下の項目が表示されます。

項目	説明
Protocol	IPv6 を選択します。
IPv6 Mode	インタフェースの IPv6 モードを有効、または無効にします。
IPv6 Prefix	1 つも IPv6 が表示されない場合、「Add」を選択し、IPv6 のプレフィックス / 長さを入力します。最後の 64 ビットが MAC アドレスから派生する場合には EUI64 オプションを選択します。 例えば、「2001::/64」と入力し、EUI64 オプションを選択して MAC アドレスから 64 ビットアドレスを計算します。 「Add」を選択すると、「IPv6 Prefix」欄が更に追加表示されます。
IPv6 Gateway	IPv6 ゲートウェイアドレス (プレフィックスを含めない) を入力します。
Default Routers	「IPv6 Gateway」に入力されたアドレスを表示します。

ネットワーク接続項目を変更した場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。再起動後も新しい値をスイッチに保持する場合、保存を行う必要があります。

DHCP クライアントオプション

リースをリクエストする場合にスイッチの DHCP クライアントが DHCP サーバに送信するベンダのクラス識別子情報を設定、および有効にします。

LAN タブ > Administration > Network > DHCP Client Options の順にメニューをクリックし、以下の画面を表示します。

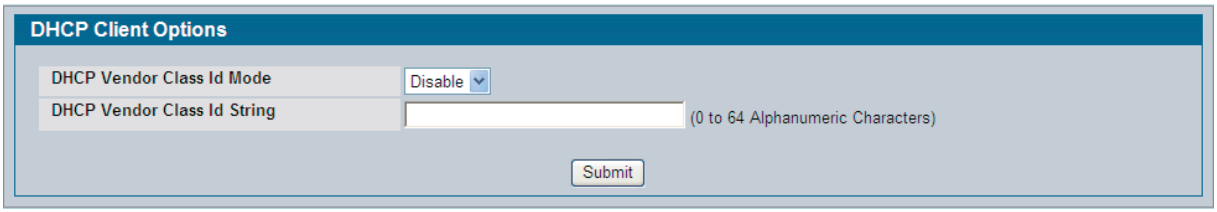


図 3-12　DHCP Client Options 画面

本画面には次の項目があります。

項目	説明
DHCP Vendor Class Id Mode	ベンダのクラス識別子モードを有効または無効にします。
DHCP Vendor Class Id String	ベンダのクラス識別子である Option-60 として DHCP リクエストに追加するテキストを入力します。

HTTP 設定

システムに HTTP サーバを設定します。

LAN タブ > Administration > HTTP 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 3-13　HTTP Configuration 画面

本画面には次の項目があります。

項目	説明
HTTP Admin Mode	HTTP の管理モードを有効または無効にします。現在の設定値は、Web 画面をオープンした場合に表示されます。初期値は有効です。本モードを無効にすると、Web インタフェースへのアクセスは Secure HTTP に制限されます。初期値は無効です。
Java Mode	Web の Java モードを有効または無効にします。これは、Secure および Unsecure HTTP 接続の両方に適用します。現在の設定値は、Web 画面をオープンした場合に表示されます。初期値は有効です。
HTTP Session Soft Timeout (Minutes)	HTTP セッションの無通信によるタイムアウトを設定します。0-60（分）の範囲で設定します。0 を指定するとタイムアウトになりません。初期値は 5（分）です。現在の設定値は、Web 画面をオープンした場合に表示されます。
HTTP Session Hard Timeout (Hours)	HTTP セッションのハード的なタイムアウトを設定します。このタイムアウトはセッションの通信レベルによる影響を受けません。0-168（時間）の範囲で設定します。0 を指定するとタイムアウトになりません。初期値は 24（時間）です。現在の設定値は、Web 画面をオープンした場合に表示されます。
Maximum Number of HTTP Sessions	許可される HTTP セッションの最大数（0-16）を設定します。初期値は 16 です。現在の設定値は、Web 画面をオープンした場合に表示されます。

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。

ユーザアカウントの設定

初期値では、スイッチには 2 つのユーザアカウントがあります。
- admin（読み書きする権限を所有）
- guest（参照のみの権限を所有）

初期値ではこれらのアカウントのパスワードはありません。名前は大文字と小文字を区別していません。読み / 書き権限を持つユーザアカウントでスイッチにログインすると、本画面を使用してパスワードを割り当てて初期アカウントにセキュリティ項目を設定することができます。また、最大 5 つの参照用アカウントを追加することができます。読み / 書きアカウントを除くすべてのアカウントを削除することができます。

注意 読み / 書き権限を持つユーザだけが本画面でデータを変更することができ、1 つのアカウントだけが読み / 書き権限を持っています。

LAN タブ > Administration > User Accounts の順にメニューをクリックし、以下の画面を表示します。

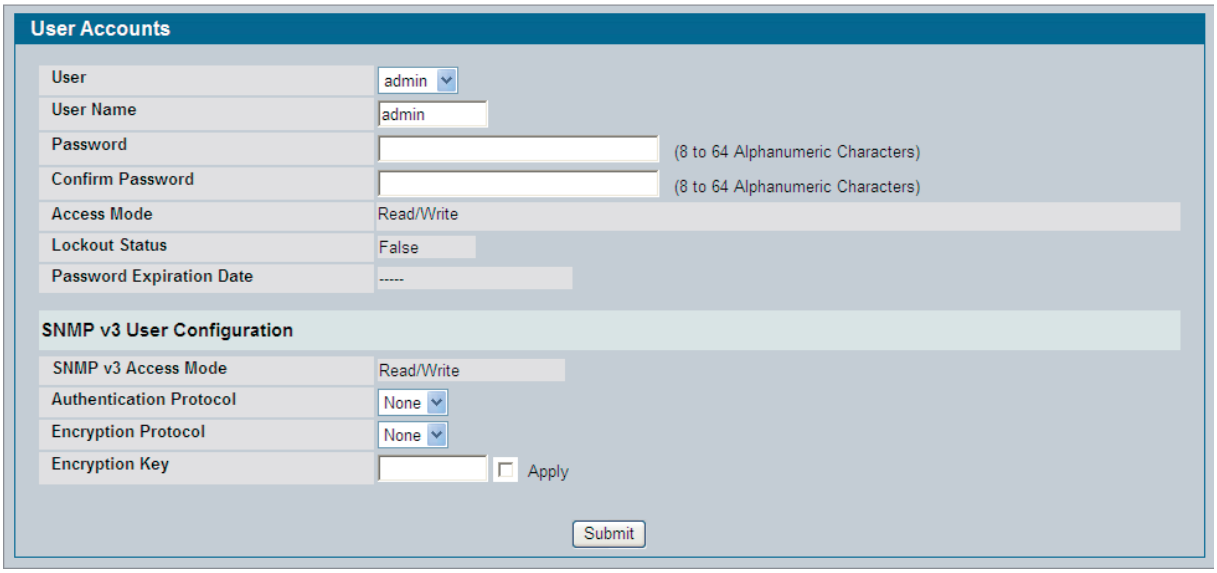


図 3-14　User Accounts 画面

本画面には次の項目があります。

項目	説明
User	設定変更する既存ユーザを選択します。または「Create」を選択し、新規ユーザアカウントを作成します。 システムは最大 5 つの参照アカウントと 1 つの読み / 書きアカウントを持つことができます。
User Name	アカウントに付与する名称を入力します。ユーザ名は、最大 8 文字で、大文字と小文字を区別しません。有効な文字にはダッシュ（-）とアンダーバー（_）などのすべての半角英数字が含まれます。ユーザ名「default」は無効です。 **注意** 読み / 書き権限を持つユーザ名を「admin」から他の名前に変更することはできますが、「Submit」ボタンをクリックすると新しいユーザ名を使用して再認証する必要があります。
Password	アカウントに新しいパスワードを入力します。画面上は表示されず、「*」だけが表示されます。パスワードは、最大 8 文字の半角英数字で、大文字と小文字を区別しています。
Confirm Password	正しく入力されたことを確認するために、再度パスワードを入力します。本欄には表示されず、「*」だけが表示されます。
Access Mode	ユーザのアクセスモードを表示します。admin は read/write（読み出し / 書き込み）のアクセス権を持ち、その他のアカウントは read-only（読み出しのみ）のアクセス権を持っています。
Lockout Status	ユーザが現在ロックされているかどうかを表示します。ログインの試みに失敗できる数を超えるとユーザはロックされます。この設定については、「DoS の設定」（40 ページ）を参照してください。
Password Expiration Date	指定ユーザの現在のパスワードの有効期限が切れる日付を表示します。これは、パスワードを作成した日および「Password Management」画面のパスワードエージング設定で指定した日数によって決定されます。

項目	説明
SNMPv3 User Configuration	
SNMPv3 Access Mode	ユーザアカウントの SNMPv3 アクセス権限を表示します。「admin」アカウントは read/write（読み出し / 書き込み）のアクセス権を持ち、他のすべてのアカウントは read-only（読み出しのみ）のアクセス権を持っています。
Authentication Protocol	選択ユーザに SNMPv3 認証プロトコルを設定します。有効な認証プロトコルは、None、MD5、または SHA です。None を選択すると、ユーザは SNMP ブラウザから SNMP データにアクセスできなくなります。MD5 または SHA を選択すると、ユーザのログインパスワードは SNMPv3 認証パスワードとして使用されるため、パスワード（8 文字）を指定する必要があります。
Encryption Protocol	選択ユーザに SNMPv3 暗号化プロトコルを設定します。有効な暗号化プロトコルは、None、または DES です。DES プロトコルを選択すると、「Encryption Key」にキーを入力する必要があります。 None を選択すると、「Encryption Key」は無視されます。
Encryption Key	「Encryption Protocol」欄で「DES」を選択した場合に、SNMPv3 暗号化キーを入力します。そうでない場合、本項目は無視されます。有効なキーの長さは 0-15 文字です。 「Encryption Protocol」と「Encryption Key」を変更するためには「Apply」欄をチェックします。

ユーザアカウントの追加

以下の手順でユーザアカウントを追加します。システムは、1 つの read/write（読み出し / 書き込み）権限を持つユーザと 5 つの read-only（読み出しのみ）権限を持つユーザをサポートしています。

1. 「User」メニューから「Create」を選択します。画面は更新されます。

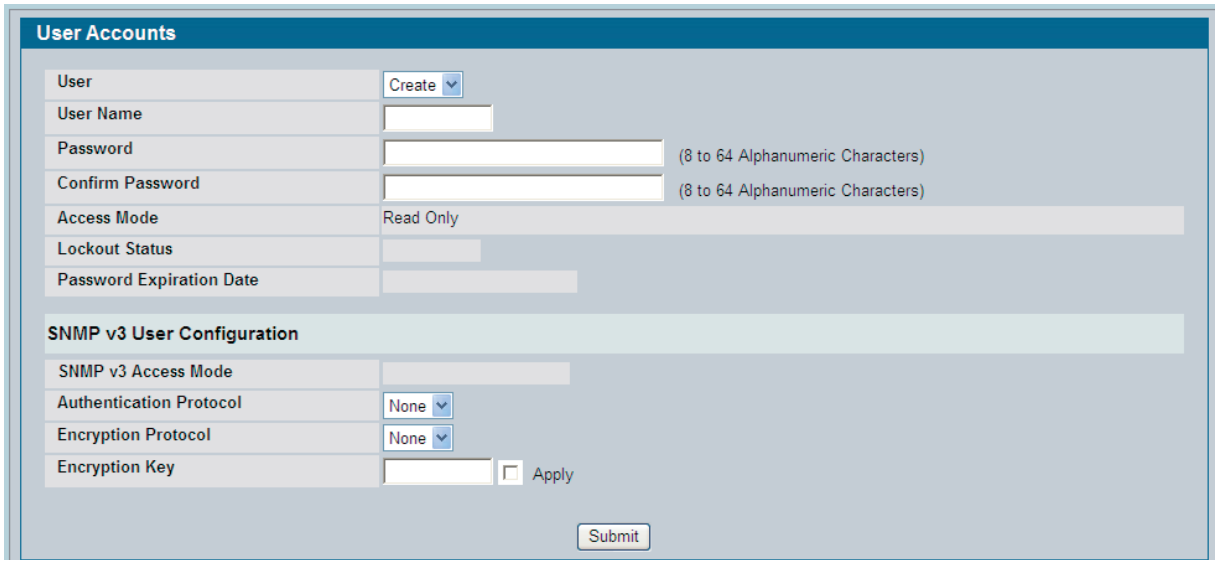


図 3-15　User Accounts 画面 - Create の選択

2. 「User Name」に新しいユーザのユーザ名、「Password」にパスワードを入力します。さらに確認のために「Confirm Password」にもパスワードを再度入力します。

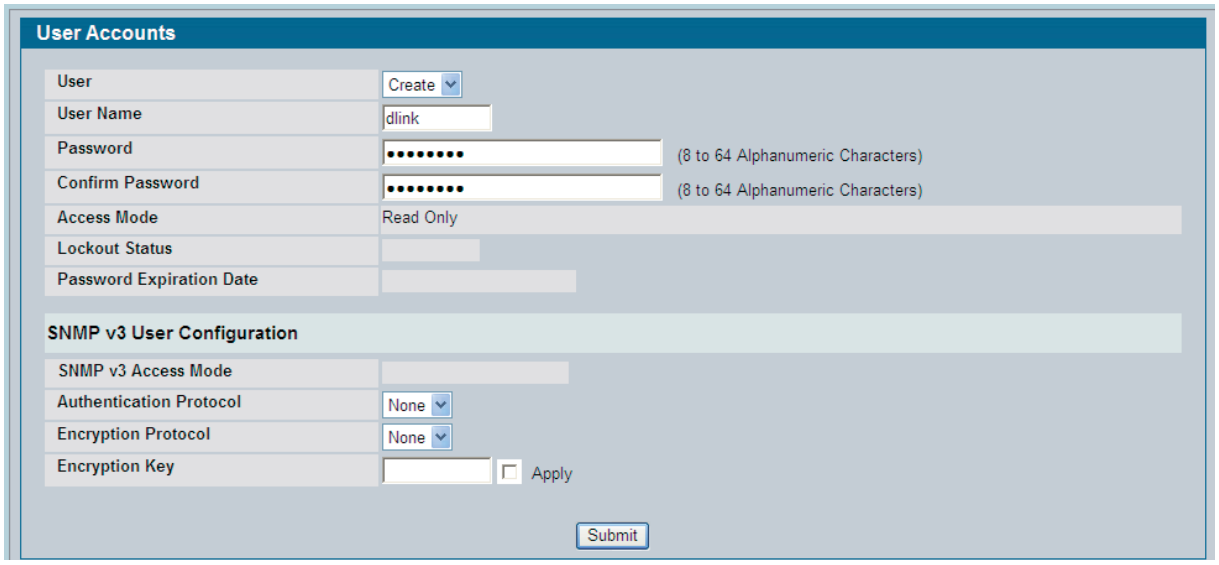


図 3-16　User Accounts 画面 - ユーザ名、パスワードの指定

3. 「Submit」ボタンをクリックして、スイッチを本画面の値に更新します。再起動後も新しい値をスイッチに保持する場合、保存を行う必要があります。

ユーザアカウント情報の変更

read/write（読み出し / 書き込み）権限を持つユーザの追加、削除はできませんが、ユーザ名とパスワードの変更を行うことができます。以下の手順で既存のアカウントのパスワードの変更、または既存のアカウントのユーザ名を上書きします。

1. 「User」メニューから変更するユーザを選択します。画面は更新されます。

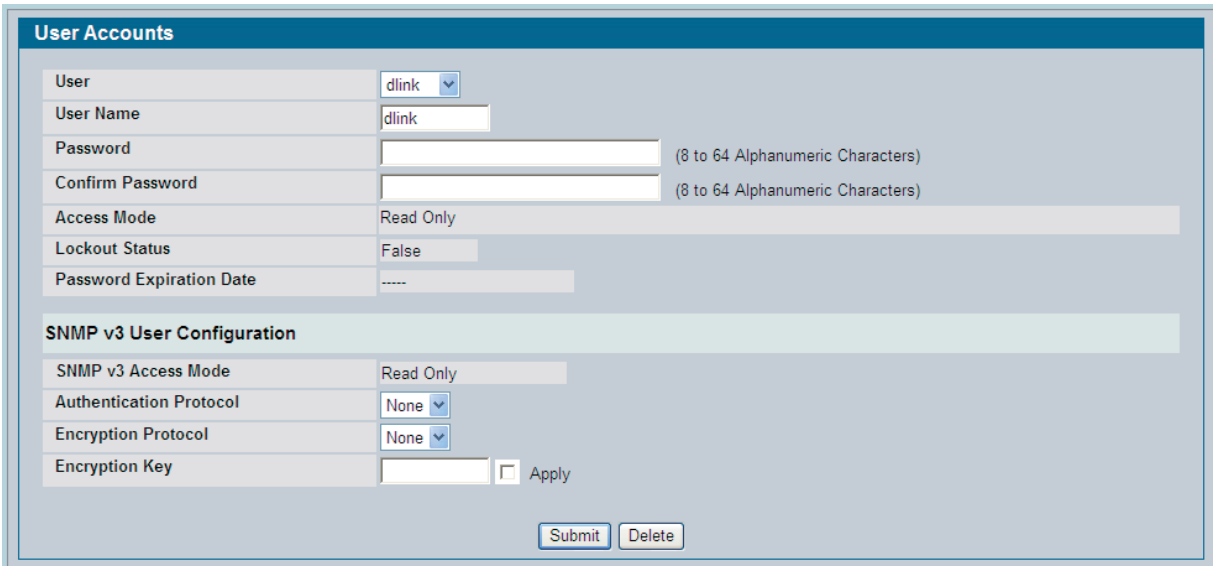


図 3-17　User Accounts 画面 - ユーザ情報の変更

2. ユーザ名を変更するためには、「User Name」の既存のユーザ名を削除し、新しいユーザ名を入力します。パスワードを変更するためには、「Password」と「Confirm Password」の「*」を削除し、新しいパスワードを入力します。

3. 「Submit」ボタンをクリックして、スイッチを本画面の値に更新します。再起動後も新しい値をスイッチに保持する場合、保存を行う必要があります。

ユーザアカウントの削除

以下の手順で read-only（読み出しのみ）権限を持つユーザアカウントを削除します。

1. 「User」メニューから削除するユーザを選択します。画面は更新されます。

2. 「Delete」ボタンをクリックし、ユーザを削除します。read-only（読み出しのみ）権限を持つユーザアカウントを選択した時だけ、本ボタンは表示されます。read/write（読み出し / 書き込み）権限を持つユーザを削除することはできません。

再起動後も新しい値をスイッチに保持する場合、保存を行う必要があります。

認証リストの設定

ログインリストを設定します。ログインリストにはリストに関連するユーザに対してスイッチまたはポートのアクセスを有効にする 1 つ以上の認証方法を指定します。

LAN タブ > Administration > Authentication List 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。

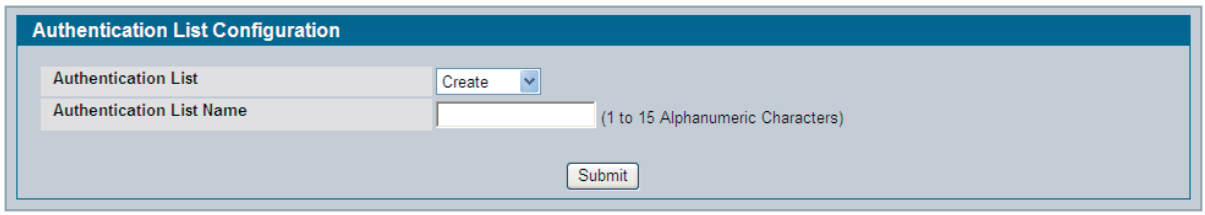


図 3-18　Authentication List Configuration 画面 - Create

ここでは、既存のリストが 1 つも選択されない場合の画面を示しています。

本画面には次の項目があります。

項目	説明
Authentication List	ここでは、新しい認証リストの作成、または参照 / 設定する既存リストの選択を行います。
Authentication List Name	新しいログインリストを作成するために、割り当てる名前を入力します。最大 15 文字の半角英数字で、大文字と小文字を区別しません。

既存の認証リストを選択すると「Authentication Profiles」画面に項目を表示します。

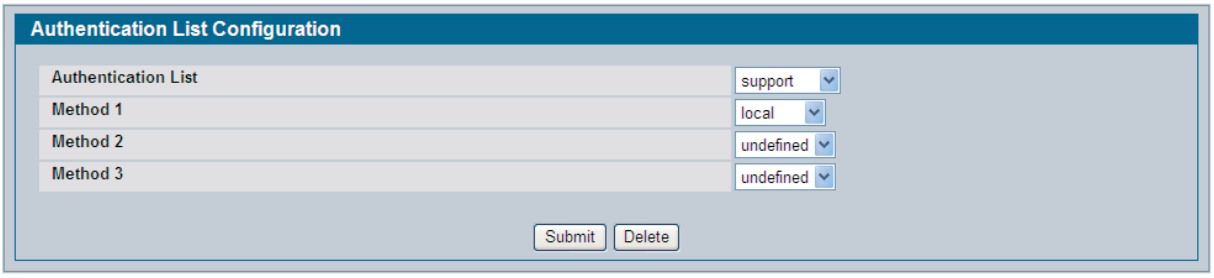


図 3-19　Authentication List Configuration 画面

本画面には次の項目があります。

項目	説明
Authentication List	新しい認証リストの作成、または参照または設定する既存のリストを選択します。
Method 1/2/3	• Method 1 - 選択された認証ログインリストに最初に表示される方式を選択します。 • Method 2 - 選択された認証ログインリストに次に表示される方式を選択します。これは、最初の方式がタイムアウトになった場合に使用される方式です。2 番目の方式としてタイムアウトをしない方式を選択すると、3 番目の方式は行われません。 • Method 3 - 選択された認証ログインリストに 3 番目に表示される方式を選択します。 ユーザ認証は選択した方式の順で行われます。可能な方式は以下の通りです。 • local - ローカルに保存されたユーザの ID とパスワードを認証に使用します。ローカルな方式がタイムアウトにならないので、最初の方式としてこのオプションを選定すると、1 つ以上の方式を指定したとしても他の方式は行われません。 • radius - RADIUS サーバを使用してユーザ ID とパスワードを認証します。最初の方式として RADIUS または TACACS+ を選択して、認証中にエラーが発生すると、スイッチは、Method 2 を使用してユーザを認証します。 • tacacs+ - TACACS+ サーバを使用してユーザ ID とパスワードを認証します。最初の方式として RADIUS または TACACS+ を選択して、認証中にエラーが発生すると、スイッチは、Method 2 を使用してユーザを認証します。 • reject - ユーザは認証されません。 • undefined - 認証方法は指定されません。本オプションは Method 2 および Method 3 でのみ利用可能です。

認証リストの作成

以下の手順で新しい認証リストを作成します。

1. 「Authentication List」で「Create」を選択します。

2. 「Authentication List Name」に、1-12 文字の範囲で名称を入力します。名称には空白を含むことはできません。

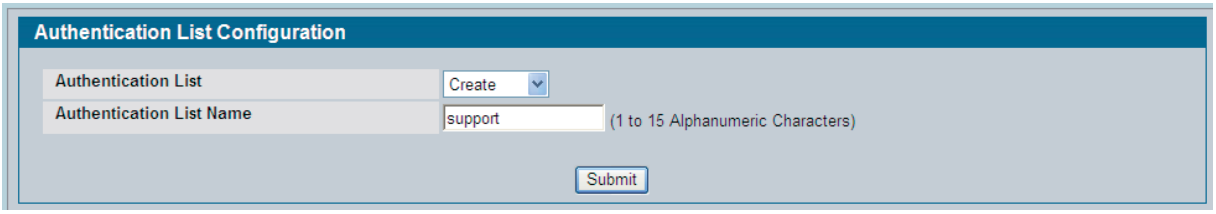


図 3-20　Authentication List Configuration 画面 - Create

3. 「Submit」ボタンをクリックして名称を作成し、新しいリストに「Method」欄を表示します。これで、認証リストを設定する準備が整います。初期値では、「local」が初期の認証方法として設定されています。

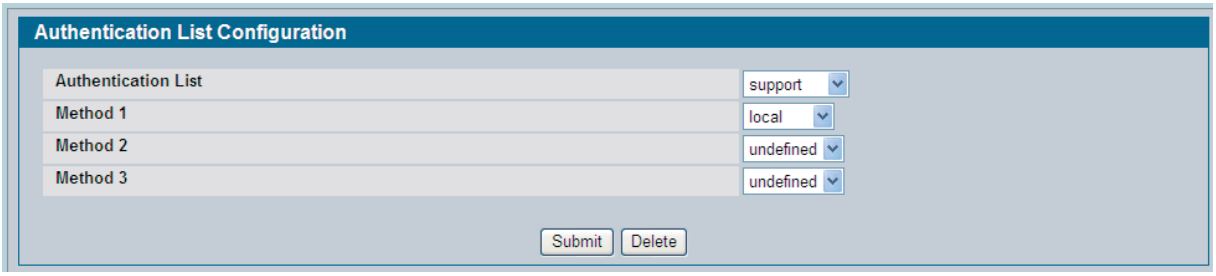


図 3-21　Authentication List Configuration 画面

再起動後も新しい値をスイッチに保持する場合、保存を行う必要があります。

認証リストの設定

以下の手順で認証リストを変更します。

1. 「Authentication List」メニューからの既存のリストを選択します。

2. 「Method 1」から最初のログイン方式を選択します。

3. 必要であれば、「Method 2」および「Method 3」から 2 番目、3 番目のログイン方式を選択します。

4. 「Submit」ボタンをクリックし、変更をスイッチに適用します。

再起動後も新しい値をスイッチに保持する場合、保存を行う必要があります。

認証リストの削除

以下の手順でコンフィグレーションから認証リストを削除します。

1. 「Authentication List」メニューからの既存のリストを選択します。

2. 「Delete」ボタンをクリックします。
選択したログインリストがシステムのログインまたは IEEE 802.1X ポートアクセスコントロールのために（初期ユーザを含む）いずれかのユーザに割り当てられていると、削除は失敗します。read/write（読み出し / 書き込み）アクセス権限を持つ場合にだけ本ボタンを使用することができます。

再起動後も新しい値をスイッチに保持する場合、保存を行う必要があります。

認証リストのサマリ

ユーザと各リストとの関連しているかなどシステム上の認証リストに関する情報を参照します。また、802.1X ポートセキュリティユーザに関する情報も表示します。

LAN タブ > Administration > Authentication List 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。

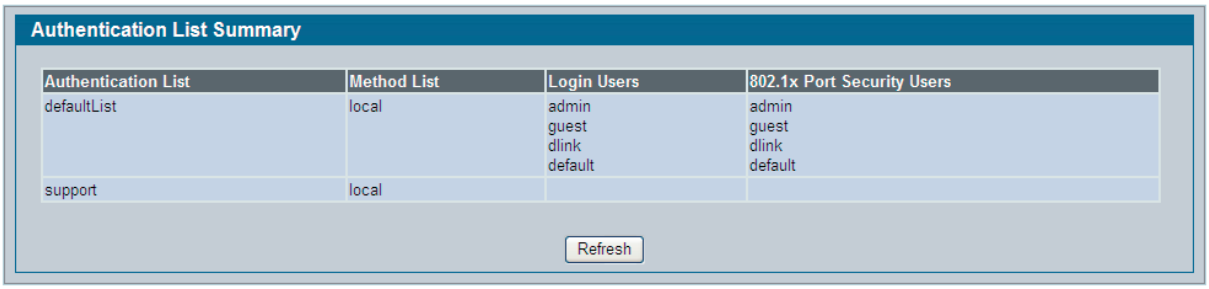


図 3-22　Authentication List Summary 画面

本画面には次の項目があります。

項目	説明
Authentication List	認証ログインリストの名称を指定します。
Method List	リストに設定されたログイン方式を順番に表示します。
Login Users	「User Login Configuration」画面でこのログインリストに割り当てられているユーザを表示します。本リストを使用して、システムのログインアクセスのためにユーザを認証します。
802.1x Port Security Users	本ログインリストに割り当てられたポートアクセスコントロールユーザを参照します。ポートアクセスのために IEEE 802.1X プロトコルを使用することでユーザを認証するのに本リストは使用されます。

「Refresh」ボタンをクリックしてと、画面の情報を更新します。

特定の認証リストにユーザを割り当てるためには、「ユーザログイン」（39 ページ）を参照してください。802.1X ポートセキュリティユーザを設定するためには、「ポートアクセスコントロール」（252 ページ）を参照してください。

ログインセッション

スイッチにログインしているユーザに関する情報を参照します。

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

図 3-23　Login Sessions 画面

本画面には次の項目があります。

項目	説明
ID	ログイン ID を表示します。
User Name	現在スイッチにログインしているユーザ名を表示します。
Connection From	ユーザが接続しているシステムの IP アドレスを表示します。接続がローカルなシリアル接続である場合、「Connection From」エントリは「EIA-232」です。
Idle Time	アクティブでないセッション時間を表示します。
Session Time	セッション時間の合計を表示します。
Session Type	セッションのタイプ（Telnet、Serial Port、HTTP、または SSH）を表示します。

「Refresh」ボタンをクリックして、画面の情報を更新します。

ユーザログイン

各設定ユーザは、スイッチへのアクセス、またはスイッチポートへのアクセスを行う場合も、ユーザを認証する方法を指定しているログインリストに割り当てられます。新しいユーザアカウントを「User Account」画面で作成した後に、「User Login」画面を使用して、スイッチのログインリストにユーザを割り当てます。

設定済みのユーザ（admin と guest）は、定義済みの defaultList に割り当てられており、削除することはできません。また、新たに作成されたすべてのユーザは、明確に別のリストに割り当てられるまで、defaultList に割り当てられます。新しい認証リストを作成するためには、「認証リストの設定」（36 ページ）を参照してください。

LAN タブ > Administration > User Login の順にメニューをクリックし、以下の画面を表示します。

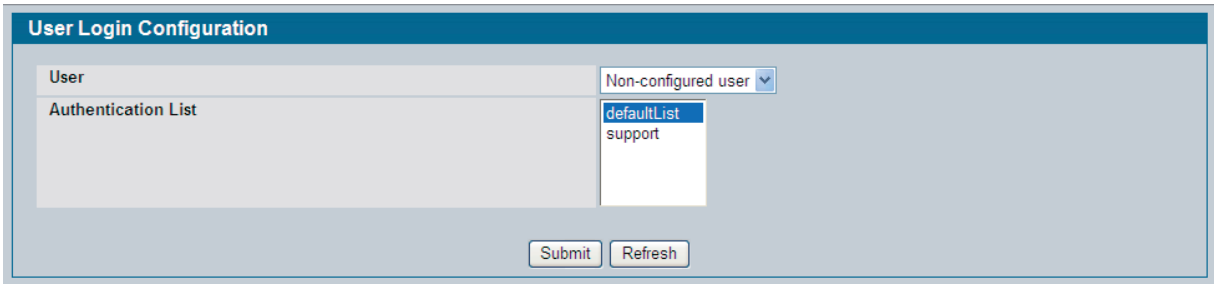


図 3-24　User Login 画面

本画面には次の項目があります。

項目	説明
User	「Non-configured user」または設定済みのユーザ名があります。 「Non-configured user」は、スイッチに設定されたアカウントを持っていないユーザです。RADIUS サーバ経由の認証を指定するログインリストにこれを割り当てる場合、各スイッチ上のユーザすべてにアカウントを作成する必要はありません。しかし、初期値では、「Non-configured user」は、local 認証を使用する「defaultList」に割り当てられています。
Authentication List	システムログインのためにユーザに割り当てる認証ログインリストを選択します。

認証リストにユーザを割り当てる

admin（読み出し / 書き込み）ユーザは、常に「defaultList」に関連付けされており、これにより admin ユーザは、スイッチ設定から完全にロックされることを防ぐためにいつもローカルで認証されます。リモート認証を必要とするログインリストにユーザを割り当てる場合、認証が完了するまで、すべての CLI、Web、および telnet セッションからのスイッチへのユーザアクセスはブロックされます。詳しくは、「RADIUS 設定」（257 ページ）の「Max Number of Retransmits」を参照してください。

1. 「User」からユーザ名を選択するか、または「Non-configured user」を選択し、スイッチに設定されていないすべてのユーザを認証リストに割り当てます。
   画面は更新されます。ユーザが現在割り当てられているリストは「Authentication List」で強調表示されています。

2. 異なるリストにユーザを割り当てるためには、「Authentication List」内のリスト名をクリックし、リストを選択します。

3. 「Submit」ボタンをクリックし、変更をスイッチに適用します。

DoS 設定

DoS の制御を設定します。D-Link のソフトウェアは、DoS 攻撃の特定のタイプを分類してブロックします。これらの攻撃タイプをモニタして、ブロックするようにシステムを設定することができます。

DoS 攻撃のタイプ	対策
SIP=DIP	送信元 IP アドレスと送信先 IP アドレスが等しいパケットの破棄。
First Fragment	設定値よりも TCP ヘッダサイズが小さいパケットの破棄。
TCP Fragment	IP Fragment Offset に「1」が設定されているパケットの破棄。
First Fragment	以下に該当するパケットの破棄。 • TCP Flag SYN が設定され、送信先ポートが 1024 未満。 • TCP Control Flags が「0」に設定され、TCP Sequence Number が「0」に設定されている。 • TCP Flags FIN、URG、および PSH が設定され、TCP Sequence Number が「0」に設定されている。 • TCP Flags SYN および FIN が設定されている。
L4 Port	送信元と送信先の TCP/UDP ポートが等しいパケットの破棄。
ICMP	ICMP Ping パケットのサイズの制限。

LAN タブ > Administration > Denial of Service 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 3-25　Denial of Service Configuration 画面

本画面には次の項目があります。

項目	説明
Denial of Service First Fragment	本オプションを有効または無効にします。First Fragment DoS 防止を有効にすると、「Min TCP Hdr Size」（最小 TCP ヘッダサイズ）より小さな TCP ヘッダを持つパケットを廃棄します。初期値は「Disable」（無効）です。
Denial of Service Min TCP Hdr Size	許可される「Min TCP Hdr Size」（最小 TCP ヘッダサイズ）を指定します。First Fragment DoS 防止を有効にすると、スイッチは、ここで設定した「Min TCP Hdr Size」より小さな TCP ヘッダを持つパケットを廃棄します。初期値は「Disable」（無効）です。
Denial of Service ICMP	本オプションを有効または無効にします。ICMP DoS 防止を有効にすると、スイッチは、ECHO_REQ（ping）に設定されたタイプおよび「ICMP Pkt Size」（ICMP パケットサイズ）より大きなサイズを持つ ICMP パケットを廃棄します。初期値は「Disable」（無効）です。
Denial of Service Max ICMP Size	許可される「Max ICMP Pkt Size」（最大 ICMP パケットサイズ）を指定します。ICMP DoS 防止を有効にすると、スイッチは、ここで設定した Max ICMP Pkt Size より大きなサイズを持つ ICMP ping パケットを破棄します。初期値は「Disable」（無効）です。
Denial of Service L4 Port	本オプションを有効または無効にします。L4 Port DoS 防止を有効にすると、スイッチは、TCP/UDP 宛先ポートに等しい TCP/UDP 送信元ポートを持つパケットを廃棄します。初期値は「Disable」（無効）です。
Denial of Service SIP=DIP	本オプションを有効または無効にします。SIP=DIP DoS 防止を有効にすると、スイッチは、送信先 IP アドレスに等しい送信元 IP アドレスを持つパケットを廃棄します。初期値は「Disable」（無効）です。
Denial of Service TCP Flag	本オプションを有効または無効にします。TCP Flag DoS 防止を有効にすると、以下に該当するパケットを破棄します。初期値は「Disable」（無効）です。 • TCP Flag SYN が設定され、送信先ポートが 1024 未満。 • TCP Control Flags が「0」に設定され、TCP Sequence Number が「0」に設定されている。 • TCP Flags FIN、URG、および PSH が設定され、TCP Sequence Number が「0」に設定されている。 • TCP Flags SYN および FIN が設定されている。
Denial of Service TCP Fragment	SIP=DIP DoS 防止を有効にすると、スイッチは、宛先 IP アドレスに等しい送信元 IP アドレスを持つパケットを廃棄します。TCP Fragment DoS 防止を有効にすると、「1」と等しい IP フラグメントオフセットを持つパケットを廃棄します。初期値は「Disable」（無効）です。

DoS 設定を変更した場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。再起動後も新しい値をスイッチに保持する場合、保存を行う必要があります。

フォワーディングデータベースの設定と検索

フォワーディングデータベースは、MAC アドレスからパケットを受信した後に MAC アドレスのリストを保持します。透過ブリッジング機能は、フォワーディングデータベースエントリを使用して、受信フレームの送信方法を決定します。

フォワーディングデータベースの設定

学習した MAC アドレスをフォワーディングデータベースに保持する時間を設定します。フォワーディングデータベースには、エージングアウトされないスタティックなエントリと指定時間内に更新されないと削除されるダイナミックに学習されたエントリがあります。

LAN タブ > L2 Features > Forwarding DB 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。

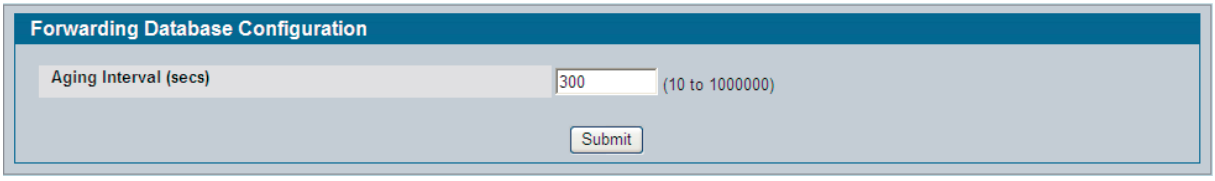


図 3-26　Forwarding DB Configuration 画面

注意　IEEE 802.1D では、初期値として 300（秒）を推奨しています。これは、工場出荷時設定です。

「Submit」ボタンをクリックし、変更をスイッチに適用します。再起動後も新しい値をスイッチに保持する場合、保存を行う必要があります。

MAC アドレステーブルの検索

フォワーディングデータベースのエントリに関する情報を表示します。

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

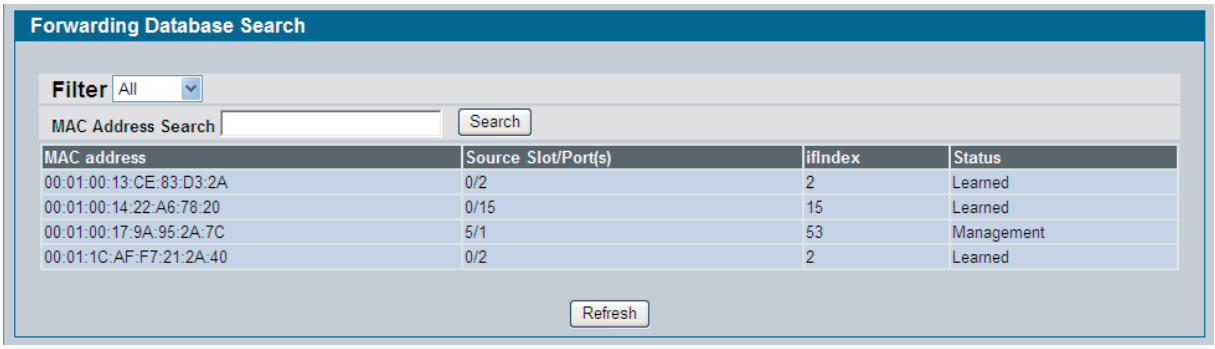


図 3-27　Forwarding Database Search 画面

本画面には次の項目があります。

項目	説明
Filter	表示するためにエントリのタイプを指定します。メニューからフィルタを選択すると、画面は更新され、選択したフィルタに基づいたエントリを表示します。以下のフィルタの 1 つを選択することができます。 • Learned - 学習された MAC アドレスだけを表示します。 • All - すべてのテーブルを表示します。
MAC Address Search	本項目では、フォワーディングデータベーステーブルの個別の MAC アドレスを検索することができます。
MAC Address	スイッチが転送および（または）フィルタした情報用のユニキャスト MAC アドレス。フォーマットは「：」（コロン）で分けられた各バイトを持つ 6 バイトの MAC アドレスの後に 2 バイトの 16 進数の VLAN ID です。例えば以下のようになります。01:23:45:67:89:AB:CD:EF（「01:23」は VLAN ID で、「45:67:89:AB:CD:EF」は MAC アドレスです。）
Source Slot/Port(s)	このアドレスを学習したポート。つまり、ここでは MAC アドレスに到達することができるポートを表示します。
ifIndex	ソースポートに関連する MIB インタフェーステーブルのエントリの ifIndex。
Status	このエントリの状態を示します。 • Static - スタティックな MAC フィルタが定義された時、エントリが追加されました。 • Learned - エントリは、入力トラフィックの送信元 MAC アドレスを監視することで学習され、現在使用中です。 • Management - インタフェース 0,1 を持つシステムの MAC アドレス。 • Self - スイッチの物理インタフェースの 1 つの MAC アドレス。

フォワーディングデータベースと検索

以下の手順でフォワーディングデータベースを検索します。

1. 「:」（コロン）で分けられた 2 桁の 6 バイトの 16 進数で表す MAC アドレスに続いて 2 バイトの 16 進数の VLAN ID を入力します。
   例えば、01:23:45:67:89:AB:CD:EF（「01:23」は VLAN ID で、「45:67:89:AB:CD:EF」は MAC アドレス）です。

2. 「Search」ボタンをクリックします。
   アドレスが存在すると、画面を更新し、テーブルの始めにエントリが表示されます。残りの MAC アドレスが大きい順にエントリの後に続きます。
   完全に一致する必要があります。「Refresh」ボタンをクリックすると、再び低い値を持つ MAC アドレスの順に表示されます。

ログの管理

スイッチは、コンフィグレーションまたは他の事象に起こった変更などプラットフォームに発生しているイベント、故障、またはエラーに応じてメッセージを生成します。これらのメッセージはプラットフォームにローカルに保存され、ストレージデバイスなど 1 つ以上の監視目的で集中させる場所に送信されます。ログの取得機能（ローカルおよびリモート）設定にはシステムレベルに基づいてログ取得され、転送されたメッセージのフィルタリングとコンポーネントの生成があります。

in-memory ログはメッセージコンポーネントとシステムレベルへの設定に基づいてメモリにメッセージを保存します。スタッカブルシステムでは、このログは管理ユニット上に存在するだけです。スタック内の他のプラットフォームはそれらのメッセージを管理ユニットのログに送信します。管理ユニットより他のユニットの in-memory ログへのアクセスはサポートされていません。

ログ機能では以下の設定を行うことができます。

- バッファされたログの設定
- バッファされたログメッセージの設定
- Command Logger の設定
- コンソールのログ出力設定
- イベントログ
- リモートホストの設定
- 持続性ログの設定
- 持続性ログの参照
- システムログ設定

バッファされたログの設定

バッファされたログは、メッセージコンポーネントとシステムレベルの設定に基づいてメモリにメッセージを保存します。

システムバッファ内のログの管理ステータスと動作を設定します。

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

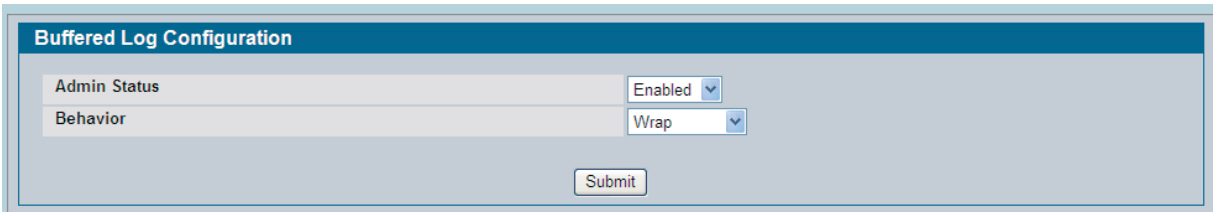


図 3-28　Buffered Log Configuration 画面

本画面には次の項目があります。

項目	説明
Admin Status	ログ取得を「Enabled」（有効）または「Disabled」（無効）にします。「Disabled」にするとメッセージのログへの出力は行いません。
Behavior	ログスペースがいっぱいになった場合に行う動作（「Wrap」または「Stop」）を指定します。

設定を変更した場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。再起動後も変更をスイッチに保持する場合、保存を行う必要があります。

バッファリングされたログメッセージの参照

システムバッファ内のログメッセージを参照します。最新のメッセージが画面の下部に表示されます。

LAN タブ > Monitoring > Log > Buffered 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。

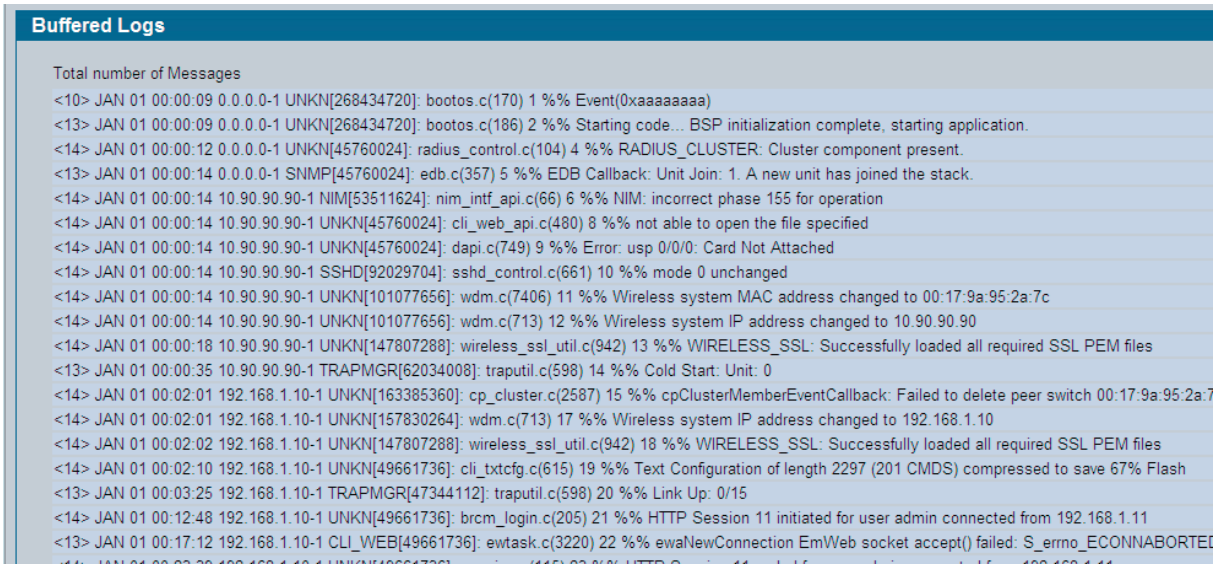


図 3-29　Buffered Logs 画面

本画面には次の項目があります。

項目	説明
Total number of Messages	システムがログ出力したバッファメッセージ数を表示します。128 個の最新のエントリだけを表示します。

ページの残りはバッファされたログメッセージを表示します。以下の例題では non-stacking システムのログメッセージの例を示しています。

```
<15>Aug 24 05:34:05 STK0 MSTP[2110]:mspt_api.c(318) 237 %% Interface 12 transitioned to root
state on message age timer expiry
```

意味

このログメッセージには、デバッグメッセージである 7（15 mod 8）のシステムレベルがあります。システムはスタックしていません（STK0）。メッセージはスレッド ID2110 で動作する MSTP コンポーネントで生成されています。メッセージはファイル「mstp_api.c」の 318 行目にあり、8 月 24 日 05:34:05 に生成されています。これは、ログ出力された 237 番目のメッセージです。

以下の例では、スタックをサポートするシステムに生成されたログメッセージを示しています。

```
<15>Aug 24 05:34:05 0.0.0.0-1 MSTP[2110]: mspt_api.c(318) 237 %% Interface 12 transitioned to
root state on message age timer expiry
```

意味

このログメッセージには、デバッグメッセージである 7(15 mod 8) のシステムレベルがあります。メッセージはスレッド ID2110 で動作する MSTP コンポーネントで生成されています。メッセージはファイル「mstp_api.c」の 318 行目にあり、8 月 24 日 05:34:05 に生成されています。システム IP「0.0.0.0」とユニット番号「1」と共にログ出力された 237 番目のメッセージです。

「Refresh」ボタンをクリックすると、最新のメッセージに更新します。

Command Logger 設定

システムに発行されるすべての CLI コマンドをログ出力することができます。コマンドログメッセージは他のシステムログメッセージと共に出力されます。

LAN タブ > Administration > Log > Command Logger 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。

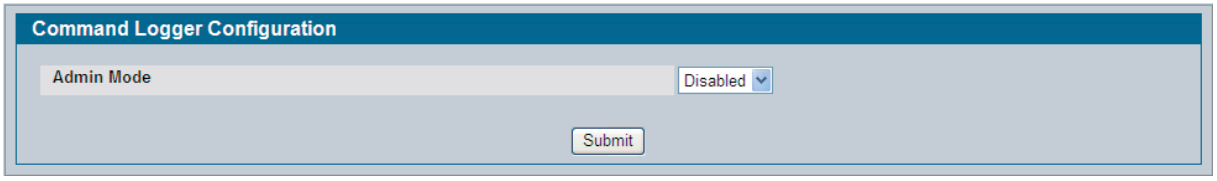


図 3-30　Command Logger Configuration 画面

本画面には次の項目があります。

項目	説明
Admin Mode	CLI コマンドをシステムログファイルにログ出力するかどうか決定します。 • Enabled - システムログの CLI コマンドをログに出力します。コマンドは「Buffered Logs」画面のメッセージに表示されます。例えば、CLI コマンド「show logging buffered」が発行された場合に以下のログメッセージが表示されます。これにはコマンドが発行された IP アドレスとコマンドを発行したユーザ名があります。 `<5> NOV 29 22:25:00 10.254.24.172-1 UNKN[243420816]: cmd_logger_api.c(87) 34 %% CLI:10.254.24.65:admin:show logging buffered` • Disabled - 本システムは CLI コマンドをログに出力しません。

管理モードを変更した場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。

Console Log Configuration（コンソールのログ出力設定）

スイッチに接続するシリアルデバイスに対するログの出力を制御します。

LAN タブ > Administration > Log > Console Log 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。

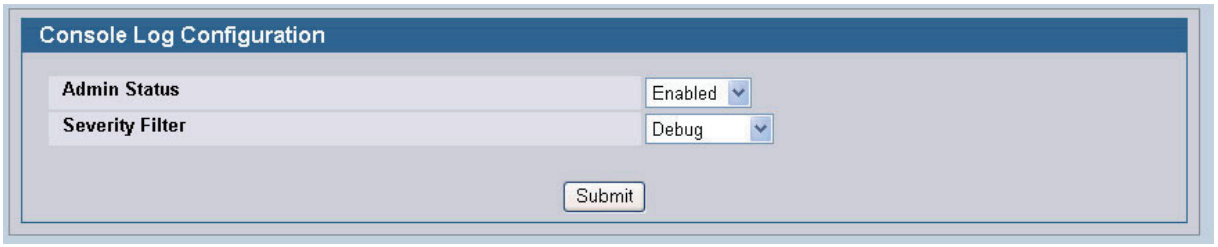


図 3-31　Console Log Configuration 画面

本画面には次の項目があります。

項目	説明
Admin Status	コンソールのログ出力を有効または無効にします。初期値では無効に設定されています。 • Enabled - スイッチシリアルポートに割り当てられるデバイスにログメッセージを出力します。 • Disabled - スイッチシリアルポートに割り当てられるデバイスへのログメッセージの出力をしません。
Severity Filter	コンソールに出力するためのログのレベルを選択します。選択したシステムレベル以上のログレベルを持つすべてのログを出力します。例えば、「Error」を選択すると、ログメッセージには「Error」、「Critical」、「Alert」および「Emergency」が含まれます。システムレベルの初期値は「Alert(1)」です。システムレベルは以下のレベルの 1 つです。 • Emergency (0) - 最も高い警告レベル。デバイスがダウンまたは適切に機能していない場合に、ログがデバイスに保存されます。 • Alert (1) - 2 番目に高い警告レベル。デバイスのすべての機能がダウンするなどの深刻なデバイスの動作不良がある場合に、ログが保存されます。 • Critical (2) - 3 番目に高い警告レベル。2 つのデバイスポートが機能していなくてもデバイスの残りのポートが動作しているなどクリティカルなデバイスの動作不良が発生するとログが保存されます。 • Error (3) - デバイスエラーはポートがオフラインである場合などに発生します。 • Warning (4) - 最も低いレベルのデバイス警告。 • Notice (5) - デバイス情報をネットワーク管理者に提供します。 • Informational (6) - デバイス情報を提供します。 • Debug (7) - ログに関する詳細情報を提供します。デバッグは適切なサポート部署の人によって照会されるべきものです。

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。

イベントログ

イベントログを表示します。これは、重大なイベントに対するエラーメッセージを保持するために使用されます。イベントがログに出力され、更新後のログがフラッシュメモリに保存されると、スイッチはリセットされます。ログは少なくとも 2,000 個のエントリ（実際の値はプラットフォームと OS に依存します。）を保持することができ、追加の際に最大値に到達すると削除されます。イベントログはシステムリセット後も保存されます。

LAN タブ > Monitoring > Log > 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。

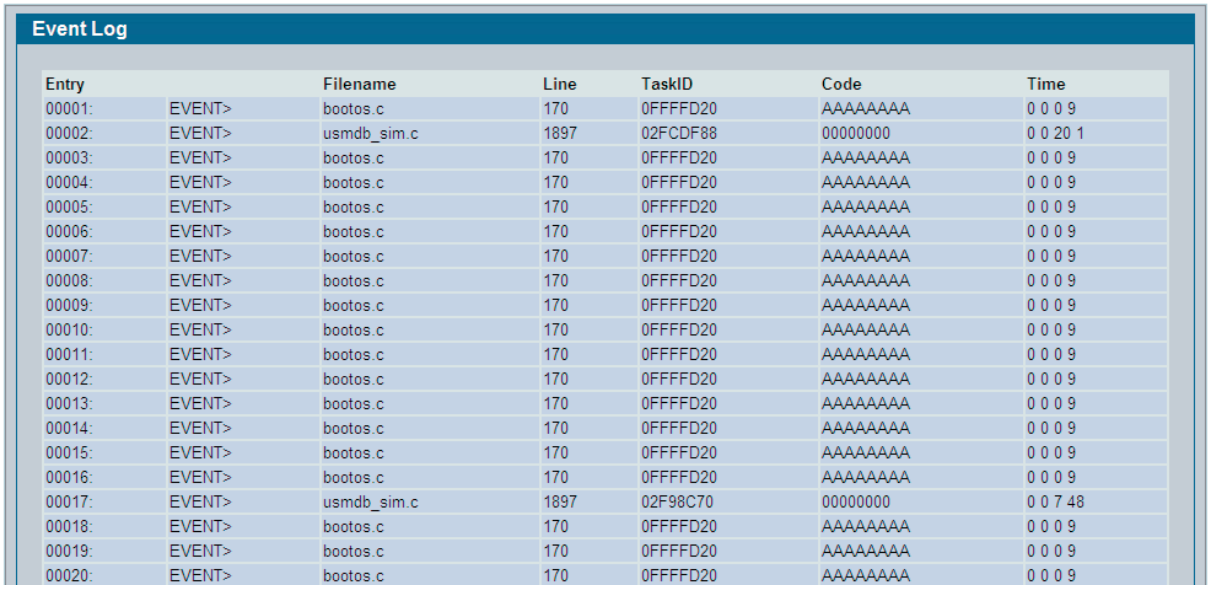


図 3-32　Event Log 画面

本画面には次の項目があります。

項目	説明
Entry	イベントログ内のエントリ数。最新のエントリが最初に表示されます。
Filename	イベントを検出したコードを識別する D-Link のソースコードファイル名。
Line	イベントを検出したコードに関するソースファイル内の行番号。
Task ID	イベントをレポートするタスクについて OS が割り当てた番号。
Code	イベントをレポートするコードによってイベントログハンドラに渡されたイベントコード。
Time	前のリセットから発生し、取得されたイベントの時刻。

「Refresh」ボタンをクリックすると、最新のログメッセージエントリに更新します。

リモートホストの設定

スイッチがログを送信するリモートログホストを設定します。リモートのログ出力を有効にするためには、「システムログ設定」（48 ページ）を参照してください。

LAN タブ > Administration > Log > Host 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。以下の図は、ログホストが追加される前の初期状態の「Host Configuration」画面を表示しています。

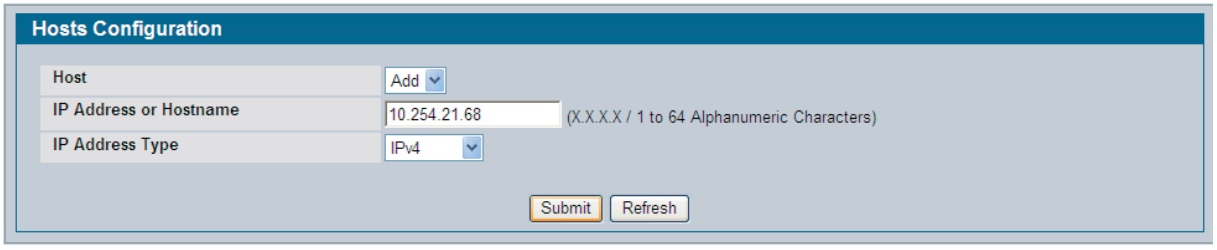


図 3-33　Host Configuration 画面

ログホストの追加後、以下の図のように、画面は追加欄を表示します。

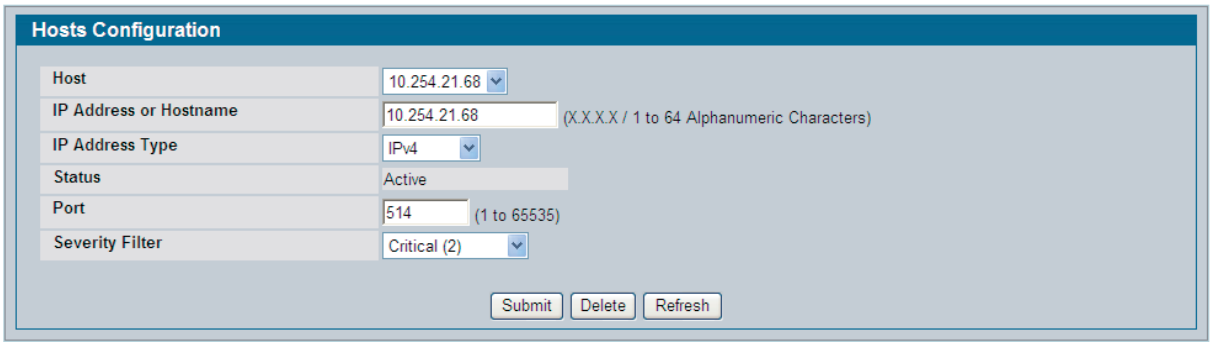


図 3-34　Host Configuration 画面 - ログホストの追加

リモートログホストの追加

以下の手順でログホストを追加、編集、または削除します。

1. 「Host」欄から、「Add」を選択して新しいホストを追加するか、または既存のホストの IP アドレスを選択してホストを設定します。
   新しいホストを追加する場合、「IP Address or Hostname」欄にホストの IP アドレスを入力して「Submit」ボタンをクリックします。画面は更新され、追加の項目が表示されます。

2. 「Port」欄に、ログが送信されるリモートホストのポート番号を入力します。

3. 「Security Filter」欄にリモートホストに送信するログのレベルを選択します。

4. 「Submit」ボタンをクリックし、変更をスイッチに適用します。

リモートログホストの削除

設定リストからリモートログホストを削除するためには、「Host」欄からホストの IP アドレスを選択し、「Delete」ボタンをクリックします。

持続性ログの設定

持続性ログは不揮発性のストレージに保存されます。つまり、ログメッセージがスイッチの再起動後も保持されることを意味します。以下のログタイプがあります。

- 最初のログタイプはシステム起動のログです。システムの起動のログにはシステム再起動後に受信した最初の N 個のメッセージを保存します。このログは、常にログがいっぱいなった場合にログ出力を中止するという操作属性があり、最大 32 個のメッセージを保存することができます。

- 2 番目のログタイプはシステム操作のログです。システム操作のログには、システム操作の間に受信した最後の N 個のメッセージを保存します。このログは、ログがいっぱいなった場合にログを上書きするという操作属性があります。最大 1000 個のメッセージを保存することができます。

システム起動のログまたはシステム操作のログの両方ではなく、いずれか一方がストレージの基準を満たすログのサブシステムにより受信したメッセージを保存します。つまり、システム起動時、起動ログが設定されていると、その限界までメッセージを保存してきます。次に設定されていれば、操作のログはメッセージの保存を開始します。

システムは、< ファイル >1.txt、< ファイル >2.txt、および < ファイル >3.txt という持続的なログを最大 3 つのバージョンまで保持します。システム起動の際に、< ファイル >3.txt は削除され、< ファイル >2.txt は < ファイル >3.txt に、< ファイル >1.txt は < ファイル >2.txt に変更されます。そして、ログ出力が < ファイル >1.txt に開始されます。（上記例題内の < ファイル > を操作ログに対しては「olog」に、起動ログに対しては「slog」に置き換えます。）

Web またはローカルなシリアルケーブル経由の CLI、xmodem を通じてローカルの持続性ログを検索することができます。以下の画面を使用して、持続性ログ出力の有効または無効、システムレベルフィルタの設定を行います。

LAN タブ >Administration > Log > Persistent Logger 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。

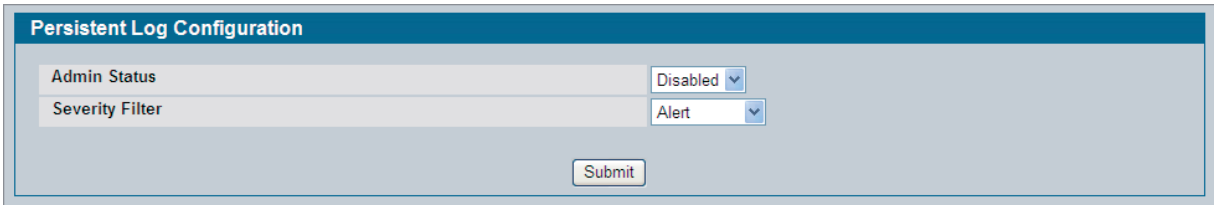


図 3-35　Persistent Log Configuration 画面

本画面には次の項目があります。

項目	説明
Admin Status	持続性ログの出力を有効または無効にします。 • Enabled - スイッチシリアルポートに割り当てられるデバイスにログメッセージを出力します。 • Disabled - スイッチシリアルポートに割り当てられるデバイスにログメッセージを出力しません。（初期値）
Severity Filter	コンソールに出力するためのログのレベルを選択します。選択したシステムレベル以上のログレベルを持つすべてのログを出力します。例えば、「Error」を選択すると、ログメッセージには「Error」、「Critical」、「Alert」および「Emergency」が含まれます。システムレベルの初期値は「Alert(1)」です。システムレベルは以下のレベルの 1 つです。 • Emergency - 最も高い警告レベル。デバイスがダウンまたは適切に機能していないと、ログがデバイスに保存されます。 • Alert - 2 番目に高い警告レベル。デバイスのすべての機能がダウンするなどの深刻なデバイスの動作不良がある場合に、ログが保存されます。 • Critical - 3 番目に高い警告レベル。2 つのデバイスポートが機能していなくてもデバイスの残りのポートが動作しているなどクリティカルなデバイスの動作不良が発生するとログが保存されます。 • Error - デバイスエラーはポートがオフラインである場合などに発生します。 • Warning - 最も低いレベルのデバイス警告。 • Notice - デバイス情報をネットワーク管理者に提供します。 • Infor - デバイス情報を提供します。 • Debug - ログに関する詳細情報を提供します。デバッグは適切なサポート部署の人によって照会されるものべきです。

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。

持続性ログの参照

持続性ログメッセージを参照します。

LAN タブ > Monitoring > Log > Persistent 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。

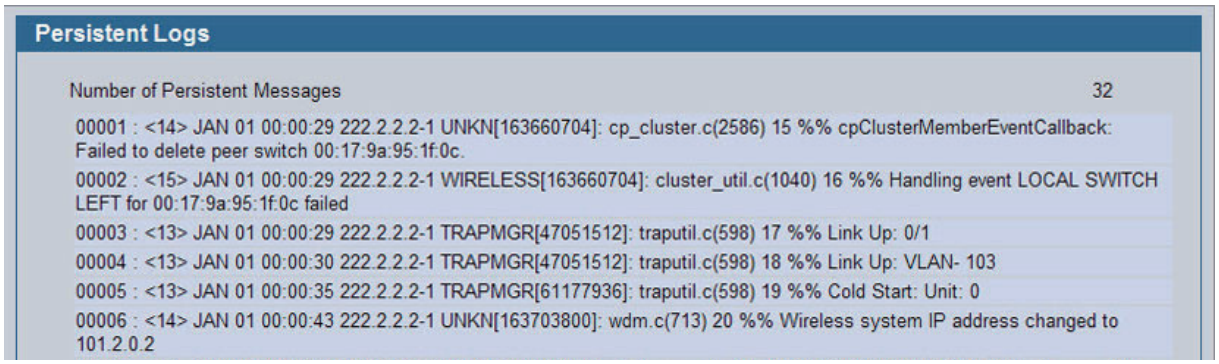


図 3-36　Persistent Logs 画面

本画面には次の項目があります。

項目	説明
Number of Persistent Messages	システムがログを出力した持続性メッセージの数を表示します。

「Apply」ボタンをクリックし、デバイスに SNTP 設定を適用します。

ページの残りはログメッセージを表示します。以下の例では non-stacking システムのログメッセージを示しています。

```
<15>Aug 24 05:34:05 STK0 MSTP[2110]: mspt_api.c(318) 237 %% Interface 12 transitioned to root
state on message age timer expiry
```

例

このログメッセージには、デバッグメッセージである 7(15 mod 8) のシステムレベルがあります。システムはスタックされていません (STK0)。メッセージはスレッド ID2110 で動作する MSTP コンポーネントで生成されています。メッセージはファイル「mstp_api.c」の 318 行目にあり、8 月 24 日 05:34:05 に生成されています。これは、ログ出力された 237 番目のメッセージです。

「Refresh」ボタンをクリックすると、最新のログエントリに更新します。

システムログ設定

設定したリモートログホストへのログメッセージの送信を許可します。

LAN タブ > Administration > Log > System Log 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。

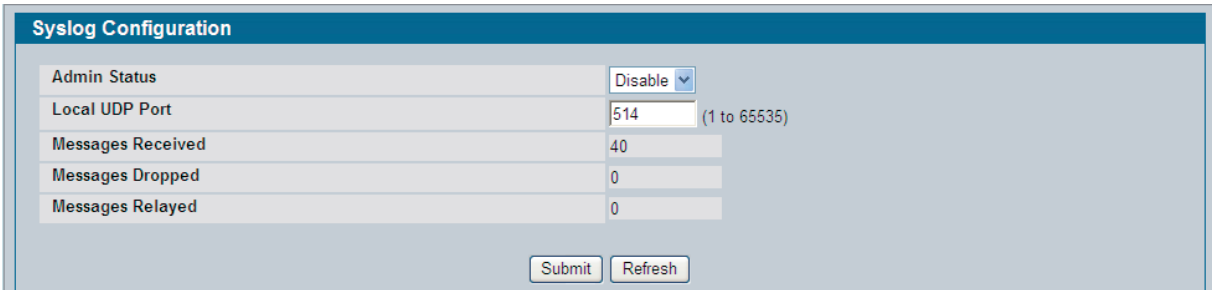


図 3-37　System Configuration 画面

本画面には次の項目があります。

項目	説明
Admin Status	スイッチに設定されたリモート Syslog ホストにログメッセージを送信するかどうかを指定します。 • Enable - 各ホストに設定された値を使用してすべての設定ホスト (Syslog コレクタまたはリレー) にメッセージを送信します。Syslog ホストの設定に関する情報については、「リモートホストの設定」(46 ページ) を参照してください。 • Disable - すべての Syslog ホストへのログ出力を停止します。どの Syslog コレクタ / リレーにもメッセージが送信されません。
Local UDP Port	Syslog メッセージが送信されるスイッチのポート (1-65535) を指定します。ポートの初期値は 514 です。
Messages Received	ログプロセスが受信するメッセージ数。これには、廃棄または無視されるメッセージも含まれます。
Messages Dropped	エラーまたはリソース不足のために処理できなかったメッセージの数。
Messages Relayed	Syslog ホストに対する Syslog 機能によって転送されたメッセージの数。複数のホストに送信されたメッセージは、各ホストの対して 1 つカウントされます。

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。

Telnet セッション

Telnet は端末をエミュレートする TCP/IP プロトコルです。ASCII 端末は、TCP/IP プロトコルのネットワークを通してローカルデバイスに仮想的に接続されます。Telnet はリモートログインが必要であるローカルな端末にログインする代替手段です。

スイッチは最大 5 個の同時 Telnet セッションをサポートしています。Telnet セッションを通じてすべての CLI コマンドを使用することができます。

以下の画面では、スイッチにおける内向きの Telnet 設定を制御することができます。内向きの Telnet セッションは、リモートシステムで生成され、そのシステム上のユーザがスイッチの CLI に接続することを許可します。リモートシステムにアクセスするためにスイッチに生成する Telnet セッションである外向きの Telnet 設定を行うためには、「アウトバウンド Telnet クライアントの設定」（50 ページ）を参照してください。

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

図 3-38　Telnet Session Configuration 画面

本画面には次の項目があります。

項目	説明
Telnet Session Timeout (minutes)	セッションがログオフされる前に Telnet セッションに起こる無通信の時間を指定します。1-160 の範囲で入力します。初期値は 5（分）です。 **注意** タイムアウトの値を変更すると、新しい値は直ちにすべてのアクティブおよびアクティブでないセッションに適用されます。新しいタイムアウト値よりも長くアイドル状態であったセッションは、すぐに切断されます。
Maximum Number of Telnet Sessions	許可する同時 Telnet セッション数を選択します。最大は 5 であり、これが初期値です。0 は、どんな外向き Telnet セッションも確立できないことを示します。
Allow New Telnet Sessions	新しい Telnet セッションを許可するかどうかを制御します。 • Yes - 許可された最大数に到達するまで、新しい Telnet セッションを許可します。 • No - 新しい Telnet セッションは許可されませんが、既存のセッションは切断されません。
Telnet Server Admin Mode	内向き Telnet セッションのための管理モード。この値を「Disable」に設定すると Telnet ポートはシャットダウンします。 admin モードが無効に設定されると、既存のすべての Telnet 接続が切断されます。初期値は有効です。

Telnet 項目を変更した場合、「Submit」ボタンをクリックして変更をスイッチに適用します。再起動後も新しい値をスイッチに保持する場合、保存を行う必要があります。

アウトバウンド Telnet クライアント設定

アウトバウンドTelnet機能はすべてのプラットフォームで利用可能というわけではありません。アウトバウンドTelnetクライアント設定を使用して、スイッチからリモートシステムに接続するTelnetセッションをコントロールします。

LAN タブ > Administration > Outbound Telnet Client Configuration を順にクリックし、以下の画面を表示します。

図 3-39　Outbound Telnet Client Configuration 画面

本画面には次の項目があります。

項目	説明
Admin Mode	アウトバウンド Telnet サービスを「Enable」または「Disable」にします。 • Enable - ユーザはスイッチの CLI でアウトバウンド Telnet セッションを初期化することができます。（初期値） • Disable - スイッチからアウトバウンドセッションを生成することはできません。
Maximum Sessions	許可するアウトバウンドセッションの最大数（0-5）を指定します。初期値は 5 です。
Session Timeout (minutes)	アウトバウンド Telnet のログインタイムアウトを指定します。初期値は 5（分）です。範囲は、1-160（分）です。

設定変更後、「Submit」ボタンをクリックします。再起動後も新しい値をスイッチに保持する場合、保存を行う必要があります。

Ping Test（Ping テスト）

本製品から指定した IP アドレスに Ping 要求を送信します。本製品が特定のネットワークホストと通信可能かをチェックするために使用します。

LAN タブ > Administration > 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。

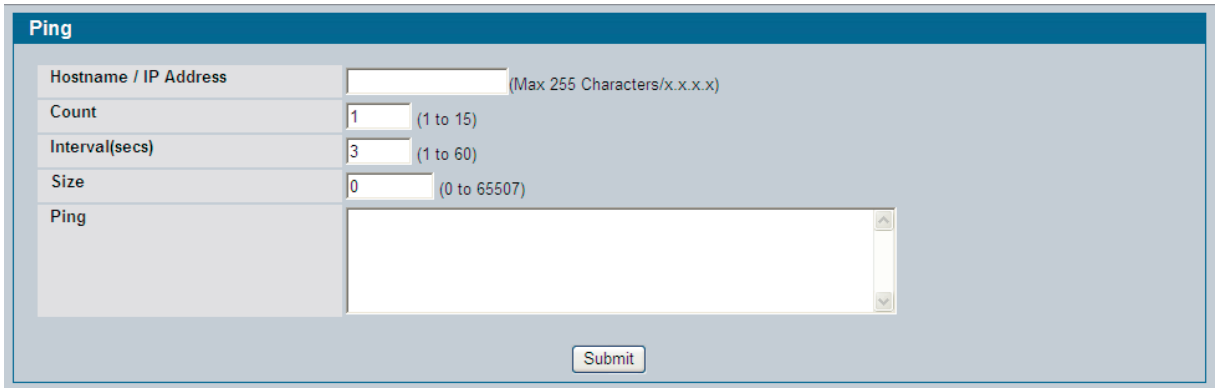


図 3-40　Ping 画面

本画面には次の項目があります。

項目	説明
Hostname/IP Address	Ping を行うホストの IP アドレスまたはホスト名を入力します。初期値は空白です。この情報は電源を切ると失われます。
Count	送信する Ping の数を指定します。
Interval (secs)	Ping を送信する間隔（秒）を指定します。
Size	送信する Ping パケットのサイズを指定します。
Ping	Ping の結果を表示します。

「Submit」をクリックして Ping を送信します。送信に成功すると「Ping」欄に結果が表示されます。

SNTP 設定

D-Link DWS-4000 シリーズスイッチのソフトウェアは、Simple Network Time Protocol（SNTP）をサポートしています。SNTP は正確なネットワークデバイスのクロックタイムの同期をミリ秒まで保証します。時刻同期はネットワーク SNTP サーバによって行われます。D-Link のソフトウェアは、SNTP クライアントとして動作し、他のシステムに時刻指定サービスを供給することはできません。

タイムソースは「Stratums」によって確立されます。「Stratums」は参照するクロックの精度を定義します。「Stratums」が高いほど（0 が最も高い）、クロックは正確です。デバイスは、自身が「Stratum 2」デバイスであるため、「Stratum 1」以上のものから時刻を受信します。

以下に「Stratums」の例を示します。
- Stratum 0 - リアルタイムクロックはタイムソース（例えば、GPS システム）として使用されます。
- Stratum 1 -「Stratum 0」のタイムソースに直接にリンクするサーバが使用されます。「Stratum 1」タイムサーバはプライマリネットワークの時刻の標準を提供します。
- Stratum 2 - タイムソースは、ネットワーク経路の上の「Stratum1」サーバから離れた場所にあります。例えば、「Stratum2」サーバは NTP を通して「Stratum1」サーバからネットワークリンクを経由して時刻を取得します。

SNTP サーバから受信した情報は、時刻レベルとサーバタイプに基づいて評価されます。

SNTP 時刻の定義は、以下の時刻レベルで評価されて、決定されます。
- T1 - オリジナルのリクエストがクライアントによって送信された時刻。
- T2 - オリジナルのリクエストがサーバによって受信された時刻。
- T3 - サーバが応答を送信した時刻。
- T4 - クライアントがサーバの応答を受信した時刻。

デバイスはサーバにユニキャストとブロードキャストサーバタイプの時刻をポーリングします。

ユニキャスト情報へのポーリングは、IP アドレスが既知のサーバにポーリングするために使用されます。デバイスに設定された SNTP サーバだけが同期情報のためにポーリングされます。T1 から T4 は、サーバ時刻を決定するのに使用されます。これは最も安全な方式であるため、デバイス時刻を同期するのに適した方法といえます。この方法を選択すると、「SNTP Server Configuration」画面を使用してデバイスに定義された SNTP サーバから SNTP 情報を受け取ります。

ブロードキャスト情報は、サーバ IP アドレスが未知である場合に使用されます。SNTP サーバからブロードキャストメッセージを送信する場合、SNTP クライアントはメッセージをリッスンします。ブロードキャストポーリングが有効であると、デバイスからリクエストされていなくても、どんな同期情報も受け取ります。これは最も安全性が低い方法です。

主体的に情報をリクエストするか、またはポーリング間隔でデバイスは同期情報を検索します。ユニキャストとブロードキャストポーリングが有効になると、情報はこの順で検索されます。
- デバイスに定義されたサーバからの情報が選択されます。ユニキャストポーリングが有効でない場合、またはデバイスに定義されたサーバがない場合、デバイスは応答するどんな SNTP サーバからの時刻情報も受け付けます。
- 1 つ以上のユニキャストデバイスが応答する場合、同期情報は最も低い Stratum を持つデバイスから選択されます。
- サーバに同じ Stratum があると、最初に応答した SNTP サーバから同期情報を受け取ります。

MD5（MessageDigest5）認証は、SNTP サーバへのデバイス同期パスを保護します。MD5 は、128 ビットのハッシュを生成するアルゴリズムです。MD5 は MD4 のバリエーションであり、MD4 セキュリティを増強したものです。MD5 は通信の保全を検証し、通信の送信元を認証します。

SNTP では以下の機能の参照または設定を行うことができます。
- SNTP 設定
- SNTP サーバの設定
- SNTP サーバステータス
- SNTP グローバルステータス
- タイムゾーン設定
- サマータイム設定
- クロック設定の参照

SNTP 設定

SNTP のグローバルなパラメータを参照および調整します。

LAN タブ > Administration > SNTP > SNTP 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。

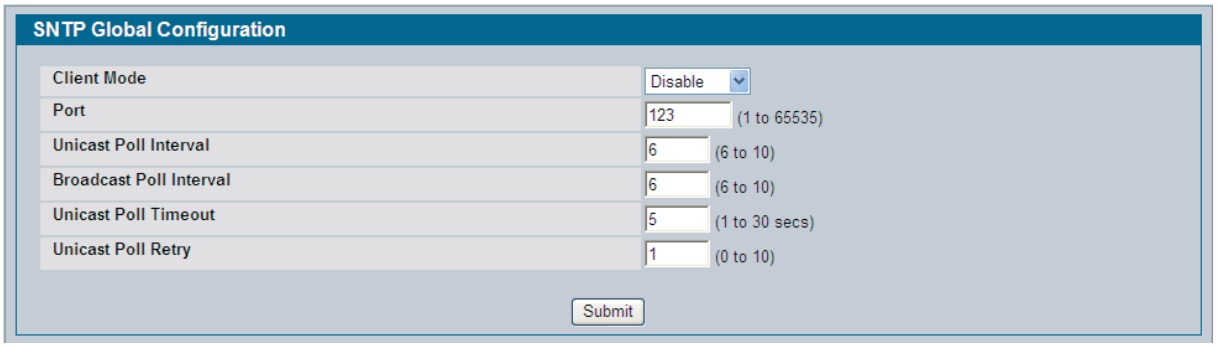


図 3-41　SNTP Global Configuration 画面

本画面には次の項目があります。

項目	説明
Client Mode	SNTP クライアントモードを指定します。以下のモードの 1 つを選択します。 • Disable - SNTP は無効です。クライアントからの SNTP リクエストが送信されないか、処理する SNTP メッセージも受信しません。 • Unicast - SNTP は、ポイント・ツー・ポイントで動作します。ユニキャストクライアントは、ユニキャストアドレスに指定したサーバにリクエストを送信し、それが時間、オプションで往復の遅延とサーバへのローカルなクロックオフセットを決定する応答を待ちます。 • Broadcast - SNTP はマルチキャストモードと同じ方法で動作しますが、マルチキャストアドレスの代わりにローカルなブロードキャストアドレスを使用します。ブロードキャストアドレスには、単一のサブネット範囲があり、一方、マルチキャストアドレスにはインターネット範囲があります。
Port	応答 / ブロードキャストにリッスンするためにローカルの UDP ポート（1-65535）を指定します。初期値は 123 です。
Unicast Poll Interval	ユニキャストモードに設定した場合にユニキャストポーリングリクエストの間隔（秒）を指定します。許可される範囲は、6-10（秒）です。初期値は 6（秒）です。
Broadcast Poll Interval	ブロードキャストモードに設定した場合にブロードキャストポーリングリクエストの間隔（秒）を指定します。この間隔の終了前に受信したブロードキャストは破棄されます。許可される範囲は、6-10（秒）です。初期値は 6（秒）です。
Unicast Poll Timeout	ユニキャストモードに設定した場合に SNTP の応答を待つ時間（秒）を指定します。許可される範囲は、1-30（秒）です。初期値は 5（秒）です。
Unicast Poll Retry	ユニキャストモードに設定した場合に最初のタイムアウト後、次に設定されたサーバの使用を試みる前に SNTP サーバにリクエストを再度行う回数を指定します。許可される範囲は、0-10 です。初期値は 1 です。

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。

SNTP サーバの設定

SNTP サーバの情報の参照および変更を行います。

LAN タブ > Administration > SNTP > SNTP Server 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。

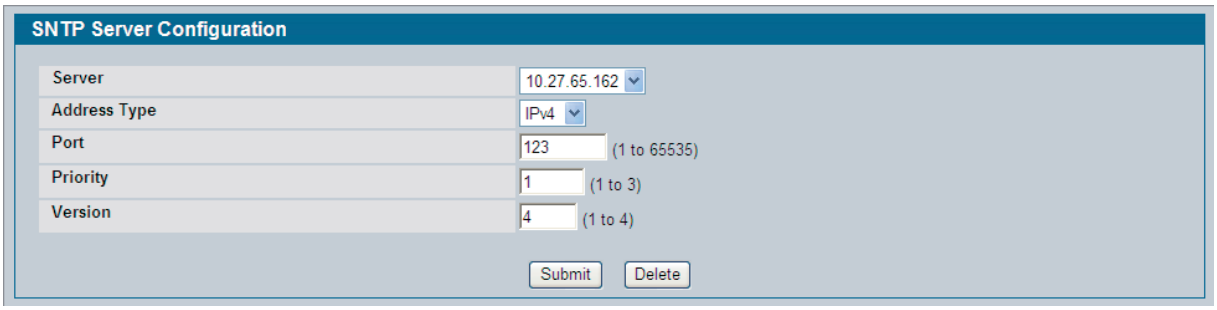


図 3-42　SNTP Server Configuration 画面 - 編集

本画面には次の項目があります。

項目	説明
Server	SNTP サーバの IP アドレスを選択し、SNTP サーバに関する情報の参照または変更を行います。最大 3 つの SNTP サーバを定義できます。
Address / Hostname	SNTP サーバの IP アドレスまたはホスト名を入力します。
Address Type	IPv4 アドレスを入力した場合には、「IPv4」を選択し、ホスト名を入力した場合には「DNS」を選択します。
Port	1-65535 の範囲でポート番号を入力します。初期値は 123 です。
Priority	SNTP リクエストが送信される一連のサーバを決定するために、このサーバエントリの優先度を指定します。値は 1-3 で、初期値は 1 です。最も下位の番号を持つサーバに優先権があります。
Version	プロトコルバージョン番号を入力します。値は 1-4 で、初期値は 4 です。

SNTP の追加

SNTP サーバを追加するためには、「Server」リストから「Create」を選択し、希望に応じて残りの欄を入力して「Submit」ボタンをクリックします。SNTP サーバは追加され、「Server」リストに反映されます。再起動後にも変更を保持するためには保存する必要があります。

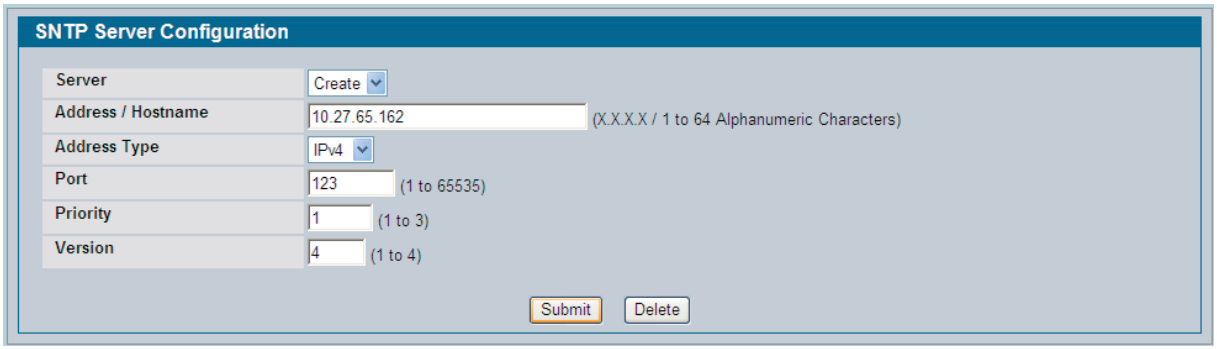


図 3-43　SNTP Server Configuration 画面 - Create

SNTP の削除

SNTP サーバを削除するためには、「Server」リストから削除するサーバの IP アドレスを選択し、「Delete」ボタンをクリックします。エントリは削除され、デバイスが更新されます。

SNTP サーバステータス

スイッチに設定した SNTP サーバに関するステータス情報を表示します。

LAN タブ > Monitoring > SNTP Summary > Server 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。

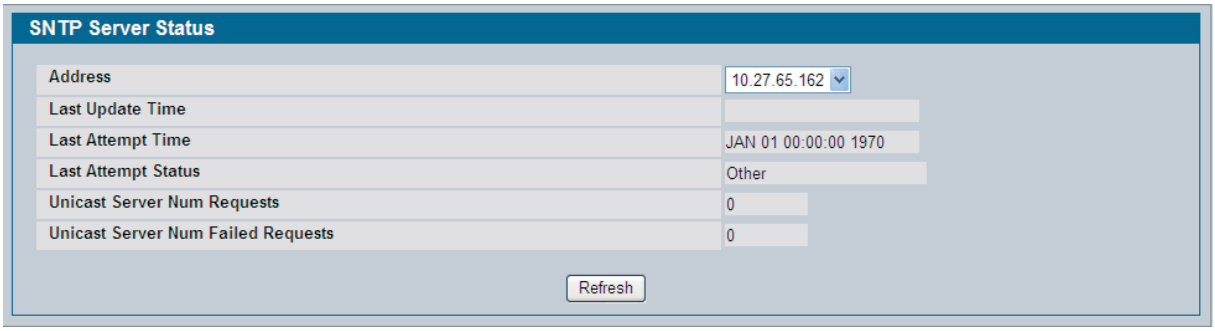


図 3-44　SNTP Server Status 画面

本画面には次の項目があります。

項目	説明
Address	既存のサーバアドレスをすべて表示します。サーバ設定が存在しない場合、画面には「No SNTP server exists」というメッセージが表示されます。
Last Update Time	本サーバからの応答によりシステムクロックを更新するのに使用したローカルな日時（UTC）を表示します。
Last Attempt Time	この SNTP サーバに最後に問い合わせをしたローカルな日時（UTC）を表示します。
Last Attempt Status	このサーバへの最後の SNTP リクエストのステータスを表示します。このサーバからパケットを受信していない場合、「Other」というステータスを表示します。 • Other - 以下のあげる値のいずれにも該当しません。 • Success - SNTP 操作は成功し、システム時刻が更新されました。 • Request Timed Out - 指示された SNTP リクエストは SNTP サーバからの応答を受信せずにタイムアウトになりました。 • Bad Date Encoded - SNTP サーバによって提供された時間が有効ではありません。 • Version Not Supported - サーバがサポートする SNTP バージョンは、クライアントがサポートするバージョンと互換性がありません。 • Server Unsynchronized - SNTP サーバはピアと同期しません。これは SNTP メッセージの「leap indicator」フィールドを経由して示されます。 • Server Kiss Of Death - このサーバに対してどんなクエリも送信されなかったことを示します。これはサーバから受信したメッセージ内の 0 と等しい「stratum」フィールドによって示されます。
Unicast Server Num Requests	最後のエージェントの再起動以来、このサーバに行われた SNTP リクエストの数を示します。
Unicast Server Num Failed Requests	最後の再起動以来、このサーバに行われたエラーとなった SNTP リクエストの数を示します。

「Refresh」ボタンをクリックし、システムの情報を最新に更新します。

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。

SNTP グローバルステータス

システムの SNTP クライアントに関する情報を参照します。

LAN タブ > Monitoring > SNTP Summary > Global 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。

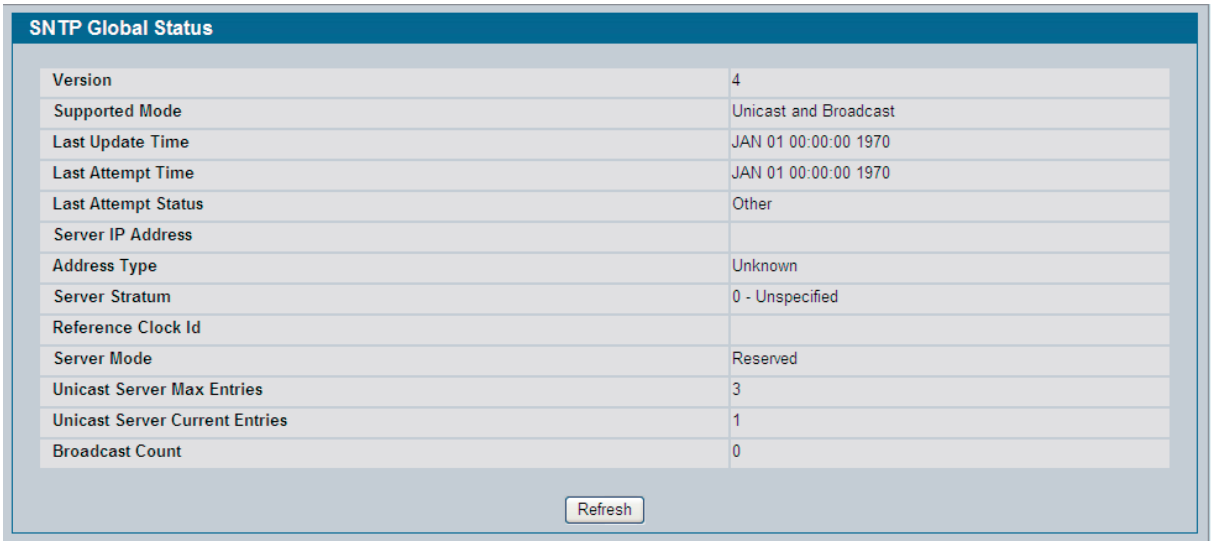


図 3-45　SNTP Global Status 画面

本画面には次の項目があります。

項目	説明
Version	クライアントがサポートする SNTP バージョンを表示します。
Supported Mode	クライアントがサポートする SNTP モードを表示します。クライアントは複数のモードをサポートしている可能性があります。
Last Update Time	システムクロックを最後に更新したローカルな日時 (UTC) を表示します。
Last Attempt Time	最後の SNTP リクエスト、または unsolicited メッセージを受信したローカルな日時 (UTC) を表示します。
Last Attempt Status	ユニキャストおよびブロードキャストモードの両方への SNTP リクエスト、または unsolicited メッセージのステータスを表示します。サーバからメッセージを受信していない場合、「Other」というステータスを表示します。 • Other - 以下のあげる値のいずれにも該当しません。 • Success - SNTP 操作は成功し、システム時刻が更新されました。 • Request Timed Out - 指示された SNTP リクエストは SNTP サーバからの応答を受信せずにタイムアウトになりました。 • Bad Date Encoded - SNTP サーバによって提供された更新が有効ではありません。 • Version Not Supported - サーバがサポートする SNTP バージョンは、クライアントがサポートするバージョンと互換性がありません。 • Server Unsynchronized - SNTP サーバはピアと同期しません。これは SNTP メッセージの「leap indicator」フィールドを経由して示されます。 • Server Kiss Of Death - このサーバに対してどんなクエリも送信されなかったことを示します。これはサーバから受信したメッセージ内の 0 と等しい「stratum」フィールドによって示されます。
Server IP Address	最後に受信した有効なパケットに対するサーバの IP アドレスを指定します。どんなサーバからもメッセージを受信していない場合、「empty」という文字列を表示します。
Address Type	最後に受信した有効なパケットに対する SNTP サーバのアドレスタイプを表示します。
Server Stratum	最後に受信した有効なパケットに対してサーバが要求した「stratum」を表示します。
Reference Clock Id	最後に受信した有効なパケットに対するサーバの参照用のクロック識別子を表示します。
Server Mode	最後に受信した有効なパケットに対するサーバモードを表示します。
Unicast Sever Max Entries	このクライアントに設定できるユニキャストサーバエントリの最大数を表示します。
Unicast Server Current Entries	このクライアントに設定されている現在の有効なユニキャストサーバエントリの数を表示します。
Broadcast Count	最後に再起動から、SNTP クライアントが受信して処理した unsolicited ブロードキャスト SNTP メッセージの数を表示します。

「Refresh」ボタンをクリックし、システムの情報を最新に更新します。

タイムゾーン設定

協定世界時（UTC）からタイムゾーンのオフセットを設定します。

LAN タブ > Administration > SNTP > Time Zone 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。

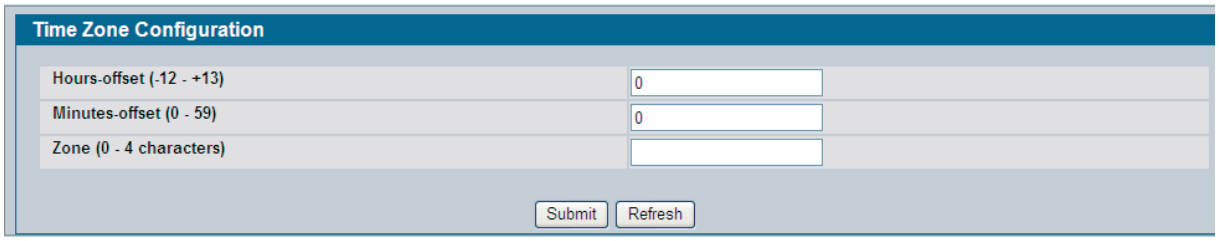


図 3-46　Time Zone Configuration 画面

エントリの新規登録

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

本画面には次の項目があります。

項目	説明
Hours-offset (-12 - +13)	UTC からオフセット（時）を設定します。（範囲 : -12 ～ +13）
Minutes-offset (0 - 59)	UTC からのオフセット（分）を設定します。（範囲 : 0-59）
Zone (0 - 4 characters)	タイムゾーンの頭字語を設定します。（範囲 : 0-4 文字）

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。

Summer Time Configuration（サマータイム設定）

「Summer Time Configuration」画面を使用して、定義済みのサマータイムとオフセットを指定します。

LAN タブ > Administration > SNTP > Summer Time 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。

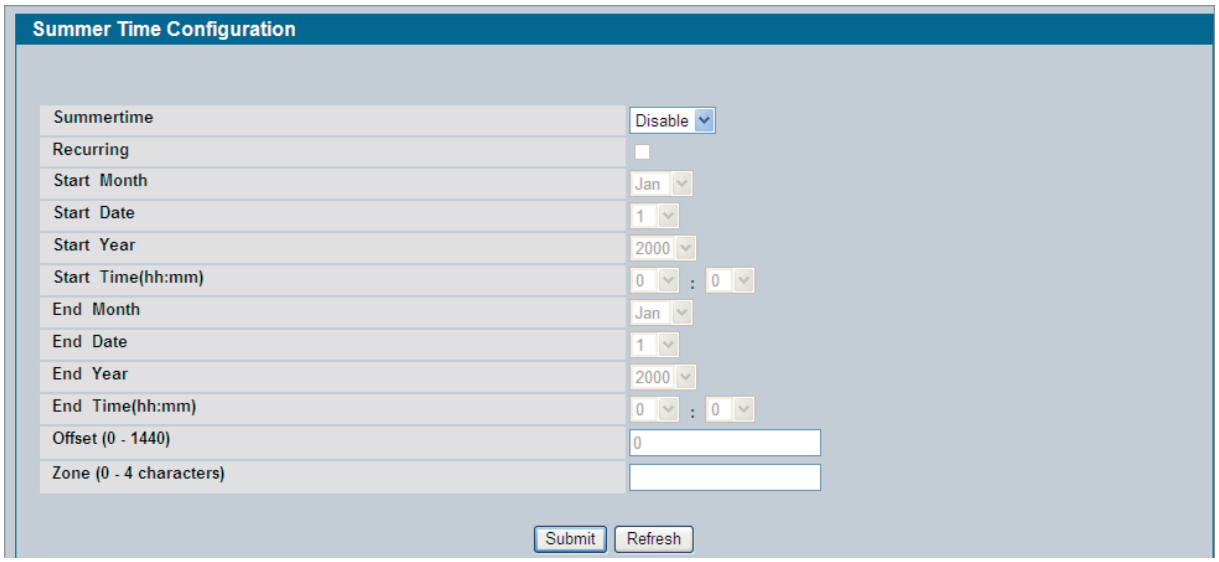


図 3-47　Summer Time Configuration 画面

サマータイムの繰り返し設定

「Recurring」チェックボックスをクリックすると、設定は毎年繰り返されることを示します。「Recurring」を選択すると、以下の画面の表示が変わります。

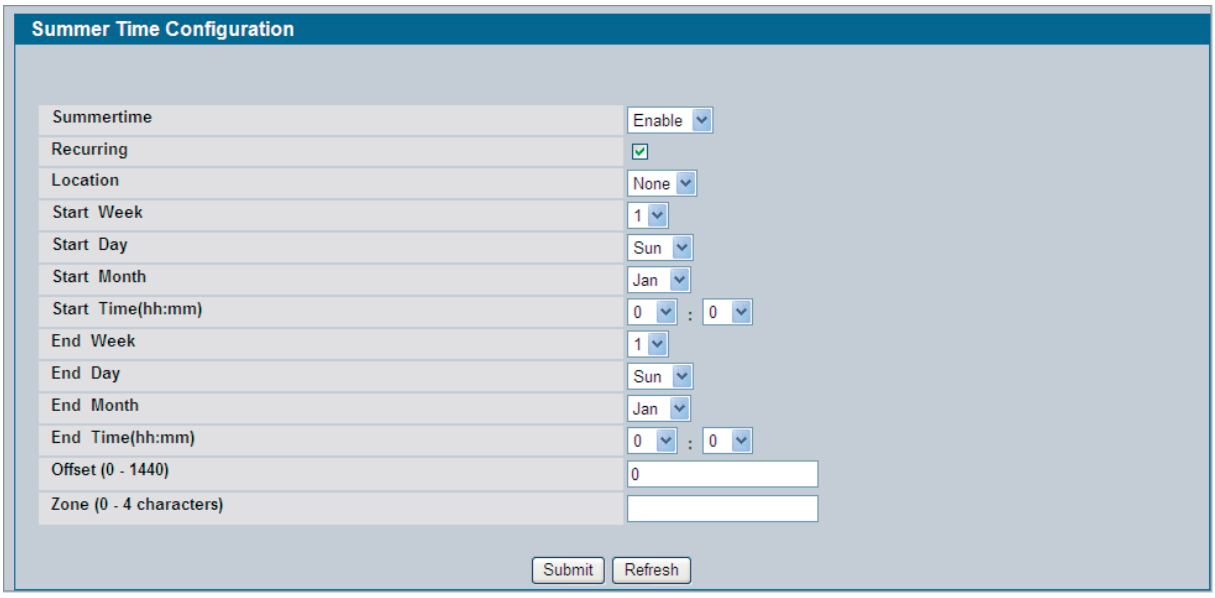


図 3-48　Summer Time Configuration 画面 - Recrring

本画面には次の項目があります。

項目	説明
Summertime	サマータイムモードを有効または無効にします。
Recurring	チェックボックスを選択して、設定が毎年繰り返されるように設定します。
Location	「Recurring」チェックボックスを選択した場合だけ、本項目は表示されます。サマータイム設定は、米国と EU 用に事前に定義されています。米国か EU 以外の場所でサマータイムを設定するためには、「None」を選択します。
Start Month	開始月を選択します。
Start Date	開始日を選択します。「Recurring」チェックボックスをクリアした場合だけ、本項目は表示されます。
Start Year	開始年を選択します。「Recurring」チェックボックスをクリアした場合だけ、本項目は表示されます。
Start Time (hh:mm)	hh:mm 形式で開始時間を選択します。
End Month	終了月を選択します。
End Date	終了日を選択します。「Recurring」チェックボックスをクリアした場合だけ、本項目は表示されます。
End Year	終了年を選択します。「Recurring」チェックボックスをクリアした場合だけ、本項目は表示されます。
End Time (hh:mm)	hh:mm 形式で終了時間を選択します。
Offset 0 - 1440)	サマータイムの間に追加する時間（分）を 0-1440 の範囲で設定します。
Zone (1 - 4 characters)	タイムゾーンの頭字語を設定すると、サマータイムが有効になった場合に表示されます。0-4 文字の範囲で指定します。

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。

クロック設定の参照

現在の時刻、タイムゾーン、およびサマータイム設定に関する情報を表示します。

LAN タブ > Monitoring > Clock Detail の順にメニューをクリックし、以下の画面を表示します。ここでは、サマータイムが有効になる日時を表示します。

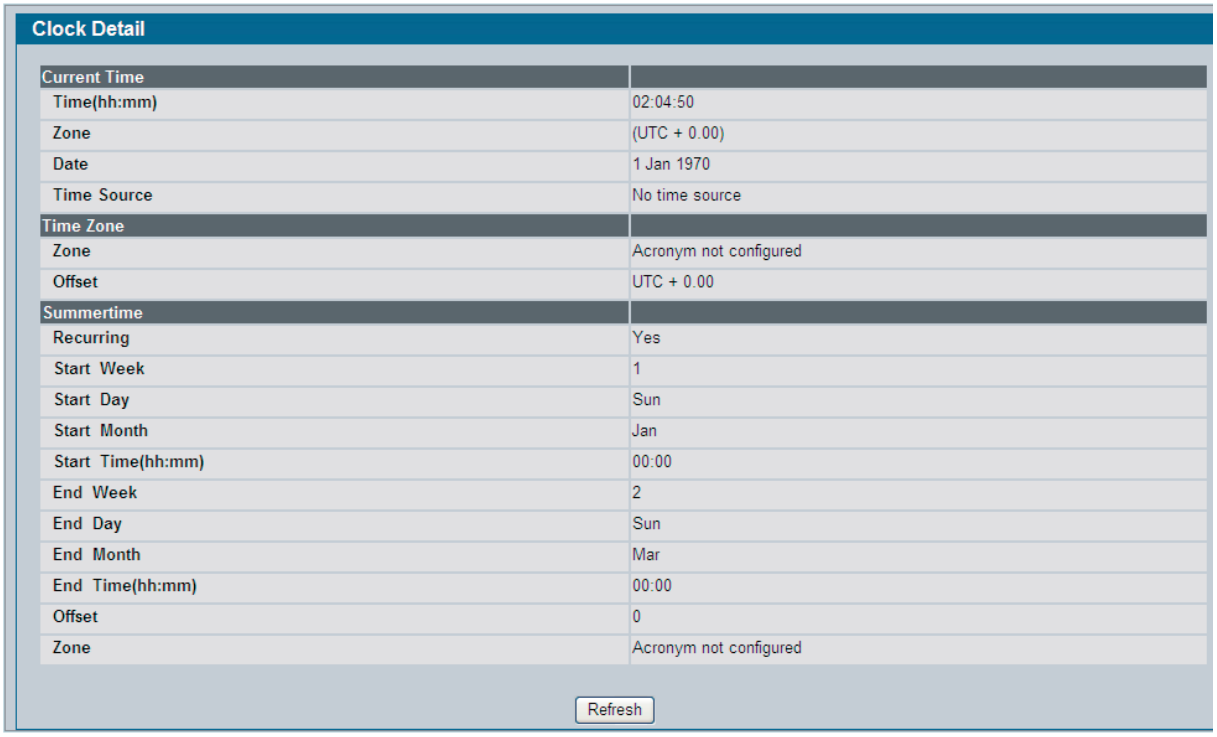


図 3-49　Clock Detail 画面

本画面には次の項目があります。

項目	説明
Current Time	現在の時刻を表示します。
Time Zone	タイムゾーン設定を表示します。
Summertime	サマータイム設定を表示します。

「Refresh」ボタンをクリックすると、最新の情報に更新されます。

デバイススロット情報の設定と参照

スイッチのスロットにインストールされたカードに関する情報を表示します。スロットの物理的な位置は、D-Linkのソフトウェアが動作しているハードウェアによって異なります。また、いくつかのプラットフォームにおけるカードに関する情報を手動で設定することができます。

カード設定

スイッチに設定済みのカードの情報を参照します。いくつかのプラットフォームでは、スロットに関する情報を手動で設定することができます。

LAN タブ > Administration > Card 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。本画面は、スロットにカードが挿入されている場合に項目を表示します。

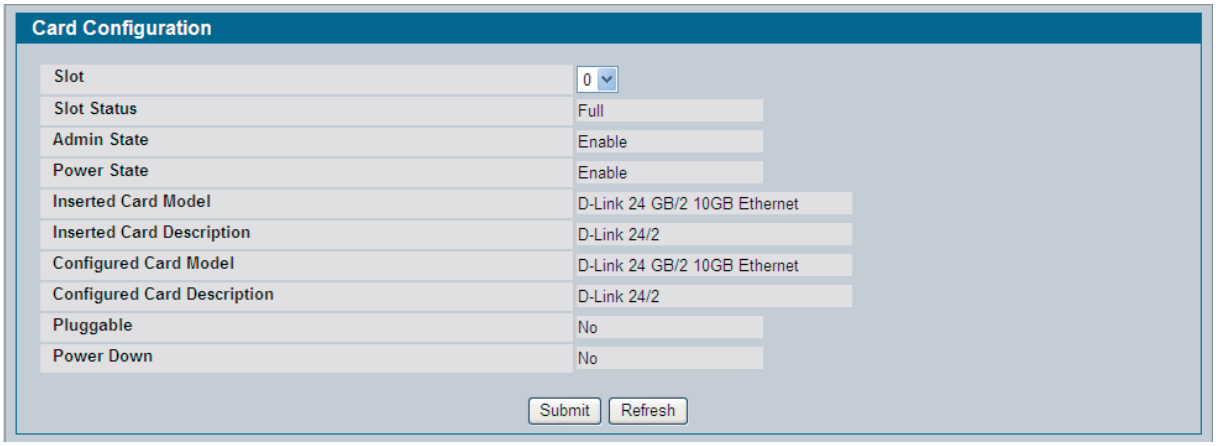


図 3-50　Card Configuration 画面

本画面には次の項目があります。

項目	説明
Unit	データを表示または設定するスタック内のユニットを指定します。
Slot	データを表示または設定する選択ユニット内のスロットを指定します。
Slot Status	カードがスロットにあるか否かを表示します。 • Full - 挿入済み • Empty - 空
Admin State	スロットが管理上有効または無効であるかを表示します。読取専用ユーザは、本項目を設定することはできません。
Power State	スロットの電源状態（オンまたはオフ）を表示します。読取専用ユーザは、本項目を設定することはできません。
Card Type	スロットに挿入可能なサポートするカードの種類をリスト表示します。これは、カードが挿入されておらず、まだ設定をしていないスロットに対してだけ有効です。読取専用ユーザは、本項目を参照することはできません。
Inserted Card Model	選択スロットに挿入されているカードのモデル識別子を表示します。カードが挿入されていないと、本項目は表示されません。
Inserted Card Description	選択スロットに挿入されているカードの説明文を表示します。カードが挿入されていないと、本項目は表示されません。
Configured Card Model	選択スロットに設定済みのカードモデルの識別子を表示します。事前に設定したカードがないと、本項目は表示されません。
Configured Card Description	選択スロットに設定済みのカードモデルの識別子を表示します。事前に設定したカードがないと、本項目は表示されません。
Pluggable	指定スロットの挿入可能状態を表示します。
Power Down	指定スロットの電源状態を表示します。

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。

カード設定の削除

「Clear」ボタンをクリックし、カードが挿入されていないスロットにおけるカードの事前設定を削除します。スロットにカードが挿入されている場合、またはスロットにカードを挿入されておらず事前に設定したカードがない場合、本ボタンは表示されません。

スロットのサマリ

スタック内の各ユニットのスロットに関する情報を表示します。

LAN タブ > Monitoring > Slot 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。

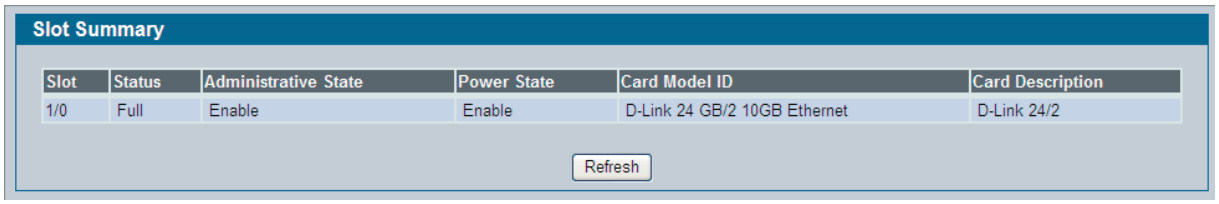


図 3-51　Slot Summary 画面

本画面には次の項目があります。

項目	説明
Slot	Unit/Slot の形式を使用してスロットを示します。
Status	スロットが空か挿入済みかどうかを表示します。
Administrative State	スロットが管理上有効または無効であるかを表示します
Power State	スロットの電源状態「Enable」（オン）または「Disable」（オフ）を表示します。
Card Model ID	スロットに設定済みのカードモデルの識別子を表示します。
Card Description	スロットに設定済みのカードの説明文を表示します。

「Refresh」ボタンをクリックし、システムの情報を最新に更新します。

デバイスポート情報の設定と参照

スイッチで有効なポートの物理ポート情報を参照またはモニタします。
「Port」フォルダには以下の画面へのリンクがあります。

- ポート設定
- ポートのサマリ
- ポートの説明

ポート設定

スイッチの物理インタフェースを設定します。

LAN タブ > Administration > Port Configuration > Host 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。

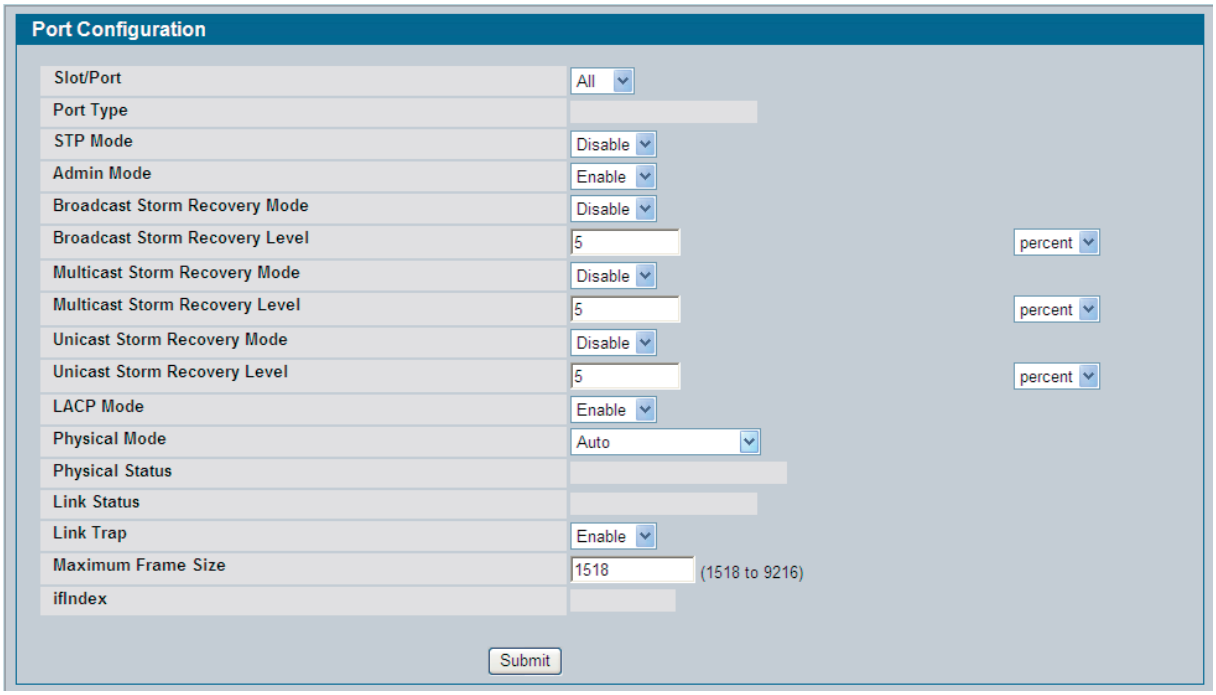


図 3-52　Port Configuration 画面

本画面には次の項目があります。

項目	説明
Slot/Port	メニューからポートを選択して、そのポートにデータを表示、設定します。 • All - 本画面で行った変更は、すべての物理ポートに適用されます。
Port Type	ポートタイプを表示します。多くのポートでは、本欄は空白です。 • Mirrored - ポートはモニタするポートとして設定され、ポートミラーリングセッションにおけるソースポートであることを示します。ポートモニタリングとポート検証に関する詳しい情報に関しては、「マルチプルポートミラーリング」（66 ページ）を参照してください。 • Probe - ポートはモニタするポートとして設定され、ポートミラーリングセッションにおける宛先ポートであることを示します。ポートモニタリングとポート検証に関する詳しい情報に関しては、「マルチプルポートミラーリング」（66 ページ）を参照してください。 • Port Channel - ポートは、リンクアグリゲーション（LAG）として知られるポートチャンネルのメンバとして設定されていることを示します。ポートチャンネルの設定に関する情報に関しては、「ポートチャンネルの作成（トランキング）」（150 ページ）を参照してください。
STP Mode	ポートまたは LAG に STP（Spanning Tree Protocol ）の管理モードを設定します。STP に関する詳しい情報は、「スパニングツリープロトコルの設定」（155 ページ）を参照してください。本項目で可能な値は以下の通りです。 • Enable - このポートに対して STP を有効にします。 • Disable - このポートに対して STP を無効にします。
Admin Mode	ポートコントロールの管理状態を選択します。 • Enable - ポートはネットワークに参加可能です。（初期値） • Disable - ポートは管理的にダウンしており、ネットワークに参加していません。

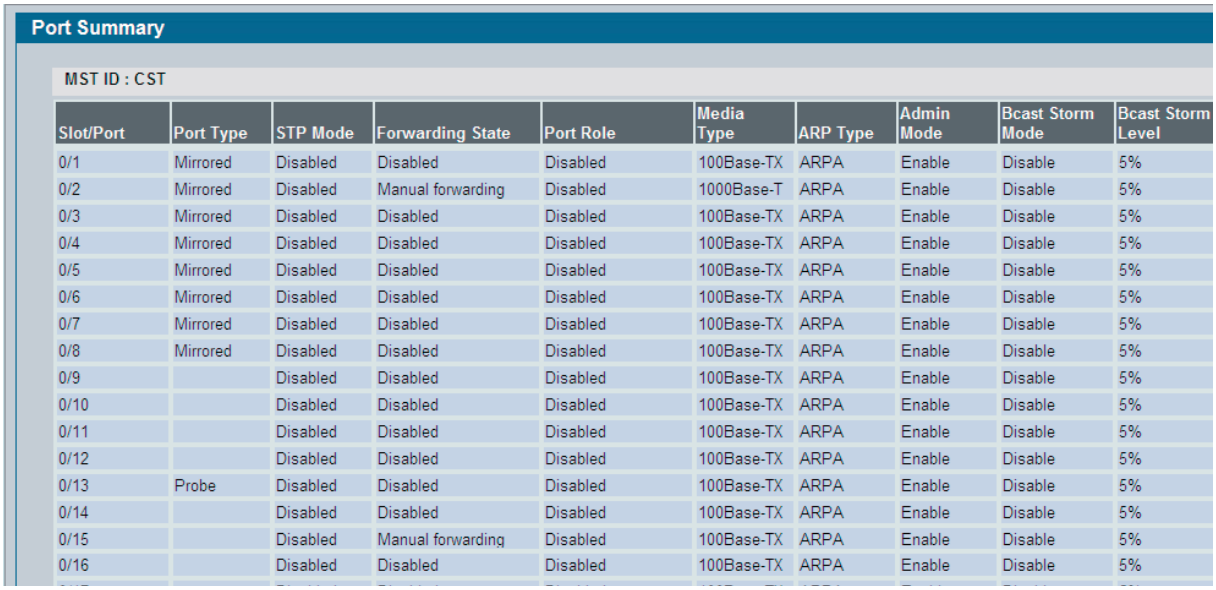
項目	説明
Broadcast Storm Recovery Mode	以下の 1 つを選択し、本オプションを有効または無効にします。 • Enable - 指定のイーサネットポートにおいてブロードキャストトラフィックがしきい値を超過した場合、スイッチはブロードキャストトラフィックを防御（廃棄）します。 • Disable - ポートのトラフィックがしきい値を超過しても、ポートはブロードキャストトラフィックを防御しません。（初期値）
Broadcast Storm Recovery Level	いずれかのストーム制御がアクティブになるデータ速度を指定します。値は、ポートスピードの割合であり、0-100 で指定します。初期値はポートスピードの 5% です。
Multicast Storm Recovery Mode	以下の 1 つを選択し、本オプションを有効または無効にします。 • Enable - 指定したイーサネットポートにおけるマルチキャストトラフィックが設定したしきい値を超過した場合、スイッチはマルチキャストトラフィックを防御（廃棄）します。 • Disable - ポートのトラフィックが設定したしきい値を超過しても、スイッチはマルチキャストトラフィックを防御しません。（初期値）
Multicast Storm Recovery Level	いずれかのストーム制御がアクティブになるデータ速度を指定します。値は、ポートスピードの割合であり、0-100 で指定します。初期値はポートスピードの 5% です。
Unicast Storm Recovery Mode	以下の 1 つを選択し、本オプションを有効または無効にします。 • Enable - 指定したイーサネットポートでユニキャストトラフィックが設定したしきい値を超過した場合、スイッチはユニキャストトラフィックを防御（廃棄）します。 • Disable - ユニキャストトラフィックが設定したしきい値を超過しても、スイッチはユニキャストトラフィックを防御しません。（初期値）
Unicast Storm Recovery Level	いずれかのストーム制御がアクティブになるデータ速度を指定します。これはポートスピードの割合であり、0-100 で指定します。初期値はポートスピードの 5% です。
LACP Mode	「Link Aggregation Control Protocol」管理ステートを選択します。 • Enable - ポートがポートチャンネル（LAG）に参加することを許可します。（初期値） • Disable - ポートはポートチャンネル（LAG）に参加できません。
Physical Mode	ポートのスピードとデュプレックスモードを選択します。 「Slot/Port」が「All」に設定され、「Auto」以外の物理モードを適用する場合、モードは適切なインタフェースすべてに適用されます。 • Auto - デュプレックスモードとスピードはオートネゴシエーション処理によって設定されます。ポートの最大性能（フルデュプレックスと 100Mbps）が通知されます。 • <Speed> Half Duplex - メニューから選択可能なポートスピードは、D-Link のソフトウェアが動作しているプラットフォームと選択するポートによって異なります。ハーフデュプレックスモードでは、伝送は一方向であり、ポートは、同時にトラフィックを送受信できません。 • <Speed> Full Duplex - メニューから選択可能なポートスピードは、D-Link のソフトウェアが動作しているプラットフォームと選択するポートによって異なります。フルデュプレックスモードでは、伝送は双方向であり、ポートは、同時にトラフィックを送受信できます。
Physical Status	ポートのスピードとデュプレックスモードを示します。
Link Status	リンクが「Up」（アクティブ）または「Down」（ダウン）しているかを表示します。
Link Trap	リンクステータスを変更した場合にトラップを送信するかどうかを決定します。 • Enable - リンクステータスが変更した場合に、システムはトラップを送信します。（初期値） • Disable - リンクステータスが変更した場合に、システムはトラップを送信しません。
Maximum Frame Size	インタフェースがサポートする最大のイーサネットフレームサイズを表示または設定します。フレームサイズにはイーサネットヘッダ、CRC、およびペイロードが含まれます。範囲は、1518-9216 です。最大フレームサイズの初期値は 1518 です。
ifIndex	本ポートに関連するインタフェーステーブルのエントリの ifIndex を表示します。「Slot/Port」に「All」が設定されていると、本項目は空白です。

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。

ポートのサマリ

プラットフォームにおけるすべての物理ポートに対する設定を参照します。

LAN タブ > Monitoring > Port Utilization > 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。



Port Summary

MST ID : CST

Slot/Port	Port Type	STP Mode	Forwarding State	Port Role	Media Type	ARP Type	Admin Mode	Bcast Storm Mode	Bcast Storm Level
0/1	Mirrored	Disabled	Disabled	Disabled	100Base-TX	ARPA	Enable	Disable	5%
0/2	Mirrored	Disabled	Manual forwarding	Disabled	1000Base-T	ARPA	Enable	Disable	5%
0/3	Mirrored	Disabled	Disabled	Disabled	100Base-TX	ARPA	Enable	Disable	5%
0/4	Mirrored	Disabled	Disabled	Disabled	100Base-TX	ARPA	Enable	Disable	5%
0/5	Mirrored	Disabled	Disabled	Disabled	100Base-TX	ARPA	Enable	Disable	5%
0/6	Mirrored	Disabled	Disabled	Disabled	100Base-TX	ARPA	Enable	Disable	5%
0/7	Mirrored	Disabled	Disabled	Disabled	100Base-TX	ARPA	Enable	Disable	5%
0/8	Mirrored	Disabled	Disabled	Disabled	100Base-TX	ARPA	Enable	Disable	5%
0/9		Disabled	Disabled	Disabled	100Base-TX	ARPA	Enable	Disable	5%
0/10		Disabled	Disabled	Disabled	100Base-TX	ARPA	Enable	Disable	5%
0/11		Disabled	Disabled	Disabled	100Base-TX	ARPA	Enable	Disable	5%
0/12		Disabled	Disabled	Disabled	100Base-TX	ARPA	Enable	Disable	5%
0/13	Probe	Disabled	Disabled	Disabled	100Base-TX	ARPA	Enable	Disable	5%
0/14		Disabled	Disabled	Disabled	100Base-TX	ARPA	Enable	Disable	5%
0/15		Disabled	Manual forwarding	Disabled	100Base-TX	ARPA	Enable	Disable	5%
0/16		Disabled	Disabled	Disabled	100Base-TX	ARPA	Enable	Disable	5%

図 3-53　Port Summary 画面

本画面には次の項目があります。

項目	説明
MST ID	Spanning Tree Protocol がスイッチで有効であると、スパニングツリーのパラメータに表示される値を決定するために、現在設定しているすべての MST ID のリストから MST インスタンス ID を選択することができます。 選択した MST ID を変更すると、画面は更新されます。STP（初期値）が無効になると、「MST ID」欄はメニューの代わりにスタティックな値の「CST」を表示します。
Slot/Port	残りの列にある情報が関連するポートを表示します。本項目は、スタックなしのプラットフォーム用です。
Port Type	ポートタイプを表示します。多くのポートでは、本欄は空白です。 • Mirrored - ポートはモニタするポートとして設定され、ポートミラーリングセッションにおけるソースポートであることを示します。 • Probe - ポートはモニタするポートとして設定され、ポートミラーリングセッションにおける宛先ポートであることを示します。ポートモニタリングとポート検証に関する詳しい情報に関しては、「マルチプルポートミラーリング」（66 ページ）を参照してください。 • Port Channel - ポートは、リンクアグリゲーション（LAG）として知られるポートチャンネルのメンバとして設定されていることを示します。ポートチャンネルの設定に関する情報に関しては、「ポートチャンネルの作成（トランキング）」（150 ページ）を参照してください。
STP Mode	ポートまたは LAG に STP（Spanning Tree Protocol）の管理モード「Enabled」（有効）または「Disabled」（無効）を表示します。STP に関する詳しい情報は、「スパニングツリープロトコルの設定」（155 ページ）を参照してください。
Forwarding State	ポートの現在のスパニングツリーの状態を表示します。この状態は、ポートがフレームを受信した場合に行うアクションを制御します。ブリッジが機能不全なポートを検出すると、そのポートを「Broken」状態にします。さらに 5 つの状態が IEEE 802.1D で定義されています。 • Disabled • Blocking • Listening • Learning • Forwarding • Broken
Port Role	有効な各 MST ブリッジポートは、各スパニングツリーに「Port Role」を割り当てられます。「Port Role」は以下のいずれかです。 • Root Port • Designated Port • Alternate Port • Backup Port • Master Port • Disabled Port
Media Type	ポートのメディアタイプを表示します。
ARP Type	ポートの ARP タイプを表示します。

項目	説明
Admin Mode	ポートコントロールの管理状態を表示します。 • Enabled - ポートはネットワークに参加可能です。（初期値）。 • Disabled - ポートは管理的にダウンしており、ネットワークに参加していません。
Bcast Storm Mode	ブロードキャストストームのリカバリモードを表示します。 • Enabled - 指定のイーサネットポートにおいてブロードキャストトラフィックがしきい値を超過した場合、スイッチはブロードキャストトラフィックを防御（廃棄）します。 • Disabled - ポートのトラフィックがしきい値を超過すると、ポートはブロードキャストトラフィックを防御しません。（初期値）
Bcast Storm Level	ストーム制御がアクティブになるデータ速度であるブロードキャストストームのリカバリレベルを表示します。これは、ポートスピードの割合であり、0-100 で指定します。初期値はポートスピードの 5% です。
Mcast Storm Mode	マルチキャストストームのリカバリモードを表示します。 • Enabled - 指定したイーサネットポートにおけるマルチキャストトラフィックがしきい値を超過した場合、スイッチはマルチキャストトラフィックを防御（廃棄）します。 • Disabled - ポートのトラフィックがしきい値を超過しても、スイッチはマルチキャストトラフィックを防御しません。（初期値）
Mcast Storm Level	ストーム制御がアクティブになるデータ速度であるマルチキャストストームのリカバリレベルを表示します。これは、ポートスピードの割合であり、0-100 で指定します。初期値はポートスピードの 5% です。
Ucast Storm Mode	ユニキャストストームのリカバリモードを表示します。 • Enabled - 指定したイーサネットポートにおいてユニキャストトラフィックがしきい値を超過した場合、スイッチはユニキャストトラフィックを防御（廃棄）します。 • Disabled - ユニキャストトラフィックがしきい値を超過しても、スイッチはユニキャストトラフィックを防御しません。（初期値）
Ucast Storm Level	ストーム制御がアクティブになるデータ速度であるユニキャストストームのリカバリレベルを参照します。値は、ポートスピードの割合であり、0-100 で指定します。初期値はポートスピードの 5% です。
LACP Mode	「Link Aggregation Control Protocol」管理ステートを表示します。ポートがリンクアグリゲーションに参加するように、モードを有効にする必要があります。以下のいずれかの状態が表示されます。 • Enable - ポートがポートチャンネル（LAG）に参加することを許可します。（初期値） • Disable - ポートはポートチャンネル（LAG）に参加できません。
Physical Mode	ポートに設定されているスピードとデュプレックスモードを表示します。 • Auto - デュプレックスモードとスピードはオートネゴシエーション処理によって設定されます。ポートの最大性能（フルデュプレックスと 100Mbps）が通知されます。 • <Speed> Half Duplex - メニューから選択可能なポートスピードは、D-Link のソフトウェアが動作しているプラットフォームと選択するポートによって異なります。ハーフデュプレックスモードでは、伝送は一方向です。つまり、ポートは、同時にトラフィックを送受信できません。 • <Speed> Full Duplex - メニューから選択可能なポートスピードは、D-Link のソフトウェアが動作しているプラットフォームと選択するポートによって異なります。フルデュプレックスモードでは、伝送は双方向です。つまり、ポートは、同時にトラフィックを送受信できます。
Physical Status	動作しているポートのスピードとデュプレックスモードを示します。
Link Status	リンクが「Up」（アクティブ）または「Down」（ダウン）しているかを表示します。
Link Trap	このオブジェクトは、リンクステータスが変更した場合にトラップを送信するかどうかを表示します。 • Enable - リンクステータスが変更した場合に、システムはトラップを送信します。（初期値） • Disable - リンクステータスが変更した場合に、システムはトラップを送信しません。

「Refresh」ボタンをクリックし、システムの情報を最新に更新します。

ポートの説明

人が読むことのできるポートの説明を設定します。

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

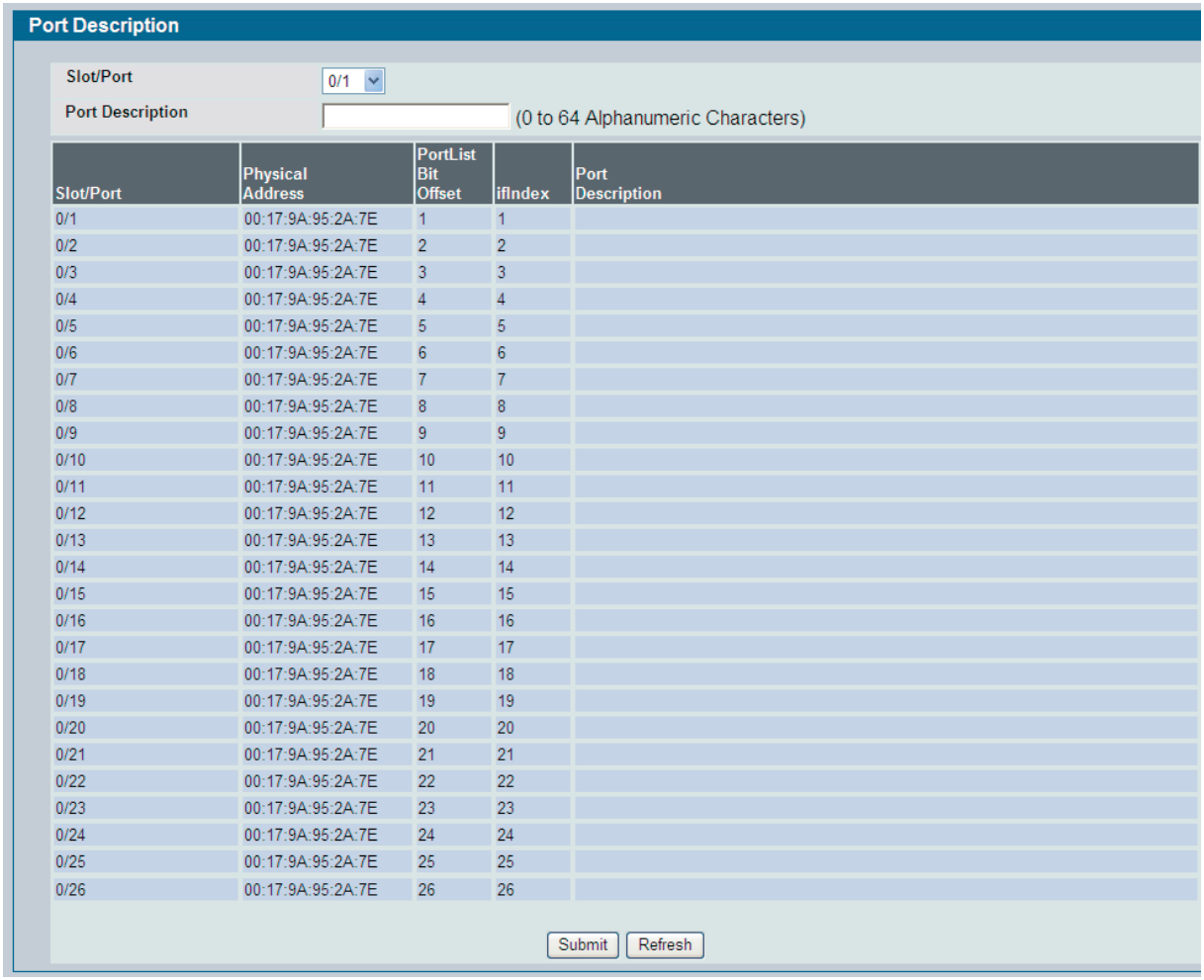


図 3-54　Port Description 画面

本画面には次の項目があります。

項目	説明
Slot/Port	データを表示または設定するインタフェースを選択します。
Port Description	ポートについて説明するテキストを 64 文字以内で指定します。説明文にはスペースと英数字以外の文字も含むことができます。
Port Description テーブル	
Slot/Port	ポートを表示します。
Physical Address	指定インタフェースのスイッチの物理アドレスを表示します。
PortList Bit Offset	MIB オブジェクトタイプ「PortList」が SNMP の管理に使用される場合、ポートに対応するビットオフセット値を表示します。
IfIndex	ポートに関連付けされているインタフェースのインデックスを表示します。
Port Description	設定したポートの説明文を表示します。初期値では、ポートには、関連する説明文はありません。

ポートの説明文を変更した場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。「Refresh」ボタンをクリックし、システムの情報を最新に更新します。

マルチプルポートミラーリング

ポートミラーリングでは、ネットワークアナライザによる分析のためにネットワークトラフィックを選択します。スイッチの特定ポートでこれは行われます。多くのスイッチポートをソースポートとして設定し、1 つのスイッチポートを宛先ポートとして設定します。トラフィックがソースポート上に反映される方法を設定することができます。ソースポートに受信されたパケット、ポートに送信されたパケット、または送受信の両方が行われたパケットを宛先ポートにミラーリングすることができます。

宛先ポートにコピーされるパケットは、有線 LAN 上のオリジナルのパケットと同じフォーマットです。これは、ミラーが受信パケットをコピーし、コピーされたパケットはソースポートに受信された通りに VLAN のタグ付けまたはタグ取りをされることを意味します。ミラーが送信されたパケットをコピーする場合、コピーされたパケットはソースポートに送信された通りに VLAN のタグ付けまたはタグ取りをされます。

ここでは、ポートミラーリングセッションを定義します。

LAN タブ > Administration > Multiple Port Mirroring の順にメニューをクリックし、以下の画面を表示します。

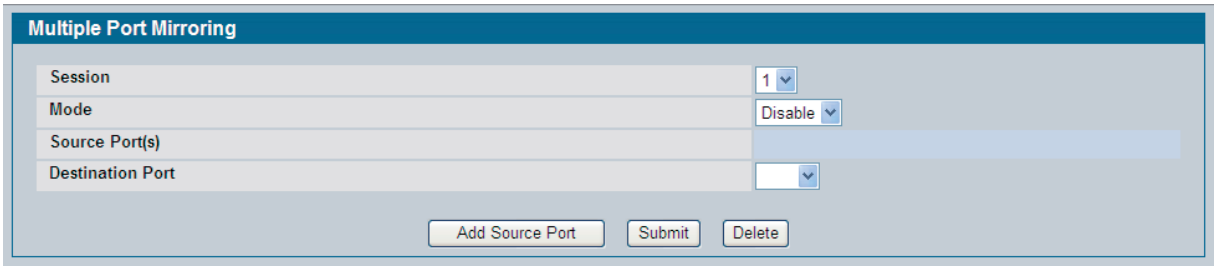


図 3-55　Multiple Port Mirroring 画面

本画面には次の項目があります。

項目	説明
Session	モニタリングセッション番号を指定します。
Mode	ポートミラーリング機能を有効または無効にします。初期値は無効です。
Source Port (s)	「Add Source Port」画面から追加されたソースポートを表示します。
Destination Port	ポートトラフィックがコピーされるポートを選択します。

ポートミラーリングセッションの追加

注意　ポートがミラーの宛先になる場合、VLAN または LAG から削除されます。

1. 「Multiple Port Mirroring」画面で「Add Source Port」ボタンをクリックし、以下の画面を表示します。

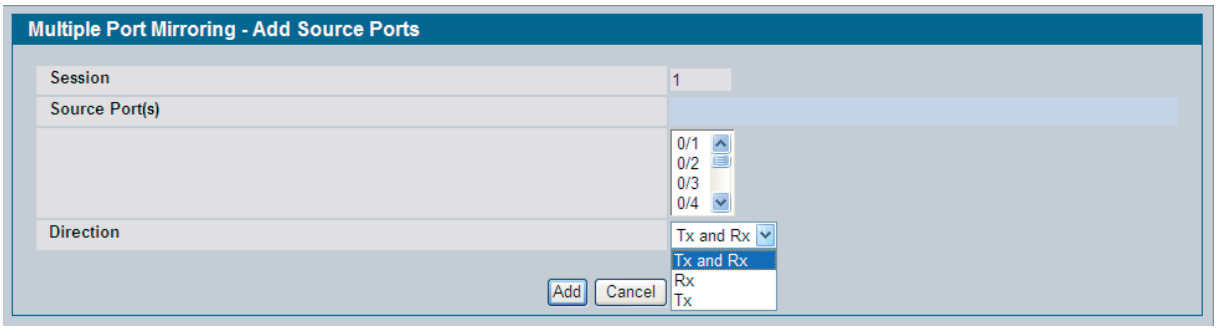


図 3-56　Multiple Port Mirroring - Add Source Ports 画面

2. 以下の項目を設定します。

項目	説明
Session	モニタリングセッションを表示します。
Source Port (s)	トラフィックがミラーリングされるユニットまたはポートを指定します。 最大 8 つのソースポートが宛先ポートにミラーリングされます。
Direction	ソースポート上のミラーリングされるトラフィックのタイプを選択します。 • Tx - 送信パケットのみをモニタリングします。 • Rx - 受信パケットのみをモニタリングします。 • Tx and Rx - 送受信パケットをモニタリングします。

3. 「Add」ボタンをクリックし、変更をスイッチに適用します。
新しいポートミラーリングセッションをユニットおよびポートに有効にし、デバイスを更新します。ソースポートは「Multiple Port Mirroring」画面の「Source Port」リストに表示されます。

ポートミラーリングセッションの削除または変更

1. 「Multiple Port Mirroring」画面で「Remove Source Port」ボタンをクリックして以下の画面を表示します。

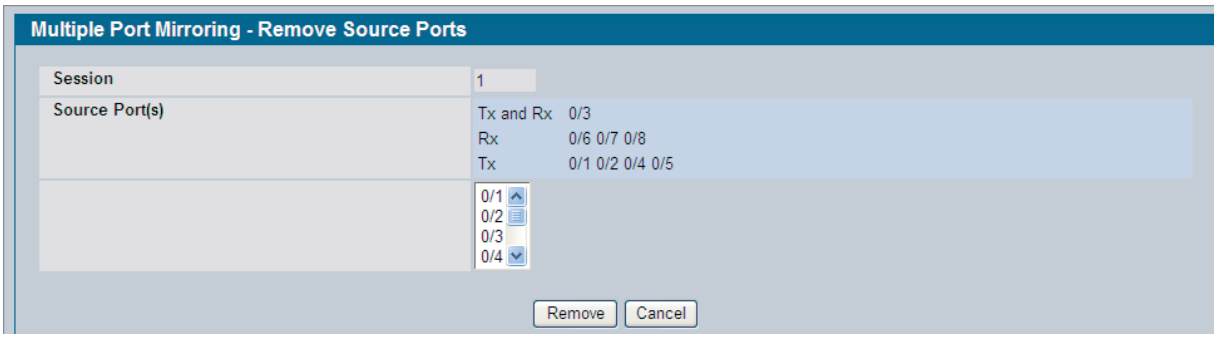


図 3-57　Multiple Port Mirroring - Remove Source Ports 画面

2. 削除する「Source Port」をクリックします。セッションから削除するために 1 つ以上のソースポートを選択します。
複数のポートを削除するために選択するためには「CTRL」キーを使用します。

3. 「Remove」ボタンをクリックします。
ポートミラーリングセッションからソースポート削除し、デバイスを更新します。

ダブル VLAN トンネリング

ダブル VLAN トンネリングはネットワークトラフィックに 2 個目のタグの使用を許可します。追加のタグは、自身の 802.1Q ドメインを入力する時に個別のカスタマの VLAN 識別子を保持していると、メトロポリタンネットワーク（MAN）においてカスタマの識別に役立ちます。

この 2 個目のタグの挿入を行うと、イーサネットベースの MAN にトラフィックを送信するために 4K VLAN ID のスペースを分割する必要はありません。
ダブル VLAN トンネリングが有効な場合、インタフェースから転送されるあらゆるフレームは DVlan タグを割り当て、一方、インタフェースから受信するあらゆるパケットは（1 つ以上のタグが存在すると）タグを削除します。

複数ポートにダブル VLAN フレームのタグの操作を設定します。

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

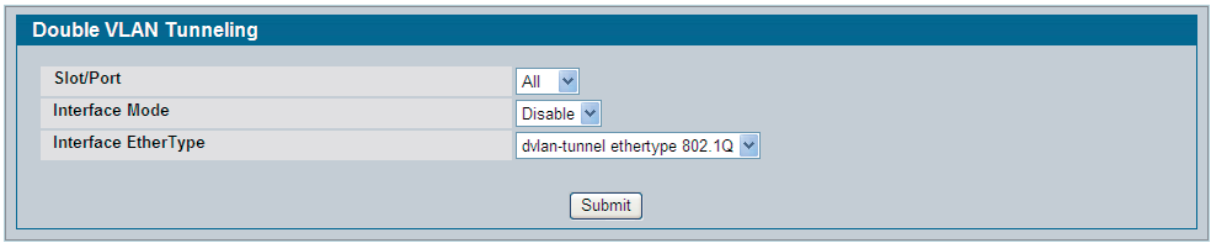


図 3-58　Double VLAN Tunneling 画面

本画面には次の項目があります。

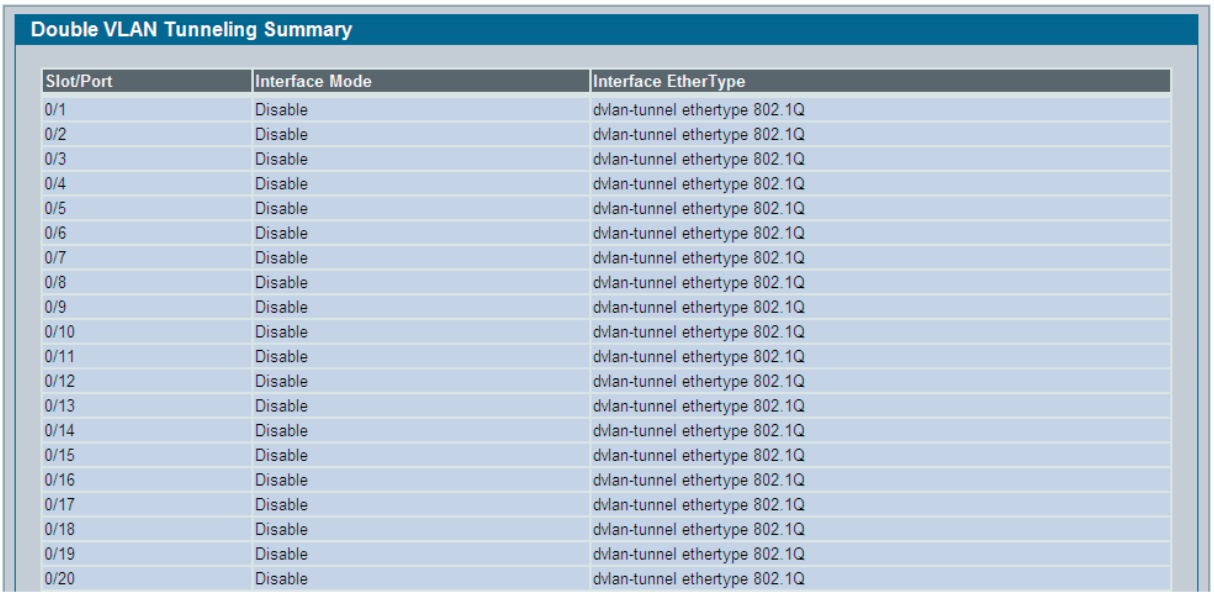
項目	説明
Slot/Port	データを表示または設定する物理インタフェースを選択します。「All」を選択すると、すべてのポートに同じ値を設定します。
Interface Mode	ダブル VLAN Tagging に管理用のモードを指定します。 • Enable - ダブル VLAN Tagging を指定ポート（または、すべてのポート）に有効にします。 • Disable - ダブル VLAN Tagging を指定ポート（または、すべてのポート）に無効にします。（初期値）
Interface EtherType	ダブル VLAN タグの最初の 16 ビットとして使用される 2 バイトの 16 進数 EtherType を指定します。 • 802.1Q Tag - 0x8100 を表す一般的に使用されるタグ。 • vMAN Tag - 0x88A8 を表す一般的に使用されるタグ。 • Custom Tag - 本オプションを選択すると画面は更新され、「Custom Value」欄が表示されます。 • Custom Value - EtherType のカスタム値（0-65535）を指定します。

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。

ダブル VLAN トンネリングステータス

システム上のすべてのポートのダブル VLAN トンネリング設定状態を表示します。

LAN タブ > Monitoring > VLAN Summary > Double VLAN 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。



Double VLAN Tunneling Summary

Slot/Port	Interface Mode	Interface EtherType
0/1	Disable	dvlan-tunnel ethertype 802.1Q
0/2	Disable	dvlan-tunnel ethertype 802.1Q
0/3	Disable	dvlan-tunnel ethertype 802.1Q
0/4	Disable	dvlan-tunnel ethertype 802.1Q
0/5	Disable	dvlan-tunnel ethertype 802.1Q
0/6	Disable	dvlan-tunnel ethertype 802.1Q
0/7	Disable	dvlan-tunnel ethertype 802.1Q
0/8	Disable	dvlan-tunnel ethertype 802.1Q
0/9	Disable	dvlan-tunnel ethertype 802.1Q
0/10	Disable	dvlan-tunnel ethertype 802.1Q
0/11	Disable	dvlan-tunnel ethertype 802.1Q
0/12	Disable	dvlan-tunnel ethertype 802.1Q
0/13	Disable	dvlan-tunnel ethertype 802.1Q
0/14	Disable	dvlan-tunnel ethertype 802.1Q
0/15	Disable	dvlan-tunnel ethertype 802.1Q
0/16	Disable	dvlan-tunnel ethertype 802.1Q
0/17	Disable	dvlan-tunnel ethertype 802.1Q
0/18	Disable	dvlan-tunnel ethertype 802.1Q
0/19	Disable	dvlan-tunnel ethertype 802.1Q
0/20	Disable	dvlan-tunnel ethertype 802.1Q

図 3-59　Double VLAN Tunneling Summary 画面

本画面には次の項目があります。

項目	説明
Slot/Port	データを表示または設定する物理インタフェースを表示します。
Interface Mode	ダブル VLAN Tagging に管理用のモードを表示します。 • Enable - ダブル VLAN Tagging を指定ポート（または、すべてのポート）に有効にします。 • Disable - ダブル VLAN Tagging を指定ポート（または、すべてのポート）に有効にします。（初期値）
Interface EtherType	ダブル VLAN タグの最初の 16 ビットとして使用される 2 バイトの 16 進数 EtherType を表示します。 • 802.1Q Tag - 0x8100 を表す一般的に使用されるタグ • vMAN Tag - 0x88A8 を表す一般的に使用されるタグ。 • Custom Tag - カスタムタグが設定されていることを示し、その値を表示します。

「Refresh」ボタンをクリックし、システムの情報を最新に更新します。

sFlow の設定

sFlow は高速にスイッチおよび送信されるネットワークのモニタリングの標準です。sFlow の技術は、ネットワーク装置に実装されており、ネットワークの動作に完全な可視性およびネットワークリソースの効果的な管理と制御の有効化を提供します。

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 エージェントはサンプリング技術を使用して、モニタリングしているデバイスからのトラフィックの統計情報をキャプチャします。sFlow データは、抽出されたトラフィック統計情報を分析のために直ちに sFlow コレクタに送信するために使用されます。

sFlow エージェントは 2 つのサンプリング形式を使用します。
- スイッチまたは送信されたパケットフローの統計的なパケットベースのサンプリング
- タイムベースのカウンタのサンプリング

sFlow エージェントのサマリ

パケットフローのサンプリングとカウンタのサンプリングは sFlow エージェント内の個々のデータソースに関連付けられた sFlow インスタンスによって実行されます。パケットフローのサンプリングとカウンタサンプリングは統合システムの一部として設計されています。両方のサンプルタイプは sFlow データで結合されます。パケットフローサンプリングは、着実に、しかしランダムに sFlow データのストリームを sFlow コレクタに送信します。

パケットフローサンプリングを実行するために、sFlow の「Sampler Instance」が「Sampling Rate」と共に設定されます。パケットフローサンプリングのプロセスはパケットフローレコードの生成を行います。カウンタサンプリングを実行するために、sFlow の「Poller Instance」が「Polling Interval」と共に設定されます。カウンタサンプリングプロセスはカウンタレコードを生成します。sFlow エージェントは、カウンタレコードとパケットフローレコードを収集し、sFlow データの形式で sFlow コレクタにそれらを送信します。

LAN タブ > Monitoring > sFlow > Agent 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。

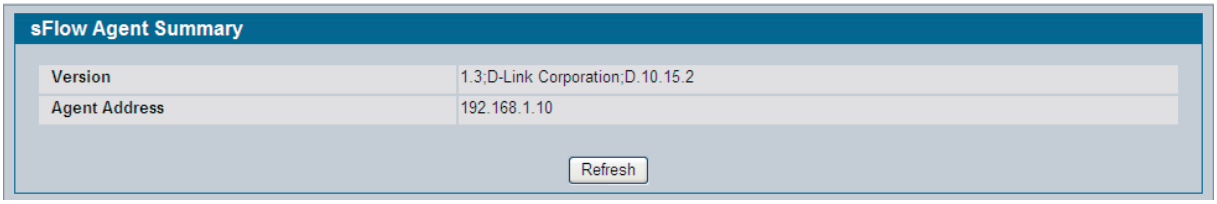


図 3-60　sFlow Agent Summary 画面

本画面には次の項目があります。

項目	説明
Version	MIB のバージョンとインプリメンテーションを示します。 バージョン文字列は以下の構造を持つ必要があります。: MIB Version;Organization;Software Revision • MIB Version - 1.3（この MIB のバージョン） • Organization - D-Link Corporation • Revision - 1.0
Agent Address	このエージェントに関連付けられた IP アドレス。

「Refresh」ボタンをクリックすると、スイッチにおける現在のデータの多くを更新します。

sFlow レシーバ設定

sFlow レシーバを設定します。

LAN タブ > Administration > sFlow > Receiver 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。

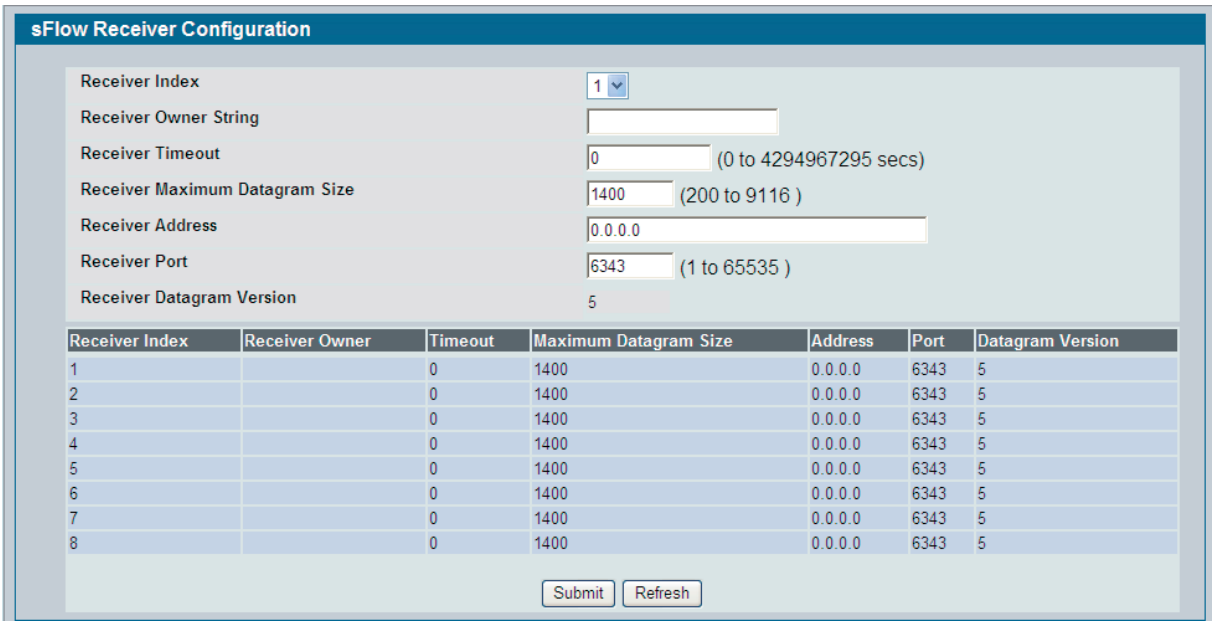


図 3-61　sFlow Receiver Configuration 画面

本画面には次の項目があります。

項目	説明
Receiver Index	データを表示または設定するレシーバを選択します。許可される範囲は、1-8 です。
Receiver Owner String	この sFlowRcvrTable エントリを利用するエンティティ。 「empty」の文字は、エントリが現在、要求されておらず、レシーバの設定が初期値にリセットされていることを示しています。sFlowRcvrTable テーブルエントリを要求するエンティティは、要求を行う前にはエントリが要求されていないことを保証する必要があります。エントリは、owner string を設定することで要求されます。どんな変更も他のサンプラオブジェクトに行われる前にエントリを要求する必要があります。
sFlow Receiver Timeout	サンプラがリリースされて、サンプリングを止める前の残り時間（秒）。サンプラの制御を維持したい管理エンティティは、期限切れになる前に新しい値に設定する必要があります。許容範囲は 0-4294967295（秒）です。0 の値は、選択したレシーバ設定を初期値にします。
sFlow Receiver Maximum Datagram Size	1 つのサンプルデータに送信される最大データバイト数（200-9116）を指定します。管理者は、sFlow データのフラグメント化を回避するために、本値を設定する必要があります。初期値は 1400 です。
sFlow Receiver Address	sFlow コレクタアナライザサーバの IP アドレス。0.0.0.0 に設定されると、sFlow データは送信されません。
sFlow Receiver Port	sFlow データの宛先ポート（1-65535）。
Receiver Datagram Version	送信されるべき sFlow データのバージョン。

「Submit」ボタンをクリックし、更新データをスイッチに適用します。変更がスイッチに反映されます。「Refresh」ボタンをクリックすると、スイッチにおける現在のデータの多くを更新します。

sFlow ポーラ設定

sFlow エージェントは、ネットワークインタフェースのタイムベースのサンプリングによる統計情報を収集して、設定済みの sFlow レシーバにそれらを送信します。カウンタサンプルに設定されているデータソースは、ポーラと呼ばれます。

カウンタのサンプリング

カウンタサンプリングの第一の目的は、効率的、定期的にデータソースに関連しているカウンタをエクスポートすることです。最大のサンプリング間隔は、データソースに関連する各 sFlow インスタンスに割り当てられます。

カウンタサンプリングは以下の通り実行されます。

- sFlow エージェントはサンプリングされたカウンタソースのリストを保持します。パケットフローのサンプルが生成される場合、sFlow エージェントは、リストを検証してサンプルデータにカウンタを追加します。最も新しくサンプリングされたものを最初に追加します。ソースが短時間（例 5 秒）内に要求されたサンプリング間隔に一致しなかった場合にだけ、カウンタはデータに追加されます。定期的（毎秒）、sFlow エージェントは、カウンタソースのリストを調べて、サンプリング間隔の要求を満たす必要があるどんなカウンタも送信します。

LAN タブ > Administration > sFlow > Poller 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。

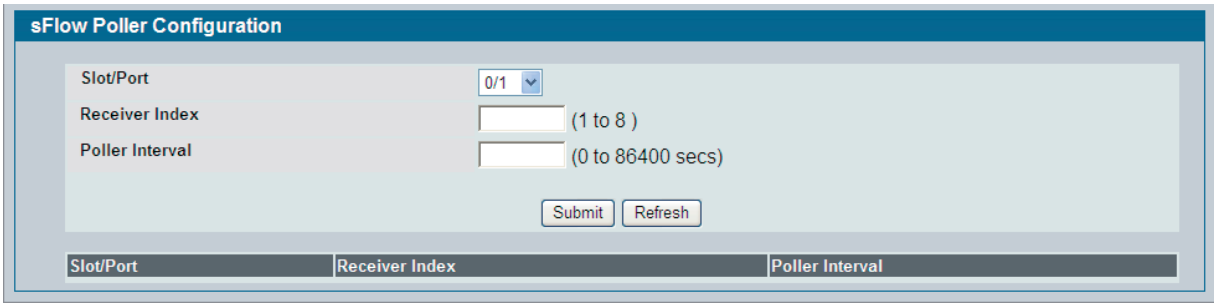


図 3-62　sFlow Poller Configuration 画面

本画面には次の項目があります。

項目	説明
Slot/Port	設定するインタフェースを指定します。
Receiver Index	この sFlow カウンタポーラの sFlow のレシーバ（1-8）を指定します。0 に設定すると、ポーラは初期値に設定され、ポーラは削除されます。アクティブなレシーバだけが設定されます。また、レシーバが期限切れになるとレシーバに関連するすべてのポーラも期限が切れます。
Poller Interval	このデータソースに関連するカウンタの連続するサンプル間隔（秒）。

「Refresh」ボタンをクリックすると、スイッチを最新のデータで更新します。

sFlow サンプラ設定

sFlow エージェントは、スイッチされるフローをパケットベースでサンプリングすることで統計情報を収集し、設定済みのレシーバにそれらを送信します。フローサンプルを収集するように設定されるデータソースは、サンプラと呼ばれます。

Packet Flow Sampling（パケットフローサンプリング）

各 sFlow インスタンスが実行されるパケットフローサンプリングメカニズムは、データソースで監視されるどんなパケットも所属するパケットフローに関係なく等しくサンプルされる機会があることを保証します。

パケットフローサンプリングは以下の通り実行されます。

- パケットがインタフェースに到着する場合、ネットワークデバイスはパケットが廃棄されるべきであるかどうかをフィルタリングが判断します。
- パケットがフィルタ（廃棄）されないと、宛先インタフェースはスイッチ / ルーティング機能によって割り当てられます。
- ここで、パケットをサンプリングするかどうかを決定します。メカニズムは各パケットで減少するカウンタに関係します。カウンタが 0 に到達する場合、サンプリングされます。サンプリングされると、次のサンプルを取得する前にいくつのパケットをスキップするかを示すカウンタをリセットします。カウンタの値はランダムな整数に設定されます。時間の経過に伴い使用されたランダムな整数のシーケンスがサンプリングレートです。

LAN タブ > Administration > sFlow > Sampler 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。

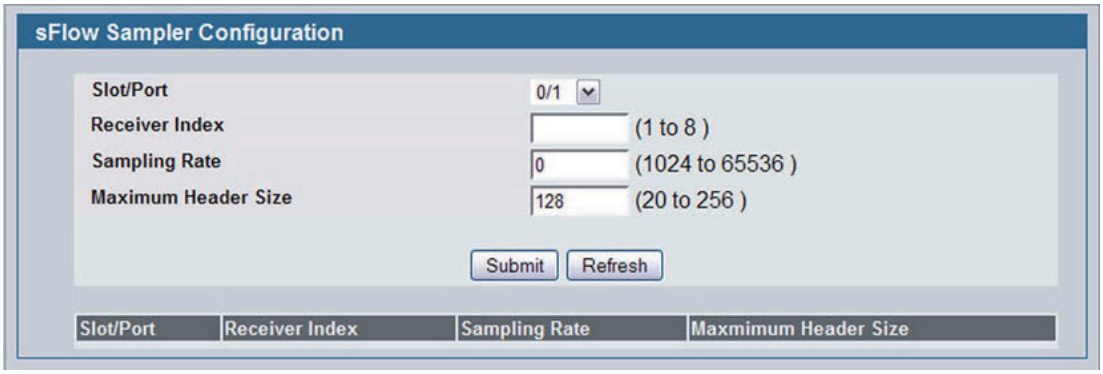


図 3-63　sFlow Sampler Configuration 画面

本画面には次の項目があります。

項目	説明
Slot/Port	設定するインタフェースを指定します。
Receiver Index	この sFlow サンプラの sFlow レシーバ（1-8）を指定します。0 にすると、パケットはサンプリングされません。アクティブなレシーバだけが設定されます。レシーバが期限切れになるとレシーバに関連しているすべてのサンプラも期限が切れます。
Sampling Rate	このソースからのパケットサンプリングの統計的なサンプリングレート（1024-65536）を指定します。1 はすべてのパケットをカウントします。0 はサンプリングを無効にします。
Maximum Header Size	1 つのサンプルデータにコピーされる最大データバイト数（20-256）を指定します。

SNMP パラメータの定義

SNMP（Simple Network Management Protocol）は、ネットワークデバイスの管理を行う方法を提供します。デバイスは、SNMP のバージョン 1、2、および 3 を実装しています。Web インタフェースは SNMPv1 と v2 の設定をサポートしています。SNMPv3 は CLI のみサポートしています。

SNMP V1、V2

SNMP エージェントは、デバイスを管理するのに使用される変数のリストを保持しています。変数は MIB（Management Information Base）に定義されています。MIB はエージェントが制御する変数を示すものです。SNMP エージェントは、情報にアクセスするために使用する形式などの MIB の仕様形式を定義しています。SNMP エージェントへのアクセス権はアクセスする文字列によって制御されます。

SNMP V3

SNMP v3 はアクセスコントロールと新しいトラップメカニズムを SNMPv1 と SNMPv2 PDU に適用します。さらに、ユーザセキュリティモデル（USM）が SNMPv3 に定義されます。以下の項目があります。

- Authentication - データ保全性とデータの送信元の認証を提供します。
- Privacy - メッセージの内容を開示することから保護します。Cipher-Bock-Chaining（CBC）が暗号化に使用されます。認証が SNMP メッセージで有効にされるか、または認証とプライバシーの両方が SNMP メッセージで有効にされます。プライバシーは認証なしでは有効にすることはできません。
- Timeliness - メッセージ遅延またはメッセージ冗長から保護します。SNMP エージェントは入力メッセージをメッセージ時刻情報と比較します。
- Key Management - 鍵生成、鍵の更新、および鍵の使用を定義します。

デバイスは、オブジェクト ID（OID）に基づいた SNMP 通知フィルタをサポートしています。OID はシステムによって使用されて、デバイス機能を管理します。SNMP v3 は以下の機能をサポートしています。

- セキュリティ
- アクセスコントロール
- トラップ

認証またはプライバシーキーは SNMPv3 ユーザセキュリティモデル（USM）内で変更されます。

「SNMP」画面で、SNMP パラメータを定義します。

LAN タブ > Administration > SNMP Manager の順にメニューをクリックし、「SNMP」画面を表示します。

SNMP コミュニティ設定

アクセス権は、「SNMPv1, 2 Community」画面でコミュニティを設定することで管理されます。また、コミュニティ名を変更すると、アクセス権も変更されます。SNMP コミュニティは SNMP v1 と SNMP v2 用に定義されます。

SNMP と認証の通知を有効にします。

LAN タブ > Administration > SNMP Manager> SNMP Community 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。

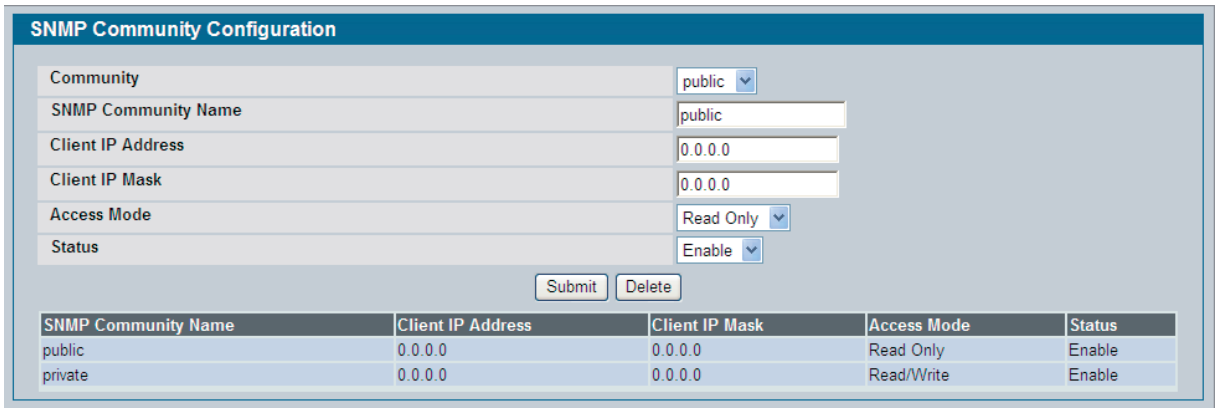


図 3-64　SNMP Community Configuration 画面

本画面には次の項目があります。

項目	説明
Community	パスワードとして機能し、SNMP 管理ステーションをデバイスに対して認証するために使用される定義済みおよびユーザ定義のコミュニティの文字列（20 文字以内）を指定します。初期値で利用可能なオプションは以下の通りです。 • public - この SNMP コミュニティには、読み出し権だけがあり、そのステータスは有効に設定されています。 • private - この SNMP コミュニティには、読み出し / 書き込み権があり、そのステータスは有効に設定されています。 • Create - 新しいユーザ定義のコミュニティの文字列を作成します。
SNMP Community Name	既存のコミュニティの再設定、または新規に作成します。有効なエントリは最大 16 文字で大文字と小文字は区別されます。
Client IP Address	「Client IP Address」および「Client IP Mask」は、SNMP クライアントが本デバイスにアクセスするのにそのコミュニティを使用する可能性がある IP アドレスの範囲を指定します。 （IP アドレスまたは IP マスクのいずれかの）値が「0.0.0.0」であると、どの IP アドレスからもアクセスが許可されます。そうでない場合、すべてのクライアントの IP アドレスは「Client IP Address」のようにマスクで論理積をとられ、値が等しい場合アクセスは許可されます。例えば、「Client IP Address」と「Client IP Mask」が「192.168.1.0/255.255.255.0」であれば、IP アドレスが「192.168.1.0-192.168.1.255」にどんなクライアントもアクセスが許可されます。1 つのステーションからだけアクセスを許可するためには、「Client IP Mask」（255.255.255.255）値を使用し、「Client IP Address」にマシンの IP アドレスを使用します。
Client IP Mask	「Client IP Address」と共に「Client IP Mask」は SNMP クライアントがこのデバイスにアクセスするのにそのコミュニティを使用する可能性のある IP アドレスの範囲を指定します。
Access Mode	コミュニティにアクセスレベルを指定します。 • Read Only - コミュニティは参照のために設定されている MIB オブジェクトへの読み出しのみ可能なアクセス権を持ちます。 • Read/Write - コミュニティは参照される MIB オブジェクトの読み出し / 変更のアクセス権を持ちます。
Status	コミュニティの状態を示します。 • Enable - コミュニティは有効とされ、コミュニティ名がすべての有効なコミュニティ名の中で固有である必要があります。そうでないと設定の要求は拒否されます。 • Disable - コミュニティは無効とされ、コミュニティ名は不正となります。

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。新しいコミュニティを作成する場合、「Submit」ボタンの下にあるテーブルに追加されます。

コミュニティの削除

「Delete」ボタンをクリックし、選択した SNMP コミュニティを削除します。

トラップレシーバ設定

トラップパケットを受信する SNMP コミュニティとトラップマネージャに関する情報を設定します。

LAN タブ > Administration > SNMP Manager > Trap Receiver 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。

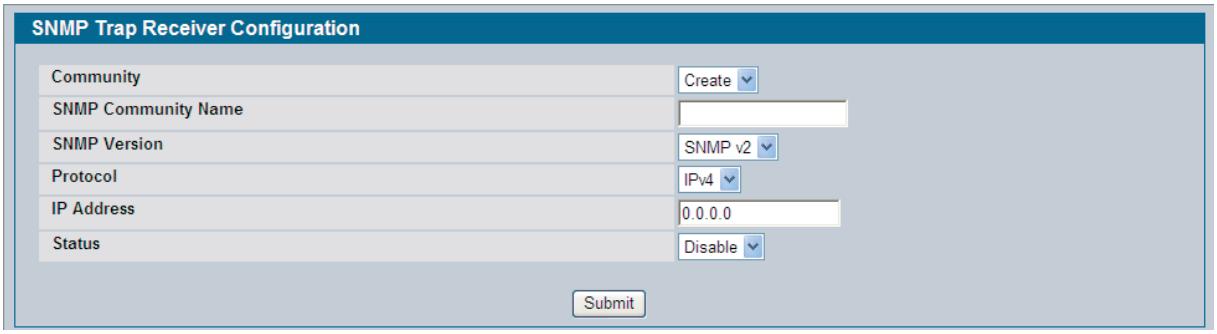


図 3-65　SNMP Trap Receiver Configuration 画面

本画面には次の項目があります。

項目	説明
Community	「Create」を選択すると、残りの欄に新しく SNMP トラップレシーバ情報を設定することができます。既に SNMP トラップレシーバを設定している場合、プルダウンメニューで選択し、設定の変更または削除を行うことができます。
SNMP Community Name	コミュニティの文字列を入力して、SNMP トラップパケットをトラップマネージャに送信します。16 文字以内で、大文字と小文字を区別します。
SNMP Version	レシーバが使用するトラップバージョンを選択します。 • SNMP v1 - SNMP v1 を使用して、トラップをレシーバに送信します。 • SNMP v2 - SNMP v2 を使用して、トラップをレシーバに送信します。
Protocol	SNMP トラップレシーバ設定で使用されるプロトコルのタイプを選択します。 • IPv4 - IPv4 を選択し、IPv4 形式でアドレスを入力します。 • IPv6 - IPv6 を選択し、IPv6 形式でアドレスを入力します。
IP Address	デバイスから SNMP トラップを受信するために、「.」（ドット）を付けた 10 進数形式の IP アドレスを入力します。
Status	レシーバのステータスを選択します。 • Enable - トラップをレシーバに送信します。 • Disable - トラップをレシーバに送信しません。

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。再起動後も新しい値をスイッチに保持する場合、保存を行う必要があります。

トラップフラグ

スイッチが SNMP マネージャに送信するコンポーネントレベルでトラップを有効または無効にします。アクティブなトラップに示された条件にスイッチが一致した場合、トラップメッセージは有効な SNMP トラップレシーバに送信され、メッセージはトラップログに書かれます。コンポーネントレベルのトラップフラグが無効であると、そのコンポーネントの個々のトラップを有効にしても、SNMP マネージャにはトラップは送信されません。

LAN タブ > Administration > SNMP Manager > Trap Flags の順にメニューをクリックし、以下の画面を表示します。

図 3-66　Trap Flags Configuration 画面

本画面には次の項目があります。

項目	説明
ACL Traps	ACL トラップを有効または無効にします。初期値は「Disable」(無効) です。
Authentication	認証エラーのトラップを有効または無効にします。初期値は「Enable」(有効) です。
Captive Portal	キャプティブポータルの SNMP トラップを生成するスイッチの SNMP エージェントを有効 / 無効にします。初期値は無効で、スイッチの SNMP エージェントは、それらが個別に有効とされていてもキャプティブポータルの SNMP トラップは生成されません。
Global Wireless Traps	Global Wireless トラップを有効または無効にします。初期値は「Enable」(有効) です。
Link Up/Down	リンクステータスのトラップを有効または無効にします。初期値は「Enable」(有効) です。
Multiple Users	マルチユーザトラップを有効または無効にします。初期値は「Enable」(有効) です。このトラップは、Telnet またはシリアルポート経由のいずれかで、同じユーザ ID で同時に複数ログインする場合に始動されます。
PoE Traps	PoE トラップを有効または無効にします。初期値は「Enable」(有効) です。
Spanning Tree	スパニングツリーのトラップを有効または無効にします。初期値は「Enable」(有効) です。

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。

サポートする MIB

システムが現在サポートする MIB を表示します。

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

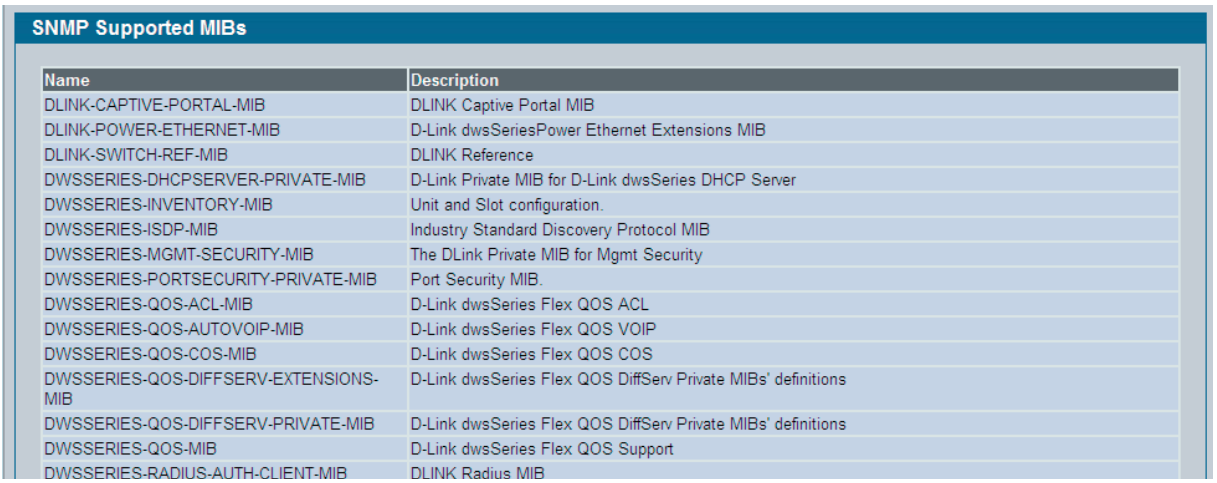


図 3-67　SNMP Supported MIBs 画面

本画面には次の項目があります。

項目	説明
Name	RFC 番号（適用できる場合）と MIB の名称。
Description	RFC のタイトルまたは MIB の説明文。

システム統計情報の参照

「Statistics」フォルダには、スイッチが送受信したトラフィック量とタイプに関する様々な情報があります。

スイッチの詳細

スイッチが処理するトラフィックに関する詳細な統計情報を表示します。

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

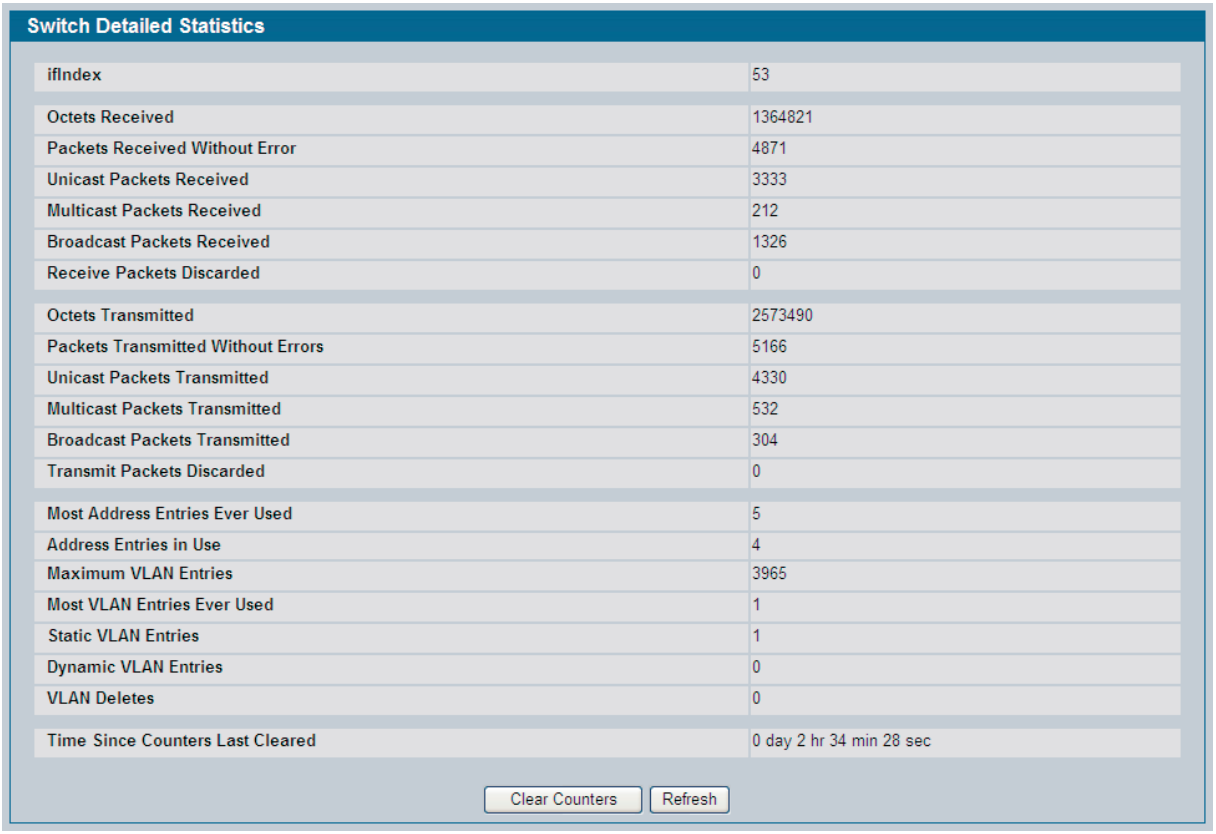


図 3-68　Switch Detailed Statistics 画面

本画面には次の項目があります。

項目	説明
fIndex	スイッチの CPU に関連するインタフェーステーブルエントリの ifIndex を表示します。
Octets Received	処理装置が受信したデータの総 64 オクテット数（フレームビットを除き、FCS オクテットを含む）。
Unicast Packets Received	上位レイヤプロトコルに送信されたサブネットワークのユニキャストパケット数。
Multicast Packets Received	マルチキャストアドレスに向けられた受信パケットの合計数。これには、ブロードキャストアドレスに向けられたパケットは含まれていないことにご注意ください。
Broadcast Packets Received	ブロードキャストアドレスに向けられた受信パケットの合計数。これには、マルチキャストパケットは含まれていないことにご注意ください。
Receive Packets Discarded	上位レイヤプロトコルに送信されることを防御するためにエラーは検出されていなかったが、破棄されるように選択された内向きパケットの数。パケットを破棄する考えられる原因は、バッファスペースの解放です。
Octets Transmitted	フレーミングキャラクタを含むインタフェースに送信されたオクテットの合計数。
Packets Transmitted Without Errors	インタフェースに送信されたパケットの合計数。
Unicast Packets Transmitted	要求された上位レベルのプロトコルがサブネットワークのユニキャストアドレスに送信されたパケットの合計数。破棄されたもの、または送信されなかったものも含みます。
Multicast Packets Transmitted	要求された上位レベルのプロトコルがマルチキャストアドレスに送信されたパケットの合計数。破棄されたもの、または送信されなかったものも含みます。
Broadcast Packets Transmitted	要求された上位レベルのプロトコルがブロードキャストアドレスに送信されたパケットの合計数。破棄されたもの、または送信されなかったものも含みます。
Transmit Packets Discarded	上位レイヤプロトコルに送信されることを防御するためにエラーが検出されていなかったが、破棄されるように選択された外向きパケットの数。パケットを破棄する考えられる原因は、バッファスペースの解放です。
Most Address Entries Ever Used	最後の起動後に学習された Forwarding Database Address Table エントリの最大数。

項目	説明
Address Entries in Use	スイッチの Forwarding Database Address Table に学習されたエントリおよびスタティックなエントリの数。
Maximum VLAN Entries	スイッチが許可する VLAN の最大数。
Most VLAN Entries Ever Used	最後の起動後にこのスイッチでアクティブである VLAN の最大数。
Static VLAN Entries	本スイッチにスタティックに作成された現在アクティブな VLAN エントリの数。
Dynamic VLAN Entries	本スイッチに GVRP 登録によって作成された現在アクティブな VLAN エントリの数。
VLAN Deletes	最後の起動後に本スイッチにスタティックに作成され、その後削除された VLAN の数。
Time Since Counters Last Cleared	スイッチの統計情報が最後にクリアされた後の経過時間（日、時、分、秒）。

「Refresh」ボタンをクリックすると、スイッチにおける現在の状態を持つ画面上のデータを更新します。

統計情報のクリア

「Clear Counters」ボタンをクリックして、すべての統計情報をクリアし、すべてのスイッチサマリと詳細な統計情報を初期値に戻します。破棄パケットのカウントはクリアすることができません。

スイッチのサマリ

スイッチにおけるトラフィックの統計情報のサマリを参照します。

LAN タブ > Monitoring > System Statistics > Switch 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。

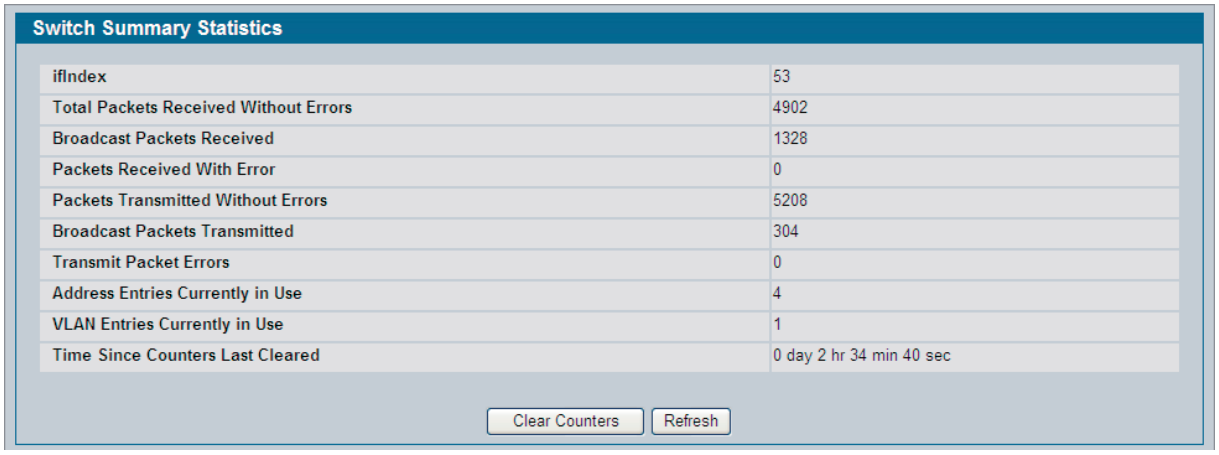


図 3-69　Switch Summary Statistics 画面

本画面には次の項目があります。

項目	説明
ifIndex	スイッチの CPU に関連するインタフェーステーブルエントリの ifIndex を表示します。
Total Packets Received Without Errors	ブロードキャストアドレスに向けられたマルチキャストパケットを含むパケットの合計数。
Broadcast Packets Received	ブロードキャストアドレスに向けられた受信パケットの合計数。これには、マルチキャストパケットは含まれていないことにご注意ください。
Packets Received With Error	上位レイヤプロトコルの送信されることを防御したエラーを含む内向きパケットの数。
Packets Transmitted Without Errors	インタフェースに送信されたパケットの合計数。
Broadcast Packets Transmitted	要求された上位レベルのプロトコルがブロードキャストアドレスに送信されたパケットの合計数。破棄されたもの、または送信されなかったものも含みます。
Transmit Packet Errors	エラーのために送信されなかった外向きパケットの数。
Address Entries Currently in Use	学習したエントリおよびスタティックなエントリを含む現在スイッチでアクティブな Forwarding Database Address Table エントリの合計数。
VLAN Entries Currently in Use	現在 VLAN テーブルを占有する VLAN エントリの数。
Time Since Counters Last Cleared	スイッチの最後の再起動からの経過時間（日、時、分、秒）。

「Refresh」ボタンをクリックすると、スイッチにおける現在のデータを更新します。

統計情報のクリア

「Clear Counters」ボタンをクリックして、すべての統計情報をクリアし、本スイッチのすべてのサマリと詳細な統計情報を初期値に戻します。破棄パケットのカウントをクリアすることができません。「Clear All Counters」ボタンをクリックして、スタック内のすべてのスイッチのカウンタをクリアします。

ポートの詳細

様々なポートごとのトラフィック統計情報を表示します。

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

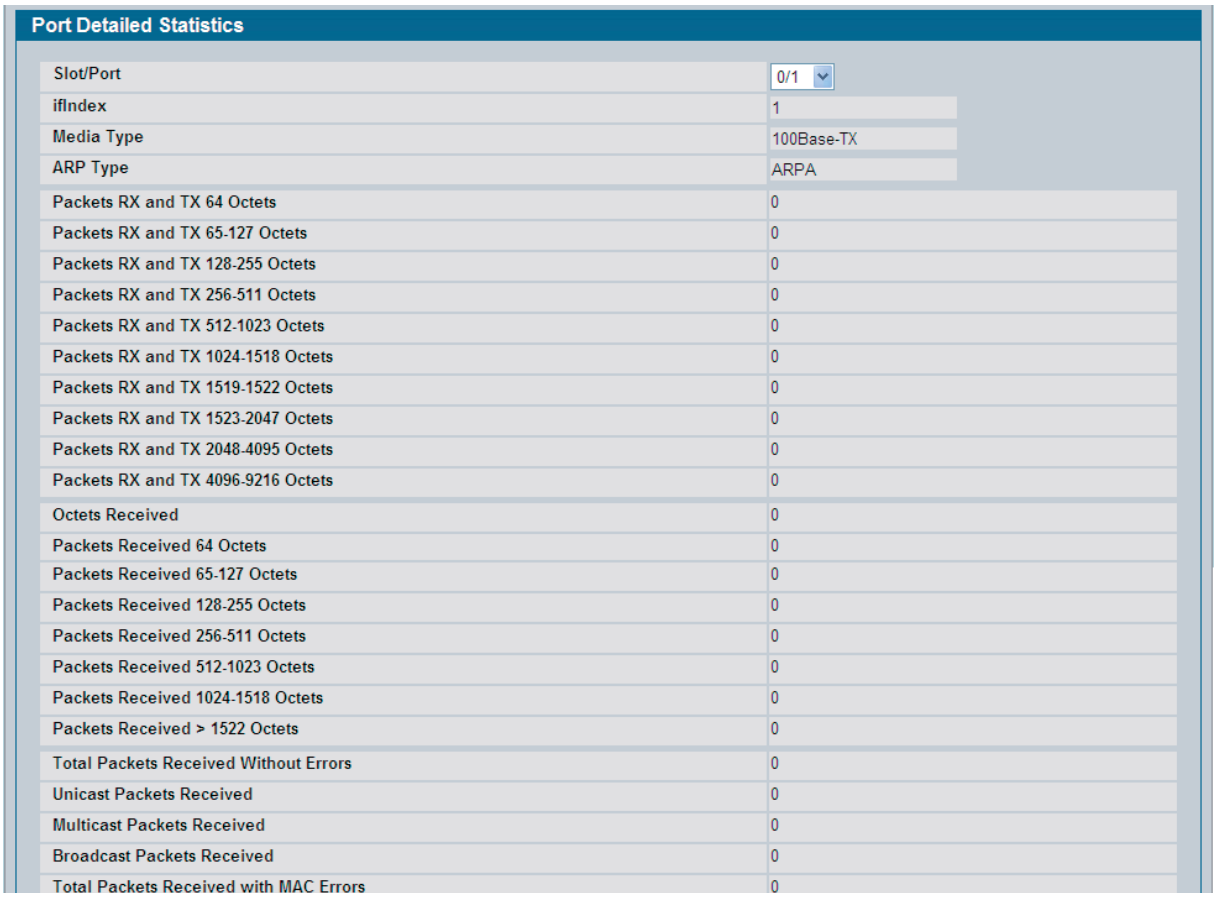


図 3-70　Port Detailed Statistics 画面

本画面には次の項目があります。

項目	説明
Slot/Port	データを表示または設定するインタフェースを選択します。
ifIndex	本ポートに関連するインタフェーステーブルのエントリの ifIndex を表示します。
Media Type	イーサネットの物理的メディアのタイプ（10Base-T、100Base-TX、100Base-FX、1000Base-X、1000Base-T、および 10GBase-X）。
ARP Type	ネットワークアドレスのカプセル化タイプ。この値は常に「ARPA」です。
Packets RX and TX 64 Octets	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）の送信または受信したパケットの合計数（不正なパケットを含む）。
Packets RX and TX 65-127 Octets	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）の送信または受信したパケットの合計数（不正なパケットを含む）。
Packets RX and TX 128-255 Octets	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）の送信または受信したパケットの合計数（不正なパケットを含む）。
Packets RX and TX 256-511 Octets	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）の送信または受信したパケットの合計数（不正なパケットを含む）。
Packets RX and TX 512-1023 Octets	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）の送信または受信したパケットの合計数（不正なパケットを含む）。
Packets RX and TX 1024-1518 Octets	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）の送信または受信したパケットの合計数（不正なパケットを含む）。
Packets RX and TX 1519-1522 Octets	サイズが 1519 から 1522 オクテット（フレームビットを除き、FCS オクテットを含む）の送信または受信したパケットの合計数（不正なパケットを含む）。
Packets RX and TX 1523-2047 Octets	サイズが 1523 から 2047 オクテット（フレームビットを除き、FCS オクテットを含む）の送信または受信したパケットの合計数（不正なパケットを含む）。
Packets RX and TX 2048-4095 Octets	サイズが 2048 から 4095 オクテット（フレームビットを除き、FCS オクテットを含む）の送信または受信したパケットの合計数（不正なパケットを含む）。
Packets RX and TX 4096-9216 Octets	サイズが 4096 から 9216 オクテット（フレームビットを除き、FCS オクテットを含む）の送信または受信したパケットの合計数（不正なパケットを含む）。

項目	説明
Octets Received	ネットワークが受信した（不正なパケットを含む）データの総オクテット数（フレームビットを除き、FCS オクテットを含む）。これは、イーサネット使用率の合理的な見積りとして使用されます。より高い精度が必要な場合、etherStatsPkts と etherStatsOctets オブジェクトを「common interval」の前後にサンプリングします。
Packets Received 64 Octets	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）。
Packets Received 65-127 Octets	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）。
Packets Received 128-255 Octets	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）。
Packets Received 256-511 Octets	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）。
Packets Received 512-1023 Octets	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）。
Packets Received 1024-1518 Octets	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）。
Packets Received > 1522 Octets	サイズが 1522 オクテット（フレームビットを除き、FCS オクテットを含む）より長くい受信パケットの合計数。
Packets Received Successfully	
Total Packets Received Without Errors	エラーなしで受信したパケットの合計数。
Unicast Packets Received	上位レイヤプロトコルに送信されたサブネットワークのユニキャストパケット数。
Multicast Packets Received	マルチキャストアドレスに向けられた正常に受信したパケットの合計数。 これには、ブロードキャストアドレスに向けられたパケットは含まれていないことにご注意ください。
Broadcast Packets Received	ブロードキャストアドレスに向けられた正常に受信したパケットの合計数。 これには、マルチキャストパケットは含まれていないことにご注意ください。
Packets Received with MAC Errors	
Total Packets Received with MAC Errors	上位レイヤプロトコルに送信されることを防いだエラーを含む内向きパケットの合計数。
Jabbers Received	サイズが 1518 オクテットより長く、オクテットの整数を持つ不正な Frame Check Sequence（FCS）（FCS エラー）、または整数でないオクテットの不正な FCS アライメントエラーのいずれかを持つ受信パケット（フレームビットを除き、FCS オクテットを含む）の合計数。 Jabber の定義は、IEEE 802.3 セクションの 8.2.1.5（10BASE5）とセクション 10.3.1.4（10BASE2）における定義とは異なることにご注意ください。これらのドキュメントはどんなパケットも 20ms を超えているという条件で Jabber を定義しています。Jabber を検出できる範囲は 20-150（ms）です。
Fragments Received	ERROR CRC を持つサイズが 64 オクテット未満の受信パケットの合計数（フレームビットを除き、FCS オクテットを含む）。
Undersize Received	GOOD CRC を持つサイズが 64 オクテット未満の受信パケットの合計数（フレームビットを除き、FCS オクテットを含む）。
Alignment Errors	サイズの範囲が 64-1518 オクテット（フレームビットを除き、FCS オクテットを含む）で、包括的ですが、整数でないオクテット数の不正な Frame Check Sequence（FCS）を持つ受信パケットの合計数。
Rx FCS Errors	サイズの範囲が 64-1518 オクテット（フレームビットを除き、FCS オクテットを含む）で、包括的ですが、整数であるオクテット数の不正な Frame Check Sequence（FCS）を持つ受信パケットの合計数 。
Overruns	このポートが入力パケットでオーバロードしたため廃棄されたフレームの合計数。
Total Ignored Frames	中止されたものを含む廃棄されたパケットの合計数。
Total Deferred Frames	コリジョンに会ったために、複数の試みを行ったが送信できなかったフレームの合計数。
Received Packets Not Forwarded	
Total Received Packets Not Forwarded	送信処理で廃棄（すなわち、フィルタ）された有効な受信フレームの回数。
Local Traffic Frames	宛先アドレスがこのポートから離れて位置しているために、送信処理で廃棄したフレームの合計数。
802.3x Pause Frames Received	PAUSE 操作を示す opcode を持つインタフェースで受信した MAC コントロールフレームの回数。 本カウンタは、インタフェースが半 2 重で動作している場合には増加しません。
Unacceptable Frame Type	許可できないフレームタイプであるために本ポートから廃棄されたフレーム数。
Multicast Tree Viable Discards	マルチキャストツリーの変更中に VLAN のためにマルチキャストツリーにルックアップが発生した場合に廃棄されたフレーム数。
Reserved Address Discards	IEEE 802.1 予約アドレスに向かう予定で、システムがサポートしていないために廃棄されたフレーム数。
Broadcast Storm Recovery	Broadcast Storm Recovery が有効である場合に FF:FF:FF:FF:FF:FF に向かう予定で廃棄されたフレーム数。
CFI Discards	CFI ビットセットを持ち、RIF のアドレスが標準フォーマットでない場合に廃棄されたフレーム数。
Upstream Threshold	パケットの優先度レベルに有効なセルディスクリプタがないために廃棄されたフレーム数。

項目	説明
Packets Transmitted Octets	
Total Packets Transmitted (Octets)	ネットワークが受信した（不正なパケットを含む）データの総オクテット数（フレームビットを除き、FCS オクテットを含む）。これは、イーサネット使用率の合理的な見積りとして使用されます。より高い精度が必要な場合、etherStatsPkts と etherStatsOctets オブジェクトを「common interval」の前後にサンプリングします。
Packets Transmitted 64 Octets	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）。
Packets Transmitted 65-127 Octets	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）。
Packets Transmitted 128-255 Octets	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）。
Packets Transmitted 256-511 Octets	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）。
Packets Transmitted 512-1023 Octets	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）。
Packets Transmitted 1024-1518 Octets	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）。
Maximum Frame Size	インタフェースがサポートしている、または設定されているイーサネットフレームサイズフレームサイズの最大値。イーサネットヘッダ、CRC、およびペイロードが含まれます。範囲は 1518-9216 です。最大フレームサイズの初期値は 1518 です。
Packets Transmitted Successfully	
Total Packets Transmitted Successfully	本ポートからセグメントに送信されたフレーム数。
Unicast Packets Transmitted	要求された上位レベルのプロトコルがサブネットワークのユニキャストアドレスに送信されたパケットの合計数。破棄されたもの、または送信されなかったものも含みます
Multicast Packets Transmitted	要求された上位レベルのプロトコルがマルチキャストアドレスに送信されたパケットの合計数。破棄されたもの、または送信されなかったものも含みます。
Broadcast Packets Transmitted	要求された上位レベルのプロトコルがブロードキャストアドレスに送信されたパケットの合計数。破棄されたもの、または送信されなかったものも含みます。
Transmit Errors	
Total Transmit Errors	Single、Multiple、および Excessive Collisions の合計数。
Tx FCS Errors	サイズの範囲が 64-1518 オクテット（フレームビットを除き、FCS オクテットを含む）で、包括的ですが、整数であるオクテット数の不正な Frame Check Sequence（FCS）を持つ受信パケットの合計数。
Tx Oversized	許可されている最大のフレームサイズを超過したフレームの合計数。 本カウンタには、10Mb/s の場合に 815 カウント / 秒の最大インクリメント速度があります。
Underrun Errors	送信の FIFO バッファがフレーム送信中に空になったために廃棄されたフレームの合計数。
Transmit Discards	
Total Transmit Packets Discarded	廃棄された Single、Multiple、および Excessive Collisions フレームの合計。
Total Output Packets Drops	エージングされたパケットの合計数。
Single Collision Frames	1 個のコリジョンにより送信されていなかった特定インタフェース上のフレーム送信に成功した回数。
Multiple Collision Frames	1 個以上のコリジョンにより送信されていなかった特定インタフェース上のフレーム送信に成功した回数。
Excessive Collision Frames	過度のコリジョンのために特定インタフェースで送信エラーをとなったフレーム数。
Late Collision Frames	512 ビットのコリジョンが通過した後に発生したコリジョンの合計数。
Port Membership Discards	イーグレスフィルタリングが有効とされていたために本ポートの入り口で廃棄されたフレーム数。
Lost/No Carrier Frames	ハードウェアのキャリア信号が検知されない場合にキャリア検出の損失が起こります。 キャリア信号を存在していなかったか、または存在していたが検出できなかったことが原因かもしれません。 そのような各イベントにより本カウンタは増えていきます。

項目	説明
Protocol Statistics	
STP BPDUs Received	受信した STP BPDU 数。
xSTP BPDUs Transmitted	選択ポートで送信した STP BPDU 数。
RSTP BPDUs Received	選択ポートで受信した RSTP BPDU 数。
RSTP BPDUs Transmitted	選択ポートで送信した RSTP BPDU 数。
MSTP BPDUs Received	選択ポートで受信した MSTP BPDU 数。
MSTP BPDUs Transmitted	選択ポートで送信した MSTP BPDU 数。
802.3x Pause Frames Transmitted	PAUSE 操作を示す opcode を持つインタフェースで送信した MAC コントロールフレームの回数。本カウンタは、インタフェースが半 2 重で動作している場合には増加しません。
GVRP PDUs Received	GVRP レイヤで受信した GVRP PDU の数。
GVRP PDUs Transmitted	GVRP レイヤで送信した GVRP PDU の数。
GVRP Failed Registrations	GVRP 登録を完了することができなかった回数。
GMRP PDUs Received	GVRP レイヤで受信した GMRP PDU の数。
GMRP PDUs Transmitted	GVRP レイヤで送信した GMRP PDU の数。
GMRP Failed Registrations	行われた GMRP 登録を完了することができなかった回数。
Time Since Counters Last Cleared	このポートの統計情報が最後にクリアされてからの経過時間（日、時、分、秒）を表示します。

「Refresh」ボタンをクリックして画面上のデータを更新し、最新の統計情報を表示します。

統計情報のクリア

「Clear Counters」ボタンをクリックして、すべての統計情報をクリアし、初期値に戻します。「Clear All Counters」ボタンをクリックして、全ポートの統計情報のすべてをクリアします。全ポートのすべての統計情報を初期値に戻します。

ポートサマリ情報

スイッチにおける 1 ポートあたりのトラフィック統計情報のサマリを表示します。

LAN タブ > Monitoring > System Statistics > Port 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。

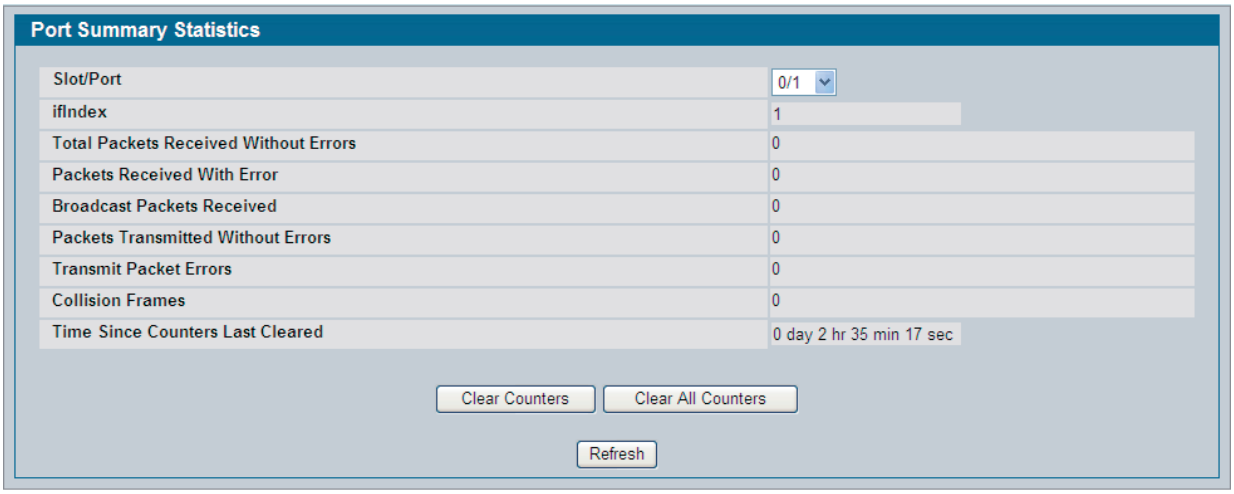


図 3-71　Port Summary Statistics 画面

本画面には次の項目があります。

項目	説明
Slot/Port	データを表示または設定するインタフェースを選択します
ifIndex	本ポートに関連するインタフェーステーブルのエントリの ifIndex を表示します。
Total Packets Received Without Errors	エラーなしで受信したパケットの合計数。
Packets Received With Error	上位レイヤプロトコルに送信されることを防御したエラーを含む内向きパケットの合計数。
Broadcast Packets Received	ブロードキャストアドレスに向けられた正常に受信したパケットの合計数。 これには、マルチキャストパケットは含まれていないことにご注意ください。
Packets Transmitted Without Errors	本ポートからセグメントに送信されたフレーム数。
Transmit Packet Errors	エラーのために、送信できなかった外向きパケット数。
Collision Frames	イーサネットセグメントにおける推定総コリジョン数。
Time Since Counters Last Cleared	このポートの統計情報が最後にクリアされてからの経過時間（日、時、分、秒）を表示します。

「Refresh」ボタンをクリックして画面上のデータを更新し、最新の統計情報を表示します。

統計情報のクリア

「Clear Counters」ボタンをクリックして、すべての統計情報をクリアし、初期値に戻します。「Clear All Counters」ボタンをクリックして、全ポートの統計情報のすべてをクリアします。全ポートのすべての統計情報を初期値に戻します。

システムのユーティリティの使用

システムのユーティリティ機能にはスイッチの管理を補助する以下の設定があります。

- 適用するすべての変更の保存
- システムのリセット
- コンフィグレーションを初期値にリセットする
- パスワードを初期値にリセットする
- TFTP を使用したファイルのスイッチへのダウンロード
- TFTP を使用したスイッチからのファイルのアップロード
- マルチイメージサービス
- HTTP ファイルのダウンロード
- Startup-config ファイルの削除
- 自動インストール
- トレースルート
- トラップログ

適用するすべての変更の保存

「Submit」ボタンをクリックすると、変更をシステムに適用し、動作中のコンフィグレーションファイルに保存します。しかし、これらの変更は、不揮発性メモリに保存されないため、システムがリセットされると失われてしまいます。「Save All Applied Changes」画面を使用して、サブミットした変更をシステムリセット後も保持します。

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

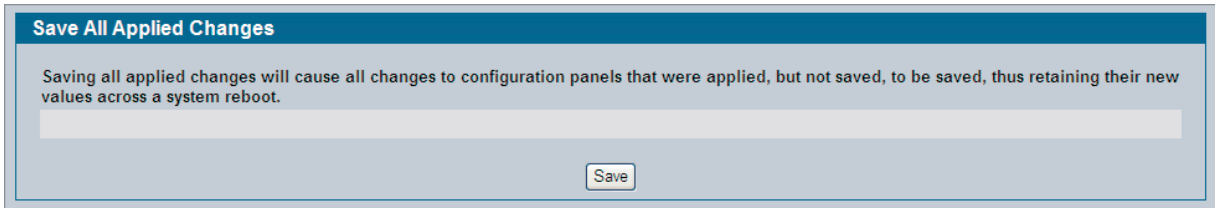


図 3-72　Save All Applied Changes 画面

「Save」ボタンをクリックして、システムに適用されたすべての変更がシステムのリセット後にも保持されるように NVRAM に保存します。

システムのリセット

システムをリセットします。プラットフォームがスタックをサポートしている場合、本画面を使用してスタック内のスイッチ、またはスタック内のすべてのスイッチをリセットすることができます。

Tool > Reboot 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。

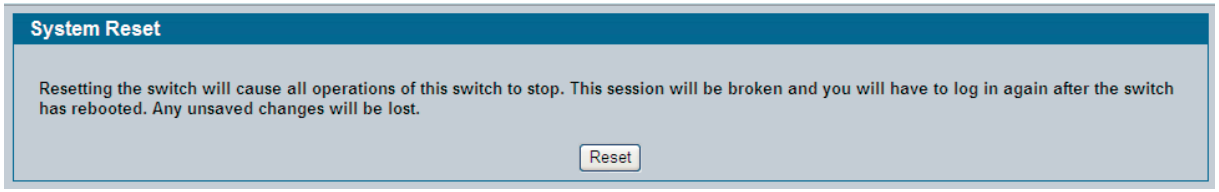


図 3-73　System Reset 画面

スタックしているプラットフォームでは、プルダウンメニューからリセットするスタック内の 1 つ、またはすべてのスイッチを選択することができます。スタックをサポートしないプラットフォームでは、この項目は表示されません。

「Reset」ボタンをクリックすると、システムのリセットが開始されます。最後のシステムリセット以後にサブミットした変更を保存していない場合、変更はリセットの後にシステムに適用されません。

コンフィグレーションを初期値にリセットする

システムのコンフィグレーションを工場出荷時の初期設定に戻します。

注意 本スイッチの IP アドレスの初期値は 10.90.90.90 で、DHCP クライアントは無効です。システムを初期値にリセットすると、ネットワーク IP アドレスは「10.90.90.90」に戻ります。ネットワーク情報に関する情報については、「スイッチのネットワークへの接続」（14 ページ）を参照してください。

Tool > Reset 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。

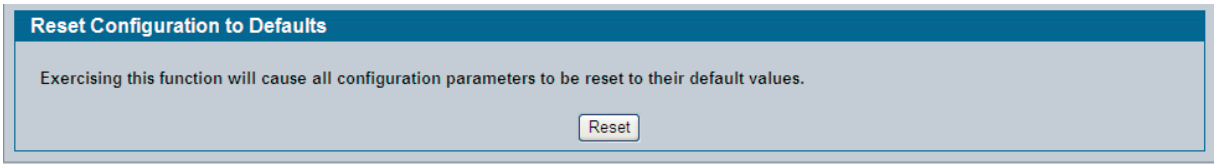


図 3-74　Reset Configuration to Defaults 画面

工場出荷時設定に戻すために「Reset」ボタンをクリックします。画面は更新され、リセットの確認画面が表示されます。再び「Reset」ボタンをクリックして、操作を終了します。

パスワードを初期値にリセットする

読み出し / 書き込み権限のあるユーザ（admin）と読み出し権限だけのユーザ（guest）のパスワードをリセットします。初期値では、パスワードは空白です。ご使用のシステムに追加の読み出し権限ユーザを設定している場合、そのパスワードには影響しません。

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

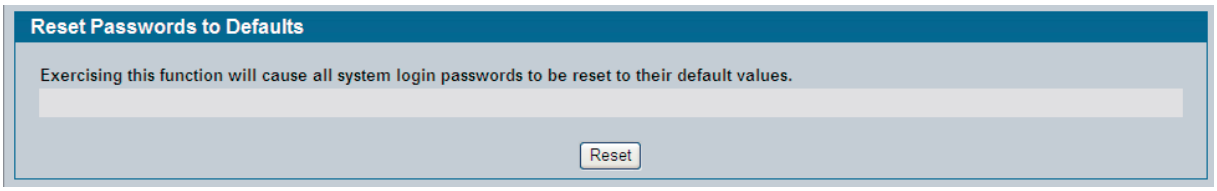


図 3-75　Reset Passwords to Defaults 画面

「Reset」ボタンをクリックし、初期値のユーザのパスワードを工場出荷時設定に戻します。

注意 読み出し / 書き込み権限のあるユーザ（admin）のパスワードを変更する場合、ユーザ名と初期パスワードで再認証を行う必要があります。

TFTP を使用したファイルのスイッチへのダウンロード

TFTP サーバからスイッチにイメージファイル、コンフィグレーションファイル、CLI バナーファイル、および SSH または SSL ファイルをダウンロードします。また、HTTP 経由でファイルをダウンロードすることもできます。

詳しくは、「HTTP ファイルのダウンロード」（90 ページ）を参照してください。

Tool > Download 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

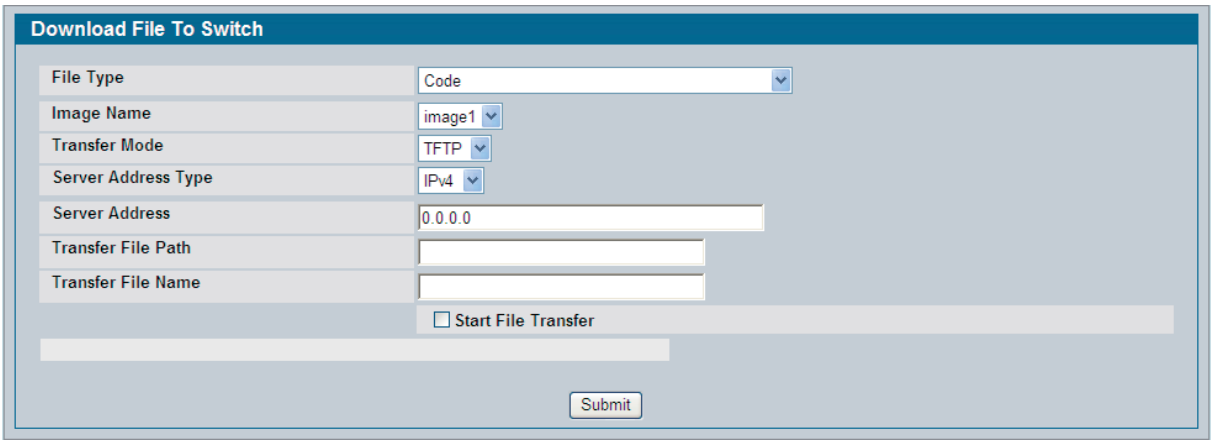


図 3-76　Download File to Switch 画面

本画面には次の項目があります。

項目	説明
File Type	スイッチにダウンロードするファイルタイプを指定します。 • CLI Banner - CLI バナーは、ログインプロンプトの前にコマンドラインインタフェースに表示されるテキストです。ダウンロードされる CLI バナーはテキストファイルであり、telnet、SSH、またはシリアル接続を使用してスイッチに接続する場合に表示されます。 • Code - コードはシステムソフトウェアのイメージであり、イメージ（image1 と image2）と呼ばれる 2 つのフラッシュセクタの 1 つに保存されています。アクティブなイメージはアクティブなコピーを保存しており、一方、他のイメージは 2 番目のコピーを保存しています。デバイスは、アクティブイメージから起動し、実行されます。アクティブイメージが不正であると、システムはアクティブでないイメージから自動的にブートされます。これは起動の更新処理で行われるフォールトトレランス機能です。 • Configuration - 有効なバイナリコンフィグレーションファイルのコピー（fastpath.cfg）が TFTP サーバ上にあると、それをスイッチにダウンロードすることができます。 • Text Configuration - テキストベースのコンフィグレーションファイルにより、D-Link ソフトウェアのためにコンテンツを移動しないで、必要に応じて、設定したテキストファイル（startup-config）をオフラインで編集することができます。テキストベースのコンフィグレーションの最も一般的な使用法は、デバイスから動作中のコンフィグレーションファイルをアップロードして、それを別の同様のデバイス用にカスタマイズ（つまり、デバイス名、シリアル番号、IP アドレスなどの変更）、そのデバイスにダウンロードすることです。 • SSH-1 RSA Key File - SSH-1 Rivest-Shamir-Adleman（RSA）Key File. SSH キーファイルをダウンロードするためには、SSH を管理上無効にして、アクティブな SSH セッションがないようにします。 • SSH-2 RSA Key PEM File - SSH-2 Rivest-Shamir-Adleman（RSA）Key File（PEM Encoded）. SSH キーファイルをダウンロードするためには、SSH を管理上無効にして、アクティブな SSH セッションがないようにします。 • SSH-2 DSA Key PEM File - SSH-2 Digital Signature Algorithm（DSA）Key File（PEM Encoded）. SSH キーファイルをダウンロードするためには、SSH を管理上無効にして、アクティブな SSH セッションがないようにします。 • SSL Trusted Root Certificate PEM File - SSL Trusted Root Certificate File（PEM Encoded） • SSL Server Certificate PEM File - SSL Server Certificate File（PEM Encoded） • SSL DH Weak Encryption Parameter PEM File - SSL Diffie-Hellman Weak Encryption Parameter File（PEM Encoded） • SSL DH Strong Encryption Parameter PEM File - SSL Diffie-Hellman Strong Encryption Parameter File（PEM Encoded）
Image Name	ダウンロードする Code イメージ（image1 または image2）を指定します。Code がファイルタイプとしてとして選定されている場合にだけ、本項目は表示されます。初期値では image1 です。

項目	説明
Transfer Mode	転送に使用されるプロトコル（TFTP、SFTP、または SCP）を指定します。
TFTP Server Address Type	サーバアドレスのタイプ（IPv4、IPv6、または DNS アドレス）を指定します。初期値では IPv4 です。
TFTP Server Address	「TFTP Server Address Type」に示された書式に応じて、TFTP サーバの IP アドレスを入力します。 工場出荷時設定は IPv4 アドレス「0.0.0.0」です。
TFTP File Path	選択ファイルが位置する TFTP サーバのパス（32 文字以内）を入力します。初期値は空白です。
TFTP File Name	TFTP サーバからダウンロードするファイル名（32 文字以内）を入力します。初期値は空白です。
Start File Transfer	ダウンロードを開始するために、このボックスをチェックして「Submit」ボタンをクリックします。

スイッチにファイルをダウンロードする

スイッチにファイルをダウンロードする前に、以下の条件が必要です。

- TFTP サーバからダウンロードするファイルが適切なディレクトリのサーバにある。
- ファイルは正しいフォーマットである。
- スイッチは TFTP サーバにパスを持っている。

以下の手順で TFTP サーバからスイッチにファイルをダウンロードします。

1. 「File Type」欄から、ダウンロードするファイルタイプを選択します。

2. D-Link イメージ（Code）をダウンロードしている場合、上書きするスイッチのイメージを選択します。別のファイルタイプをダウンロードしている場合、「Image Name」は使用できません。

注意 アクティブイメージを上書きしないことをお勧めします。

3. TFTP サーバの IP アドレスを検証し、ダウンロードされるソフトウェアイメージまたは他のファイルが TFTP サーバで使用できることを確認します。

4. 「TFTP Server IP Address」と「TFTP File Name」（TFTP サーバの IP アドレスのないフルパス）を入力します。

5. 「Start File Transfer」チェックボックスをクリックする、そして、次に、「Submit」ボタンをクリックします。
「Submit」ボタンのクリック後に、画面は更新され、「File transfer operation started」メッセージが表示されます。
ソフトウェアがデバイスにダウンロードされた後に、ファイル転送の操作が正常に終了したことを示すメッセージが表示されます。

スイッチにダウンロードするソフトウェアイメージをアクティブにするためには、「マルチイメージサービス」（89 ページ）を参照してください。

TFTP を使用したスイッチからのファイルのアップロード

コンフィグレーション（ASCII）とイメージ（バイナリ）ファイルをスイッチから TFTP サーバにアップロードします。

Tool > Upload 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。

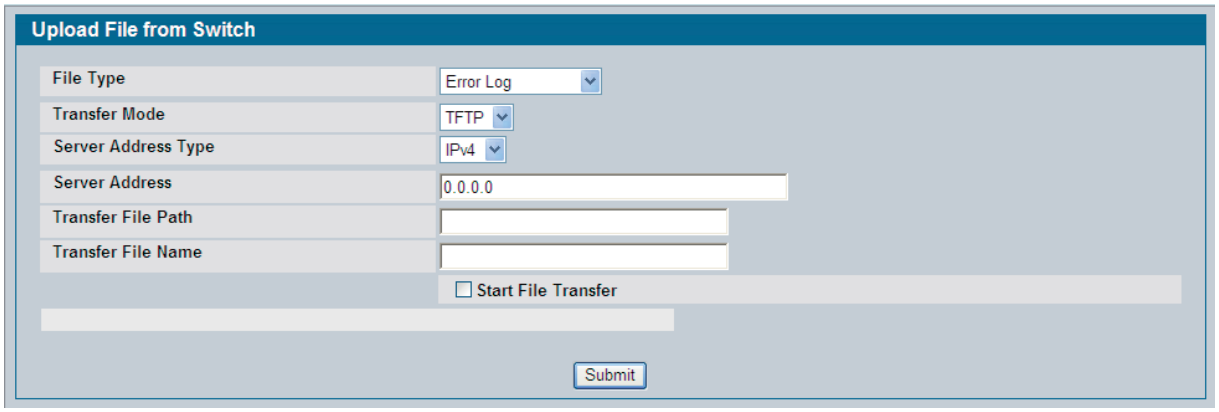


図 3-77　Upload File from Switch 画面

本画面には次の項目があります。

項目	説明
File Type	スイッチにアップロードするファイルタイプを指定します。 • CLI Banner - CLI バナーファイルを検索します。 • Code - 保存されたコードイメージを検索します。 • Configuration - 保存されている起動コンフィグレーション（.cfg）を検索し、TFTP サーバにコピーします。 • Text Configuration - テキストのコンフィグレーションファイル（startup-config）を検索します。 • Error Log - イベントログとして時々参照するシステムエラー（persistent）ログを検索します。 • Buffered Log - システムにバッファされた（in-memory）ログを検索します。 • Trap Log - システムトラップの記録を検索します。
Transfer Mode	アップロードする Code イメージ（image1 または image2）を指定します。「File Type」に Code が選択されている場合にだけ、本項目は表示されます。初期値は「image1」です。
Server Address Type	「Server Address」の書式を示すために、IPv4 または IPv6 を指定します。初期値は IPv4 です。
Server Address	「Server Address Type」に示された書式に応じて、TFTP サーバの IP アドレスを入力します。初期値は IPv4 アドレス「0.0.0.0」です。
Transfer File Path	ファイルをおく TFTP サーバのパス（32 文字以内）を入力します。初期値は空白です。
Transfer File Name	アップロードするファイルの宛先ファイル名（32 文字以内）を入力します。初期値は空白です。
Start File Transfer	アップロードを開始するために、このボックスをチェックして「Submit」ボタンをクリックします。

ファイルのアップロード

以下の手順で TFTP サーバからスイッチにファイルをアップロードします。

1. 「File Type」で、スイッチから TFTP サーバにコピーするファイルタイプを選択します。

2. D-Link イメージ（Code）をアップロードする場合、アップロードするスイッチのイメージを選択します。別のファイルタイプをアップロードしている場合、「Image Name」は使用できません。

3. 「Server Address Type」と「Server IP Address」（TFTP サーバの IP アドレスのないフルパス）を入力します。

4. 「Start File Transfer」チェックボックスをクリックし、「Submit」ボタンをクリックします。
   「Submit」ボタンをクリックした後に、画面は更新され、「File transfer operation started」メッセージが表示されます。
   ソフトウェアがデバイスにダウンロードされた後に、ファイル転送の操作が正常に終了したことを示すメッセージが表示されます。

マルチイメージサービス

システムは不揮発性ストレージに D-Link ソフトウェアの 2 つのバージョンを保持します。1 つのイメージがアクティブなイメージで、2 つ目のイメージはバックアップイメージです。アクティブなイメージはスイッチの再起動の際にロードされます。D-Link ソフトウェアをアップグレードまたはダウングレードする場合、本機能はスイッチのダウンタイムを減少させます。

古いソフトウェアバージョンを実行するシステムは、新しいソフトウェアバージョンで作成されたコンフィグレーションファイルを無視します（ロードしません）。新しいソフトウェアバージョンで作成されたコンフィグレーションファイルが、古いソフトウェアバージョンを実行するシステムによって検出される場合、システムは適切な警告を表示します。

起動イメージを設定します。

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

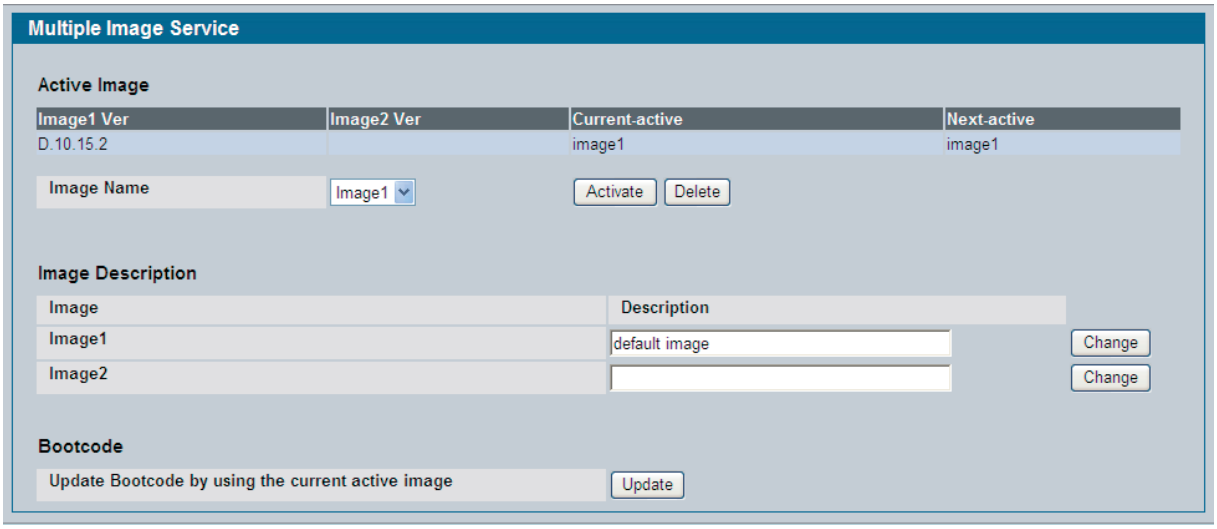


図 3-78　Multiple Image Service 画面

本画面には次の項目があります。

項目	説明
Image Name	メニューからの「Image1」または「Image2」を選択し、次にリロード時にアクティブまたは削除されます。
Current-active	現在のアクティブイメージ名を表示します。
Next-active	次にスイッチがリロードする際にアクティブになるように設定するイメージ名を表示します。
Image Description	必要であれば、個々の Image1 または Image2 のソフトウェアイメージを説明する名称を入力します。

- 「Activate」ボタンをクリックして、「Image Name」で選択されたイメージを次回の再起動用のアクティブイメージにします。

注意　イメージをアクティブ化した後、新しいコードを実行するためにスイッチのシステムリセットを実行する必要があります。

イメージの削除

「Delete」ボタンをクリックし、スイッチの不揮発性ストレージから選択したイメージを削除します。アクティブなイメージは削除できません。

イメージの説明の更新

「Change」ボタンをクリックしてと、スイッチのイメージの説明を更新します。

ブートコードの更新

アップロードしたファイルがブートローダコードだけを含める場合、「Update」ボタンをクリックします。

HTTP ファイルのダウンロード

HTTP セッション（ご使用の Web ブラウザ）を使用して様々なタイプのファイルをスイッチにダウンロードすることができます。

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

図 3-79　HTTP File Download

本画面には次の項目があります。

項目	説明
File Type	スイッチにアップロードするファイルタイプを指定します。 • Code - フラッシュメモリ内の OS を更新します。（初期値） • Configuration - スイッチのコンフィグレーションを更新します。ファイルにエラーがあると、更新は中止されます。 • SSH-1 RSA Key File - SSH-1 Rivest-Shamir-Adleman（RSA）Key File • SSH-2 RSA Key PEM File - SSH-2 Rivest-Shamir-Adleman（RSA）Key File（PEM Encoded） • SSH-2 DSA Key PEM File - SSH-2 Digital Signature Algorithm（DSA）Key File（PEM Encoded） • SSL Trusted Root Certificate PEM File - SSL Trusted Root Certificate File（PEM Encoded） • SSL Server Certificate PEM File - SSL Server Certificate File（PEM Encoded） • SSL DH Weak Encryption Parameter PEM File - SSL Diffie-Hellman Weak Encryption Parameter File（PEM Encoded） • SSL DH Strong Encryption Parameter PEM File - SSL Diffie-Hellman Strong Encryption Parameter File（PEM Encoded） • CLI Banner - ログインプロンプトが現れる前に表示するバナーファイルをダウンロードします。 注意　SSH キーファイルをダウンロードするためには、SSH を管理上無効にして、アクティブな SSH セッションがないようにします。
Image Name	ダウンロードする Code イメージ（image1 または image2）を指定します。初期値は image1 です。 Code が「File Type」で選択されている場合にだけ、本項目は表示されます。
Select File	ダウンロードするファイルのパスとファイル名を 80 文字以内で入力します。

「Start File Transfer」ボタンをクリックすると、ダウンロードが開始されます。

Startup-config ファイルの削除

不揮発性メモリに保存されているテキストベースのコンフィグレーションファイルを削除します。

Tool > Erase Startup-config 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。

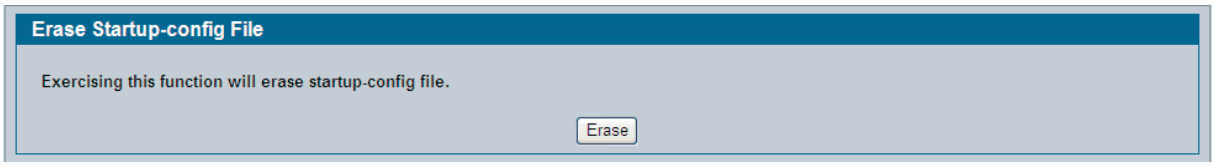


図 3-80　Erase Startup-config File 画面

「Erase」ボタンをクリックしてファイルを削除します。

自動インストール

AutoInstall 機能は、デバイスの電源がオンになり、起動処理中にコンフィグレーションファイルがデバイスストレージに見つからなかった場合に自動的にスイッチのコンフィグレーションを有効にします。DHCP サーバと通信することで、AutoInstall はスイッチの IP アドレスと TFTP サーバの IP アドレスを取得します。さらに、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して、スイッチにインストールを行います。

スイッチと TFTP サーバの両方の IP アドレスを取得した後に、DHCP サーバが指定した起動ファイル名を使用することでホストが指定したコンフィグレーションのダウンロードを行います。

スイッチがファイルの取得に失敗すると、それは無期限に再試行されます。

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

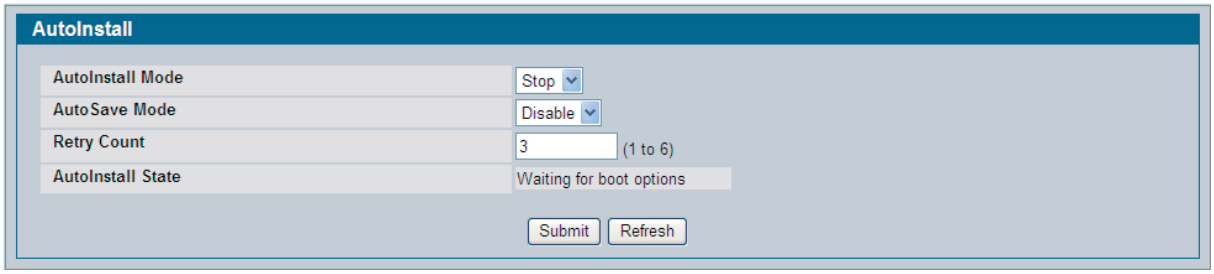


図 3-81　AutoInstall 画面

本画面には次の項目があります。

項目	説明
AutoInstall Mode	自動インストールのモードを選択します。 • Start - サーバの IP アドレスおよびコンフィグレーションファイル名を取得し、DHCP サーバへのリクエストの送信を開始します。サーバアドレスを取得すると、AutoInstall はサーバからコンフィグレーションファイルを検索して、ダウンロードを開始します。成功すると、スイッチにそのコンフィグレーションファイルを適用します。AutoInstall 処理の開始後に、「AutoInstall State」および「Retry Count」欄のメッセージによって処理の状態をモニタリングできます。 • Stop - 処理を終了します。
AutoSave Mode	不揮発性メモリへのネットワークコンフィグレーションの保存を有効または無効にします。 • Enable - コンフィグレーションは TFTP サーバからオペレータの介在なしでダウンロード後に保存されます。 • Disable - 必要に応じてオペレータがコンフィグレーションを明示的に保存する必要があります。
Retry Count	現在の AutoInstall セッション中にスイッチが TFTP サーバにコンタクトを試みる回数。
AutoInstall State	現在またはごく最近終了した AutoInstall セッションの状態。

「Submit」ボタンをクリックして、スイッチを本画面の値に更新します。「Refresh」ボタンをクリックして、画面の情報を更新します。

トレースルート

パケットがリモートにある宛先へのパスを検出します。

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

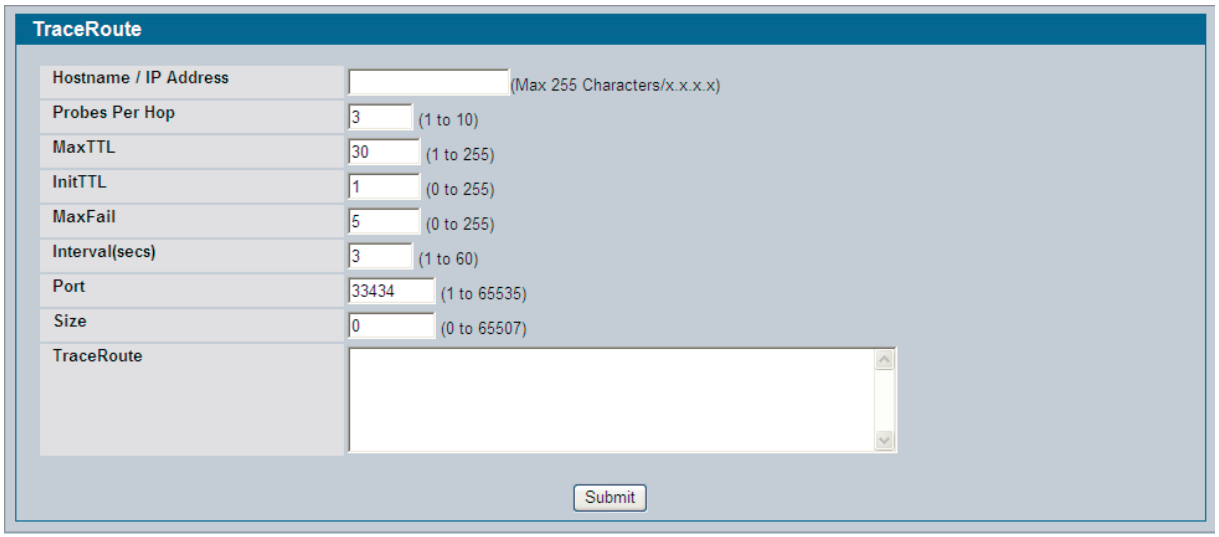


図 3-82　TraceRoute 画面

本画面には次の項目があります。

項目	説明
Hostname/IP Address	スイッチがパスの検出を行うステーションの IP アドレスまたはホスト名を入力します。
Probes Per Hop	各ホップが調査される回数を入力します。
MaxTTL	ホップ数内のパケットの最大稼働期間を入力します。
InitTTL	ホップ数内のパケットの最初の稼働期間を入力します。
MaxFail	セッション内に許可されるエラーの最大数を指定します。
Interval (secs)	調査の間隔（秒）を入力します。
Port	プローブパケットに UDP の宛先ポートを入力します。
Size	プローブパケットのサイズを入力します。
TraceRoute	トレースルートからの出力を表示します。

「Submit」ボタンをクリックして、トレースルートを開始します。結果は TraceRoute ボックスに表示されます。

Trap Log（トラップログ）

トラップログ内のエントリを参照します。TFTP サーバにファイルをコピーする方法に関する情報に関しては、「TFTP を使用したスイッチからのファイルのアップロード」（88 ページ）を参照してください。

LAN > Monitoring > Log > Trap 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 3-83　Trap Log 画面

本画面には次の項目があります。

項目	説明
Number of Traps Since Last Reset	最後にトラップログエントリをクリアしてから生成されたトラップの数。
Trap Log Capacity	ログ内に保存されているトラップの最大数。トラップ数が容量を超えると、エントリは最も古いエントリを上書きします。
Number of Traps Since Log Last Viewed	トラップが最後に表示されてから発生したトラップの数。 何らかの方式（端末のインタフェースの表示、Web の表示、スイッチからアップロードされたファイルなど）でトラップを表示することで、このカウンタを 0 にクリアします。
Log	このトラップのシーケンス番号。
System Up Time	スイッチの最後の再起動後にトラップが発生した時間（日、時、分、秒）。
Trap	トラップを識別する情報を表示します。

「Clear Log」ボタンをクリックして、ログ内のすべてのエントリをクリアします。その後ログの表示は新しいログエントリだけです。

DHCP サーバの管理

DHCP は、一般的に、IP アドレス、ゲートウェイ、および DNS、NTP、そして / または、SIP パラメータなどの他のネットワーク定義を割り当てる目的のために、クライアント（例 : ホスト）とサーバ（例 : ルータ）間で使用されます。「DHCP Server」フォルダには DHCP パラメータとデータを定義して、表示する Web 画面へのリンクがあります。以下の画面は、DHCP Server フォルダからアクセス可能です。

- グローバル設定
- プール設定
- プールオプション
- 設定のリセット
- DHCP サーバのサマリ
- サーバの統計情報

グローバル設定

DHCP のグローバルな設定を行います。

LAN タブ > Administration > DHCP Server > 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。

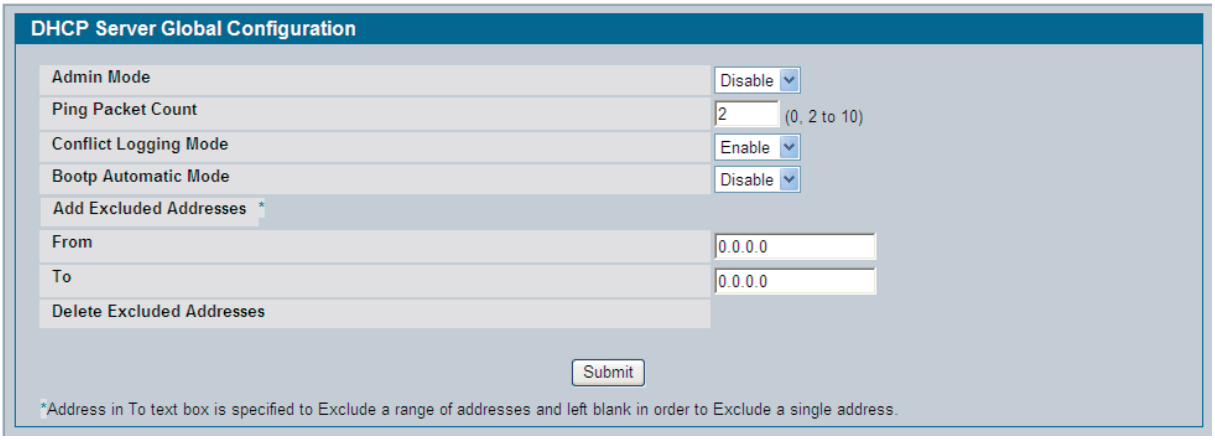


図 3-84　DHCP Server Global Configuration 画面

本画面には次の項目があります。

項目	説明
Admin Mode	スイッチ上における DHCP サーバ機能を有効または無効にします。初期値は「Disabled」（無効）です。
Ping Packet Count	ping 機能の一部として重複のチェックを行うために、サーバが Pool アドレスに送信するパケットの数を指定します。初期値は 2（秒）です。範囲は 0、2-10 です。0 に値を設定すると、機能は無効となります。
Conflict Logging Mode	DHCP サーバに重複してログインすることを有効または無効にします。初期値は有効です。
Bootp Automatic Mode	ダイナミックプールへの Bootp を有効または無効にします。 • Enable - BootP クライアントに対して自動的にアドレスプール内のアドレスの割り当てを許可します。（初期値） • Disable - BootP クライアントに自動アドレスプールアドレスを使用しません。
Add Excluded Addresses	「From」と「To」を使用して、サーバがクライアントに割り当てない IP アドレスを指定します。 アドレスの範囲を除外する場合、範囲の境界値を設定します。 注意　範囲に何千ものアドレスを追加しないことを強くお勧めします。範囲が大きいと、DHCP サーバで IP アドレスを割り当てるのにかかる時間が長くなります。
From	アドレス範囲を除外するために、範囲には低い値のアドレスを指定します。 1 つの IP アドレスを除外するためには、初期値「0.0.0.0」の場合に「From」にアドレスを入力し、「To」は空白のままにします。例えば、除外するアドレスリストにアドレス「192.168.17.100」を追加します。
To	アドレス範囲を除外するために、範囲には高い値のアドレスを指定します。1 つの IP アドレスを除外する場合には、ここには値を入力しません。
Delete Excluded Addresses	除外するアドレスを追加すると、この項目名の下に表示されます。各アドレス（アドレス範囲）には、チェックボックスがあります。

設定の変更、または除外アドレス範囲の追加をした場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。「From」か「To」に値を入力するたびに「Submit」ボタンをクリックして、アドレスまたはアドレス範囲を除外アドレスリストに追加します。

アドレス範囲の削除

除外アドレス範囲からアドレスまたはアドレス範囲を削除するためには、「Delete Excluded Addresses」欄の下にある 1 つ以上のチェックボックスを選択し、「Submit」ボタンをクリックします。

プール設定

サーバで割り当てることができるアドレスのプールを作成します。

LAN タブ > Administration > DHCP Server > Pool 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。

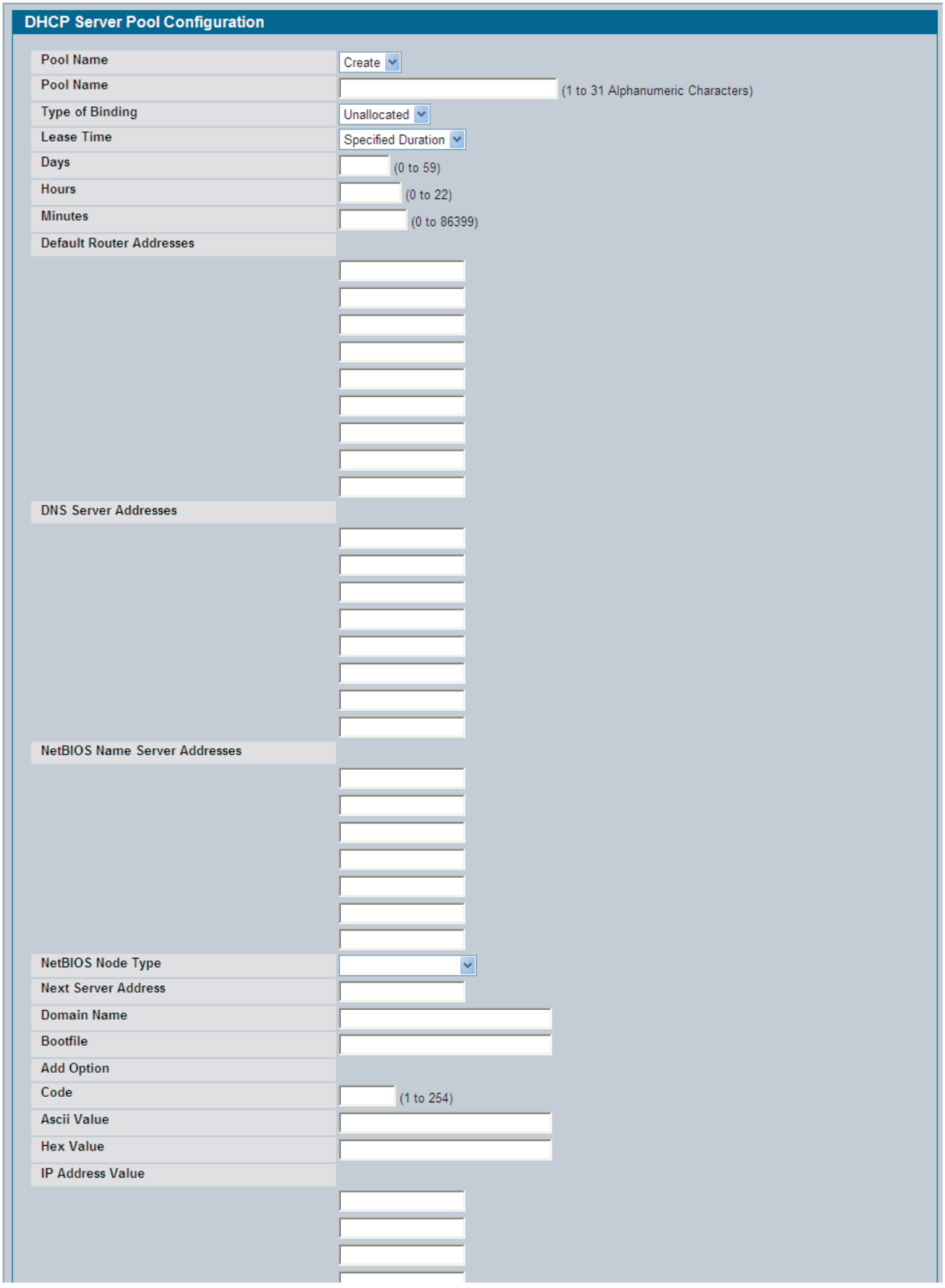


図 3-85　DHCP Server Pool Configuration 画面

「Default Router Addresses」、「DNS Server Addresses」、「NetBIOS name Server Addresses」、および「IP Address Value」に最大 8 つのアドレスを追加することができます。

「Type of Binding」から「Dynamic」または「Manual」を選択すると、画面が更新されて少し異なる設定用欄が表示されます。

本画面には次の項目があります。

項目	説明
Pool Name	読み出し / 書き込み権限を持つユーザに対して、追加オプションの「Create」およびすべての既存プール名を表示します。「Create」を選択すると、別のテキストボックス「Pool Name」が表示されます。ここで作成するプール名を入力します。参照権限だけを持つユーザに対しては、本項目は既存のプール名だけを表示します。
Pool Name	読み出し / 書き込み権限を持つユーザが「Pool Name」のプルダウンメニューで「Create」を選択した場合に、本欄は表示されます。作成するプール名を半角英数字 31 文字以内で指定します。
Type of Binding	プールに割り当てるタイプを指定します。 • Unallocated - IP アドレスはクライアントに割り当てられません。 • Dynamic - IP アドレスは DHCP サーバによって自動的にクライアントに割り当てられます。 • Manual - クライアントの MAC アドレスに基づいてクライアントに IP アドレスをスタティックに割り当てます。
Network Number	「Type of Binding」に「Dynamic」を指定すると、本欄は表示されます。ダイナミックなプールの DHCP アドレスにネットワーク番号（ホストビット）を指定します。 例えば「192.168.5.0」がネットワーク番号であり、「255.255.255.0」がプールへのネットワークマスク（または 24 のプレフックス長）であれば、プール範囲の IP アドレスは「192.168.5.1」から「192.168.5.254」となります。
Network Mask	「Type of Binding」に「Dynamic」を指定すると、ダイナミックプールの DHCP アドレスに対してサブネットマスクを指定します。サブネットマスクを指定するために、「Network Mask」または「Prefix Length」に値を入力することができますが、両方の欄に値を入力しないでください。
Prefix Length	「Type of Binding」に「Dynamic」を指定すると、ダイナミックプールの DHCP アドレスに対してサブネット番号を指定します。サブネットマスクを指定するために、「Network Mask」または「Prefix Length」に値を入力することができますが、両方の欄に値を入力しないでください。値の範囲は 0-32 です。
Client Name	「Type of Binding」に「Manual」を指定すると、DHCP サーバがスタティックに IP アドレスを割り当てるクライアントに名前を指定します。この項目はオプションです。
Hardware Address	「Type of Binding」に「Dynamic」を指定すると、DHCP クライアントのハードウェアプラットフォームの MAC アドレスを指定します。
Hardware Address Type	「Type of Binding」に「Dynamic」を指定すると、DHCP クライアントのハードウェアプラットフォームのプロトコルを指定します。有効なタイプは、「ethernet」と「ieee802」です。初期値は「ethernet」です。
Client ID	「Type of Binding」に「Dynamic」を指定すると、DHCP マニュアルプールにクライアントの識別子を指定します。
Host Number	「Type of Binding」に「Dynamic」を指定すると、DHCP クライアントにスタティックに割り当てられる IP アドレスを指定します。クライアント識別子またはハードウェアアドレスの中の少なくとも 1 つが指定される場合にだけホストは設定されます。ホストを削除すると、「Manual Pool」の「Client Name」、「Client ID」、「Hardware Address」が削除されて、「Pool Type」は「Unallocated」に設定されます。
Host Mask	「Type of Binding」に「Dynamic」を指定すると、DHCP クライアントにスタティックに割り当てられるサブネットマスクを指定します。サブネットマスクを指定するために、「Host Mask」または「Prefix Length」に値を入力することができますが、両方の欄に値を入力しないでください。
Prefix Length	「Type of Binding」に「Dynamic」を指定すると、DHCP クライアントに手動でバインディングするためにサブネットマスクを指定します。サブネットマスクを指定するために、「Network Mask」または「Prefix Length」に値を入力することができますが、両方の欄に値を入力しないでください。値の範囲は 0-32 です。
Lease Time	クライアントを割り当てるリースのタイプを指定します。 • Infinite - ダイナミックバインディングのために、infinite リースタイムは最低 60 日間です。手動バインディングのために、infinite リースタイムは終了しないことを意味します。 • Specified Duration - リース期間を指定することを許可します。（初期値）
Days	「Specified Duration」リースタイムとして、本欄にはリース日数を指定します。初期値は 1 で、値の範囲は 0-59 です。
Hours	「Specified Duration」リースタイムとして、本欄にはリース時間を指定します。初期値は 1 で、値の範囲は 0-1439 です。
Minutes	「Specified Duration」リースタイムとして、本欄にはリース時間（0-86399 分）を指定します。初期値は 1 です。
Default Router Addresses	デフォルトルータの IP アドレスのリストをプールに指定します。希望する順に最大 8 つのアドレスを指定することができます。
DNS Server Addresses	DNS サーバの IP アドレスのリストをプールに指定します。希望する順に最大 8 つのアドレスを指定することができます。
NetBIOS Name Server Addresses	NetBIOS ネームサーバの IP アドレスのリストをプールに指定します。希望する順に最大 8 つのアドレスを指定することができます。
NetBIOS Node	DHCP クライアントに NetBIOS のノードタイプを入力します。 • b-node Broadcast - ブロードキャストクエリを使用します。 • p-node Peer-to-Peer - ネームサーバに対してポイント・ツー・ポイントのネームクエリを使用します。 • m-node Mixed - 最初にブロードキャストを使用し、次にネームサーバへのクエリを使用します。 • h-node Hybrid - 最初にネームサーバへのクエリを使用し、次にブロードキャストを使用します。

項目	説明
Next Server Address	TFTP サーバなどのクライアントの起動プロセスにおけるネクストサーバの IP アドレスを指定します。
Domain Name	DHCP クライアントに対するドメイン名を半角英数字 255 文字以内で指定します。
Bootfile	DHCP クライアントにデフォルトブートイメージ名を指定します。ファイル名は半角英数字 128 文字以内で指定します。
Add Options	本画面の残りの項目で、DHCP オプションの追加と設定を行うことができます。DHCP オプションの詳しい情報については、RFC 2132 を参照してください。
Code	DHCP オプションコードを指定します。有効範囲は 1-254 です。
Ascii Value	NVT ASCII 文字列を指定します。
Hex Value	16 進数のデータを区切って指定します。16 進数文字列における各バイトは 2 桁の 16 進数です。「:」(コロン) またはスペースで各バイトを分けることができます。「.」(ピリオド) は 2 バイト /4 桁の 16 進数を分けます。
IP Address Values	オプションの IP アドレスを指定します。

DHCP アドレスプールの値を変更した場合、「Submit」ボタンをクリックし、プールの変更をスイッチに適用します。

プールの削除

プールを削除するためには、プルダウンメニューから「Pool Name」を選択し、「Delete」ボタンをクリックします。

プールオプション

DHCP サーバがクライアントに渡すことができる DHCP オプションを設定します。DHCP オプションの詳しい情報については、RFC 2132 を参照してください。

LAN タブ > Administration > DHCP Server > Pool Options の順にメニューをクリックし、以下の画面を表示します。DHCP プールが存在しないと、「Pool Options」画面はここで示す項目を表示しません。

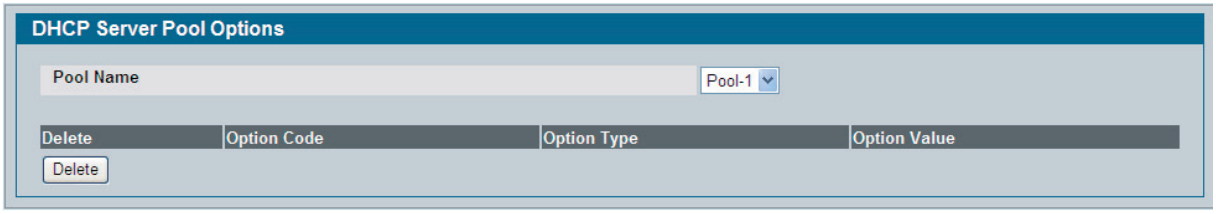


図 3-86　Pool Options 画面

DHCP プールがシステムに設定されていると、画面には以下の項目が表示されます。

項目	説明
Pool Name	参照または設定するオプションを持つ DHCP プール名を選択します。
Option Code	選択プールに設定されている DHCP オプションコードを表示します。
Option Type	選択プールに設定されているオプションコードに関連するオプションのタイプを表示します。 • Ascii - オプションタイプはテキストの文字列です。 • Hex - オプションタイプは 16 進数です。 • IP Address - オプションタイプは IP アドレスです。
Option Value	DHCP サーバからクライアントに渡されるオプションを表示します。

オプションコードの削除

選択プールのオプションコードを削除するためには、オプションコードを指定し、「Delete」ボタンをクリックします。読取専用ユーザは、本ボタンを参照することはできません。

設定のリセット

DHCP サーバクライアントに割り当てている IP アドレスバインディングをクリアします。

LAN タブ > Administration > DHCP Server > Reset 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

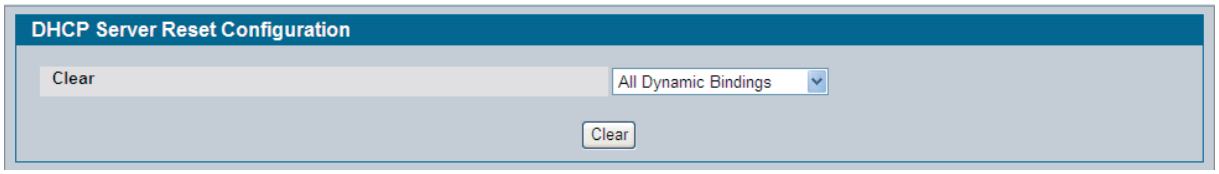


図 3-87　Reset Configuration 画面

本画面には次の項目があります。

項目	説明
Clear	DHCP サーバデータベースからクリアするものを指定します。 • All Dynamic Bindings - すべてのアドレスプールから全ダイナミックバインディングを削除します。（初期値） • Specific Dynamic Binding - 指定したバインディングを削除します。 • All Address Conflicts - DHCP サーバデータベースからコンフリクトするアドレスを削除します。 • Specific Address Conflict - データベースから指定したコンフリクトしているアドレスを削除します。
Clear IP Address	「Clear」欄から「Specific Dynamic Bindings」または「Specific Address Conflicts」を選択すると画面は更新され、「Clear IP Address」欄が表示されます。特定の IP アドレスを入力し、DHCP サーバからクリアします。

クリアするバインディングかコンフリクトを選択後に、必要であれば IP アドレスを指定して「Clear」ボタンをクリックし、DHCP サーバからバインディングを削除します。

DHCP サーバのサマリ

バインディング情報

DHCP サーバデータベースにおける IP アドレスバインディングに関する情報に参照します。

LAN タブ > Monitoring > DHCP Server Summary > Binding 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。

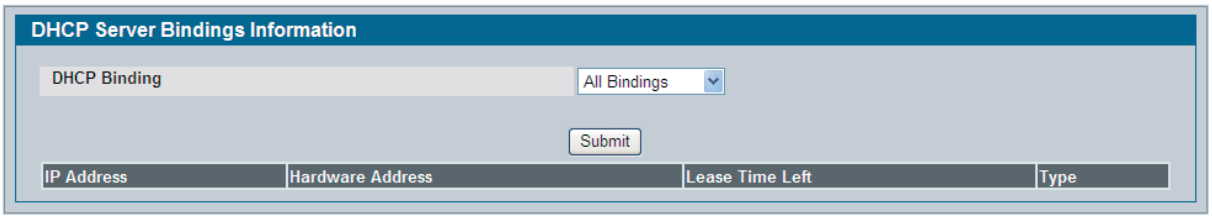


図 3-88　DHCP Server Bindings Information 画面

本画面には次の項目があります。

項目	説明
DHCP Binding	表示するバインディングを選択します。 • All Bindings - すべてのバインディングを表示します。 • Specific Binding - 指定のバインディングを表示します。本オプションを選択すると画面は更新され、「Binding IP Address」欄が表示されます。
Binding IP Address	バインディング情報を参照する IP アドレスを指定します。 「DHCP Binding」から「Specific Binding」を選択した場合にだけ、本項目を使用することができます。
IP Address	クライアントの IP アドレスを表示します。
Hardware Address	クライアントの MAC アドレスを表示します。
Lease Time Left	「Days」、「Hours」および「Minutes」（dd:hh:mm 形式）のリースに対する残り時間を表示します。
Type	バインディングのタイプ（dynamic または manual）を表示します。

「DHCP Server」を選択して「Submit」ボタンをクリックすると、情報が表示されます。

サーバの統計情報

DHCP サーババインディングとメッセージに関する情報を参照します。

LAN タブ > Monitoring > DHCP Server Summary > Server 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。

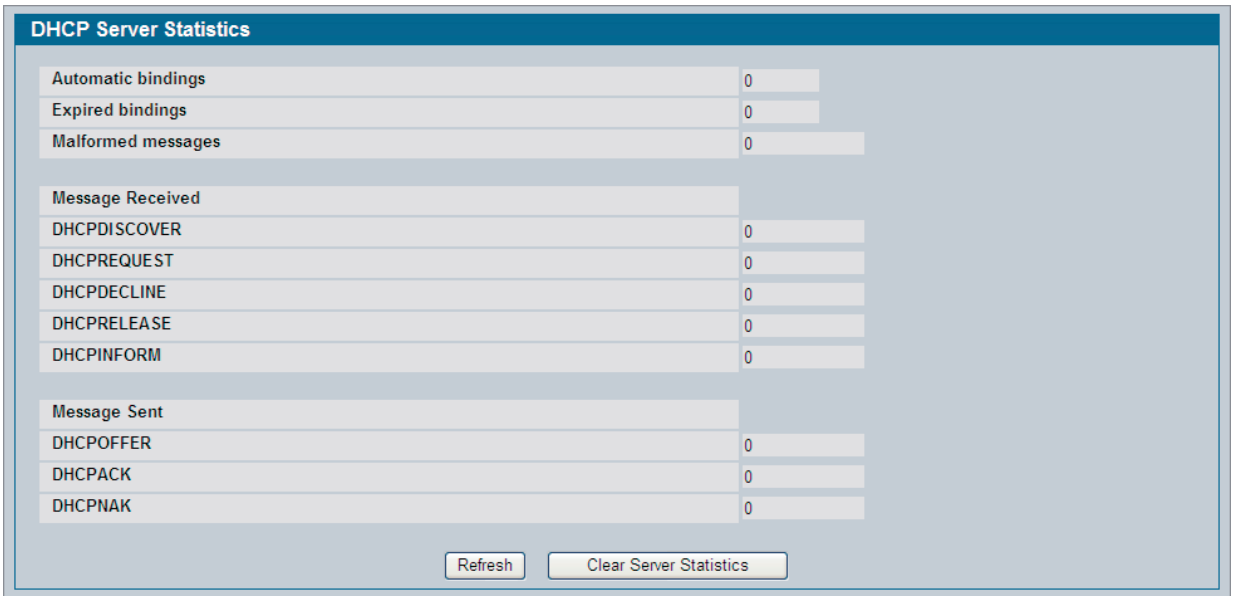


図 3-89　DHCP Server Statistics 画面

本画面には次の項目があります。

項目	説明
Automatic bindings	DHCP サーバにおけるオートバインディング数を表示します。
Expired bindings	DHCP サーバにおいて完了したバインディング数を表示します。
Malformed messages	不正なメッセージ数を表示します。
Message Received	
DHCPDISCOVER	DHCP サーバが受信した DHCPDISCOVER メッセージの数。
DHCPREQUEST	DHCP サーバが受信した DHCPREQUEST メッセージの数。
DHCPDECLINE	DHCP サーバが受信した DHCPDECLINE メッセージの数。
DHCPRELEASE	DHCP サーバが受信した DHCPRELEASE メッセージの数。
DHCPINFORM	DHCP サーバが受信した DHCPINFORM メッセージの数。
Message Sent	
DHCPOFFER	DHCP サーバが送信した DHCPOFFER メッセージの数。
DHCPACK	DHCP サーバが送信した DHCPACK メッセージの数。
DHCPNAK	DHCP サーバが送信した DHCPNAK メッセージの数。

「Refresh」ボタンをクリックしてと、画面の情報を更新します。

統計情報のクリア

「Clear Server Statistics」ボタンをクリックして、すべてのカウンタを 0 にリセットします。

Conflicts Information（コンフリクト情報）

同じ IP アドレスがネットワーク上の 2 つ以上のデバイスに割り当てられている場合などアドレスのコンフリクトを持つホストの情報を参照します。

LAN タブ > Monitoring > DHCP Server Summary > Conflicts 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。

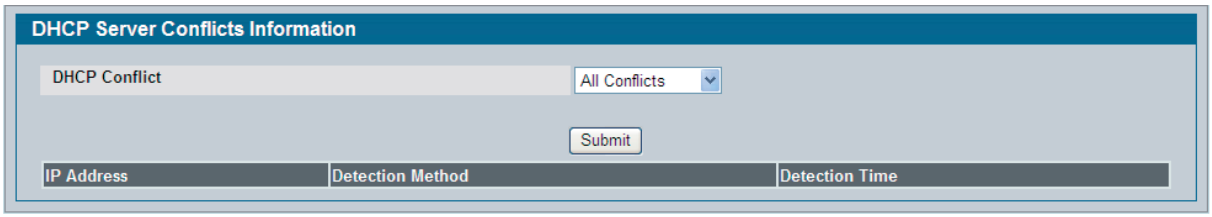


図 3-90　Conflicts Information 画面

本画面には次の項目があります。

項目	説明
DHCP Conflict	表示する DHCP コンフリクトを選択します。 • All Conflicts - すべてのコンフリクトを表示します。 • Specific Conflict - 指定のコンフリクトを表示します。本オプションを選択すると画面は更新され、「Conflict IP Address」欄が表示されます。
Conflict IP Address	コンフリクト情報を参照する IP アドレスを指定します。「DHCP Conflict」から「Specific Conflict」を選択した場合にだけ、本項目を使用することができます。
IP Address	クライアントの IP アドレスを表示します。
Detection Method	DHCP サーバ上でホストの IP アドレスを検索する方法を表示します。
Detection Time	コンフリクトが検出された時刻をシステムの稼働時間に基づく「N day NNh:NNm:NNs」形式で表示します。

DNS クライアントの設定

ネットワークが使用する DNS サーバの情報の設定、およびスイッチ / ルータが DNS クライアントとして動作する方法を設定します。

グローバル設定

グローバルな DNS の設定、および DNS クライアント状態情報の参照を行います。

LAN タブ > Administration > DNS Client > 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。

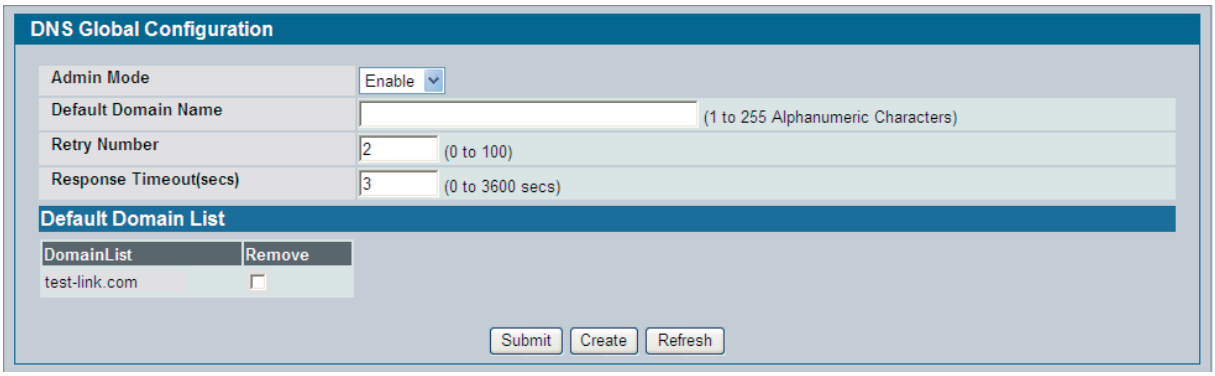


図 3-91　DNS Global Configuration 画面

本画面には次の項目があります。

項目	説明
Admin Mode	DNS クライアントの管理ステータスを有効または無効に設定します。初期値は「Enable」（有効）です。
Default Domain Name	DNS クライアントメッセージに対するデフォルトドメイン名を半角英数字 255 文字以内で指定します。 システムが資格のないホスト名に検索を実行している場合、本項目がドメイン名として提供されます。例えば、デフォルトドメイン名が「.com」であり、「hotmail」と入力すると、「hotmail」は「hotmail.com」に変更され、名前の解決が行われます。 初期値では、システムにはデフォルトドメイン名は設定されていません。
Retry Number	DNS クエリの再送信回数（0-100）を入力します。初期値は 2 です。
Response Timeout (secs)	リトライを行う前に DNS サーバがリクエストに応じることができる時間（0-3600 秒）を入力します。初期値は 3（秒）です。
Domain List	ドメインリストを入力して、資格のないホスト名に検索を実行する場合に使用するドメインを定義します。各名称は 256 文字未満で指定します。デフォルトドメイン名リストを使用して複数のデフォルトドメイン名が設定できます。 ドメインリストがないと、設定済みのデフォルトドメイン名が使用されます。

設定を変更した場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。

ドメイン名リストの作成

「Create」ボタンをクリックし、ドメイン名の新しいリストを作成します。

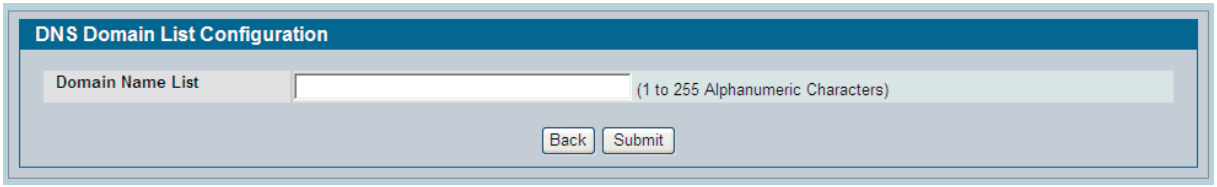


図 3-92　DNS Domain List Configuration 画面

リスト名を入力して「Submit」ボタンをクリックします。本手順を繰り返して、デフォルトドメインリストに複数のドメインを追加します。

ドメインの削除

デフォルトリストからドメインを削除するためには、削除する項目横の「Remove」オプションを選択して「Submit」ボタンをクリックします。

サーバ設定

ルータが使用する DNS サーバに関する情報を設定します。それらを作成する順番がそれらの優先度を決定します。つまり、DNS リクエストは最初に高い優先度サーバに向かいます。そのサーバが無効であるか、または設定されている応答時間に応答しないと、リクエストは次に高い優先度を持つサーバに向かいます。

LAN タブ > Administration > DNS Client > Server 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。

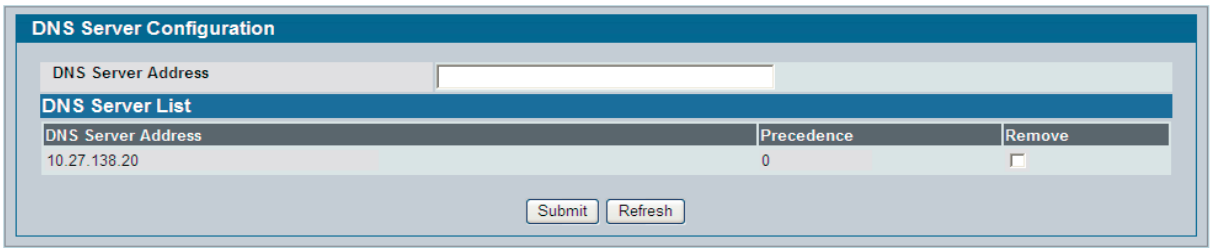


図 3-93　DNS Server Configuration 画面

本画面には次の項目があります。

項目	説明
DNS Server Address	新しい DNS サーバをリストに追加するためには、DNS サーバの IPv4 または IPv6 アドレスを入力します。
Precedence	最初にどのサーバに接続するかを決定するサーバの優先度を表示します。より低い数がより高い優先度があることを示します。

DNS サーバの新規作成

新しい DNS サーバを作成するために、「DNS Server Address」に標準の IPv4 か IPv6 の形式で IP アドレスを入力し、「Submit」ボタンをクリックします。サーバは下のリストに表示されます。優先度は作成された順番に設定されます。

優先度設定

優先度を変更するためには、「Remove」ボックスをクリックして、「Submit」ボタンをクリックすることでサーバを削除し、希望する順番でサーバを追加します。

DNS ホスト名の IP マッピング設定

ネットワーク上のホストに対して DNS ホスト名を設定します。ホスト名はネットワークにおける IPv4 か IPv6 アドレスに関連付けられており、アドレスはスタティックに特定のホストに割り当てられています。

LAN タブ > Administration > DNS Client > HostName IP Mapping の順にメニューをクリックし、以下の画面を表示します。

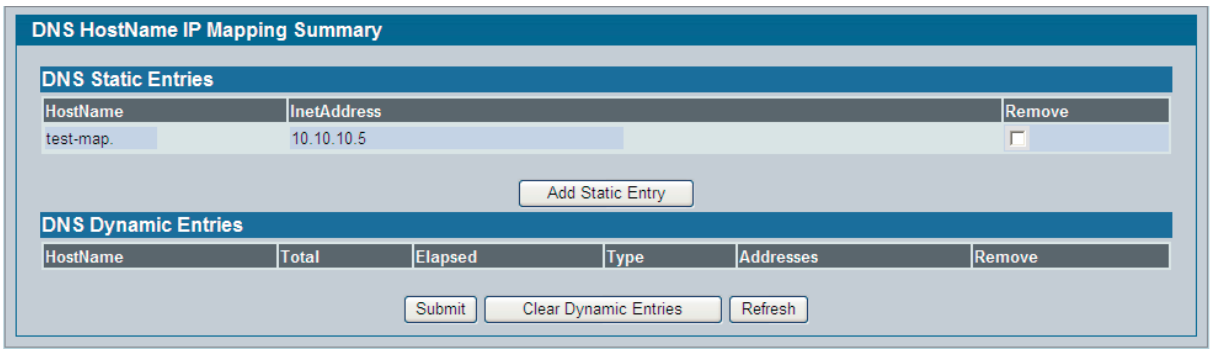


図 3-94　DNS Host Name Mapping Configuration 画面

「DNS Static Entries」セクションには次の項目があります。

項目	説明
Host Name	スタティックエントリのホスト名。
Inet Address	スタティックエントリの IP4 または IPv6 アドレス。
Remove	「Host Name IP Mapping」リストからホスト名の IP マッピングを削除します。

「Add Static Entry」をクリックして、「Host Name IP Mapping Configuration」画面を表示し、「Host Name IP Mapping」エントリを設定します。

「DNS Dynamic Entries」セクションには次の項目があります。

項目	説明
Host Name	ダイナミックエントリのホスト名。
Total	ダイナミックエントリの合計時間。
Elapsed	ダイナミックエントリの経過時間。
Type	ダイナミックエントリのタイプ。
Addresses	ダイナミックエントリの IP4 または IPv6 アドレス。
Remove	「Host Name IP Mapping」リストからエントリを削除します。

「Submit」ボタンをクリックし、新しい設定をスイッチに適用します。変更は直ちに反映されます。「Save」が実行されないと、これらの変更は再起動後に保持されません。

エントリの参照

設定ホスト名の IP マッピングエントリを参照するためには、「Back」ボタンをクリックしてキャンセルを行い、「HostName IP Mapping」画面を表示します。

エントリの削除

「Clear Dynamic Entries」ボタンをクリックすると、すべての「Host Name IP Mapping」エントリが削除されます。確認のプロンプトが表示されます。ボタンをクリックして、削除を確認し、「Host Name IP Mapping」のダイナミックエントリをクリアします。

「Refresh」ボタンをクリックすると、スイッチにおける現在のデータの多くを更新します。

ISDP 情報の設定と参照

Industry Standard Discovery Protocol（ISDP）は、Cisco Discovery Protocol（CDP）が動作する Cisco 社製デバイスと相互通信をするプロプライエタリなレイヤ 2 のネットワークプロトコルです。ISDP は、隣接しているデバイス間で情報を共有するために使用されます。D-Link ソフトウェアは、CDP プロトコルに参加して、他の CDP をサポートするデバイスと相互に検出を行うことができます。

以下の機能があります。

- グローバル設定
- キャッシュテーブルの参照
- インタフェース設定
- 統計情報

グローバル設定

スイッチに管理モードなどの ISDP 設定を行います。

LAN タブ > Administration > ISDP > 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。

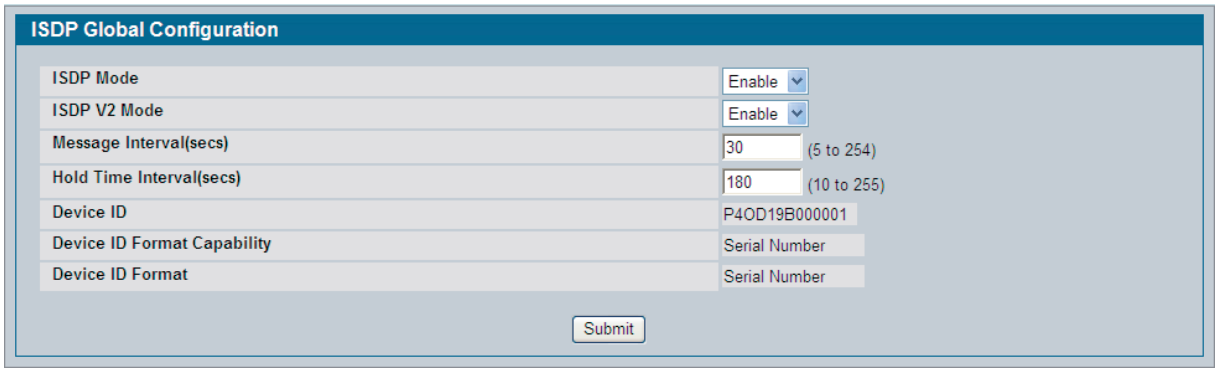


図 3-95　ISDP Global Configuration 画面

本画面には次の項目があります。

項目	説明
ISDP Mode	スイッチにおける ISDP を有効または無効にします。
ISDP V2 Mode	スイッチにおける ISDP V2 を有効または無効にします。
Message Interval (secs)	ISDP 送信間隔（5-254）を指定します。初期値は 30（秒）です。
Hold Time Interval (secs)	受信デバイスはこの期間、ISDP メッセージを維持します。範囲は 10-255 です。初期値は 180 です。
Device ID	本デバイスが通知したデバイス番号。この Device ID のフォーマットは Device ID フォーマットオブジェクトの値によって記述されます。
Device ID Format Capability	デバイスの Device ID フォーマットのケイパビリティを表示します。 • Serial Number - デバイスが Device ID にフォーマットとしてシリアル番号を使用することを示します。 • Mac Address - デバイスが Device ID にフォーマットとしてレイヤ 2 MAC アドレスを使用することを示します。 • Other - デバイスが Device ID にフォーマットとしてプラットフォーム指定のフォーマットを使用することを示します。
Device ID Format	デバイスの Device ID フォーマットを示します。 • Serial Number - 値がデバイスのシリアル番号を含む ASCII 文字列の形式であることを示します。 • Mac Address - 値がレイヤ 2 MAC アドレスの形式であることを示します。 • Other - 値がデバイスを識別する情報を含むプラットフォーム指定の ASCII 文字列の形式であることを示します。例えば、ASCII 文字列にはシステム名に追加、または最初に付加された Serial Number が含まれます。

キャッシュテーブルの参照

スイッチが ISDP を通して検出した他のデバイスに関する情報を参照することができます。

LAN タブ > Monitoring > ISDP > Cache 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。

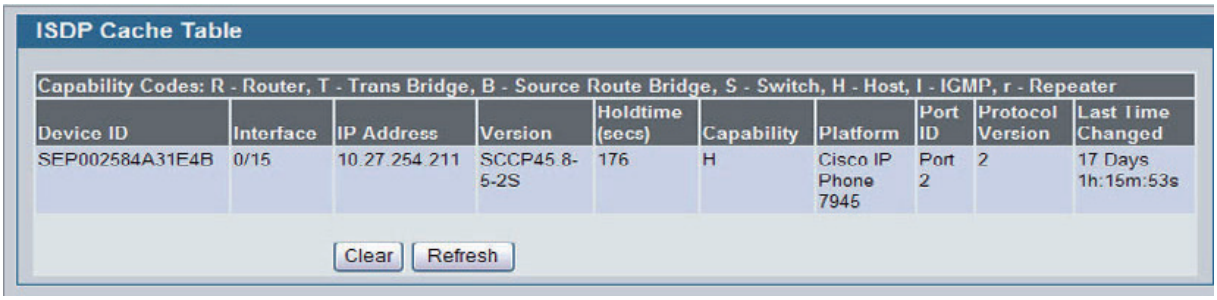


図 3-96　ISDP Cache Table 画面

本画面には次の項目があります。

項目	説明
Device ID	最新の ISDP メッセージでレポートされる Device ID を持つ文字列を表示します。
Interface	この Neighbor が割り当てられているインタフェースを表示します。
IP Address	最も最近受信した ISDP メッセージの Address TLV 内にレポートされる（最初の）ネットワークレイヤアドレス。
Version	Neighbor のバージョンの文字列を表示します。
Holdtime (secs)	Neighbor の ISDP 保持時間を表示します。
Capability	Neighbor の ISDP 機能のケイパビリティを表示します。
Platform	Neighbor の ISDP ハードウェアプラットフォームを表示します。
Port ID	Neighbor の ISDP ポート番号を表示します。
Protocol Version	Neighbor の ISDP のプロトコルバージョンを表示します。
Last Time Changed	エントリが最後に変更された時間を表示します。

インタフェース設定

スイッチに管理モードなどの ISDP 設定を行うことができます。

LAN タブ > Administration > ISDP > Interface 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。

注意　ISDP がインタフェースで有効な場合に ISDP パケットを送信するためには、各インタフェースに ISDP をグローバルに有効にする必要があります。ISDP が以下の画面で無効にされると、インタフェースモードが設定されていてもインタフェースは ISDP パケットを送信しません。

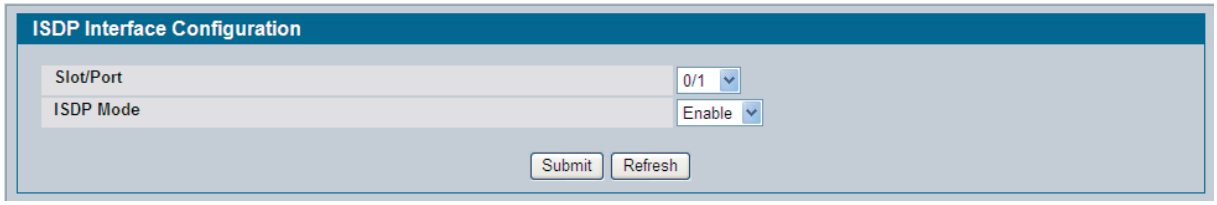


図 3-97　ISDP Interface Configuration 画面

本画面には次の項目があります。

項目	説明
Slot/Port	設定するインタフェースを選択します。
ISDP Mode	スイッチにおける ISDP を有効または無効にします。

統計情報

スイッチが ISDP を通して検出した他のデバイスに関する情報を参照します。

LAN タブ > Monitoring > ISDP > 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。

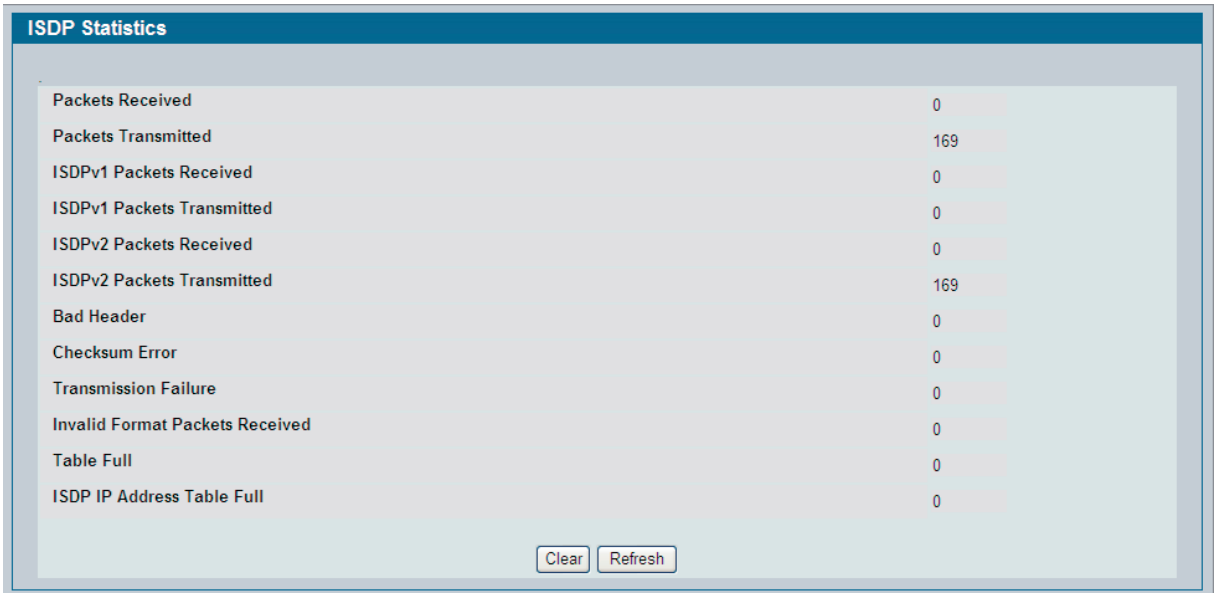


図 3-98　ISDP Statistics 画面

本画面には次の項目があります。

項目	説明
Packets Received	受信したすべての ISDP の protocol data units（PDU）の数を表示します。
Packets Transmitted	送信したすべての ISDP PDU の数を表示します。
ISDPv1 Packets Received	受信した v1 ISDP PDU の数を表示します。
ISDPv1 Packets Transmitted	送信した v1 ISDP PDU の数を表示します。
ISDPv2 Packets Received	受信した v2 ISDP PDU の数を表示します。
ISDPv2 Packets Transmitted	送信した v2 ISDP PDU の数を表示します。
Bad Header	不正なヘッダと共に受信した ISDP PDU の数を表示します。
Checksum Error	チェックサムエラーと共に受信した ISDP PDU の数を表示します。
Transmission Failure	ISDP PDU 送信エラーの数を表示します。
Invalid Format Packets Received	不正な形式で受信した ISDP PDU の数を表示します。
Table Full	システムが ISDP テーブルにエントリの追加を試みたが、テーブルがいっぱいであったために失敗した回数を表示します。
ISDP IP Address Table Full	システムが「ISDP IP Address」テーブルにエントリの追加を試みたが、テーブルがいっぱいであったために失敗した回数を表示します。

第 4 章　L2 機能の設定

設定項目	説明	参照ページ
DHCP Snooping の設定	DHCP Snooping 機能を設定します。	107 ページ
VLAN の管理	VLAN を設定します。	116 ページ
保護ポートの設定	保護ポートグループを設定します。	120 ページ
プロトコルベースの VLAN の管理	プロトコルベースの VLAN を設定します。	121 ページ
IP サブネットベースの VLAN の管理	IP サブネットを VLAN に割り当てます。	123 ページ
MAC ベース VLAN の管理	MAC エントリを VLAN に割り当てます。	124 ページ
音声 VLAN の設定	音声 VLAN 機能を使用して音声トラフィックを制御します。	125 ページ
MAC フィルタの作成	MAC アドレスと VLAN、および送信元ポートと宛先ポートのセットを関連付けて、MAC アドレスを制御します。	126 ページ
GARP の設定	GARP 設定を行います。	128 ページ
ダイナミックな ARP 検査の設定	ダイナミックな ARP 検査の設定を行い、無効で悪意がある ARP パケットを拒否します。	130 ページ
IGMP Snooping の設定	IGMP Snooping 機能の設定を行います。	134 ページ
IGMP Snooping クエリアの設定	ネットワーク、VLAN ごとの IGMP Snooping クエリアに関する情報を設定、および表示します。	139 ページ
MLD Snooping の設定	MLD Snooping 機能の設定を行います。	142 ページ
MLD Snooping クエリアの設定	ネットワーク、VLAN ごとの MLD Snooping クエリアに関する情報を設定、および表示します。	147 ページ
ポートチャンネルの作成（トランキング）	スタティックな LAG を設定します。	150 ページ
マルチキャストフォワーディングデータベース情報	マルチキャストフォワーディングデータベース情報を参照します。	152 ページ
スパニングツリープロトコルの設定	スイッチに STP を設定します。	155 ページ
ポートセキュリティの設定	ポートベースでセキュリティを設定します。	163 ページ
LLDP の管理	LLDP の設定を行います。	167 ページ

DHCP Snooping の設定

DHCP Snooping は、DHCP クライアントと DHCP サーバの間の DHCP メッセージを監視して有害な DHCP メッセージをフィルタし、認可されているとする「MAC アドレス、IP アドレス、VLAN ID、ポート」タプルのバインディングデータベースを構築するセキュリティ機能です。DHCP Snooping をグローバルに、および特定の VLAN での有効化、また、VLAN ポートをトラストまたはアントラストに設定できます。トラストポートを通じて DHCP サーバに到達する必要があります。DHCP Snooping は以下のセキュリティルールを実行します。

- DHCP サーバからの DHCP パケット（DHCPOFFER、DHCPACK、DHCPNAK、DHCPRELEASEQUERY）は、アントラストポートに受信されると廃棄されます。
- DHCPRELEASE および DHCPDECLINE メッセージは、Snooping データベース内の MAC アドレスに行く予定であると破棄されますが、Snooping データベース内の関連する IP アドレスは、メッセージを受信したインタフェースと異なります。
- アントラストインタフェースでは、スイッチは送信元 MAC アドレスがクライアントのハードウェアアドレスに一致しない DHCP パケットを廃棄します。

本機能は設定可能なオプションです。ハードウェアは DHCP Snooping が有効なポートに到来するすべての DHCP パケットを識別します。(a) DHCP Snooping がグローバルに有効な場合、(b) ポートが DHCP Snooping が有効な VLAN のメンバである場合に、DHCP Snooping はポートで有効にされます。アントラストポートでは、ハードウェアは CPU に到来するすべての DHCP パケットをトラップします。トラストポートでは、ハードウェアは、DHCP Snooping がバインディングを学習できるように、クライアントメッセージを送信して CPU にサーバメッセージをコピーします。

グローバルな DHCP Snooping の設定

DHCP Snooping 機能をグローバルに有効または無効にします。

LAN タブ > L2 Features > DHCP Snooping > 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。

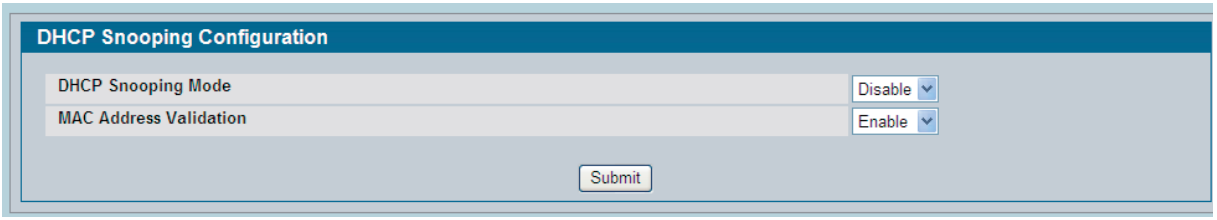


図 4-1　DHCP Snooping Configuration 画面

本画面には次の項目があります。

項目	説明
DHCP Snooping Mode	DHCP Snooping 機能を有効、または無効にします。初期値は「Disable」(無効) です。
MAC Address Validation	DHCP Snooping のために送信側 MAC アドレスの検証を有効、または無効にします。初期値は「Enable」です。

「Submit」ボタンをクリックし、新しい設定をスイッチに適用します。「Save」が実行されないと、これらの変更は再起動後に保持されません。

DHCP Snooping の VLAN 設定

DHCP Snooping アプリケーションは、ハードウェアにサーバメッセージが送信されるためサーバメッセージを送信しません。

DHCP Snooping は経路制御のない VLAN が受信した有効な DHCP クライアントメッセージを送信します。VLAN のすべてのトラストインタフェースにメッセージを転送します。

DHCP Snooping は、中継する VLAN とルーティングする VLAN に設定されます。DHCP パケットをルーティング VLAN で受信すると、DHCP Snooping アプリケーションは、フィルタリングルールを適用し、バインディングデータベースを更新します。クライアントメッセージがフィルタリングルールを通過すると、メッセージはソフトウェアフォワーディングパスにおかれます。そして、DHCP リレーエージェント、ローカルの DHCP サーバによって処理されるか、または IP パケットとして転送されます。

DHCP Snooping は初期値ではグローバルにすべての VLAN で無効です。ポートは初期値でアントラストポートです。

LAN タブ > L2 Features > DHCP Snooping > VLAN 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。

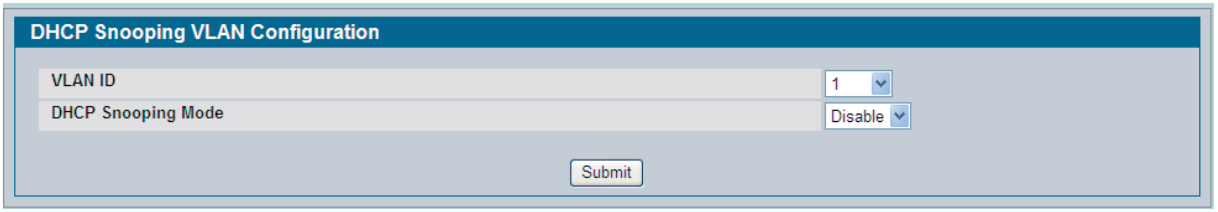


図 4-2　DHCP Snooping VLAN Configuration 画面

本画面には次の項目があります。

項目	説明
VLAN ID	DHCP Snooping アプリケーションに関する情報を表示または設定する VLAN を選択します。
DHCP Snooping Mode	選択された VLAN に関する DHCP Snooping 機能を有効または無効にします。初期値は「Disable」(無効) です。

「Submit」ボタンをクリックし、新しい設定をスイッチに適用します。「Save」が実行されないと、これらの変更は再起動後に保持されません。

DHCP Snooping のインタフェース設定

ハードウェアレートはアントラストインタフェースインタフェースから CPU に送信される DHCP パケットを 15 パケット / 秒に制限します。トラストインタフェースにおけるハードウェアレートに制限はありません。

DHCP Snooping が有効な場合に DHCP パケットが DoS 攻撃に使用されることを防止するために、Snooping アプリケーションはアントラストインタフェースにレート制限を行います。DHCP Snooping は個別に各インタフェースの受信レートを監視します。受信レートが設定した制限を超えていると、DHCP Snooping はインタフェースをダウンします。そのポートでさらに動作するようにするためには、本インタフェースに「no shutdown」の設定を行う必要があります。レートとバースト期間の両方を設定します。

DHCP Snooping アプリケーションは入力の DHCP メッセージを処理します。アプリケーションは、DHCPRELEASE と DHCPDECLINE メッセージについては、受信インタフェースおよび VLAN を、バインディングデータベース内のクライアントのインタフェースおよび VLAN と比較します。インタフェースが一致しない場合、アプリケーションはイベントをログに出力し、メッセージを破棄します。有効なクライアントメッセージに対して、DHCP Snooping は DHCP クライアントのハードウェアアドレスを送信元の MAC アドレスと比較します。一致しないと、DHCP Snooping はログに出力し、パケットを破棄します。以下の画面に示す画面または「no ip dhcp snooping verify mac-address」コマンドを使用することで本機能を無効にすることができます。DHCP Snooping は VLAN 内の有効なクライアントメッセージとトラストメンバを送信します。DHCP リレー、そして / または、DHCP サーバが DHCP Snooping に同時に存在すると、さらに処理するために DHCP リレー、そして / または、DHCP サーバに DHCP クライアントメッセージを送信します。

LAN タブ > L2 Features > DHCP Snooping > Interface 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。

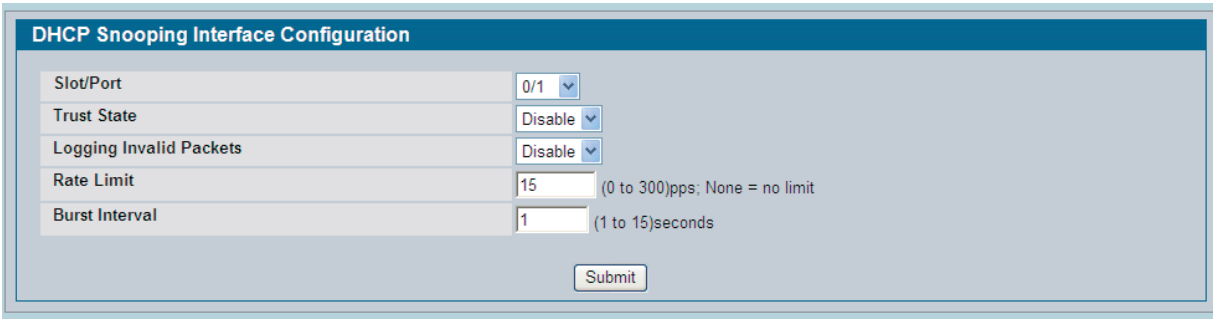


図 4-3　DHCP Snooping Interface Configuration 画面

本画面には次の項目があります。

項目	説明
Slot/Port	データを表示または設定するインタフェースを選択します。
Trust State	有効な場合、DHCP Snooping アプリケーションは、ポートが信頼されたものと見なします。初期値は「Disable」（無効）です。
Logging Invalid Packets	有効な場合、DHCP Snooping アプリケーションは、このインタフェースにおける不正なパケットをログに出力します。初期値は「Disable」（無効）です。
Rate Limit	DHCP Snooping の目的のためにレート限界値（0-300）を指定します。DHCP パケットの入力レートが連続して「Burst Interval」（バースト間隔）このオブジェクトの値を超えていると、ポートはシャットダウンされます。この値が「None」の場合、制限はありません。初期値は 15（パケット / 秒）です。
Burst Interval	このインタフェースでレート制限するためにバースト間隔（1-15）を指定します。「None」を指定すると、バースト間隔は意味を持たないため、「N/A」と表示されます。初期値は 1（秒）です。

「Submit」ボタンをクリックし、新しい設定をスイッチに適用します。「Save」が実行されないと、これらの変更は再起動後に保持されません。

DHCP Snooping バインディング設定

DHCP Snooping アプリケーションは DHCP メッセージを使用してバインディングデータベースの構築と保持を行います。バインディングデータベースにはノントラストポート上のクライアントへのデータだけがあります。DHCP Snooping は DHCP DISCOVER と REQUEST メッセージから一時的なバインディングを作成します。一時的なバインディングはポート（DHCP クライアントメッセージを受信するポート）とクライアントを結びつけます。DHCP Snooping がトラストポートにおいて DHCP ACK メッセージからクライアントの IP アドレスを学習する場合には、一時的なバインディングは終了しています。DHCP Snooping は DECLINE、RELEASE、および NACK メッセージに応じてバインディングを削除します。DHCP Snooping アプリケーションは、トラストポートに受信した DHCP Inform メッセージへの応答として ACK メッセージを無視します。また、バインディングデータベースにスタティックなバインドを入力することができます。

ユーザ設定によって、DHCP バインディングデータベースは設定された外部サーバまたはローカルなフラッシュに保持されます。チェックサムは、リモートに設定したサーバに保存されるテキストファイル内に行ごとに置かれます。リロード時に、スイッチは、設定したバインディングを参照し、DHCP Snooping データベースを構築します。スイッチが起動して計算したチェックサムが、保存されているチェックサムに等しいと、スイッチはバインディングファイルからエントリを読み、バインディングデータベースを設定します。

IP Source Guard（IPSG）、そして / または、DAI が有効にされると、外部で設定されたサーバへのチェックサムの失敗、または接続問題によりスイッチはバインディングを解放してホストのデータ損失を引き起こします。スイッチが新しいバインディングを学習するか、またはすぐにバインディングを失う場合、スイッチはデータベースのエントリを直ちに更新します。さらに、スイッチはバインディングファイル内のエントリを更新します。ファイルが更新される頻度は設定可能な遅延に基づいており、更新はバッチ処理されます。

Snooping データベースエントリの絶対リースタイムの期限が切れると、そのエントリは削除されます。再起動後に矛盾がないようにシステム時間に注意する必要があります。そうでないと、Snooping エントリは適切に期限を終了しません。スイッチの起動中にホストが DHCP リリースを送信する場合にスイッチが DHCP の検出またはリクエストの受信を行うと、クライアントのバインディングは、以下の図に示すように、一時的なバインディングになります。

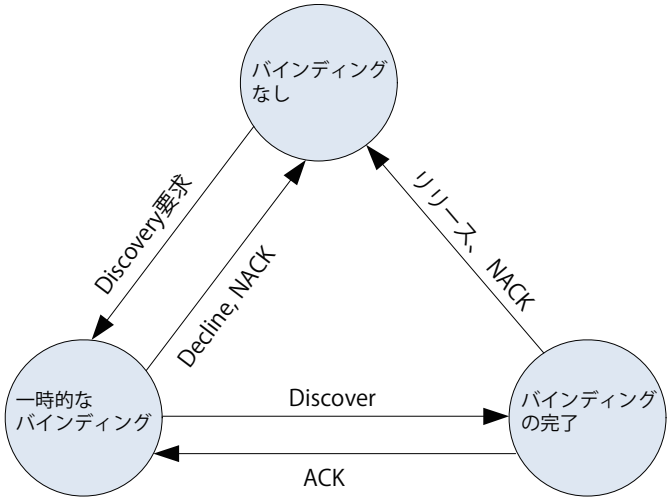


図 4-4　クライアントバインディングのステート

LAN タブ > L2 Features > DHCP Snooping > Binding 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。

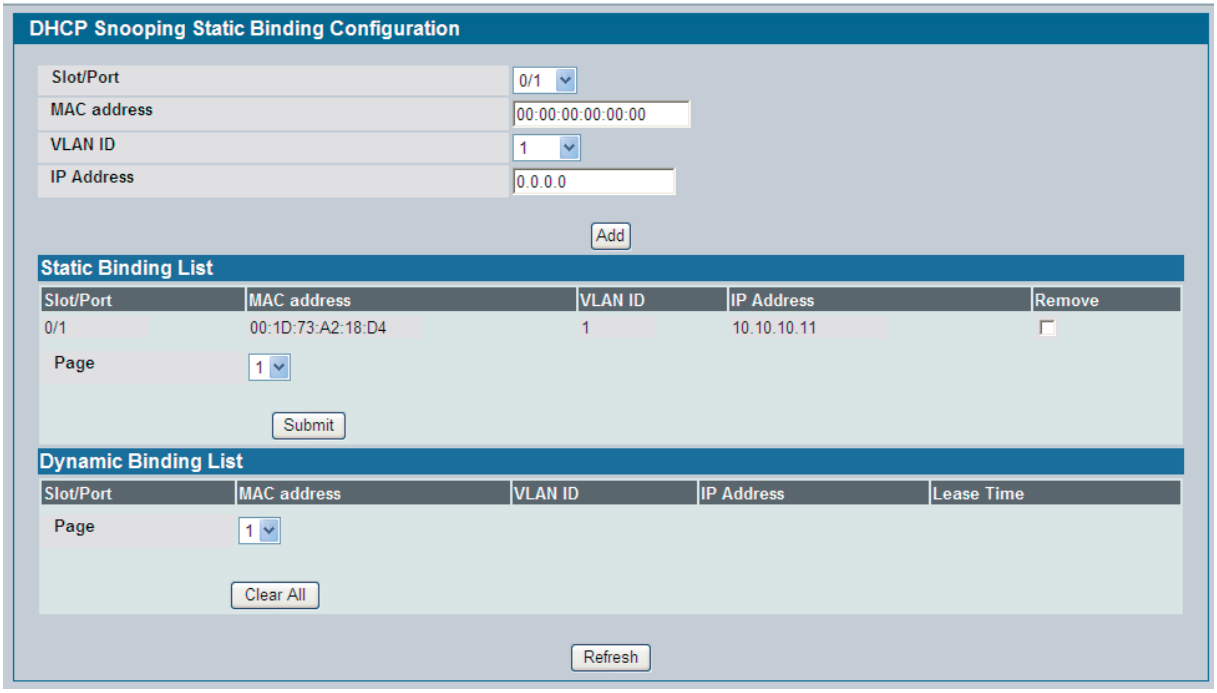


図 4-5　DHCP Snooping Static Binding Configuration 画面

本画面には次の項目があります。

項目	説明
Slot/Port	DHCP Snooping データベースにバインディングを追加するために、インタフェースを選択します。
MAC address	バンディングに対して MAC アドレスを指定して追加します。これはバインディングデータベースへのキーです。
VLAN ID	バインディングのリストから VLAN を選択します。範囲は 1-3965 です。
IP Address	バインディングルールに有効な IP アドレスを指定します。
Static Binding List セクション : すべての DHCP Snooping のスタティックなバインディングエントリをページごとに表示します。	
Slot/Port	インタフェースを表示します。
MAC address	MAC アドレスを表示します。
VLAN ID	VLAN ID を表示します。
IP Address	IP アドレスを表示します。
Remove	これを選択して、特定のバインディングエントリを削除します。
Page	スタティックなバインディングエントリが占めるページ数を示します。リストからページ番号を選択してエントリを表示します。
Dynamic Binding List セクション : すべての DHCP Snooping のダイナミックなバインディングエントリをページごとに表示します。	
Slot/Port	インタフェースを表示します。
MAC address	MAC アドレスを表示します。
VLAN ID	VLAN ID を表示します。
IP Address	IP アドレスを表示します。
Lease Time	ダイナミックエントリのリースタイムの残りを表示します。
Page	ダイナミックバインディングエントリが占めるページ数を示します。リストからページ番号を選択してエントリを表示します。

「Submit」ボタンをクリックし、新しい設定をスイッチに適用します。「Save」が実行されないと、これらの変更は再起動後に保持されません。「Refresh」ボタンをクリックすると、スイッチを最新のデータで更新します。

エントリの追加

「Add」ボタンをクリックして、DHCP Snooping バインディングエントリをデータベースに追加します。

エントリの削除

「Clear All」ボタンをクリックして、すべての DHCP Snooping バインディングエントリを削除します。

DHCP Snooping 統計情報

DHCP Snooping インタフェースの統計情報を表示します。

LAN タブ > Monitoring > DHCP Snooping > 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。

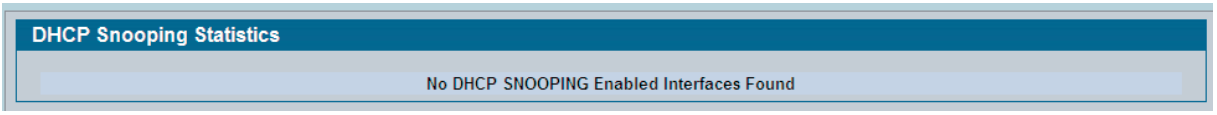


図 4-6　DHCP Snooping Statistics 画面

本画面には次の項目があります。

項目	説明
Slot/Port	統計情報を表示するアントラストで Snooping が有効なインタフェースを選択します。
MAC Verify Failures	DHCP Snooping バインディングエントリへの一致が検出されないために、DHCP Snooping に破棄されたパケット数。
Client Ifc Mismatch	送信元 MAC アドレスとクライアントのハードウェアアドレスの検証に基づいて破棄された DHCP メッセージの数。
DHCP Server Msgs Received	アントラストポートで破棄されたサーバメッセージの数。

インタフェース統計情報のクリア

「Clear Stats」ボタンをクリックして、すべてのインタフェース統計情報をクリアします。

DHCP L2 リレーの設定

同じ IP サブネットに DHCP クライアントとサーバがある場合、それらは、IP アドレスのリクエストと応答を交換するために直接接続することができます。しかし、各サブネットに DHCP サーバを持つことは、高価であり、現実的ではありません。その代わりとして、ネットワークインフラストラクチャデバイスを異なるサブネットにある DHCP クライアントとサーバ間のパケットのリレーが使用できます。一般に、そのようなデバイス（レイヤ 3 リレーエージェント）は、クライアントとサーバサブネットの両方に IP インタフェースを持って、それらの間で送信できるルータです。しかし、レイヤ 2 のネットワークには、クライアントと L3 リレーエージェント /DHCP サーバの間に 1 つ以上のインフラストラクチャデバイス（例 : スイッチ）があります。この例では、L3 リレーエージェントによって必要とされるクライアントのデバイス情報のいくつかが表示されないかもしれません。この場合、L2 リレーエージェントを使用して、L3 リレーエージェントと DHCP サーバが、アドレス、コンフィグレーションにおける役割と割り当てを実行する必要があるという情報を追加します。

クライアントからの DHCP リクエストをリレーする前に、スイッチは Circuit ID と Remote ID を追加することができます。これらは、クライアントに接続する circuit とポート番号に関する情報を提供します。この情報は DHCP Option 82 パケット内のサブオプションとして追加されます。RFC 3046 のセクション 3.1、3.1 を参照してください。スイッチは L3 リレーエージェント /DHCP サーバからクライアントまでリレーするパケットからこのオプションを削除します。

これらのサブオプションは DHCP サーバによって使用され、それがクライアントを扱う方法に影響するかもしれません。また、リレーエージェントによって使用されて、ブロードキャストの応答をクライアントの特定の位置に制限するかもしれません。

Switching > DHCP Snooping > DHCP L2 Relay フォルダは以下の画面への接続を提供します。

- Global Configuration（グローバル設定）
- Interface Configuration（インタフェース設定）
- VLAN Configuration（VLAN の設定）
- Interface Statistics（インタフェース統計情報）

Global Configuration（DHCP L2 リレーグローバル設定）

スイッチが DHCP L2 リレーエージェントとして動作することを「Enabled」（有効）/「Disabled」（無効）にします。このサービスを動作させる各ポートでこの機能を有効にする必要があります。「Interface Configuration（インタフェースの設定）」（113 ページ）を参照してください。また、リクエストするクライアントの VLAN が L2 DHCP リレー機能と共に有効にされているサービスプロバイダの VLAN ID に対応する場合にだけ、リクエストのリレー設定をスイッチに行うことができます。「VLAN Configuration（VLAN 設定）」（114 ページ）を参照してください。

LAN タブ > L2 Features > DHCP Snooping > DHCP L2 Relay > 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。

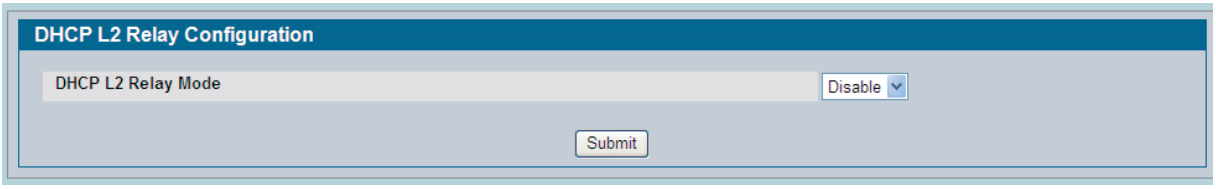


図 4-7　DHCP L2 Relay Configuration 画面

本機能を有効または無効にした場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。

Interface Configuration（インタフェースの設定）

個々のポートに L2 DHCP リレーを有効にします。また、L2 DHCP リレーはスイッチにグローバルに有効とする必要があります。

LAN タブ > L2 Features > DHCP Snooping > DHCP L2 Relay > Interface 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。

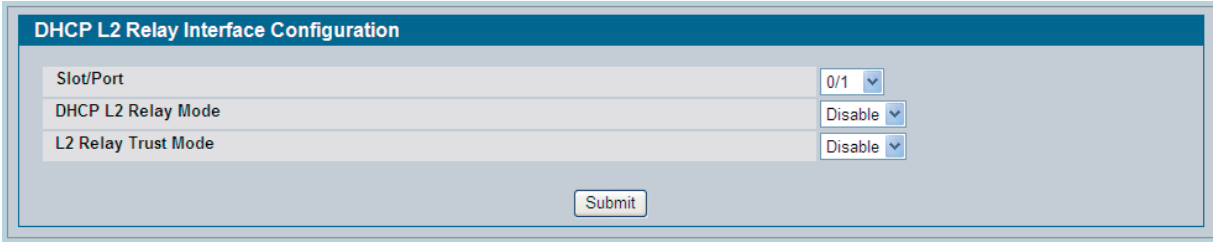


図 4-8　DHCP L2 Relay Interface Configuration 画面

本画面には次の項目があります。

項目	説明
Slot/Port	機能を設定するスロット / ポートを選択します。
DHCP L2 Relay Mode	選択インタフェースの L2 リレーモードを有効、または無効にします。
DHCP L2 Relay Trust Mode	選択インタフェースの L2 リレートラストモードを有効、または無効にします。通常、トラストインタフェースは DHCP インタラクション（例えば、他の L2、L3 リレーエージェントまたはサービス）に参加する他のエージェントまたはサーバに接続します。トラストモードを有効にすると、インタフェースは、いつもオプション 82 情報を含む DHCP パケットの受信するものと考えます。オプション 82 情報が含まれていないと、これらのパケットは破棄されます。一般に、アントラストインタフェースはクライアントに接続します。アントラストインタフェースに到着する DHCP パケットは、オプション 82 を送信することを予想しておらず、破棄されます。

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。

VLAN Configuration（VLAN 設定）

特定の VLAN で L2 DHCP リレーを有効にすることができます。VLAN はサービス VLAN ID（S-VID）によって識別されます。サービスプロバイダは、プロバイダネットワークを複数のリモートサイトにトラバーシングしている間にカスタマのトラフィックを識別するために使用します。スイッチは、スイッチポートのクライアント（カスタマ VLAN ID、または C-VID）の VLAN メンバシップを使用して、対応する S-VID にルックアップを実行します。

S-VID が DHCP L2 リレーに有効であると、次に、パケットを送信することができます。C-VID が DHCP L2 リレーに有効である S-VID に対応していないと、スイッチは DHCP リクエストパケットをリレーしません。

LAN タブ > L2 Features > DHCP Snooping > DHCP L2 Relay > VLAN 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。

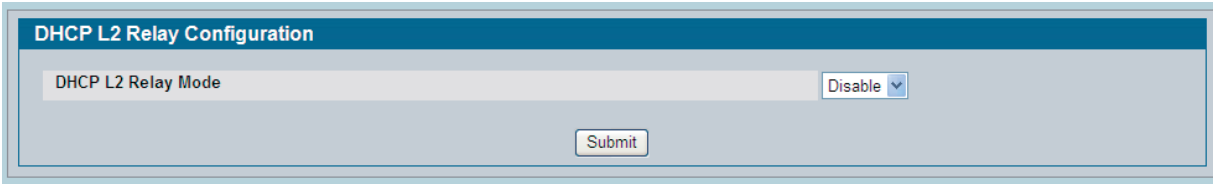


図 4-9　DHCP L2 Relay VLAN Configuration 画面

本画面には次の項目があります。

項目	説明
VLAN ID	VLAN ID を選択します。これは、プロバイダネットワークを通じて DHCP パケットをリレーすることを認可される VLAN を識別する S-VID（サービスプロバイダによって示される）です。
L2 Relay Mode	DHCP L2 リレーサービスのために選択した VLAN を有効または無効にします。
DHCP L2 Relay Circuit-Id	有効である場合、クライアントが DHCP リクエストをスイッチに送信し、クライアントが選択した S-VID に対応する VLAN にあると、スイッチは DHCP リクエストパケットのオプション 82 の Circuit ID サブオプションにクライアントのインタフェース番号を追加します。 有効にするとブロードキャストビットが DHCP パケットに設定される場合にサーバの応答が切り換えられるブロードキャストドメインをスイッチが減少させることができます。このビットが設定されると、サーバは、応答にオプション 82 をエコーバックするために必要とされます。circuit-id フィールドがクライアントインタフェース番号を含んでいるため、L2 リレーエージェントは、VLAN 内のすべてのポートではなくてリクエストしているインタフェースだけに応答を送信することができます。
L2 Relay Remote-Id	文字列を入力すると、クライアントが DHCP のリクエストをスイッチに送信し、クライアントが選択した SVID に対応する VLAN にあると、DHCP リクエストパケットのオプション 82 の Remote-ID sub-option に文字列を追加します。サーバはパラメータ指定に本サブオプションを使用することができます。このオプションの内容はベンダで設定します。

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。

Interface Statistics（インタフェース統計情報）

本画面を使用して、選択したポートに受信した L2 DHCP リレーリクエストにおける統計情報を表示します。

LAN タブ > Monitoring > DHCP Snooping > DHCP L2 Relay > Interface 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。

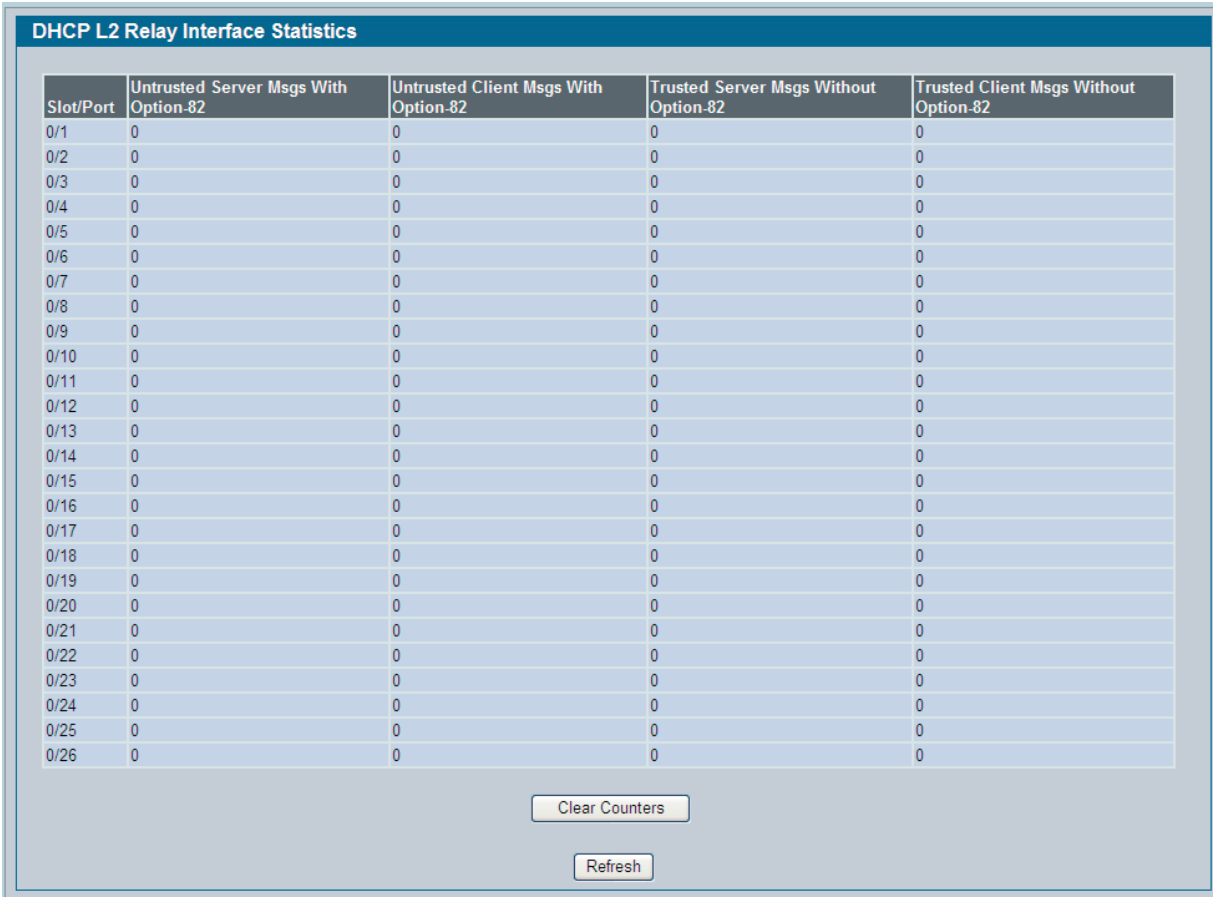


図 4-10　DHCP L2 Relay Interface Statistics 画面

本画面には次の項目があります。

項目	説明
Slot/Port	機能を設定するスロット / ポートを選択します。
Untrusted Server Msgs With Option.82	選択したインタフェースがアントラストモードで設定されていると、オプション 82 データが含まれる DHCP サーバからインタフェースに受信したメッセージ数を表示します。これらのメッセージは破棄されます。
Untrusted Client Msgs With Option.82	選択したインタフェースがアントラストモードで設定されていると、オプション 82 データが含まれる DHCP クライアントからインタフェースに受信したメッセージ数を表示します。これらのメッセージは破棄されます。
Trusted Server Msgs Without Option.82	選択したインタフェースがアントラストモードで設定されていると、オプション 82 データが含まない DHCP サーバからインタフェースに受信したメッセージ数を表示します。これらのメッセージは破棄されます。
Trusted Client Msgs Without Option.82	選択したインタフェースがアントラストモードで設定されていると、オプション 82 データが含まない DHCP クライアントからインタフェースに受信したメッセージ数を表示します。これらのメッセージは破棄されます。

「Refresh」ボタンをクリックし、システムの情報を最新に更新します。

統計情報のクリア

「Clear Counters」ボタンをクリックして、このポートの統計情報を初期値に設定します。「Clear All」をクリックして、すべてのポートの統計情報は初期値に設定します。

VLAN の管理

レイヤ 2 スイッチに Virtual LAN（VLAN）を追加することで、ブリッジおよびルーティングの両方の利点うちのいくつかを提供することができます。ブリッジと同様に VLAN スイッチはレイヤ 2 ヘッダに基づいてトラフィックを送信します。これは処理が速く、ルータのように論理セグメントにネットワークを分割します。これによりマルチキャストトラフィックの、より高い管理および保証を提供します。

VLAN は、エンドステーションとそれらに接続するスイッチポートのセットです。部署またはプロジェクトのメンバなど論理的な分割には多くの理由があるかもしれません。唯一の物理的要件は、接続するエンドステーションとポートが共に同じ VLAN に所属するということです。

ネットワークにおける各 VLAN には関連する VLAN ID があります。これは、VLAN に送信されるパケットのレイヤ 2 ヘッダの IEEE 802.1Q タグにあります。エンドステーションはタグ、またはタグの VLAN 部分を省略するかもしれません。その場合、パケットを受信する最初のスイッチポートは、それを拒否するか、またはデフォルト VLAN ID を使用することでタグを挿入します。特定のポートは 1 つ以上の VLAN に対してトラフィックを処理することもありますが、サポートするのは 1 つのデフォルト VLAN ID のみです。

「VLAN」フォルダには以下の機能へのリンクがあります。

- VLAN の設定
- VLAN ステータス
- VLAN ポート設定
- VLAN ポート概要
- VLAN 設定のリセット

VLAN の設定

VLAN メンバシップテーブルに保存される VLAN グループを定義します。スイッチは 3965 個の VLAN をサポートしています。VLAN 1 は、すべてのポートがメンバであるデフォルト VLAN です。

LAN タブ > L2 Features > VLAN > VLAN 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。

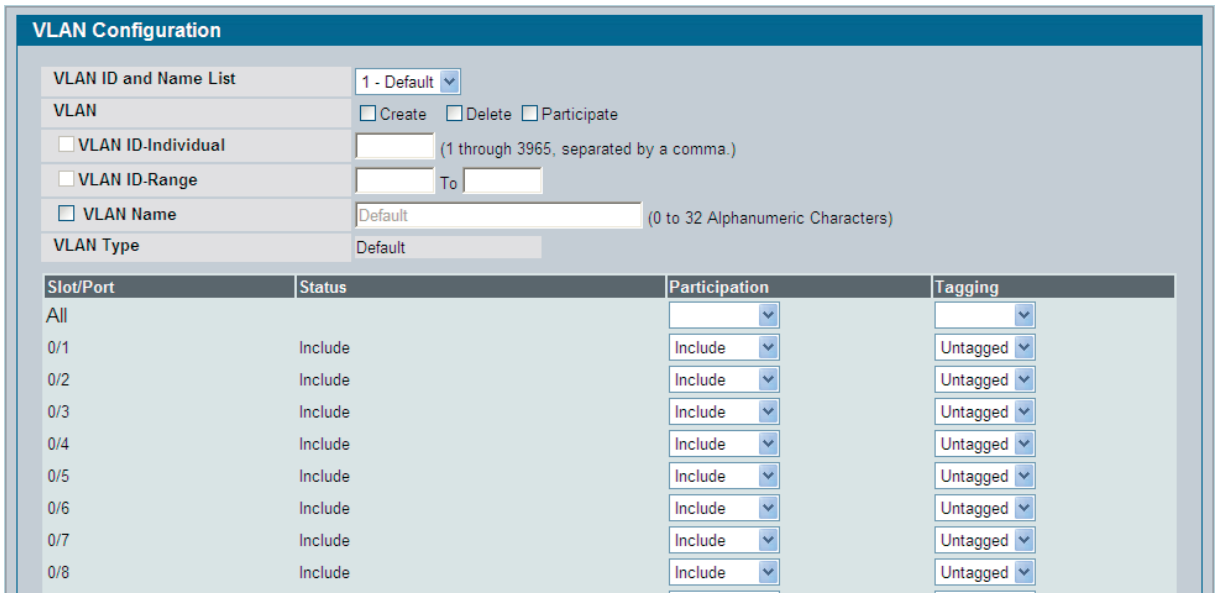


図 4-11　VLAN Configuration 画面

本画面には次の項目があります。

項目	説明
VLAN ID and Name List	既存の VLAN の再設定、または新規に作成します。既存の VLAN の 1 つを選択します。または、「Create」を選択して新しく追加します。
VLAN ID-Individual	新しい VLAN に VLAN 識別子を指定します。新しい VLAN を作成している場合だけ、本欄にデータを入力することができます。VLAN ID の範囲は、1-3965 です。
VLAN ID-Range	新しく作成する VLAN に VLAN 識別子の範囲を指定します。

項目	説明
VLAN Name	VLAN 名を半角英数字 32 文字以内（空白を含む）で設定します。初期値は空白です。VLAN ID1 は常に「default」という名称で、変更することはできません。
VLAN Type	VLAN のタイプを指定します。デフォルト VLAN（VLAN ID=1）のタイプを変更することはできません。VLAN を作成する場合、タイプは「Static」となります。最初に GVRP 登録で作成される VLAN は、「Dynamic」のタイプを持っています。プルダウンメニューを使用して「Static」にタイプを変更します。
Slot/Port	インタフェースを表示します。
Status	ポートに参加パラメータの現在の値を示します。
Participation	ポートがこの VLAN に参加するかどうか指定します。 • Include - ポートを VLAN メンバに含めます。これは、IEEE 802.1Q 標準における fixed 登録にあたります。 • Exclude - ポートは VLAN メンバから除外します。これは、IEEE 802.1Q 標準における forbidden 登録にあたります。 • Autodetect - ポートが GVRP 経由でこの VLAN にダイナミックに登録されることを指定します。GVRP リクエストを受信しないと、ポートは本 VLAN に参加しません。これは、IEEE 802.1Q 標準における normal 登録にあたります。（初期値）
Tagging	VLAN ポートへのタギングを選択します。 • Tagged - この VLAN に送信されるすべてのフレームがタグ付けされます。 • Untagged - この VLAN に送信されるすべてのフレームからタグを削除します。（初期値）

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。

VLAN の削除

VLAN を削除するためには、「VLAN ID」および「Name」欄から VLAN を選択し、「Delete」ボタンをクリックします。デフォルト VLAN は削除できません。

VLAN ステータス

システムに設定した VLAN に関する情報を参照します。

LAN タブ > Monitoring > VLAN Summary > VLAN 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。

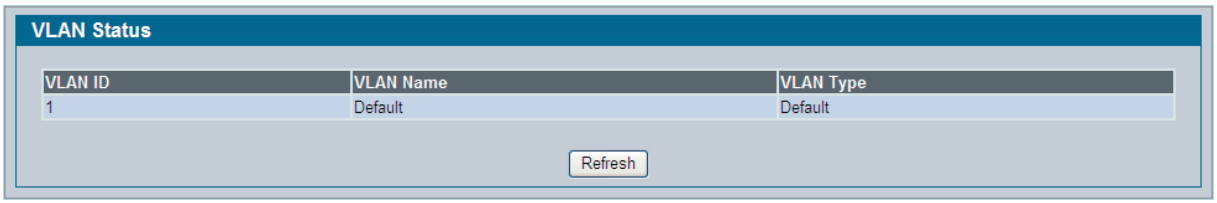


図 4-12　VLAN Status 画面

本画面には次の項目があります。

項目	説明
VLAN ID	VLAN の VLAN 識別子（VID）を表示します。範囲は 1-3965 です。
VLAN Name	VLAN 名。VLAN ID1 は常に「default」です。
VLAN Type	VLAN のタイプを表示します。 • Default - VLAN ID は 1 です。常に存在します。 • Static - ユーザが定義した VLAN。 • Dynamic - GVRP 登録で作成された VLAN。これを「Static」に変更することはできません。また、GVRP によってだけ削除されます。

「Refresh」ボタンをクリックし、システムの情報を最新に更新します。

PVLAN ポート設定

ポートに VLAN を設定します。

LAN タブ > L2 Features > VLAN > Port 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。

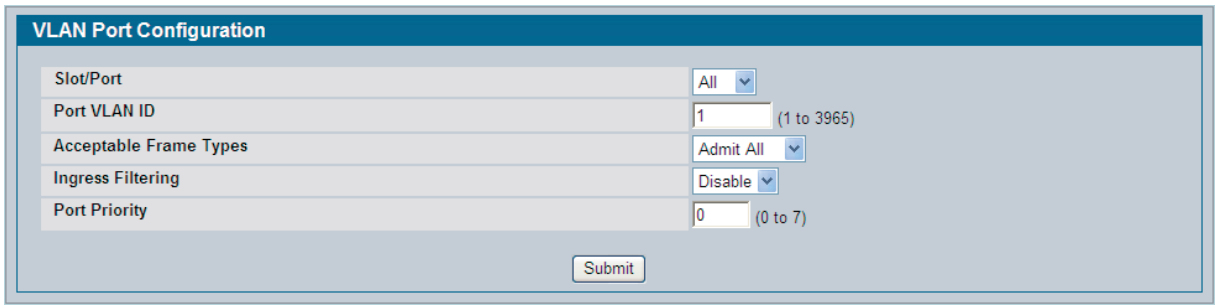


図 4-13　VLAN Port Configuration 画面

本画面には次の項目があります。

項目	説明
Slot/Port	データを表示または設定する物理インタフェースを選択します。「All」を選択すると、すべてのポートに同じ値のパラメータを設定します。
Port VLAN ID	ポートに受信したタグなしまたはプライオリティのタグ付きフレームに割り当てる VLAN ID を指定します。 初期値は 1 です。
Acceptable Frame Types	ポートがタグなしまたはプライオリティのタグ付きフレームを処理する方法を指定します。どちらを選択しても、VLAN タグ付きフレームは、IEEE 802.1Q VLAN 標準に従って転送されます。 • VLAN Only - ポートは、どんな受信するタグなし、プライオリティのタグ付きフレームも破棄します。 • Admit All - ポートに受信したタグなし、プライオリティのタグ付きフレームを受け入れて、このポートの「Port VLAN ID」の値を割り当てます。（初期値）
Ingress Filtering	ポートがタグ付きフレームを処理する方法を指定します。 • Enable - タグ付きフレームは、このポートがタグの VLAN ID によって識別される VLAN のメンバでないと破棄されます。 • Disable - すべてのタグ付きフレームを受け付けます。（初期値）
Port Priority	ポートに到着するタグなしパケットに割り当てられたデフォルト 802.1p プライオリティを指定します。

情報の変更した場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。

VLAN ポートステータスの参照

システムにおけるすべてのポートの VLAN 設定を参照します。

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

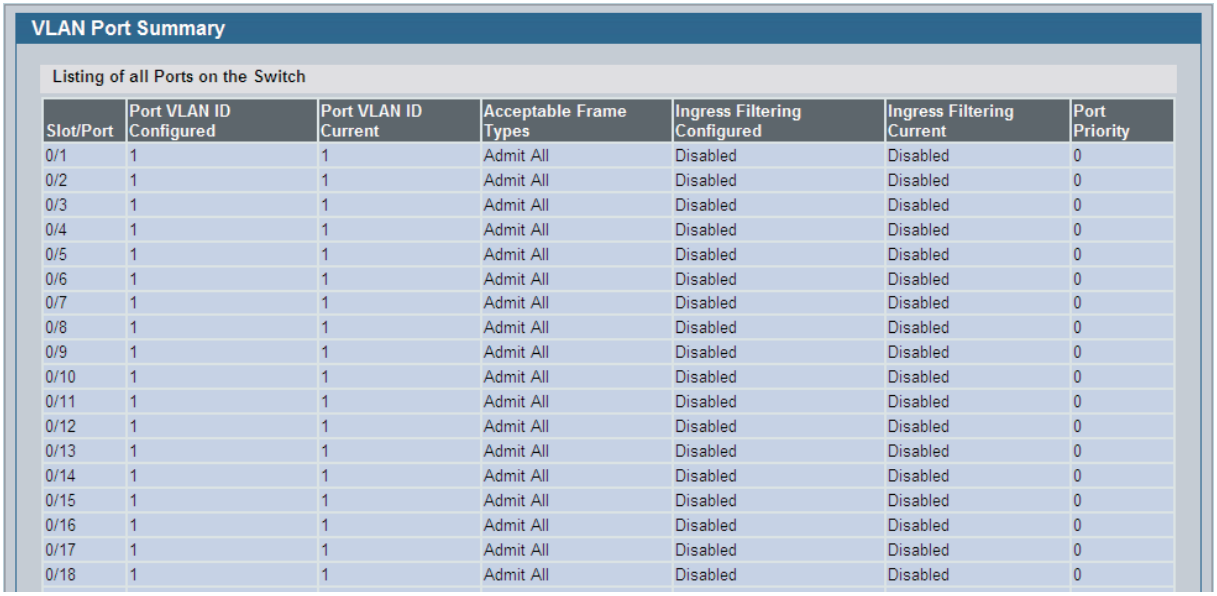


図 4-14　VLAN Port Summary 画面

本画面には次の項目があります。

項目	説明
Slot/Port	残りのデータに関連する物理インタフェースを表示します。
Port VLAN ID Configured	ポートに受信したタグなしまたはプライオリティのタグ付きフレームに割り当てる VLAN ID を表示します。 初期値は 1 です。
Port VLAN ID Current	ポートで使用中の実際の VLAN ID を表示します。ポートが別のモジュールで取得されると、実際の値は設定された VLAN ID と異なる可能性があります。例えば、ポートがポートチャンネルのメンバで、ポートチャンネルが設定した値とは異なるポート VLAN ID を持つと、2 つは異なります。
Acceptable Frame Types	ポートがタグなしまたはプライオリティのタグ付きフレームを処理する方法を表示します。 • VLAN Only - ポートは、受信するどんなタグなし、プライオリティのタグ付きフレームも破棄します。 • Admit All - ポートに受信したタグなし、プライオリティのタグ付きフレームを受け入れて、このポートの「Port VLAN ID」の値を割り当てます。
Ingress Filtering Configured	ポートがタグ付きフレームを処理する方法を表示します。 • Enable - タグ付きフレームは、ポートがタグの VLAN ID によって識別される VLAN のメンバでないと破棄されます。 • Disable - すべてのタグ付きフレームを受け入れます。（初期値）
Ingress Filtering Current	ポートの現在のタグ付きフレーム処理方法を表示します。
Port Priority	ポートに到着するタグなしパケットに割り当てられたデフォルト 802.1p プライオリティを表示します。

「Refresh」ボタンをクリックして、最新の情報を参照します。

VLAN 設定のリセット

すべてのインタフェースにおけるすべての VLAN パラメータを工場出荷時の設定に戻します。

LAN タブ > L2 Features > VLAN > Reset 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。

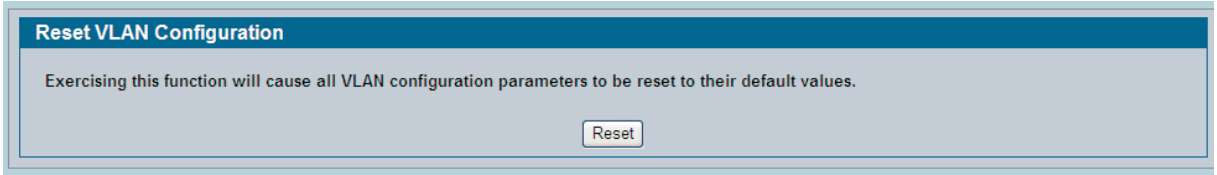


図 4-15　Reset VLAN Configuration 画面

「Reset」ボタンをクリックすると、画面は更新されてリセットの確認ダイアログが表示されます。再度「Reset」ボタンをクリックして、システムのポートに対してデフォルト VLAN 設定をリストアします。

保護ポートの設定

保護ポート機能はレイヤ 2 セキュリティを向上します。設定された保護ポートは、同じ VLAN メンバシップを持っていても、同じグループの他の保護ポートにトラフィックを転送します。しかし、保護ポートは他の保護されたグループと同様に保護されていないポートにもトラフィックを送ることができます。保護されていないポートは、保護されているポートと保護されていないポートの両方にトラフィックを送信することができます。

保護されたポートの設定

3 つまでの保護されたポートグループを作成し、物理ポートをグループに割り当てます。

LAN タブ > L2 Features > Protected Ports > 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。

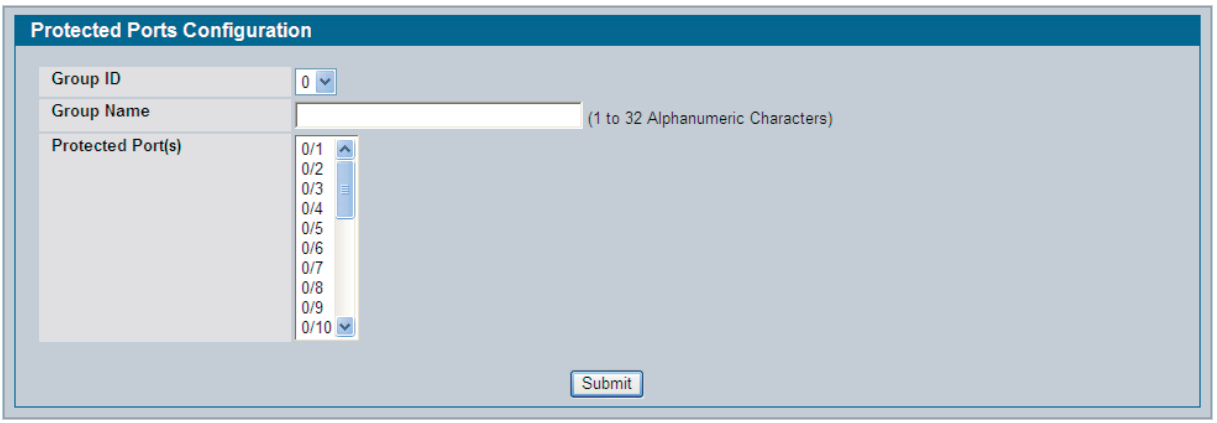


図 4-16　Protected Port Configuration 画面

本画面には次の項目があります。

項目	説明
Group ID	保護ポートを論理グループに結合できます。トラフィックは、異なるグループに所属しながら保護ポート間をフローすることができますが、同じグループ内ではできません。選択ボックスは現在のプラットフォーム用にサポートされているすべての可能な保護ポートの Group ID を表示します。有効範囲はプラットフォームに依存しています。
Group Name	保護ポートグループに関連付けるためにオプション名を割り当てます。この名称は識別の目的のものであり、半角英数字 32 文字以内（空白を含む）で設定します。初期値は空白です。
Protected Port(s)	パラメータを定義するスロット / ポートを選択します。

ポートをグループへの割り当て

1. 「Group ID」からグループ ID を選択します。
2. 「Protected Port(s)」から、ポートを 1 つクリックし、グループに追加します。また、「CTRL」キーを押しながら複数のポートをクリックして、1 つ以上のポートをグループに追加します。
3. 「Submit」ボタンをクリックし、変更をスイッチに適用します。

保護ポートのサマリ

保護されたポートグループとそれらに含まれるポートに関する情報を参照します。

LAN タブ > Monitoring > Protected Ports > 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。

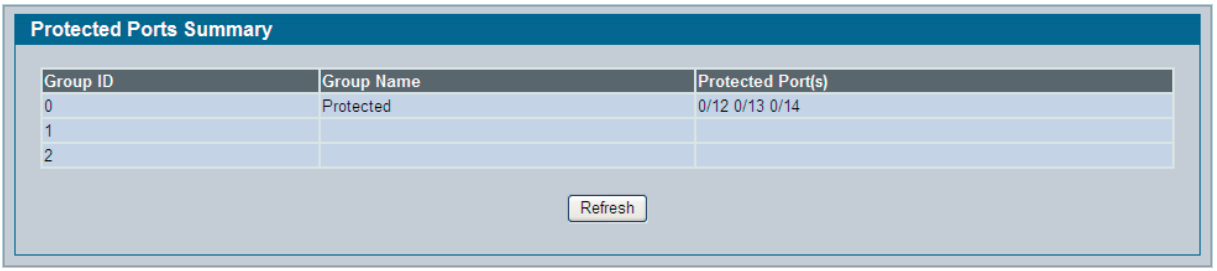


図 4-17　Protected Ports Summary 画面

本画面には次の項目があります。

項目	説明
Group ID	Group0、1、または 2 の保護ポートグループを示します。
Group Name	ユーザ定義の文字列を持つ保護ポートグループを示します。
Protected Port(s)	保護ポートグループのメンバであるスロット / ポートを参照します。

「Refresh」ボタンをクリックして、画面を更新し、最新の情報を参照します。

プロトコルベースの VLAN の管理

プロトコルベースの VLAN では、トラフィックは VLAN に関連するプロトコルに基づいて、指定されたポートを通じてブリッジされます。ユーザ定義のパケットフィルタは、特定のパケットが特定の VLAN に所属するかどうかを決定します。プロトコルベースの VLAN は、ネットワークセグメントが複数のプロトコルを実行しているホストを含む状況で多く使用されます。

タグなしパケットのフィルタリング基準を定義するのにプロトコルベースの VLAN を使用することができます。ポートベース（IEEE 802.1Q）またはプロトコルベース VLAN も設定していないと、初期値では、タグなしパケットは VLAN 1 に割り当てられます。ポートベース VLAN、プロトコルベース VLAN、または両方を定義することによって、この動作を書き換えることができます。タグ付きパケットは、IEEE 802.1Q 標準に従って常に処理されており、プロトコルベースの VLAN には含まれていません。

特定のプロトコルのためにプロトコルベースの VLAN にポートを割り当てると、そのプロトコルのためにそのポートに受信したタグなしフレームは、プロトコルベースの VLAN ID に割り当てられます。他のプロトコルのためにポートに受信したタグなしフレームが Port VLAN ID（PVID）に割り当てられます。それは、「Port VLAN Configuration」画面を使用してポートに明確に割り当てたデフォルト PVID（1）または PVID のどちらかです。

プロトコルベースの VLAN 設定

どのプロトコルが、どの VLAN を通過するかを設定し、次にこれらの設定を使用するポートを有効または無効にします。

グループを作成することによって、プロトコルベースの VLAN を定義します。各グループは、VLAN ID との 1 対 1 関係を持っていて、1 つ以上のプロトコル定義を含むことができます。また、複数のポートを含むこともできます。

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

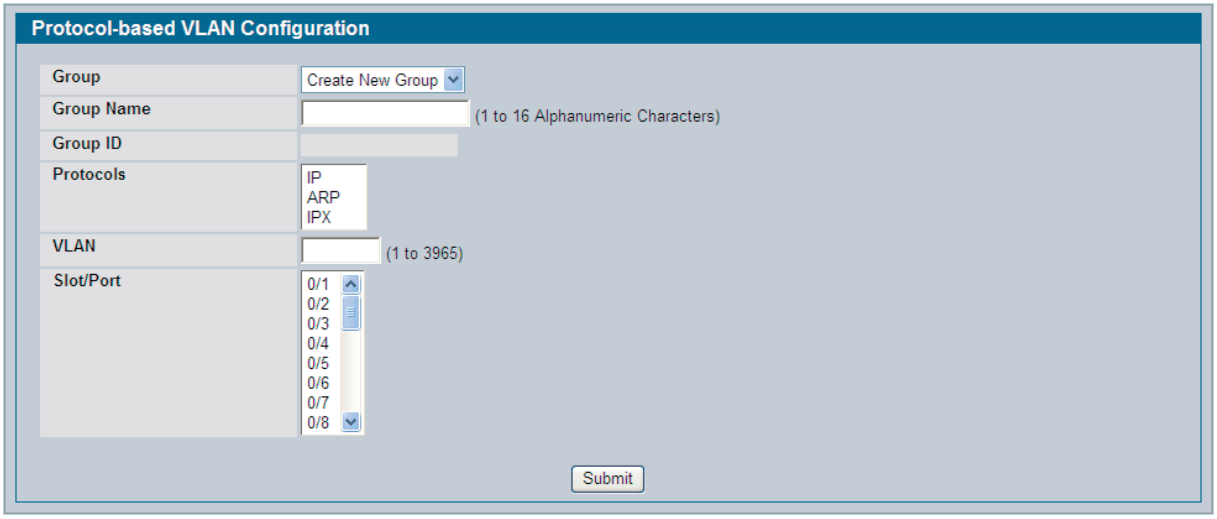


図 4-18　Protocol-based VLAN Configuration 画面

本画面には次の項目があります。

項目	説明
Group	プロトコルグループを作成または編集します。最大 128 個のグループを作成できます。
Group Name	グループを作成する場合には、プロトコルグループ ID に割り当てる名前を入力します。また、既存のグループ名を変更することができます。最大 16 文字まで入力することができます。
Group ID	作成するグループを識別する番号を示しています。グループを作成する場合、自動的に割り当てられます。
Protocols	グループに関連付けする 1 個以上のプロトコルを選択します。「CTRL」を押しながらクリックして複数のプロトコルを選択します。 • IP - データの送信のためにコネクションレス型サービスを提供するネットワーク層のプロトコルです。 • ARP - ダイナミックに MAC（medium access control）アドレスにネットワークレイヤのアドレスをマップする低レベルのプロトコルです。 • IPX - ネットワークにデータを転送するコネクションレス型のデータネットワークレイヤプロトコルです。
VLAN	プロトコルグループに割り当てた VLAN ID（1-3965）を表示します。
Slot/Port	プロトコルグループを追加、または削除するインタフェースを選択します。「CTRL」を押しながらクリックして複数のポートを選択します。

プロトコルベース VLAN グループの作成、変更

プロトコルベースの VLAN グループを作成、または変更するためには、項目を編集し、次に「Submit」ボタンをクリックします。

プロトコルベース VLAN グループの削除

既存のプロトコルベースの VLAN グループを削除するためには、「Group ID」欄からグループを選択し、「Delete Group」ボタンをクリックします。

プロトコルベースの VLAN のサマリ

システムに設定されているプロトコルベースの VLAN グループに関する情報を表示します。

LAN タブ > Monitoring > VLAN Summary > Protocol-based VLAN Port 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。

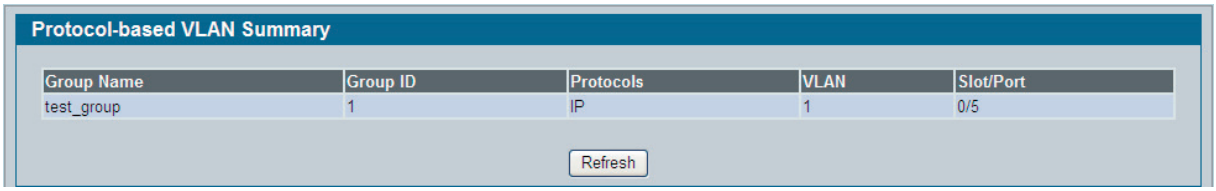


図 4-19　Protocol-based VLAN Summary 画面

本画面には次の項目があります。

項目	説明
Group Name	プロトコルグループに割り当てられているユーザ定義名を表示します。
Group ID	作成するグループを識別する番号を示しています。グループを作成する場合、自動的に割り当てられます。
Protocols	本グループに割り当てられているプロトコルを参照します。以下の項目の 1 つ以上が表示されます。 • IP - データの送信のためにコネクションレス型サービスを提供するネットワーク層のプロトコルです。 • ARP - ダイナミックに MAC（medium access control）アドレスにネットワークレイヤのアドレスをマップする低レベルのプロトコルです。 • IPX - ネットワークにデータを転送するコネクションレス型のデータネットワークレイヤプロトコルです。
VLAN	プロトコルグループに割り当てた VLAN ID を表示します。
Slot/Port	プロトコルグループに参加しているインタフェースを表示します。

「Refresh」ボタンをクリックして、画面を更新し、最新の情報を参照します。

IP サブネットベースの VLAN の管理

パケットがタグなしまたはプライオリティのタグ付きであると、デバイスは一致する IP サブネットの分類とパケットを関連付けます。IP サブネットの分類が行われないと、パケットはデバイスの正常な VLAN 分類ルールを受けます。IP subnet-to-VLAN のマッピングは、IP subnet-to-VLAN テーブルにエントリを設定することで定義されます。エントリは送信元 IP アドレス、ネットワークマスク、および必要な VLAN ID によって指定されます。IP subnet-to-VLAN 設定は、スイッチのすべてのポートを経由して共有されます。

IP サブネット VLAN の設定

IP サブネットを VLAN に割り当てます。

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

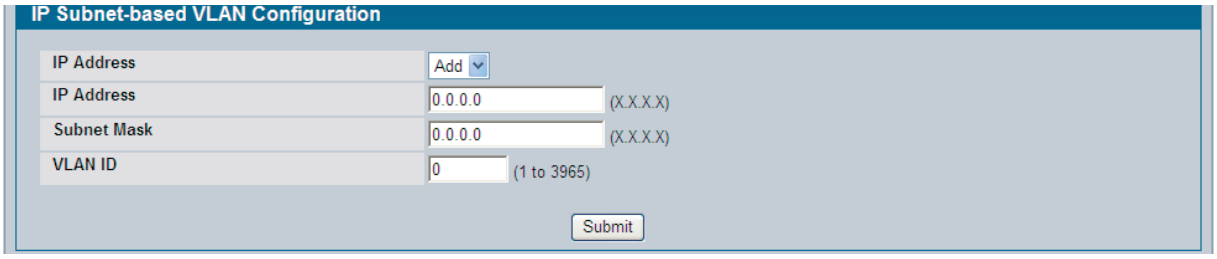


図 4-20　IP Subnet-based VLAN Configuration 画面

本画面には次の項目があります。

項目	説明
IP Address	バインディングを参照または削除する IP-to-VLAN binding の IP アドレスを選択します。または、新しいバインディングを作成するためには「Add」を選択します。
IP Address	パケットの送信元 IP アドレスを指定します。新しい IP がサブネットベースの VLAN を作成する場合のみ、本欄は設定可能です。「.」（ドット）を付けた 10 進数形式の IP アドレスを入力します。
Subnet Mask	パケットの送信元 IP サブネットマスクアドレスを指定します。新しい IP がサブネットベースの VLAN を作成する場合のみ、本欄は設定可能です。「.」（ドット）を付けた 10 進数形式でのサブネットマスクを入力します。
VLAN ID	IP アドレスを割り当てる VLAN（1-3965）を指定します。

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。

バインディングの削除

既存のバインディングを削除するために、「IP Address」メニューから送信元 IP アドレスを選択し、「Delete」ボタンをクリックします。

IP サブネットベース VLAN のサマリ

システムに設定されている IP subnet-to-VLAN に関する情報を表示します。マッピングがないと、画面には「No IP Subnet-based VLAN Configured」というメッセージを表示します。

LAN タブ > Monitoring > VLAN Summary > IP Subnet-based VLAN 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。

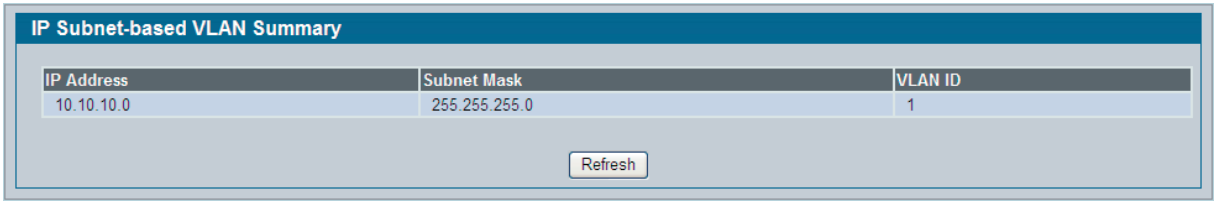


図 4-21　IP Subnet-based VLAN Summary 画面

本画面には次の項目があります。

項目	説明
IP Address	パケットの送信元 IP アドレスを示します。
Subnet Mask	パケットの送信元 IP サブネットマスクアドレスを示します。
VLAN ID	IP アドレスが割り当てられている VLAN を表示します。

「Refresh」ボタンをクリックして、画面を更新し、最新の情報を参照します。

MAC ベース VLAN の管理

MAC ベース VLAN の設定

パケットにタグ取りまたはプライオリティのタグ付けが行われる場合、優先順位がタグ付けをされて、デバイスは MAC ベース VLAN のテーブルにある送信元 MAC アドレスに対応する VLAN にそれを関連付けするものとします。テーブルに一致するエントリがないと、パケットはデバイスの通常の VLAN 分類ルールを受けます。

MAC エントリを VLAN にマップします。送信元 MAC アドレスと VLAN ID の指定後、MAC-to-VLAN 設定は、スイッチのすべてのポートを経由して共有されます。

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

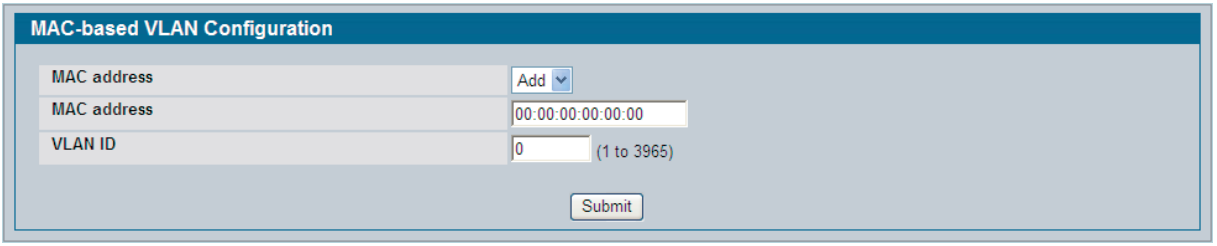


図 4-22　MAC-based VLAN Configuration 画面

本画面には次の項目があります。

項目	説明
MAC address	VLAN にマップする MAC アドレスを選択します。新しい MAC アドレスを入力するためには「Add」を選択します。
MAC address	VLAN にマップする送信元 MAC アドレスを指定します。
VLAN ID	送信元の MAC アドレスがバインドされる VLAN を指定します。

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。

MAC ベース VLAN のサマリ

システムに設定されている MAC-to-VLAN マッピングに関する情報を表示します。

LAN タブ > Monitoring > VLAN Summary > MAC-based VLAN 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。

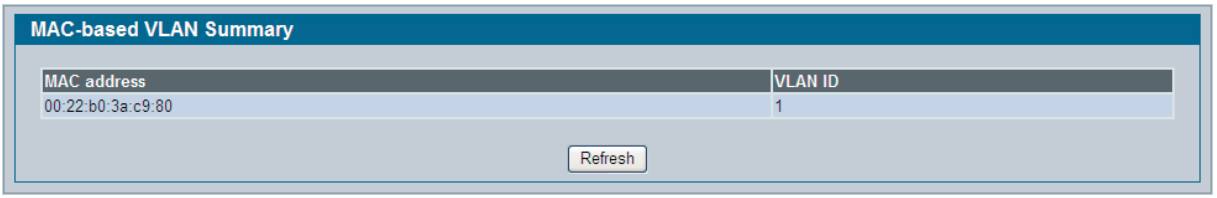


図 4-23　MAC-based VLAN Summary 画面

本画面には次の項目があります。

項目	説明
MAC address	VLAN にマップする MAC アドレスを表示します。
VLAN ID	MAC アドレスがバインドされる VLAN を表示します。

「Refresh」ボタンをクリックして、画面を更新して最新の情報を参照します。

音声 VLAN の設定

音声 VLAN 機能によりスイッチポートは、ポートに到着した時に音声とデータトラフィックに分離するように定義した設定を使用して音声トラフィックを送信することができます。音声 VLAN は、ポートのデータトラフィックが高い時に、IP 電話の音声品質の劣化から確実に保護します。

VLAN が提供する固有の隔離機能は、Inter-VLAN トラフィックを管理制御下におき、ネットワークを攻撃するクライアントが音声コンポーネントに直接攻撃を開始できないようにします。IEEE 802.1P class-of service（CoS）プロトコルに基づいた QoS プロトコルは、分類とスケジューリングを使用して、予測できる方法でスイッチからのネットワークトラフィックを送信します。システムは、IP 電話データのフローを識別するために、ポートを経由して移動するトラフィックの送信元 MAC を使用します。

音声 VLAN はポート単位に有効にすることができます。ポートは一度に 1 つの音声 VLAN にのみ参加することができます。音声 VLAN 機能は、初期値では「Disabled」（無効）になっています。

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

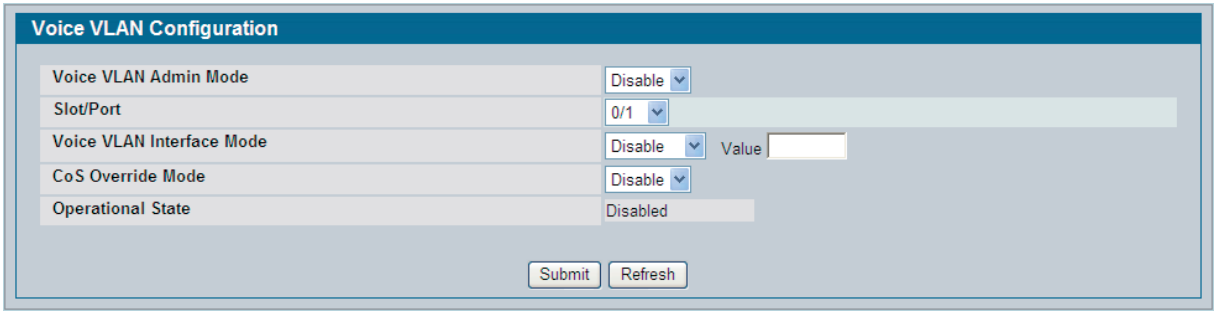


図 4-24　Voice VLAN Configuration 画面

本画面には次の項目があります。

項目	説明
Voice VLAN Admin Mode	「Enable」または「Disable」ボタンをクリックし、すべてのポートの音声 VLAN 機能を有効または無効にします。
Slot/Port	サービスを設定するスロット / ポートを選択します。
Voice VLAN Interface Mode	以下のインタフェースモードの 1 つを選択します。 • Disable - 音声 VLAN サービスはこのインタフェースで無効にされます。「Voice VLAN Admin Mode」欄が優先することにご注意ください。つまり、特定のインタフェースが可能にされても、「Voice VLAN Admin Mode」欄が「Disable」に設定されると、サービスは行われません。 • None - 音声 VLAN サービスはこのインタフェースで無効にされます。しかし、Disable モードと異なり CoS オーバライド機能はポートで操作可能です。 • VLAN ID - 音声 VLAN パケットは割り当てる番号によってユニークに識別されます。すべての音声トラフィックは、ポートのデフォルト VLAN ID が割り当てられる他のデータトラフィックと区別するためにこの VLAN ID に送信します。しかし、音声トラフィックは他のトラフィックと異なり最優先とされません。 • dot1p - VoIP デバイスによってすべての音声トラフィックが他のトラフィックと音声データを区別するように設定されます。他のすべてのトラフィックは、ポートのデフォルトプライオリティを割り当てられます。 • Untagged - VoIP デバイスは、タグなしの音声トラフィックを送信します。
CoS Override Mode	802.1p class-of-service（CoS）を、ポートに到着するすべてのデータ（音声ではない）パケットに対して優先します。そのため、音声 VLAN ポートに接続するどんな不正クライアントも、音声トラフィックの品質を低下させることはできません。
Operational State	音声 VLAN が操作可能かどうかを示します。

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。「Refresh」ボタンをクリックし、システムの情報を最新に更新します。

MAC フィルタの作成

MAC アドレスと VLAN、および送信元ポートと宛先ポートのセットを関連付けます。イングレスポートが送信元ポートのセットに含まれている場合にだけ、指定 VLAN 内のスタティックな MAC アドレスを持つパケットが許可されます。許可されると、宛先リストにあるすべてのポートにパケットを送信します。

LAN タブ > L2 Features > Filters > MAC Filter 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。

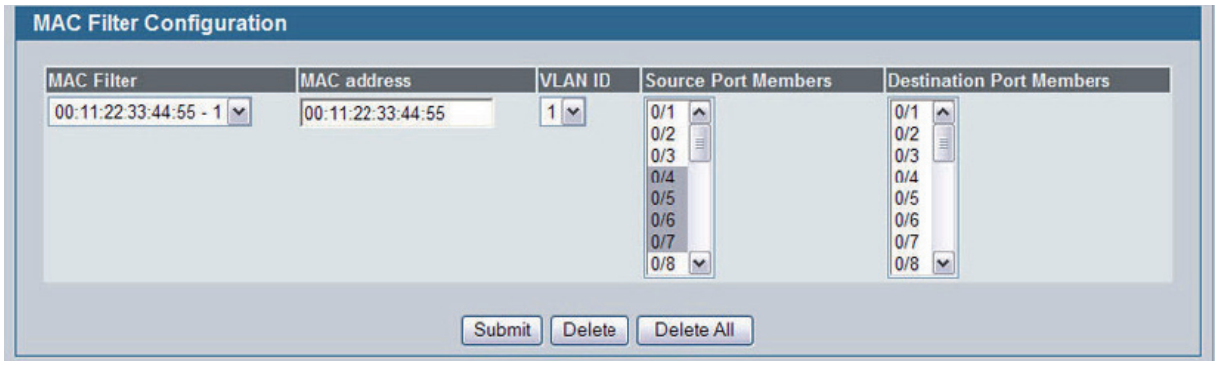


図 4-25　MAC Filter Configuration 画面

本画面には次の項目があります。

項目	説明
MAC Filter	MAC フィルタがシステムに設定されていない場合、「Create Filter」だけがメニューに表示されます。 また、1 つ以上の MAC フィルタが存在すると、リストには設定されたフィルタの MAC アドレスと関連する VLAN ID が表示されます。
MAC address	「00:01:1A:B2:53:4D」形式のフィルタの MAC アドレス。「Create Filter」オプションを選択すると、この欄だけを変更することができます。 **注意**　以下の MAC アドレスにはフィルタを定義することはできません。 • 00:00:00:00:00:00 • 01:80:C2:00:00:00 - 01:80:C2:00:00:0F • 01:80:C2:00:00:20 - 01:80:C2:00:00:21 • FF:FF:FF:FF:FF:FF
VLAN ID	フィルタするパケットを完全に特定するのに MAC アドレスと共に使用される VLAN ID。 「Create Filter」オプションを選択すると、この欄だけを変更することができます。
Source Port Members	内向きフィルタに含めるポートを選択します。 選択した MAC のアドレスと VLAN ID を持つパケットをリストにないポートに受信すると、破棄されます。
Destination Port Members	アウトバウンドフィルタに含めるポートを選択します。 選択した MAC のアドレスと VLAN ID を持つパケットだけが、リストにあるポートから送信されます。

「Submit」ボタンをクリックして、スイッチを本画面の値に更新します。再起動後も新しい値をスイッチに保持する場合、保存を行う必要があります。

フィルタの削除
「Delete」ボタンをクリックし、現在選択したフィルタを削除します。「Delete All」ボタンをクリックして、すべての設定フィルタを削除します。

MAC フィルタの追加
1. MAC フィルタを追加するために、「MAC Filter」メニューから「Create Filter」を選択します。
2. 「MAC address」に有効な MAC アドレスを入力し、メニューから VLAN ID を選択します。VLAN ID メニューは現在システムに設定されている VLAN だけを示します。
3. フィルタに含める 1 つ以上のポートを選択します。「CTRL」を押しながらクリックして複数のポートを選択します。
4. 「Submit」ボタンをクリックし、変更をスイッチに適用します。

MAC フィルタの編集
既存のフィルタのポートマスクを変更するためには、「MAC Filter」からエントリを選択し、次にフィルタに含めるポートをクリックします。または、「CTRL」+ ポートをクリックします。「Submit」ボタンをクリックした際に強調表示されたポートだけが、フィルタに含まれています。

フィルタに関連する MAC アドレスまたは VLAN を変更するためには、フィルタを削除して、再度作成する必要があります。

MAC フィルタの削除
フィルタを削除するためには、「MAC Filter」メニューからフィルタを選択し、「Delete」ボタンをクリックします。フォワーディングデータベースからすべてを削除するためには、「Delete All」ボタンをクリックします。

MAC フィルタのサマリ
MAC フィルタの情報を表示します。

LAN タブ > Monitoring > Filters > MAC Filter 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 4-26　MAC Filter Summary 画面

GARP の設定

GARP（Generic Attribute Registration Protocol ）は、ネットワークの接続性またはメンバシップスタイルの情報を示す汎用プロトコルです。GARP は VLAN またはマルチキャストアドレスなどの特定のネットワーク属性に関連するスイッチのセットを定義します。

GVRP（GARP VLAN Registration Protocol ）は、ネットワークスイッチが同じセグメントに割り当てられているネットワークデバイスに VLAN メンバシップ情報をダイナミックに登録（または登録の解除）し、その情報を GMRP をサポートするブリッジ LAN 内のすべてのネットワークスイッチを経由して広めることができるメカニズムを提供します。

ネットワークデバイスは、GMRP（GARP Multicast Registration Protocol）を使用して、同じセグメントに割り当てられたネットワークデバイスに対してダイナミックにグループメンバシップ情報を登録または登録を解除することができます。
GMRP によってグループメンバシップ情報が GMRP をサポートするブリッジ LAN 内のすべてのネットワークデバイスを経由して広められます。

GVRP および GMRP の動作は、GARP が提供するサービスに依存します。

GARP ステータス

システムと各インタフェースの GARP 設定を参照します。

LAN タブ > Monitoring > GARP Status > 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。

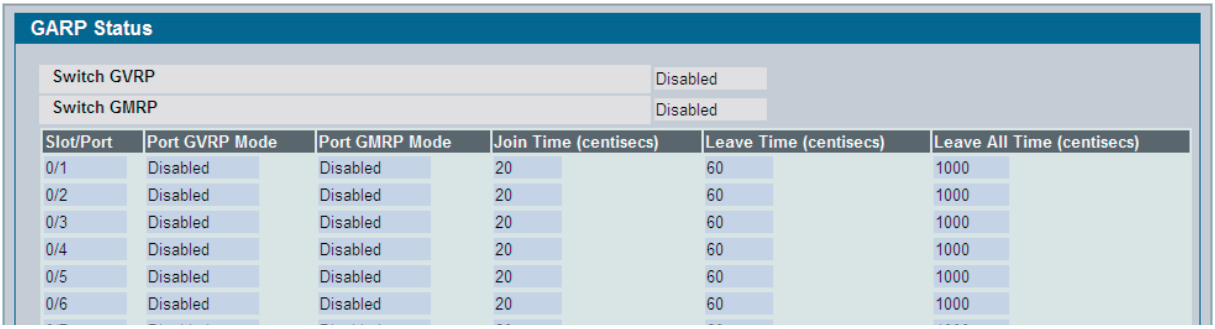


図 4-27　GARP Status 画面

本画面には次の項目があります。

項目	説明
Switch GVRP	スイッチの GVRP プロトコルの有効または無効を表示します。
Switch GMRP	スイッチの GMRP プロトコルの有効または無効を表示します。
Slot/Port	システムインタフェースを示します。
Port GVRP Mode	ポートの GARP VLAN Registration Protocol の管理モードを表示します。モードが「Disabled」であると、プロトコルはアクティブではなく、「Join Timer」、「Leave Timer」および「Leave All Timer」は無効です。
Port GMRP Mode	ポートの GARP Multicast Registration Protocol の管理モードを表示します。モードが「Disabled」であると、プロトコルはアクティブではなく、「Join Timer」、「Leave Timer」および「Leave All Timer」は無効です。
Join Timer (centisecs)	VLAN またはマルチキャストグループに対してメンバシップを登録する（または、再登録する）GARP PDU の送信間隔（センチ秒）を示します。
Leave Timer (centisecs)	GARP 状態を離脱する前にスイッチが待機する経過時間（センチ秒）を表示します。「Leave」タイムは、送信または受信した「Leave All Time」によりアクティブ化され、受信した「Join」メッセージによりキャンセルされます。これにより、別のステーションのための時間を連続したサービスを維持するために同じ属性に必ず登録することができます。
Leave All Timer (centisecs)	GARP 状態を離脱する前にすべてのスイッチが待機する経過時間（センチ秒）を表示します。Leave All Time は Leave Time より長くする必要があります。「Leave All Timer」は「LeaveAll PDU」が生成される間隔を制御します。LeaveAll PDU は、すべての登録がすぐに解除されることを示します。参加者は、登録を維持するために再び参加する必要があります。

GARP スイッチの設定

システムの GARP 設定を行います。

LAN タブ > L2 Features > GARP > Switch 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。

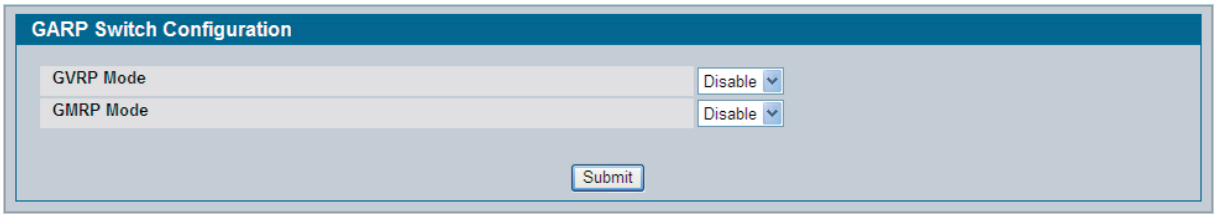


図 4-28　GARP Switch Configuration 画面

本画面には次の項目があります。

項目	説明
GVRP Mode	スイッチの GARP VLAN Registration Protocol の管理モードを設定します。スイッチ GVRP モードは、GVRP がポートで有効であっても、GARP プロトコルで機能するためにポートに有効とされる必要があります。
GMRP Mode	スイッチの GARP Multicast Registration Protocol の管理のモードを参照します。スイッチ GMRP モードは、GMRP がポートで有効であっても、GARP プロトコルで機能するためにポートに有効とされる必要があります。

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。

GARP ポートの設定

指定インタフェースに GARP 設定を行います。

LAN タブ > L2 Features > GARP > Port 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。

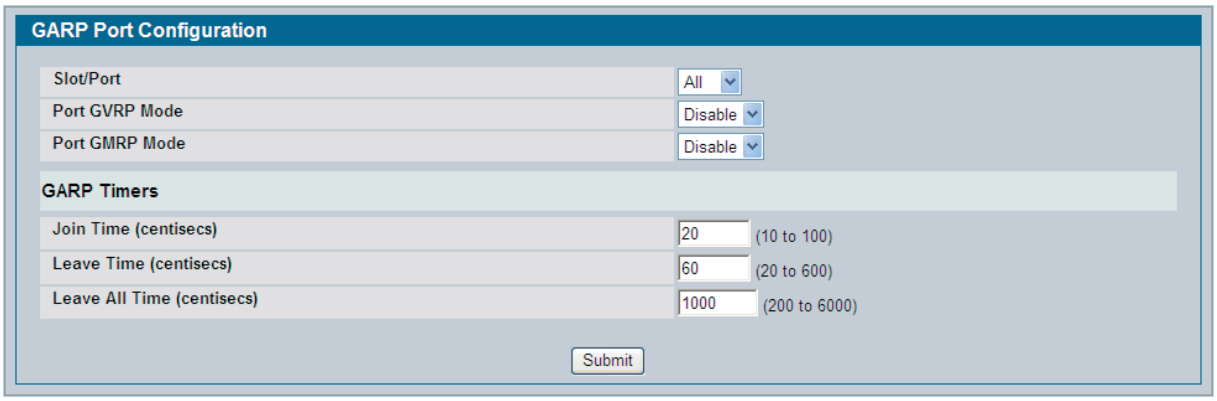


図 4-29　GARP Port Configuration 画面

本画面には次の項目があります。

項目	説明
Slot/Port	GARP 設定を行うインタフェースを指定します。メニューから「All」を選択すると、画面上の設定はすべてのインタフェースに影響します。
Port GVRP Mode	「Enable」または「Disable」を選択することでポートの GARP VLAN Registration Protocol の管理モードを選択します。「Disable」を選択すると、プロトコルはアクティブではなく、「Join Timer」、「Leave Timer」および「Leave All Timer」は無効となります。初期値は「Disable」(無効) です。
Port GMRP Mode	「Enable」または「Disable」を選択することでポートの GARP Multicast Registration Protocol の管理モードを選択します。「Disable」を選択すると、プロトコルはアクティブではなく、「Join Timer」、「Leave Timer」および「Leave All Timer」は無効となります。初期値は「Disable」(無効) です。

項目	説明
GARP Timers	
Join Timer (centisecs)	VLAN またはマルチキャストグループに対してメンバシップを登録する（または、再登録する）GARP PDU の送信間隔（センチ秒）を指定します。10-100（0.1-1.0 秒）の範囲で入力します。初期値は 20 センチ秒（0.2 秒）です。 このタイマのインスタンスは各ポートの各 GARP 参加者のために存在しています。
Leave Timer (centisecs)	GARP 状態を離脱する前にスイッチが待機する経過時間（センチ秒）を表示します。「Leave」タイムは、送信または受信した「Leave All Timer」によりアクティブ化され、受信した「Join」メッセージによりキャンセルされます。 これにより、別のステーションのための時間を連続したサービスを維持するために同じ属性に必ず登録することができます。20-600（0.2-6.0 秒）の範囲で入力します。「Leave Timer」は、「Join Timer」に 3 倍以上である必要があります。初期値は 60 センチ秒（0.6 秒）です。このタイマのインスタンスは各ポートの各 GARP 参加者のために存在しています。
Leave All Timer (centisecs)	GARP 状態を離脱する前にすべてのスイッチが待機する経過時間（ミリ秒）を表示します。「Leave All Timer」は「Leave Timer」より長くする必要があります。可能な範囲は 200-6000 です。初期値は 1000（センチ秒）です。「Leave All Timer」は「LeaveAll PDU」が生成される間隔を制御します。「LeaveAll PDU」は、すべての登録がすぐに解除されることを示します。参加者は、登録を維持するために再び加わる必要があります。「Leave All Period Timer」は「LeaveAllTime」-「1.5*LeaveAllTime」の範囲の乱数で設定されます。タイマはセンチ秒で指定されます。200-6000（2-60 秒）範囲で入力します。初期値は 1000 センチ秒（10 秒）です。このタイマのインスタンスは各ポートの各 GARP 参加者のために存在しています。

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。

ダイナミックな ARP 検査の設定

Dynamic ARP Inspection（DAI）は、無効で悪意がある ARP パケットを拒否するセキュリティ機能です。DAI は、好ましくないステーションが、疑わない Neighbor の ARP キャッシュを害することで他のステーションへのトラフィックを妨害する man-in-the-middle 攻撃（中間者攻撃）の類を防ぎます。悪意のある攻撃者は、別のステーションの IP アドレスをそれ自身の MAC アドレスにマッピングする ARP リクエストまたは応答を送信します。

DAI は DHCP Snooping に基づいています。DHCP Snooping は、DHCP をメッセージ交換をリッスンし、有効な｛MAC アドレス、IP アドレス、VLAN、およびインタフェース｝の組み合わせのバインディングデータベースを構築します。

DAI を有効にすると、スイッチは送信者の MAC アドレスと IP アドレスが DHCP Snooping バインディングデータベース内のエントリに一致しない ARP パケットを破棄します。オプションで追加の ARP パケット検証を設定することができます。

DAI の設定

グローバルな DAI の設定を行います。

LAN タブ > L2 Features > Dynamic ARP Inspection > DAI 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。

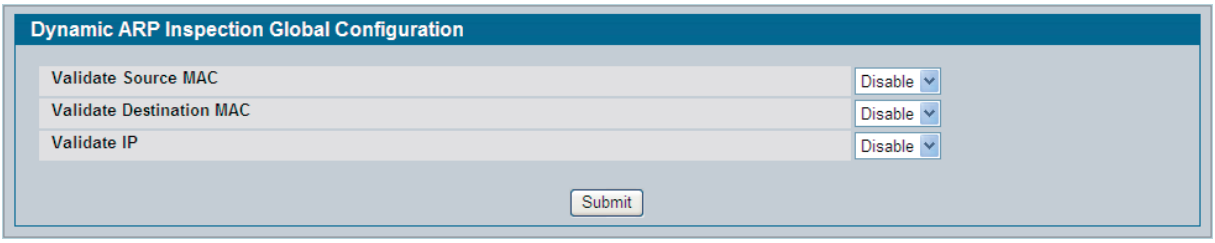


図 4-30　Dynamic ARP Inspection Configuration 画面

本画面には次の項目があります。

項目	説明
Validate Source MAC	スイッチの DAI Source MAC Validation Mode を選択します。「Enable」を選択すると、ARP パケットの Sender MAC 検証が有効になります。初期値は「Disable」（無効）です。
Validate Destination MAC	スイッチの DAI Destination MAC Validation Mode を選択します。「Enable」を選択すると、ARP パケットの Destination MAC 検証が有効になります。初期値は「Disable」（無効）です。
Validate IP	スイッチの DAI IP Validation Mode を選択します。「Enable」を選択すると、ARP パケットの IP Address 検証が有効になります。初期値は「Disable」（無効）です。

「Submit」ボタンをクリックし、新しい設定をスイッチに適用します。「Save」が実行されないと、これらの変更は再起動後に保持されません。

DAI VLAN 設定

情報を表示または設定する DAI-capable VLAN を選択します。

LAN タブ > L2 Features > Dynamic ARP Inspection > DAI VLAN 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。

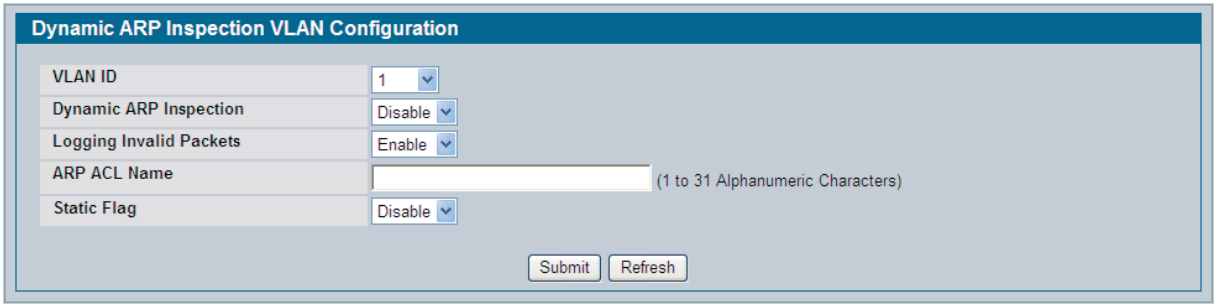


図 4-31　Dynamic ARP Inspection VLAN Configuration 画面

本画面には次の項目があります。

項目	説明
VLAN ID	情報を表示または設定する VLAN ID を選択します。
Dynamic ARP Inspection	この VLAN おける Dynamic ARP Inspection を有効または無効にします。初期値は「Disable」(無効) です。
Logging Invalid Packets	この VLAN おける Dynamic ARP Inspection ログ出力を有効または無効にします。初期値は「Disable」(無効) です。
ARP ACL Name	ARP アクセスリスト名。ARP パケット検証のフィルタとしてルールを含むこの ARP ACL を使用するために VLAN を設定します。半角英数字 31 以内で指定します。
Static Flag	ARP ACL ルールが一致しない場合にこのフラグを使用して、ARP パケットが DHCP Snooping データベースを使用した検証を必要とするかどうかを決定します。 • Enable - ARP パケットは ARP ACL ルールだけに検証されます。 • Disable - ARP パケットは、さらに DHCP Snooping エントリを使用した検証を必要とします。(初期値)

「Submit」ボタンをクリックし、新しい設定をスイッチに適用します。「Save」が実行されないと、これらの変更は再起動後に保持されません。
「Refresh」ボタンをクリックすると、スイッチにおける現在のデータの多くを更新します。

DAI インタフェース設定

情報の表示または設定を行います。

LAN タブ > L2 Features > Dynamic ARP Inspection > DAI Interface 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。

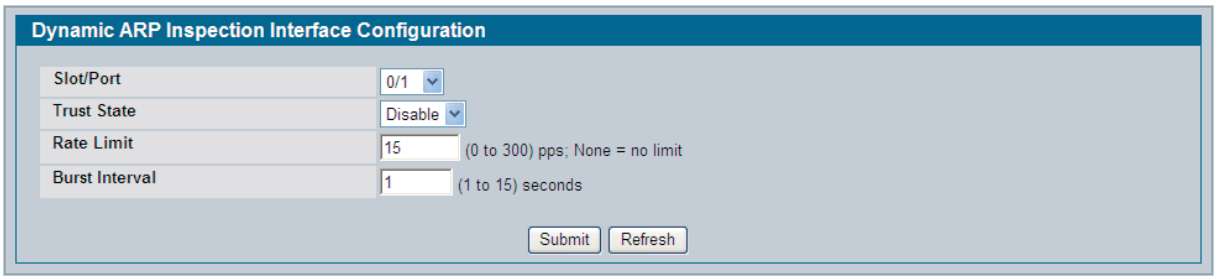


図 4-32　Dynamic ARP Inspection Interface Configuration 画面

本画面には次の項目があります。

項目	説明
Slot/Port	データを表示または設定する物理インタフェースを選択します。
Trust State	インタフェースをダイナミック ARP 検証にために信頼するかどうかを指定します。 • Enable - インタフェースは信頼されます。本インタフェースから到着する ARP パケットをチェックなしで転送します。 • Disable - インタフェースは信頼されません。本インタフェースから到着する ARP パケットには、ARP 検査が行われます。(初期値)
Rate Limit	Dynamic ARP Inspection にレート制限値を指定します。入力レートが連続してバースト間隔 (秒) の制限値を超えている場合、ARP パケットは廃棄されます。この値が「None」の場合、制限はありません。初期値は 15 パケット / 秒です。
Burst Interval	このインタフェースにおけるレート制限のためにバースト間隔を指定します。レートリミットが「None」であると、バースト間隔は意味がなくなり、「N/A」と表示されます。初期値は 1 (秒) です。

「Submit」ボタンをクリックし、新しい設定をスイッチに適用します。「Save」が実行されないと、これらの変更は再起動後に保持されません。
「Refresh」ボタンをクリックすると、スイッチにおける現在のデータの多くを更新します。

DAI ARP ACL 設定

DAI ARP ACL の追加または削除を行います。

LAN タブ > L2 Features > Dynamic ARP Inspection > DAI ARP ACL 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。

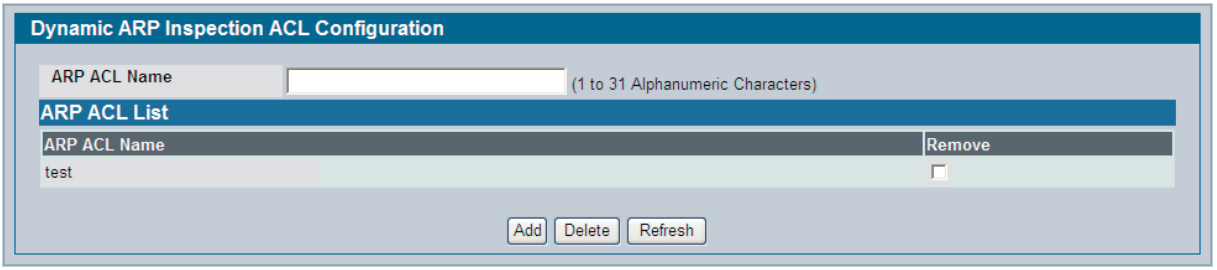


図 4-33　Dynamic ARP Inspection ACL Configuration 画面面

本画面には次の項目があります。

項目	説明
ARP ACL Name	ダイナミック ARP 検査のために新しい ARP ACL を作成します。半角英数字 31 文字以内で指定します。
ARP ACL List	設定したすべての ARP ACL のリストを名前ごとに表示します。「Remove」欄を使用して、削除する ACL を選択します。

「Refresh」ボタンをクリックすると、スイッチにおける現在のデータを更新します。

ARP ACL の追加

「Add」ボタンをクリックして新しい ARP ACL を作成します。

ARPACL エントリの削除

「Delete」ボタンをクリックして、「Remove」欄で選択した設定済み ARP ACL エントリを削除します。

DAI ARP ACL ルールの設定

DAI ARP ACL ルールの追加または削除を行います。

LAN タブ > L2 Features > Dynamic ARP Inspection > DAI ARP ACL Rule 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。

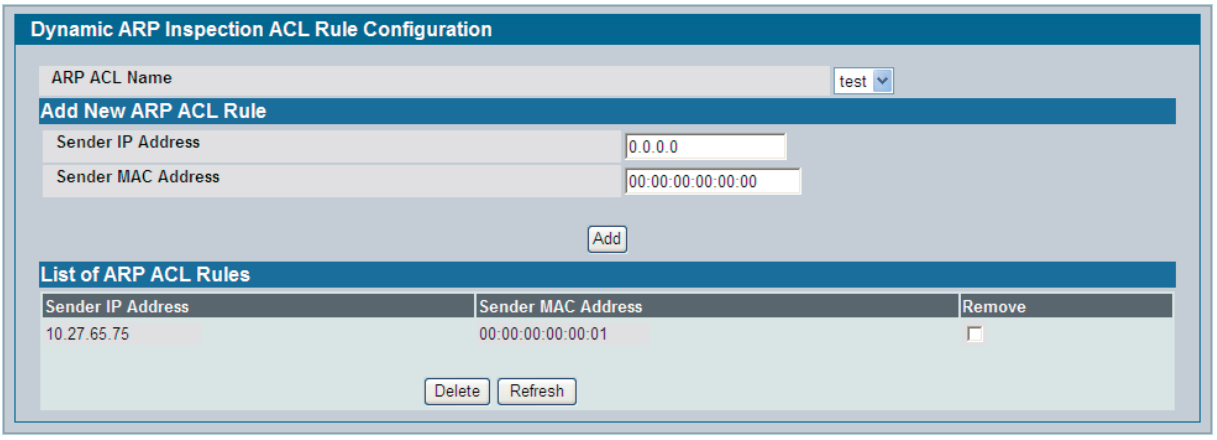


図 4-34　Dynamic ARP Inspection ACL Rule Configuration 画面

本画面には次の項目があります。

項目	説明
ARP ACL Name	情報を表示または設定する ARP ACL を選択します。
Sender IP Address	選択した ARP ACL に新しいルールを作成するためには、ARP ACL に一致する送信元 IP アドレスの値を入力します。
Sender MAC Address	選択した ARP ACL に新しいルールを作成するためには、ARP ACL に一致する送信元 MAC アドレスの値を入力します。
Remove	「Remove」欄を使用して、削除する ARP ACL ルールを選択します。

「Refresh」ボタンをクリックすると、スイッチにおける現在のデータの多くを更新します。

ARP ACL ルールの追加

「Add」ボタンをクリックして新しい ARP ACL ルールを追加します。

ARPACL ルールエントリの削除

「Submit」ボタンをクリックして、「Remove」欄に選択したエントリを削除します。

Dynamic ARP Inspection Statistics（ダイナミックな ARP 検査の統計情報）

VLAN ごとの統計情報を表示します。

LAN タブ > Monitoring > Dynamic ARP Inspection 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。

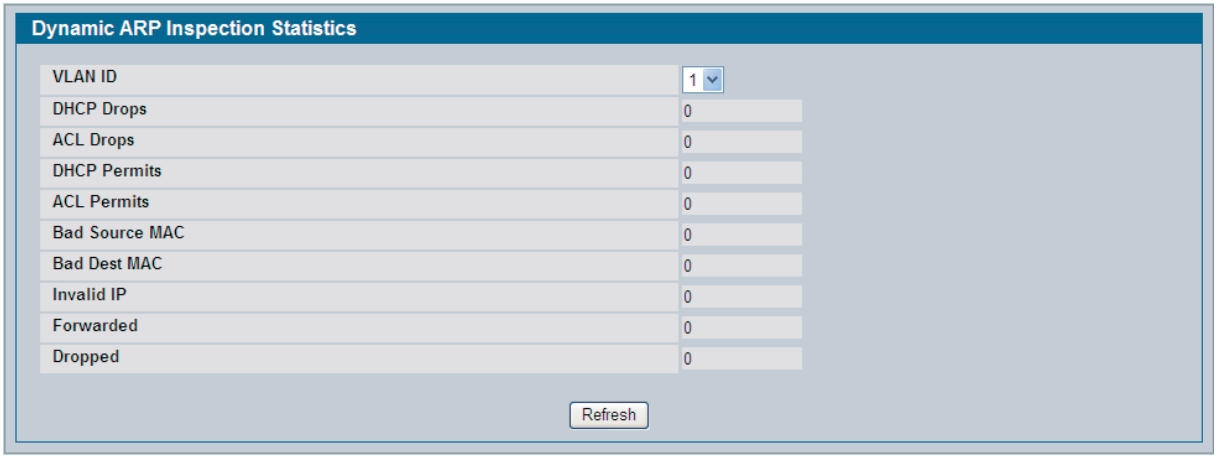


図 4-35　Dynamic ARP Inspection Statistics 画面

本画面には次の項目があります。

項目	説明
VLAN ID	統計情報を表示する DAI が有効な VLAN ID を選択します。
DHCP Drops	DHCP Snooping バインディングエントリへの一致が検出されないために、DAI に破棄された ARP パケット数。
ACL Drops	ARP ACL ルールへの一致が検出されないために、DAI に破棄された ARP パケット数。スタティックフラグはこの VLAN に設定されます。
DHCP Permits	DHCP Snooping バインディングエントリへの一致が検出されたため、DAI が転送した ARP パケット数。
ACL Permits	ARP ACL ルールへの一致が検出されたために、DAI に許可された ARP パケット数。
Bad Source MAC	ARP パケット内の送信元 MAC アドレスがイーサネットヘッダの送信元 MAC に一致しないために DAI が破棄した ARP パケット数。
Bad Dest MAC	ARP 応答パケット内の宛先 MAC アドレスがイーサネットヘッダの宛先 MAC に一致しないために DAI が破棄した ARP パケット数。
Invalid IP	ARP パケット内の送信元 IP アドレスまたは ARP 応答パケット内の宛先 IP アドレスが有効でないために DAI が破棄した ARP パケット数。有効でないアドレスは、「0.0.0.0」、「255.255.255.255」、IP マルチキャストアドレス、クラス E アドレス（240.0.0.0/4）、およびループバックアドレス（127.0.0.0/8）を含んでいます。
Forwarded	DAI が転送した ARP パケット数。
Dropped	DAI が破棄した ARP パケット数。

「Refresh」ボタンをクリックすると、スイッチにおける現在のデータを更新します。

IGMP Snooping の設定

IGMP（Internet Group Management Protocol）Snooping は、スイッチがスイッチ上のマルチキャストトラフィックをインテリジェントに転送できる機能です。マルチキャスト IP トラフィックは、ホストグループに向かうトラフィックです。ホストグループは、クラス D の IP アドレス（範囲 224.0.0.0 - 255.255.255.255）によって示されます。IGMP クエリとレポートメッセージに基づいて、スイッチはマルチキャストトラフィックを要求するポートだけにトラフィックを送信します。これはスイッチがトラフィックをすべてのポートにブロードキャストし、ネットワーク性能に影響することを防ぎます。

伝統的なイーサネットネットワークは、多くのデバイスを同じ共有メディアにおかないように別のネットワークセグメントに分離されます。ブリッジとスイッチはこれらのセグメントに接続します。ブロードキャストまたはマルチキャスト宛先アドレスを持つパケットを受信すると、IEEE MAC Bridge 標準に従って、スイッチは残りの各ネットワークセグメントにコピーを送信します。最終的に、パケットはネットワークに接続するすべてのノードからアクセス可能となります。

この手法は、接続するすべてのノードが参照または処理されるべきブロードキャストパケットに適切に動作します。しかし、マルチキャストパケットの場合、この手法は、とりわけパケットが少数のノードだけに向かっている場合にネットワーク帯域の効果的な使用を導くものではありません。パケットは、パケットの受信を希望するノードがないネットワークセグメントにもフラッドされます。リクエストされていないグループアドレスのパケットをフィルタするためにノードがあまり処理オーバヘッドを小さくしている場合には、マルチキャストパケットがフラッドする間に共有メディアに新しいパケットを送信することはできません。帯域幅を浪費するという問題は、Full Duplex リンクなど LAN セグメントが共有されない場合にはさらに悪くなります。

スイッチに IGMP パケットの検索を許可することは、この問題を解決するための創造的な試みと言えます。スイッチは、ネットワーク経由で送信される IGMP パケット内の情報を使用して、どのセグメントがグループアドレスに向かうパケットを受信するかを決定します。

グローバルな設定とステータス

スイッチの IGMP Snooping 機能の有効化、および現在の IGMP 設定に関する情報の参照を行います。

LAN タブ > L2 Features > IGMP Snooping > IGMP 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。

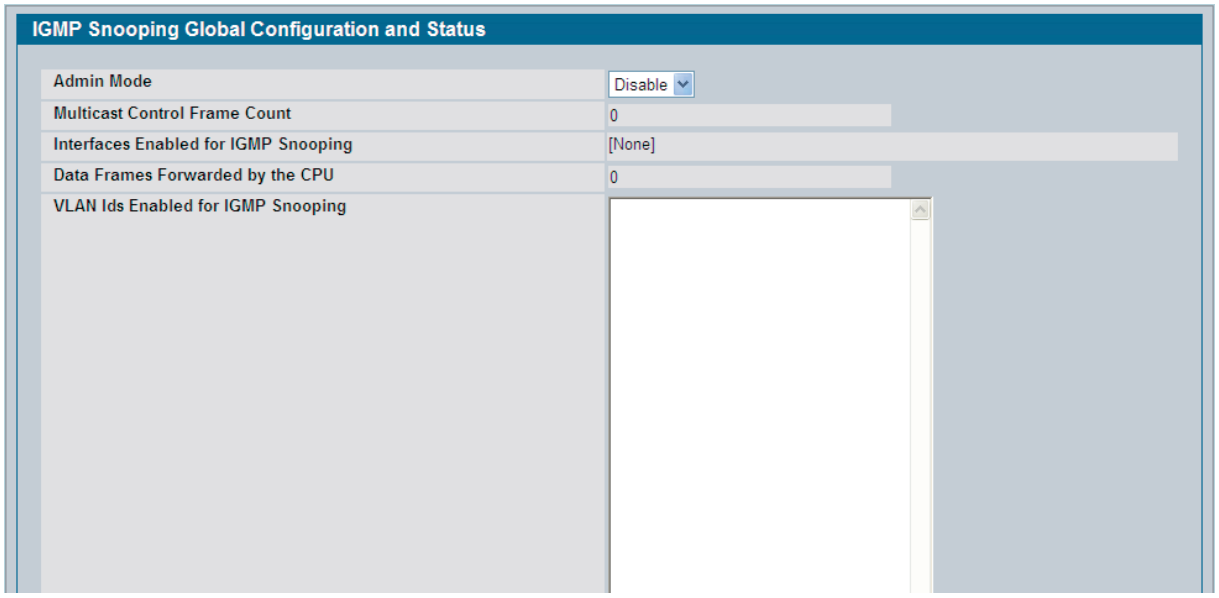


図 4-36　IGMP Snooping Global Configuration and Status 画面

本画面には次の項目があります。

項目	説明
Admin Mode	スイッチにおける IGMP Snooping の管理モードを選択します。初期値は無効です。
Multicast Control Frame Count	CPU が処理したマルチキャスト制御フレーム数を表示します。
Interfaces Enabled for IGMP Snooping	現在 IGMP Snooping が有効であるインタフェースを表示します。IGMP Snooping を有効にするためには、「インタフェース設定」（135 ページ）を参照してください。
Data Frames Forwarded by the CPU	CPU が送信したデータフレーム数を表示します。
VLAN Ids Enabled For IGMP Snooping	IGMP Snooping が有効な VLAN を表示します。IGMP Snooping に VLAN を有効にするためには、「マルチキャストルータのステータス」（138 ページ）を参照してください。

「Enable」または「Disable」ボタンをクリックし、「Submit」ボタンをクリックして「Admin Mode」を有効または無効にします。
再起動後にも変更を保持するためには保存する必要があります。

インタフェース設定

特定のインタフェースに IGMP snooping 設定を行います。

LAN タブ > L2 Features > IGMP Snooping > Interface 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。

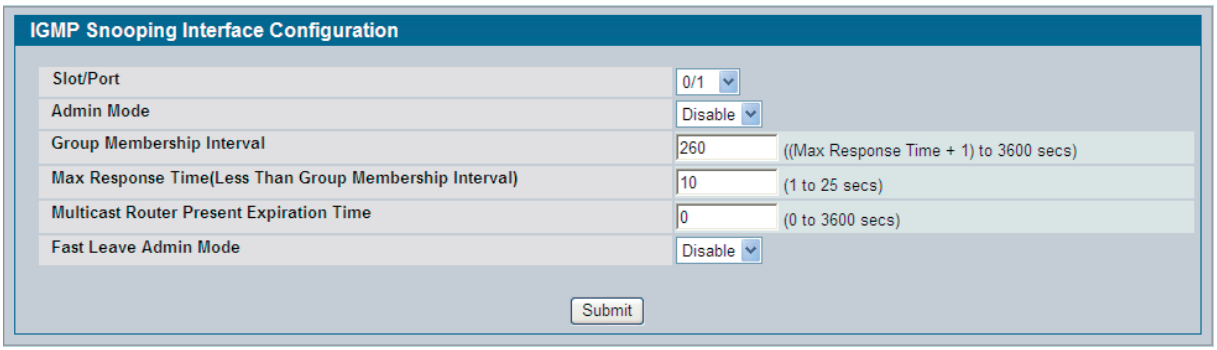


図 4-37　IGMP Snooping Interface Configuration 画面

本画面には次の項目があります。

項目	説明
Slot/Port	設定する物理または LAG インタフェースを選択します。
Admin Mode	スイッチにおける IGMP Snooping の選択インタフェースにおけるインタフェースモードを選択します。初期値では無効に設定されています。
Group Membership Interval	グループからそのインタフェースを削除する前に、指定インタフェース上の指定グループのレポートをスイッチが待つ時間を指定します。有効範囲は 2-3600（秒）です。初期値は 260（秒）です。
Max Response Time (Less Than Group Membership Interval)	インタフェース上の指定グループのレポートを受信しなかったためにインタフェースにクエリを送信した後にスイッチが待機する時間を指定します。1 以上で「Group Membership Interval」より小さい値を入力します。初期値は 10（秒）です。
Multicast Router Present Expiration Time	割り当てられているマルチキャストルータを持つインタフェースリストから削除する前に、インタフェース上のクエリの受信をスイッチが待つ時間 0-3600（秒）を指定します。初期値は 0（秒）です。0 は無限のタイムアウト、つまり期限がないことを示します。
Fast Leave Admin Mode	指定インタフェースの Fast Leave モードを選択します。初期値は「Disable」（無効）です。Fast Leave モードを有効にすると、スイッチは、インタフェースへの MAC ベースの汎用クエリを最初に送信しないで、マルチキャストグループの IGMP Leave メッセージを受信するフォワーディングテーブルからレイヤ 2 の LAN インタフェースを直ちに削除することができます。

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。

VLAN の設定

システムにおける VLAN に IGMP snooping 設定を行います。

LAN タブ > L2 Features > IGMP Snooping > VLAN 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。

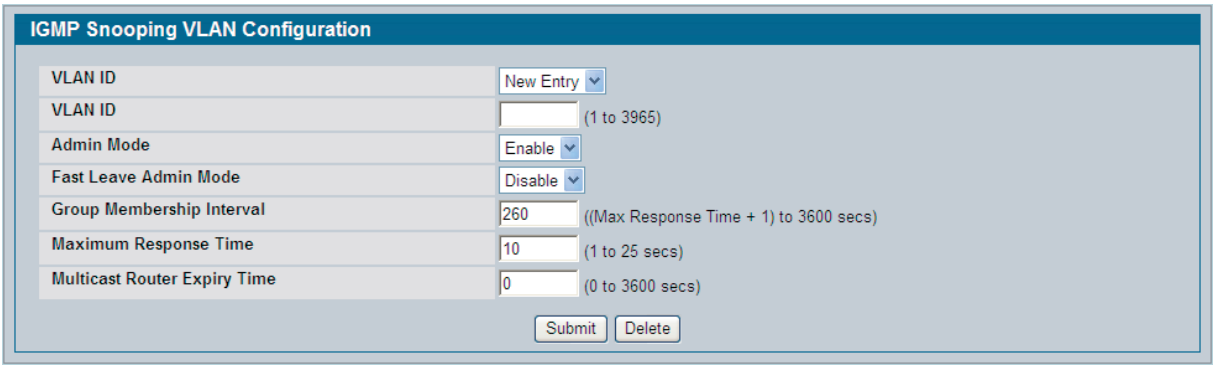


図 4-38　IGMP Snooping VLAN Configuration 画面

本画面には次の項目があります。

項目	説明
VLAN ID	編集する VLAN の VLAN ID を選択します。または、「New Entry」を選択し、IGMP Snooping を有効にします。
Admin Mode	「Enable」のみ利用可能です。VLAN の IGMP Snooping の admin モードを無効にするためには、「VLAN ID」から VLAN を選択し、「Delete」ボタンをクリックします。
Fast Leave Admin Mode	Fast Leave モードを有効にすると、スイッチは、インタフェースへの MAC ベースの汎用クエリを最初に送信しないで、マルチキャストグループの IGMP Leave メッセージを受信するフォワーディングテーブルからレイヤ 2 の LAN インタフェースを直ちに削除することができます。1 台のホストだけが各レイヤ 2 の LAN ポートに接続している VLAN に fast-leave admin モードを有効にすべきです。これは同じレイヤ 2 の LAN ポートに接続し、そのグループに向けられたマルチキャストトラフィックの受信を希望する他のホストをうかつに破棄してしまうことを防止します。また、fast-leave の処理は IGMP のバージョン 2 のホストでサポートされます。
Group Membership Interval	エントリからインタフェースを削除する前に、指定インタフェース上の指定グループのレポートをスイッチが待つ時間を指定します。IGMPv3 Maximum Response より大きい値を指定する必要があります。範囲は 2-3600（秒）です。
Maximum Response Time	インタフェース上の指定グループのレポートを受信しなかったためにインタフェースにクエリを送信した後にスイッチが待機する時間（秒）を指定します。この値には「Group Membership Interval」より小さい値を入力してください。範囲は、1-25（秒）です。
Operational Maximum Response Time	指定 VLAN ID への IGMP Snooping の最大応答時間を表示します。この値は、この VLAN に受信した IGMPv2 または IGMPv3 からダイナミックに学習されます。マルチキャストトラフィックが妨害されないように、group membership interval をこの値より大きくなるように設定する必要があります。
Multicast Router Expiry Time	マルチキャストルータが割り当てられているインタフェースがインタフェースリストから削除される前に、インタフェースへのクエリの受信をスイッチが待つ時間 0-3600（秒）を指定します。0 は無限のタイムアウト、つまり期限がないことを示します。

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。

VLAN ステータス

IGMP Snooping に設定されている VLAN に関する情報を参照します。

LAN タブ > Monitoring > IGMP Snooping Status > VLAN 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 4-39　IGMP Snooping VLAN Status 画面

本画面には次の項目があります。

項目	説明
VLAN ID	IGMP Snooping モードが有効である VLAN ID を表示します。
Admin Mode	VLAN ID に対する IGMP Snooping モードを表示します。
Fast Leave Admin Mode	IGMP Snooping Fast-leave が VLAN でアクティブであるかどうかを表示します。
Group Membership Interval (secs)	エントリからインタフェースを削除する前に、VLAN に参加している指定インタフェース上の指定グループからのレポートをスイッチが待つ時間（秒）を表示します。
Max Response Time (secs)	インタフェース上の指定グループのレポートを受信しなかったために VLAN に参加しているインタフェースにクエリを送信した後にスイッチが待機する時間を表示します。
Operational Maximum Response Time (secs)	指定 VLAN ID への IGMP Snooping の最大応答時間を表示します。この値は、この VLAN に受信した IGMPv2 または IGMPv3 からダイナミックに学習されます。
Multicast Router Expiry Time (secs)	マルチキャストルータを持つインタフェースリストから VLAN に参加しているインタフェースを削除する前に待機する時間を表示します。クエリを受け取らないと、インタフェースは削除されます。

「Refresh」ボタンをクリックし、システムの情報を最新に更新します。

マルチキャストルータ設定

マルチキャストルータがスイッチに割り当てられると、その存在はダイナミックに学習されます。スイッチは、マルチキャストルータインタフェースとしてスイッチポートをスタティックに設定できます。

スタティックなマルチキャストルータインタフェースとして手動でインタフェースを設定します。

LAN タブ > L2 Features > IGMP Snooping > Multicast Router 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。

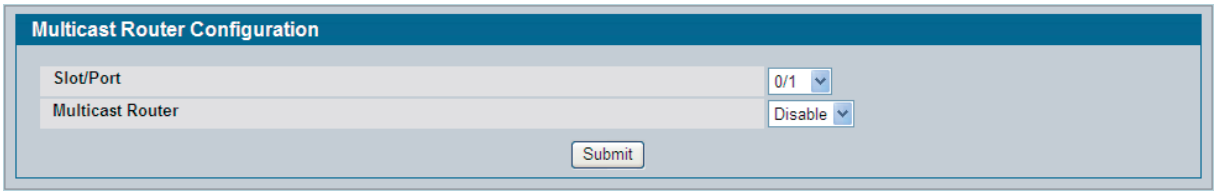


図 4-40　Multicast Router Configuration 画面

本画面には次の項目があります。

項目	説明
Slot/Port	設定する物理または LAG インタフェースを選択します。
Multicast Router	マルチキャストルータのステータスを設定します。 • Enable - ポートはマルチキャストルータインタフェースです。 • Disable - ポートは、マルチキャストルータを設定しません。

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。

マルチキャストルータのステータス

特定のインタフェースがマルチキャストルータインタフェースとして設定されるかどうか確認します。

LAN タブ > Monitoring > IGMP Snooping Status > Multicast Router 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。

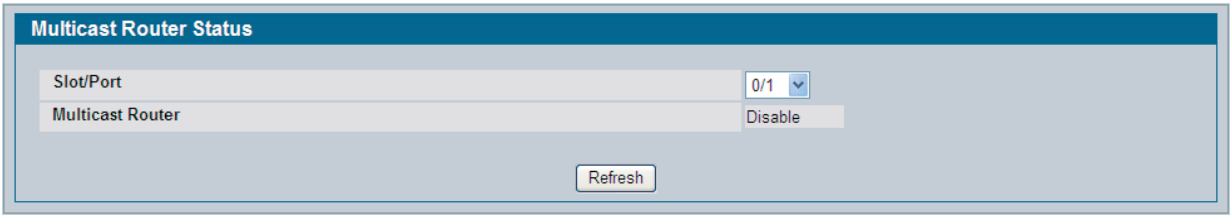


図 4-41　Multicast Router Status 画面

本画面には次の項目があります。

項目	説明
Slot/Port	表示する物理または LAG インタフェースを選択します。
Multicast Router	指定インタフェースがマルチキャストルータとして設定されているかどうかを表示します。

Multicast Router VLAN Configuration（マルチキャストルータ VLAN 設定）

インタフェース上の VLAN にマルチキャストルータの設定を行います。

LAN タブ L2 Features > IGMP Snooping > Multicast Router VLAN 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。

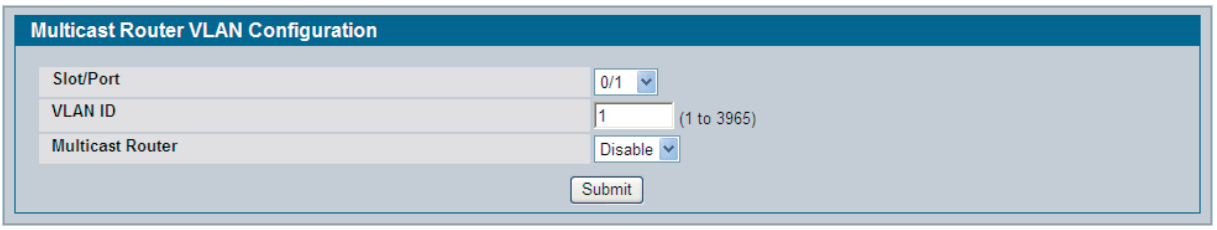


図 4-42　Multicast Router VLAN Configuration 画面

本画面には次の項目があります。

項目	説明
Slot/Port	設定する物理または LAG インタフェースを選択します。
VLAN ID	マルチキャストルーティングを有効または無効にする VLAN ID を入力します。
Multicast Router	「Enable」または「Disable」を選択し、このインタフェースに関連している VLAN のマルチキャストルータモードを変更します。

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。

Multicast Router VLAN Status（マルチキャストルータ VLAN ステータス）

指定インタフェース上の VLAN のマルチキャストルータ設定を参照します。

LAN タブ > Monitoring > IGMP Snooping Status > Multicast Router VLAN 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。

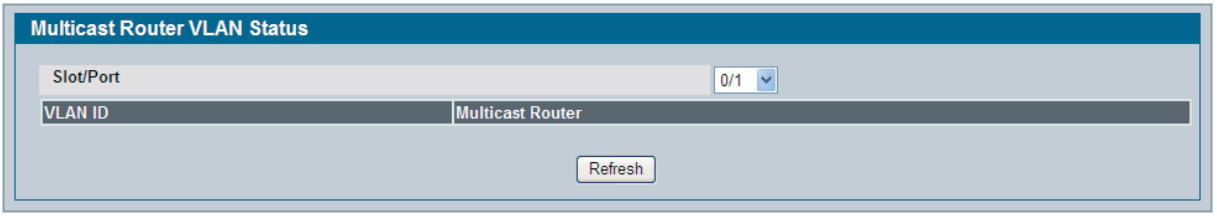


図 4-43　Multicast Router VLAN Status 画面

本画面には次の項目があります。

項目	説明
Slot/Port	表示する物理または LAG インタフェースを選択します。
VLAN ID	VLAN がインタフェースのマルチキャストルーティングに有効にされると、ID を表示します。
Multicast Router	マルチキャストルータがこのインタフェースの VLAN に対して有効かどうかを表示します。

「Refresh」ボタンをクリックし、システムの情報を最新に更新します。

IGMP Snooping クエリアの設定

IGMP Snooping では、ネットワークにおける中央スイッチまたはルータがマルチキャストメンバシップを通知するために定期的にすべての端末にクエリを送信することが必要です。この中央デバイスが「IGMP クエリア」です。IGMP レポートとして知られている IGMP クエリの応答は、ポートごとに現在のマルチキャストグループメンバシップと共に更新されたスイッチを保持します。スイッチは、更新後のメンバシップ情報をすぐに受け取らないと、端末が位置するポートにマルチキャストを送信することを中止します。

以下の画面を使用して、ネットワーク上の、および VLAN ごとの IGMP Snooping クエリアに関する情報を設定、および表示することができます。

Snooping クエリアの設定

IGMP Snooping クエリア機能の有効 / 無効化、クエリを実行するルータの IP アドレスの指定、および関連するパラメータの設定を行います。本画面のデータを変更するためには、ユーザは Read/Write のアクセス権を持つ必要があります。

LAN タブ > L2 Features > IGMP Snooping Querier > Querier 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。

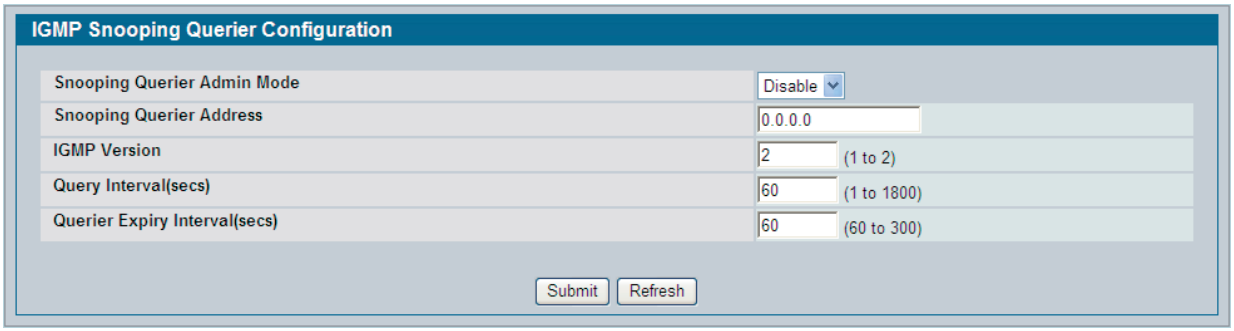


図 4-44　IGMP Snooping Querier Configuration 画面

本画面には次の項目があります。

項目	説明
Snooping Querier Admin Mode	スイッチの IGMP Snooping の管理モードを選択します。初期値は「Disable」（無効）です。
Snooping Querier Address	送信元 IP アドレスとして定期的な IGMP クエリに使用される Snooping クエリアアドレスを指定します。アドレスがクエリが送信される VLAN に設定されていない場合に、このアドレスが使用されます。
IGMP Version	定期的な IGMP クエリに使用される IGMP プロトコルバージョンを指定します。
Query Interval (secs)	Snooping クエリアが送信する定期的なクエリの間隔 1-1800（秒）を指定します。初期値は 60（秒）です。
Querier Expiry Interval (secs)	最後のクエリア情報の削除の間隔 60-300（秒）を指定します。初期値は 60（秒）です。

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。「Refresh」ボタンをクリックし、スイッチの情報を最新に更新します。

IGMP Snooping クエリア VLAN 設定

ネットワーク上のホストに対して DNS ホスト名を設定します。

LAN タブ > L2 Features > IGMP Snooping > VLAN 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。

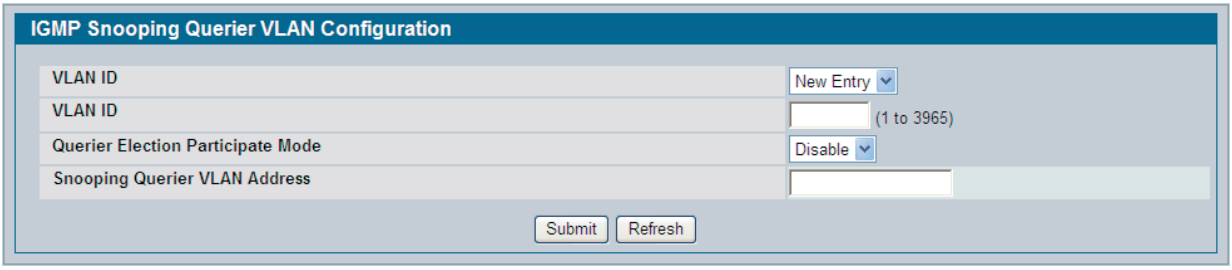


図 4-45　IGMP Snooping Querier VLAN Configuration 画面

本画面には次の項目があります。

項目	説明
VLAN ID	IGMP Snooping Querier が有効である VLAN ID を表示します。「NewEntry」を選択して、IGMP Snooping 用に新しい VLAN ID を作成します。
Querier Election Participate Mode	「Querier Participate」モードを有効または無効にします。このモードが無効であると、VLAN 内の同じバージョンの別のクエリを参照する場合に Snooping クエリアは non-querier 状態に移行します。有効であると、Snooping クエリアはクエリアの選出に参加します。その場合、最小 IP アドレスがその VLAN においてクエリアとして動作します。もう一方のクエリアは non-querier 状態に移行します。
Snooping Querier VLAN Address	指定 VLAN に送信される定期的な IGMP クエリ内の送信元 IP アドレスとして使用されるアドレスを指定します。

「Refresh」ボタンをクリックし、スイッチの情報を最新に更新します。

Snooping クエリア VLAN 設定のサマリ

ネットワークにおける VLAN の IGMP snooping クエリアのサマリ情報を参照します。

LAN タブ > L2 Features > IGMP Snooping Querier > Querier VLAN Configuration 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。

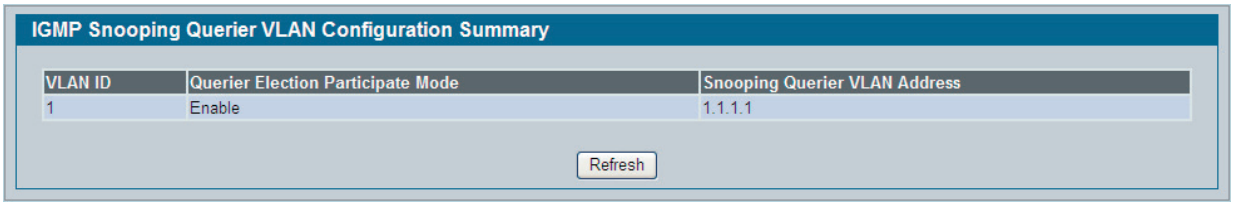


図 4-46　IGMP Snooping Querier VLAN Configuration Summary 画面

本画面には次の項目があります。

項目	説明
VLAN ID	IGMP Snooping クエリアが管理上有効である VLAN ID を表示します。
Querier Election Participate Mode	VLAN における「Querier Election Participate Mode」を表示します。本モードが無効であると、VLAN 内の同じバージョンの別のクエリを参照する場合に Snooping クエリアは non-querier 状態に移行します。有効であると、Snooping クエリアはクエリアの選出に参加します。その場合、最小 IP アドレスがその VLAN においてクエリアとして動作します。もう一方のクエリアは non-querier 状態に移行します。
Snooping Querier VLAN Address	指定 VLAN に送信される定期的な IGMP クエリ内の送信元 IP アドレスとして使用されるアドレスを表示します。

「Refresh」ボタンをクリックし、システムの情報を最新に更新します。

IGMP Snooping クエリア VLAN ステータス

ネットワーク上の VLAN の IGMP snooping クエリアの動作状態などの情報を参照します。

LAN タブ > Monitoring > Querier VLAN 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

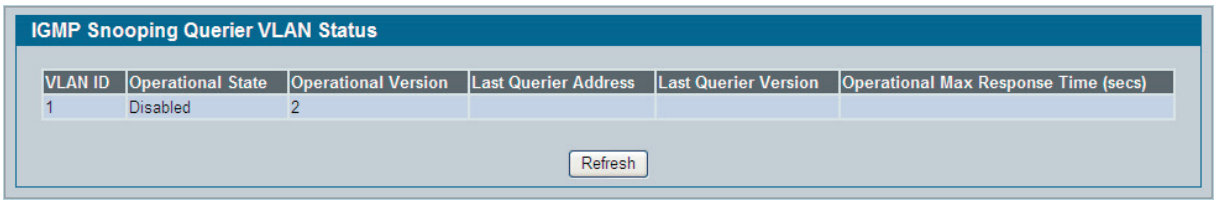


図 4-47　IGMP Snooping Querier VLAN Status 画面

本画面には次の項目があります。

項目	説明
VLAN ID	IGMP Snooping クエリアが管理上有効であり、VLAN が VLAN データベースに存在する VLAN ID を表示します。
Operational State	VLAN 上の IGMP Snooping クエリアの動作状態を表示します。 • Querier - Snooping スイッチは VLAN のクエリアです。Snooping スイッチは、設定したクエリアのクエリ間隔と等しい間隔で定期的なクエリを送信します。Snooping スイッチが VLAN 内により適切なクエリア（数字が低い方）を見つけると、「Non-querier」モードに移行します。 • Non-Querier - Snooping スイッチが VLAN において「Non-querier」モードです。クエリアのタイマが期限切れとなると、Snooping スイッチは querier モードに移行します。 • Disabled - Snooping クエリアは VLAN では操作されません。IGMP Snooping が VLAN で操作可能でない場合、クエリアアドレスが設定されていない場合、またはネットワーク管理アドレスが設定されていない場合に Snooping クエリアは無効モードに移行します。
Operational Version	操作可能なクエリアの IGMP バージョンを表示します。
Last Querier Address	クエリが VLAN でスヌープされた最後のクエリアの IP アドレスを表示します。
Last Querier Version	クエリが VLAN でスヌープされた最後のクエリアの IGMP プロトコルバージョンを表示します。
Operational Max Response Time (secs)	Snooping クエリアが送信するクエリに使用される最大の応答時間を表示します。

「Refresh」ボタンをクリックし、スイッチの情報を最新に更新します。

MLD Snooping の設定

IPv4 では、レイヤ 2 スイッチは、IGMP Snooping を使用してダイナミックにレイヤ 2 インタフェースを設定することでマルチキャストトラフィックのフラッディングを制限し、IP マルチキャストアドレスに関連するインタフェースだけにマルチキャストトラフィックを送信します。IPv6 では、Multicast Listener Discovery（MLD）Snooping が同様の機能を実行します。VLAN のすべてのポートにフラッディングする代わりに、MLD Snooping を使用してデータの受信を希望するポートのリストに IPv6 マルチキャストデータを選択的に転送します。このリストは、IPv6 マルチキャスト制御パケットをスヌープすることで設定されます。

MLD は、IPv6 マルチキャストルータによって使用されるプロトコルで、直接接続するリンク上のマルチキャストリスナ（IPv6 マルチキャストパケットの受信を希望するノード）の存在の検出し、どのマルチキャストパケットが Neighbor ノードに関連するかを検出します。MLD バージョン 1（MLDv1）は IGMPv2 と同等であり、MLD バージョン 2（MLDv2）は IGMPv3 と同等です。MLD は ICMPv6（Internet Control Message Protocol バージョン 6）であり、MLD メッセージは ICMPv6 メッセージのサブセットです。

スイッチは MLDv1 と MLDv2 両方のプロトコルパケットをスヌープし、宛先 IPv6 マルチキャストの MAC アドレスに基づいて IPv6 マルチキャストデータをブリッジします。同時に MLD Snooping と IGMP snooping を実行するようにスイッチを設定できます。

設定とステータス

スイッチの MLD Snooping 機能の有効化および現在の MLD Snooping 設定に関する情報を参照します。

LAN タブ > L2 Features > MLD Snooping > Configuration and 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。

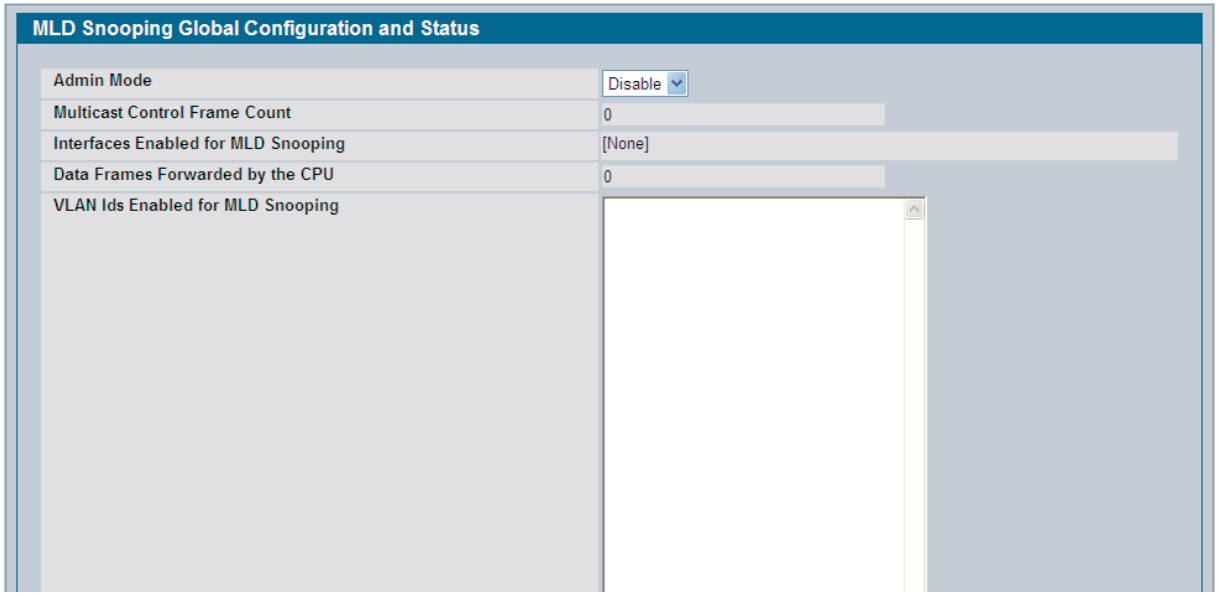


図 4-48　MLD Snooping Global Configuration and Status 画面

本画面には次の項目があります。

項目	説明
Admin Mode	スイッチのおける MLD Snooping の管理モードを選択します。初期値は無効です。
Multicast Control Frame Count	CPU が処理したマルチキャスト制御フレーム数を表示します。
Interfaces Enabled for MLD Snooping	現在 MLD Snooping が有効であるインタフェースを表示します。MLD Snooping を有効にするためには、「インタフェース設定」（143 ページ）を参照してください。
Data Frames Forwarded by the CPU	CPU が送信したデータフレーム数を表示します。
VLAN Ids Enabled For MLD Snooping	MLD Snooping が有効な VLAN を表示します。MLD Snooping 用のインタフェースを有効にするためには、「インタフェース設定」（143 ページ）を参照してください。

「Enable」または「Disable」ボタンをクリックし、「Submit」ボタンをクリックして「Admin Mode」を有効または無効にします。
再起動後にも変更を保持するためには保存する必要があります。

インタフェース設定

特定のインタフェースに Snooping 設定を行います。

LAN タブ > L2 Features > MLD Snooping > Interface 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。

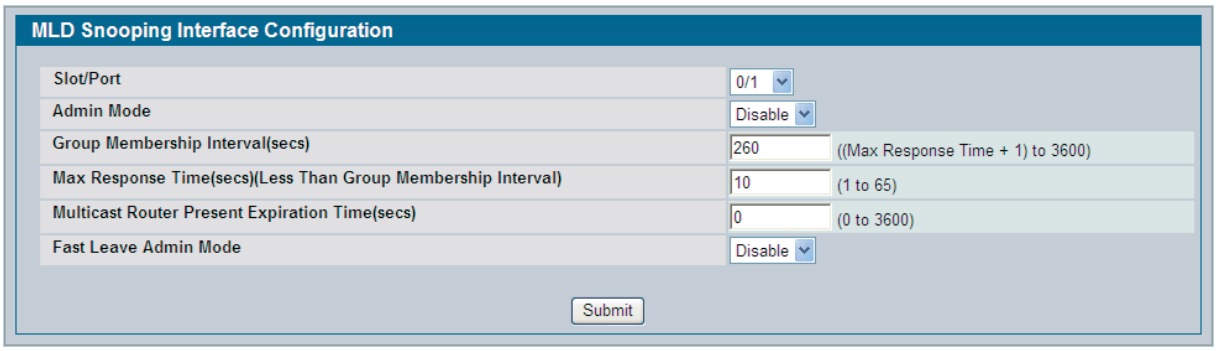


図 4-49　MLD Snooping Interface Configuration 画面

本画面には次の項目があります。

項目	説明
Slot/Port	設定する物理または LAG インタフェースを選択します。
Admin Mode	スイッチにおける MLD Snooping の選択インタフェースにおけるインタフェースモードを選択します。初期値は「Disable」(無効) です。
Group Membership Interval (secs)	グループからそのインタフェースを削除する前に、指定インタフェース上の指定グループのレポートをスイッチが待つ時間を指定します。有効範囲は 2-3600 (秒) です。初期値は 260 (秒) です。
Max Response Time (secs) (Less Than Group Membership Interval)	インタフェース上の指定グループのレポートを受信しなかったためにインタフェースにクエリを送信した後にスイッチが待機する時間を指定します。1 以上で「Group Membership Interval」より小さい値を入力します。初期値は 10 (秒) です。
Multicast Router Present Expiration Time (secs)	マルチキャストルータを持つインタフェースリストから削除する前に、インタフェース上のクエリの受信をスイッチが待つ時間 0-3600 (秒) を指定します。初期値は 0 (秒) です。0 は無限のタイムアウト、つまり期限がないことを示します。
Fast Leave Admin Mode	指定インタフェースの Fast Leave モードを選択します。初期値は「Disable」(無効) です。

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。

VLAN ステータス

MLD Snooping に設定されている VLAN に関する情報を参照します。

LAN タブ > Monitoring > MLD Snooping > VLAN 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。

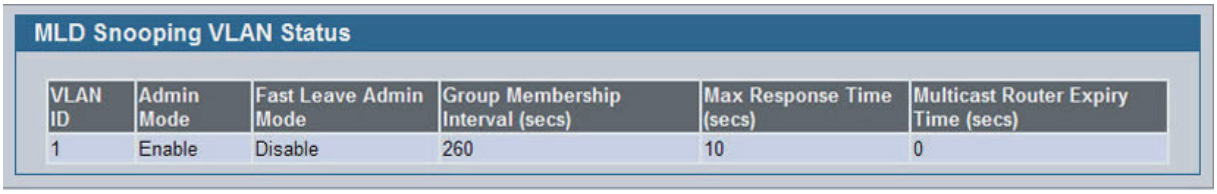


図 4-50　MLD Snooping VLAN Status 画面

本画面には次の項目があります。

項目	説明
VLAN ID	MLD Snooping モードが有効である VLAN ID を表示します。
Admin Mode	VLAN ID に対する MLD Snooping モードを表示します。
Fast Leave Admin Mode	MLD Snooping Fast-leave が VLAN でアクティブであるかどうかを表示しまします。
Group Membership Interval (secs)	エントリからインタフェースを削除する前に、VLAN に参加している指定インタフェース上の指定グループからのレポートをスイッチが待つ時間 (秒) を表示します。有効範囲は 2-3600 (秒) です。
Maximum Response Time (secs)	インタフェース上の指定グループのレポートを受信しなかったために VLAN に参加しているインタフェースにクエリを送信した後にスイッチが待機する時間を表示します。有効範囲は、1-3599 です。「Group Membership Interval」より大きい値を指定します。
Multicast Router Expiry Time (secs)	マルチキャストルータを持つインタフェースリストから VLAN に参加しているインタフェースを削除する前に待機する時間を表示します。クエリを受け取らないと、インタフェースは削除されます。有効範囲は 0-3600 です。

「Refresh」ボタンをクリックし、システムの情報を最新に更新します。

VLAN の設定

システムにおける VLAN に MLD Snooping 設定を行います。

LAN タブ > L2 Features > MLD Snooping > VLAN 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。

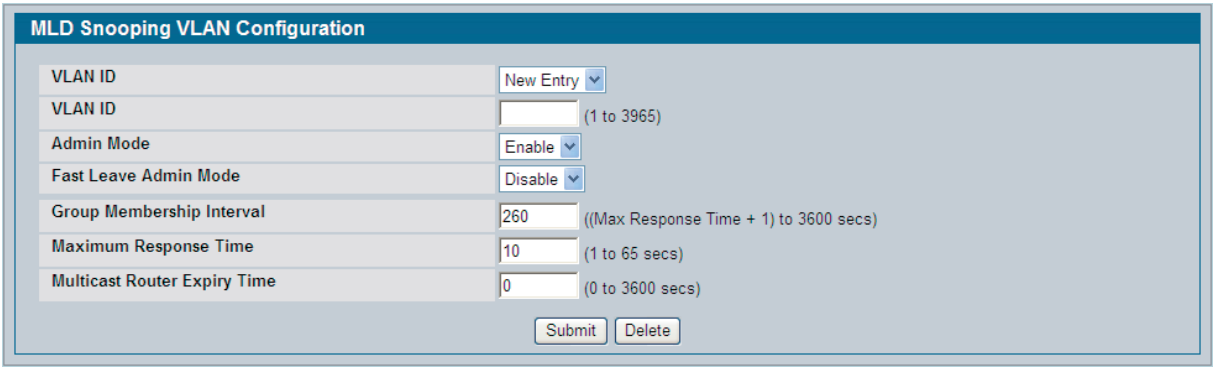


図 4-51　MLD Snooping VLAN Configuration 画面

本画面には次の項目があります。

項目	説明
VLAN ID	MLD Snooping が有効である VLAN ID を表示します。エントリが存在しない場合、「New Entry」が表示されます。MLD Snooping を設定する VLAN の VLAN ID を指定します。
Admin Mode	「Enable」のみ利用可能です。VLAN の MLD Snooping の admin モードを無効にするためには、「VLAN ID」から VLAN を選択し、「Delete」ボタンをクリックします。
Fast Leave Admin Mode	Fast Leave モードを有効にすると、インタフェースへの MAC ベースの汎用クエリを最初に送信しないで、マルチキャストグループの MLD Leave メッセージを受信するフォワーディングテーブルからレイヤ 2 の LAN インタフェースを直ちに削除することができます。1 台のホストだけが各レイヤ 2 の LAN ポートに接続している VLAN に fast-leave admin モードを有効にします。これは同じレイヤ 2 の LAN ポートに接続し、そのグループに向けられたマルチキャストトラフィックの受信を希望する他のホストをうかつに破棄してしまうことを防止します。
Group Membership Interval	エントリからインタフェースを削除する前に、指定インタフェース上の指定グループのレポートをスイッチが待つ時間を指定します。「Maximum Response Time」より大きい値を指定する必要があります。範囲は 2-3600（秒）です。
Maximum Response Time	インタフェース上の指定グループのレポートを受信しなかったためにインタフェースにクエリを送信した後にスイッチが待機する時間（秒）を指定します。この値は「Group Membership Interval」より小さい値とします。範囲は、1-65（秒）です。
Multicast Router Expiry Time	マルチキャストルータを持つインタフェースリストから削除される前に、インタフェースにクエリの受信をスイッチが待つ時間 0-3600（秒）を指定します。0 は無限のタイムアウト、つまり期限がないことを示します。

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。

Admin モードの無効化

VLAN の MLD Snooping の admin モードを削除するためには、「VLAN ID」から VLAN を選択し、「Delete」ボタンをクリックします。

マルチキャストルータ設定

スイッチがダイナミックに割り当てられているマルチキャストルータを学習することができます。または、マルチキャストルータインタフェースとしてスイッチポートを設定できます。

スタティックなマルチキャストルータインタフェースとしてインタフェースを設定します。

LAN タブ > L2 Features> MLD Snooping > Multicast Router 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。

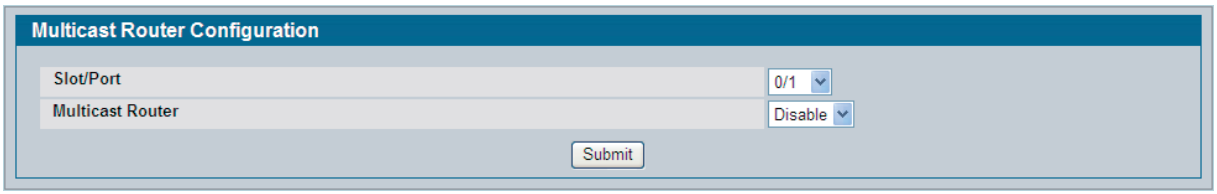


図 4-52　Multicast Router Configuration 画面

本画面には次の項目があります。

項目	説明
Slot/Port	設定する物理または LAG インタフェースを選択します。
Multicast Router	マルチキャストルータのステータスを設定します。 • Enabled - ポートは、マルチキャストルータインタフェースです。 • Disabled - ポートは、マルチキャストルータを設定しません。

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。

マルチキャストルータのステータス

選択ポートのマルチキャストルータ設定を参照します。

LAN タブ > Monitoring > MLD Snooping > Multicast Router 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。

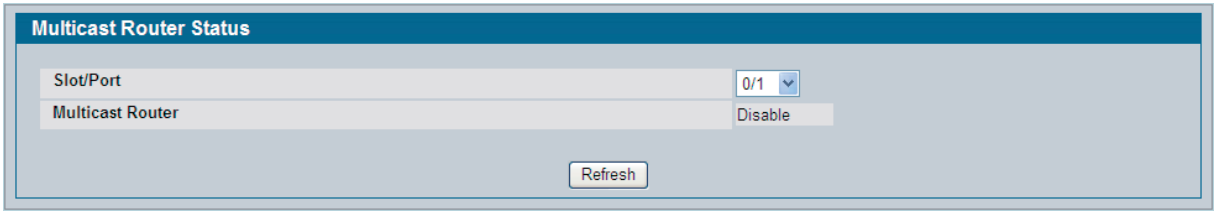


図 4-53　MLD Snooping Multicast Router Status 画面

本画面には次の項目があります。

項目	説明
Slot/Port	情報を参照するスロットとポートを選択します。
Multicast Router	指定インタフェースがマルチキャストルーティングを指定するように設定されているかどうかを表示します。

「Refresh」ボタンをクリックし、システムの情報を最新に更新します。

マルチキャストルータ VLAN 設定

インタフェース上の VLAN にマルチキャストルータ設定を行います。

LAN タブ > L2 Features > MLD Snooping > Multicast Router VLAN 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。

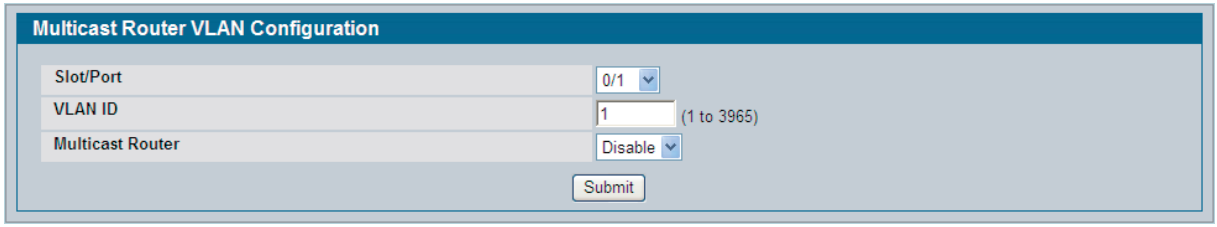


図 4-54　Multicast Router VLAN Configuration 画面

本画面には次の項目があります。

項目	説明
Slot/Port	設定する物理または LAG インタフェースを選択します。
VLAN ID	マルチキャストルーティングを有効または無効にする VLAN ID を入力します。
Multicast Router	「Enable」または「Disable」を選択し、このインタフェースに関連している VLAN のマルチキャストルータモードを変更します。

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。

マルチキャストルータ VLAN ステータス

指定インタフェース上の VLAN のマルチキャストルータ設定を参照します。

LAN タブ > Monitoring > MLD Snooping > Multicast Router VLAN 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。

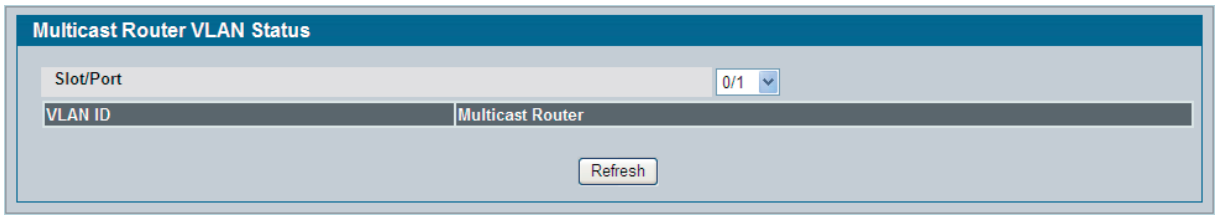


図 4-55　Multicast Router VLAN Status 画面

本画面には次の項目があります。

項目	説明
Slot/Port	表示する物理または LAG インタフェースを選択します。
VLAN ID	VLAN インタフェースでマルチキャストルーティングが有効な場合、ID を表示します。
Multicast Router	マルチキャストルータがインタフェースの VLAN で有効かどうかを表示します。

「Refresh」ボタンをクリックし、システムの情報を最新に更新します。

MLD Snooping クエリア

IPv6 環境において、MLD Snooping は、ネットワークにおける中央スイッチまたはルータがマルチキャストメンバシップを通知するために定期的にすべての端末にクエリを送信することが必要です。この中央デバイスが「MLD クエリア」です。MLD レポートとして知られている MLD クエリの応答は、ポートごとに現在のマルチキャストグループメンバシップと共に更新されたスイッチを保持します。スイッチは、更新後のメンバシップ情報をすぐに受け取らないと、端末が位置するポートにマルチキャストを送信することを中止します。

ネットワーク上の、および VLAN ごとの MLD Snooping クエリアに関する情報を設定、および表示することができます。

MLD Snooping クエリアの設定

MLD Snooping クエリア機能の有効 / 無効化、クエリを実行するルータの IP アドレスの指定し、および関連するパラメータの設定を行います。本画面のデータを変更するためには、ユーザは Read/Write のアクセス権を持つ必要があります。

LAN タブ > L2 Features > MLD Snooping Querier > MLD Snooping Querier 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。

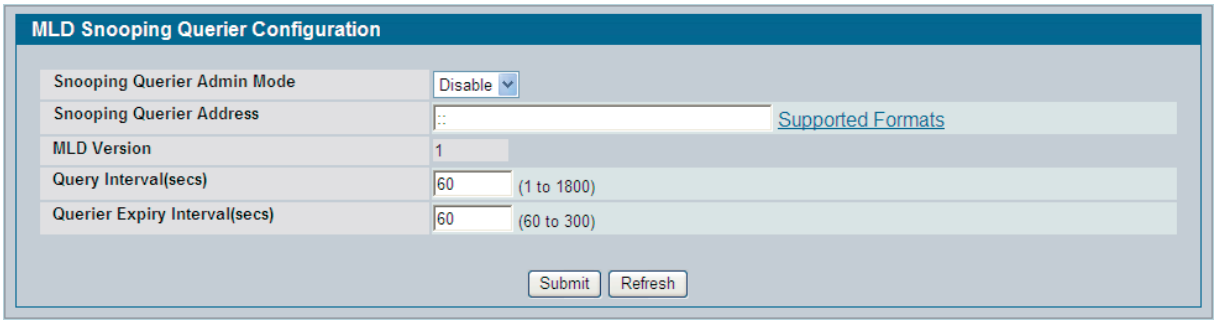


図 4-56　MLD Snooping Querier Configuration 画面面

本画面には次の項目があります。

項目	説明
Snooping Querier Admin Mode	スイッチのおける MLD Snooping の管理モードを選択します。初期値は「Disable」(無効) です。
Snooping Querier Address	送信元 IPv6 アドレスとして定期的な MLD クエリに使用される Snooping クエリアアドレスを指定します。アドレスがクエリが送信される VLAN に設定されていない場合に、このアドレスが使用されます。
MLD Version	定期的な MLD クエリに使用される MLD プロトコルバージョンを指定します。
Query Interval (secs)	Snooping クエリアが送信する定期的なクエリの間隔 1-1800 (秒) を表示します初期値は 60 (秒) です。
Querier Expiry Interval (secs)	最後のクエリア情報の削除の間隔 60-300 (秒) を指定します。初期値は 60 (秒) です。

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。「Refresh」ボタンをクリックし、システムの情報を最新に更新します。

MLD Snooping クエリア VLAN 設定

ネットワーク上の VLAN と共に使用する MLD クエリアを設定します。

LAN タブ > L2 Features > MLD Snooping Querier > Querier VLAN 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。

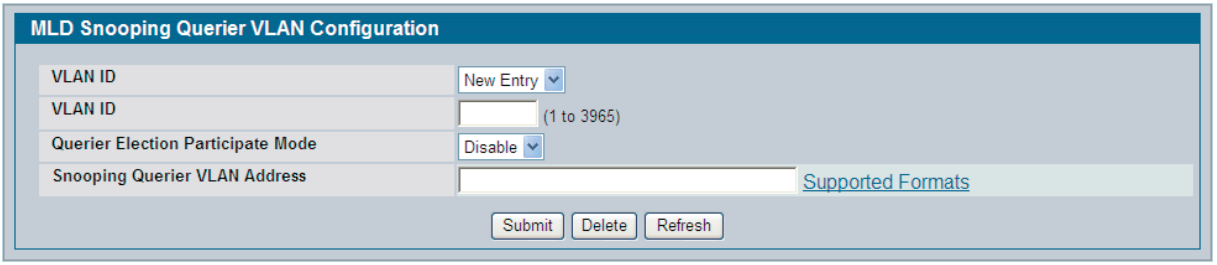


図 4-57　MLD Snooping Querier VLAN Configuration 画面

本画面には次の項目があります。

項目	説明
VLAN ID	MLD Snooping クエリアが有効である VLAN ID を表示します。「NewEntry」を選択して、MLD Snooping 用にのために新しい VLAN ID を作成します。
Querier Election Participate Mode	「Querier Participate」モードを有効または無効にします。このモードが無効であると、VLAN 内の同じバージョンの別のクエリを参照する場合に Snooping クエリアは non-querier 状態に移行します。有効であると、Snooping クエリアはクエリアの選出に参加します。その場合、最小 IP アドレスがその VLAN においてクエリアとして動作します。もう一方のクエリアは non-querier 状態に移行します。
Snooping Querier VLAN Address	指定 VLAN に送信される定期的な MLD クエリ内の送信元 IP アドレスとして使用されるアドレスを指定します。

Snooping クエリアの関連モードの設定または変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。「Refresh」ボタンをクリックし、システムの情報を最新に更新します。

クエリアの削除

ネットワークからクエリアを削除するためには、「VLAN ID」を選択し、「Delete」ボタンをクリックします。

MLD Snooping クエリア VLAN 設定のサマリ

ネットワークにおける VLAN に対する MLD snooping クエリアのサマリ情報を参照します。

LAN タブ > Monitoring > MLD Snooping Querier > Querier VLAN Configuration 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。

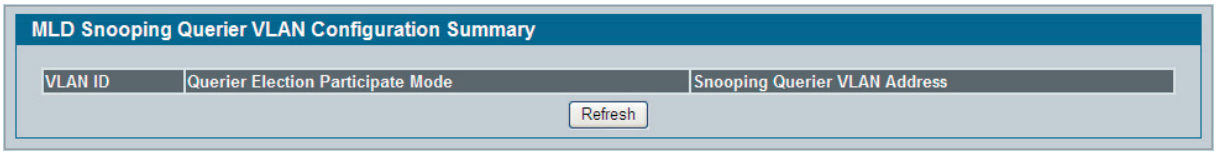


図 4-58　MLD Snooping Querier VLAN Configuration Summary 画面

本画面には次の項目があります。

項目	説明
VLAN ID	MLD Snooping クエリアが管理上有効である VLAN ID を表示します。
Querier Election Participate Mode	VLAN における「Participate Mode」を表示します。本モードが無効であると、VLAN 内の同じバージョンの別のクエリを参照する場合に Snooping クエリアは non-querier 状態に移行します。有効であると、Snooping クエリアはクエリアの選出に参加します。その場合、最小 IP アドレスがその VLAN においてクエリアとして動作します。もう一方のクエリアは non-querier 状態に移行します。
Snooping Querier VLAN Address	指定 VLAN に送信される定期的な MLD クエリ内の送信元 IPv6 アドレスとして使用されるアドレスを指定します。

「Refresh」ボタンをクリックし、システムの情報を最新に更新します。

MLD Snooping クエリア VLAN ステータス

ネットワーク上の VLAN に対する MLD snooping クエリアの操作状態などの情報を参照します。

LAN タブ > Monitoring > MLD Snooping Querier > Querier VLAN 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。

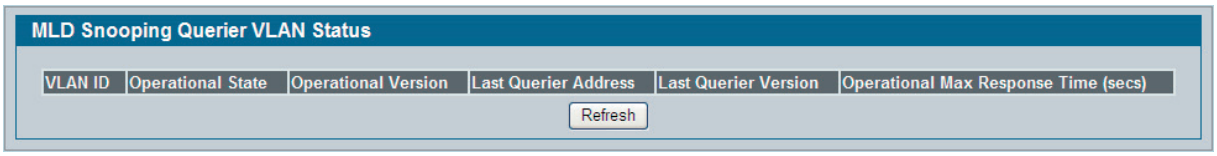


図 4-59　MLD Snooping Querier VLAN Status 画面

本画面には次の項目があります。

項目	説明
VLAN ID	MLD Snooping クエリアが管理上有効であり、VLAN データベースに存在する VLAN ID を表示します。
Operational State	VLAN 上の MLD Snooping クエリアの動作状態を表示します。 • Querier - Snooping スイッチは VLAN のクエリアです。Snooping スイッチは、設定したクエリアのクエリ間隔と等しい間隔で定期的なクエリを送信します。Snooping スイッチが VLAN 内により適切なクエリア（数字が低い方）を見つけると、non-querier モードに移行します。 • Non-Querier - Snooping スイッチが VLAN において non-querier モードです。クエリアのタイマが期限切れとなると、Snooping スイッチは querier モードに移行します。 • Disabled - Snooping クエリアは VLAN では操作されません。MLD Snooping が VLAN で操作可能でない場合、クエリアアドレスが設定されていない場合、またはネットワーク管理アドレスが設定されていない場合に Snooping クエリアは無効モードに移行します。
Operational Version	操作可能なクエリアの MLD プロトコルバージョンを表示します。
Last Querier Address	クエリが VLAN でスヌープされた最後のクエリアの IP アドレスを表示します。
Last Querier Version	クエリが VLAN でスヌープされた最後のクエリアの MLD プロトコルバージョンを表示します。
Operational Max Response Time (secs)	Snooping クエリアが送信するクエリに使用される最大の応答時間を表示します。

「Refresh」ボタンをクリックし、システムの情報を最新に更新します。

ポートチャンネル（トランキング）の作成

リンクアグリゲーション（LAG）として知られるポートトランキングは、複数のフルデュプレックスのイーサネットを 1 つの論理リンクに束ねることができます。ネットワーク装置はそれを単一のリンクであるかのように扱います。これは、フォールトトレラントを増強し、負荷分散を提供します。ポートトランンキングの作成後にポートチャンネル（LAG）に VLAN メンバシップを割り当てます。ポートチャンネルは初期状態で管理 VLAN のメンバになっています。

ポートトランキング（LAG）インタフェースは、スタティック、ダイナミックのいずれかで、両方であることはできません。ポートチャンネルのすべてのメンバは同じプロトコルに参加する必要があります。スタティックなポートトランクインタフェースでは、パートナーシステムがメンバポートを集約する必要はありません。

注意 ご使用のプラットフォームがサポートするダイナミックなポートチャンネル（LAG）の最大数を設定すると、設定する追加のポートチャンネルは、自動的にスタティックとなります。

スタティックな LAG をサポートしています。ポートがスタティックなメンバとして LAG に追加される場合、LACPDU の送信も受信もしません。

ポートチャンネル設定

複数のフルデュプレックスのイーサネットリンクをグループ化し、1 つのポートチャンネルを形成するように集約します。これは、リンクアグリゲーション（LAG）として知られています。スイッチはまるでそれが単一のリンクであるかのようにポートチャンネルを扱います。

LAN タブ > L2 Features > Trunking > 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。

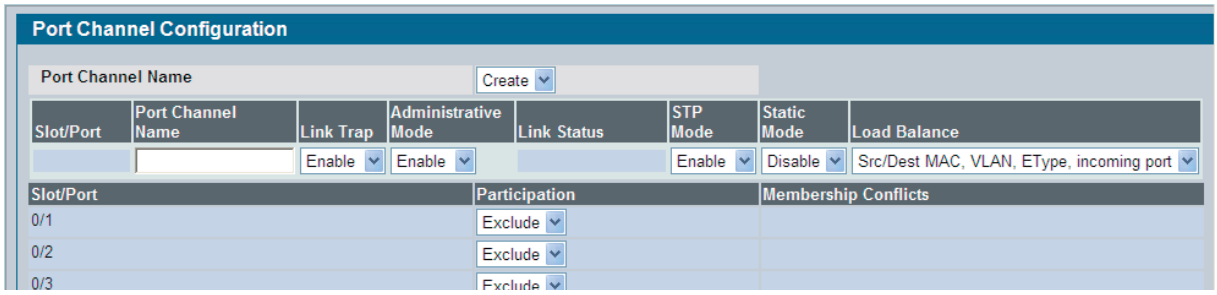


図 4-60　Port Channel Configuration 画面

本画面には次の項目があります。

項目	説明
Port Channel Name	新しいポートチャンネルの設定するためには「Create」を選択します。または設定を編集するためにインタフェースおよび名前で特定される既存のポートチャンネルを選択します。ポートチャンネルの最大数はプラットフォームに依存しています。
Slot/Port	設定を行うインタフェースを表示します。新しい Port Channel を設定する場合には、本欄は表示されません。
Port Channel Name	ポートチャンネルに割り当てる名称を入力します。15 文字までの半角英数字を入力します。
Link Trap	リンクステータスが変更した場合にトラップを送信するかどうかを指定します。初期値は有効で、トラップを送信します。
Administrative Mode	「Enable」または「Disable」を選択します。Port Channel が無効な場合、トラフィックはフローせず、LACPDU 破棄されますが、Port Channel を形成するリンクは解放されません。初期値は「Enable」（有効）です。
Link Status	リンクステータス「Up」（アクティブ）または「Down」（ダウン）を表示します。
STP Mode	ポートチャンネルに関連付ける STP（Spanning Tree Protocol）管理モードを設定します。 • Disable - このポートチャンネルに対して STP を無効にします。 • Enable - このポートチャンネルに対して STP を有効にします。
Static Mode	「Enable」または「Disable」を選択します。 • Enable - ポートチャンネルがスタティックに保持されます。つまり、ポートチャンネルは受信した LAGPDU の送信または処理を行いません。メンバポートは LAGPDU を転送せず、受信する可能のあるすべての LAGPDU は破棄されます。スタティックなポートトランクインタフェースでは、パートナーシステムがメンバポートを集約する必要はありません。 • Disable - ポートチャンネルはダイナミックに維持されます。インタフェースは、LAGPDU の送信および処理を行い、パートナシステムを必要とします。（初期値）
Load Balance	LAG で利用可能な物理ポートでトラフィックの負荷を分散するのに使用されるハッシュアルゴリズムを選択します。 スイッチのタイプによって、可能な値の範囲は異なります。 • Src MAC, VLAN, EType, incomming port • Dest MAC, VLAN, EType, incomming port • Src/Dest MAC, VLAN, EtherType, incomming port • Src IP and Src TCP/UDP Port field • Dest IP and Dest TCP/UDP Port field • Src/Dest IP and TCP/UDP Port field

項目	説明
Port Channel Members	複数のポートチャンネルの作成後に、本欄は「Slot/Port」インタフェースの形式で「Port Channel」のメンバを表示します。システム上にポートチャンネルがないと、表示されません。
Slot/Port	システムで利用可能な物理ポートを表示します。
Participation	設定しているポートチャンネルに各ポートのメンバシップステータスを選択します。ポートチャンネルに割り当てられる最大 8 個のポートが可能です。 • Include - ポートはポートチャンネルに参加します。 • Exclude - ポートはポートチャンネルに参加しません。（初期値）
Membership Conflicts	既に他のポートチャンネルのメンバであるポートを表示します。ポートは、同時に 1 つのポートチャンネルのメンバだけになります。エントリが空白であると、ポートは現在どのポートチャンネルのメンバでもありません。

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。

ポートチャンネルの削除

ポートチャンネルを削除するためには、「Port Channel Name」から削除する名前を選択し、「Delete」ボタンをクリックします。このポートチャンネルのメンバであるすべてのポートが、ポートチャンネルから削除され、デフォルト VLAN に含まれます。新しいポートチャンネルを作成する場合には、本欄は表示されません。

ポートチャンネルステータス

ポートチャンネルのステータスを表示します。

LAN タブ > Monitoring > Trunking > 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。

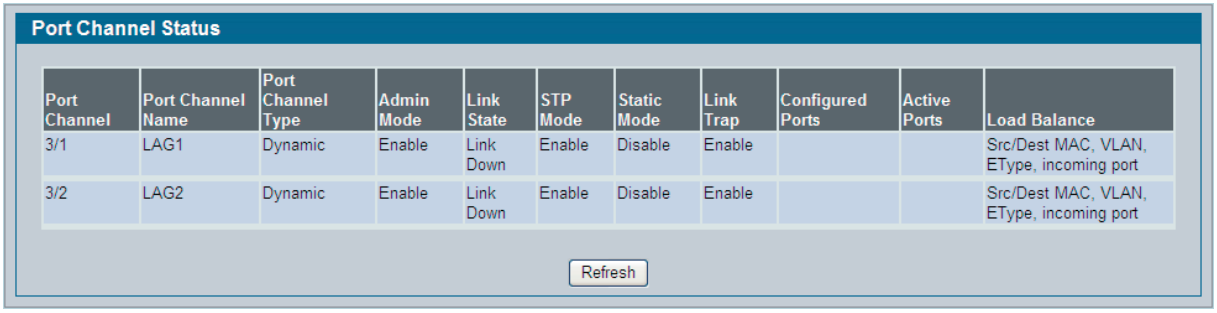


図 4-61　Port Channel Status 画面

本画面には次の項目があります。

項目	説明
Port Channel	「Slot/Port」インタフェースの形式でポートチャンネルを表示します。
Port Channel Name	ユーザ定義のポートチャンネル名を示します。
Port Channel Type	ポートチャンネルのタイプは以下のモードの 1 つです。 • Static - ポートチャンネルはスタティックに維持されます。 • Dynamic - ポートチャンネルはダイナミックに維持されます。
Admin Mode	「Enable」または「Disable」を選択します。Port Channel が無効な場合、トラフィックはフローせず、LACPDU 破棄されますが、ポートチャンネルを形成するリンクは解放されません。初期値は「Enable」（有効）です。
Link State	リンクステータス「Up」（アクティブ）または「Down」（ダウン）を表示します。
STP Mode	STP（Spanning Tree Protocol）管理モードがポートチャンネルにおいて有効または無効であるかを表示します。
Static Mode	スタティックモードがこのポートチャンネルで有効かどうかを表示します。
Link Trap	リンクステータスが変更した場合にトラップを送信するかどうかを表示します。ステータスが有効な場合、トラップを送信します。
Configured Ports	「Slot/Port」インタフェースの形式でポートチャンネルのメンバであるポートを表示します。ポートチャンネルに割り当てられる最大 8 個のポートが可能です。
Active Ports	このポートチャンネルに参加しているアクティブなメンバであるポートを「Slot/Port」形式で表示します。
Load Balance	LAG で利用可能な物理ポートでトラフィックの負荷を分散するのに使用されるハッシュアルゴリズムを表示します。スイッチのタイプによって、可能な値の範囲は異なります。 • Src MAC, VLAN, EType, incomming port • Dest MAC, VLAN, EType, incomming port • Src/Dest MAC, VLAN, EtherType, incomming port • Src IP and Src TCP/UDP Port field • Dest IP and Dest TCP/UDP Port field • Src/Dest IP and TCP/UDP Port field

マルチキャストフォワーディングデータベース情報の参照

スイッチは、レイヤ 2 マルチキャストフォワーディングデータベース（MFDB）を使用して、マルチキャスト宛先 MAC アドレスを持つ到着パケットに転送の決定を行います。マルチキャストをスイッチの特定ポートだけに制限することで、そのトラフィックが不要であるネットワークの部分にトラフィックが向かうことを防止します。

パケットをスイッチに入力する時に、宛先 MAC アドレスは VLAN ID に組み合わされて、レイヤ 2 マルチキャストフォワーディングデータベースで検索が実行されます。一致するものがないと、スイッチの設定に従って、パケットを VLAN のすべてのポートにフラッドするか、または破棄します。一致するものがあれば、そのマルチキャストグループのメンバであるポートにだけパケットを送信します。

マルチキャストフォワーディング機能には以下の設定があります。

- MFDB テーブル
- MFDB GMRP テーブル
- MFDB IGMP Snooping テーブル
- MFDB の統計情報

MFDB テーブル

アクティブなマルチキャストアドレスエントリすべてのポートメンバシップ情報を参照します。主なエントリは VLAN ID と MAC アドレスのペアから構成されます。エントリには 1 つ以上のプロトコル用のデータを含みます。

LAN タブ > Monitoring > Multicast Forwarding Database > MFDB 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。

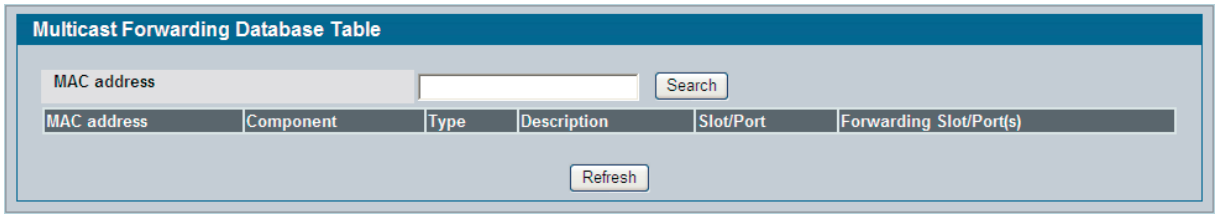


図 4-62　Multicast Forwarding Database Table 画面

本画面には次の項目があります。

項目	説明
MAC address	表示する MFDB テーブルエントリの VLAN ID/MAC アドレスのペアを入力します。2 桁ずつ「:」（コロン）で区切った 8 個の 16 進数（例 : 00:01:23:43:45:67:89:AB）を入力します。最初の 2 つの 2 桁の 16 進数が VLAN ID で、残りの数字が MAC アドレスです。次に「Search」ボタンをクリックします。アドレスが存在していると、そのエントリを表示します。完全な一致が必要とされます。
MAC address	データをリクエストしたマルチキャスト MAC アドレス。
Component	マルチキャストフォワーディングデータベースにおけるこのエントリに関連するコンポーネント（MLD Snooping、GMRP、IGMP Snooping、および Static Filtering）です。
Type	エントリのタイプを表示します。スタティックなエントリは、エンドユーザによって設定されるものです。 ダイナミックエントリは、学習処理またはプロトコルの結果、テーブルに追加されます。
Description	このマルチキャストテーブルエントリを説明する文字列（Management Configured、Network Configured、および Network Assisted）。
Slot/Port	選択アドレスへのフォワーディング（Fwd）およびフィルタリング（Flt）用に指定されているインタフェースのリスト。
Forwarding Slot/Port(s)	すべてのフォワーディングインタフェースの組み合わせ、およびスタティックなフィルタリングインタフェースとして表示されるインタフェースの削除からフォワーディングリストが結果として取得されます。

「Refresh」ボタンをクリックしてと、画面の情報を現在のデータで更新します。

リストがスキャンできないほど長い場合、MAC アドレスを検索するためには、MAC アドレスを 16 進形式で入力し、「Search」ボタンをクリックします。

MFDB GMRP テーブル

GARP Multicast Registration プロトコルのために作成されたマルチキャストフォワーディングデータベース内のすべてのエントリを参照します。

LAN タブ > Monitoring > Multicast Forwarding Database > GMRP 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。

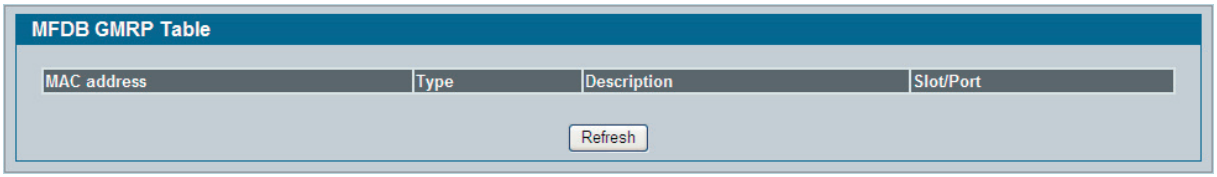


図 4-63　MFDB GMRP Table 画面

本画面には次の項目があります。

項目	説明
MAC address	スイッチが転送および（または）フィルタした情報用の VLAN ID/ マルチキャスト MAC アドレスのペア。 形式は 2 桁ずつ「:」（コロン）で区切った 8 個の 16 進数（例 : 00:01:23:45:67:89:AB:CD）です。
Type	エントリのタイプを表示します。スタティックなエントリは、エンドユーザによって設定されるものです。 ダイナミックエントリは、学習処理またはプロトコルの結果、テーブルに追加されます。
Description	このマルチキャストテーブルエントリを説明する文字列（Management Configured、Network Configured、および Network Assisted）。
Slot/Port	関連するアドレスへのフォワーディング（Fwd）およびフィルタリング（Flt）用に指定されているインタフェースのリスト。

「Refresh」ボタンをクリックしてと、画面の情報を更新します。

MFDB IGMP Snooping テーブル

IGMP Snooping に設定されているマルチキャストフォワーディングデータベース内のすべてのエントリを参照します。

LAN タブ > Monitoring > Multicast Forwarding Database > IGMP Snooping 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。

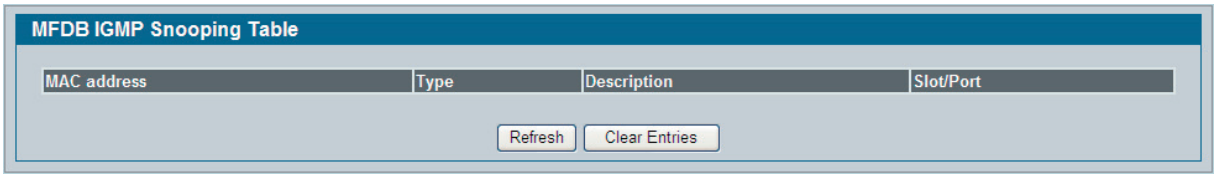


図 4-64　IGMP Snooping Table 画面

本画面には次の項目があります。

項目	説明
MAC address	スイッチが転送および（または）フィルタした情報用の VLAN ID/ マルチキャスト MAC アドレスのペア。 形式は 2 桁ずつ「:」（コロン）で区切った 8 個の 16 進数（例 : 00:01:23:45:67:89:AB:CD）です。
Type	エントリのタイプを表示します。スタティックなエントリは、エンドユーザによって設定されるものです。 ダイナミックエントリは、学習処理またはプロトコルの結果、テーブルに追加されます。
Description	このマルチキャストテーブルエントリを説明する文字列（Management Configured、Network Configured、および Network Assisted）。
Slot/Port	関連するアドレスへのフォワーディング（Fwd）およびフィルタリング（Flt）用に指定されているインタフェースのリスト。

「Refresh」ボタンをクリックしてと、画面の情報を更新します。

エントリの削除

「Clear Entries」ボタンをクリックして、マルチキャストフォワーディングデータベースからすべてのエントリを削除します。

MFDB の統計情報

MFDB テーブルに関する統計情報を参照します。

LAN タブ > Monitoring > Multicast Forwarding Database > 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 4-65　Multicast Forwarding Database Statistics 画面

本画面には次の項目があります。

項目	説明
Max MFDB Table Entries	マルチキャストフォワーディングデータベーステーブルが保持できる最大エントリ数を表示します。
Most MFDB Entries Since Last Reset	最後の再起動後にマルチキャストフォワーディングデータベーステーブルに存在している最大エントリ数。この値は、MFDB のハイウォータマスクとして知られています。
Current Entries	マルチキャストフォワーディングデータベーステーブルの現在のエントリ数を表示します。

「Refresh」ボタンをクリックしてと、画面の情報を現在のデータで更新します。

スパニングツリープロトコルの設定

スパニングツリープロトコル（STP）はブリッジの配置に関係なくツリー型トポロジを提供します。また、STP はループを排除して、ネットワークにおけるエンドステーション間に 1 つの経路を提供します。サポートするスパニングツリーのバージョンには、Common STP、Multiple STP、および Rapid STP があります。

標準的な STP はエンドステーション間にループの回避または排除を行う 1 つの経路を提供します。一般的な STP 設定に関する情報は、CST Port Configuration/Status（MST ポート設定 / ステータス）を参照してください。

MSTP（Multiple Spanning Tree Protocol ）は、VLAN トラフィックを異なるインタフェースに効率よく切り替えるためにスパニングツリーの複数のインスタンスをサポートしています。スパニングツリーの各インスタンスは、動作中にわずかな変更があっても、IEEE 802.1w Rapid Spanning Tree（RSTP）で指定される方法で動作します。主な効果は、ポートの状態を「Forwarding」に素早く遷移することです。RSTP と従来の STP（IEEE 802.1D）の違いは、エンドステーションに接続するポートの設定、フルデュプレックス接続の認識です。そのため、ポートを「Forwarding」状態に素早く遷移させたり、トポロジ変更通知（TCN）を抑制できます。これらの機能はパラメータ「pointtopoint」と「edgeport」で表されます。MSTP は RSTP と STP の両方に互換性があります。それは STP と RSTP ブリッジに対して適切に動作します。完全に RSTP ブリッジまたは STP ブリッジとして動作するように MSTP ブリッジを設定できます。

注意 2 つブリッジが同じ領域にあるためには、行使するバージョンは 802.1S であるべきで、それらの設定名、ダイジェストキー、およびリビジョンレベルは一致する必要があります。範囲に関する詳しい情報とネットワークトポロジへの影響については、IEEE 802.1Q 標準を参照してください。

スパニングツリーには以下の設定があります。

- スイッチの設定 / ステータス
- CST 設定 / ステータス
- MST 設定 / ステータス
- MST ポート設定 / ステータス
- MST ポート設定 / ステータス
- 統計情報

スイッチの設定

スイッチにおける STP を有効にします。

LAN タブ > L2 Features > Spanning Tree > Switch Configuration 順にメニューをクリックし、以下の画面を表示します。

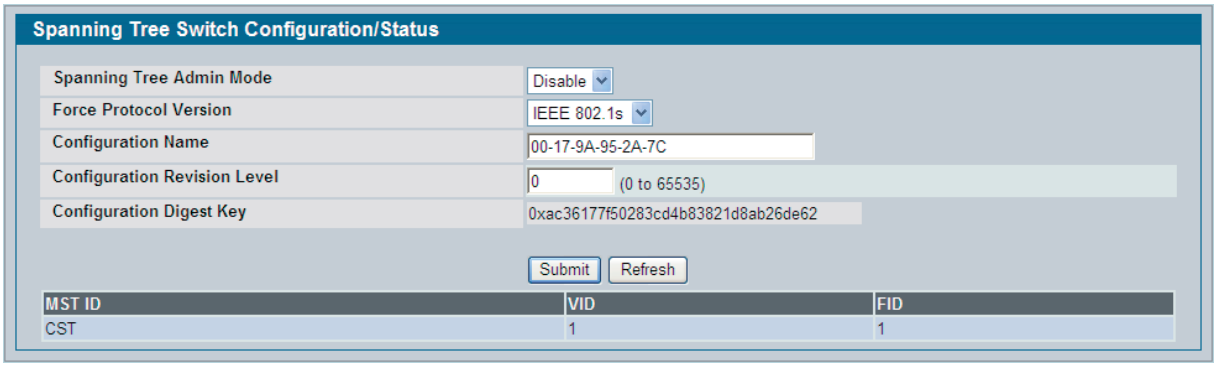


図 4-66　Spanning Tree Switch Configuration/Status 画面

本画面には次の項目があります。

項目	説明
Spanning Tree Admin Mode	スイッチの STP を有効または無効にします。
Force Protocol Version	スイッチに Force プロトコルバージョンパラメータを指定します。 • IEEE 802.1d - Spanning Tree Protocol（STP） • IEEE 802.1w - Rapid Spanning Tree Protocol（RSTP） • IEEE 802.1s - Multiple Spanning Tree Protocol（MSTP）
Configuration Name	現在使用されている設定を識別するために使用される名称。半角英数字 32 文字以内。
Configuration Revision Level	現在使用されている設定を識別するために使用される番号。許可される値は 1-65535 です。初期値は 0 です。
Configuration Digest Key	現在使用されている設定を識別するために使用されるキー。ダイジェストキーは異なるインスタンスに関連する VLAN に基づいて生成されます。ダイジェストキーが確実に 2 つの異なるスイッチで同じであるために、VLAN とインスタンスのマッピングが同じである必要があります。
MST ID	現在スイッチに設定されている MST ID を表示します。相互に関連する MST インスタンス（CST を含む）と対応する VLAN で構成されるテーブル。
VID	この MSTI ID に設定される VID を表示します。テーブルは、VLAN 識別子（VID）と各 VID に関連している対応するフィルタリング識別子（FID）から構成されています。
FID	フィルタリング識別子を表示します。

「Submit」ボタンをクリックし、変更をスイッチに適用します。「Refresh」ボタンをクリックして画面の情報を現在のデータで更新します。

CST 設定 / ステータス

CST（Common Spanning Tree）と Internal Spanning Tree を設定します。

LAN タブ > L2 Features > Spanning Tree > CST 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。

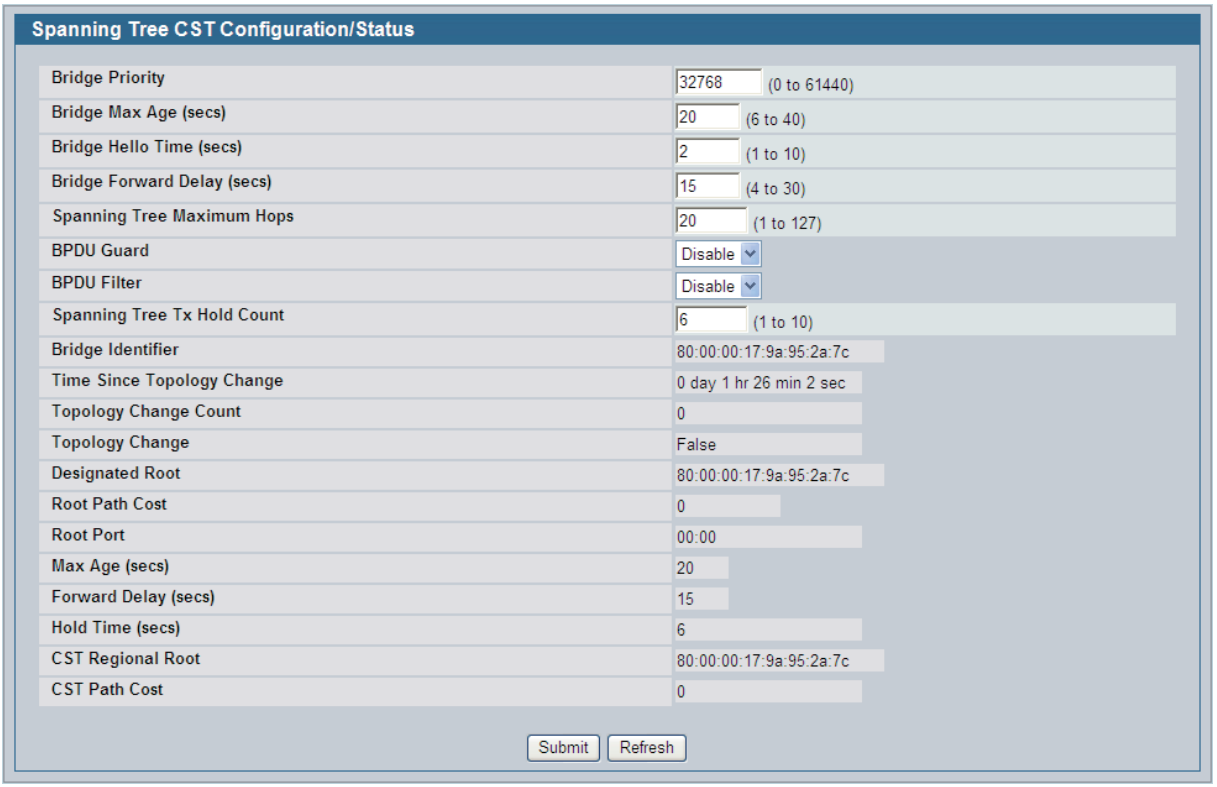


図 4-67　Spanning Tree CST Configuration/Status 画面

本画面には次の項目があります。

項目	説明
Bridge Priority	ブリッジの優先度を指定します。スイッチまたはブリッジが STP を実行している場合、それぞれに優先度が割り当てられます。BPDU の交換後に、最も低い優先度を持つスイッチがルートブリッジとなります。 ブリッジの優先度は 4096 の倍数です。4096 の倍数でない優先度を指定すると、優先度は自動的に 4096 の倍数ある次に低い優先度に設定されます。例えば、優先度が 0-4095 間の任意の値に設定しようとすると、0 に設定されます。優先度の初期値は 32768 です。有効な範囲は 0-61440 です。
Bridge Max Age (secs)	スイッチの最大エージング時間を指定します。これは、トポロジ変更の実行前にブリッジが待機する時間（秒）を示します。有効範囲は 6-40 で、値は「(2 * Bridge Forward Delay) -1」以下で「2 * (Bridge Hello Time +1)」以上です。初期値は 20 です。
Bridge Hello Time (secs)	スイッチの Hello タイムを指定します。これは、構成メッセージ間にルートブリッジが待機する時間（秒）を示します。範囲は 1-10 で、初期値は 2 です。値は「(Bridge Max Age / 2) - 1」以下とします。
Bridge Forward Delay (secs)	スイッチのフォワード遅延時間を指定します。これは、パケットの転送前にブリッジが「listening」と「learning」状態に置かれる時間（秒）を示します。値は「(Bridge Max Age / 2) + 1」以上とします。時間の範囲は 4-30（秒）です。初期値は 15（秒）です。
Spanning Tree Maximum Hops	破棄される前に特定の CST インスタンスの情報が移動できるブリッジの最大ホップ数を指定します。
BPDU Guard	BPDU ガードを有効または無効にします。BPDU ガードが有効であるエッジポートの背後にあるスイッチは全般的な STP トポロジに影響を及ぼすことができません。BPDU ガード機能を使用すると、STP ドメイン境界を強制し、アクティブなトポロジを一貫性があり予測可能な状態に保つことができます。
BPUD Filter	BPDU フィルタを有効または無効にします。BPDU フィルタリングを有効にすると、ポートは受信した BPDU を破棄します。
Spanning Tree Tx Hold Count	ブリッジが Hello タイム以内に送信を許可される BPDU の最大数を設定します。初期値は 6 です。
Bridge Identifier	CST のためのブリッジ識別子。ブリッジ優先度とブリッジのベース MAC アドレスを使用することで作成されます。
Time Since Topology Change	最後にトポロジの変更した後の時間を表示します。この時間は、hour/minute/second の形式（例 5 hours 10 minutes and 4 seconds）で表示されます。
Topology Changes Count	発生した STP の状態変更の総量を表示します。
Topology Change	トポロジ変更が CST に割り当てられたどのポートにも進行中であることを示します。 有効な値は「True」または「False」です。
Designated Root	ルートブリッジのブリッジ優先度を表示します。これは、ブリッジ優先度とブリッジのベース MAC アドレスから作成されます。
Root Path Cost	ブリッジから指名されたルートまでパスコストを表示します。
Root Port	選択されたインスタンスのルートポートを示します。
Max Age (secs)	CST の指名ルートまでのパスコストを示します。
Forward Delay (secs)	ルートポートブリッジの送信遅延を示します。
Hold Time (secs)	BPDU 伝送間の最短時間を示します。
CST Regional Root	CST Regional Root の優先度と MAC アドレスを示します。
CST Path Cost	CST ツリーの Regional Root へのパスコストを示します。

MST 設定

MST（Multiple Spanning Tree）を設定します。

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

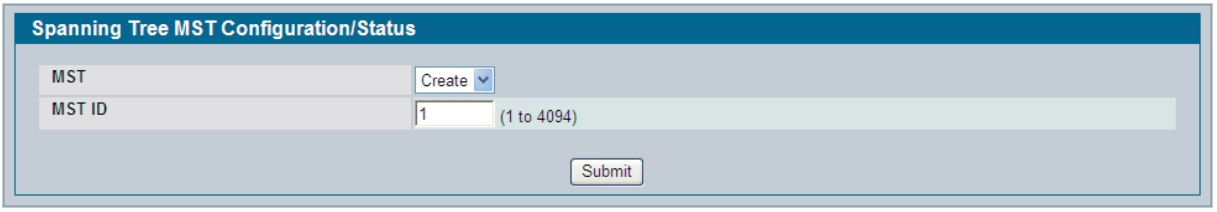


図 4-68　Spanning Tree MST Configuration/Status 画面

MST インスタンスが存在しない場合、または「MST」から「Create」を選択して「Submit」ボタンを押すと、以下の画面が表示されます。

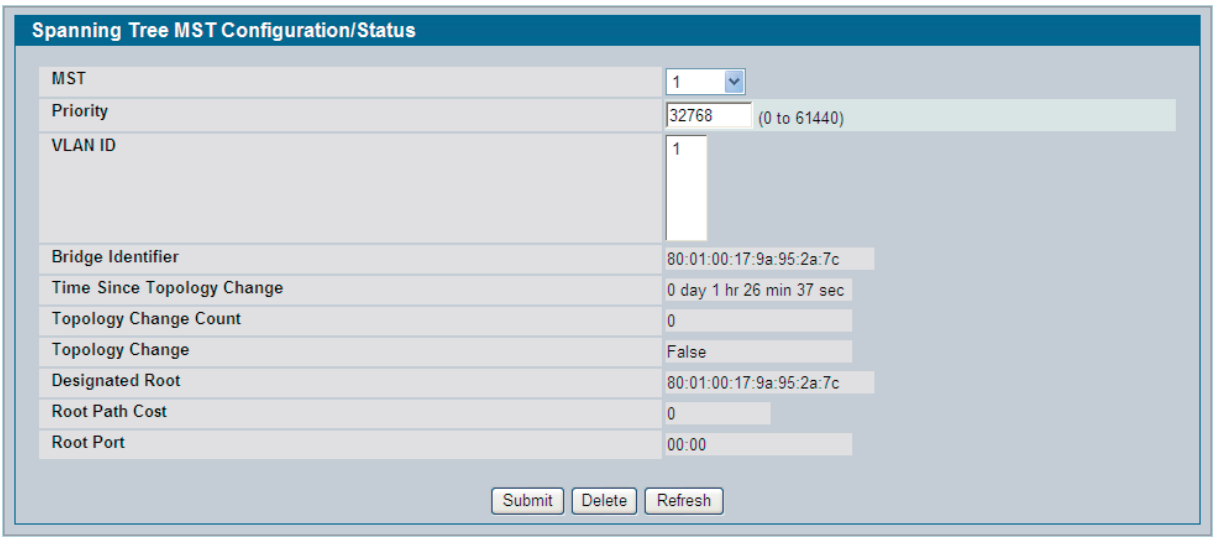


図 4-69　Spanning Tree MST Configuration/Status 画面

本画面には次の項目があります。

項目	説明
MST	新しい MST の作成および設定、または表示、設定を行う既存の MST を選択します。
MST ID	「MST」から「Create」が選択した時だけ表示されます。作成す MST の ID（1-4094）を指定します。
Priority	MST のブリッジ優先度値を指定します。スイッチまたはブリッジが STP を実行している場合、それぞれに優先度が割り当てられます。BPDU の交換後に、最も低い優先度を持つスイッチがルートブリッジとなります。 ブリッジの優先度は 4096 の倍数です。4096 の倍数でない優先度を指定すると、優先度は自動的に 4096 の倍数ある次に低い優先度に設定されます。例えば、優先度が 0-4095 間の任意の値に設定しようとすると、0 に設定されます。優先度の初期値は 32768 です。有効な範囲は 0-61440 です。
VLAN ID	MST インスタンスに対する VLAN の対応付けを再設定するために選択または選択解除をします。スイッチ上のすべての VLAN ID のリストボックスを表示します。選択される MST インスタンスに関連している VLAN はリストで強調表示されます。
Bridge Identifier	選択した MST インスタンスのためのブリッジ識別子を表示します。ブリッジ優先度とブリッジのベース MAC アドレスを使用することで作成されます。
Time Since Topology Change	最後にトポロジの変更した後の総時間を表示します。この時間は、hour/minute/second の形式（例 5 hours 10 minutes and 4 seconds）で表示されます。
Topology Changes Count	発生した MSTP の状態変更の総量を表示します。
Topology Change	トポロジ変更が CST に割り当てられたどのポートにも進行中かどうかを示します。有効な値は「True」または「False」です。
Designated Root	ルートブリッジのブリッジ優先度を表示します。これは、ブリッジ優先度とブリッジのベース MAC アドレスから作成されます。
Root Path Cost	この MST の指名ルートまでのパスコストを示します。
Root Port	この MST インスタンスに対する指名ルートにアクセスするポートを示します。

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。「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。「Force」をクリックすると、ポートは 802.1w か 802.1D BPDU を送信します。

CST ポート設定

スイッチの特定ポートに Common Spanning Tree（CST）と Internal Spanning Tree を設定します。

LAN タブ > L2 Features > Spanning Tree > CST Port 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。

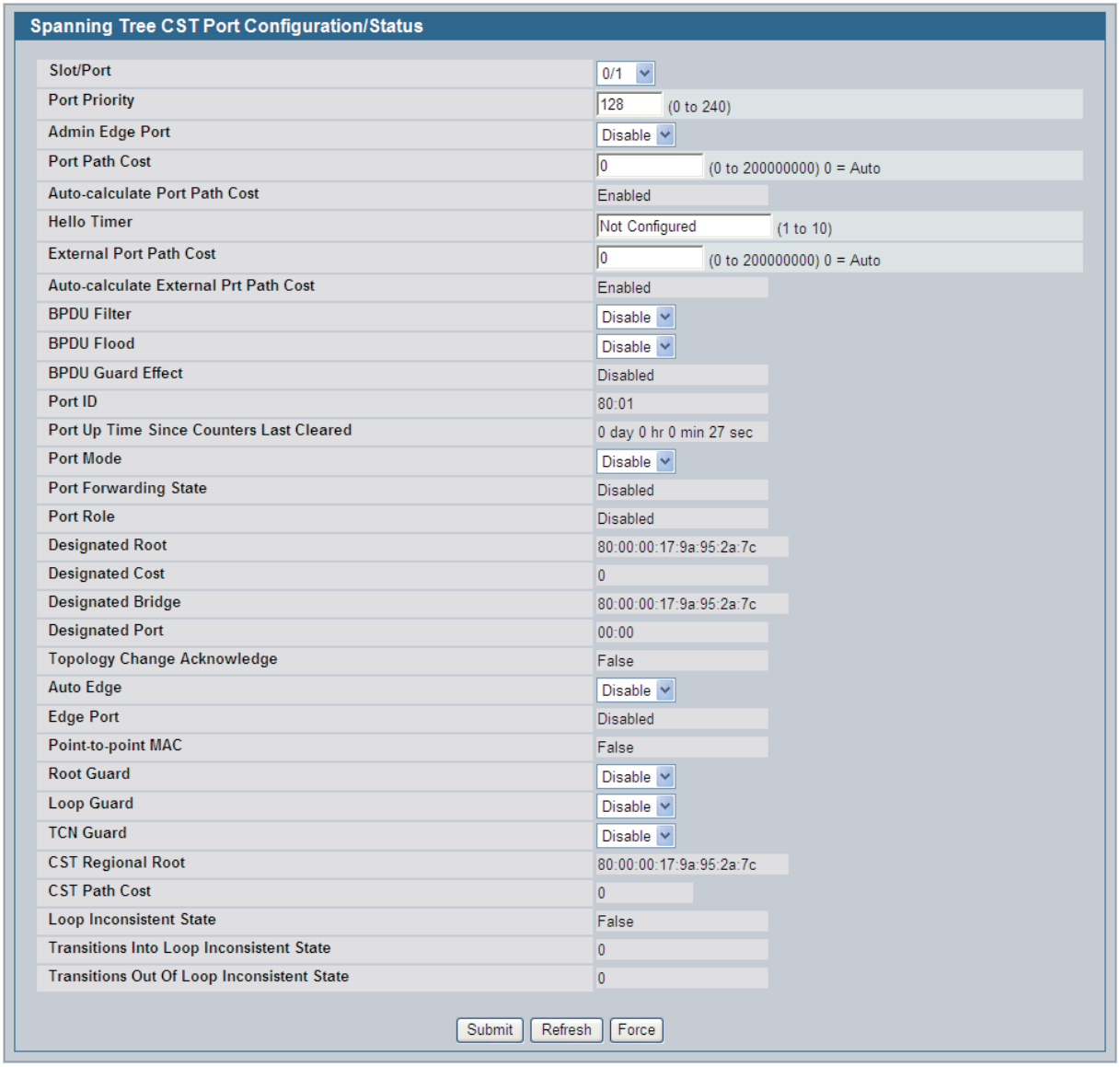


図 4-70　Spanning Tree CST Port Configuration/Status 画面

本画面には次の項目があります。

項目	説明
Slot/Port	設定する物理またはポートチャンネルインタフェースを選択します。ポートは CST に関連する VLAN に関連付けられています。
Port Priority	CST 内の指定ポート優先度。ポート優先度は 16 の倍数で設定されます。16 の倍数でない値を指定すると、優先度は自動的に 16 の倍数に次に低い優先度に設定されます。例えば、優先度が 0-15 間の値に設定すると、0 に設定されます。16-31 の数を指定すると、優先度は 16 に設定されます。
Admin Edge Port	指定ポートが CIST 内のエッジポートであるかどうか判断します。「Enable」または「Disable」（初期値）の値を取得します。
Port Path Cost	パスコストを汎用の内部スパニングツリーにおける指定ポートの新しい値（1-200000000）に設定します。
Auto-calculate Port Path Cost	パスコストが自動的に計算される（Enabled）または計算されない（Disabled）を表示します。パスコストは Port Path の設定値が 0 であるとポートのリンクスピードに基づいて計算されます。
Hello Timer	スイッチの Hello タイムを指定します。これは、構成メッセージ間にポートが待機する時間（秒）を示します。 範囲は 1-10 で、初期値は 2 です。値は「（Bridge Max Age/2）-1」以下とします。
External Port Path Cost	外部パスコストをスパニングツリーにおける指定ポートの新しい値（1-200000000）に設定します。
Auto-calculate External Port Path Cost	外部パスコストが自動的に計算される（Enabled）または計算されない（Disabled）を表示します。外部パスコストは External Port Path の設定値が 0 であるとポートのリンクスピードに基づいて計算されます。
BPDU Filter	BPDU フィルタを有効または無効にします。STP がこのポートで有効である場合、このポート上で BPDU トラフィックをフィルタします。

項目	説明
BPDU Flood	BPDU フラッドを有効または無効にします。STP がこのポートで無効である場合、このポートに到着する BPDU トラフィックをフラッドします。
BPDU Guard Effect	BPDU ガードがスイッチに有効にされ、エッジポートが BPDU を受信すると、ポートは無効になり、このステータスは有効になります。
Port ID	CST 内の指定のポートの識別子。ポート優先度とポートのインタフェース番号から作成されます。
Port Up Time Since Counters Last Cleared	カウンタが最後にクリアされてからの経過時間（日、時、分、秒）を表示します。
Port Mode	ポートまたはポートチャンネルに関連付ける STP（Spanning Tree Protocol）管理モード。「Enable」または「Disable」です。
Port Forwarding State	ポートの現在の STP ステートを示します。有効にされると、ポートステートは、トラフィックに行うフォワーディングアクションを決定します。可能なポートステートは以下の通りです。 • Disabled - STP は現在ポートで無効です。ポートは MAC アドレスの学習中にトラフィックを転送します。 • Blocking - ポートは現在ブロックされ、トラフィックの転送または MAC アドレスの学習に使用されません。 • Listening - ポートは現在 listening モードです。ポートはトラフィックの転送または MAC アドレスの学習もできません。 • Learning - ポートは現在 learning モードです。ポートはトラフィックの転送はできませんが、新しい MAC アドレスの学習はできます。 • Forwarding - ポートは現在 forwarding モードです。ポートは、トラフィックの転送および新しい MAC アドレスの学習ができます。
Port Role	有効な各 MST ブリッジポートは、各スパニングツリーに対する役割（Root Port、Designated Port、Alternate Port、Backup Port、Master Port、または Disabled Port）を割り当てられます。
Designated Root	CST のためのルートブリッジ。ブリッジ優先度とブリッジのベース MAC アドレスを使用することで作成されます。
Designated Cost	STP トポロジに参加するポートのコストを表示します。STP がループを検出すると、より低いコストを持つポートはブロックされやすくなります。
Designated Bridge Bridge	Designated Port を持つブリッジの識別子。ブリッジ優先度とブリッジのベース MAC アドレスを使用することで作成されます。
Designated Port Port	LAN への最も低いコストを提供する Designated Bridge の識別子。ポート優先度とポートのインタフェース番号から作成されます。
Topology Change Acknowledge	ポートに送信される次の BPDU が設定されたトポロジ変更の承認フラグを持つかどうかを示します。「True」または「False」のいずれかです。
Auto Edge	ポートの自動エッジモード（Enable/Disable）を表示します。有効にすると、しばらくの間継続して BPDU を検出しないと、ポートはエッジポートになります。
Edge Port	ポートがエッジポートとして有効または無効かを示します。
Point-to-point MAC	ポイントツーポイントステータスの最終値。
Root Guard	ルートガードモードのステータスが有効な場合、ポートが受信するどんな優れた情報も破棄し、その結果、変更からデバイスのルートから保護するようにポートを設定することができます。ポートは discarding ステートに置かれ、パケットを送信しません。
Loop Guard	ループガードモードのステータス。有効な場合、ポートが BPDU の受信を中止した場合にポートが blocking ステートから誤って transitioning になることを防止します。ポートは loop-inconsistent ステートにあるとして示されます。この状態では、ポートはパケットを送信しません。
TCN Guard	TCN ガードのステータス。有効にすると、そのポートから受信するどんなトポロジ変更情報もポートが伝搬することを制限します。
CST Regional Root	CST Regional Root の優先度と MAC アドレスを示します。
CST Path Cost	CST ツリーの Regional Root へのパスコストを示します。
Loop Inconsistent State	現在、ポートが loop inconsistent 状態にあるかどうかを示します。ポートが loop inconsistent 状態にあると、パケットを送信しません。
Transitions Into Loop Inconsistent State	インタフェースが loop inconsistent 状態に移行した回数を表示します。
Transitions Out Of Loop Inconsistent State	インタフェースが loop inconsistent 状態から移行した回数を表示します。

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。「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。「Force」をクリックすると、ポートは 802.1w か 802.1D BPDU を送信します。

MST ポート設定とステータス

スイッチに MST（Multiple Spanning Tree）を設定します。

LAN タブ > L2 Features > Spanning Tree > MST Port 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。MST インスタンスがスイッチに設定されていない場合、画面には「No MSTs Available」メッセージが表示され、以下の画面は表示されません。

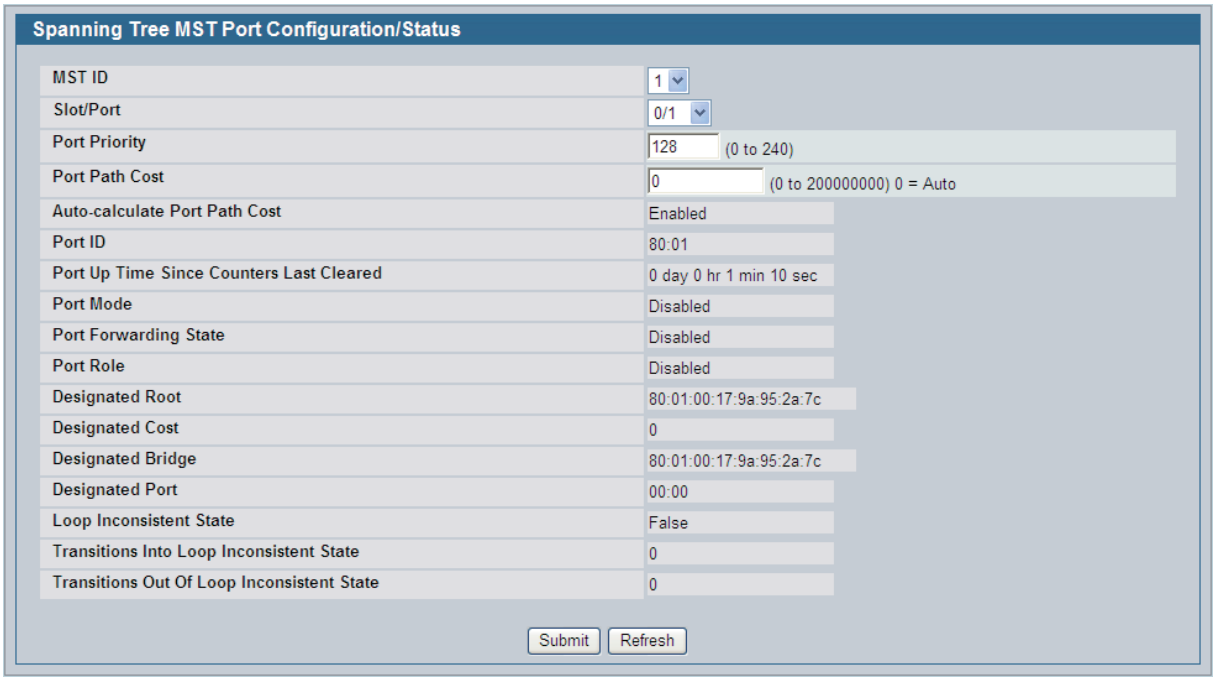


図 4-71　Spanning Tree MST Port Configuration/Status 画面

本画面には次の項目があります。

項目	説明
MST ID	値を表示または設定する既存の MST インスタンスを選択します。
Slot/Port	設定する物理またはポートチャンネルインタフェースを選択します。ポートは MST に関連する VLAN に関連付けられています。
Port Priority	MST 内の指定ポート優先度。ポート優先度は 16 の倍数で設定されます。16 の倍数でない値を指定すると、優先度は自動的に 16 の倍数の次に低い優先度に設定されます。例えば、優先度が 0-15 間の値に設定すると、0 に設定されます。16-31 の数を指定すると、優先度は 16 に設定されます。
Port Path Cost	パスコストを選択した MST インスタンス内の指定ポートに新しい値（1-200000000）に設定します。
Auto-calculate Port Path Cost	パスコストが自動的に計算される（Enabled）または計算されない（Disabled）を表示します。パスコストは Port Path の設定値が 0 であるとポートのリンクスピードに基づいて計算されます。
Port ID	CST 内の指定のポートのポート識別子。ポート優先度とポートのインタフェース番号から作成されます。
Port Up Time Since Counters Last Cleared	カウンタが最後にクリアされてからの経過時間（日、時、分、秒）を表示します。
Port Mode	STP がポートで有効かどうかを表示します。ポートの STP を有効にするためには、**System > Port > Configuration** 画面を使用します。
Port Forwarding State	ポートの現在の STP ステートを示します。有効にすると、ポートステートは、トラフィックに行うフォワーディングアクションを決定します。 • Disabled - STP は現在ポートで無効です。ポートは MAC アドレスの学習中にトラフィックを転送します。 • Blocking - ポートは、現在ブロックされ、トラフィックの転送または MAC アドレスの学習に使用されません。 • Listening - ポートは、現在 listening モードです。ポートはトラフィックの転送または MAC アドレスの学習もできません。 • Learning - ポートは、現在 learning モードです。ポートはトラフィックの転送はできませんが、新しい MAC アドレスの学習はできます。 • Forwarding - ポートは、現在 forwarding モードです。ポートは、トラフィックの転送および新しい MAC アドレスの学習ができます。
Port Role	有効な各 MST ブリッジポートは、各スパニングツリーに対する役割（Root Port、Designated Port、Alternate Port、Backup Port、Master Port、または Disabled）を割り当てられます。
Designated Root	選択した MST インスタンスのためのルートブリッジ識別子。ブリッジ優先度とブリッジのベース MAC アドレスを使用することで作成されます。

項目	説明
Designated Cost	STP トポロジに参加するポートのコストを表示します。STP がループを検出すると、より低いコストを持つポートはブロックされやすくなります。
Designated Bridge Bridge	Designated Port を持つブリッジの識別子。ブリッジ優先度とブリッジのベース MAC アドレスを使用することで作成されます。
Designated Port	LAN への最も低いコストを提供する Designated Bridge のポート識別子。ポート優先度とポートのインタフェース番号から作成されます。
Loop Inconsistent State	ポートが指定した MST インスタンスで loop inconsistent 状態にあるかどうかを示します。ポートが loop inconsistent 状態にあると、パケットを送信しません。
Transitions Into Loop Inconsistent State	インタフェースが loop inconsistent 状態に移行した回数を表示します。
Transitions Out Of Loop Inconsistent State	インタフェースが loop inconsistent 状態から移行した回数を表示します。

「Submit」ボタンをクリックし、変更をスイッチに適用します。「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。

統計情報

各ポートに送受信された BPDU（bridge protocol data units）の数とタイプに関する情報を参照します。

LAN タブ > Monitoring > Spanning Tree > Statistics > 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。

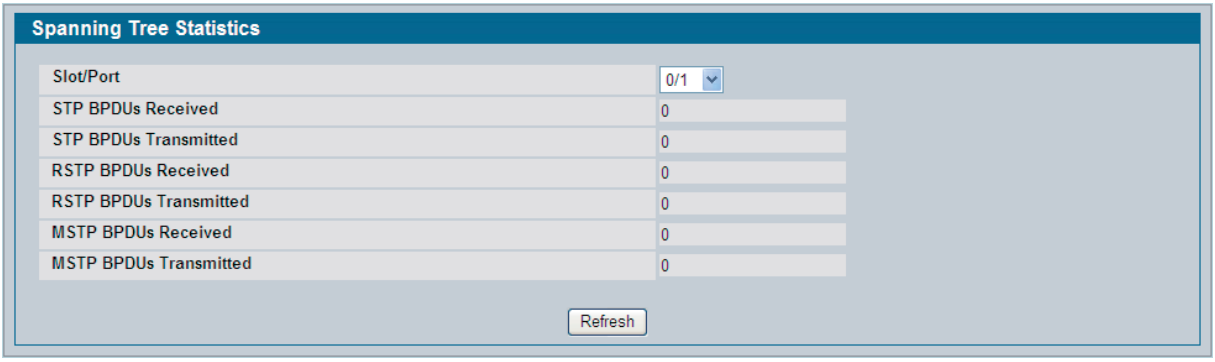


図 4-72　Spanning Tree Statistics 画面

本画面には次の項目があります。

項目	説明
Slot/Port	その統計情報を参照する物理またはポートチャンネルインタフェースを選択します。
STP BPDUs Received	選択ポートで受信した STP BPDU 数。
STP BPDUs Transmitted	選択ポートで送信した STP BPDU 数。
RSTP BPDUs Received	選択ポートで受信した RSTP BPDU 数。
RSTP BPDUs Transmitted	選択ポートで送信した RSTP BPDU 数。
MSTP BPDUs Received	選択ポートで受信した MSTP BPDU 数。
MSTP BPDUs Transmitted	選択ポートで送信した MSTP BPDU 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。

ポートセキュリティの設定

ポートセキュリティは、ポートベースで有効にすることができます。ポートをロックすると、許可される送信元 MAC アドレスを持つパケットだけが送信され、他のすべてのパケットが破棄されます。MAC アドレスは、2 種類（ダイナミックまたはスタティック）のうち 1 つで許可されるように定義されます。ポートがロックされる場合、両方が同時に使用されることにご注意ください。

ダイナミックなロックは、ポートセキュリティの「first arrival」メカニズムを実行します。ロックされたポートで学習できるアドレス数を指定します。制限に到達していないと、通常、未知の送信元 MAC アドレスを持つパケットを学習し、転送します。一度、制限に到達すると、それ以上のアドレスはポートで学習されません。学習されなかった送信元 MAC アドレスを持つすべてのパケットが破棄されます。許可できるダイナミックエントリの数を 0 に設定することでダイナミックなロックを事実上、無効にできることに注意します。

スタティックなロックでは、ポートに許可される MAC アドレスのリストを指定することができます。パケットの動作はダイナミックなロックと同じで、許可される送信元 MAC アドレスを持つパケットだけが送信されます。

指定ポートで学習された MAC アドレスを参照するためには、「フォワーディングデータベースの設定と検索」（41 ページ）を参照してください。

無効なポートは「Configuring Ports」画面からアクティブ化できるだけです。

ポートセキュリティには以下の機能があります。

- ポートセキュリティの管理
- ポートセキュリティインタフェースの設定
- ポートセキュリティ - スタティック
- ポートセキュリティ - ダイナミック
- ポートセキュリティ侵害の状況

ポートセキュリティの管理

スイッチのポートセキュリティ機能を有効または無効にします。

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

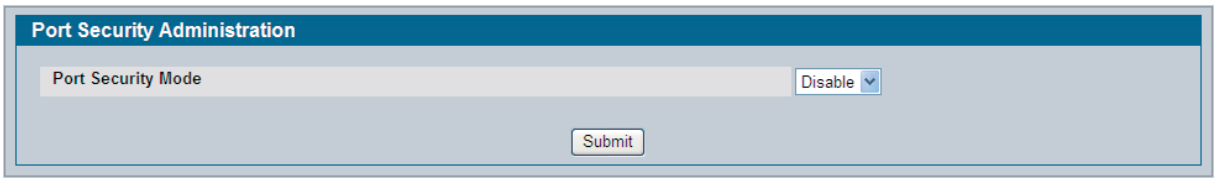


図 4-73　Port Security Administration 画面

「Port Security Mode」リストから「Enable」または「Disable」を選択して、「Submit」ボタンをクリックします。

ポートセキュリティインタフェースの設定

選択ポートにポートセキュリティ機能を設定します。

LAN タブ > Security > Port Security Interface 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。

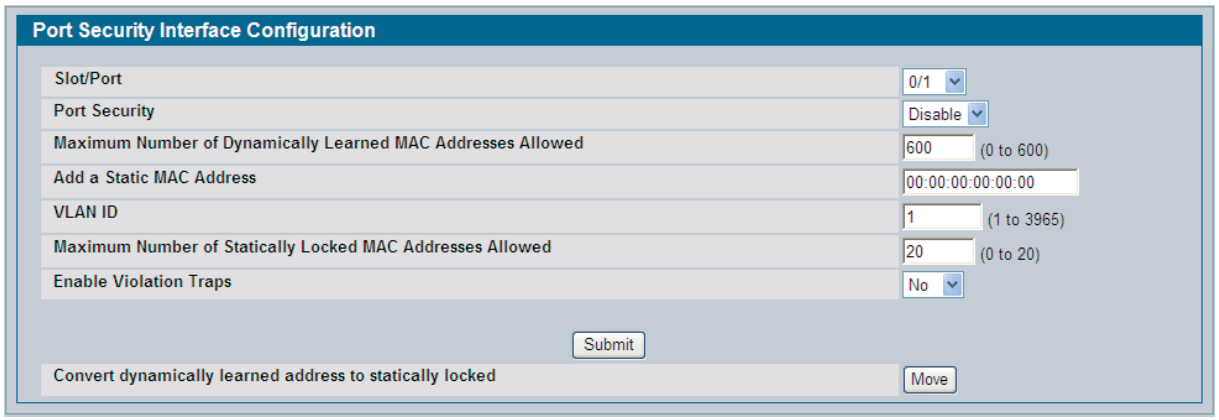


図 4-74　Port Security Interface Configuration 画面

本画面には次の項目があります。

項目	説明
Slot/Port	ポートセキュリティ情報を設定する物理インタフェースまたは LAG を選択します。
Port Security	ポートセキュリティを有効とするかどうか決定します。 • Enable - ポートをロックされると、許可される送信元 MAC アドレスを持つパケットだけが送信されます。他のすべてのパケットが破棄されます。 • Disable - ポートがロックされていないため、どんなポートセキュリティの制限も適用されてません。（初期値）
Maximum Number of Dynamically Learned MAC Addresses Allowed	選択インタフェースにダイナミックに学習される MAC アドレスの最大数を設定します。一度、制限に到達すると、それ以上のアドレスはポートで学習されません。学習されなかった送信元 MAC アドレスを持つすべてのパケットが破棄されます。許可できるダイナミックエントリの数を 0 に設定することでダイナミックなロックを事実上無効にできます。
Add a Static MAC Address	選択インタフェースに対してスタティックにロックされた MAC アドレスのリストに MAC アドレスを追加します。許可される送信元 MAC アドレスを持つパケットだけが送信されます。
VLAN ID	選択インタフェースに対してスタティックにロックされた MAC アドレスのリストに追加される MAC アドレスに対応する VLAN ID を追加します。
Maximum Number of Statically Locked MAC Addresses Allowed	選択インタフェースでスタティックにロックされる MAC アドレスの最大数を設定します。
Enable Violation Traps	Violation トラップを有効または無効にします。
Convert dynamically learned address to static locked	「Move」ボタンをクリックすると、このインタフェースでダイナミックに学習された全エントリが、このインタフェースのスタティック MAC アドレスリストに追加されます。それらを移動させた後に、「Port Security Static」画面でそれらを参照することができます。

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。

ポートセキュリティ - スタティック

インタフェースに設定されているスタティックな MAC アドレスを参照します。

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

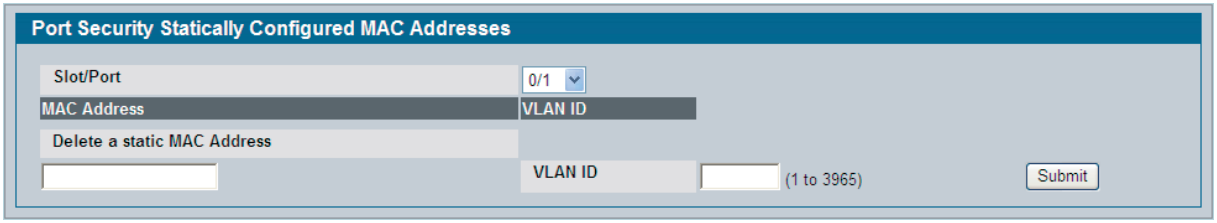


図 4-75　Port Security Statically Configured MAC Addresses 画面

本画面には次の項目があります。

項目	説明
Slot/Port	ダイナミックに学習した MAC アドレスを参照する物理インタフェースまたは LAG を選択します。
MAC Address	選択ポートに設定されているスタティックな MAC アドレスを示します。
VLAN ID	スタティックに設定された MAC アドレスに対応する VLAN ID を表示します。
Delete a static MAC Address	削除するスタティックに設定された MAC アドレスを入力します。 削除される可能性のあるすべての MAC アドレスが「MAC Address - VLAN ID」テーブルに表示されます。
VLAN ID	削除するスタティックに設定された MAC アドレスに対応する VLAN ID を入力します。

MAC アドレスおよびスタティックに設定されている MAC アドレスの VLAN ID を入力後、「Submit」ボタンをクリックして、ポートから MAC アドレスを削除し、新しい設定をシステムに適用します。画面は更新され、MAC アドレスは画面上のテーブルには表示されません。

ポートセキュリティ - ダイナミック

インタフェースにおけるダイナミックに学習された MAC アドレスを持つテーブルを参照します。ダイナミックなロックでは、MAC アドレスは「初動時」ベースで学習されます。ロックされたポートで学習できるアドレス数を指定します。

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

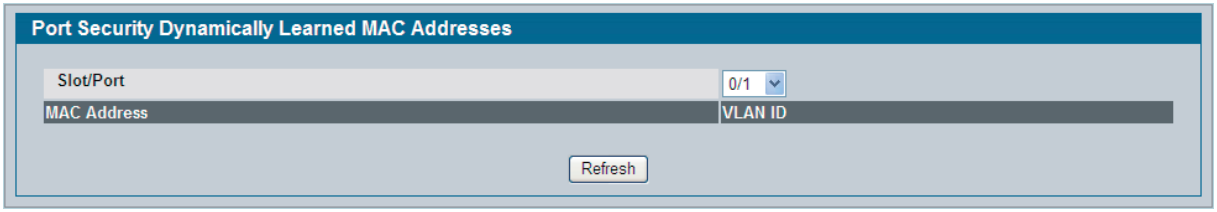


図 4-76　Port Security Dynamically Learned MAC Addresses 画面

本画面には次の項目があります。

項目	説明
Slot/Port	ダイナミックに学習した MAC アドレスを参照する物理インタフェースまたは LAG を選択します。
MAC Address	選択ポートでダイナミックに学習した MAC アドレスをテーブルに示します。
VLAN ID	ダイナミックに学習した MAC アドレスに対応する VLAN ID を表示します。

ポートセキュリティ侵害の状況

スイッチにおけるポートセキュリティ機能の状態を表示します。

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

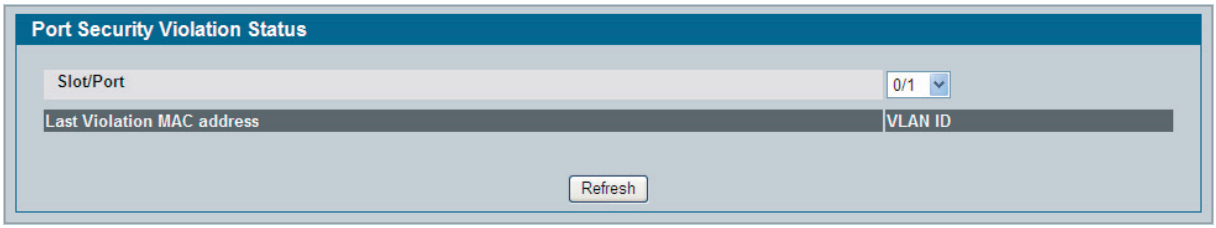


図 4-77　Port Security Violation Status 画面

本画面には次の項目があります。

項目	説明
Slot/Port	セキュリティの侵害情報を参照する物理インタフェースまたは LAG を選択します。
Last Violation MAC Address	ロックポートで破棄された最後のパケットの送信元 MAC アドレスを表示します。
VLAN ID	「Last Violation MAC Address」に対応する VLAN ID を表示します。

LLDP（LLDP の管理）

IEEE 802.1AB 定義の標準 LLDP（Link Layer Discovery Protocol）により、802 LAN に常駐するステーションは主要な機能と物理的な説明を通知することができます。この情報をネットワークマネージャが参照し、システムトポロジを特定して、LAN において適切でない構成を検出することができます。

LLDP は一方向のプロトコルであり、リクエスト / レスポンスのシーケンスはありません。情報は、送信機能を実行するステーションに通知され、受信機能を実行するステーションによって受信、処理されます。送信および受信機能は、ポートごとに別々に有効 / 無効ににされます。初期値では、送受信ともにすべてのポートで無効です。アプリケーションには、ポートの設定状態および操作状態に基づいて適切に送信および受信状態の各マシンを起動する責任があります。

D-Link では、インタフェースごとに複数の LLDP Neighbor を持つことができます。そのような Neighbor 数はメモリの制約により制限されます。製品が指定する定数は、スイッチでサポートする Neighbor の最大数を定義します。LLDP ポートごとにサポートされる Neighbor 数には制限がありません。
スイッチのすべてのリモートエントリがいっぱいになると、新しい Neighbor は無視されます。1 つのインタフェース上の複数の VoIP デバイスがある場合には、802.1ab コンポーネントはすべての VoIP デバイスに音声 VLAN コンフィグレーションを送信します。

LLDP には以下の機能があります。

- グローバル設定
- インタフェース設定
- インタフェースのサマリ
- 統計情報
- ローカルデバイス情報
- ローカルデバイスサマリ
- リモートデバイス情報
- リモートデバイスサマリ
- LLDP-MED

グローバル設定

スイッチに適用される LLDP 項目を指定します。

LAN タブ > L2 Features > LLDP > 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。

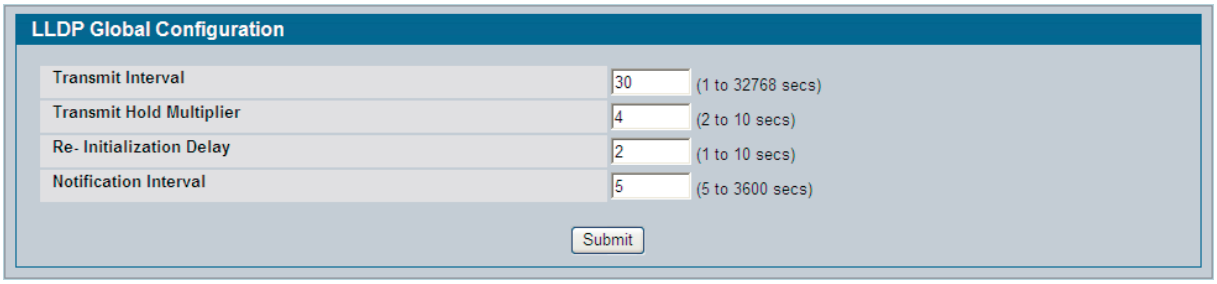


図 4-78　LLDP Global Configuration 画面

本画面には次の項目があります。

項目	説明
Transmit Interval	LLDP フレームが送信される間隔を示しています。初期値は 30（秒）で、値の範囲は 1-32768（秒）です。
Transmit Hold Multiplier	TTL に割り当てる送信間隔の乗数を指定します。初期値は 4 で、範囲は 2-10 です。
Re-Initialization Delay	再初期化の前の遅延を指定します。初期値は 2（秒）で、範囲は 1-10（秒）です。
Notification Interval	通知の送信を制限します。初期値は 5（秒）で、範囲は 5-3600（秒）です。

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。

インタフェース設定

特定のインタフェースに適用される LLDP パラメータを指定します。

LAN タブ > L2 Features > LLDP > Interface 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。

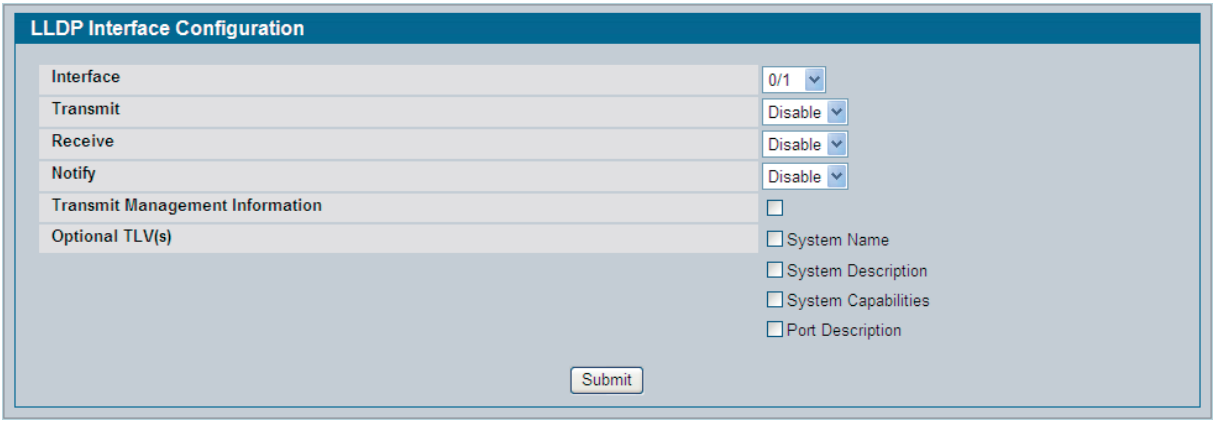


図 4-79　LLDP Interface Configuration 画面

本画面には次の項目があります。

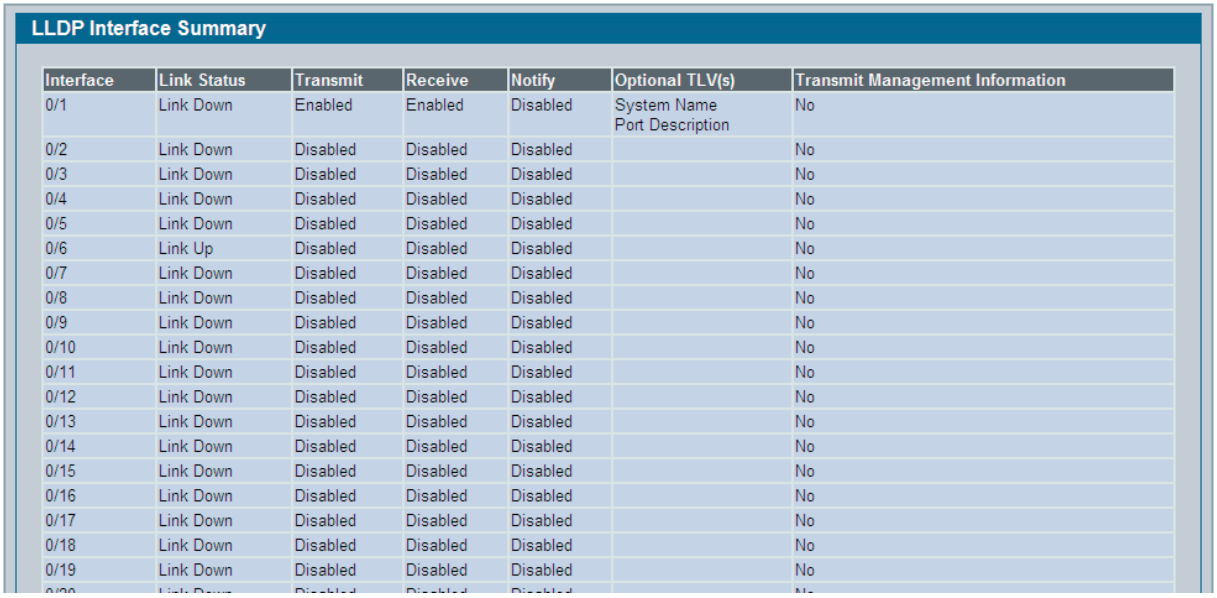
項目	説明
Interface	LLDP を設定するインタフェースを指定します。
Transmit	LLDP の protocol data units（PDU）の送信を有効または無効にします。初期値は無効です。
Receive	LLDP PDU を受信するポートの機能を有効または無効にします。初期値は無効です。
Notify	通知が有効である場合、LLDP はトラップマネージャと通信を行い、リモートデータ変更の統計情報について加入者に通知します。初期値は無効です。
Transmit Management Information	チェックボックスを選択して、管理アドレスのインスタンスの転送を有効にします。チェックを外して、管理情報の転送を無効にします。初期値は無効です。
Optional TLV(s)	転送する type-length value（TLV）情報の各チェックボックスを選択します。 • System Name - LLDP フレームにシステム名 TLV を含めます。システム名を設定するためには、「システム説明の設定」（25 ページ）を参照してください。 • System Description - LLDP フレームに system description TLV を含めます。 • System Capabilities - LLDP フレームに system capability TLV を含めます。 • Port Description - LLDP フレームに port description TLV を含めます。Port Description を設定するためには、「ポートの説明」（65 ページ）を参照してください。

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。

インタフェースのサマリ

システムにおける各物理ポートに設定された LLDP パラメータを参照します。

LAN タブ > Monitoring > LLDP Status > Interface 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。



LLDP Interface Summary

Interface	Link Status	Transmit	Receive	Notify	Optional TLV(s)	Transmit Management Information
0/1	Link Down	Enabled	Enabled	Disabled	System Name Port Description	No
0/2	Link Down	Disabled	Disabled	Disabled		No
0/3	Link Down	Disabled	Disabled	Disabled		No
0/4	Link Down	Disabled	Disabled	Disabled		No
0/5	Link Down	Disabled	Disabled	Disabled		No
0/6	Link Up	Disabled	Disabled	Disabled		No
0/7	Link Down	Disabled	Disabled	Disabled		No
0/8	Link Down	Disabled	Disabled	Disabled		No
0/9	Link Down	Disabled	Disabled	Disabled		No
0/10	Link Down	Disabled	Disabled	Disabled		No
0/11	Link Down	Disabled	Disabled	Disabled		No
0/12	Link Down	Disabled	Disabled	Disabled		No
0/13	Link Down	Disabled	Disabled	Disabled		No
0/14	Link Down	Disabled	Disabled	Disabled		No
0/15	Link Down	Disabled	Disabled	Disabled		No
0/16	Link Down	Disabled	Disabled	Disabled		No
0/17	Link Down	Disabled	Disabled	Disabled		No
0/18	Link Down	Disabled	Disabled	Disabled		No
0/19	Link Down	Disabled	Disabled	Disabled		No

図 4-80　LLDP Interface Summary 画面

本画面には次の項目があります。

項目	説明
Interface	LLDP-802.1AB を設定するすべてのポートを表示します。
Link Status	ポートのリンクステータス「Up」（アクティブ）または「Down」（ダウン）を表示します。
Transmit	インタフェースの LLDP-802.1AB 転送モードを表示します。
Receive	インタフェースの LLDP-802.1AB 受信モードを表示します。
Notify	インタフェースの LLDP-802.1AB 通知モードを表示します。
Optional TLV(s)	含まれる LLDP-802.1AB のオプションの type-length values（TLV）を表示します。TVL が送信されないと、エントリは空白です。以下で示す TVL のうち 1 つ以上が含まれます。 ・System Name ・System Capabilities ・System Description ・Port Description
Transmit Management Information	管理アドレスが LLDP フレームに転送されるかどうかを指定します。

「Refresh」ボタンをクリックすると、最新データで画面を更新します。

統計情報

グローバルなインタフェース LLDP 統計情報を参照します。

LAN タブ > Monitoring > LLDP Status > 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。

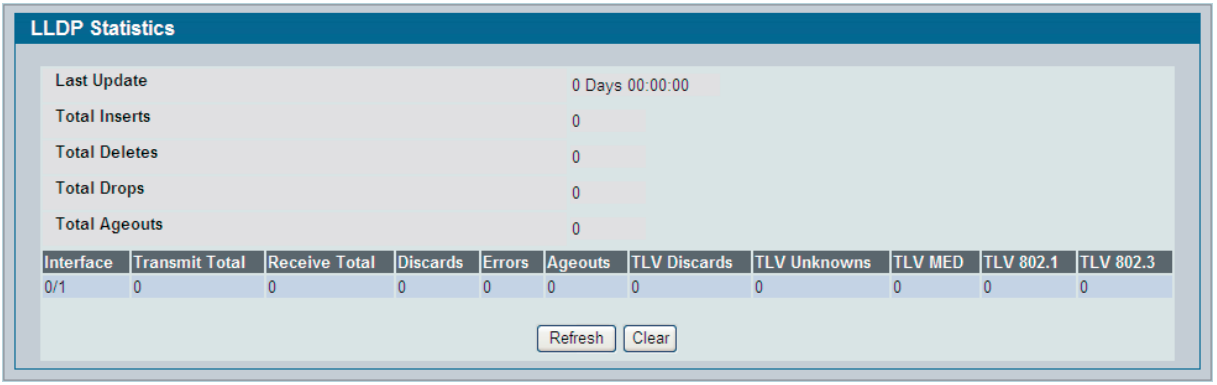


図 4-81　LLDP Statistics 画面

本画面には次の項目があります。

項目	説明
システム全体の統計情報	
Last Update	エントリがリモートシステムに関連しているテーブルに作成、変更、または削除された時間を表示します。
Total Inserts	特定の MAC Service Access Point（MSAP）によって通知された完全な情報のセットをリモートシステムに関連しているテーブルに挿入した回数を表示します。
Total Deletes	特定の MAC Service Access Point（MSAP）によって通知された完全な情報のセットをリモートシステムに関連しているテーブルから削除された回数を表示します。
Total Drops	特定の MAC Service Access Point（MSAP）によって通知された完全な情報のセットをリモートシステムに関連しているテーブルに挿入されなかった回数を表示します。
Total Ageouts	情報のタイムラインがタイムアウトになったために特定の MAC Service Access Point（MSAP）によって通知された完全な情報のセットをリモートシステムに関連しているテーブルから削除した回数を表示します。
ポートの統計情報	
Interface	インタフェースのスロット / ポートを表示します。
Transmit Total	対応ポートで LLDP エージェントが転送した LLDP フレームの合計数を表示します。
Receive Total	LLDP エージェントが有効な場合に対応ポートで LLDP エージェントが受信した LLDP フレームの合計数を表示します。
Discards	対応ポートで LLDP エージェントが何らかの理由のために破棄された LLDP TLV の合計数を表示します。
Errors	LLDP エージェントが有効な場合に対応ポートで LLDP エージェントが受信した不正な LLDP フレームの合計数を表示します。
Ageouts	指定ポートに発生したエージングアウト数を表示します。情報のタイムラインがタイムアウトになったために特定の MAC Service Access Point（MSAP）によって通知された完全な情報のセットをリモートシステムに関連しているテーブルから削除した回数を表示します。
TLV Discards	対応ポートで LLDP エージェントが何らかの理由のために破棄された LLDP TLV（Type、Length、Value のセット）の数を表示します。
TLV Unknowns	対応ポートで LLDP エージェントが認識しなかったローカルポートに受信した LLDP TLV の数を表示します。
TLV MED	ローカルポートに受信した LLDP-MED TLV の合計数を表示します。
TLV 802.1	ローカルポートに受信した 802.1 タイプの LLDP TLV の合計数を表示します。
TLV 802.3	ローカルポートに受信した 802.3 タイプの LLDP TLV の合計数を表示します。

「Refresh」ボタンをクリックすると、最新の情報に更新します。

統計情報のクリア

「Clear」ボタンをクリックして、すべてのインタフェースの LLDP 統計情報をクリアします。

ローカルデバイス情報

LLDP を通じて各ポートが通知するデータを参照します。

LAN タブ > Monitoring > LLDP Status > Local Device 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。

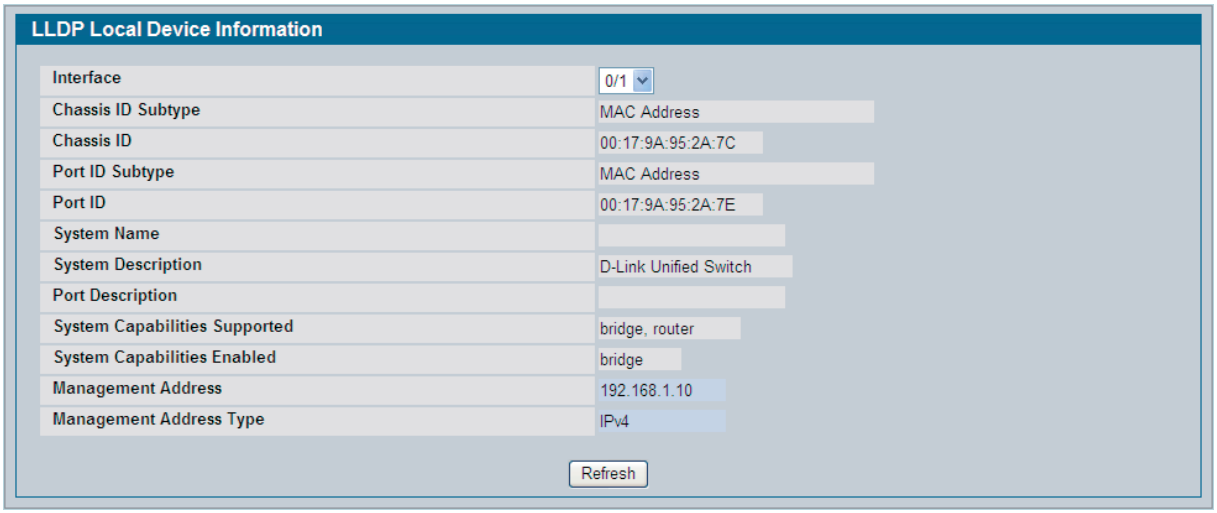


図 4-82　LLDP Local Device Information 画面

本画面には次の項目があります。

項目	説明
Interface	LLDP-802.1AB フレームが送信されるすべてのポートリストを選択します。
Chassis ID Subtype	筐体の識別子のソースについて説明する文字列を表示します。
Chassis ID	ローカルシステムに関連する筐体のコンポーネントを識別するのに使用した文字列を表示します。
Port ID Subtype	ポート識別子のソースを説明する文字列を表示します。
Port ID	ポートの物理アドレスを表示します。
System Name	ローカルシステムのシステム名を表示します。
System Description	ローカルシステムに関連している選択ポートの説明文を表示します。
Port Description	ユーザ定義のポートの説明を表示します。
System Capabilities Supported	ローカルシステムのシステムの機能を表示します。
System Capabilities Enabled	サポートされて有効であるローカルシステムの機能を表示します。
Management Address	通知されたローカルシステムの管理アドレスを表示します。
Management Address Type	管理アドレスのタイプを指定します。

「Refresh」ボタンをクリックしてと、画面の情報を現在のデータで更新します。

ローカルデバイスサマリ

LLDP 情報の送信が有効であるデバイス上のすべてのインタフェースに関する情報を参照します。

LAN タブ > Monitoring > LLDP Status > Local Device 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。

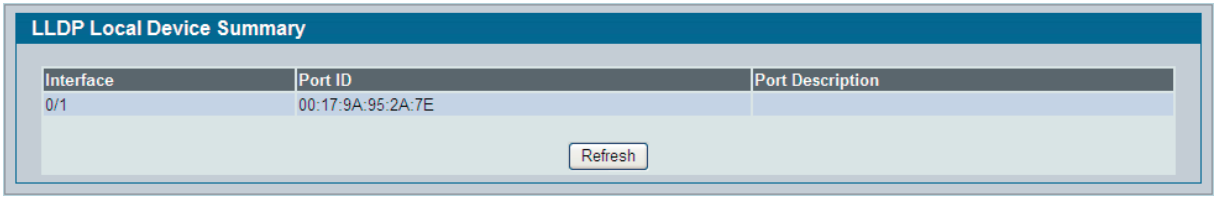


図 4-83　LLDP Local Device Summary 画面

本画面には次の項目があります。

項目	説明
Interface	LLDP-802.1AB が転送されるスロット / ポートを表示します。
Port ID	ポート識別子のソースを説明する文字列を表示します。
Port Description	ローカルシステムに関連しているポートの説明文を表示します。

「Refresh」ボタンをクリックしてと、画面の情報を現在のデータで更新します。

リモートデバイス情報

特定のインタフェースが他の LLDP が有効なシステムから受信したデータを参照します。

LAN タブ > Monitoring > LLDP Status > Remote Device 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。

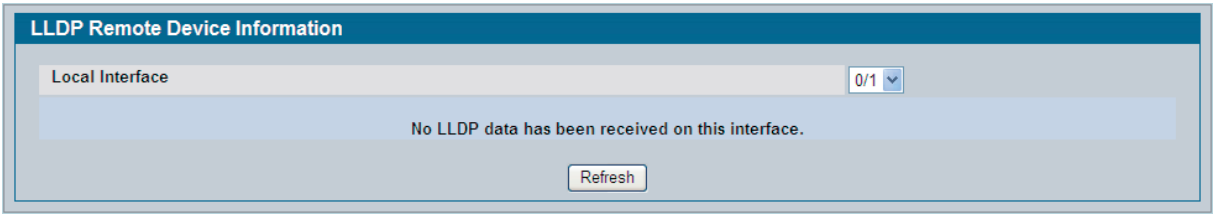


図 4-84　LLDP Remote Device Information 画面

本画面には次の項目があります。

項目	説明
Local Interface	ローカルシステムのスロット / ポートを選択して、それが受信した LLDP 情報を表示します。 **注意** LLDP データが選択インタフェースで受信されていないと、「No LLDP data has been received on this interface」が表示されます。選択インタフェースがリモートデバイスから LLDP 情報を受信すると、以下のフィールドが表示されます。
Remote ID	リモートシステムに割り当てられているリモートクライアント識別子を表示します。
Chassis ID Subtype	リモートシステムで「Chassis ID」に表示されるデータのタイプを示します。
Chassis ID	リモートシステムに関連する筐体のコンポーネント表示します。
Port ID Subtype	リモートシステムの「Port ID」に表示されるデータのタイプを示します。
Port ID	データが送信されたリモートシステムのポートの物理アドレスを表示します。
System Name	リモートシステムのシステム名を表示します。
System Description	リモートシステムに関連している選択ポートの説明を表示します。
Port Description	ユーザ定義のポートの説明を表示します。
System Capabilities Supported	リモートシステムのシステム機能を表示します。
System Capabilities Enabled	サポートされて有効であるリモートシステムの機能を表示します。
Time to Live	受信したリモートエントリの Time to Live 値（秒）を表示します。
Management Address	通知されたリモートシステムの管理アドレスを表示します。
Management Address Type	管理アドレスのタイプを表示します。

「Refresh」ボタンをクリックしてと、画面の情報を現在のデータで更新します。

リモートデバイスサマリ

LLDP 情報の送信が有効であるデバイス上のすべてのインタフェースに関する情報を参照します。

LAN タブ > Monitoring > LLDP Status > Remote Device 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。

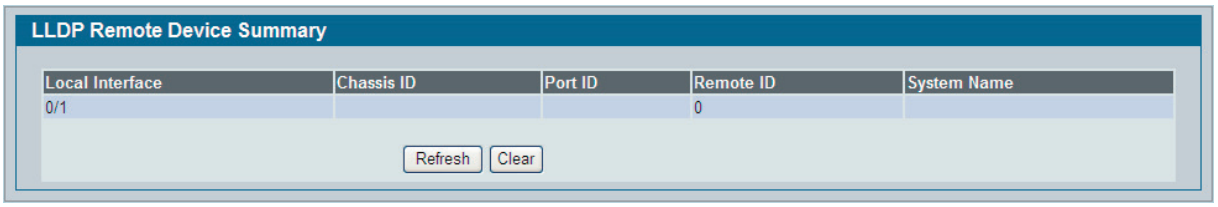


図 4-85　LLDP Remote Device Summary 画面

本画面には次の項目があります。

項目	説明
Local Interface	リモートシステムによって通知された LLDP フレームを受け取るローカルシステムのスロット / ポートを表示します。
Chassis ID	リモートシステムに関連する筐体のコンポーネント表示します。
Port ID	LLDP データが送信されたリモートシステム上のポートの物理アドレスを表示します。
Remote ID	リモートシステムに割り当てられているリモートクライアント識別子を表示します。
System Name	リモートデバイスのシステム名を表示します。システム名が設定されていないと、空白となります。

「Refresh」ボタンをクリックしてと、画面の情報を現在のデータで更新します。

LLDP-MED

LLDP-MED（Link Layer Discovery Protocol-Media Endpoint Discovery）は、LLDP に以下の機能をエンハンスしたものです。

- プラグアンドプレイネットワークを可能にする LAN ポリシー（VLAN、レイヤプライオリティ、および DiffServ 設定など）の自動検出。
- ロケーションデータベース作成のためのデバイスロケーション検出。
- 拡張および自動化された PoE エンドポイントのパワー管理。
- 在庫管理、ネットワーク管理者がネットワークデバイスを追跡して、それらの特性（製造者、ソフトウェアとハードウェアバージョン、シリアル / 資産番号）を判断することを可能にします。

LLDP-MED には以下の機能があります。

- LLDP-MED グローバル設定
- LLDP-MED インタフェース設定
- LLDP-MED インタフェースサマリ
- LLDP ローカルデバイス情報
- LLDP-MED リモートデバイス情報

LLDP-MED グローバル設定

LLDP-MED 操作にグローバルなパラメータを設定します。

LAN タブ > L2 Features > LLDP > LLDP-MED > 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。

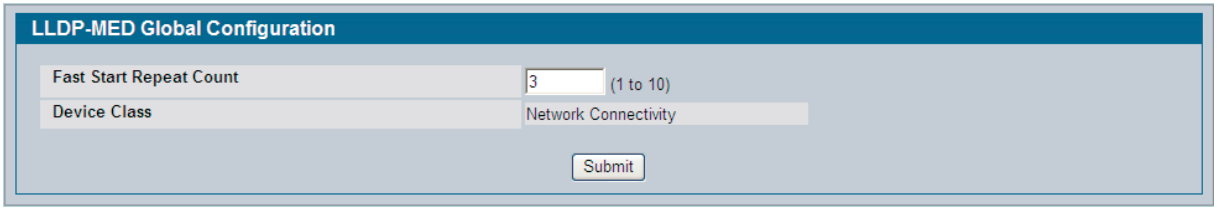


図 4-86　LLDP-MED Global Configuration 画面

本画面には次の項目があります。

項目	説明
Fast Start Repeat Count	プロトコルが有効な場合に転送される LLDP PDU の数を指定します。範囲は 1-10 です。初期値は 3 です。
Device Class	ローカルデバイスの MED Classification を指定します。以下の 3 つは実際のエンドポイントを表しています。 • クラス I ジェネリック - IP 通信コントローラなど • クラス II メディア - カンファレンスブリッジなど • クラス III 通信 - IP 電話など 4 番目のデバイスはネットワーク接続デバイスです。これは、通常 LAN スイッチ / ルータ、IEEE 802.1 ブリッジ、IEEE 802.11 無線アクセスポイントなどです。

「Submit」ボタンをクリックして、スイッチを本画面の値に更新します。保存が行われないと、これらの変更は再起動後に保持されません。

LLDP-MED インタフェース設定

インタフェースにおける LLDP-MED モードを有効にして、プロパティを設定します。

LAN タブ > L2 Features > LLDP > LLDP-MED > Interface 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。

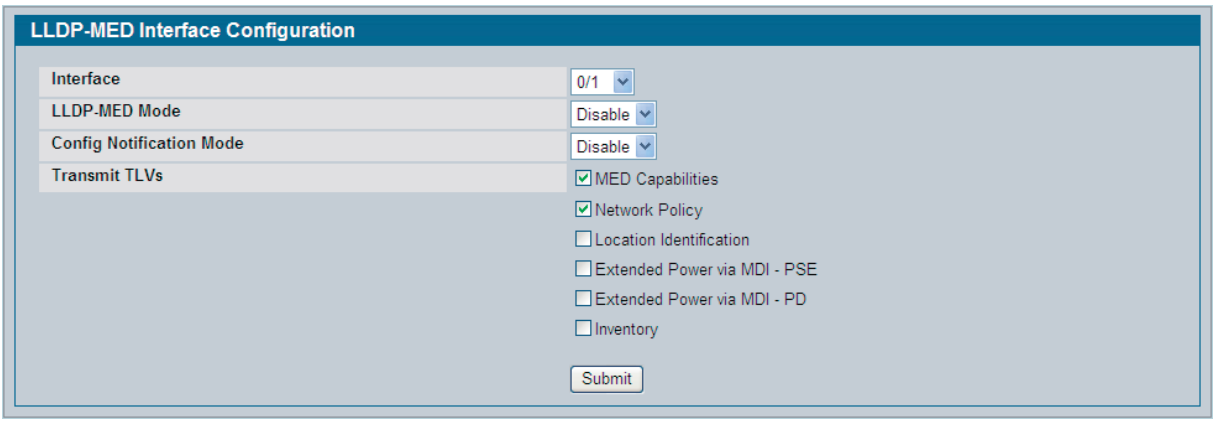


図 4-87　LLDP-MED Interface Configure 画面

本画面には次の項目があります。

項目	説明
Interface	LLDP-MED - 802.1AB を設定するポートを選択します。「All」を選択すると、同じプロパティを持つ DUT 上のすべてのインタフェースを設定します。すべてのインタフェースのサマリを参照するためには、「LLDP-MED インタフェースサマリ」（175 ページ）を参照してください。「Interface Configuration」画面には「All」インタフェースのサマリは表示されません。個別のインタフェースのサマリは「Interface Configuration」画面で参照できます。「All」オプション用の「Interface Configuration」画面は、「Disabled」としていつも LLDP-MED モードと通知モードを表示し、「Transmit TLVs」のチェックボックスは常にチェックされません。
LLDP-MED Mode	選択インタフェースの LLDP-MED モードを有効または無効にします。MED を有効にすることで、事実上、LLDP の送受信を有効にすることができます。
Config Notification Mode	選択インタフェースの LLDP-MED トポロジ変更通知モードを有効または無効にします。
Transmit TLVs	選択されたインタフェースの LLDP PDU フレームに送信する TLV を指定します。 • MED Capabilities - LLDP フレームに capabilities TLV を送信します。 • Network Policy - LLDP フレームに network policy TLV を送信します。 • Location Identification - LLDP フレームに location TLV を送信します。 • Extended Power via MDI - PSE - LLDP フレームに extended PSE TLV を送信します。 • Extended Power via MDI - PD - LLDP フレームに extended PD TLV を送信します。 • Inventory - LLDP フレームに inventory TLV を送信します。

「Submit」ボタンをクリックし、更新した設定内容をスイッチに送信します。これらの変更は直ちに適用されますが、保存が行われないと、再起動後に保持されません。

LLDP-MED インタフェースサマリ

各スイッチインタフェースとその LLDP コンフィグレーションのステータスを表示します。

LAN タブ > Monitoring > LLDP Status > LLDP-MED > Interface 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。

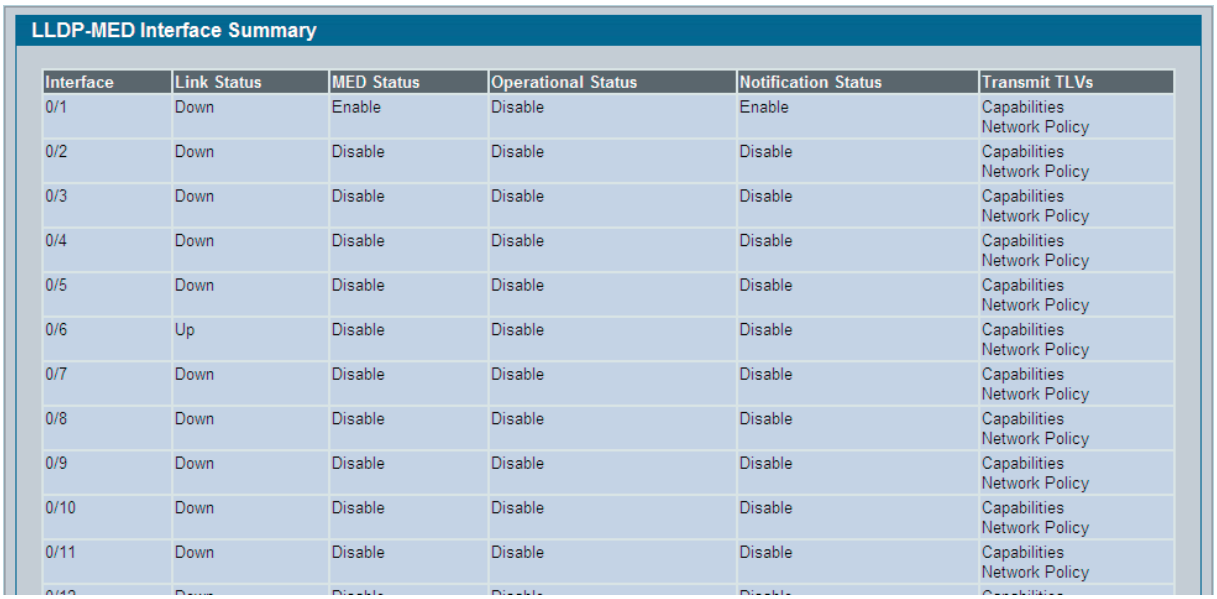


図 4-88　LLDP-MED Interface Summary 画面

本画面には次の項目があります。

項目	説明
Interface	LLDP-MED を設定するすべてのポートを表示します。
Link Status	ポートのリンクステータス「Up」（アクティブ）または「Down」（ダウン）を表示します。
MED Status	送信および（または）受信 LLDP-MED モードがインタフェースに有効または無効であることを表示します。
Operational Status	インタフェースが TLVs を送信するかどうか表示します。
Notification Status	インタフェースの LLDP-MED トポロジ通知モードを表示します。
Transmit TLVs	含まれている LLDP-MED transmit TLV(s) を示します。

「Refresh」ボタンをクリックし、システムの情報を最新に更新します。

LLDP-MED ローカルデバイス情報

選択されたローカルインタフェースに通知される LLDP-MED 情報について表示します。

LAN タブ > Monitoring > LLDP Status > LLDP-MED > Local Device 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。

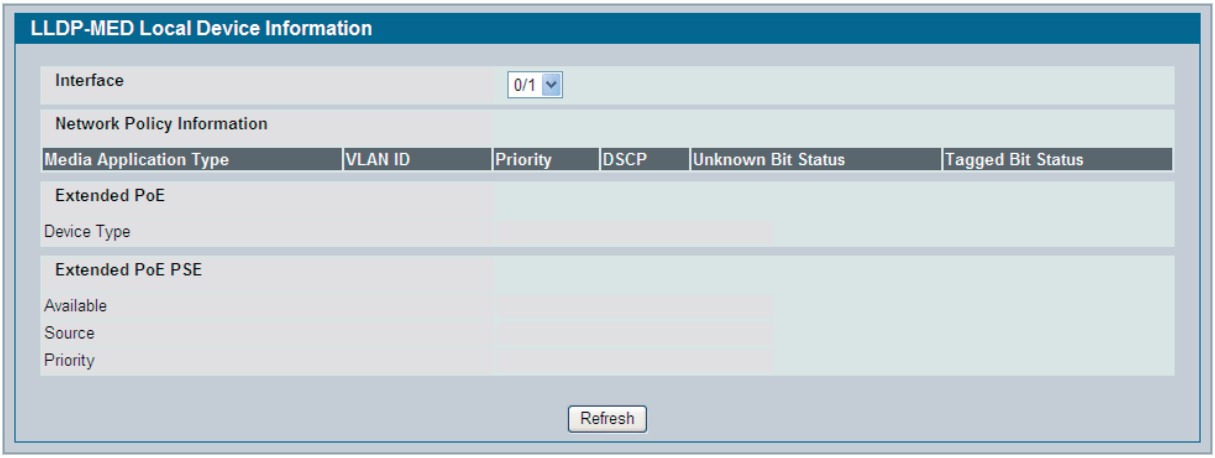


図 4-89　LLDP-MED Local Device Information 画面

本画面には次の項目があります。

項目	説明
Interface	LLDP-MED 情報を表示するインタフェースを選択します。
Network Policy Information	ネットワークポリシー TLV が LLDP フレームに存在しているかどうか表示します。 • Media Application Type - アプリケーションのタイプを指定します。アプリケーションのタイプには unknown、voicesignaling、guestvoice、guestvoicesignalling、softphonevoice、videoconferencing、streammingvideo、vidoesignalling があります。受信した各アプリケーションのタイプには、VLAN ID、優先度、DSCP、タグ付けされたビットステータス、および未知のビットステータスがあります。ポートは 1 つ以上のアプリケーションタイプを受信することができます。ネットワークポリシー TLV を転送すると、本情報が表示されます。 • VLAN ID - 特定のポリシータイプを割り当てた VLAN ID を表示します。 • Priority - 特定のポリシータイプに割り当てた優先度を表示します。 • DSCP - 特定のポリシータイプに割り当てた DSCP を表示します。 • Unknown Bit Status - 特定のポリシータイプに割り当てた未知のビットを表示します。 • Tagged Bit Status - 特定のポリシータイプに割り当てたタグ付きビットを表示します。
Inventory	LLDP フレームの inventory TLV を表示します。 • Hardware Revisions - ハードウェアバージョンを示します。 • Firmware Revisions - ファームウェアバージョンを示します。 • Software Revisions - ソフトウェアバージョンを示します。 • Serial Number - シリアル番号を示します。 • Manufacturer Name - 製造者名を示します。 • Model Name - モデル名を示します。 • Asset ID - 資産番号を示します。
Location Information	LLDP フレームの location TLV を表示します。 • Sub Type - ロケーション情報のタイプを表示します。 • Location Information - 与えられたロケーション ID のロケーション情報を示します。
Extended PoE	ローカルなデバイスが PoE デバイスであるかどうか示します。
Extended PoE PSE	extended PSE TLV が LLDP フレームに存在するかそうかを示します。 • Available - ローカルデバイスのポートに可能な電源装置の電力値（1/10W）を示します。 • Source - このポートの電源を示します。 • Priority - PSE ポートの電力優先度を示します。
Extended PoE PD	extended PD TLV が LLDP フレームに存在するかどうかを示します。 • Required - ローカルデバイスのポートに必要な電源装置の電力値（1/10W）を示します。 • Source - このポートの電源を示します。 • Priority - PD ポート電力優先度を示します。

「Refresh」ボタンをクリックし、システムの情報を最新に更新します。

LLDP-MED リモートデバイス情報

選択されたローカルインタフェースにリモートクライアントから受信した LLDP-MED 情報について表示します。

LAN タブ > Monitoring > LLDP Status > LLDP-MED > Remote Device 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。

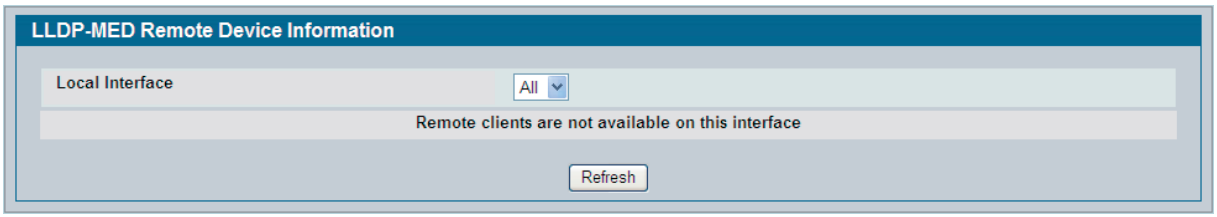


図 4-90　LLDP Remote Device Information 画面

本画面には次の項目があります。

項目	説明
Local Interface	LLDP-MED が有効であるすべてのポートを表示します。
Remote ID	リモートシステムに割り当てられているリモートクライアントの識別子を指定します。
Capability Information	このポートでサポートされており、MED TLV に受信された有効な機能を示します。 • Supported Capabilities - このポートの MED TLV に受信されたサポートする機能を示します。 • Enabled Capabilities - このポートの MED TLV に受信された有効な機能を示します。 • Device Class - ポートにリモート接続するデバイスが通知するデバイスのクラスを示します。
Network Policy Information	ネットワークポリシー TLV がこのポートの LLDP フレームに受信されるかどうかを示します。 • Media Application Type - アプリケーションのタイプを指定します。アプリケーションのタイプには unknown、voicesignaling、guestvoice、guestvoicesignalling、softphonevoice、videoconferencing、streammingvideo、vidoesignalling があります。受信した各アプリケーションのタイプには、VLAN ID、優先度、DSCP、タグ付けされたビットステータス、および未知のビットステータスがあります。ポートは 1 つ以上のアプリケーションタイプを受信することができます。ネットワークポリシー TLV を受信した場合にだけ、本情報が表示されます。 • Vlan ID - 特定のポリシータイプを割り当てた VLAN ID を表示します。 • Priority - 特定のポリシータイプに割り当てた優先度を表示します。 • DSCP - 特定のポリシータイプに割り当てた DSCP を表示します。 • Unknown Bit Status - 特定のポリシータイプに割り当てた未知のビットを表示します。 • Tagged Bit Status - 特定のポリシータイプに割り当てたタグ付きビットを表示します。
Inventory	本ポートで LLDP フレームに受信した inventory TLV を表示します。 • Hardware Revisions - リモートデバイスのハードウェアバージョンを示します。 • Firmware Revisions - リモートデバイスのファームウェアバージョンを示します。 • Software Revisions - リモートデバイスのソフトウェアバージョンを示します。 • Serial Number - リモートデバイスのシリアルナンバーを示します。 • Manufacturer Name - リモートデバイスの製造者名を示します。 • Model Name - リモートデバイスのモデル名を示します。 • Asset ID - リモートデバイスの資産番号を示します。
Location Information	本ポートの LLDP フレームに受信した location TLV を表示します。 • Sub Type - ロケーション情報のタイプを表示します。 • Location Information - 与えられたロケーション ID のタイプの文字列としてロケーション情報を示します。
Extended PoE	リモートデバイスが PoE デバイスであるかどうか示します。 • Device Type - 本ポートに接続するリモートデバイスの PoE デバイスタイプを示します。
Extended PoE PSE	extended PSE TLV が本ポートの LLDP フレームに存在するかどうかを示します。 • Available - リモートデバイスのポートに可能な電源装置（PSE）の電力値（1/10W）を示します。 • Source - リモートポートの PSE 電源を示します。 • Priority - リモートポートの PSE 電源優先度を示します。
Extended PoE PD	extended PD TLV が本ポートの LLDP フレームに存在するかどうかを示します。 • Required - リモートポートの電源装置の電力要求を示します。 • Source - リモートポートの PD 電源を示します。 • Priority - リモートポートの PD 電源優先度を示します。

「Refresh」ボタンをクリックし、システムの情報を最新に更新します。

第 5 章　L3 機能の設定

D-Link 統合アクセスシステムは IP ルーティングをサポートしています。**LAN タブ > L3 Features** の順にメニューをクリックし、機能のリンクを使用してシステムのルーティングを管理します。このセクションには以下の情報があります。

設定項目	説明	参照ページ
ARP の設定	レイヤ 2 の MAC アドレスをレイヤ 3 の IPv4 アドレスに関連付けします。	178 ページ
グローバルおよびインタフェース IP の設定	IP ルーティングデータを設定します。	181 ページ
BOOTP/DHCP リレーエージェントの管理	BOOTP/DHCP リレーエージェントの設定および表示を行います。	185 ページ
RIP の設定	RIP の設定を行います。	187 ページ
ルータの検出	Router Discovery プロトコルを使用して、サブネット上の動作可能なルータを識別します。	192 ページ
ルーティング設定	ルートテーブルの設定および参照を行います。	194 ページ
VLAN ルーティング	VLAN ルーティングの設定を行います。	198 ページ
VRRP 設定	仮想ルータの設定を行います。	200 ページ
ループバックインタフェース	ループバックインタフェースの新規作成、削除、および管理を行います。	206 ページ

パケットがスイッチに入力されると、宛先 MAC アドレスが設定済みのルーティングインタフェースのどれかに一致するかどうかをチェックします。これを行う場合、次に宛先 IP アドレスの照合のためにホストテーブルを検索します。エントリが見つかると、パケットは、そのホストに送信されます。一致するエントリがなければ、スイッチは宛先 IP アドレスで最も長いプレフィックスの照合を実行します。エントリが見つかると、パケットは次のホップに送信されます。一致しないと、パケットはデフォルトルートに指定されている次のホップに送信されます。デフォルトルートが設定されていない場合、パケットは CPU に渡され、適切に処理されます。

ルーティングテーブルには、管理者がスタティックに追加したエントリ、またはルーティングプロトコル経由でダイナミックに追加したエントリがあります。ホストテーブルには、管理者がスタティックに、または ARP 経由でダイナミックに追加したエントリがあります。

ARP の設定

ARP プロトコルは、レイヤ 2 の MAC アドレスをレイヤ 3 の IPv4 アドレスに関連付けします。D-Link ソフトウェアはダイナミックおよびマニュアル ARP 設定の両方をサポートしています。マニュアル ARP 設定を使用する場合、エントリをスタティックに ARP テーブルに追加することができます。

ARP は、インターネットプロトコル（IP）の必要な部分であり、イーサネットなどのローカルエリアネットワーク（LAN）によって定義されたメディア（MAC）アドレスに IP アドレスを変換するために使用されます。IP パケットを送信する必要があるステーションは、宛先が同じサブセットでない場合、IP 宛先、または次のホップルータの MAC アドレスを学習する必要があります。これは、ARP リクエストパケットをブロードキャストすることによって実行されます。指定の受信者は、MAC アドレスを含む ARP リプライをユニキャスティングすることによって応答します。一度学習すると、MAC アドレスは IP パケットに最初に付加されたレイヤ 2 ヘッダの宛先アドレスフィールドで使用されます。

ARP キャッシュは、ネットワークの各ステーション内にローカルに保持されているテーブルです。ARP キャッシュエントリは、ARP リクエストまたは応答であるかにかかわらず ARP パケットペイロードフィールドにおける送信元情報を検証することによって学習されます。そのため、ARP リクエストが LAN セグメントまたは仮想 LAN（VLAN）上のすべてのステーションにブロードキャストされる場合、すべての受信者には、それぞれの ARP キャッシュにある送信元の IP および MAC アドレスを保存する機会があります。ユニキャストである ARP の応答は、通常、ARP キャッシュにある送信元情報を保存しているリクエストを行った送信者にだけ参照されます。新しい情報は、常に ARP キャッシュにある既存のコンテンツと置き換えられます。

サポートしている ARP エントリ数は D-Link 統合スイッチでは 2048 です。

デバイスは、ネットワーク内で移動することができます。つまり、ある MAC アドレスに関連付けされている IP アドレスが異なる MAC を使用して検出されたり、再設定、接続の解除、または電源オフのためにネットワーク全体から見えなくなります。
アドレスがまだ存在しているかどうか判断するためには、定期的に更新されるネットワークで検出される新しい情報に合わせてエントリを更新するか、エントリが、通常はコンフィグレーションを通じて設定されているエージングアウトで ARP パケットの送信者として特定されない場合にはキャッシュから削除しないと、ARP キャッシュ内の古い情報を引き継ぎます。

LAN タブ > L3 Features > ARP には ARP の詳細の設定および参照する以下の機能があります。

- ARP の作成
- ARP テーブルの設定

ARP の作成

Address Resolution Protocol テーブルにエントリを追加します。

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

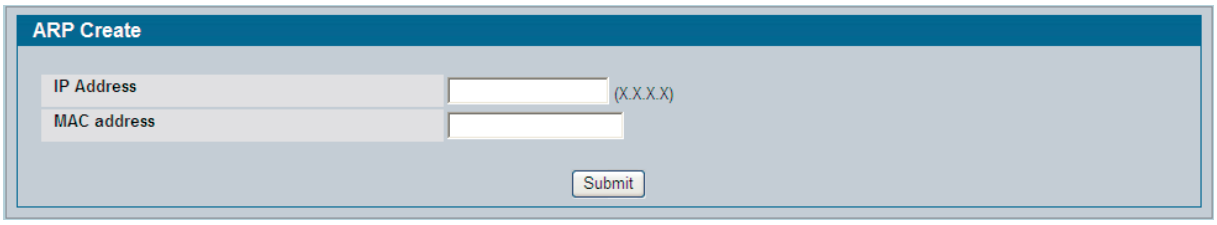


図 5-1　ARP Create 画面

本画面には次の項目があります。

項目	説明
IP Address	追加する IP アドレスを入力します。スイッチに存在するルーティングインタフェースの 1 つに接続するサブネットにあるデバイスの IP アドレスである必要があります。
MAC Address	デバイスのユニキャスト MAC アドレス。2 桁ずつ「:」（コロン）で区切った 6 個の 16 進数（例 :00:06:29:32:81:40）を入力します。

IP アドレスと関連 MAC アドレスを入力後に、「Submit」ボタンをクリックして変更をスイッチに適用し、ARP テーブルにエントリを作成します。

ARP テーブルの設定

ARP テーブルの設定項目の変更、およびテーブルの内容の参照を行います。

LAN タブ > L3 Features > ARP > ARP Table 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。

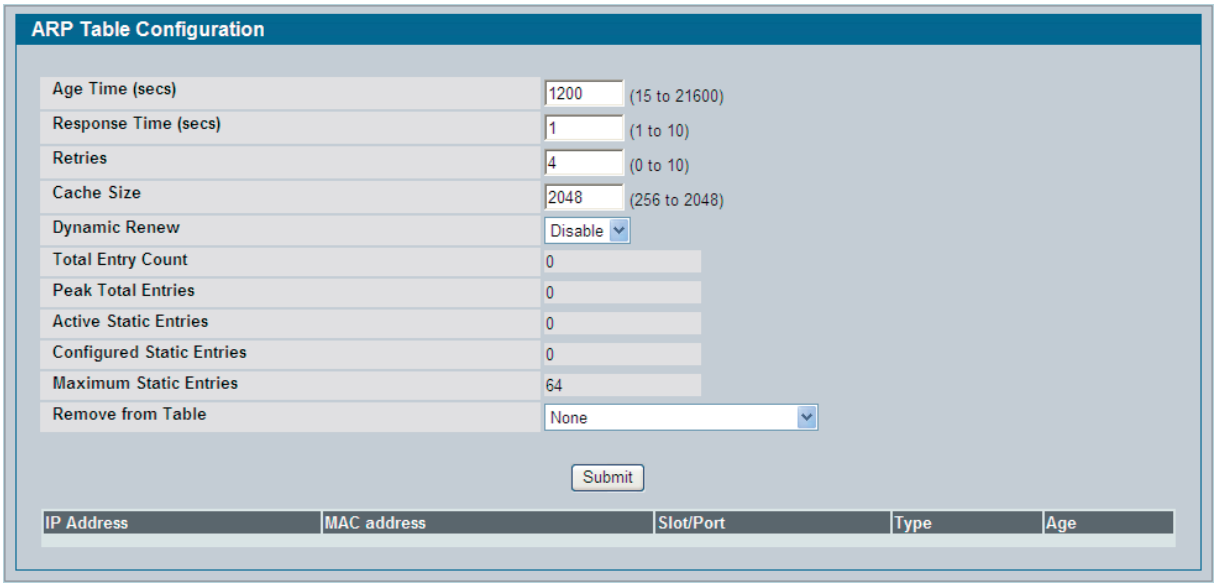


図 5-2　ARP Table Configuration 画面

本画面には次の項目があります。

項目	説明
Age Time (secs)	ARP エントリがエージングアウトに要する時間 15-21600（秒）を指定します。初期値は 1200（秒）です。
Response Time (secs)	スイッチの ARP レスポンス時間を入力します。この範囲は 1-10（秒）です。初期値は 1（秒）です。
Retries	ARP リクエストが再試行される最大数を整数で入力します。この範囲は 1-10 です。再試行回数の初期値は 4 です。
Cache Size	ARP キャッシュの最大登録数を入力します。この値の範囲はプラットフォームに依存します。初期値は 896 です。
Dynamic Renew	ARP コンポーネントがエージングアウトの際に「Dynamic」タイプの ARP エントリを自動的に更新するかどうかを制御します。初期値は「Disable」です。
Total Entry Count	ARP テーブルのエントリの合計数を表示します。
Peak Total Entries	「Total Entry Count」が到達する最も高い値。ARP テーブルの「Cache Size」値を変更する時にはいつも、このカウンタは再起動されます。
Active Static Entries	ARP テーブル内のアクティブなエントリの合計数。
Configured Static Entries	ARP テーブル内のスタティックなエントリの合計数。
Maximum Static Entries	定義できるスタティックエントリの最大数。
Remove from Table	ARP テーブルから削除する ARP エントリのタイプを指定します。 • All Dynamic Entries • All Dynamic and Gateway Entries • Specific Dynamic Gateway Entry • Specific Static Entry
Remove IP Address	ARP テーブルから削除するエントリの IP アドレスを入力します。「Remove from Table」画面で「Specific Dynamic/Gateway Entry」または「Specific Static Entry」を選択した場合に表示されます。
ARP テーブル	
IP Address	スイッチのルーティングインタフェースの 1 つに接続するサブネット上のデバイスの IP アドレス。
MAC Address	デバイスのユニキャスト MAC アドレス。形式は、2 桁ずつ「:」（コロン）で区切った 6 個の 16 進数（例 :00:06:29:32:81:40）です。
Slot/Port	ARP エントリに関連しているルーティングインタフェース。
Type	ARP エントリのタイプ。
Age	エントリが最後に ARP テーブルで更新された時間。フォーマットは hh:mm:ss です。

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。

IP（グローバルおよびインタフェース IP の設定）

LAN タブ > L3 Features > IP には IP ルーティングデータを設定する以下の Web 画面へのリンクがあります。

- Configuration（IP の設定）
- IP Interface Configuration（IP インタフェース設定）

Configuration（IP の設定）

インタフェースに対応するスイッチにルーティングパラメータを設定します。

LAN タブ > L3 Features > IP > 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。

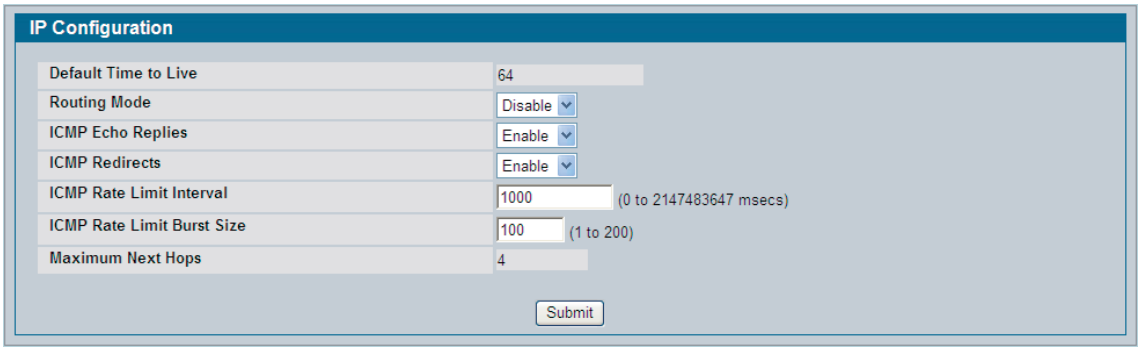


図 5-3　IP Configuration 画面

本画面には次の項目があります。

項目	説明
Default Time to Live	TTL 値がトランスポートレイヤプロトコルに提供されないと、スイッチが生成したデータの IP ヘッダの Time-To-Live フィールドには初期値が挿入されます。
Routing Mode	「Enable」または「Disable」を選択します。インタフェースのどれかを通して送信する前にスイッチのルーティングを有効にする必要があります。ルーティングは、VLAN インタフェースごとに有効または無効にされます。初期値は「Disable」（無効）です。
ICMP Echo Replies	「Enable」または「Disable」を選択します。「Enable」を選択すると、ルータだけがエコーリプライを送信することができます。初期値では、エコーリクエストに対して ICMP エコーリプライを送信します。
ICMP Redirects	インタフェースレベルでグローバルに有効にすると、ルータだけが ICMP リダイレクトを送信することができます。
ICMP Rate Limit Interval	ICMP エラーパケットを制御するために、バースト間隔ごとに許可される ICMP エラーパケット数を指定できます。初期値では、レートのリミットは 100（パケット / 秒）、つまり、バースト間隔は 1000（ミリ秒）です。ICMP レートの制限を無効にするために、本フィールドを 0 に設定します。有効範囲は 0-2147483647（ミリ秒）です。
ICMP Rate Limit Burst Size	ICMP エラーパケットを制御するために、バースト間隔ごとに許可される ICMP エラーパケット数を指定します。初期値では、バーストサイズは 100 パケットです。バース間隔を 0 にすると、本項目は無効になります。有効なバーストサイズの範囲は、1-200 です。
Maximum Next Hops	スイッチでサポートするホップの最大数を表示します。

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。

IP インタフェース設定

本スイッチに対する IP インタフェースデータを更新します。

LAN タブ > L3 Features > IP > Interface 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。

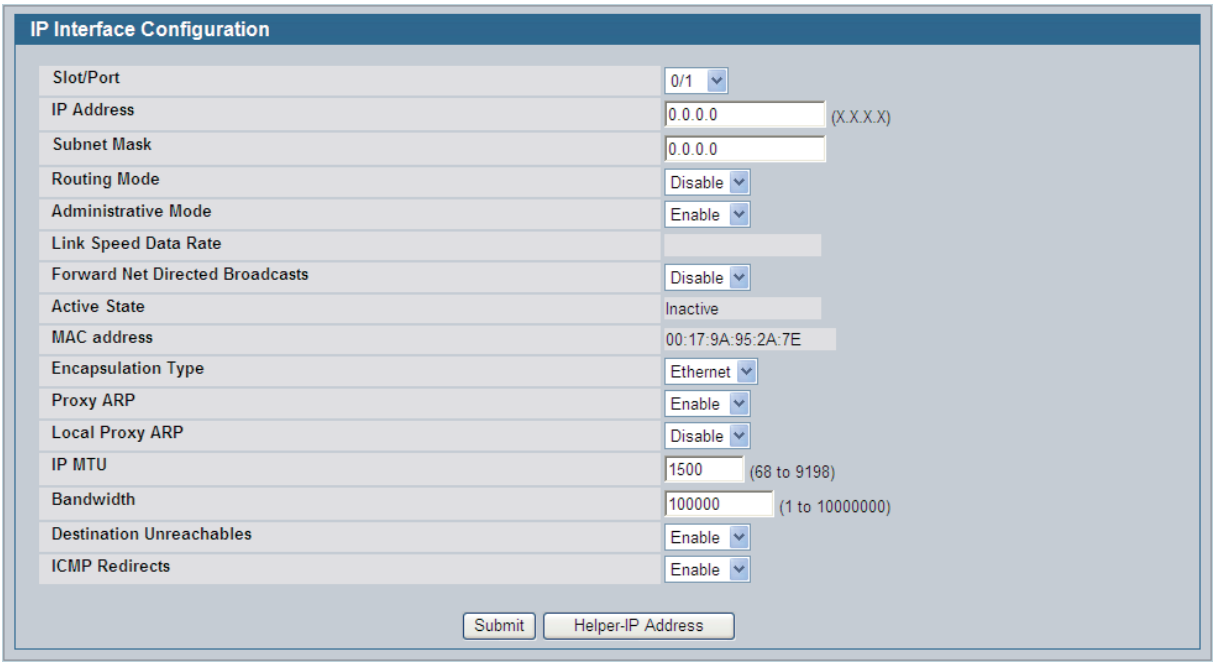


図 5-4　IP Interface Configuration 画面

本画面には次の項目があります。

項目	説明
Slot/Port	設定するインタフェースを選択します。インタフェースにはループバックインタフェースと VLAN ルーティングインタフェースを含む論理インタフェースがあります。
IP Address	インタフェースの IP アドレスを入力します。
Subnet Mask	インタフェースの IP サブネットマスクを入力します。これは、サブネット / ネットワークマスクとして参照され、接続するネットワークを識別するのに使用されます。
Routing Mode	インタフェースに対するルーティングを有効または無効に設定します。初期値では、ルーティングはポートベースのルーティングインタフェースでは無効に、VLAN ベースのルーティングインタフェースでは有効になっています。
Administrative Mode	インタフェースの管理モード。初期値は有効です。
Link Speed Data Rate	指定インタフェースの物理リンクのデータレート（Mbits）を示します。このデータは、物理インタフェースにだけ有効です。
Forward Net Directed Broadcasts	ネットワーク directed ブロードキャストパケットが処理される方法を選択します。 • Enable - ネットワークが指示するブロードキャストは転送されます。 • Disable - ブロードキャストは破棄されます。（初期値）
Active State	指定インタフェースの状態（「Active」または「Inactive」）を表示します。リンクがアップしていて、forwarding 状態であるなら、インタフェースはアクティブであると見なされます。
MAC Address	指定インタフェースの物理アドレスを表示します。形式は、2 桁ずつ「:」（コロン）で区切った 6 個の 16 進数（例 :00:06:29:32:81:40）です。この値は物理インタフェースに有効です。VLAN ルーティングインタフェースなどの論理インタフェースに対しては、システムの MAC アドレスを表示します。
Encapsulation Type	指定インタフェースから送信されたパケットに対するリンクレイヤのカプセル化タイプ（「Ethernet」と「SNAP」）を選択します。初期値は「Ethernet」です。
Proxy ARP	「Disable」または「Enable」を選択し、指定インタフェースのプロキシ ARP を有効または無効にします。
Local Proxy ARP	「Disable」または「Enable」を選択し、指定インタフェースのローカルプロキシ ARP を有効または無効にします。
IP MTU	インタフェースに送信される IP パケットの最大転送単位（MTU）。有効範囲は 68-9198 です。初期値は 1500 です。
Bandwidth	インタフェースの設定帯域幅（Kbps）を指定します。これが設定されないと、帯域幅はポートベースルーティングインタフェースには実際のインタフェース帯域幅に、VLAN ルーティングインタフェースには 10Mbps を初期値として設定します。この値はインタフェースの実際のスピードに影響しません。
Destination Unreachables	インタフェースに ICMP Destination Unreachables を送信するモードを指定します。これが無効にされると、インタフェースは ICMP Destination Unreachables を送信しません。初期値は「Enable」です。
ICMP Redirects	Redirects がグローバルにインタフェースで有効にされる場合にだけ、ルータは ICMP Redirect をインタフェースに送信します。初期値は「Enable」です。

「Submit」ボタンをクリックし、変更をスイッチに適用します。「Save」が実行されないと、これらの変更は再起動後に保持されません。

Helper IP のインタフェース設定

Helper IP のアドレスをインタフェースに追加します。IP Helper 機能により、スイッチは特定の UDP ブロードキャストパケットを特定の IP アドレスに送信することができます。これにより、様々なアプリケーションは、アプリケーションがサーバが常にローカルサブネットにあると仮定するように設計されていても、non-local サブネットにあるサーバに到達することができます。また、（限定的なブロードキャストアドレス 255.255.255.255 またはネットワークの directed ブロードキャストアドレスのいずれかを持つ）ブロードキャストパケットを使用してサーバに到達することができます。

グローバルに指定したルーティングインタフェースにリレーエントリを設定できます。各リレーのエントリは、1 つの IPv4 アドレス（helper アドレス）にイングレスインタフェースと宛先 UDP 番号をマップします。同じインタフェースと UDP ポートに複数のリレーエントリを設定できます。この場合、リレーエージェントは、各サーバのアドレスに一致するパケットをリレーします。インタフェース設定はグローバル設定より優先します。
つまり、パケットの宛先 UDP ポートがイングレスインタフェース上のいずれかのエントリに一致すると、インタフェース設定に従って、パケットは処理されます。

「Helper-IP Address」ボタンをクリックし、「Helper IP Interface Configuration」画面を表示します。

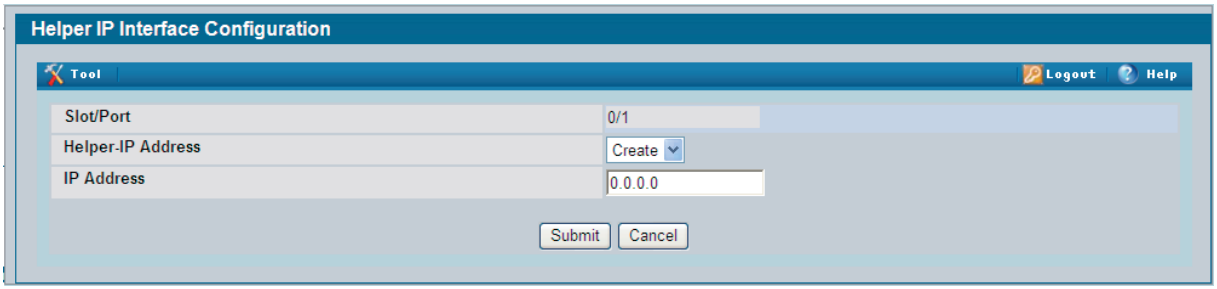


図 5-5　Helper IP Interface Configuration 画面

本画面には次の項目があります。

項目	説明
Slot/Port	データを表示または設定するインタフェース。
Helper-IP Address	データを表示する IP アドレス。Helper IP アドレスをインタフェースに追加するためには「Create」を選択します。
IP Address	インタフェースの Helper IP アドレスを入力します。この値は、設定後は読取専用となります。

「Submit」ボタンをクリックし、更新した設定内容をスイッチに送信します。「Save」が実行されないと、これらの変更は再起動後に保持されません。

Helper IP アドレスを削除

「Delete」ボタンをクリックし、インタフェースから選択した Helper IP アドレスを削除します。「Cancel」ボタンをクリックすると、画面の設定は取り消され、スイッチの最新の値に画面のデータはリセットされます。

IP 統計情報

IP 統計情報を表示します。レポートされる統計情報は、RFC1213 で指定されています。

LAN タブ > Monitoring > L3 Status > IP 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。

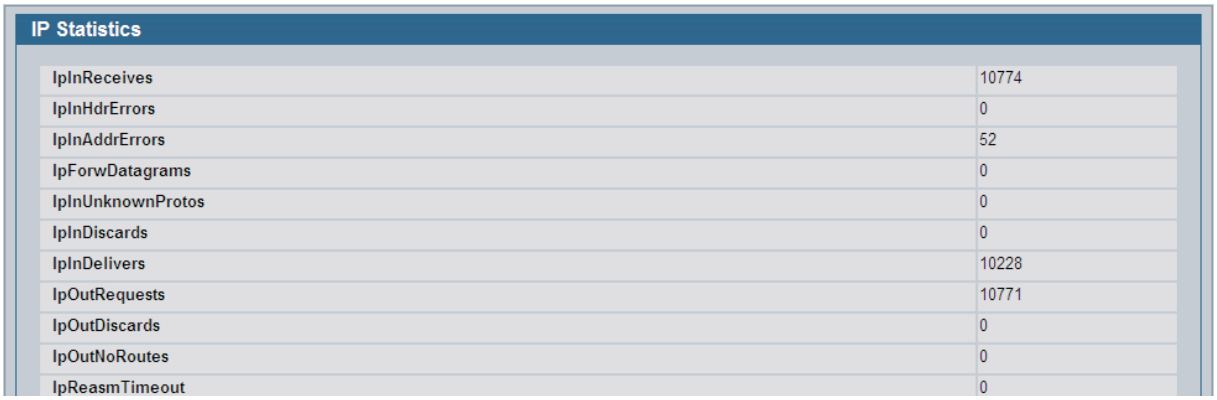


図 5-6　IP Statistics 画面

本画面には次の項目があります。

項目	説明
IpInReceives	インタフェースから受信した入力データの総数（エラーデータも含む）。
IpInHdrErrors	不正なチェックサム、バージョン番号の不一致、他のフォーマットエラー、time-to-live の超過など IP オプションの処理中に検出されたエラーのために破棄された入力データ数。
IpInAddrErrors	IP ヘッダの宛先フィールドにある IP アドレスがこのエンティティで受信されるべき有効なアドレスではないため、破棄された入力データ数。このカウンタには不正なアドレス（例：0.0.0.0）および未サポートのクラス（例：クラス E）を含みます。IP ゲートウェイではないのでデータを転送しないエンティティは、本カウンタに宛先アドレスがローカルアドレスではないので破棄したデータも含まれます。

項目	説明
IpForwDatagrams	最終到達先にそれらを転送する経路を検索しようとした結果、このエンティティが最終 IP の宛先ではなかった入力データ数。IP ゲートウェイとして動作しないエンティティでは、本カウンタには、このエンティティ経由で Sourced-Routed パケットで、Sourced-Routed オプションの処理に成功したパケットだけが含まれます。
IpInUnknownProtos	正常に受信した自分宛てのデータグラムのうち、未知または未サポートのプロトコルのため破棄されたデータ数。
IpInDiscards	受信した IP データのうち、継続的な処理を妨げるような問題がなかったが、バッファスペースの不足などの理由で破棄された入力 IP データ数。このカウンタが再構成を待つ間に廃棄されたデータを含まないことに注意してください。
IpInDelivers	IP ユーザプロトコル（ICMP を含む）に正常に転送された IP データ合計数。
IpOutRequests	ローカルな IP ユーザプロトコル（ICMP を含む）が送信要求で IP に提供した IP データの総数。このカウンタには、ipForwDatagrams でカウントされたデータは含まれないことに注意してください。
IpOutDiscards	宛先への送信を妨げるような問題がなかったが、バッファスペースの不足などの理由で破棄された出力 IP データの数。そのようなパケットがこの（任意の）廃棄基準を満たした場合は、このカウンタは ipForwDatagrams の中でカウントされるデータも含まれます。
IpOutNoRoutes	宛先へ送信するための経路が見つからなかったために破棄された IP データの数。このカウンタは「no-route」（ルートなし）の基準を満たす ipForwDatagrams の中で間とされたパケットを含みます。また、そのデフォルトゲートウェイがすべてダウンしているためにホストがルーティングすることができないデータグラムを含まれます。
IpReasmTimeout	受信したフラグメントが、このエンティティで再構成待ちである間、保持される最大時間（秒）。
IpReasmReqds	エンティティで再構成が必要とされる受信した IP フラグメントの数。
IpReasmOKs	再構成に成功した IP データの数。
IpReasmFails	タイムアウト、エラーなど何らかの理由で IP 再構成アルゴリズムにより検出された失敗の回数。いくつかのアルゴリズムがフラグメントの受信時に結合したために、フラグメント数のトラッキングに失敗する可能性があるため、これが必ずしも廃棄された IP フラグメントのカウントではないことに注意してください。
IpFragOKs	エンティティでフラグメント化に成功した IP データの数。
IpFragFails	このエンティティでフラグメント化される必要があるにもかかわらず、Don't Fragment フラグが設定されているなどの理由で行われなかったために破棄された IP データの数。
IpFragCreates	このエンティティでフラグメンテーションの結果として生成された IP データフラグメントの数。
IpRoutingDiscards	それらが有効であっても破棄されるように選択されたルーティングエントリの数。エントリなどを破棄する理由は、他のルーティングエントリのためにバッファスペースを解放することです。
IcmpInMsgs	エンティティが受信した ICMP メッセージの総数。これには icmpInErrors によってカウントされるすべてのものを含みます。
IcmpInErrors	エンティティが受信した ICMP メッセージのうち ICMP 特有のエラー（不正な ICMP チェックサム、不正な長さなど）を持っている判断された数。
IcmpInDestUnreachs	受信した ICMP Destination Unreachable メッセージの数。
IcmpInTimeExcds	受信した ICMP Time Exceeded メッセージの数。
IcmpInParmProbs	受信した ICMP Parameter Problem メッセージの数。
IcmpInSrcQuenchs	受信した ICMP Source Quench メッセージの数。
IcmpInRedirects	受信した ICMP Redirect メッセージの数。
IcmpInEchos	受信した ICMP Echo（request）メッセージの数。
IcmpInEchoReps	受信した ICMP Echo Reply メッセージの数。
IcmpInTimestamps	受信した ICMP Timestamp（request）メッセージの数。
IcmpInTimestampReps	受信した ICMP Timestamp Reply メッセージの数。
IcmpInAddrMasks	受信した ICMP Address Mask Request メッセージの数。
IcmpInAddrMaskReps	受信した ICMP Address Mask Reply メッセージの数。
IcmpOutMsgs	このエンティティが送信を試みた ICMP メッセージの総数。このカウンタには icmpOutErrors によってカウントされたすべてのものを含みます。
IcmpOutErrors	バッファの不足など ICMP の中で発見された問題のためにこのエンティティが送信しなかった ICMP メッセージの数。この値は、IP が結果として生じるデータをルーティングできないような ICMP レイヤの外側で発見されたエラーを含むべきではありません。いくつかのインプリメンテーションでは、このカウンタの値に寄与するエラータイプが存在しません。
IcmpOutDestUnreachs	送信した ICMP Destination Unreachable メッセージの数。
IcmpOutTimeExcds	送信した ICMP Time Exceeded メッセージの数。
IcmpOutParmProbs	送信した ICMP Parameter Problem メッセージの数。
IcmpOutSrcQuenchs	送信した ICMP Source Quench メッセージの数。
IcmpOutRedirects	送信した ICMP Redirect メッセージの数。ホストが redirect を送信しないため、ホストではこのオブジェクトは常に 0 です。
IcmpOutEchos	送信した ICMP Echo（request）メッセージの数。
IcmpOutEchoReps	送信した ICMP Echo Reply メッセージの数。
IcmpOutTimestamps	送信した ICMP Timestamp（request）メッセージの数。
IcmpOutTimestampReps	送信した ICMP Timestamp Reply メッセージの数。
IcmpOutAddrMasks	送信した ICMP Address Mask Request メッセージの数。

「Refresh」ボタンをクリックすると、最新の情報に更新します。

BOOTP/DHCP リレーエージェントの管理

BootP/DHCP リレーエージェントにより、BootP/DHCP クライアントとサーバが異なるサブネットを経由して BootP/DHCP メッセージを交換することが可能です。リレーエージェントは、クライアントからリクエスト受信して、有効なホップと giaddr フィールドをチェックします。ホップの数が設定より大きいと、エージェントは、パケットがエージェントを通してループしていると見なして、パケットを破棄します。giaddr フィールドが 0 であると、エージェントは、リクエストを受信したインタフェースの IP アドレスを本フィールドに記入する必要があります。エージェントは次に設定されている宛先に有効なパケットをユニキャストします。サーバは、giaddr フィールドの表示に従い、クライアントに最も近いリレーエージェントを送信先とするユニキャスト BOOTREPLY で応答します。サーバから BOOTREPLY を受信すると、エージェントはこの応答を BOOTREQUEST が受信したインタフェース上のブロードキャストまたはユニキャストとして転送します。このインタフェースは、giaddr フィールドによって識別されます。

統合スイッチは、DHCP リレーエージェントオプションをサポートしており、カスタマが高速モデムを使用してインターネットに接続している場合、送信元の回路を識別することができます。リレーエージェントは、サーバにリクエストを転送する場合にこれらのオプションを挿入し、クライアントに応答を送信する場合にこれを削除します。インタフェースに 1 つ以上の IP アドレスがある場合、リレーエージェントは、自身のリレーエージェント IP アドレスとして設定されているプライマリ IP アドレスを使用する必要があります。

以下の項目では、BOOTP/DHCP リレーエージェントの設定および表示を行います。

- BOOTP/DHCP リレーエージェントの設定
- BOOTP/DHCP リレーエージェントステータス

BOOTP/DHCP リレーエージェントの設定

BOOTP/DHCP リレーエージェントの設定および表示を行います。

LAN タブ > L3 Features > BOOTP/DHCP Relay Agent 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。

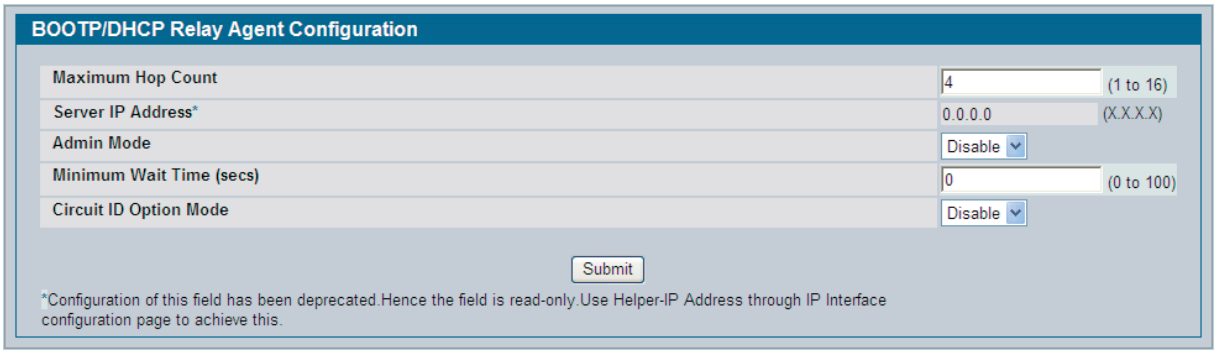


図 5-7　BOOTP/DHCP Relay Agent Configuration 画面

本画面には以下の項目があります。

項目	説明
Maximum Hop Count	破棄されるまでにクライアントリクエストが受け取ることのできる最大ホップ数を入力します。
Server IP Address	BOOTP/DHCP サーバの IP アドレス、または、次の BOOTP/DHCP リレーエージェントのいずれかの IP アドレスを入力します。 注意 この設定は推奨されません。「Helper IP のインタフェース設定」（183 ページ）を使用して同じ機能を実現することができます。
Admin Mode	「Enable」（有効）または「Disable」（無効）を選択します。「Enable」を選択すると、BOOTP/DHCP リクエストは、「Server IP Address」に入力した IP アドレスに転送されます。
Minimum Wait Time (secs)	最小待機時間（秒）を入力します。この値は、クライアントのリクエストパケット内のタイムスタンプと比較されます。タイムスタンプは、クライアントが電源オンされてからの経過時間を表しています。タイムスタンプが最小待機時間を超過した場合にだけパケットは転送されます。
Circuit ID Option Mode	「Enable」（有効）または「Disable」（無効）を選択します。「Enable」を選択すると、リレーエージェントは、サーバに転送する前に、オプション 82 のヘッダパケットを DHCP Request パケットに追加し、応答をクライアントに転送する間に削除します。

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。

BOOTP/DHCP リレーエージェントステータス

BOOTP/DHCP リレーエージェント設定とステータス情報を表示します。

LAN タブ > Monitoring > L3 Status > BOOTP/DHCP Relay Agent 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。

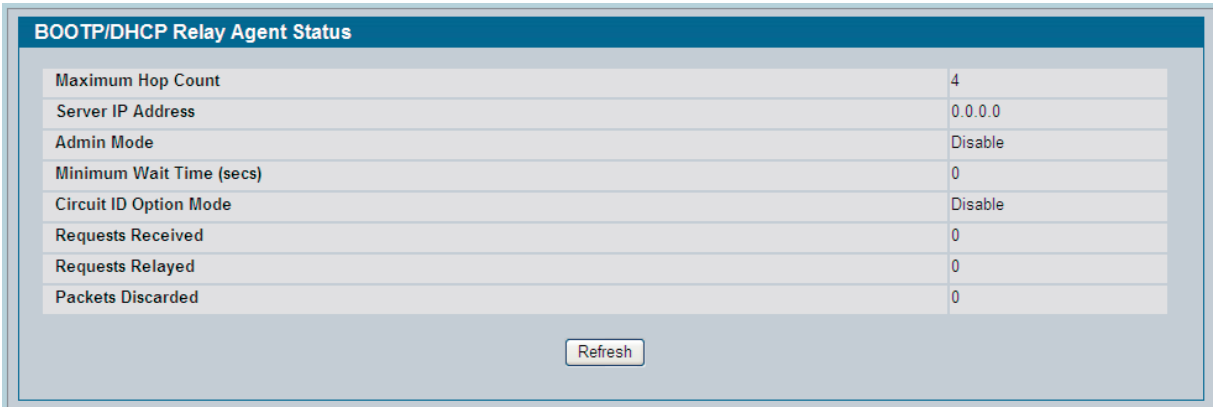


図 5-8　BOOTP/DHCP Relay Agent Status 画面

本画面には以下の項目があります。

項目	説明
Maximum Hop Count	破棄されずにクライアントリクエストが移動できる最大ホップ数。
Server IP Address	BOOTP/DHCP サーバの IP アドレス、または次の BOOTP/DHCP リレーエージェントの IP アドレス。
Admin Mode	リレーの管理モード。「Enable」（有効）を選択すると、BOOTP/DHCP リクエストは、「Server IP Address」に入力した IP アドレスに転送されます。
Minimum Wait Time (secs)	最小時間（秒）。この値は、クライアントのリクエストパケット内のタイムスタンプと比較されます。タイムスタンプは、クライアントが電源オンされてからの経過時間を表しています。タイムスタンプが最小待機時間を超過した場合にのみパケットは転送されます。
Circuit ID Option Mode	これはリレーエージェントオプションの状態。「Enable」（有効）の場合、リレーエージェントは、サーバに転送する前に、オプション 82 のヘッダパケットを DHCP Request パケットに追加し、応答をクライアントに転送する間に削除します。
Requests Received	スイッチが最後にリセットされてから、すべてのクライアントから受信した BOOTP/DHCP リクエストの総数。
Requests Relayed	スイッチが最後にリセットされてから、サーバに転送された BOOTP/DHCP リクエストの総数。
Packets Discarded	スイッチが最後にリセットされてから、このリレーエージェントによって破棄された BOOTP/DHCP パケットの総数。

RIP の設定

RIP は、Bellman-Ford アルゴリズムに基づく Interior ゲートウェイプロトコル（IGP）で、小さいネットワーク（15 以下のネットワーク規模）をターゲットにしています。ルーティング情報は、定期的、およびネットワークトポロジに変更があった場合に送信される RIP 更新パケット内に反映されます。RIP の更新を受信すると、指定したルートがルートテーブルに存在するかどうかによって、ルータはルートテーブル内のルートを変更、削除、またはルートテーブルにルートを追加します。

LAN タブ > L3 Features > RIP フォルダには RIP パラメータとデータを設定および参照する以下の機能があります。

- RIP の設定
- RIP インタフェースのサマリ
- RIP インタフェース設定
- RIP インタフェースのサマリ
- RIP 経路再配布のサマリ

RIP の設定

「Global」モードの RIP の設定、RIP の有効 / 無効を行います。

LAN タブ > L3 Features > RIP > 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。

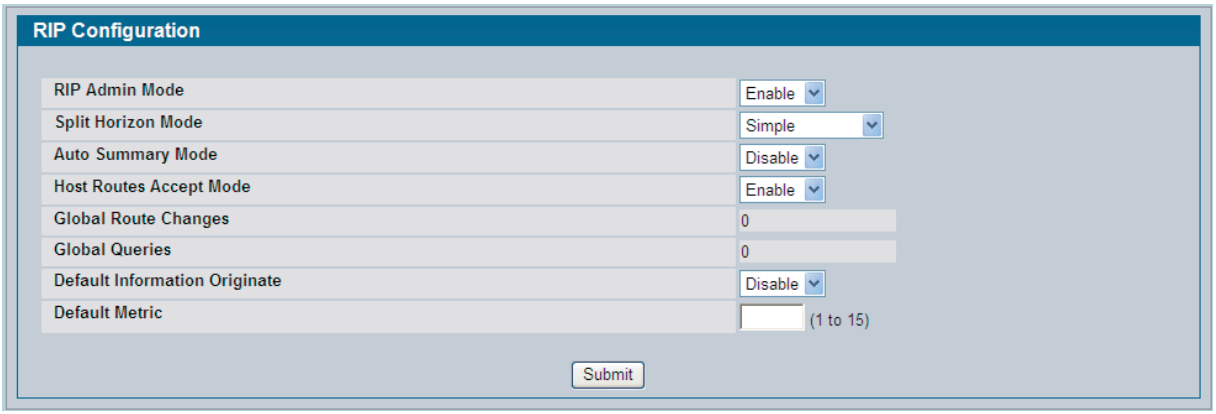


図 5-9　RIP Configuration 画面

本画面には以下の項目があります。

項目	説明
RIP Admin Mode	「Enable」（有効）または「Disable」（無効）を選択します。「Enable」を選択すると、RIP はスイッチに有効となります。初期値は「Disable」（無効）です。
Split Horizon Mode	「None」、「Simple」、または「Poison Reverse」を選択します。Split horizon（水平分割）は、ルートを最初に学習したルータに送信される更新にルートを含めることによって発生する問題を回避するためのテクニックです。 • None - この場合には特別な処理は行いません。 • Simple - ルートは、学習されたルータに送信される更新に含まれていません。（初期値） • Poison Reverse - ルートは、学習されたルータに送信される更新に含まれますが、メトリックが無限に設定されます。
Auto Summary Mode	「Enable」（有効）または「Disable」（無効）を選択します。「Enable」を選択すると、隣接するルートのグループは、エントリの総数を減少させるために、単一のエントリにまとめられます。初期値は「Disable」です。
Host Routes Accept Mode	「Enable」（有効）または「Disable」（無効）を選択します。「Enable」を選択すると、ルータはホストルートを受け入れます。初期値は「Enable」です。
Global Route Changes	RIP が IP ルートデータベースに行ったルート変更の回数を表示します。これには、ルートのエージングのリフレッシュは含まれません。
Global Queries	RIP クエリに対して他のシステムから送信された応答数を表示します。
Default Information Originate	有効な場合、RIP はデフォルトルート（0.0.0.0/0.0.0.0）を生成します。
Default Metric	再割り当てされたルートのメトリックに初期値を設定します。既に設定されている場合にはデフォルトメトリックを、以前に設定していない場合にはブランクが表示されます。有効な値は 1-15 です。

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。

RIP インタフェース設定

特定のインタフェースの RIP の設定、RIP の有効 / 無効化を行います。

LAN タブ > L3 Features > RIP > Interface 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。

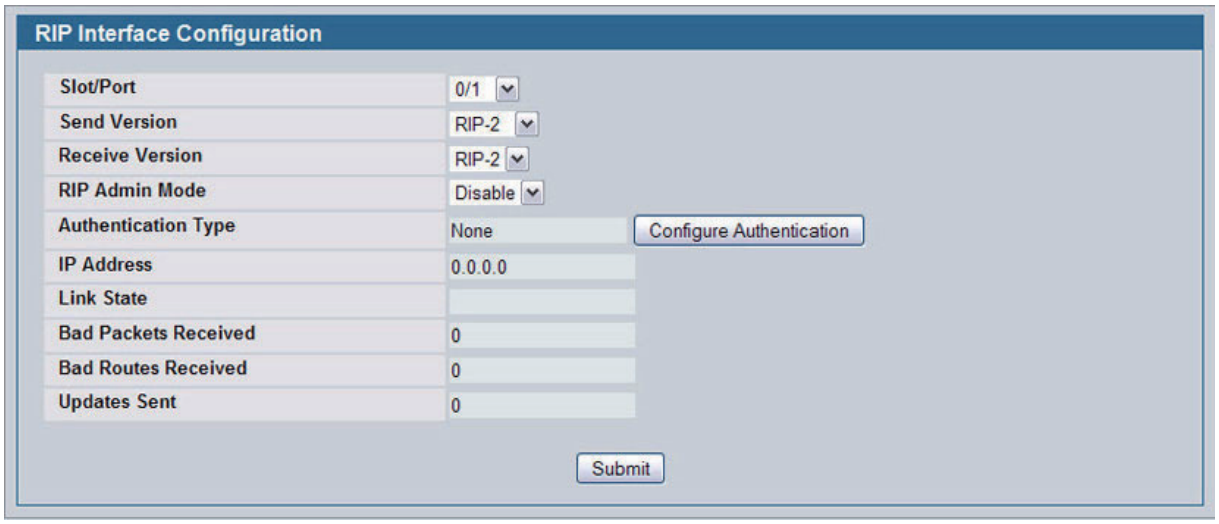


図 5-10　RIP Interface Configuration 画面

本画面には以下の項目があります。

項目	説明
Slot/Port	データを設定するインタフェースを選択します。
Send Version	ルータがルーティングの更新と共に送信する RIP バージョンを指定します。 • RIP-1 - ブロードキャスト経由で RIP バージョン 1 形式のパケットを送信します。 • RIP-1c - RIP バージョン 1 互換モードです。ブロードキャスト経由で RIP バージョン 2 形式のパケットを送信します。 • RIP-2 - マルチキャストを使用して RIP バージョン 2 パケットを送信します。（初期値） • None - RIP 制御パケットは送信されません。
Receive Version	ルータが受け入れる必要のあるルーティング更新の RIP バージョン。 • RIP-1 - RIP バージョン 1 形式のパケットを受け入れます。 • RIP-2 - RIP バージョン 2 形式のパケットを受け入れます。 • Both - どちらの形式のパケットも受け入れます。（初期値） • None - RIP 制御パケットは受け付けません。
RIP Admin Mode	「Enable」（有効）または「Disable」（無効）を選択します。RIP バージョン 1 またはバージョン 1c をインタフェースで有効にする前に、最初に関連するインタフェースのネットワーク directed broadcast モードを有効にします。初期値は「Disabled」です。
Authentication Type	「Configuration Authentication」ボタンをクリックして、「None」以外の認証タイプを選択します。新しい画面で認証タイプを選択します。 • None - これはインタフェースの初期状態です。2 番目の画面のプルダウンメニューからこのオプションを選択すると、認証プロトコルは実行されずに最初の画面に戻ります。 • Simple - これを選択すると、認証キーの入力用のプロンプトが表示されます。このキーは、ネットワークにおいて送信されるすべてのパケットの RIP ヘッダにプレーンテキストで含まれています。ネットワーク上のすべてのルータは、同一のキーで設定される必要があります。 • Encrypt - これを選択すると、認証キーと認証 ID の両方のプロンプトが表示されます。暗号化は、MD5 メッセージダイジェストアルゴリズムを使用します。ネットワーク上のすべてのルータは、同一のキーと ID で設定される必要があります。
IP Address	ルータインタフェースの IP アドレスを表示します。
Link State	RIP インタフェースがアップまたはダウンしているかどうかを表示します。
Bad Packets Received	無効または不正であることが見つけられた RIP パケットの数を表示します。
Bad Routes Received	このインタフェースに実際に送信され、始動される RIP の更新数など何らかの理由で無視された無効な RIP パケット内のルートの数を表示します。これは、新しい情報が含まれた状態で送信されたフルアップデートは明確に含まれません。
Updates Sent	送信されたルート更新数を表示します。

RIP インタフェースの設定

1. 「RIP Interface Configuration」画面を表示します。

2. 設定するデータのインタフェースを選択します。

3. 必要とされるデータを入力します。

4. 「Authentication Type」を変更するためには、「Configure Authentication」ボタンをクリックし、別の認証タイプを設定します。画面は更新され、「RIP Interface Authentication Configuration」画面が表示されます。

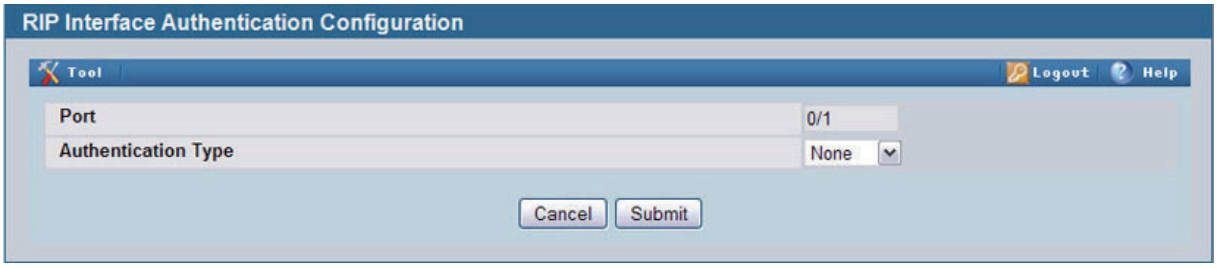


図 5-11　RIP Interface Authentication Configuration 画面

5. 使用する認証タイプを選択します。認証として「Simple」または「Encrypt」を選択すると、画面が更新され、追加の欄が表示されます。ここに必要情報を入力します。

6. 「Submit」ボタンをクリックし、変更をスイッチに適用して「RIP Interface Configuration」画面に戻ります。

7. 認証設定を取り消して、「 RIP Interface Configuration」画面に戻るためには、「Cancel」ボタンをクリックします。

RIP インタフェースのサマリ

インタフェースに RIP コンフィグレーションのステータスを表示します。

LAN タブ > Monitoring > L3 Status > RIP > Interface 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 5-12　RIP Interface Summary 画面

本画面には以下の項目があります。

項目	説明
Slot/Port	RIP が有効であるルーティングが可能な VLAN などのインタフェース。
IP Address	ルータインタフェースの IP アドレス。
Send Version	インタフェースから送信された RIP 制御パケットが従う RIP バージョンを表示します。 • RIP-1 - RIP バージョン 1 パケットをブロードキャストを使用して送信します。 • RIP-1c - RIP バージョン 1 互換モードです。ブロードキャストを使用して RIP バージョン 2 形式のパケットを送信します。 • RIP-2 - マルチキャストを使用して RIP バージョン 2 パケットを送信します。（初期値） • None - RIP 制御パケットは送信されません。
Receive Version	インタフェースによって受け付けられる RIP バージョンの制御パケットを表示します。 • RIP-1 - RIP バージョン 1 形式のパケットだけが受信されます。 • RIP-2 - RIP バージョン 2 形式のパケットだけが受信されます。 • Both - どちらのフォーマットでもパケットを受信します。（初期値） • None - RIP 制御パケットは受信されません。
RIP Admin Mode	RIP がインタフェースで有効または無効であるかを示します。
Link State	RIP インタフェースがアップまたはダウンしているかどうかを表示します。

「Refresh」ボタンをクリックしてと、画面の情報を更新します。

RIP 経路再配布の設定

どのルートが RIP を使用することで他のルータに再配布されるかを設定します。

LAN タブ > L3 Features > RIP > Route Redistribution 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。

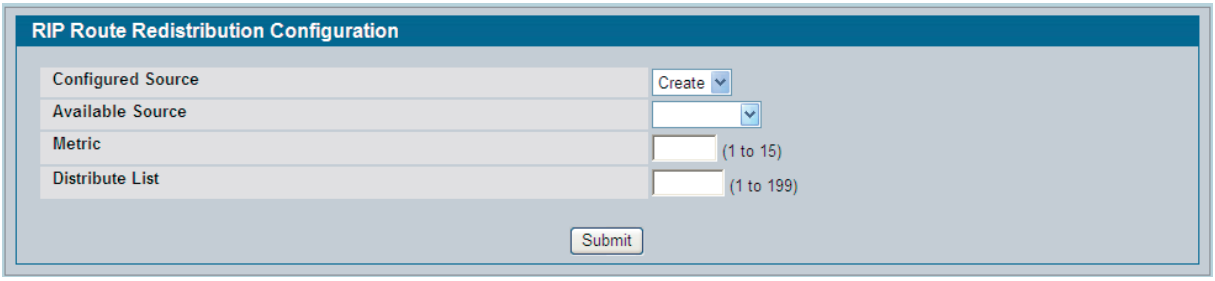


図 5-13　RIP Route Redistribution Configuration 画面

本画面には以下の項目があります。

項目	説明
Configured Source	RIP に既に再配布用に設定されている送信元ルートを表示します。設定されていない場合、「Create」を使用して利用可能な送信元ルートを設定します。パラメータの参照または編集を行うためには、既存のルートを選択します。
Available Source	RIP によって再配布用に設定済みの送信元ルートだけが表示されます。本項目は、「Configured Source」として「Create」を選択した場合にだけ利用可能です。 • Static - ルートは手動で設定されました。 • Connected - ホストが直接接続しているため、ルートは自動的に決定されました。 • RIP - ルートは RIP を通じて決定しました。
Metric	再配布するルートのメトリックとして使用するメトリック値を設定します。本フィールドには、送信元が事前に設定されていて、変更可能であるとメトリックが表示されます。有効な値は 1-15 です。
Distribute List	宛先のプロトコルによって再配布するルートをフィルタするアクセスリストの ACL ID を入力します。許可されたルートだけが再配布されます。

LAN > Access Control Lists > IP Access Control Lists の順にメニューをクリックし、ACL の設定を行います。
ルートフィルタリングに使用される場合、以下の項目がアクセスリストで使用されます。

- 送信元 IP アドレスとネットマスク
- 送信先 IP アドレスとネットマスク
- アクション（許可または拒否）

他のすべてのフィールド（送信元と送信先ポート、優先度、ToS など）は無視されます。変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。

送信元 IP アドレスは、ルートの宛先 IP アドレスと比較されます。アクセスリストルール内の送信元 IP ネットマスクは、ワイルドカードマスクとして扱われ、送信元 IP アドレス内のどのビットがルートの宛先アドレスとマッチする必要があるのかを示しています。マスク内の「1」は、対応するアドレスビット内の「Don't Care」（指定しない）を示します。

アクセスリストルールに送信先 IP アドレスとネットマスク（拡張アクセスリスト）が含まれる場合、送信先の IP アドレスはルートの宛先ネットワークマスクと比較されます。
アクセスリスト内の送信先ネットマスクはワイルドカードマスクとして機能し、ルートの送信先マスク内のどのビットがフィルタリング操作のために重要であることを示します。

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。

経路の削除

設定された経路を削除するために、「Delete」ボタンをクリックします。

RIP 経路再配布のサマリ

経路の再配布の設定を表示します。

LAN タブ > Monitoring > L3 Status > RIP > Route Redistribution 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。

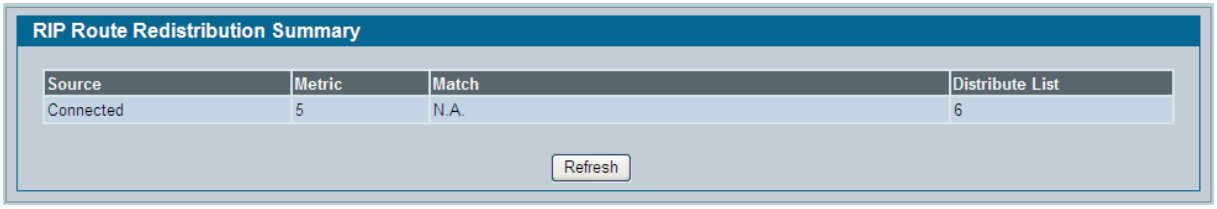


図 5-14　RIP Route Redistribution Summary 画面

本画面には以下の項目があります。

項目	説明
Source	ルートを取得するために使用されるプロトコル。
Metric	指定された送信元ルートに再配布されるルートのメトリック。未設定の場合は、「Unconfigured」が表示されます。
Match	OSPF が送信元として選択されている場合に再配布するルートリストを表示します。「N.A.」は OSPF 以外であることを示しています。
Distribute List	宛先プロトコルが再配布するルートをフィルタするアクセスリスト。配布リストが未設定の場合、このフィールドは空白です。

「Refresh」ボタンをクリックしてと、画面の情報を更新します。

ルータの検出

Router Discovery プロトコルは、サブネット上の動作可能なルータを識別するためにホストによって使用されます。

LAN タブ > L3 Features > Routing > Router Discovery フォルダには Router Discovery データの設定および参照する以下の機能があります。

- ルータディスカバリの設定
- ルータディスカバリの状態

ルータディスカバリの設定

「Router Discovery」パラメータの入力または変更を行います。Router Discovery メッセージには、「Router Advertisements」と「Router Solicitations」の 2 つのタイプがあります。プロトコルは、すべてのルータが関連付けられている IP アドレスを定期的に通知します。ホストはこの通知をリッスンし、隣接ルータの IP アドレスを検出します。

LAN タブ > L3 Features > Router Discovery > 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。

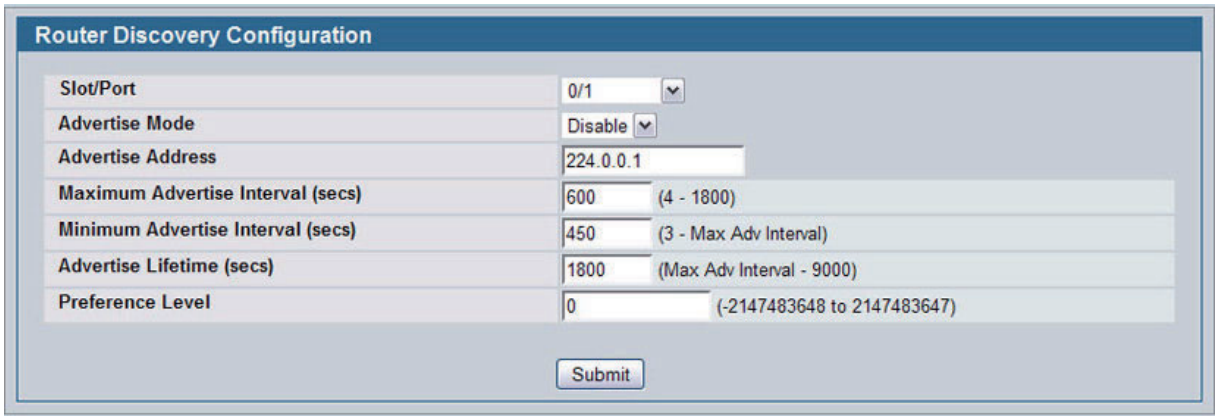


図 5-15　Router Discovery Configuration 画面

本画面には以下の項目があります。

項目	説明
Slot/Port	設定するデータのルータインタフェースを選択します。
Advertise Mode	「Enable」（有効）または「Disable」（無効）を選択します。「Enable」を選択すると、選択したインタフェースから Router Advertisements メッセージが送信されます。
Advertise Address	ルータを通知するために使用される IP アドレスを入力します。
Maximum Advertise Interval (secs)	インタフェースから送信される Router Advertisements メッセージ間の最長時間（秒）を入力します。
Minimum Advertise Interval (secs)	インタフェースから送信される Router Advertisements メッセージ間の最短時間（秒）を入力します。
Advertise Lifetime (secs)	インタフェースから送信される Router Advertisements 内の有効期間フィールドとして使用される値（秒）を入力します。これは、通知されたアドレスが、ホストによって有効なルータのアドレスと見なされる最大の期間です。
Preference Level	同じサブネットにあり他のルータに関連するデフォルトルータとして、このルータの優先度レベルを指定します。より高い数値のアドレスが優先されます。

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。

ルータディスカバリの状態

各ポートの Router ディスカバリデータを表示します。

LAN タブ > Monitoring > L3 Status > Router Discovery 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。

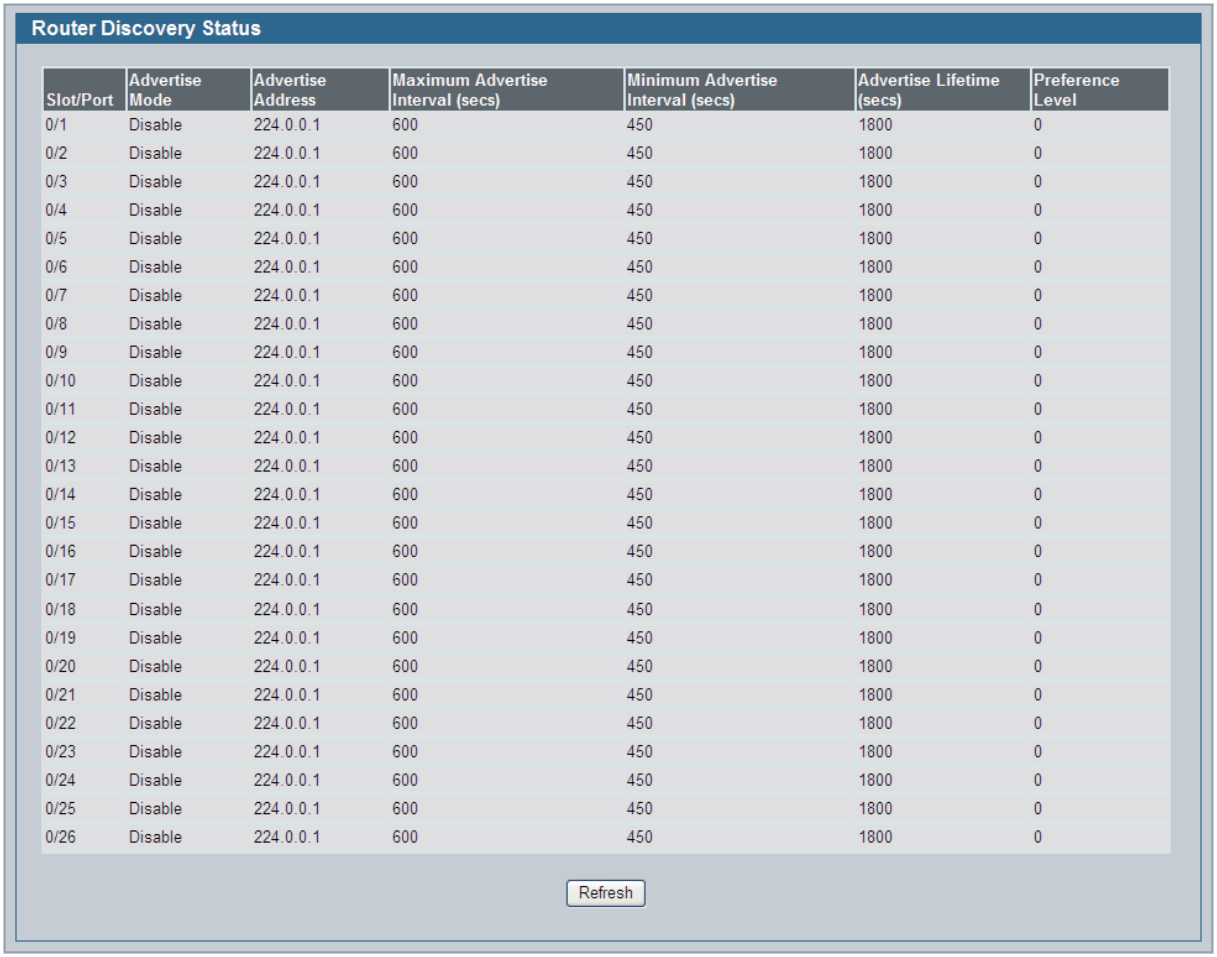


図 5-16　Router Discovery Status 画面

本画面には以下の項目があります。

項目	説明
Slot/Port	データを表示するルータインタフェース。
Advertise Mode	値は「Enable」または「Disable」です。「Enable」（有効）は、そのインタフェースで Router Discovery が有効であることを示します。
Advertise Address	ルータを通知するために使用される IP アドレス。
Maximum Advertise Interval (secs)	インタフェースから送信される Router Advertisements メッセージ間に許容される最長時間（秒）。
Minimum Advertise Interval (secs)	インタフェースから送信される Router Advertisements メッセージ間に許容される最短時間（秒）。
Advertise Lifetime (secs)	インタフェースから送信される Router Advertisements 内の有効期間フィールドとして使用される値（秒）。これは、通知されたアドレスが、ホストによって有効なルータのアドレスと見なされる最大の期間です。
Preference Level	同じサブネットにあり、他のルータに関連するデフォルトルータとしてのルータの優先度レベル。より高い数値のアドレスが優先されます。

「Refresh」ボタンをクリックしてと、画面の情報を更新します。

ルーティング設定

LAN タブ > L3 Features > RouterARP フォルダにはルートテーブルの設定および参照を行う以下の機能があります。

- ルートテーブル
- 最適なルートテーブル
- スタティックルートの設定
- ルート優先度設定

ルートテーブル

ルートテーブルマネージャは複数のソース（スタティックルート、RIP ルート、およびローカルルート）からルートを収集します。ルートテーブルマネージャは、複数ソースから同じ宛先へのルートを複数学習します。ルートテーブルにはすべてのルートがあります。「Best Routes Table」は、各宛先に最も適切なルートだけを表示します。詳しくは、「最適なルートテーブル」（195 ページ）を参照してください。

LAN タブ > Monitoring > L3 Status > 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。

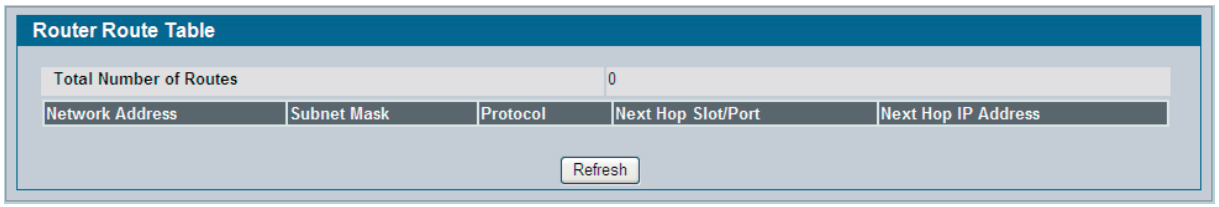


図 5-17　Router Route Table 画面

本画面には以下の項目があります。

項目	説明
Total Number of Routes	ルートテーブルのルートの総数。
Network Address	宛先用の IP ルートのプレフィックス。
Subnet Mask	サブネット / ネットワークマスクとも呼ばれ、これは、接続するネットワークを識別する IP インタフェースアドレス内の部分を示します。
Protocol	指定ルートを作成したプロトコルを示します。可能な値は以下の 1 つです。 • Local • Static • Default • RIP
Next Hop Slot/Port	トラフィックを宛先に送信する場合に使用する外向きのルータインタフェース。
Next Hop IP Address	宛先に向かう経路にある次のルータにトラフィックを転送する場合に使用する外向きのルータの IP アドレス。次のルータは、常に近接ルータの 1 つであるか、直接接続するネットワークのローカルインタフェースの IP アドレスです。

「Refresh」ボタンをクリックしてと、画面の情報を更新します。

最適なルートテーブル

ルートテーブルマネージャは複数のソース（スタティックルート、RIP ルート、およびローカルルート）からルートを収集します。ルートテーブルマネージャは、複数ソースから同じ宛先へのルートを複数学習します。その場合、ルートテーブルマネージャは宛先へのフォワーディングに使用する使用する最も低いルート優先度値を持つルートを選択します。

「Best Routes Table」画面を使用して、ルーティングテーブルから最適なルートを表示します。同じ宛先への複数ルートを含むすべてのルートを参照するためには、「ルートテーブル」（194 ページ）を参照してください。

LAN タブ > L3 Features > Router > Best Routes 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。

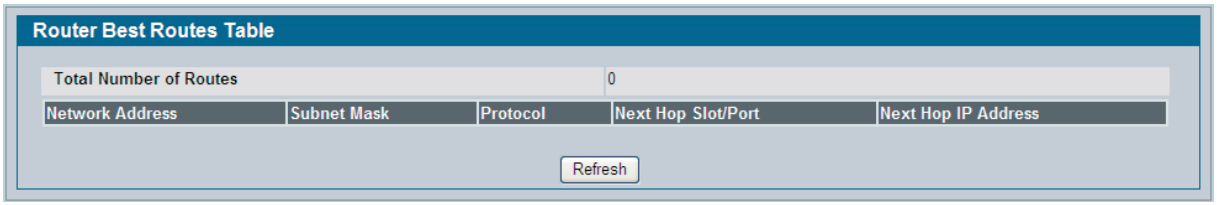


図 5-18　Best Routes Table 画面

本画面には以下の項目があります。

項目	説明
Total Number of Routes	ルートテーブルのルートの総数。
Network Address	宛先用の IP ルートのプレフィックス。
Subnet Mask	サブネット / ネットワークマスクとも呼ばれ、これは、接続するネットワークを識別する IP インタフェースアドレス内の部分を示します。
Protocol	指定ルートを作成したプロトコルを示します。 • Local • Static • Default • RIP
Next Hop Slot/Port	トラフィックを宛先に送信する場合に使用する外向きのルータインタフェース。
Next Hop IP Address	宛先に向かう経路にある次のルータにトラフィックを転送する場合に使用する外向きのルータの IP アドレス。次のルータは、常に近接ルータの 1 つであるか、直接接続するネットワークのローカルインタフェースの IP アドレスです。

「Refresh」ボタンをクリックしてと、画面の情報を更新します。

スタティックルートの設定

スタティックルートの作成および表示をします。

LAN タブ > L3 Features > Router > Configured Routes の順にメニューをクリックし、以下の画面を表示します。

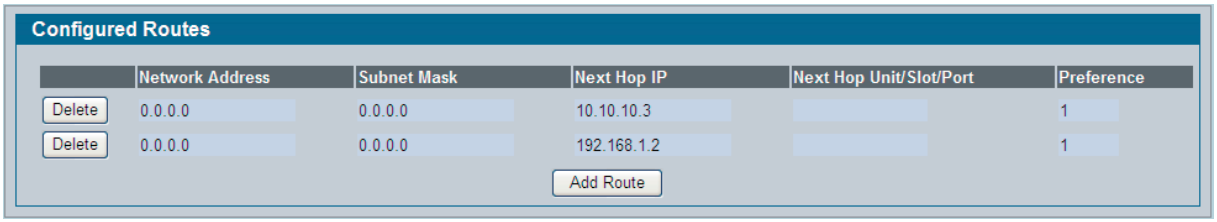


図 5-19　Configured Routes 画面

本画面には以下の項目があります。

項目	説明
Network Address	宛先用の IP ルートのプレフィックス。
Subnet Mask	サブネット / ネットワークマスクとも呼ばれ、これは、接続するネットワークを識別する IP インタフェースアドレス内の部分を示します。
Next Hop IP	トラフィックを宛先に送信する場合に使用するネクストホップルータ。
Next Hop Slot/Port	トラフィックを宛先に送信する場合に使用する外向きのインタフェース。スタティックな拒否ルートに対して、それは Null0 です。
Preference	追加ルートに設定される優先度。

「Refresh」ボタンをクリックして、画面の情報を更新します。

スタティックルートの追加

1. 「Configured Routes」画面を表示します。

2. 「Add Route」ボタンをクリックし、以下の画面を表示します。

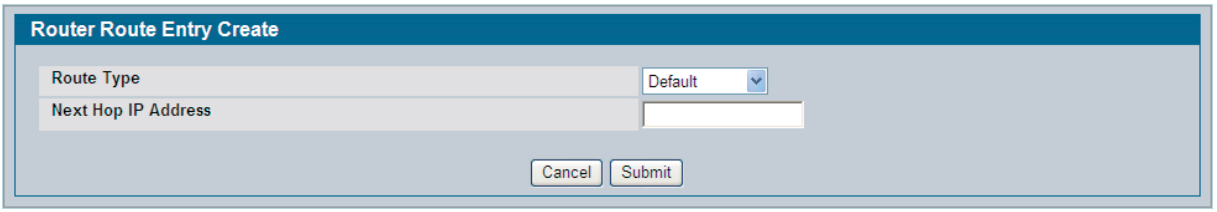


図 5-20　Router Route Entry Create 画面

3. 「Route Type」から「Default」ルート、「Static」、または「Static Reject」を選択します。

- Default -「Next Hop IP Address」にデフォルトゲートウェイアドレスを入力します。
- Static -「Network Address」、「Subnet Mask」、「Next Hop IP Address」、および「Preference」の値を入力します。
- Static Reject - これらの宛先へのパケットは破棄されます。

ルートタイプとして「Static」を選択すると、画面が更新され、追加の欄が表示されます。

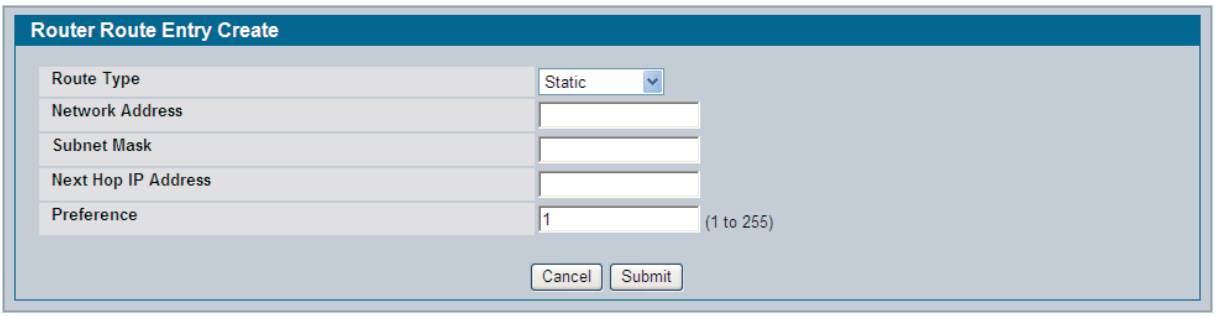


図 5-21　Router Route Entry Create 画面 - Static

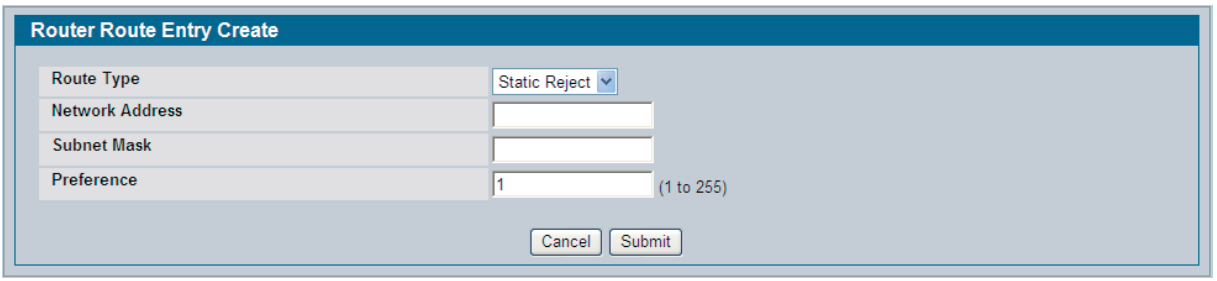


図 5-22　Router Route Entry Create 画面 - Static Reject

本画面には以下の項目があります。

項目	説明
Network Address	宛先用の IP ルートのプレフィックスを指定します。ルートを作成するためには、有効なルーティングインタフェースが存在し、ネクストホップ IP アドレスがルーティングインタフェースと同じネットワークにある必要があります。ルーティングインタフェースは、「IP Interface Configuration」画面で作成されます。有効なネクストホップ IP アドレスは、「Route Table」画面で参照することができます。
Subnet Mask	サブネット / ネットワークマスクとも呼ばれ、これは、接続するネットワークを識別する IP インタフェースアドレス内の部分を示します。
Protocol	指定ルートを作成したプロトコルを示します。 • Local • Static • Default • RIP
Next Hop IP Address	宛先に向かう経路にある次のルータにトラフィックを転送する場合に使用する外向きのルータの IP アドレス。 次のルータは、常に近接ルータの 1 つであるか、直接接続するネットワークのローカルインタフェースの IP アドレスです。 ルートを作成する場合は、ネクストホップ IP がルーティングインタフェースと同じネットワーク上にある必要があります。 有効なネクストホップ IP アドレスは、「Route Table」画面で参照することができます。
Metric	宛先へのパスの管理コスト。値を入力しないと、初期値は 1 となります。範囲は 0-255 です。本項目は、スタティックルートを作成した場合にだけ表示されます。
Preference	設定済みネクストホップの優先度値を指定します。
Route Type	ルートがデフォルトルートまたはスタティックルートであるかを指定します。

4. 「Submit」ボタンをクリックします。新しいルートが追加され、「Configured Routes」画面に戻ります。

ルートの削除

「Delete」ボタンをクリックして、設定したルートを削除します。

ルート優先度設定

各プロトコルのためのデフォルト優先度を設定します。これらの値は、1 から 255 までの範囲の任意の値であり、ルートメトリックには依存しません。ほとんどのルーティングプロトコルは、その他のプロトコルとは無関係に、そのプロトコルに知られている最短パスを判断するためにルートメトリックを使用します。優先度 255 を持つルートはフォワーディングに使用されません。

宛先への最適なルートの選択は、最も低い優先度値を持つルートを選ぶことによって行われます。宛先へのルートが複数ある場合は、優先されるルートを決定するために優先度値が使用されます。

LAN タブ > L3 Features > Router > Route Preferences 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 5-23　Router Route Preferences Configuration 画面

本画面には以下の項目があります。

項目	説明
Local	ローカルなルート優先度値の 0 を表示します。この値は変更できません。
Static	ルータのスタティックルートの優先度値。初期値は 1 です。範囲は 1-255 です。
RIP	ルータの RIP ルートの優先度値。初期値は 15 です。範囲は 1-255 です。
BGP4	BGP4 ルート優先度。初期値は 0 です。範囲は 1-255 です。

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。

VLAN ルーティング

VLAN およびルーティングをサポートする D-Link のソフトウェアを設定することができます。さらに、ソフトウェアを設定することで VLAN がルータのポートであるかのように VLAN 上のトラフィックを処理できるようになります。

ポートがルーティングではなくブリッジに有効になっている場合（初期値）、内向きパケットに対して通常のブリッジ処理のすべてが実行され、VLAN に関連付けられます。その MAC Destination Address（MAC DA）と VLAN ID は、MAC アドレステーブルを検索するために使用されます。ルーティングが VLAN に有効であり、内向きユニキャストパケットの MAC DA が内部ブリッジルータのインタフェースの MAC DA であると、パケットはルーティングされます。内向きマルチキャストパケットがルーティングされる VLAN で受信されると、VLAN におけるすべてのポートと内部ブリッジルータインタフェースに転送されます。

1 つのポートが複数の VLAN に所属するように設定できるため、VLAN ルーティングは、そのポート上のすべての VLAN、またはサブセットに対して有効にすることができます。VLAN ルーティングを使用すると、複数の物理ポートが同じサブセットに所属できるようになります。さらに、1 つの VLAN が複数の物理ネットワークにまたがる場合、または追加のセグメンテーションやセキュリティが必要とされる場合にも使用できます。

本セクションでは、VLAN ルーティングをサポートするために D-Link 統合スイッチを設定する方法について説明します。ポートは、VLAN ポートまたはルータポートのいずれかに設定することができますが、両方に設定することはできません。しかし、VLAN ポートが、自身がルータポートである VLAN の一部になることはできます。

LAN タブ > L3 Features > VLAN Routing フォルダには VLAN Routing パラメータとデータを設定および参照する以下の機能があります。

- VLAN ルーティング設定
- VLAN ルーティングサマリ

VLAN ルーティング設定

システムに VLAN ルーティングインタフェースを設定します。

LAN タブ > L3 Features > VLAN Routing 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。

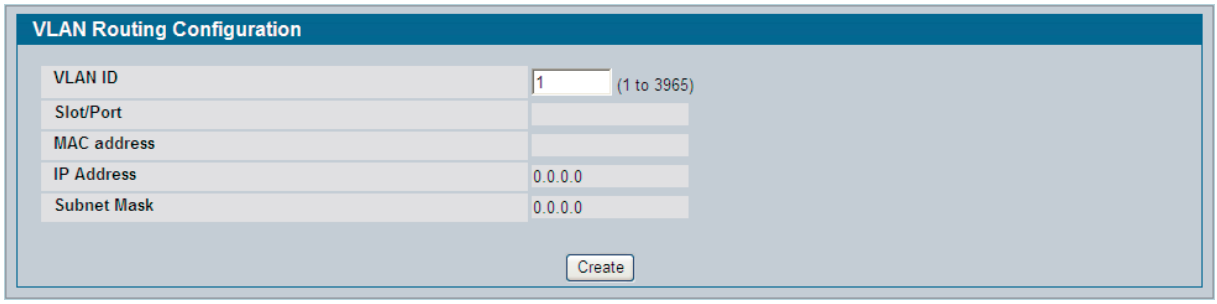


図 5-24　VLAN Routing Configuration 画面

本画面には以下の項目があります。

項目	説明
VLAN ID	VLAN ルーティングに設定する VLAN の ID を入力します。ここには、最初の VLAN の ID を表示します。新しい VLAN ID を入力し、「Create」ボタンをクリックした後に、設定できないデータが表示されます。
Slot/Port	VLAN ルーティングインタフェースに割り当てられる論理スロットとポート番号。
MAC Address	VLAN ルーティングインタフェースに割り当てられている MAC アドレス。
IP Address	VLAN ルーティングインタフェースに設定済みの IP アドレス。VLAN が作成され、IP アドレスが設定されていない場合には、初期値として IP アドレス「0.0.0.0」が表示されます。 **LAN タブ > L3 Features > Routing > IP > Interface Configuration** の順にメニューをクリックし、IP アドレスを設定します。
Subnet Mask	VLAN ルーティングインタフェースに設定済みのサブネットマスク。VLAN ルーティングインタフェースが初めて設定される場合、これは「0.0.0.0」となっており、「IP Interface Configuration」画面で入力する必要があります。

VLAN ルーティングインタフェースの作成

1. 「VLAN」欄に新しい VLAN ID を入力します。

2. 「Create」ボタンをクリックします。画面は更新され、新しい VLAN に割り当てられているインタフェースと MAC アドレスが表示されます。インタフェースは「Slot/Port」で表示されます。「IP Address」と「Subnet Mask」欄は「0.0.0.0」です。

注意 「Interface Configuration」画面から設定するためには正しいインタフェースを選択するように、インタフェース「Slot/Port」指定に注意してください。

3. **LAN タブ > L3 Features > IP > Interface Configuration** の順にメニューをクリックします。

4. VLAN に割り当てられているインタフェースを選択します。「IP Address」と「Subnet Mask」欄は初期値で「0.0.0.0」です。

5. VLAN 用の IP アドレスとサブネットマスクを入力し、他のインタフェース設定を行います。

6. 「Submit」ボタンをクリックして、VLAN ルーティングインタフェースに設定を適用します。

7. **LAN タブ > Monitoring > VLAN Routing Summary** の順にメニューをクリックし、テーブル内の新しい VLAN を参照します。

VLAN ルータインタフェースの削除

選択された VLAN ルーティングインタフェースを削除するため、「Delete」ボタンをクリックします。

VLAN ルーティングサマリ

システムに設定されている VLAN ルーティングインタフェースに関する情報を参照します。

LAN タブ > Monitoring > L3 Status > VLAN Routing 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。

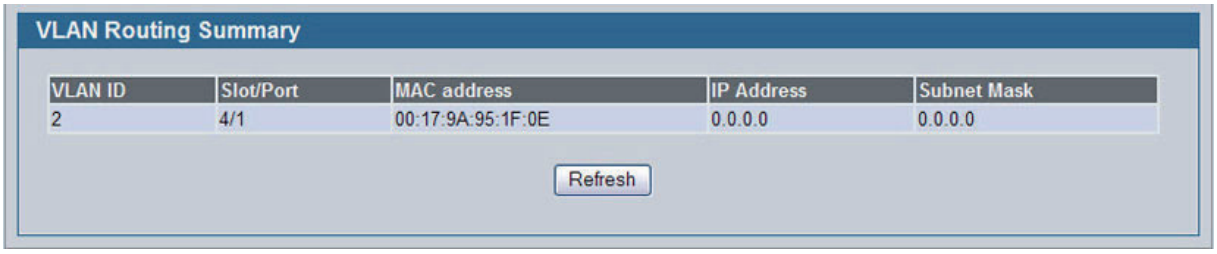


図 5-25　VLAN Routing Summary 画面

本画面には以下の項目があります。

項目	説明
VLAN ID	現在のテーブルにデータを表示する VLAN の ID。
Slot/Port	VLAN ルーティングインタフェースに割り当てられる論理スロットとポート番号。
MAC address	VLAN ルーティングインタフェースに割り当てられている MAC アドレス。
IP Address	VLAN ルーティングインタフェースに設定済みの IP アドレス。VLAN が作成され、IP アドレスが設定されていない場合には、初期値として IP アドレス「0.0.0.0」が表示されます。**LAN タブ > L3 Features > IP > Interface Configuration** の順にメニューをクリックし、IP アドレスを設定します。
Subnet Mask	VLAN ルーティングインタフェースに設定済みのサブネットマスク。VLAN ルーティングインタフェースが初めて設定される場合、これは「0.0.0.0」となっており、「IP Interface Configuration」画面で入力する必要があります。

VRRP 設定

VRRP（Virtual Routing Redundancy Protocol）は、バックアップルータをダイナミックに選出する体系を提供することでデフォルトルータの障害を処理するために設計されています。これは、デフォルトゲートウェイルータの障害のために、その障害が検出されるまで、そのルータに向かうすべてのトラフィックが喪失するという「ブラックホール」期間を最小限に抑えることができます。デフォルトルートをスタティックに設定するのが一般的ですが、このような方法だと、デフォルトルータに障害が発生した場合に単一の障害に影響されやすくなります。VRRP では、デフォルトゲートウェイとして動作する 1 つ以上の IP アドレスに関連付ける「仮想ルータ」という概念を提唱しています。これらの IP アドレスを制御する VRRP ルータ（マスタとして知られる）が故障した場合、バックアップ VRRP ルータがその IP アドレスグループとデフォルトフォワーディングの役割を引き継ぎます。

LAN タブ > L3 Features > VRRP folder and LAN > Monitoring > L3 Status フォルダには VRRP パラメータとデータを設定および参照する以下の機能があります。

- VRRP 設定
- 仮想ルータの設定
- 仮想ルータのステータス
- 仮想ルータの統計情報

VRRP 設定

仮想のルータの管理用のステータスを有効または無効にします。

LAN タブ > L3 Features > VRRP > VRRP 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。

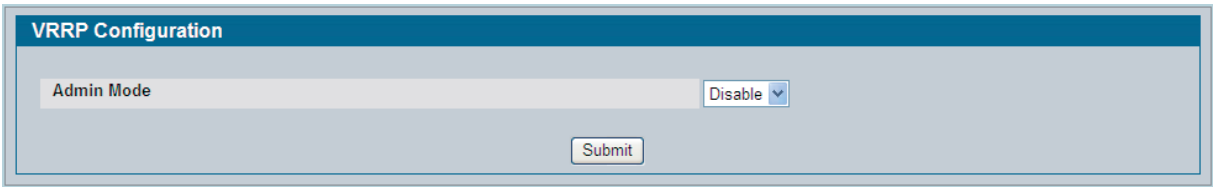


図 5-26　VRRP Configuration 画面

本画面には以下の項目があります。

項目	説明
Admin Mode	VRRP の管理用の管理ステータスを有効または無効にするようにルータに設定します。「Enable」（有効）または「Disable」（無効）を選択します。初期値は「Disable」です。

管理モードを変更した場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。

仮想ルータの設定

新しい仮想ルータの作成、または既存可能ルータの設定を行います。

LAN タブ > L3 Features > VRRP > Virtual Router 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。

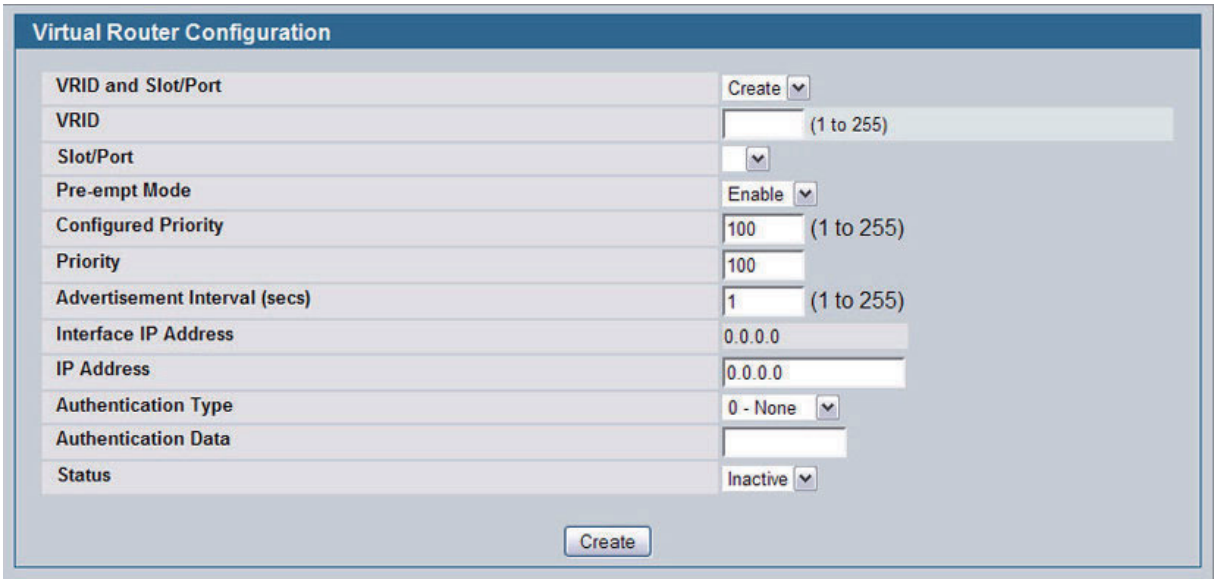


図 5-27　Virtual Router Configuration 画面

本画面には以下の項目があります。

項目	説明
VRID and Slot/Port	「Create」を選択し、新しい仮想ルータを設定します。または、インタフェース番号と VRID で示されている既存の仮想ルータを選択します。
VRID	新しい仮想ルータを作成している場合にだけ本項目は設定可能です。1-255 の範囲で VRID を入力します。
Slot/Port	新しい仮想ルータを作成している場合にだけ本項目は設定可能です。新しい仮想ルータ用のインタフェースを選択します。
Pre-empt Mode	「Enable」（有効）または「Disable」（無効）を選択します。「Enable」を選択した場合、マスタが仮想ルータの IP アドレスの所有者でないと、バックアップルータである仮想ルータがマスタの仮想ルータの優先度よりも高い優先度を持っている場合、バックアップルータがマスタルータに変わります。初期値は「Enable」です。
Configured Priority	マスタの仮想ルータの選出に VRRP ルータが使用する優先度値を入力します。仮想 IP アドレスがインタフェースの IP アドレスと同じであると、何に入力しても優先度は 255 に設定されます。仮想 IP アドレスとインタフェース IP アドレスが同じでない場合に優先度に 255 を入力すると、優先度は初期値の 100 に設定されます。
Priority	VRRP ルータの操作優先度。操作優先度は設定済みの優先度に依存し、優先度はトラッキング処理を通じては減少します。
Advertisement Interval (secs)	仮想ルータによる Advertisement パケットの送信間隔（秒）を入力します。1-255 の範囲で入力します。初期値は 1（秒）です。
Interface IP Address	選択インタフェースに関連付けられている IP アドレスを示します。
IP Address	仮想ルータに関連付ける IP アドレスを入力します。初期値は「0.0.0.0」であり、「Create」ボタンをクリックする前に変更する必要があります。
Authentication Type	仮想ルータの認証タイプを選択します。 • 0-None - 認証を行いません。（初期値） • 1-Simple - 認証は、テキストパスワードを使用して行われます。
Authentication Data	simple 認証を選択した場合、パスワードを入力します。
Status	「Active」または「Inactive」を選択し、仮想ルータの操作を開始または中止します。初期値は、「Inactive」です。

「Submit」ボタンをクリックし、新しい設定をスイッチに適用します。「Save」が実行されないと、これらの変更は再起動後に保持されません。

セカンダリの設定
「Secondary IP Address」ボタンをクリックし、「Secondary IP Address Configuration」画面を表示します。

仮想ルータの削除
「Delete」ボタンをクリックし、選択した仮想ルータを削除します。

注意 設定されたセカンダリアドレスがあるとルータを削除できませんのでご注意ください。

「Track Interface」ボタンをクリックし、「VRRP Track Interface Configuration」画面を表示します。
「Track Route」ボタンをクリックして、「VRRP Track Route Configuration」画面を表示します。

セカンダリ VRRP アドレスの設定

セカンダリ VRRP アドレスを設定するためには、仮想ルータに IP アドレス（プライマリアドレス）を最初に設定します。次に、そのインタフェースに複数のセカンダリアドレスを追加することができます。

「Submit」ボタンをクリックし、新しい設定をスイッチに適用します。「Save」が実行されないと、これらの変更は再起動後に保持されません。

仮想ルータの削除
「Delete」ボタンをクリックし、選択したセカンダリ IP アドレスを削除します。

「Cancel」ボタンをクリックし、「Virtual Router Configuration」画面に戻ります。

新しい仮想ルータの作成

1. 「Virtual Router Configuration」画面を使用して、「VRID and Slot/Port」から「Create」を選択します。
2. 新しい仮想のルータに VRID、仮想のルータアドレス、およびインタフェースを指定します。
3. 必要とされる残りのデータを定義します。
4. 「Create」ボタンをクリックし、変更をシステムに適用します。新しい仮想ルータが保存され、デバイスは更新されます。

仮想のルータの変更

既存の仮想ルータの設定を変更するために、「VRID and Slot/Port」から「ID」を選択し、必要に応じて項目を変更します。「Submit」ボタンをクリックし、変更をスイッチに適用します。

VRRP インタフェースのトラッキング設定

VRRP グループの仮想ルータの優先度レベルを変更できるルータ内の特定インタフェースの IP ステートを追跡します。これの例外は、そのVRRP グループが IP アドレスの所有者である場合、優先度は 255 に固定されていて、トラッキング処理を通じて減少させることはできません。

LAN タブ > L3 Features > VRRP > Virtual Router Configuration の順にメニューをクリックし、次に「Track Interface」ボタンをクリックして以下の画面を表示します。

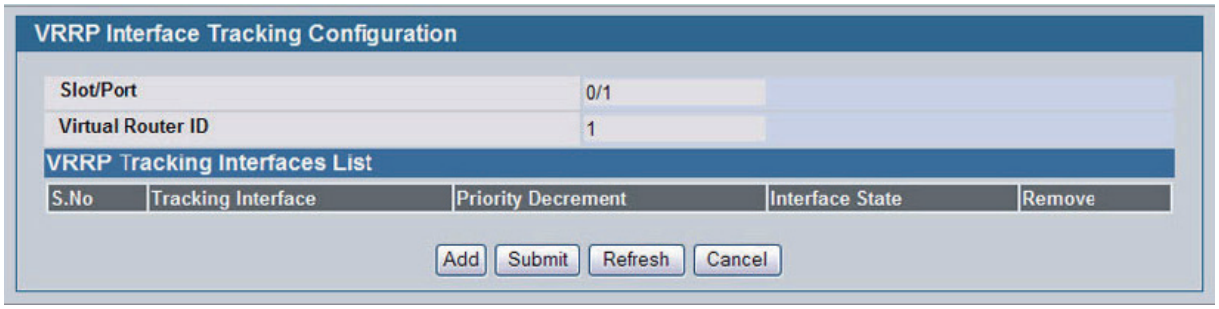


図 5-28　VRRP Interface Tracking Configuration 画面

本画面には以下の項目があります。

項目	説明
Slot/Port	Virtual Router ID に関連しているインタフェース。
Virtual Router ID	表示されるトラッキングデータの Virtual Router ID。
S. No	シリアル番号。
Tracking Interface	データの表示のためにトラッキングされるインタフェース。
Priority Decrement	トラッキングされるインタフェースの優先度の減少値。有効範囲は、1-254 です。初期値は 10 です。
Interface State	トラッキングされる IP の状態。
Remove	VRRP トラックリストから選択したトラッキングインタフェースを削除します。

1. 「Add」ボタンをクリックし、「VRRP Interface Tracking」画面を表示します。

2. 「Submit」ボタンをクリックし、新しい設定をスイッチに適用します。変更は直ちに反映されます。「Save」が実行されないと、これらの変更は再起動後に保持されません。

「Refresh」ボタンをクリックすると、スイッチにおける現在のデータを更新します。「Cancel」ボタンをクリックし、「Virtual Router Configuration」画面に戻ります。

VRRP インタフェースのトラッキング

トラッキングリストにインタフェースを追加します。

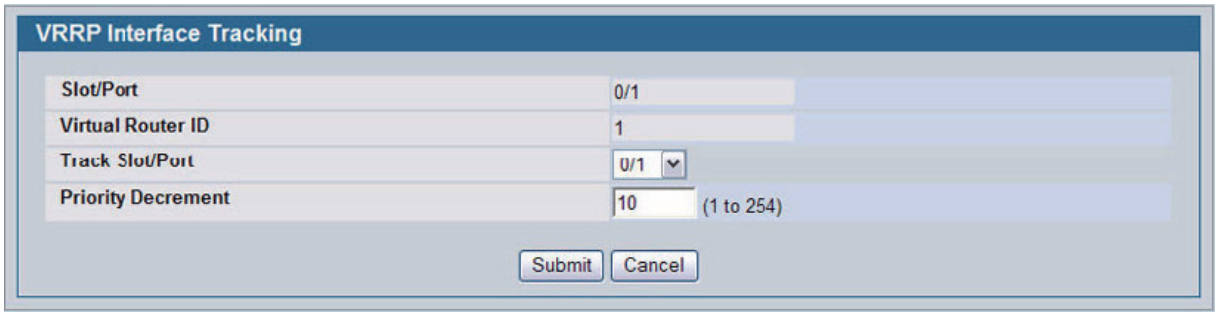


図 5-29　VRRP Interface Tracking 画面

本画面には以下の項目があります。

項目	説明
Slot/Port	Virtual Router ID に関連しているインタフェース。
Virtual Router ID	表示されるトラッキングデータの Virtual Router ID。
Track Slot/Port	この仮想ルータ ID とインタフェース設定にトラッキングをまだ実施していないすべてのルーティングインタフェースを表示します。ループバックおよびトンネルはトラッキングされません。
Priority Decrement	トラッキングされるインタフェースの優先度の減少値。有効範囲は 1-254 です。初期値は 10 です。

「Submit」ボタンをクリックし、更新した設定内容をスイッチに送信します。変更は直ちに反映されます。「Save」が実行されないと、これらの変更は再起動後に保持されません。

「Cancel」ボタンをクリックし、「VRRP Interface Tracking Configuration」画面に戻ります。

VRRP ルートトラッキング設定

VRRP グループの仮想ルータのプライオリティレベルを変更できるルータ内の特定の IP が指定したルートを追跡します。

LAN タブ > L3 Features > VRRP > Virtual Router Configuration の順にメニューをクリックし、次に「Track Route」ボタンをクリックして以下の画面を表示します。

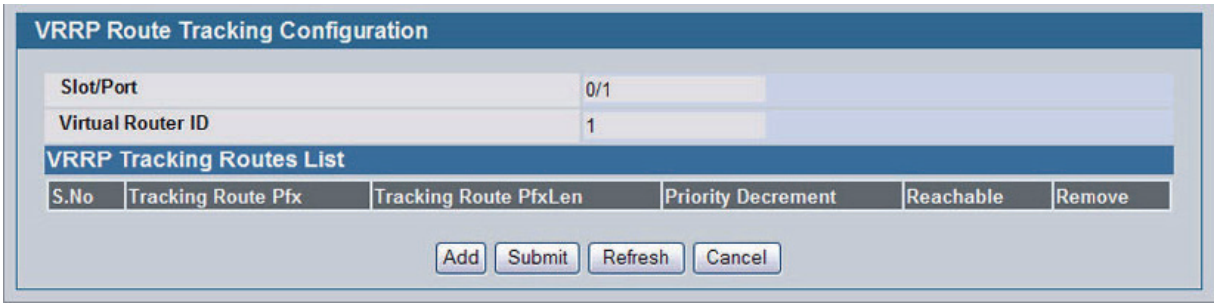


図 5-30　VRRP Route Tracking Configuration 画面

本画面には以下の項目があります。

項目	説明
Slot/Port	Virtual Router ID に関連しているインタフェース。
Virtual Router ID	トラッキングデータを表示する Virtual Router ID を表示します。
S.No	シリアル番号。
Tracking Route Pfx	トラッキングされるルートのプレフィックス。
Tracking Route PfxLen	トラッキングされるルートのプレフィックス長。
Priority Decrement	トラッキングされるルートの優先度の減少値を入力します。有効範囲は 1-254 です。初期値は 10 です。
Reachable	トラッキングされるルートの到達性。
Remove	VRRP トラックリストから選択したトラッキングルートを削除します。

「Add」ボタンをクリックし、「VRRP Route Tracking」画面を表示します。

「Submit」ボタンをクリックし、更新した設定内容をスイッチに送信します。変更は直ちに反映されます。「Save」が実行されないと、これらの変更は再起動後に保持されません。

「Refresh」ボタンをクリックすると、スイッチにおける現在のデータを更新します。
「Cancel」ボタンをクリックし、「Virtual Router Configuration」画面に戻ります。

VRRP ルートトラッキング

「VRRP Route Tracking」画面を使用して、トラッキングリストにルートを追加します。

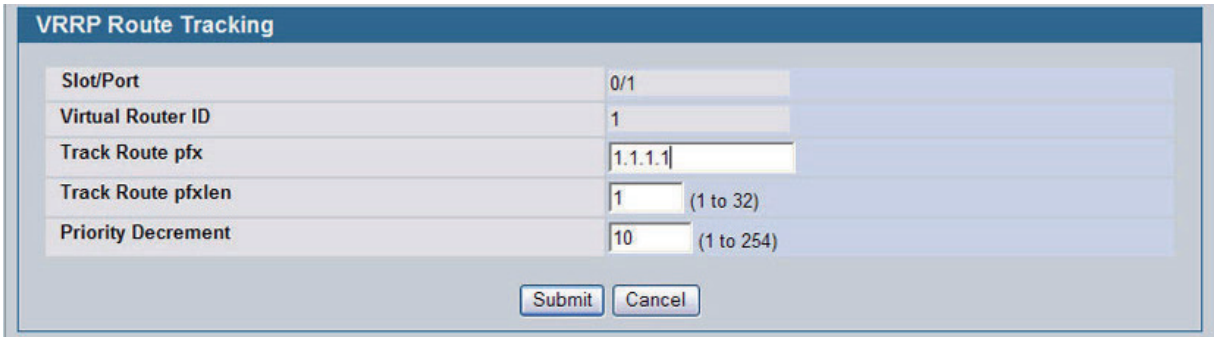


図 5-31　VRRP Route Tracking 画面

本画面には以下の項目があります。

項目	説明
Slot/Port	Virtual Router ID に関連しているインタフェース。
Virtual Router ID	表示されるトラッキングデータの Virtual Router ID。
Track Route Pfx	ルートのプレフィックス。
Track Route PfxLen	ルートのプレフィックス長。
Priority Decrement	ルートの優先度の減少値。有効範囲は 1-254 です。初期値は 10 です。

「Submit」ボタンをクリックし、更新した設定内容をスイッチに送信します。変更は直ちに反映されます。「Save」が実行されないと、これらの変更は再起動後に保持されません。

「Cancel」ボタンをクリックし、「VRRP Route Tracking Configuration」画面に戻ります。

仮想ルータのステータス

仮想ルータのステータスを表示します。

LAN タブ > Monitoring > L3 Status > Virtual Router 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 5-32　Virtual Router Status 画面

本画面には以下の項目があります。

項目	説明
VRID	仮想ルータの識別子。
Slot/Port	VRID に関連しているインタフェースを示します。
Priority	マスタの仮想ルータの選出に VRRP ルータが使用する優先度値。
Pre-empt Mode	• Enable - マスタがバックアップルータである仮想ルータがマスタの仮想ルータの優先度よりも高いプライリティを持っている場合に仮想ルータの IP アドレスの所有者でないと、バックアップルータはマスタルータに変わります。 • Disable - 仮想ルータがバックアップルータである場合、その優先度がより高くてもマスタルータにはなりません。
Advertisement Interval(secs)	仮想ルータによる Advertisement パケットの送信間隔（秒）。
Virtual IP Address	仮想ルータに関連付けされた IP アドレス。
Interface IP Address	仮想ルータが使用するインタフェースに関連する実際の IP アドレス。
Address Owner	「Virtual IP Address」と「Interface IP Address」が同じである場合、「True」に設定し、そうでない場合「False」に設定します。「True」に設定されると、仮想ルータは仮想 IP アドレスの所有者となり、それがアクティブである場合、常にマスタルータとなります。
VMAC Address	24 ビットの構成上ユニークな識別子、16 ビットの VRRP アドレスブロックを識別する定数、および 8 ビットの VRID から生成されている仮想ルータに関連付けされている仮想 MAC アドレス。仮想 MAC アドレスは「00:00:5e:00:01:XX」（XX は VRID）です。
Auth Type	仮想ルータで使用中の認証タイプ。 • None - 認証タイプはありません。 • Simple - 認証タイプが簡単なテキストパスワードです。
State	仮想ルータの現在の状態。 • Initialize - 初期化 • Master - マスタ • Backup - バックアップ
Status	仮想ルータの現在の状態。 • Inactive - 非アクティブ • Active - アクティブ
Secondary IP Address	プライマリ VRRP に対して設定されているセカンダリ VRRP アドレス。

「Refresh」ボタンをクリックすると、画面の情報をスイッチにおける現在のデータを使用して更新します。

仮想ルータの統計情報

指定した仮想ルータの統計情報を表示します。

LAN タブ > Monitoring > L3 Status > Virtual Router 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。

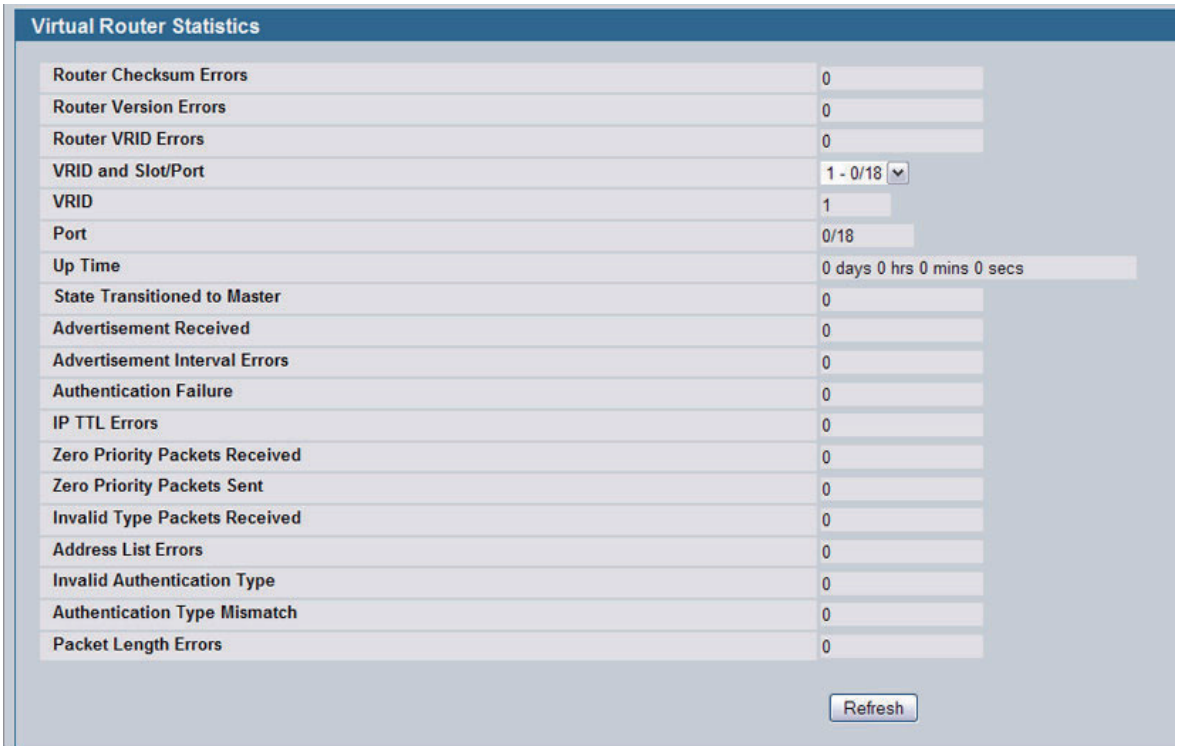


図 5-33　Virtual Router Statistics - 設定済みの仮想ルータ画面

ここでは 1 つ以上の仮想ルータを構成するスイッチの画面を表示しています。

本画面には以下の項目があります。有効な VRRP 設定がある場合に多くの項目が表示されます。

項目	説明
Router Checksum Errors	不正な VRRP チェックサムと共に受信した VRRP パケットの総数。
Router Version Errors	未知の、または、サポートされないバージョン番号と共に受信した VRRP パケットの総数。
Router VRID Errors	仮想ルータに不正な VRID と共に受信した VRRP パケットの総数。
VRID and Slot/Port	統計情報を表示するインタフェース番号と VRID によって示された既存の仮想ルータを選択します。
VRID	選択された仮想ルータの VRID。
Port	選択された仮想ルータ用のインタフェース。
Up Time	仮想ルータの最後の再起動から経過した（日、時、分、秒）。
State Transitioned to Master	仮想ルータの状態がマスタに移行した回数。
Advertisement Received	仮想ルータが受信した VRRP 通知の総数。
Advertisement Interval Errors	通知間隔がローカル仮想ルータの設定とは異なるパケットが受けた VRRP Advertisement の総数。
Authentication Failure	認証を通過しなかった、受信 VRRP パケットの総数。
IP TTL Errors	仮想ルータが受信した 255 に等しくない IP TTL（TimeTo-Live）を持つ VRRP パケットの総数。
Zero Priority Packets Received	仮想ルータが受信した優先度 0 を持つ VRRP パケットの総数。
Zero Priority Packets Sent	仮想ルータが送信した優先度 0 を持つ VRRP パケットの総数。
Invalid Type Packets Received	仮想ルータが受信した Type フィールドに不正な値を持つ VRRP パケットの数。
Address List Errors	アドレスリストがローカルに設定した仮想ルータのリストに一致しない受信パケットの総数。
Invalid Authentication Type	未知の認証タイプで受信したパケットの総数。
Authentication Type Mismatch	ローカルに設定した認証方式とは異なる認証タイプで受信したパケットの総数。
Packet Length Errors	VRRP ヘッダの長さより短いパケット長を持つ受信パケットの総数。

「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。

ループバックインタフェース

D-Link ソフトウェアではループバックインタフェースの新規作成、削除、および管理を提供します。ユーザ設定により作成、削除されるダイナミックインタフェースです。D-Link ソフトウェアは、複数のループバックインタフェースをサポートしています。

ループバックインタフェースは常に起動しているものとします。このため、それは他のスイッチによって参照される可能性のあるデバイスに安定した IP アドレスを設定する手段を提供します。このインタフェースは、送信パケットの送信元アドレスを提供して、ローカルおよびリモートパケットの両方を受信することができます。それは日常的にはルーティングプロトコルが使用しています。

ループバックインタフェースは、ルータがこのアドレスで通信できるようにローカルアドレスを割り当てるための疑似デバイスです。そして、常に起動し、既存のアクティブなインタフェースのいずれかからトラフィックを受信できるものです。そのため、リモートからの到達性を提供し、ループバックのアドレスは telnet や SSH などの様々なサービスを経由したルータとの通信に使用されます。このように、ループバックに関するアドレスは入力パケットの処理においてルータのローカルのアドレスのいずれにも同様に動作します。

LAN タブ > L3 Features > Loopbacks folder and LAN > Monitoring > L3 Status フォルダにはループバックのパラメータとデータを設定および参照する以下の機能があります。

- ループバック設定
- ループバックのサマリ

ループバック設定

ループバックインタフェースの作成、設定、または削除を行います。また、ループバック用セカンダリアドレスの設定、または削除も行います。

LAN タブ > L3 Features > Loopbacks > 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。ループバックインタフェースがシステムに存在していないと、以下のように、画面には 2 つの項目のみ表示されます。

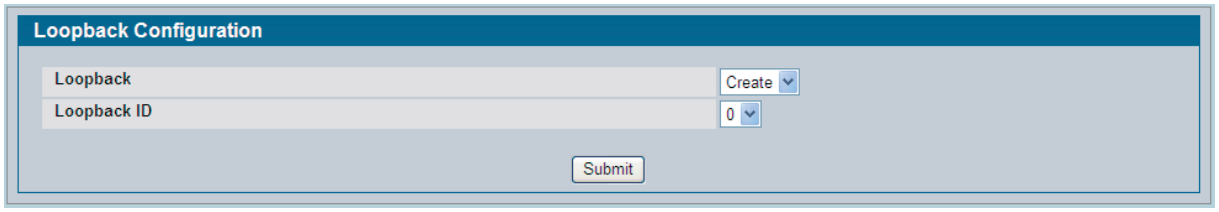


図 5-34　Loopback Configuration - Create 画面

ループバックインタフェースが設定済みの場合は、以下の画面が表示されます。

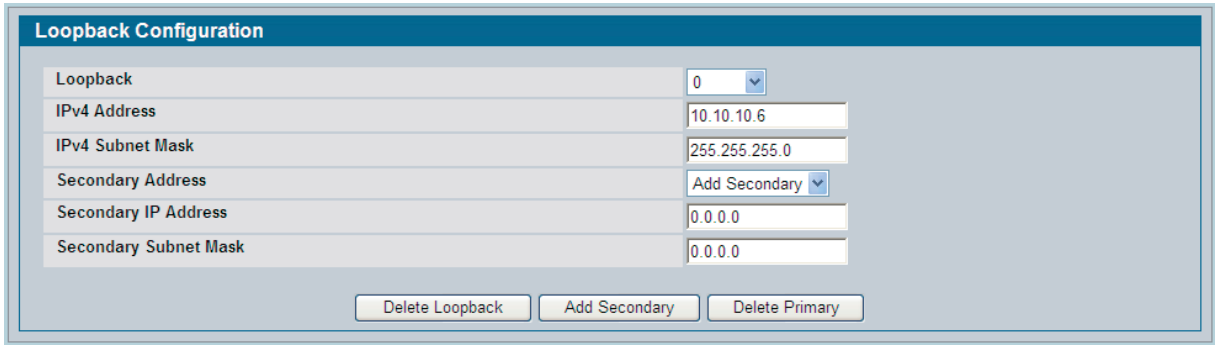


図 5-35　Loopback Configuration 画面

本画面で利用可能な項目は、存在するループバックインタフェースの種類によって異なります。

以下の表ではすべての項目について説明しています。それは、同時に同じ画面に表示されません。

項目	説明
Loopback	現在設定されているループバックインタフェースのリストから選択します。また、ループバックインタフェースが作成されていない場合、「Create」が利用できます。
Loopback ID	「Loopback」で「Create」が選択されると、利用可能なループバック ID のリストが表示されます。
Protocol	「IPv4」または「IPv6」を選択し、ループバックインタフェースに対応する属性を設定します。選択されたプロトコルは、この画面に表示される項目に影響します。
IPv4 Address	「.」（ドット）を付けた 10 進数形式のプライマリ IPv4 アドレス。指定されたプロトコルが、IPv4 である場合にだけ、このオプションは表示されます。
IPv4 Subnet Mask	「.」（ドット）を付けた 10 進数形式のプライマリサブネットマスク。指定されたプロトコルが、IPv4 である場合にだけ、このオプションは表示されます。

プライマリアドレスが設定されている場合、以下の項目が表示されます。複数のセカンダリアドレスを設定することができます。

項目	説明
Secondary Address	選択したループバックインタフェース用に設定した IPv4 セカンダリアドレスを選択します。新しいアドレスは、この「Add Secondary」を選択することで、「Secondary IP Address」に入力することができます。（セカンダリアドレスの設定されていない場合。）セカンダリアドレスを追加する前にプライマリアドレスを設定します。
Secondary IP Address	「.」（ドット）を付けた 10 進数形式のセカンダリ IPv4 アドレス。「Add Secondary」が選択される場合にだけ、本入力欄が表示されます。
Secondary Subnet Mask	「.」（ドット）を付けた 10 進数形式のセカンダリサブネットマスク。「Add Secondary」が選択される場合にだけ、本入力欄が表示されます。

新しいループバック（IPv4）の作成

1. 「Loopbacks Configuration」画面を使用して、「Loopback」メニューから「Create」を選択し、「Submit」ボタンをクリックします。以下の画面が表示されます。

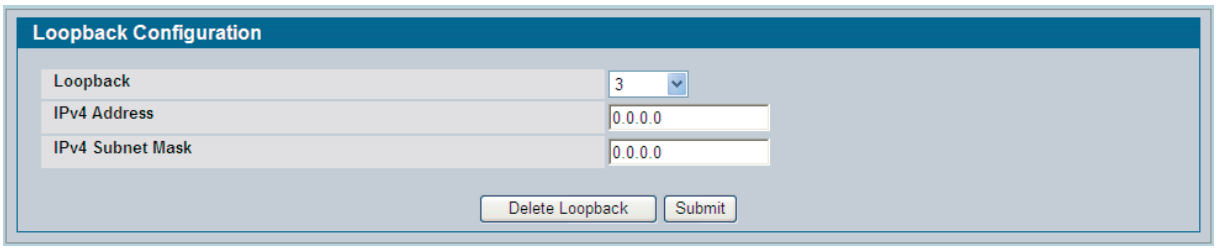


図 5-36　Loopback Configuration - Create 画面

2. 「Loopback ID」に使用する ID を指定します。
3. 「Submit」ボタンをクリックします。「Loopback ID」の表示はなくなり、以下の図が示すように、追加のループバックフィールドが表示されます。

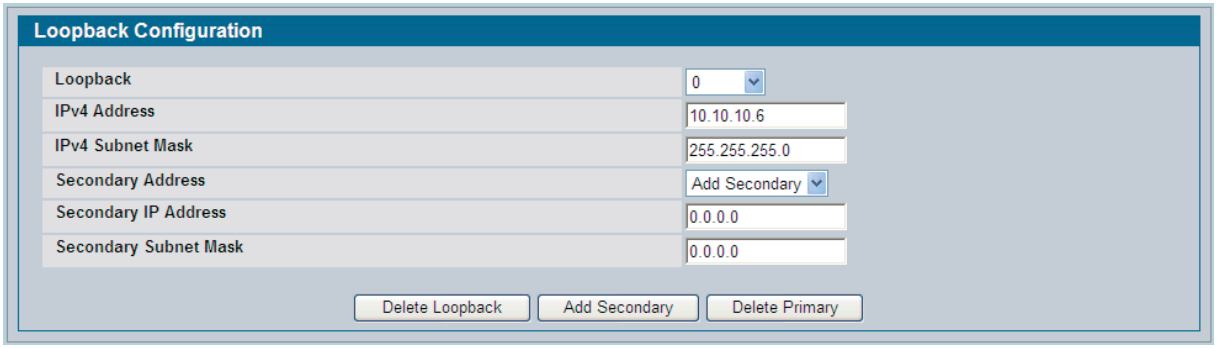


図 5-37　Loopback Configuration - IPv4 エントリ画面

4. 「Protocol」で、IPv4 を選択します。
5. 残りの欄に必要な値を入力します。
6. 「Submit」ボタンをクリックします。新しいループバックが保存され、Web 画面は、セカンダリアドレス設定欄を再度表示します。この画面の項目の例に関しては、図 5-35 を参照してください。
7. オプションで、「Secondary Address」、「Secondary IP Address」、および「Secondary Subnet Mask」を入力します。
8. 「Add Secondary」ボタンをクリックします。セカンダリアドレスが保存され、Web 画面は、プライマリ / セカンダリアドレス設定フィールドを再度表示します。

既存のループバックの設定

1. 「Loopback Configuration」画面を表示します。
2. 「Loopback」で設定するループバックを指定します。
3. 残りの項目を必要な値に変更します。
4. 「Apply Changes」ボタンをクリックします。新しい設定が保存され、デバイスは更新されます。

ループバックの削除

1. 「Loopback Configuration」画面を表示します。
2. 「Loopback」で削除するループバックを指定します。
3. 「Delete Loopback」ボタンをクリックします。ループバックは削除され、デバイスが更新されます。

セカンダリアドレスの削除

1. 「Loopback Configuration」画面を表示します。
2. 関係するループバックを指定します。
3. 削除するセカンダリアドレスを指定します。
4. 「Delete Selected Secondary」ボタンをクリックします。セカンダリアドレスは削除され、デバイスが更新されます。

ループバックのサマリ

設定したループバックの概要を表示します。

LAN タブ > Monitoring > L3 Status > Loopback 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。

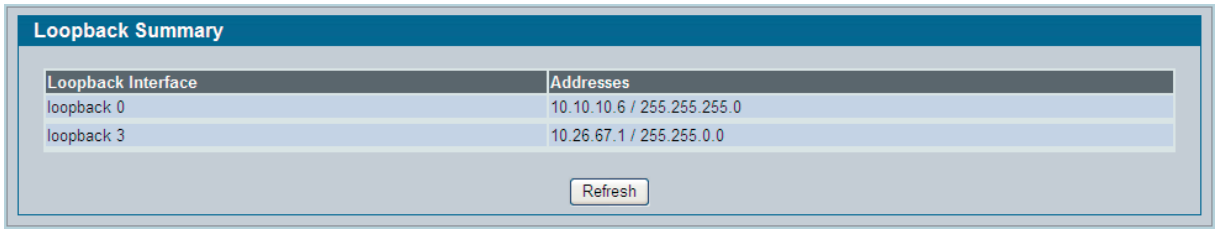


図 5-38　Loopback Summary 画面

本画面には以下の項目があります。

項目	説明
Loopback Interface	ループバックインタフェースの ID。
Addresses	ループバックインタフェースに設定されたアドレスリスト。

「Refresh」ボタンをクリックして、画面の情報を更新します。

第 7 章　アクセスコントロールリスト機能の設定

アクセスコントロールリスト（ACL）は、認可ユーザだけが指定リソースにアクセスすることを保証します。一方、ネットワークリソースに不当にアクセスしようとする試みをブロックします。ACL は、トラフィックフロー制御の提供、ルーティング更新の内容の制限により、どのタイプのトラフィックを転送するか、またはブロックするかの決定、そして何よりもネットワークにセキュリティを提供するために使用されます。D-Link ソフトウェアは、IPv4 および MAC ACL をサポートしています。D-Link ソフトウェアによってサポートされている MAC と IP ACL の総数は 100 個です。

アクセスコントロールリストには以下の機能があります。

設定項目	説明	参照ページ
IP アクセスコントロールリスト	IP ベースの ACL を設定します。	222 ページ
MAC アクセスコントロールリスト	MAC ベースの ACL を設定します。	227 ページ

最初に、IPv4 ベース、または、MAC ベースのルールを作成して、ユニークな ACL ID を割り当てます。次に、ルールを定義します。ルールにはプロトコル、送信元 / 送信先 IP、MAC アドレス、および他のパケットを照合する基準を指定することができます。最終的に、ACL をポートに割り当てるのに ID 番号を使用します。

IP アクセスコントロールリスト

IP アクセスコントロールリスト（ACL）によりネットワーク管理者は指定ポート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。ACL は、アクセス制御エントリ（ACE）、またはルールで構成されており、それらはトラフィックの分類を決定するフィルタから成ります。各 ACL に定義できるルールの総数は 12 です。これらのルールは、連続してパケットを照合されます。パケットがルールの基準に一致する場合、パケットの破棄やポートの無効化を含む指定ルールのアクション「Permit（許可）/Deny（破棄）」を適用し、追加のルールをチェックしません。例えば、ネットワーク管理者が、ポート番号 20 が TCP パケットを受信するという ACL ルールを定義します。しかし、UDP パケットが受信すると、そのパケットは破棄されます。

IP アクセスコントロールリストには、IP ACL の設定および参照を行う以下の機能があります。

- IP ACL の設定
- IP ACL ルール設定

まず、「IP ACL Configuration」を使用して、IP ACL タイプを定義し、それに ID を割り当てます。次に、「IP ACL Rule Configuration」画面を使用して、その ACL にルールを作成します。最後に、「ACL Interface Configuration」画面を使用して、ID 番号によって ACL をポートに割り当てます。

IP ACL の設定

IP ベースの ACL の追加または削除を行います。ここでは、内向きまたは外向きトラフィックへの適用の有無など IP ACL を適用するインタフェースを指定します。IP ACL ルールは、以下の画面を使用して、指定 / 作成します。

LAN タブ > Access Control Lists > IP Access Control Lists > 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。

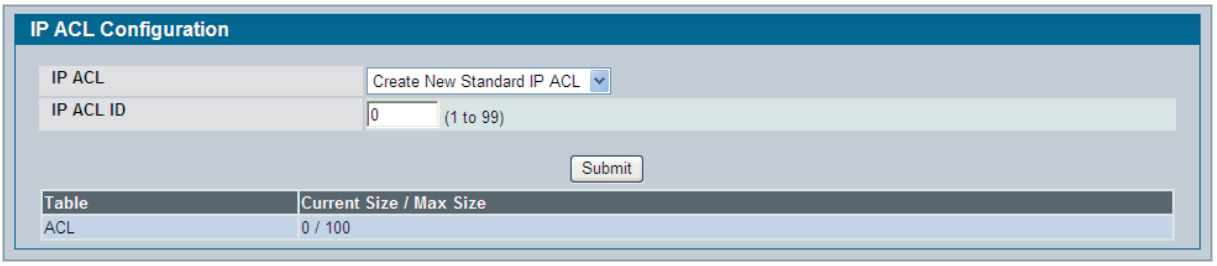


図 7-1　IP ACL Configuration 画面

本画面には次の項目があります。

項目	説明
IP ACL	作成する ACL のタイプを選択します。また、削除するためには既存の ACL 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	設定する ACL の ID 番号を入力します。「IP ACL」で「Create New Standard IP ACL」または「Create Extended IP ACL」を選択すると、本項目が表示されます。標準の IP ACL に有効な ID は 1-99 です。Extended IP ACL に有効な ID は 101-199 です。
IP ACL Name	「IP ACL」から「Create New Named IP ACL」を選択すると、本項目が表示されます。半角英数字で指定します。名前は英字から開始する必要があります。ACL が既に作成されている場合、現在選択されている IP ACL の名前が表示されます。画面下にある ACL テーブルでは、ACL テーブルの最大サイズに対する現在のサイズが表示されます。現在のサイズは、設定済みの IPv4 および IPv6 ACL に設定済みの MAC ACL をプラスした数と等しくなります。最大サイズは 100 です。

エントリの追加

IP ACL を追加するためには、「IP ACL」から ACL タイプを選択して追加します。次に「ACL ID」に入力し、「Submit」ボタンをクリックします。

エントリの削除

IP ACL を削除するために、「IP ACL ID」で ACL ID を選択し、「Delete」ボタンをクリックします。IP ACL が選択されると、「Delete」ボタンだけが表示されます。

IP ACL ルール設定

「IP Access Control List Configuration」画面で作成した IP ベースの ACL にルールを定義します。アクセスリストの定義には、基準に一致するトラフィックを通常通りに転送または破棄するかを指定するルールが含まれています。さらに、トラフィックの特定のキューへの割り当て、および（または）特定ポートへのトラフィックのミラーリングを指定することができます。

注意 ACL リストの最後に、暗黙の「deny all」（すべて拒否）のルールがあります。つまり、ACL があるパケットに適用される場合、および明示的なルールに一致しない場合には、最後にある暗黙の「deny all」ルールが適用され、パケットは破棄されます。

LAN タブ > QoS > Access Control Lists > IP Access Control Lists > Rule 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。

画面で利用可能な項目は、「IP ACL」から「standard」、「extended IP」、または「named IP ACL」を選択するかどうか、「Rule」から「Create Rule」または既存のルールを選択するかによって変わります。

以下は、「Rule」で「Create Rule」が選択される場合に利用可能な項目を示しています。

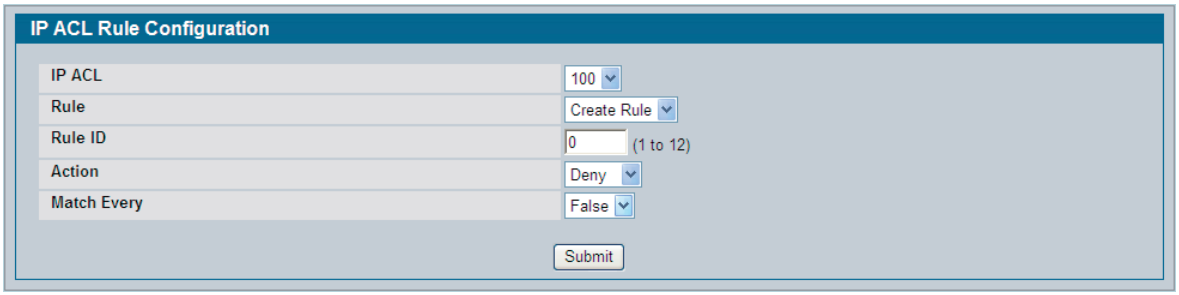


図 7-2　IP ACL Rule Configuration（Create Rule）画面

以下は「extended IP ACL」にルールを作成する場合に利用可能な項目を示しています。

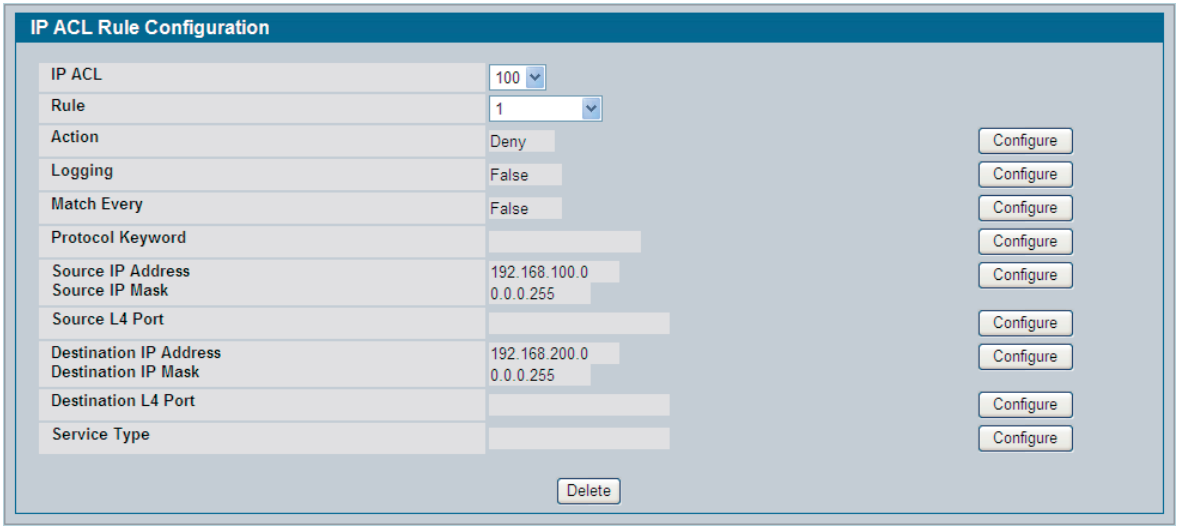


図 7-3　IP ACL Rule Configuration（Extended ACL Rule）画面

以下の表は「 IP ACL Rule Configuration」画面の利用可能な項目です。実際に利用可能な項目は、新しいルールの作成、または既存のルールの変更、さらにそのルールアクション「Permit」または「Deny」などどんなタイプのルールを設定するかによって変わります。

本画面には次の項目があります。

項目	説明
IP ACL	画面に設定された既存の IP ACL が表示されます。新しい IP ACL を設定するために、「IP アクセスコントロールリスト」（222 ページ）を参照してください。
Rule	編集するためには、既存の Rule ID を選択し、新しい ACL ルールを設定するためには「Create Rule」を選択します。ルールの最大数に到達すると、新しいルールを作成することができなくなります。各ルールに対して、パケットは、正確に指定ルールアクション「Permit」（許可）/「Deny」（拒否）を行うためにはすべての指定基準に適合する必要があります。
Rule ID	「Rule」から「Create Rule」を選択した場合に本項目は表示されます。新しい「Rule ID」を 1-12 の範囲で入力し、ルールを識別するために使用します。「Submit」ボタンをクリックすると、新しい ID が作成され、ルール設定を行うことができます。ACL に作成可能なルール数はプラットフォームに依存します。

項目	説明
Action	ACL を転送するアクションを選択します。「Configure」ボタンをクリックして、アクションを変更します。必要なアクションを選択し、「Submit」ボタンをクリックします。または、「Cancel」ボタンをクリックして「Rule Configuration」画面に戻ります。可能な値は以下の通りです。 • Permit - ACL 基準に適合するパケットを転送します。 • Deny - ACL 基準に適合するパケットを破棄します。
Logging	「Action」に「Deny」を選択した場合に表示されます。「True」に設定すると、ログ取得が ACL ルールに有効になります。（デバイスのリソース性能に依存します。）また、「Access List Trap Flag」が有効にされると、ログは現在のレポート間隔でこのルールが作用した回数を示す定期的なトラップを生成します。レポート間隔を 5 分に固定すると、全システムに使用されます。ACL ルールヒットカウントを現在の間隔に対して 0 にすると、トラップは発行されません。
Assign Queue ID	「Action」に「Permit」を選択した場合に表示されます。この AP ACL ルールに適合するすべてのパケットを処理するために使用されるハードウェアイーグレスキューの識別子を指定します。「Configure」ボタンをクリックし、適切な欄にキューを識別する番号（0-7）を入力します。「Submit」または「Cancel」ボタンをクリックし、「Rule Configuration」画面に戻ります。
Mirror Interface	「Action」に「Permit」を選択した場合に表示されます。通常のデバイスによる送信に加えて、一致するトラフィックストリームがコピーされる特定のイーグレスインタフェースを指定します。「Configure」ボタンをクリックし、メニューからインタフェースを選択します。ルールに一致するパケットは、選択インタフェースにミラーリングされます。「Submit」または「Cancel」ボタンをクリックし、「Rule Configuration」画面に戻ります。
Match Every	この ACL の基準に一致することをパケットに要求します。「Configure」ボタンをクリックし、メニューか「True」または「False」を選択します。「Submit」または「Cancel」ボタンをクリックし、「Rule Configuration」画面に戻ります。 「True」は、すべてのパケットが選択した IP ACL に一致し、許可または拒否されること意味します。「Match Every」（全一致）は、他のフィルタリングルールに対して排他的であるため、これを「True」にすると、画面にはその他のルールは表示されません。ルールに対する特定の一致基準の作成、ルールの削除、および再作成するためには、「Match Every」を他の一致基準に対して「False」に再設定します。
Protocol Keyword	選択した IP ACL ルールに対して一致させるパケットの IP プロトコルを指定します。指定可能な値は ICMP、IGMP、IP、TCP、および UDP です。「Protocol Keyword」または「Protocol Number」を使用して、一致基準として IP プロトコルの値を指定します。「Configure」ボタンをクリックし、メニューからプロトコルのキーワードを選択します。「Submit」または「Cancel」ボタンをクリックし、「Rule Configuration」画面に戻ります。
Protocol Number	選択した IP ACL ルールに対して一致させるパケットの IP プロトコルを指定します。プロトコルは番号で指定します。プロトコル番号は、IANA によって割り当てられた規格値であり、0-255 の整数で解釈されます。「Protocol Keyword」または「Protocol Number」を使用して、一致基準として IP プロトコルの値を指定します。
Source IP Address	パケットの送信元ポートの IP アドレスがここで示すアドレスに一致する必要があります。「Configure」ボタンをクリックし、適切な欄に IP アドレスを「.」で区切った 10 進数を使用して入力します。入力したアドレスは、パケットの送信元 IP アドレスと比較されます。また、画面で「Source IP Mask」も設定します。
Source IP Mask	送信元 IP アドレスのワイルドカードマスクを指定します。ワイルドカードマスクはどのビットが使用され、どのビットが無視されるかを決定します。「255.255.255.255」のワイルドカードマスクは、どのビットも重要でないことを示します。「0.0.0.0」のワイルドカードは、すべてのビットが重要であることを示します。ACL に対するワイルドカードマスク処理は、サブネットマスクとは異なる動作をします。ワイルドカードマスクは、本質的にサブネットマスクの逆です。サブネットマスクを使用する場合、マスクには、ネットワークアドレスに使用されるビット位置に「1」を持ち、使用されないビット位置に「0」を持っています。対照的に、ワイルドカードマスクはチェックしなければならないビット位置に「0」を持っています。ACL マスクのビット位置の「1」は、対応するビットを無視できることを示しています。送信元 IP アドレスを設定する場合、本項目が必要となります。「Source IP Address and Source IP Mask」画面で必要な情報を入力した後に、「Submit」または「Cancel」ボタンをクリックして「Rule Configuration」画面に戻ります。
Source L4 Port	パケットの TCP/UDP 送信元ポートがここで示すポートに一致する必要があります。「Configure」をクリックして設定画面にアクセスし、以下の項目の 1 つを指定します。 • Source L4 Keyword - ルールに基づく送信元ポートリストから希望する L4 キーワードを選択します。「Other」より他のキーワードを選択すると、画面が更新されて「Source L4 Port Number」が表示されます。 • Source L4 Port Number -「Source L4 Keyword」が「Other」の場合、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 IP Address	パケットの宛先ポートの IP アドレスがここで示すアドレスに一致する必要があります。「Configure」ボタンをクリックし、適切な欄に IP アドレスを「.」で区切った 10 進数を使用して入力します。入力するアドレスは、パケットの宛先 IP アドレスと比較されます。また、「Destination IP Mask」も設定します。
Destination IP Mask	「Destination IP Address」値と共に使用される IP マスクを「.」で区切った 16 進数で指定します。
Destination L4 Port	パケットの TCP/UDP 宛先ポートがここで示すポートに一致する必要があります。「Configure」をクリックして設定画面にアクセスし、以下の項目の 1 つを指定します。 • Destination L4 Keyword - ルールに基づいた宛先ポートリストから希望する L4 キーワードを選択します。「Other」より他のキーワードを選択すると、画面が更新されて「Destination L4 Port Number」が表示されます。 • Destination L4 Port Number -「Destination L4 Keyword」が「Other」の場合、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。有効範囲は 0-65535 です。

項目	説明
Service Type	「extended IP ACL」ルールに対して以下の 3 つの「Match」条件から 1 つを選択します。これらは IP ヘッダ内の同じ「Service Type」に一致条件を指定する別の方法ですが、それぞれが異なるユーザ表記を使用します。選択後に、適切な欄に値を指定します。 • IP DSCP - パケットの DSCP 値をルールと照合します。DSCP は、IP ヘッダの「Service Type」オクテットの上位 6 ビットとして定義されます。これはオプション設定であり、0-63 の整数で入力します。IP DSCP は、メニューから DSCP キーワードの 1 つを選択します。メニューの「Other」オプションを選択すると DSCP 値を入力するテキストボックスが表示されます。 • IP Precedence - パケット内の「IP Precedence」は、IP ヘッダの「Service Type」オクテットの上位 3 ビットとして定義されます。これはオプション設定です。チェックすると、本欄は、パケットの「IP Precedence」値をルールと照合します。「IP Precedence」値は、0-7 の整数です。パケットを ACL と照合するために、DSCP 値または IP Precedence 値が使用されます。 • IP TOS Bits - パケット内の IP TOS フィールドは、IP ヘッダの「Service Type」オクテットの全 8 ビットとして定義されます。チェックすると、IP ヘッダの「Service Type」のビットと照合します。例えば、ビット 7（ビット 7 は非常に重要です。）と 5 を設定した IP TOS 値をチェックし、ビット 1 をクリアするためには、TOS ビット値「0xA0」と TOS Mask「0xFF」を使用します。これはオプション設定です。 - TOS Bits - この値は、00-FF までの 16 進数です。パケットの TOS フィールド内のビットがここで入力した 2 桁の 16 進数と一致することが必要です。 - TOS Mask - この値は、00-FF までの 16 進数です。パケット内の IP TOS フィールドと比較するために使用されるビット位置を指定します。

IP ベースルールの変更

ルールは、所属する ACL がインタフェースにバインドされていない場合にだけ変更することができます。

1. 「IP ACL Rule Configuration」画面を表示します。

2. 「IP ACL」メニューから希望する ACL ID を選択します。

3. 「Rule ID」メニューから希望のルールを選択します。

4. 必要とされる残りのデータを編集します。

5. 「Submit」ボタンをクリックします。IP ベースルールを変更し、デバイスを更新します。

IP ベース ACL への新しいルールの追加

1. 「IP ACL Rule Configuration」画面を表示します。

2. 「IP ACL」メニューから希望する ACL ID を選択します。

3. 「Rule ID」に「Create Rule」を指定し、新しい ID 番号を入力します。

4. 必要とされる残りのデータを定義します。

5. 「Submit」ボタンをクリックします。新しいルールは指定した IP ベース ACL に割り当てられます。

IP ベース ACL からルールを削除する

1. 「IP ACL Rule Configuration」画面を表示します。

2. 「IP ACL」メニューから希望する ACL ID を選択します。

3. 「Rule」メニューから削除するルールを選択します。

4. 「Delete」ボタンをクリックします。新しいルールは指定した IP ベース ACL に割り当てられます。

5. 「Refresh」ボタンをクリックすると、最新の情報に更新します。

MAC アクセスコントロールリスト

MAC ACL は、連続してパケットを照合する 1 セットのルールからなります。パケットがルールの基準に一致する場合、指定ルールのアクション「Permit（許可）/Deny（破棄）」を適用し、追加のルールはチェックされません。本メニューでは、MAC ACL を適用するインタフェースを指定します。
MAC ACL のルールは、「MAC ACL Rule Configuration」画面を使用して、指定 / 作成されます。

MAC ACL には以下の機能があります。

- MAC ACL の設定
- MAC ACL ルール設定

まず、「MAC ACL Configuration」画面を使用して、ACL タイプを定義し、それに ID を割り当てます。次に、「MAC ACL Rule Configuration」画面を使用して、その ACL にルールを作成します。最後に、「ACL Interface Configuration」画面を使用して、ID 番号によって ACL をポートまたは VLAN に割り当てます。

MAC ACL の設定

MAC ベースの ACL の追加を行います。ACL については、「IP アクセスコントロールリスト」（222 ページ）を参照してください。

LAN タブ > QoS > Access Control Lists > MAC Access Control Lists > 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。

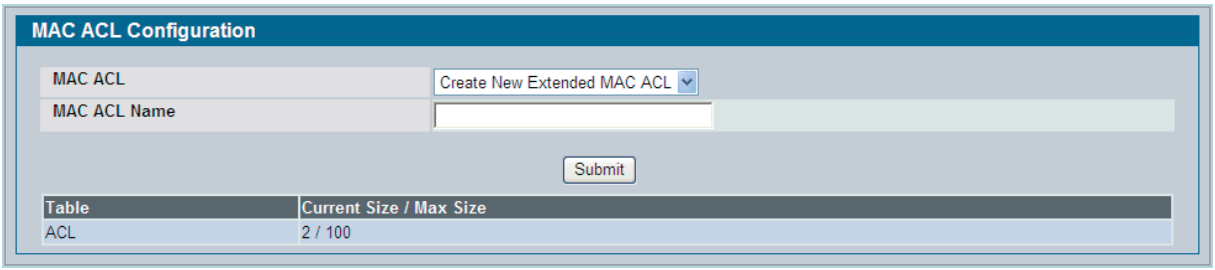


図 7-4　MAC ACL Configuration 画面

本画面には次の項目があります。

項目	説明
MAC ACL	新しい MAC ACL の作成、または名称を変更する既存リストの選択を行います。
MAC ACL Name	新しい MAC ACL の作成、または名称を変更する既存リストの選択を行います。

MAC ACL の追加

MAC ACL を追加するためには、「MAC ACL」メニューから「Create New Extended MAC ACL」を選択し、適切な欄に名前を入力し、「Submit」ボタンをクリックします。

名称の変更

名前を変更する MAC ACL を、「MAC ACL」メニューから選択します。適切な欄に新しい名称を入力し、「Rename」ボタンをクリックします。設定済みの MAC ACL が選択される場合にだけ、「Rename」ボタンが表示されます。

MAC ACL の削除

MAC ACL を削除するために、「MAC ACL」メニューから ACL 名を選択し、「Delete」ボタンをクリックします。設定した MAC ACL が選択される時にだけ、「Delete」ボタンが表示されます。

MAC ACL ルール設定

MAC ベースの ACL にルールを定義します。

アクセスリスト定義は、一致するトラフィックを通常通り転送するか、または破棄するかを指定するルールがあります。初期値の「deny all」は、すべてのリストにおける究極のルールです。

LAN タブ > QoS > Access Control Lists > MAC Access Control Lists > Rule 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。画面で利用可能な項目は、ルールアクションが許可または拒否するのか、「Rule」から「Create Rule」または既存のルールを選択するかによって異なります。

以下の図は「Rule」で「Create New Rule」が選択される場合に利用可能な項目を示しています。

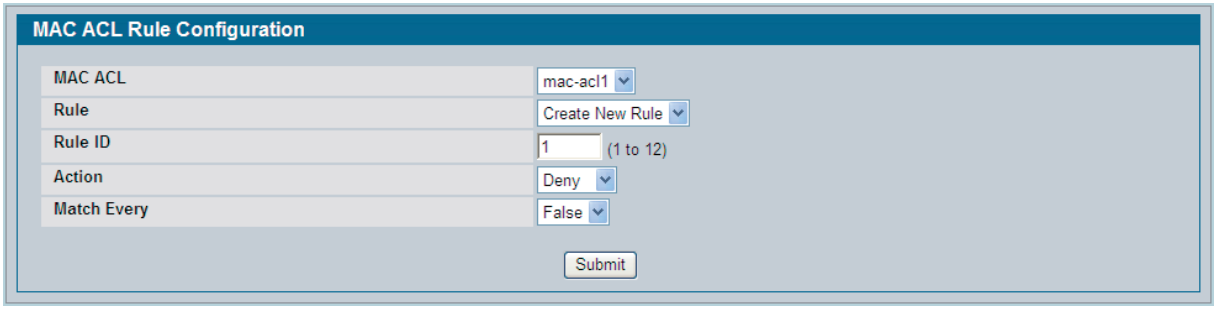


図 7-5　MAC ACL Rule Configuration - Create Rule 画面

以下の図は「MAC ACL Rule」に「Deny」アクションを指定する場合に利用可能な項目を示しています。

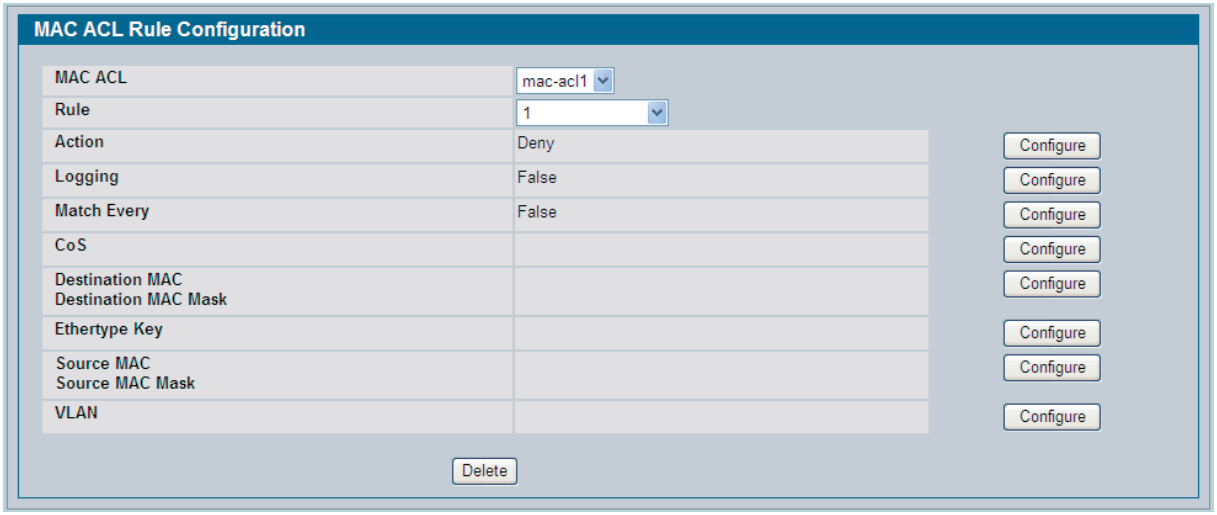


図 7-6　MAC ACL Rule Configuration - Deny アクション画面

以下の図は MAC ACL にルールを作成する場合に利用可能な項目を示しています。

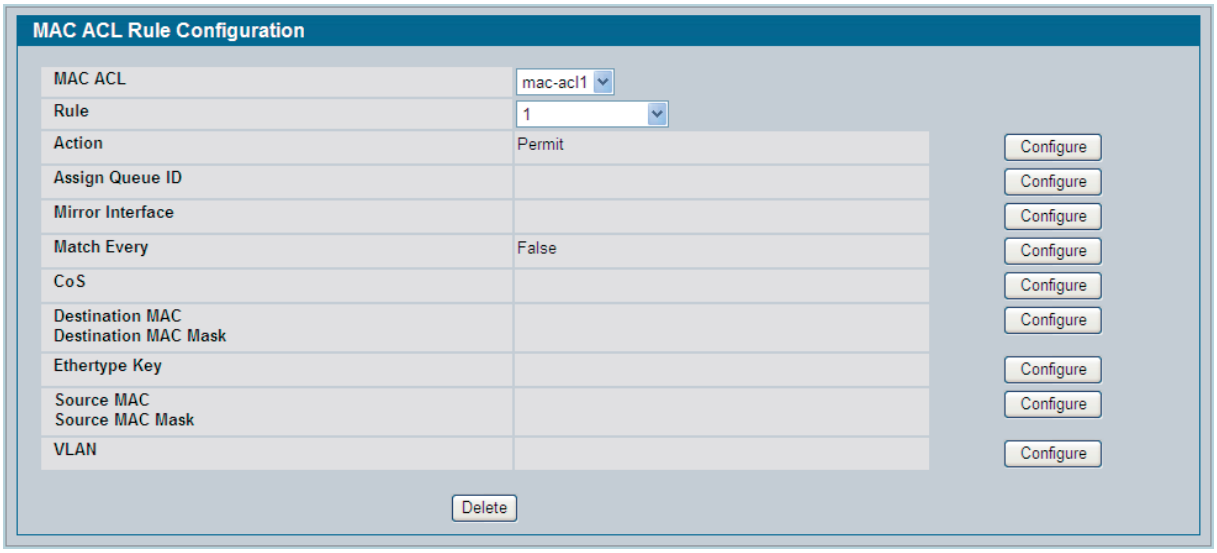


図 7-7　MAC ACL Rule Configuration - Permit アクション画面

以下の表は「MAC ACL Rule Configuration」画面で利用可能な項目を示しています。実際に利用可能な項目は、新しいルールを作成するか、または既存のルールを変更するか、さらにそのルールアクションを「Permit」または「Deny」とするかによって変わります。

項目	説明
MAC ACL	既存の MAC ACL を指定します。新しい MAC ACL を設定するためには、「MAC アクセスコントロールリスト」(227 ページ) を参照してください。
Rule	編集するためには、既存の Rule ID を選択し、新しい ACL ルールを設定するためには「Create Rule」を選択します。1-12 の範囲の番号を入力し、ルールを識別するために使用します。ルールの最大数に到達すると、新しいルールを作成することができなくなります。パケットは、各ルールに対して正確に指定ルールアクション「Permit」(許可) /「Deny」(拒否) を行うためにすべての指定基準に適合する必要があります。
Rule ID	「Rule」から「Create Rule」を選択した場合にだけ、本項目を使用することができます。新しい Rule ID を入力します。「Submit」ボタンをクリックするとに、新しい ID が作成され、ルール設定を行うことができます。各 ACL ごとに最大 12 個のルールを作成することができます。
Action	パケットがルールの基準に一致する場合に行うアクションを指定します。 • Permit - ACL 基準に適合するパケットを転送します。 • Deny - ACL 基準に適合するパケットを破棄します。
Logging	本欄は、「Action」に「Deny」を選択した場合に表示されます。「True」に設定すると、ログ取得が ACL ルールに有効になります。(デバイスのリソース性能に依存します。) また、「Access List Trap Flag」が有効にされると、ログは現在のレポート間隔でこのルールが作用した回数を示す定期的なトラップを生成します。レポート間隔を 5 分に固定すると、全システムに使用されます。ACL ルールヒットカウントを現在の間隔に対して 0 にすると、トラップは発行されません。
Assign Queue ID	本欄は、「Action」に「Permit」を選択した場合に表示されます。この AP ACL ルールに適合するすべてのパケットを処理するために使用されるハードウェアイーグレスキューの識別子を指定します。「Configure」ボタンをクリックし、適切な欄にキューを識別する番号 (0-6) を入力します。「Submit」または「Cancel」ボタンをクリックし、「Rule Configuration」画面に戻ります。
Match Every	この ACL の基準に一致することをパケットに要求します。「Configure」ボタンをクリックし、「True」または「False」を選択します。「Submit」または「Cancel」ボタンをクリックし、「Rule Configuration」画面に戻ります。 「Match Every」(全一致) は、他のフィルタリングルールに対して排他的であるため、これを「True」にすると、画面にはその他のルールは表示されません。「False」は、選択された ACL ルールに一致することがすべてのパケットに必須ではないことを示しています。
Mirror Interface	本欄は、「Action」に「Permit」を選択した場合に表示されます。デバイスによる通常の送信に加えて、一致するトラフィックストリームがコピーされる特定のイーグレスインタフェースを指定します。
CoS	Ethernet フレームと比較するために、802.1p ユーザプライオリティを指定します。パケットの CoS がここで示す CoS 値に一致する必要があります。「Configure」ボタンをクリックし、0-7 の CoS 値を入力して、この評価基準を適用します。「Submit」または「Cancel」ボタンをクリックし、「Rule Configuration」画面に戻ります。
Destination MAC Address	Ethernet フレームの宛先ポートの MAC アドレスがここで示すアドレスに一致する必要があります。「Configure」ボタンをクリックし、適切な欄に MAC アドレスを入力します。有効フォーマットは xx_xx_xx_xx_xx_xx です。BPDU キーワードは、Destination MAC アドレス「01:80:C2:xx:xx:xx」を使用して指定されます。「Submit」または「Cancel」ボタンをクリックし、「Rule Configuration」画面に戻ります。
Destination MAC Mask	必要に応じて、照合する送信先 MAC に関連する MAC マスクを入力します。MAC アドレスマスクは、Ethernet フレームに対して宛先 MAC のどのビットを比較するか指定します。MAC マスクには、ワイルドカードフォーマットで「F」と「0」を使用します。「F」はビットがチェックされないことを意味し、ビット位置の「0」はデータがそのビットに与えられた値と等しくなければならないことを意味しています。例えば、MAC アドレスが「aa_bb_cc_dd_ee_ff」でマスクが「00_00_ff_ff_ff_ff」である場合、「aa_bb_xx_xx_xx_xx」を持つすべての MAC アドレスが照合の結果となります (x は 16 進数)。「Submit」または「Cancel」ボタンをクリックし、「Rule Configuration」画面に戻ります。
Ethertype Key	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。「Configure」ボタンをクリックし、EtherType を選択します。「User Value」を選択すると、カスタム EtherType 値を入力することができます。
Ethertype User Value	「EtherType」から「User Value」を選択する場合にだけ、この項目は表示されます。入力値は、Ethernet フレームに比較するためにカスタマイズしている Ethertype を指定します。有効範囲は 0x0600-0xFFFF です。
Source MAC Address	パケットの送信元ポートの MAC アドレスがここで示すアドレスに一致する必要があります。「Configure」ボタンをクリックし、適切な欄に MAC アドレスを入力します。有効なフォーマットは xx:xx:xx:xx:xx:xx です。
Source MAC Mask	必要に応じて、照合する送信元 MAC に関連する MAC マスクを入力します。MAC マスクには、ワイルドカードフォーマットで「F」と「0」を使用します。「F」はビットがチェックされないことを意味し、ビット位置の「0」はデータがそのビットに与えられた値と等しくなければならないことを意味しています。有効なフォーマットは xx:xx:xx:xx:xx:xx です。「Submit」または「Cancel」ボタンをクリックし、「Rule Configuration」画面に戻ります。
VLAN	パケットの VLAN ID がここで示す ID に一致する必要があります。「Configure」ボタンをクリックし、この評価基準を適用する VLAN ID を入力します。有効範囲は、1-3599 です。「VLAN Range」または「VLAN」を設定できます。「Submit」または「Cancel」ボタンをクリックし、「Rule Configuration」画面に戻ります。

MAC ベース ACL への新しいルールの追加

MAC ACL を設定すると、ACL にルールを追加することができます。

1. 「MAC ACL Rule Configuration」画面を表示します。
2. 1 つ以上の MAC ACL がシステムに設定されている場合、「MAC ACL」メニューから希望の ACL を選択します。
3. 「Rule」メニューから「Create New Rule」を選択します。
4. 「Rule ID」に新しい ID 番号を入力します。
5. 必要とされる残りのデータを設定します。
6. 「Submit」ボタンをクリックします。新しいルールは指定した MAC ベース ACL に割り当てられます。

MAC ベース ACL からルールを削除する

1. 「MAC ACL Rule Configuration」画面で、「MAC ACL」から ACL を選択します。
2. 「Rule」メニューからルールを選択します。
3. 「Delete」ボタンをクリックします。MAC ベース ACL からルールを削除し、デバイスを更新します。

ACL インタフェース設定

ACL がインタフェースに割り当てられている場合、定義されたすべてのルールが、選択インタフェースに適用されます。以下の画面を使用して、ACL とインタフェースを割り当てて、各インタフェースに割り当てられる ACL を最優先とします。

LAN タブ > QoS > Access Control Lists > Interface 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。

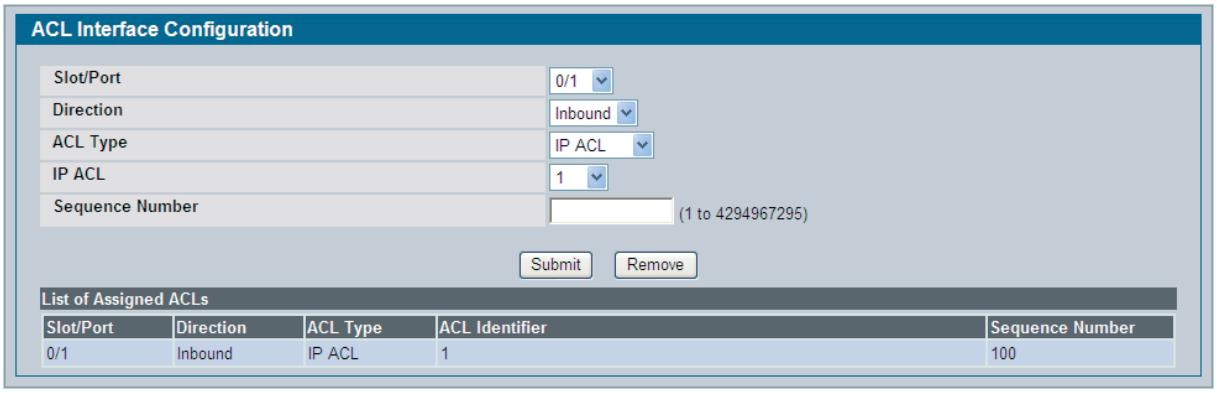


図 7-8　ACL Interface Configuration 画面

ACL をインタフェースに割り当てると、ページ下部のテーブルに表示されます。

本画面には次の項目があります。

項目	説明
Slot/Port	1 つ以上のインタフェースまたは LAG を選択します。
Direction	ACL にパケットフィルタリング方向を指定します。システムは内向きのフィルタリングをサポートしています。内向きのフィルタリングは、システムがインタフェースに入力されたパケットに ACL をルール適用することを意味します。
ACL Type	照合される入力パケットに適用する ACL タイプを選択します。「IP/MAC ACL」を指定すると、パケットは、IP ベースまたは MAC ベース ACL に照合されます。
Sequence Number	ACL に優先度を割り当てます。 1 つ以上の ACL がインタフェースに適用されると、最も高いシーケンスの ACL の適合基準が最初にチェックされます。より低い番号が高い優先度を示しています。シーケンス番号がこのインタフェースと「Direction」に既に使用されていると、指定のアクセスリストは、そのシーケンス番号を使用して現在割り当てられているアクセスリストを交換します。シーケンス番号が指定されないと、このインタフェースおよび「Direction」で現在使用している最も高いシーケンス番号より高い番号が使用されます。有効範囲は 1-4294967295 です。

ACL をインタフェースに割り当てる

1. 「ACL Interface Configuration」画面を表示します。

2. ACL を割り当てるインタフェースを「Slot/Port」から選択します。

3. 「ACL Type」で ACL のタイプを選択します。

4. インタフェースに割り当てる ACL ID または名称を選択します。ACL がポートまたは LAG に割り当てられる場合にはいつも、ACL に照合しないイングレスインタフェースからのフローは、一致しないパケットを破棄するデフォルトルールと照合されます。

5. 「Sequence」にプライオリティを指定します。

6. 「Submit」ボタンをクリックします。ACL は指定インタフェースに割り当てられます。

インタフェースから ACL を削除する

1. ACL がインタフェースにバインドされている場合、「Slot/Port」からインタフェースを選択すると「Remove」ボタンが画面に表示されます。

2. インタフェースから ACL を削除するためには、削除する ACL のタイプを選択し、その ID または名称を指定後「Remove」ボタンをクリックします。

第 6 章　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
クラス別サービスの設定	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。	209 ページ
CoS の設定	CoS 設定を行います。	217 ページ
オート VoIP の設定	分類メカニズムを音声パケットに提供します。	221 ページ

標準のスイッチでは、各物理ポートは、接続するネットワーク上でパケットを送信するために 1 つ以上のキューで構成されます。多くの場合、ポートごとに複数のキューが提供され　ユーザ定義の基準に基づいて特定のパケットが他のパケットより優先されます。パケットがポート内の送信キューにある場合に、これを処理する速度はキューの設定方法、ポートのその他のキューに存在するトラフィック量に依存します。遅延が必要な場合は、パケットは、スケジューラが送信のためにそのキューを許可するまで、キューに保持されます。キューが一杯になると、パケットを送信のために保持する場所がないため、スイッチによって破棄されます。

QoS は、厳しいタイミング要求のパケットを遅延が許容されるパケットと識別することで、一貫性があり予測可能な送信を提供する方法です。タイミング要求の厳しいパケットは、QoS をサポートするネットワークでは「特別扱い」を受けます。この点を考慮して、ネットワークのすべての要素が QoS 対応である必要があります。QoS 対応でないノードが少なくとも 1 つ存在するとネットワークパスに不具合が起こり、パケットフロー全体のパフォーマンスが低下します。

クラス別サービスの設定

QoS 機能が、Differentiated Services（DiffServ）のサポートを含んでいるため、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 処理を行うことができます。

標準の IP ベースのネットワークは、「最適な」データ送信サービスを提供するために設計されています。「最適な」サービスは、ネットワークがデータをタイムリーに送信することを意味しますが、保証はありません。輻輳状態の場合には、パケットには遅延、散発的な送信、破棄が起こるかもしれません。E-mail およびファイル転送などの代表的なインターネットアプリケーションでは、サービスのわずかな低下は容認され、多くの場合気づかれません。逆に、音声またはマルチメディアなどの厳しいタイミング要求を持つアプリケーションでは、サービスの低下は望ましくない結果をもたらします。

Diffserv の定義

QoS に DiffServ を使用するためには、最初に、以下のカテゴリとそれらの基準を定義するのに「Differentiated Services」メニューからアクセス可能な Web ページを使用する必要があります。

1. Class - クラスを作成し、クラスの基準を定義します。
2. Policy - ポリシーを作成し、ポリシーにクラスを関連付けてポリシーのステートメントを定義します。
3. Service - 内向きインタフェースにポリシーを追加します。

パケットは、定義した基準に基づいて分類されて、処理されます。分類の基準はクラスによって定義されます。その処理はポリシーの属性によって定義されます。ポリシーの属性はクラスごとにインスタンスベースで定義し、これらの属性は一致する場合に適用されます。ポリシーには、複数のクラスを含めることができます。ポリシーがアクティブな場合は、パケットがどのクラスに一致するかによって、アクションを行います。

パケット処理は、パケットに対してクラスの基準に一致するかどうかをテストすることで開始します。そのポリシーで一致するクラスが見つかると、ポリシーがパケットに適用されます。

「Differentiated Services」画面は様々な Diffserv 設定へのリンクを含みます。

LAN タブ > QoS > Differentiated Services には以下の機能があります。

- Diffserv 設定
- クラス設定
- ポリシー設定
- ポリシークラス設定
- サービス設定

Diffserv 設定

パケットは、定義した基準に基づいてフィルタされて、処理されます。フィルタリングの基準はクラスによって定義されます。その処理はポリシーの属性によって定義されます。ポリシーの属性はクラスごとにインスタンスベースで定義し、これらの属性は一致する場合に適用されます。

設定処理は、クラスに 1 つ以上の一致する基準を定義することから開始します。その後、1 つ以上のクラスがポリシーに追加されます。ポリシーはインタフェースに追加されます。

パケット処理は、パケットに対して基準に一致するかどうかをテストすることで開始します。クラスタイプオプションの「all」は、パケットがそのクラスに一致するために、クラス内のそれぞれの一致基準で評価する必要があることを定義します。クラスタイプオプションの「any」は、少なくとも 1 つの一致基準がパケットに対してそのクラスに一致するように評価する必要があることを定義します。クラスは、ポリシーに追加された順番でテストされます。そのポリシーで一致するクラスが見つかると、ポリシーがパケットに適用されます。

「Diffserv Configuration」画面を使用して、「DiffServ General Status Group information」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値の行数と最大行および現在の管理モード設定が含まれます。

LAN タブ > 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。

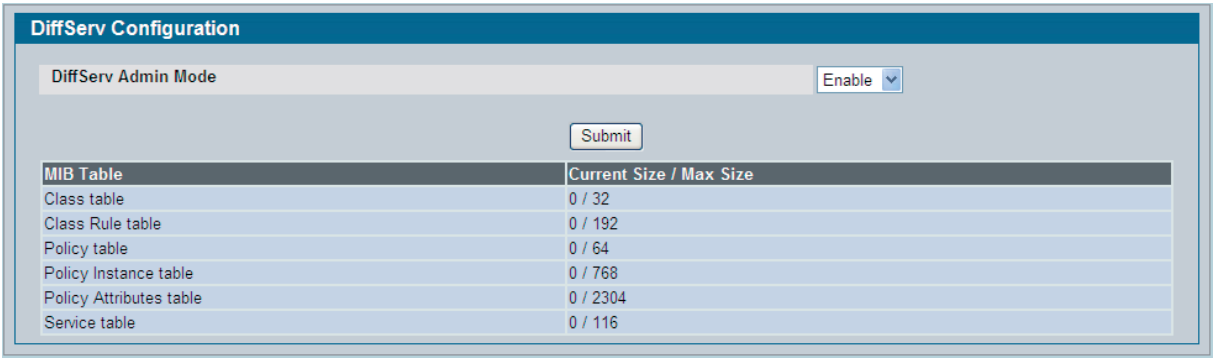


図 6-1　Diffserv Configuration 画面

本画面には次の項目があります。

項目	説明
Diffserv Admin Mode	admin モードをオン / オフを切り換えます。初期値は有効です。 • Enable - Differentiated Services はアクティブです。 • Disable - DiffServ 設定は保持され、変更できますが、アクティブではありません。
Class table	クラステーブルの現在の行数と最大の行数を表示します。
Class Rule table	クラステーブルの現在の行数と最大の行数を表示します。
Policy table	ポリシーテーブルの現在の行数と最大の行数を表示します。
Policy Instance table	ポリシーインスタンステーブルの現在の行数と最大の行数を表示します。
Policy Attributes table	ポリシー属性テーブルの現在の行数と最大の行数を表示します。
Service table	サービステーブルの現在の行数と最大の行数を表示します。

DiffServ admin モードを変更した場合、「Submit」ボタンをクリックし、変更をシステムに適用します。

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。本画面では、Diffserv クラスに割り当てる基準を定義します。パケットの受信時に、Diffserv クラスがパケットを最優先にするために使用されます。クラスに複数の一致する基準を持つことができます。この論理はこの評価基準用のブール論理積です。

LAN タブ > QoS > Differentiated Services > Class 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。

本画面で利用可能な項目は、新しいクラスを作成するか、または既に作成されたクラスを設定するかによって変わります。以下の画面は「Class Selector」オプションが「Create」である場合の画面です。

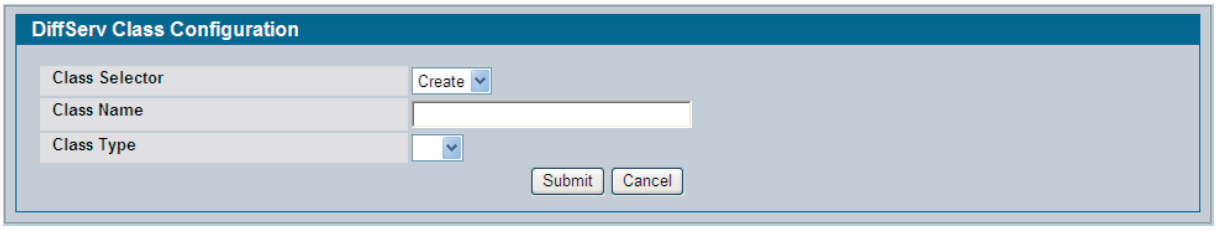


図 6-2　Diffserv Class Configuration 画面 - Create

以下の画面は、クラスが設定されている場合を示しています。

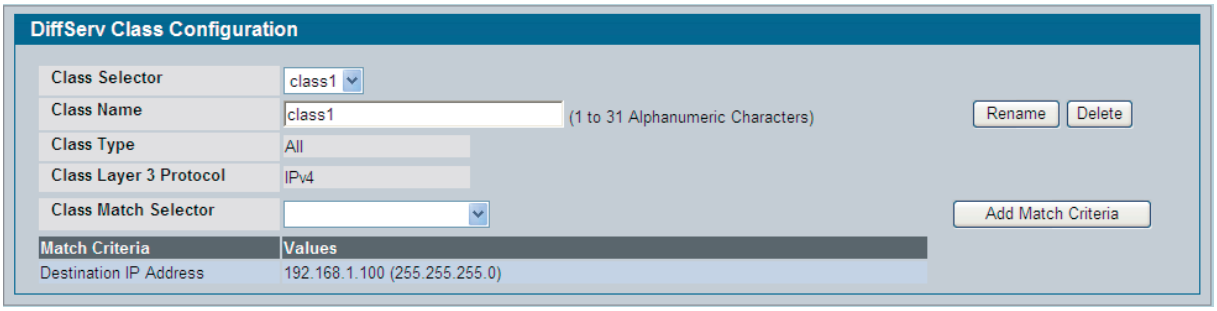


図 6-3　Diffserv Class Configuration 画面

本画面には次の項目があります。

項目	説明
Class Selector	新しい DiffServ クラスを設定するために、「Create」を選択します。既存のクラスを変更または参照するためには、クラス名を選択します。
Class Name	クラス名を入力します。新しいクラスを作成するためには、クラスタイプを選択し、「Submit」ボタンをクリックします。既存のクラス名を変更するためには、クラス名を入力後、「Rename」ボタンをクリックします。
Class Type	すべてのクラスタイプを表示します。現在、本ハードウェアは、クラスタイプに「All」だけをサポートしています。これは、パケットの一致のためには、クラスに対して定義された様々な一致基準のすべてが満たされる必要があることを意味します。「All」は、すべての一致基準の論理和を表しています。
Class Match Selector	指定クラスに追加できるすべての一致基準を示します。基準を設定するためには、リストから一致基準を選択し、「Add Match Criteria」ボタンをクリックします。画面は、そのクラス用の基準設定画面に変わります。基準を設定後、「Submit」ボタンをクリックしてクラスを基準に適用し、「Diffserv Class Configuration」画面に戻ります。基準を適用せずに「Diffserv Class Configuration」画面に戻るためには、「Cancel」ボタンをクリックします。一致基準と設定の各項目は以下の通りです。 • Destination IP Address - パケットの宛先ポートの IP アドレスがここで示すアドレスに一致する必要があります。「IP Address」に、有効な宛先 IP アドレスを「.」で区切った 10 進数形式で入力します。「IP Mask」に、IP アドレスのどのビットが意味があるかを決定するサブネットを入力します。これはワイルドカードマスクでないことに注意してください。 • Destination Layer 4 Port - パケットの TCP/UDP 送信元ポートがここで示すポートに一致する必要があります。ルールに基づくリストから希望する L4 キーワードを選択します。「Other」を選択すると、画面が更新されて「Port ID」が表示されます。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。有効範囲は 0-65535 です。 • 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 - これを選択すると、パケットの DSCP がクラスの基準に一致します。メニューから DSCP タイプを選択するか、または一致させる DSCP 値を入力します。「Other」を選択すると、「DSCP Value」が表示され、カスタム値を入力します。有効範囲は 0-63 です。 • IP Precedence -「0-7」の範囲で値を入力すると、パケットの IP 優先度値がクラスの基準に一致します。 • IP TOS - この値を入力すると、パケットの IP ヘッダ内のサービスのタイプビットがクラスの基準に一致します。「TOS Bits」に、パケットの「TOS」内のビットに一致する 2 桁の 16 進数を入力します。「TOS Mask」に、パケットの「IP TOS」と比較するために使用されるビット位置を指定します。 • Protocol - 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。「Other」を選択すると、フィールドが表示され、ここにプロトコル値を入力します。有効範囲は 0-255 です。 • Reference Class - 基準の参照を開始するクラスを選択します。指定クラスが別のクラスを参照する場合、指定クラスが大体同じタイプの別のクラスを 1 つ参照するため、「Reference Class」の一致基準は別のクラスの参照を追加させないように一致リストからなくなります。さらに、「Remove Class Reference」ボタンが画面に表示されます。ボタンをクリックして、現在のクラスから参照を削除します。 • Source IP Address - パケットの送信元ポートの IP アドレスがここで示すアドレスに一致する必要があります。「IP Address」に、有効な送信元 IP アドレスを「.」で区切った 10 進数形式で入力します。「IP Mask」に、IP アドレスのどのビットが意味があるかを決定するサブネットを入力します。これはワイルドカードマスクでないことに注意してください。 • Source Layer 4 Port - パケットの TCP/UDP 送信元ポートがここで示すポートに一致する必要があります。ルールに基づくリストから希望する L4 キーワードを選択します。「Other」を選択すると、画面が更新されて「Port ID」が表示されます。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。有効範囲は 0-65535 です。 • EtherType - フレームの Ethertype が選択した Ethertype リストに一致している必要があります。

新規エントリの追加

1. 「Diffserv Class Configuration」画面で「Create」を選択し、「Class Name」および「Class Type」を設定します。

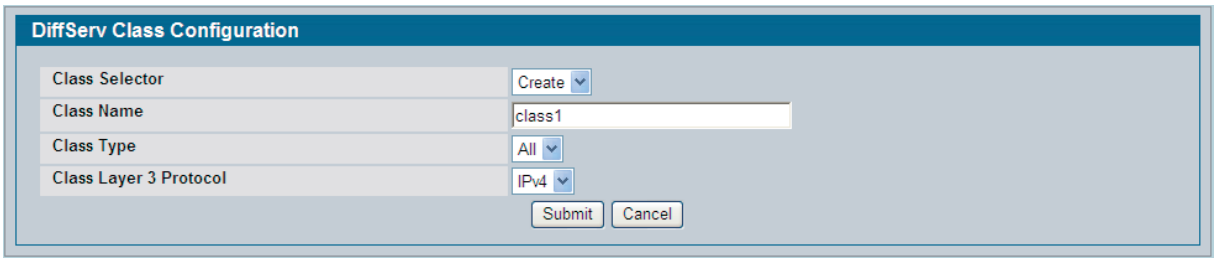


図 6-4　Diffserv Class Configuration 画面 - Create

2. 「Submit」ボタンをクリックして以下の画面を表示します。

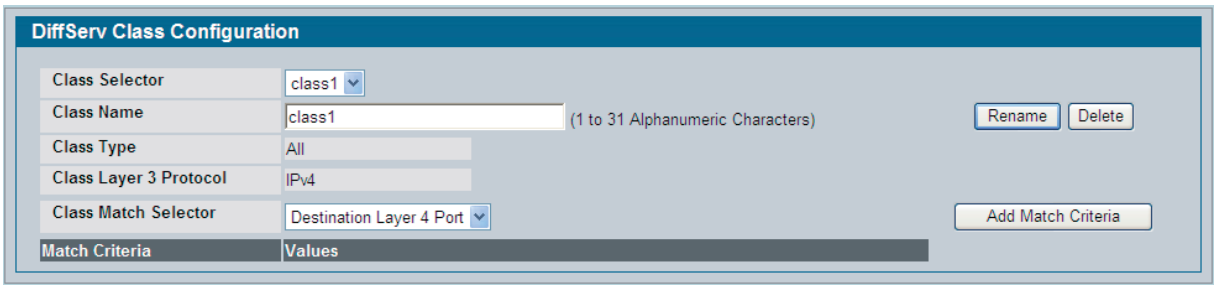


図 6-5　Diffserv Class Configuration 画面

3. 「Class Match Selector」を選択し、「Add Match Criteria」ボタンをクリックします。

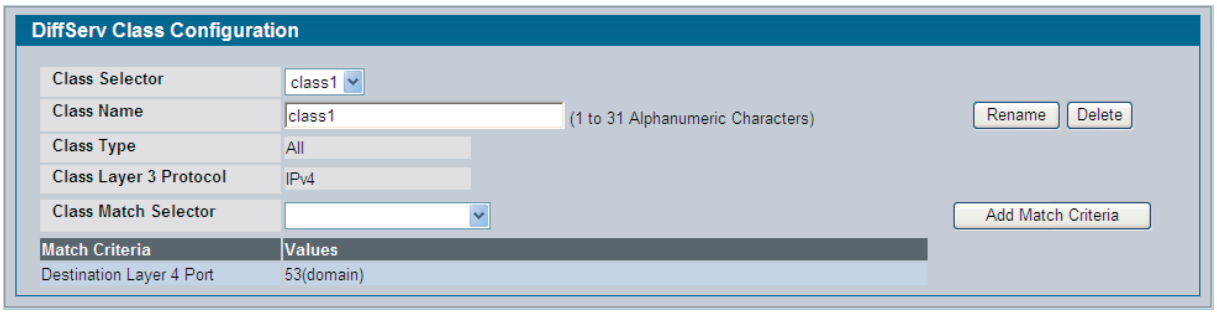


図 6-6　Diffserv Class Configuration 画面

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。

LAN タブ > 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。

利用可能な項目は、新しいクラスを作成するか、または既に作成されたクラスを設定するかによって変わります。
以下は、「Policy Selector」オプションが「Create」である場合の画面です。

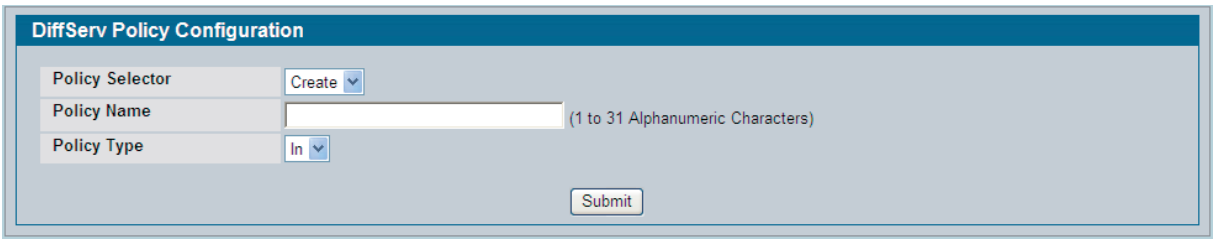


図 6-7　Diffserv Policy Configuration - Create 画面

以下は、「Policy Selector」オプションがメンバクラスを持つ設定ポリシーを表示している場合の画面です。メンバクラスを設定するためには、「クラス設定」（211 ページ）を参照してください。

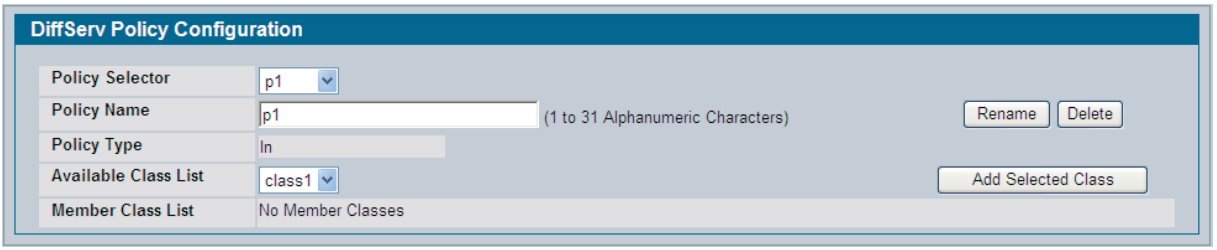


図 6-8　Diffserv Policy Configuration 画面

本画面には次の項目があります。

項目	説明
Policy Selector	新しくポリシーを作成するためには、「Create」を選択すると、新しいポリシーを作成する別の画面が表示されます。ポリシー名の変更、またはクラスリストのメンバを変更するためには、メニューからポリシー名を選択します。既存のポリシーを削除するために、削除するポリシーを選択し、「Delete」ボタンをクリックします。
Policy Name	「Policy Selector」から「Create」を選択し、クラスに関連付けるポリシー名を選択します。ポリシーをユニークに識別する名称は半角英数字 31 文字以内（大文字、小文字区別あり）で指定します。既存のポリシー名を変更するためには、「Policy Selector」で変更する名前を選択し、新しい名前を「Policy Name」に入力して、「Rename」ボタンをクリックします。
Policy Type	利用可能なポリシータイプは「In」です。これは、そのタイプが内向きトラフィック用であることを示しています。「Out」は、タイプが外向きトラフィック用であることを示しています。新しいポリシーを作成する場合のみ、本欄は設定可能です。ポリシーの作成後、これは設定済みのポリシータイプを表示する「設定不可能」な欄になります。
Available Class List	既存の DiffServ クラス名のすべてを表示します。新しいクラスの追加、またはポリシークラスを削除を行うと、自動的にリストは更新されます。DiffServ クラスをポリシーに関連付けるためには、リストからクラス名を選択し、「Add Selected Class」ボタンをクリックします。
Member Class List	ポリシーに追加されたすべての DiffServ クラス名を表示します。ポリシーから DiffServ クラスを削除するためには、リストからクラス名を選択して、「Remove Selected Class」ボタンをクリックします。ポリシーから新しいクラスを加えるか、または削除する場合、自動的にこのリストを更新します。

ポリシークラス設定

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。

LAN タブ > 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。

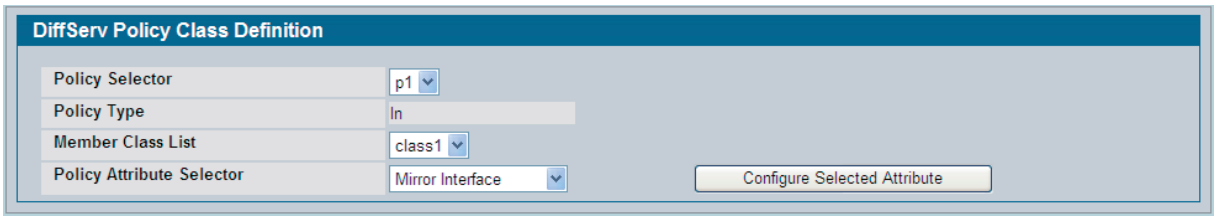


図 6-9　Diffserv Policy Class Definition 画面

選択したポリシー属性によっては、「Configure Selected Attribute」ボタンをクリックする場合に、適切な値の入力を有効にする画面を表示します。

これらの画面で利用可能な項目は以下の通りです。

項目	説明
Policy Selector	メンバクラスに関連付けるポリシーを選択します。
Policy Type	ポリシータイプを表示します。本項目は参照用です。
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	このポリシータイプにサポートされているすべての属性を表示します。ここから 1 つ選択することができます。属性を設定するためには、リストから属性を選択し、「Configure Selected Attribute」ボタンをクリックします。画面は、その属性用の属性設定画面に変わります。属性を設定後、「Submit」ボタンをクリックして変更を適用し、「Diffserv Policy Class Definition」画面に戻ります。属性を適用せずに「Diffserv Policy Class Definition」画面に戻るためには、「Cancel」ボタンをクリックします。属性と設定の各項目は以下の通りです。 • Assign Queue - このポリシークラスのパケットをキューに割り当てます。「Queue Id Value」に 0-7 を入力します。 • Drop Packets - 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。設定する項目はありません。「Drop」を選択し、「Configure Select Attribute」ボタンをクリック後、「Submit」ボタンをクリックすると属性はポリシーに追加されます。 • Mark CoS - 指定した「Class of Service」キュー番号を入力し、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を割り当てられてい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。（単一のタグ付きパケットにはタグだけ、ダブル VLAN のタグ付きパケットには first または outer 802.1Q タグ）パケットがまだこのヘッダを持っていない場合、1 つ挿入されます。CoS 値は、0-7 の整数です。 • Mark IP DSCP - この属性を使用して、メニューから選択した IP DSCP 値が割り当てられているトラフィックストリームに対するパケットのすべてをマークします。 • Mark IP Precedence - この属性を使用して、「IP Precedence Value」に入力した IP Precedence 値が割り当てられているトラフィックストリームに対するパケットのすべてをマークします。 • Police Simple - この属性を使用して、指定クラスのためにトラフィックポリシングスタイルを設定します。police コマンドのシンプルな形式では、単一のデータレートとバーストサイズを使用します。適合と違反の 2 つの結果がもたらされます。適合するデータレートは 1-4294967295（Kbps）で示されます。違反するバーストサイズは 1-128（KB）で示されます。「Police Simple」画面には以下の項目があります。 - Color Mode 「Color Aware」（カラー認識）モードには、このポリシーインスタンスと共に使用できる複数のカラークラスの存在が必要です。有効なカラークラスには、以下の項目に除外されない一致基準があります。（フィールドがポリシーインスタンス自身のクラシファイアとコンフリクトしない場合。） • IP DSCP • IP Precedence - Conform Action Selector 適合していると見なされるとパケットに何を行うアクションを決定します。 • Send -（初期値）これらのパケットは 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。 • Drop - これらのパケットは直ちに破棄されます。 • Mark CoS - これらのパケットは、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 DiffServe によって指定済みの CoS 値にマークされます。「Mark CoS value」でこれを選択する必要があります。 • Mark IP DSCP - これらのパケットは、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 DiffServe によって指定済みの DSCP 値にマークされます。「DSCP value」でこれを選択する必要があります。 • Mark IP Precedence - これらのパケットは、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 DiffServe によって指定済みの IP Precedence 値にマークされます。「Mark IP Precedence value」でこれを選択する必要があります。

項目	説明
Violate Action	適合していると見なされないパケットに行うアクションを決定します。 • Drop -（初期値）これらのパケットは直ちに破棄されます。 • Mark CoS - これらのパケットは、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 DiffServe によって指定済みの CoS 値でマークされます。「Mark CoS value」でこれを選択する必要があります。 • Mark IP DSCP - これらのパケットは、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 DiffServe によって指定済みの DSCP 値にマークされます。「DSCP value」でこれを選択する必要があります。 • Mark IP Precedence - これらのパケットは、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 DiffServe によって指定済みの IP Precedence 値にマークされます。「Mark IP Precedence value」でこれを選択する必要があります。 • Send -（初期値）これらのパケットは 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。

サービス設定

ポートのポリシーをアクティブ化します。

LAN タブ > QoS > Differentiated Services > Service 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。

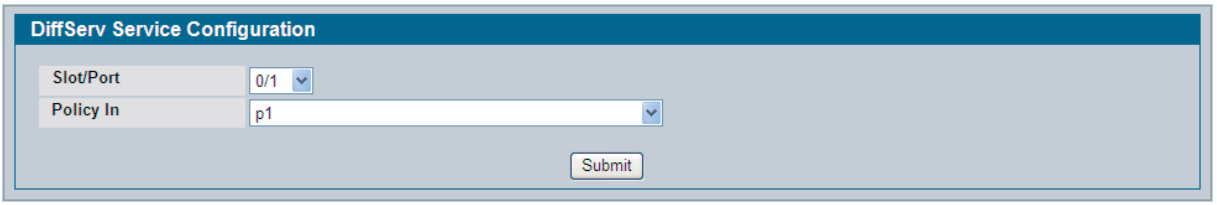


図 6-10　Diffserv Service Configuration 画面

本画面には次の項目があります。

項目	説明
Slot/Port	設定を行うインタフェース（physical、LAG、または All）を選択します。有効なスロット番号とポート番号の組合せリストです。
Policy In	ポートに関連付けるタイプが「In」のポリシー名を全て表示します。ここからポートに関連付けるポリシーを選択することができます。「None」を選択すると、この方向のインタフェースからポリシーが取り外されます。「Slot/Port」が「All」に指定されると、以下の項目が表示されます。
Direction	「Slot/Port」が「All」に指定されると、「Read/Write」権限のあるユーザだけがこれを選択することができます。このサービスインタフェースのトラフィック方向を選択します。
Operational Status	このサービスインタフェースの操作ステータス（Up または Down）を表示します。
Policy Name	インタフェースに割り当てられているポリシーを表示します。

インタフェースのポリシーをアクティブ化するために、インタフェースとポリシーを選択し、「Submit」ボタンをクリックします。

CoS の設定

CoS のキュー機能を使用すると、スイッチキューの特定の部分を直接設定できます。これは、複雑な DiffServ が必要とされない場合に、異なるネットワークトラフィックに対して希望する QoS の動作を提供します。インタフェースに到着したパケットの優先度は、マッピングテーブルを通じてパケットを適切な外向き CoS キューに送るために使用されます。最低保証帯域幅、送信レートシェーピングなどキューのマッピングに影響する CoS キューの特性は、キュー（またはポート）レベルでユーザが設定できます。システムはポートごとに 8 個（0-7）のキューをサポートしています。

CoS には以下の機能があります。

- 802.1p プライオリティのマッピング
- トラストモード設定
- IP DSCP マッピング設定
- CoS インタフェース設定
- CoS インタフェースキュー設定
- オート VoIP の設定

802.1p プライオリティのマッピング

IEEE 802.1p 機能は、MAC レベルにおいてトラフィックへの優先順位付けを許可します。スイッチは L2 フレームに割り当てられている 802.1p タグに基づいてトラフィックを優先させることができます。スイッチ上の各ポートには、指定する CoS 基準のクラスに基づいて、特定のパケットを他のパケットより優先させる複数のキューがあります。パケットがポート内の送信キューにある場合に、これを処理する速度はキューの設定方法、ポートのその他のキューに存在するトラフィック量に依存します。遅延が必要な場合は、パケットは、スケジューラが送信のためにそのキューを許可するまで、キューに保持されます。

802.1p 優先度値を 1 つ以上のインタフェース上の様々なトラフィッククラスに割り当てます。

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

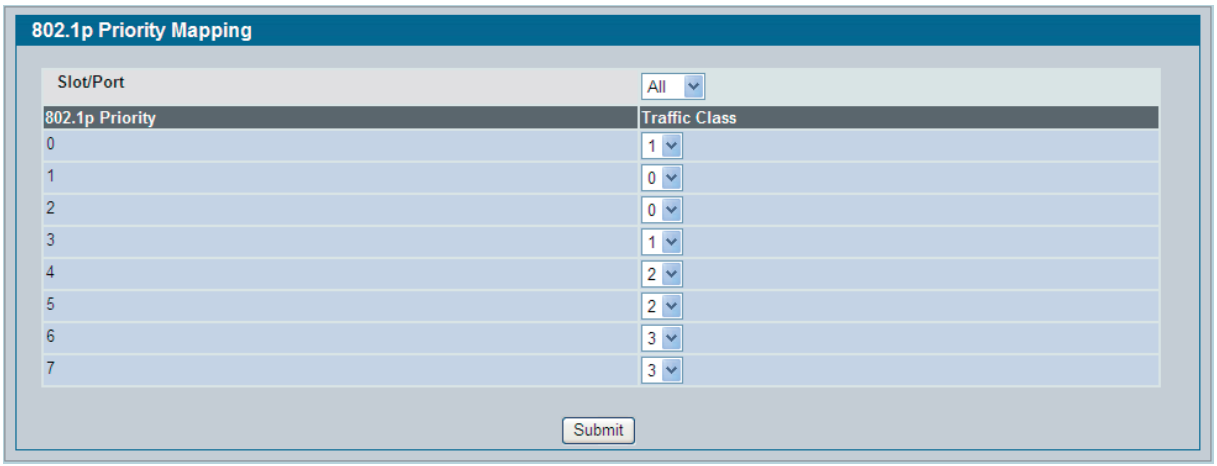


図 6-11　802.1p Priority Mapping 画面

本画面には次の項目があります。

項目	説明
Slot/Port	CoS 設定が適用されるインタフェースを選択します。
802.1p Priority	マップされる 802.1p 優先度を表示します。優先度は低い（0）から高い（7）まであります。例えば、0 の優先度を持つトラフィックが多くのデータトラフィックにあり、「ベストエフォート」を使用して送信されます。6 などの高い優先度を持つトラフィックは音声やビデオなどの時間に敏感なトラフィックである可能性があります。
Traffic Class	トラフィッククラスはポートのためのハードウェアキューです。優先度の高いトラフィッククラス値は、より高い位置を示します。低いキューにあるトラフィックが送信される前に、高いキューのトラフィックが送信されるのを待つ必要があります。優先度 -to- キューのマッピングの初期値を変更するためには、新しいトラフィッククラス値を選択します。

変更を行った場合、「Submit」ボタンをクリックし、新しい値をシステムに適用します。

トラストモード設定

インタフェースにおける CoS のトラストモードを設定します。スイッチの各ポートがパケットフィールド（802.1p または IP DSCP）の 1 つを信頼するように、またはどのパケットの優先度の指定も信頼しない（アントラストモード）ように設定することができます。ポートがトラストモードに設定されると、使用される信頼されたフィールドに適切なマッピングテーブルを使用します。このマッピングテーブルは、CoS キューが適切なイーグレスポートにパケットを転送するように指定します。もちろん、信頼されたフィールドはマッピングテーブルのためにパケットに存在する必要があり、そのためこれが事実である場合には初期アクションが実行されます。これらのアクションは、802.1p マッピングテーブルによってトラフィッククラスをマップされた既存のポートのデフォルト優先度に基づいて、イングレスポートに設定された特定の CoS レベルにパケットを送信することが必要です。

あるいは、ポートが信頼されていないとして設定される場合、ポートは入力パケットの優先度指定も信頼せず、代わりにポートデフォルト優先度の値を使用します。イングレスポートの設定済みデフォルト優先度に従って、アントラストポートのイングレスに到着するすべてのパケットが適切なイーグレスポートにある特定の CoS キューに向けられます。また、この処理は、non-IP パケットが IP 優先度または IP DSCP 値を信頼するように設定されたポートに到着する場合などトラストポートマッピングが有効でない場合に使用されます。

LAN タブ > QoS > Class of Service > Trust Mode 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。

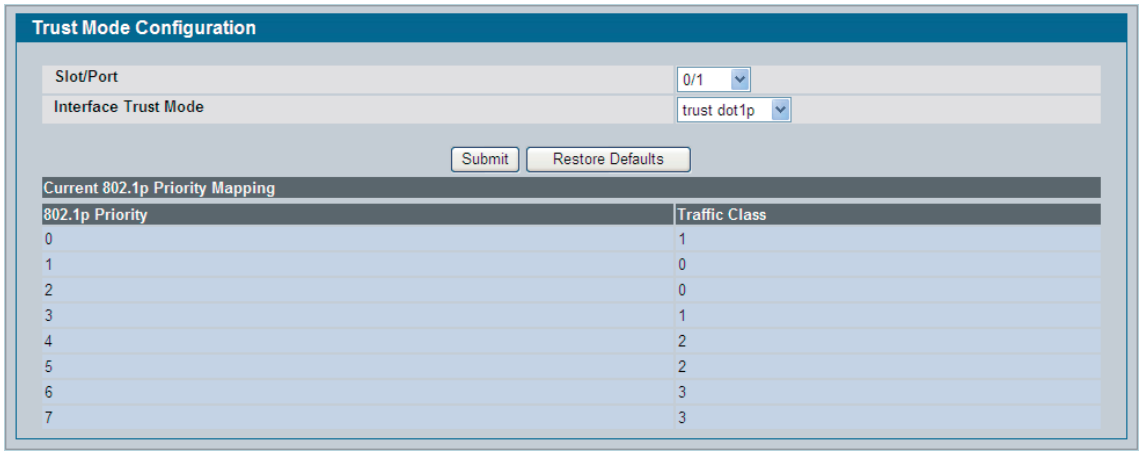


図 6-12　Trust Mode Configuration 画面

本画面には次の項目があります。

項目	説明
Slot/Port	CoS が設定可能な全インタフェースがあります。「Global」を選択するとすべてのインタフェースに同じトラストモードを適用します。メニューから個別のインタフェースを選択して、1 インタフェース毎にグローバル設定を上書きします。
Interface Trust Mode	インタフェース（「Slot/Port」が「Global」に設定される場合はすべてのインタフェース）が、パケットがポートに入る時にマークする特定のパケットを信頼するかどうかを指定します。以下のモードから 1 つ選択します。 • untrusted • trust dot1p（初期値） • trust ip-dscp
Non-IP Traffic Class	指定インタフェースのトラストモードが「trust ip-dscp」であると、本項目が表示されます。「trust ip-dscp」がインタフェースのトラストモードである場合、すべての non-IP トラフィックが向けられるトラフィッククラス（キュー）を表示します。値は 1 に固定されています。
Untrusted Traffic Class	指定インタフェースのトラストモードが「untrusted」であると、本項目が表示されます。「untrusted」モードである場合、すべてのトラフィックが向けられるトラフィッククラス（キュー）を表示します。値は 1 に固定されています。

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。

「Trust Mode Configuration」画面は、「Current 802.1p Priority Mapping 」テーブルも表示します。802.1p プライオリティマッピングについての情報は、「802.1p プライオリティのマッピング」（217 ページ）を参照してください。

LAN タブ > QoS > Class of Service > 802.1p Priority Mapping の順にメニューをクリックし、「802.1p Priority Mapping」画面を表示します。
詳しくは、「802.1p プライオリティのマッピング」（217 ページ）を参照してください。

設定のクリア

「Restore Defaults」ボタンをクリックして、選択したインタフェース（または「Global」が選択されている場合、全インタフェース）を初期値にリセットします。

IP DSCP マッピング設定

IP DSCP 値を内部トラフィッククラスにマップします。

LAN タブ > QoS > Class of Service > IP DSCP Mapping 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。

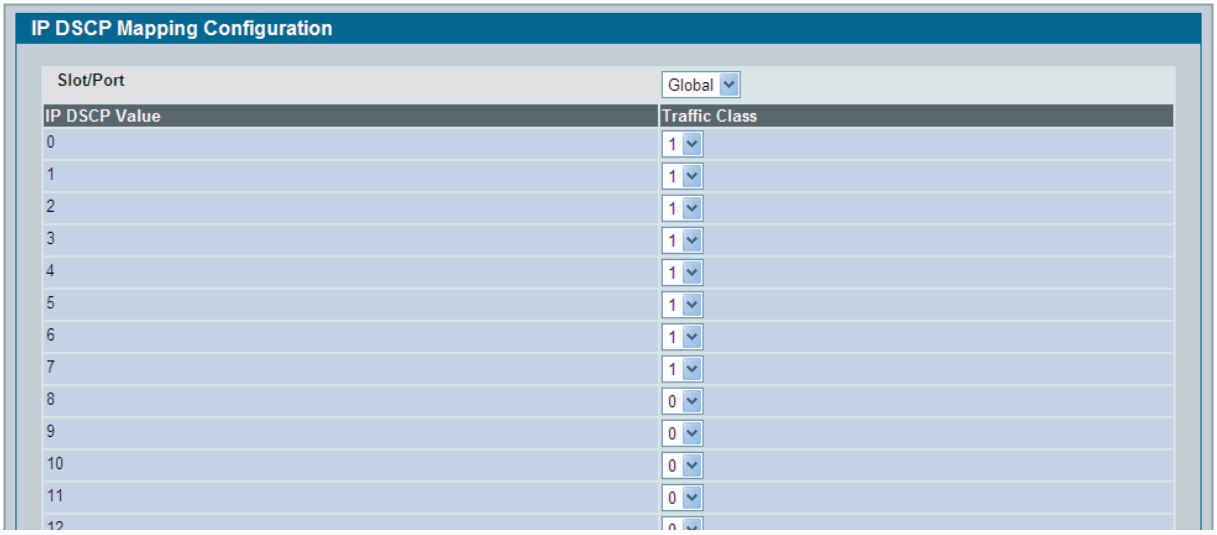


図 6-13　IP DSCP Mapping Configuration 画面

本画面には次の項目があります。

項目	説明
Slot/Port	メニューには CoS が設定可能な全インタフェースを含んでいます。オプションは「Global」だけです。これは、IP DSCP マッピング設定がすべてのインタフェースに適用され、1 インタフェース毎に適用できないことを意味します。
IP DSCP Values	内部トラフィッククラスをマップした IP DSCP 値を指定します。値の範囲は、0-63 です。
Traffic Class	トラフィッククラスはポートのためのハードウェアキューです。優先度の高いトラフィッククラス値は、より高いキュー位置を示します。低いキューにあるトラフィックは送信前に、高いキューのトラフィックの送信を待つ必要があります。有効範囲は 0-7 です。

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。

設定のクリア

「Restore Defaults」ボタンをクリックすると、すべてのインタフェースを初期値に戻ります。

CoS インタフェース設定

すべてのポート、または、指定ポートにインタフェースシェーピングレートを適用します。

LAN タブ > QoS > Class of Service > CoS Interface 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。

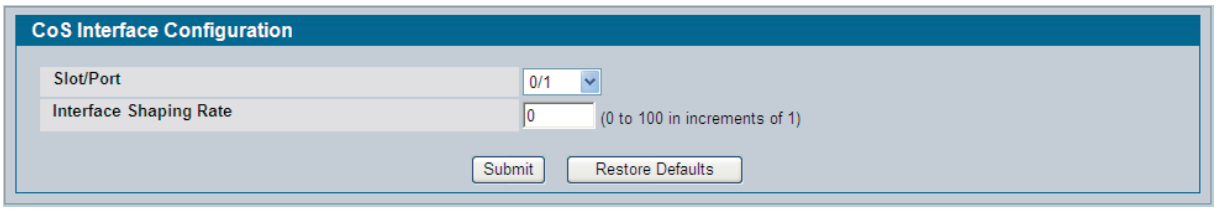


図 6-14　Interface Configuration 画面

本画面には次の項目があります。

項目	説明
Slot/Port	インタフェースシェーピングレートの影響を受ける CoS の設定可能なインタフェース を選択します。「Global」を選択するとすべてのインタフェースにレートを適用します。個別のポートを選択して、グローバル設定を上書きします。
Interface Shaping Rate	ポート上に残すことができるトラフィック量の上限を設定します。最大の伝送帯域幅の制限は時間がたつにつれて一時的なトラフィックバーストを円滑にする効果があるため、転送されるトラフィックレートが境界となります。指定値は、最大ネゴシエーション帯域幅の割合を表します。初期値は 0 です。有効な値は 0-100 で、増分は 1 です。0 の値は、無制限であることを意味します。

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。

設定のクリア

「Restore Defaults」ボタンをクリックして、すべてのインタフェースを初期値にリセットします。

CoS インタフェースキュー設定

どの指定キューがスイッチのイーグレスキューを設定することで動作するかを定義します。ユーザが設定可能なパラメータによって、キューが使用する帯域幅の量、輻輳時のキューの長さ、ポート上のすべてのキューのセットからのパケット送信スケジュールを制御します。
各ポートには、自身の CoS キューに関連した設定があります。

設定プロセスは、各 CoS キューパラメータがグローバルまたはポートごとに設定されることで簡素化されます。
グローバルな設定の変更は、システムにおけるすべてのポートに自動的に適用されます。

LAN タブ > QoS > Class of Service > CoS Interface Queue 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。

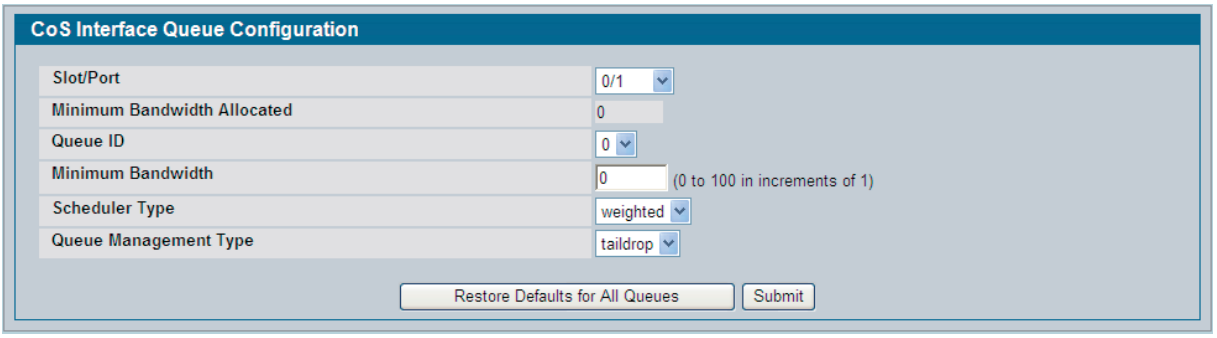


図 6-15　CoS Interface Queue Configuration 画面

本画面には次の項目があります。

項目	説明
Slot/Port	設定を行うインタフェース（physical、LAG、または All）を選択します。
Minimum Bandwidth Allocated	インタフェースにおけるすべてのキューに対して各最小帯域幅の合計を表示します。合計は定義した最大値の 100 を超えることはできません。この値は選択されたインタフェースにおけるキューに対する最小帯域幅を設定している際に考慮されます。
Queue ID	インタフェースに設定されるキューを選択します。
Minimum Bandwidth	インタフェースにおける選択キューに割り当てる最小の保証帯域幅を指定します。この値を対応する最大帯域幅よりも高く設定すると、最大値は自動的に同じ値に増えます。初期値は 0 です。有効範囲は 0-100 で、増分は 1 です。0 の値は、保証される最小値がないことを意味します。選択インタフェースにおけるすべてのキューに対する各最小帯域幅の合計は、定義した最大値の 100 を超えることはできません。
Scheduler Type	キューを処理するタイプを選択します。キューごとに定義することで、異なるトラフィックタイプに要求されるサービス特性を作成することができます。 • Weighted - 重み付けラウンドロビンが各キューに重みを割り当てます。（初期値） • Strict - 絶対優先度は、キューで優先度が最も高いトラフィックを最初に処理します。
Queue Management Type	本インタフェースのすべてのキューに使用される Queue Depth（キュー深度）管理のタイプを表示します。キュー管理タイプは「taildrop」だけです。キューのすべてのパケットは、輻輳が発生するまでは安全です。輻輳が発生した時点で、キューに追加されたパケットは破棄されます。

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。

設定のクリア

「Restore Defaults for All Queues」ボタンをクリックして、すべてのインタフェースを初期値にリセットします。
すべてのインタフェースに対して初期値にリセットするために、「Restore Defaults All Queues」ボタンをクリックする前に「Slot/Port」から「Global」を選択します。

オート VoIP の設定

Voice over Internet Protocol（VoIP）を使用すると、インターネットのようなデータネットワークを経由してコンピュータネットワークを使用することで通話をすることができます。遅延に敏感であるアプリケーション（音声、ビデオ、および他のマルチメディアアプリケーション）の重要性が増大し、今日ネットワークに展開している状態では、適切な QoS 設定が高品質なアプリケーション性能を確実にします。Auto VoIP 機能は、より適切な QoS を提供するためにデータパケットで優先されるように簡単な分類メカニズムを音声パケットに提供することを目的としています。

Auto VoIP 機能は、イーサネットスイッチにおける VoIP ストリームに明らかに一致しており、通常のトラフィックより適切なサービスクラスを提供します。インタフェースにおいて Auto VoIP 機能を有効にすると、インタフェースは以下の呼制御プロトコルのために入力トラフィックをスキャンします。

- Session Initiation Protocol（SIP）
- H.323
- Skinny Client Control Protocol（SCCP）

呼制御プロトコルがそのセッションで検出されると、スイッチは時間に敏感なトラフィックに一般的に使用される最も高い CoS キューにトラフィックを割り当てます。

オート VOIP の設定

オート VOIP の設定をします。

LAN タブ > QoS > Auto VoIP 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。

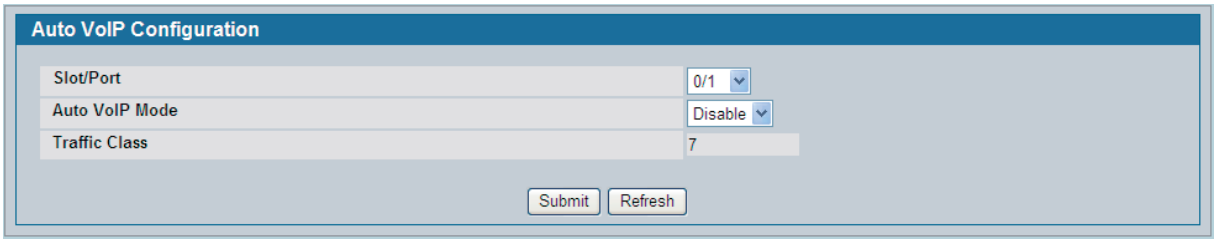


図 6-16　Auto VoIP Configuration 画面

本画面には次の項目があります。

項目	説明
Slot/Port	すべての Auto VoIP を設定可能なインタフェースを指定します。「All」はすべてのポートに行われた最新の設定を示します。これらの設定をインタフェース毎に上書きすることができます。
Auto VoIP Mode	オート VoIP モードを「Enable」または「Disable」にするために使用します。初期値は「Disable」（無効）です。
Traffic Class	VoIP トラフィック（値 7）に使用されるトラフィッククラスを表示します。

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。変更は直ちに反映されます。「Save」が実行されないと、これらの変更は再起動後に保持されません。

「Refresh」ボタンをクリックすると、画面の情報をスイッチにおける現在のデータを使用して更新します。

第 8 章　セキュリティ機能の設定

ポート、ユーザおよびサーバのセキュリティに管理セキュリティパラメータを設定します。以下の機能があります。

設定項目	説明	参照ページ
キャプティブポータル設定	ユーザ検証が確立されるまで無線クライアントのネットワークへのアクセスを防御します。	232 ページ
ポートアクセスコントロール	802.1X 機能の参照、および設定を行います。	252 ページ
RADIUS 設定	RADIUS サーバの設定および参照を行います。	257 ページ
TACACS+ の設定	TACACS+ サーバ間の通信のために TACACS+ の設定を行います。	262 ページ
HTTPS の設定	管理ステーションとスイッチ間の HTTPS 通信の設定を行います。	264 ページ
SSH の設定	管理ステーションとスイッチ間のセキュアなコマンドラインベースの通信のために設定を行います。	266 ページ

Captive Portal（キャプティブポータル設定）

キャプティブポータル（CP : Captive Portal）機能により、ユーザ検証が確立されるまで無線クライアントのネットワークへのアクセスを防御します。

キャプティブポータル認証を設定して、ゲストおよび認証されているユーザの両方にアクセスを許可することができます。認証済みのユーザは、アクセスを許可される前に、必ず認証済みキャプティブポータルユーザのデータベースに対して有効にしてください。このデータベースはスイッチに、または外部の RADIUS サーバに保持できます。

キャプティブポータルには「Captive Portal」設定を参照または設定する以下の機能があります。

- キャプティブポータルグローバル設定
- キャプティブポータル設定
- Local User 設定
- インタフェース接続
- CP グローバルステータス
- インタフェースステータス
- クライアント接続ステータス
- SNMP トラップ設定

キャプティブポータルグローバル設定

CP 機能の管理用ステータスを制御し、スイッチに設定されたすべてのキャプティブポータルに影響するグローバル設定を行います。

LAN タブ > Security > Captive Portal > 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。

ナビゲーションツリー内の WLAN タブと同様に、LAN タブから同じ「Captive Portal」フォルダにアクセスすることができます。グローバル設定の項目は、どこから「Captive Portal」フォルダにアクセスしているかに関係なく、無線および有線の CP 機能に適用することができます。

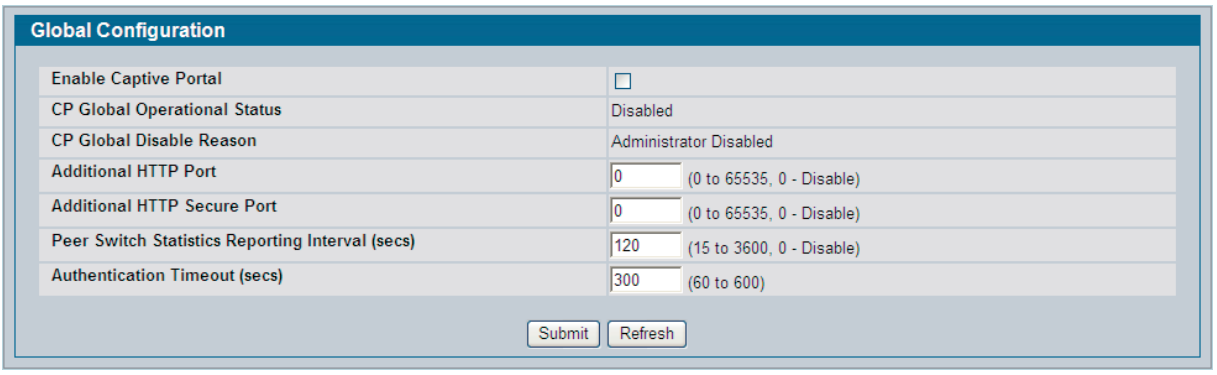


図 8-1　Global Configuration 画面

本画面には次の項目があります。

項目	説明
Enable Captive Portal	チェックボックスを選択して、スイッチの CP 機能を有効にします。キャプティブポータル機能を無効にするためには、チェックを外します。
CP Global Operational Status	CP 機能が有効かどうかを表示します。
CP Global Disable Reason	CP が無効の場合、以下の原因から一つが表示されます。 • None - なし。 • Administratively Disabled - 管理上無効です • No IPv4 Address - IPv4 アドレスではありません • Routing Enabled、But no IPv4routing interface - ルーティングが有効ですが、IPv4 ルーティングインタフェースではありません。
Additional HTTP Port	HTTP トラフィックはポート 80 を使用しますが、HTTP トラフィックに追加ポートを設定することができます。0-65535（ポート 80、443、およびスイッチのセキュリティ管理ポートに設定したポートは除く）のポート番号を入力します。
Additional HTTP Secure Port	SSL（HTTPS）上の HTTP トラフィックはポート 443 を使用しますが、HTTP トラフィックに追加ポートを設定することができます。0-65535（ポート 80、443、およびスイッチのセキュリティ管理ポートに設定したポートは除く）のポート番号を入力します。
Peer Switch Statistics Reporting Interval (sec)	スイッチにクラスタリングがサポートされている場合には、認証されたクライアント統計情報をクラスタコントローラに送信する頻度を決定する値（秒）を入力します。0 を入力すると、スイッチは統計情報を送信しません。
Authentication Timeout (secs)	認証セッションをクライアントと共にオープンしておく時間（秒）。ポータル経由でネットワークにアクセスするために、無線クライアントははじめに認証 Web ページに認証情報を入力する必要があります。タイムアウト時間になると、スイッチは、クライアントと接続するどんなアクティブな TCP や SSL も切断します。

キャプティブポータル設定

キャプティブポータルに関するサマリ情報の参照、キャプティブポータルの追加および設定済みのキャプティブポータルの設定を行います。また、「CP Summary」タブを使用してキャプティブポータル設定の作成、または削除をします。

スイッチは、10 個の CP 設定をサポートしています。CP 設定の 1 は初期状態で作成されて、削除することはできません。各キャプティブポータル設定には、固有のゲストまたはグループのアクセスモードとカスタマイズされた承認があり、クライアントが接続する場合に表示するポリシーを使用できます。

LAN > Security > Captive Portal > 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。

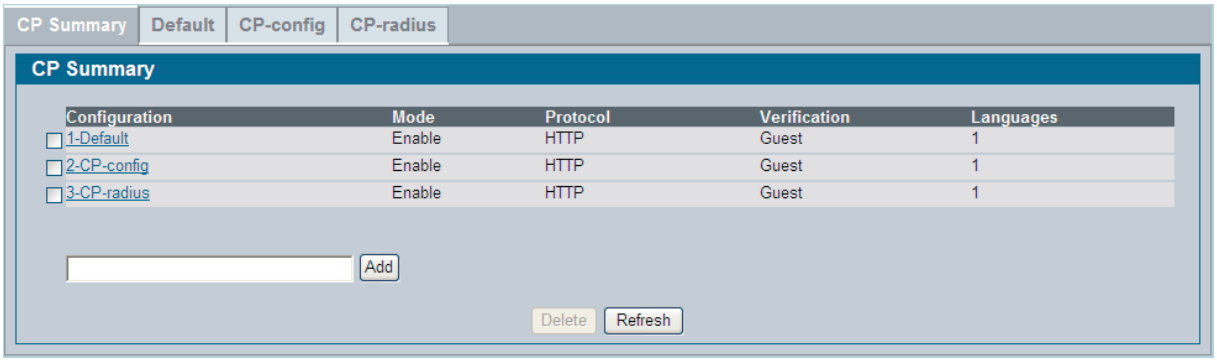


図 8-2　CP Summary 画面

CP 設定を作成するためには、テキストボックスに設定名を入力し、「Add」ボタンをクリックします。設定を追加すると、その設定の「CP Configuration」画面が表示され、設定名のタブが作成されます。

既存の CP を削除するためには、削除する CP にチェックを入れ、「Delete」ボタンをクリックします。既存の CP 設定を変更するためには、「Configuration」欄の名前をクリックし、対応するタブをクリックします。

注意　本書では、「CP Configuration」の代わりに「captive portal」、「CP」あるいは「portal」と呼ぶことがあります。

「CP Summary」画面には次の項目があります。

項目	説明
Configuration	キャプティブポータル ID と名前を表示します。定義済み CP の設定ページにアクセスするためには、設定名をクリックします。
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 を使用するか否かを表示します。
Verification	実行するユーザ検証のタイプを指定します。 • 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。 ローカルまたはリモートな RADIUS データベースで認証ユーザを設定するためには、「ローカルユーザの設定」（240 ページ）を参照してください。
Languages	このキャプティブポータルに設定されている言語の数を表示します。

Changing the Captive Portal Settings（キャプティブポータル設定の変更）

スイッチには、初期状態で 1 つのキャプティブポータルがあります。キャプティブポータルの設定変更、および最大 9 個までの追加ポータルを作成することができます。以下の画面からキャプティブポータルを作成した後に、設定を変更することができます。

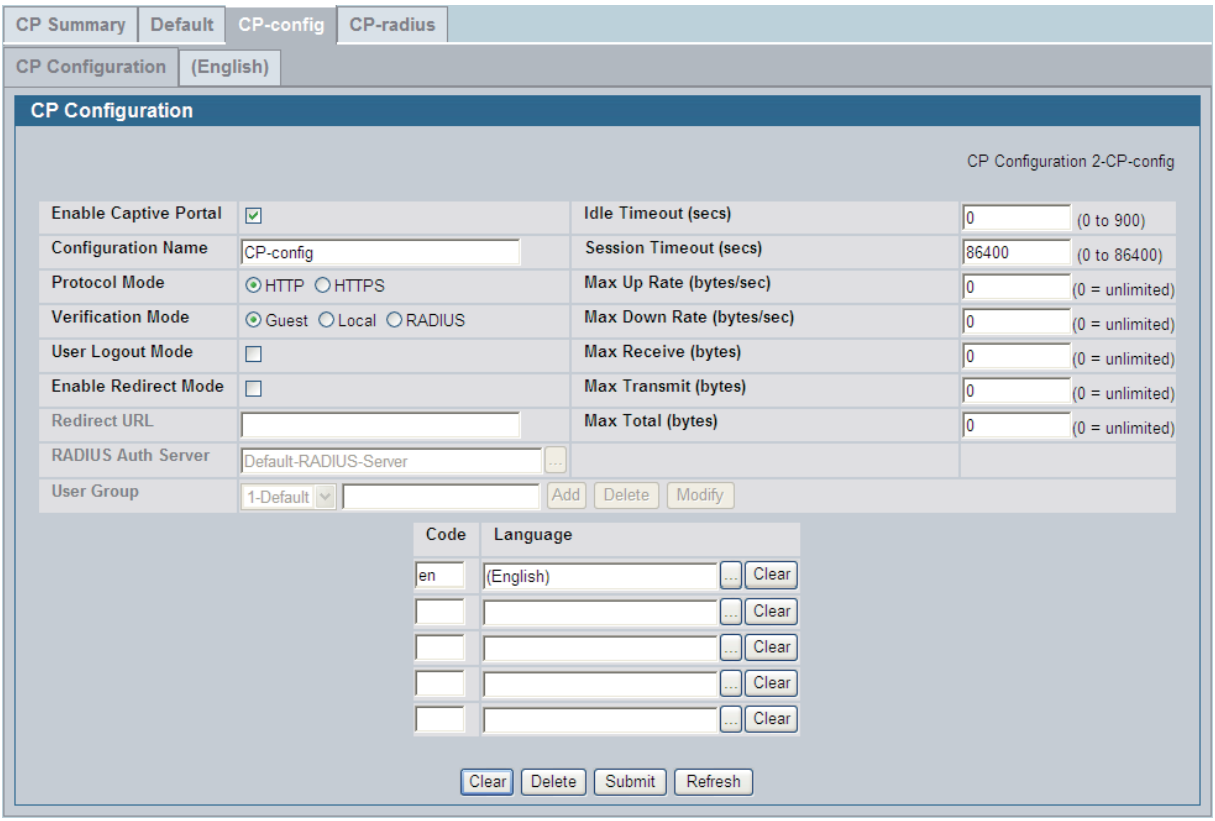


図 8-3　Captive Portal Configuration 画面

画面には次の項目があります。

項目	説明
Enable Captive Portal	チェックボックスを選択して、CP を有効にします。チェックを外して、機能を無効にします。
Configuration Name	「CP Summary」画面で追加されたポータル名を変更することができます。
Protocol Mode	検証プロセスの間にポータル用に使用するプロトコルを HTTP または HTTPS から選択します。 • HTTP - 検証プロセス中に暗号化は行われません。 • HTTPS - Secure Sockets Layer（SSL）を使用し、これは暗号化を提供する証明書を必要とします。証明書は接続時にユーザに提示されます。
Verification Mode	クライアントを認証するために、CP の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	認証クライアントをネットワークからその認証を解除することができます。このオプションが無効、あるいはユーザが特にログアウトを要求しない場合、クライアントの接続ステータスは、CP が、例えば「Idle Timeout」または「Session Timeout」に到達するなどでそのユーザの認証を取り消すまで継続します。

項目	説明
Enable Redirect Mode	CP が新しく認証したクライアントを、設定した URL にリダイレクトするように指定します。オプションがクリアされると、認証の成功後に指定した「welcome」画面が表示されます。
Redirect URL	「Enable Redirect Mode」モードを有効にした場合に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 を指定します。
RADIUS Auth Server	「Verification Mode」が「RADIUS」の場合、「…」ボタンをクリックして、クライアント認証に使用する RADIUS サーバ名を選択します。スイッチは RADIUS クライアントとして機能して、クライアントのためにすべての RADIUS トランザクションを行います。RADIUS サーバ情報を設定するためには、**LAN タブ > Security > RADIUS > RADIUS Authentication Server Configuration** の順にメニューをクリックします。
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。値を 0 に設定すると、タイムアウトにはなりません。初期値は 0 です。 **注意** 本バージョンではハードウェアの制限のため、有線のキャプティブポータルクライアントにアイドルタイムアウトは実施できません。
Session Timeout (secs)	セッション終了前の待機時間（秒）。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。値を 0 に設定すると、タイムアウトにはなりません。初期値は 0 です。
Max Up Rate (bytes/sec)	クライアントがキャプティブポータルを使用する場合にクライアントがトラフィックを送信できる最大値（byte）を入力します。この設定により、クライアントがデータをネットワークに送信できる帯域幅を制限します。
Max Down Rate (bytes/sec)	クライアントがキャプティブポータルを使用する場合にクライアントがトラフィックを受信できる最大値（byte）を入力します。この設定により、クライアントがデータをネットワークに受信できる帯域幅を制限します。
Max Receive (byte)	キャプティブポータルを使用する場合にクライアントが許可される受信の最大値（byte）を入力します。この制限値に達すると、ユーザは接続を切断されます。
Max Transmit (byte)	キャプティブポータルを使用する場合にクライアントが許可される送信の最大値（byte）を入力します。この制限値に達すると、ユーザは接続を切断されます。
Max Total (byte)	キャプティブポータルを使用する場合にクライアントが許可される通信（送受信の総和）の最大値（byte）を入力します。この制限値に達すると、ユーザは接続を切断されます。
User Group	「Verification Mode」が「Local」または「RADIUS」の場合、既存のユーザグループをキャプティブポータルに割り当てるか、または新しいグループを作成します。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。「User Group」リストは、スイッチのすべての CP 設定で同じです。 すべてのキャプティブポータルに対するユーザグループの追加、削除または名前の変更ができます。 • 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、「User Group」欄にグループ名を入力し、「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、メニューから変更する名前を選択し、新しい名前を空白の欄に入力して、「Modify」ボタンをクリックします。 • ユーザグループを削除するためには、メニューから削除する名前を選択し、「Delete」ボタンをクリックします。 **注意** 「Verification Mode」が「Guest」の場合、「User Group」欄は使用できません。
Code	IANA 言語タグに言語コードを入力します。すべてのコードは IANA 言語タグに表示されます。スイッチに言語がサポートされている場合、言語を選択するとコードが自動的に入力されます。
Language	スイッチがサポートする言語にキャプティブポータル設定を追加するためには、「…」ボタンをクリックしてキャプティブポータルに使用する言語を表示、選択します。

キャプティブポータル Web ページのカスタマイズ

無線クライアントがアクセスポイントに接続すると、Web ページが表示されます。「CP Web Customization」画面では、特定のテキストや画像で画面のカスタマイズをすることができます。

すべてのページが同じ認証タイプを使用していれば、それぞれのキャプティブポータルに対し最大 5 つのローカル Web 画面（ゲスト用または認証ユーザ用）を作成することが可能です。これによってさまざまな言語で画面を作成することが可能となり、異なるグループやユーザに対応することができます。

「CP WEB Customization」画面にアクセスするためには、画面タイトルの上の言語タブをクリックします。例えば、キャプティブポータル画面の「English」をクリックして、画面表示を英語にカスタマイズします。

カスタマイズ欄の上のメニューを使用してカスタマイズする Web 画面の範囲を選択します。本画面は以下の 5 つのカテゴリに区分されています。

- 「Global」パラメータ - 他の CP 画面と設定が共有できます。
- 「Authentication」画面 - ユーザが CP を経由してネットワークに接続をしようとする時に初めに表示される画面の設定をします。
- 「Welcome」画面 - ユーザがネットワークの接続に成功した場合に表示される画面の設定をします。
- 「Logout」画面 - ユーザが認証に成功した後に表示されるクライアントログアウト画面の設定をします。本画面には「logout」ボタンが含まれます。
- 「Logout Success」画面 - ユーザの認証が無効になった後に表示される画面の設定をします。

「CP Web Customization」画面の入力可能な項目はメニューから選択したカテゴリによって異なります。カテゴリ内の項目を変更した後は、必ず「Submit」ボタンをクリックしてから別のカテゴリを選択してください。そうしないと、変更は保存されません。

「Authentication」、「Welcome」、「Logout」、および「Logout Success」画面の例を表示するためには、「Preview」ボタンをクリックします。新しくブラウザ画面が開いてその画面が表示されます。

リモート RADIUS サーバ内のポータルユーザを設定するためには、「リモート RADIUS サーバにユーザを設定する」（242 ページ）を参照してください。

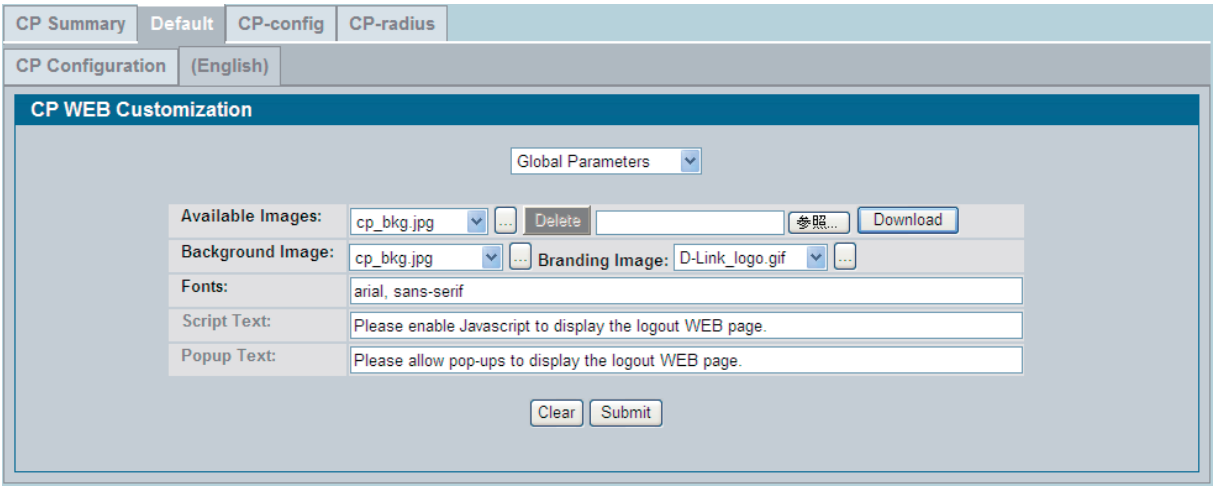


図 8-4　CP Web Customization - Global Parameters 画面

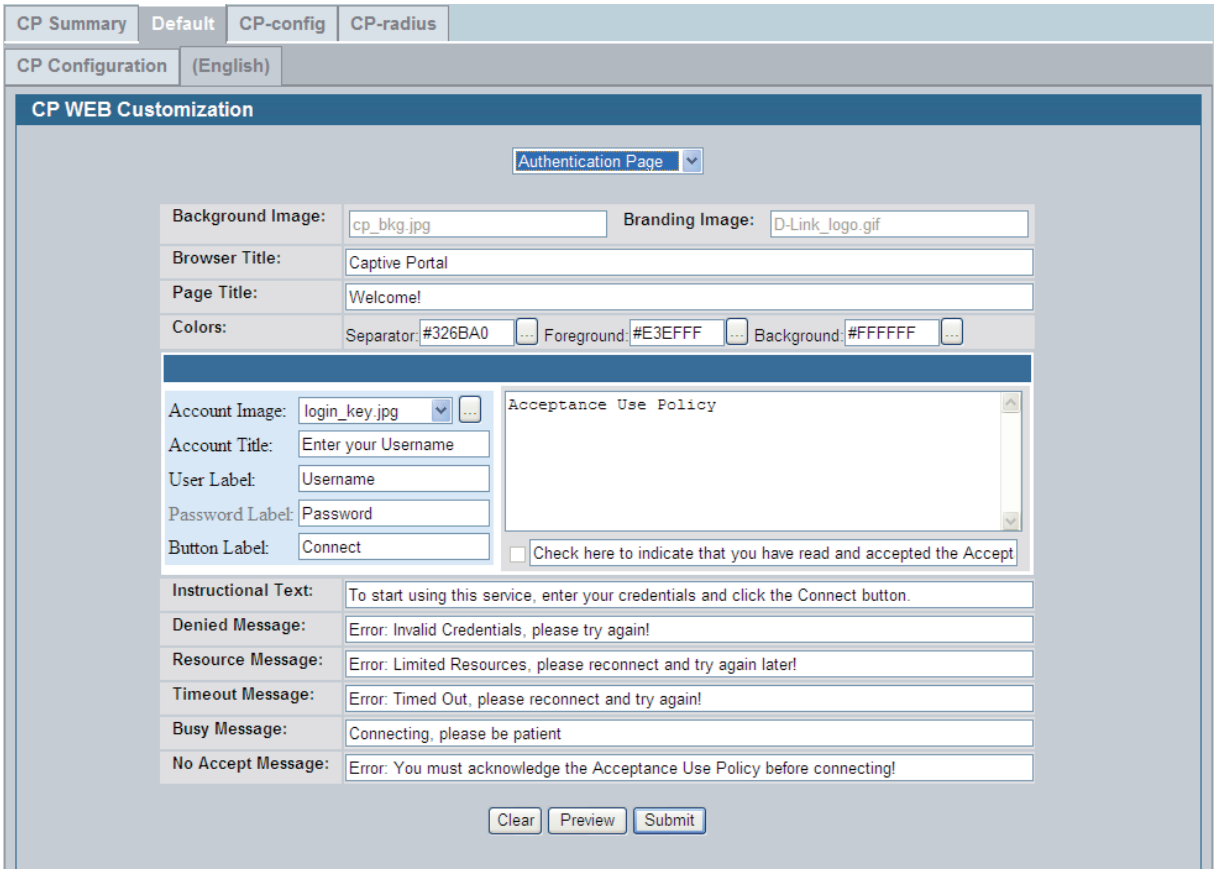


図 8-5　CP Web Customization - Authentication 画面

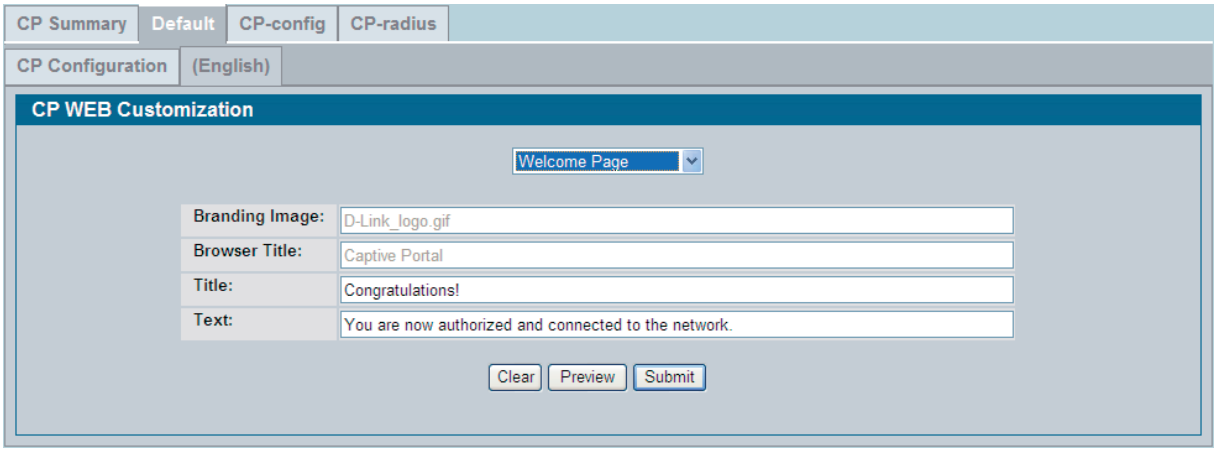


図 8-6　CP Web Customization - Welcome 画面

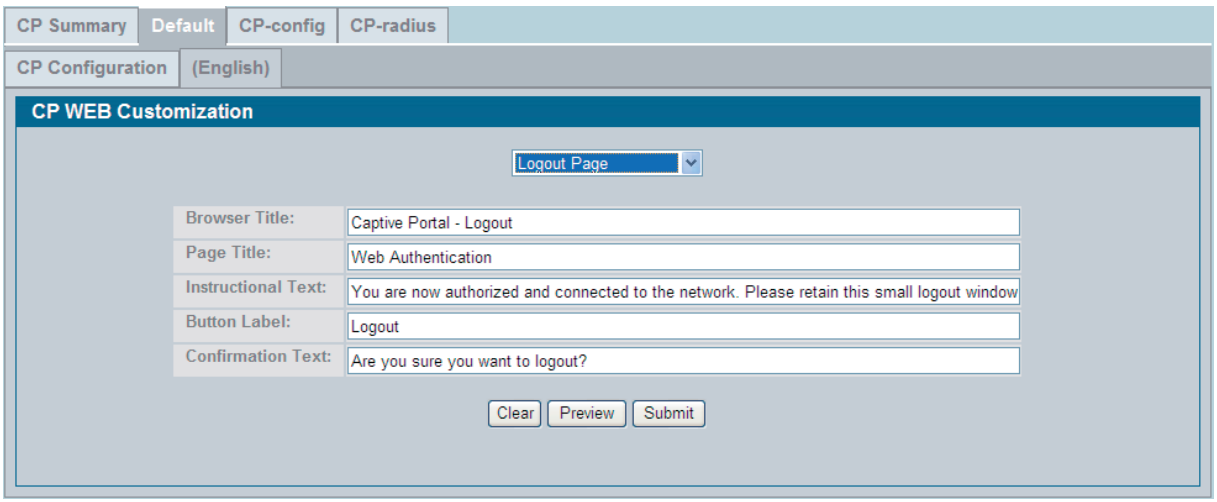


図 8-7　CP Web Customization - Logout Page 画面

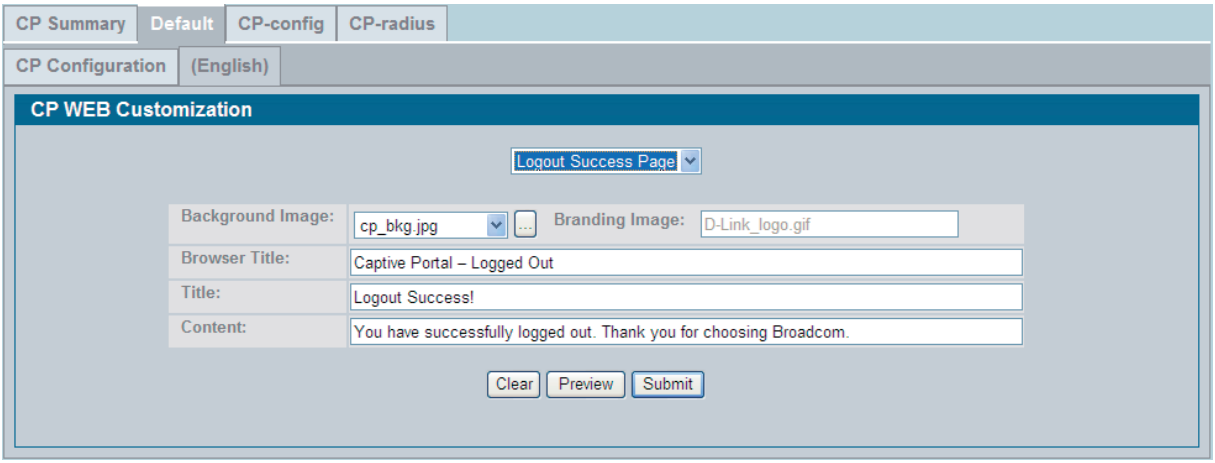


図 8-8　CP Web Customization - Logout Success Page 画面

本画面には次の項目があります。

項目	説明
グローバルパラメータ	
Available Images	メニューには画面背景、ブランド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。画像を追加する場合は、「Browse」ボタンをクリックし、ご使用のコンピュータ（または共有システム）から画像を選択します。「Download」ボタンをクリックすると、画像のダウンロードを開始します。画像は最大 5KB、200x200 画素、GIF または JPG 形式とします。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	画像ファイル名を選択して画面背景として表示します。プルダウンメニューを使用して、利用可能な画像のファイル名を表示します。「...」ボタンをクリックして利用可能な画像を表示します。選択した画像をクリックします。背景画像を使用しないように指定するためには、「No Selection」を選択します。
Branding Image	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目的に使用します。プルダウンメニューを使用して、利用可能な画像のファイル名を表示します。「...」ボタンをクリックし、利用可能な画像を表示します。選択した画像をクリックします。ブランド画像を使用しないように指定するためには、「No Selection」を選択します。
Fonts	CP 画面のテキストに使用するフォント名を入力します。
Script Text	ログアウトの Web 画面を表示するのに JavaScript を有効にする必要があることをユーザに示すテキストの指定を行います。これは「User Logout Mode」が有効の場合にのみ適用されますが、機能の有効、無効に関わらずテキストの変更は可能です。
Popup Text	ログアウトの 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ユーザに示すテキストの指定を行います。これは「User Logout Mode」が有効の場合にのみ適用されますが、機能の有効、無効に関わらずテキストの変更は可能です。
Authentication Page	
Background Image	「Authentication」画面の現在の背景画像のファイル名を表示します。本設定は「CP WEB Customization Global Parameters」画面で行うことができます。
Branding Image	「Authentication」画面の現在のブランド画像名を表示します。本設定は「CP WEB Customization Global Parameters」画面で行うことができます。
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され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。画面を識別するテキストです。
Colors	CP 画面に使用する色を選択します。ボタンをクリックして、使用する色を選択します。選択した色によってサンプルアカウント情報が更新されます。
Account Image	キャプティブポータル画面でログイン欄の上部に表示する画像を選択します。画像表示領域は縦横 55X310 画素です。 注意　画像は表示領域に合わせてサイズが変更されます。 新しい画像をダウンロードするためには、「CP WEB Customization Global Parameters」画面の「Available Image」を使用します。
Account Title	ユーザに認証を指示するサマリテキストを入力します。
User Label	ユーザがユーザ名を入力するフィールドの横に表示するテキストを入力します。
Password Label	ユーザがパスワードを入力するフィールドの横に表示するテキストを入力します。
Button Label	ユーザが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」フィールドに表示され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ている時に状況を示します。ポリシーは 8192 文字のテキストを含むことができます。

項目	説明
Acceptance Check Box Prompt	ユーザが使用条件を承諾したことを示す時に選択する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なテキストを入力します。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示さない場合に表示するテキストを入力します。このメッセージは、ユーザがボタンをクリックしてネットワークに接続した後に表示されます。
Resource Message	システムリソース制限のためシステムが認証を拒否した場合に表示するテキストを入力します。このメッセージは、ユーザがボタンをクリックしてネットワークに接続した後に表示されます。
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テキストを入力します。これはユーザの入力時間、または全体のトランザクションのタイムアウト時に表示されます。
Busy Message	キャプティブポータル機能が認証リクエストを処理している時に表示されるテキストを入力します。このメッセージは、ユーザがボタンをクリックしてネットワークに接続した後に表示されます。
No Accept Message	ユーザが「Acceptance Use Policy」を承諾しなかった場合に表示するテキストを入力します。このメッセージは、ユーザがボタンをクリックしてネットワークに接続した後に表示されます。
Welcome Page	
Branding Image	「Welcome」画面の現在の背景画像の名前を表示します。本設定の変更は「CP WEB Customization Global Parameters」画面で行うことができます。
Branding Title	「Welcome」画面の現在のブランド画像名を表示します。本設定の変更は「CP WEB Customization Global Parameters」画面で行うことができます。
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テキストを入力します。
Text	CP ユーザが接続したネットワークの詳細を表示するためのオプションテキストを入力します。このメッセージは「Welcome Title」の下に表示されます。
Logout Page	
注意 この画面の項目は「User Logout」モードが有効の場合にのみ適用されますが、項目の変更は機能の有効、無効に関係なく可能です。	
Browser Title	「Logout」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。画面を識別するテキストです。
Instructional Text	ユーザに認証されたこと確認し、ログアウトの方法を指示することを表示する詳細なテキストを入力します。
Button Label	ユーザがクリックしてログアウトを行うボタンに表示するテキストを入力します。
Confirmation Text	ユーザにログアウトの続行を確認するために表示する詳細なテキストを入力します。
Logout Success 画面	
注意 この画面の項目は「User Logout」モードが有効の場合にのみ適用されますが、項目の変更は機能の有効、無効に関係なく可能です。	
Background Image	「Logout Success」画面の現在の背景画像の名前を表示します。本設定の変更は「CP WEB Customization Global Parameters」画面にて行うことができます。
Branding Image	「Logout Success」画面の現在のブランド画像の名前を表示します。本設定の変更は「CP WEB Customization Global Parameters」画面にて行うことができます。
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。
Title	画面タイトルとして使用するテキストを入力します。画面を識別するテキストです。
Content	ユーザにログアウトしたことを確認するために表示するテキストを入力します。

ローカルユーザの設定

ゲストユーザと認証ユーザに対応するポータルを設定します。ゲストユーザにはユーザ名およびパスワードの割り当てはありません。認証ユーザには、はじめにローカルデータベースまたは RADIUS サーバに認証されるべき有効なユーザ名とパスワードがあります。スイッチが一度ユーザの証明書を確認すると、認証されたユーザはネットワークへのアクセス権を取得します。

ローカルデータベースに認証ユーザを追加することができ、データベースには最大 1024 個のユーザエントリを持つことができます。また、「Local User Summary」でローカルデータベースからユーザを削除することもできます。

LAN > Security > Captive Portal > 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。既に設定済みのユーザは「Local User Summary」タブにリスト表示されます。

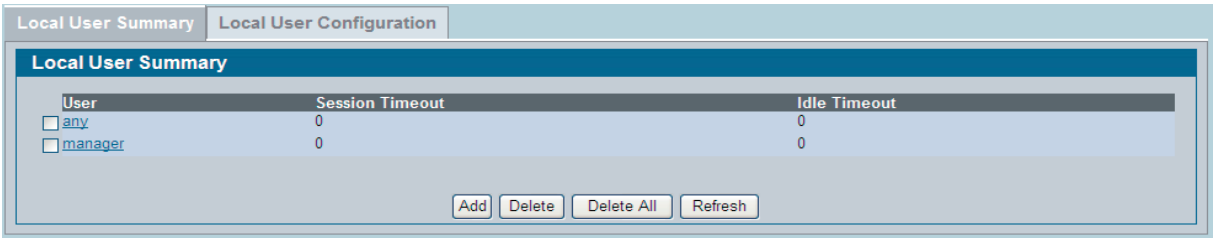


図 8-9　Local User Summary 画面

本画面には次の項目があります。

項目	説明
User	ユーザ名を指定します。
Session Timeout	ユーザがネットワークに接続されたままで残っていることを許容される時間（秒）を表示します。「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。0 は、ユーザが「Session Timeout」制限を持たないことを意味します。
Idle Timeout	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）を示します。0 は、ユーザが自動的にログアウトされないことを意味します。

画面にリストされている指定ユーザの設定画面にアクセスするためには、ユーザ名をクリックします。ローカルユーザテーブルの画面下部のボタンを使用して次のようなタスクを行います。

- Add - 新規ユーザをローカルユーザテーブルに登録するためには、「Add」ボタンをクリックします。
- Delete - 削除するユーザの横にあ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。複数のチェックボックスを選択し、一度に 1 人以上のユーザを削除します。
- Delete All -「Delete All」ボタンをクリックして、ローカルデータベースからすべての設定ユーザを削除します。
- Refresh -「Refresh」ボタンをクリックすると、最新の情報に更新します。

ローカルユーザの追加

「Local User Summary」画面の「Add」ボタンをクリックすると、画面が更新され、ローカルユーザデータベースに新規ユーザを追加することができます。新規ユーザに追加のパラメータを設定するためには、「Local User Summary」画面に戻り、その新規ユーザの名前をクリックします。ローカルユーザデータベースがサポートする最大ユーザ数は、「captive portal Global Status」画面に表示されます。

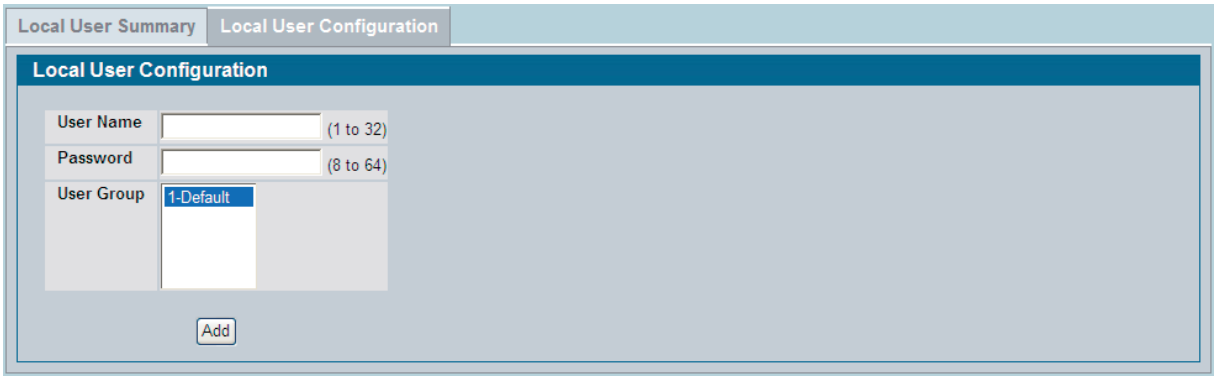


図 8-10　Local User Configuration - 新規ユーザの登録 画面

以下の表ではローカル CP データベースに新規ユーザを追加するのに使用する項目の詳細を示します。

項目	説明
User Name	ユーザ名前を入力します。
Password	ユーザのパスワードを入力します。パスワードは 8 ー 64 文字です。
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。新しいユーザは、初期値では 1-Default のユーザグループに割り当てられます。

各項目入力後、「Add」ボタンをクリックするとユーザを追加して「Local User Summary」画面に戻ります。

ローカルデータベース内のユーザ設定

ローカルデータベース内の定義済み CP ユーザに追加の設定を行います。

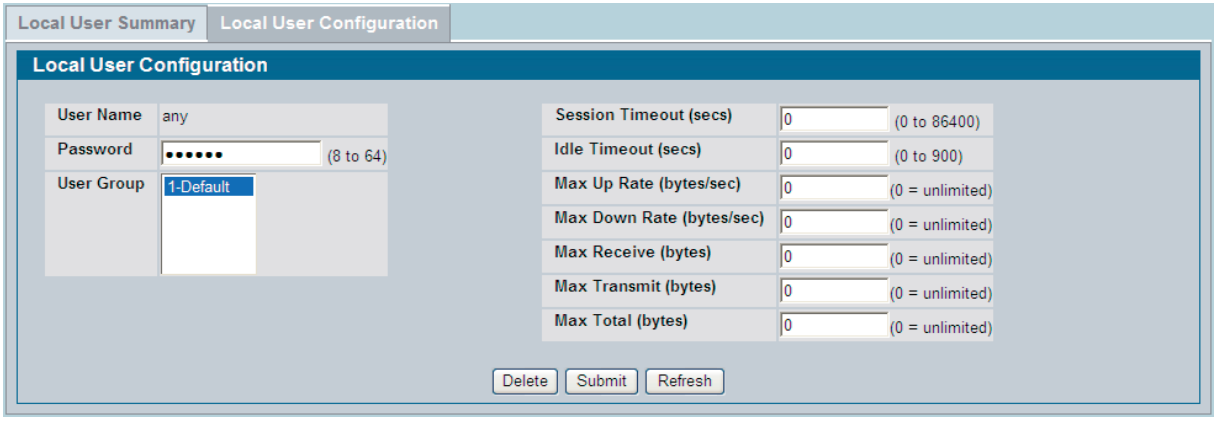


図 8-11　Local User Configuration 画面

以下の表ではローカルデータベースに CP ユーザを設定するために使用する項目について説明します。

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。パスワードは 8 - 64 文字です。
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。新しいユーザは、初期値では 1-Default のユーザグループに割り当てられます。
Session Timeout (secs)	ユーザがネットワークに接続されたままでいることを許可される時間（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。0 は、ユーザが「Session Timeout」制限を持たないことを意味します。
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。0 は、ユーザが「Session Timeout」制限を持たないことを意味します。
Max Up Rate (bytes/sec)	ユーザがキャプティブポータルを使用した時に送信できるトラフィックの最大速度（bps）を入力します。この設定では、ユーザがネットワークに送信できるデータの帯域を制限します。

項目	説明
Max Down Rate (bytes/sec)	ユーザがキャプティブポータルを使用した時に受信できるトラフィックの最大速度（bps）を入力します。この設定では、ユーザがネットワークから受信できるデータの帯域を制限します。
Max Receive (bytes)	ユーザがキャプティブポータルを使用した時に許可される受信量（バイト）を入力します。この制限値に達すると、ユーザは接続を切断されます。
Max Transmit (bytes)	ユーザがキャプティブポータルを使用した時に許可される送信量（バイト）を入力します。この制限値に達すると、ユーザは接続を切断されます。
Max Transmit (bytes)	ユーザが許可される最大通信量（送受信の合計バイト）を入力します。この制限値に達すると、ユーザは接続を切断されます。

リモート RADIUS サーバにユーザを設定する

リモート RADIUS サーバクライアント認証を使用することができます。すべてのユーザを RADIUS サーバに追加する必要があります。統合スイッチにおけるローカルデータベースは、リモートの RADIUS データベースとはいかなる情報も共有しません。

以下の表は、認証済みのキャプティブポータルクライアントを設定するために使用する RADIUS 属性を示しています。本テーブルは RADIUS 属性とベンダ特有の属性（VSA）の両方を示しています。VSA は、「Attribute」欄に表示され、「,」カンマで区切られています。（例 vendor id、attribute id）

属性	番号	説明	範囲	使用方法	初期値
User-Name	1	認証されるユーザ名	1-32 文字の半角英数字	必要な場合。	なし
User-Password	2	ユーザパスワード	8-64 文字	必要な場合。	なし
Session-Timeout	27	セッションタイムアウト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
Idle-Timeout	28	アイドルタイムアウト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
WISPr-Bandwidth-Max-Up	14122, 7	クライアントの最大送信速度（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	ー
WISPr-BandwidthMax-Down	14122, 8	クライアントの最大受信速度（b/s）。クライアントがネットワークからデータを受信できる帯域を制限します。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	ー
D-Link-Max-InputOctets	171, 124	ユーザが許可される送信の最大オクテット数。この制限値に達すると、ユーザは接続を切断されます。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	ー
D-Link-Max-OutputOctets	171, 125	ユーザが許可される受信の最大オクテット数。この制限値に達すると、ユーザは接続を切断されます。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	ー
D-Link-Max-TotalOctets	171, 126	ユーザが許可される送受信トータルの最大オクテット数。この制限値に達すると、ユーザは接続を切断されます。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	ー

インタフェースへのキャプティブポータルの割り当て

特定の物理的インタフェースや無線ネットワーク（SSID）に設定したキャプティブポータルを関連付けることができます。CP 機能は、指定する有線または無線インタフェースで動作します。CP は複数のインタフェースと関連付けできますが、インタフェースは一度に 1 つの CP とだけしか関連付けできません。

注意 キャプティブポータル設定に物理インタフェースを関連させる場合、以下のような制限があります。

- キャプティブポータルと STP を同じ物理インタフェースで有効にすることはできません。
- キャプティブポータルと 802.1X を同じ物理インタフェースで有効にすることはできません。
- ポートセキュリティとキャプティブポータルを同じ物理インタフェースで有効にすることはできません。
- 物理インタフェースが LAG メンバである場合、キャプティブポータルはそのインタフェースでは無効になります。

インタフェースに CP を割り当てるためには、**WLAN タブ > Security > Captive Portal > Interface Association** の順にメニューをクリックします。

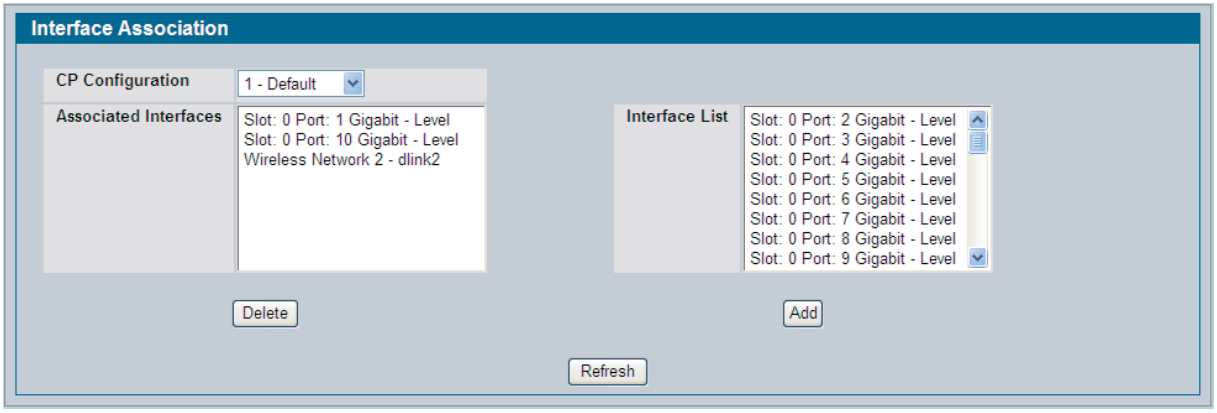


図 8-12　Interface Association 画面

以下の項目が表示されます。

項目	説明
CP Configuration	スイッチに設定されたキャプティブポータルを番号と名前ごとに表示します。
Associated Interfaces	選択されたキャプティブポータルに関連する無線インタフェースを示します。無線インタフェースは、無線ネットワーク番号と SSID により識別されます。物理（有線）インタフェースは、スロット番号、ポート番号およびインタフェースタイプを含むポート種別により識別されます。
Interface List	現在 CP に関連付けされていないスイッチで利用可能な無線インタフェースを示します。無線インタフェースは、無線ネットワーク番号と SSID により識別されます。物理（有線）インタフェースは、スロット番号、ポート番号およびインタフェースタイプを含むポート種別により識別されます。

以下の手順で 1 つ以上のインタフェースをキャプティブポータルに関連付けします。

1. 「CP Configuration」リストから希望のキャプティブポータルを選択します。
2. 「Interface List」から 1 つ以上のインタフェースを選択します。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、複数のインタフェースをクリックします。
3. 「Add」ボタンをクリックします。

注意 キャプティブポータルにインタフェースを関連付けると、そのインタフェースは「Interface List」から削除されます。各インタフェースは一度に 1 つの CP にだけ関連付けされます。

以下の手順を使用して、キャプティブポータルのために「Associated Interfaces」リストからインタフェースを削除します。

1. 「CP Configuration」リストから希望のキャプティブポータルを選択します。
2. 「Associated Interfaces」欄で削除するインタフェースを選択します。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、複数のインタフェースをクリックします。
3. 「Delete」ボタンをクリックします。

インタフェースは、「Associated Interface」リストから削除されて、「Interface List」に表示されます。

キャプティブポータルのステータス

CP 機能に関するさまざまな情報があります。CP の動作およびインタフェースに関する情報を参照します。

Global Status タブ

CP のグローバル情報を参照します。

LAN タブ > Security > Captive Portal > CP Status の順にメニューをクリックし、さらに「Global Status」タブをクリックして以下の画面を表示します。

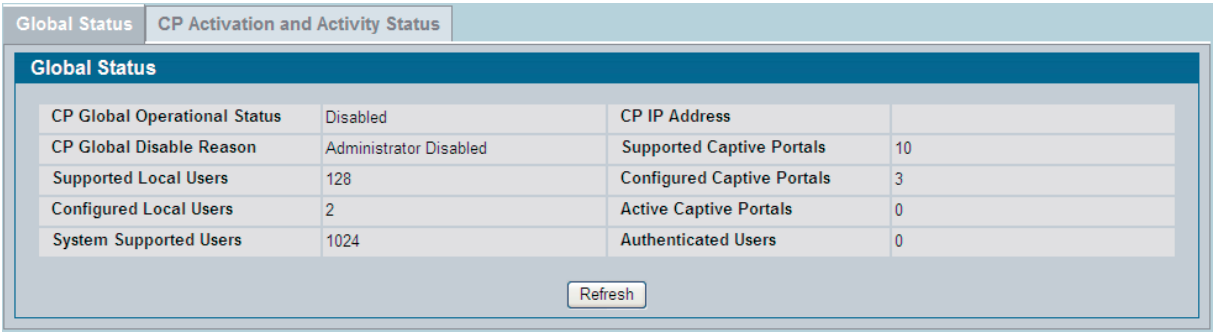


図 8-13　Global Status 画面

以下の項目が表示されます。

項目	説明
CP Global Operational Status	CP 機能が有効かどうかを表示します。
CP Global Disable Reason	CP が無効の場合、無効にされた理由を表示します。 • None - 以下のいずれでもない状態です。 • Administratively Disabled - 管理上無効です。 • No IPv4 Address - IPv4 アドレスではありません。 • Routing Enabled、But no IPv4routing interface - ルーティングが有効ですが、IPv4 ルーティングインタフェースではありません。
Supported Local Users	ローカルユーザデータベースがサポートしているエントリ数を表示します。
Configured Local Users	システム内に設定されているユーザ数を表示します。
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。
CP IP Address	キャプティブポータルの IP アドレスを表示します。
Supported Captive Portals	システムのサポートしているキャプティブポータルの数を表示します。
Configured Captive Portals	スイッチに設定されたキャプティブポータル数を表示します。
Active Captive Portals	操作上有効であるキャプティブポータル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キャプティブポータルインスタンスに対して認証されているユーザ数を表示します。

CP Activation and Activity Status タブ

各 CP の CP アクティベーションと動作のステータスを参照します。

LAN タブ > Security > Captive Portal > CP Status の順にメニューをクリックし、さらに「CP Activation and Activity Status」タブをクリックし、以下の画面を表示します。

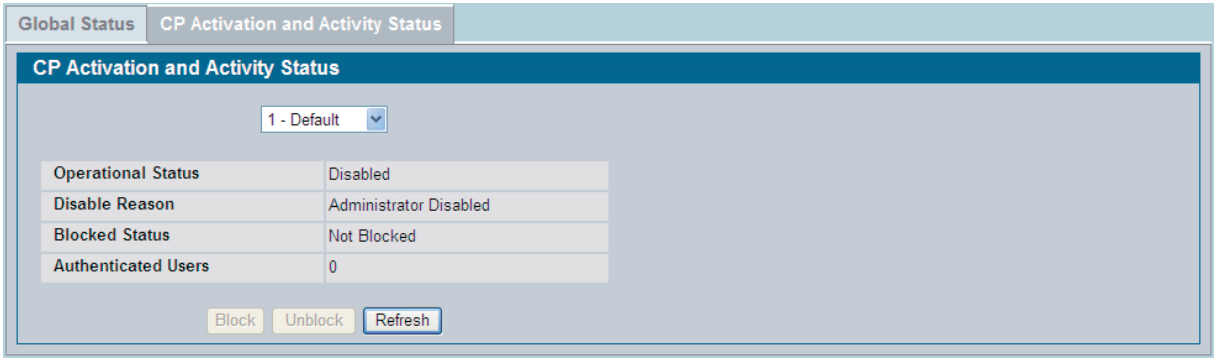


図 8-14　CP Activation and Activity Status 画面

本画面には、スイッチに設定されているすべてのキャプティブポータルを含むメニューがあります。キャプティブポータルを選択し、そのポータルのためのアクティベーションと動作のステータスを表示します。

以下の表は各ポータルに対する情報について説明します。

項目	説明
Operational Status	キャプティブポータルの有効または無効を表示します。
Disable Reason	キャプティブポータルが無効の場合、この欄はその理由を表示します。ポータルインスタンスは以下の理由で無効になった可能性があります。 • None - CP が有効です。 • Administratively Disabled - 管理上無効です。 • RADIUS Authentication mode enabled, but RADIUS server is not defined. - RADIUS 認証モードが有効にされましたが、RADIUS サーバは定義されていません。 • Not associated with any interfaces. - どのインタフェースにも関連付けされていません。 • The associated interfaces do not exist or do not support the CP capability. - 割り当てられたインタフェースが存在しないか、または CP 機能をサポートしていません。
Blocked Status	キャプティブポータルへの認証の試みが現在防御されているか否かを表示します。 「Block」と「Unblock」ボタンを使用して、防御ステータスを制御します。CP が防御されると、ユーザは CP を経由したネットワークへのアクセスを行うことができません。本機能を使用して、DoS 攻撃などの予期しないイベントの間、一時的にネットワークを保護します。 注意 「Blocked Status」は、運用上のステータスであり、設定されたステータスではありません。これは再起動後には保持されません。初期値は、「Unblock」です。 CP の操作上のステータスが「Enabled」である時にだけ、「Block」と「Unblock」は使用できます。
Authenticated Users	このキャプティブポータルへの認証に成功し、現在ポータルを使用しているユーザ数を表示します。

本画面では、以下のボタンが利用できます。

項目	説明
Block	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。
Unblock	選択したキャプティブポータルの「Blocked Status」が「Blocked」の場合、本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。
Refresh	画面を最新の情報に更新します。

インタフェースステータス

「Interface Status」画面からリンクする画面では、キャプティブポータルインタフェース情報および機能を設定できます。

インタフェースアクティベーションステータスの参照

「Interface Activation Status」タブではキャプティブポータルインスタンスに割り当てられたすべてのインタフェースの情報を表示します。プルダウンメニューを使用して、情報を参照するポータルまたはインタフェースを選択します。

LAN タブ > Security > Captive Portal > Interface Status の順にメニューをクリックし、「Interface Activation Status」タブを参照します。

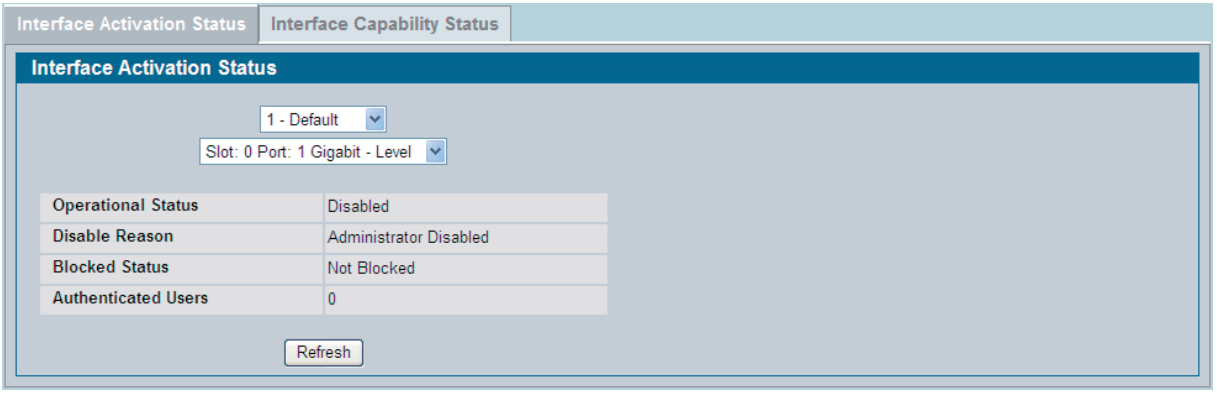


図 8-15　Interface Activation Status 画面

画面には以下の項目が表示されます。

項目	説明
Operational Status	ポータルが指定インタフェースでアクティブであるか否かを表示します。
Disable Reason	選択した CP が本インタフェースで無効の場合、以下の原因から 1 つが表示されます。 • Interface Not Attached - インタフェースは割り当てされていません。 • Disabled by Administrator - 管理者が無効にしました。
Blocked Status	キャプティブポータルが一時的に認証に対してブロックされるかどうかを表示します。
Authenticated Users	本インタフェースにおけるキャプティブポータルインスタンスを使用して認証されているユーザ数を表示します。

インタフェース情報の参照

「Interface Capability Status」タブには、割り当てられた CP を持つインタフェースに関する情報、さまざまな機能に関する情報があります。本画面は、特に本インタフェースに接続するクライアントに対して CP 経由で提供するサービスを表示します。サービスのリストはインタフェースの能力によって決定されます。

WLAN タブ > Security > Captive Portal > Interface Status の順にメニューをクリックし、「Interface Capability Status」タブを参照します。

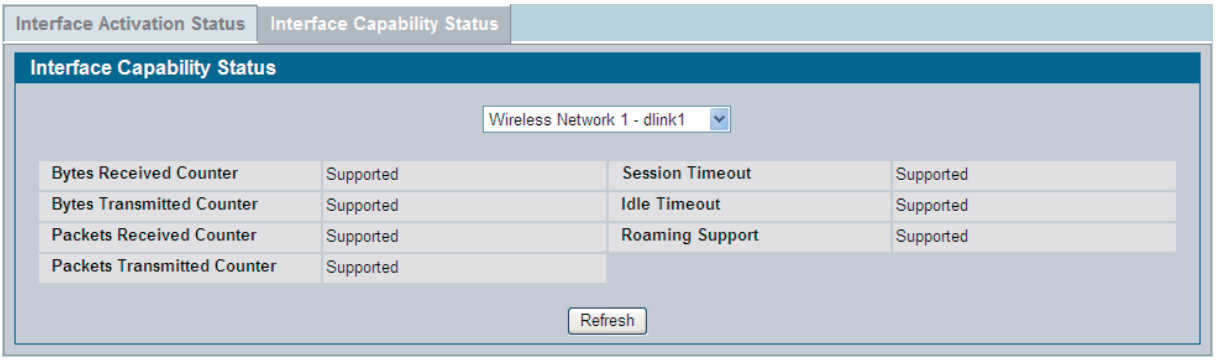


図 8-16　Interface Capability Status 画面

プルダウンメニューにはスイッチで利用可能なすべての物理的インタフェースおよび無線インタフェースがあります。無線インタフェースは、無線ネットワーク番号と SSID により識別されます。物理（有線）インタフェースは、スロット番号、ポート番号およびインタフェースタイプを含むポート種別により識別されます。ポート種別にはスロット番号、ポート番号およびインタフェースタイプが含まれます。プルダウンメニューを使用して、表示する情報を持つインタフェースを選択します。

画面には以下の項目があります。

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信または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。

クライアント接続ステータス

「Client Connection Status」画面から、CP を使用してスイッチに接続しているクライアントの情報を提供するいくつかの画面にアクセスできます。

「Client Summary」画面を使用して、キャプティブポータル経由で接続するすべての認証無線クライアントに関するサマリ情報を参照します。本画面を使用すると、キャプティブポータルは、1 つ以上の認証クライアントを手動で強制的に切断します。無線クライアントのリストはクライアント MAC アドレスによってソートされます。スイッチがクラスタリングをサポートしていてクラスタ内にピアスイッチがある場合、画面に表示されるクライアントの何人かは他のスイッチを経由してネットワークに接続している可能性があります。クライアントに関する詳細情報およびスイッチがクライアントの認証処理に関する情報を参照するためには、そのクライアントの MAC アドレスをクリックしてください。

Client Summary タブ（無線クライアントに関する情報）

キャプティブポータルを経由して統合スイッチに接続する無線クライアントに関する情報を参照します。

LAN タブ > Security > Captive Portal > Client Connection Status の順にメニューをクリックし、さらに「CP Summary」タブをクリックして以下の画面を表示します。

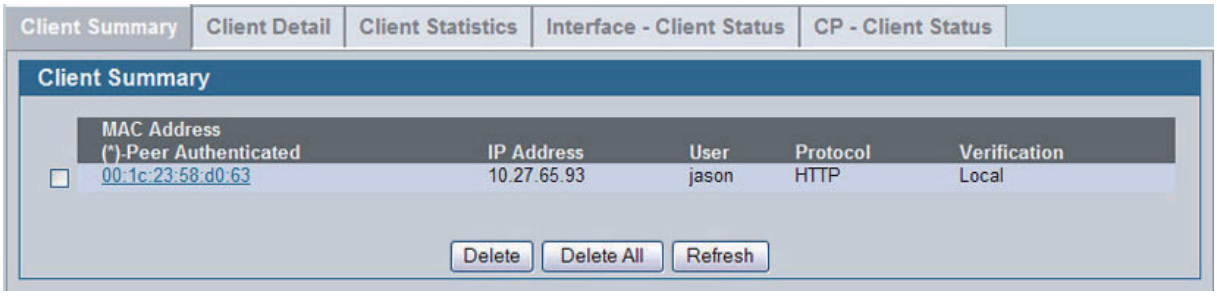


図 8-17　Client Summary 画面

「CP Summary」ページの各項目を説明します。

項目	説明
MAC Address	該当する場合、無線クライアントの MAC アドレスを指定します。MAC アドレスにアスタリスク（*）のついている場合、認証済みクライアントはピアスイッチで認証されています。つまり、クラスタコントローラは認証を行っていないということです。
Client IP Address	該当する場合、無線クライアントの 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 MAC アドレスをクリックすると、追加のステータス情報を表示できます。

認証クライアントの接続の解除

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 アドレスの左側にあ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り離すためには、「Delete All」ボタンをクリックします。

Client Detail タブ（クライアントの詳細情報）

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。

LAN タブ > Security > Captive Portal > Client Connection Status の順にメニューをクリックし、さらに「Client Detail」タブをクリックして以下の画面を表示します。

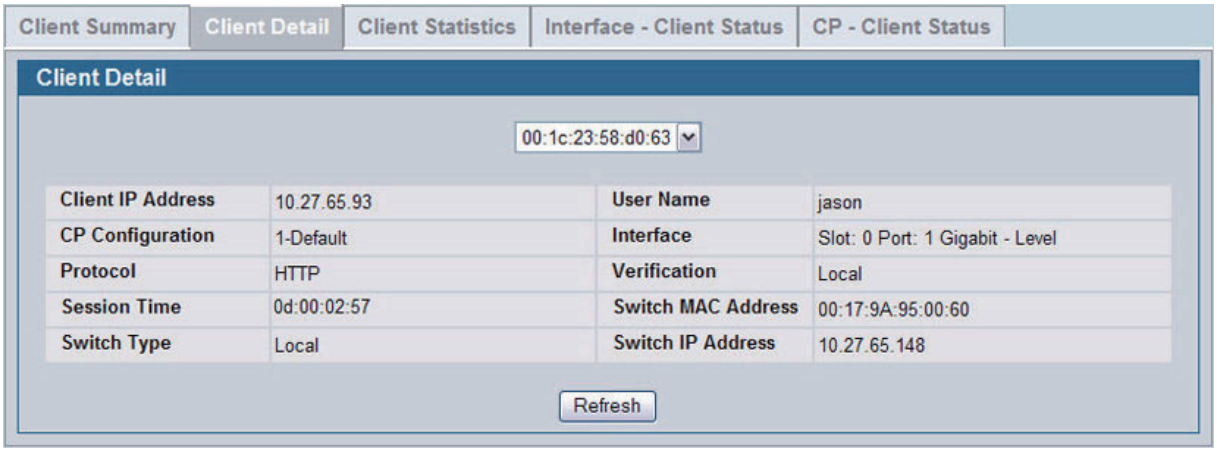


図 8-18　Client Detail 画面

プルダウンメニューでは MAC アドレスに関連付けされているクライアントを表示します。クライアントに関するステータス情報を参照するためには、リストから選択します。

画面には以下の項目があります。

項目	説明
Client IP Address	無線クライアントの IP アドレスを表示します。
CP Configuration	無線クライアントが使用している CP 名を表示します。
Protocol	現在の接続プロトコル（HTTP または HTTPS）を表示します。
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 Type	このクライアントの認証を扱うスイッチがローカルスイッチ、あるいはクラスタ内のピアスイッチかどうかを表示します。
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。
Interface	無線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。
Verification	現在のアカウントタイプ（Guest、Local または RADIUS）を表示します。
Switch MAC Address	このクライアントの認証を扱うスイッチの 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ている場合、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 IP Address	このクライアントの認証を扱うスイッチの 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ている場合、クラスタ内のピアスイッチの IP アドレスを表示します。

Client Statistic タブ（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。

LAN タブ > Security > Captive Portal > Client Connection Status の順にメニューをクリックし、さらに「Client Statistics」タブをクリックして以下の画面を表示します。

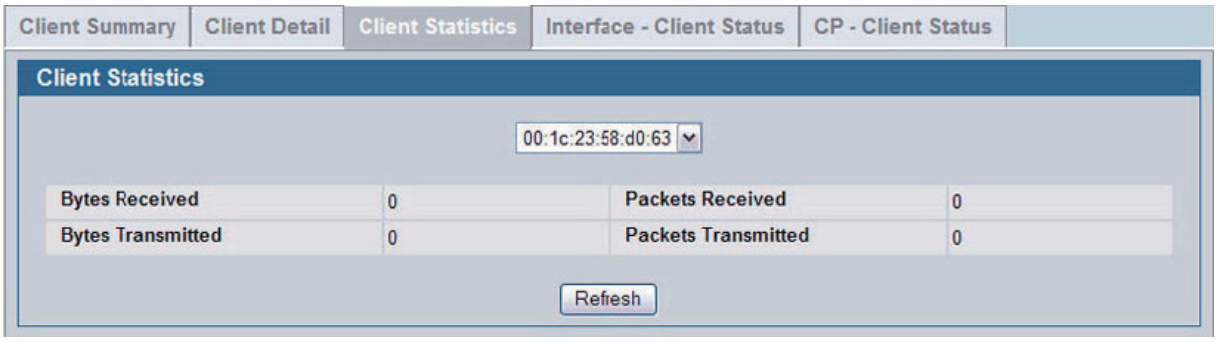


図 8-19　Client Statistics 画面

プルダウンメニューには MAC アドレスに関連付けされている各クライアントを表示します。クライアントに関する統計情報を参照するために、リストから選択します。

画面には以下の項目があります。

項目	説明
Bytes Transmitted	クライアントが送信した合計バイト数。
Bytes Received	クライアントが受信した合計バイト数。
Packets Transmitted	クライアントが送信した合計パケット数。
Packets Received	クライアントが受信した合計パケット数。

Interface - Client Status タブ（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。

LAN タブ > Security > Captive Portal > Client Connection Status の順にメニューをクリックし、さらに「Interface - Client Status」タブをクリックして以下の画面を表示します。

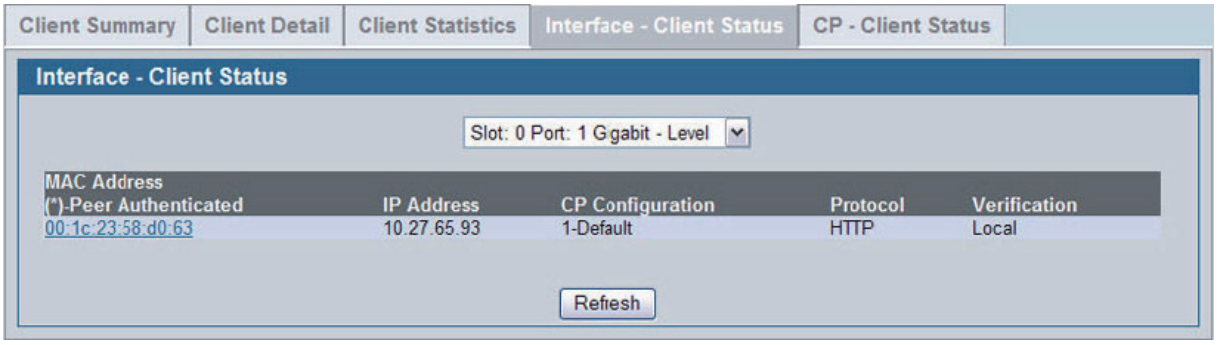


図 8-20　Interface - Client Status 画面

プルダウンメニューにはスイッチのインタフェースのリストが表示されます。このインタフェース上で CP に接続するクライアントに関するステータス情報を参照するためには、リストから選択します。

画面には以下の項目があります。

項目	説明
MAC Address	無線クライアントの MAC アドレスを示します。MAC アドレスにアスタリスク（*）のついている場合は、認証済みクライアントはピアスイッチで認証されています。つまり、クラスタコントローラは認証を行っていないということです。
IP Address	無線クライアントの IP アドレスを示します。
CP Configuration	クライアントがネットワークにアクセスするために使用したキャプティブポータルを示します。
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。

CP - Client Status タブ（Client CP Association Status 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。

LAN タブ > Security > Captive Portal > Client Connection Status の順にメニューをクリックし、さらに「CP - Client Status」タブをクリックして以下の画面を表示します。

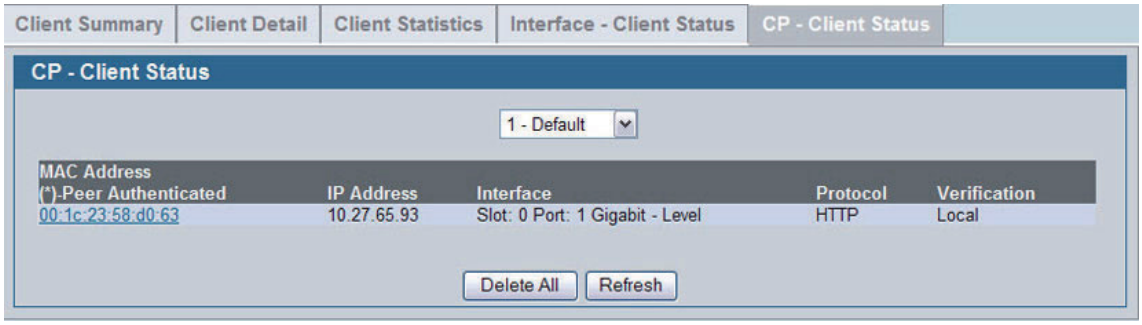


図 8-21　CP - Client Status 画面

プルダウンメニューはスイッチに設定されている各 CP を表示します。CP に接続するクライアントに関する情報を参照するためには、リストから CP を選択します。

画面には以下の項目があります。

項目	説明
MAC Address	無線クライアントの MAC アドレスを示します。MAC アドレスにアスタリスク（*）のついている場合は、認証済みクライアントはピアスイッチで認証されています。つまり、クラスタコントローラは認証を行っていないということです。
IP Address	無線クライアントの IP アドレスを示します。
Interface	クライアントがネットワークにアクセスするために使用したインタフェースを示します。
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。

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。

キャプティブポータルトラップの設定は「Captive Portal Trap Mode」が有効な場合のみ可能です。これは、**LAN タブ > Administration > SNMP Manager > Trap Flags** の順にクリックして設定を行います。すべての CP SNMP トラップは初期値では無効に設定されています。

各種のキャプティブポータル機能に SNMP トラップ設定を行うためには、**LAN タブ > Security > Captive Portal > 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 9-22　SNMP Trap Configuration 画面

以下の表で指定されるトラップは、特に指定されない限り、クラスタコントローラによってのみ作成されます。

ここでは、ステータスが有効された際に SNMP トラップを生成するイベントについて説明します。

項目	説明
Captive Portal Trap Mode	以下のキャプティブポータルのトラップモードから 1 つを選択します。 • Enabled - スイッチの SNMP エージェントは有効とされているキャプティブポータルの SNMP トラップを生成します。 • Disabled - スイッチの SNMP エージェントは、それらが個別に有効とされていてもキャプティブポータルの SNMP トラップは生成しません。 このモードを有効、または無効にするためには、キャピタルポータルメニューを使用して L**AN タブ > Administration > SNMP Manager > Trap Flags** の順にクリックします。
Client Authentication Failure Traps	有効にすると、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します。
Client Connection Traps	有効にすると、クライアントが認証され、キャプティブポータルに接続した場合、SNMP エージェントがトラップを送信します。
Client Database Full Traps	有効にすると、エントリがフル状態のクライアントデータベースに追加されなかった場合に SNMP エージェントがトラップを送信します。
Client Disconnection Traps	有効にすると、クライアントがキャプティブポータルから切断された場合、SNMP エージェントがトラップを送信します。

ポートアクセスコントロール

「port-based authentication mode」では、802.1X がグローバルおよびポート上で有効な場合、誰でもそのポートでの認証に成功するということは、すべてのユーザがそのポートを制限なしに使用できるということになります。このモードでは、1 つのポート上で認証されるのは常に 1 つのクライアントだけです。このモードでは、ポートは双方向に制御されます。これは、認証モードの初期値です。

802.1X ネットワークには、3 つのコンポーネントがあります。

- Authenticators - システムへのアクセスを許可する前に認証されるポートを指定します。
- Supplicants - システムサービスへのアクセスを要求する認証済みのポートに接続するホストを指定します。
- Authentication Server - 例えば RADIUS サーバなど、オーセンティケータとして認証を行う外部サーバを指定して、ユーザがシステムサービスにアクセスする権限があるかどうかを示します。

ポートアクセスコントロールには、システムに 802.1X 機能を参照、設定することができる以下の機能があります。

グローバルポートアクセスコントロール設定

システムのポートアクセスコントロールを有効または無効にします。

LAN タブ > Security > Port Access Control > 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。

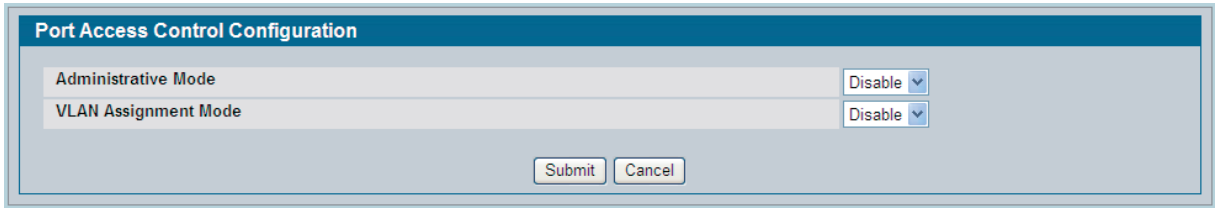


図 8-23　Port Access Control 画面

以下の項目を表示します。

項目	説明
Administrative Mode	スイッチの 802.1X モードを「Enable」（有効）または「Disable」（無効）にします。初期値は「Disable」です。本機能は、スイッチのポートベース認証を許可します。
VLAN Assignment Mode	有効にした場合、サプリカントが認証サーバに認証されると、サプリカントが接続するポートは RADIUS サーバが指定する特定の VLAN に配置されます。本モードは、スイッチがポートを RADIUS サーバが割り当てた VLAN に配置できるかどうかをコントロールします。ポートの VLAN 割り当ては、ポートで最初に認証されたサプリカントによって決定されます。

モードの変更後、「Submit」ボタンをクリックして新しい設定をシステムに適用します。

ポート設定

1 つ以上のポートにポートアクセスコントロールを設定します。

LAN > Security > Port Access Control > Port 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。

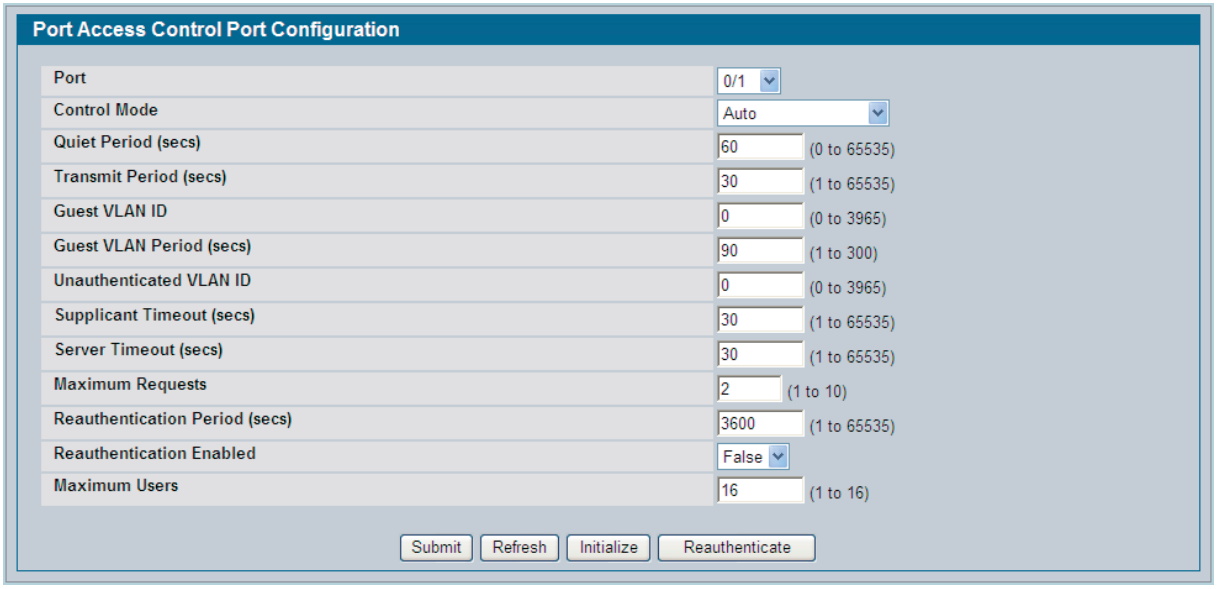


図 8-24　Port Access Control Port Configuration 画面

以下の項目を表示します。

項目	説明
Port	設定するポートを選択します。
Control Mode	ポートの認証状態を定義します。コントロールモードは、ポートのリンクステータスがリンクアップの場合にのみ、設定できます。以下の値が可能です。 • Auto - インタフェースのモードを自動的に検出します。 • Force Authorized - インタフェースを認証せずに認証ステータスに配置します。インタフェースは、クライアントのポートベース認証を行わずに、通常のトラフィックの送受信を行います。 • Force Unauthorized - 選択したインタフェースを未認証ステータスにすることによって、そのインタフェースのシステムアクセスを拒否します。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。
Quiet Period (secs)	クライアントの認証に失敗した後、クライアントとの通信を拒否する期間を設定します。値は 0-65535（秒）です。初期値は 60（秒）です。
Transmit Period (secs)	選択ポートの送信期間を設定します。これは、指定したポートの認証元デバイスがいつ EAPOL の EAP 要求 / 識別フレームをサプリカントに送信するかを決定するのに使用するタイマの時間（秒）です。範囲は 1-65535（秒）です。初期値は 30（秒）です。
Guest VLAN ID	インタフェースのゲスト VLAN を定義します。範囲は 0-3965 です。初期値は 0 です。0 を入力すると、インタフェースのゲスト VLAN ID をクリアします。
Guest VLAN Period (secs)	選択ポートのゲスト VLAN 期間を定義します。これは、ゲスト VLAN 認証に使用するタイマの時間（秒）です。範囲は 1-300（秒）です。初期値は 90（秒）です。
Unauthenticated VLAN ID	選択ポートの非認証 VLAN ID を定義します。範囲は 0-3965 です。初期値は 0 です。0 を入力すると、インタフェースの非認証 VLAN ID をクリアします。
Supplicant Timeout (secs)	EAP 要求をユーザに再送信するまでの時間を定義します。範囲は 1-65535（秒）です。初期値は 30（秒）です。
Server Timeout (secs)	スイッチが認証サーバに要求を再送信するまでの時間を定義します。値は秒単位です。範囲は 1-65535（秒）で、初期値は 30（秒）です。
Maximum Requests	スイッチが返答を受信しない場合、認証を再開するまでに送信できる EAP 要求の最大再送回数を定義します。範囲は 1-10 です。初期値は 2（回）です。
Reauthentication Period (secs)	選択したポートを再認証するタイムスパン（秒）を定義します。範囲は 1 - 65535（秒）で、初期値は 3600（秒）です。
Reauthentication Enabled	有効にすると、選択ポートの再認証を定期的に行います。初期値は「False」です。
Maximum Users	「MAC-based dot1x authentication」モードの時、ポート上で認証できるクライアントの最大数を定義します。範囲は 1-16 です。初期値は 16 です。

「Submit」をクリックすると、更新がスイッチに送信され、変更が有効になりますが、「save」を行わない限り、電源をオフにするとこれらの変更内容は失われます。「Refresh」ボタンをクリックすると、情報を更新します。

選択ポートの初期化

「Initialize」をクリックすると、選択ポートの設定の初期化を開始します。このボタンはコントロールモードが「auto」の場合にのみ選択可能です。ボタンがグレー表示の時は選択できません。ボタンをクリックすると、直ちに実行されます。「Submit」ボタンを押す必要はありません。

選択ポートの再認証

「Reauthenticate」をクリックすると、選択ポートの再認証を開始します。このボタンはコントロールモードが「auto」の場合にのみ選択可能です。ボタンがグレー表示の時は選択できません。ボタンをクリックすると、直ちに実行されます。「Submit」ボタンを押す必要はありません。

PAE Capability Configuration（PAE 対応設定）

ポートを「authenticator」または「supplicant」として設定します。

LAN > Security > Port Access Control > PAE Capability 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。

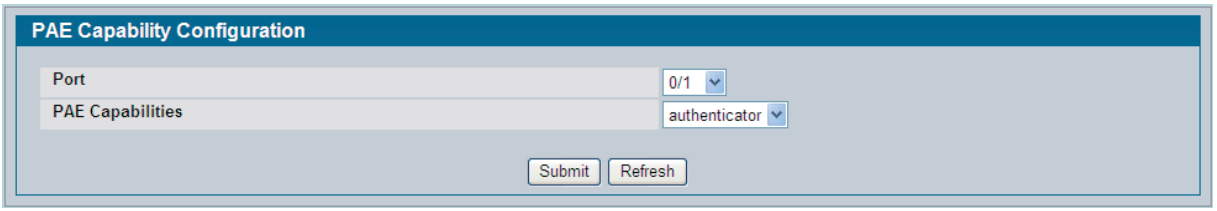


図 8-25　PAE Capability Configuration 画面

以下の項目を表示します。

項目	説明
Port	設定するスロット / ポートを選択します。
PAE Capabilities	リストから「authenticator」または「supplicant」を選択します。

「Submit」ボタンをクリックして、PAE 対応を設定します。「Save All Applied Changes」をクリックしないと、これらの変更は電源をオフにすると失われます。

ポートを「supplicant」として設定した場合は、「Supplicant Port Configuration」画面を使用してポートの動作パラメータを追加設定します。

Supplicant Port Configuration（ポートのサプリカント設定）

ポートをサプリカントとして設定した後、ポートの動作プロパティを設定します。

LAN > Security > Port Access Control > Supplicant Port 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。

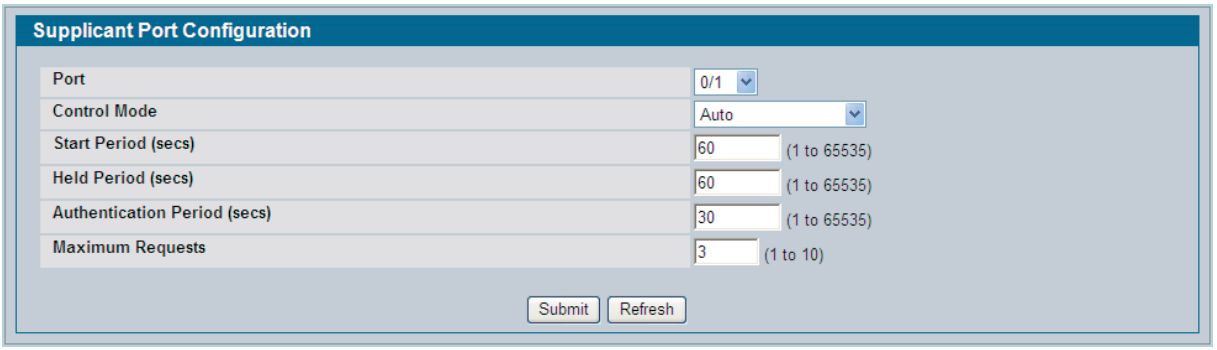


図 8-26　Supplicant Port Configuration 画面

以下の項目を表示します。

項目	説明
Port	設定するポートを選択します。
Control Mode	ポートの認証ステートを選択します。コントロールモードは、ポートのリンクステータスがリンクアップの場合にのみ設定できます。 • Auto - サプリカントと認証サーバとの 802.1X 変換により、ポートモード（「Authorized」、「Unauthorized」など）を決定します。 • Force Authorized - インタフェースを認証せずに認証ステータスに配置します。インタフェースは、クライアントのポートベース認証を行わずに、通常のトラフィックの送受信を行います。 • Force Unauthorized - 選択したインタフェースを未認証ステータスにすることによって、そのインタフェースのシステムアクセスを拒否します。スイッチはこのインタフェースではサプリカントに認証を行いません。
Start Period (secs)	サプリカントが認証元の EAP 識別要求メッセージを受信する待ち時間（秒）を入力します。
Held Period (secs)	先の認証が失敗した後、サプリカントが次の認証処理を開始するまでの待ち時間（秒）を入力します。
Authentication Period (secs)	サプリカントが認証元から EAP チャレンジ要求を受信する待ち時間（秒）を入力します。
Maximum Requests	サプリカントが認証元が EAPOL スタートメッセージの最大数を入力します。

「Submit」をクリックしてサプリカントを設定します。「Save All Applied Changes」をクリックしないと、これらの変更は電源をオフにすると失われます。「Refresh」ボタンをクリックし、スイッチの情報を最新に更新します。

User Login Configuration（ユーザログイン設定）

システムで設定済みの認証リストにシステムユーザの関連付けを行います。

認証リストについての詳細情報は、「認証リスト設定」（36 ページ）を参照してください。

LAN タブ > Security > Port Access Control > User Login 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。

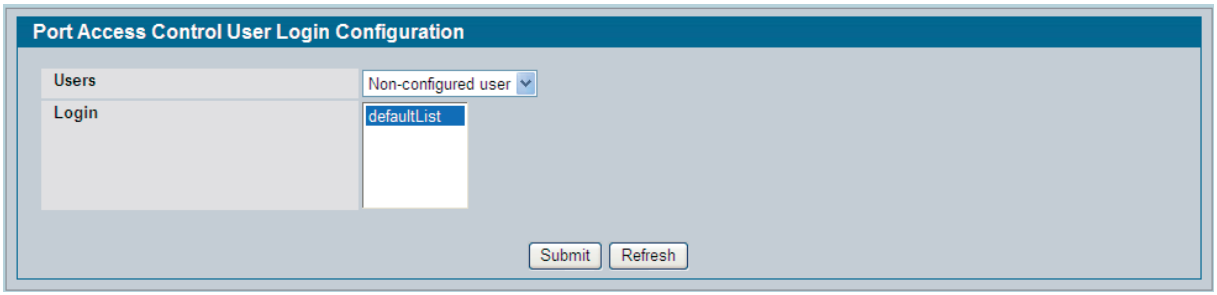


図 8-27　Port Access Control User Login Configuration 画面

以下の項目を表示します。

項目	説明
Users	システムに設定されたユーザ名が表示されます。802.1X ポートセキュリティのためのログインリストと関連付けるユーザ名を選択します。ユーザを選択して画面を更新すると、ユーザが関連付けられているリストのログインフィールドがハイライトされます。「Non-configured user」オプションを選択すると、システムで未定義のユーザに認証リストを割り当てます。
Login	システムに設定された認証リストを表示します。初期設定は、「defaultList」1 つです。1 つのユーザを 1 つの認証リストにのみ割り当てることができます。追加の認証リストを設定するためには、「Use the Authentication List」画面を参照してログインリストを設定してください。ログインリストは、リストに関連付けられたユーザのスイッチやポートへのアクセスを有効にする 1 つまたは複数の認証方式を指定します。

ユーザを認証リストに関連付けるためには、「Users」からユーザ名を選択します。「Login」から希望の認証リストを選択し、「Submit」ボタンをクリックして変更を適用します。

「Refresh」ボタンをクリックすると、最新の情報に更新します。

ポートアクセス権限

システムに設定されたユーザのポートアクセス権を許可、または拒否します。

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

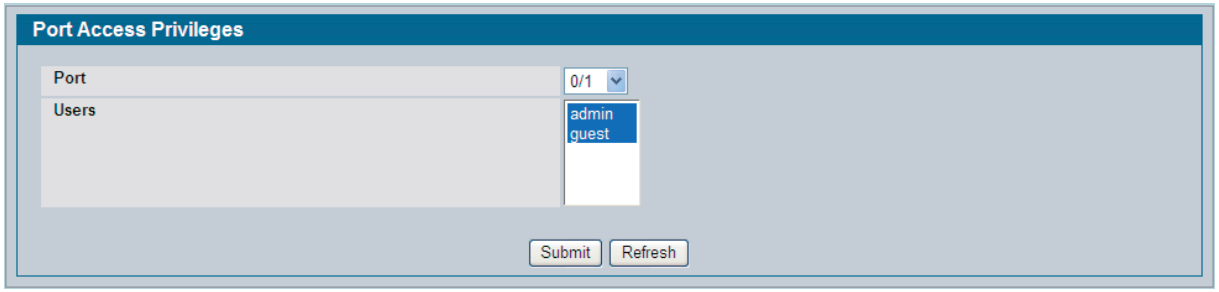


図 8-28　Port Access Privileges 画面

以下の項目を表示します。

項目	説明
Port	アクセスを許可、または拒否するポートを選択します。すべてのポートで、ユーザのポートアクセス権を許可、または拒否するためには、「All」を選択します。
Users	システムに設定されたユーザを表示します。ハイライトされているユーザは選択ポートに対してアクセス権を持っています。初期値では、すべてのユーザがすべてのポートに対しアクセス権を持っています。あるポートへのアクセスを拒否するためには、「Shift」キーを押したままアクセスを許可するユーザだけをクリックします。ポートアクセスを拒否するユーザ名が選択されていないことを確認し、「Submit」ボタンをクリックします。

RADIUS 設定

RADIUS（Remote Authentication Dial-in User Service）サーバは、ネットワークに更なるセキュリティを提供します。RADIUS サーバには、ユーザごとの認証情報を含むユーザデータベースがあります。

RADIUS サーバは、以下のように集中的な認証方式を提供します。

- Telnet アクセス
- Web アクセス
- コンソールアクセス
- ポートアクセスコントロール（802.1X）

RADIUS には、以下のような機能があり、システムの RADIUS の参照、設定を行います。

- RADIUS 設定
- RADIUS 認証サーバ設定
- 統計情報のクリア

RADIUS 設定

システムに設定されている RADIUS サーバの各設定の参照、設定を行います。

LAN タブ > Security > RADIUS > RADIUS 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。

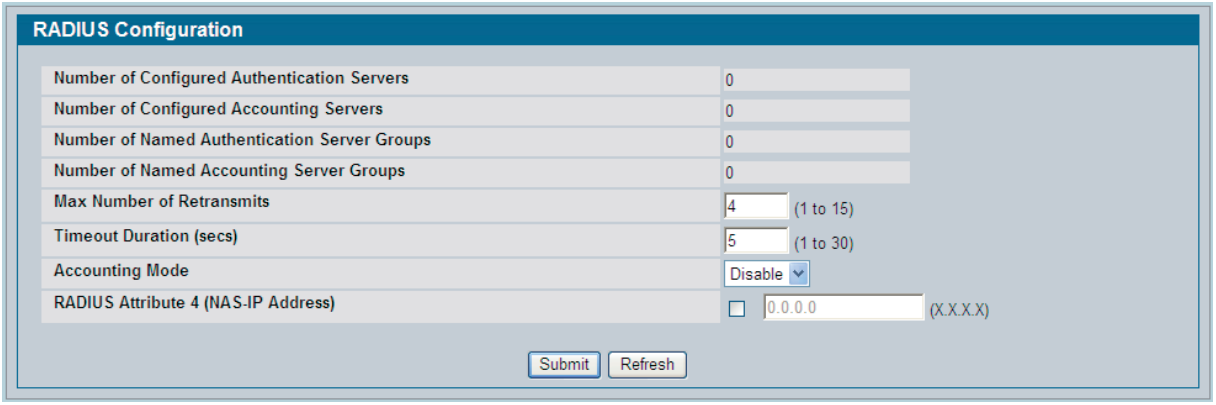


図 8-29　RADIUS Configuration 画面

以下の項目を表示します。

項目	説明
Number of Configured Authentication Servers	システム内に設定されている RADIUS 認証サーバの数。範囲は 0-32 です。
Number of Configured Accounting Servers	システム内に設定されている RADIUS アカウンティングサーバ数。範囲は 0-32 です。
Number of Named Authentication Server Groups	システム内に設定されている認証サーバグループ数。認証サーバグループには、同じ RADIUS サーバ名を共有する 1 つまたは複数の認証サーバがあります。
Number of Named Accounting Server Groups	システム内に設定されているアカウンティングサーバグループの数。アカウンティングサーバグループには、同じ RADIUS サーバ名を共有する複数の認証サーバがあります。
Max Number of Retransmits	要求パケットが再送信される最大回数。範囲は 1-15 です。 RADIUS の最大再送信回数およびタイムアウトを設定する際は、最大の遅延時間を考慮してください。これは、複数の RADIUS サーバが設定されている場合には、次のサーバが送信を開始する前に、各サーバの最大再送信回数が終了してしまうからです。サーバに設定されたタイムアウト時間が、RADIUS サーバからの返答がないまま経過するまで再送信は行われません。従って、RADIUS アプリケーションからの返答を受信する時の最大遅延時間は、設定されているすべてのサーバの再送信時間タイムアウトの総計と等しくなります。RADIUS 要求がユーザログインによって生成された場合、すべてのユーザインタフェースは、RADIUS アプリケーションが返答を送信するまでブロックされます。
Timeout Duration (secs)	再送信要求のタイムアウト時間（秒）。範囲は 1-30（秒）です。「Timeout Duration」の設定についての詳細は、「Max Number of Retransmits」欄の説明を参照してください。
Accounting Mode	現在のサーバ上の RADIUS アカウンティングモードの有効、または無効を選択します。
RADIUS Attribute 4 (NAS-IP Address)	RADIUS サーバに NAS サーバの IP アドレスを設定するためには、オプションを選択して NAS サーバの IP アドレスを入力します。アドレスは、必ず RADIUS サーバの範囲内でその NAS に対しユニークなものにします。NAS IP アドレスは認証要求パケットでのみ使用されます。

「Refresh」ボタンをクリックすると、最新の情報に更新します。画面で変更をした場合、「Submit」ボタンをクリックし、変更をシステムに適用します。

RADIUS 認証サーバ設定

新しい RADIUS サーバの追加、または既存の RADIUS サーバの設定および RADIUS サーバステータス情報の参照を行うことができます。スイッチの RADIUS クライアントは、最大 32 個の認証およびアカウンティングサーバをサポートします。

LAN タブ > Security > RADIUS > RADIUS Authentication Server Configuration の順にクリックし、以下の画面を表示します。

RADIUS サーバがシステムに設定されていない場合、あるいは「RADIUS Server Host Address」メニューから「Add」を選択した場合、以下の表にあるサブフィールドが使用できます。RADIUS ホストアドレスを入力した後、「Submit」をクリックすると追加の設定項目が表示されます。

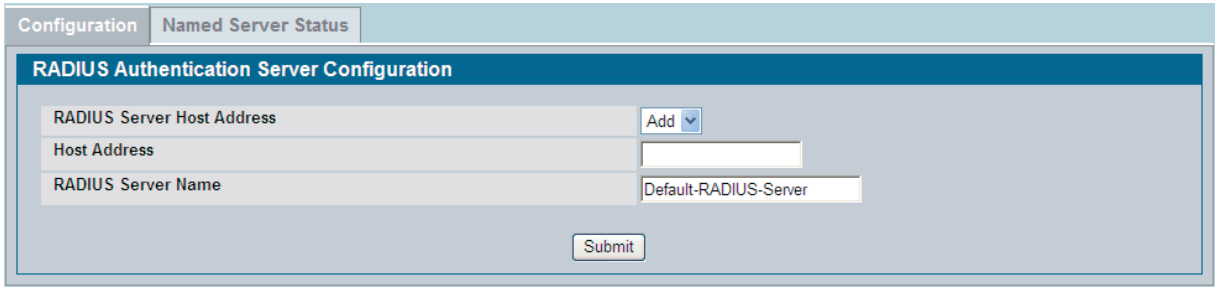


図 8-30　RADIUS Authentication Server Configuration - Add Server 画面

スイッチに少なくとも 1 つの RADIUS サーバが設定されており、「RADIUS Server Host Address」でホストアドレスが選択されている場合、本画面の追加項目を使用できます。

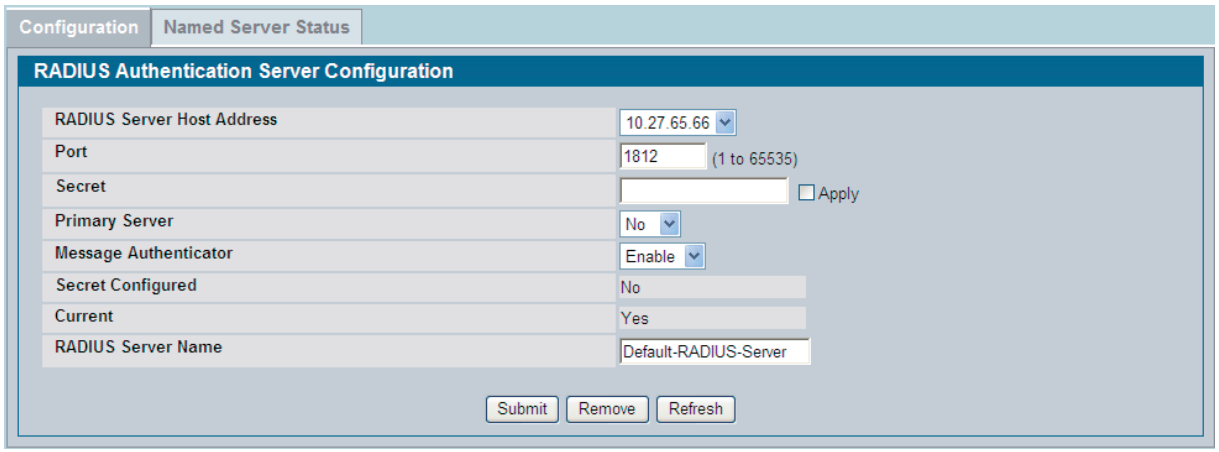


図 8-31　RADIUS Authentication Server Configuration - Server Added 画面

以下の項目を表示します。

項目	説明
RADIUS Server Host Address	参照または設定を行う RADIUS サーバの IP アドレスを選択します。「Add」を選択し、追加の RADIUS サーバを設定します。
Port	サーバが使用する認証ポートを識別して、RADIUS サーバ認証を確認します。ポートは UDP ポートで、範囲は 1-65535 です。RADIUS 認証の初期設定ポートは 1812 です。
Secret	デバイスと RADIUS サーバ間のすべての RADIUS 通信を認証、暗号化するために使用する共有秘密鍵テキスト文字列です。この秘密鍵は RADIUS サーバの暗号化方式と一致する必要があります。
Apply	ボックスをチェックした場合にのみ、「Secret」が適用されます。ボックスがチェックされていないと、「Secret」に入力したことは作用、保持されません。本項目は、ユーザが Read/Write アクセスを行っている場合にのみ表示されます。
Primary Server	選択したサーバを「Primary（Yes）」または「Secondary（No）」サーバに設定します。 同じサーバ名で複数の RAIDUS サーバを設定している場合、1 つのサーバをプライマリサーバ、他のサーバはバックアップサーバとして指定します。スイッチは、まずプライマリサーバを使用し、プライマリサーバが応答しない場合には、同じ RADIUS サーバ名を持つバックアップサーバの 1 つを使用します。
Message Authenticator	選択サーバの Message-Authenticator 属性を有効、または無効にします。
Secret Configured	このサーバの共有秘密鍵が設定されているかどうかを示します。
Current	選択した RADIUS サーバがカレントサーバ（Yes）、またはバックアップサーバ（No）であることを示します。 同じ名前の RADIUS サーバが 1 つ以上設定されている場合、スイッチは、同じ名前のサーバグループから 1 つのサーバをカレントサーバとして選択します。 スイッチが RADIUS 要求をサーバに送信すると、要求はカレントサーバとして選択されているサーバに送信されます。初期設定では、プライマリサーバがカレントサーバとして指定されています。プライマリサーバが故障した場合、他のサーバの 1 つがカレントサーバになります。プライマリサーバが設定されていない場合、最後に設定された RADIUS サーバがカレントサーバになります。

項目	説明
RADIUS Server Name	RADIUS サーバ名を表示します。 名前の変更には、最大 32 文字のテキストを入力します。スペース、ハイフン、およびアンダースコアを入力することができます。名前を割り当てない場合、サーバにはデフォルト名「Default-RADIUS-Server」が割り当てられます。 **注意** 少なくとも 1 つの RADIUS サーバが「Default-RADIUS-Server」で設定されます。802.1X など、スイッチの機能のいくつかは、RADIUS サーバがデフォルト名を使用することを見込んでいます。 複数の RADIUS 認証サーバに同じ名前を使用することができます。RADIUS クライアントは、お互いに同じ名前の RADIUS サーバをバックアップサーバとして使用することができます。

画面下部のボタンを使用して、以下のアクションを実行します。

- 変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。
- 設定済みの RADIUS サーバを削除するためには、「RADIUS Server Host Address」メニューから削除するサーバの IP アドレスを選択し、「Remove」ボタンをクリックします。
- 「Refresh」ボタンをクリックすると、最新の情報に更新します。

Named Server Status タブ（ネームサーバステータス情報の参照）

システムに設定済みの RADIUS サーバに関するサマリ情報を表示します。

LAN タブ > Security > RADIUS > RADIUS Authentication Server Configuration の順にクリックし、さらに「Named Server Status」タブをクリックして以下の画面を表示します。

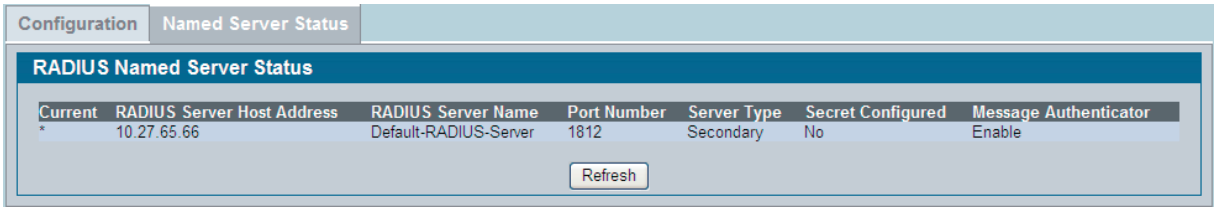


図 8-32　Named Server Status 画面

以下の項目を表示します。

項目	説明
Current	コラムのアスタリスク（*）は、そのサーバが認証サーバグループのカレントサーバであることを示します。アスタリスクが表示されていないサーバは、バックアップサーバです。同じ名前の RADIUS サーバが 1 つ以上設定されている場合、スイッチは、同じ名前のサーバグループから 1 つのサーバをカレントサーバとして選択します。 スイッチが RADIUS 要求をされたサーバに送信する場合、要求はカレントサーバとして選択されているサーバに送信されます。初期設定では、プライマリサーバがカレントサーバとして指定されています。プライマリサーバが故障した場合、他のサーバの 1 つがカレントサーバになります。
RADIUS Server Host Address	RADIUS サーバの IP アドレスを表示します。
RADIUS Server Name	RADIUS サーバ名。 複数の RADIUS サーバは同じ名前を使用することができます。この場合、RADIUS クライアントはお互いに同じ名前の RADIUS サーバをバックアップサーバとして使用することができます。
Port Number	サーバが使用する認証ポートを識別して、RADIUS サーバ認証を確認します。ポートは、UDP ポートです。
Server Type	プライマリサーバ、またはセカンダリサーバであることを示します。
Secret Configured	このサーバの共有秘密鍵が設定されているかどうかを示します。
Message Authenticator	選択サーバの Message-Authenticator 属性が有効、または無効であることを表示します。

「Refresh」ボタンをクリックすると、最新の情報に更新します。

Configuration タブ（RADIUS アカウンティングサーバ設定）

新しい RADIUS アカウンティングサーバの追加、新規または既存の RADIUS アカウンティングサーバへの設定、および RADIUS アカウンティングサーバステータス情報の参照を行います。スイッチの RADIUS クライアントは、最大 32 個の認証およびアカウンティングサーバをサポートします。
RADIUS サーバがシステムに設定されていない場合、あるいは「RADIUS Server Host Address」メニューから「Add」を選択した場合、以下の表にあるサブフィールドが使用できます。

LAN タブ > Security > RADIUS > RADIUS Authentication Server Configuration の順にクリックし、さらに「Configuration」タブをクリックして以下の画面を表示します。

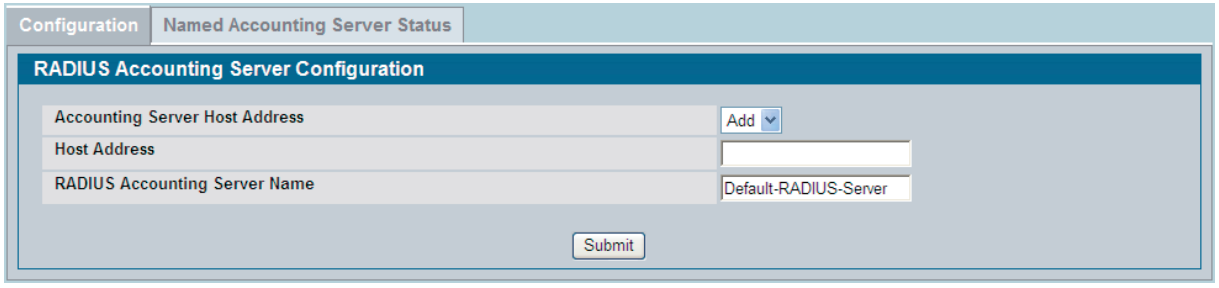


図 8-33　RADIUS Accounting Server Configuration - Add 画面

アカウンティングサーバホストのアドレスを入力し、「Submit」をクリックすると追加の設定フィールドが表示されます。

スイッチに少なくても 1 つの RADIUS サーバが設定されており、「Accounting Server Host Address」でホストアドレスが選択されている場合、「RADIUS Accounting Server Configuration」画面で追加項目を使用できます。

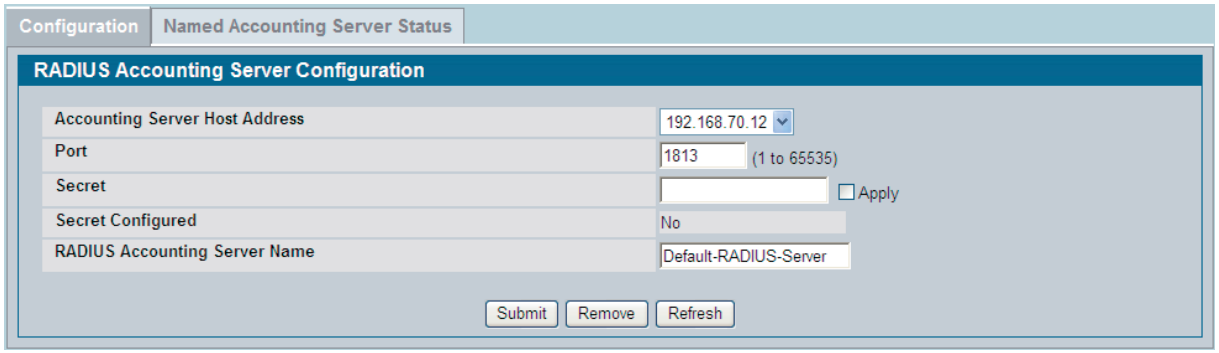


図 8-34　RADIUS Accounting Server Configuration - サーバの追加 画面

以下の項目を表示します。

項目	説明
Accounting Server Host Address	参照または設定を行うアカウンティングサーバの IP アドレスを選択します。「Add」を選択し、追加の RADIUS サーバを設定します。
Port	サーバが使用する認証ポートを識別して、RADIUS アカウンティングサーバ認証を確認します。ポートは UDP ポートで、範囲は 1-65535 です。初期値は 1813 です。
Secret	選択したアカウンティングサーバに使用する共有秘密鍵を指定します。本項目は、ユーザが Read/Write アクセスでログインしている場合にのみ表示されます。
Apply	ボックスをチェックした場合にのみ、「Secret」が適用されます。ボックスがチェックされていないと、「Secret」に入力したことは作用、保持されません。本欄は、ユーザが Read/Write アクセスでログインしている場合にのみ表示されます。
Secret Configured	このサーバの共有秘密鍵が設定されているかどうかを示します。
RADIUS Accounting Server Name	RADIUS アカウンティングサーバ名を入力します。 最大 32 文字のテキストを含むことができます。スペース、ハイフン、およびアンダースコアを入力することができます。名前を割り当てない場合、サーバにはデフォルト名「Default-RADIUS-Server」が割り当てられます。複数の RADIUS アカウンティングサーバに同じ名前を使用することができます。RADIUS クライアントは、お互いに同じ名前のアカウンティングサーバをバックアップサーバとして使用することができます。

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。「Refresh」ボタンをクリックすると、最新の情報に更新します。

RADIUS アカウンティングサーバを削除

設定済みの RADIUS アカウンティングサーバを削除するためには、「RADIUS Server IP Address」メニューから削除するサーバの IP アドレスを選択し、「Remove」ボタンをクリックします。

ネームアカウンティングサーバステータスの参照

スイッチに設定したアカウンティングサーバに関するサマリ情報を表示します。

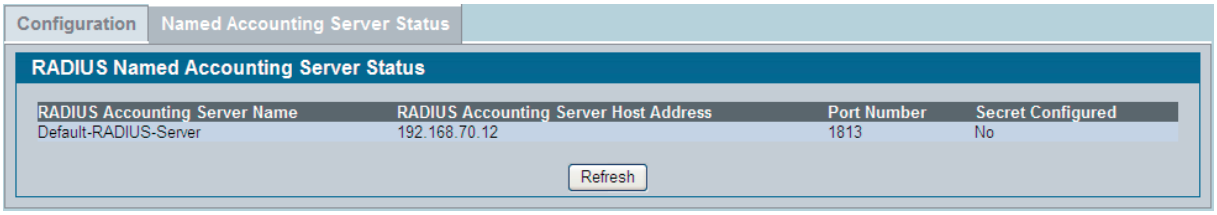


図 8-35　RADIUS Named Accounting Server Status 画面

以下の項目を表示します。

項目	説明
RADIUS Accounting Server Name	RADIUS アカウンティングサーバ名を表示します。 複数の RADIUS アカウンティングサーバは同じ名前を持つことができます。この場合、RADIUS クライアントは、お互いに同じ名前の RADIUS サーバをバックアップサーバとして使用することができます。
RADIUS Accounting Server Host Address	RADIUS サーバの IP アドレスを表示します。
Port Number	サーバが使用する認証ポートを識別して、RADIUS サーバ認証を確認します。ポートは、UDP ポートです。
Secret Configured	このサーバの共有秘密鍵が設定されているかどうかを示します。

「Refresh」ボタンをクリックすると、最新の情報に更新します。

統計情報のクリア

すべての RADIUS 認証とアカウンティング統計情報を 0 にリセットします。

LAN タブ > Security > RADIUS > Clear RADIUS 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。

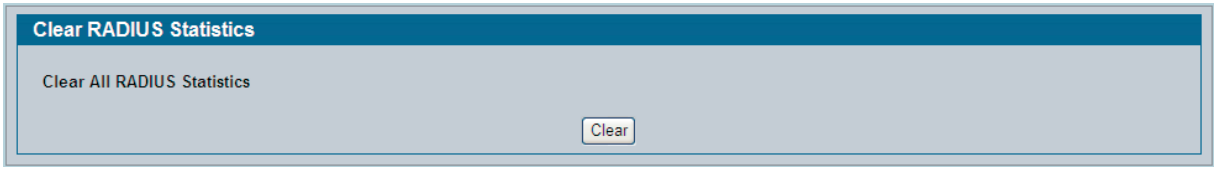


図 8-36　Clear RADIUS Statistics 画面

「Clear」ボタンをクリックし、RADIUS 認証とアカウンティングサーバのすべての統計情報をクリアします。

TACACS+ の設定

D-Link ソフトウェアは TACACS+（Terminal Access Controller Access Control System）クライアントをサポートしています。TACACS+ は、デバイスにアクセスするユーザ検証用に中央に集約化したセキュリティを提供します。

TACACS+ は、RADIUS および他の認証処理との互換性も保持しながら中央に集約化したユーザ管理システムを提供します。TACACS+ は、以下のサービスを提供します。

- Authentication - ユーザ名およびユーザ定義のパスワードを経由したログインによる認証を提供します。
- Authorization - ログイン時に実行されます。Authentication セッションが完了すると、認証ユーザ名を使用した Authentication セッションが開始します。TACACS+ は、ユーザの権限をチェックします。

TACACS+ プロトコルは、デバイスと TACACS+ サーバ間における暗号化プロトコルの交換を通じてネットワークセキュリティを保証します。TACACS+ フォルダには以下の Web 画面へのリンクがあります。

- TACACS+ の設定
- TACACS+ サーバの設定

TACACS+ の設定

設定するスイッチと TACACS+ サーバ間の通信のために TACACS+ の設定を行います。

LAN タブ > Security > TACACS+ > 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。

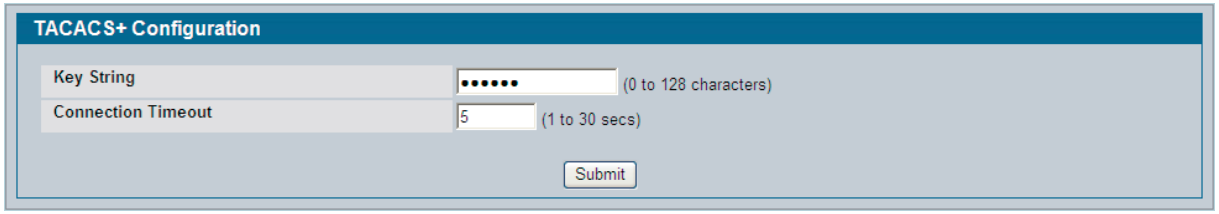


図 8-37　TACACS+ Configuration 画面

以下の項目を表示します。

項目	説明
Key String	デバイスと TACACS+ サーバ間の通信のために TACACS+ の認証および暗号化の設定を行います。範囲は 0-128 です。鍵は TACACS+ サーバ上で登録されているものと一致する必要があります。
Connection Timeout	デバイスと TACACS+ サーバ間の TCP 接続が確立するまでのタイムアウト時間（秒）。

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。

TACACS+ サーバ設定

スイッチが通信する 5 つまでの TACACS+ サーバを設定します。

LAN タブ > Security > TACACS+ > Server 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。

TACACS+ サーバが設定されていない場合、または「TACACS+ Server」から「Add」を選択した場合、次の画面を表示します。

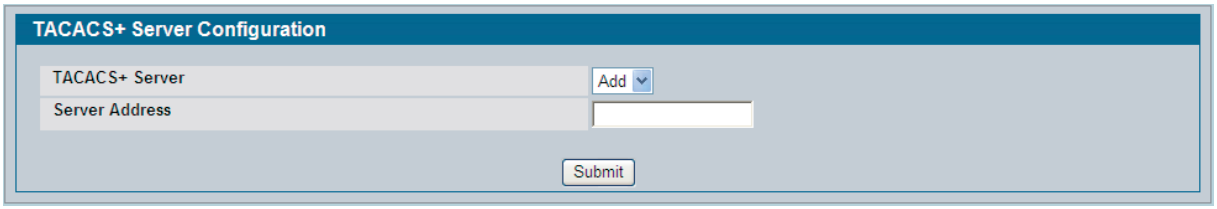


図 8-38　TACACS+ Configuration 画面 - サーバがない場合

1 つ以上の TACACS+ サーバの追加後、追加の項目が「TACACS+ Server Configuration」画面に表示されます。

以下の項目を表示します。

項目	説明
TACACS+ Server	TACACS+ サーバの IP アドレスを選択して参照または設定を行います。システムに設定されている TACACS+ サーバが 4 つ以下の場合、「Add」オプションも利用可能です。「Add」を選択し、追加の TACACS+ サーバを設定します。
IP Address	追加する TACACS+ サーバの IP アドレス。本項目は、「TACACS+ Server」で「Add」が選択された場合にだけ有効となります。
Port	TACACS+ セッションが起こる認証ポート番号。初期値は 49 で、範囲は 0-65535 です。
Key String	スイッチと TACACS+ サーバ間の通信のために TACACS+ の認証および暗号鍵の設定を行います。この鍵は TACACS+ サーバで登録されている暗号化方式と一致している必要があります。入力できるのは 0-128 文字です。
Connection Timeout	タイムアウトまでのデバイスと TACACS+ サーバ間の接続時間。範囲は 1-30（秒）です。

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。「Refresh」ボタンをクリックすると、最新の情報に更新します。

TACACS+ サーバの削除

設定済みの TACACS+ サーバを削除するためには、「TACACS+ Server Host Address」から削除するサーバの IP アドレスを選択し、「Remove」ボタンをクリックします。

HTTPS の設定

SECURE HTTP は、SSL（Secure Sockets Layer）または TLS（Transport Layer Security）接続を可能にします。Web インタフェースを使用してスイッチを管理する場合、SECURE HTTP は、盗聴や中間者攻撃から保護されているスイッチと管理システムとの間の通信を確実に行うことができます。

SECURE HTTP の設定

管理ステーションとスイッチ間の HTTPS 通信の設定を行います。

LAN タブ > Security > SSL 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。

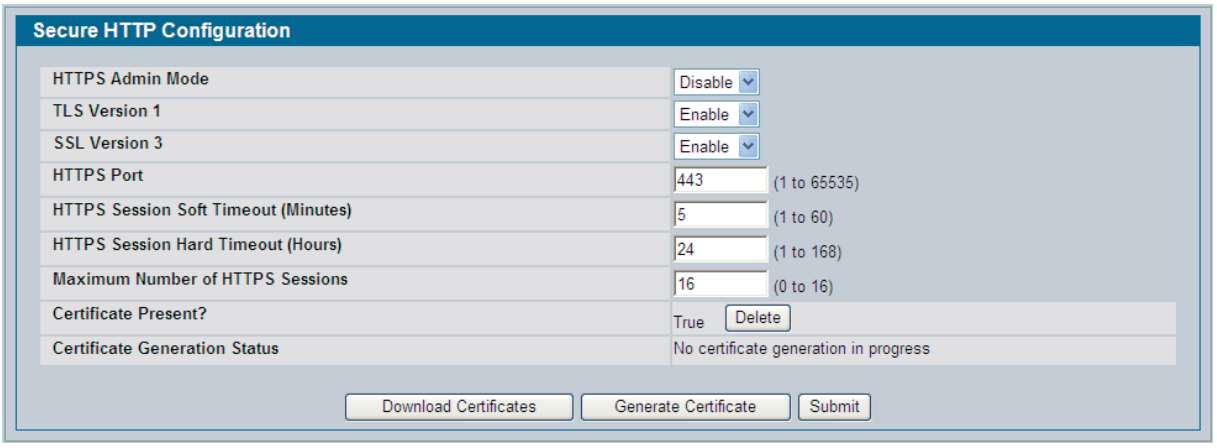


図 8-39　Secure HTTP Configuration 画面

以下の項目を表示します。

項目	説明
HTTPS Admin Mode	HTTPS Admin モードを有効、または無効にします。Web ページを開いた時に現在の設定値が表示されます。初期値は「Disable」です。「Download Certificates」ボタンは HTTPS Admin モードが無効な場合にのみ使用することができます。
TLS Version 1	Transport Layer Security Version 1.0 を有効、または無効にします。Web ページを開いた時に現在の設定値が表示されます。初期値は「Enable」です。
SSL Version 3	Secure Sockets Layer Version 3.0。Web ページを開いた時に現在の設定値が表示されます。初期値は「Enable」です。
HTTPS Port	HTTP ポート番号。範囲は 1-65535 です。初期値は 443 です。Web ページを開いた時に現在の設定値が表示されます。
HTTPS Session Soft Timeout (Minutes)	HTTPS セッションのタイムアウト時間を設定します。範囲は 1-60（分）です。初期値は 5（分）です。Web ページを開いた時に現在の設定値が表示されます。
HTTPS Session Hard Timeout (Hours)	HTTPS セッションのタイムアウト時間を設定します。このタイムアウトはセッションのアクティビティレベルには左右されません。範囲は 1-168（時間）です。初期値は 24（時間）です。Web ページを開いた時に現在の設定値が表示されます。
Maximum Number of HTTPS Sessions	HTTPS の最大セッション数を設定します。範囲は 0-16 です。初期値は 16 です。Web ページを開いた時に現在の設定値が表示されます。

スイッチの Web サーバが管理ステーションからの HTTPS 接続を許可するためには、Web サーバには公開鍵認証が必要です。統合スイッチには初期値で実装された自己生成証明書があります。また、スイッチは自身の証明書の生成、または外部で（つまりオフラインで）生成してスイッチにダウンロードすることもできます。

証明書の生成

スイッチで証明書を作成します。

1. 「Generate Certificate」ボタンをクリックします。画面には「Certificate generation in progress」が表示されます。

2. 「Submit」をクリックして、処理を完了します。画面に「No certificate generation in progress」メッセージが表示され、成功すると「Certificate Present」が表示されます。

SSL 証明書のダウンロード

スイッチにファイルをダウンロードする前に、以下の条件であることを必ず確認してください。

- TFTP サーバからダウンロードするファイルがサーバの適切なディレクトリにあること。
- ファイルが正しいフォーマットであること。
- スイッチが TFTP サーバへのパスを持っていること。

以下の手順で SSL 証明書をダウンロードします。

1. ページ下にある「Download Certificates」ボタンをクリックします。

注意 「Download Certificates」ボタンは HTTPS admin モードが無効な場合にのみ使用することができます。モードが有効である場合、それを無効にしてから「Submit」ボタンをクリックします。画面が更新され、「Download Certificates」ボタンが表示されます。

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

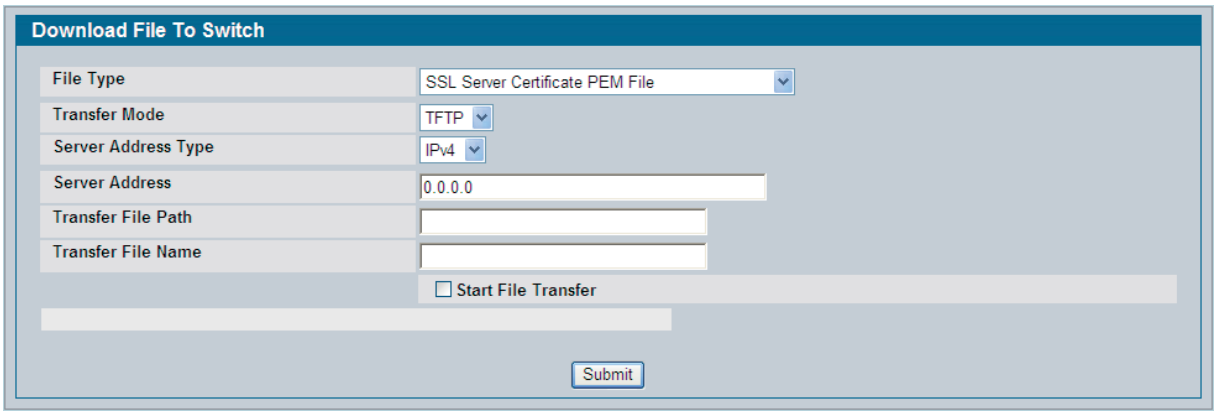


図 8-40　Download File to Switch 画面

2. 「File Type」から以下に示すダウンロードする SSL ファイルのタイプを選択します。

- SSL Trusted Root Certificate PEM File : SSL Trusted Root Certificate File（PEM Encoded）
- SSL Server Certificate PEM File : SSL Server Certificate File（PEM Encoded）
- SSL DH Weak Encryption Parameter PEM File : SSL Diffie-Hellman Weak Encryption Parameter File（PEM Encoded）
- SSL DH Strong Encryption Parameter PEM File : SSL Diffie-Hellman Strong Encryption Parameter File（PEM Encoded）

3. TFTP サーバの IP アドレスを検証し、ダウンロードされるソフトウェアイメージまたは他のファイルが TFTP サーバで有効であることを確実にします。

4. 「TFTP Server IP Address」および「TFTP File Name」（TFTP サーバの IP アドレスでフルパス）を入力します。

5. 「Start File Transfer」ボックスをチェックし、「Submit」ボタンをクリックします。

「Submit」ボタンのクリック後、画面が更新され、「File transfer operation started」メッセージが表示されます。ソフトウェアがデバイスにダウンロードされた後、ファイル転送操作が成功したことを示すメッセージが表示されます。

6. **LAN タブ > Security > SSL Configuration** の順にメニューをクリックし、「Secure HTTP Configuration」に戻ります。

7. 「HTTPS admin」モードを有効にするためには、「HTTPS Admin Mode」から「Enable」を選択し、「Submit」ボタンをクリックします。

SSH の設定

コマンドラインインタフェース（CLI）を使用してリモートシステムからスイッチを管理する場合、セキュアな接続を確立するために SSH（Secure Shell）を使用することができます。SSH は、公開鍵暗号を使用してコンピュータを認証します。

SSH の設定

管理ステーションとスイッチ間のセキュアなコマンドラインベースの通信のために設定を行います。

LAN タブ > Security > SSH 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。

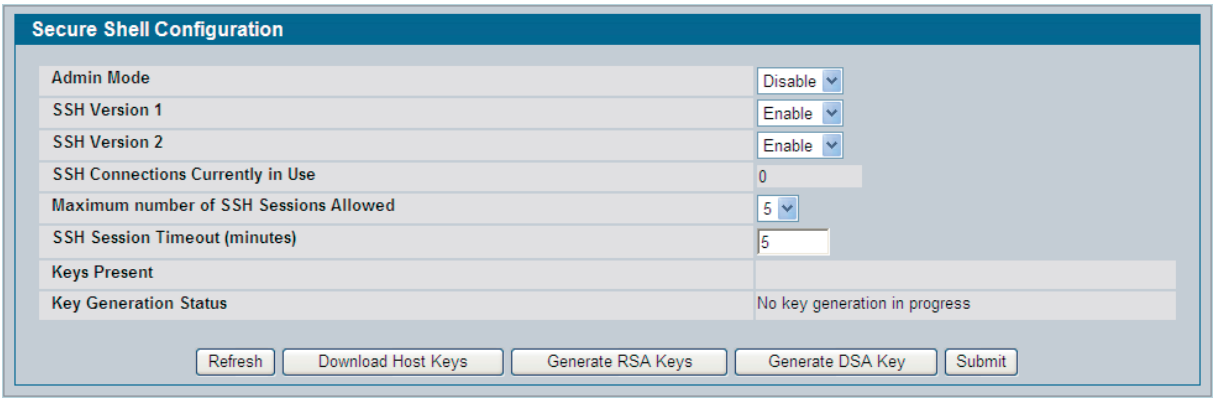


図 8-41　Secure Shell Configuration 画面

以下の項目を表示します。

項目	説明
Admin Mode	SSH の管理モードを有効、または無効にします。Web ページを開いた時に現在の設定値が表示されます。初期設定は「Disable」です。
SSH Version 1	SSH Version 1 を有効、または無効にします。Web ページを開いた時に現在の設定値が表示されます。初期値は「Enable」です。
SSH Version 2	SSH Version 2 を有効、または無効にします。Web ページを開いた時に現在の設定値が表示されます。初期値は「Enable」です。
SSH Connections in Use	システム内で現在使用されている SSH 接続数を表示します。
Maximum Number of SSH Sessions Allowed	スイッチ上で許可されている SSH の最大インバウンドセッション数を設定します。Web ページを開いた時に現在の設定値が表示されます。範囲は 0-5 です。
SSH Session Timeout (minutes)	スイッチに送信される SSH セッションのタイムアウトを設定します。範囲は 1-160（分）です。
Keys Present	現在使われているキーを表示します :「RSA」、「DSA」、または「both」
Key Generation Status	キーの生成ステータスを表示します :「RSA」または「DSA」

「Refresh」ボタンをクリックすると、最新の設定とステータスを使用して現在の画面を更新します。

「Download Host Keys」をクリックしてホストキーダウンロードのために「File Transfer」画面にリンクします。

注意 SSH キーファイルをダウンロードするためには、SSH を管理上無効にして、アクティブな SSH セッションがないようにします。

「Generate RSA Host Keys」ボタンをクリックして、RSA ホストキーの生成を開始します。

注意 RSA キーファイルをダウンロードするためには、RSA を管理上無効にして、アクティブな SSH セッションがないようにします。

「Generate DSA Host Keys」ボタンをクリックして、DSA ホストキーの生成を開始します。

注意 DSA キーファイルをダウンロードするためには、DSA を管理上無効にして、アクティブな SSH セッションがないようにします。

「Delete」ボタンをクリックし、対応するキーファイル（RSA または DSA）を、存在する場合に削除します。

変更を行った場合、「Submit」ボタンをクリックし、変更をスイッチに適用します。

SSH ホストキーのダウンロード

スイッチが管理ステーションからの SSH 接続を許可するためには、スイッチには SSH ホストキーまたは証明書が必要です。スイッチは自身のキーまたは証明書の生成、または外部で（つまりオフラインで）生成してスイッチにダウンロードすることもできます。

TFTP サーバからスイッチに SSH ホストキーをダウンロードするために、「SSL 証明書のダウンロード」の手順を使用します。「File Download」画面で「File Type」から以下に示すダウンロードするキーファイルのタイプを選択します。

- SSH-1 RSA Key File : SSH-1 Rivest-Shamir-Adleman（RSA）Key File
- SSH-2 RSA Key PEM File : SSH-2 Rivest-Shamir-Adleman（RSA）Key File（PEM Encoded）
- SSH-2 DSA Key PEM File : SSH-2 Digital Signature Algorithm（DSA）Key File（PEM Encoded）

第 9 章　無線機能の設定

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。

以下を含む WLAN フォルダには利用可能な機能に関する情報があります。

設定項目	説明	参照ページ
D-Link 統合アクセスシステムのコンポーネント	統合アクセスシステムがサポートするコンポーネントについて説明します。	268 ページ
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必要な基本設定について説明します。	274 ページ
アクセスポイント管理	統合スイッチでアクセスポイントの管理 / 維持を行う設定について説明します。	296 ページ
状態および統計情報のモニタリング	統合スイッチネットワークでステータスや統計情報の監視を行う方法について説明します。	306 ページ
侵入検知に関するモニタリングと管理	統合スイッチネットワーク内のアクセスポイントと無線クライアントの管理、監視を行い、不正なデバイスから防御する方法について説明します。	342 ページ
システムの詳細設定	統合スイッチに行う詳細な設定について説明します。	357 ページ
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ためのオプション機能について説明します。	376 ページ

D-Link 統合アクセスシステムのコンポーネント

D-Link 統合アクセスシステムには以下のコンポーネントがあります。

- D-Link DWS-4026 統合スイッチ
- D-Link DWL-8600AP は統合アクセスポイント（UAP）

各統合スイッチは最大 64 台までのアクセスポイントを管理します。また、各アクセスポイントは最大 400 台までの無線クライアントと接続が可能です（各無線インタフェースにつき 200）。統合スイッチ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。

より大規模なネットワークを運用するために、無線スイッチをクラスタ（ピアグループ）に登録することができます。クラスタには最大 8 台までのスイッチを構成することができ、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。各クラスタは、最大 256 のアクセスポイントと合計 8000 の無線クライアントをサポートすることができます。クラスタ内のスイッチは管理するアクセスポイント間の L3 ローミングを有効にします。つまり、この WLAN スイッチにより、無線クライアントは、クラスタ内でネットワークへの接続を保ったままアクセスポイント間をローミングすることが可能となります。さらに、無線設定の一部をクラスタ内の複数のスイッチに割り当てることができるということです。

クラスタ内のスイッチの 1 つが、自動的にクラスタコントローラに選出、設定されます。クラスタコントローラは、クラスタ内のすべてのアクセスポイントおよびクライアントのステータスと統計情報を収集して、ネットワークのステータス情報を参照し、クラスタ内のすべてのデバイスを 1 つのスイッチから管理できるようにします。

無線システム内のスイッチは、相互の直接接続、レイヤ 2 ブリッジによる分割、また異なる IP サブネットへの所属を行うことができます。

クラスタの有無に関わらず、統合スイッチでは、合計 8000 台までの無線クライアントをサポートできます。

DWS-4026 統合スイッチ

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、レイヤ 3、レイヤ 4 のスイッチングおよびルーティング機能を持っており、最大 64 台のアクセスポイントを管理します。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、不正アクセスポイント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。

DWL-8600AP 統合アクセスポイント（UAP）

UAP 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
  統合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
  統合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、統合スイッチを使用して管理を行います。アクセスポイントが本モードの場合、管理用 Web インタフェースおよび SNMP サービスはアクセスポイントで使用できなくなります。アクセスはシリアルケーブル接続を経由した CLI に制限されます。

スタンドアロンモードは数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おり、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。アクセスポイントの使用をスタンドアロンモードで開始しても、統合スイッチをネットワークに追加する際にそのアクセスポイント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。

UAP は 2 個の周波数帯域を持っており、以下の無線モードでブロードキャストすることができます。

- IEEE 802.11b モード
- IEEE 802.11g モード
- IEEE 802.11a モード
- IEEE 802.11n モード（2.5 GHz および 5 GHz）

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 32 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。

統合スイッチとアクセスポイントディスカバリ方法

統合スイッチとアクセスポイントは、以下の方式を使用して相互に検出を行います。

- レイヤ 2 検出
- アクセスポイントの IP アドレスをスイッチに登録
- スイッチの IP アドレスをアクセスポイントに登録

注意 スイッチの管理下にあるアクセスポイントは、アクセスポイント上の管理モードを有効にする必要があります。アクセスポイントの管理モードを有効にするためには、アクセスポイントの CLI にログインをして「set managed-mode」コマンドを使用するか、または管理 Web ユーザインタフェースにアクセスして「Managed Access Point」画面から管理モードオプションを有効にします。

注意 アクセスポイントおよびそのアクセスポイントを管理すべきスイッチは NAT（Network Address Translation）デバイスで分離することはできません。アクセスポイントおよびスイッチは、検出のデータやその他のメッセージ内で相互の IP アドレスを交換するためです。これらのアドレスは、スイッチとアクセスポイント間のその後の通信に使用されます。このアドレスは変換されないため、スイッチとアクセスポイントは通信することはできません。しかし、スイッチとアクセスポイントには、離れた場所や VPN によって接続しているリモートサイトや支店などの通信において問題点はありません。VPN 機能は通常ファイアウォールに搭載されているためです。この問題は、NAT を使用するネットワーク間の VPN アクセスを設定することで解決します。

レイヤ 2 検出

アクセスポイントと統合スイッチが直接接続している場合や、同じレイヤ 2 のブロードキャストドメインに属し、デフォルト VLAN 設定を使用している場合には、統合スイッチはレイヤ 2 の Discovery メッセージのブロードキャストを使用してアクセスポイントを自動的に検出します。レイヤ 2 でのデバイス検出は、デバイスが直接接続される時、またはレイヤ 2 ブリッジを使用して接続される時に自動的に実行されます。

レイヤ 2 検出に関する詳しい情報は、「レイヤ 2/VLAN 検出」（278 ページ）を参照してください。

アクセスポイントの IP アドレスをスイッチに登録

アクセスポイントが統合スイッチではなく異なるブロードキャストドメイン内にある場合や、異なる管理 VLAN を使用する場合は、アクセスポイントの IP アドレスをスイッチのレイヤ 3 検出リストに追加することが可能です。統合スイッチはリスト内の IP アドレスに対して、UDP Discovery メッセージを送信します。アクセスポイントがそのメッセージを受信し、そのスイッチに接続できることを確認すると、スイッチに対し SSL による TCP 接続を開始します。

スイッチへのアクセスポイント IP アドレスの設定関する詳細は、「レイヤ 3/IP 検出」（278 ページ）を参照してください。

スイッチの IP アドレスをアクセスポイントに登録

スタンドアロンモードではアクセスポイントに接続することはできません。アクセスポイントの管理を許可されている 4 個までのスイッチの IP アドレスまたは DNS 名をスタティックに設定します。

アクセスポイントは、UDP Discovery メッセージをリスト中の一番目の IP アドレス宛てに送信します。スイッチがそのメッセージを受信すると、そのアクセスポイントの Vendor ID は有効であるか、アクセスポイントに SSL による TCP 接続が既に存在していないか、また管理するアクセスポイントの最大数に達していないかを確認します。すべての条件が整うと、統合スイッチはアクセスポイントに対し invitation メッセージを送信し、SSL による TCP 接続を開始します。

リスト中 1 番目の統合スイッチから invitation メッセージを受信しないと、最初の統合スイッチへの UDP Discovery メッセージ送信から 5 秒後に、2 番目の統合スイッチに向けて UDP Discovery メッセージを送信します。

アクセスポイントに統合スイッチの IP アドレスの登録がされていれば、他のスイッチが別の方法でアクセスポイントを検出しても、そのアクセスポイントは登録済みスイッチとだけ接続をします。

注意 この方法を使う場合には、アクセスポイントが統合スイッチへのルートを知っている必要があります。

アクセスポイントの Web インタフェースにアクセスしてスイッチの IP アドレス情報を登録するためには、Web ブラウザからアクセスポイントにログインして「Managed Access Point」画面を開きます。情報を入力して、「Update」ボタンをクリックします。

CLI を使用してアクセスポイント内の IP アドレス情報を設定します。手順は以下の通りです。

1. シリアルまたは Telnet 接続を使用してアクセスポイントにログインします。

2. 「set managed-ap switch-address-<1.4>」を使用して、アクセスポイントの管理に使用できる 4 台までのスイッチの IP アドレスを入力します。例として、IP アドレス 192.168.66.202 のスイッチと 192.168.19.242 の 2 台を登録します。

```
WLAN-AP# set managed-ap switch-address-1 192.168.66.202
WLAN-AP# set managed-ap switch-address-2 192.168.19.242
```

3. get managed-ap コマンドを実行して、登録した情報を確認します。

```
WLAN-AP# get managed-ap
```

プロパティ	値
mode	up
ap-state	down
switch-address-1	192.168.66.202
switch-address-2	192.168.19.242
switch-address-3	
switch-address-4	
managed-mode-watchdog 0	

DHCP オプション設定

アクセスポイントが DHCP サーバに送信する DHCP 要求に対する DHCP 応答中のオプションとして統合スイッチの IP アドレスを設定します。

アクセスポイントは、DHCP オプション 43（ベンダ情報オプション）を使用して、最大 4 台までのスイッチの IP アドレスまたは DNS 名を設定できます。アクセスポイントにスタティック IP アドレスが設定されている場合は、DHCP オプション 43 は無視されます。

注意 この検出方法は、アクセスポイントが DHCP サーバからネットワーク情報を受信する前に、DHCP オプションの設定が行われている場合のみ有効となります。

DHCP オプション 43 のデータフォーマットは、RFC 2132 で規定されています。

DHCP サーバに DHCP オプションを登録する方法は、ご使用の DHCP サーバによって異なります。Microsoft Windows 2000 または 2003 で DHCP サーバをご使用であれば、以下の手順に従って、アクセスポイントへの DHCP オプション 43 に使用するスコープを作成します。

1. Windows の「コントロールパネル」で「管理ツール」アイコンをクリックし、「管理ツール」画面を表示します。「DHCP」アイコンをクリックし、DHCP マネージャを起動します。

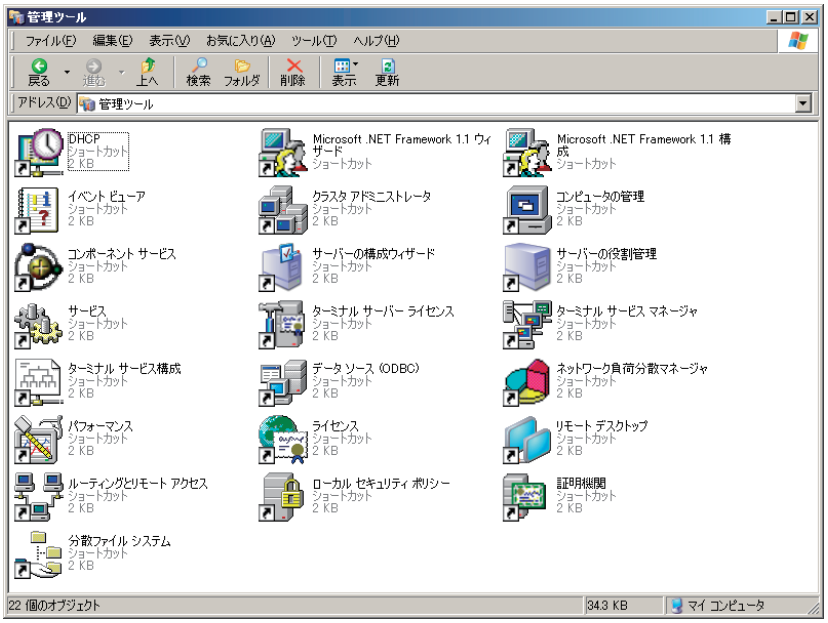


図 9-1 「管理ツール」画面

2. 「DHCP」アイコンをクリックし、DHCP マネージャを起動します。

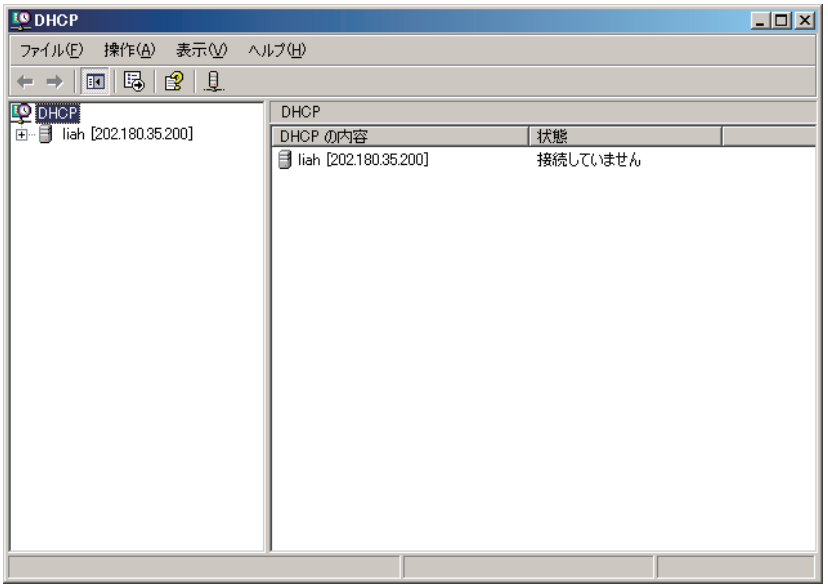


図 9-2 DHCP マネージャ画面

3. DHCP マネージャで、目的のスコープの「スコープオプション」を右クリックし、「オプションの構成」を選択します。

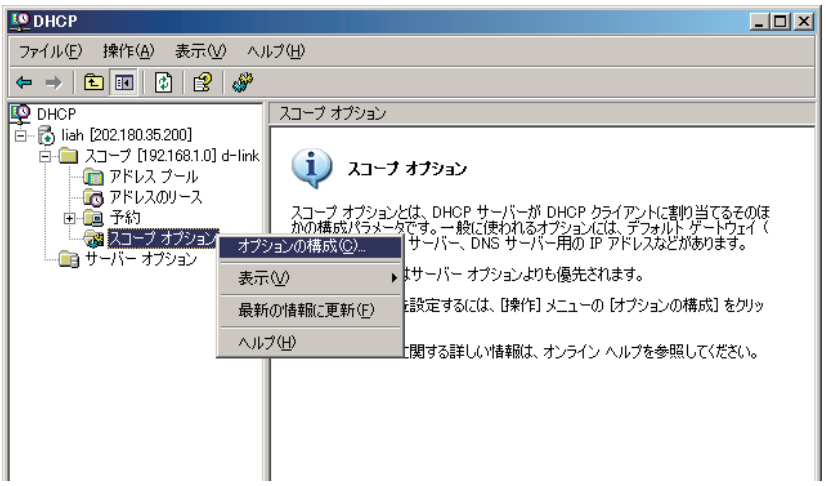


図 9-3　Windows の DHCP サーバ設定画面 1

4. 「スコープオプション」の「全般」タブ内の利用可能なオプションリストをスクロールし、「043 ベンダ固有情報」ボックスにチェックを入れます。

5. オプション 43 データを「データ入力」欄に入力します。
DHCP オプション 43 のデータフォーマットは、RFC 2132 で規定されています。192.168.1.10 の IP アドレスをバイナリコラムに入力するためには、データタイプコード（01）、アドレス長（04）、次に 16 進数表記で IP アドレスを入力します。その後も登録するアドレスのごとに、データタイプ、アドレス長、16 進数の IP アドレスの順で入力を続けます。

例えば、4 つの IP アドレス（192.168.1.10、192.168.2.10、192.168.3.10、192.168.4.16）をオプション 43 に登録する場合、データエントリ欄に以下の 16 進数コードを入力します。

```
01 04 0C A8 01 0A 01 04 0C A8 02 0A 01 04 0C A8 03 0A 01 04 0C A8 04 10
```

以下の図は、Windows DHCP サーバのデータエントリ欄に 4 件の IP アドレスを入力した状態を示しています。

図 9-4　Windows の DHCP サーバ設定画面 2

6. 「OK」ボタンをクリックします。
以下の図は、オプション 43 の設定を行ったスコープを示しています。

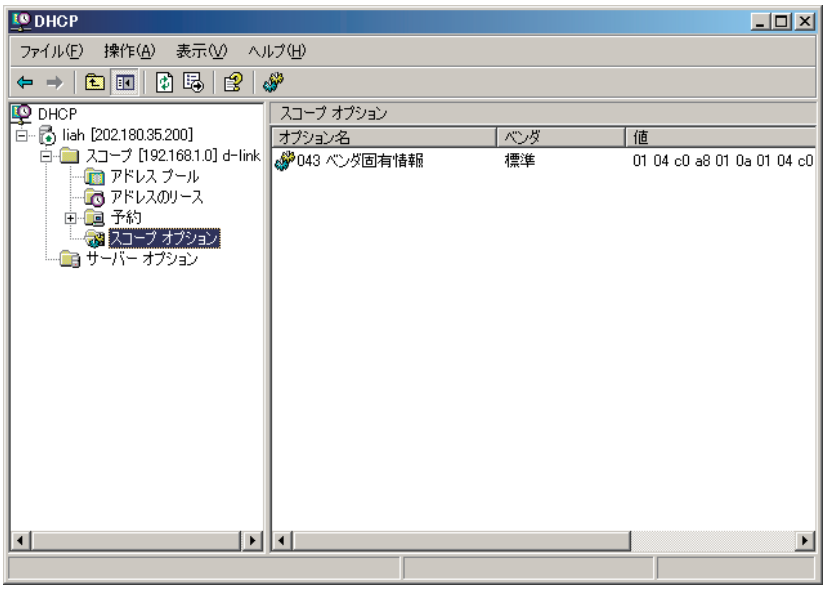


図 9-5　Windows の DHCP サーバ設定画面 3

検出とピアスイッチ

ネットワーク中に複数のピアスイッチが存在する場合、どのスイッチが検出メソッドを使用して、どのアクセスポイントの検出をするかを制御することができます。

あるアクセスポイントの検出をある特定のスイッチから行う場合は、以下の方法のうち、いずれか一つを実行します。

- すべてのスイッチでレイヤ 2 検出を無効にし、1 台の統合スイッチにのみ検出するアクセスポイントの IP アドレスを登録する。
- アクセスポイントに 1 台の統合スイッチの IP アドレスを登録する。
- DHCP オプション 43 に 1 台の統合スイッチの IP アドレスのみを登録する。

さらに他の方法として、RADIUS サーバがアクセスポイント認証プロセスでアクセスポイントの MAC アドレスを確認中に、スイッチの IP アドレスをリプライさせる方法もあります。RADIUS サーバが、管理対象として有効なアクセスポイントであると認識し、スイッチと異なる IP アドレスをリプライすると、このスイッチは re-link メッセージに、このアクセスポイントが接続を行うべきスイッチの IP アドレスを付与して、アクセスポイントに送信します。アクセスポイントは re-link メッセージを受け取ると、そのスイッチの IP アドレスを登録して、前のスイッチとの TCP 接続を切断し、新規に検出プロセスを開始します。

クラスタ内のスイッチからアクセスポイントの管理を行えるように、統合スイッチを設定することが可能です。あるアクセスポイントを管理する統合スイッチがダウンした場合、他のバックアップスイッチに管理を引き継がせることも可能です。

1 台以上のスイッチをアクセスポイント管理のバックアップスイッチとして使用にする場合は、以下の検出方法を実行します。

- アクセスポイントといずれかのピアスイッチが同一のレイヤ 2 ブロードキャストドメインに属しており、レイヤ 2 検出が有効に設定されており、すべてのデバイスがデフォルト VLAN 設定されている場合、プライマリ統合スイッチが接続不能に陥った際には、ピアスイッチが自動的にアクセスポイントを検出します。
- 複数スイッチにアクセスポイントの IP アドレスを登録する。
- スタンドアロンモードのアクセスポイントに 4 台までのスイッチの IP アドレスを登録する。
- DHCP オプション 43 にクラスタ内のスイッチ（最高 4 台）の IP アドレスを登録する。

基本設定

WLAN タブ > 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）

無線グローバル基本設定（Global タブ）

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。WLAN コンポーネントは初期値で有効です。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。

WLAN タブ > Administration > Basic Setup の順にメニューをクリックし、さらに「Global」タブをクリックして以下の画面を表示します。

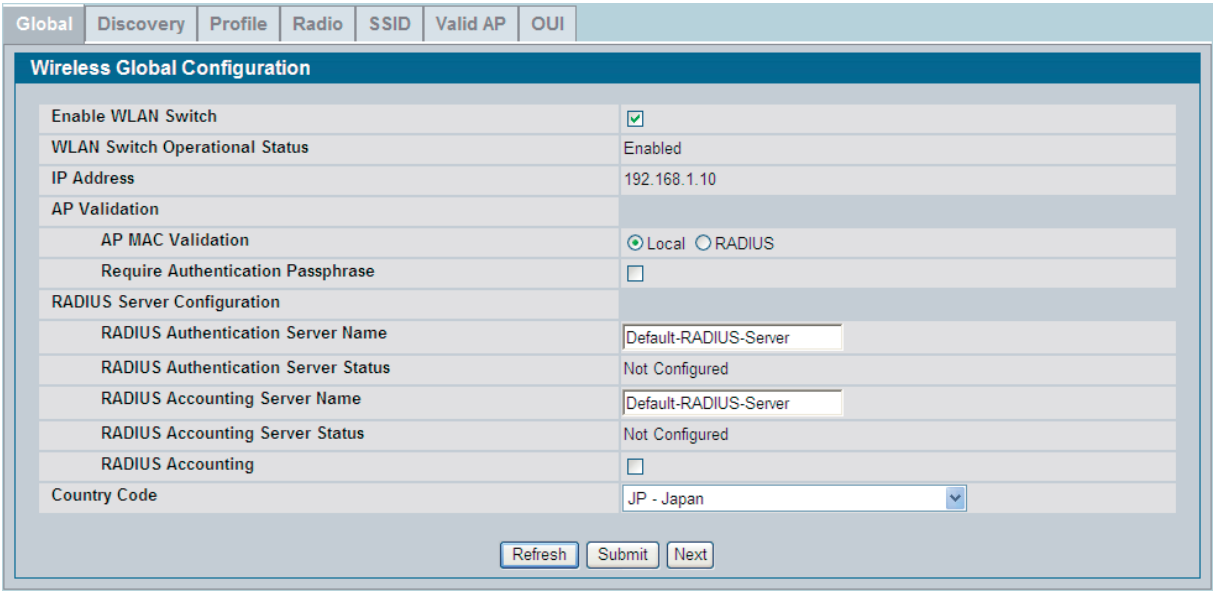


図 9-6　Wireless Global Configuration 画面

以下の表では「Wireless Global Configuration」画面の利用可能な項目を説明します。

項目	説明
Enable WLAN Switch	このオプションを選択すると、システムの WLAN スイッチ機能を有効にします。WLAN スイッチ機能を管理上無効にするためには、オプションをクリアします。 オプションをクリアすると、本スイッチに接続中のピアスイッチやアクセスポイントは切断されます。 WLAN スイッチ機能を無効にしても、VLAN や STP などのその他の機能には影響しません。
WLAN Switch Operational Status	スイッチの稼動状況を表示します。以下のいずれかが表示されます。 • Enabled • Enable-Pending（有効保留中） • Disabled • Disable-Pending（無効保留中） 状況が保留中の場合は「Refresh」をクリックして画面を更新してください。
WLAN Switch Disable Reason	WLAN スイッチ機能が無効である場合、本項目が現れて以下の原因の一つが表示されます。 • None - なし。機能無効の原因が不明です。 • Administrator disabled -「Enable WLAN Switch」チェックボックスのチェックが外されました。 • No IP Address - WLAN インタフェースに IP アドレスが割り当てられていません。 • No SSL Files - 統合スイッチとアクセスポイントの通信は、アクセスポイントと SSL 暗号化通信を行っています。統合スイッチの電源を投入すると、自動的にサーバ証明書が発行され、SSL 接続の確立に使用されます。SSL 証明書およびキーの発行には約 1 時間を要します。 スイッチ上でルーティングが有効になっていても、稼動状況は以下の原因で無効とされている場合があります。 • No Loopback Interface - スイッチにループバックインタフェースが存在しません。 • Global Routing Disabled - グローバルルーティングが無効です。稼動状況を有効にするためには、WLAN スイッチインタフェース上でルーティングモードだけでなく、グローバルルーティングも有効にする必要があります。
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。スイッチにルーティングパッケージがインストールされていない場合やルーティング機能を無効にしている場合は、表示 IP アドレスはネットワークインタフェースのものになります。ルーティングパッケージがインストールされ機能を有効にしている場合は、統合スイッチに登録したルーティングインタフェースまたはループバックインタフェースの IP アドレスになります。 ルーティング機能を有効にしている場合は、スイッチ上のループバックインタフェースを定義することを強くお勧めします。ループバックインタフェースを定義することにより、複数のルーティングインタフェースが存在する場合に、無線機能の IP アドレスとしてどのルーティングインタフェースを使用するかを指定することができます。これにより、アクセスポイントが統合スイッチの IP アドレスを検出する検出モード時のトラブルを回避することができます。ループバックインタフェースを使用すれば、無線機能用の IP アドレスとして常に同じものを使用できます。 上のループバックインタフェースとは、自分自身を示す IP アドレス 127.0.0.1 を持つループバックインタフェースとは異なります。スイッチの無線インタフェースとしてループバックインタフェースを設定する際は、それが永続的な論理インタフェースであり、IP アドレス 127.0.0.1 ではないということが重要になります。ループバックインタフェースには専用のサブネットを設け、ネットワーク中の他のデバイスはループバックインタフェースにアクセス可能である必要があります。
AP Validation	
AP MAC Validation	統合スイッチがアクセスポイントを管理するためには、ローカルまたは外部 RADIUS サーバに保存されている Valid アクセスポイントデータベースに、アクセスポイントの MAC アドレスを登録する必要があります。スイッチが他の統合スイッチの管理下にないアクセスポイントを検出すると、Valid AP データベース内で MAC アドレスを検索します。データベースにそのアクセスポイントの MAC アドレスが存在すれば、スイッチはアクセスポイントの認証を行い、自分の管理対象とします。 使用するデータベースを選択して、アクセスポイントの認証、または Require Authentication Passphrase オプションを選択している場合には認証を行います。 • Local - 選択した場合、各アクセスポイントの MAC アドレスをローカル Valid AP データベースに登録する必要があります。 • RADIUS - 選択した場合、各アクセスポイントの MAC アドレスを外部 RADIUS サーバに登録する必要があります。

項目	説明
Require Authentication Passphrase	アクセスポイントがスイッチと接続する際に認証が必要な場合に選択します。このオプションを選択した場合、アクセスポイントがスタンドアロンモードの時 Valid AP データベースに登録が必要なのと同様、アクセスポイントにパスフレーズを登録する必要があります。スタンドアロン AP にパスフレーズの設定は、アクセスポイントの管理 Web インタフェースにログインして「Managed Access Point」画面で行うか、またはアクセスポイントの CLI にログインして「set managed-ap pass-phrase」コマンドを実行してください。 ローカルの Valid AP データベースにアクセスポイントのパスフレーズを登録するためには、「Basic Setup」画面から Valid AP タブをクリックします。それからアクセスポイントの MAC アドレスをクリックし、「Authentication Password」フィールドにパスフレーズを入力します。認証を有効に設定すると、スイッチがアクセスポイントを認知した直後に認証を行います。
RADIUS Server Configuration	
RADIUS Authentication Server Name	**Basic Setup > SSID** の順にクリックして表示される「Wireless Network Configuration」画面で、ネットワークレベルの RADIUS サーバが定義されていない場合は、アクセスポイントとクライアント認証に使用する RADIUS サーバ名を入力します。最大 32 文字のテキストを含むことができます。スペース、ハイフン、およびアンダースコアを入力することができます。 スイッチは RADIUS クライアントとして機能して、アクセスポイントおよび無線クライアントのためにすべての RADIUS トランザクションを行います。
RADIUS Authentication Server Status	RADIUS 認証サーバが設定状況を示します。RADIUS サーバ情報を設定するためには、**LAN タブ > Security > RADIUS > Server Configuration** の順にメニューをクリックします。
RADIUS Accounting Server Name	**Basic Setup > SSID > Wireless Network Configuration** の順にクリックして表示される画面でネットワークレベルの RADIUS アカウンティングサーバが設定されていない場合に、無線クライアントの関連および分離状況を報告するのに使用する RADIUS サーバ名を入力します。最大 32 文字のテキストを含むことができます。スペース、ハイフン、およびアンダースコアを入力することができます。
RADIUS Accounting Server Status	RADIUS アカウンティングサーバの設定状況を示します。RADIUS アカウンティングサーバ情報を設定するためには、**LAN タブ > Security > RADIUS > Accounting Server Configuration** の順にメニューをクリックします。
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。
Country Code	スイッチおよびアクセスポイントを運用する国の国コードを選択します。「Submit」をクリックすると、変更を確認する画面が表示されます。 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。 **注意** 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。 国コードは beacon フレームや prove Response に乗せてアクセスポイントから送信されます。

無線ディスカバリの設定（Discovery タブ）

統合スイッチは以下のデバイスの検出、確認、認証および監視を行います。

- ピア無線スイッチ
- アクセスポイント
- 無線クライアント
- 不正アクセスポイント
- 不正無線クライアント

統合スイッチはピア無線スイッチやアクセスポイントを検出します。検出は、それらのデバイスが相互に接続しているか、同じレイヤ 2 ブロードキャストドメインに存在しているか、または異なる IP サブネットに属しているかなどに関係なく行われます。

スイッチおよびピアスイッチ、またはアクセスポイント間の検出機能は、以下のメカニズムのいずれかにより有効にできます。

1. スタンドアロンモードのアクセスポイントにスイッチの IP アドレスを手動で登録する。
2. アクセスポイントからの DHCP Client Request に応答する DHCP Response 内にスイッチの IP アドレスを含むように、DHCP サーバに設定をする。
3. L2 無線デバイス検出プロトコルのブロードキャストに VLAN を使用する。
4. アクセスポイントの IP アドレスを手動でスイッチに登録する。

注意 この方法では、複数のピアスイッチが同じアクセスポイントを検出することがあります。最初の接続が優先されます。一度スイッチとの接続が確立されると、アクセスポイントはその接続が切れるまで、または相手スイッチから一度切断し、他のスイッチと接続するように指示されるまで接続を持続させます。

WLAN タブ > Basic Setup の順にメニューをクリックし、「Discovery」タブをクリックします。方式 3 と 4 を使用して、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。

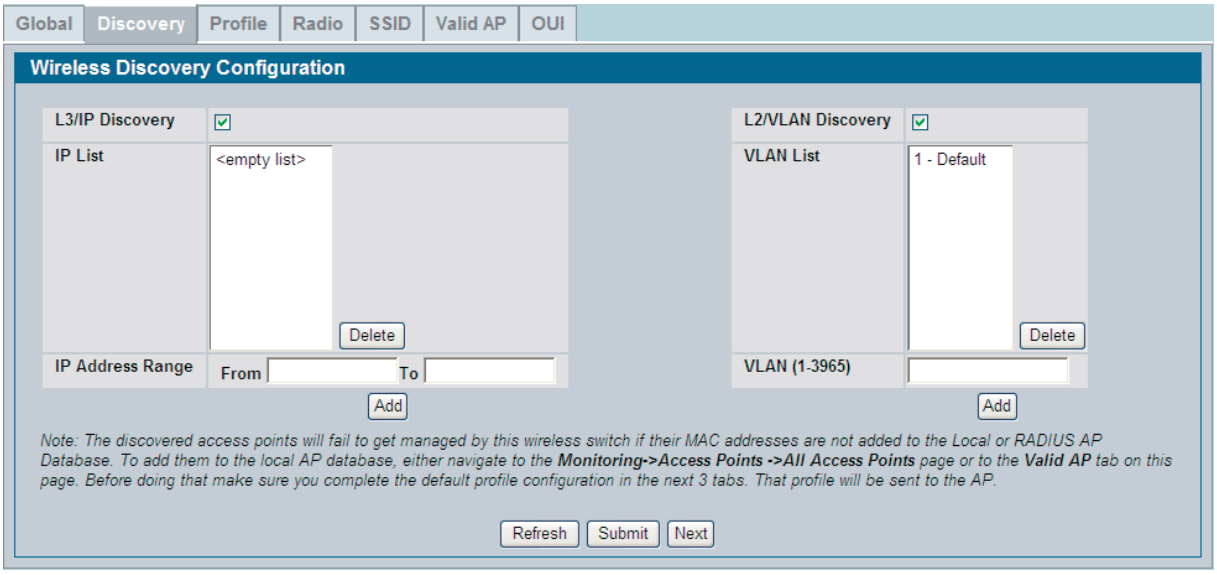


図 9-7　Wireless Discovery Configuration 画面

統合スイッチが他の WLAN デバイスを検出し通信を確立するためには、それらのデバイスに IP アドレスが設定され、他の WLAN デバイスの検出が可能で、かつ統合スイッチと互換性を持つ必要があります。

統合スイッチがアクセスポイントを検出し認証する時、スイッチはそのアクセスポイントの管理も開始します。アクセスポイントをスタンドアロンモードで設定すると、既存のアクセスポイント設定はスイッチに設定されているデフォルトのアクセスポイントプロファイル設定に置き換えられます。

L3/IP 検出

統合スイッチには、ピアスイッチとアクセスポイント用に 256 件までの IP アドレスを登録できます。スイッチは、このリストに登録されているすべての IP アドレスに対して association invitation を送信します。デバイスがこの invitation を受け取り、スイッチによる認証にパスすると、スイッチとアクセスポイント / ピアスイッチは接続を開始します。

この検出方法は、検出するデバイスが異なるサブネットに属する場合に便利です。実際、スイッチが異なるサブネット内のピアを認識するためには、ピアのレイヤ 3 検出リストに各スイッチの IP アドレスを登録する必要があります。

注意 IP アドレスリストは管理対象 Valid AP リストとは異なります。本リストにより検出されたデバイスが有効なアクセスポイントやスイッチではない場合があります。

注意 既に他の方法によってアクセスポイントが検出されている場合は、統合スイッチはそのアクセスポイントの IP アドレスに対してポーリングを行いません。

項目	説明
L3/IP Discovery	アクセスポイントおよびピアスイッチの IP ベースの検出を有効または無効にします。選択すると、IP ポーリングが有効になり、スイッチは IP リスト中の各アドレスに対して定期的にポーリングを行います。初期値は有効です。
IP List	検出用に登録されたする IP アドレスのリストです。 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。デフォルトのエントリはありません。最大 256 件までのエントリをサポートします。
IP Address Range	「IP List」に登録する IP アドレスの範囲を入力します。「From」にアドレス範囲で最小のものを入力し、「To」に範囲で最大のアドレスを入力して「Add」ボタンをクリックします。指定した範囲内のすべてのアドレスが「IP List」に追加されます。「From」アドレスと「To」アドレスの最後の 8 ビットバイトだけを変えることができます。 **注意** 1 件の IP アドレスを登録する場合は、「From」フィールドにのみ入力し、「To」フィールドは空白のままにして、「Add」ボタンをクリックします。 必要なアドレスの追加後、「Submit」ボタンをクリックしてコンフィグレーションに保存します。

スイッチが入力した IP アドレスのポーリングに成功したかどうかなど、IP アドレスに追加したデバイスの IP 検出状況を表示するためには、に対して正しく呼び出しを行っていることを確認するためには、**WLAN タブ > Monitoring > Global > IP** の順にクリックして「IP Discovery」タブを表示します。

L2/VLAN 検出

統合スイッチとアクセスポイントが同一レイヤ 2 マルチキャストドメインに存在している場合、無線デバイス検出プロトコルはとても有効な検出方法であると言えます。統合スイッチはデバイス検出が有効に設定されている各 VLAN に、定期的に Discovery メッセージを含むマルチキャストパケットを送信します。最大 16 個の VLAN 上で検出プロトコルを有効にすることができます。

デフォルトでは、VLAN 1 はアクセスポイント上で有効にされ、統合スイッチを検出する設定になっています。スイッチとアクセスポイントが同じレイヤ 2 マルチキャストドメインに存在している場合、アクセスポイントがスイッチを検出するための設定は必要ありません。また、統合スイッチは L2/VLAN 検出機能を使用して、L2 マルチキャストドメインにあるピアスイッチを検出します。

アクセスポイントは、管理用 VLAN からの Discovery メッセージのみを処理します。また、アクセスポイントは無線メディアへの Discovery メッセージ転送は行いません。

統合スイッチからアクセスポイントおよびピアスイッチの検出状況を確認することができます。スイッチ側からのアクセスポイントの検出状況を確認するためには、メニューから **WLAN タブ > Monitoring > Access Point > Managed AP Status** の順にクリックします。アクセスポイントの MAC アドレスをローカルデータベースまたは RADIUS Valid AP データベースに登録していない場合、アクセスポイントは **Monitoring > Access Point > Authentication Failed Access Points** とクリックして表示される「Authentication Failed Access Points」リストで、「No Database Entry」と表示されます。

スイッチ側からのピアスイッチの検出状況を確認するためには、**WLAN タブ > Monitoring > Peer Switch** の順にクリックします。

プロファイル（Profile タブ）

スイッチは、周波数番号および IEEE 802.11 モードなど異なるハードウェア機能を持つアクセスポイントをサポートしています。同じプロファイルを使用するアクセスポイントは、プロファイルに定義した設定がプロファイル内のすべてのアクセスポイントに対し有効になるように、同じ能力のハードウェアを持つ必要があります。異なるハードウェアプラットフォームだと、異なるソフトウェアが必要になることがあります。
リリース 1.0 では、D-Link 統合スイッチは DWL-8600AP ハードウェアタイプのみサポートしています。

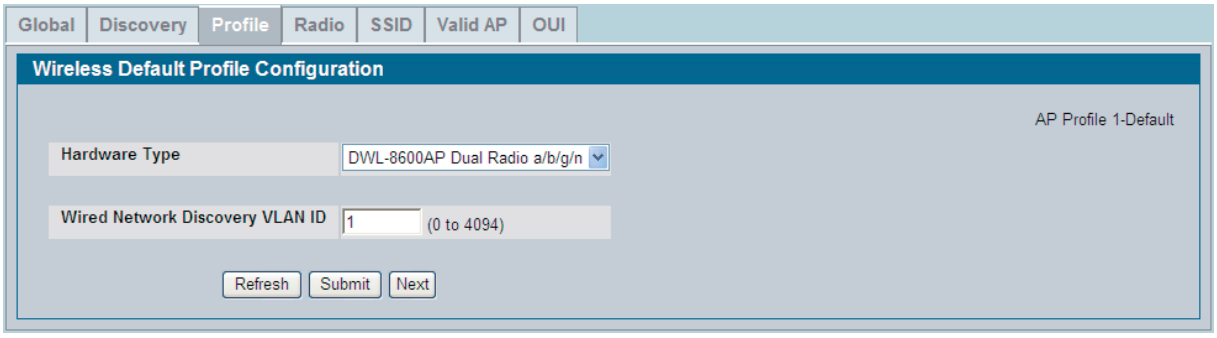


図 9-8　AP Hardware Capabilities 画面

以下の表では「Profile」画面で利用可能な項目を示します。

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。ハードウェアタイプは、製品、アクセスポイントがサポートする周波数帯域（シングルまたはデュアル）、無線がサポートする IEEE 802.11 モード a/b/g or a/b/g/n）により決定されます。 ハードウェアタイプ ID で利用可能なオプションは以下の通りです。 • DWL-8600AP Dual Radio a/b/g/n
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。

新しいプロファイルを追加するためには、**WLAN タブ > Administration > Advanced Configuration > AP Profile** の順にメニューをクリックし、有効なフィールドに新しいプロファイル名を入力して「Add」ボタンをクリックします。

周波数帯域（Radio タブ）

DWL-8600AP は、広帯域の無線クライアントと無線ネットワーク要求に対応するために 2 個の周波数帯域をサポートしています。
帯域 1 は、以下のモードの一つでブロードキャストします。
- IEEE 802.11a モード
- IEEE 802.11a と IEEE 802.11n モード
- 5 GHz IEEE 802.11n モード

帯域 2 は、以下のモードの一つでブロードキャストします。
- IEEE 802.11b と IEEE 802.11g のモード
- IEEE 802.11b、IEEE 802.11g、および IEEE 802.11n モード
- 2.4 GHz IEEE 802.11n モード

デフォルト帯域設定を行います。

WLAN タブ > Basic Setup > Radio 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。

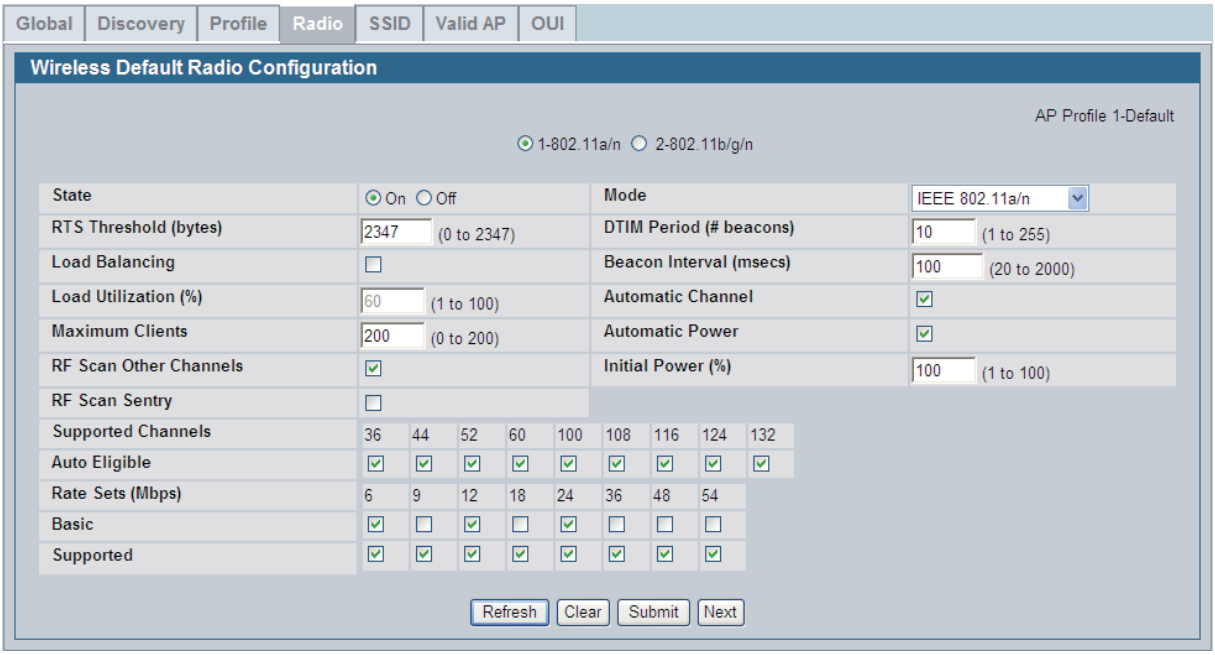


図 9-9　Wireless Default Radio Configuration 画面

以下の表は、「Basic Setup」ページの「Radio」タブを使用して無線設定をする際の各項目について説明しています。本画面の設定を変更するためには、最初に設定する帯域（1 または 2）を選択します。設定内容を変更した後は、「Submit」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。

項目	説明
1-802.11b/g/n 2-802.11a/n	設定を行う無線インタフェースを選択します。一方、IEEE 802.11a モードで運用する Radio 1 と IEEE 802.11g モードで運用する Radio 2 をサポートしています。モードを変更すると、無線インタフェースの表示も変更になります。変更した設定は選択した無線インタフェースにのみ適用されます。
State	「On」または「Off」ボタンを選択して、無線インタフェースをオンまたはオフにします。無線インタフェースをオフにすると、アクセスポイントは配下のすべての無線クライアントに向けて接続解除フレームを送信します。この手順で無線インタフェースのシャットダウンが行われ、クライアントは他のアクセスポイントとの間で接続プロセスを開始します。
Mode	無線インタフェースが使用する物理層（PHY）の標準を定義します。各無線インタフェースのモードを次から 1 つ選択します。 帯域 1 のサポートは以下の通りです。 • IEEE 802.11a は、5GHz 内の U-NII 帯域での動作と OFDM 方式の採用を規定している物理層標準です。6-54Mbps の通信速度をサポートします。 • IEEE 802.11a/n 規格は、5GHz 内の ISM 帯域で動作し、IEEE 802.11a および 802.11n 規格のデバイスのサポートも行います。IEEE 802.11n は IEEE 802.11 規格の機能を拡張した規格で、複数アンテナによる送受信を行う MIMO テクノロジを持っています。IEEE 802.11n 規格は、最大 248 Mbps のデータ範囲をサポートし、IEEE 802.11b、802.11g、802.11a 規格の屋内レンジの 2 倍近くをサポートします。 • IEEE 802.11n デバイスを使用したネットワークには、5 GHz 周波数で動作し、IEEE 802.11a や 802.11b/g 規格のデバイスをサポートする必要のない、5 GHz の IEEE 802.11n 規格が推奨されます。IEEE 802.11n 規格は、従来デバイス（802.11b/g or 802.11a）との互換性を必要としない場合には、より早いスループットを獲得することができます。 帯域 2 のサポートは以下の通りです。 • IEEE 802.11b/g 規格は、2.4 GHz 内の ISM 帯域で動作します。IEEE 802.11b は IEEE 802.11 規格の物理層標準を拡張した規格で、5.5 Mbps および 11 Mbps のデータ速度をサポートします。これは、直接拡散方式（DSSS）、周波数ホッピング方式（FHSS）、および CCK 方式を使用してより早いデータ速度を提供します。1-11Mbps の通信速度をサポートします。IEEE 802.11g 規格は、802.11b より高速化されています（最大通信速度 54Mbps）。直交周波数分割多重（OFDM）方式を採用しています。1-54Mbps の通信速度をサポートします。 • IEEE 802.11b/g/n 規格は、2.4GHz 内の ISM 帯域で動作し、IEEE 802.11b、802.11g、および 802.11n 規格のデバイスのサポートも行います。 • IEEE 802.11n 規格のデバイスを使用したネットワークで推奨されるモードは、2.4GHz 周波数で動作し、IEEE 802.11a や 802.11b/g 規格のデバイスをサポートする必要のない、2.4 GHz の IEEE 802.11n 規格です。IEEE 802.11n 規格は、従来デバイス（802.11b/g or 802.11a）との互換性を必要としない場合には、より早いスループットを獲得することができます。

項目	説明
RTS Threshold (bytes)	0 から 2347 の範囲で指定します。RTS しきい値は、RTS/CTS ハンドシェイクが実行されない MPDU の 8 オクテット数を示しています。RTS しきい値を変更すると、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に役立ちます。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)	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。1 ～ 255 の範囲で指定します。 数字はビーコンの数で表します。例えば、「1」と入力した場合、アクセスポイントの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)	ビーコン間隔。ビーコンフレームは無線ネットワークの存在を通知するために、アクセスポイントから定期的に送信されます。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。20 - 2000 の範囲から指定します。
Load Balancing	ロードバランシング機能を有効にすると、アクセスポイントにかかるトラフィック量を制御することができます。
Load Utilization (%)	その無線インタフェースでのネットワーク帯域使用率（%）のしきい値を設定します。このしきい値に使用率が達すると、アクセスポイントは新しいクライアントとの接続を拒否します。1-100 の範囲で使用率を入力します。
Maximum Clients	本アクセスポイントに一度にアクセスできるステーションの最大数を指定します。範囲は 0-200 です。
Automatic Channel	チャンネルとは、無線インタフェースがデータの送受信に使用する無線スペクトラムのある一部分を定義するものです。チャンネルの範囲およびデフォルトのチャンネルは、無線インタフェースのモードにより決定されます。アクセスポイントが再起動する時、アクセスポイントは RF エリア内で使用されているチャンネルをスキャンし、干渉のない空きチャンネルを選択します。ただし、チャンネルの状況は刻々と変化しています。 「Automatic Channel」を有効にすると、本プロファイルを適用したアクセスポイントでは、自動チャンネル選択が可能になります。自動的に、または手動で自動チャンネル選択アルゴリズムを実行させ、統合スイッチが WLAN 状態の変化に伴ってアクセスポイントのチャンネル調整をできるようにすることができます。 初期値では、グローバル自動チャンネルモードは「Manual」に設定されています。自動チャンネル選択モードを有効にする場合は、**WLAN タブ > Administration > AP Management > RF Management** の順にクリックし、チャンネルプランモードで「Fixed」または「Interval」を選択します。また、「Manual Channel Plan」画面で、手動で自動チャンネル選択アルゴリズムを実行させることも可能です。 **注意** Valid AP データベース内、または「Advanced AP Management」画面で、アクセスポイントの無線インタフェースにスタティックチャンネルを割り当てている場合は、そのアクセスポイントの無線インタフェースは自動チャンネル選択を実行できません。
Automatic Power	送信電力レベルは、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します。電力レベルが低すぎると、無線クライアントは信号検出ができなかったり、WLAN の品質低下につながります。逆に送信電力レベルが高すぎると、RF 信号は他のアクセスポイントと干渉を起こすこともあります。 自動送信電力調整機能では、独自のアルゴリズムを使用して、RF 信号がなるべく遠くの無線クライアントまで到達し、かつ他のアクセスポイントがブロードキャストする RF 信号と干渉を起こすほど遠くまでは到達しないように、自動的に調整を行います。電力レベルアルゴリズムはパケット再送エラーの有無に基づき送信電力を 10% の割合で増減します。
Initial Power (%)	初期電力レベル。自動電力調整アルゴリズムは、本フィールドで指定した送信電力の割合以下に電力を落とすことはありません。初期値の初期電力レベルは 100% になっています。つまり、自動電力調整を有効にした場合、RF 信号送信電力は増加することがあっても減少はしません。単位は RF 信号の最大送信電力に対するパーセンテージ（%）です。
RF Scan Other Channels	アクセスポイントは RF スキャンを実行し、自分の通信範囲内の他の無線デバイスの情報を集め、統合スイッチに報告します。「Scan Other Channels」オプションを選択すると、動作チャンネルから外れて他のチャンネルのスキャンを行います。このモードを有効にすると、ユーザトラフィックの遮断が発生し、特に音声通信中はそれが顕著になります。「Scan Other Channels」オプションを外すと、アクセスポイントは動作中のチャンネルだけをスキャンします。
RF Scan Sentry	無線インタフェースを Sentry（監視）モードで使用します。 チェックボックスを選択すると、RF スキャンを専門に実行します。無線インタフェースは送信されてくるビーコンフレーム、およびクライアントと他のアクセスポイント間のトラフィックを受動的に学習していますが、クライアントからの接続には応じません。Sentry（監視）モードでは、すべての VAP は無効になります。アクセスポイントや無線インタフェースの監視を行うように配置されたネットワークは、ネットワーク上のデバイスをより早く検出し、より徹底的にセキュリティ分析を行うことができます。 本モードでは、スキャンはチャンネル間を移動して行われます。各チャンネルに費やす時間は「RF Scan Duration（スキャン時間）」によって制御されます。初期値は 10 ミリ秒です。
Supported Channels	画面で現在選択されている無線モードのために、「Global Wireless Settings」画面で設定された国に対し、サポートされているチャンネルを表示します。
Auto Eligible	各チャンネルの下にある「Auto Eligible」オプションを選択すると、そのチャンネルを自動チャンネル割り当てに設定します。
Rate Sets (Mbps)	アクセスポイントがサポートする通信速度（Supported rate set）およびアクセスポイントが通知をする速度（Basic rate set）を指定します。単位は Mbit/ 秒です。

項目	説明
Basic	アクセスポイントと接続しているすべてのステーションがサポートしなくてはならないデータ速度を示します。
Supported	アクセスポイントがサポートする通信速度です。複数の速度を選択することができます。 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。

WLAN タブ > Administration > Advanced Configuration > AP Profile の順にメニューをクリックします。設定するプロファイルのリンクをクリック後、「Radio」タブをクリックし、「Access Point Profile Radio Configuration」にアクセスすると、追加の項目を設定可能です。

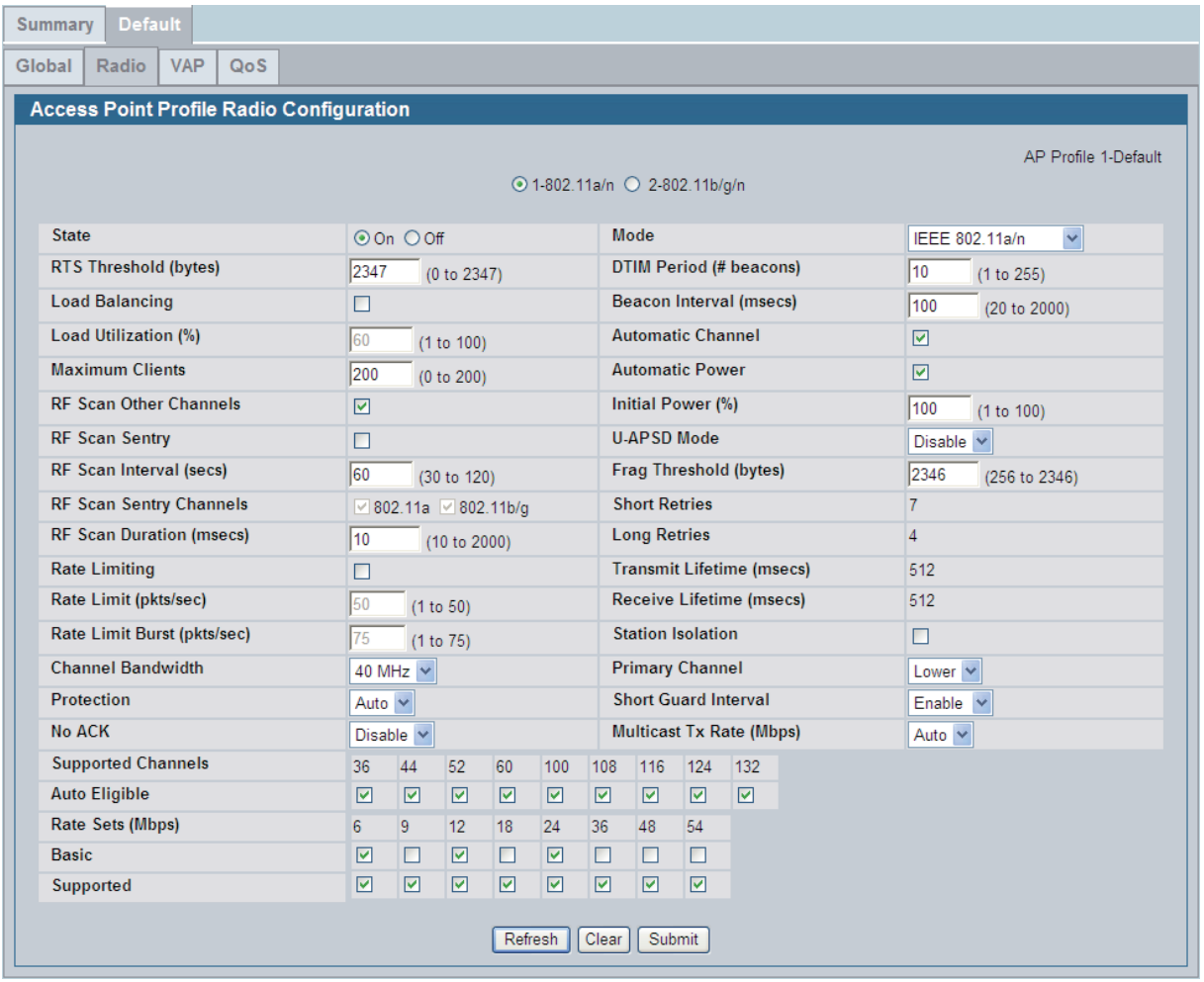


図 9-10　Access Point Profile Radio Configuration 画面

以下の表は「Advanced Configuration」メニューで使用できるアクセスポイント帯域の項目について説明します。

項目	説明
RF Scan Interval	RF スキャン中のアクセスポイントがチャンネルを変更する間隔を指定します。
RF Scan Sentry Channels	無線インタフェースは 802.11b/g（2.4 GHz）周波数帯、802.11a（5 GHz）周波数帯、または両方の周波数帯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周波数帯を選択します。 **注意**　周波数帯の選択は、「RF Scan Sentry」選択時のみ指定します。DWL-8600AP の 2 つの無線インタフェースは両方の周波数をスキャンできます。
RF Scan Duration	本フィールドは RF スキャン時に他のチャンネルのスキャンに要する時間を指定します。単位はミリ秒です。
Rate Limiting	マルチキャストおよびブロードキャスト通信速度制限機能を有効にすると、ネットワーク内で送信されるパケット数を制限することで、ネットワーク全体の性能を改善します。初期値は無効です。 **注意**　利用可能な速度制限値は多くの環境では大変低いので、この機能を有効にすることは推奨しません。
Rate Limit	マルチキャストおよびブロードキャストトラフィックに設定する速度制限値を入力します。制限は、必ず 1 以上 50 パケット / 秒以下で設定します。この制限値を下回ったトラフィックは、常に適切な送信先に従って送信されます。 初期値および最大速度設定は 50 パケット / 秒です。「Rate Limiting」機能が無効の場合、このフィールドは無効になります。

項目	説明
Rate Limit Burst	速度制限バースト値の設定は、すべてのトラフィックがその速度制限値を超えるまでのトラフィックバースト値を決定します。バースト値の制限上で、ネットワーク速度制限値を設定したトラフィックが間欠的にバーストするのを許可します。 初期値および最大速度制限バースト値設定は 75 パケット / 秒です。「Rate Limiting」機能が無効の場合、この項目は無効になります。
Channel Bandwidth	IEEE 802.11n 規格は、従来モデルで利用可能な 20MHz に加え、40MHz の広帯域チャンネルの使用が可能です。 40MHz の広帯域チャンネルは、より高速なデータ速度が可能ですが、2.4GHz 帯および 5GHz 帯のデバイスが利用可能なチャンネルを残しません。40MHz オプションは IEEE 802.11a/n 規格のモデルで、20 MHz は IEEE 802.11b/g/n 規格のモデルで、それぞれデフォルトで有効になっています。この設定は、20-MHz チャンネルのデバイスのチャンネル周波数帯域使用を制限するために使用することもできます。
Protection	保護機能には、IEEE 802.11 規格の通信が従来のデバイスやアプリケーションと干渉を起こさないことを保証するためのルールが含まれます。初期設定では、これらの保護メカニズムは有効（Auto）です。保護機能を有効にすると、従来デバイスがアクセスポイントの範囲内にある場合に保護メカニズムが呼び出されます。 これらの保護メカニズムは無効（Off）にすることもできますが、保護機能を無効にすると、帯域内にある従来のクライアントまたはアクセスポイントの IEEE 802.11n 規格の通信に影響を与える可能性があります。保護機能は IEEE 802.11b/g 規格のモデルでも利用可能です。このモードで保護機能を有効にすると、IEEE 802.11b 対応のクライアントおよびアクセスポイントを IEEE 802.11g 規格の通信から保護します。
No ACK	「Enable」を選択して、アクセスポイントが QosNoAck フレームをサービスクラス値としてアクノリッジしないように設定します。
U-APSD Mode	「Enable」を選択して、電源管理方法である Unscheduled Automatic Power Save Delivery（U-APSD）への対応を有効にします。アクセスポイントを経由して VoIP 電話でネットワークにアクセスする場合、「U-U-APSD」を推奨します。「U-APSD」では、クライアントがトリガフレームを送信すると、アクセスポイントがバッファフレームをクライアントに送信します。フレーム送信はアクセスポイントではスケジュールしません。クライアントが起動した時にトリガを送信すればバッファフレームを受け取ることができるので、この方法は有益です。
Frag Threshold	フラグメントしきい値。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。 256 ～ 2345 の範囲で指定します。本フィールドで指定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 という値は、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、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。1 ～ 255 の範囲から指定します。
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。1 ～ 255 の範囲から指定します。
Transmit Lifetime	最初の MSDU 送信から送信リトライを終了までの時間を指定します。単位はミリ秒です。
Receive Lifetime	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を指定します。単位はミリ秒です。
Station Isolation	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。無線クライアント間の通信は行えなくなりますが、ネットワークの無線クライアントと有線デバイス間のデータトラフィックは許可します。初期値は無効です。
Primary Channel	この設定は、選択チャンネルの帯域幅が 40MHz に設定されている場合にのみ、変更できます。40MHz のチャンネルは、周波数ドメインで隣接する 2 つの 20MHz チャンネルで構成されていると見なされます。これら 2 つの 20MHz チャンネルは、プライマリおよびセカンダリチャンネルと呼ばれます。プライマリチャンネルは、20MHz チャンネルの周波数帯域をサポートする IEEE 802.11n 対応のクライアントと従来クライアントだけに使用されます。 この設定を使用して 40MHz 帯域内で、上位、または下位の 20MHz チャンネルをプライマリチャンネルとして設定します。
Short Guard Interval	ガードインターバルは、OFDM シンボルの間のデッドタイム（単位はナノ秒）です。ガードインターバルにより、シンボル間干渉（ISI）および 搬送波間干渉（ICI）を防止します。802.11n モードは、このガードインターバルで、802.11a および 802.11g 規格から 800（ナノ秒）から 400（ナノ秒）に低減を行うことが可能です。ガードインターバルの削減でデータスループットを約 10% 改善することができます。 以下の 1 つを選択します。 • Enable - アクセスポイントは、同様に短いカードインターバルをサポートするクライアントと通信を行う際、400（ナノ秒）のガードインターバルを使用してデータを送信します。 • Disable - アクセスポイントは、800（ナノ秒）のガードインターバルを使用してデータ送信を行います。
Multicast Tx Rate (Mbps)	無線インタフェースがマルチキャストフレームを送信する 802.11 の速度を選択します。単位は Mbps です。 5 GHz 帯域における最低速度は 6 Mbps です。

SSID 設定（SSID タブ）

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 16 つまでの VAP を定義できます。

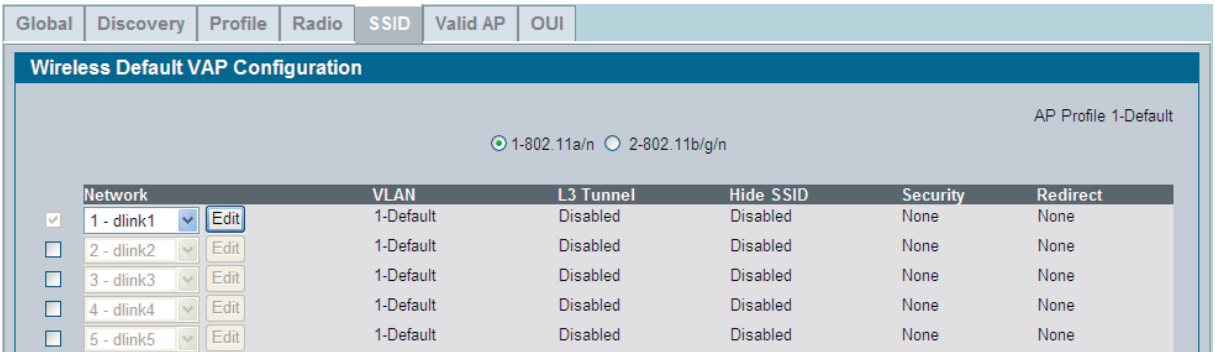


図 9-11　Wireless Default VAP Configuration 画面

イーサネットの VLAN と同様に、無線 LAN は VAP により複数のブロードキャストドメインに分割することができます。各無線クライアントにとって、各 VAP は 1 台の物理アクセスポイントと同じように見えます。しかし、それぞれの VAP は同じチャンネルを使用するため、1 台のアクセスポイント上のネットワーク間では RF 干渉が発生するリスクがありません。

VAP の使用により、ブロードキャストやマルチキャストのトラフィック管理が容易になり、ネットワークのパフォーマンスも向上します。また、VAP ごとに異なるセキュリティ方式を設定することも可能です。

VAP は " 物理的な " エンティティ（存在）です。各 VAP は 1 つの MAC アドレスに対応します。一方、ネットワークは各 VAP に対して割り当てる " 論理的な " エンティティです。ネットワークはネットワーク番号と SSID で認識します。SSID はネットワークごとに固有のものである必要はありません。
1 つのネットワークの作成または変更を行い、それを 1 つまたはそれ以上の VAP に割り当てることができます。これにより、異なるプロファイルのネットワークを、すべての設定をやり直すことなく構成することができます。複数の VAP に割り当てたネットワーク設定を編集する場合は、そのネットワークを使用するすべての VAP に対して編集を行います。

仮想アクセスポイント設定の管理

デフォルト AP プロファイルでは初期値各帯域で 1 つの VAP が有効になっています。デフォルト VAP は、SSID に「dlink1」を使用しており、無線クライアントからの VAP 接続を防ぐセキュリティを使用していません。他の VAP を有効にするためには、VAP の隣のチェックボックスにチェックを入れます。（図 9-11 参照）。有効にした VAP にはプルダウンメニューからネットワーク（SSID）を選択することができます。ネットワーク設定内容を変更するためには「Edit」ボタンをクリックします。

以下の表では SSID 設定画面の各フィールドについてを示します。

項目	説明
Radio 1 Radio 2	VAP の設定は 802.11a と 802.11g について別々に行います。VAP を有効にする前に、設定する無線インタフェースを選択します。
Network	選択した無線インタフェース上の対応する VAP を有効、または無効にします。有効にした場合、メニューから VAP に割り当てたいネットワークを選択します。本スイッチには 64 個の異なるネットワークが登録可能で、それらを複数の無線インタフェースおよび VAP インタフェースに適用できます。初期値では 16 個のネットワークが登録済みで、各無線インタフェースの VAP に割り当てられています。1 つの無線インタフェース上の VAP を有効にしても、他の無線インタフェース上の VAP は自動的に有効にはなりません。 **注意**　デフォルト VAP および VAP 0 は無効にできません。 新規のネットワークを登録するためには、**WLAN タブ > Administration > Advanced Configuration Networks** を順にクリックしてください。
Edit	選択したネットワークの設定を変更する場合、本ボタンをクリックします。「Wireless Network Configuration」ページが表示されます。
VLAN	VAP の VLAN ID を表示します。設定内容を変更するためには、「Edit」ボタンをクリックします。
L3 Tunnel	VAP において L3 トンネリングが有効または無効であるかを表示します。設定内容を変更するためには、「Edit」ボタンをクリックします。 **注意**　L3 トンネリングが有効である時、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。
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。設定内容を変更するためには、「Edit」ボタンをクリックします。
Security	VAP の現在のセキュリティ設定を表示します。設定内容を変更するためには、「Edit」ボタンをクリックします。
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。

デフォルトネットワークの設定

各ネットワークは SSID によって識別されます .SSID は英数字のキーで無線 LAN を識別します。統合スイッチ上に 64 個の異なるネットワークを設定することができます。各ネットワークに固有の SSID を、または複数のネットワークに同一の SSID を設定することも可能です。

VAP 設定用画面の「Edit」ボタンをクリックすると、以下の図で示すような無線ネットワーク設定用画面が表示されます。

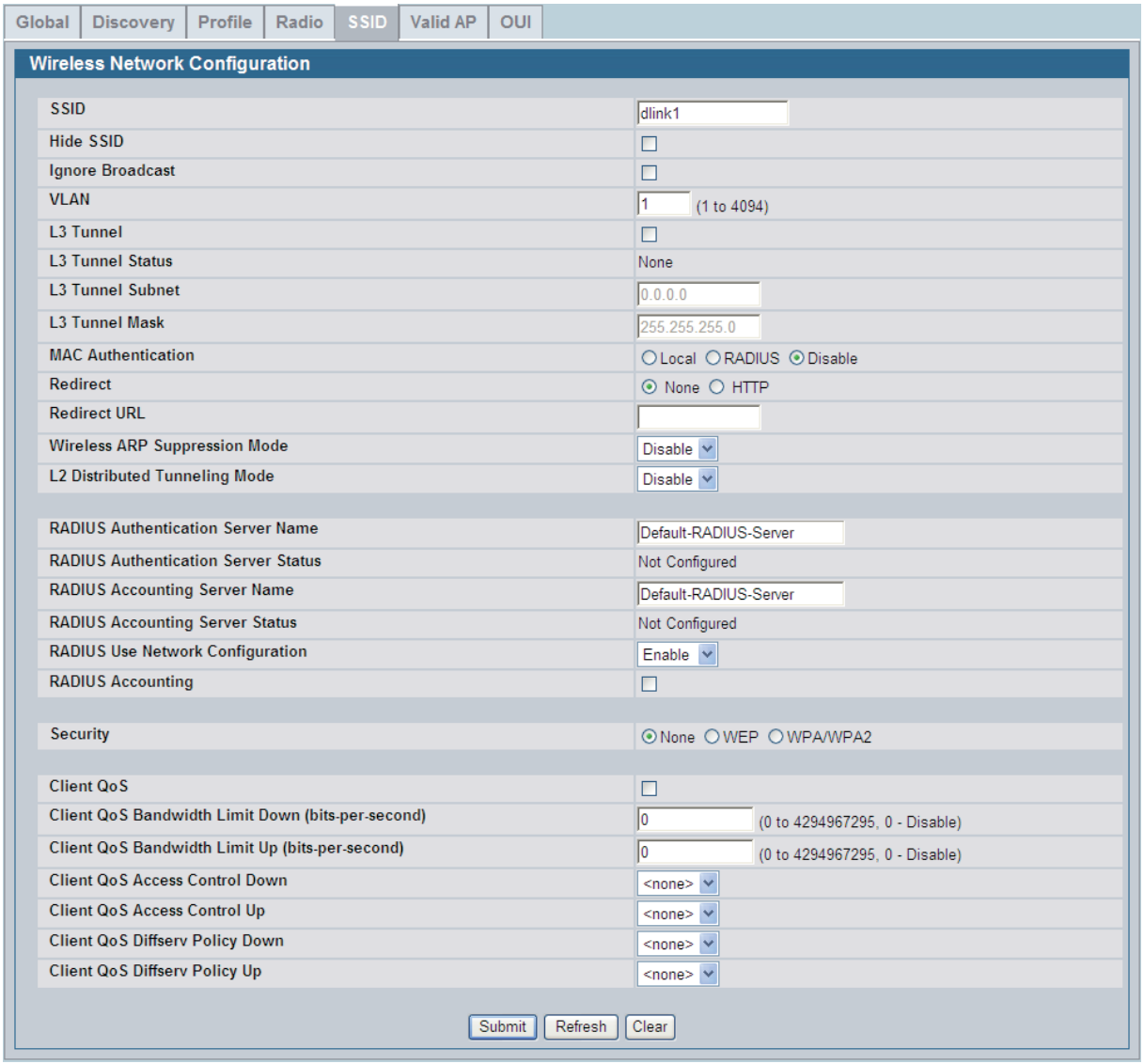


図 9-12　Wireless Network Configuration 画面

以下の表は「Wireless Network Configuration」ページの各項目の詳細を説明します。

項目	説明
SSID	無線クライアントは、SSID によって無線ネットワークを識別します。SSID とは無線 LAN を一意に識別する半角英数字から成るキーです。SSID は 32 文字以内で指定し、使用する文字に制限はありません。
Hide SSID	SSID を非公表にします。SSID のブロードキャストを無効にすることにより、クライアントによるアクセスポイントの自動検出を阻止します。SSID を隠すと、クライアント側の「使用可能ネットワークリスト」にネットワーク名が表示されなくなります。その代わりに、クライアントは接続前に、サプリカントに接続する相手の正しいネットワーク名を登録する必要があります。 SSID のブロードキャストを無効にすることで、あるクライアントが偶然ネットワークに入ってくることを防ぐことができます。しかし、ハッカーからの簡単な攻撃を防いだり、暗号化されていないトラフィックを監視するためには十分ではありません。 本機能は、ゲストネットワークのような、クライアントからの接続が容易であることに重点を置いた、比較的無防備なネットワークに対して、最低限のレベルの防御を提供するものです。
Ignore Broadcast	無線クライアントがプローブ要求をすべての利用可能な SSID にブロードキャストする場合、本機能でアクセスポイントがプローブ要求に返答するかどうかをコントロールします。 • アクセスポイントがクライアントのプローブ要求に返答するのを禁止します。 • 本機能を無効にすると、アクセスポイントはクライアントのプローブ要求に返答するのを許可されます。

項目	説明
VLAN	仮想 LAN は、ソフトウェアベースで 1 つのネットワーク上のデバイスを論理的にグループ分けしたもので、あたかも 1 つの物理ネットワークであるかのような動きをします。VLAN 内のノードはリソースや帯域を共有し、ネットワーク内で独立しています。 D-Link 統合スイッチは無線 VLAN 設定をサポートしています。各 VAP を 1 つの VLAN 上に配置したり、他の VAP と同一の VLAN に所属させることもできます。 無線クライアントが SSID を使用してアクセスポイントに接続する場合、アクセスポイントはクライアントのトラフィックに、ここで入力した VLAN ID をタグ付けします。デフォルトではすべてのネットワークは VLAN 1 であり、デフォルトでタグなしになっています。 **注意** ここに設定した VLAN ID は、RADIUS サーバ側に設定されているアクセスポイントの VLAN ID に上書きされます。つまり、ネットワークが無線クライアントを VLAN に割り当てるために RADIUS サーバを使用している場合、その無線クライアントは RADIUS サーバからの VLAN ID を使用し、VAP に設定されている VLAN ID は無視します。
L3 Tunnel	L3 トンネル機能を有効または無効にします。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 トンネリングの状況を表示します。トンネリングの設定を正しくするためには、ルーティングを有効にし、スイッチにはトンネルサブネット内のルーティングインタフェース IP アドレスを持つ必要があります。トンネリング状況は、以下の 4 つのうちのいずれかになります。 • None - L3 トンネリング機能が無効です。またはネットワークに AP プロファイルが関連付けられていません。 • Configured - 設定済み • Not Configured-Routing Disabled - 設定なし（ルーティング無効） • Not Configured-No Routing Interface - 設定なし（ルーティングインタフェースなし）
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 トンネルマスク。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。
MAC Authentication	MAC 認証。MAC 認証を有効にしている時、無線クライアントがネットワークに接続するために、アクセスポイントにより認証を受ける必要があります。MAC 認証の使用は、クライアントの MAC アドレスを以下のいずれかのデータベースに登録して行います。 • Local • RADIUS データベースにクライアントに対するデフォルトのアクションを「accept」「deny」、または **WLAN タブ > Administration > Advanced Configuration > Global** の順にクリックして設定したグローバルアクションを使用する「use the global action」から設定します。 MAC 認証は、特定の MAC アドレスのクライアントへのアクセスを「grant」または「deny」する「Open」モードで動作するネットワークにおいて役立ちます。MAC 認証は、MAC 認証が 802.1X 認証に先立ち実行される場合において、802.1X セキュリティメソッドと共に使用することもできます。
Redirect	HTTP を選択すると、無線クライアントをカスタム Web 画面にリダイレクトします。 本モードが有効の場合、無線クライアントがアクセスポイントを使って接続し、インターネットにアクセスする Web ブラウザを開くと、そのユーザは指定した URL にリダイレクトされます。 カスタム Web 画面は、必ず外部の Web サーバに設定する必要があります。また、会社ロゴやネットワークの使用ポリシーなどの情報を載せることができます。 **注意** 無線クライアントは、アクセスポイントを使用して接続した場合にのみ、外部の Web サーバにリダイレクトされます。 リダイレクト機能により、キャプティブポータル機能を実行することができます。キャプティブポータルは Wi-Fi 接続のホットスポットで頻繁に使用されており、ホットスポットのプロバイダにブランディングを提供し、またユーザがクリックしないとインターネット接続ができない法的注意書きの表示を行います。
Redirect URL	すべてのイニシャル HTTP 接続がリダイレクトされる URL。HTTP をリダイレクトタイプとして選択した場合にのみ、本フィールドは表示されます。

項目	説明
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を確保するのに役立ちます。パワーセーブ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	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、有効、または無効にします。 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インタフェースおよび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されるようになった後、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、新しく配置されたネットワークで 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、ホームのアクセスポイントを管理するスイッチが故障した場合、関連するアクセスポイント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.** 関連するアクセスポイント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、すべての無線インタフェースをダウンさせ、クライアントは接続を切断されます。
RADIUS Authentication Server Name	VAP がアクセスポイントとユーザの認証に使用する RADIUS サーバ名を入力します。最大 32 文字のテキストを含むことができます。スペース、ハイフン、およびアンダースコアを入力することができます。 無線ネットワークで設定した RADIUS 情報はすべて、「Wireless Global Configuration」画面で設定したグローバル RADIUS 情報を上書きします。 スイッチは RADIUS クライアントとして機能して、アクセスポイントおよび無線クライアントのためにすべての RADIUS トランザクションを行います。
RADIUS Authentication Server Status	RADIUS 認証サーバの VAP 設定状況を示します。RADIUS サーバ情報を設定するためには、**LAN タブ > Security > RADIUS > Server Configuration** の順にメニューをクリックします。
RADIUS Accounting Server Name	VAP が無線クライアントの接続および切断状況を報告するのに使用する RADIUS サーバ名を入力します。最大 32 文字のテキストを含むことができます。スペース、ハイフン、およびアンダースコアを入力することができます。 無線ネットワークで設定した RADIUS 情報はすべて、「Wireless Global Configuration」画面で設定したグローバル RADIUS 情報を上書きします。
RADIUS Accounting Server Status	RADIUS アカウンティングサーバの設定状況を示します。RADIUS アカウンティングサーバ情報を設定するためには、**LAN タブ > Security > RADIUS > Accounting Server Configuration** の順にメニューをクリックします。
RADIUS Use Network Configuration	VAP がネットワークの RADIUS 設定とグローバル RADIUS 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 サーバを使用します。 • Disable -「Wireless Global Configuration」画面で設定した RADIUS サーバを使用します。
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	デフォルト AP プロファイルには、初期状態ではセキュリティが使用されていません。ネットワークを保護するために、セキュリティ方式を指定して、権限のないクライアントのネットワーク侵入を防ぐことを強くお勧めします。以下の WLAN ネットワークセキュリティオプションが選択できます。 • None • WEP • WPA/WPA2 • WPA Personal • WPA Enterprise セキュリティ方式として WEP または WPA/WPA2 を選択すると、ダイアログボックスが表示されネットワークセキュリティの変更を確認します。「OK」ボタンをクリックすると、新しいフィールドが表示され、変更したネットワーク設定内容はスイッチに反映されます。 WEP または WPA/WPA2 を選択した場合、「アクセスポイントのセキュリティ設定」（289 ページ）のセキュリティメカニズムを参照して、さらに設定を行うこともできます。
Client QoS	本機能により、スイッチは、アクセスポイントに接続する無線クライアントにアクセスコントロールリスト（ACL）および DiffServ ポリシーを適用して、スイッチの QoS 機能を無線ドメインに拡大できるようになります。 選択すると、前の項目で SSID 設定したアクセスポイントと接続する無線クライアントの QoS 機能を有効にします。 本機能は、ネットワークに接続する無線クライアントの QoS のある局面、例えば、各クライアントが送受信を許可される帯域幅やトラフィックのタイプなどをコントロールします。HTTP トラフィックや特定のサブネットからのトラフィックなどのような、トラフィックの一般的なカテゴリを制御するために、1 つまたは複数の VAP に割り当てるアクセスコントロールリストを設定することができます。クライアント QoS により、クライアントごとに DiffServ を使用して様々な詳細なフローを調整する設定も行うことが可能です。 アクセスコントロールリストは、ルールと呼ばれる許可と拒否の条件を集めたものであり、認証されていないユーザが特定のリソースに接続することを拒否し、認証されているユーザには許可をすることでセキュリティを提供します。アクセスコントロールリストでは、ネットワークリソースに接続しようとする不当な試みをすべて拒否することができます。 各アクセスコントロールリストは、最大 10 個のルールから成り、無線クライアントから送信されたトラフィックや、無線クライアントにより受信されるトラフィックに適用されます。各ルールは、特定のフィールドのコンテンツがパケットの送信を許可するのか、あるいは拒否するのかを指定します。ルールは各種の基準に基づき、パケット内の 1 つまたは複数のフィールド、例えば送信元、送信先 IP アドレス、送信元、送信先 L4 ポート、あるいはパケット内のプロトコルなどに適用されます。 DiffServ ポリシーは、一般的な詳細フローの定義および処理特性を設定するのに役立つツールで、各無線クライアントがネットワーク認証された場合にインバウンド、アウトバウンド両方に適用することができます。パケットは、定義した基準に従って分類、処理されます。分類基準は、クラスによって定義されます。処理はポリシー属性によって定義されます。
Client QoS Bandwidth Limit Down (bits - per - second)	アクセスポイントから無線クライアントへの送信速度（bps）を決める最大帯域幅を入力します。範囲は 0-4294967295（bps）です。 0 以外の値を指定すると、アクセスポイントが使用できるように 64Kbps に近くなるように切り捨てられますが、64Kbps 以下になることはありません。0 は、最大帯域幅制限が実施されないことを意味します。
Client QoS Bandwidth Limit Up (bits - per - second)	無線クライアントからアクセスポイントへの送信速度（bps）を決める最大帯域幅を入力します。範囲は 0-4294967295（bps）です。 0 以外の値を指定すると、アクセスポイントが使用できるように 64Kbps に近くなるように切り捨てられますが、64Kbps 以下になることはありません。0 は、最大帯域幅制限が実施されないことを意味します。
Client QoS Access Control Down	アウトバウンド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。メニューには既存の IP アクセスリストのみがアクセスリストタイプと共に表示されます。 IP アクセスリストの作成は、**LAN タブ > Access Control Lists** の順にクリックして行います。 • 「IP ACL Configuration」画面で、「new standard」、「extended」、または「named」IP アクセスコントロールリストを作成します。 • 「IP ACL Rule Configuration」画面では、パケットの一致基準、各ルールに対し拒否または許可のアクションを定義する 1 つ以上のルールを作成します。 パケットがアウトバウンドのインタフェースに到達すると、そのパケットに合致するアクセスコントロールリストが照査されます。パケットは、許可された場合には送信され、拒否された場合には廃棄されます。

項目	説明
Client QoS Access Control Up	インバウンド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。メニューには既存の IP アクセスリストのみがアクセスリストタイプと共に表示されます。 IP アクセスリストの作成は、**LAN タブ > Access Control Lists** の順にクリックして行います。 • 「IP ACL Configuration」画面で、「new standard」、「extended」、または「named」IP アクセスコントロールリストを作成します。 • 「IP ACL Rule Configuration」画面では、パケットの一致基準、各ルールに対し拒否または許可のアクションを定義する 1 つ以上のルールを作成します。 アクセスポイントがパケットを受信すると、そのパケットに合致するアクセスコントロールリストが照査されます。パケットは、許可された場合には送信され、拒否された場合には廃棄されます。
Client QoS DiffServ Policy Down	アウトバウンド方向のトラフィックに適用する DiffServ ポリシー名を選択します。メニューには既存の DiffServ ポリシーのみが表示されます。 DiffServ ポリシーの作成は、**LAN タブ > QoS > Differentiated Services** の順にクリックして行います。 • 「Class Configuration」画面で、クラスを作成し、クラス基準を定義します。 • 「Policy Configuration」画面で、ポリシーを作成し、クラスを関連づけします。 • 「Policy Class Definition」画面では、パケットがクラス基準に一致した場合、そのパケットへのアクションを決めるポリシーステートを定義します。
Client QoS DiffServ Policy Up	アクセスポイントに送信されるインバウンド方向のトラフィックに適用する DiffServ ポリシー名を選択します。メニューには既存の DiffServ ポリシーのみが表示されます。 DiffServ ポリシーの作成は、**LAN タブ > QoS > Differentiated Services** の順にクリックして行います。 • 「Class Configuration」画面で、クラスを作成し、クラス基準を定義します。 • 「Policy Configuration」画面で、ポリシーを作成し、クラスを関連づけします。 • 「Policy Class Definition」画面では、パケットがクラス基準に一致した場合、そのパケットへのアクションを決めるポリシーステートを定義します。

無線ネットワーク設定の入力を終了後、「Submit」ボタンをクリックして設定を保存します。

アクセスポイントのセキュリティ設定

デフォルト AP プロファイルには、初期状態でセキュリティが設定されていません。ネットワークを保護するために、セキュリティ方式を指定し、権限のない無線クライアントのネットワーク侵入を防ぐことを強くお勧めします。

以下の図が示すように、「Wireless Network Configuration」画面で WLAN セキュリティ方式として「None」、「WEP」、「WPA/WPA2」から 1 つ選択します。デフォルトでは「None」が選択されています。

図 9-13　Wireless Network Configuration - AP Security Option 画面

以下の項では、各セキュリティ方式について説明します。

セキュリティなし

セキュリティモードに「None」を選択すると、そのアクセスポイントに対してそれ以上の設定は不必要です。本モードでは、アクセスポイントと接続する無線クライアント間のデータ転送には暗号化が行われず、どんな無線クライアントでもアクセスポイントに接続が可能となります。

本セキュリティモードは初期のネットワーク設定時、または問題解決時の使用に便利です。しかし、本モードの選択は、安全性が極めて低いため、内部用ネットワークでの通常使用にはお勧めできません。

スタティック / ダイナミック WEP の使用

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。本セキュリティ方式を選択すると、ネットワーク上のすべての無線クライアントやアクセスポイントは、データの暗号化に 64 ビット（秘密鍵 40 ビット + 初期化ベクタ（IV）24 ビット）、または 128 ビット（秘密鍵 104 ビット +IV 24 ビット）の共有鍵を用います。

スタティック WEP は最も安全なモードではありませんが、外部ユーザが暗号化されてない無線トラフィックを探し出すのを防止することは可能であり、セキュリティモードに「None」を設定するよりもネットワーク保護に役立ちます。

ダイナミック WEP はスタティック WEP よりも安全性が高くなりますが、自動生成したキーの管理のために RADIUS サーバが必要となります。

WEP は無線ネットワーク中を移動するデータをスタティックキーを基に暗号化します（暗号化のアルゴリズムは RC4 と呼ばれるストリーム暗号です）。

セキュリティモードとして WEP を選択すると、以下の図に示すような追加項目が表示されます。

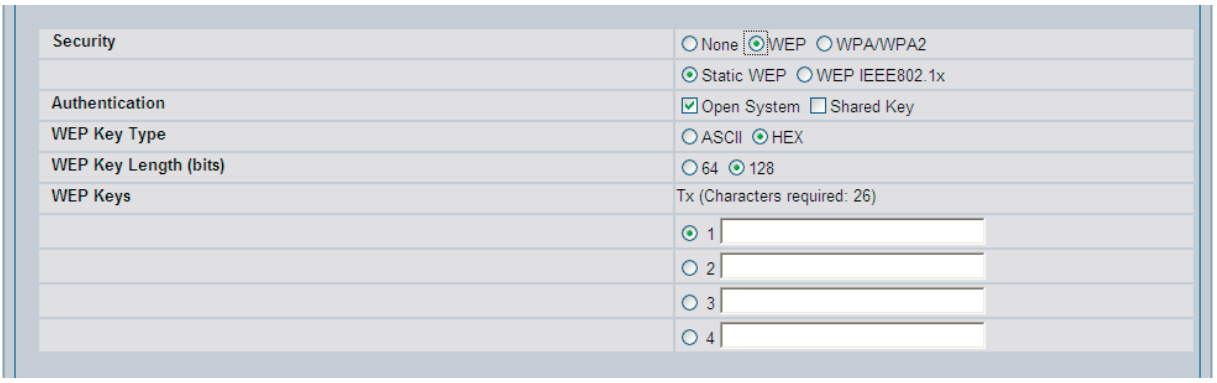


図 9-14　Wireless Network Configuration - Static WEP Configuration 画面

以下の表に WEP の設定オプションの内容を示します。

項目	説明
Static WEP or WEP IEEE 802.1X	Static WEP はスタティックキーを管理し使用します。無線クライアントとアクセスポイントの両方にデータを暗号化するための同じキーを手動で設定します。ダイナミック WEP IEEE 802.1X では、クライアントからアクセスポイントへのトラフィックの暗号化に動的に生成されたキーを使用します。 WEP IEEE 802.1X は Static WEP より安全ですが、キーの管理のために RADIUS サーバが必要になります。WEP IEEE 802.1X を選択すると、画面が更新されます。その他設定が必要な項目はありません。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。 統合スイッチのグローバル RADIUS サーバ設定についての詳細は、「無線グローバル基本設定（Global タブ）」（274 ページ）を参照してください。
Authentication	認証タイプを選択します。 • Open System - 認証を行いません。 • Shared Key - 共通鍵。簡単なユーザ認証を行いますが、WEP キーをテキスト形式でクライアントに配布するため、オープンシステムより安全性が低いと考えられています。 • Both - WEP クライアントのみが認証されます。
WEP Key Type	ラジオボタンでどちらかのキー種別を選択します。 • ASCII - 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 - 16 進数。0-9 と A-F を含みます。
WEP Key Length (bits)	ラジオボタンで以下の WEP キー長を選択します。 • 64 bits • 128 bits
Tx	送信キーインデックスは、アクセスポイントがどの WEP キーを送信するデータの暗号化に使用するかを示します。キー番号の左側にあるラジオボタンをクリックして送信キーを選択します。xx ページの図 xx の例では、送信キー 3 を選択しています。
WEP Keys	4 つまでの WEP キーを登録できます。各テキストボックスに、各キーの文字列を入力します。これらは RC4 WEP キーでアクセスポイントを使用するクライアントと共有します。各キーには同じ文字数を使用します。登録するキーの文字数はキータイプとキー長によって異なります。入力するキーの文字数は以下の通りです。 • 64 bit - ASCII : 5 文字、Hex : 10 文字 • 128 bit - ASCII : 13 文字、Hex : 26 文字 各クライアントは、アクセスポイント用に指定したのと同じスロットに、同じ WEP キーから 1 つ登録します。

スタティック WEP 設定時のルール

スタティック WEP を使用する際は、以下のルールが適用されます。

- すべてのクライアントは WLAN セキュリティを「WEP」に設定し、アクセスポイントからクライアントへの送信データを復号するために、アクセスポイントで指定されている WEP キーのうちの 1 つを持つ必要があります。
- アクセスポイントは、クライアント側からのデータを復号するために、クライアントがアクセスポイントへの送信に使用するすべてのキーを持つ必要があります。
- すべてのノード（アクセスポイントとクライアント）で、キーは同じスロットを使用する。例えばアクセスポイントが "abc12" キーを WEP キー 3 と定義したならば、クライアント側も同じキーを WEP キー 3 と定義する必要があります。
- クライアントは、アクセスポイントへのデータ送信用にそれぞれ異なるキーを使用できます。（複数のクライアントが同じキーを使用することもできますが、その場合は他のクライアントからのデータを解読できるため、安全性は低くなります。）
- 無線クライアントソフトウェアによっては、複数の WEP キーを登録し、" 送信キーインデックス " を定義し、異なるキーを切り替えてデータを暗号化するように設定をすることもできます。これにより、近接するアクセスポイントがお互いの通信内容を解読できなくなります。
- アクセスポイントとクライアント間で、64 ビット、128 ビット、および 152 ビットの WEP キーを混在させることはできません。

WPA/WPA2 パーソナル / エンタープライズの使用

WPA と WPA2 は Wi-Fi Alliance により発表された IEEE 802.11i 標準に準拠した暗号化方式規格です。本規格は AES-CCMP および TKIP というメカニズムを採用しています。WPA/WPA2 パーソナルは事前共有キーを用いて証明書の初期チェックします。WPA/WPA2 エンタープライズでは RADIUS サーバを使用してユーザ認証します。

セキュリティモードとして「WPA/WPA2」を選択すると以下の図に示すような追加フィールドが表示されます。

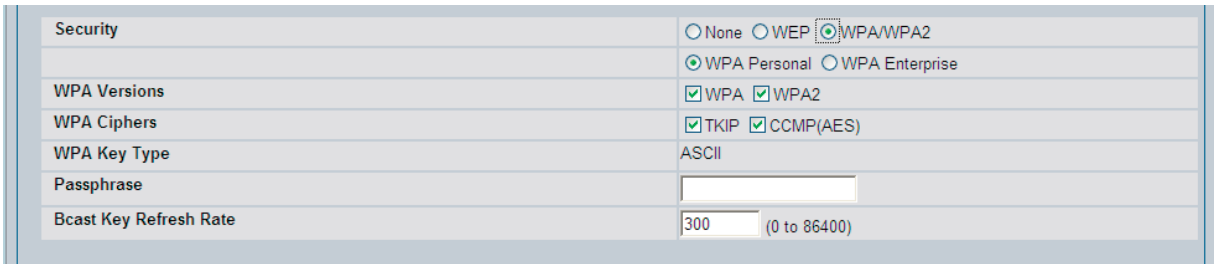


図 9-15　Wireless Network Configuration - WPA Personal Configuration 画面

以下の表に WPA Personal および WPA Enterprise セキュリティモード用の設定オプションの内容を示します。

項目	説明
WPA Personal or WPA Enterprise	WPA/WPA2 パーソナルではスタティックキーを使用します。無線クライアントとアクセスポイントの両方にデータを暗号化するための同じキーを手動で設定します。WPA/WPA2 エンタープライズでは RADIUS サーバを使用し、動的にキーを生成してクライアントからアクセスポイントへのトラフィックを暗号化します。WPA エンタープライズは WPA パーソナルより安全性が高いのですが、キーの管理のために RADIUS サーバを必要とします。 本オプションを選択すると画面は更新され、WPA キータイプおよび WPA キーのフィールドは入力できなくなります。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。 統合スイッチのグローバル RADIUS サーバ設定についての詳細は、「無線グローバル基本設定（Global タブ）」（274 ページ）を参照してください。
WPA Versions	サポートするクライアントステーションの WPA のタイプを選択します。 • WPA - ネットワーク上のすべてのクライアントが WPA をサポートし、WPA2 をサポートしていない場合は、WPA を選択します。 • WPA2 - ネットワーク上のすべてのクライアントが WPA2 をサポートしている場合は、IEEE 802.11i で最も安全なセキュリティを提供する WPA2 を使用することをお勧めします。 • WPA and WPA2 - WPA と WPA2 をサポートするクライアントが混在している場合は、両方のボックスを選択します。サポートする方式に関わらずクライアント間の接続および認証が行えます。ただし、WPA2 サポートのクライアントに対しては、多少セキュリティは高くなります。本設定では相互運用性を実現する代わりに、セキュリティを若干低くしています。
WPA Ciphers	使用する暗号化方式を選択します。 • TKIP • CCMP（AES） • TKIP and CCMP（AES） TKIP と AES サポートのクライアントのどちらも、アクセスポイントへの接続が可能です。アクセスポイントとの接続のために、WPA クライアントは以下のどちらかを持っている必要があります。 • 有効な TKIP キー • 有効な AES-CCMP キー
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 から 63 の半角英数字を入力します。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（グループ）キーの更新間隔時間を入力します。 範囲は 0-86400（秒）です。0 は、ブロードキャストキーが更新されないことを示します。

項目	説明
WPA/WPA2 Enterprise 追加設定フィールド	
Pre-Authentication	WPA/WAP2 エンタープライズを選択すると、事前認証を有効にすることができます。 WAP2 対応の無線クライアントから事前認証パケットの送信をする場合は、「Pre-Authentication」チェックボックスにチェックを入れます。事前認証情報はクライアントが接続中のアクセスポイントから、送信先のアクセスポイントに受け渡されます。 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を分単位で指定します。 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。
Session Key Refresh Rate	この VAP に接続する各クライアントが使用するセッション（ユニキャスト）キーの更新間隔時間を入力します。範囲は 0-86400（秒）です。0 は、ブロードキャストキーが更新されないことを示します。

Valid アクセスポイントの設定（Valid AP タブ）

アクセスポイント認証にローカルデータベースを使用するか、または RADIUS データベースを使用するかを指定します。「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。

アクセスポイント認証が RADIUS に設定されている場合は、スイッチが管理するアクセスポイントの情報を必ず外部 RADIUS データベースに追加してください。

Valid アクセスポイントリストへの登録は、**WLAN タブ > Administration > Basic Setup > Valid AP タブ**（以下の画面参照）を使用して行うことができます。または **WLAN タブ > Monitor > Access Point** の「AP Authentication Failures」または「Rogue AP/RF Scan」画面から登録することもできます。

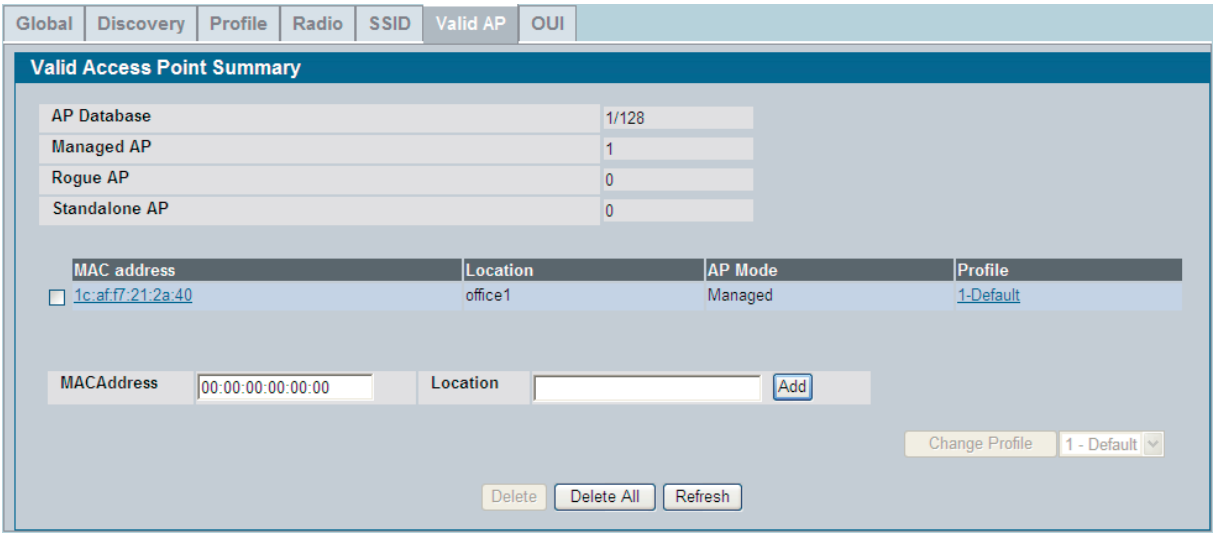


図 9-16　Valid Access Point Summary - Valid AP の追加 画面

以下の項目が表示されます。

項目	説明
AP Database	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。「Add」ボタンをクリックすると、そのアクセスポイントはスイッチのローカルデータベースに追加されます。
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。記号を含む 32 文字までの半角英数字を入力できます。
AP Mode	現在のアクセスポイントのモードを表示します。 • Managed • Standalone • Rogue 異なるモードに設定するためには、アクセスポイントの MAC アドレスをクリックして、「Valid Access Point Configuration」画面で設定します。
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。 アクセスポイントに異なるプロファイルを適用するためには、アクセスポイントの MAC アドレスをクリックして「Valid Access Point Configuration」画面で設定します。プロファイル名をクリックして、プロファイル設定画面に接続します。

「Refresh」ボタンを使用して、AP リストを更新します。「Change Profile」ボタンを使用して、選択したアクセスポイントに割り当てされているプロファイルを変更します。

MAC アドレスとアクセスポイントの場所をリストに追加後、「Add」ボタンをクリックしてそのアクセスポイントをデータベースに追加し、そのアクセスポイント用の設定ページへ移行します。既にデータベース内に登録されているアクセスポイントについては、その MAC アドレスをクリックすると、それぞれの設定ページへ移行できます。

エントリの削除

「Delete」を使用して、現在のリストからエントリをクリアします。「Delete All」ボタンを使用して、リストからすべてのエントリをクリアします。

Valid AP 設定

「Valid AP」画面では、各アクセスポイントに対しチャンネルや RF 信号送信電力レベルを指定します。また AP モードやローカル認証パスワード、さらにアクセスポイントが使用するプロファイルを指定することもできます。

アクセスポイント確認のためにローカルデータベースを選択すると、確認するアクセスポイントのデータベースはスイッチにより保持されます。データベースに MAC アドレスを追加する時に、そのアクセスポイントが「managed AP」、「standalone AP」または「rogue」であるかを指定することができます。アクセスポイントがスイッチに管理されている場合、アクセスポイントプロファイルをそのスイッチに適用することができます。スイッチが RF スキャンにより情報を収集すると、データベースにあるアクセスポイントに適切なステータスを割り当てます。

注意 「managed AP」への設定変更は、そのアクセスポイントがリセットされ再認証されるまで適用されません。「managed AP」の場合、変更を行うとリセットを確認するポップアップ画面が表示されます。「OK」をクリックすると、アクセスポイントがリセットされます。

Valid AP の一覧からリンクをクリックして表示します。

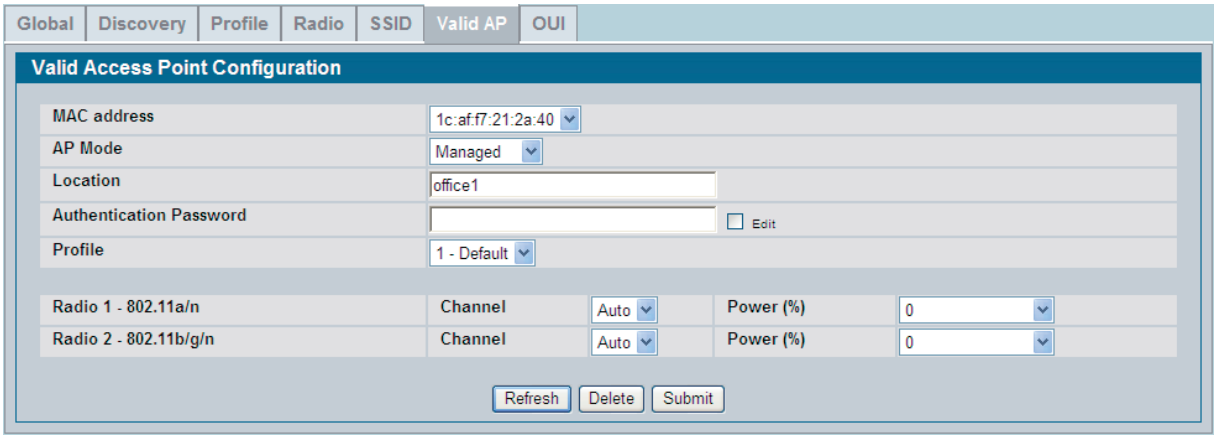


図 9-17　Valid Access Point Configuration - Valid AP 画面

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 アドレスが表示されます。この値を変更するためには、該当する Valid アクセスポイントの設定のすべてを削除し、MAC アドレスを登録し直す必要があります。
AP Mode	アクセスポイントは以下の 3 種類のモード設定が可能です。 • 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。スイッチを使用してアクセスポイントを管理しません。代わりに、アクセスポイント自身にログインして、管理者用の Web ユーザインタフェース（UI）または CLI を使用することで管理します。本オプションを選択すると画面は更新され、さらにフィールドが表示されます。「Standalone」モードのフィールド詳細は以下の表を参照してください。 • Managed - アクセスポイントは D-Link 統合スイッチの一部となり、統合スイッチを使用して管理を行います。アクセスポイントが本モードの場合、管理用 Web インタフェースおよび SNMP サービスはアクセスポイントで使用できなくなります。 • Rogue - 本モードを選択すると、そのアクセスポイントをネットワーク内で検出した時に通知（SNMP トラップが有効の場合）をします。さらに、RF スキャンでこのアクセスポイントをした時は、ステータスが「Rogue」としてリストアップされます。本モードを選択した場合、画面が更新し、本モードに適用されないフィールドは入力ができなくなります。
Location	アクセスポイントを識別しやすくするために、場所を登録します。32 文字までの半角英数字を入力することができます。
Authentication Password	スイッチがアクセスポイントを検出する際にアクセスポイントの認証するように設定することができます。認証が必要な場合は、Basic Setup > Global tab の順にクリックし、Edit オプションを選択してパスワードを入力します。パスワードは半角英数字 8 ～ 63 文字です。本フィールドのパスワードはアクセスポイント上で登録されているものと一致する必要があります。
Profile	複数の AP プロファイルが登録されている場合は、プロファイルを選択してアクセスポイントに適用することができます。アクセスポイントプロファイルの設定について野詳細は、「Global（高度なグローバル設定）」（357 ページ）を参照してください。
Channel	チャンネルとは、無線インタフェースがデータの送受信に使用する無線スペクトラムのある一部分を定義するものです。チャンネルの範囲やデフォルトのチャンネルは無線インタフェースのモードやアクセスポイントを使用する国により異なります。 IEEE 802.11b/802.11g モードおよび IEEE 802.11n（802.11 b/g/n）/2.4GHz モードではチャンネル 1 から 13 を使用し、IEEE 802.11a モードおよび IEEE 802.11n（802.11 b/g/n）/5.0GHz モードではより広範囲で非連続の次のチャンネルを使用します。: W52（ 36、40、44、48）、W53 *（ 52、56、60、64）、W56*（ 100、104、108、112、116、120、124、128、132、136、140） *W53、W56 については次期バージョンで対応予定。 複数のアクセスポイントが互いの範囲内において、同一または重複するチャンネル上でブロードキャストする時に干渉が発生します。大量のデータや中継トラフィックが帯域獲得のために争っているような高トラフィックの状況下では、干渉による影響は増大します。 「Auto」を選択すると、アクセスポイントは RF エリア内の既に占有されているチャンネルをスキャンし、干渉のない、または空いているチャンネルを自動的に選択します。アクセスポイントは、無線が再起動する時にはいつも最適なチャンネルを選択します。チャンネルを指定する場合は、隣接するアクセスポイントが使用するチャンネルに干渉を与えないように注意してください。 **注意** Valid AP データベース内のアクセスポイントに対して設定したチャンネルは固定され、アクセスポイントによる初期チャンネル選択や、スイッチによる自動チャンネルプランによるチャンネル設定より優先されます。 **注意** IEEE 802.11a および（または）IEEE 802.11n/5.0GHz モードを使用する無線インタフェースに関しては、無線電波の検出を必要とする規制範囲を持つ国もあります。これらの国（国コード設定に基づく）においては、スタティックに割り当てられているチャンネルで電波を検出すると、無線インタフェースは、自動的に IEEE 802.11h プロトコルを使用してチャンネル選択を行います。
Power (%)	送信電力レベルは、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します。電力レベルが低すぎると、無線クライアントが信号を検知できなかったり、WLAN のパフォーマンスの低下が発生します。逆に、電力レベルが高すぎると、RF 信号が通信範囲内の他のアクセスポイントとの間に干渉を起こす可能性が出てきます。 初期値 "0" は AP プロファイルに設定されている送信電力レベルを使用することを意味しています。 **注意** Valid AP データベース内に設定した送信電力レベルは固定され、アクセスポイントやスイッチによる自動送信電力調整の影響を受けることはありません。

「Standalone」モードのアクセスポイントは、個別に管理され、D-Link 統合スイッチを使用した管理はできません。Valid AP データベースに「Standalone」モードのアクセスポイントを登録し、設定を指定することで、ネットワークに認証されているアクセスポイントだけを持つことができます。**WLAN タブ > Administration > Advanced Configuration > WIDS Security** の順にクリックして「Standalone AP with unexpected configuration test」を有効にした場合、および「Standalone」モードのアクセスポイントに設定した「expected setting」が、RF スキャンで検出された設定に全く一致しない場合は、その「Standalone」モードのアクセスポイントは、**WLAN タブ > Monitoring > Access Point Rogue/RF Scan** の順にクリックして表示される画面で「Rogue」としてリストアップされます。

「Valid Access Point Configuration」画面でメニューから「Standalone」モードを選択すると、画面が更新され、追加の入力フィールドが表示されます。次の表では、Valid アクセスポイントデータベースに設定する Standalone モードのアクセスポイントについて、入力できる追加情報を説明します。

追加情報は以下の通りです。

項目	説明
Expected SSID	Standalone モードのアクセスポイントのむセンネットワークを識別する SSID を入力します。
Expected Channel	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 WDS Mode	Standalone モードのアクセスポイントは、WDS リンクを使用して相互に無線で通信することができます。 以下のオプションがメニューに表示されます。 • Bridge - Valid AP データベースに追加した Standalone モードのアクセスポイントは、1 つ以上の WDS リンクを使用します。 • Normal - Standalone モードのアクセスポイントが WDS リンクを全く使用しないように設定されている場合は、本オプションを選択します。 • Any - Standalone モードのアクセスポイントが WDS リンクを使用する可能性がある場合は、本オプションを選択します。
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。

ローカルの OUI データベース概要（OUI タブ）

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。これは参照専用のリストで 10,000 件以上の登録があります。「Local OUI Database Summary」画面で 64 個まで OUI を入力することできます。ローカルリストが検出されると、OUI は参照用リスト共にローカルリストに置かれます。

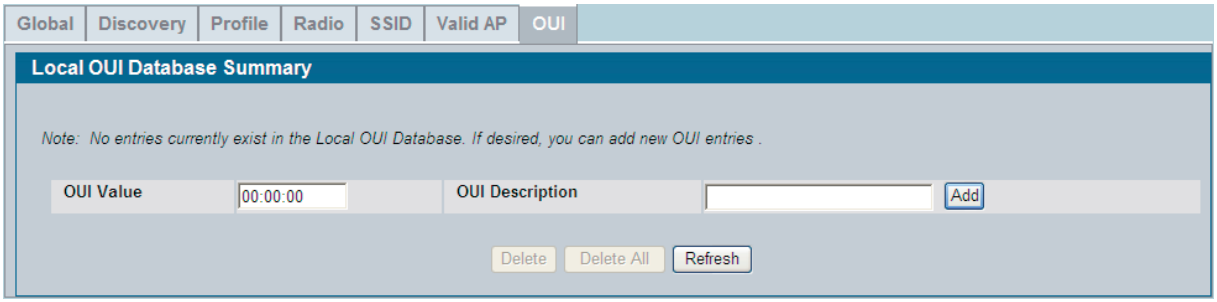


図 9-18　Local OUI Database Summary 画面

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。 **注意** OUIの第1バイトでは、最下位ビットに0を設定する必要があります。例えば以下のようになります。「02:FF:FF」は正しい OUI ですが、「03:FF:FF」は正しくありません。
OUI Description	OUI に関連付けされる組織名。半角英数字 32 文字以内。

OUI Value と OUI Description を入力後、「Add」ボタンをクリックして、ローカルデータベースに OUI を追加します。

アクセスポイント管理

「AP Management」フォルダには D-Link 統合スイッチでアクセスポイントの管理 / 維持を補助する以下の画面へのリンクがあります。

- Reset
- RF Management
- Access Point Software Download
- Managed AP Advanced Settings

Reset（再起動）

統合スイッチから、1 つ以上のアクセスポイントを再起動することができます。アクセスポイントを再起動する命令を送ると、アクセスポイントはハードウェアリセットする前に、スイッチとの間の SSL 接続を切断します。

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

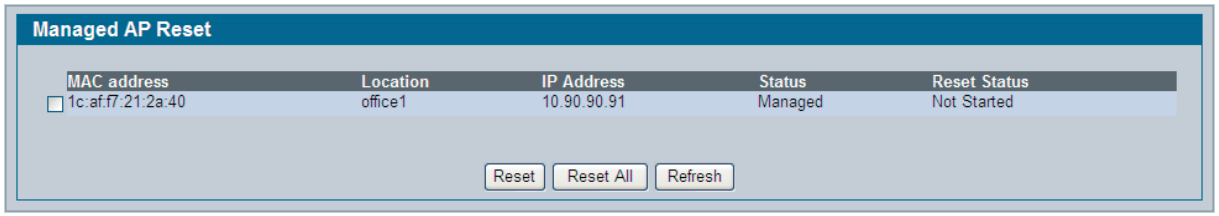


図 9-19　Managed AP Reset 画面

再起動するアクセスポイントを選択して「Reset」ボタンをクリックするか、または「Reset All」ボタンをクリックしてスイッチ管理下のすべてのアクセスポイントを再起動します。

アクセスポイントが再起動し、スイッチとの通信を再開するまでには数分かかります。再起動中にはアクセスポイントの状態は一度 "failed" になりますが、オンライン状態に戻ると "Managed" に戻ります。

RF 管理

無線周波数（RF）ブロードキャストチャンネルとは、アクセスポイント上の無線インタフェースが、データの送受信に使用する無線スペクトラムのある一部分を定義するものです。アクセスポイントが使用するためのチャンネル範囲は、アクセスポイントの IEEE 802.11 モード（バンドとも呼ばれる）により決定されます。

- 各アクセスポイントは、複数モードで動作可能な動作可能なデュアルバンドシステムです。
- IEEE 802.11b と 802.11g モード（802.11b/g）は 2.4GHz 周波数帯で動作し、チャンネル 1 から 13 をサポートします。
- IEEE 802.11a モードは 5GHz 周波数帯で動作し、より広範囲で非連続の次のチャンネルを使用します。:
  W52（36、40、44、48）、W53 *（52、56、60、64）、W56*（100、104、108、112、116、120、124、128、132、136、140）

*W53、W56 については次期バージョンで対応予定。。

- IEEE 802.11n は 2.4GHz 帯または 5GHz 帯で動作します。

注意　使用可能なチャンネルはアクセスポイントを使用する国によって異なります。本項で説明するチャンネルは日本国において有効なものです。

大量のデータや中継トラフィックが帯域獲得のために争っているような高トラフィックの状況下では、干渉による影響は増大します。b/g 周波数帯の一般的な干渉ゼロのチャンネルセットは 1,6,11 です。チャンネル 1,4,8,11 の使用でオーバーラップを最低限に抑えることができます。同じような干渉ゼロのチャンネルセットは、オーバーラップしていないためそのモードにすべてのチャンネルを含む無線バンドにも使用されます。

Configuration タブ（チャンネル計画と送信電力設定）

統合スイッチのソフトウェアには、RF 干渉を最小限に抑えるために、各アクセスポイントがどの RF チャンネルを使用すべきかを自動で判断する、チャンネルプランアルゴリズムを採用しています。チャンネルプランアルゴリズムを有効にすると、スイッチは管理下にある各アクセスポイントが使用しているチャンネルを定期的に評価し、干渉が認められる場合には、チャンネルを変更します。

注意 周波数およびチャンネルの割り当てに関する規則は、国によって異なります。802.11b/g/n においてチャンネル 1,6,11 をサポートしない国では、本チャンネルプランアルゴリズムは無効になります。5GHz の周波数帯では、そのアルゴリズムは 802.11h 電波の検出を必要とする国では無効であり、ヨーロッパ各国と日本が含まれます。

自動チャンネル選択アルゴリズムは、以下の条件に一致するアクセスポイントには影響を与えません。

- アクセスポイントへのチャンネル割り当てが、RADIUS サーバまたはローカル AP データベースで静的に行われた。
- アクセスポイントへのチャンネル割り当てが、「AP Management」の下の「Advanced Settings」画面によりスタティックに行われた。
- アクセスポイントは、**Administration > Advanced Configuration > AP Profiles** の「Radio」タブ内の「Automatic Channel」フィールドを無効に設定しているプロファイルを持っている（「Radio Configuration」の設定）。

注意 アクセスポイントが固定チャンネルに割り当てられない場合、または自動チャンネル選択アルゴリズムによって特定のチャンネルに割り当てられない場合、AP チャンネル選択モードは「最適」に設定されます。つまり、無線が再起動する場合には必ず、またはアクセスが電波信号を検出する場合、アクセスポイントが「最適」チャンネルを選択することを意味します。

RF 送信電力レベルは、アクセスポイントが RF 信号をブロードキャストできる距離に影響します。電力レベルが低すぎると、無線クライアントは信号検出ができなかったり、WLAN の品質低下につながります。逆に、電力レベルが高すぎると、RF 信号が通信範囲内の他のアクセスポイントとの間に干渉を起こす可能性が出てきます。また、物理的にビルやネットワークの枠を超えた RF 信号のブロードキャストは、ネットワークにセキュリティ上の危険をもたらします。

自動送信電力調整機能では、独自のアルゴリズムを使用して、RF 信号がなるべく遠くの無線クライアントまで到達し、かつ他のアクセスポイントがブロードキャストする RF 信号と干渉を起こすほど遠くまでは到達しないように、自動的に調整を行います。

チャンネルプランと自動電力調整の設定のためには、**WLAN タブ > 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。

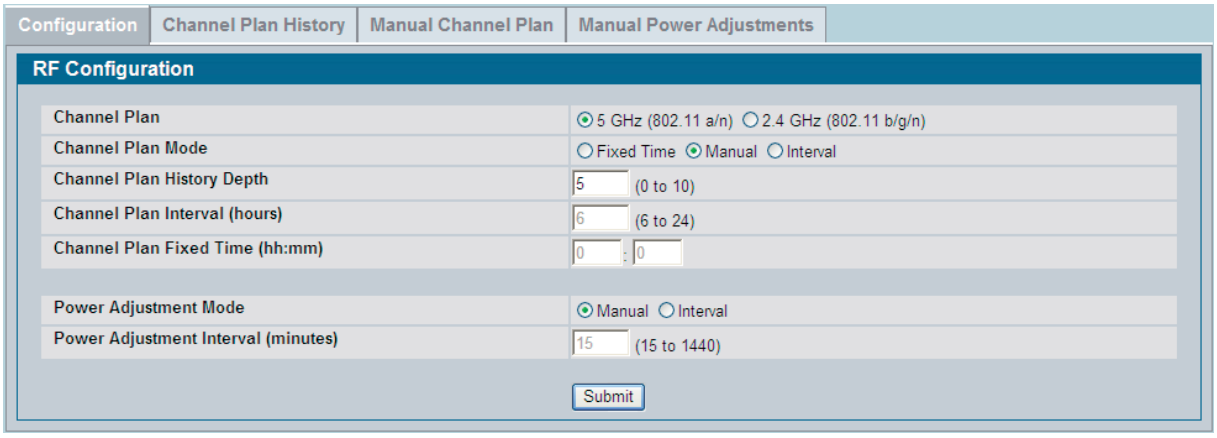


図 9-20　RF Channel Plan and Power Configuration 画面

以下の表は設定する RF チャンネルプランと送信電力調整設定用の項目について説明しています。

注意 アクセスポイントがチャンネル変更する時、すべての接続中の無線クライアントの接続は中断され、再接続が必要になります。再接続には数秒を要するため、音声や映像などの時間に依存するサービスに影響を与える場合があります。

以下の項目が表示されます。

項目	説明
Channel Plan	各アクセスポイントは 2.4GHz と 5Ghz の周波数で動作できるデュアルバンドです。802.11a/n および 802.11b/g/n モードが異なるチャンネルを使用します。チャンネルプランを設定する前に、無線モードを選択します。
Channel Plan Mode	チャンネル割付けのモードを示します。チャンネル割り当てモードを選択します。 • Fixed Time -「Cannel Plan Mode」に「Fixed Time」を選択した場合、チャンネルプランの計算とチャンネル割り当ての時間を指定する必要があります。1 日のうちの指定した時刻に実行されます。 • Manual -「Cannel Plan Mode」に「Manual」を選択した場合、チャンネルプランの計算と割り当てを手動で行うモードです。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適用します。 • Interval -「Cannel Plan Mode」に「Interval」を選択した場合、スイッチは定期的にチャンネルプランを計算して適用します。実行間隔を 6~24 時間の間で指定します。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。
Channel Plan History Depth	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。ここで指定した数字により、チャンネル割り当ての繰り返し回数が制御されます。 **注意** チャンネルを変更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。
Channel Plan Interval (hours)	「Channel Plan Mode」で「Interval」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間隔を指定します。単位は時間で、6~24 時間の間で指定します。
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。1 日のうちのここで指定した時刻に実行されます。
Power Adjustment Mode	アクセスポイントの無線送信電力は、AP プロファイル、ローカルデータベース、または RADIUS サーバで指定できます。AP プロファイルの送信電力レベルは、アクセスポイントの初期値のレベルであり、送信電力は AP プロファイルの値以下に調整はされません。ローカルデータベースと RADIUS サーバでの設定は、常にプロファイルでの設定より優先されます。手動で送信電力をセットした場合は、その値が固定され、そのアクセスポイントでは自動送信電力アルゴリズムを使用できなくなります。最大送信電力が、規制範囲（地域）やハードウェアの性能により、チャンネルに許可される最低の電力レベルになるように、最大送信電力のパーセンテージ（%）単位で設定できます。 • Manual -「Manual Power Adjustments」ページから手動で電力調整を実行します。 • 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適した送信電力を適用します。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。 **注意** ローカルまたは RADIUS データベースに電力レベルを設定する場合、その値は AP プロファイルに設定した値より優先されます。 **注意** この設定はアクセスポイントの両方の無線モードに適用されます。電力レベルの手動設定についての詳細は「周波数帯域（Radio タブ）」（279 ページ）および「Valid アクセスポイントの設定（Valid AP タブ）」（292 ページ）を参照してください。
Power Adjustment Interval (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。アルゴリズムは、「Power Adjustment Mode」フィールドで "Interval" を指定した場合のみ実行されます。 **注意** この設定はアクセスポイントの両方の無線モードに適用されます。

Channel Plan History タブ（チャンネルプランヒストリの表示）

統合スイッチはアクセスポイントへのチャンネル割り当て情報を記録し、管理します。
チャンネルプランヒストリ情報にアクセスするためには、**Administration > AP Management > RF Management** とクリックし、「Channel Plan History」タブを表示します。

クラスタを管理するクラスタコントローラは、クラスタ内にあるすべてのスイッチのチャンネルヒストリ情報を保持します。
クラスタコントローラでは、チャンネルを割り当てるのに適したクラスタ内のスイッチにより管理され、新しいチャンネルの割り当てに成功したすべてのアクセスポイントの無線情報を表示します。

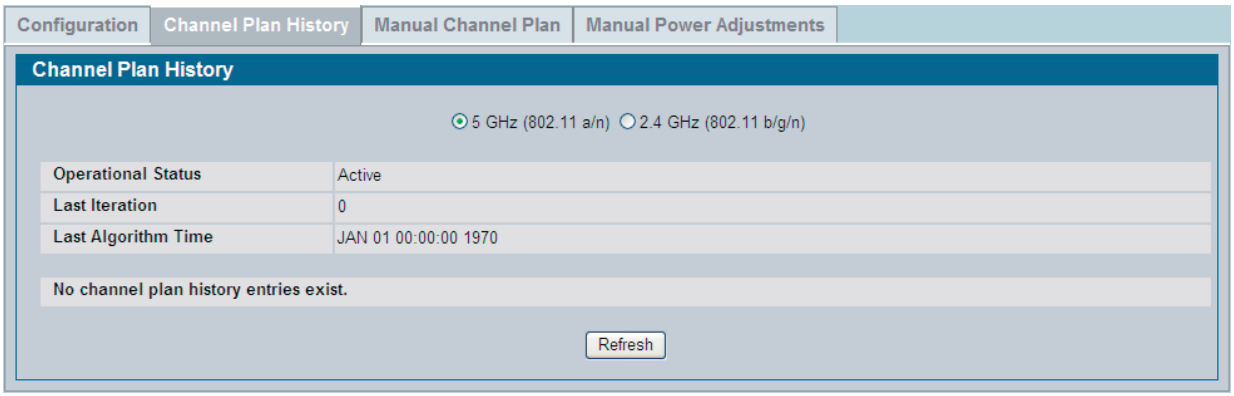


図 9-21　Channel Plan History 画面

以下の表は「Channel Plan History」タブについて説明します。

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。本ページに表示されるチャンネル情報は、選択したいずれかのモードになります。
Operational Status	スイッチがアクセスポイントの無線モード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示します。
Last Iteration	本フィールド内の数字は、チャンネルプラン調整を行った最後の反復サイクルを示します。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** タブを選択して、「Channel Plan History depth」を設定することにより、記録・表示する最大反復サイクル回数を指定できます。
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。SNTP クライアントとサーバの設定は、Web インタフェースを使用して、**LAN タブ > Administration > System** の順にメニューをクリックし、「SNTP Settings」画面で行います。CLI では「Global Config」モードで「sntp」コマンドを実行します。
AP MAC Address Location Radio Iteration Channel	チャンネルプランの反復サイクルで、アクセスポイントに割り当てられたチャンネルを表示します。

Manual Channel Plan タブ（手動チャンネルプランの起動）

「Configuration」タブにおいて「Channel Plan Mode」に「Manual」を指定すると、「Manual Channel Plan」タブ画面からチャンネルプランアルゴリズムを起動できるようになります。

手動でチャンネルプラン調整機能を実行するためには、チャンネルを調整する周波数（5 GHz または 2.4 GHz）を選択して「Start」ボタンをクリックします。

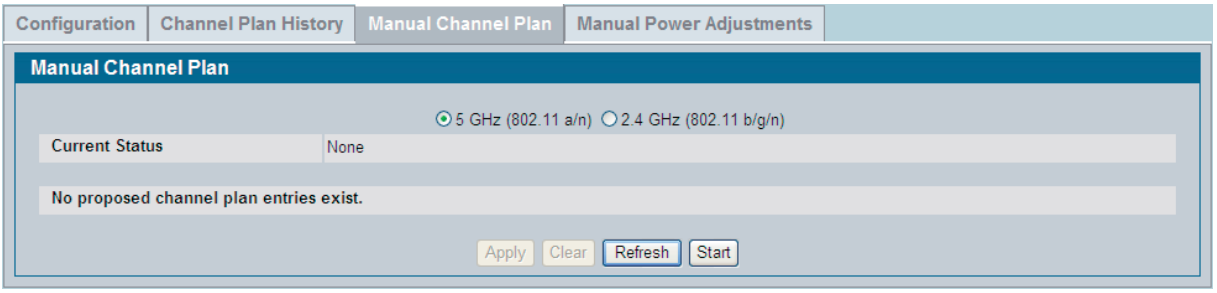


図 9-22　Manual Channel Plan 画面

以下の項目が表示されます。

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。本ページに表示されるチャンネル情報は、選択したいずれかのモードになります。
Current Status	• 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。

チャンネルプランを実行すると、アルゴリズムによりチャンネルの変更が望ましいアクセスポイントが表示されます。「Current Channel」には現在使用しているチャンネルが、また「New Channel」には変更案が表示されます。変更案を実行するためには「Apply」ボタンをクリックします。アルゴリズムの実行後、どのアクセスポイントも表示されなければ、チャンネルの変更の必要がないことを示しています。

自動チャンネル選択が動作する時間と、チャンネル変更案を適用する時間の間に、ネットワークコンフィグレーションを変更することは可能です。

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静的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 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。

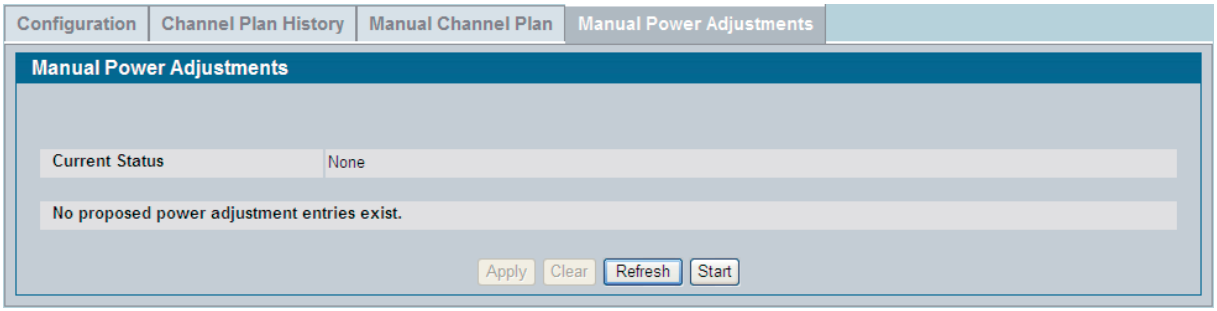


図 9-23　Manual Power Adjustments 画面

以下の項目が表示されます。

項目	説明
Current Status	• 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。

Software Downloads（アクセスポイントソフトウェアのダウンロード）

統合スイッチによって、管理下にあるアクセスポイントのソフトウェアをアップグレードできます。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。

WLAN タブ > Administration > AP Management > Software Downloads 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。

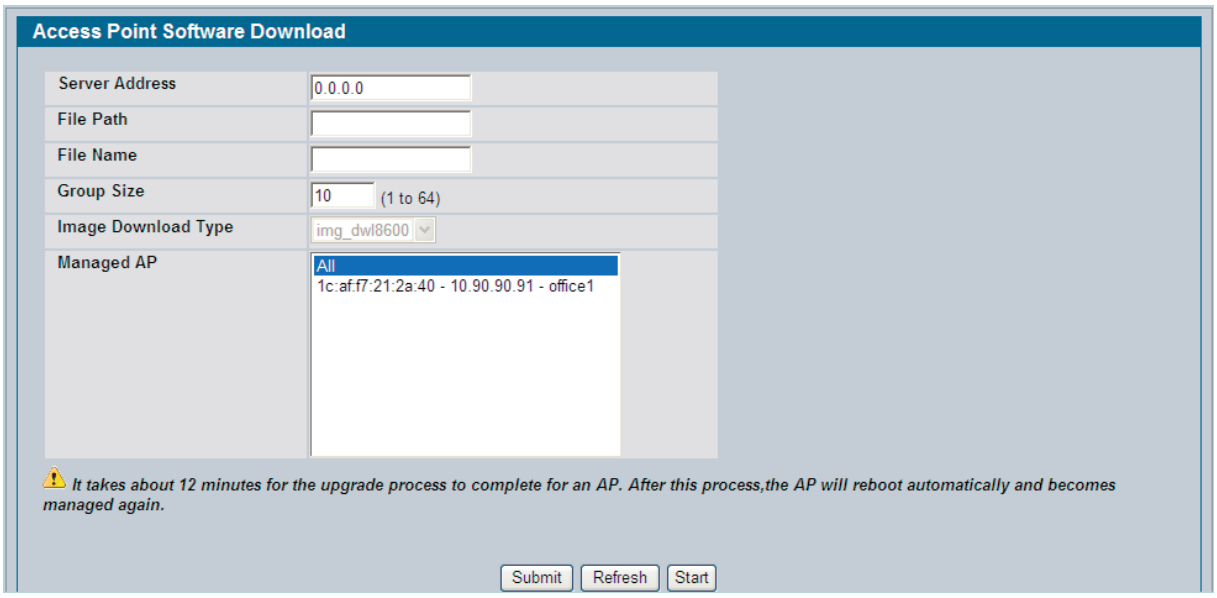


図 9-24　Access Point Software Download 画面

以下のテーブルで説明されるようにアップグレードファイルについての情報を入力後、「Start」ボタンをクリックしてアップグレードプロセスを開始します。追加のフィールドがダウンロード後に表示され、アップグレードの状況と結果を確認できます。

注意　プログラムのダウンロードに成功すると、アクセスポイントは自動的に再起動します。

以下の表では、アクセスポイントをアップグレードするために使用する各項目について説明します。

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。ホストには TFTP サーバがインストールされ、起動している必要があります。
File Path	選択ファイルは位置する TFTP サーバのパス。96 文字まで入力することができます。
File Name	アップグレード用ファイルの名前を 32 文字までの半角英数字で入力します。拡張子 ".tar" の入力が必要です。
Group Size	複数のアクセスポイントをアップグレードする場合、各アクセスポイントが TFTP サーバに接続してファイルをダウンロードします。TFTP サーバの過負荷防止のため、一度にアップグレードするアクセスポイント数を制限できます。 一度にアップグレードするアクセスポイントの数。1 つのグループのアップグレード後に、次のグループのアップグレードが開始されます。
Image Download Type	ダウンロードされるべきイメージのタイプ。D-Link 統合スイッチは DWL-8600AP ハードウェアタイプのみをサポートしています。
Managed AP	リストにスイッチが管理するすべてのアクセスポイントが表示されます。スイッチがクラスタコントローラである場合、リストにはクラスタ内のすべてのスイッチが管理するアクセスポイントを表示します。 各アクセスポイントは MAC アドレス、IP アドレス、およびロケーションの <MAC - IP - Location> 形式により識別されます。1 台のアクセスポイントをアップグレードする場合、プルダウンリストから目的のアクセスポイントを選択します。すべてのアクセスポイントを対象にする場合は、リストの一番上の「All」を選択します。 All を選択した場合、「Group Size」の入力により、同時にアップグレードするアクセスポイントの数を制限して TFTP サーバの過負荷を防止します。 アップグレードのために複数のアクセスポイント選択するためには、「CTRL」＋アクセスポイントをクリックします。 **注意** すべての管理アクセスポイントを同時にアップグレードすることをお勧めします。「Start」ボタンをクリックすると以下のフィールドが表示されます。
設定テーブル	
Status (Global)	すべてのアクセスポイントのアップグレードプロセスの状況を表示します。 • Not Started - 統合スイッチはダウンロードプロセスを開始していません。 • Requested - アクセスポイントのソフトウェアにダウンロードリクエストが発行されたが、スイッチはまだダウンロードをしていません。 • Code Transfer in Progress - ダウンロードは進行中です。 • Failure - すべてのアクセスポイントでダウンロードに失敗しました。 • Aborted - アクセスポイントに 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。 • NVRAM-Update-In-Progress - ダウンロードに成功しました。アクセスポイントに Reset コマンドを送信しました。 • Success - すべてのアクセスポイントが統合スイッチに接続されています。
Status (per-AP)	同ページ中のリストに、アクセスポイントごとにダウンロードの状況とダウンロード中のソフトウェアのバージョンが表示されます。各アクセスポイントの「Status」欄には以下に示す状況の一つが表示されます。 • 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廃止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。
Download Count	現在ダウンロードリクエストでソフトウェアをダウンロードした管理アクセスポイントの数が表示されます。「Managed AP」に「All」を選択した場合は、ダウンロードリクエストを開始した時点で、統合スイッチの管理下にあったすべてのアクセスポイントの数が表示されます。1 台アップグレードしていれば、「1」と表示されます。
Success Count	新しいプログラムのダウンロードに成功したアクセスポイントの数が表示されます。はじめは「0」と表示されていますが、アクセスポイントがダウンロードに成功するごとに数値が増加していきます。
Failure Count	新しいプログラムのダウンロードに失敗したアクセスポイントの数が表示されます。0 から開始して、各失敗ごとに増えていきます。
Abort Count	新しいプログラムのダウンロードを中止したアクセスポイントの数が表示されます。0 から開始して、各失敗ごとに増えていきます。

Advanced Settings（管理アクセスポイントの詳細設定）

アクセスポイントが「Managed」モードにある時は、アクセスポイントへのリモートアクセスは無効です。しかし、**WLAN タブ > Administration >AP Management > Advanced Settings** 画面で、デバッグ機能を有効にして Telnet によりアクセスすることが可能です。「Managed AP Advanced Settings」画面から、アクセスポイントの各無線インタフェースに対して、手動で RF チャンネルと送信電力を変更することもできます。手動による電力とチャンネルの変更は、アクセスポイントのプロファイル（自動チャンネル選択を含む）に設定された内容を上書きして、直ちに適用されます。アクセスポイントがスイッチとの接続を解除し、再び接続する場合など、アクセスポイントがリセットされる場合、またはプロファイルがアクセスポイントに再度適用される場合には手動のチャンネルと電力割当ては保持されません。

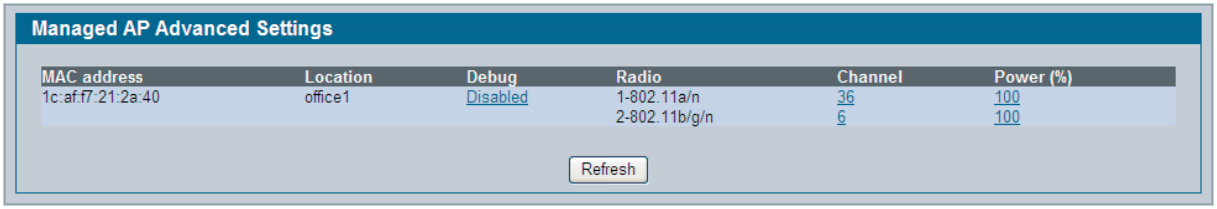


図 9-25　Managed AP Advanced Settings 画面

統合スイッチによって管理されるアクセスポイントの MAC アドレスと場所が表示されます。場所は RADIUS またはローカルの有効 AP データベースの値に基づいています。
以下の表では、アクセスポイントに設定可能な高度な機能について説明します。

項目	説明
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ロケーションを表示します。これは、RADIUS またはローカルの Valid AP データベースに設定された値に基づいています。
Debug	トラブルシューティング用にアクセスポイントへの Telnet 接続を有効にし、CLI を使用してデバイスのデバッグを可能にします。以下のいずれかの状態を表示します。 • Disabled - 無効 • Set Requested - 要求の設定 • Set in Progress - 進行中 • Enabled - 有効 状態を変更するためには、「Debug」の状態のリンクをクリックして、「Managed AP Debug」画面を表示します。「Managed AP Debug」画面に関する説明を参照してください。
Radio	チャンネルと電力設定が適用される無線モードを指定します。
Channel	「Channel」のリンクをクリックすると「Managed AP Channel/Power Adjust」画面が表示され、周波数 1 または周波数 2 に対して新しいチャンネルを設定できます。使用できるチャンネルは、無線モードとアクセスポイントを使用する国によって異なります。手動のチャンネル変更は、アクセスポイントのプロファイルに設定されたチャンネルを上書きすると、アクセスポイントのリブート時、またはアクセスポイントのプロファイルが再度使用されている場合には保持されません。「Managed AP Debug」画面に関する説明を参照してください。
Power	「Power」のリンクをクリックすると「Managed AP Channel/Power Adjust」画面が表示され、アクセスポイントの新しい送信電力を設定できます。手動の電力変更は、アクセスポイントのプロファイルに設定された電力設定を上書きすると、アクセスポイントのリブート時、またはアクセスポイントのプロファイルが再度使用される場合には保持されません。「Managed AP Debug」画面に関する説明を参照してください。

アクセスポイントのデバッグ

Administration > AP Management > Advanced の順にメニューをクリックし、「Managed AP Advanced」画面上の管理アクセスポイントの「Debug」リンクをクリックすると、以下の画面が表示されます。

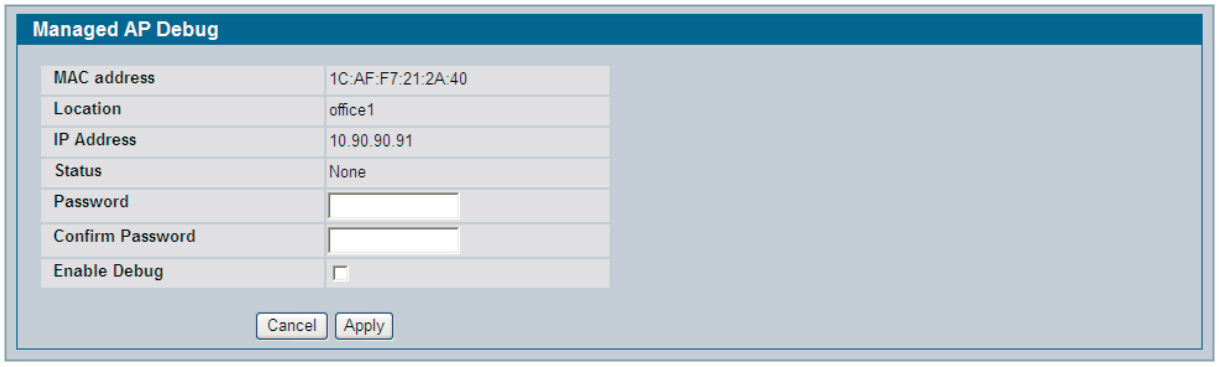


図 9-26　Managed AP Debug 画面

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。以下のいずれかが表示されます。 • None - デバッグ機能は有効、無効のいずれでもありません。 • Set Requested - デバッグ機能の状態を変更する要求が発行されています。 • Set Complete - デバッグ機能が有効または無効になりました。
Password	アクセスポイントの管理者用パスワードを入力します。初期値は「admin」です。
Confirm Password	パスワードは暗号化されるため、確認のため、もう一度パスワードを入力します。
Enable Debug	本チェックボックスにより、デバッグ機能を有効または無効にします。チェックすると有効になります。 アクセスポイントに Telnet で接続すると、「AP interface login」プロンプトが表示されます。ユーザ名は「admin」です。上記「Password」に入力したパスワードを入力します。パスワードを変更していない場合、パスワードの初期値「admin」を使用します。アクセスポイントの CLI から、「!」を入力することにより、通常の Linux プロンプトにアクセスできます。Linux OS プロンプト表示時には、以下のデバッグ用コマンドが実行できます。 • get management - 管理用インタフェースの情報を表示します。 • get managed-ap - Linux OS プロンプト表示時には、以下のデバッグ用コマンドが実行できます。: • ifconfig - すべてのインタフェースを表示します。 • cat /proc/meminfo - メモリの使用率を参照します。

チャンネルと電力の調整

チャンネルと送信電力の調整チャンネルと送信電力の変更は、動作中の変更に限定されます。チャンネルと送信電力の設定を変更しても、新しい変更内容はアクセスポイントまたはスイッチが再起動した時に失われます。

Administration > AP Management > Advanced Settings の順にメニューをクリックし、「Managed AP Advanced Settings」画面上で、現在の「Channel」または「Power」をクリックします。

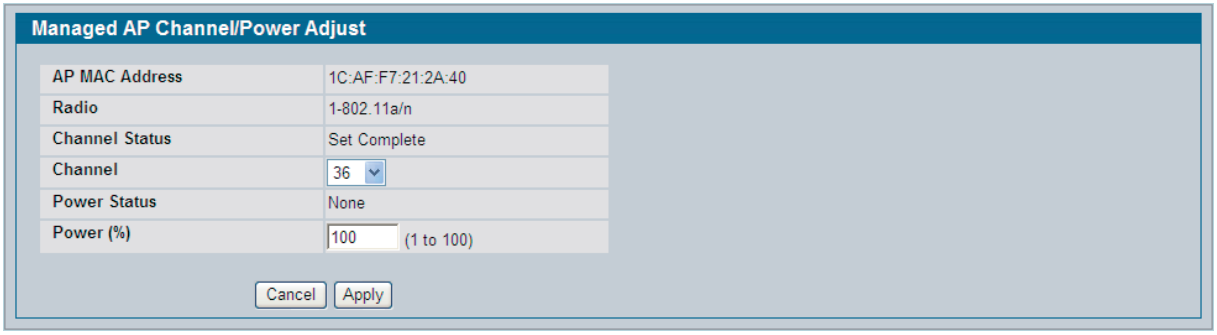


図 9-27　Managed AP Channel/Power Adjust 画面

以下の項目が表示されます。

項目	説明
AP MAC Address	アクセスポイントの MAC アドレスを示します。
Radio	無線インタフェースとそのモードを示します。変更はここで表示される無線インタフェースにだけ適用されます。
Channel Status	以下の状態の一つが表示されます。 • None • Set Requested（要求の設定） • Set Complete（変更完了）
Channel	チャンネルとは、無線インタフェースがデータの送受信に使用する無線スペクトラムのある一部分を定義するものです。チャンネルの範囲およびデフォルトのチャンネルは、無線インタフェースのモードにより決定されます。 IEEE 802.11b/802.11g モードおよび IEEE 802.11n（802.11 b/g/n）/2.4GHz モードではチャンネル 1 から 13 を使用し、IEEE 802.11a モードおよび IEEE 802.11n（802.11 b/g/n）/5.0GHz モードではより広範囲で非連続の次のチャンネルを使用します。：W52（36、40、44、48）、W53 *（52、56、60、64）、W56*（100、104、108、112、116、120、124、128、132、136、140） *W53、W56 については次期バージョンで対応予定。 **注意** 使用可能なチャンネルはアクセスポイントを使用する国によって異なります。 **注意** 5.0GHz モードを使用する無線インタフェースに関しては、無線電波の検出を必要とする規制範囲を持つ国もあります。これらの国（国コード設定に基づく）においては、スタティックに割り当てられているチャンネルで電波を検出すると、無線インタフェースは、自動的に IEEE 802.11h プロトコルを使用してチャンネル選択を行います。 複数のアクセスポイントが互いの範囲内において、同一または重複するチャンネル上でブロードキャストする時に干渉が発生します。大量のデータや中継トラフィックが帯域獲得のために争っているような高トラフィックの状況下では、干渉による影響は増大します。 ここで「Auto」を選択すると、アクセスポイントは RF エリア内の既に占有されているチャンネルをスキャンし、干渉のない、または空いているチャンネルを自動的に選択します。チャンネルを指定する場合は、隣接するアクセスポイントが使用するチャンネルに干渉を与えないように注意してください。
Power Status	以下の状態の一つが表示されます。 • None • Set Requested（要求の設定） • Set Complete（変更完了）
Power	電力レベルが低すぎると、無線クライアントは信号検出ができなかったり、WLAN の品質低下につながります。 逆に送信電力レベルが高すぎると、RF 信号は他のアクセスポイントと干渉を起こすこともあります。

状態および統計情報のモニタリング

D-Link 統合スイッチネットワークでステータスや統計情報の監視を補助する以下の機能があります。

- Wireless Global Status/Statistics
- Managed AP Status
- Associated Client Status/Statistics
- Peer Switch Status

Global（グローバル状態 / 統計情報）

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。「Global」タブを参照することにより、スイッチや接続するデバイスの状況や統計情報を参照できます。

Global タブ

WLAN 全体の統計情報にアクセスします。

WLAN タブ > 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 9-28　Wireless Global Status/Statistics 画面

画面の各項目について説明します。

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」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。スイッチの IP アドレス。
WLAN Switch Disable Reason	WLAN スイッチ機能が無効である場合、本項目が表示されて以下の原因の一つが表示されます。 • None - ステータス無効の原因が不明です。 • Administrator disabled -「global configuration」画面の「Enable WLAN Switch」チェックボックスのチェックが外されました。 • No IP Address - WLAN インタフェースには IP アドレスが割り当てられていません。 • No SSL Files - 統合スイッチは、SSL 接続を使用してスイッチが管理するアクセスポイントと通信を行います。統合スイッチの電源を投入すると、自動的にサーバ証明書が生成され、SSL 接続の確立に使用されます。SSL 証明書およびキーの発行には約 1 時間を要します。 スイッチ上でルーティングが有効になっていても、稼動状況は以下の原因で無効とされている場合があります。 • No Loopback Interface - スイッチにループバックインタフェースが存在しません。 • Global Routing Disabled - 例え WLAN スイッチインタフェース上でルーティングモードが有効であっても、動作ステータスをグローバルに有効にする必要があります。
IP Address	スイッチの IP アドレス。
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いてクラスタコントローラであるか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、自動的に選出されるか、または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、全クラスタにおいて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"、"Connection Failed Access Points"、"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	スタンドアロンモードのトラストアクセスポイント数。スタンドアロンモードのアクセスポイントは、スイッチで管理することはできません。
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「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。
Connection Failed Access Points	以前に認証され、スイッチの管理下にあったが、現在は統合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 上で検出されている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されている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です。
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認証解除メッセージを送信するアクセスポイント数。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。

項目	説明
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総数。
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。
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。
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 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 ビアが Distributed トンネル経由で送信したパケットの総数。
Distributed Tunnel Roamed Clients	Distributed 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	Distributed トンネリングを使用す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 Distributed トンネルを設定できなかったクライアントの総数。

Switch Status タブ（スイッチの状態および統計情報の参照）

各スイッチの「Switch Status/Statistics」画面では、そのスイッチが管理するアクセスポイントや関連するクライアントに関する情報を提供します。スイッチがクラスタコントローラである場合、それはグループ内の各スイッチに関するスイッチステータスと統計情報を提供します。

注意 クラスタコントローラスイッチだけが、全クラスタの管理アクセスポイント、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。

プルダウンメニューを使用して、表示する情報を持つスイッチを選択します。ローカルなスイッチが唯一利用可能なオプションである場合、それは単にクラスタ内のスイッチであり、クラスタコントローラではありません。

WLAN タブ > 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。

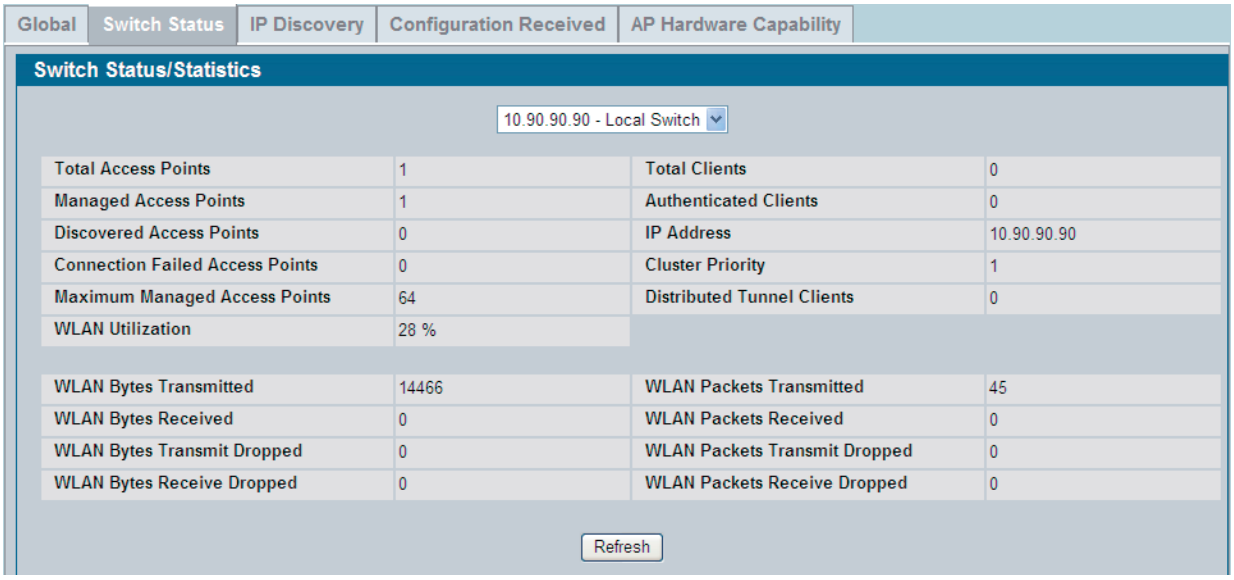


図 9-29　Switch Status/Statistics 画面

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。
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。
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。
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。
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。
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総数。
IP Address	スイッチの IP アドレス。
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。
Distributed Tunnel Clients	Distributed 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 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 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 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 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 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 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 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 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受信し、破棄された総パケット数。

IP Discovery タブ（IP 検出状態の確認）

WLAN タブ > Monitoring > Global > IP Discovery タブをクリックして「IP Discovery」タブを表示すると、**WLAN タブ > Administration > Basic Setup > Discovery タブ**の「IP discovery List」にあるデバイスとの通信情報を確認できます。

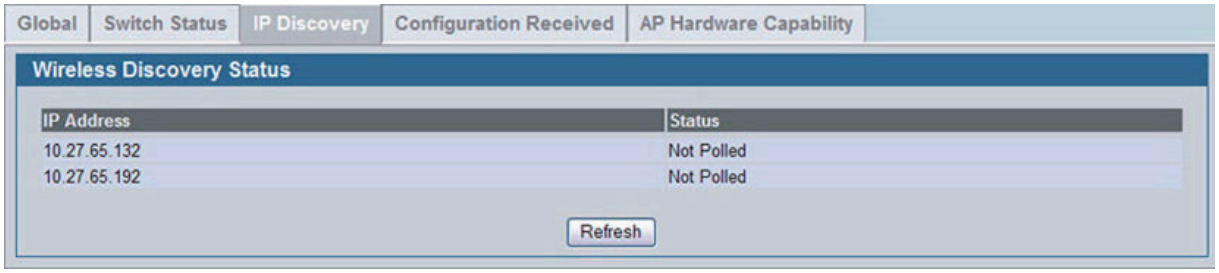


図 9-30　Wireless Discovery Status 画面

以下の項目が表示されます。

項目	説明
Wireless Discovery Status	• 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「L3/IP Discovery」リスト中の本 IP アドレスを持つデバイスに接続を試みました。 • Discovered - スイッチは「L3/IP Discovery」リスト中のピアス一致またはアクセスポイントに接続し、認証または認知しました。 • 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、認証または認知に失敗しました。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。

Configuration Received タブ（状態を受信したピアスイッチ設定の参照）

ピアスイッチ設定機能により、1 つのスイッチから他のすべてのスイッチにクリティカル無線設定を送信することができます。本機能は、スイッチの同期を維持することに加え、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。以下の画面では、スイッチがピアの 1 つから送受信した設定に関する情報を表示します。

WLAN タブ > Monitoring > Global > Configuration Received 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。

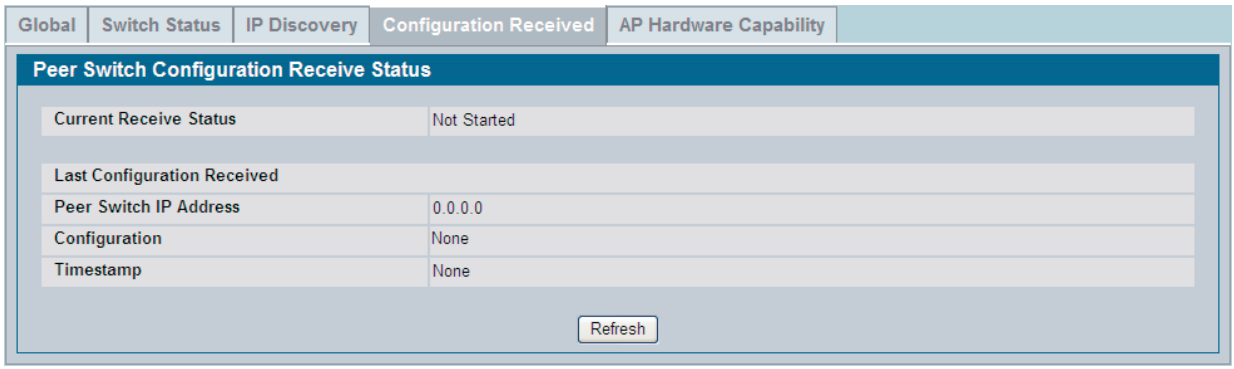


図 9-31　Peer Switch Configuration Received Status 画面

各項目について説明します。

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。可能なステータス値は以下の通りです。 • 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 プロファイルのコンフィグレーションを適用中です。 • 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。
Last Configuration Received	
Peer Switch IP Address	このスイッチが無線の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示します。
Configuration	コンフィグレーションのどの部分を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 つ以上項目が表示されます。 • Global • Discovery • Channel/Power • AP Database • AP Profiles • Known Client • Captive Portal • RADIUS Client • QoS ACL • QoS DiffServ スイッチが他のスイッチのコンフィグレーション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 タブ（AP ハードウェア機能リストの参照）

スイッチは、周波数、IEEE 802.11 モード、およびアクセスポイントが必要とするソフトウェアイメージなど異なるハードウェア機能を持つアクセスポイントをサポートしています。「AP Hardware Capability」タブから、アクセスポイントのハードウェアサポート、ハードウェアがサポートする周波数帯、IEEE モード、アクセスポイントにダウンロード可能なソフトウェアイメージに関するサマリ情報にアクセスできます。

Summary タブ（サマリ情報）

WLAN タブ > Monitoring > Global > AP Hardware Capability タブ > 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。

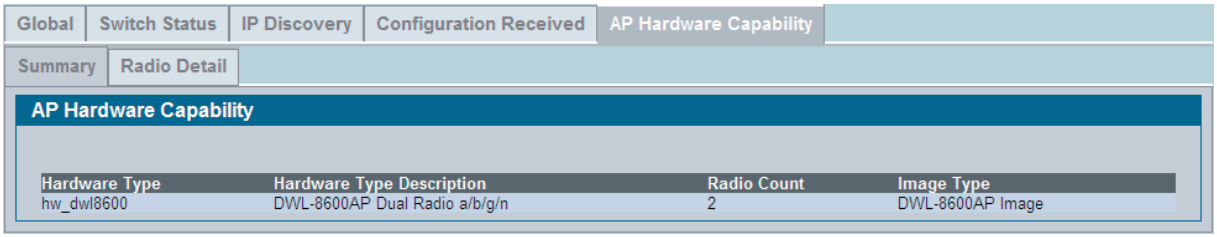


図 9-32　AP Hardware Capability 画面

利用可能な各項目を説明します。

項目	説明
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 モードがあります。
Radio Count	ハードウェアがサポートする周波数帯（1 または 2）を表示します。
Image Type	ハードウェアが要求するソフトウェアのタイプを指定します。
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リセット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 タブ（AP ハードウェア帯域性能）

無線帯域の詳細を参照します。

WLAN タブ > Monitoring > Global > AP Hardware Capability タブ > Radio 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。

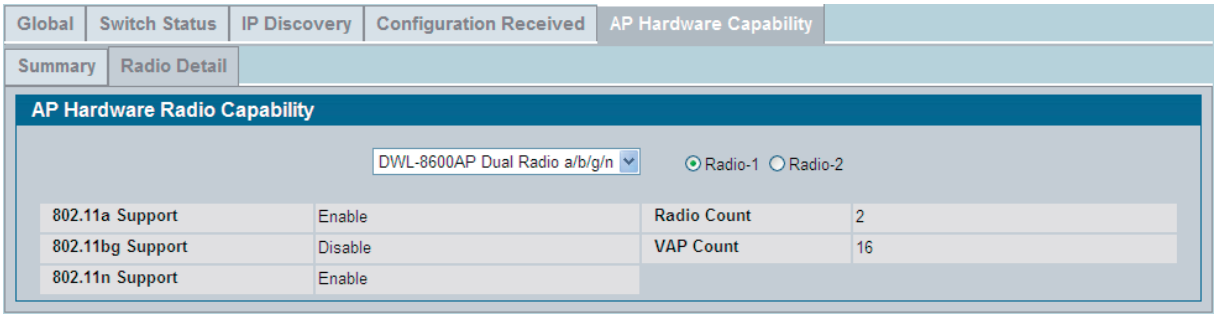


図 9-33　AP Hardware Radio Capability - Radio Detail 画面

各項目について説明します。

項目	説明
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。
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インタフェース番号（1 または 2）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。

All Access Points（すべてのアクセスポイントの状態）

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）を表示します。

WAN タブ > Monitoring > Access Point > All Access Points の順にメニューをクリックして、以下の画面を表示します。

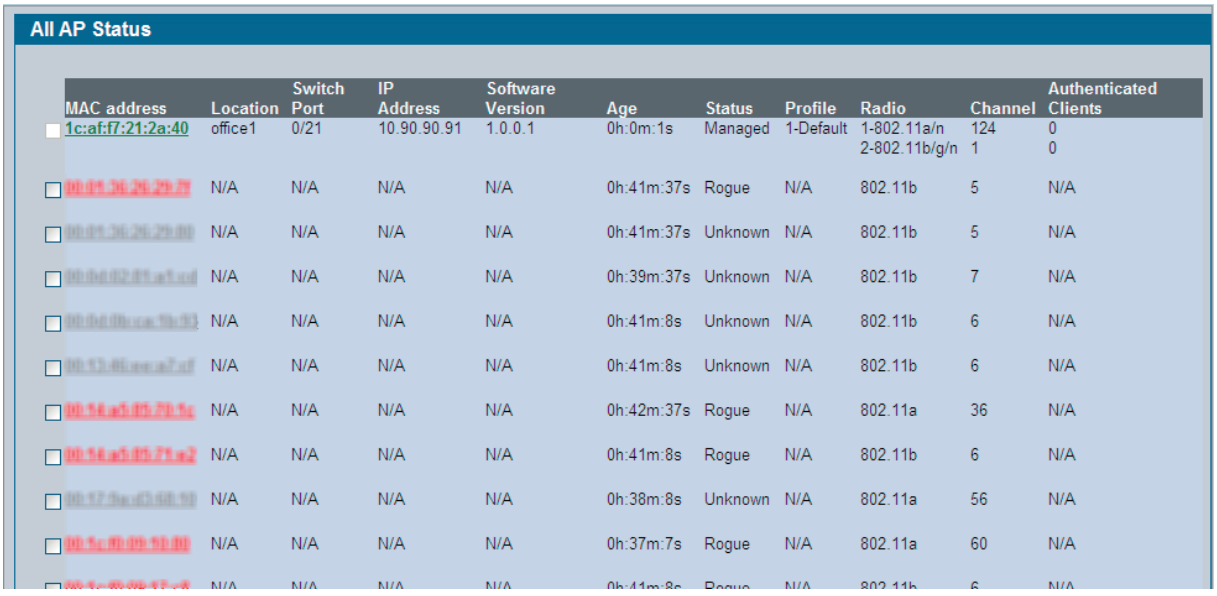


図 9-34　All AP Status 画面

リスト中のアクセスポイントの MAC アドレスの色により、以下のアクセスポイントの状態を示しています。

- 緑 - 管理されているアクセスポイント
- 赤 - エラーとなったアクセスポイント
- グレー - 不正なアクセスポイント
- 橙 - 管理されているピアアクセスポイント

手動でステータスエントリを削除することができます。管理されているアクセスポイントを除いて、「All Access Points status」ページからすべてのアクセスポイントをクリアするためには、「Delete All」ボタンをクリックします。

不正アクセスポイントの次回検出時に、スイッチが管理する認証に失敗したアクセスポイントを設定するため、MAC アドレスの左のチェックボックスを選択し、「Manage」ボタンをクリックします。「Valid Access Point Configuration」ページに表示されます。ローカルの Valid AP データベースにアクセスポイントを保存するためには、アクセスポイントを設定し、「Submit」ボタンをクリックします。アクセスポイントの認知に RADIUS サーバを使用している場合は、アクセスポイントの MAC アドレスを RADIUS サーバの AP データベースに登録する必要があります。

アクセスポイントを認識済みのローグ（不正）として定義するためには、MAC アドレスの左のチェックボックスを選択し、「Acknowledge」ボタンをクリックします。スイッチはそのアクセスポイントを認識済ローグ（不正）として Valid AP データベースに追加します。

検出されたアクセスポイントについての詳細情報を確認するためには、そのエントリの MAC アドレスをクリックしてください。

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 アドレスを示します。
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 / ポート形式）。アクセスポイントが L3 ネットワークの境界を超えている場合、「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の経過時間。
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。 • 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 "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）で変更されて新しいプロファイルが適用される場合、そのアクセスポイントは自動的に再起動します。
Radio	アクセスポイントの無線インタフェースが使用している無線モード。
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。

注意 「All AP Status」リスト内のアクセスポイントのステータス値には無効であるものも含まれています。そのような値は "N/A" と表記されます。

注意 Radio、Channel および Authenticated Clients を除きヘッダの列ごとに AP リストの順番を並び替えることができます。例えば、使用するプロファイルごとにアクセスポイントを並び替えたい場合は、"Profile" をクリックしてください。

Managed AP Status（管理対象アクセスポイントの状態）

WLAN タブ > Monitoring > Access Point > Managed AP Status 画面にアクセスすると、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確認することができます。

- 「Status」タブ - 管理対象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確認できます。
- 「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

アクセスポイントの状態のモニタリング

以下の図に 2 つの管理対象アクセスポイントが表示されている「Managed AP Status」画面の例を示します。

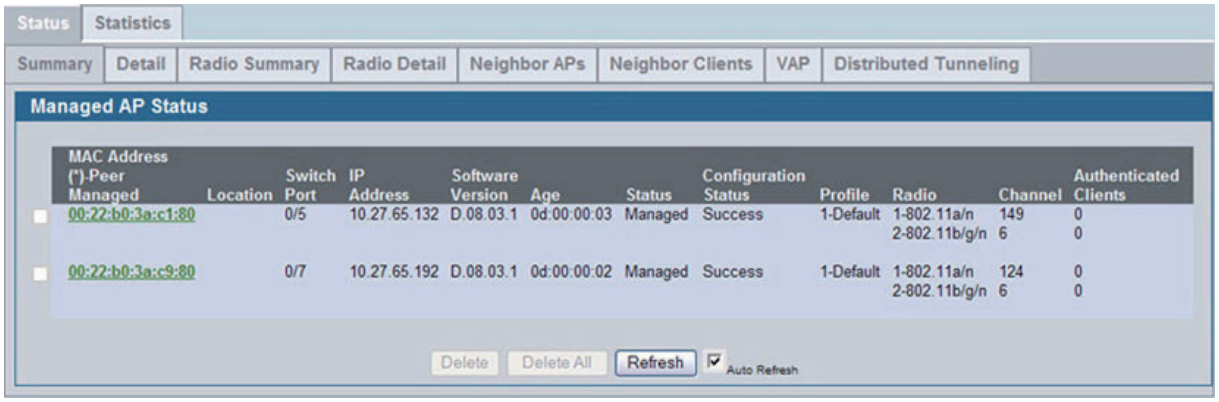


図 9-35　Managed AP Status 画面 -「Status」タブ「Summary」タブ

「Managed AP Status」画面「Status」タブでは、以下のタブが使用できます。

項目	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	無線インタフェースの詳細な状況を表示します。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当該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ついてのサマリ情報を表示します。
Distributed Tunneling	現在、アクセスポイントで使用中の L2 トンネルに関する情報を表示します。

以下の表はスイッチが管理するアクセスポイントに関するサマリ情報を提供します。スイッチがクラスタコントローラである場合、画面はクラスタ内のすべてのスイッチが管理するアクセスポイントに関する情報を提供します。

以下の表に「Managed AP Status」画面「Status」タブの「Summary」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。（*）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 / ポート形式）。アクセスポイントが L3 ネットワークの境界を超えている場合、「Unknown」が表示されます。
IP Address	管理対象アクセスポイントのネットワーク IP アドレス。
Software Version	管理対象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。
Age	統合スイッチとアクセスポイント間との最後の通信からの経過時間。
Status	アクセスポイントの状態を示します。以下の値があります。 • 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アクセスポイント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。以下の状態の一つが表示されます。 • 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。
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、新しいプロファイルが適用される場合、そのアクセスポイントは自動的に再起動します。
Radio	アクセスポイントの無線インタフェースが使用している無線モード。
Channel	無線インタフェースで運用中のチャンネル。
Authenticated Clients	インタフェースごとにアクセスポイントに接続し、認証されたクライアント数。

注意 AP リスト中のエントリの順番を、欄のヘッダをクリックすることで並び替えることができます。例えば、使用するプロファイルごとにアクセスポイントを並び替えたい場合は、"Profile" をクリックしてください。

「Delete」を使用して、現在のリストからエントリをクリアします。

注意 管理されているアクセスポイントのエントリを削除することはできません。

Detail タブ（管理対象アクセスポイントの詳細な状態を確認する）

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参照するには、「Summary」画面の「MAC Address」をクリックし、「Detail」タブ内の表の上部にあるプルダウンリストから、目的のアクセスポイントの MAC アドレスを選択します。

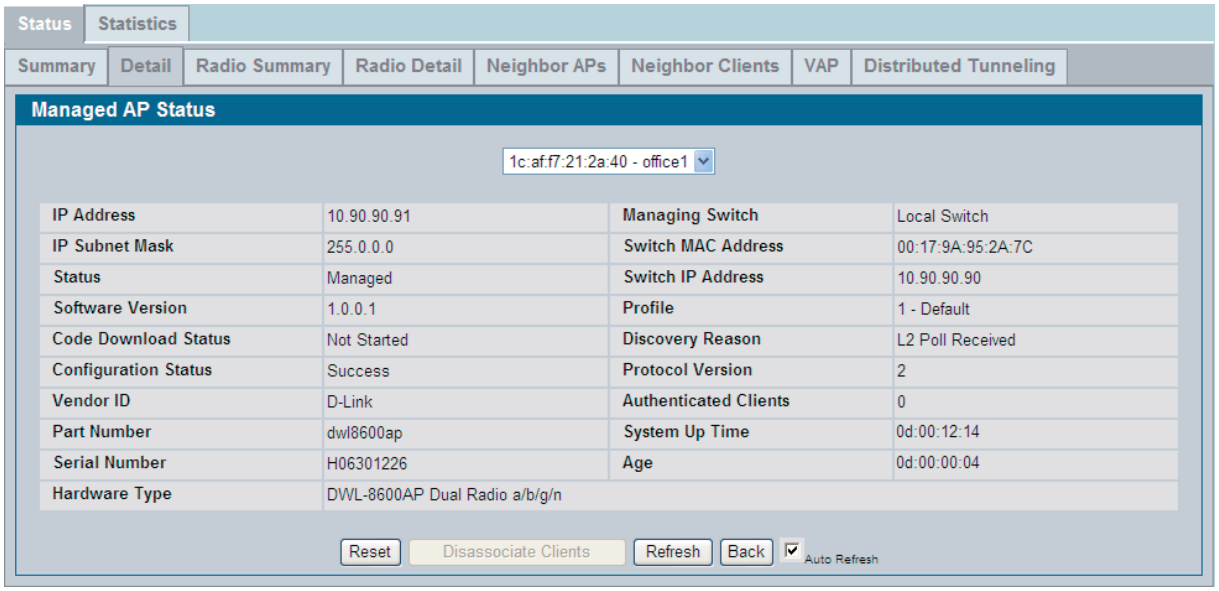


図 9-36　Managed AP Status 画面 -「Status」タブ「Detail」タブ

以下の表に「Managed AP Status」画面の「Detail」タブ内の各項目について説明します。テーブル先頭のラベルは、画面で値を適用するアクセスポイントの MAC アドレスと場所を示しています。プルダウンメニューから詳細データを表示する 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。アクセスポイントの再起動を行うかを確認するポップアップメッセージが表示されます。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。

項目	説明
IP Address	管理アクセスポイントの IP アドレス。
IP Subnet Mask	管理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状態を示します。以下の値があります。 • 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。 • Connection 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アクセスポイント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取得される情報です。
Code Download Status	アクセスポイントへの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。以下の状態の一つが表示されます。 • 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廃止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。

項目	説明
Configuration Status	アクセスポイントに割り当てられているプロファイルで設定が成功したかどうかを確認できます。 以下の状態の一つが表示されます。 • 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。
Configuration Failure Error Message	「Configuration Status」で "Partial Success"、"Complete Failure" が表示されている場合、コンフィグレーション中に失敗した最後のエレメントに関する情報が表示されます。本項目には最後に失敗した設定エレメントについてのエラーメッセージを含むアクセスポイントからの ASCII 文字情報が表示されます。
Configuration Failure Element	「Configuration Status」には "Partial Success"、"Complete Failure" が表示されます。最後に失敗した設定エレメントのエレメント ID を表示します。
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	本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。
Switch MAC Address	アクセスポイントを管理しているスイッチの MAC アドレスを示します。
Switch IP Address	アクセスポイントを管理しているスイッチの IP アドレスを示します。
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、新しいプロファイルが適用される場合、その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。以下の一つが表示されます。 • 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の IP アドレスを RADIUS サーバからの応答により取得）。 • Switch IP Configured - 管理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 - 管理アクセスポイントは DWL-8600AP の IP アドレスを DHCP オプション 43 を通じて取得した。 • 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。
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。アクセスポイントの検出の際に取得される情報です。
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。単位は秒。
Age	統合スイッチとアクセスポイント間との最後の通信からの経過時間。

Radio Summary タブ（管理対象アクセスポイントの無線サマリ情報の参照）

スイッチ管理下のアクセスポイント上で動作する各無線インタフェースに関する一般情報を参照することができます。「Managed AP Radio Summary」ページでは、すべての管理対象アクセスポイントについてチャンネル、送信電力、および接続中のクライアントの情報を確認できます。特定のアクセスポイント上での無線インタフェースについての詳細情報は、該当する無線インタフェースをクリックして表示してください。

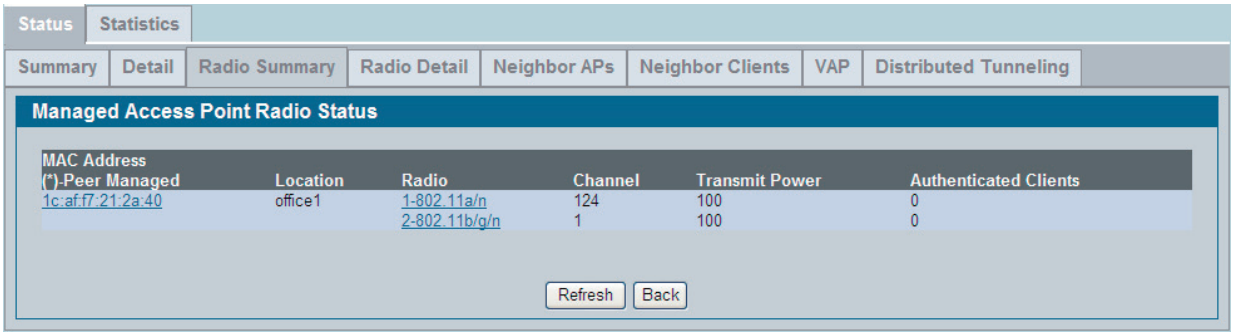


図 9-37　Managed AP Status 画面 -「Status」タブ「Radio Summary」タブ

以下の表に「Managed AP Status」画面の「Radio Summary」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。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された無線モード。無線インタフェース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。
Channel	無線インタフェースが有効な場合、現在動作状態にあるチャンネルが表示されます。
Transmit Power	無線インタフェースが有効である場合は、現在の送信電力が表示されます。
Authenticated Clients	物理インタフェース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。

Radio Detail タブ（管理対象アクセスポイントの無線詳細情報の参照）

統合スイッチの管理対象のアクセスポイント上の各無線インタフェースについての詳細情報は、「Managed AP Status」ページの「Radio Detail」タブで参照することができます。上記テーブルのオプションメニューを使用して、参照する情報を持つアクセスポイントとその無線モードを選択します。各アクセスポイントは MAC アドレスとロケーションで識別されます。各インタフェースは、無線ネットワーク番号と設定モードにより識別されます。無線インタフェースが無効に設定されていれば、無線モードには、「Off」と表示されます。

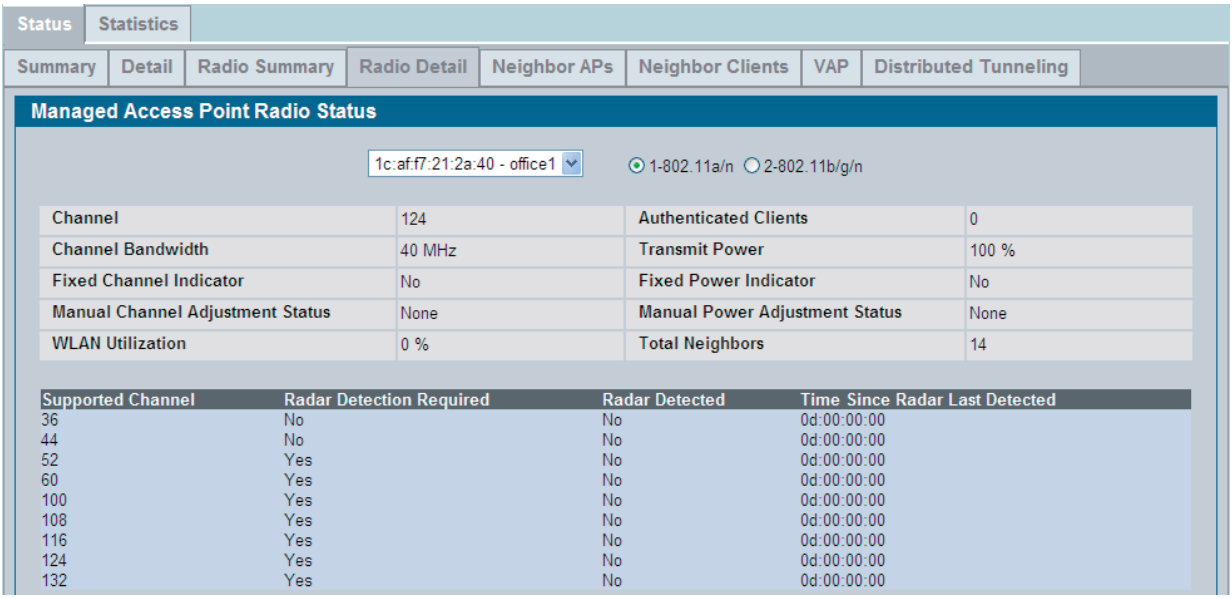


図 9-38　Managed AP Status 画面 -「Status」タブ「Radio Summary」タブ

以下の表に「Managed AP Status」画面の「Status」タブの「Radio Detail」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	無線インタフェースが有効な場合、現在動作状態にあるチャンネルが表示されます。
Channel Bandwidth	チャンネル帯域幅が 20MHz または 40MHz のいずれかであることを示します。
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。以下の一つが表示されます。 • 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	物理帯域でのネットワーク使用率の合計を示します。この値は無線統計情報を元にしています。
Authenticated Clients	物理インタフェースにあるアクセスポイントに認証されたクライアントの合計数。指定した無線モードで有効な 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	無線インタフェースが有効である場合は、現在の送信電力が表示されます。
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。
Fixed Power Indicator	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 1 つが表示されます。 • 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。

IEEE 802.11a、IEEE 802.11a/n、または 5GHz 802.11n をサポートする無線インタフェースに対しては、電波検知情報を持つ追加テーブルを表示します。

項目	説明
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 タブ（管理対象アクセスポイントの隣接アクセスポイントの参照）

RF スキャン中、アクセスポイントは隣接アクセスポイントから送信されているビーコン情報を収集し保存しています。アクセスポイントは、最大 64 台の隣接アクセスポイントの情報を保存できます。隣接スキャン情報が許容量を超えると、古いデータは上書きされます。

メニューを使用して、表示する隣接アクセスポイント情報を持つアクセスポイントを選択します。アクセスポイントは MAC アドレスとロケーションで識別されます。アクセスポイントに 2 つの無線インタフェースがある場合、無線インタフェースを選択し、そのインタフェースで RF スキャンを行うことで検出された隣接アクセスポイントを表示します。各インタフェースは、無線ネットワーク番号と設定モードにより識別されます。無線インタフェースが無効に設定されていれば、無線モードには、「Off」と表示されます。

「Delete All Neighbors」ボタンをクリックすると、「Neighbor APs and Neighbor Clients」リスト内のデータをすべて削除します。削除後は、新規に検出された隣接アクセスポイントの情報を書きます。

「Neighbor Clients」タブをクリックし、「Managed Access Point Neighbor AP Status」画面を表示します。

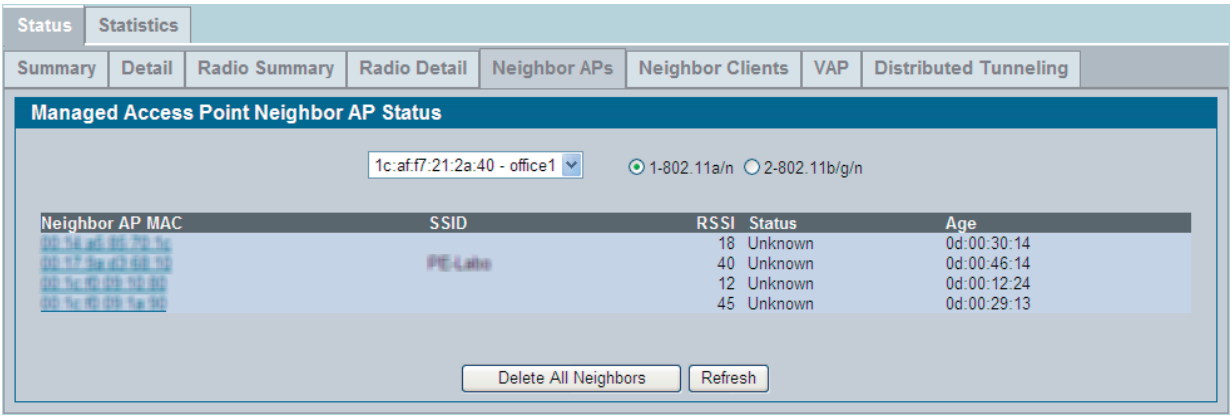


図 9-39　Managed AP Status 画面 -「Status」タブ「Neighbor APs」タブ

以下の表に「Managed AP Status」画面の「Status」タブの「Neighbor APs」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 受信信号強度表示信号。
RSSI	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、管理対象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 です。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 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	無線インタフェースで、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の経過時間。

Neighbor Clients タブ（隣接アクセスポイントに接続中のクライアントの参照）

「Neighbor Clients」タブを使用すると、指定したアクセスポイントにより検出された無線クライアントの情報を表示します。アクセスポイントは 512 台の無線クライアントの情報を保存できます。クライアントの情報が許容量を超えると、古いデータから上書きされます。

メニューを使用して、表示するクライアント情報を持つアクセスポイントを選択します。アクセスポイントは MAC アドレスとロケーションで識別されます。アクセスポイントに 2 つの無線インタフェースがある場合、無線インタフェースを選択し、そのインタフェースで RF スキャンを行うことで検出された隣接クライアントを表示します。各インタフェースは、無線ネットワーク番号と設定モードにより識別されます。無線インタフェースが無効に設定されていれば、無線モードには、「Off」と表示されます。

「Delete All Neighbors」ボタンをクリックすると、「Neighbor APs and Neighbor Clients」リスト内のデータをすべて削除します。削除後は、新規に検出された隣接アクセスポイントの情報が書かれ、接続するクライアントが検出されます。

隣接する管理アクセスポイントに接続するクライアントののステータスを参照するためには「Neighbor Clients」タブをクリックし、「Managed Access Point Neighbor Client Status」画面を表示します。

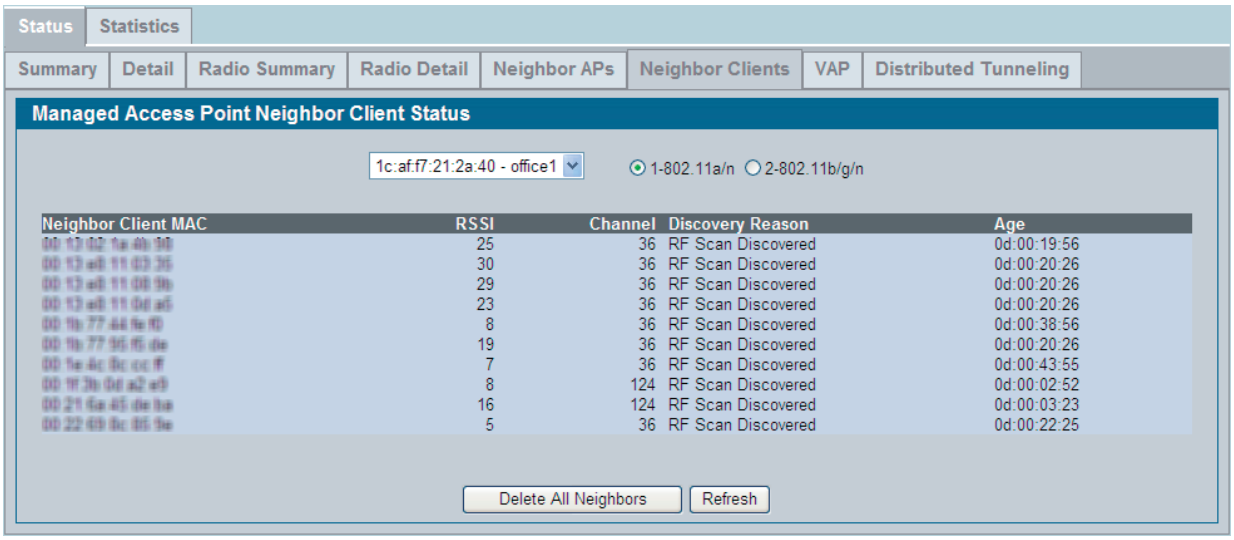


図 9-40　Managed AP Status 画面 -「Status」タブ「Neighbor Clients」タブ

以下の表に「Managed AP Status」ページの「Neighbor Clients」タブ内の各項目について説明します。

項目	説明
Neighbor Client MAC	クライアントの MAC アドレス。
RSSI	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、管理対象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 です。1 が最も弱い信号強度です。
Channel	クライアントからのフレームを受信した管理対象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 Discovered - クライアントが無線インタフェースの 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の経過時間。

VAP タブ（管理対象アクセスポイントの仮想アクセスポイントの参照）

1 台のアクセスポイントの各インタフェースに対して 16 個までの仮想アクセスポイント（VAP）を設定できます。スイッチの管理下のアクセスポイントの各無線インタフェースに設定した VAP の設定サマリ情報、および各 VAP に接続中のクライアントの数を表示することができます。「VAP」タブをクリックし、「Managed Access Point VAP Status」を表示します。

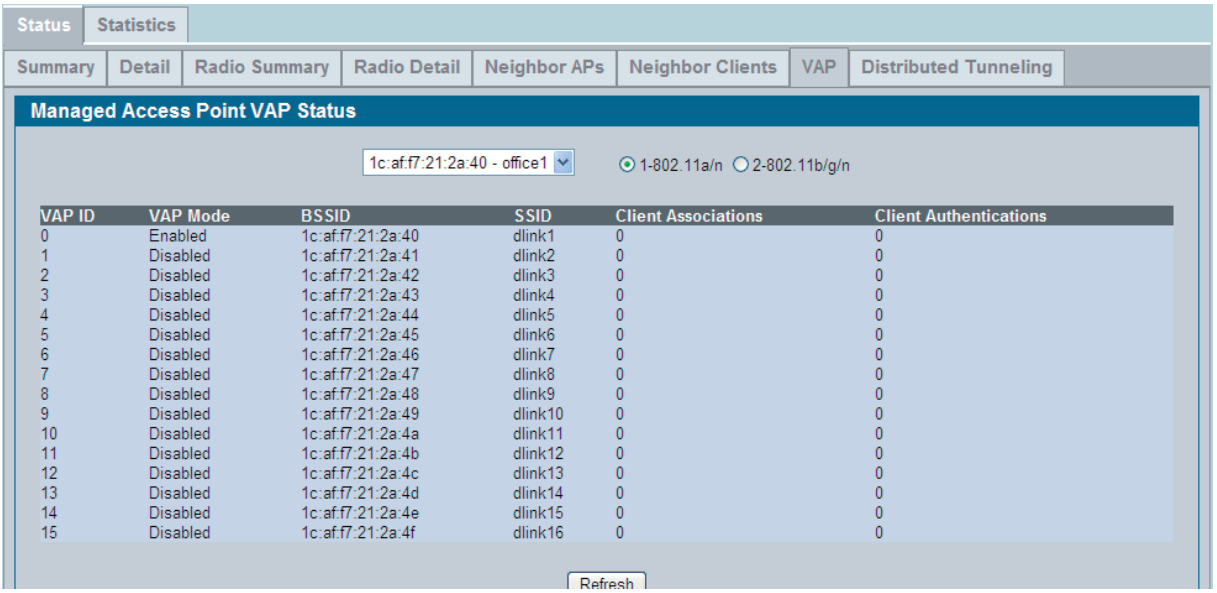


図 9-41　Managed AP Status 画面 -「Status」タブ「VAP」タブ

テーブルの上にあるメニューを使用して、表示する VAP 情報を持つアクセスポイントを選択します。アクセスポイントは MAC アドレスとロケーションで識別されます。アクセスポイントに 2 つの無線インタフェースがある場合、無線インタフェースを選択し、そのインタフェースの VAP に関する詳細を表示します。各インタフェースは、無線ネットワーク番号と設定モードにより識別されます。無線インタフェースが無効に設定されていれば、無線モードには、「Off」と表示されます。

以下の表に「Managed Access Point Status」ページの「VAP」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）。これは、CLI または SNMP 経由の設定に対して VAP を識別するために使用します。
VAP Mode	VAP の有効または無効を表示します。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 Associations	VAP に現在接続中のクライアントの総数。
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 タブ（Distributed トンネル情報の参照）

AP-AP トンネルモードは、無線スイッチに何のデータトラフィックも送信せずに無線クライアントに L3 ローミングをサポートするために使用されます。

AP-AP トンネルモードでは、クライアントが最初に無線システムでアクセスポイントに接続する場合、アクセスポイントは、VLAN のフォワーディングモードを使用することで無線クライアントのデータを転送します。クライアントが最初に接続するアクセスポイントをホーム AP と呼びます。クライアントがローミングするアクセスポイントをアソシエーション AP と呼びます。

テーブル上の各メニューを使用して、Distributed トンネル情報を持つアクセスポイントを選択します。アクセスポイントは MAC アドレスとロケーションで識別されます。

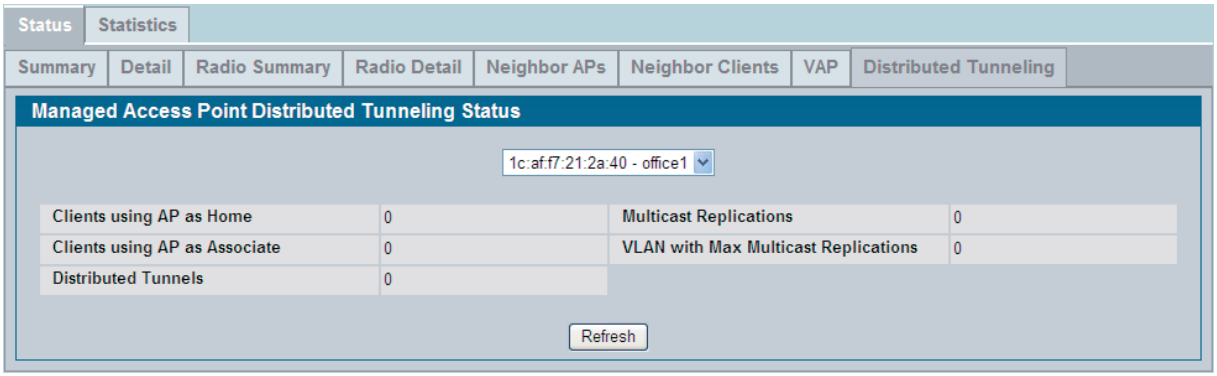


図 9-42　Managed AP Status 画面 -「Status」タブ「Distributed Tunneling」タブ

管理アクセスポイントのステータスに対しては、以下の表に「Managed Access Point Distributed Tunneling Status」画面の各項目について説明します。

項目	説明
Distributed Tunnel Clients using AP as Home	Distributed 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送するクライアントの数。
Distributed Tunnel Clients using AP as Associate	Distributed 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るクライアントの数。
Distributed Tunnels	このアクセスポイントとの Distributed 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。
Distributed Tunnel 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	Distributed 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 タブ（管理アクセスポイントの統計情報）

管理アクセスポイントの統計情報からは、アクセスポイント上の有線 / 無線インタフェースのトラフィックの情報が確認できます。本情報をスループットの問題などネットワークのトラブルの診断に役立てることができます。

WLAN タブ > Monitoring > Access Point > Managed AP Status とクリックし、「Statistics」タブをクリックします。

以下の図は、管理アクセスポイントを表示する「Managed Access Point Statistics」画面の例です。

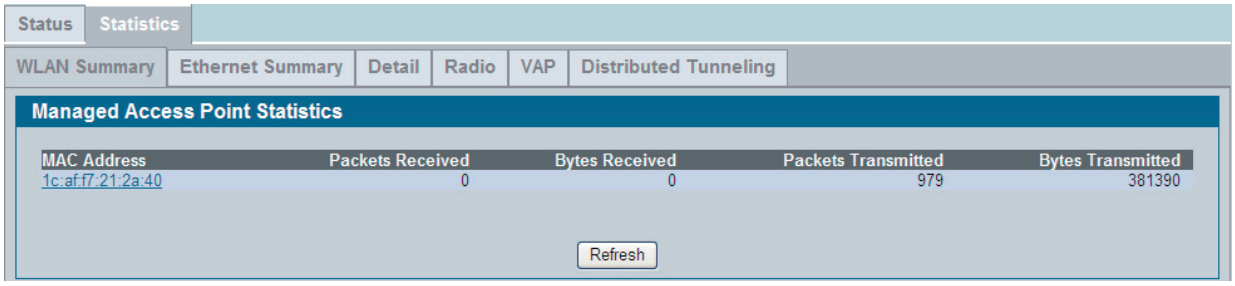


図 9-43　Managed Access Point Statistics 画面 -「Statistics」タブ「WLAN Summary」タブ

「Managed Access Point Statistics」ページには以下のタブが利用できます。

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	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無線インタフェースごとに表示します。
VAP	指定の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	現在、アクセスポイントで使用中の L2 トンネルに関する情報を表示します。

「WLAN Summary」タブや「Ethernet 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。

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	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。単位はバイトです。
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。単位はバイトです。

注意　AP リスト中のエントリの順番を、欄のヘッダをクリックすることで並び替えることができます。例えば、送信パケット数の順番でアクセスポイントを並び替える場合は、"Packets Transmitted" をクリックします。

Ethernet Summary タブ（管理対象アクセスポイントのイーサネット統計情報の参照）

「Ethernet Summary」タブでは、スイッチの管理下にあるアクセスポイントの有線（イーサネット）インタフェースが送受信したパケット数およびデータ量を表示します。有線インタフェースは LAN と物理的に接続しています。

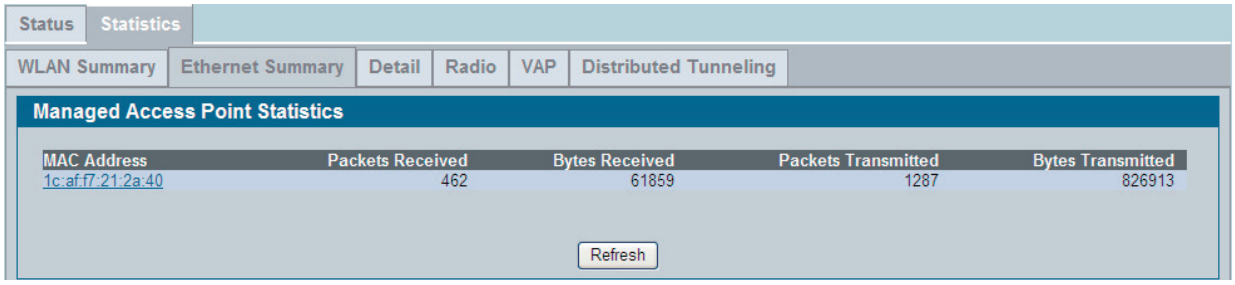


図 9-44　Managed Access Point Statistics 画面 -「Statistics」タブ「Ethernet Summary」タブ

以下の表は「Managed Access Point Statistics」ページの「Ethernet Summary」タブ内の項目の情報を示します。

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。単位はバイトです。
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。単位はバイトです。

Detail タブ（管理対象アクセスポイントの統計詳細情報の参照）

「Detail」タブでは、スイッチ管理下にある指定したアクセスポイントの無線/有線インタフェースで送受信したパケットの数とデータ量を表示します。スイッチの管理下にあるアクセスポイントの統計情報を参照するには、「Detail」タブ内の表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。また、利用可能であるなら、MAC アドレスと共にロケーションを表示します。

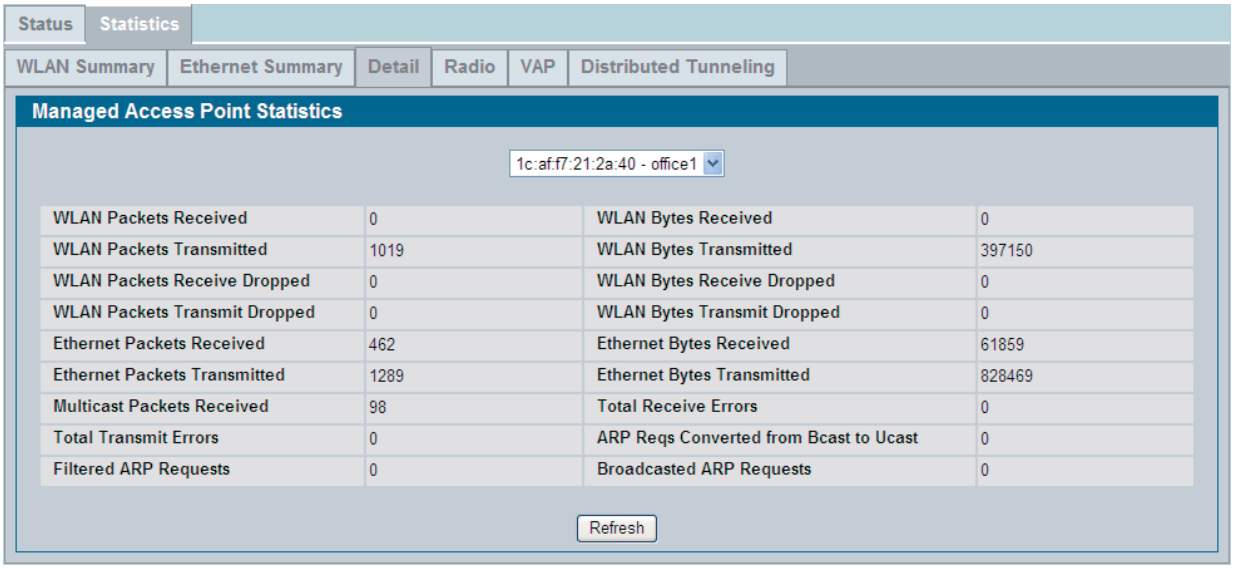


図 9-45　Managed Access Point Statistics 画面 -「Statistics」タブ「Detail」タブ

以下の表は「Managed Access Point Statistics」画面の「Detail」タブ内の項目の情報を示します。

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。単位はバイトです。
WLAN Bytes Received	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。単位はバイトです。
WLAN Packets Receive 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 Receive 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 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。単位はバイトです。
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。単位はバイトです。
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 Requests	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。

Radio タブ（管理対象アクセスポイントの無線統計情報の参照）

「Radio」タブでは、スイッチの管理下の指定アクセスポイントについて、無線インタフェースの送受信パケット数、内容などの詳細情報を参照できます。

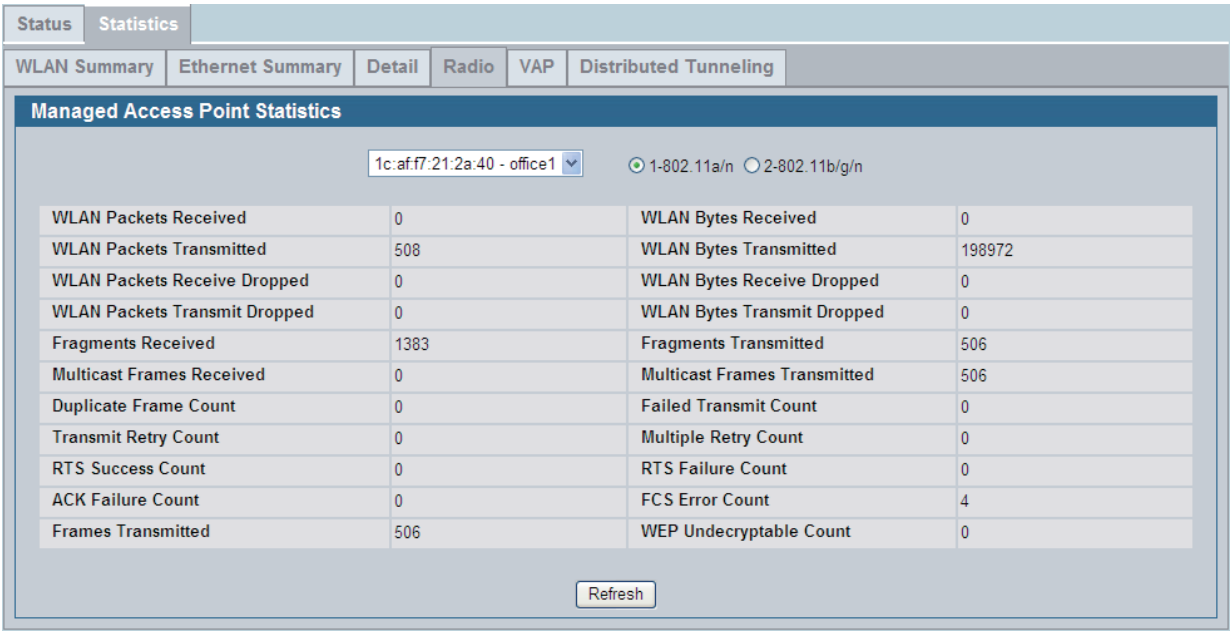


図 9-46　Managed Access Point Statistics 画面 -「Statistics」タブ「Radio」タブ

テーブル上部のオプションメニューを使用して、参照する情報を持つアクセスポイントとその無線モードを選択します。アクセスポイントは MAC アドレスとロケーションで識別されます。各インタフェースは、無線ネットワーク番号と設定モードにより識別されます。無線インタフェースが無効に設定されていれば、無線モードには、「Off」と表示されます。

以下の表は「Managed Access Point Statistics」ページの「Radio」タブ内の項目の情報を示します。

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。単位はバイトです。
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。単位はバイトです。
WLAN Packets Receive 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 Receive 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）。
Fragments Received	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。

VAP タブ（管理対象アクセスポイントの VAP 統計情報の参照）

「VAP」タブでは、アクセスポイント上の指定インタフェースに定義されている VAP へのクライアントの接続・認証の失敗や、各 VAP が送受信したパケット数やデータ量の統計情報を参照できます。

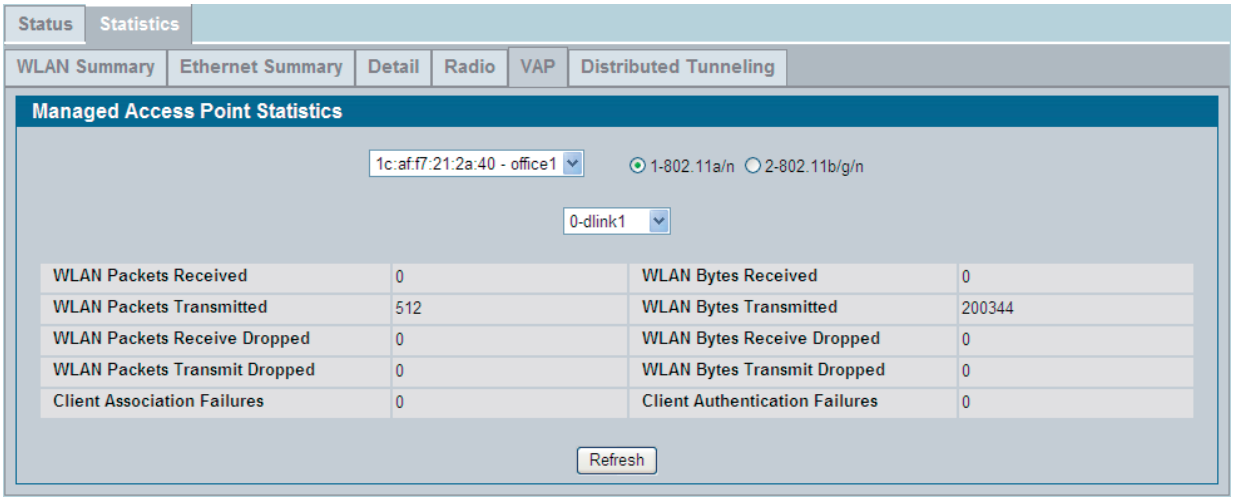


図 9-47　Managed Access Point Statistics 画面 -「Statistics」タブ「VAP」タブ

テーブル上部のオプションメニューを使用して、参照する情報を持つアクセスポイント、その無線モードおよび VAP を選択します。アクセスポイントは MAC アドレスとロケーションで識別されます。各インタフェースは、無線ネットワーク番号と設定モードにより識別されます。無線インタフェースが無効に設定されていれば、無線モードには、「Off」と表示されます。VAP は VAP ID とその SSID によって特定される。VAP の状態（有効 / 無効）に関わらず選択できます。

以下の表は「Managed Access Point Statistics」ページの「VAP」タブ内の項目の情報を示します。

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 Bytes Received	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 Receive Dropped	この VAP 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 Receive Dropped	この VAP 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	この VAP 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 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）。
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。

Distributed Tunneling タブ（Distributed トンネル統計情報の参照）

「Distributed Tunneling」タブでは、スイッチの管理下にある 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数およびデータ量に関する情報を表示します。

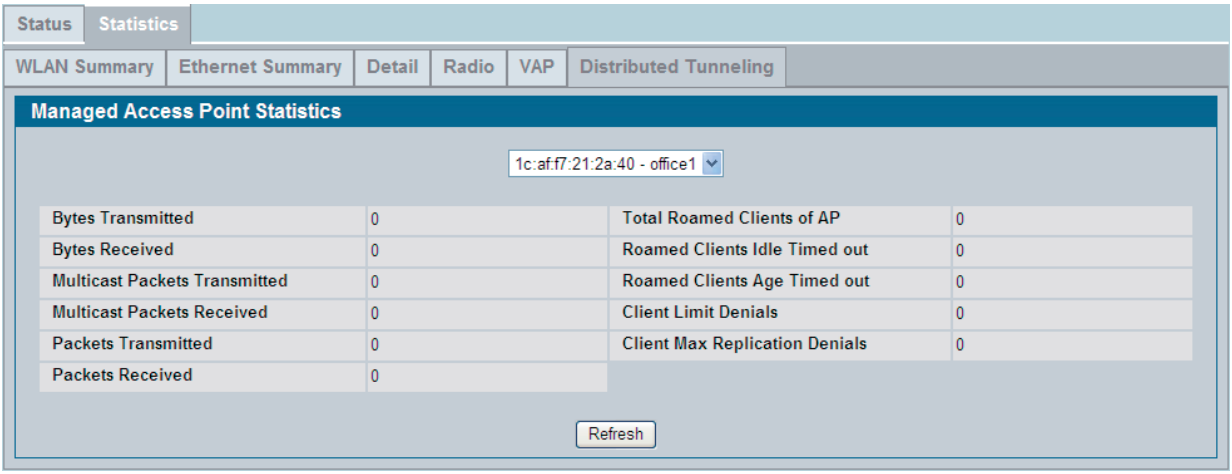


図 9-48　Managed Access Point Statistics 画面 -「Statistics」タブ「Distributed Tunneling」タブ

テーブルの上にあるメニューを使用して、表示する設定を持つアクセスポイントを選択します。アクセスポイントは MAC アドレスとロケーションで識別されます。

以下の表は、管理アクセスポイント統計情報のための「Distributed Tunneling」ページの項目についてを示します。

項目	説明
Bytes Transmitted	すべての Distributed トンネルを経由してアクセスポイントが送信した総データ量（バイト）。
Bytes Received	すべての Distributed トンネルを経由してアクセスポイントが受信した総データ量（バイト）。
Multicast Packets Transmitted	すべての Distributed トンネルを経由してアクセスポイントが送信したマルチキャストパケットの合計。
Multicast Packets Received	すべての Distributed トンネルを経由してアクセスポイントが受信したマルチキャストパケットの合計。
Packets Transmitted	すべての Distributed トンネルを経由してアクセスポイントが送信した総パケット数。
Packets Received	すべての Distributed トンネルを経由してアクセスポイントが受信した総パケット数。
Total Roamed Clients of AP	Distributed トンネルのために、このアクセスポイントを使用したクライアントの数。このカウントにはローミングをしてこのアクセスポイントから離れていったもの、および接続したものが含まれます。
Roamed Clients Idle Timed Out	このアクセスポイントから離れたために、トンネルにトラフィックを送信できずにタイムアウトになったクライアントの数。
Roamed Clients Age Timed Out	このアクセスポイントから離れたために、トンネルの有効期限が過ぎてタイムアウトになったクライアントの数。
Client Limit Denials	トンネルクライアント数の制限にアクセスポイントが到達したために、クライアントによる Distributed トンネル設定を拒否した回数。
Client Max Replication Denials	VLAN レプリケーションの最大数にアクセスポイントが到達したために、クライアントによる Distributed トンネル設定を拒否した回数。

Associated Client（接続クライアントの状態 / 統計情報）

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、様々な情報を参照することができます。

WLAN タブ > Monitoring > Client > Associated 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。

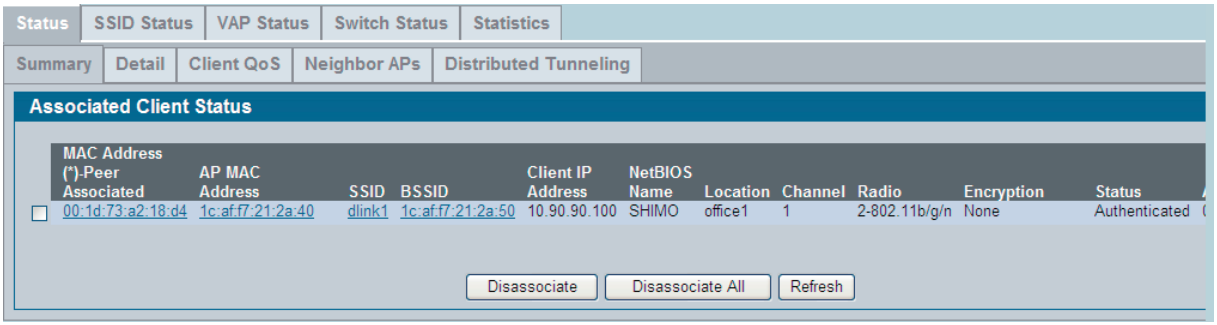


図 9-49　Associated Client Status 画面

「Associated Client」ページでは、以下のタブが使用できます。

項目	説明
Status	スイッチが管理するアクセスポイントと接続中のクライアントの状態を表示します。以下の情報が含まれます。 • Summary - 接続中のクライアントの基本的な情報を表示します。 • 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 やクライアントがアクティブでない時間など）。 • 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 Distributed トンネル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 アドレスを表示します。
VAP Status	アクセスポイント上の指定 VAP に接続中のクライアントを表示します。
Statistics	スイッチ管理下の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。 • Association 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を表示します。 • Session Summary - クライアントが、異なる管理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を表示します。 • Association Detail - 1 台の管理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追加情報を表示します。 • Session Detail - 接続するクライアントがセッション中に送受信するパケットに関する追加情報を表示します。クライアントがローミングを行った 1 台以上の管理アクセスポイントの統計情報を含みます。

接続クライアントデータベースがアクセスポイント間のローミングをサポートするため、クライアントがあるアクセスポイントと接続を終了しても、エントリは削除されません。接続終了後のエントリは、クライアントのタイムアウト時間後に削除されます。このタイムアウト時間は、**WLAN タブ > Administration > Advanced Configuration > Global** の「Client Roam Timeout」で設定できます。このタイムアウト時間はクライアントが他の管理アクセスポイントにローミングするために許可された時間と一致します。

Status タブ

Summary タブ（接続中のクライアントのステータスサマリの参照）

接続中のクライアントの情報を表示します。

WLAN タブ > Monitoring > Client > Associated Clients > Status タブ > 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。

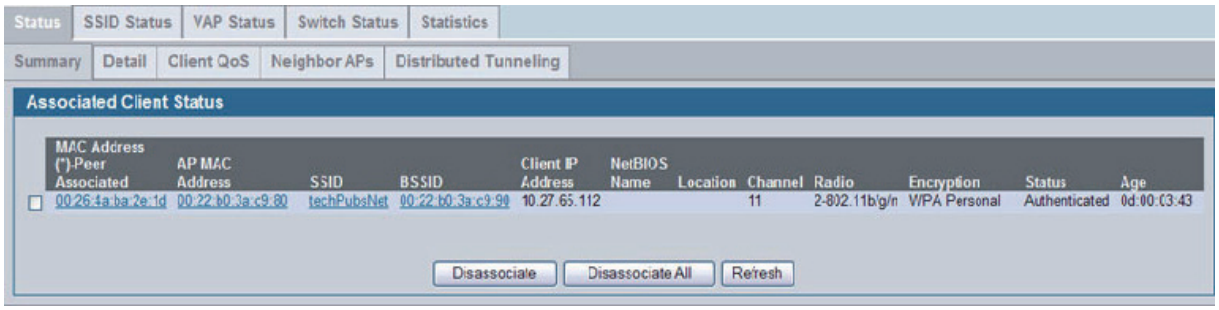


図 9-50　Associated Client Status 画面 -「Status」タブ「Summary」タブ

以下の項目が表示されます。

項目	説明
MAC Address	クライアントステーションの MAC アドレス。MAC アドレスのあとに（*）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。
AP MAC Address	アクセスポイントの MAC アドレス。
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。
Client IP Address	必要に応じて接続するクライアントの IP アドレスを示します。
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。
Location	アクセスポイントの場所。
Channel	クライアントの接続に使用されているチャンネル。
Radio	無線インタフェースとモード。
Encryption	使用中の暗号化タイプ。
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。
Age	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。

Detail タブ（接続中のクライアントの詳細情報の参照）

スイッチの管理下にあるアクセスポイントと接続中の各クライアントについて、詳細な接続状況を確認することができます。テーブル上部にあるメニューを使用して、参照する情報を持つクライアントの MAC アドレスを選択します。

WLAN タブ > Monitoring > Client > Associated Clients > Status タブ > 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。

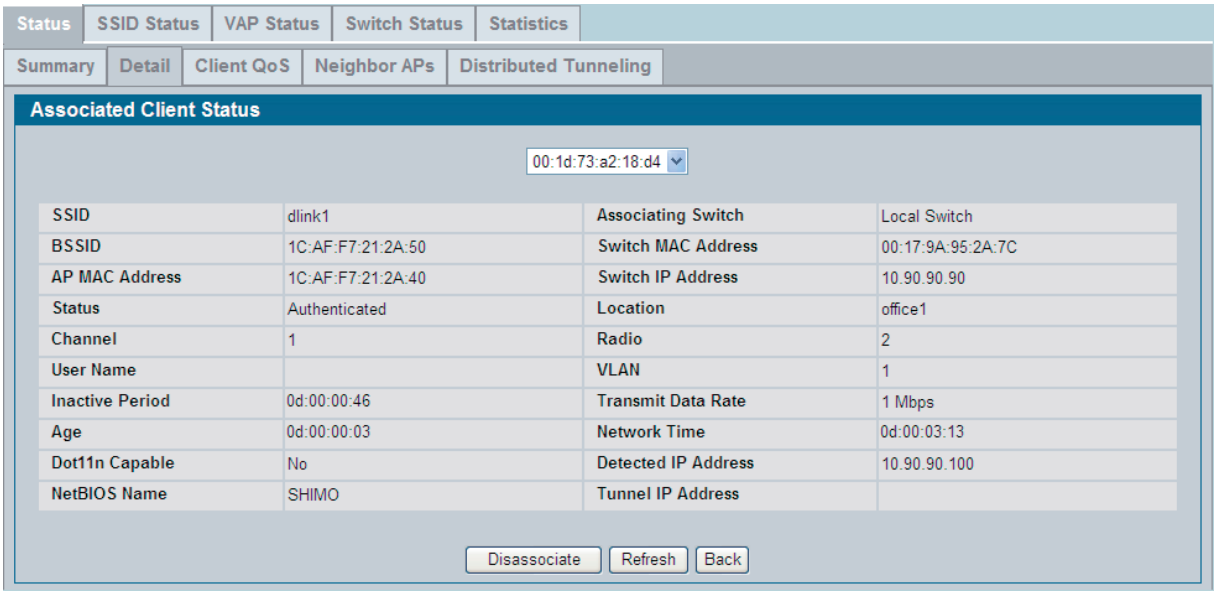


図 9-51　Associated Client Status 画面 -「Status」タブ「Detail」タブ

以下の表は「Associated Client Status」ページの「Detail」タブ内の項目の情報を示します。

項目	説明
SSID	クライアントが接続しているネットワークを示します。
BSSID	クライアントが接続中のアクセスポイントの VAP の MAC アドレス。
AP MAC Address	管理対象アクセスポイントの MAC アドレス。
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。以下の一つが表示されます。 • 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しているチャンネル。
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に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	このクライアントの新しいステータスおよび更新統計情報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、通常ホスト名に同じか、またはホスト名に基づいています。
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。
Switch MAC 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 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	管理対象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。
VLAN	クライアントが VAP と接続中で VLAN データ送信モードである時、現在割り当てられている VLAN を表示します。
Transmit Data Rate	クライアントの現在のデータ送信速度。
Network Time	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。
Detected IP Address	必要に応じ、クライアントの IPv4 アドレスを表示します。
Tunnel IP Address	トンネルを使用しないクライアントの場合、何も表示されません。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。
Captive Portal	クライアントがキャピタルポータルを通じて認証される場合、本項目には関連する「Captive Portal client status」画面へのリンクがあります。キャピタルポータルが有効なスイッチ設定にだけ、本欄は表示されます。

Client QoS タブ（接続中のクライアントの QoS 状態の参照）

スイッチが管理するアクセスポイントに接続する各クライアントの帯域制限について情報を表示します。テーブル上部にあるメニューを使用して、参照する情報を持つクライアントの MAC アドレスを選択します。

WLAN タブ > Monitoring > Client > Associated Clients > Status タブ > Client QoS 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。

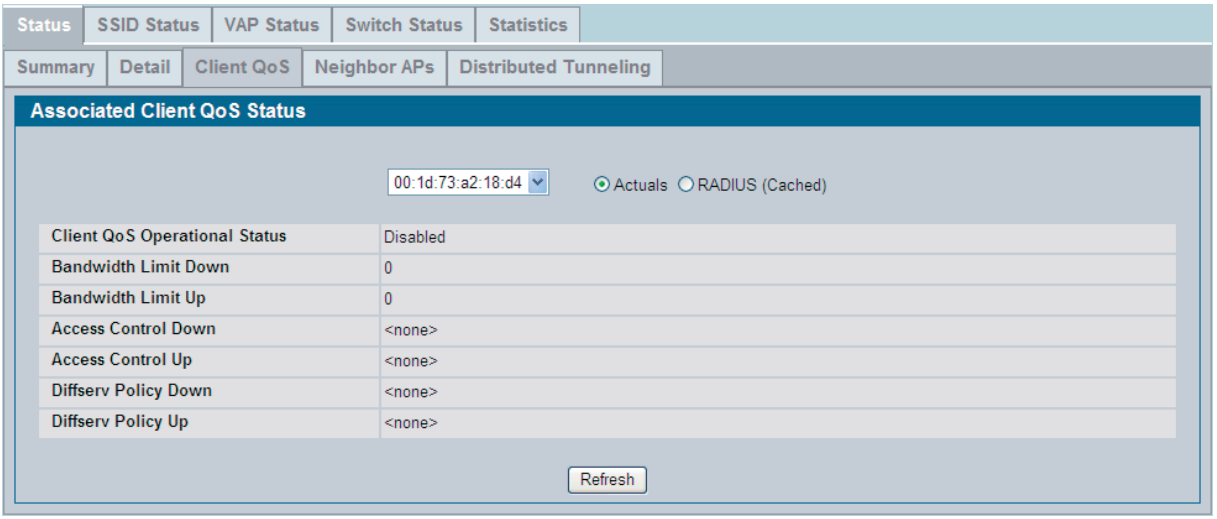


図 9-52　Associated Client QoS Status 画面 -「Status」タブ「Client QoS」タブ

以下の表には「Associated Client Status」ページの「Client QoS 」タブ内の項目の情報を表示します。

項目	説明
Actual RADIUS (Cached)	セレクタを使用して、画面が表示する情報のソースを決定します。 • Actual - 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 (Cached) - 802.1X 認証を使用する場合、RADIUS からクライアント用に取得するクライアントの 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 は、帯域幅に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 は、帯域幅に制限がないことを意味します。
Access Control Down	どの ACL が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かを表示します。
Access Control Up	どの ACL が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かを表示します。
Diffserv Policy Down	どの DiffServ ポリシーが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かを表示します。
Diffserv Policy Up	どの DiffServ ポリシーが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かを表示します。

Neighbor APs タブ（接続中のクライアントの隣接アクセスポイントの状態の参照）

接続中のクライアントの状態のために、クライアントを検出するアクセスポイントの情報を参照することができます。表示する情報は、接続中のクライアントがローミングするために使用するアクセスポイントを決定する際に役立てることができます。テーブル上部にあるメニューを使用して、参照する情報を持つクライアントの MAC アドレスを選択します。

WLAN タブ > Monitoring > Client > Associated Clients > Status タブ > Neighbor APs の順にメニューをクリックし、以下の画面を表示します。

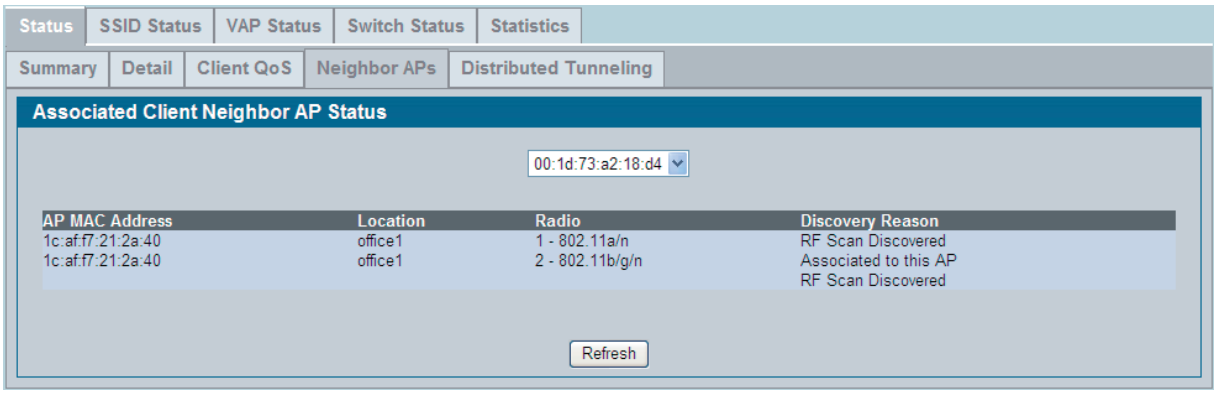


図 9-53　Associated Client Neighbor AP Status 画面 -「Status」タブ「Neighbor AP」タブ

以下の表には「Associated Client Status」ページの「Neighbor AP」タブ内の情報を表示します。

項目	説明
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	アクセスポイントの場所。
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 Discovered - 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。

Distributed Tunneling タブ（接続中のクライアントの配布トンネル状態の参照）

接続中のクライアントの状態のために、クライアントを検出するアクセスポイントの情報を参照することができます。AP-AP トンネルモードは、無線スイッチに何のデータトラフィックも送信せずに無線クライアントに L3 ローミングをサポートするために使用されます。

AP-AP トンネリングモードで、クライアントが最初に無線システムでアクセスポイントに接続する場合、アクセスポイントは、VLAN のフォワーディングモードを使用することで無線クライアントのデータを転送します。クライアントが最初に接続するアクセスポイントをホーム AP と呼びます。クライアントがローミングするアクセスポイントをアソシエーション AP と呼びます。

WLAN タブ > Monitoring > Client > Associated Clients > Status タブ > 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。テーブル上部にあるメニューを使用して、参照する情報を持つクライアントの MAC アドレスを選択します。

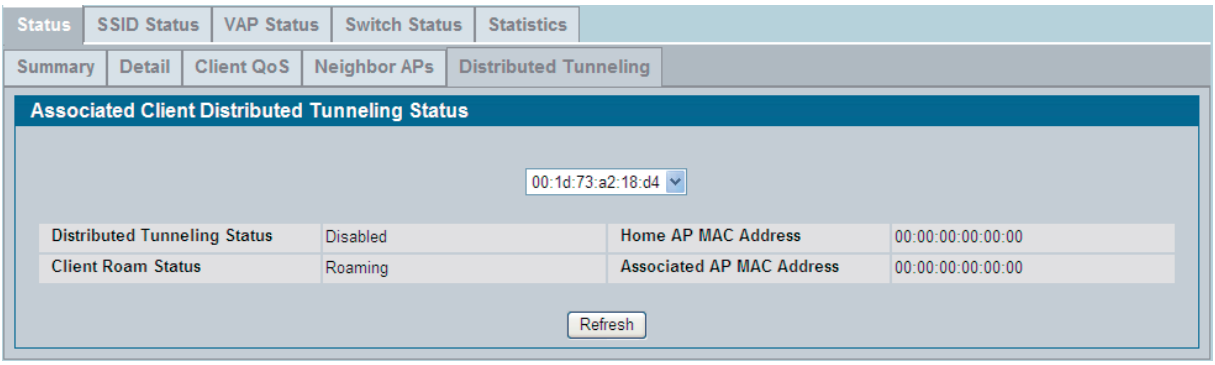


図 9-54　Associated Client Distributed Tunneling Status 画面

以下の表には「Associated Client Status」ページの「Distributed Tunneling」タブ内の情報を表示します。

項目	説明
Distributed Tunneling Status	このクライアントが L2 の Distributed トンネルをサポートするネットワークに接続する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、トンネルを使用しているかどうかを表示しています。本フィールド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。 Distributed トンネリングを無効にすると、フィールドにはローミング状況を「Roaming」として表示されます。
Home AP MAC Address	クライアント対するホーム AP の MAC アドレス。この値は、Distributed 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 Distributed トンネルプロトコルを通じて接続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（SSID の関連クライアント状態の参照）

各アクセスポイントは、それぞれ異なる SSID を持つ 16 個までのネットワークを持つことができます。複数のクライアントが同一の物理アクセスポイントに接続していても、同じ SSID を使用して接続していない場合もあります。「SSID Status」タブでは、管理アクセスポイントに接続する無線クライアントが無線 LAN アクセスに使用するネットワークの SSID を表示します。

WLAN タブ > Monitoring > Client > Associated Clients > SSID Status タブの順にメニューをクリックします。アクセスポイントからクライアントの接続を終了するためには、SSID の横のボックスを選択し、「Disassociate」ボタンをクリックします。

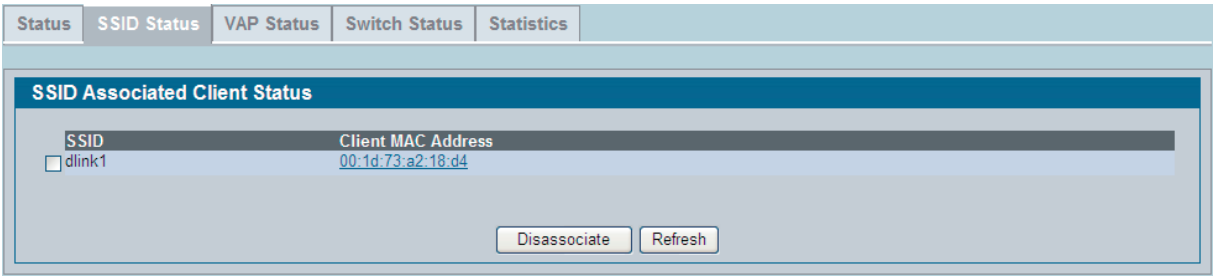


図 9-55　SSID Associated Client Status 画面 -「SSID Status」タブ

項目	説明
SSID	クライアントが接続しているネットワークを示します。
Client MAC Address	クライアントステーションの MAC アドレス。

VAP Status タブ（VAP の関連クライアント状態の参照）

各アクセスポイントは、各無線インタフェースに対して 16 個の仮想アクセスポイント（VAP）を持ち、各 VAP は固有の MAC アドレス（BSSID）を持ちます。無線クライアントと接続している管理アクセスポイント上の VAP の情報を参照することができます。

WLAN タブ > Monitoring > Client > Associated Clients > VAP 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。アクセスポイントからクライアントの接続を終了するためには、BSSID の横のボックスを選択し、「Disassociate」ボタンをクリックします。

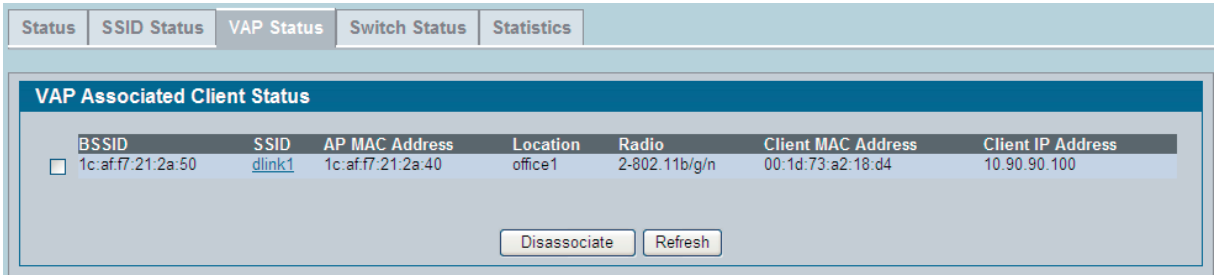


図 9-56　VAP Associated Client Status 画面 -「VAP Status」タブ

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しているアクセスポイントの VAP の MAC アドレス。
SSID	クライアントが接続しているアクセスポイントの VAP ポイントの SSID。
AP MAC Address	管理対象アクセスポイントの MAC アドレス。
Location	管理対象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。
Client MAC Address	クライアントステーションの MAC アドレス。
Client IP Address	クライアントステーションの IP アドレス。

Switch Status タブ（スイッチに関連するクライアントの状態の参照）

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に関する情報を参照します。

WLAN タブ > Monitoring > Client > Associated Clients > 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。

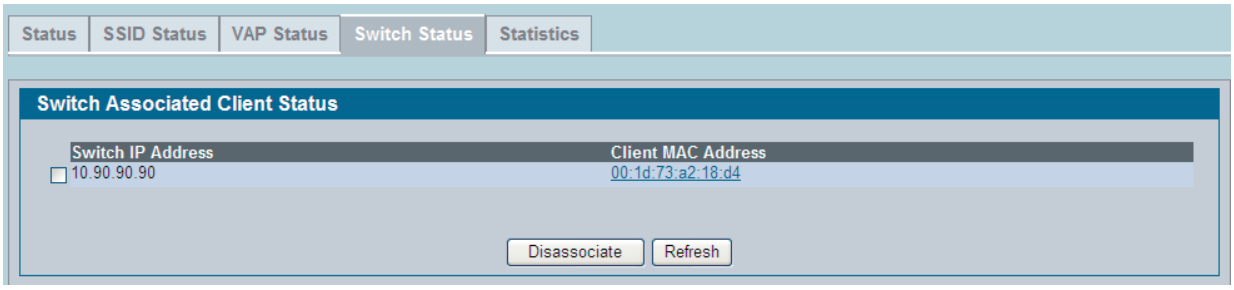


図 9-57　Switch Associated Client Status 画面 -「Switch Status」タブ

アクセスポイントからクライアントの接続を終了するためには、スイッチの IP アドレスの横のボックスを選択し、「Disassociate」ボタンをクリックします。

以下の項目が表示されます。

項目	説明
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。
Client MAC Address	接続するクライアントの MAC アドレスを表示します。

Statistics タブ（統計情報）

Association Summary タブ（接続中のクライアントの統計情報の参照）

無線クライアントは、WLAN サービスを中断せずに、アクセスポイント間をローミングすることができます。統合スイッチは、スイッチが管理するアクセスポイントの間をクライアントがローミングをする間のすべての無線セッション中に送受信されるトラフィックをトレースしています。スイッチはクライアントが 1 台のアクセスポイントと接続中も、また複数台のアクセスポイント間をローミング中でも、統計情報を記録しています。

1 台のアクセスポイントと通信中のクライアントが送受信したトラフィックの情報を示しています。
WLAN タブ > Monitoring > Client > Associated Clients > Statistics タブ > Association 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。

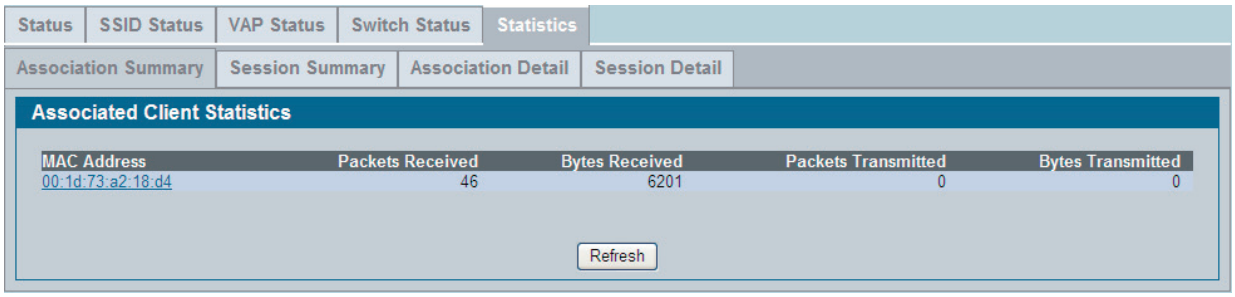


図 9-58　Associated Client Statistics - Association Summary 画面

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。単位はバイトです。
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。単位はバイトです。

Session Summary Summary タブ（接続中のクライアントの統計情報の参照）

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ついての情報を確認することができます。

WLAN タブ > Monitoring > Client > Associated Clients > Statistics タブ > Session 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。

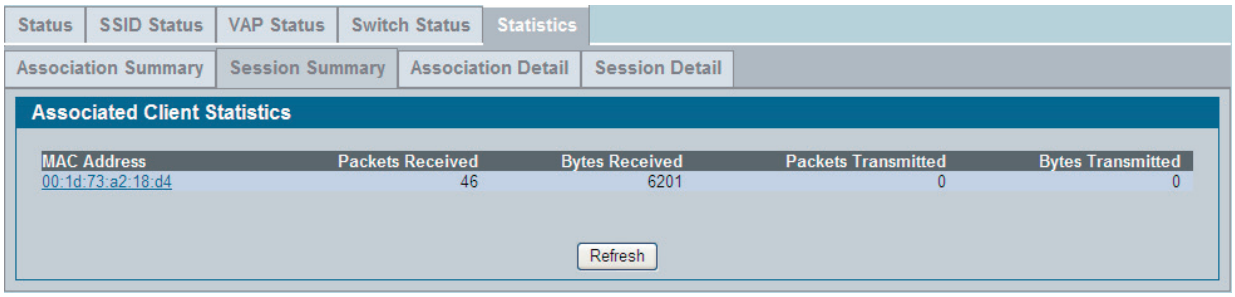


図 9-59　Associated Client Statistics - Session Summary 画面

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、セッション統計は累積されます。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。

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総データ量。単位はバイトです。
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。単位はバイトです。

Association Detail タブ（接続中のクライアントに関係する詳細な統計情報の参照）

1 台のアクセスポイントと通信中のクライアントが送受信したトラフィックの情報を示しています。テーブルの上にあるメニューを使用して、接続するクライアントに関する詳細情報を表示します。各クライアントは MAC アドレスで識別されます。

WLAN タブ > Monitoring > Client > Associated Clients > Statistics タブ > Association 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。

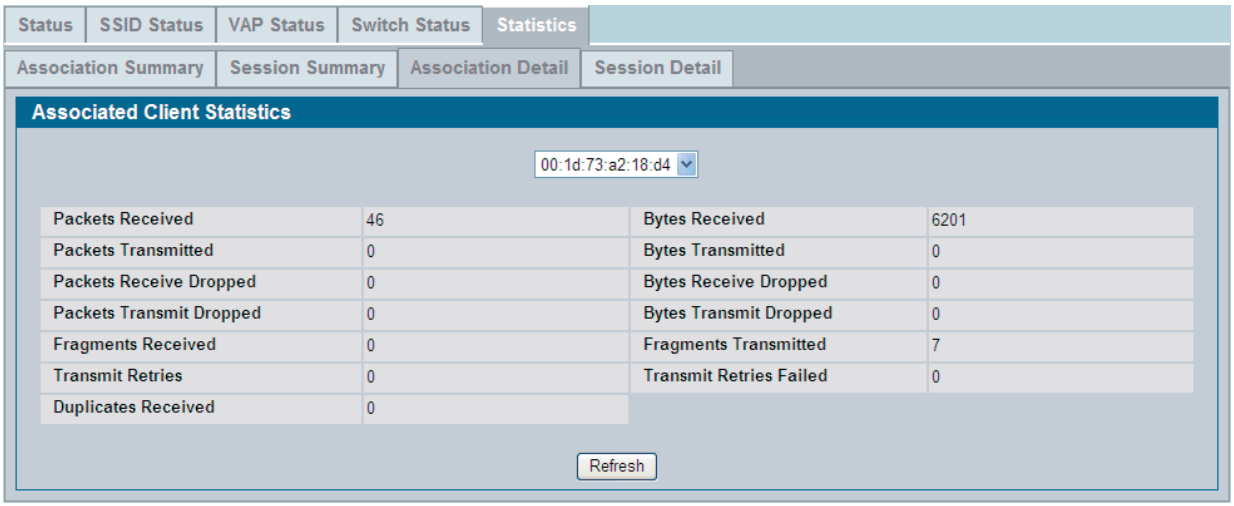


図 9-60　Associated Client Statistics - Association Detail 画面

以下の項目が表示されます。

項目	説明
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 Receive Dropped	クライアントから受信し、破棄されたパケット数。
Bytes Receive 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	クライアントに送信し、破棄されたパケット数。
Bytes Transmit Dropped	クライアントに送信し、破棄されたデータ量（バイト）。
Bytes Transmit Dropped	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 タブ（接続中のクライアントの詳細情報の参照）

「Session Detail」の統計情報では、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の情報を参照することができます。テーブルの上にあるメニューを使用して、接続するクライアントに関する詳細情報を表示します。各クライアントは MAC アドレスで識別されます。

WLAN タブ > Monitoring > Client > Associated Clients > Statistics タブ > Session 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。

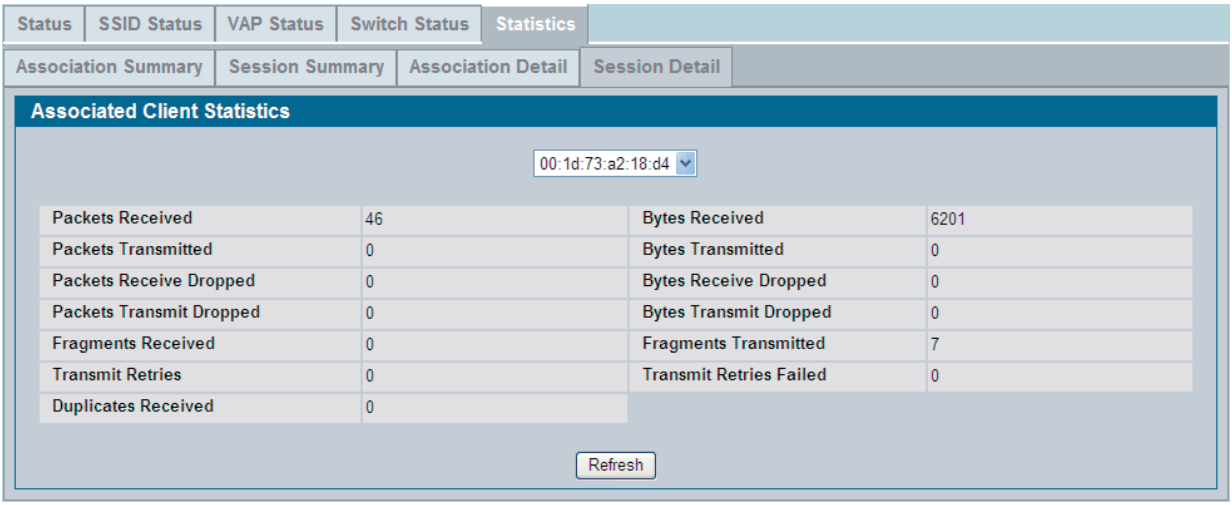


図 9-61　Associated Client Statistics - Session Detail 画面

項目	説明
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 Receive Dropped	クライアントから受信し、破棄されたパケット数。
Bytes Receive 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。

Peer Switch（ピアスイッチの状態）

ネットワーク上の他の統合スイッチの情報を提供します。

同一クラスタ内の、ピア無線スイッチ同士は、スイッチ、スイッチの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。スイッチとピアとの接続が切れると、すべてのピアスイッチの情報は削除されます。

1 つのスイッチがクラスタコントローラとして選出されます。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、ピ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 タブ（状態表示）

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

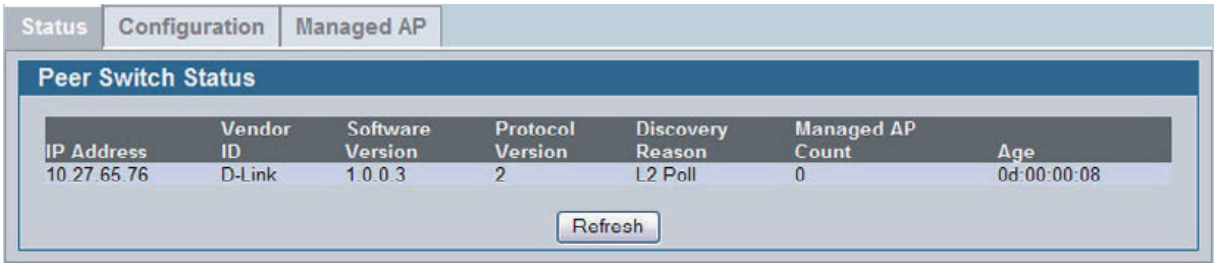


図 9-62　Peer Switch Status 画面 -「Status」タブ

以下の項目が表示されます。

項目	説明
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 タブ（ピアスイッチ設定状態の参照）

クラスタ内の 1 つのスイッチから別のスイッチまでのスイッチ設定を表示します。クラスタ内のピアスイッチが送信した設定に関する情報を表します。設定情報を受信した各ピアス一致の IP アドレスを表示します。

ローカルスイッチが受信した設定に関する情報を参照します。

WLAN タブ > 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 9-63　Peer Switch Configuration Status 画面 -「Configuration」タブ

画面内の各項目の情報を示します。

項目	説明
Peer IP Address	設定情報を受信したクラスタ内の各ピアスイッチの IP アドレスを表示します。
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 アドレスを表示します。
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 • Discovery • Channel/Power • AP Database • Channel/Power • AP Profiles • Known Client • Captive Portal • RADIUS Client • QoS ACL • QoS DiffServ 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 タブ（ピアスイッチが管理するアクセスポイントの状態の参照）

クラスタ内の各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。上記テーブルのメニューを使用して、表示するアクセスポイント情報を持つピアスイッチを選択します。各ピアスイッチは IP アドレスによって識別されます。

WLAN タブ > 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。

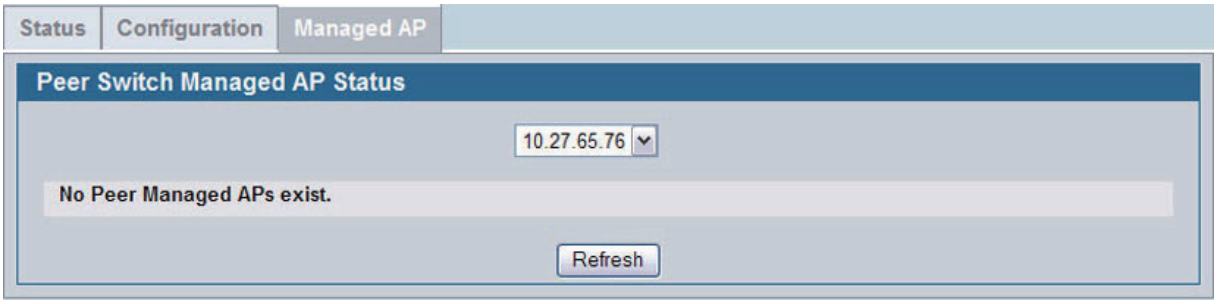


図 9-64　Peer Switch Managed AP Status 画面 -「Managed AP」タブ

以下の表は「Peer Switch Managed AP Status」画面内で使用可能なフィールドの情報を示します。

項目	説明
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	管理対象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。

侵入検知に関するモニタリングと管理

本セクションには D-Link 統合スイッチネットワーク内のアクセスポイントと無線クライアントの管理、監視を補助し、不正なデバイスから防御する以下の機能があります。

- AP RF Scan Status
- Detected Client Status
- Ad Hoc Client Status
- AP Authentication Failure Status
- AP De-Authentication Attack Status

「Intrusion Detection」画面のステータスエントリは、時間内のある時点で収集され、最後に削除されます。リスト中の「Age」には、リストに追加されてからの経過時間が表示されます。**Administration > Advanced Configuration > Global** ページを開いて、ステータスエントリを削除するタイミング（Age out）を指定することができます。また、手動でエントリを削除することも可能です。

AP RF Scan Status（AP RF スキャン状態）

定期的に無線通信範囲内をスキャンすることにより、他のアクセスポイントや無線クライアントの情報を収集しています。
アクセスポイントの通常の動作モードでは常に使用可能なチャンネルのスキャンをしています。

D-Link アクセスポイントでは、通常の動作モードの他に、以下の 2 種類のスキャンモードを用意しています。

- Scan Other Channels - アクセスポイントに定期的に使用可能なチャンネルを離れて、無線帯域内の他のチャンネルのスキャンを行うように設定します。
- Scan Sentry - 通常の無線動作を無効にし、無線スキャンを継続的に行います。本モードのアクセスポイントではビーコン送信は無効になり、クライアントからの接続も拒否します。

「Scan Other Channels」または「Scan Sentry」モードでは、アクセスポイントは無線インタフェースのすべてのチャンネルについてスキャンします。スキャンが完了すると、アクセスポイントは収集した情報を、自分を管理しているスイッチに送信します。スキャンモードの設定方法については「周波数帯域（Radio タブ）」（279 ページ）を参照してください。

統合スイッチは、アクセスポイントが RF スキャンプロセス中に検出され、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ると、これを不正なアクセスポイントであると見なします。システムで有効な脅威検出アルゴリズムを参照するためには、**WLAN タブ > Administration > Advanced Configuration > WIDS Security** の順にメニューをクリックし、「WIDS Security」画面を表示します。

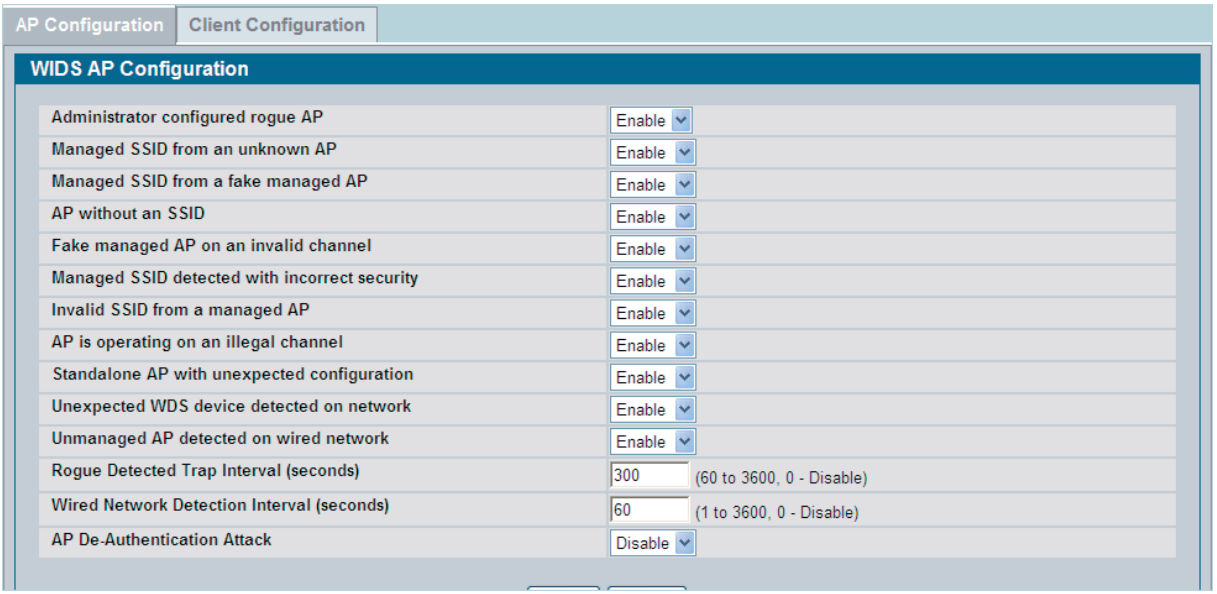


図 9-65　WIDS AP Configuration 画面 -「AP Configuration」タブ

WLAN タブ > Monitoring > Access Point > AP RF Scan Status の順にメニューをクリックし、RF スキャンによって検出されたすべてのアクセスポイント（不正と報告されたものも含む）の情報を確認することができます。

リスト中のエントリの順番を、欄の項目ごとに並び替えることができます。例えば、不正と報告されたアクセスポイントのグループを集めたい場合は「Status」をクリックします。

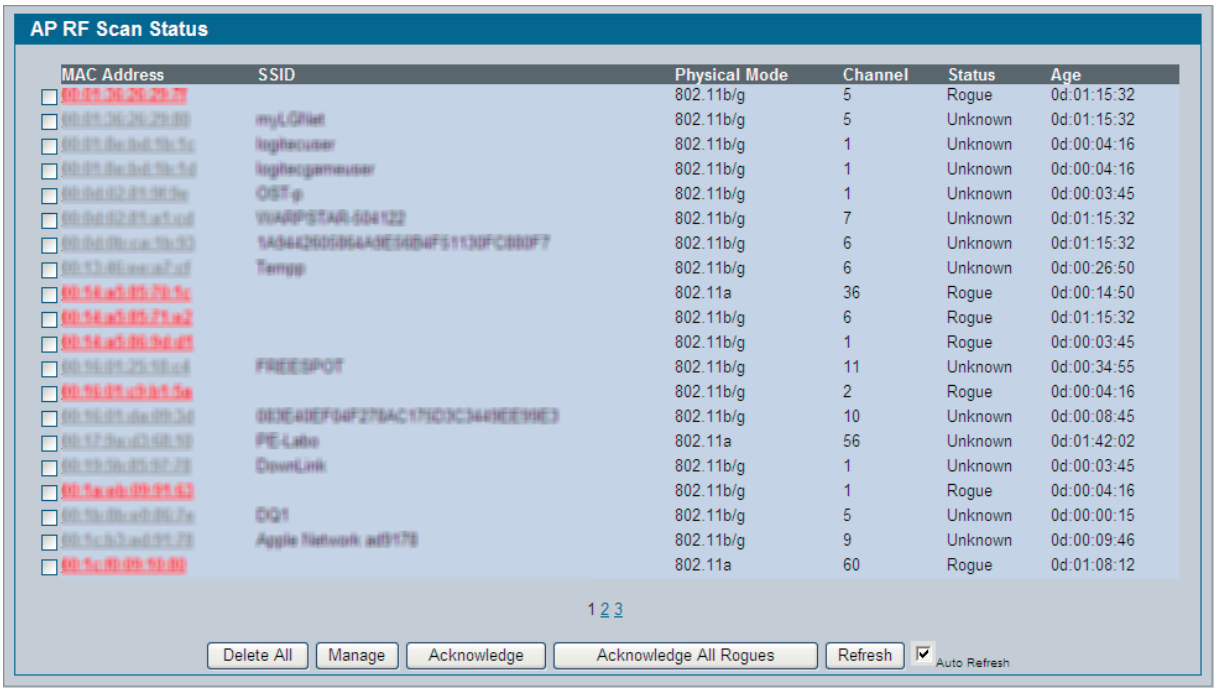


図 9-66　AP RF Scan Status 画面

出されたアクセスポイントについての詳細情報を確認するためには、そのアクセスポイントの MAC アドレスをクリックしてください。

以下の表はでは「Rogue/RF Scan」画面の項目について説明します。

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 アドレスです。
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。以下の一つが表示されます。 • 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。
Transmit Rate	アクセスポイントの現在の送信速度。
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の経過時間。

画面下部のボタンを使用して、以下のテーブルで記述したアクションを実行します。

項目	説明
Delete All	RF スキャンリストからすべてのアクセスポイントを削除します。本リストは、新規に検出されたアクセスポイントを書きます。
Manage	不正アクセスポイントの次回検出時に、スイッチにより管理されるためには、MAC アドレスの左のチェックボックスを選択し、「Manage」ボタンをクリックします。スイッチはそのアクセスポイントを Valid AP データベースに追加し、デフォルト AP プロファイルに割り当てます。その後スイッチからアクセスポイントを設定することができます。アクセスポイントの認知に RADIUS サーバを使用している場合は、アクセスポイントの MAC アドレスを RADIUS サーバの AP データベースに登録する必要があります。
Acknowledge	RF スキャンデータベース内のアクセスポイントの不正ステータスをクリアするためには、アクセスポイントの MAC アドレス隣のチェックボックスを選択し、「Acknowledge」ボタンをクリックします。

項目	説明
Acknowledge All Rogues	不正なステータスを持つすべてのアクセスポイントを承認するためには、「Acknowledge All Rogues」ボタンをクリックします。承認された不正なアクセスポイントのステータスは、それが最初に検出された時に持っていたステータスに戻ります。検出されたアクセスポイントが、脅威として分類するいずれかのテストでエラーになると、再び「Rogue」としてリストに表示されます。
Refresh	現在のデータを読よして画面を更新します。

詳細を参照するアクセスポイントのMACアドレスをクリックすると、そのアクセスポイントに関する詳細な「AP RF Scan Status」画面が表示されます。

RF スキャン中に検出したアクセスポイントの詳細ステータスは、RF スキャンを通じて検出した個別のアクセスポイントに関する情報を表示します。RF スキャンを通じて検出した別のアクセスポイントに関する情報を表示するためには、メインの「AP RF Scan Status」画面に戻り、参照する情報を持つアクセスポイントの MAC アドレスをクリックします。

AP RF Scan Status タブ

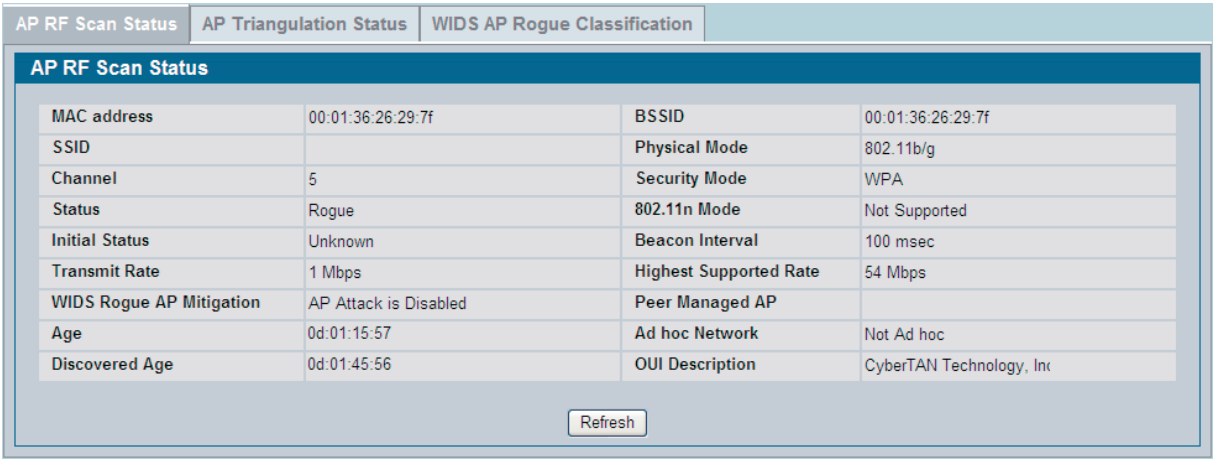


図 9-67　AP RF Scan Status 画面 -「AP RF Scan Status」タブ

以下の表では、個別のアクセスポイントを示す「AP RF Scan Status」におけるアクセスポイントの詳細画面の情報を示します。

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 アドレスです。
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。以下の一つが表示されます。 • 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、初期のステータスは「Managed」、「Standalone」、または「Unknown」と等しくなります。不正なアクセスポイントには、初期のステータスはこのアクセスポイントが不正になる前の「classification」です。
Transmit Rate	アクセスポイントの現在の送信速度。
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します。移行が進んでいない場合、以下の原因から一つが表示されます。 • Not Required (AP s not rogue) - 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、非常に多くのアクセスポイントを移行しています。 • 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アドホックモードです。
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の経過時間。
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の経過時間。
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。

項目	説明
Physical Mode	アクセスポイントで使用している 802.11 のモードを示します。
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が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	アドホック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のアダプタのメーカを表示します。

AP Triangulation Status タブ（アクセスポイントトライアングレーション状況の参照）

トライアングレーション情報は、どの管理アクセスポイントが RF スキャンを通じて各デバイスを検出したかを参照することで不正なクライアントの位置の確認を補助します。最大 6 個のトライアングレーションエントリが、RF スキャンを通じて検出した各アクセスポイントに報告されます。

3 個のエントリは non-sentry AP で、別の 3 個が sentry AP です。アクセスポイントは sentry モードで設定された 1 つの無線インタフェースと non-sentry モードで設定された別の無線モードを持つため、同じアクセスポイントがリストに表示されます。アクセスポイントが 3 つのアクセスポイントに検出されなければ、リストには 0、1 または 2 つのエントリが含まれます。

RF スキャンを通じて検出した別のアクセスポイントに関する情報を表示するためには、メインの「AP RF Scan Status」画面に戻り、参照する情報を持つアクセスポイントの MAC アドレスをクリックしします。

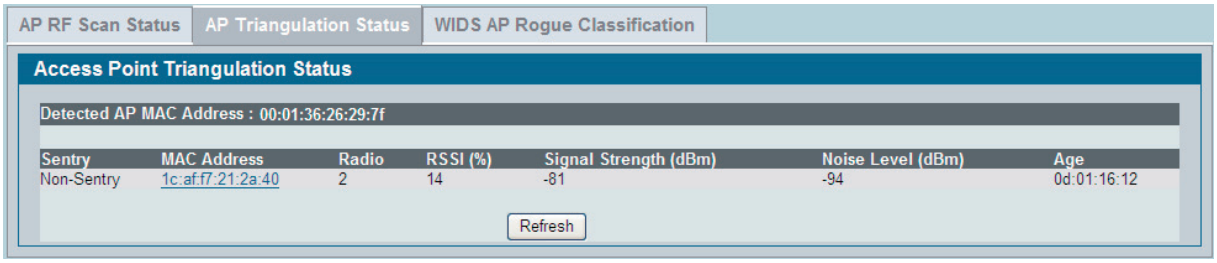


図 9-68　AP RF Scan Status - AP Triangulation Status 画面

以下の表に「 Access Point Triangulation Status」ページから情報を表示します。

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モードを表示します。
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、アクセスポイント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の経過時間。

WIDS AP Rogue Classification タブ（WIDS AP 不正な分類情報の参照）

Wireless Intrusion Detection システム（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。統合スイッチにより、様々な脅威検出テストを有効または無効にし、脅威検出に使用するしきい値を設定することができます。「WIDS AP Rogue Classification」画面では、これらのテストの結果に関する情報を提供します。アクセスポイントが不正であるとして分類されると、本画面では、アクセスポイントが分類を始動するのに失敗したテストに関する情報を提供します。

アクセスポイントが不正であると分類されると、システムは、スイッチが不正であるとしてアクセスポイントを分類することになった脅威のタイプを特定する追加情報を提供します。

WIDS RF セキュリティには 3 つの機能があります。

- 制御フレームとデータフレームをリッスンすることで、無線デバイスを検出します。
- 無線ネットワークにトレースフレームを送信または無線ネットワーク上のトレースフレームをリッスンするなど受信データを様々なデータベースと比較することで、無線デバイスが脅威であるかどうかを分類します。
- 脅威からネットワークを保護するためにアクションを行います。

これらの変更は、ネットワークの接続性を混乱させずに行うことができます。アクセスポイントがいくつかの作業を行うので、スイッチは、WIDS の操作プロパティを変更するためにアクセスポイントにメッセージを送信する必要があります。

RF スキャンを通じて検出した別のアクセスポイントに関する情報を表示するためには、メインの「AP RF Scan Status」画面に戻り、参照する情報を持つアクセスポイントの MAC アドレスをクリックします。

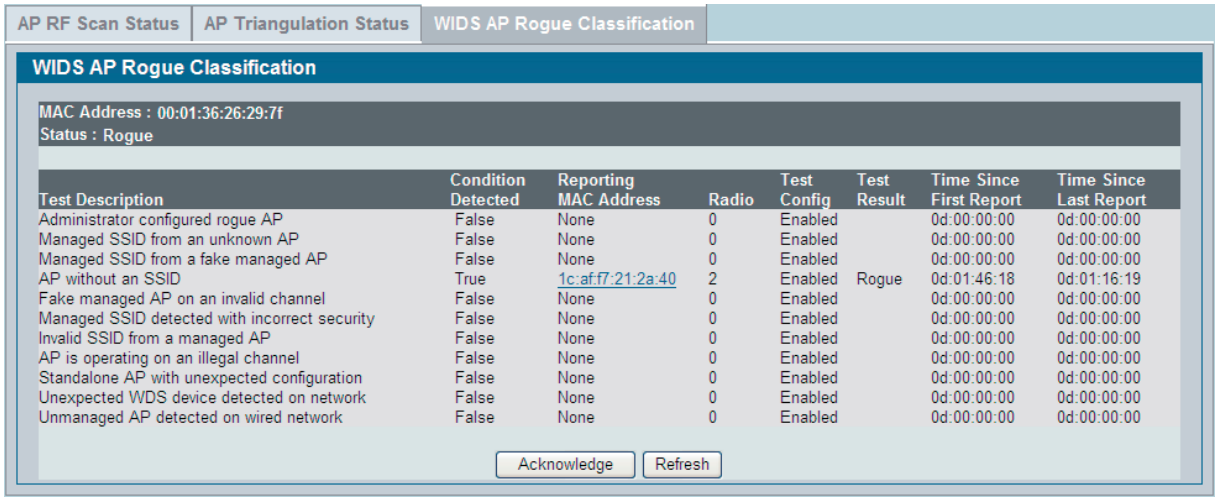


図 9-69　AP RF Scan Status - WIDS AP Rogue Classification 画面

以下の表に「WIDS AP Rogue Classification」ページから確認できる個別のアクセスポイントの情報を示します。

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 アドレスです。
Test Description	実行されたテストを表示します。 • 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 received from an AP without SSID - SSID を持たないアクセスポイントから受信した管理 SSID • Beacon Received from a fake managed AP on a invalid channel - 不正なチャンネルにある偽の管理アクセスポイントから受信したビーコン • 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です。 • Standalone AP is operating with unexpected configuration. - スタンドアロン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です。 • Unexpected WDS device is detected on the network. - 予期しない WDS デバイスがネットワークで検出されました。 • Unmanaged AP detected on wired network. - 管理されていないアクセスポイントが無線ネットワークで検出されました。

項目	説明
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インタフェース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有効または無効にします。
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、テストは肯定的な結果を報告し、有効であるため、不正なものとしてレポートしない場合もあります。
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。

Detected Clients（検出されたクライアントのステータス）

クライアントが、システムとの通信を試みる場合、または、システムがクライアントからのトラフィックを検出する場合、無線クライアントは無線システムによって検出されます。

離脱して、もうシステムに接続され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があります。

Detected Client Summary タブ

WLAN タブ > 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。

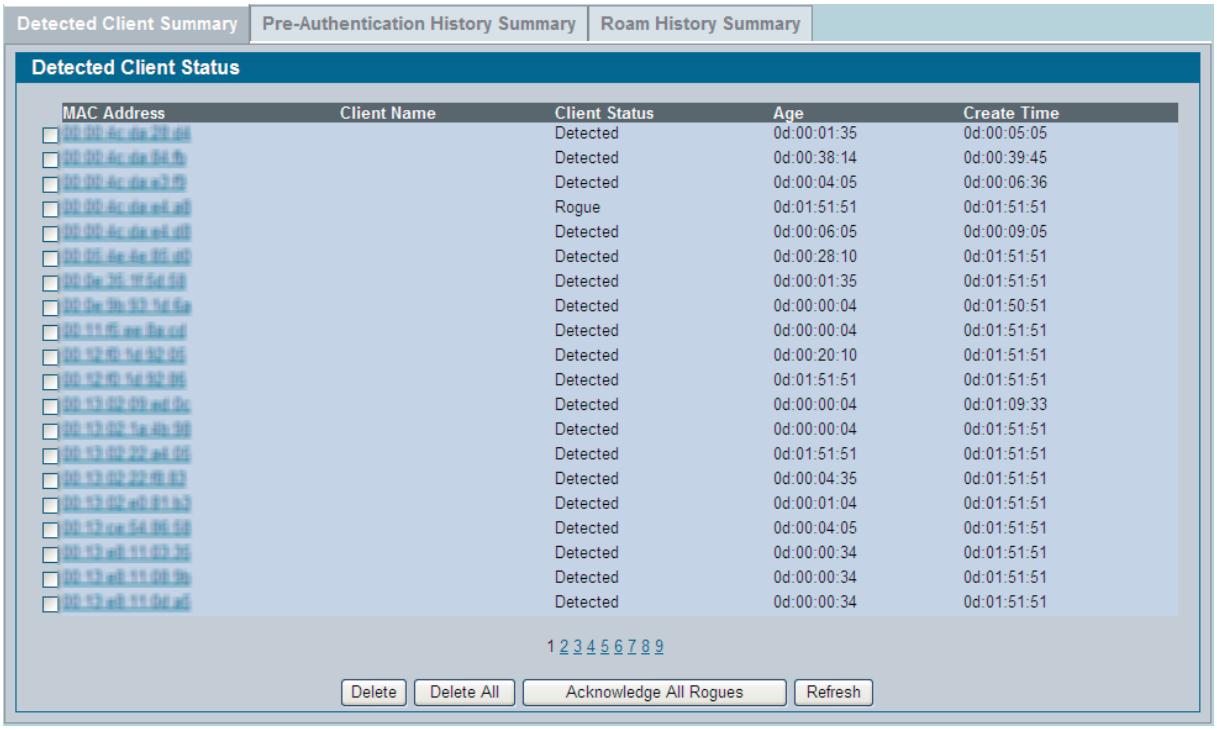


図 9-70　Detected Client Status 画面

クラスタコントローラは、クラスタ内のすべてのスイッチから接続するクライアントに関する情報を受信します。そして、クラスタコントローラからクライアントをクラスタ内のいかなるアクセスポイントに接続するクライアントの接続も解除することができます。

「Detected Client」データベースに不正なものとして示されたすべてのクライアントを不正なステータスから取り除くためには、「Acknowledge All Rogues」ボタンをクリックします。承認されたクライアントのステータスは、それが最初に検出された時に持っていたステータスに戻ります。検出されたクライアントが、脅威として分類するいずれかのテストでエラーになると、再び「Rogue」としてリストに表示されます。

「Detected Client」データベースから、個別のクライアントを削除するためには、各クライアントの MAC アドレス横の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。すべての検出クライアントを削除するためには、「Detected Client」データベースで「Delete All」ボタンをクリックします。

「Detected Client Summary」タブの項目は以下の通りです。

項目	説明
MAC Address	クライアントの MAC アドレス。
Client Name	必要に応じ、「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されます。 • Detected - 無線クライアントは無線システムで検出されますが、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 - クライアントは、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。 • Know Client - クライアントは、Know Client データベースで検出されますが、認証されません。
Age	検出されたクライアントのデータベースエントリを更新したこのクライアントに何らかのイベントが受信されてから経過した時間。
Create Time	このエントリが検出された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。

画面に表示されたクライアントに関して詳しく学習するためには、クライアントの MAC アドレスをクリックします。

Detected Clients Status タブ（検出されたクライアントの詳細ステータスの参照）

無線ネットワークで検出された指定クライアントに関する情報を表示します。ネットワークに検出された他のクライアントに関する情報を参照するためには、「Detected Clients Status」画面に戻り、異なるクライアントの MAC アドレスをクリックします。

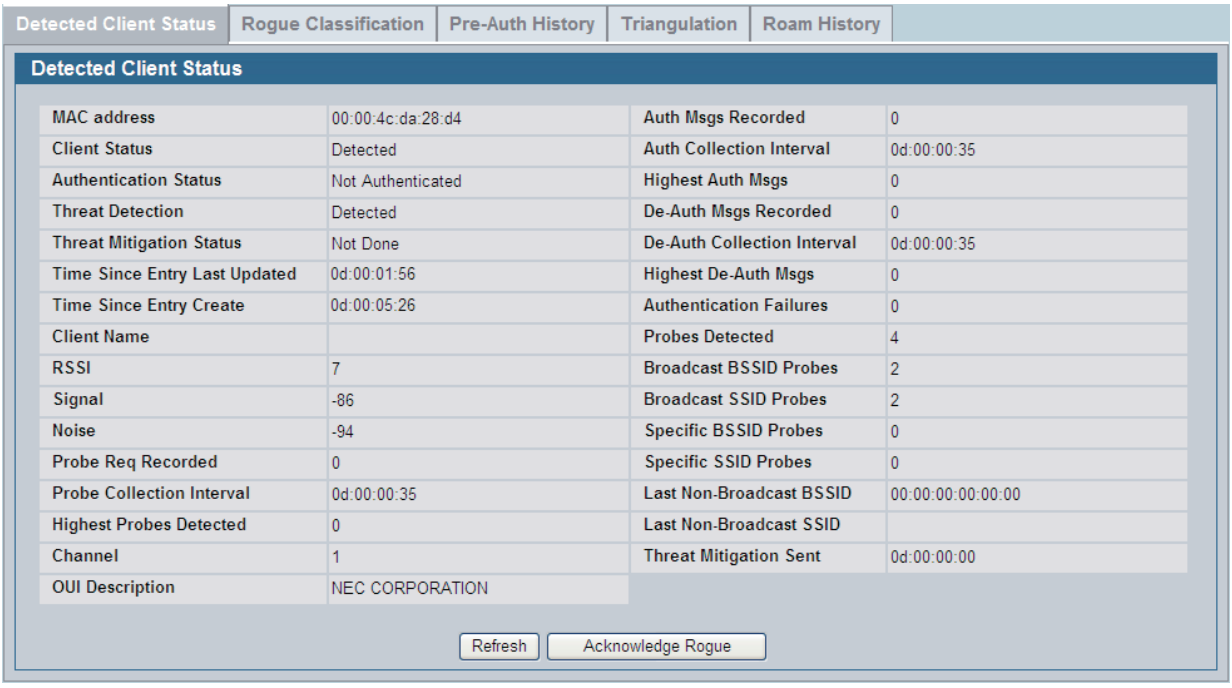


図 9-71　Detected Client Status 画面 - Detected Client Status タブ

「Detected Client Status」データベース内のクライアントの不正なステータスを削除するためには、「Acknowledge Rogues」ボタンをクリックします。承認されたクライアントのステータスは、それが最初に検出された時に持っていたステータスに戻ります。検出されたクライアントが、脅威として分類するいずれかのテストでエラーになると、再び「Rogue」としてリストに表示されます。

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されますが、Rogue ではありません。 • Detected - クライアントは検出されますが、認証されず、Rogue ではなく、Known Clients データベースでは見つけられません。 • Known Clients - クライアントは、Known Clients データベースで検出されますが、認証されません。 • 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	このクライアントが認証されるかどうかを表示します。 **注意** クライアントステータスが Rogue であっても、認証ステータスはまだ 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	検出されたクライアントのデータベースエントリを更新したこのクライアントに何らかのイベントが受信されてから経過した時間を表示します。
Time Since Entry Create	このエントリが検出された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を表示します。
Client Name	必要に応じ、「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対象のアクセスポイントに認証されると、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アクセスポイントが報告した最後の信号強度を表示します。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	各プローブ収集に消費された時間。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。
Auth Msgs Recorded	「Auth Collection Interval」（認証収集間隔）に記録した IEEE 802.11 の Authentication メッセージ数を表示します。
Auth Collection Interval	各認証収集に消費した時間を参照します。認証の収集は、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 Auth Msgs	スイッチが認証収集期間に検出した認証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 の認証解除メッセージ数を表示します。
De-Auth Collection Interval	各時間が認証解除の収集期間に消費した時間を参照します。認証解除の収集は、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のに役に立ちます。
Highest De-Auth Msgs	スイッチが認証解除の収集期間に検出した認証解除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の数を表示します。
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。

Rogue Classification タブ（WIDS クライアントの不正な分類の参照）

Wireless Intrusion Detection システム（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。統合スイッチにより、様々な脅威検出テストを有効または無効にし、脅威検出に使用するしきい値を設定することができます。「WIDS Client Rogue Classification」画面では、これらのテスト結果に関する情報を提供します。クライアントが不正であるとして分類されると、本画面では、クライアントが分類を始動するのに失敗したテストに関する情報を提供します。

RF スキャンを通じて検出した別のクライアントに関する情報を表示するためには、メインの「Detected Clients Status」画面に戻り、参照する情報を持つクライアントの MAC アドレスをクリックします。

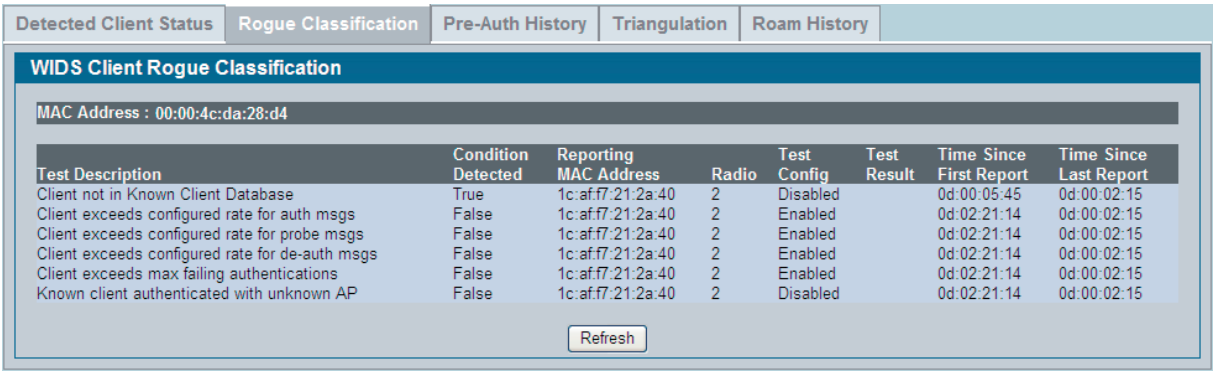


図 9-72　WIDS Client Rogue Classification 画面

以下の表は、検出したクライアントに実行されるセキュリティテストに関する情報を表示します。

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。 • クライアントは、Known Clients データベースに表示されません。 • クライアントは 802.11 の認証要求の送信のために設定レートを超えます。 • クライアントはプローブ要求の送信のために設定レートを超えます。 • クライアントは認証解除要求の送信のために設定レートを超えます。 • クライアントはプローブ要求の送信のために設定レートを超えます。 • Known（既知）クライアントは、Unknown（未知）のアクセスポイントで認証されます。
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インタフェース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有効または無効にします。
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。

Pre-Auth History タブ（検出されたクライアントの事前認証に関するヒストリを参照する）

セッションの損失および事前認証を行わないで、認証クライアントのローミングを補助するために、無線クライアントは、クライアントが接続することのできる範囲内の他のアクセスポイントに対して認証を試みることができます。事前の認証に成功するためには、ターゲットアクセスポイントの SSID と MAC 認証、暗号化方式、事前共有鍵または RADIUS パラメータを含むセキュリティ設定がクライアントの設定に一致する VAP が必要です。クライアントが接続するアクセスポイントは、すべての事前認証要求を取得してスイッチに送信します。

検出されたクライアントが行った事前認証要求に関する情報を表示します。

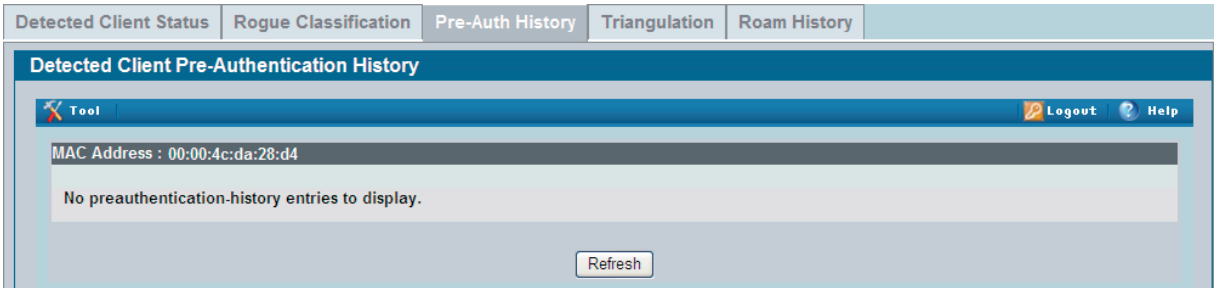


図 9-73　Detected Client Pre-Authentication History 画面

以下の表に「Detected Client Pre-Authentication History」画面の各フィールドについてを示します。

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（1 または 2）。
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の経過時間。
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。
Pre-Authentication Status	クライアントが認証に成功したかどうかを「Success」（成功）または「Failure」（失敗）のステータスで表示します。

Triangulation タブ（検出されたクライアントのトライアングレーションの参照）

クライアントを検出した 3 個までの non-sentry および同じく 3 個までの管理アクセスポイントを示します。アクセスポイントが報告した最後の信号強度は、クライアントのロケーションを測定するために役立ちます。アクセスポイントは sentry モードで設定された 1 つの無線インタフェースと non-sentry モードで設定された別の無線モードを持つため、同じアクセスポイントが両方のリストに表示されます。アクセスポイントまたはクライアントが 3 つのアクセスポイントに検出されなければ、リストには 0、1 または 2 つのエントリが含まれます。

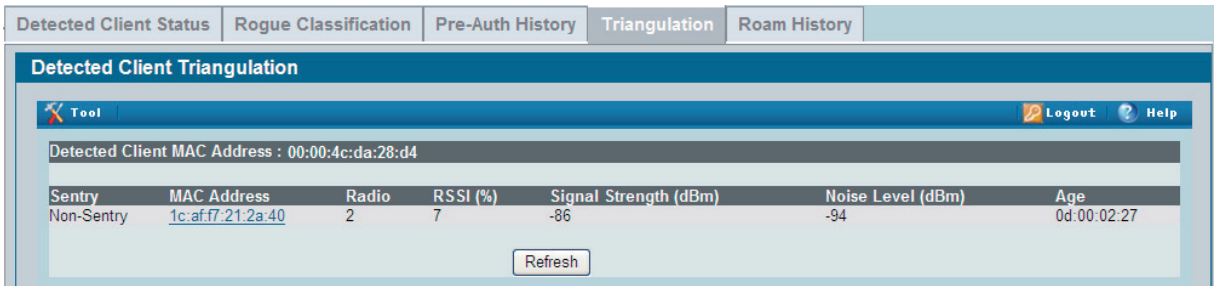


図 9-74　Detected Client Triangulation 画面

以下の表に「Detected Client Triangulation」画面の各項目についてを示します。

項目	説明
Detected Client MAC Address	クライアントの MAC アドレス。
Sentry	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インタフェースは、sentry モードでは設定されません。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インタフェースが 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。
MAC Address	クライアントを検出した管理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（1 または 2）。
RSSI (%)	non-sentry AP の受信信号強度（%）。範囲は 0-100 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 Strength (dBm)	受信信号強度（dBm）。有効な範囲は -127 ～ 127（dBm）です。現実的な範囲は -95 ～ -10 です。
Noise Level (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。

Roam History タブ（検出クライアントのローミングヒストリ）

1 つの管理アクセスポイントから別の管理アクセスポイントまでローミングする場合に、無線システムはクライアントに関する記録をつけます。最大 10 個のアクセスポイントのヒストリが各クライアントのために保持されます。

クライアントが接続する管理アクセスポイントを表示します。クライアントリストの最初にあるエントリが最も古いものです。リストがいっぱいなると、最も古いエントリが削除され、他のすべてのエントリが上に 1 つずつ移動します。

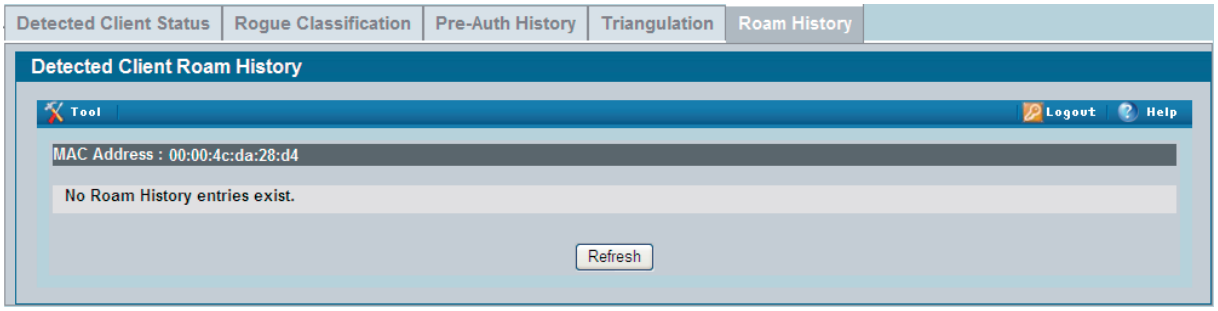


図 9-75　Detected Client Roam History 画面

以下の表に「Detected Client Roam History」画面の各項目についてを示します。

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	ヒストリの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の経過時間。

Pre-Authentication History Summary タブ（検出されたクライアントの事前認証のサマリ）

セッションの損失および事前認証を行わないで、認証クライアントのローミングを補助するために、無線クライアントは、クライアントが接続することのできる範囲内の他のアクセスポイントに対して認証を試みることができます。事前の認証に成功するためには、ターゲットアクセスポイントには、SSID と MAC 認証か、暗号化方式、事前共有鍵または RADIUS パラメータを含むセキュリティ設定がクライアントのものに一致する VAP が必要です。クライアントが接続するアクセスポイントは、すべての事前認証要求を取得してスイッチに送信します。

事前認証要求を行った検出クライアントと要求を受信したアクセスポイントを表示します。

WLAN タブ > Monitoring > Client > Detected Clients > Pre-Authentication History 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。

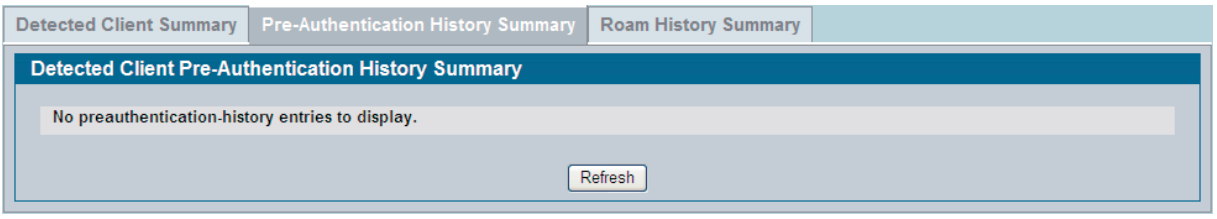


図 9-76　Detected Client Pre-Authentication History Summary 画面

以下の表は「Detected Client Pre-Authentication History Summary」画面の各項目を説明します。

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（検出クライアントのローミングヒストリのサマリ）

1 つの管理アクセスポイントから別の管理アクセスポイントまでローミングする場合に、無線システムはクライアントに関する記録をつけます。最大 10 個のアクセスポイントのヒストリが各クライアントのために保持されます。

少なくとも 1 つのアクセスポイントからローミングした各クライアントを表示し、そのローミングヒストリに関する情報を提供します。

WLAN タブ > Monitoring > Client > Detected Clients > Roam History 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。

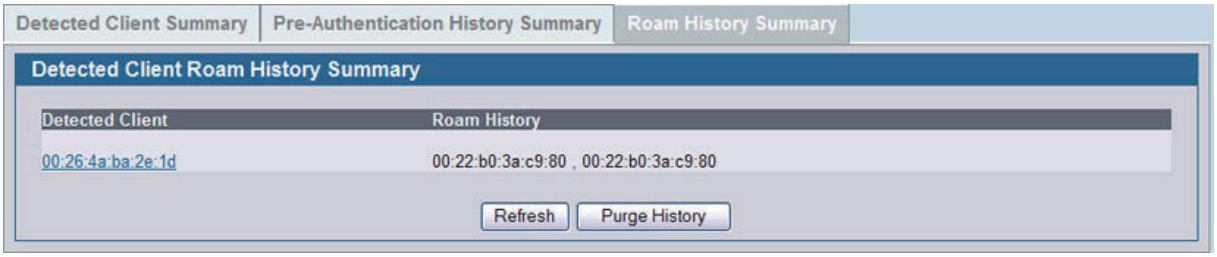


図 9-77　Detected Client Roam History Summary 画面

以下の表は「Detected Client Roam History Summary」画面の各項目を説明します。

項目	説明
Detected Client	検出されたクライアントの MAC アドレス。
Roam History	クライアントを認証した管理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（Ad Hoc クライアントステータス）

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。

アドホックネットワークを通じて WLAN に接続する無線クライアントを参照または管理します。

WLAN タブ > 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。

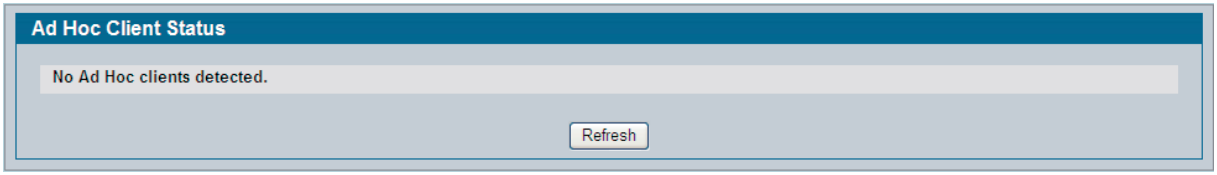


図 9-78　Ad Hoc Clients 画面

リストからすべてのアドホッククライアントを削除するためには、「Delete All」ボタンをクリックします。本リストはクリアされます。

注意　リストをクリアしても、アドホッククライアントは切断されません。また、クライアントはアドホックネットワークに残っている場合があります。

アドホッククライアントを WLAN アクセスからブロックするためには、目的のクライアントの MAC アドレスの横にあるチェックボックスを選択して「Deny」ボタンをクリックします。
するとその MAC アドレスは、デフォルトアクションが "Deny（拒否）" である「Known Client」データベースに追加されます。
「Known Client」データベースにクライアントを追加し、WLAN へのアクセスするためには、クライアントを選択して「Allow」ボタンをクリックします。

注意　「Deny MAC」ボタンが使用できない場合は、すべてのプロファイルが MAC 認証動作の初期値として "Allow（許可）" を使用することを意味します。同様に「Allow」ボタンが使用できない場合は、"Allow（許可）" を初期値とするアクション持つプロファイルはありません。

注意　AP プロファイルにおいて、MAC 認証に RADIUS サーバを使用しているものがある場合は、クライアントの MAC アドレスを RADIUS サーバのデータベースに追加する必要があります。

無線クライアントに指定されたアクションの初期値（Allow、Deny、または Global）を参照または編集するためには、**WLAN タブ > Administration > Advanced Configuration > Clients > Known Client** 画面を表示し、参照または設定するクライアントの MAC アドレスをクリックします。

クライアントがアクセスポイントによる認証に成功した場合でも、スイッチは本リストから MAC エントリを削除することはありません。
アドホックデータヒストリに記録が残るので、WLAN 上でアドホックネットワークを構成するクライアントを慎重に扱うことができます。

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。検出モードがビーコンフレームの場合、RF スキャンデータベースや隣接 AP リストには、クライアントはアクセスポイントとして表示されます。検出モードがデータフレームの場合、クライアント情報は隣接クライアントリストに表示されます。
AP MAC Address	クライアントを検出したアクセスポイントの MAC アドレス。
Location	アクセスポイントの場所。
Radio	アドホッククライアントが検出された無線インタフェースと無線モード。
Detection Mode	アドホッククライアントの検出方式。Beacon Frame または "Data Frame" が表示されます。
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。

AP Authentication Failure Status（AP 認証失敗ステータス）

アクセスポイントからスイッチへの接続は、不正なパケットフォーマットやベンダ ID などによるエラーのため、またはローカル /RADIUS データベースに Valid AP としての正しい認証情報が設定されていないなどの原因で失敗することがあります。

統合スイッチとの接続に失敗したアクセスポイントのリストを表示します。

WLAN タブ > 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。

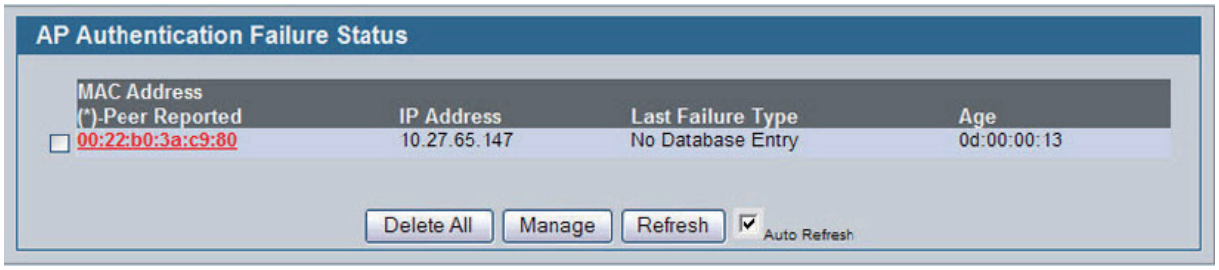


図 9-79　AP Authentication Failure Status 画面

「AP authentication failure」画面には、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の情報が表示されます。アクセスポイントは以下のいずれかの原因により通信に失敗します。

項目	説明
No Database Entry	アクセスポイントの MAC アドレスがローカル Valid AP データベースまたは外部 RADIUS サーバデータベース中に登録されていないため、アクセスポイントの認可ができません。
Local Authentication	アクセスポイントに設定されている認証用パスワードがローカルデータベースに登録されているものと一致しません。
Not Managed	アクセスポイントは Valid AP データベースにありますが、ローカルのデータベースの AP モードは Managed に設定されません。
RADIUS Authentication	RADIUS サーバの RADIUS クライアントに設定されたパスワードは、サーバによって拒否されました。
RADIUS Challenged	RADIUS サーバは、Challenge-Response 認証モードを使用するために設定されます。これは、アクセスポイントとは互換性がありません。
RADIUS Unreachable	アクセスポイントが設定されている RADIUS サーバに未到達です。
Invalid RADIUS Response	アクセスポイントが未承認または不正な RADIUS サーバから応答パケットを受信しました。
Invalid Profile ID	RADIUS データベースに指定されているプロファイル ID はスイッチに存在しない可能性があります。ピアスイッチから設定を受信した場合、これはローカルのデータベースに起こります。
Profile Mismatch-Hardware Type	AP プロファイルに指定されたアクセスポイントのハードウェアタイプは、実際のアクセスポイントのハードウェアと互換性がありません。
AP Image Not Available	スイッチには、アクセスポイントを配置するために利用可能な適切なイメージがありません。スイッチが、Auto AP イメージ更新をサポートし、このモードが有効である場合にだけ、このエラーは有効です。

リストからすべてのアクセスポイント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。
「Access Point Failure」リストから、Valid AP データベースへエントリを登録するためには、MAC アドレス横のチェックボックスを選択して、「Manage」ボタンをクリックしてください。

アクセスポイントの認可のためにローカルデータベースを使用する場合は、**WLAN タブ > Administration > Basic Setup** の順にメニューをクリックし、「Valid AP」タブで、アクセスポイントの設定を変更します。アクセスポイントの認可を RADIUS サーバデータベースを使用して行っている場合は、RADIUS サーバデータベースにアクセスポイントの MAC アドレスを登録する必要があります。

以下の項目があります。

項目	説明
MAC Address	アクセスポイントの MAC アドレス。 アクセスポイントの MAC アドレスのあとに（*）が続いている場合、それはピアスイッチによって報告されます。
IP Address	アクセスポイントの IP アドレス
Last Failure Type	発生した最後のエラーのタイプを表示します。 • Local Authentication - ローカル認証 • No Database Entry - データベースエントリがありません。 • Not Managed - 管理されていません。 • RADIUS Authentication - RADIUS 認証 • RADIUS Challenged - RADIUS チャレンジ • RADIUS Unreachable - RADIUS 未到達 • Invalid RADIUS Response - 不正な RADIUS 応答 • Invalid Profile ID - 不正なプロファイル ID • Profile Mismatch-Hardware Type - プロファイルが不一致のハードウェアタイプ
Age	失敗発生からの経過時間。

認証失敗リスト中のアクセスポイントについての追加情報（ビーコン情報）を参照するために、「Rogue/RF Scan」画面の failed AP の MAC アドレスで検索することができます。ただし、スイッチに有線ネットワークで接続を試みているアクセスポイントについては、RF スキャン中の検出ができない場合があります。

リスト中の「MAC Address」のリンクをクリックすることにより、以下のようにそのアクセスポイントの詳しい情報を参照できます。ただし、アクセスポイントが D-Link アクセスポイント以外の場合は、いくつか参照できない値があります。

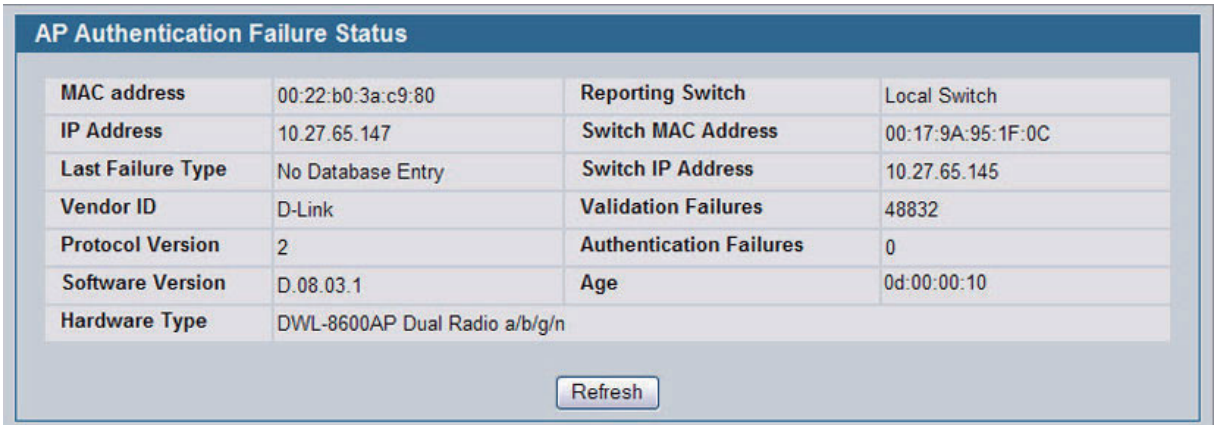


図 9-80　AP Authentication Failure Status - Details 画面

以下の表では「AP Authentication Failure Status - Details」画面内の各項目の情報を示します。

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	発生した最後のエラーのタイプを表示します。以下のいずれかが表示されます。 • Local Authentication（ローカル認証） • No Database Entry（データベースエントリがありません。） • Not Managed（管理されていません。） • RADIUS Authentication（RADIUS 認証） • RADIUS Challenged（RADIUS チャレンジ） • RADIUS Unreachable（RADIUS 未到達） • Invalid RADIUS Response（不正な RADIUS 応答） • Invalid Profile ID（不正なプロファイル ID） • Profile Mismatch-Hardware Type（プロファイルが不一致のハードウェアタイプ）
Vendor ID	アクセスポイントのソフトウェアベンダ。
Protocol Version	アクセスポイント上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。
Software Version	アクセスポイント上のソフトウェアのバージョン。
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。

項目	説明
Reporting Switch	アクセスポイント認証エラーを報告したスイッチの種類（ローカルスイッチまたはピアスイッチ）を表示します。
Switch MAC Address	アクセスポイントの認証エラーを報告したクラスタ内のスイッチの MAC アドレスを表示します。
Switch IP Address	アクセスポイントの認証エラーを報告したクラスタ内のスイッチの IP アドレスを表示します。
Validation Failures	本アクセスポイントが接続（認可）に失敗した回数。
Authentication Failures	本アクセスポイントが認証に失敗した回数。
Age	エラー発生からの経過時間。

AP De-Authentication Attack Status（AP 認証解除攻撃ステータス）

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な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が 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「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。認証解除攻撃は、すべての不正なタイプには有効というわけではないため、検出された不正なアクセスポイントのすべてに使用することはできません。以下の不正アクセスポイントには攻撃を行うことはできません。

- 検出された不正アクセスポイントが有効な管理アクセスポイントの BSSID を偽造している場合、その攻撃が正しいアクセスポイントへのサービスを拒否し、ハッカーがシステムを攻撃するように別の手段を提供する可能性があるため、無線システムは攻撃を行いません。
- Ad hoc ネットワークにおける認証解除攻撃は、これらが認証を使用しないため有効ではありません。
- カントリードメインが認可するチャンネル以外で動作するアクセスポイントは、不正チャンネルにおけるどんなトラフィックの送信も法律に反しているため、攻撃しません。

無線スイッチは、認証解除攻撃を行っている BSSID のリストを保持します。スイッチは、あらゆる管理アクセスポイントに対して、不正なアクセスポイントが動作している BSSID とチャンネルのリストを送信します。

WLAN タブ > 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。

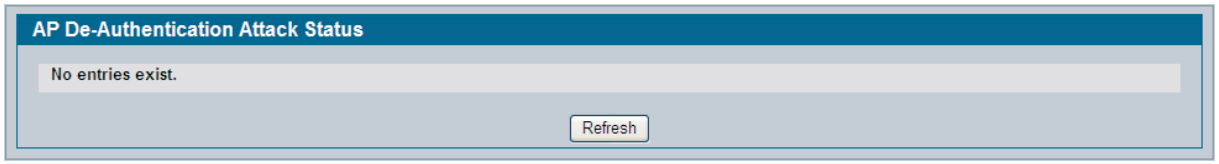


図 9-81　AP De-Authentication Attack Status 画面

以下の表には「AP De-Authentication Attack Status」画面内の各項目について説明します。

項目	説明
BSSID	攻撃を開始するアクセスポイントの BSSID を参照します。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	アクセスポイントが起動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。

リスト内のアクセスポイントの MAC アドレスをクリックして、アクセスポイントの詳細な RF スキャン情報にアクセスします。

システムの詳細設定

「Advanced Configuration」フォルダには以下の画面へのリンクがあります。

- Advanced Global Setting
- Known Client
- AP Profiles
- Peer Switch
- WIDS Security

Global（高度なグローバル設定）

統合スイッチにグローバルな設定を行います。

Genral タブ

WLAN タブ > 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。

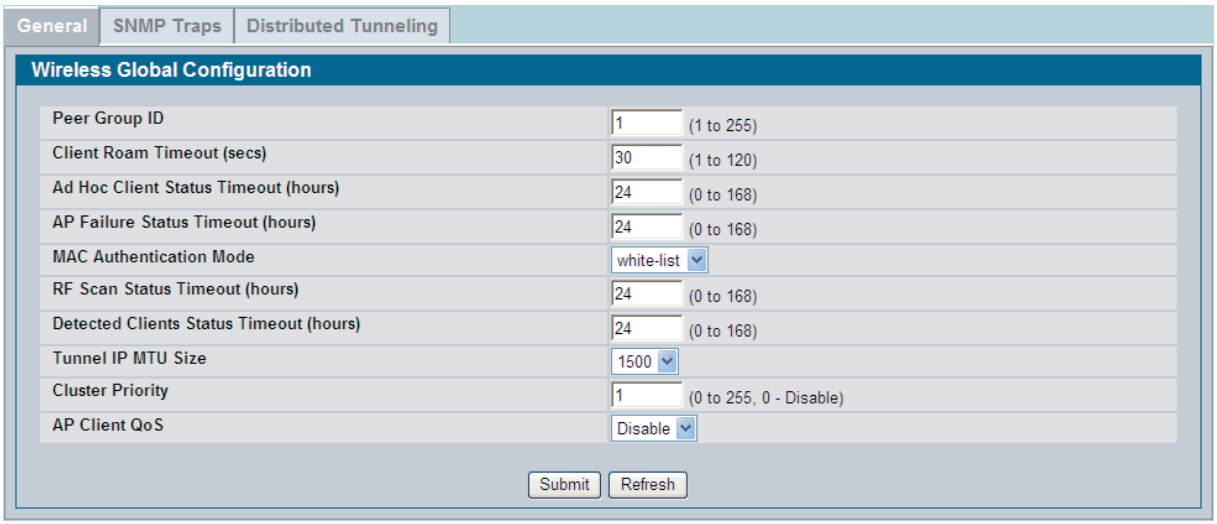


図 9-82　Wireless Global Configuration 画面

以下の表に「Wireless Global Configuration」画面の各項目について説明します。

項目	説明
Peer Group ID	大規模なネットワークを運用するために、クラスタ（ピアグループ）内の 64 台までのスイッチと共にピアとして無線スイッチを設定することができます。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。ピアはグループ ID によりグループ分けされます。
Client Roam Timeout (secs)	クライアントとアクセスポイント間の接続が切れてから、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。リストには、切断してからの経過時間（Age）が表示され、この値がこの項目で指定した値に到達した時にそのエントリがリストから削除されます。
Ad Hoc Client Status Timeout (hours)	「Ad Hoc Client Status」リストにエントリを表示しておく時間を指定します。リストには、切断してからの経過時間（Age）が表示され、この値がこの項目で指定した値に到達した時にそのエントリがリストから削除されます。
AP Failure Status Timeout (hours)	この値は、「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。リストには、切断してからの経過時間（Age）が表示され、この値がこの項目で指定した値に到達した時にそのエントリがリストから削除されます。
MAC Authentication Mode	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。 MAC 認証はネットワークレベルで有効にされます。また、ネットワーク設定は、MAC アドレスがローカルデータベース、または、RADIUS サーバで検索されるかどうかを定義します。
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。リストには、切断してからの経過時間（Age）が表示され、この値がこの項目で指定した値に到達した時にそのエントリがリストから削除されます。
Detected Clients Status Timeout (hours)	この値は「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。リストには、切断してからの経過時間（Age）が表示され、この値がこの項目で指定した値に到達した時にそのエントリがリストから削除されます。

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出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 機能を有効または無効にします。AP Client QoS を無効にすると、クライアント QoS 設定はそのまま残りますが、無線トラフィックに適用されるどんな ACL または DiffServ ポリシーも実行されません。クライアント QoS 機能は、統合スイッチのプライマリ QoS 機能を無線ドメインまで拡張します。より詳しく述べると、アクセスコントロールリスト（ACL）と DiffServ ポリシーはアクセスポイントに接続する無線クライアントに適用されます。

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。

WLAN タブ > 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 9-83　Wireless SNMP Trap Configuration 画面

アクセスポイントがスイッチに管理されている場合、どんなトラップも送出しません。スイッチは自身のイベントと、配下のアクセスポイントからの情報更新により学習したイベントを元にすべての SNMP トラップを生成します。

注意 無線トラップモードを有効にした場合にだけ無線トラップを設定することができます。**LAN タブ > Administration > SNMP Manager** の順にメニューをクリックし、「Trap Flags」画面を表示します。

すべての無線 SNMP トラップは初期値で無効に設定されています。以下の表では SNMP トラップを生成するイベントを示します。すべてのトラップは初期値で無効に設定されています。

特に記載しない限り、以下の表で示すトラップはクラスタコントローラだけに生成されます。

項目	説明
AP Failure Traps	有効にすると、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	有効にすると、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。 • 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	有効にすると、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。
Client State Change Traps	有効にすると、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	有効にすると、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	有効にすると、RF スキャンによって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が検出された時 SNMP エージェントがトラップを送信します。
Rogue AP Traps	有効にすると、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	有効にすると、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	有効にすると、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

Distributed Tunneling タブ（Distributed トンネリング設定）

Distributed トンネリングモードは AP-AP トンネリングモードとしても知られ、どんなデータも無線スイッチに送信されないで無線クライアント用に L3 ローミングをサポートするために使用されます。

AP-AP トンネリングモードでは、クライアントが最初に無線システム内でアクセスポイントに接続する場合、アクセスポイントは、VLAN のフォワーディングモードを使用することで無線クライアントのデータを転送します。クライアントが初めに接続するアクセスポイントはホーム AP です。クライアントがローミングするアクセスポイントはアソシエーション AP です。

クライアントが異なるサブネットで別のアクセスポイントにローミングする場合、CAPWAP L2 トンネルを使用することでアソシエーション AP はすべてのトラフィックをクライアントからホーム AP までにトンネリングします。ホーム AP はトンネルを経由してトラフィックを有線ネットワークにフローします。クライアントが同じサブネットで別のアクセスポイントにローミングする場合、トンネルは作成されず、新しいアクセスポイントはクライアント用のホーム AP になります。

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。

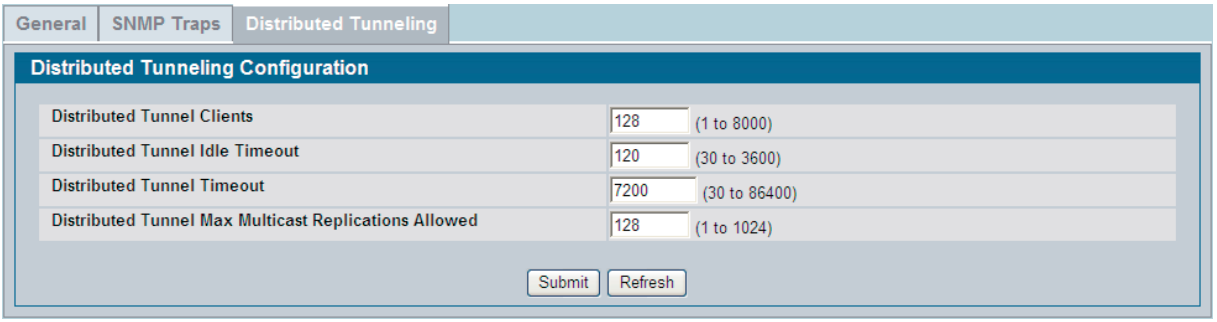


図 9-84　Distributed Tunneling Configuration 画面

以下の表は「Distributed Tunneling Configuration」画面の項目を示しています。

項目	説明
Distributed Tunnel Clients	ホーム AP から同時に移動できる Distributed 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。

Known Client（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。データベースには無線クライアントの MAC アドレスと名前があります。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。

WLAN タブ > 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 9-85　Known Client Summary 画面

以下の表は「Known Client Summary」画面の各項目を説明します。

項目	説明
MAC Address	既知のクライアントの 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。 • 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 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、クライアントを処理する方法を決定します。

「Known Client」リストに無線クライアントを追加するためには、クライアントの MAC アドレスを入力して、「Add」ボタンをクリックします。

「Known Client」データベースからクライアントを削除するためには、クライアントの MAC アドレス横の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。

データベースからすべてのクライアントを削除するためには、「Delete All」ボタンをクリックします。

既存クライアントに関する情報を参照または設定するために、クライアントの「MAC Address」のリンクをクリックします。

Known Client Configuration（既知のクライアントの設定）

Known Client データベースにクライアントを追加するか、または「Known Client Summary」画面からクライアントの「MAC Address」のリンクをクリックすると、以下の画面が表示されます。

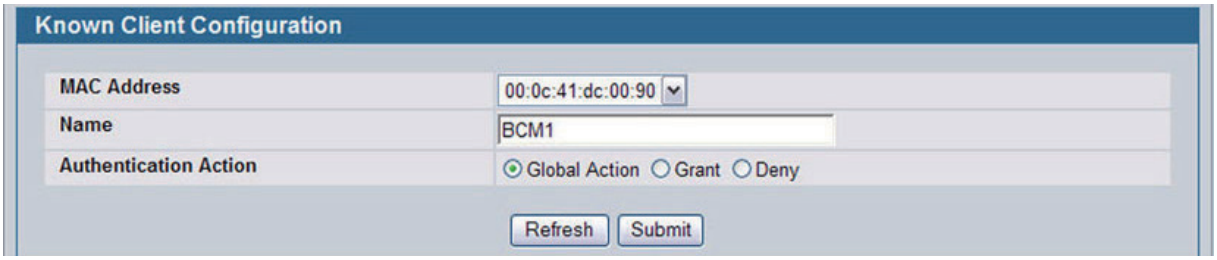


図 9-86　Known Client Configuration 画面

ネットワークへのアクセスを試みる場合に、クライアントに記述名を追加して、クライアントを引き受けるために認証動作を指定できます。

以下の表は「Known Client Configuration」画面の各項目の説明をします。

項目	説明
MAC Address	クライアントの MAC アドレスを表示します。Known Client データベース内の別のクライアントに名称または認証の動作を参照、または設定するためには、メニューから MAC アドレスを選択します。
Name	クライアントの記述名（半角英数字 32 文字以内）を入力します。この項目はオプションです。
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 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、クライアントを処理方法を決定します。

Wireless Network List（無線ネットワークリスト）

無線ネットワークリストでは、スイッチに設定されているすべての無線ネットワークを表示します。最初に 16 個のネットワークが初期値で作成されます。デフォルトネットワークを変更できますが、削除することはできません。合計 128 個の無線ネットワークが可能であるため、最大 112 個の追加ネットワークを設定することができます。マルチネットワークは同じ SSID を持つことができます。

WLAN タブ > 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 9-87　Known Client Summary 画面

以下の項目が表示されます。

項目	説明
ID	自動的に生成されたネットワークの識別子。初期値では 16 個のネットワークに 16 までの ID が割り当てられます。 スイッチは最大 128 個のネットワークをサポートします。
SSID	ネットワーク名を指定します。SSIDは、ネットワークのための「Wireless Network Configuration」画面へのハイパーリンクを持っています。
VLAN	無線ネットワークが使用する VLAN ID を表示します。
Hide SSID	ネットワークが 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。設定内容を変更するためには、「Edit」ボタンをクリックします。
L3 Tunnel	ネットワークにおいて L3 トンネリングが有効かどうかを表示します。 **注意** L3 トンネリングが有効である時、上で設定した VLAN ID は使用されません。実際には、スイッチはアクセスポイントに向かうトンネリングパケットに管理用 VLAN ID を設定します。
Security	ネットワーク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。本フィールドに設定可能な値は以下の通りです。 • 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。

ネットワークの削除

ネットワークを削除するためには、ネットワーク ID 横にあ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。ネットワーク（1-16）を削除することはできません。

ネットワークの作成

新しいネットワークを作成するためには、「Wireless Network List」で「SSID」を入力し、「Add」ボタンをクリックします。新しいネットワーク用の「Wireless Network Configuration」画面が表示されます。

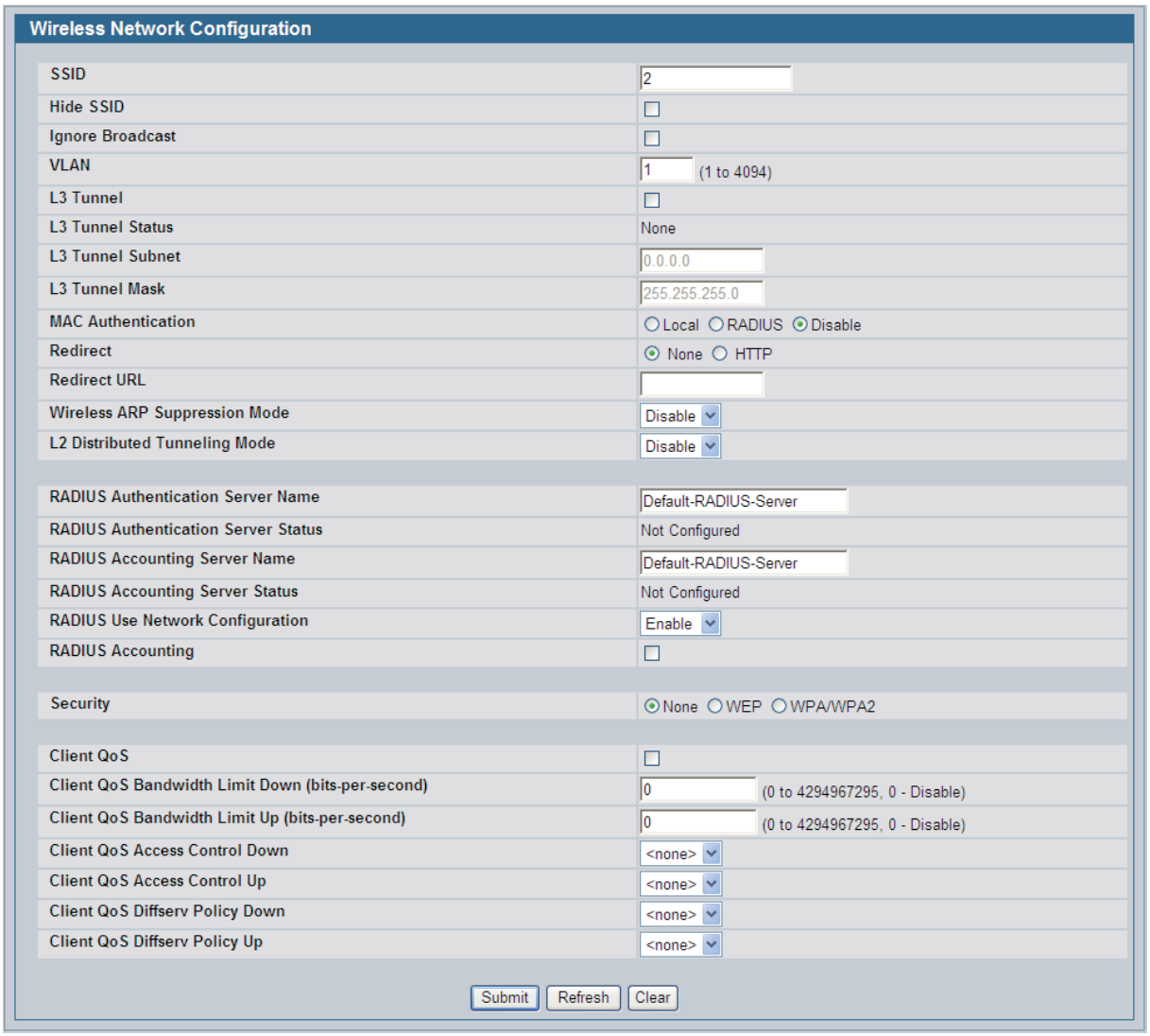


図 9-88　Known Client Summary 画面

各項目についての詳細情報は「デフォルトネットワークの設定」（285 ページ）を参照してください。

AP プロファイル

アクセスポイント・コンフィグレーションプロファイルは、様々なユーザ層において使用されるアクセスポイントを集約する、規模の大きな無線ネットワークに非常に有効な機能です。統合スイッチ上で複数の AP プロファイルを作成することにより、場所、機能なまたは他の要素に基づいてアクセスポイントをカスタマイズすることができます。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。

各 AP プロファイルには、以下の機能を設定することができます。

- プロファイル設定（Name、Hardware Type ID、Wired Network Discovery VLAN ID）
- 無線設定
- SSID 設定
- QoS 設定

以下の図は、あるキャンパスのネットワークにおいて、統合スイッチの管理下に 10 台のアクセスポイントがあることを示しています。各建物には複数のアクセスポイントが設置されており、ネットワークの必要条件は各建物により異なるものとします。本 WLAN の管理者は、「Default」プロファイルに加えて、2 つの AP プロファイルを作成しています。

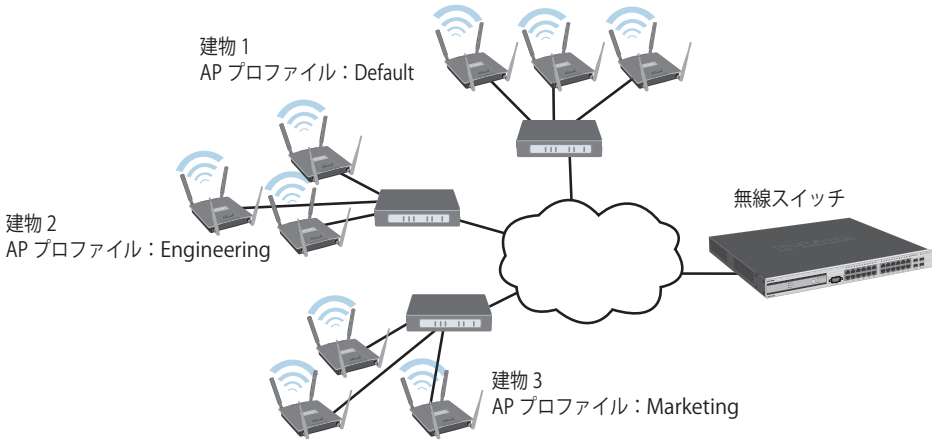


図 9-89　Multiple AP Profiles 画面

建物 1 にはメインロビーといくつかの会議室があります。この場所の WLAN ユーザは主に職員以外の人と訪問者です。建物 1 のアクセスポイントには、デフォルト AP プロファイルを適用し、追加のネットワークおよびセキュリティの設定はしていません。

建物 2 は工学部の建物です。建物 2 のアクセスポイントには「Engineering」というプロファイルを使用しています。「Engineering」AP プロファイルには、異なる SSID（Hardware、Software、Test）を持つ 3 つの VAP が定義されています。

建物 3 はセールスとマーケティングの建物です。建物 3 のアクセスポイントには「Marketing」というプロファイルを使用しています。「Marketing」AP プロファイルには、異なる SSID（Sales、Marketing、Program Management）を持つ 3 つの VAP が定義されています。

ネットワーク管理者が建物 2 にもう 1 台のアクセスポイントを設置する場合、AP 認知プロセス中に、アクセスポイントに対して「Engineering」プロファイルが割り当てられます。

注意　無線システムから一貫した情報を取得するために、スイッチクラスタ内では、プロファイルをすべてのスイッチで一致させることをお勧めします。

アクセスポイントプロファイルの作成、コピー、削除

AP プロファイルの作成、コピーおよび削除をすることができます。統合スイッチでは 16 件までの AP プロファイルを作成できます。

WLAN タブ > Administration > Advanced Configuration > AP Profile の順にメニューをクリックし、以下の画面を表示します。

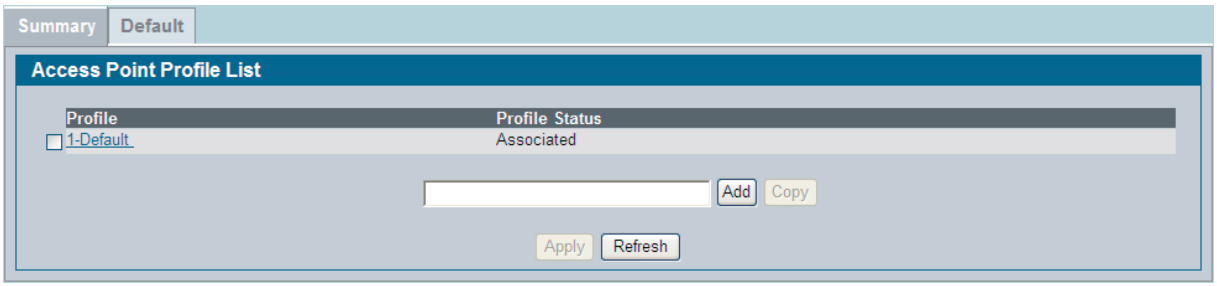


図 9-90　Access Point Profile List - プロファイルの追加 画面

プロファイルの追加

新しいプロファイルを作成するためには、プロファイル名を入力し、「Add」ボタンをクリックします。

プロファイルを追加すると、そのプロファイル用にプロファイル設定ページが表示され、そのページの上部に、作成したプロファイル名のタブが表示されます。新しいプロファイルを追加すると、付録 B で示す内容のデフォルト AP 設定が割り当てられます。以下の画面は AP Profile 設定のためのレイアウトを示しています。

プロファイルのコピー

既に作成済みのプロファイルとその設定内容をコピーするためには、コピー元のプロファイルを選択し、新しいプロファイル名を入力したら「Copy」ボタンをクリックします。

プロファイルの削除

プロファイルを削除するためには、プロファイルを選択して「Delete」ボタンをクリックします。

定義済みプロファイルへのアクセス

作成済みのプロファイルにアクセスするためには、目的のプロファイル名のタブをクリックします。

プロファイルへの追加機能の設定

「Global」、「Radio」、「SSID」、「QoS」のタブをクリックし、プロファイルに追加機能を設定します。

Global タブ

作成済みのプロファイルにアクセスするためには、目的のプロファイル名のタブをクリックし、以下の画面を表示します。

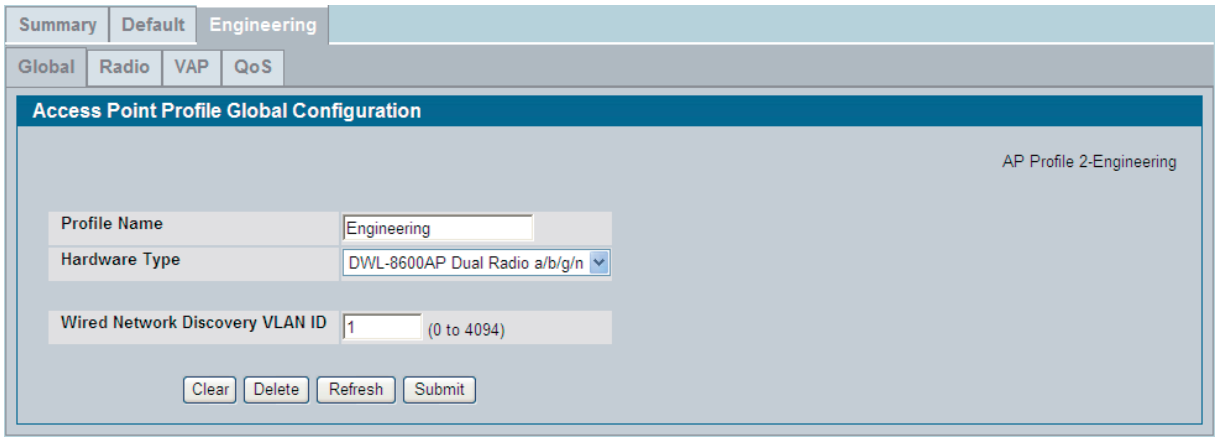


図 9-91　Access Point Profile Global Configuration 画面

以下の項目があります。

項目	説明
Profile Name	追加したアクセスポイントのプロファイル名。0-32 文字を使用します。英数字だけが許可されます。特殊文字は許可されません。
Hardware Type ID	このプロファイルを使用するアクセスポイントに対してハードウェアタイプを選択します。ハードウェアタイプは、アクセスポイントがサポートする無線インタフェース数（シングルまたはデュアル）と無線インタフェースがサポートする IEEE 802.11 モード（a/b/g/ または a/b/g/n）により決定されます。 ハードウェアタイプで利用可能なオプションは以下の通りです。 • DWL-8600AP Dual Radio a/b/g/n
Wired Network Discovery 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、スイッチが D-Link 統合アクセスシステムに所属しないが、有線ネットワークに接続する未認証アクセスポイントを識別するために使用されます。

プロファイルを選択し、「Clear」ボタンをクリックすると、すべての設定はプロファイル名を除き、プロファイルの初期値に設定されます。
プロファイルを削除するためには、プロファイルを選択して「Delete」ボタンをクリックします。
「Refresh」ボタンをクリックすると、画面に表示した情報はスイッチの設定に更新されます。
設定を変更した場合、「Submit」ボタンをクリックし、新しい設定をスイッチに適用します。

タブ	説明
Global	「プロファイル（Profile タブ）」（279 ページ）を参照してください。
Radio	「周波数帯域（Radio タブ）」（279 ページ）を参照してください。
Network	「SSID 設定（SSID タブ）」（284 ページ）を参照してください。
QoS	「QoS タブ（アクセスポイントプロファイル QoS 設定）」（368 ページ）を参照してください。

アクセスポイントプロファイルの適用

統合スイッチ上で AP プロファイルを更新した場合、その変更内容は、そのプロファイルを使用しているアクセスポイントに自動的には適用されません。プロファイルの変更内容の適用は「Access Point Profile Summary」ページにて明示的に行うか、またはそのプロファイルを使用するアクセスポイントを再起動する必要があります。

注意 無線ネットワークの VLAN ID を変更する場合、アクセスポイントは、更新したプロファイルを適用する際に一時的に DHCP に割り当てられた IP アドレスを喪失します。これが発生すると、アクセスポイントは Standalone モードになります。アクセスポイントがご使用のネットワークの DHCP サーバから IP アドレスを再取得すると直ちに通常操作を管理アクセスポイントとして再開します。また、VAP（SSID）を有効または無効にする場合、および AP プロファイルを最適用する場合の動作を参照します。

プロファイルの変更を、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適用するためには、以下の図に示すように、プロファイルを選択して「Apply」ボタンをクリックします。

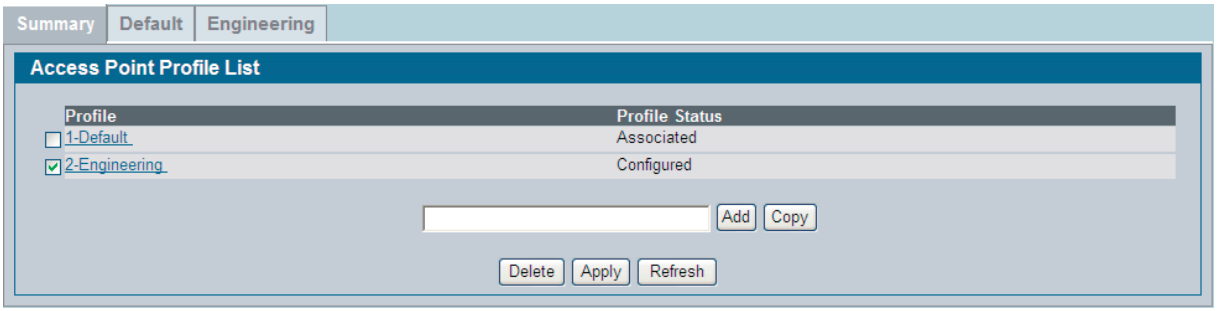


図 9-92　Access Point Profile List - Applying the AP Profile 画面

注意 新しい AP プロファイルをアクセスポイントに適用する際、アクセスポイントは一旦停止し、システムプロセスを再開します。この時、無線クライアントは一時的に接続を失います。アクセスポイントの設定変更は WLAN のトラフィックが低い時間帯にすることをお勧めします。

「Profile Status」には以下のいずれかの状態が表示されます。

項目	説明
Associated	本プロファイルは登録されており、1 台以上のスイッチ管理下のアクセスポイントに割り当てられています。
Associated-Modified	本プロファイルは複数のアクセスポイントに割り当てられた後に変更されています。再適用して、変更内容をアクセスポイントに反映する必要があります。
Apply Requested	プロファイルを指定して「Apply」ボタンをクリックすると、画面が更新され、リクエストが適用されたことを表示します。
Apply In Progress	本プロファイルを使用するすべてのアクセスポイントに対して、プロファイルを適用されているところです。本プロセス中にアクセスポイントが再起動され、クライアントとの接続が切断されます。
Configured	本プロファイルは登録済みですが、現在どのアクセスポイントも本プロファイルを使用していません。

注意 Valid AP データベースに登録されているアクセスポイントにプロファイルを割り当てます。

QoS タブ（アクセスポイントプロファイル QoS 設定）

D-Link 統合スイッチにおける QoS（Quality of Service）機能は、複数のキューにパラメータを指定することで、従来の IP データをはじめ VoIP（Voice over IP）や音声、映像、ストリーミングメディアなどの多くの無線トラフィックのスループットとパフォーマンスの向上を可能にします。

AP プロファイルの「QoS Configuration」画面を表示するためには、**WLAN タブ > Advanced Configuration > AP Profile** の順にメニューをクリックし、プロファイルのタブを選択し、「QoS」タブをクリックします。設定する無線インタフェースに対応するラジオボタンをクリックします。（QoS は無線インタフェースごとに設定されます。）

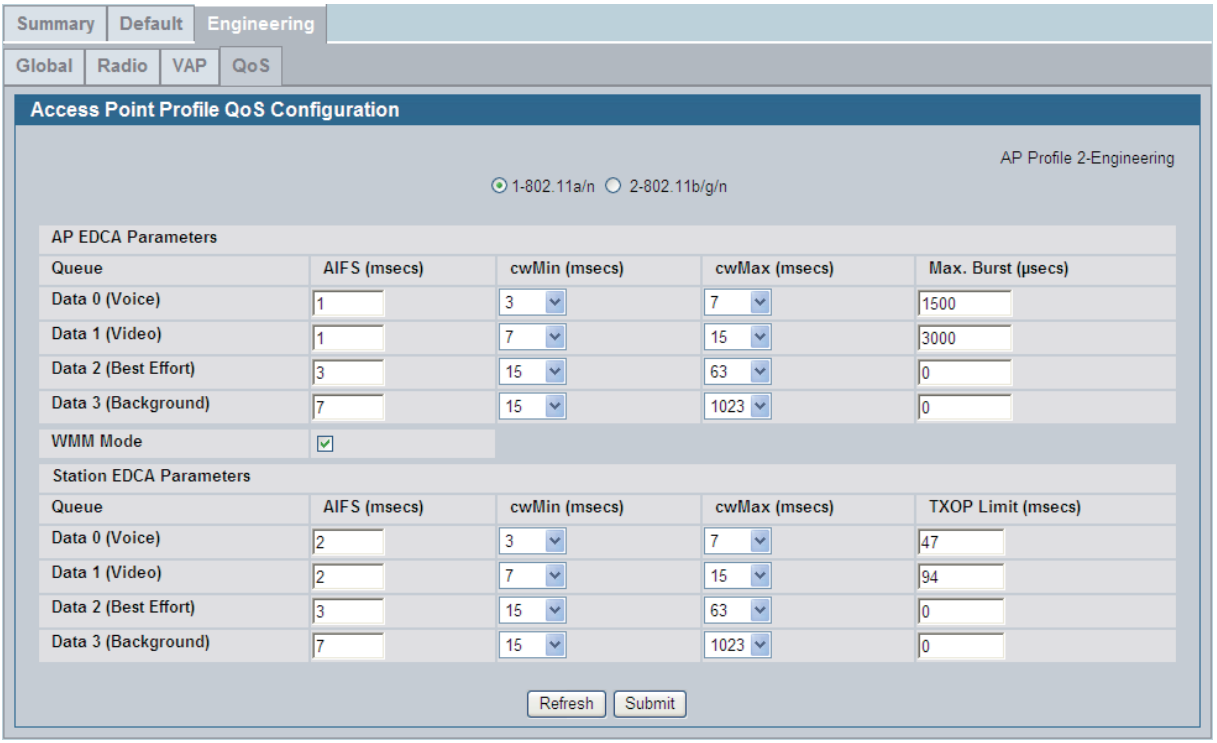


図 9-93　Access Point Profile QoS Configuration 設定画面

D-Link 統合スイッチで使用する QoS は、主に様々な種類の無線トラフィック用のキューにパラメータを設定すること、そして、伝送時の最大 / 最小待ち時間を（コンテンション画面により）効果的に指定することができます。ここで説明された設定は、データ伝送動作をアクセスポイントにだけ適用され、クライアントステーションには適用されません。

「AP EDCA（Enhanced Distributed Channel Access）Parameters」はアクセスポイントからクライアント向きのトラフィックフローに影響し、逆に「Station EDCA Parameters」は、クライアントからアクセスポイント向きのトラフィックフローに影響します。

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
AP EDCA Parameters	
Queue	アクセスポイントからクライアントに送信する様々なデータタイプにキューを定義します。 • Data 0（Voice）- 高優先度キュー、最小遅延。遅延に敏感な VoIP やストリーミングメディアなどのデータは自動的に本キューに送られます。 • Data 1（Video）- 高優先度キュー、最小遅延。遅延に敏感なビデオデータは自動的に本キューに送られます。 • Data 2（best effort）- 中優先度キュー、中スループット・中遅延。一般的な IP データは本キューに送られます。 • Data 3（Background）- 最低優先度キュー、高スループット。高いスループットを要する大容量データや、遅延に敏感ではないデータは本キューに送られます（例 :FTP データなど）。
AIFS (Inter-Frame Space)	AIFS（Arbitration Inter-Frame Spacing）では、データフレーム間の待ち時間を指定します。待機時間はスロットで測定されます。1 から 255 の間の値を指定します。単位はミリ秒です。
cwMin (Minimum Contention Window)	本パラメータは、伝送リトライの " 初回ランダムバックオフ待ち時間 "（画面）を定義するアルゴリズムに使用します。 本フィールドの値は、" 初回ランダムバックオフ待ち時間 " の範囲の上限として指定します。単位はミリ秒です。 1 番目のランダム（任意）番号は、0 から本欄で指定する値の中から生成されます。 データフレームが送信される前に、1 番目のランダムバックオフ待ち時間が失効すると、リトライカウンタは 1 増加し、ランダムバックオフ値（画面）は 2 倍の値になります。このランダムバックオフ値が、次のフィールドの cwMax で定義する値に到達するまで、失効に伴って値を倍にしていきます。cwmin に対する有効な値は、1,3,7,15,31,63,127,255,511, または 1024 です。cwmin 値には cwMax で定義する値より小さい値を指定してください。

項目	説明
cwMax (Maximum Contention Window)	ランダムバックオフ値の上限です。ランダムバックオフ値は、データフレームが送信されるか、本フィールドで指定した値に到達するまで、倍掛けされていきます。単位はミリ秒です。ランダムバックオフ値が、本欄で指定した値に到達すると、リトライは " リトライ許可最大回数 " に到達するまで継続されます。 cwma に対する有効な値は、1,3,7,15,31,63,127,255,511, または 1024 です。cwmax 値には cwmin で定義する値より大きい値を指定してください。
Max.Burst Length	AP EDCA パラメータ用のみ（本欄に指定する値はアクセスポイントからクライアントへのトラフィックフローに対してのみ適用されます）。本値は無線ネットワークでのパケットバーストに認められる最大バースト長です。パケットバーストとはヘッダ情報なしで送信できる複数のフレームの集まりです。オーバヘッドを少なくすることにより、高スループットと高パフォーマンスを実現できます。最大バースト長に有効な値は、0.0 から 999 です。
General Parameters	
WMM Mode	WMM（Wi-Fi Multimedia）機能は、デフォルトで有効になっています。WMM が有効であると、QoS 優先制御や無線メディアアクセスの調整も有効になります。また D-Link 統合スイッチシステムの QoS 設定は上りと下り両方のトラフィック（クライアントからアクセスポイント [Station EDCA パラメータ]、およびアクセスポイントからクライアント [AP EDCA パラメータ]）に対して有効になります。 WMM を無効に設定すると、QoS 制御は上りのトラフィック（クライアントからアクセスポイント [Station EDCA パラメータ]）に対して無効になります。下りについては、いくつかのパラメータ [AP EDCA パラメータ] の設定は有効です。 Station EDCA パラメータ（クライアントからアクセスポイントへの上りトラフィック）のみの設定です。 WMM 機能を無効にするためには「Disabled」を、有効にするためには「Enabled」を選択してください。
Station EDCA Parameters	
Queue	ステーションからアクセスポイントに送信する様々なデータタイプにキューを定義します。 • Data 0（Voice）- 最高優先度キュー、最小遅延。遅延に敏感な VoIP やストリーミングメディアなどのデータは自動的に本キューに送られます。 • Data 1（Video）- 最高優先度キュー、最小遅延。遅延に敏感なビデオデータは自動的に本キューに送られます。 • Data 2（best effort）- 中優先度キュー、中スループット・中遅延。一般的な IP データは本キューに送られます。 • Data 3（Background）- 最低優先度キュー、高スループット。高いスループットを要する大容量データや、遅延に敏感ではないデータは本キューに送られます（例 :FTP データなど）。
AIFS (msecs) (Inter-Frame Space)	AIFS（Arbitration Inter-Frame Spacing）では、データフレーム間の待ち時間を指定します。待機時間はスロットで測定されます。1 から 255 の間の値を指定します。単位はミリ秒です。
cwMin (Minimum Contention Window)	コンテンション期間のデータ転送のために " 初回ランダムバックオフ待ち時間 "（画面）を定義するアルゴリズムに使用されます。本フィールドの値は、" 初回ランダムバックオフ待ち時間 " の範囲の上限（ミリ秒）として「Minimum Contention Window」画面で指定します。 1 番目のランダム（任意）番号は、0 から本フィールドで指定する値の中から生成されます。データフレームが送信される前に、1 番目のランダムバックオフ待ち時間が失効すると、リトライカウンタは 1 増加し、ランダムバックオフ値（画面）は 2 倍の値になります。このランダムバックオフ値が、次の欄の cwMax で定義する値に到達するまで、失効に伴って値を倍にしていきます。
cwMax (Maximum Contention Window)	ランダムバックオフ値の上限で、「Maximum Contention Window」画面で指定します。ランダムバックオフ値は、データフレームが送信されるか、本欄で指定した値に到達するまで、倍掛けされていきます。単位はミリ秒です。 ランダムバックオフ値が、本欄で指定した値に到達すると、リトライは " リトライ許可最大回数 " に到達するまで継続されます。
TXOP Limit (msecs)	ステーション EDCA パラメータのみ（本フィールドに指定する値はクライアントステーションからアクセスポイントへのトラフィックフローに対してのみ適用されます）。 TXOP（Transmission Opportunity: 送信権）は、WME クライアントが無線メディア上で送信を始める権利が発生する間隔です。本欄で設定した間隔（ミリ秒）で、WMM クライアントは無線ネットワーク上に送信する権利を与えられます。

ピアスイッチ

ピアスイッチコンフィグレーション機能を使用すると、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できるようになります。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。「Peer Switch Configuration Request Status」画面は、クラスタのスイッチにおけるコンフィグレーション更新のステータスに関する情報を提供します。

Configuration Request タブ

WLAN タブ > 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。

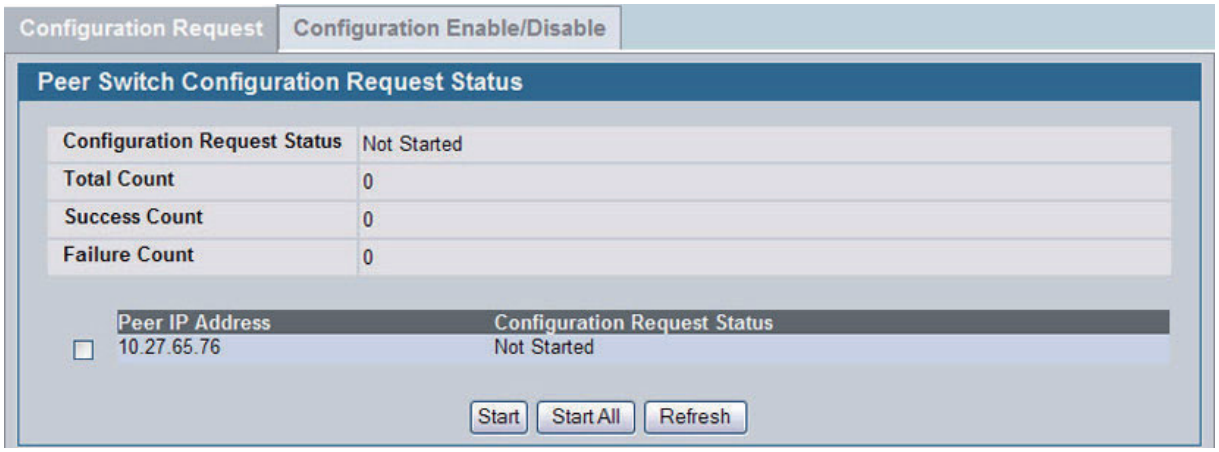


図 9-94　Peer Switch Configuration Request Status 画面

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。

以下の表は「Peer Switch Configuration Request Status」画面内の各項目の情報を示します。

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 アドレスと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。

Configuration Enable/Disable タブ

クラスタ内の 1 つのスイッチから別のスイッチにスイッチのコンフィグレーションの一部をコピーすることができます。ここでは、コンフィグレーションの部分を選択し、グループ内の 1 つ以上のスイッチにコピーすることができます。

WLAN タブ > Administration > Advanced Configuration > Peer Switch > Configuration Enable/Diable 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。

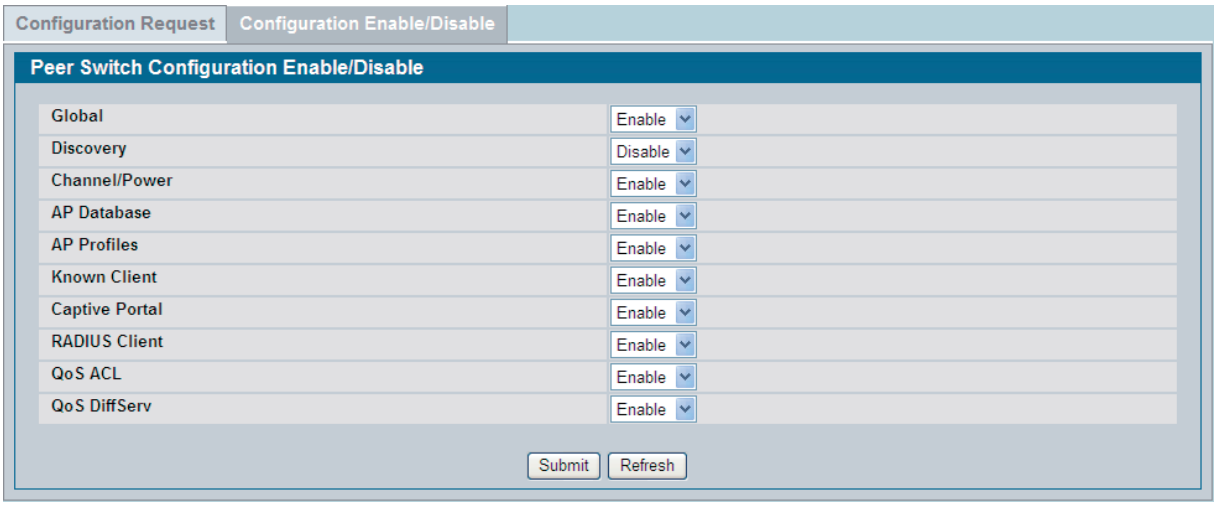


図 9-95　Peer Switch Configuration Enable/Disable 画面

1 つ以上のピアスイッチに送信されたコンフィグレーションを変更することができます。また、ピアスイッチから受信したコンフィグレーションを変更することもできます。 1 つのスイッチからクラスタに変更を伝達することはできません。どのようなコンフィグレーションもピアにコピーするためには、スイッチに手動でリクエストする必要があります。

以下の項目が表示されます。

項目	説明
Global	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的および高度なグローバル設定を含めるためには有効にします。そのコンフィグレーションには、ユニークな設定であるためスイッチの IP アドレスを含めません。 現在の基本的なグローバル設定を参照するためには、**WLAN タブ > Administration > Basic Setup > Global タブ**の順にメニューをクリックします。現在の高度なグローバル設定を参照するためには、**WLAN タブ > Advanced Configuration > Global タブ** をクリックします。
Discovery	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るためには有効にします。ローカルスイッチにおけるディスカバリ設定を参照するためには、**WLAN タブ > Administration > Basic Setup > Discovery タブ**の順にメニューをクリックします。
Channel/Power	スイッチがピアに設定するコンフィグレーションに RF 管理情報を含めるためには有効にします。 ローカルスイッチのチャンネルとパワー設定を参照するためには、**WLAN タブ > Administration > AP Management > RF Management タブ**の順にメニューをクリックします。
AP Database	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るためには有効にします。 ローカルな AP データベースを参照する場合は、**WLAN タブ > Administration > Basic Setup** の順にメニューをクリックし、「Valid AP」タブをクリックします。
AP Profiles	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るためには有効にします。AP プロファイルにはハードウェアタイプ、無線設定、VAP、および無線ネットワーク設定や、QoS 設定などのグローバルなアクセスポイント設定があります。 ローカルな AP プロファイル設定を参照するためには、**WLAN タブ > Administration > Advanced Configuration > AP Profile タブ**の順にメニューをクリックします。
Known Client	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るためには有効にします。 ローカルな AP データベースの内容を参照するためには、**WLAN タブ > Administration > Advanced Configuration > Clients > Known Client タブ**の順にメニューをクリックします。

項目	説明
Captive Portal	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るためには有効にします。 ローカルスイッチのキャプティブポータル情報を参照するためには **Security > Captive Portal** フォルダで有効なページをクリックします。 **注意** LAN か WLAN タブのいずれかから Captive Portal ページにアクセスできます。
RADIUS Client	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 情報を含めるためには有効にします。 ローカルスイッチの Client RADIUS を表示するためには、**LAN タブ > Security > RADIUS** の順にメニューをクリックします。
QoS ACL	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 を含めるためには有効にします。 ローカルスイッチの ACL 設定を表示するためには、**LAN タブ > Access Control Lists** の順にメニューをクリックします。
Qos DiffServ	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るためには有効にします。 ローカルスイッチの DiffServ 設定を表示するためには、**LAN タブ > QoS > Differentiated Services** の順にメニューをクリックします。

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）

「WIDS AP Configuration」画面では、無線ネットワークにおいて不正なアクセスポイントの検出を補助するために、様々な脅威検知のテストのアクティブ化の有効 / 無効、および脅威検知のしきい値の設定を行います。これらの変更はネットワークの接続を中断しないで行うことができます。アクセスポイントがいくつかの作業が必要であるため、スイッチは、WIDS の操作プロパティを変更するためにアクセスポイントにメッセージを送信する必要があります。

注意 「WIDS AP Configuration」画面の分類の設定は、スイッチのグローバルなコンフィグレーションの一部であり、そのコンフィグレーションを同期させるように手動で他のスイッチに行われる必要があります。

多くのテストが管理 SSID を通知していても、実は管理アクセスポイントではないアクセスポイントを識別することに焦点を合わせています。そのようなアクセスポイントの検出は、ネットワークがミスによって設定されたか、またはハッカーがパスワードまたは他のセキュアな情報を集めようとしてハニーポットアクセスポイントを設定したことを意味します。

操作可能な無線モードでは、多くの脅威を検出できますが、特に潜在的に不正なものが、管理されたアクセスポイントの無線モードのいずれとも異なるチャンネルで動作している場合、sentry モードでより速く脅威を検出できます。多くの sentry モードをおくことは、ネットワーク内のあらゆる場所に sentry モードによる適用範囲を提供するために必要です。より密度の高い sentry の配置は、不正または信号の干渉の測定を改善するために望ましいと言えます。

WLAN タブ > 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。

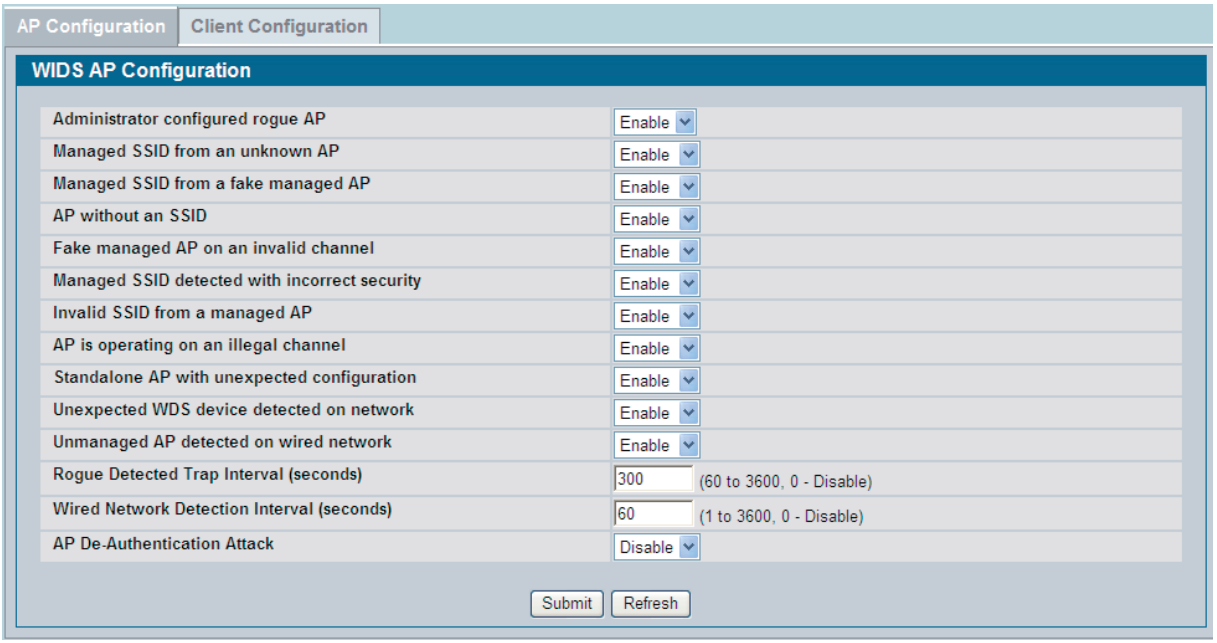


図 9-96　WIDS AP Configuration 画面

以下の表は「WIDS AP Configuration」画面の項目を示しています。

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「Rogue」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。
Invalid SSID from a managed AP	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	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。 このテストは潜在的な侵入試みと共にネットワークの構成ミスを検出する可能性があります。以下のパラメータがチェックされます。 • チャンネル番号 • SSID • セキュリティモード • WDS モード • 有線ネットワークにおける存在
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。

項目	説明
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。値に 0 を設定すると、トラップは送信されません。
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。 値に 0 を設定すると、有線ネットワーク検出は無効になります。
AP De-Authentication Attack	アクセスポイント認証解除攻撃を有効または無効にします。 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。

Client Configuration タブ（WIDS クライアントの設定）

D-Link 統合スイッチの Wireless Intrusion Detection システム（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。「WIDS Client Configuration」画面で行う設定は、検出されたクライアントが不正として分類されるかどうかの決定を補助します。不正として分類されたクライアントは、ネットワークセキュリティへの脅威であると見なされます。

注意 「WIDS Client Configuration」画面の分類設定は、スイッチのグローバルなコンフィグレーションの一部であり、そのコンフィグレーションを同期させるように手動で他のスイッチに行われる必要があります。

一般的な結合と認証プロセスの一部として、無線クライアントは 802.11 の管理メッセージをアクセスポイントに送信します。
WIDS 機能は、各検出クライアントが送信する以下に示す管理メッセージのタイプを追跡します。

- プローブ要求
- 802.11 の認証要求
- 802.11 の認証解除要求

管理トラフィックを使用してネットワークをフラッドすることで、クライアントがネットワークに脅威を引き起こしているかどうか判断するために、システムはアクセスポイントが各タイプのメッセージを受信した回数、および 1 つの RF スキャンレポートに検出された最も高いメッセージレートに絶えず注意を払います。「WIDS Client Configuration」画面では、送信される各メッセージタイプのしきい値を設定し、アクセスポイントはどんなクライアントもこのしきい値を超えていないかどうか監視またはテストします。

WLAN タブ > 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。

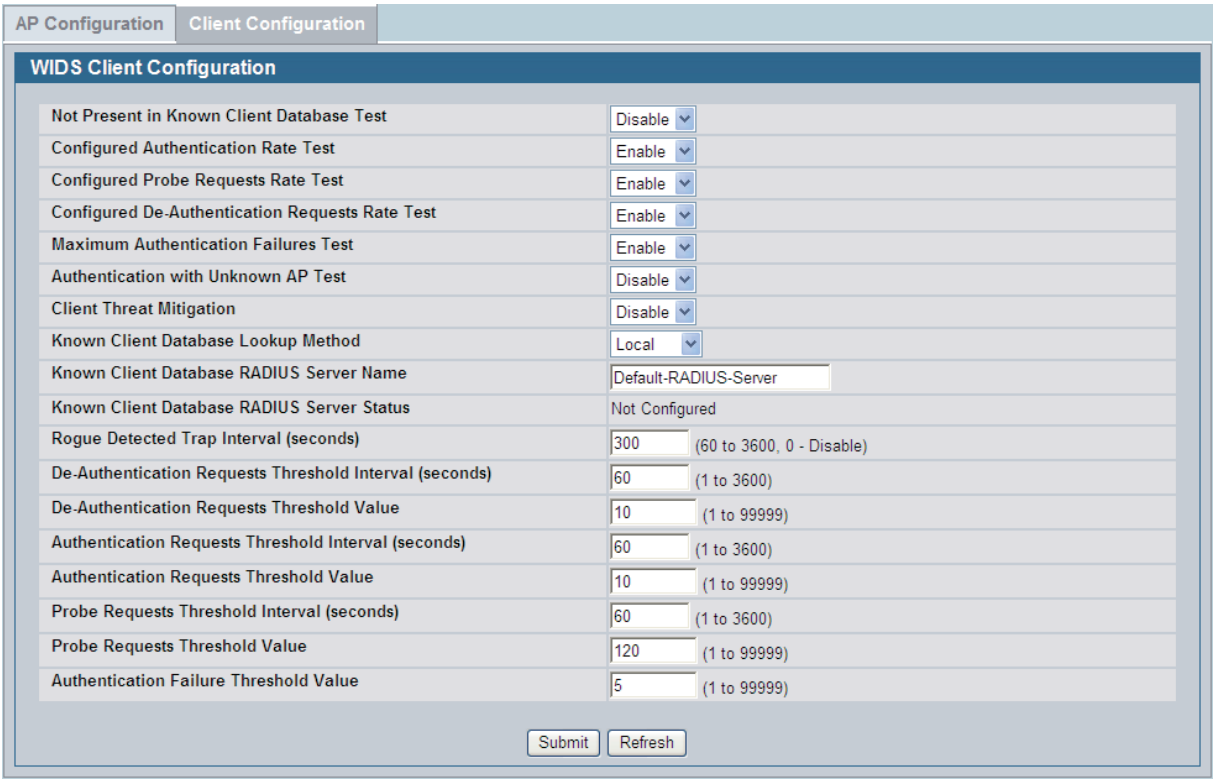


図 9-97　WIDS Client Configuration 画面

以下の表は「WIDS Client Configuration」画面の各項目について説明します。

項目	説明
Not Present in Known Client Database Test	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	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	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	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	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	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。
Known Client Database Radius Server Name	Known Client データベースの検索方法が RADIUS である場合、本欄には RADIUS サーバ名を指定します。
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。値に 0 を設定すると、トラップは送信されません。
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	しきい値の間、指定メッセージよりも多く受信すると。スイッチは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。
Authentication Requests Threshold Value	しきい値の間、指定メッセージよりも多く受信すると。スイッチは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。

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。

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。

- 背景画像のインポートと設定
- グラフコンポーネントの設定
- メニューバーについて
- グラフの管理

以下の図では、フロアプランと、統合スイッチと配下のアクセスポイントで構成するフロア計画の例を示します。

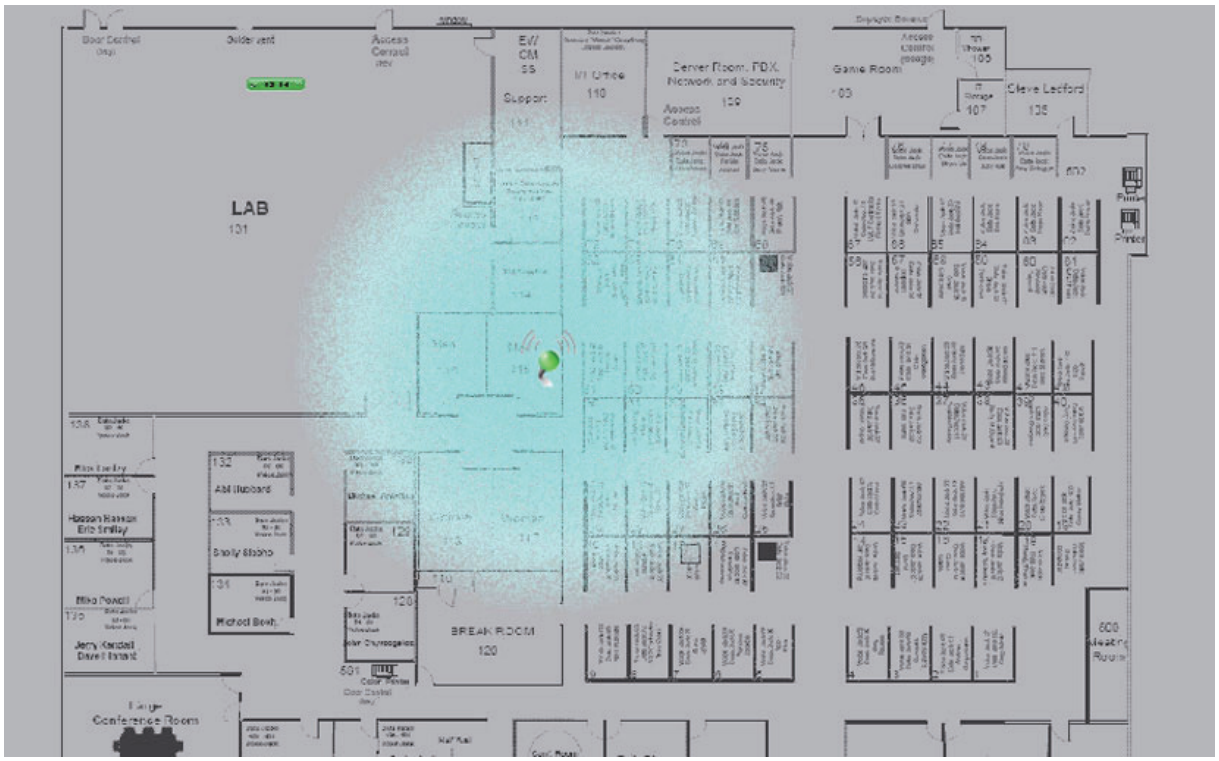


図 9-98　Sample WLAN Visualization 画面

背景画像のインポートと設定

初期状態では、WLAN 視覚化グラフ（図）に背景画像は設定されていません。例えば、オフィスの見取り図など、1 つまたは複数の画像をアップロードして、サイトの状況や、サイトに関係した情報をグラフを提供します。1MB の総サイズ制限で最大 16 個のイメージをアップロードできます。

アップロードする画像のフォーマットは、以下の通りです。

- GIF（Graphics Interchange Format）
- JPG（Joint Photographic Experts Group）

また、WLAN コンポーネントがグラフ内で目立たなくなるため、カラー画像をご使用にならないことをお勧めします。

以下の手順で、WLAN 視覚化グラフに使用する画像をスイッチにアップロードしてください。

1. **WLAN タブ > WLAN Visualization > Download Image** をクリックします。
2. 「参照」ボタンをクリックしてファイルの場所を検索します。
3. アップロードするファイルを選択して「Start File Transfer」ボタンをクリックします。

図 9-99　ダウンロードファイルの指定

画像ファイルをアップロードして現在の設定を保存すると、その画像はスイッチに登録されます。その後 WLAN 視覚化アプリケーションを使用して、グラフに割り付けることができるようになります。

グラフコンポーネントの設定

WLAN 視覚化ツールを起動するためには、**WLAN タブ > WLAN Visualization > Launch...** をクリックします。新しいブラウザの画面が表示され、Java アプレットが起動します。

初めて WLAN 視覚化ツールを起動する場合、背景画像が表示されません。また、検出された WLAN コンポーネントは図示されません。画面は 2 つの区画で構成されています。左側の区画は、さらに 3 つに分割されており、図示されていないコンポーネントが表示されます。右側の区画は、定義した図が表示されるエリアです。この図表示エリアは、初めは空白になっています。WLAN コンポーネントを取り込む前に、このエリアに背景を取り込んでおきます。

新規グラフの作成

新規にグラフ（図）を作成し、背景画像をアップロードするためには、WLAN 視覚化ツールを起動して以下の手順を実行してください。

1. 「WLAN Visualization」メニューバーの「Edit」で「New Graph...」を選択し、「New Graph Definition」ダイアログボックスを表示します。

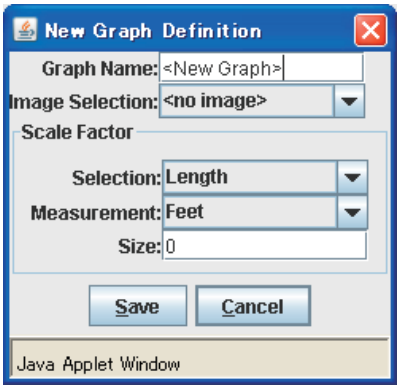


図 9-100　画像の選択と寸法の指定

2. グラフを識別する名前を入力し、背景として使用する画像を選択します。画像をグラフの背景として使用する方法については、「背景画像のインポートと設定」（377 ページ）を参照してください。

3. インポートする背景画像の大きさ（高さまたは幅）を示す、サイトでの実際の寸法を指定します。
「Selection」と「Measurement」プルダウンメニューから、指定した寸法を「Height（高さ）」または「Width（幅）」から、さらに単位を「メートル」または「フィート」から選択します。

ここで指定する値により背景画像の縮尺が決定されます。そしてこの縮尺値により、WLAN 視覚化ツールによるアクセスポイントの RF カバー範囲の見え方が変わってきます。そのため正確な寸法を入力する必要があります。

例えば、次のページの 2 つの図では、同じ背景画像を使用し、アクセスポイントも同じ位置に配置しています。一つ異なるのは、片方のグラフでは図の高さが 200 フィートと指定しているのに対して、もう片方では 800 フィートと指定しています。

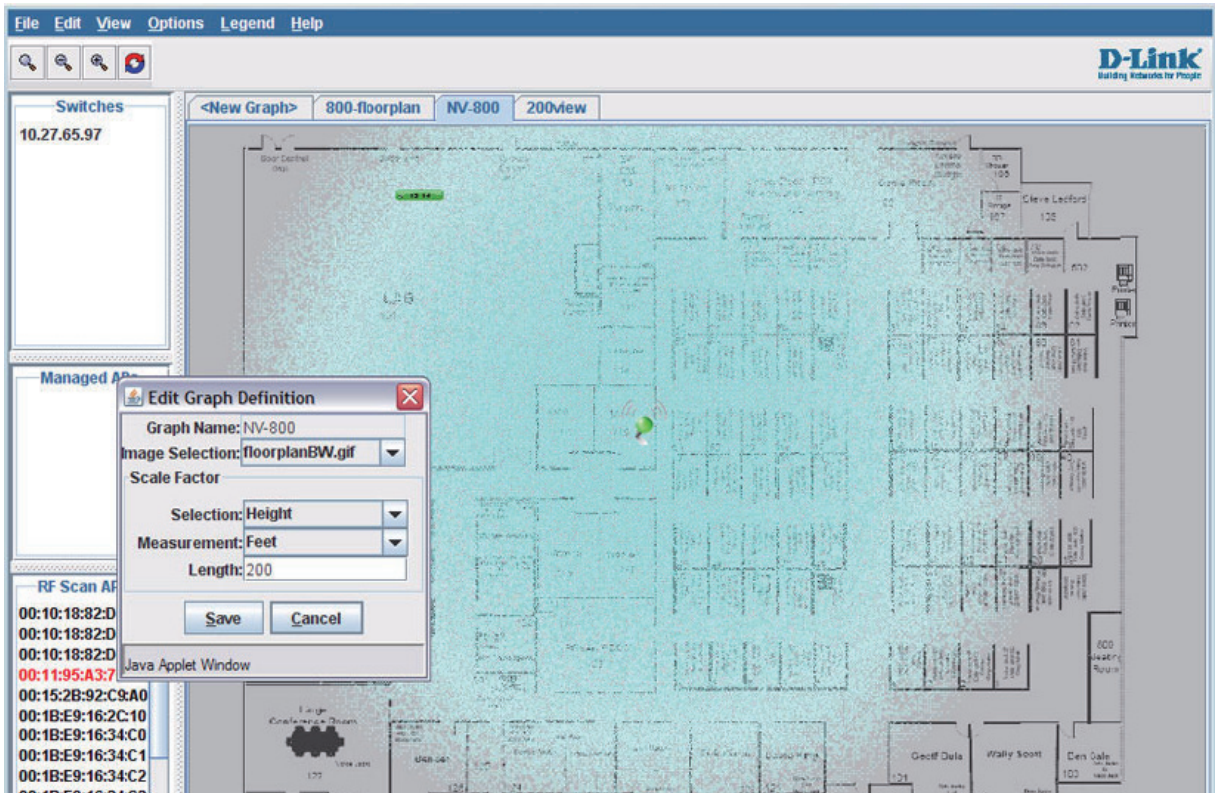


図 9-101　高さを 200 フィートにしたグラフ

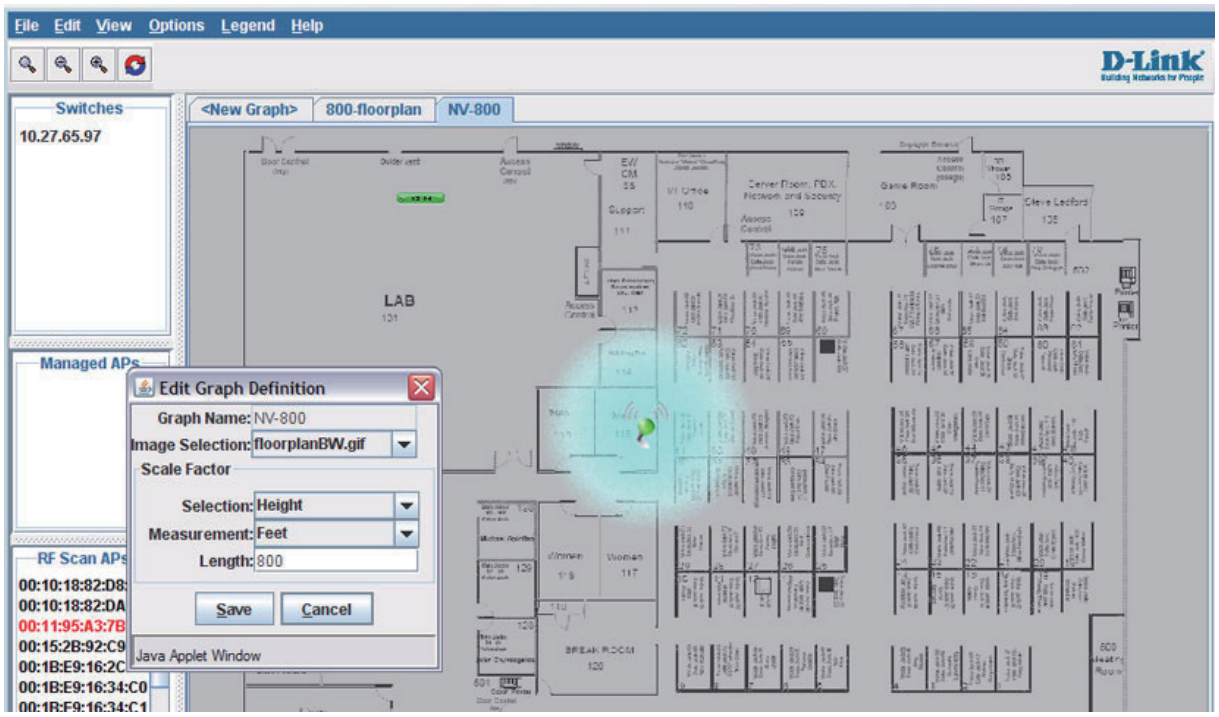


図 9-102　高さ = 800 フィートにしたグラフ

4. 「Save」ボタンをクリックして、グラフの設定を完了させます。
スイッチにアップロードした背景画像が、グラフの背景画像として表示されます。

本ツールでは、複数のグラフの作成も可能です。例えば、ご使用のネットワークが複数階のフロアにまたがっている場合は、各階ごとにグラフを作成することができます。追加したグラフは、以下の図で示すように、グラフ上部にタブの形で表示されます。

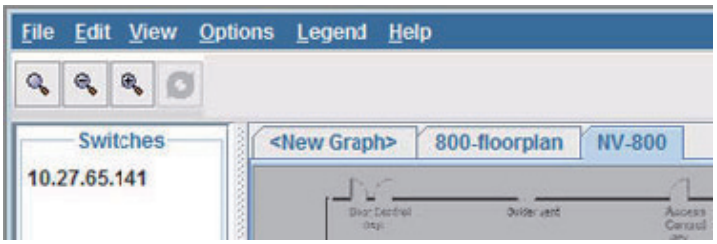


図 9-103　複数のグラフの場合

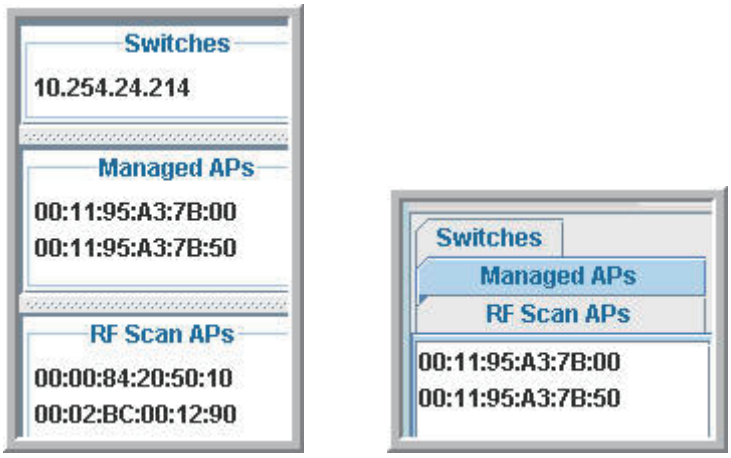
グラフの追加は、本項の手順を繰り返して行います。

WLAN コンポーネントの図示化

WLAN 視覚化ツールでは、スイッチが検出した WLAN コンポーネントを自動的に表示します。
画面上には、以下の種類のコンポーネントが表示されます。

- スイッチ（統合スイッチおよびピアスイッチ）
- 管理対象アクセスポイント
- RF スキャンアクセスポイント

これらのコンポーネントは、グラフ上にドラッグされるまでは、画面左の区画に表示されています。「View」メニューから、コンポーネントを「リスト表示（上記 3 種類がすべて表示されているタイプ）」または「タブ表示（1 種類のみの表示で残りはタブにまとめられているタイプ）」のいずれかを選択することができます。以下に同じ内容のコンポーネント群の「リスト表示」と「タブ表示」の例を示します。アクセスポイントについてはその場所名、または MAC アドレスが表示され、スイッチについてはその IP アドレスが表示されます。



リスト表示　　タブ表示

図 9-104　リスト表示とタブ表示

無線クライアントは、左側の区画には表示されず、図示化された D-Link アクセスポイントとの接続が検出されると、自動的にグラフエリアに表示されます。

図示化されていないコンポーネント上にマウスをポイントすると、以下の図のように、そのコンポーネントに関する詳細情報がポップアップ表示されます。

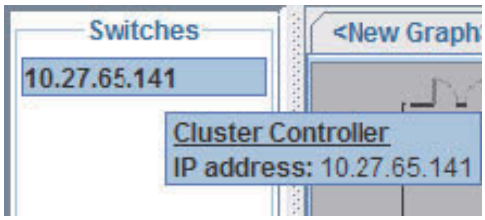


図 9-105　コンポーネント情報とポップアップ表示

左区画にリスト表示されているコンポーネントを図示化するためには、そのコンポーネントを選択し、そのままグラフエリア内にドラッグします。サイト内でコンポーネントが実際に配置されている場所を示すグラフエリア内の位置までドラッグしたら、マウスから手を離します。
スイッチまたはアクセスポイントをグラフエリアに移動させると、そのコンポーネントは左区画のリスト表示から削除されます。

「Shift」キーまたは「Ctrl」キーを押下しながら、コンポーネントを選択すると複数選択が可能になります。複数選択したものうちのどれか 1 つの上で右クリックをすると、選択したものすべてを一括してグラフエリア内へドラッグすることができます。

図 9-106　グラフ化されたコンポーネント

グラフからコンポーネントを削除するためには、コンポーネント上で右クリックし、「Edit」から「Un-Graph」を選択します。

メニューバーについて

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。

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	アクティブな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 回に 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 - 3 種類すべてのコンポーネントを左のパネルに表示します。 xx ページの図 9-104 に上記の 2 種類の表示方法の違いを示しています。
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 。 • 5 GHz 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を持つすべての管理アクセスポイントの送信電力を表示します。 • 2.4 GHz 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を持つすべての管理アクセスポイントの送信電力を表示します。 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	グラフ上での D-Link アクセスポイントの表示を指定します。チェックボックスのチェックを外すと、クライアントは見えなくなりますが、アイコン化したオブジェクト自体は記憶されています。
Show RF Scan APs	グラフ上に RF スキャンにより検出されたアクセスポイントを表示するかどうかを指定します。チェックボックスのチェックを外すと、クライアントは見えなくなりますが、アイコン化したオブジェクト自体は記憶されています。
Show Managed AP Clients	グラフ上にアクセスポイントと接続中のクライアントを表示するかどうかを指定します。チェックボックスのチェックを外すと、クライアントは見えなくなりますが、アイコン化したオブジェクト自体は記憶されています。
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	
Help	新しい HTML 画面を表示し、WLAN オンラインヘルプ画面を表示します。

「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。

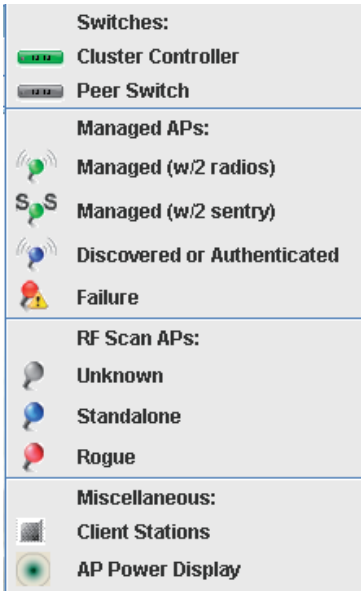


図 9-107　Legend 画面

凡例が示すように、スイッチ配下のアクセスポイントは、その状態によって青、緑または赤で表示されます。

- 青 - 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 - AP プロファイルが適用されており、管理対象モードで動作中です。
- 赤 - 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、以下の図で示すように、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 9-108　「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。

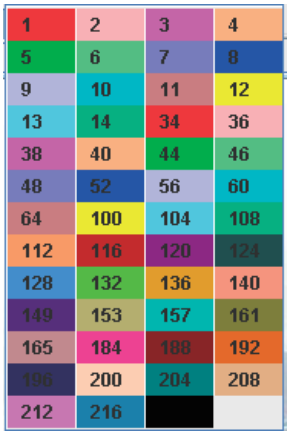


図 9-109　チャンネルの色

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。

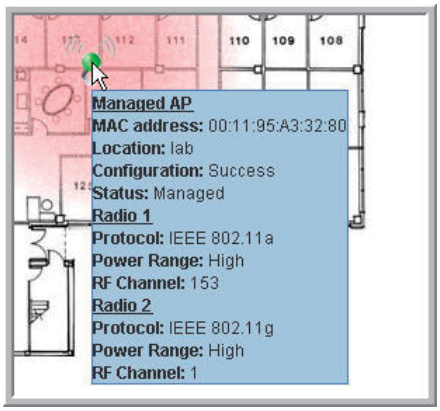


図 9-110　アクセスポイント情報ポップアップ画面

各オブジェクト上で右クリックすることにより、さらに詳細な情報を確認できます。

グラフの管理

グラフにコンポーネントを配置後、コンポーネント上で右クリックすることにより、そのコンポーネントについてのさらに詳細な情報の取得や、グラフからの削除、または Web インタフェースのページに遷移して、コンポーネントの管理やモニタを行うことができます。

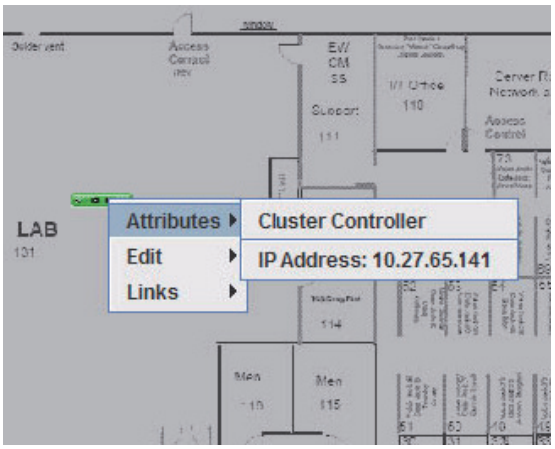


図 9-111　Wireless Component Attributes 画面

第 10 章　統合スイッチのログメッセージ

ここでは、統合スイッチが提供する一般的なログメッセージを各メッセージの原因に関する情報と共に記述します。メッセージ毎に行われる特定のアクションはありません。診断される問題がある場合、イベントログ内のこれらのメッセージのセットはシステムコンフィグレーションと問題の詳細を理解するために、また、D-Link がそのような問題の根本的な原因の判断をサポートするために便利です。

注意　本セクションはすべての syslog メッセージを表示しているわけではありません。

本セクションには以下のサブセクションがあります。

CORE

BSP ログメッセージ

コンポーネント	メッセージ	原因
BSP	Event(0xaaaaaaaa)	スイッチは再起動しました。
BSP	Starting code...	BSP の初期化は終了し、統合スイッチアプリケーションは開始しています。

NIM ログメッセージ

コンポーネント	メッセージ	原因
NIM	NIM: L7_ATTACH out of order for intIfNum(x) unit x slot x port x	インタフェース作成エラー
NIM	NIM: Failed to find interface at unit x slot x port x for event(x)	USP とインタフェース番号間にマッピングがありません。
NIM	NIM: L7_DETACH out of order for intIfNum(x) unit x slot x port x	インタフェース作成エラー
NIM	NIM: L7_DELETE out of order for intIfNum(x) unit x slot x port x	インタフェース作成エラー
NIM	NIM: event(x),intf(x),component(x), in wrong phase	間違った設定段階（おそらく段階 1、2、または WMU）で、イベントは NIM に発行されました。
NIM	NIM: Failed to notify users of interface change	イベントはシステムに伝搬されませんでした。
NIM	NIM: failed to send message to NIM message Queue.	NIM メッセージキューがいっぱいか、または存在しません。
NIM	NIM: Failed to notify the components of L7_CREATE event	インタフェースは作成されませんでした。
NIM	NIM: Attempted event (x), on USP x.x.x before phase 3	コンポーネントは間違った初期設定段階でインタフェースのイベントを発行しました。
NIM	NIM: incorrect phase for operation	間違った初期設定段階で API コールが行われました。
NIM	NIM: Component(x) failed on event(x) for intIfNum(x)	コンポーネントはインタフェースイベントに間違った指示で応答しました。
NIM	NIM: Timeout event(x), intIfNum(x) remainingMask = xxxx	NIM タイムアウトが発生する前にコンポーネントは応答しませんでした。

System ログメッセージ

コンポーネント	メッセージ	原因
SYSTEM	Configuration file fastpath.cfg size is 0 (zero) bytes	設定ファイルを読むことができませんでした。このメッセージは、コンフィグレーションが保存されていないか、またはコンフィグレーションが削除されているシステムに発生する可能性があります。
SYSTEM	could not separate SYSAPI_CONFIG_FILENAME	設定ファイルを読むことができませんでした。このメッセージは、コンフィグレーションが保存されていないか、またはコンフィグレーションが削除されているシステムに発生する可能性があります。
SYSTEM	Building defaults for file <file name> version <version num>	コンフィグレーションは存在しなかったか、指定機能またはファイルのために読み取ることができませんでした。コンフィグレーションの初期値が使用されます。ファイル名とバージョンが表示されます。
SYSTEM	File <filename>: same version (version num) but the sizes (<version size>-><expected version size) differ	ロードされたコンフィグレーションファイルは、バージョン番号で予想されるものとは異なるサイズでした。このメッセージは、コンフィグレーションファイルがコードイメージに適するバージョン番号に移行する必要あることを示しています。このメッセージは、コードイメージをより新しいリリースにアップグレードした後に表示されます。
SYSTEM	Migrating config file <filename> from version <version num> to <version num>	指定されたコンフィグレーションファイルは、以前のバージョンから移行されます。古いバージョン番号と新しいバージョン番号の両方が指定されます。このメッセージは、コードイメージをより新しいリリースにアップグレードした後に表示されます。
SYSTEM	Building Defaults	コンフィグレーションは存在しなかったか、指定機能のために読み取ることができませんでした。コンフィグレーションの初期値が使用されます。
SYSTEM	sysapiCfgFileGet failed size = <expected size of file> version = <expected version>	コンフィグレーションは存在しなかったか、指定機能のために読み取ることができませんでした。 このメッセージは、通常コンフィグレーションの初期値を使用することを示すメッセージの後に表示されます。

UTILITIES

Trap Mgr ログメッセージ

コンポーネント	メッセージ	原因
Trap Mgr	Link Up/Down: slot/port	インタフェースはリンク状態を変更しました。

DHCP Filtering ログメッセージ

コンポーネント	メッセージ	原因
DHCP Filtering	Unable to create r/w lock for DHCP Filtering	DHCP フィルタリングのコンフィグレーション構造に使用されるセマフォは作成することができません。
DHCP Filtering	Failed to register with nv Store.	コンフィグレーションの保存のために save と restore 機能の実行ができませんでした。
DHCP Filtering	Failed to register with NIM	インタフェースのコールバック機能のために NIM と共に登録することができませんでした。
DHCP Filtering	Error on call to sysapiCfgFileWrite file	コンフィグレーションの保存でエラーになりました。

NVStore ログメッセージ

コンポーネント	メッセージ	原因
NVStore	Building defaults for file XXX	コンポーネントのコンフィグレーションファイルが存在しないか、ファイルのチェックサムが不正であるため、コンポーネントのコンフィグレーションの初期ファイルが構築されます。
NVStore	Error on call to osapiFsWrite routine on file XXX	ファイルをオープンできなかったか、または OS のファイル I/O がファイルへの書き込みエラーを返しました。
NVStore	File XXX corrupted from file system. Checksum mismatch.	ファイルシステム内のコンポーネントのコンフィグレーションファイルの計算されたチェックサムがメモリ内のファイルのチェックサムに一致しませんでした。
NVStore	Migrating config file XXX from version Y to Z	コンフィグレーションファイルのバージョンの不一致が検出されたため、コンフィグレーションファイルのマイグレーションが開始しました。

RADIUS ログメッセージ

コンポーネント	メッセージ	原因
RADIUS	RADIUS: Invalid data length ? xxx	RADIUS クライアントはサーバから不正なメッセージを受信しました。
RADIUS	RADIUS: Failed to send the request	RADIUS サーバとの通信に問題が発生しました。
RADIUS	RADIUS: Failed to send all of the request	転送中に RADIUS サーバとの通信に問題が発生しました。
RADIUS	RADIUS: Could not get the Task Sync semaphore!	RADIUS クライアントサービスのリソース問題。
RADIUS	RADIUS: Buffer is too small for response processing	RADIUS クライアントは、リソースが許可するより大きい応答を構築しようとしました。
RADIUS	RADIUS: Could not allocate accounting requestInfo	RADIUS クライアントサービスのリソース問題。
RADIUS	RADIUS: Could not allocate requestInfo	RADIUS クライアントサービスのリソース問題。
RADIUS	RADIUS: osapiSocketRecvFrom returned error	RADIUS サーバからデータを読み込み中にエラーが発生しました。
RADIUS	RADIUS: Accounting-Response failed to validate,id = xxx	RADIUS クライアントはサーバから不正なメッセージを受信しました。
RADIUS	RADIUS: User (xxx) needs to respond for challenge	設定ユーザが予期しない Challenge を受信しました。
RADIUS	RADIUS: Could not allocate a buffer for the packet	RADIUS クライアントサービスのリソース問題。
RADIUS	RADIUS: Access-Challenge failed to validate,id =xxx	RADIUS クライアントはサーバから不正なメッセージを受信しました。
RADIUS	RADIUS: Failed to validate Message-Authenticator, id = xxx	RADIUS クライアントはサーバから不正なメッセージを受信しました。
RADIUS	RADIUS: Access-Accpet failed to validate, id=xxx	RADIUS クライアントはサーバから不正なメッセージを受信しました。
RADIUS	RADIUS: Invalid packet length ? xxx	RADIUS クライアントはサーバから不正なメッセージを受信しました。
RADIUS	RADIUS: Response is missing Message-Authenticator, id=xxx	RADIUS クライアントはサーバから不正なメッセージを受信しました。
RADIUS	RADIUS: Server address doesn't match configured server	RADIUS クライアントは未設定のサーバからサーバ応答を受信しました。

TACACS+ ログメッセージ

コンポーネント	メッセージ	原因
TACACS+	TACACS+: authentication error, no server to contact	TACACS+ 要求が必要とされましたが、設定されているサーバはありません。
TACACS+	TACACS+: connection failed to server x.x.x.x	TACACS+ 要求をサーバ x.x.x.x に送信しましたが、応答を受信しませんでした。
TACACS+	TACACS+: no key configured to encrypt packet for server x.x.x.x	指定サーバにはキーが設定されていませんでした。
TACACS+	TACACS+: received invalid packet type from server.	サポートされていないパケットタイプを受信しました。
TACACS+	TACACS+: invalid major version in received packet.	メジャーバージョンの不一致。
TACACS+	TACACS+: invalid minor version in received packet.	マイナーバージョンの不一致。

LLDP Log Message

コンポーネント	メッセージ	原因
LLDP	lldpTask(): invalid message type:xx. xxxxxx:xx	未サポートの LLDP パケットを受信しました。

SNTP Log Message

コンポーネント	メッセージ	原因
SNTP	SNTP: system clock synchronized on %s UTC	SNTP は、サーバを搭載するスイッチへの同期に成功しました。

MANAGEMENT

EmWeb ログメッセージ

コンポーネント	メッセージ	原因
EmWeb	EMWEB (Telnet): Max number of Telnet login sessions exceeded	ユーザは、Telnet セッションの最大数が既にアクティブである時に Telnet で接続を試みました。
EmWeb	EMWEB (SSH): Max number of SSH login sessions exceeded	ユーザは、SSH セッションの最大数が既にアクティブである時に SSH で接続を試みました。
EmWeb	Handle table overflow	利用可能なすべての EmWeb 接続ハンドルが使用されていたため、接続を行うことができませんでした。
EmWeb	ConnectionType EmWeb socket accept() failed: errno	指定接続タイプへのソケットの受け入れエラー。
EmWeb	ewsNetHTTPReceive failure in NetReceiveLoop() - closing connection.	ソケットの受信エラー。
EmWeb	EmWeb: connection allocation failed	新しい接続に対するメモリアロケーションの失敗。
EmWeb	EMWEB TransmitPending : EWOULDBLOCK error sending data	送信時のソケットエラー。
EmWeb	ewaNetHTTPEnd: internal error - handle not in Handle table	EmWeb のハンドルインデックスが不正です。
EmWeb	ewsNetHTTPReceive:recvBufCnt exceeds MAX_QUEUED_RECV_BUFS!	受信バッファの制限に到達しました。間違った要求または DoS 攻撃。
EmWeb	EmWeb accept: XXXX	新しい SSH 接続が失敗したことを受け付けました。XXXX はエラー情報を示しています。

CLI_UTIL ログメッセージ

コンポーネント	メッセージ	原因
CLI_UTIL	Telnet Send Failed errno = 0x%x	Telnet クライアントへの文字列の送信に失敗しました。
CLI_UTIL	osapiFsDir failed	ボリュームディレクトリからディレクトリ情報の取得に失敗しました。

WEB ログメッセージ

コンポーネント	メッセージ	原因
WEB	Max clients exceeded	このメッセージは、許可されているスイッチへの Java クライアントの最大接続数を超えると表示されます。
WEB	Error on send to sockfd XXXX, closing connection	ソケットから Java クライアントへのデータの送信に失敗しました。
WEB	# (XXXX) Form Submission Failed. No Action Taken.	サブミッションの形式が間違っており、いずれのアクションも行われません。XXXX は検討中のファイルを示します。
WEB	ewaFormServe_file_download() - WEB Unknown return code from tftp download result	Web インタフェースから TFTP を使用してダウンロード中に未知のエラーが返されました。
WEB	ewaFormServe_file_upload() - Unknown return code from tftp upload result	Web インタフェースから TFTP を使用してアップロード中に未知のエラーが返されました。
WEB	Web UI Screen with unspecified access attempted to be brought up	ewsAuthRegister() 内のアプリケーションが EmWeb/ サーバに提供したアプリケーション指定の認証ハンドルの取得に失敗しました。指定した Web ページは読み取り専用モードで提供されます。

CLI_WEB_MGR ログメッセージ

コンポーネント	メッセージ	原因
CLI_WEB_MGR	File size is greater than 2K	バナーファイルサイズが 2K バイトを上回っています。
CLI_WEB_MGR	No. of rows greater than allowed maximum of XXXX	列の数が許可されている最大数を超えている場合。

SSHD ログメッセージ

コンポーネント	メッセージ	原因
SSHD	SSHD: Unable to create the global (data) semaphore	グローバルデータ保護のためのセマフォの作成に失敗しました。
SSHD	SSHD: Msg Queue is full, event = XXXX	メッセージキューがいっぱいであるため、SSHD メッセージキューへのメッセージの送信に失敗しました。XXXX は送信されるイベントを示します。
SSHD	SSHD: Unknown UI event in message, event=XXXX	不正なイベントのため、適切な SSHD 機能への UI イベントの送信に失敗しました。XXXX は送信されるイベントを示します。
SSHD	sshdApiCnfgrCommand: Failed calling sshdIssueCmd.	SSHD メッセージキューへのメッセージの送信に失敗しました。

SSLT ログメッセージ

コンポーネント	メッセージ	原因
SSLT	SSLT: Exceeded maximum, ssltConnectionTask	許可された SSLT 接続の最大数を超えました。
SSLT	SSLT: Can't connect to unsecure server at XXXX, result = YYYY, errno = ZZZZ	セキュアでないサーバへの接続のオープンに失敗しました。XXXX はセキュアでないサーバのソケットアドレスを示します。YYYY は接続機能から返された結果で、ZZZZ はエラーコードです。
SSLT	SSLT: Msg Queue is full, event=XXXX	メッセージキューがいっぱいであるため、SSLT メッセージキューへの受信メッセージの送信に失敗しました。XXXX は送信されるイベントを示します。
SSLT	SSLT: Unknown UI event in message, event=XXXX	不正なイベントのため、適切な SSLT 機能への受信 UI イベントの送信に失敗しました。XXXX は送信されるイベントを示します。
SSLT	ssltApiCnfgrCommand: Failed calling ssltIssueCmd.	SSLT メッセージキューへのメッセージの送信に失敗しました。
SSLT	SSLT: Error loading certificate from file XXXX	指定ファイルからの SSL 証明書のローディング中にエラーになりました。XXXX は証明書が読まれるファイルを示します。
SSLT	SSLT: Error loading private key from file	SSL 接続のために秘密鍵をロードしている最中にエラーになりました。
SSLT	SSLT: Error setting cipher list (no valid ciphers)	暗号リストを設定している最中にエラーになりました。
SSLT	SSLT: Could not delete the SSL semaphores	OpenSSL Locking セマフォに関連しているすべてのリソースの削除中に、SSL セマフォの削除に失敗しました。

User_Manager ログメッセージ

コンポーネント	メッセージ	原因
User_Manager	User Login Failed for XXXX	ユーザログインの認証に失敗しました。XXXX は送信されるユーザ名を示します。
User_Manager	Access level for user XXXX could not be determined. Setting to READ_ONLY.	無効なアクセスレベルがユーザに指定されました。アクセスレベルが READ_ONLY に設定されました。XXXX はユーザ名を示しています。
User_Manager	Could not migrate config file XXXX from version YYYY to ZZZZ. Using defaults.	config ファイルのマイグレーションに失敗しました。XXXX は config ファイルの名称です。YYYY は古いバージョン番号で、ZZZZ は新しいバージョン番号です。

SWITCHING

Protected Ports ログメッセージ

コンポーネント	メッセージ	原因
Protected Ports	Protected Port: failed to save configuration	これは、保護ポートの設定を保存できない場合に表示されます。
Protected Ports	protectedPortCnfgrInitPhase1Process: Unable to create r/w lock for protectedPort	これは、protectedPortCfgRWLock のエラーの場合に表示されます。
Protected Ports	protectedPortCnfgrInitPhase2Process: Unable to register for VLAN change callback	これは、VLAN を持つ nimRegisterIntfChange のエラーの場合に表示されます。
Protected Ports	Cannot add intIfNum xxx to group yyy	これは、特定のグループにインタフェースを追加できなかった場合に表示されます。
Protected Ports	unable to set protected port group	これは、dtl コールがドライバレベルでインタフェースマスクの追加に失敗した場合に表示されます。
Protected Ports	Cannot delete intIfNum xxx from group yyy	これは、dtl コールがグループからのインタフェースの削除に失敗した場合に表示されます。
Protected Ports	Cannot update group YYY after deleting interface XXX	このメッセージは、アップデートグループがインタフェース削除に失敗した場合に表示されます。
Protected Ports	Received an interface change callback while not ready to receive it	これは、保護ポートのコンポーネントが準備完了する前に、インタフェースの変更のコールが戻ってきた場合に表示されます。

IP Subnet VLANS ログメッセージ

コンポーネント	メッセージ	原因
IPsubnet vlans	ERROR vlanIpSubnetSubnetValid :Invalid subnet	これは、サブネットとネットマスクの無効なペアが CLI に指定された場合に発生します。
IPsubnet vlans	IP Subnet Vlans: failed to save configuration	これは、サブセット VLAN のコンフィグレーションの保存に失敗した場合に表示されます。
IPsubnet vlans	vlanIpSubnetCnfgrInitPhase1Process: Unable to create r/w lock for vlanIpSubnet	このメッセージは、読取り書込みのロックに失敗した場合に表示されます。
IPsubnet vlans	vlanIpSubnetCnfgrInitPhase2Process: Unable to register for VLAN change callback	これは、コンポーネントが VLAN 変更通知を登録できない場合に表示されます。
IPsubnet vlans	vlanIpSubnetCnfgrFiniPhase1Process: could not delete avl semaphore	これは、このコンポーネントのセマフォの削除に失敗する場合に表示されます。
IPsubnet vlans	vlanIpSubnetDtlVlanCreate: Failed	これは、dtl コールがテーブルへのエントリの追加に失敗した場合に表示されます。
IPsubnet vlans	vlanIpSubnetSubnetDeleteApply: Failed	これは、dtl がテーブルからエントリの削除に失敗した場合に表示されます。
IPsubnet vlans	vlanIpSubnetVlanChangeCallback: Failed to add an Entry	これは、dtl が vlan の追加通知イベントのエントリの追加に失敗する場合に表示されます。
IPsubnet vlans	vlanIpSubnetVlanChangeCallback: Failed to delete an Entry	これは、vlan 削除通知イベントのエントリの削除に失敗する場合に表示されます。

MAC-based VLANs ログメッセージ

コンポーネント	メッセージ	原因
Mac based VLANS	MAC VLANs: Failed to save configuration	これは、Mac VLAN のコンフィグレーションの保存に失敗した場合に表示されます。
Mac based VLANS	vlanMacCnfgrInitPhase1Process: Unable to create r/w lock for vlanMac	このメッセージは、読取り書込みのロックに失敗した場合に表示されます。
Mac based VLANS	Unable to register for VLAN change callback	これは、コンポーネントが VLAN 変更通知を登録できない場合に表示されます。
Mac based VLANS	vlanMacCnfgrFiniPhase1Process: could not delete avl semaphore	これは、このコンポーネントのセマフォの削除に失敗する場合に表示されます。
Mac based VLANS	vlanMacAddApply: Failed to add an entry	これは、dtl コールがテーブルへのエントリの追加に失敗した場合に表示されます。
Mac based VLANS	vlanMacDeleteApply: Unable to delete an Entry	これは、dtl がテーブルからエントリの削除に失敗した場合に表示されます。
Mac based VLANS	vlanMacVlanChangeCallback: Failed to add an entry	これは、dtl が vlan の追加通知イベントのエントリの追加に失敗する場合に表示されます。
Mac based VLANS	vlanMacVlanChangeCallback: Failed to delete an entry	これは、vlan 削除通知イベントのエントリの削除に失敗する場合に表示されます。

802.1x ログメッセージ

コンポーネント	メッセージ	原因
802.1X	function: Failed calling dot1xIssueCmd	802.1X メッセージキューがいっぱいです。
802.1X	function: EAP message not received from server	RADIUS サーバは要求された EAP メッセージを送信しませんでした。
802.1X	function: Out of System buffers	802.1 X は、内部バッファの不足のためにメッセージの処理 / 送信はできませんでした。
802.1X	function: could not set state to <authorized/unauthorized>, intf xxx	DTL コールは、ポートの認証ステートの設定に失敗しました。
802.1X	dot1xApplyConfigData: Unable to <enable/disable> dot1x in driver	DTL コールは、802.1X の有効か / 無効化に失敗しました。
802.1X	dot1xSendRespToServer: dot1xRadiusAccessRequestSend failed	RADIUS サーバへのメッセージの送信に失敗しました。
802.1X	dot1xRadiusAcceptProcess: error calling radiusAccountingStart, ifIndex=xxx	RADIUS サーバへのアカウンティング開始の送信に失敗しました。
802.1X	function: failed sending terminate cause, intf xxx	RADIUS サーバへのアカウンティング終了の送信に失敗しました。

IGMP Snooping ログメッセージ

コンポーネント	メッセージ	原因
IGMP Snooping	function: osapiMessageSend failed	IGMP Snooping メッセージキューがいっぱいです。
IGMP Snooping	Failed to set global igmp snooping mode to xxx	メッセージキューがいっぱいのためにグローバルな IGMP Snooping モードの設定に失敗しました。
IGMP Snooping	Failed to set igmp snooping mode xxx for interface yyy	メッセージキューがいっぱいのためにインタフェースの IGMP Snooping モードの設定に失敗しました。
IGMP Snooping	Failed to set igmp mrouter mode xxx for interface yyy	メッセージキューがいっぱいのためにマルチキャストルータモードの設定に失敗しました。
IGMP Snooping	Failed to set igmp snooping mode xxx for vlan yyy	メッセージキューがいっぱいのために VLAN の IGMP Snooping モードの設定に失敗しました。
IGMP Snooping	Failed to set igmp mrouter mode %d for interface xxx on Vlan yyy	メッセージキューがいっぱいのために VLAN のマルチキャストルータモードの設定に失敗しました。
IGMP Snooping	snoopCnfgrInitPhase1Process: Error allocating small buffers	小さい IGMP パケット用にバッファを割り当てることができませんでした。
IGMP Snooping	snoopCnfgrInitPhase1Process: Error allocating large buffers	大きい IGMP パケット用にバッファを割り当てることができませんでした。

GARP/GVRP/GMRP ログメッセージ

コンポーネント	メッセージ	原因
GARP/GVRP/GMRP	garpSpanState, garpIfStateChange, GarpIssueCmd, garpDot1sChangeCallBack, garpApiCnfgrCommand, garpLeaveAllTimerCallback, garpTimerCallback: QUEUE SEND FAILURE:	garpQueue はいっぱいです。内部インタフェース番号、メッセージタイプなどのメッセージコンテンツの詳細をログに出力します。
GARP/GVRP/GMRP	GarpSendPDU: QUEUE SEND FAILURE	garpPduQueue はいっぱいです。GPDU、内部インタフェース番号、VLAN ID、バッファハンドルなどの詳細をログに出力します。
GARP/GVRP/GMRP	garpMapIntfIsConfigurable, gmrpMapIntfIsConfigurable: Error accessing GARP/GMRP config data for interface %d in garpMapIntfIsConfigurable.	初期設定はこのインタフェースには存在しません。新しいインタフェースが作成される、事前の設定がない場合が一般的な例です。
GARP/GVRP/GMRP	garpTraceMsgQueueUsage: garpQueue usage has exceeded fifty/eighty/ninety percent	メッセージキューの構築をトレースします。 GARP におけるロードを決定する際に役立ちます。
GARP/GVRP/GMRP	gid_destroy_port: Error Removing port %d registration for vlan-mac %d - %02X:%02X:%02X:%02X:%02X:%02X	gmd（gmrp データベース）と MFDB 間の不一致。
GARP/GVRP/GMRP	gmd_create_entry: GMRP failure adding MFDB entry: vlan %d and address %s	MFDB テーブルがいっぱいです。

802.3ad ログメッセージ

コンポーネント	メッセージ	原因
802.3ad	dot3adReceiveMachine: received default event %x	受信した LAG PDU と RX ステートのマシンは、この LAGPDU を無視しています。
802.3ad	dot3adNimEventCompletionCallback, dot3adNimEventCreateCompletionCallback: DOT3AD: notification failed for event(%d), intf(%d), reason(%d)	NIM に送信されたイベントは、完全に終了しませんでした。

FDB Log Message

コンポーネント	メッセージ	原因
FDB	fdbSetAddressAgingTimeOut: Failure setting fid %d address aging timeout to %d	エージングタイムをハードウェアに設定することができませんでした。

Double VLAN Tag Log Message

コンポーネント	メッセージ	原因
Double Vlan Tag	dvlantagIntfIsConfigurable: Error accessing dvlantag config data for interface %d	初期設定はこのインタフェースには存在しません。 新しいインタフェースが作成される、事前の設定がない場合が一般的な例です。

MFDB Log Message

コンポーネント	メッセージ	原因
MFDB	mfdbTreeEntryUpdate: entry does not exist	存在しないエントリをアップデートしようとしています。

802.1Q ログメッセージ

コンポーネント	メッセージ	原因
802.1Q	dot1qIssueCmd: Unable to send message %d to dot1qMsgQueue for vlan %d - %d msgs in queue	dot1qMsgQueue はいっぱいです。
802.1Q	dot1qVlanCreateProcess: Attempt to create a vlan with an invalid vlan id %d ; VLAN %d not in range,	これは、予約された vlan ID（つまり、4094 - X）に適応します。
802.1Q	dot1qMapIntfIsConfigurable: Error accessing DOT1Q config data for interface %d in dot1qMapIntfIsConfigurable.	初期設定はこのインタフェースには存在しません。新しいインタフェースが作成される、事前の設定がない場合が一般的な例です。
802.1Q	dot1qVlanDeleteProcess: Deleting the default VLAN	一般的に Vlan のクリア、および config のクリアの間に遭遇します。
802.1Q	dot1qVlanMemberSetModify, dot1qVlanTaggedMemberSetModify: Dynamic entry %d can only be modified after it is converted to static	この vlan が GVRP 経由で学習され、我々が変更できない場合、それは、マネジメントを通して設定されたメンバです。

802.1S ログメッセージ

コンポーネント	メッセージ	原因
802.1S	dot1sIssueCmd: Dot1s Msg Queue is full!!!!Event: %u, on interface: %u, for instance: %u	メッセージキューがいっぱいです。
802.1S	dot1sStateMachineRxBpdu(): Rcvd BPDU Discarded	ポートが有効でない、または現在同じインタフェースで別の BPDU の処理を終了していないというし現在の条件では、この BPDU の処理は許可されません。
802.1S	dot1sBpduTransmit(): could not get a buffer	システムバッファが不足しています。

Port Mac Locking Log Message

コンポーネント	メッセージ	原因
Port Mac Locking	pmlMapIntfIsConfigurable: Error accessing PML config data for interface %d in pmlMapIntfIsConfigurable.	初期設定はこのインタフェースには存在しません。 新しいインタフェースが作成される、事前の設定がない場合が一般的な例です。

Protocol-based VLANs ログメッセージ

コンポーネント	メッセージ	原因
Protocol Based VLANs	pbVlanCnfgrInitPhase2Process: Unable to register NIM callback	nimRegisterIntfChange が Link-state 変更のために pbVlan の登録に失敗する場合に表示されます。
Protocol Based VLANs	pbVlanCnfgrInitPhase2Process: Unable to register pbVlan callback with vlans	vlanRegisterForChange が vlan 変更のために pbVlan の登録に失敗する場合に表示されます。
Protocol Based VLANs	pbVlanCnfgrInitPhase2Process: Unable to register pbVlan callback with nvStore	nvStoreRegister がコンフィグレーションの保存のために save および restore 機能の実行に失敗する場合に表示されます。

QOS

ACL ログメッセージ

コンポーネント	メッセージ	原因
ACL	Total number of ACL rules (x) exceeds max (y) on intf i.	インタフェースに適用されるすべての ACL の組合せはプラットフォームがサポートする以上のルールを必要とする結果となりました。
ACL	ACL name, rule x: This rule is not being logged	ACL 設定がプラットフォームがサポートする以上のログ取得ルールの要求をもたらしました。指定したルールは、通常、ログ出力アクションを除いて機能しています。
ACL	aclLogTask: error logging ACL rule trap for correlator number	システムはログ出力属性を含むこの ACL ルールに SNMP トラップを送信することができませんでした。
ACL	IP ACL number: Forced truncation of one or more rules during config migration	保存された設定を処理している間、システムは最新版でサポートされるより多くのルールを持つ ACL に遭遇しました。 コードを、以前のバージョンよりも ACL あたりのルールが少ないバージョンにアップデートする場合に、これは起こるかもしれません。

CoS Log Message

コンポーネント	メッセージ	原因
COS	cosCnfgrInitPhase3Process: Unable to apply saved config -- using factory defaults	COS コンポーネントが、保存したコンフィグレーションを適用できなかったため、工場出荷時設定に初期化しました。

DiffServ ログメッセージ

コンポーネント	メッセージ	原因
DiffServ	diffserv.c 165: diffServRestore Failed to reset DiffServ. Recommend resetting device	動作中のコンフィグレーションのクリア中に、現在の設定の削除でエラーが起こりました。これはシステムに矛盾した状態を引き起こすため、リセットすることが推奨されます。
DiffServ	Policy invalid for service intf: "policy name,intIfNum x, direction y	DiffServ ポリシー定義は指定されるインタフェースの能力と互換性がありません。 コンフィグレーションの制限に関する情報がないかどうかプラットフォームのリリースノートをチェックしてください。

ROUTING

DHCP Relay ログメッセージ

コンポーネント	メッセージ	原因
DHCP relay	REQUEST hops field more than config value	TDHCP リレーエージェントは、HOPS フィールドが許可されている最大値より大きい DHCP 要求を処理しました。 リレーエージェントは 4 以上のホップカウントを持つメッセージを転送しません。
DHCP relay	Request's seconds field less than the config value	DHCP リレーエージェントは SECS フィールドが許可されている待ち時間の最小値よりも大きい DHCP 要求を処理しました。
DHCP relay	processDhcpPacket: invalid DHCP packet type: %u\n	DHCP リレーエージェントは不正な DHCP パケットを処理しました。そのようなパケットはリレーエージェントによって破棄されます。

Routing Table Manager ログメッセージ

コンポーネント	メッセージ	原因
Routing Table Manager	RTO is full. Routing table contains 8000 best routes, 8000 total routes.	また、「RTO」と呼ばれるルーティングテーブルマネージャはハードウェア容量に基づいてベストルートの制限数を保存します。ルーティングテーブルがいっぱいである時、RTO はこのアラートをログに出力します。総ルートのカウントには、ハードウェアにインストールされない代替ルートも含まれます。
Routing Table Manager	RTO no longer full. Bad adds: 10. Routing table contains 7999 best routes, 7999 total routes.	ベストルートの数が全容量を下回っている時、RTO はこの通知をログに出力します。不正な追加数が、RTO がいっぱいで失敗したルート追加数を表示しますが、フル状態のルーティングテーブルが、このカウントを増加させる唯一の理由です。

VRRP ログメッセージ

コンポーネント	メッセージ	原因
VRRP	Changing priority to 255 for virtual router with VRID 1 on interface 0/1	ルータが仮想ルータ ID として使用されるアドレスに設定される時、ルータの優先度は、アドレスの所有者が確実に VRRP のマスタになるように自動的に最大値に設定されます。
VRRP	Changing priority to 100 for virtual router with VRID 1 on interface 0/1	ルータがアドレス所有者でなくなった場合には、ソフトウェアはルータの優先度を初期値に戻します。
VRRP	vrrpPacketValidate: Invalid TTL	VRRP は、IP ヘッダの time to live（TTL）が 255 ではなかった入力メッセージを無視しました。

ARP ログメッセージ

コンポーネント	メッセージ	原因
ARP	ARP received mapping for IP address xxx to MAC address yyy. This IP address may be configured on two stations.	同じ IP アドレスを持つ別のステーションから異なる MAC アドレスを持つ ARP 応答を受信する場合。これは不正なコンフィグレーションのケースの可能性があります。

RIP ログメッセージ

コンポーネント	メッセージ	原因
RIP	RIP : discard response from xxx via unexpected interface	RIP の応答を入力インタフェースのサブセットに一致しない送信元アドレスと共に受信した場合。

TECHNOLOGIES

Driver エラーメッセージ

コンポーネント	メッセージ	原因
Driver	Invalid USP unit = x, slot = x, port =x	ポートは受信中に正しく変換されませんでした。
Driver	In hapiBroadSystemMacAddress call to 'bcm_l2_addr_add' - FAILED : x	L2 アドレスの MAC テーブルへの追加に失敗しました。 これは、ハッシュコリジョンの発生、またはテーブルフルの場合に発生します。
Driver	Failed installing mirror action - rest of the policy applied successfully	以前に設定したプローブポートはポリシーに使用されていません。リリースノートでは、1 つのプローブポートしか設定できないことを記載しています。
Driver	Policy x does not contain rule x	ルールは、この指定ポリシーのルールカウントにおける矛盾のためにポリシーに追加されませんでした。 さらに、既存のルールを変更しているが、既存のルールがポリシーにない場合にメッセージは表示されます。
Driver	ERROR: policy x, tmpPolicy x, size x, data x x x x x x x x	可能な重複ハッシュのためポリシーをインストールする問題。
Driver	ACL x not found in internal table	存在しない ACL を削除しようとしています。
Driver	ACL internal table overflow	フルテーブルに ACL を追加しようとしています。
Driver	In hapiBroadQosCosQueueConfig, Failed to configure minimum bandwidth. Available bandwidth x	能力を超えて帯域幅を設定しようとしています。
Driver	USL: failed to put sync response on queue	sync 要求への応答がキューに入りませんでした。 これは、前の sync 要求をタイムアウト後に受信したことを表示しています。
Driver	USL: failed to sync ipmc table on unit=x	転送は失敗したか、またはメッセージが破棄されました。
Driver	usl_task_ipmc_msg_send(): failed to send with x	転送は失敗したか、またはメッセージが破棄されました。
Driver	USL: No available entries in the STG table	Spanning Tree Group テーブルは USL でいっぱいです。
Driver	USL: failed to sync stg table on unit=x	転送失敗またはリモートユニットの API 問題のために、ユニット x を同期させることができませんでした。同期のリトライが行われます。
Driver	USL: A Trunk doesn't exist in USL	存在しないトランクを変更しようとしています。
Driver	USL: A Trunk being created by bcmx already existed in USL	アプリケーション、ハードウェア、および sync レイヤ間であり得る同期の問題。
Driver	USL: A Trunk being destroyed doesn't exist in USL	アプリケーション、ハードウェア、および sync レイヤ間であり得る同期の問題。
Driver	USL: A Trunk being set doesn't exist in USL	アプリケーション、ハードウェア、および sync レイヤ間であり得る同期の問題。
Driver	USL: failed to sync trunk table on unit=x	転送失敗またはリモートユニットの API 問題のために、ユニット x を同期させることができませんでした。同期のリトライが行われます。
Driver	USL: Mcast entry not found on a join	アプリケーション、ハードウェア、および sync レイヤ間であり得る同期の問題。
Driver	USL: Mcast entry not found on a leave	アプリケーション、ハードウェア、および sync レイヤ間であり得る同期の問題。
Driver	USL: failed to sync dvlan data on unit=x	転送失敗またはリモートユニットの API 問題のために、ユニット x を同期させることができませんでした。同期のリトライが行われます。
Driver	USL: failed to sync policy table on unit=x	転送失敗またはリモートユニットの API 問題のために、ユニット x を同期させることができませんでした。同期のリトライが行われます。
Driver	USL: failed to sync VLAN table on unit=x	転送失敗またはリモートユニットの API 問題のために、ユニット x を同期させることができませんでした。同期のリトライが行われます。
Driver	Invalid LAG id x	BCM ドライバと HAPI 間であり得る同期の問題。
Driver	Invalid uport calculated from the BCM uport bcmx_l2_addr->lport = x	BCM ドライバから計算された不正な Uport です。
Driver	Invalid USP calculated from the BCM uport\nbcmx_l2_addr->lport = x	USP は、学習した BCM ドライバのイベントから計算することはできません。
Driver	Unable to insert route R/P	プレフィックス「P」を持つルート「R」をハードウェアルートテーブルに挿入できませんでした。リトライが行われます。

コンポーネント	メッセージ	原因
Driver	Unable to Insert host H	ハードウェアホストテーブルにホスト H を挿入できませんでした。リトライが行われます。
Driver	USL: failed to sync L3 Intf table on unit=x	転送失敗またはリモートユニットの API 問題のために、ユニット x を同期させることができませんでした。同期のリトライが行われます。
Driver	USL: failed to sync L3 Host table on unit=x	転送失敗またはリモートユニットの API 問題のために、ユニット x を同期させることができませんでした。同期のリトライが行われます。
Driver	USL: failed to sync L3 Route table on unit=x	転送失敗またはリモートユニットの API 問題のために、ユニット x を同期させることができませんでした。同期のリトライが行われます。
Driver	USL: failed to sync initiator table on unit=x	転送失敗またはリモートユニットの API 問題のために、ユニット x を同期させることができませんでした。同期のリトライが行われます。
Driver	USL: failed to sync terminator table on unit=x	転送失敗またはリモートユニットの API 問題のために、ユニット x を同期させることができませんでした。同期のリトライが行われます。
Driver	USL: failed to sync ip-multicast table on unit=x	転送失敗またはリモートユニットの API 問題のために、ユニット x を同期させることができませんでした。同期のリトライが行われます。

O/S SUPPORT

OSAPI VxWorks ログメッセージ

コンポーネント	メッセージ	原因
OSAPI VxWorks	ftruncate failed ? File resides on a read-only file system.	ftruncate は、書込みの後にファイルシステムに正しくファイルサイズを設定するためにコールされます。 ファイルシステムは読み書き可能であるため、この msg はファイルシステムが壊れる可能性があることを示します。
OSAPI VxWorks	ftruncate failed ? File is open for reading only.	ftruncate は、書込みの後にファイルシステムに正しくファイルサイズを設定するためにコールされます。 ファイルは読み書き可能であるため、この msg はファイルシステムが壊れる可能性があることを示します。
OSAPI VxWorks	ftruncate failed ? File descriptor refers to a file on which this operation is impossible.	ftruncate は、書込みの後にファイルシステムに正しくファイルサイズを設定するためにコールされます。 この msg はファイルシステムが壊れる可能性があることを示します。
OSAPI VxWorks	ftruncate failed ? Returned an unknown code in errno.	ftruncate は、書込みの後にファイルシステムに正しくファイルサイズを設定するためにコールされます。 この msg はファイルシステムが壊れる可能性があることを示します。
OSAPI VxWorks	ping: bad host!	ping に要求されたアドレスをインターネットアドレスに変換することはできません。
OSAPI VxWorks	osapiTaskDelete: Failed for (XX) error YYY	削除要求が ISR からコールされている、タスクが既に削除されている、またはタスク ID が無効であるために要求されたタスクを削除することはできません。
OSAPI VxWorks	osapiCleanupIf: NetIPGet	ルートテーブルからインタフェースを削除するコール中に、スタックから ipv4 インタフェースアドレスを取得する試みに失敗しました。
OSAPI VxWorks	osapiCleanupIf: NetMaskGet	ルートテーブルからインタフェースを削除するコール中に、スタックから ipv4 インタフェースマスクを取得する試みに失敗しました。
OSAPI VxWorks	osapiCleanupIf: NetIpDel	ルートテーブルからインタフェースを削除するコール中に、スタックからプライマリ ipv4 アドレスを取得する試みに失敗しました。
OSAPI VxWorks	osapiSemaTake failed	ISR からコールが行われている、またはセマフォ ID が無効であるため要求されたセマフォを取得することができません。

付録 A 設定例

この付録では D-Link 統合アクセスシステムのソフトウェアで利用可能な選択機能を設定する方法例を説明します。各例には、Web インタフェース、CLI、および SNMP を使用することで機能を設定する方法に関する手順があります。この付録では以下の手順を行う方法を説明しています。

- VLAN の設定
- VLAN のルーティング設定
- 複数のスパニングツリープロトコルの設定
- 802.1X ネットワークアクセスコントロールの設定
- 仮想アクセスポイントの設定
- VoIP のクラス別サービスの設定

VLAN の設定

以下の図では、２つの VLAN へのトラフィックを処理する 4 つのポートを持つスイッチを示しています。ポート 0/2 は両方の VLAN のトラフィックを処理します。一方、ポート 0/1 は VLAN2 だけのメンバであり、ポート 0/3 と 0/4 は VLAN3 だけのメンバです。

以下の例は、VLAN を作成する方法を示しており、ポートを VLAN に割り当てて、デフォルト VLAN として VLAN をポートに割り当てます。

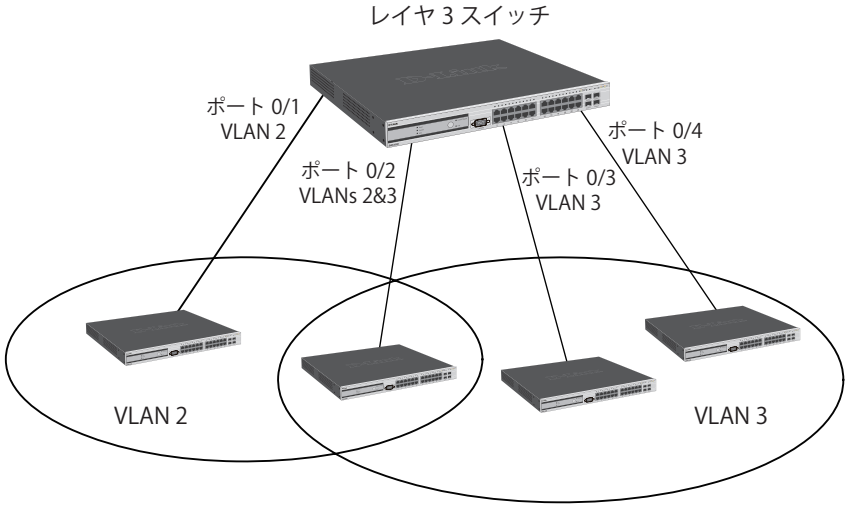
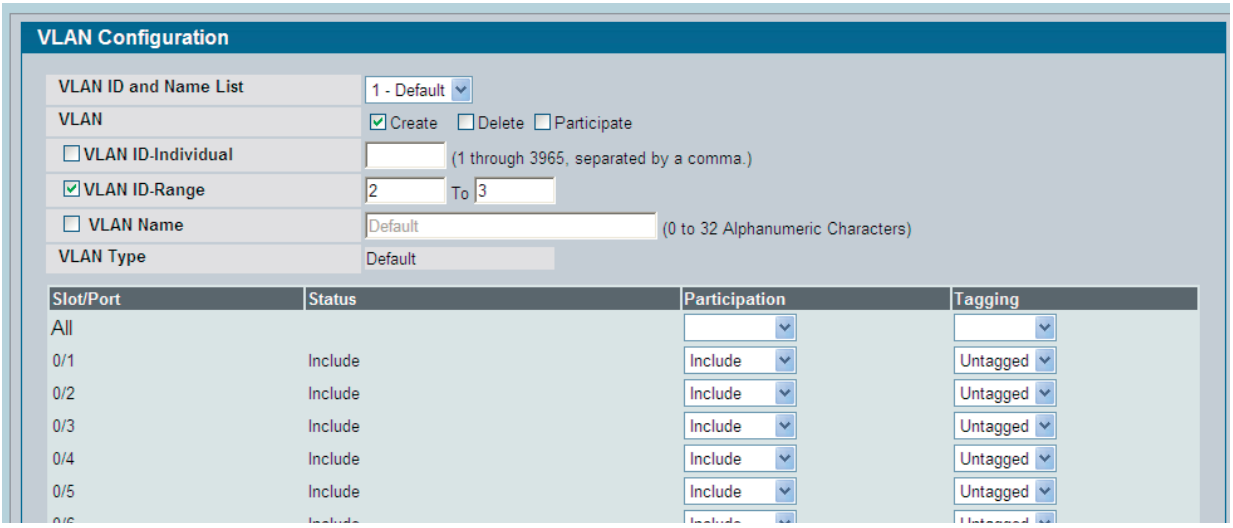


図 A-1　VLAN を使用したネットワーク例

1. **LAN タブ > L2 Features > VLAN > VLAN Configuration** の順にメニューをクリックします。
2. 「VLAN」で「Create」オプションを選択します。
3. 「VLAN ID-Range」オプションを選択し、範囲に 2-3 を入力します。

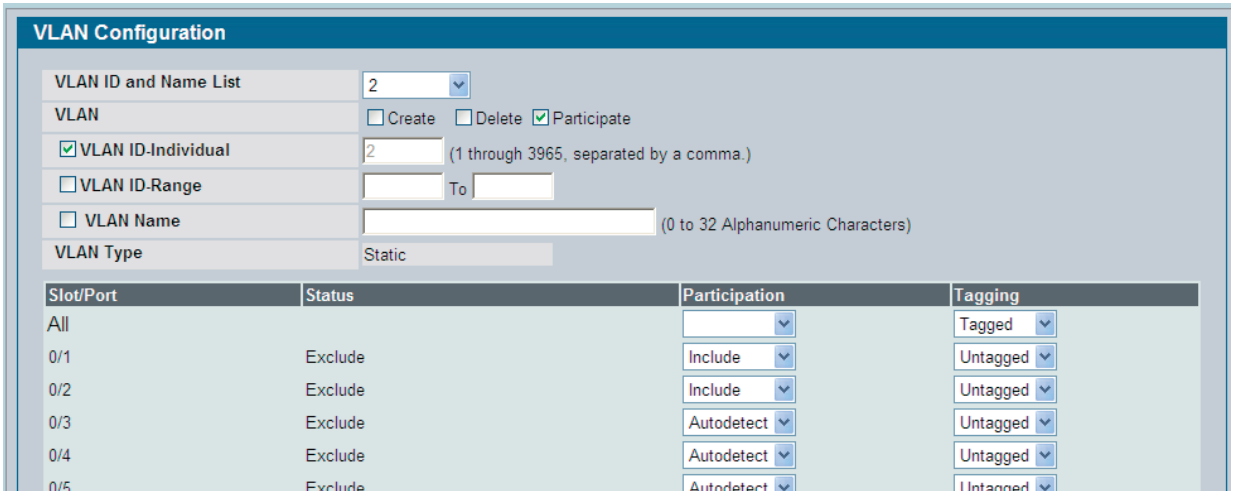


4. 「Submit」ボタンをクリックします。
5. 「VLAN ID」および「Name List」からから「VLAN2」を選択します。

6. 「VLAN」で「Participate」オプションを選択します。

7. ポート 0/1 と 0/2 に対して、「Participation」メニューから「Include」を選択して、これらのポートを VLAN2 のメンバに指定します。

8. 「Tagging」メニューから、最初の列（All）で「Tagged」を選択して、フレームが VLAN2 のメンバであるポートから、常にタグ付けをされて送信されることを指定します。

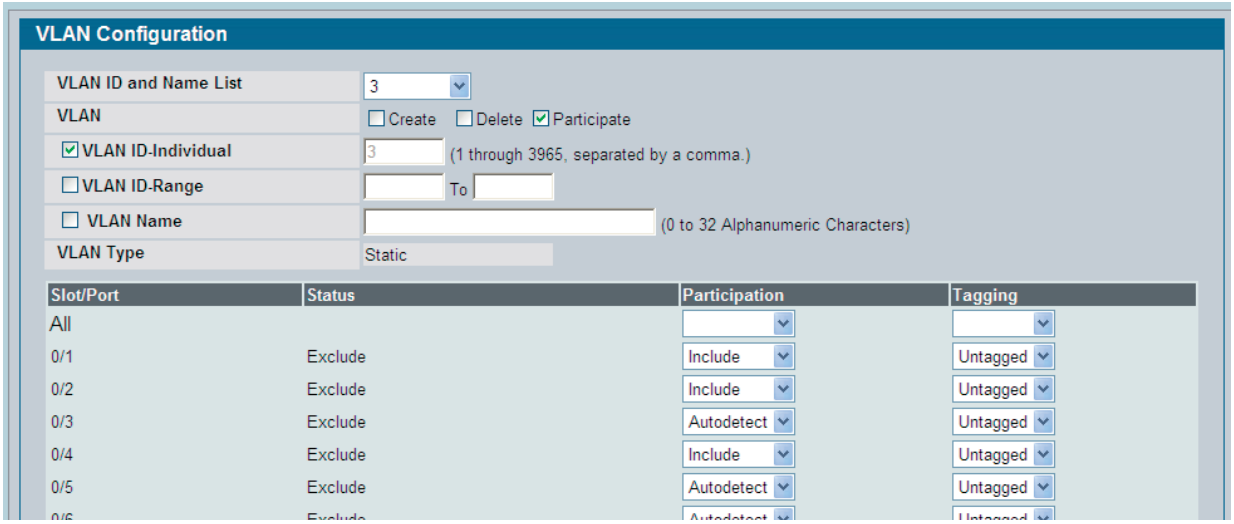


9. 「Submit」ボタンをクリックします。

10. 「VLAN ID」および「Name List」からから「VLAN3」を選択します。

11. 「VLAN」で「Participate」オプションを選択します。

12. ポート 0/1、0/2、および 0/4 に対して、「Participation」メニューから「Include」を選択して、これらのポートを VLAN3 のメンバに指定します。

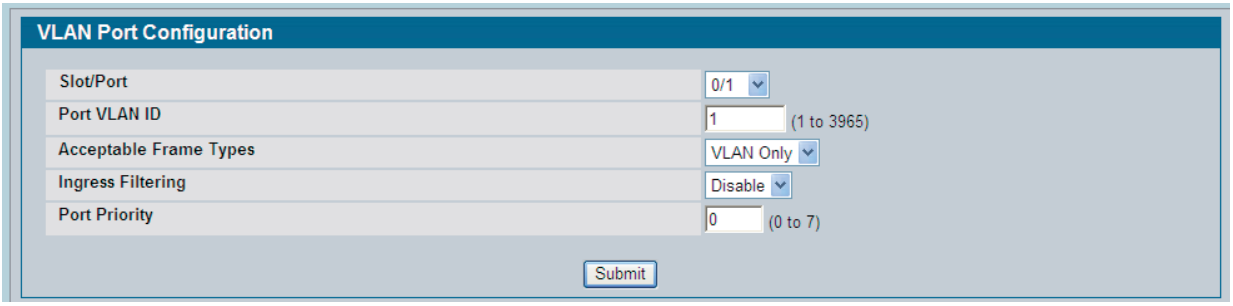


13. 「Submit」ボタンをクリックします。

14. **LAN タブ > L2 Features > VLAN > Port Configuration** の順にメニューをクリックします。

15. 「Slot/Port」メニューから「0/1」を選択します。

16. 「Acceptable Frame Types」から「VLAN Only」を選択し、タグなしフレームを受信時に拒否するように指定します。

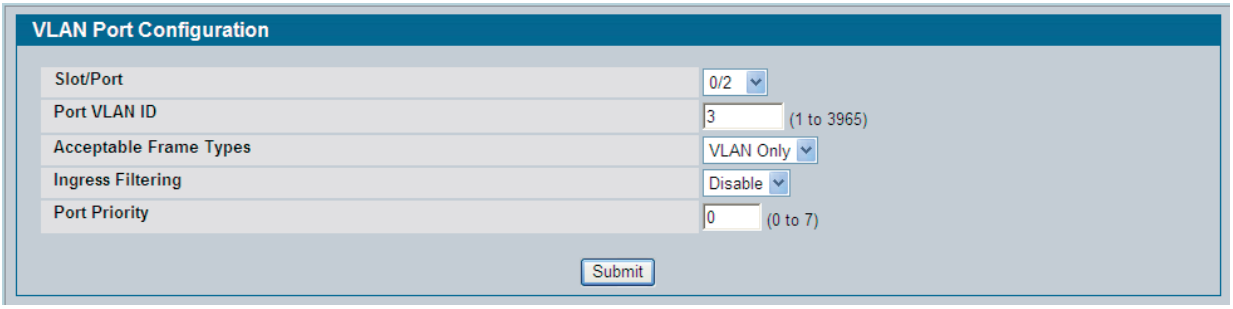


17. 「Submit」ボタンをクリックします。

18. 「Slot/Port」メニューから「0/2」を選択します。

19. 「Port VLAN ID」に 3 を入力し、ポートへのデフォルト VLAN として VLAN3 を割り当てます。

20. 「Acceptable Frame Types」から「VLAN Only」を選択し、タグなしフレームを受信時に拒否するように指定します。



21. 「Submit」ボタンをクリックします。

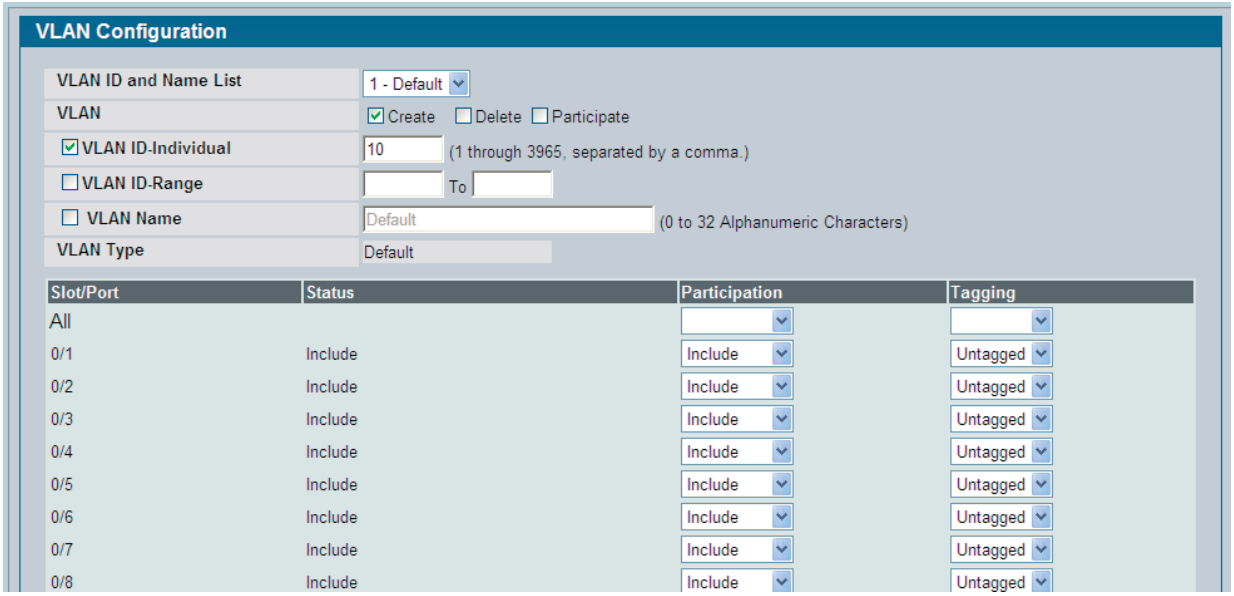
複数のスパニングツリープロトコルの設定

この例は、スイッチとすべてのポートに IEEE 802.1 Multiple Spanning Tree（MST）プロトコルを有効にして、ブリッジの優先度を設定する方法を示しています。

複数のスイッチが同じ MSTP リージョンに属するように、すべてのスイッチの Force プロトコルバージョン設定が IEEE 802.1s であることを確認します。また、そのリージョンのすべてのスイッチにおけるコンフィグレーション名、ダイジェストキー、およびリビジョンレベルが同じであることを確認します。

ダイジェストキーは異なるインスタンスに関連する VLAN に基づいて生成されます。ダイジェストキーが確実に同じであるために、VLAN とインスタンスのマッピングがリージョン内の各スイッチで同じである必要があります。例えば、VLAN 10 が 1 つのスイッチにインスタンス 10 を割り当てる場合、他のスイッチにも VLAN 10 とインスタンス 10 を割り当てる必要があります。

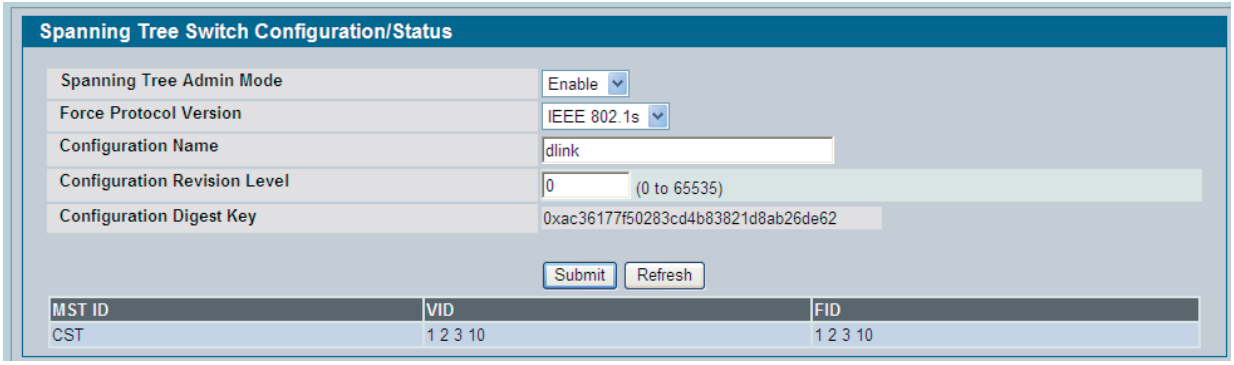
1. VLAN 10 と 20 作成します。
- **a.** **LAN タブ > L2 Features > VLAN > VLAN Configuration** の順にメニューをクリックします。
- **b.** 「VLAN」で「Create」オプションを選択します。
- **c.** 「VLAN ID-Individual 」オプションを選択し、10 を入力します。



- **d.** 「Submit」ボタンをクリックします。
- **e.** 同様に、VLAN20 を追加します。

2. スイッチにおいて「MSTP」を有効にして設定名を変更します。

3. 設定名を変更すると、同じエリアの使用を希望するブリッジすべてを接続することができます。
- **a.** **LAN タブ > L2 Features > Spanning Tree > Switch Configuration** の順にメニューをクリックします。
- **b.** 「Spanning Tree Admin Mode」メニューから「Enable」を選択します。
- **c.** 「Configuration Name」に「dlink」を入力します。



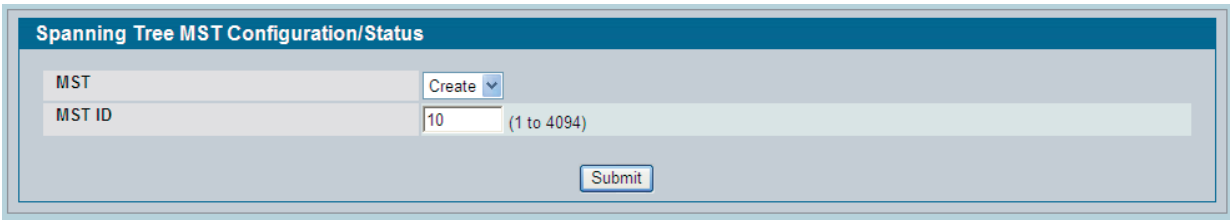
- **d.** 「Submit」ボタンをクリックします。

4. 2 つの MST インスタンスを作成します。

a. **LAN タブ > L2 Features > Spanning Tree > MST Configuration** 順にメニューをクリックします。

b. 「MST」から「Create」を選択します。

c. 「MST ID」に 10 を入力します。



d. 「Submit」ボタンをクリックします。

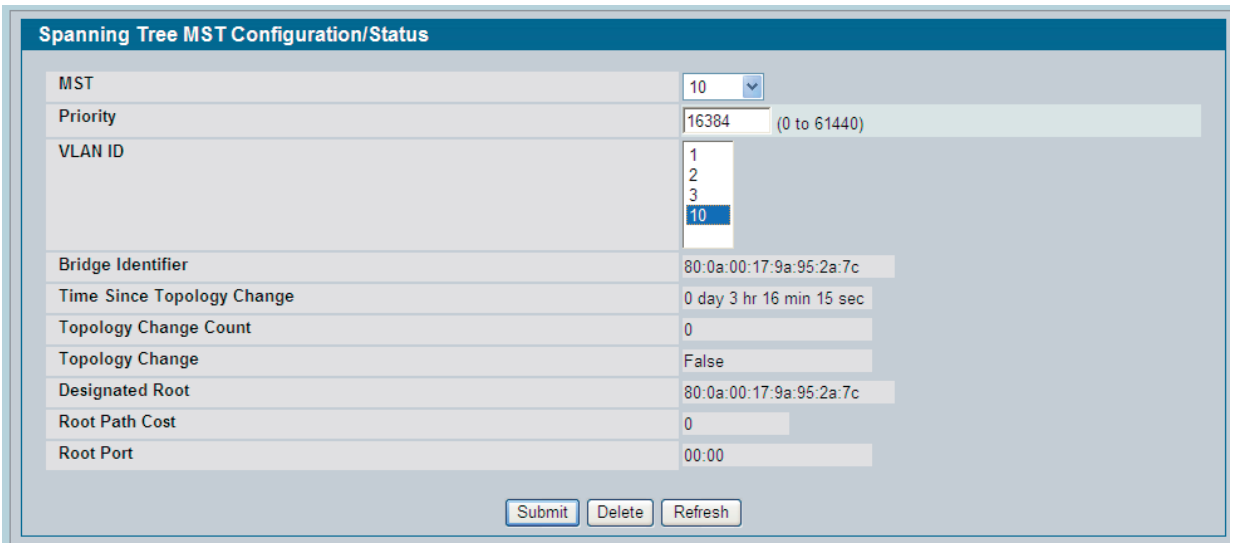
e. 同様の手順を繰り返して、ID 20 を持つ MST インスタンスを作成します。

5. MST ID 10 を VLAN 10 に関連付け、ブリッジ優先度に 16384 の割り当てます。

a. MST メニューから MST 10 を選択します。

b. 「Priority」に 16384 を入力します。

c. VLAN 10 をクリックして、「VLAN ID」から選択します。



d. 「Submit」ボタンをクリックします。

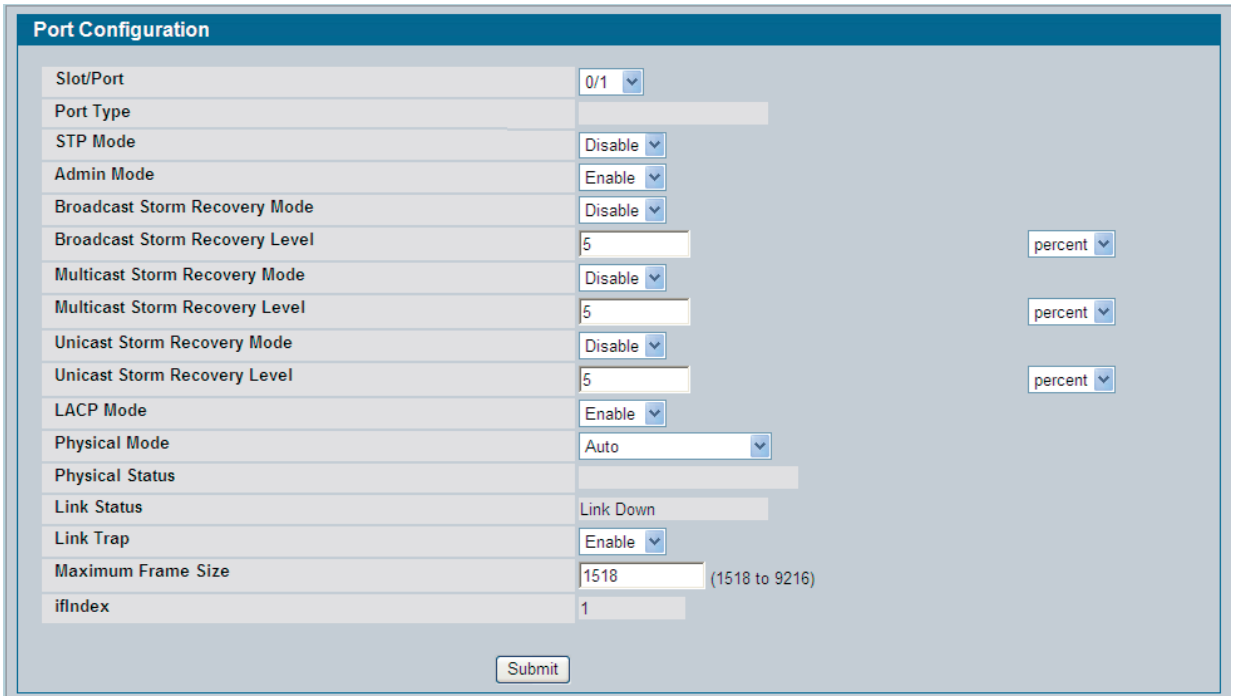
6. 同様の手順で、MST インスタンス 20 を VLAN 20 に関連付け、ブリッジ優先度に 61440 の割り当てます。
MST 20 により低い優先度を使用することによって、MST 10 はルートブリッジになります。

7. ポート 0/1 で STP を有効にします。

a. **LAN タブ > Administration > Port Configuration > Port Configuration** の順にメニューをクリックします。

b. 「Slot/Port」メニューからポート「0/1」を選択します。

c. 「STP Mode」メニューから「Enable」を選択します。



d. 「Submit」ボタンをクリックします。

8. 同様の手順でポート 0/2 で STP を有効にします。

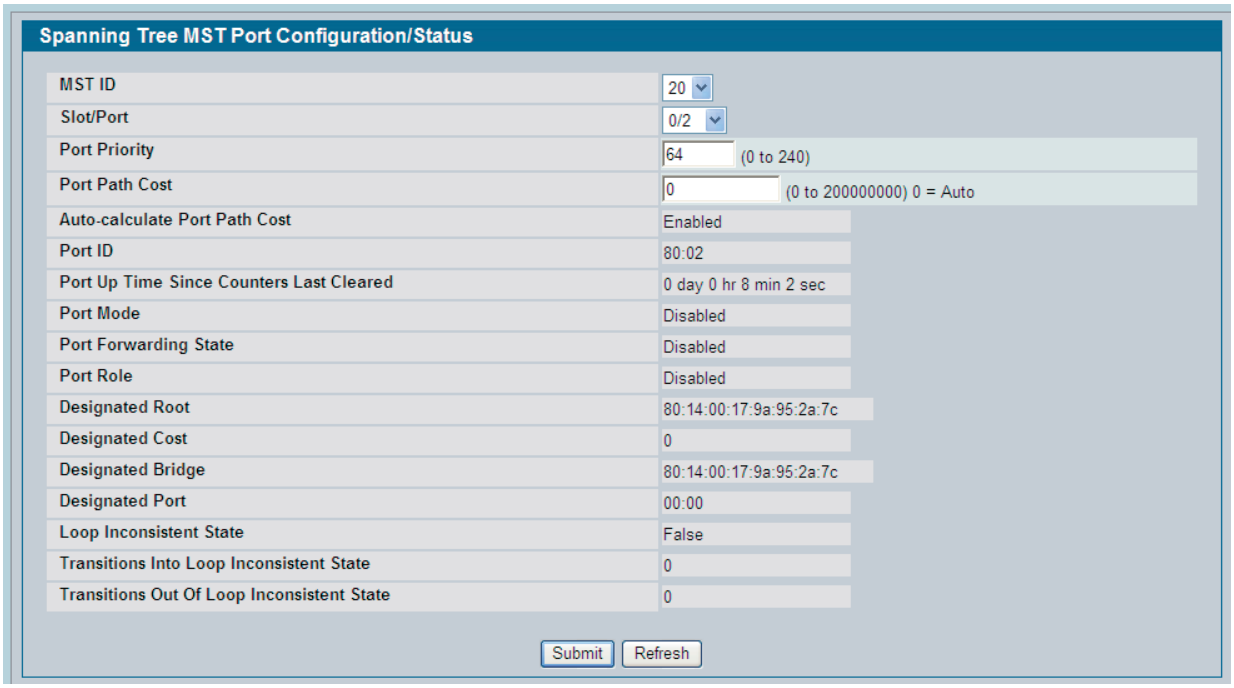
9. ポート 0/2 を non-root ブリッジである MST 20 に対するルートポートにします。

a. **LAN タブ > L2 Features > Spanning Tree > MST Port Configuration** の順にメニューをクリックします。

b. 「MST ID」メニューから「20」を選択します。

c. 「Slot/Port」メニューから「0/2」を選択します。

d. 「Port Priority」メニューに 64 を入力します。



e. 「Submit」ボタンをクリックします。

VLAN のルーティング設定

ここでは、VLAN ルーティングをサポートするために、D-Link 統合アクセスシステムのソフトウェアを設定する例を説明します。
VLAN ルータポートの設定は物理ポートの設定と同様です。主な違いは、VLAN 作成後にルータ設定コマンドに使用できるように VLAN のインタフェース ID を決定する「show ip vlan」コマンドを使用しなければならないという点です。

以下の図では、ポートルーティングに設定したレイヤ 3 スイッチを示しています。 2 つの VLAN が接続し、一方の VLAN には 2 ポート参加し、他方には 1 ポート参加しています。図で示された VLAN ルーティングを提供するために D-Link 統合アクセスシステムのソフトウェアを設定するために使用するコマンドを示しています。

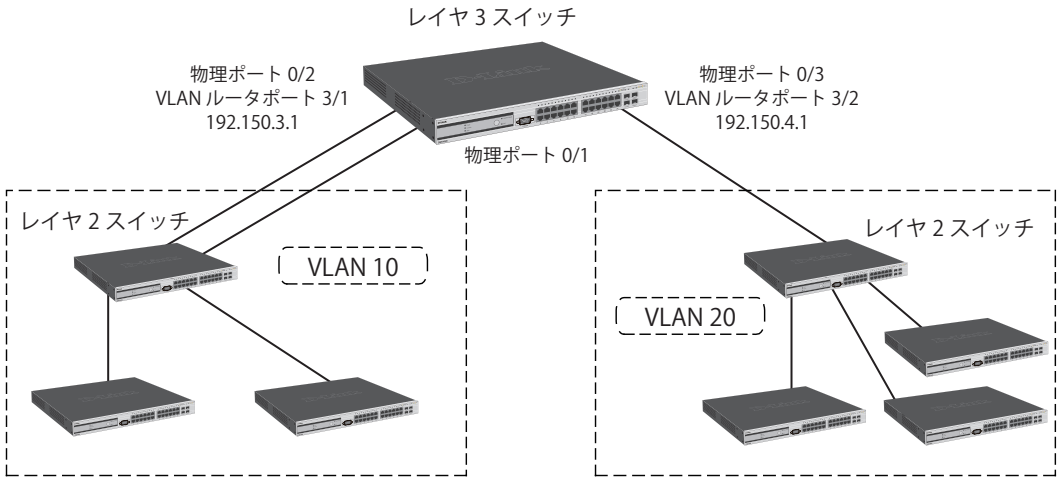


図 A-2　VLAN ルーティングを使用したネットワーク例

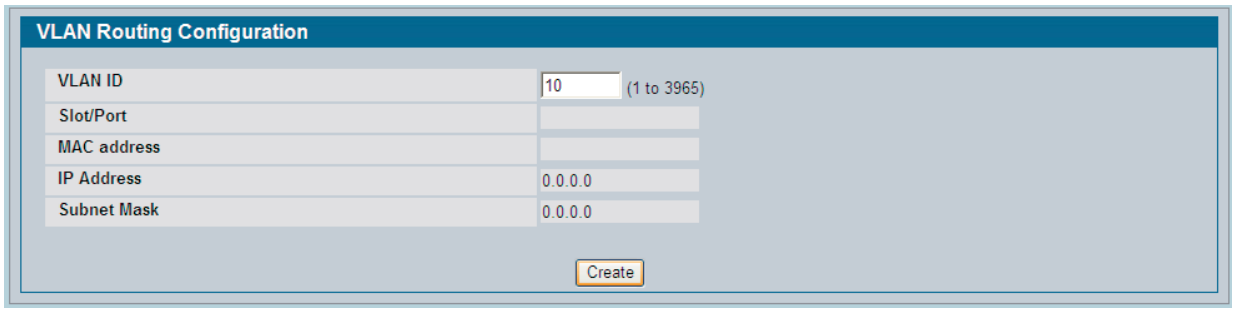
以下の画面で、Web インタフェースを使用した設定を行います。

1. **LAN タブ > L2 Features > VLAN > VLAN Configuration** の順にメニューをクリックします。
   - VLAN 10 と 20 を作成します。
   - VLAN 10 のメンバとしてインタフェース 0/1 と 0/2 を指定し、全てのインタフェースのタグ付けとして「Tagged」を設定します。
   - VLAN 20 のメンバとしてインタフェース 0/3 を指定し、全てのインタフェースのタグ付けとして「Tagged」を設定します。

2. **LAN タブ > L2 Features > VLAN > Port Configuration** の順にメニューをクリックし、インタフェース 0/1 および 0/2 のポートの VLAN ID には 10 を、インタフェース 0/3 には 20 を設定します。

3. **LAN タブ > L3 Features > VLAN Routing Configuration** の順にメニューをクリックします。

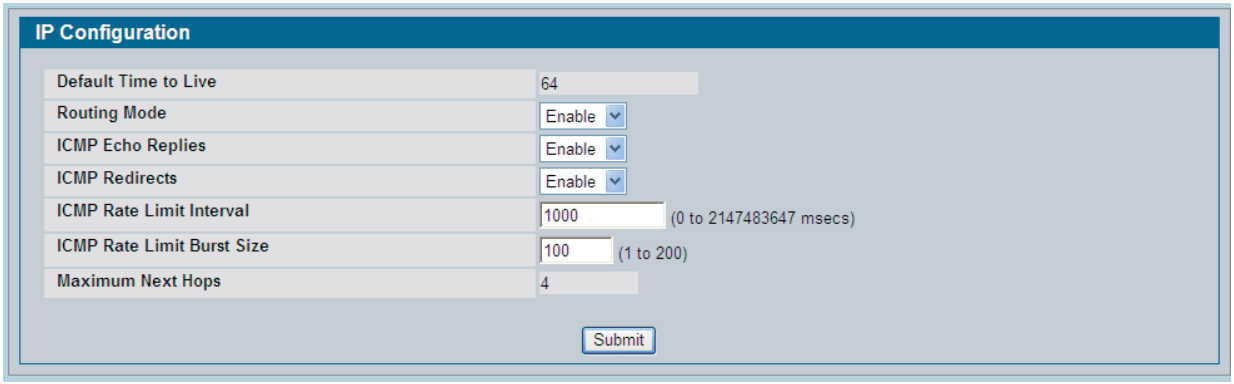
4. 「VLAN ID」に 10 を入力し、「Create」ボタンをクリックします。



5. 「VLAN ID」に 20 を入力し、「Create」ボタンをクリックします。

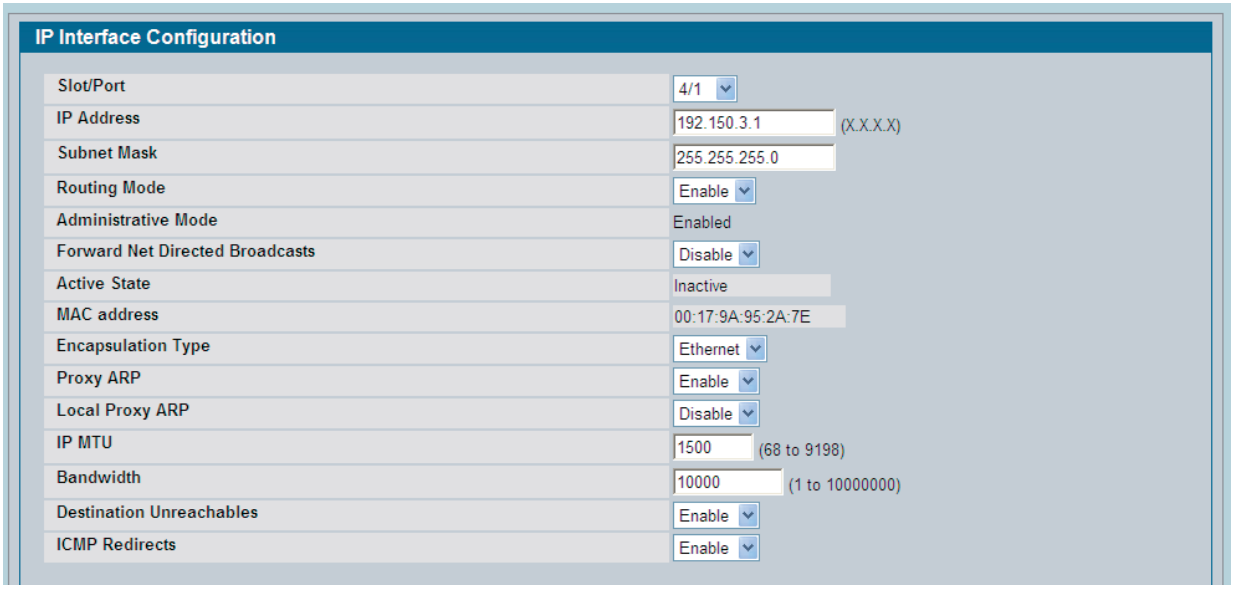
6. **LAN タブ > Monitoring > VLAN Summary > VLAN Port Status** の順にメニューをクリックし、VLAN インタフェースに割り当てられている論理インタフェース ID を参照します。
   ID4/1 は VLAN 10 に割り当てられ、ID4/2 は VLAN 20 に割り当てられます。

7. スイッチにルーティングを有効にするためには、**LAN タブ > L3 Features > IP > Configuration** の順にメニューをクリックし、「Routing Mode」から「Enable」を選択して「Submit」ボタンをクリックします。



8. **LAN タブ > L3 Features > IP > Interface Configuration** の順にメニューをクリックし、仮想ルータポートに IP アドレスとサブネットマスクを設定します。

a. 「Unit/Slot/Port」メニューから「4/1」を選択します。
b. 「IP Address」に「192.150.3.1」を入力します。
c. 「Subnet Mask」に「255.255.255.0」を入力します。
d. 「Submit」ボタンをクリックします。



「Slot/Port」からインタフェース「4/2」を選択し、IP アドレス「192.150.4.1」とサブネットマスク「255.255.255.0」を使用して設定します。

802.1X ネットワークアクセスコントロールの設定

この例では認証に使用される RADIUS サーバと「10.10.10.10」にサーバアカウンティングを作成します。共有秘密鍵は「secret」に設定されます。以下の手順で、認証方法として RADIUS を使用する「radiusList」という新しい認証リストを作成します。この認証リストは 802.1X default login に関連付けます。IEEE 802.1X ポートベースアクセスコントロールをシステムに有効とし、インタフェース 0/1 を、これが RADIUS サーバと保護されたネットワークリソースが位置している場所であるため force-authorized モードになるように設定します。

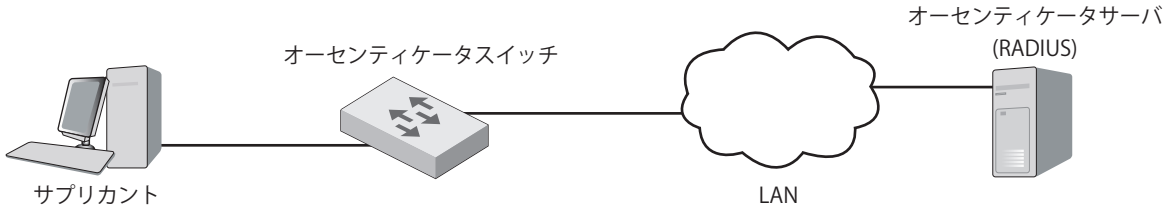
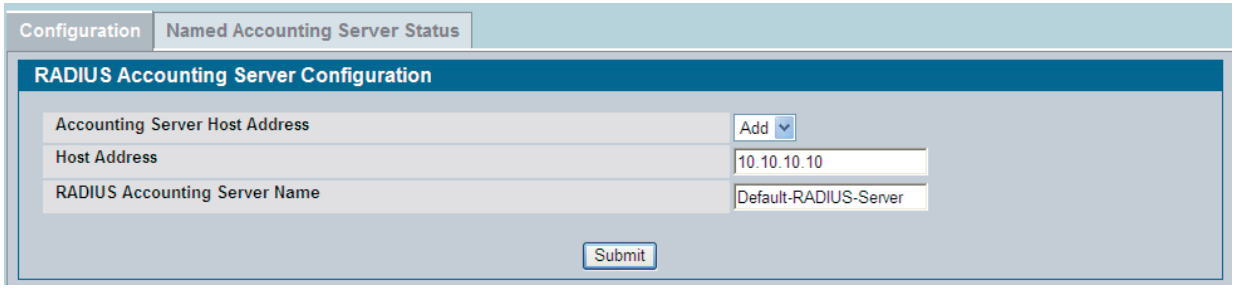


図 A-3　802.1X ネットワークアクセスコントロールを使用したスイッチ設定

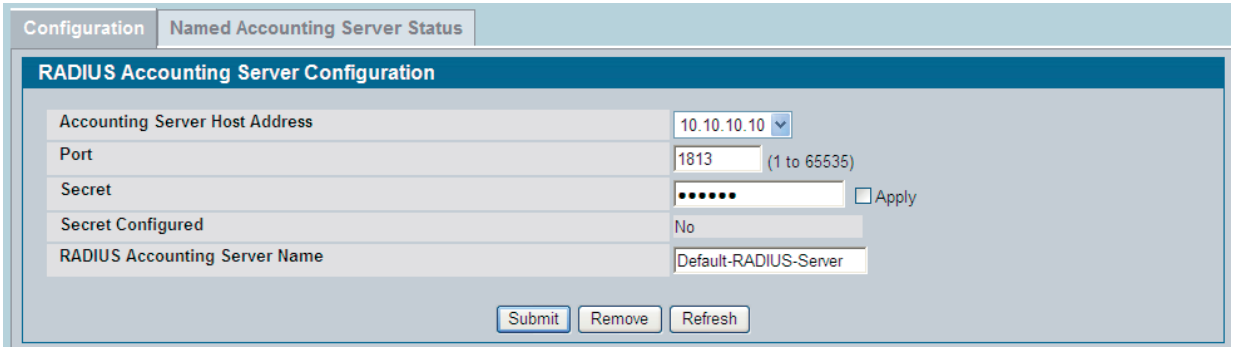
ユーザまたはサプリカントが、インタフェース 0/1 以外のいずれかのインタフェースにあるスイッチを経由する通信を試みる場合、システムはログイン証明をサプリカントに要求します。システムは、提供された情報を暗号化して、RADIUS サーバに転送します。RADIUS サーバがアクセスを許可すると、システムはインタフェースの 802.1X ポートステータスを認証済みに設定し、サプリカントはネットワークリソースにアクセスできるようになります。

1. **LAN タブ > Security > RADIUS > RADIUS Authentication Server Configuration** の順にメニューをクリックし、スイッチに RADIUS サーバ情報を設定します。
2. 「RADIUS Server Host Address」から「Add」を選択します。
3. 「Host Address」に「10.10.10.10」を入力します。
4. 「Submit」ボタンをクリックします。画面は更新され、追加の項目が表示されます。
5. 「Secret」に「secret」を入力し、「Apply」オプションを選択します。
6. 「Primary Server」から「Yes」を設定します。



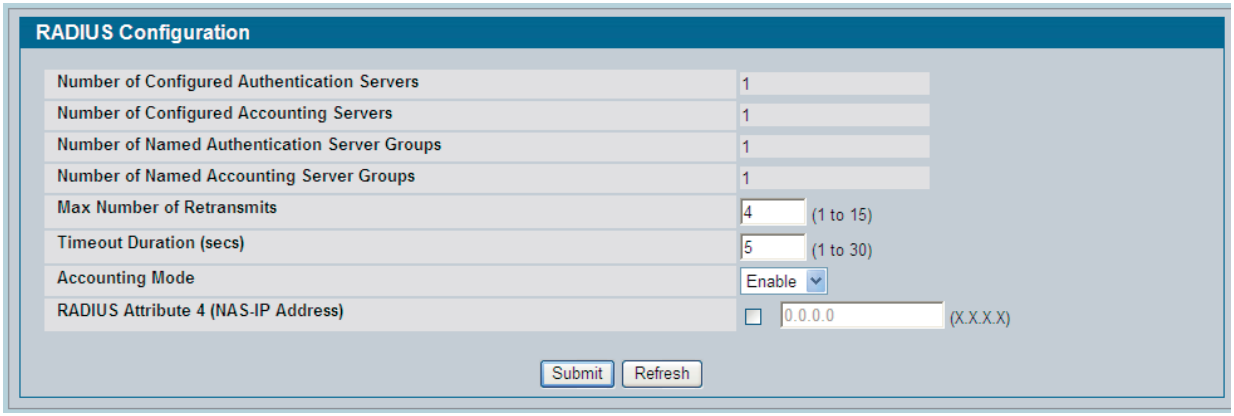
7. 「Submit」ボタンをクリックし、変更をスイッチに適用します。

8. RADIUS アカウンティングサーバ情報を設定します。
   a. **LAN タブ > Security > RADIUS > Accounting Server** の順にメニューをクリックします。
   b. 「Accounting Server Host Address」から「Add」を選択します。
   c. 「Accounting Server Host Address」に「10.10.10.10」を入力します。
   d. 「Submit」ボタンをクリックします。

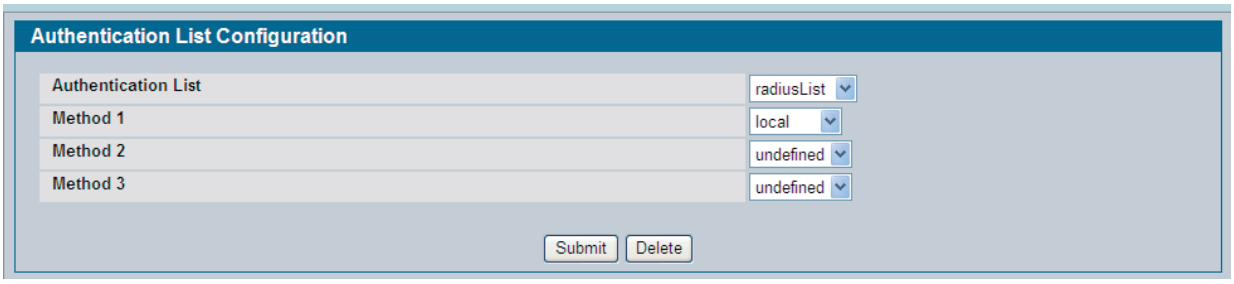


   e. 「Secret」に「secret」を入力し、「Apply」オプションを選択します。
   f. 「Submit」ボタンをクリックします。

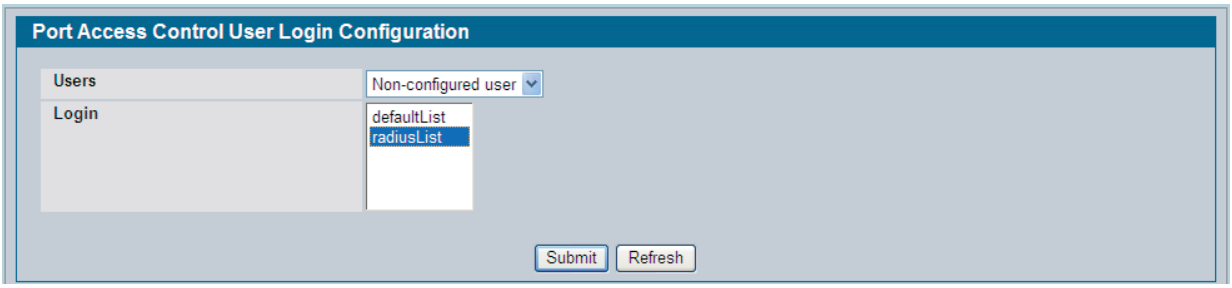
9. RADIUS アカウンティングを有効にするためには、**LAN タブ > Security > RADIUS > RADIUS Configuration** の順にメニューをクリックし、「Accounting Mode」メニューから「Enable」を選択し「Submit」ボタンをクリックします。



10. 認証リストを作成します。
   a. **LAN タブ > Administration > Authentication List Configuration** の順にメニューをクリックします。
   b. 「Authentication List Name」に「radiusList」を入力します。
   c. 「Submit」ボタンをクリックします。
   d. 「Method 1」メニューから「radius」を選択し「Submit」ボタンをクリックします。

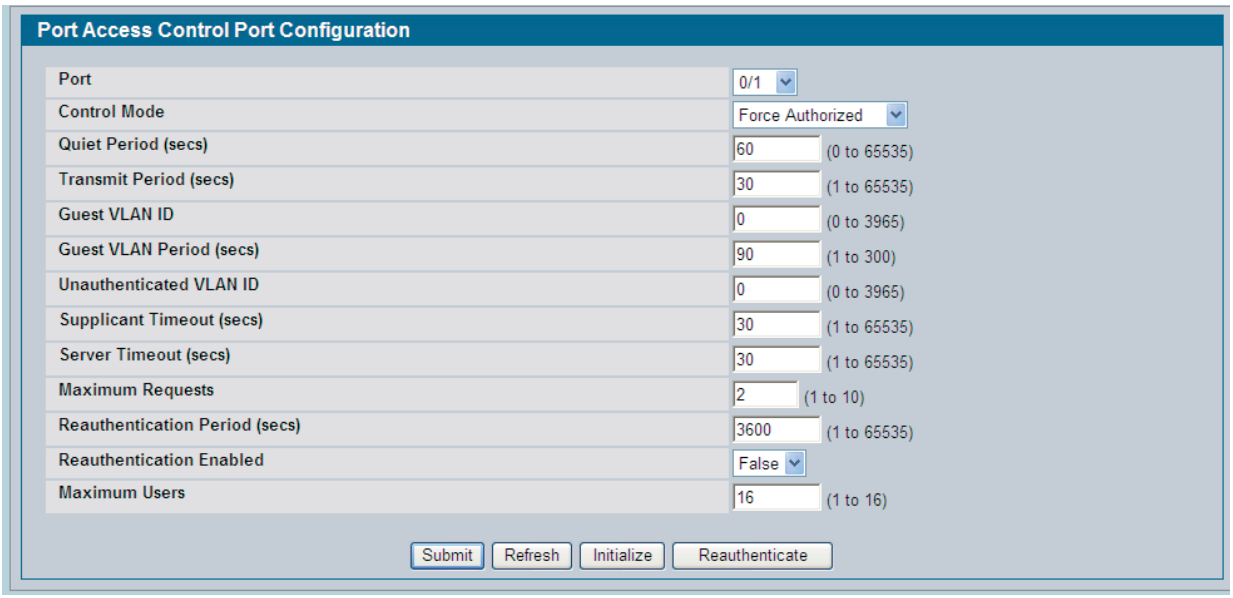


11. システムに設定されていないユーザ用のデフォルトログインリストとして「radiusList」を設定するためには、**LAN タブ > Security > Port Access Control > User Login Configuration** の順にメニューをクリックし、「Login」から「radiusList」を選択して「Submit」ボタンをクリックします。



12. **LAN タブ > Security > Port Access Control > Configuration** の順にメニューをクリックし、「Administrative Mode」メニューから「Enable」を選択し「Submit」ボタンをクリックします。

13. ポート 1/0/1 に 802.1X モードを設定するためには、**LAN タブ > Security > Port Access Control > Port Configuration** の順にメニューをクリックし、「Control Mode」メニューから「Force Authorized」を選択し「Submit」ボタンをクリックします。



仮想アクセスポイントの設定

以下の例は、スイッチ上でデフォルトの仮想アクセスポイント（VAP）プロファイルを設定する方法を示しています。スイッチは、ネットワークで検出したアクセスポイントを認証した後に、デフォルトプロファイルをアクセスポイントに割り当てます。スイッチとアクセスポイントが相互に検出するためには、UWS で WLAN スイッチ機能を有効にし、アクセスポイントでは Managed Mode モードを有効にする必要があります。

この例のデフォルトプロファイルには、以下の設定で示すように 3 つの有効な VAP があります。

Network (SSID)	VLAN	Security	Redirect	Client QoS
Visitor	10	None	http://www.dlink.com.tw	http://www.dlink.com.tw Bandwidth Restrictions
Corporate	20	WPA Personal	None	None
Voice	30	WPA Enterprise	None	DiffServ Policy Up

音声ネットワークは、システムに設定したデフォルト RADIUS サーバを使用してクライアントを認証します。また、「L2 Distributed Tunneling Mode」を有効にします。

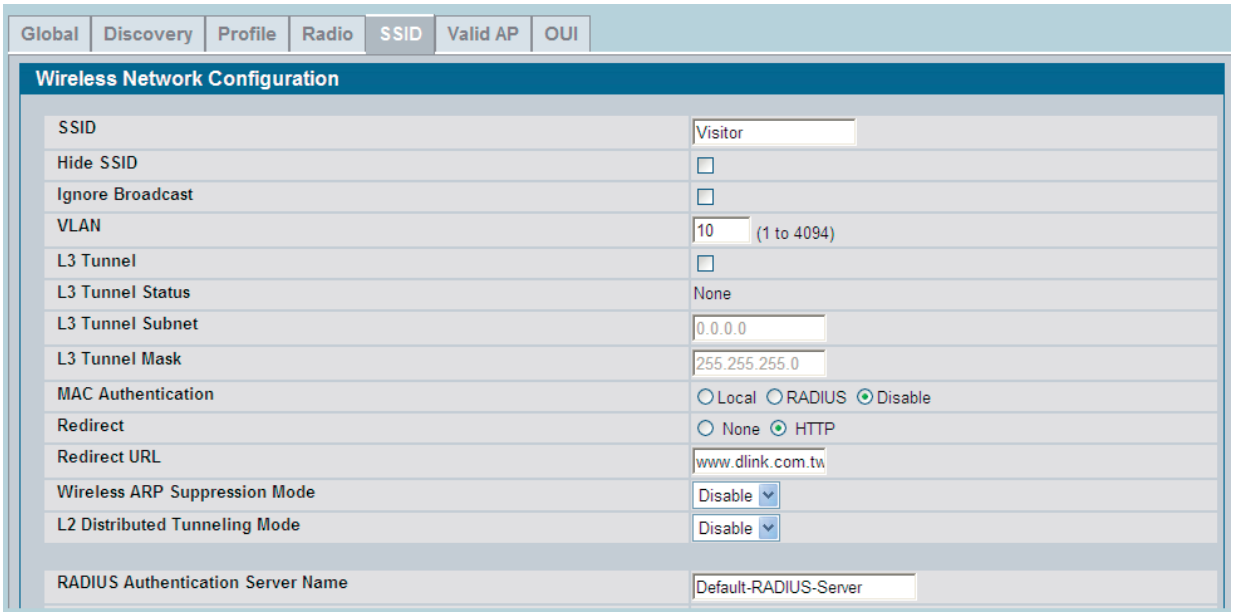
注意 L2 Distributed トンネリングを有効にした場合、以下のネットワーク問題点に注意します。

- アクセスポイントが異なるサブネットに位置している場合、VLAN が 1 つのブリッジセグメントを形成しないようにルータでクライアントの VLAN を分ける必要があります。
- アクセスポイントの IP アドレスが同じサブネットにある場合、無線クライアントが使用するすべての VLAN が、同じブリッジセグメントに位置する必要があります。

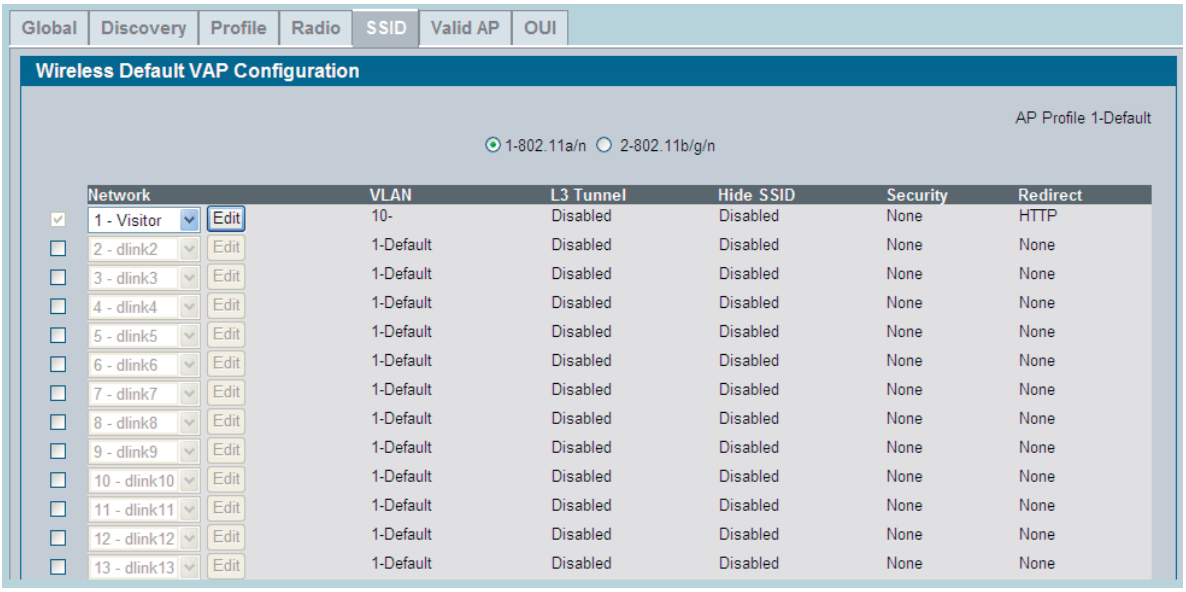
音声ネットワークは、音声トラフィックを処理するために DiffServ ポリシーを使用します。ポリシーは、音声ネットワークに関連付けるために既に設定されている必要があります。**LAN タブ > QoS > Differentiated Services** フォルダで利用可能な画面を使用してポリシーを設定します。DiffServ ポリシーの設定に関する情報は、「VoIP のクラス別サービスの設定」（410 ページ）を参照してください。

1. **WLAN タブ > Administration > Basic Setup** 画面にアクセスし、「SSID」タブをクリックします。
   初期値では、Network 1 は有効で、SSID として「Guest Network」を使用します。

2. 最初の VAP を設定します。
   a. Network 1 の「Edit」ボタンをクリックし、そのネットワーク用の「Wireless Network Configuration」画面にアクセスします。
   b. 既存の SSID を削除し、「SSID」に「Visitor」を入力します。
   c. 「VLAN」に「10」を入力します。
   d. 「Redirect」で「HTTP」オプションを選択します。
   e. 「Redirect URL」で「www.dlink.com.tw」を入力します。



f. 「Bandwidth Limit Down」に「3000000」を入力し、VAP のダウンロード速度を 3Mbps に制限します。
g. 「Bandwidth Limit Up」に「1000000」を入力し、VAP のアップロード速度を 1Mbps に制限します。
h. 「Submit」ボタンをクリックしてスイッチに設定を適用します。



3. 「SSID」タブをクリックし、「Wireless Default VAP Configuration」画面に戻ります。

4. 「Network 2」隣のチェックボックスを選択し、「Edit」ボタンをクリックします。

5. 2 つ目の VAP を設定します。
a. 既存の SSID を削除し、「SSID」に「Corporate」を入力します。
b. 「VLAN」に「20」を入力します。
c. セキュリティオプションから、WPA を選択します。追加のセキュリティフィールドが表示されます。
d. WPA2 クライアントだけが VAP に接続できるように、WPA オプションをクリアします。
e. CCMP（AES）オプションを選択します。
f. WPA キーを入力します。
g. 「Submit」ボタンをクリックします。

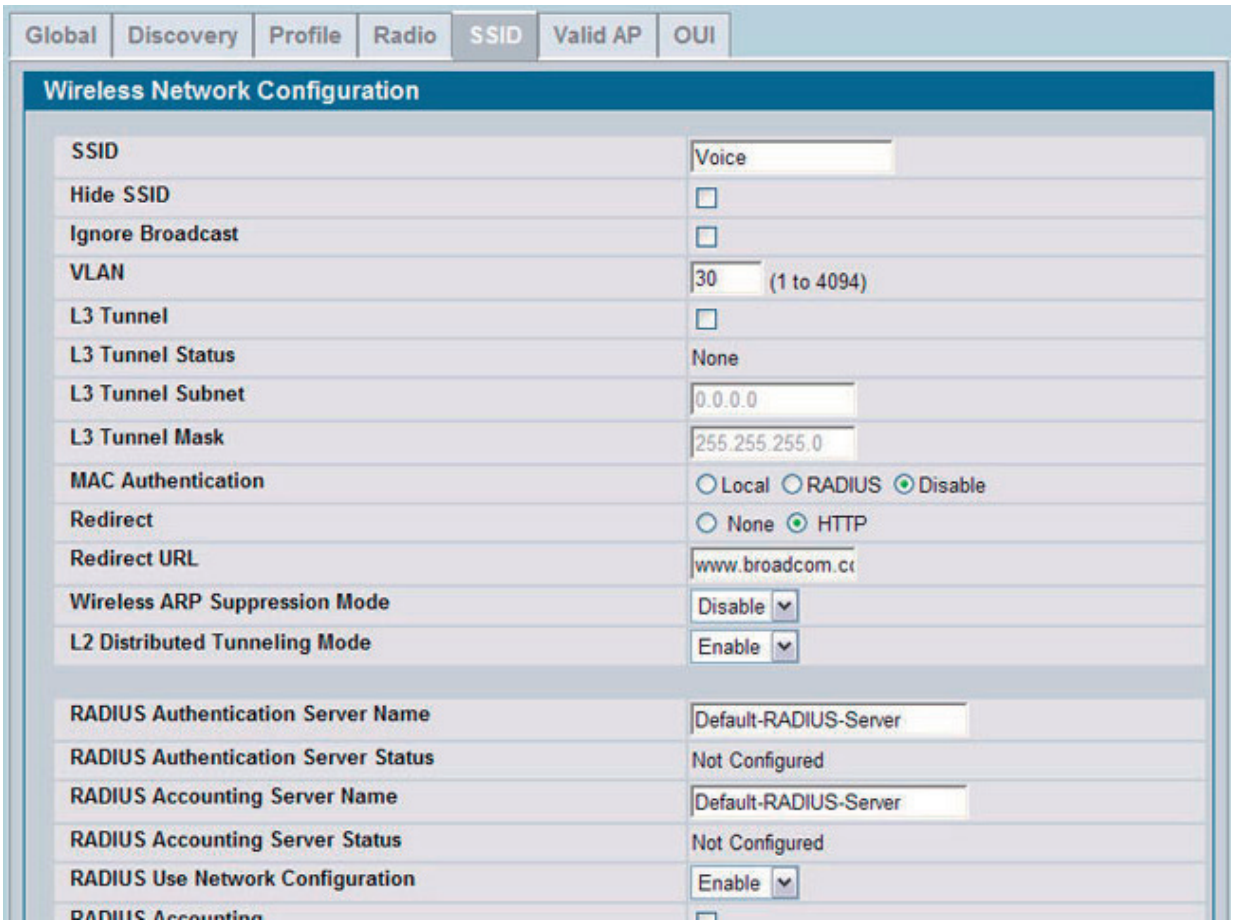
6. VAP タブをクリックし、「Wireless Default VAP Configuration」画面に戻ります。

7. 「Network 3」隣のチェックボックスを選択し、「Edit」ボタンをクリックします。

8. 3 つ目の VAP を設定します。

注意 このVAPがWPAエンタープライズを使用するため、無線クライアントは外部のRADIUSサーバを使用して認証する必要があります。「RADIUS Authentication Server Configured」が「Configured」としてステータスを表示していることを確認してください。RADIUS サーバ設定に関する詳しい情報に関しては、「802.1X ネットワークアクセスコントロールの設定」（404 ページ）で RADIUS サーバ設定の手順を参照してください。

a. 既存の SSID を削除し、「SSID」に「Voice」を入力します。
b. 「VLAN」に「30」を入力します。
c. セキュリティオプションから、WPA を選択します。追加のセキュリティフィールドが表示されます。
d. WPA2 クライアントだけが VAP に接続できるように、WPA オプションをクリアします。
e. WPA エンタープライズを選択します。
f. CCMP（AES）オプションを選択します。
g. 「L2 Distributed Tunneling Mode」から「Enable」を選択すると、クライアントはネットワーク接続を喪失せずに異なるサブネットにあるアクセスポイント間をローミングできるようになります。
i. 「DiffServ Policy UP」フィールドから無線クライアントからアクセスポイントに AP まで転送されるトラフィックに適用するポリシーを選択します。
j. 「Submit」ボタンをクリックします。



VoIP のクラス別サービスの設定

DiffServ の最も有効な用途の 1 つは、VoIP（Voice over IP）のサポートです。VoIP トラフィックは本質的に時間に敏感です。ネットワークが許容できるサービスを提供するためには、保証される通信速度が重大となります。この例ではサービスに必要な品質を提供する 1 つの方法を示しています。UDP トラフィッククラスを設定し、トラフィックにインバウンド側でマークを付けて、次にアウトバウンド側でトラフィックを処理する方法です。以下の図では、設定スクリプトはルータ 1 用です。同様のスクリプトがルータ 2 に適用される必要があります。

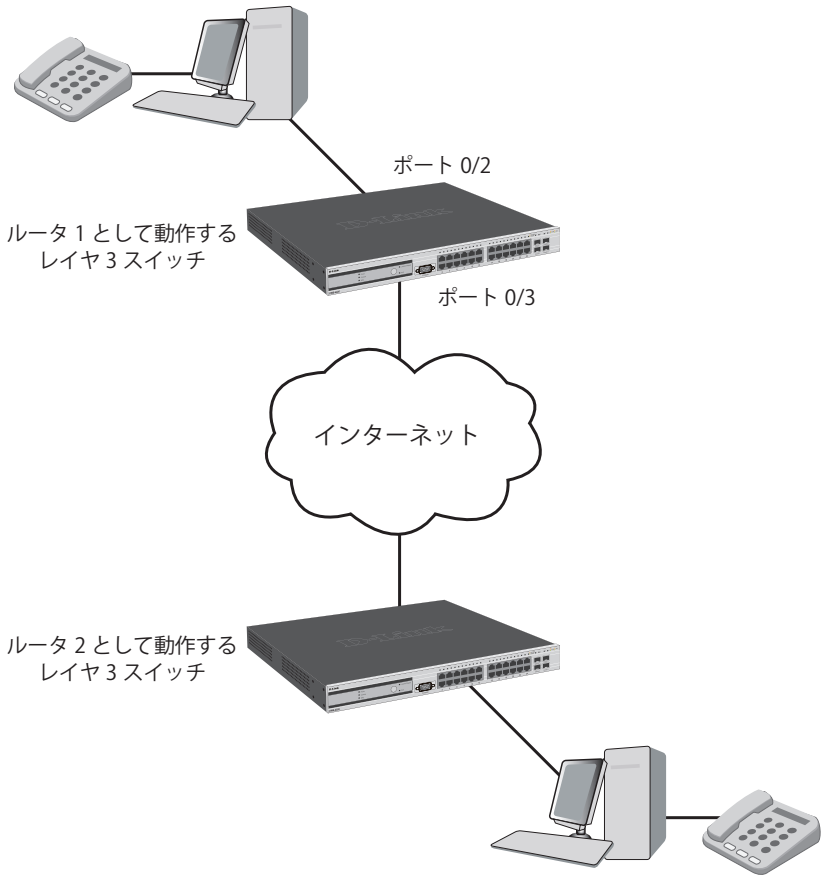
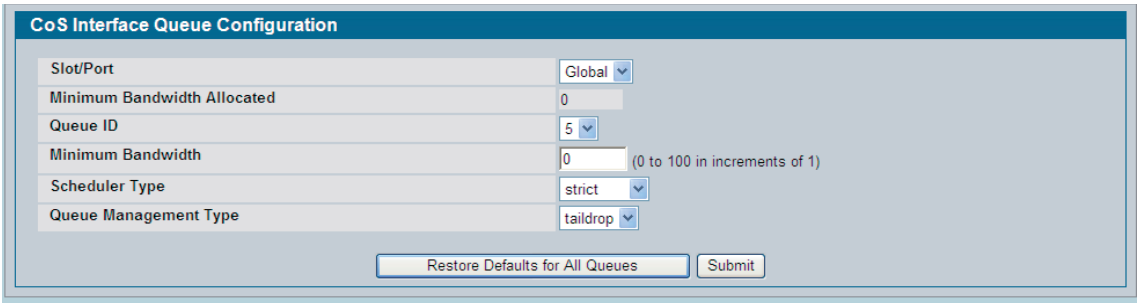


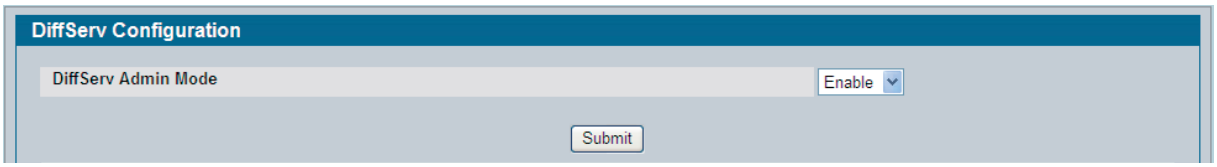
図 A-4　DiffServ VoIP ネットワーク例

1. すべてのポートに「strict」優先度モードを使用するようにキュー 5 を設定するためには、**LAN タブ > QoS > Class of Service > CoS Interface Queue Configuration** の順にメニューをクリックし、以下の設定を行います。
- Slot/Port : Global
- Queue ID : 5
- Scheduler Type : Strict

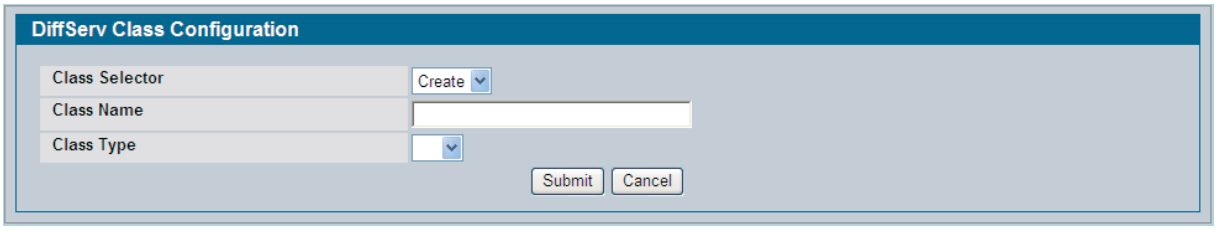
2. 「Submit」ボタンをクリックします。
キュー 5 はすべての VoIP パケットに使用されます。



3. **LAN タブ > QoS > Differentiated Services > DiffServ Configuration** の順にメニューをクリックし、スイッチに DiffServ を有効にします。



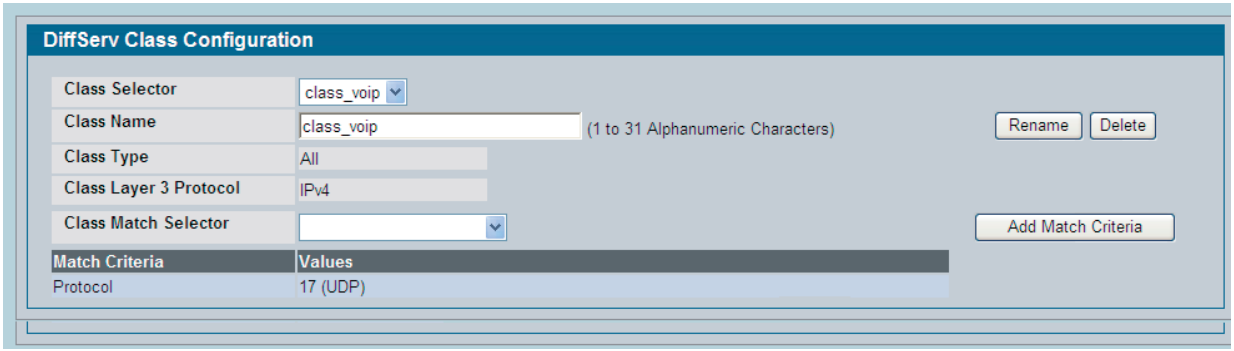
4. **LAN タブ > QoS > Differentiated Services > Class Configuration** の順にメニューをクリックします。「Class Selector」から「Create」を選択し、「Class Name」に「class_voip」と入力します。また、「Class Type」で「All」を選択して「Submit」ボタンをクリックします。



5. 「Class Layer 3 Protocol」に「IPv4」を選択し、「Submit」ボタンをクリックします。

6. 「Class Match Selector」メニューから「Protocol」を選択し、「Add Match Criteria」ボタンをクリックします。

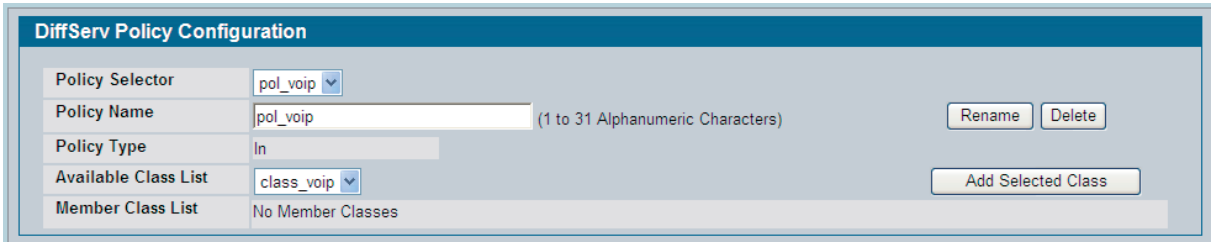
7. 「Protocol Keyword」メニューから「UDP」を選択し、「Submit」ボタンをクリックします。



8. 「class_ef」という名前の 2 つ目の DiffServ クラシファイアを作成し、ef（expedited forwarding）の DSCP（DiffServ code point）を検出する 1 つの照合基準を定義します。
これは、ネットワークの他の場所で「expedited」として以前にマークされた入力トラフィックを処理します。

9. 「Policy Configuration」画面で「Policy Selector」メニューから「Create」を選択し、「Policy Name」に「pol_voip」を入力して「Submit」ボタンをクリックします。

10. 「Available Class List」メニューから「class_voip」を選択し、「Add Selected Class」ボタンをクリックします。



11. 「Available Class List」メニューから「class_ef」を選択し、「Add Selected Class」ボタンをクリックします。

12. 「Policy Class Definition」画面でポリシーに一致するクラスを処理する方法を設定します。
入力パケットが既に「EF」（class_ef 定義毎）の DSCP 値でマークされる、または「EF」の DSCP 値で UDP パケット（class_voip 定義毎）をマークするというポリシーを以下の手順で設定します。両方の場合で、パケットを送信するイーグレスポートのキュー 5 を使用するために一致したパケットが内部的に割り当てられます。

- **a.** 「Policy Selector」から「pol_viop」、「Member Class List」から「class_ef」、および「Policy Attribute Selector」から「Assign Queue」を選択し、「Configure Selected Attribute」ボタンをクリックします。
- **b.** 「Queue ID Value」フィールドに「5」を入力し、「Submit」ボタンをクリックします。
- **c.** 「Policy Selector」メニューから「pol_viop」、「Member Class List」から「class_voip」、および「Policy Attribute Selector」から「Assign Queue」を選択し、「Configure Selected Attribute」ボタンをクリックします。
- **d.** 「DSCP Keyword」から「ef」を選択し、「Submit」ボタンをクリックします。
- **e.** 「Policy Selector」メニューから「pol_viop」、「Member Class List」から「class_voip」、および「Policy Attribute Selector」から「Mark IP DSCP」を選択し、「Configure Selected Attribute」ボタンをクリックします。
- **f.** 「DSCP Keyword」メニューから「ef」を選択し、「Submit」ボタンをクリックします。

13. 内向きのサービスインタフェースに定義済みのポリシーを割り当てるためには、「Service Configuration」画面を表示します。

14. 「Slot/Port」からインタフェース 0/2 を選択します。

15. 「Policy In」メニューから「pol_voip」を選択します。

16. 「Submit」ボタンをクリックします。

付録 B　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。

B.1 DWS-4026 の初期設定

表 B-1 は、DWS-4026 初期設定を示します。

表 B-1　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	admin
	Password	None
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

B.2 D-Link アクセスポイントプロファイルの初期設定

表 B-2 はデフォルト 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。

表 B-2　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

設定項目		初期値
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
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

B.3 キャプティブポータル設定の初期値

表 B-3 はキャプティブポータル設定の初期値を示します。

表 B-3　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 (unlimited)
	Idle Timeout	0 (unlimited)
	Languages	English