

D-Link DGS-3420 シリーズ
Layer2+ Gigabit Stackable Managed Switch

..... ユーザマニュアル






安全にお使いいただくために



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

安全上のご注意










必ずお守りください

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


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

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










危険

-  **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。
分解禁止
-  **ぬれた手でさわらない**
感電のおそれがあります。
ぬれ手禁止
-  **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。
水ぬれ禁止
-  **水などの液体（飲料水、汗、海水、ペットの尿など）でぬれた状態で触ったり、電源を入れたりしない**
火災、やけど、けが、感電または故障のおそれがあります。
ぬれ手禁止
-  **各種端子やスロットに水などの液体（飲料水、汗、海水、ペットの尿など）をいれない。万が一、入ってしまった場合は、直ちに電源プラグをコンセントから抜く**
火災、やけど、けが、感電または故障のおそれがあります。
水ぬれ禁止
-  **油煙、湯気、湿気、埃の多い場所、高温になる場所や熱のこもりやすい場所（火のそば、暖房器具のそば、こたつや布団の中、直射日光の当たる場所、炎天下の車内、風呂場など）、振動の激しい場所では、使用、保管、放置しない**
火災、やけど、けが、感電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
-  **砂や土、泥をかけたり、直に置いたりしない。また、砂などが付着した手で触れない**
火災、やけど、けが、感電または故障のおそれがあります。
禁止
-  **電子レンジ、IH 調理器などの加熱調理機、圧力釜など高圧容器に入れたり、近くに置いたりしない**
火災、やけど、けが、感電または故障のおそれがあります。
禁止















警告

-  **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。
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。
-  **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
-  **製品付属の AC アダプタもしくは電源ケーブルを指定のコンセントに正しく接続して使用する**
火災、感電、または故障の原因となります。
-  **各光源をのぞかない**
光ファイバケーブルの断面、コネクタおよび製品のコネクタや LED をのぞきますと強力な光源により目を損傷する恐れがあります。
禁止
-  **各種端子やスロットに導電性異物（金属片、鉛筆の芯など）を接触させたり、ほごりが内部に入ったりしないようにする**
火災、やけど、けが、感電または故障の恐れがあります。
禁止
-  **使用中に布団で覆ったり、包んだりしない**
火災、やけどまたは故障の恐れがあります。
禁止
-  **ガソリンスタンドなど引火性ガスが発生する可能性のある場所や粉じんが発生する場所に立ち入る場合は、必ず事前に本製品の電源を切る**
引火性ガスなどが発生する場所で使用すると、爆発や火災の恐れがあります。
-  **カメラのレンズに直射日光などを長時間あてない**
素子の退色、焼付きや、レンズの集光作用により、火災、やけど、けがまたは故障の恐れがあります。
禁止
-  **無線製品は病院内で使用する場合は、各医療機関の指示に従って使用する**
電子機器や医療電気機器に悪影響を及ぼす恐れがあります。
-  **本製品の周辺に放熱を妨げるようなもの（フィルムやシールでの装飾を含む）を置かない**
火災、または故障の恐れがあります。
禁止
-  **耳を本体から離してご使用ください**
大きな音を長時間連続して聞くと、難聴などの耳の障害の恐れがあります。
-  **無線製品をご使用の場合、医療電気機器などを装着している場合は、医用電気メーカーもしくは、販売業者に、電波による影響について確認の上使用する**
医療電気機器に悪影響を及ぼす恐れがあります。
-  **高精度な制御や微弱な信号を取り扱う**
電子機器の近くでは使用しない
電子機器が誤作動するなど、悪影響を及ぼす恐れがあります。
-  **ディスプレイ部やカメラのレンズを破損した際は、割れたガラスや露出した端末内部に注意する**
破損部や露出部に触れると、やけど、けが、感電の恐れがあります。
-  **ペットなどが本機に噛みつかないように注意する**
火災、やけど、けがなどの恐れがあります。
-  **コンセントに AC アダプタや電源ケーブルを抜き差しするときは、金属類を接触させない**
火災、やけど、感電または故障の恐れがあります。
禁止
-  **AC アダプタや電源ケーブルに**
海外旅行用の変圧器等を使用しない
発火、発熱、感電または故障の恐れがあります。
禁止

警告

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

注意

-  乳幼児の手の届く場所では使わないやけど、ケガまたは感電の恐れがあります。
-  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ると故障の恐れがあります。
-  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。
-  付属品の使用は取扱説明書に従う付属品は、取扱説明書に従い、他の製品に使用しないでください。機器の破損の恐れがあります。
-  破損したまま使用しない火災、やけどまたはけがの恐れがあります。
-  ぐらついた台の上や傾いた場所などの不安定な場所や高所には置かない落下して、けがなどの恐れがあります。
-  子供が使用する場合は、保護者が取扱いの方法を教え、誤った使い方をさせないけがや故障などの恐れがあります。
-  本機を長時間連続使用する場合は、温度が高くなることもあるため、注意する。また、使用中に眠ってしまうなどして、意図せず長時間触れることがないようにする温度の高い部分に直接長時間触れるとお客様の体質や体調によっては肌の赤みやかゆみ、かぶれ、低温やけどの恐れがあります。
-  高温注意動作中に高温になる場合があります。製品の移動や取り外しの際は、慎重に触れるようにしてください。低温やけどの原因となります。
-  長時間触れたまま使用しない動作中、製品が熱くなることがあります。長時間触れたまま使用しないでください。低温やけどの原因となります。
-  コンセントにつないだ状態で、電源アダプタや電源コンセントに長時間触れないやけど、感電の恐れがあります。
-  一般の電話機やテレビ、ラジオなどをお使いになっている近くで使用しない近くで使用すると、悪影響を及ぼす原因となるため、なるべく離れた場所で使用してください。
-  D-Link が指定したオプション品がある場合は、指定オプションを使用する不正なオプション品を使用した場合、故障、破損の恐れがあります。

電波障害自主規制について

本製品は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラス A 情報技術装置です。

この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

ご使用上の注意

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

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

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. 機器を箱から取り出すときは、機器をシステム等に取り付ける準備が完了するまで、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がしてください。
2. 静電気に敏感な部品を運ぶ場合、最初に静電気防止容器またはパッケージに入れてください。
3. 静電気に敏感な機器の扱いは、静電気のない場所で行います。可能であれば、静電気防止床パッド、作業台パッド、および帯電防止接地ストラップを使用してください。

電源の異常

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

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

ラック搭載型製品に関する一般的な注意事項

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

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

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

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

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

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

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

バッテリーの取り扱いについて

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

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、ご使用前にご確認ください。製品保証、保守サービス、テクニカルサポートご利用について、詳しくは弊社ホームページのサポート情報をご確認ください。

<http://www.dlink-jp.com/support>

目次

| | |
|-----------------------------------|-----------|
| 安全にお使いいただくために..... | 2 |
| ご使用上の注意..... | 4 |
| 静電気障害を防止するために..... | 4 |
| 電源の異常..... | 4 |
| ラック搭載型製品に関する一般的な注意事項..... | 5 |
| バッテリーの取り扱いについて..... | 5 |
| はじめに | 15 |
| 本マニュアルの対象者..... | 16 |
| 表記規則について..... | 16 |
| 第1章 本製品のご使用にあたって | 17 |
| xStack DGS-3420 シリーズについて..... | 17 |
| ポート..... | 17 |
| 前面パネル..... | 19 |
| アラームコネクタ..... | 21 |
| LED 表示..... | 22 |
| 背面パネル..... | 24 |
| 側面パネル..... | 25 |
| SFP スロット..... | 26 |
| 第2章 スイッチの設置 | 27 |
| パッケージの内容..... | 27 |
| ネットワーク接続前の準備..... | 27 |
| ゴム足の取り付け (19 インチラックに設置しない場合)..... | 28 |
| 19 インチラックへの取り付け..... | 28 |
| 電源の投入 (AC 電源)..... | 29 |
| 電源の異常..... | 29 |
| リダンダント電源システムの設置..... | 30 |
| DPS-500..... | 30 |
| DPS-800..... | 31 |
| DPS-700..... | 31 |
| 第3章 スイッチの接続 | 32 |
| エンドノードと接続する..... | 32 |
| ハブまたはスイッチと接続する..... | 32 |
| バックボーンまたはサーバと接続する..... | 33 |
| 第4章 スイッチ管理の導入 | 34 |
| 管理オプション..... | 34 |
| 端末をコンソールポートに接続する..... | 34 |
| スイッチへの初回接続..... | 35 |
| 管理ポートへの接続..... | 36 |
| パスワード設定..... | 36 |
| IP アドレスの割り当て..... | 37 |
| SNMP 設定..... | 38 |
| トラップ..... | 38 |
| MIB..... | 38 |
| 第5章 Web ベースのスイッチ管理 | 39 |
| Web ベースの管理について..... | 39 |
| Web マネージャへのログイン..... | 39 |
| Web マネージャの画面構成..... | 40 |
| Web マネージャのメイン画面について..... | 40 |
| Web マネージャのメニュー構成..... | 41 |

| | |
|---|-----------|
| 第 6 章 System Configuration (スイッチの主な設定) | 44 |
| Device Information (デバイス情報) | 45 |
| System Information Settings (システム情報設定) | 47 |
| Port Configuration (ポート設定) | 48 |
| DDM (DDM 設定) | 48 |
| Port Settings (スイッチのポート設定) | 52 |
| Port Description Settings (ポート名設定) | 53 |
| Port Error Disabled (エラーによるポートの無効) | 54 |
| Port Media Type (ポートメディアタイプ) | 54 |
| Port Auto Negotiation Information (オートネゴシエーション情報) | 55 |
| Jumbo Frame Settings (ジャンボフレームの有効化) | 55 |
| EEE Settings (EEE 設定) (H/W バージョン B1 のみ) | 56 |
| PoE Configuration (PoE 設定) (DGS-3420-28PC/52P のみ) | 56 |
| PoE System Settings (PoE システムの設定) | 57 |
| PoE Port Settings (PoE ポート設定) | 58 |
| Serial Port Settings (シリアルポート設定) | 59 |
| Warning Temperature Settings (警告温度設定) | 59 |
| System Log Configuration (システムログ構成) | 60 |
| System Log Settings (システムログ設定) | 60 |
| System Log Server Settings (システムログサーバの設定) | 60 |
| System Log (Syslog ログ) | 61 |
| System Log & Trap Settings (Syslog とトラップ設定) | 62 |
| System Severity Settings (システムセベリティ設定) | 62 |
| Time Range Settings (タイムレンジ設定) | 63 |
| Port Group Settings (ポートグループ設定) | 64 |
| Time Settings (時刻設定) | 64 |
| User Accounts Settings (ユーザアカウントの設定) | 65 |
| Command Logging Settings (コマンドログ設定) | 66 |
| Stacking (スタッキング設定) | 67 |
| Stacking Device Table (スタックデバイステーブル) | 69 |
| Stacking Mode Settings (スタックモード設定) | 69 |
| 第 7 章 Management (スイッチの管理) | 70 |
| ARP (ARP 設定) | 71 |
| Static ARP Settings (スタティック ARP 設定) | 71 |
| Proxy ARP Settings (プロキシ ARP 設定) | 72 |
| ARP Table (ARP テーブルの参照) | 72 |
| Gratuitous ARP (Gratuitous ARP の設定) | 73 |
| Gratuitous ARP Global Settings (Gratuitous ARP グローバル設定) | 73 |
| Gratuitous ARP Settings (Gratuitous ARP 設定) | 73 |
| IPv6 Neighbor Settings (IPv6 Neighbor 設定) | 74 |
| IP Interface (IP インタフェース設定) | 75 |
| System IP Address Settings (IP アドレス設定) | 75 |
| Interface Settings (インタフェース設定) | 76 |
| Loopback Interface Settings (ループバックインタフェース設定) | 80 |
| Management Settings (管理設定) | 81 |
| Out of Band Management Settings (アウトバンド管理設定) | 82 |
| Session Table (セッションテーブル) | 82 |
| Single IP Management (シングル IP マネジメント設定) | 83 |
| シングル IP マネジメント (SIM) の概要 | 83 |
| Single IP Settings (シングル IP 設定) | 84 |
| Topology (トポロジ) | 85 |
| ツールヒント | 87 |
| メニューバー | 90 |
| Firmware Upgrade (ファームウェア更新) | 91 |
| Configuration File Backup/ Restore (コンフィグレーションファイルの更新) | 91 |
| Upload Log File (ログファイルのアップロード) | 91 |
| SNMP Settings (SNMP 設定) | 92 |
| SNMP Global Settings (SNMP グローバル設定) | 93 |
| SNMP Trap Settings (SNMP トラップ設定) | 93 |
| SNMP Linkchange Traps Settings (SNMP リンクチェンジトラップ設定) | 94 |
| SNMP View Table Settings (SNMP ビューテーブル) | 94 |
| SNMP Community Table Settings (SNMP コミュニティテーブル設定) | 95 |
| SNMP Group Table Settings (SNMP グループテーブル) | 96 |
| SNMP Engine ID Settings (SNMP エンジン ID 設定) | 97 |

| | |
|---|------------|
| SNMP User Table Settings (SNMP ユーザーテーブル設定) | 97 |
| SNMP Host Table Settings (SNMP ホストテーブル設定) | 98 |
| SNMP v6Host Table Settings (SNMP v6 ホストテーブル設定) | 99 |
| RMON Settings (RMON 設定) | 99 |
| SNMP Community Encryption Settings (SNMP コミュニティ暗号化設定) | 100 |
| SNMP Community Masking Settings (SNMP コミュニティマスク設定) | 100 |
| Telnet Settings (Telnet 設定) | 101 |
| Web Settings (Web 設定) | 101 |
| Power Saving (省電力機能) | 102 |
| LED State Settings (LED 設定) | 102 |
| Power Saving Settings (省電力設定) | 102 |
| Power Saving LED Settings (LED 省電力設定) | 103 |
| Power Saving Port Settings (ポート省電力設定) | 103 |
| 第 8 章 L2 Features (L2 機能の設定) | 104 |
| VLAN について | 105 |
| IEEE 802.1p プライオリティについて | 105 |
| VLAN とは | 105 |
| IEEE 802.1Q VLAN | 106 |
| VLAN (VLAN 設定) | 111 |
| 802.1Q VLAN Settings (802.1Q VLAN 設定) | 111 |
| 802.1v Protocol VLAN (802.1v プロトコル VLAN) | 114 |
| Asymmetric VLAN Settings (Asymmetric VLAN 設定) | 117 |
| GVRP (GVRP の設定) | 117 |
| MAC-based VLAN Settings (MAC ベース VLAN 設定) | 119 |
| Private VLAN Settings (プライベート VLAN 設定) | 120 |
| PVID Auto Assign Settings (PVID 自動割り当て設定) | 121 |
| Subnet VLAN (サブネット VLAN) | 122 |
| VLAN Precedence Settings (VLAN 優先度設定) | 123 |
| Voice VLAN (音声 VLAN) | 123 |
| VLAN Trunk Settings (VLAN トランク設定) | 127 |
| Browse VLAN (VLAN の参照) | 128 |
| Show VLAN Ports (VLAN ポートの参照) | 128 |
| QinQ (QinQ 設定) | 129 |
| QinQ Settings (QinQ 設定) | 130 |
| VLAN Translation Settings (VLAN 変換機能の設定) | 131 |
| VLAN Translation Port Mapping Settings (VLAN 変換ポートのマッピング設定) | 132 |
| VLAN Translation Profile List (VLAN 変換プロファイルリスト) | 132 |
| Layer 2 Protocol Tunneling Settings (レイヤ 2 プロトコルトンネリング設定) | 134 |
| Spanning Tree (スパンニングツリーの設定) | 135 |
| 802.1Q-2005 MSTP | 135 |
| 802.1D-2004 Rapid Spanning Tree | 135 |
| ポートの状態遷移 | 135 |
| STP Bridge Global Settings (STP ブリッジグローバル設定) | 136 |
| STP Port Settings (STP ポートの設定) | 138 |
| MST Configuration Identification (MST の設定) | 139 |
| STP Instance Settings (STP インスタンス設定) | 140 |
| MSTP Port Information (MSTP ポート情報) | 141 |
| Link Aggregation (ポートトランッキングの設定) | 143 |
| ポートトランクグループについて | 143 |
| Port Trunking Settings (ポートトランッキング設定) | 144 |
| LACP Port Settings (LACP ポートの設定) | 145 |
| FDB (FDB 設定) | 146 |
| Static FDB Settings (スタティック FDB の設定) | 146 |
| MAC Notification Settings (MAC 通知設定) | 148 |
| MAC Address Aging Time Settings (MAC アドレスエイジングタイムの設定) | 148 |
| MAC Address Table (MAC アドレステーブル) | 149 |
| ARP & FDB Table (ARP と FDB テーブル) | 150 |
| L2 Multicast Control (L2 マルチキャストコントロール) | 151 |
| IGMP Proxy (IGMP プロキシ) | 151 |
| IGMP Snooping (IGMP Snooping の設定) | 153 |
| MLD Proxy (MLD プロキシ) | 161 |
| MLD Snooping (MLD Snooping 設定) | 163 |
| Multicast VLAN (マルチキャスト VLAN) | 170 |
| IP Multicast VLAN Replication (IP マルチキャスト VLAN レプリケーション) | 177 |

| | |
|---|------------|
| Multicast Filtering (マルチキャストフィルタリング) | 179 |
| IPv4 Multicast Filtering (IPv4 マルチキャストフィルタリング) | 179 |
| IPv6 Multicast Filtering (IPv6 マルチキャストフィルタリング) | 183 |
| Multicast Filtering Mode (マルチキャストフィルタリングモード) | 187 |
| ERPS Settings (イーサネットリングプロテクション設定) | 188 |
| LLDP (LLDP 設定) | 191 |
| LLDP (LLDP 設定) | 191 |
| LLDP-MED (LLDP-MED 設定) | 198 |
| NLB FDB Settings (NLB FDB 設定) | 200 |
| PTP (PTP の設定) | 201 |
| PTP Global Settings (PTP グローバル設定) | 201 |
| PTP Port Settings (PTP ポート設定) | 202 |
| PTP Boundary Clock Settings (PTP 境界クロック設定) | 202 |
| PTP Boundary Port Settings (PTP 境界ポート設定) | 203 |
| PTP Peer to Peer Transparent Port Settings (PTP ピアツーピア透過ポート設定) | 204 |
| PTP Clock Information (PTP クロック情報の表示) | 204 |
| PTP Port Information (PTP ポート情報) | 205 |
| PTP Foreign Master Records Port Information (PTP 外部マスタレコードのポート情報) | 205 |
| 第 9 章 L3 Features (レイヤ 3 機能の設定) | 206 |
| IPv4 Static/Default Route Settings (IPv4 スタティック / デフォルトルート設定) | 207 |
| IPv4 Route Table (IPv4 ルートテーブル) | 208 |
| IPv6 Static/Default Route Settings (IPv6 スタティック / デフォルトルート設定) | 208 |
| IPv6 Route Table (IPv6 ルートテーブル) | 209 |
| Policy Route Settings (ポリシールート設定) | 210 |
| IP Forwarding Table (IP フォワーディングテーブル) | 212 |
| Route Preference Settings (ルート優先度設定) | 212 |
| Route Redistribution (ルート再配布) | 213 |
| Route Redistribution Settings (ルート再配布設定) | 213 |
| IPv6 Route Redistribution Settings (IPv6 ルート再配布設定) | 213 |
| IP Tunnel (IP トンネル) | 214 |
| IP Tunnel Settings (IP トンネル設定) | 214 |
| IP Tunnel GRE Settings (IP トンネル GRE 設定) | 215 |
| RIP (RIP 設定) | 216 |
| RIP Settings (RIP 設定) | 218 |
| RIPng (RIPng 設定) | 219 |
| VRRP (VRRP 設定) | 221 |
| VRRP Global Settings (VRRP グローバル設定) | 221 |
| VRRP Virtual Router Settings (VRRP 仮想ルータ設定) | 221 |
| VRRP Authentication Settings (VRRP 認証設定) | 223 |
| 第 10 章 QoS (QoS 機能の設定) | 224 |
| QoS について | 225 |
| 802.1p Settings (802.1p 設定) | 226 |
| 802.1p Default Priority Settings (ポートへのパケットプライオリティの割り当て) | 226 |
| 802.1p User Priority Settings (802.1p ユーザプライオリティ) | 227 |
| Bandwidth Control (帯域幅の設定) | 227 |
| Bandwidth Control Settings (帯域幅の設定) | 227 |
| Queue Bandwidth Control Settings (キュー帯域幅制御の設定) | 228 |
| Traffic Control Settings (トラフィックコントロールの設定) | 229 |
| DSCP (DSCP 設定) | 231 |
| DSCP Trust Settings (DSCP トラスト設定) | 231 |
| DSCP Map Settings (DSCP マップ設定) | 231 |
| HOL Blocking Prevention (HOL ブロッキング防止) | 232 |
| Scheduling Settings (スケジューリング設定) | 232 |
| QoS Scheduling (QoS スケジューリング作成) | 232 |
| QoS Scheduling Mechanism (QoS スケジューリングメカニズム設定) | 233 |
| WRED (WRED 設定) | 234 |
| WRED Port Settings (WRED ポート設定) | 234 |
| WRED Profile Settings (WRED プロファイル設定) | 235 |

| | |
|--|------------|
| 第 11 章 ACL (ACL 機能の設定) | 236 |
| ACL Configuration Wizard (ACL 設定ウィザード) | 236 |
| Access Profile List (アクセスプロファイルリスト) | 238 |
| アクセスプロファイルリストの作成 (Ethernet) | 238 |
| アクセスプロファイルリストの作成 (IPv4) | 242 |
| アクセスプロファイルリストの作成 (IPv6) | 247 |
| アクセスプロファイルリストの作成 (パケットコンテンツ) | 251 |
| CPU Access Profile List (CPU アクセスプロファイルリスト) | 255 |
| CPU アクセスプロファイルの作成 (Ethernet) | 256 |
| CPU アクセスプロファイルの作成 (IPv4) | 259 |
| CPU アクセスプロファイルの作成 (IPv6) | 263 |
| CPU アクセスプロファイルの作成 (パケットコンテンツ) | 266 |
| ACL Finder (ACL 検索) | 270 |
| ACL Flow Meter (ACL フローメータ) | 271 |
| Egress Access Profile List (Egress アクセスプロファイルリスト) | 275 |
| アクセスプロファイルリストの作成 (Ethernet) | 275 |
| アクセスプロファイルリストの作成 (IPv4) | 279 |
| アクセスプロファイルリストの作成 (IPv6) | 283 |
| Egress ACL Flow Meter (Egress ACL フローメータリング) | 288 |
| 第 12 章 Security (セキュリティ機能の設定) | 291 |
| 802.1X (802.1X 設定) | 293 |
| Port Access Entity (ポートアクセスエンティティ) | 293 |
| 802.1X Global Settings (802.1X グローバル設定) | 297 |
| 802.1X Port Settings (802.1X ポート設定) | 297 |
| 802.1X User Settings (802.1X ユーザ設定) | 299 |
| Guest VLAN (ゲスト VLAN の設定) | 300 |
| Authenticator State (オーセンティケータの状態) | 301 |
| Authenticator Statistics (オーセンティケータ統計情報) | 302 |
| Authenticator Session Statistics (オーセンティケータセッション統計情報) | 303 |
| Authenticator Diagnostics (オーセンティケータ診断) | 304 |
| Initialize Port-based Port(s) (初期化ポート - ポートベース) | 304 |
| Initialize Host-based Port(s) (初期化ポート - ホストベース) | 305 |
| Reauthenticate Port-based Port(s) (再認証ポート - ポートベース) | 305 |
| Reauthenticate Host-based Port(s) (再認証ポート - ホストベース) | 305 |
| RADIUS (RADIUS 設定) | 306 |
| Authentication RADIUS Server Settings (認証 RADIUS サーバ設定) | 306 |
| RADIUS Authentication (RADIUS 認証) | 308 |
| RADIUS Account Client (RADIUS アカウンティングクライアント) | 309 |
| IP-MAC-Port Binding (IMPB : IP-MAC- ポートバインディング) | 310 |
| IMPB Global Settings (IMPB グローバル設定) | 310 |
| IMPB Port Settings (IMPB ポート設定) | 311 |
| IMPB Entry Settings (IMPB エントリ設定) | 312 |
| MAC Block List (MAC ブロックリスト) | 313 |
| DHCP Snooping (DHCP Snooping 設定) | 313 |
| ND Snooping (ND Snooping 設定) | 314 |
| MAC-based Access Control (MAC ベースアクセスコントロール) | 316 |
| MAC-based Access Control Settings (MAC ベースアクセスコントロール設定) | 316 |
| MAC-based Access Control Local Settings (MAC ベースアクセスコントロール ローカル設定) | 318 |
| MAC-based Access Control Authentication State (MAC ベースアクセスコントロールの認証状態) | 319 |
| Web-based Access Control (WAC) (Web ベースのアクセス制御) | 320 |
| 条件および制限 | 321 |
| WAC Global Settings (WAC グローバル設定) | 322 |
| WAC User Settings (WAC ユーザ設定) | 323 |
| WAC Port Settings (WAC ポート設定) | 324 |
| WAC Authentication State (WAC 認証状態) | 325 |
| WAC Customize Page (WAC カスタマイズページ設定) | 325 |
| Japanese Web-based Access Control (JWAC : JWAC 設定) | 326 |
| JWAC Global Settings (JWAC グローバル設定) | 326 |
| JWAC Port Settings (JWAC ポート設定) | 327 |
| JWAC User Settings (JWAC ユーザ設定) | 328 |
| JWAC Authentication State (JWAC 認証状態) | 329 |
| JWAC Customize Page Language (JWAC 画面言語のカスタマイズ) | 329 |
| JWAC Customize Page (JWAC 画面のカスタマイズ) | 330 |

| | |
|---|------------|
| Compound Authentication (コンパウンド認証) | 331 |
| Compound Authentication Settings (コンパウンド認証設定) | 331 |
| Compound Authentication Guest VLAN Settings (コンパウンド認証ゲスト VLAN の設定) | 332 |
| Compound Authentication MAC Format Settings (コンパウンド認証 MAC 形式設定) | 332 |
| IGMP Access Control Settings (IGMP アクセスコントロール設定) | 333 |
| Port Security (ポートセキュリティ) | 334 |
| Port Security Settings (ポートセキュリティの設定) | 334 |
| Port Security VLAN Settings (ポートセキュリティ VLAN 設定) | 336 |
| Port Security Entries (ポートセキュリティエントリ) | 337 |
| ARP Spoofing Prevention Settings (ARP Spoofing 防止設定) | 338 |
| BPDU Attack Protection (BPDU アタック防止設定) | 339 |
| Loopback Detection Settings (ループバック検知設定) | 340 |
| NetBIOS Filtering Setting (NetBIOS フィルタリング設定) | 341 |
| Traffic Segmentation Settings (トラフィックセグメンテーション設定) | 342 |
| DHCP Server Screening (DHCP サーバスクリーニング) | 343 |
| DHCP Server Screening Port Settings (DHCP サーバスクリーニング設定) | 343 |
| DHCP Offer Permit Entry Settings (DHCP オファー許可エントリ設定) | 344 |
| Filter DHCPv6 Server (DHCPv6 サーバフィルタ設定) | 344 |
| Filter ICMPv6 (ICMPv6 フィルタ設定) | 345 |
| Access Authentication Control (アクセス認証コントロール) | 346 |
| Enable Admin (管理者レベルの認証) | 347 |
| Authentication Policy Settings (認証ポリシー設定) | 347 |
| Application Authentication Settings (アプリケーションの認証設定) | 348 |
| Accounting Settings (アカウント設定) | 349 |
| Authentication Server Group Settings (認証サーバグループ設定) | 350 |
| Authentication Server Settings (認証サーバ設定) | 351 |
| Login Method Lists Settings (ログインメソッドリスト) | 352 |
| Enable Method Lists Settings (メソッドリストの有効化) | 353 |
| Accounting Method Lists Settings (アカウントメソッドリスト設定) | 354 |
| Local Enable Password Settings (ローカルユーザパスワード設定) | 355 |
| Authentication Source IP Interface Settings (認証送信元 IP インタフェース設定) | 355 |
| SSL Settings (Secure Socket Layer の設定) | 356 |
| SSL Certification Settings (SSL 証明書設定) | 358 |
| SSH (Secure Shell の設定) | 359 |
| SSH Settings (SSH サーバ設定) | 359 |
| SSH Authentication Method and Algorithm Settings (SSH 認証モードとアルゴリズム設定) | 360 |
| SSH User Authentication Lists (SSH ユーザ認証リスト) | 361 |
| DoS Attack Prevention Settings (DoS 攻撃防止設定) | 362 |
| Trusted Host Settings (トラストホスト) | 363 |
| Safeguard Engine Settings (セーフガードエンジン設定) | 364 |
| SFTP Server Settings (SFTP サーバ設定) | 365 |
| 第 13 章 Network Application (ネットワークアプリケーション) | 366 |
| DHCP (DHCP 設定) | 367 |
| DHCP Relay (DHCP リレー) | 367 |
| DHCP Server (DHCP サーバ) | 372 |
| DHCPv6 Server (DHCPv6 サーバ設定) | 380 |
| DHCPv6 Relay (DHCPv6 リレー) | 383 |
| DHCP Local Relay Settings (DHCP ローカルリレー設定) | 385 |
| DNS (ドメインネームシステム) | 386 |
| DNS Relay (DNS リレー) | 386 |
| DNS Resolver (DNS リゾルバ) | 388 |
| DNS Resolver Global Settings (DNS リゾルバグローバル設定) | 388 |
| DNS Resolver Static Name Server Settings (DNS リゾルバスタティックネームサーバ設定) | 388 |
| DNS Resolver Dynamic Name Server Table (DNS リゾルバダイナミックネームサーバテーブル) | 389 |
| DNS Resolver Static Host Name Settings (DNS リゾルバスタティックホスト名設定) | 389 |
| DNS Resolver Dynamic Host Name Table (DNS リゾルバダイナミックホスト名テーブル) | 389 |
| RCP Server Settings (RCP サーバ設定) | 390 |
| SMTP Settings (SMTP 設定) | 391 |
| SNTP (SNTP 設定) | 393 |
| SNTP Settings (SNTP 設定) | 393 |
| Time Zone Settings (タイムゾーン設定) | 394 |
| UDP (UDP 設定) | 396 |
| UDP Helper (UDP ヘルパー) | 396 |
| Flash File System Settings (フラッシュファイルシステム設定) | 398 |

| | |
|--|------------|
| 第 14 章 OAM (Operations, Administration, Maintenance : 運用・管理・保守) | 400 |
| CFM (Connectivity Fault Management : 接続性障害管理) | 401 |
| CFM Settings (CFM 設定) | 401 |
| CFM Port Settings (CFM ポート設定) | 407 |
| CFM MIPCCM Table (CFM MIPCCM テーブル) | 408 |
| CFM Loopback Settings (CFM ループバック設定) | 408 |
| CFM Linktrace Settings (CFM リンクトレース設定) | 409 |
| CFM Packet Counter (CFM パケットカウンタ) | 410 |
| CFM Fault Table (CFM 障害テーブル) | 410 |
| CFM MP Table (CFM MP テーブル) | 411 |
| Ethernet OAM (イーサネット OAM) | 412 |
| Ethernet OAM Settings (イーサネット OAM 設定) | 412 |
| Ethernet OAM Configuration Settings (イーサネット OAM コンフィグレーション設定) | 413 |
| Ethernet OAM Event Log (イーサネット OAM イベントログ) | 414 |
| Ethernet OAM Statistics (イーサネット OAM 統計情報) | 414 |
| DULD Settings (単方向リンク検出設定) | 415 |
| Cable Diagnostics (ケーブル診断機能) | 416 |
| 第 15 章 Monitoring (スイッチのモニタリング) | 417 |
| Utilization (使用率) | 417 |
| CPU Utilization (CPU 使用率) | 417 |
| DRAM & Flash Utilization (DRAM とフラッシュ利用率) | 418 |
| Port Utilization (ポート使用率) | 418 |
| Statistics (統計情報) | 419 |
| Port Statistics (ポート統計情報) | 419 |
| Packet Size (パケットサイズ) | 428 |
| Mirror (ポートミラーリング) | 430 |
| Port Mirror Settings (ポートミラーリング設定) | 430 |
| RSPAN Settings (RSPAN 設定) | 431 |
| sFlow (sFlow 設定) | 433 |
| sFlow Global Settings (sFlow グローバル設定) | 433 |
| sFlow Analyzer Server Settings (sFlow アナライザ設定) | 433 |
| sFlow Flow Sampler Settings (sFlow サンプラ設定) | 434 |
| sFlow Counter Poller Settings (sFlow カウンタポーラ設定) | 435 |
| Ping (Ping 設定) | 436 |
| Broadcast Ping Relay Settings (ブロードキャスト Ping リレー設定) | 436 |
| Ping Test (Ping テスト) | 436 |
| Trace Route (トレースルート) | 438 |
| Peripheral (周辺機器) | 439 |
| Device Environment (デバイス環境の参照) | 439 |
| External Alarm Settings (外部アラームの設定) | 439 |
| 第 16 章 Maintenance (スイッチのメンテナンス) | 440 |
| Save Configuration / Log (コンフィグレーションとログの保存) | 441 |
| Tools (ツールメニュー) | 442 |
| Stacking Information (スタック情報) | 442 |
| Download Firmware (ファームウェアのダウンロード) | 443 |
| Upload Firmware (ファームウェアのアップロード) | 445 |
| Download Configuration (コンフィグレーションのダウンロード) | 446 |
| Upload Configuration (コンフィグレーションファイルのアップロード) | 448 |
| Upload Log File (ログファイルのアップロード) | 450 |
| Reset (リセット) | 451 |
| Reboot System (システムの再起動) | 452 |

| | |
|--|-----|
| 付録 A ケーブルとコネクタ | 453 |
| イーサネットケーブル..... | 453 |
| コンソールケーブル | 453 |
| リダンダント電源 (RPS) ケーブル | 454 |
| 付録 B ケーブル長 | 455 |
| 付録 C ログエントリ | 456 |
| 付録 D トラップログ | 477 |
| 付録 E パケットコンテンツ ACL を使用した ARP スプーフィング攻撃の軽減 | 482 |
| ARP を動作させる方法 | 482 |
| ARP スプーフィングでネットワークを攻撃する方法 | 484 |
| パケットコンテンツ ACL 経由で ARP スプーフィング攻撃を防止する | 485 |
| 設定 | 486 |
| 付録 F パスワードのリカバリ手順 | 488 |
| 付録 G 用語解説 | 489 |

はじめに

xStack DGS-3420 シリーズユーザマニュアルは、本スイッチのインストールおよび操作方法を例題と共に記述しています。

第 1 章 本製品のご使用にあたって

- 本スイッチの概要とその機能について説明します。また、前面、背面、側面の各パネルと LED 表示について説明します。

第 2 章 スイッチの設置

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

第 3 章 スイッチの接続

- スイッチをご使用のネットワークに接続する方法を説明します。

第 4 章 スイッチの管理

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

第 5 章 Web ベースのスイッチ設定

- Web ベースの管理機能への接続方法および使用方法について説明します。

第 6 章 System Configuration (スイッチの主な設定)

- デバイス情報、ポート設定、ユーザアカウント、システムログ設定、時刻設定、シリアルポートなどの基本機能の設定について説明します。

第 7 章 Management (スイッチの管理)

- IP インタフェース設定、ARP 設定、シングル IP マネジメント設定、SNMP 設定、Telnet 設定、Web 設定、省電力設定などの管理機能について説明します。

第 8 章 L2 Features (L2 機能の設定)

- VLAN、トランキング、スパンニングツリー、フォワーディング、フィルタリング、ERPS、LLDP などのレイヤ 2 機能について説明します。

第 9 章 L3 Features (レイヤ 3 機能の設定)

- ルート再配布設定、スタティック / デフォルトルート設定、ルート優先度設定、IP トンネル、RIP などのレイヤ 3 機能について説明します。

第 10 章 QoS (QoS 機能の設定)

- QoS 機能について説明します。帯域制御、QoS スケジューリング、802.1p プライオリティ設定、トラフィックコントロールなどの機能を含みます。

第 11 章 ACL (ACL 機能の設定)

- アクセスプロファイルテーブルや CPU インタフェースフィルタリングなどの ACL (アクセスコントロールリスト) 機能、フローベースのコントロールについて説明します。

第 12 章 Security (セキュリティ機能の設定)

- 802.1X、トラストホスト、アクセス認証コントロール、ポートセキュリティ、トラフィックセグメンテーション、SSL、SSH、IP-MAC-ポートバインディング、Web ベースアクセスコントロール、MAC ベースアクセスコントロールおよびセーフガードエンジンなどのセキュリティ機能について説明します。

第 13 章 Network Application (ネットワークアプリケーション)

- DHCP サーバ設定、DNS 設定、SNTP などのネットワークアプリケーション機能について説明します。

第 14 章 OAM (Object Access Method: オブジェクトアクセス方式)

- CFM (接続性障害管理)、イーサネット OAM、ケーブル診断機能機能について説明します。

第 15 章 Monitoring (スイッチのモニタリング)

- CPU 使用率、パケット統計情報、ケーブル診断、ミラーリング、sFlow、Ping、トレースルートなどのモニタ機能について説明します。

第 16 章 スイッチメンテナンス

- リセット、システムの再起動、変更の保存について説明します。

はじめに

付録 A ケーブルとコネクタ

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

付録 B ケーブル長

- ケーブルの種類と最大ケーブル長についての情報を示します。

付録 C ログエントリ

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

付録 D トラップログ

- スイッチで検出されるのトラップログとその意味について説明します。

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

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

付録 F パスワードのリカバリ手順

- スイッチのパスワードのリセット方法について説明します。

付録 G 用語解説

- 本マニュアルに使用される用語の定義を示します。

本マニュアルの対象者

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

表記規則について

本項では、本マニュアル中での表記方法について説明します。

注意 注意では、特長や技術についての詳細情報を記述します。

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

表 1 に、本マニュアル中での字体・記号についての表記規則を表します。

表 1 字体・記号の表記規則

| 字体・記号 | 解説 | 例 |
|-------------------|----------------------------------|--|
| [] | メニュータイトル、ページ名、ボタン名。 | 「Submit」 ボタンをクリックして設定を確定してください。 |
| 青字 | 参照先。 | " ご使用になる前に " (13 ページ) をご参照ください。 |
| courier フォント | CLI 出力文字、ファイル名。 | (switch-prompt)# |
| courier 太字 | コマンド、ユーザによるコマンドライン入力。 | show network |
| courier 斜体 | コマンドパラメータ (可変または固定)。 | value |
| < > | 可変パラメータ。< > にあたる箇所に値または文字を入力します。 | <value> |
| [] | 任意の固定パラメータ。 | [value] |
| [< >] | 任意の可変パラメータ。 | [<value>] |
| { } | { } 内の選択肢から 1 つ選択して入力するパラメータ。 | {choice1 choice2} |
| (垂直線) | 相互排他的なパラメータ。 | choice1 choice2 |
| { { } | 任意のパラメータで、指定する場合はどちらかを選択します。 | { {choice1 choice2} } |

第 1 章 本製品のご使用にあたって

- xStack DGS-3420 シリーズについて
- サポートする機能
- ポート
- 前面パネル
- 背面パネル
- 側面パネル
- SFP スロット

xStack DGS-3420 シリーズについて

D-Link の DGS-3420 シリーズは D-Link xStack® ファミリーの高性能なメンバーです。10/100/1000Mbps エッジスイッチからコアのギガビットスイッチまでの広範囲においてご使用いただけます。また、ネットワーク管理者向けに操作性のよい管理インタフェースと共にフォールトトレランス、柔軟性、ポート数、高セキュリティ、および高スループットを提供します。

本スイッチは費用対効果の高いギガビットスイッチであり、管理者に手ごろな価格でネットワークを高速のギガビット接続にアップグレードするソリューションを提供します。専用スタックポートは、最大 40 ギガの双方向帯域幅を提供し、これにより DGS-3420 シリーズを SMB のバックボーンソリューションとしても適切なスイッチとなります。スイッチにおけるアドバンスド ACL およびユーザ認証機能はコアからエッジまでネットワークセキュリティ適用範囲を拡張します。ユニークな D-Link セーフガードエンジンはワームとウィルスの脅威から DGS-3420 シリーズを保護します。その結果、総合的な信頼度、実用性、および可用性を増強します。

本スイッチは、PC、ハブ、およびその他のスイッチを含むスイッチに各種ネットワークデバイスをアップリンクさせる 1000BASE-T ポート / SFP スロットの組み合わせを搭載し、フルデュプレックスモードの 10 ギガビットイーサネットを提供します。SFP(Small Form Factor Pluggable) コンポポート、SFP+ スロットは、長距離伝送のためのギガビットリンクにアップリンクさせるために光ファイバトランシーバを装着することが可能です。これらの SFP スロットは、フルデュプレックス通信をサポートしており、(別売の) トランシーバと共に使用されます。

本マニュアルでは、DGS-3420 シリーズの設置、管理、および設定の方法について記述しています。

ポート

DGS-3420 シリーズは以下のポートを搭載しています。

| 型番 | DGS-3420-26SC | DGS-3420-28TC | DGS-3420-28SC | DGS-3420-28PC | DGS-3420-52T | DGS-3420-52P |
|---|---------------|---------------|---------------|---------------|--------------|--------------|
| 10BASE-T/100BASE-TX/1000BASE-T ポート (4 ポートは 1000BASE-T とのコンボ) | 4 | 24 | 4 | 24 | 48 | 48 |
| PoE 給電 (IEEE 802.3af/at) | — | — | — | ○ | — | ○ |
| SFP スロット (4 ポートは 1000BASE-T とのコンボ) | 24 | 4 | 24 | 4 | — | — |
| SFP+ スロット (10 ギガアップリンク用拡張スロット) | 2 | 4 | | | | |
| RJ-45 コンソールポート | 1 | | | | | |
| 管理ポート | 1 | | | | | |
| アラームポート | 入力 x 2、出力 x 1 | | | | | |
| RPS コネクタ | 1 | | | | | |
| SD カードスロット | 1 | | | | | |
| 電源 | AC | AC | AC | AC | AC | AC |

本製品のご使用にあたって

各ポートタイプの特長および使用可能なオプションは次の通りです。

| 10BASE-T/100BASE-TX/1000BASE-T | SFP スロット | SFP+ スロット |
|---|--|--|
| <ul style="list-style-type: none"> IEEE 802.3 IEEE 802.3u IEEE 802.3ab IEEE 802.3af/at (DGS-3420-28PC および DGS-3420-52P のみ) 全二重通信 全二重モード時の IEEE 802.3x フローコントロール | <ul style="list-style-type: none"> IEEE 802.3u IEEE 802.3z <p>対応 SFP トランシーバ:</p> <ul style="list-style-type: none"> DEM-210 (100BASE-FX) DEM-211 (100BASE-FX) DEM-220T/R (WDM) DEM-310GT (1000BASE-LX) DEM-311GT (1000BASE-SX) DEM-312GT2 (1000BASE-SX2) DEM-314GT (1000BASE-LH) DEM-315GT (1000BASE-ZX) DGS-712 (1000BASE-T) DEM-330T/R (WDM) DEM-331T/R (WDM) | <ul style="list-style-type: none"> IEEE 802.3ae IEEE 802.3aq IEEE 802.3z <p>対応 SFP+ トランシーバ:</p> <ul style="list-style-type: none"> DEM-310GT (1000BASE-LX) DEM-311GT (1000BASE-SX) DEM-312GT2 (1000BASE-SX2) DEM-314GT (1000BASE-LH) DEM-315GT (1000BASE-ZX) DEM-330T/R (WDM) DEM-331T/R (WDM) DEM-431XT (10GBASE-SR) DEM-432XT (10GBASE-LR) DEM-433XT (10GBASE-ER) DEM-434XT (10GBASE-ZR) DEM-435XT (10GBASE-LRM) DEM-436XT-BXU (10GBASE-LR WDM) DEM-436XT-BXD (10GBASE-LR WDM) DEM-431XT-DD (10GBASE-SR with DDM) DEM-432XT-DD (10GBASE-LR with DDM) DEM-433XT-DD (10GBASE-ER with DDM) DEM-435XT-DD (10GBASE-LRM with DDM) <p>ダイレクト 接続ケーブル:</p> <ul style="list-style-type: none"> DEM-CB100S DEM-CB300S DEM-CB700S |

注意 SFP コンボスロットは、対応する 1000BASE-T ポートと同時に使用することはできません。同時に使用すると（例：SFP のポート 24 と 1000BASE-T のポート 24）、SFP スロットが優先となり 1000BASE-T ポートは使用不可能となります。

注意 D-Link 社のオリジナルの SNMP 管理ソフトウェアに -View に興味のあるカスタマは、<http://dview.dlink.com.tw/> にて、ソフトウェアとマニュアルをダウンロードしてください。

前面パネル

前面パネルには、10BASE-T/100BASE-TX/1000BASE-T ポート、SFP コンボスロット、管理ポート、SD カードスロット、および RJ-45 コンソールポートが配置されています。また、電源、コンソール、RPS (冗長電源システム)、およびオプションモジュール用の SFP スロットを含む各ポートの Link/Act/Speed の状態を表示する LED を搭載しています。「LED 表示」の項で詳細の動作について説明します。

DGS-3420-26SC

- SFP スロット × 24
- 10BASE-T/100BASE-TX/1000BASE-T コンボポート × 4
- SFP+ スロット × 2
- SD カードスロット
- アラームコネクタ (デジタル in × 2/out × 1)
- RJ-45 コンソールポート × 1
- 管理ポート × 1
- LED: Power、Console、RPS、SD、MGMT、Link/Act/Speed (各ポート)
- スタックモジュール番号 LED

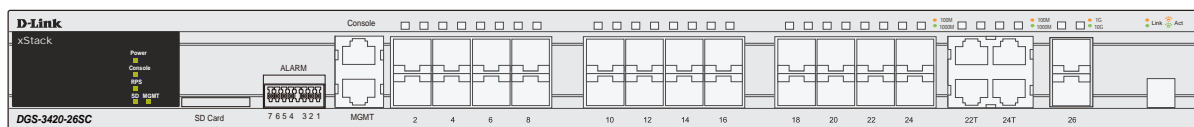


図 1-1 DGS-3420-26SC の前面パネル

DGS-3420-28TC

- 10BASE-T/100BASE-TX/1000BASE-T ポート × 24
- SFP コンボスロット × 4
- SFP+ スロット × 4
- SD カードスロット
- アラームコネクタ (デジタル in × 2/out × 1)
- RJ-45 コンソールポート × 1
- 管理ポート × 1
- LED: Power、Console、RPS、SD、MGMT、Link/Act/Speed (各ポート)
- スタックモジュール番号 LED

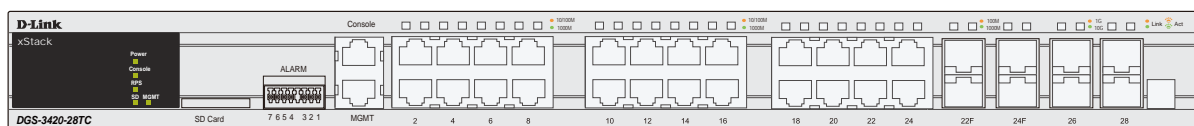


図 1-2 DGS-3420-28TC の前面パネル

DGS-3420-28SC

- SFP スロット × 24
- 10BASE-T/100BASE-TX/1000BASE-T コンボポート × 4
- SFP+ スロット × 4
- SD カードスロット
- アラームコネクタ (デジタル in × 2/out × 1)
- RJ-45 コンソールポート × 1
- 管理ポート × 1
- LED: Power、Console、RPS、SD、MGMT、Link/Act/Speed (各ポート)
- スタックモジュール番号 LED

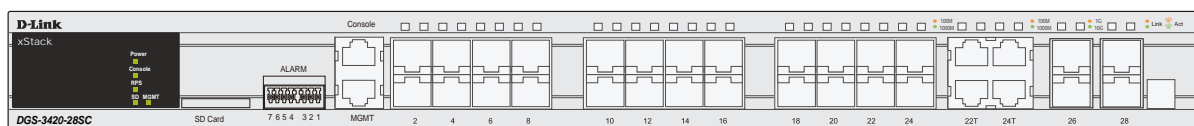


図 1-3 DGS-3420-28SC の前面パネル

DGS-3420-28PC

- 10BASE-T/100BASE-TX/1000BASE-T ポート x 24
- SFP コンボスロット x 4
- SFP+ スロット x 4
- SD カードスロット
- アラームコネクタ (デジタル in x 2/out x 1)
- RJ-45 コンソールポート x 1
- 管理ポート x 1
- LED: Power、Console、RPS、SD、MGMT、PoE、Link/Act/Speed (各ポート)
- スタックモジュール番号 LED

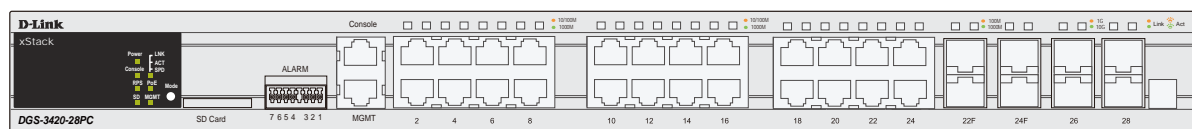


図 1-4 DGS-3420-28PC の前面パネル

DGS-3420-52T

- 10BASE-T/100BASE-TX/1000BASE-T ポート x 48
- SFP+ スロット x 4
- LED: Power、Console、RPS、SD、MGMT、Link/Act/Speed (各ポート)
- スタックモジュール番号 LED

注意 SD カードスロット、アラームコネクタ、RJ-45 コンソールポート、管理ポートは背面に配置されています。

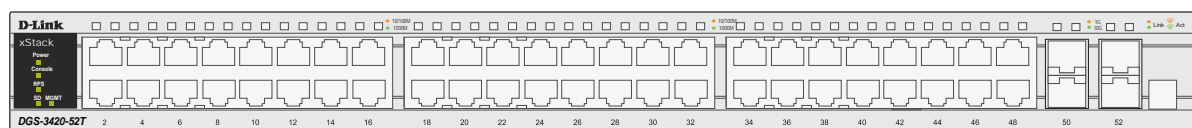


図 1-5 DGS-3420-52T の前面パネル

DGS-3420-52P

- 10BASE-T/100BASE-TX/1000BASE-T ポート x 48
- SFP+ スロット x 4
- LED: Power、Console、RPS、SD、MGMT、PoE、Link/Act/Speed (各ポート)
- スタックモジュール番号 LED

注意 SD カードスロット、アラームコネクタ、RJ-45 コンソールポート、管理ポートは背面に配置されています。

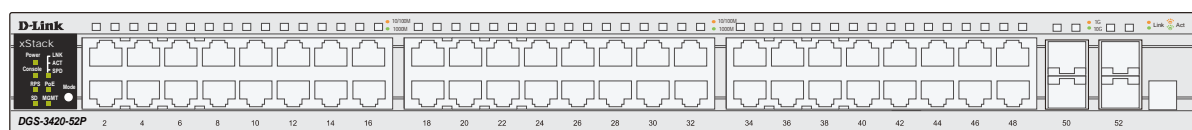


図 1-6 DGS-3420-52P の前面パネル

アラームコネクタ

注意 アラーム PIN の 1、2、3 は 60V で動作し、ピン 4、5、6 は 3V で動作します。

注意 DGS-3420 シリーズのアラームポートは、ファンまたは温度障害などスイッチに影響する可能性のある外部イベントの起動を行います。

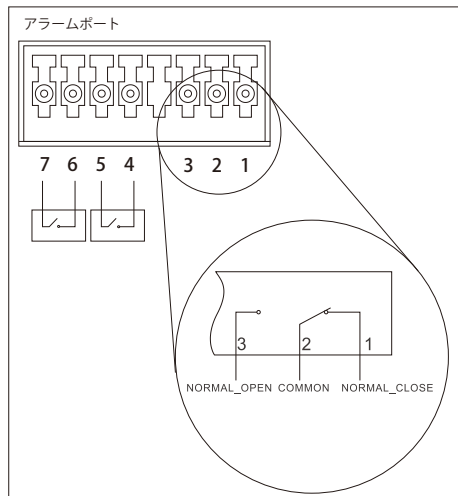


図 1-7 アラームコネクタ

表 アラームコネクタポート

| コンタクト | アラームコネクタポート |
|-------|---------------------------------|
| 1 | 出力、ノーマルクローズピン (42VAC または 60VDC) |
| 2 | 出力、コモピン (42VAC または 60VDC) |
| 3 | 出力、ノーマルオープンピン (42VAC または 60VDC) |
| 4 | 入力 2 |
| 5 | 入力 2 |
| 6 | 入力 1 |
| 7 | 入力 1 |

スイッチのアラーム入力ピンを他のデバイス上のアラーム出力端子に接続してください。
外部デバイスの出力ピンをスイッチのアラーム入力ピンに接続してください。

LED 表示

スイッチの前面パネルには、ギガビットイーサネットポートを含むすべてのポートに Power、Console、RPS、Master（スタック制御）、SD、スタック ID、MGMT および Link/Act の LED があります。DGS-3420-28PC および DGS-3420-52P スイッチは、ポートが PoE モードであるかどうかを示す PoE LED も搭載されています。以下に、スイッチ上の LED の配置と、各 LED の状態が表す意味を示します。

DGS-3420-26SC

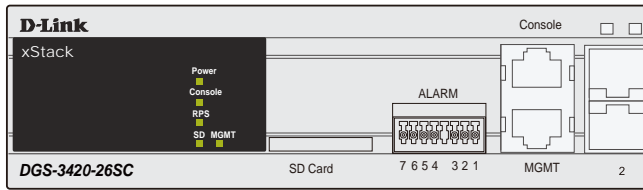


図 1-8 DGS-3420-26SC の前面パネル LED 配置図

DGS-3420-28TC

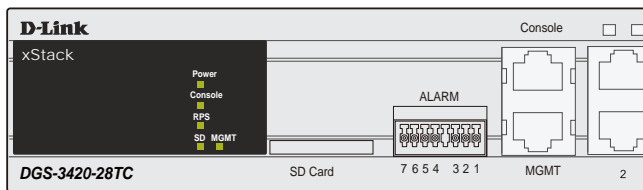


図 1-9 DGS-3420-28TC の前面パネル LED 配置図

DGS-3420-28SC

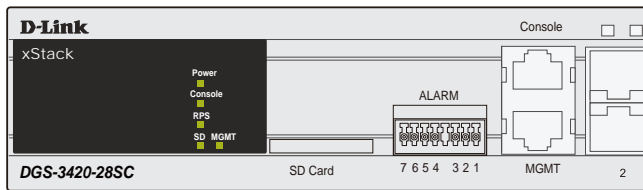


図 1-10 DGS-3420-28SC の前面パネル LED 配置図

DGS-3420-28PC

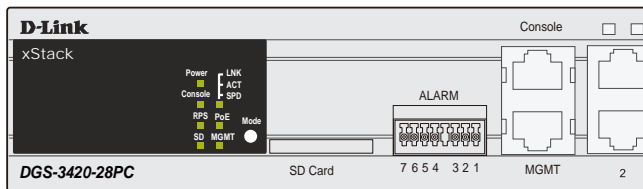


図 1-11 DGS-3420-28PC の前面パネル LED 配置図

DGS-3420-52T

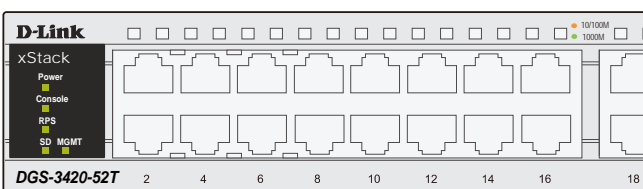


図 1-12 DGS-3420-52T の前面パネル LED 配置図

DGS-3420-52P

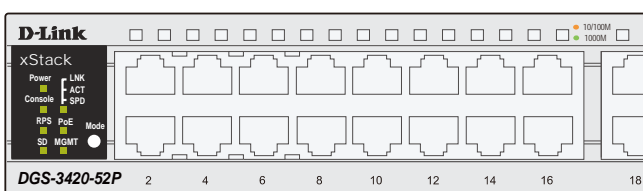


図 1-13 DGS-3420-52P の前面パネル LED 配置図

以下の表に LED の状態が意味するスイッチの状態を示します。

| LED | 色 | 状態 | 状態説明 |
|-------------------------------------|---|----------------------|---|
| システム LED | | | |
| Power | 緑 | 点灯 | スイッチに電源が供給され正常に動作しています。 |
| | — | 消灯 | スイッチに電源が供給されていません。 |
| Console | 緑 | 点滅 | 電源投入後の Power ON Self Test (POST) 中に点滅し、終了すると消灯します。 |
| | | 点灯 | コンソールポートのリンクが確立しています。 |
| MGMT | 緑 | 点滅 | 10/100/1000Mbps でデータを送受信しています。 |
| | | 点灯 | 管理ポートで安全な接続またはリンクが確立しています。 |
| SD | 緑 | 点灯 | SD カードが挿入されています。 |
| | | 点滅 | リード/ライト中です。 |
| | — | 消灯 | SD カードは挿入されていません。 |
| | 橙 | 点灯 | リード/ライトエラー |
| RPS | 緑 | 点灯 | 内蔵電源ユニットの異常により、拡張のリダンダント電源ユニットが動作しています。 |
| | — | 点滅 | RPS ケーブルの接続を検出しています。 |
| | — | 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/SPD (DGS-3420-28PC/52P) | 緑 | 点灯 | Link/ACT/SPD モードを選択中です。 |
| PoE (DGS-3420-28PC/52P) | 緑 | 点灯 | PoE モードを選択中です。 |
| スタック ID LED | 緑 | 1-12、 H、h、G 表示 | <p>スタンドアロンスイッチでは「1」を表示します。スタックスイッチでは、スタックしているボックス ID の位置を示します。ユーザ (static モード) またはシステム (automatic モード) によってボックス ID は割り当てられます。</p> <ul style="list-style-type: none"> 「1」から「12」を表示する場合、これは、スイッチのスタック位置を示します。 「H」は、デバイスがスタックマスタとして割り当てられたことを示します。 「h」は、デバイスがバックアップマスタとして選択されたことを意味します。 「G」は、セーフガードエンジン機能が「exhausted」モードに入っていることを示します。 |
| GE ポート LED | | | |
| Link/ACT/SPD | 緑 | 点灯 | 1000Mbps でリンクが確立しています。 |
| | | 点滅 | 1000Mbps でデータを送受信しています。 |
| | 橙 | 点灯 | 10/100Mbps でリンクが確立しています。 |
| | | 点滅 | 10/100Mbps でデータを送受信しています。 |
| | — | 消灯 | リンクが確立していません。 |
| PoE (DGS-3420-28PC/52P) | 緑 | 点灯 | 接続中の PoE 受電機器に給電中です。 |
| | 橙 | 点灯 | <p>PoE ポートにエラーが発生しました。</p> <p>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 I min 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。</p> |
| | | — | 消灯 |
| SFP スロット LED | | | |
| Link/ACT/SPD | 緑 | 点灯 | 1000Mbps でリンクが確立しています。 |
| | | 点滅 | 1000Mbps でデータを送受信しています。 |
| | 橙 | 点灯 | 100Mbps でリンクが確立しています。 |
| | | 点滅 | 100Mbps でデータを送受信しています。 |
| | — | 消灯 | リンクが確立していません。 |
| SFP+ スロット LED | | | |
| Link/ACT/SPD | 緑 | 点灯 | 10Gbps でリンクが確立しています。 |
| | | 点滅 | 10Gbps でデータを送受信しています。 |
| | 橙 | 点灯 | 1000Mbps でリンクが確立しています。 |
| | | 点滅 | 1000Mbps でデータを送受信しています。 |
| | — | 消灯 | リンクが確立していません。 |

背面パネル

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

DGS-3420-28TC

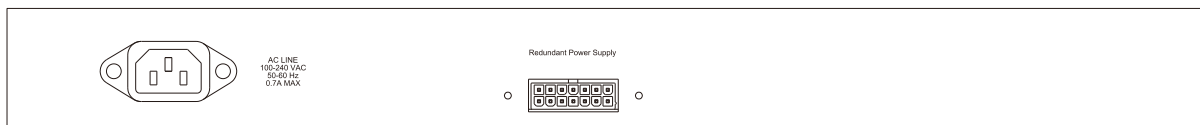


図 1-14 DGS-3420-28TC 背面パネル図

DGS-3420-26SC / 28SC

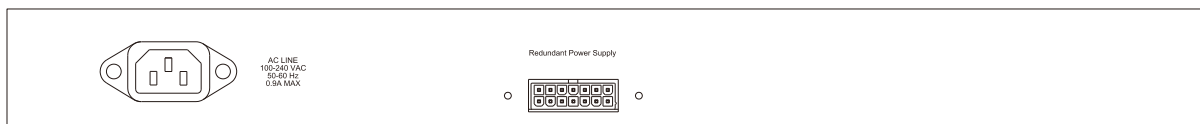


図 1-15 DGS-3420-26SC / 28SC 背面パネル図

DGS-3420-28PC

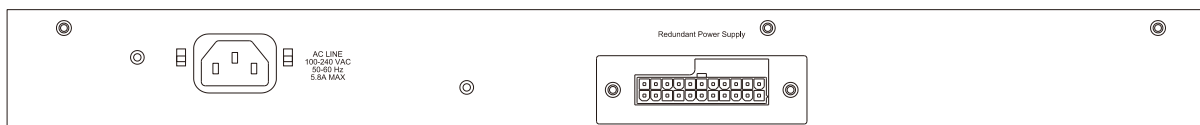


図 1-16 DGS-3420-28PC 背面パネル図

DGS-3420-52T

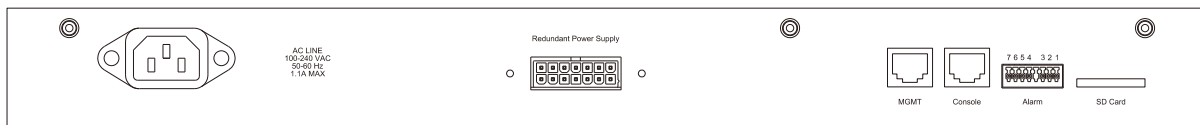


図 1-17 DGS-3420-52T 背面パネル図

DGS-3420-52P

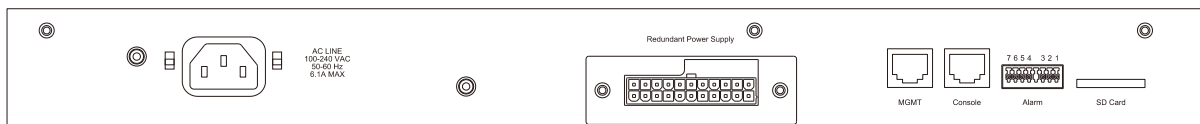


図 1-18 DGS-3420-52P 背面パネル図

電源コネクタは、標準の三極インレットです。このソケット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。オプションの外部リダンダント電源 (DGS-3420-28TC/28SC/26SC/52T には DPS-500 (500A)、DGS-3420-28PC/52P には DPS-700) を上記の RPS コネクタに接続します。内部電源の故障の際に、このオプション外部 RPS は、直ちに自動で全電源を代わりに供給します。

側面パネル

システムのファンと通気口がスイッチにあり内部の熱を放出します。これらをふさがないようにご注意ください。スイッチの適切な通気のためには、少なくとも 16cm 以上のスペースを確保してください。最適な熱放出、空気の循環をしないとシステム障害や部品の激しい損傷を引き起こす場合がありますのでご注意ください。

DGS-3420-28TC / DGS-3420-26SC / DGS-3420-28SC

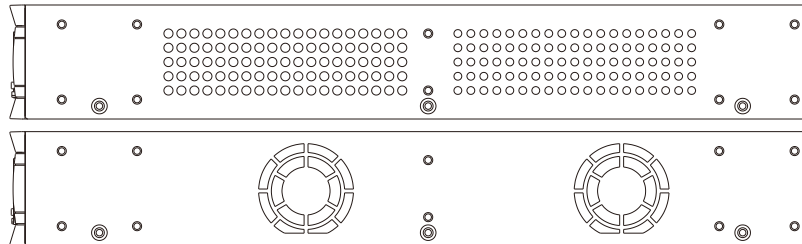


図 1-19 側面パネル図

DGS-3420-52T

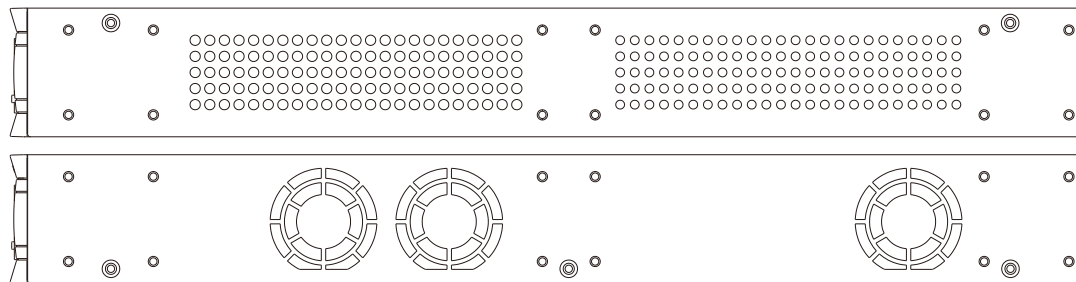


図 1-20 側面パネル図

DGS-3420-28PC / DGS-3420-52P

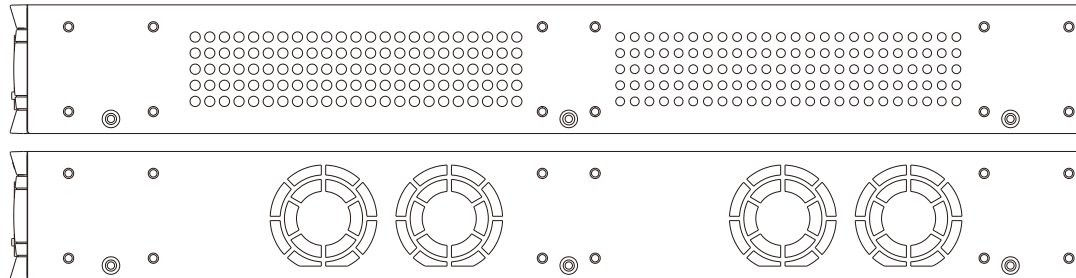


図 1-21 側面パネル図

SFP スロット

スイッチは SFP と SFP+ スロットを搭載しており、光ファイバケーブルに接続するフルデュプレックス転送、オートネゴシエーションをサポートする SFP スロットと共に使用されて、ギガビットネットワークをまたがる各種スイッチにアップリンクすることができます。SFP スロットは最大 1Gbps、SFP+ スロットは最大 10Gbps の転送速度をサポートしています。

以下に、スイッチに SFP スロットモジュールを挿入した例を図に示します。

注意

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

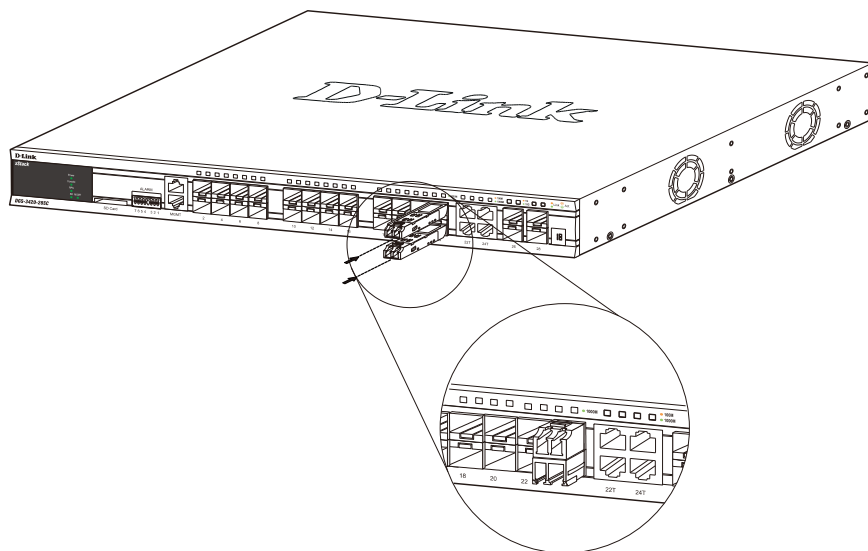


図 1-22 DGS-3420 シリーズ前面パネルの SFP スロットへのモジュールの挿入

第2章 スwitchの設置

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

パッケージの内容

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

- 本体 x 1
- AC 電源ケーブル x 1
- 電源抜け防止金具 x 1
- ラックマウントキット 1 式 (ブラケット 2 枚、ネジ)
- ゴム足 (貼り付けタイプ) x 4
- CD-ROM
- RS-232C/RJ-45 コンソールケーブル
- クイックインストールガイド
- シリアルラベル

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

ネットワーク接続前の準備

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

- スイッチは、しっかりとした水平面で耐荷重性のある場所に設置してください。また、スイッチの上に重いものを置かないでください。
- 本スイッチから 1.82m 以内の電源コンセントを使用してください。
- 電源ケーブルが AC/DC 電源ポートにしっかりと差し込まれているか確認してください。
- 本スイッチの周辺で熱の放出と十分な換気ができることを確認してください。換気のためには少なくとも製品の前後 16cm 以上の空間を保つようにしてください。
- スイッチは動作環境範囲内の温度と湿度を保つことができる、なるべく涼しくて乾燥した場所に設置してください。
- スイッチは強い電磁場が発生するような場所 (モータの周囲など) や、振動、ほこり、および直射日光を避けて設置してください。
- スイッチを水平面に設置する際は、スイッチ底面に同梱のゴム足を取り付けてください。ゴム製の足はスイッチのクッションの役割を果たし、筐体自体や他の機器に傷がつくのを防止します。

ゴム足の取り付け (19 インチラックに設置しない場合)

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

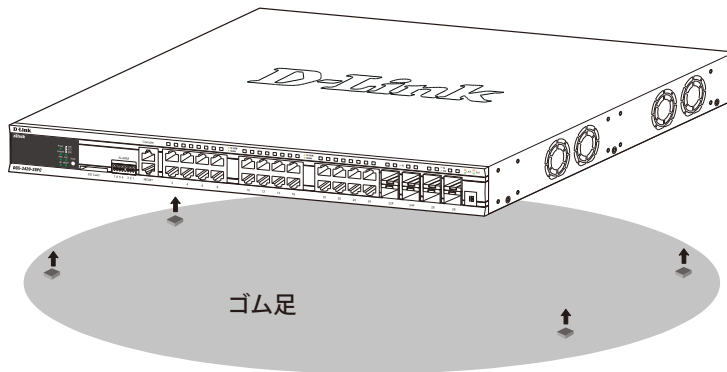


図 2-1 机や棚の上に設置する場合の準備

19 インチラックへの取り付け

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

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

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

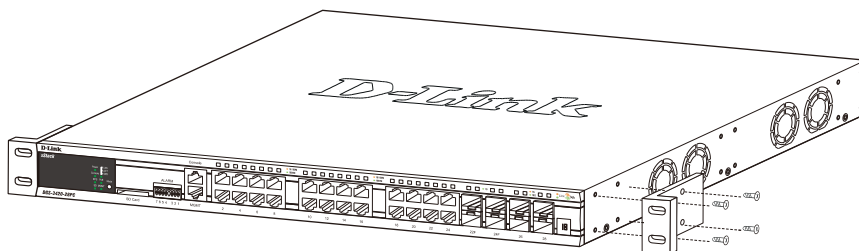


図 2-2 スイッチへのブラケットの取り付け図

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

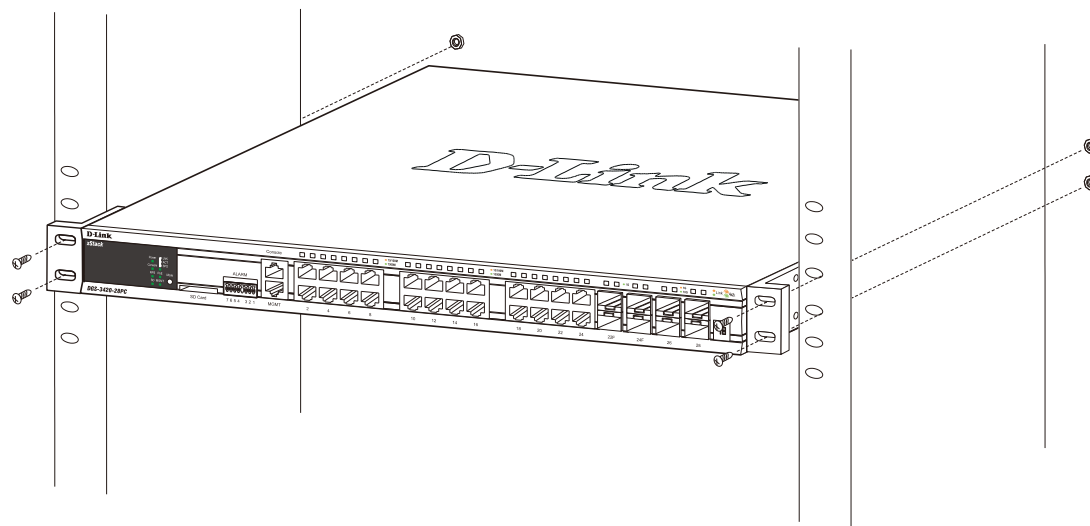


図 2-3 スwitchのラックへの設置図

電源の投入 (AC 電源)

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

電源の異常

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

リダンダント電源システムの設置

スイッチは外付けのリダンダント電源システム（RPS）をサポートしています。DPS-500 は DGS-3420-26SC、DGS-3420-28TC、DGS-3420-28SC、および DGS-3420-52T に、DPS-700 は DGS-3420-28PC および DGS-3420-52P に必要な電力を供給するリダンダント電源ユニットです。DPS-500 は DPS-800 に取り付けることができます。

本スイッチへリダンダント電源ユニットを接続する手順は以下の通りです。

警告 DPS-500 および DPS-700 の設置を行う前に、スイッチの AC 電源ケーブルを抜いておいてください。また、はじめに必ず電源ケーブルとコネクタの仕様書および設定手順をご確認ください。

警告 フロントおよびサイドのスタビライザを装着せずにシステムをラックに搭載すると、ラックが倒れ、人身事故を引き起こす場合があります。ラックにシステムの搭載を行う前には、必ずスタビライザを装着してください。ラックにシステム / コンポーネントを搭載した後は、一度にスライド・アセンブリに掛けて引き出すコンポーネントは 1 つのみとしてください。2 つ以上のコンポーネントが引き出されると、ラックがバランスを失い、倒れて重大な事故につながる恐れがあります。

DPS-500

DPS-500 は DGS-3420-26SC、DGS-3420-28TC、DGS-3420-28SC、および DGS-3420-52T に対応しています。DPS-500 のマスタスイッチへの接続は、14 ピンの DC 電源ケーブルを使用して行います。標準の三極の AC 電源ケーブルでリダンダント電源装置とメイン電源を接続します。

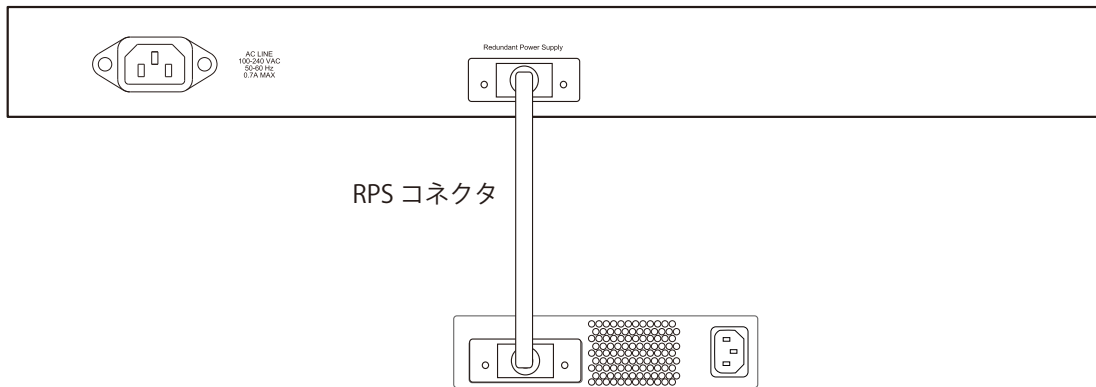


図 2-4 DGS-3420-28TC と DPS-500 RPS の接続

1. 14 ピン DC 電源ケーブルの一端をスイッチのソケットに挿入し、もう一端をリダンダント電源装置に挿入します。
2. 標準の AC 電源ケーブルでリダンダント電源装置とメインの AC 電源を接続します。DPS-500 前面の緑の LED 点灯により、正しく接続が行われたことが確認できます。
3. スイッチを再び AC 電源に接続します。RPS LED が点灯してリダンダント電源が動作していることを確認できます。
4. 本手順の実行による設定変更は必要ありません。

警告 DGS-3420-26SC、DGS-3420-28TC、DGS-3420-28SC、および DGS-3420-52T を DPS-500 以外のリダンダント電源ユニットに使用しないでください。

注意 さらに詳細な情報については DPS-500 のマニュアルをご参照ください。

DPS-800

DPS-800 は標準サイズのラックマウント（1.5U サイズ）です。2 台までの DPS-500 を収容できます。

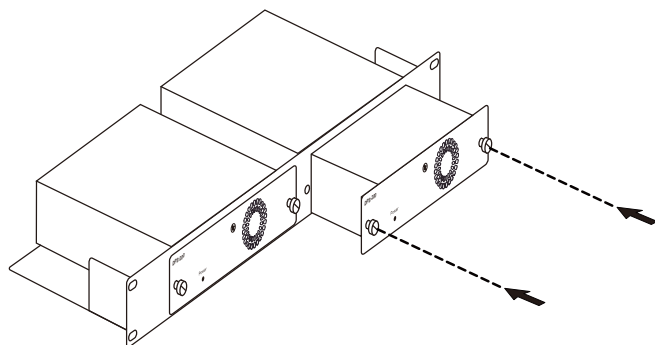


図 2-9 DPS-500 を DPS-800 に取り付ける

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

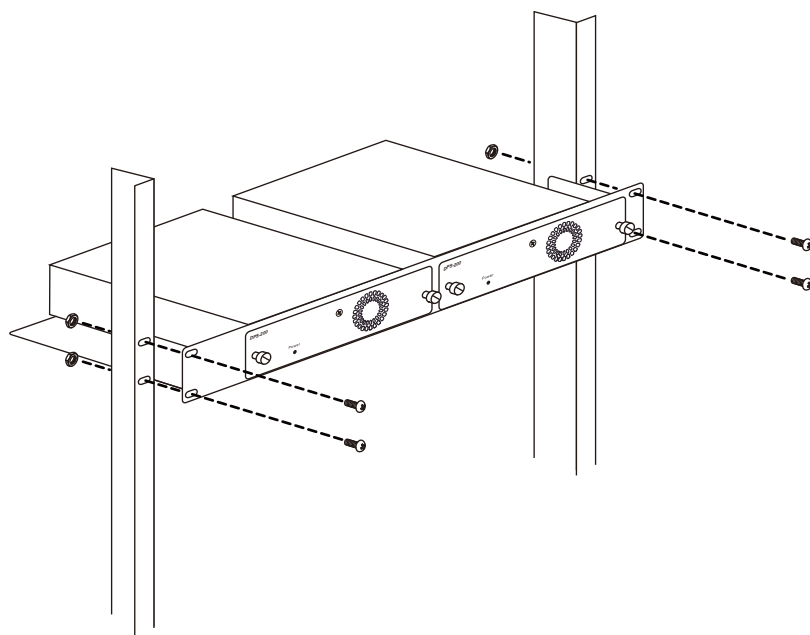


図 2-10 DPS-800 をラックに取り付ける

DPS-700

DGS-3420-28PC および DGS-3420-52P は DPS-700 外部リダント電源ユニットに対応しています。

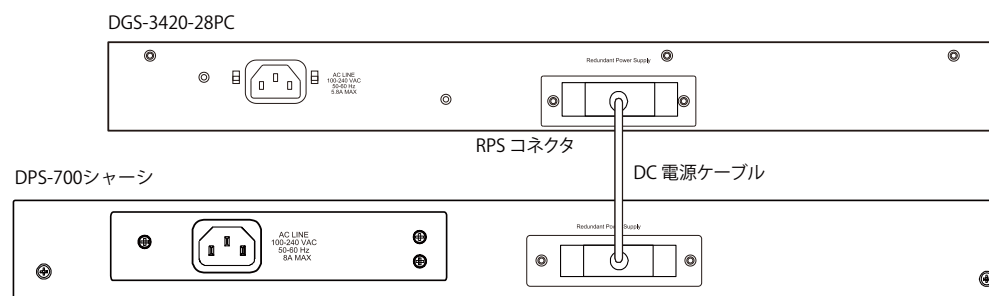


図 2-15 DPS-700 と DGS-3420-28PC の接続

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

警告 DGS-3420-28PC および DGS-3420-52P を DPS-700 以外のリダント電源ユニットに使用しないでください。

第3章 スwitchの接続

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

注意 すべてのポートは Auto MDI/MDI-X 接続をサポートしています。

エンドノードと接続する

本スイッチの 1000BASE-T ポートとエンドノードをカテゴリ 3、4、5 の UTP/STP ケーブルを使用して接続します。エンドノードとは、RJ-45 コネクタ対応 10/100/1000Mbps ネットワークインタフェースカードを装備した PC やルータを指しています。エンドノードとスイッチ間はカテゴリ 3、4、または 5 の UTP ケーブルで接続できます。エンドノードへの接続はスイッチ上のすべてのポートから行えます。

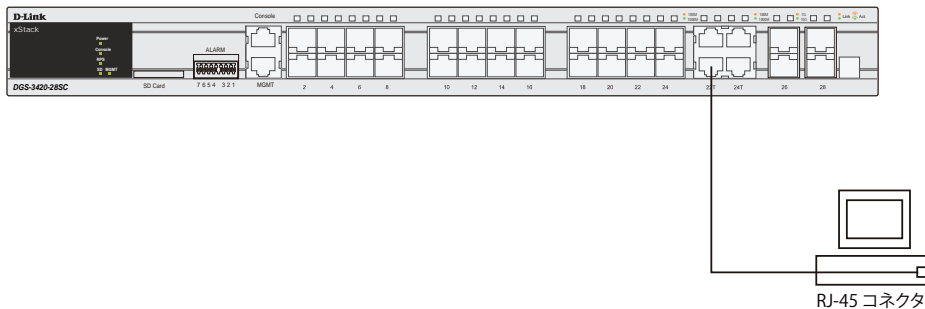


図 3-1 エンドノードと接続した図

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

ハブまたはスイッチと接続する

使用するケーブルによって以下のように接続します。

- ・ カテゴリ 3 以上の UTP ケーブル：10BASE-T ハブまたはスイッチと接続する。
- ・ カテゴリ 5 以上の UTP ケーブル：100BASE-TX ハブまたはスイッチと接続する。
- ・ エンハンストカテゴリ 5 以上の UTP ケーブル：1000BASE-T スイッチと接続する。
- ・ 光ファイバケーブル：SFP ポート経由で光ファイバをサポートするスイッチにアップリンクする。

ケーブル仕様については「[付録 A ケーブルとコネクタ](#)」(437 ページ) を参照してください。

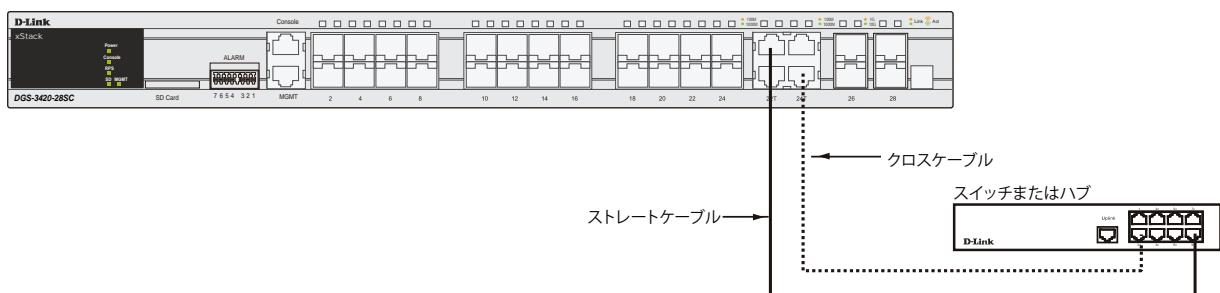


図 3-2 ストレート、クロスケーブルでハブまたはスイッチと接続する図

バックボーンまたはサーバと接続する

SFP ポートと 1000BASE-T ポートは、ネットワークバックボーンやサーバとのアップリンク接続に適しています。RJ-45 ポートは、全二重モード時において 10/100/1000Mbps の速度を提供し、SFP ポートは、全二重モード時において 100Mbps または 1000Mbps の速度を提供します。

ギガビットイーサネットポートとの接続はポートのタイプによって光ファイバケーブルまたはエンハンスドカテゴリ 5 ケーブルを使用します。正しくリンクが確立すると Link LED が点灯します。

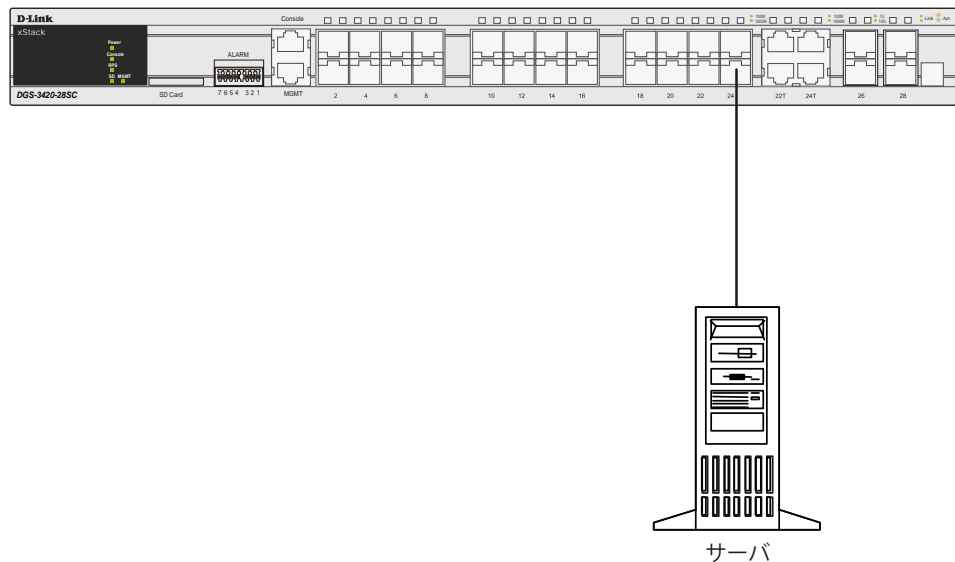


図 3-3 サーバ、PC、スイッチスタックとのアップリンク接続図

第4章 スイッチ管理の導入

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

管理オプション

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

- Web ベースの管理インタフェース
本スイッチの設置完了後、Microsoft® Internet Explorer (バージョン 7 以降)、Mozilla Firefox (2.0 以降)、Safari (4.0 以降)、および Google Chrome (6.0 以降) などの Web ブラウザを使用してによって本スイッチの設定、LED のモニタ、および統計情報をグラフィカルに表示することができます。
- SNMP ベースの管理
SNMP をサポートするコンソールプログラムでスイッチの管理をすることができます。本スイッチは SNMP v1、v2c、および v3 をサポートしています。SNMP エージェントは、受信した SNMP メッセージを復号化し、マネージャからの要求に対してデータベースに保存された MIB オブジェクトを参照して応答を返します。SNMP エージェントは MIB オブジェクトを更新し、統計情報およびカウンタ情報を生成します。
- シリアルポートまたはリモートの Telnet 経由によるコマンドラインインタフェース管理
スイッチのモニタリングと設定のために RJ-45 シリアルポートを搭載しています。
コンソールポートを使用するためには以下をご用意ください。
 - ターミナルソフトを操作するシリアルポート搭載の端末またはコンピュータ
 - 同梱のコンソールケーブル (D-Sub9 ピン オスコネクタ / RJ-45 コネクタ) を使用して接続します。

端末をコンソールポートに接続する

1. 本製品付属の RS-232C ケーブルの RJ-45 コネクタをスイッチの RJ-45 コンソールポートに接続します。
2. ケーブルのもう一方を端末またはターミナルソフトが動作するコンピュータのシリアルコネクタに接続します。以下の手順でターミナルソフトを設定します。
3. 「接続の設定」画面の「接続方法」で、適切なシリアルポート (COM ポート) を選択します。
4. 選択したポートの「プロパティ」画面で「115200」ビット / 秒にデータ速度を設定します。
5. 「データビット」は「8」、「ストップビット」は「1」、「パリティ」は「なし」に設定します。
6. 「フロー制御」は「なし」に設定します。
7. 「エミュレーションモード」を「VT100」に設定します。
8. 「ファンクションキー」、「方向キー」、「Ctrl キー」の使い方で「ターミナルキー」を選択します。「ターミナルキー」(Windows キーではない) の選択を確認します。

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

9. 端末設定の完了後、本スイッチに電源ケーブルを接続し、電源プラグをコンセントに接続します。端末でブートシーケンスが始まります。
10. ブートシーケンスが完了すると、コンソールのログイン画面が表示されます。
11. 購入後はじめてログインする場合は、ユーザ名 (UserName) とパスワード (PassWord) プロンプトで Enter キーを押します。本スイッチには、ユーザ名 (UserName) とパスワード (PassWord) の初期値はありません。はじめに、管理者によるユーザ名 (UserName) とパスワード (PassWord) の作成が必要です。既にユーザアカウントを作成している場合は、ログインし、続けて本スイッチの設定をします。
12. コマンドを入力して設定を行います。コマンドの多くは管理者レベルのアクセス権が必要です。次のセクションでユーザアカウントの設定について説明します。CLI のすべてのコマンドリストおよび追加情報については、製品付属 CD-ROM に収録された「[DGS-3420 Series CLI Reference Guide](#)」を参照してください。
13. 管理プログラムを終了する場合は、logout コマンドを使用するか、ターミナルソフトを終了します。
14. 接続する端末または PC が以上の通り設定されたことを確認してください。

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

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

```

Boot Procedure                                     V1.00.003
-----
Power On Self Test ..... 100 %

MAC Address   : 00-01-02-03-04-00
H/W Version  : B1

Please Wait, Loading V1.50.010 Runtime Image ..... 100 %
UART init ..... 100 %
Starting runtime image
Device Discovery ..... 100 %
Configuration init ..... 100 %
    
```

図 4-1 コンソールのブート画面

スイッチへの初回接続

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

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

スイッチに初めて接続すると、次のログイン画面が表示されます。

```

DGS-3420-28SC Gigabit Ethernet Switch
Command Line Interface

Firmware: Build 1.50.010
Copyright (C) 2013 D-Link Corporation. All rights reserved.

UserName:
    
```

図 4-2 コマンドプロンプト

初回接続する場合、「UserName」または「PassWord」は登録されていません。「UserName」と「PassWord」には何も入力せず、「Enter」キーを押します。既に設定されている場合は、「UserName」と「PassWord」の両方を入力します。「DGS-3420-28xx:admin#」というコマンドプロンプトが表示されます。

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

管理ポートへの接続

スイッチの前面パネルには Out-of-Band（帯域外）管理ポートがあります。ポートは、標準的なイーサネットケーブルを使用してノート PC に簡単に接続可能な RJ-45 ポートです。Web ブラウザまたは Telnet コマンドプロンプトインターフェイスを使用して、Out-of-Band 管理を行うポートに接続します。管理ポートは初期値で有効であるため、初めてスイッチに接続するために使用することができます。

管理ポートを使用するためには、イーサネットケーブルを使用してスイッチ管理に使用するコンピュータのイーサネットインターフェイスにポートを接続します。IP アドレスの初期値は 192.168.0.1 で、サブネットマスクは 255.255.255.0 です。スイッチ管理に使用するコンピュータが、192.168.0.x サブネットで重複しない IP アドレスを持っていることを確認してください。

コンソールポート、または Web ベースのスイッチ管理インターフェイスを通じて IP 設定または管理ポートのステータスを変更することができます。管理ポートの設定を変更するためには、以下のコマンドを使用します。:

```
config out_band_ipif {ipaddress <network_address> | state [enable | disable] | gateway <ipaddr>}
```

IP 設定のステータスを参照するためには、以下のコマンドを使用します。

```
show out_band_ipif
```

Web インタフェースにおける Out-of-Band 管理ポートの設定を変更するためには、**Management > Out of Band Management Settings** メニューを使用します。

パスワード設定

本スイッチは、初期値としてユーザ名およびパスワードの設定はありません。はじめにユーザアカウントの作成を行います。定義済みの管理者レベルのユーザ名でログインすることでスイッチ管理ソフトウェアに接続できます。

はじめてログインした際に本スイッチに対する不正アクセスを防ぐためにユーザ名に対して必ず新しいパスワードを定義してください。このパスワードは忘れないように記録しておいてください。

管理者レベルのアカウントを作成する手順は以下の通りです。

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

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

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

```
DGS-3420-28SC:admin# create account admin newmanager
Command: create account admin newmanager

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

DGS-3420-28SC:admin#
```

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

IP アドレスの割り当て

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

本スイッチの IP アドレスの初期値は 10.90.90.90 です。

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

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

```
DGS-3420-28SC:admin#show switch
Command: show switch

Device Type           : DGS-3420-28SC Gigabit Ethernet Switch
MAC Address           : 00-01-02-03-04-00
IP Address             : 10.90.90.90 (Manual)
VLAN Name              : default
Subnet Mask            : 255.0.0.0
Default Gateway        : 0.0.0.0
Boot PROM Version     : Build 1.00.003
Firmware Version      : Build 1.50.010
Hardware Version      : B1
System Name           :
System Location        :
System Uptime          : 0 days, 0 hours, 21 minutes, 21 seconds
System Contact         :
Spanning Tree          : Disabled
GVRP                   : Disabled
IGMP Snooping         : Disabled
MLD Snooping          : Disabled
RIP                    : Disabled
RIPng                  : Disabled
VLAN Trunk             : Disabled
Telnet                 : Enabled (TCP 23)
Web                    : Enabled (TCP 80)
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

図 4-3 show switch コマンドによる表示画面

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

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

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

コマンドラインプロンプトの後に、以下のコマンドを入力します。

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

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

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

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

```
DGS-3420-28SC:admin# config ipif System ipaddress 10.90.90.91/255.0.0.0
Command: config ipif System ipaddress 10.90.90.91/8

Success.

DGS-3420-28SC:admin#
```

図 4-4 スイッチへの IP アドレス割り当て時の表示画面

上記例では、スイッチに IP アドレス「10.90.90.91」とサブネットマスク「255.0.0.0」を割り当てています。CIDR 表記（10.90.90.91/8）でのアドレス指定も可能です。「Success.」というメッセージにより、コマンドの実行が成功したことが確認できます。スイッチのアドレス設定が終了すると、Telnet での CLI、または Web ベースによる管理を開始することができます。

SNMP 設定

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

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

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

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

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

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

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

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

個別のユーザや SNMP マネージャグループに SNMP バージョン 3 を使用すると、特定の SNMP 管理機能を許可または制限できるようになります。そのような管理機能の可否は、各 MIB に関連付けられる OID (Object Identifier) を使用して定義します。SNMP バージョン 3 では SNMP メッセージを暗号化することにより、さらに強固なセキュリティを実現できます。スイッチでの SNMP バージョン 3 の設定方法については [75 ページ「System IP Address Settings \(IP アドレス設定\)」](#) をご参照ください。

トラップ

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

MIB

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

第5章 Webベースのスイッチ管理

- Webベースの管理について
- Webマネージャへのログイン
- Webベースのユーザインタフェース
- ユーザインタフェースの各エリア
- Webページの構成

Webベースの管理について

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

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

Webマネージャへのログイン

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

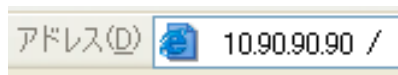


図 5-1 URL の入力

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

以下のユーザ認証画面が表示されます。

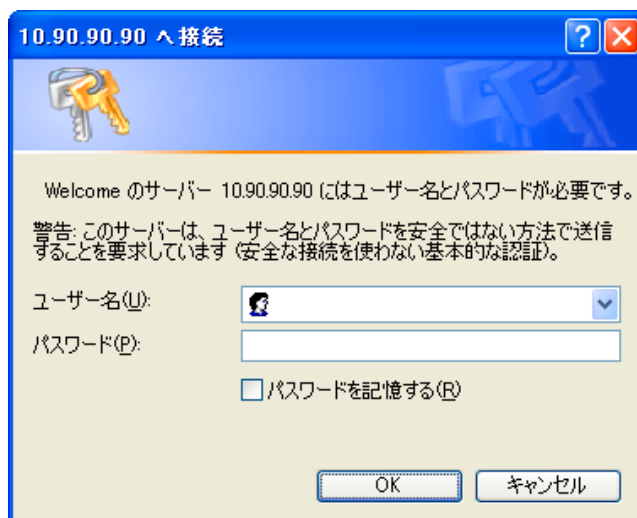


図 5-2 パスワード入力用画面

「ユーザー名」欄と「パスワード」欄を空白のまま「OK」をクリックし、Webベースユーザインタフェースに接続します。Webブラウザによって使用可能な機能を以下で説明します。

CLIでユーザ名、パスワードを既に設定している場合は、設定したパラメータを入力します。

Web マネージャの画面構成

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

Web マネージャのメイン画面について

Web マネージャのメイン画面は3つのエリアで構成されています。

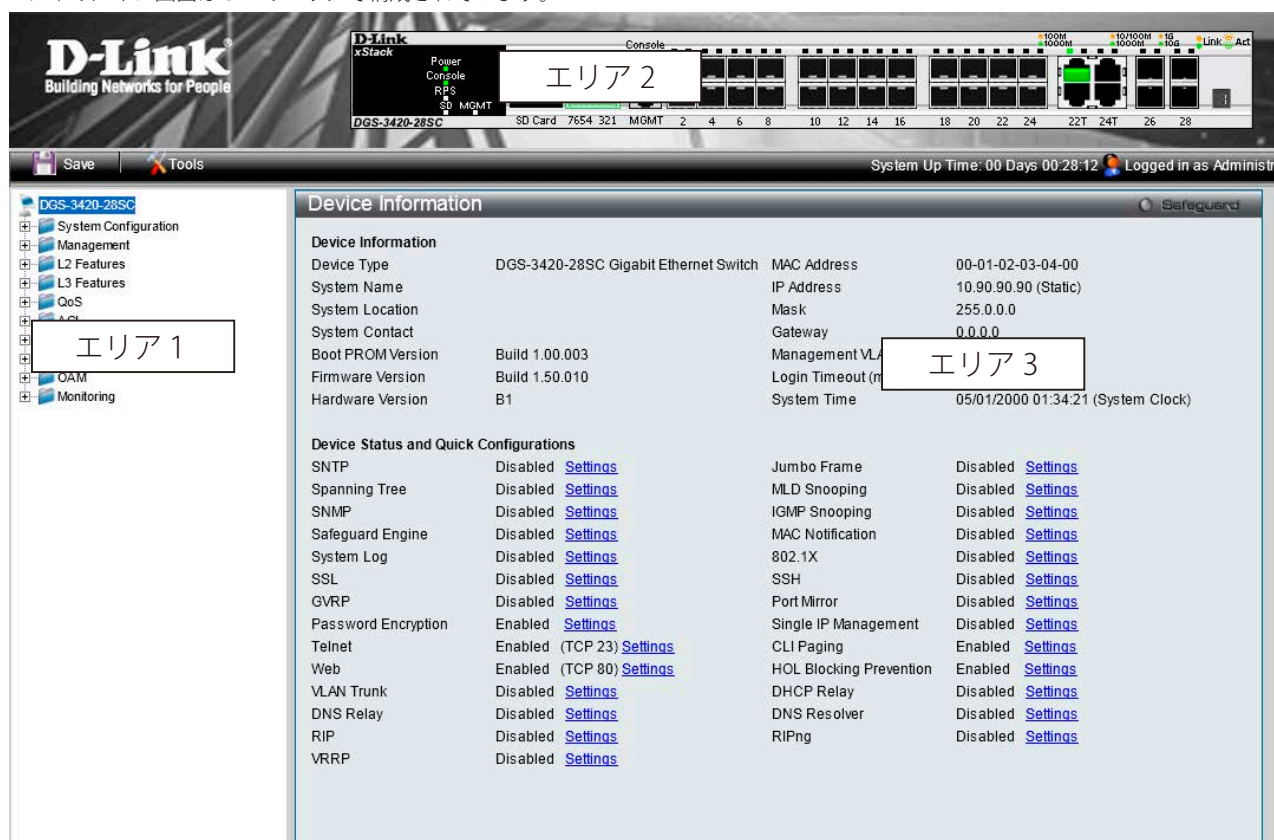


図 5-3 Web マネージャのメインページ

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

注意

現在のセッション中にスイッチのコンフィグレーションに行った変更は、「Save Configuration / Log」画面またはコマンドラインインタフェース (CLI) の「save」コマンドにて保存する必要があります。

Web マネージャのメニュー構成

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

| メインメニュー | サブメニュー | 説明 | 参照ページ |
|----------------------|--|---|---------------------|
| System Configuration | Device Information | スイッチの主な設定情報を表示します。 | 48 |
| | System Information Settings | スイッチの基本情報を表示します。 | 50 |
| | Port Configuration Settings | ポート設定、ジャンボフレーム設定などを行います。 | 51 |
| | PoE Configuration (DGS-3420-28PC/52P のみ) | PoE システムの設定を行います。 | 59 |
| | Serial Port Settings | ボーレートの値と自動ログアウト時間を調整します。 | 62 |
| | Warning Temperature Settings | システムの警告温度パラメータを設定します。 | 62 |
| | System Log Configuration | フラッシュメモリにスイッチのログを保存する方法、Syslog サーバの設定を行います。 | 63 |
| | Time Range Settings | アクセスプロファイル機能を実行する期間を決定します。 | 66 |
| | Port Group Settings | ポートグループを作成します。 | 67 |
| | Time Settings | スイッチに時刻を設定します。 | 67 |
| | User Accounts Settings | ユーザおよびユーザの権限を設定します。 | 68 |
| | Command Logging Settings | コマンドログ設定を有効または無効にします。 | 69 |
| | Stacking | 複数のスイッチを1つに結合し、Telnet、Web などのインタフェースから管理します。 | 70 |
| Management | ARP | スタティック ARP、プロキシ ARP、ARP テーブルを設定します。 | 74 |
| | Gratuitous ARP | Gratuitous ARP の設定をします。 | 76 |
| | IPv6 Neighbor Settings | IPv6 Neighbor の設定を行います。 | 77 |
| | IP Interface | スイッチの IP インタフェース設定を行います。 | 78 |
| | Management Settings | CLI ページング、DHCP 自動設定などの管理設定を行います。 | 84 |
| | Out of Band Management Settings | RJ-45 のアウトバンド管理の詳細を設定します。 | 85 |
| | Session Table | スイッチが最後に起動してからの管理セッションを表示します。 | 85 |
| | Single IP Management | シングル IP マネジメント機能を設定します。 | 86 |
| | SNMP Settings | SNMP 設定を行います。 | 95 |
| | Telnet Settings | スイッチに Telnet 設定をします。 | 104 |
| | Web Settings | スイッチに Web ステータスを設定します。 | 104 |
| | Power Saving | リンクダウン状態のポートの電源をオフにしてスイッチへの電力を節約します。 | 105 |
| L2 Features | VLAN | 802.1Q スタティック VLAN 設定を行います。 | 114 |
| | QinQ | Q-in-Q 機能を有効または無効にします。 | 132 |
| | Layer 2 Protocol Tunneling Settings | レイヤ 2 プロトコルトンネリング機能を設定します。 | 137 |
| | Spanning Tree | スパニングツリープロトコルの設定を行います。 | 138 |
| | Link Aggregation | ポートランキング設定を行います。 | 146 |
| | FDB | スタティック FDB、MAC アドレスエイジングタイム、MAC アドレステーブルなどを設定します。 | 149 |
| | L2 Multicast Control | IGMP プロキシ、MLD プロキシ、IGMP Snooping、MLD Snooping の設定を行います。 | 154 |
| | Multicast Filtering | マルチキャストフィルタリングの設定を行います。 | 182 |
| | ERPS Settings | イーサネットリングプロテクション設定を有効にします。 | 191 |
| | LLDP | LLDP 設定を行います。 | 194 |
| | NLB FDB Settings | NLB 機能を設定します。 | 203 |
| PTP | PTP システムを設定します。 | 204 | |

| メインメニュー | サブメニュー | 説明 | 参照ページ |
|-------------|--|---|---------------------|
| L3 Features | IPv4 Static/Default Route Settings | IPv4 スタティック / デフォルトルートの設定を行います。 | 210 |
| | IPv4 Route Table | IPv4 ルーティングテーブルの外部経路情報を参照します。 | 211 |
| | IPv6 Static/Default Route Settings | IPv6 スタティック / デフォルトルートの設定を行います。 | 211 |
| | IPv6 Route Table | IPv6 ルーティングテーブルの外部経路情報を参照します。 | 212 |
| | Policy Route Settings | ポリシーベースルーティングは、指定したデバイスにインターネットへの最適な経路を与えます。 | 213 |
| | IP Forwarding Table | 直接接続するすべての IP 情報を参照します。 | 215 |
| | Route Preference Settings | ルート優先度の設定を行います。 | 215 |
| | Route Redistribution Settings | OSPF または RIP が動作するネットワーク上のルータに OSPF と RIP 間のルーティング情報を再配送する設定を行います。 | 216 |
| | IP Tunnel | IP トンネルを設定します。以下のメニューがあります。 IP Tunnel Settings (IP トンネル設定)、IP Tunnel GRE Settings (IP トンネル GRE 設定) | 217 |
| | RIP | RIP の設定を行います。 | 219 |
| | VRRP | VRRP (Virtual Routing Redundancy Protocol) は、LAN 上の VRRP ルータの 1 つに仮想ルータとしての役割を動的に割り当てる機能です | 226 |
| QoS | 802.1p Settings | ポート単位にプライオリティを割り当てます。 | 229 |
| | Bandwidth Control | 送信と受信のデータレートを制限します。 | 230 |
| | Traffic Control Settings | ストームコントロールの有効 / 無効の設定、およびマルチキャスト、ブロードキャストストームのしきい値を調整します。 | 232 |
| | DSCP | DSCP の設定を行います。 | 234 |
| | HOL Blocking Prevention | HOL ブロッキング防止機能を有効または無効にします。 | 235 |
| | Scheduling Settings | QoS スケジューリングを設定します。 | 235 |
| | WRED | WRED の状態とそのポート設定を行います。 | 237 |
| ACL | ACL Configuration Wizard | ウィザードを使用してアクセスプロファイルとルールを作成します。 | 239 |
| | Access Profile List | パケットヘッダに含まれる情報に基づくパケット転送可否の基準を設定するプロファイルを設定します。 | 241 |
| | CPU Access Profile List | CPU インタフェースフィルタリング機能を設定します。 | 258 |
| | ACL Finder | ACL エントリを検索します。 | 273 |
| | ACL Flow Meter | フローごとの帯域幅制御設定を行います。 | 274 |
| | Egress Access Profile List | フローごとのパケット処理を実行します。 | 278 |
| | Egress ACL Flow Meter | Egress アクセスプロファイルおよびルールに基づいてパケットフローベースのメータリングを設定します。 | 291 |
| Security | 802.1X | 802.1X 認証を設定します。 | 296 |
| | RADIUS | RADIUS サーバの設定を行います。 | 309 |
| | IP-MAC-Port Binding | IP アドレス、MAC アドレスおよびポートを結合し、レイヤ間通信を行います。 | 313 |
| | MAC-based Access Control | MAC アドレス認証機能を設定します。 | 319 |
| | Web-based Access Control | Web ベースアクセスコントロールを設定します。 | 323 |
| | Japanese Web-based Access Control | JWAC の有効化および設定をします。 | 329 |
| | Compound Authentication | コンパウンド認証方式を設定します。 | 334 |
| | IGMP Access Control Settings | 各ポートに IGMP 認証 (IGMP アクセスコントロール) を設定することができます。 | 336 |
| | Port Security | ダイナミックな MAC アドレス学習をロックします。 | 337 |
| | ARP Spoofing Prevention Settings | パケットコンテンツ ACL を使用して、ARP スプーフィング攻撃を防止します。 | 341 |
| | BPDU Attack Protection | ポートに BPDU 防止機能を設定します。 | 342 |
| | Loopback Detection Settings | ループバック検知機能の設定を行います。 | 343 |
| | Traffic Segmentation Settings | ポートのトラフィックフローを制限します。 | 345 |
| | NetBIOS Filtering Setting | NetBIOS フィルタ設定を行います。 | 344 |
| | DHCP Server Screening | 不正な DHCP サーバへのアクセスを拒否します。 | 346 |
| | Access Authentication Control | TACACS+/XTACACS+/RADIUS 認証の設定を行います。 | 349 |
| | SSL Settings | 証明書の設定、暗号スイートの設定を行います。 | 359 |
| | SSH | SSH サーバ、SSH アルゴリズム、SSH ユーザ認証の設定を行います。 | 362 |
| | DoS Attack Prevention Settings | 各 DoS 攻撃に対して防御設定を行います。 | 365 |

| メインメニュー | サブメニュー | 説明 | 参照ページ |
|---------------------|--|---|---------------------|
| Security | Trusted Host Settings | リモートのスイッチ管理用トラストホストを設定します。 | 366 |
| | Safeguard Engine Settings | セーフガードエンジンの設定を行います。 | 367 |
| | SFTP Server Settings | SFTP 機能を設定します。「SFTP over SSH2」はすべてのファイル操作に安全性を提供するセキュアなファイル送信プロトコルです。 | 368 |
| Network Application | DHCP | DHCP リレーの設定を行います。 | 370 |
| | DNS | DNS リレーの設定を行います。 | 389 |
| | DNS Resolver | DNS リゾルバの設定を行います。 | 391 |
| | RCP Server Settings | RCP サーバの設定を行います。 | 393 |
| | SMTP Settings | スイッチのイベントを送信する SMTP サーバを設定します。 | 394 |
| | SNTP | 本製品に時刻設定をします。 | 396 |
| | UDP | UDP 送信先ポートに応じて、特定のブロードキャストをサーバに送信します。 | 399 |
| | Flash File System Settings | フラッシュファイルシステムを利用したファイル操作を行います。 | 401 |
| OAM | CFM | CFM 機能を設定します。 | 405 |
| | Ethernet OAM | ポートにイーサネット OAM モード、イベント、ログを設定します。 | 416 |
| | DULD Settings | ポートにおいて単方向リンク検出の設定および表示を行います。 | 419 |
| | Cable Diagnostics | ケーブル診断を行います。 | 420 |
| Monitoring | Utilization | CPU 使用率、ポートの帯域使用率を表示します。 | 420 |
| | Statistics | パケット統計情報とエラー統計情報を表示します。 | 422 |
| | Mirror | ポートミラーリングの設定を行います。 | 433 |
| | sFlow | sFlow 機能を使用し、データネットワークのトラフィックをモニタリング設定を行います。 | 436 |
| | Ping | IPv4 アドレスまたは IPv6 アドレスに Ping することができます。 | 439 |
| | Trace Route | ネットワーク上のスイッチとホスト間の経路をトレースします。 | 441 |
| | Peripheral | デバイス環境機能はスイッチの内部温度ステータスを表示します。 | 442 |

第 6 章 System Configuration (スイッチの主な設定)

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

| サブメニュー | 説明 | 参照ページ |
|--|---|--------------------|
| Device Information (デバイス情報) | スイッチの主な設定情報を表示します。 | 45 |
| System Information Settings (システム情報設定) | スイッチの基本情報を表示します。 | 47 |
| Port Configuration Settings (ポート設定) | ポート設定、ジャンボフレーム設定などを行います。以下のメニューがあります。 DDM (DDM 設定)、Port Settings (スイッチのポート設定)、Port Description Settings (ポート名設定)、Port Settings (スイッチのポート設定)、Port Description Settings (ポート名設定)、Port Error Disabled (エラーによるポートの無効)、Port Auto Negotiation Information (オートネゴシエーション情報)、Jumbo Frame (ジャンボフレームの有効化) EEE Settings (EEE 設定) | 48 |
| PoE Configuration (PoE 設定) (DGS-3420-28PC/52P のみ) | PoE システムの設定を行います。以下のメニューがあります。 PoE System Settings (PoE システムの設定)、PoE Port Settings (PoE ポート設定) | 56 |
| Serial Port Settings (シリアルポート設定) | ボーレートの値と自動ログアウト時間を調整します。 | 59 |
| Warning Temperature Settings (警告温度設定) | システムの警告温度パラメータを設定します。 | 59 |
| System Log Configuration (システムログ構成) | フラッシュメモリにスイッチのログを保存する方法、Syslog サーバの設定を行います。以下のメニューがあります。 System Log Settings (システムログ設定)、System Log Server Settings (システムログサーバの設定)、System Log (Syslog ログ)、System Log & Trap Settings (Syslog とトラップ設定)、System Severity Settings (システムセベリティ設定) | 60 |
| Time Range Settings (タイムレンジ設定) | アクセスプロファイル機能を実行する期間を決定します。 | 63 |
| Port Group Settings (ポートグループ設定) | ポートグループを作成します。 | 64 |
| Time Settings (時刻設定) | スイッチに時刻を設定します。 | 64 |
| User Accounts Settings (ユーザアカウントの設定) | ユーザおよびユーザの権限を設定します。 | 65 |
| Command Logging Settings (コマンドログ設定) | コマンドログ設定を有効または無効にします。 | 66 |
| Stacking (スタッキング設定) | 複数のスイッチを 1 つに結合し、Telnet、Web などのインタフェースから管理します。以下のメニューがあります。 Stacking Device Table (スタックデバイステーブル)、Stacking Mode Settings (スタックモード設定) | 67 |

Device Information (デバイス情報)

本画面は、ログインを行うと自動的に表示される画面で、スイッチの主な設定情報を確認できます。本画面に戻るためには「DGS-3420 シリーズ」フォルダをクリックします。本画面には、スイッチの「MAC Address」(工場による設定のため変更不可)、「Boot PROM Version」と「Firmware Version」、「Hardware Version」などが表示されます。これらの情報は、PROMやファームウェアの更新状況の把握や他のネットワークデバイスのアドレステーブルにスイッチのMACアドレスを登録する際の確認などに便利です。さらに、スイッチの各機能の状態を表示し、現在のグローバルステータスにアクセス可能です。いくつかの機能は、各設定画面にリンクしており、本画面から接続できます。

| Device Information | | | |
|---|---|-------------------------|------------------------------------|
| Device Information | | | |
| Device Type | DGS-3420-28SC Gigabit Ethernet Switch | MAC Address | 00-01-02-03-04-00 |
| System Name | | IP Address | 10.90.90.90 (Static) |
| System Location | | Mask | 255.0.0.0 |
| System Contact | | Gateway | 0.0.0.0 |
| Boot PROM Version | Build 1.00.003 | Management VLAN | default |
| Firmware Version | Build 1.50.010 | Login Timeout (min) | Never |
| Hardware Version | B1 | System Time | 11/01/2000 20:48:58 (System Clock) |
| Device Status and Quick Configurations | | | |
| SNTP | Disabled Settings | Jumbo Frame | Disabled Settings |
| Spanning Tree | Disabled Settings | MLD Snooping | Disabled Settings |
| SNMP | Disabled Settings | IGMP Snooping | Disabled Settings |
| Safeguard Engine | Disabled Settings | MAC Notification | Disabled Settings |
| System Log | Disabled Settings | 802.1X | Disabled Settings |
| SSL | Disabled Settings | SSH | Disabled Settings |
| GVRP | Disabled Settings | Port Mirror | Disabled Settings |
| Password Encryption | Enabled Settings | Single IP Management | Disabled Settings |
| Telnet | Enabled (TCP 23) Settings | CLI Paging | Enabled Settings |
| Web | Enabled (TCP 80) Settings | HOL Blocking Prevention | Enabled Settings |
| VLAN Trunk | Disabled Settings | DHCP Relay | Disabled Settings |
| DNS Relay | Disabled Settings | DNS Resolver | Disabled Settings |
| RIP | Disabled Settings | RIPng | Disabled Settings |
| VRRP | Disabled Settings | | |

図 6-1 Device Information 画面

画面には以下の項目があります。

| 項目 | 説明 |
|---------------------|---|
| Device Information | |
| Device Type | 工場にて定義した機種名と型式を表示します。 |
| System Name | ユーザが定義したシステム名を表示します。 |
| System Location | システムが現在動作している場所を表示します。(半角英数字 160 文字以内) |
| System Contact | 担当者名を表示します。(半角英数字 31 文字以内) |
| Boot PROM Version | デバイスのブートバージョンを表示します。 |
| Firmware Version | デバイスのファームウェアバージョンを表示します。 |
| Hardware Version | デバイスのハードウェアバージョンを表示します。 |
| Serial Number | デバイスのシリアル番号を表示します。 |
| MAC Address | デバイスに割り当てられた MAC アドレスを表示します。 |
| IP Address | デバイスに割り当てられた IP アドレスを表示します。 |
| Mask | デバイスに割り当てられたサブネットマスクを表示します。 |
| Gateway | デバイスに割り当てられたデフォルトゲートウェイを表示します。 |
| Management VLAN | デバイスに割り当てられた VLAN 名を表示します。 |
| Login Timeout (min) | ユーザが何もしなかった場合にデバイスがタイムアウトするまでの時間を表示します。初期値は 10 (分) です。 |
| System Time | 最後のデバイスリセットからの経過時間を表示します。日、時、分、秒の形式で表示します。 例: 41days 2 hours 22 mins 5 seconds |

System Configuration (スイッチの主な設定)

| 項目 | 説明 |
|--|--|
| Device Status and Quick Configurations | |
| SNTP | SNTP 機能の状態 (有効 / 無効) を表示します。SNTP 設定にリンクします。 |
| Jumbo Frame | Jumbo Frame 機能の状態 (有効 / 無効) の表示と、Jumbo Frame の設定にリンクします。 |
| MLD Snooping | MLD Snooping 機能の状態 (有効 / 無効) の表示と、MLD の設定にリンクします。 |
| IGMP Snooping | IGMP Snooping 機能の状態 (有効 / 無効) の表示と、IGMP の設定にリンクします。 |
| MAC Notification | MAC 通知機能の状態 (有効 / 無効) を表示します。MAC 通知設定にリンクします。 |
| 802.1X | 802.1X 機能の状態 (有効 / 無効) の表示と、802.1X の設定にリンクします。 |
| SSH | SSH (Secure Shell Protocol) 機能の状態 (有効 / 無効) の表示と、SSH の設定にリンクします。 |
| Port Mirror | ポートミラーリング機能の状態 (有効 / 無効) の表示と、ポートミラーリングの設定にリンクします。 |
| Single IP Management | SIM 機能の状態 (有効 / 無効) を表示します。SIM 設定にリンクします。 |
| CLI Paging | CLI ページング機能を有効 / 無効にします。CLI ページングの設定にリンクします。 |
| HOL Blocking Prevention | HOL ブロッキング防止機能を有効または無効にします。HOL ブロッキング防止機能の設定にリンクします。 |
| DHCP Relay | DHCP リレー機能を有効または無効にします。DHCP リレー機能の設定にリンクします。 |
| DNS Resolver | DNS リゾルバ機能を有効または無効にします。DNS リゾルバ機能の設定にリンクします。 |
| RIPng | RIPng 機能を有効 / 無効にします。RIPng の設定にリンクします。 |
| Spanning Tree | STP 機能の状態 (有効 / 無効) を表示します。STP 設定にリンクします。 |
| SNMP | SNMP 機能の状態 (有効 / 無効) を表示します。SNMP 設定にリンクします。 |
| Safeguard Engine | Safeguard エンジン機能の状態 (有効 / 無効) の表示と、Safeguard エンジンの設定にリンクします。 |
| System Log | Syslog 機能をグローバルに有効 / 無効にします。初期値は無効です。Syslog の設定にリンクします。 |
| SSL | SSL (Secure Socket Layer) 機能の状態 (有効 / 無効) の表示と、SSL の設定にリンクします。 |
| GVRP | GVRP (Group VLAN Registration Protocol) 機能の状態 (有効 / 無効) の表示と、GVRP の設定にリンクします。 |
| Password Encryption | パスワードの暗号化機能を有効 / 無効にします。パスワードの設定にリンクします。 |
| Telnet | Telnet 機能の状態 (有効 / 無効) の表示と、Telnet 設定にリンクします。 |
| Web | Web ベースの管理機能を有効 / 無効にします。Web ベースの管理は初期値で有効になっています。無効に設定し、システムに適用すると、Web インタフェースによるシステム設定は行えなくなります。Web ベースの設定にリンクします。 |
| VLAN Trunk | VLAN トランク機能を有効 / 無効にします。VLAN トランクの設定にリンクします。 |
| DNS Relay | DNS リレー機能を有効 / 無効にします。DNS リレーの設定にリンクします。 |
| RIP | RIP 機能を有効または無効にします。RIP 機能の設定にリンクします。 |

デバイスの機能設定の参照手順

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

System Information Settings (システム情報設定)

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

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

図 6-2 System Information Settings 画面

画面には次の項目があります。

| 項目 | 説明 |
|------------------|--|
| Unit ID | デバイスのユニット番号を表示します。 |
| MAC Address | デバイスに割り当てられた MAC アドレスを表示します。 |
| Firmware Version | スイッチのファームウェアバージョンを表示します。 |
| Hardware Version | スイッチのハードウェアバージョンを表示します。 |
| System Name | ユーザが定義するシステム名を設定します。 |
| System Location | システムが現在動作している場所を定義します。(半角英数字 160 文字以内) |
| System Contact | スイッチの管理者情報を入力します。 |

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

Port Configuration (ポート設定)

DDM (DDM 設定)

本フォルダにはスイッチに Digital Diagnostic Monitoring (DDM) 機能を実行する画面があります。これらの画面により、スイッチに挿入した SFP モジュールの DDM 状態の参照、各種設定 (アラーム設定、警告設定、温度しきい値設定、電圧しきい値設定、バイアス電流しきい値設定、Tx (送信) 電力しきい値設定、および Rx (受信) 電力しきい値設定) を行うことができます。

DDM Settings (DDM 設定)

超過しているアラームしきい値または警告しきい値を超過するイベントが発生した場合に、指定ポートに行う動作を設定します。

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

図 6-3 DDM Settings 画面

以下の項目を使用して設定します。

| 項目 | 説明 |
|----------------|--|
| Trap State | SFP ポートにおけるトラップを「Enabled」(有効) / 「Disabled」(無効) にします。 |
| Log State | SFP ポートにおけるログ出力を「Enabled」(有効) / 「Disabled」(無効) にします。 |
| Power Unit | 使用する電力の単位を指定します。「mW」「dBm」から指定できます。 |
| Unit | 設定するユニット番号を指定します。 |
| From / To Port | 適用するポートまたはポート範囲を指定します。 |
| State | 指定したポートまたはポート範囲を「Enabled」(有効) / 「Disabled」(無効) にします。初期値は「Enabled」です。 |
| Shutdown | シャットダウンした場合の通知をアクション (Alarm、Warning、None) を選択します。 |

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

DDM Temperature Threshold Settings (DDM 温度しきい値設定)

スイッチの特定ポートに DDM 温度しきい値設定を行います。

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

図 6-4 DDM Temperature Threshold Settings 画面

以下の項目を使用して設定します。

| 項目 | 説明 |
|----------------|------------------------|
| Unit | 設定するユニット番号を指定します。 |
| From / To Port | 適用するポートまたはポート範囲を指定します。 |

| 項目 | 説明 |
|--------------------------------|---|
| High Alarm (-128-127.996) | アラーム温度の上限を指定します。操作パラメータが本値より高くなると、アラームに関連するアクションが行われます。 |
| Low Alarm (-128-127.996) | アラーム温度の下限を指定します。操作パラメータが本値より低くなると、アラームに関連するアクションが行われます。 |
| High Warning (-128-127.996) | 警告温度の上限を指定します。操作パラメータが本値より高くなると、警告に関連するアクションが行われます。 |
| Low Warning (-128-127.996) | 警告温度の下限を指定します。操作パラメータが本値より低くなると、警告に関連するアクションが行われます。 |

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

DDM Voltage Threshold Settings (DDM 電圧しきい値設定)

スイッチの特定ポートに電圧しきい値を設定します。

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

The screenshot shows the 'DDM Voltage Threshold Settings' interface. At the top, there are dropdown menus for 'Unit' (set to 1), 'From Port' (set to 21), and 'To Port' (set to 21). To the right are four input fields for 'High Alarm (0-6.55)', 'Low Alarm (0-6.55)', 'High Warning (0-6.55)', and 'Low Warning (0-6.55)', each followed by a 'Volt' label and an 'Apply' button. Below this is a table with the following structure:

| Port | High Alarm (Volt) | Low Alarm (Volt) | High Warning (Volt) | Low Warning (Volt) |
|------|-------------------|------------------|---------------------|--------------------|
| 1:21 | - | - | - | - |
| 1:22 | - | - | - | - |
| 1:23 | - | - | - | - |
| 1:24 | - | - | - | - |
| 1:25 | - | - | - | - |
| 1:26 | - | - | - | - |

図 6-5 DDM Voltage Threshold Settings 画面

以下の項目を使用して設定します。

| 項目 | 説明 |
|----------------------------|---|
| Unit | 設定するユニット番号を指定します。 |
| From / To Port | 適用するポートまたはポート範囲を指定します。 |
| High Alarm (0-6.5535) | アラーム電圧の上限を指定します。操作パラメータが本値より高くなると、アラームに関連するアクションが行われます。 |
| Low Alarm (0-6.5535) | アラーム電圧の下限を指定します。操作パラメータが本値より低くなると、アラームに関連するアクションが行われます。 |
| High Warning (0-6.5535) | 警告電圧の上限を指定します。操作パラメータが本値より高くなると、警告に関連するアクションが行われます。 |
| Low Warning (0-6.5535) | 警告電圧の下限を指定します。操作パラメータが本値より低くなると、警告に関連するアクションが行われます。 |

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

DDM Bias Current Threshold Settings (DDM バイアス電流しきい値設定)

スイッチの特定ポートにバイアス電流しきい値を設定します。

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

| Unit | From Port | To Port | High Alarm (0-131) | Low Alarm (0-131) | High Warning (0-131) | Low Warning (0-131) |
|------|-----------|---------|--------------------|-------------------|----------------------|---------------------|
| 1 | 21 | 21 | | | | |

| Port | High Alarm (mA) | Low Alarm (mA) | High Warning (mA) | Low Warning (mA) |
|------|-----------------|----------------|-------------------|------------------|
| 1:21 | - | - | - | - |
| 1:22 | - | - | - | - |
| 1:23 | - | - | - | - |
| 1:24 | - | - | - | - |
| 1:25 | - | - | - | - |
| 1:26 | - | - | - | - |

図 6-6 DDM Bias Current Threshold Settings 画面

以下の項目を使用して設定します。

| 項目 | 説明 |
|----------------------|---|
| Unit | 設定するユニット番号を指定します。 |
| From / To Port | 適用するポートまたはポート範囲を指定します。 |
| High Alarm (0-131) | アラーム電流の上限を指定します。操作パラメータが本値より高くなると、アラームに関連するアクションが行われます。 |
| Low Alarm (0-131) | アラーム電流の下限を指定します。操作パラメータが本値より低くなると、アラームに関連するアクションが行われます。 |
| High Warning (0-131) | 警告電流の上限を指定します。操作パラメータが本値より高くなると、警告に関連するアクションが行われます。 |
| Low Warning (0-131) | 警告電流の下限を指定します。操作パラメータが本値より低くなると、警告に関連するアクションが行われます。 |

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

DDM TX Power Threshold Settings (DDM 送信電力しきい値設定)

スイッチの特定ポートに送信電力しきい値を設定します。

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

| Unit | From Port | To Port | High Alarm (0-6.5535) | Low Alarm (0-6.5535) | High Warning (0-6.5535) | Low Warning (0-6.5535) |
|------|-----------|---------|-----------------------|----------------------|-------------------------|------------------------|
| 1 | 21 | 21 | | | | |

| Port | High Alarm (mW) | Low Alarm (mW) | High Warning (mW) | Low Warning (mW) |
|------|-----------------|----------------|-------------------|------------------|
| 1:21 | - | - | - | - |
| 1:22 | - | - | - | - |
| 1:23 | - | - | - | - |
| 1:24 | - | - | - | - |
| 1:25 | - | - | - | - |
| 1:26 | - | - | - | - |

図 6-7 DDM TX Power Threshold Settings 画面

以下の項目を使用して設定します。

| 項目 | 説明 |
|-------------------------|---|
| Unit | 設定するユニット番号を指定します。 |
| From / To Port | 適用するポートまたはポート範囲を指定します。 |
| High Alarm (0-6.5535) | アラーム送信電力の上限を指定します。操作パラメータが本値より高くなると、アラームに関連するアクションが行われます。 |
| Low Alarm (0-6.5535) | アラーム送信電力の下限を指定します。操作パラメータが本値より低くなると、アラームに関連するアクションが行われます。 |
| High Warning (0-6.5535) | 警告送信電力の上限を指定します。操作パラメータが本値より高くなると、警告に関連するアクションが行われます。 |
| Low Warning (0-6.5535) | 警告送信電力の下限を指定します。操作パラメータが本値より低くなると、警告に関連するアクションが行われます。 |

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

DDM RX Power Threshold Settings (DDM 受信電力しきい値設定)

スイッチの特定ポートに受信電力しきい値を設定します。

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

| Port | High Alarm (mW) | Low Alarm (mW) | High Warning (mW) | Low Warning (mW) |
|------|-----------------|----------------|-------------------|------------------|
| 1:21 | - | - | - | - |
| 1:22 | - | - | - | - |
| 1:23 | - | - | - | - |
| 1:24 | - | - | - | - |
| 1:25 | - | - | - | - |
| 1:26 | - | - | - | - |

図 6-8 DDM RX Power Threshold Settings 画面

以下の項目を使用して設定します。

| 項目 | 説明 |
|-------------------------|---|
| Unit | 設定するユニット番号を指定します。 |
| From / To Port | 適用するポートまたはポート範囲を指定します。 |
| High Alarm (0-6.5535) | アラーム受信電力の上限を指定します。操作パラメータが本値より高くなると、アラームに関連するアクションが行われます。 |
| Low Alarm (0-6.5535) | アラーム受信電力の下限を指定します。操作パラメータが本値より低くなると、アラームに関連するアクションが行われます。 |
| High Warning (0-6.5535) | 警告受信電力の上限を指定します。操作パラメータが本値より高くなると、警告に関連するアクションが行われます。 |
| Low Warning (0-6.5535) | 警告受信電力の下限を指定します。操作パラメータが本値より低くなると、警告に関連するアクションが行われます。 |

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

DDM Status Table (DDM ステータステーブル)

指定ポートで現在操作中の DDM パラメータと SFP モジュールの値を表示します。

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

| Port | Temperature (Celsius) | Voltage (V) | Bias Current (mA) | TX Power (mW) | RX Power (mW) |
|------|-----------------------|-------------|-------------------|---------------|---------------|
| 1:21 | - | - | - | - | - |
| 1:22 | - | - | - | - | - |
| 1:23 | - | - | - | - | - |
| 1:24 | - | - | - | - | - |
| 1:25 | - | - | - | - | - |
| 1:26 | - | - | - | - | - |

図 6-9 DDM Status Table 画面

以下の項目を使用して設定します。

| 項目 | 説明 |
|--------------|----------------------|
| Port | ポート番号を表示します。 |
| Temperature | ポートの現在の温度を表示します。 |
| Voltage | ポートの現在の電圧を表示します。 |
| Bias Current | ポートの現在のバイアス電流を表示します。 |
| TX Power | ポートの現在の送信電力を表示します。 |
| RX Power | ポートの現在の受信電力を表示します。 |

Port Settings (スイッチのポート設定)

スイッチポートの詳細を設定します。

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

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

| Unit | From Port | To Port | State | Flow Control | Address Learning | MDIX | Medium Type |
|------|-----------|---------|---------|--------------|------------------|------|-------------|
| 1 | 01 | 01 | Enabled | Disabled | Enabled | Auto | Copper |

Speed/Duplex: Auto
 Capability Advised: 10 Half 10 Full 100 Half 100 Full 1000 Full
 Auto Negotiation: Restart An

Unit 1 Settings

| Port | State | Speed/Duplex | Flow Control | Connection | MDIX | Address Learning |
|------|---------|--------------|--------------|-----------------|------|------------------|
| 01 | Enabled | Auto | Disabled | Link Down | Auto | Enabled |
| 02 | Enabled | Auto | Disabled | 1000M/Full/None | Auto | Enabled |
| 03 | Enabled | Auto | Disabled | Link Down | Auto | Enabled |
| 04 | Enabled | Auto | Disabled | Link Down | Auto | Enabled |
| 05 | Enabled | Auto | Disabled | Link Down | Auto | Enabled |
| 06 | Enabled | Auto | Disabled | Link Down | Auto | Enabled |
| 07 | Enabled | Auto | Disabled | Link Down | Auto | Enabled |
| 08 | Enabled | Auto | Disabled | Link Down | Auto | Enabled |
| 09 | Enabled | Auto | Disabled | Link Down | Auto | Enabled |
| 10 | Enabled | Auto | Disabled | Link Down | Auto | Enabled |
| 11 | Enabled | Auto | Disabled | Link Down | Auto | Enabled |
| 12 | Enabled | Auto | Disabled | Link Down | Auto | Enabled |
| 13 | Enabled | Auto | Disabled | Link Down | Auto | Enabled |
| 14 | Enabled | Auto | Disabled | Link Down | Auto | Enabled |
| 15 | Enabled | Auto | Disabled | Link Down | Auto | Enabled |
| 16 | Enabled | Auto | Disabled | Link Down | Auto | Enabled |
| 17 | Enabled | Auto | Disabled | Link Down | Auto | Enabled |
| 18 | Enabled | Auto | Disabled | Link Down | Auto | Enabled |

図 6-10 Port Settings 画面

「From Port」と「To Port」のプルダウンメニューからポートまたはポートの範囲を選択します。

残りのプルダウンメニューから以下に示す項目について設定を行います。

| 項目 | 説明 |
|--------------------|--|
| Unit | 設定するユニットを選択します。 |
| From Port/To Port | 本設定に使用される適切なポート範囲を選択します。 |
| State | 指定したポートまたはポート範囲を「Enabled」(有効) / 「Disabled」(無効) にします。初期値は「Enabled」です。 |
| Speed/ Duplex | <p>「Speed/Duplex」欄を切り替えることでポートの速度および全二重 / 半二重状態を選択します。「Auto」は 10/100/1000Mbps のデバイス間(全二重または半二重モード時)のオートネゴシエーションを示します。(常時全二重の 1000Mbps を除く)。「Auto」を指定すると、接続相手の状況に合わせて、最適な通信を行うよう自動的に判別します。</p> <p>他のオプションには「10M Half」、「10M Full」、「100M Half」、「100M Full」、「1000M Full_Master」、および「1000M Full_Slave」があります。「Auto」以外のオプションのポート設定は固定となります。</p> <p>スイッチは 2 つのタイプ (「1000M Full_Master」および「1000M Full_Slave」) のギガビット接続設定ができます。</p> <p>ギガビット接続はフルデュプレックス接続だけをサポートしており、他の選択肢とは異なる特徴を持っています。「1000M Full_Master」および「1000M Full_Slave」パラメータは、ギガビット接続が可能なスイッチポートと他のデバイス間を 1000BASE-T ケーブルで結ぶ接続を表示しています。</p> <p>マスタ設定 (1000M Full_Master) によりポートはデュプレックス、速度および物理レイヤタイプに関連する情報を通知することができます。さらに 2 つの接続している物理レイヤ間のマスタおよびスレーブを決定します。この関係は 2 つの物理レイヤ間のタイミングコントロールを確立するために必要です。タイミング制御は、ローカルソースによってマスタの物理層に設定されます。スレーブ設定 (1000M Full_Slave) はループタイミングを使用します。マスタから受信したデータストリームによりタイミングを合わせます。一方の接続に「1000M Full_Master」を設定すると、他方の接続は「1000M Full_Slave」とする必要があります。その他の設定は両ポートのリンクダウンを引き起こします。</p> |
| Capability Advised | 「Speed/Duplex」を「Auto」に設定する場合、オートネゴシエーション時にこれらの機能を通知します。 |

| 項目 | 説明 |
|------------------|---|
| Flow Control | 各ポートのフローコントロール設定を選択します。Full-Duplex では 802.3x フローコントロールを、Half-Duplex ではバックプレッシャーによる制御を自動で行います。「Enabled」(フロー制御あり) または「Disabled」(フロー制御なし) を選択します。初期値は「Disabled」(フロー制御なし) です。 |
| MDIX | <ul style="list-style-type: none"> Auto - 最適なケーブル配線タイプを自動的に感知します。 Normal - 標準のケーブル配線となります。「normal」状態に設定すると、MDI モードになり、ストレートケーブルを通し PC の NIC に接続し、クロスケーブルを通して他のスイッチ上のポートに接続することができます。 Cross - クロスケーブル接続のために選択します。ストレートケーブルを通して別のスイッチの上のポート (MDI モード) に接続することができます。 |
| Address Learning | <p>選択ポートにおける MAC アドレスの学習の有無を設定します。</p> <ul style="list-style-type: none"> Enabled - 終点と始点 MAC アドレスをフォワーディングテーブルに自動的にリストアップします。 Disabled - MAC アドレスはフォワーディングテーブルに手動で登録します。セキュリティや効率上の理由で使用されることがあります。フォワーディングテーブルに MAC アドレスを登録する方法については、「FDB (FDB 設定)」(144 ページ) を参照してください。初期値は「Enabled」です。 |
| Medium Type | コンボポートを設定する場合、使用するケーブルメディアのタイプを定義します。 |
| Auto Negotiation | <p>プルダウンメニューを使用して、オートネゴシエーション設定を選択します。</p> <ul style="list-style-type: none"> Restart An - オートネゴシエーション処理を再開します。 Remote Fault Advertised - リモートの障害通知を設定します。 |
| Connection | 現在の接続スピードが表示されます。 |

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

「Refresh」ボタンをクリックして、本画面を更新します。

Port Description Settings (ポート名設定)

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

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

図 6-11 Port Description Settings 画面

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

以下の項目を使用して設定します。

| 項目 | 説明 |
|---------------------|--|
| Unit | 設定する各ユニットを選択します。 |
| From Port / To Port | 本設定に使用される適切なポート範囲を選択します。 |
| Medium Type | 選択ポートのメディアタイプを指定します。コンボポートを設定する場合、使用している通信メディアのタイプを指定します。SFP ポートの場合は「Fiber」を指定し、10/100/1000BASE-T ポートの場合は「Copper」を指定します。 |
| Description | 選択ポートの説明を入力します。 |

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

Port Error Disabled (エラーによるポートの無効)

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

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

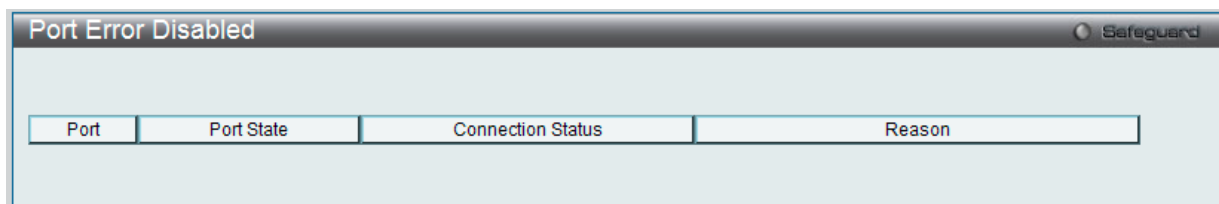


図 6-12 Port Error Disabled 画面

以下の項目が表示されます。

| 項目 | 説明 |
|-------------------|--|
| Port | エラーのために無効になっているポートを表示します。 |
| Port State | 現在のポートのステータス (「Enabled」または「Disabled」) を表示します。 |
| Connection Status | 各ポートのアップリンク状況 (「Enabled」または「Disabled」) を表示します。 |
| Reason | ストームコントロールによるポートのシャットダウンなどポートがエラーによって無効になった理由を表示します。 |

Port Media Type (ポートメディアタイプ)

ポートメディアのタイプに関する情報を表示します。

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

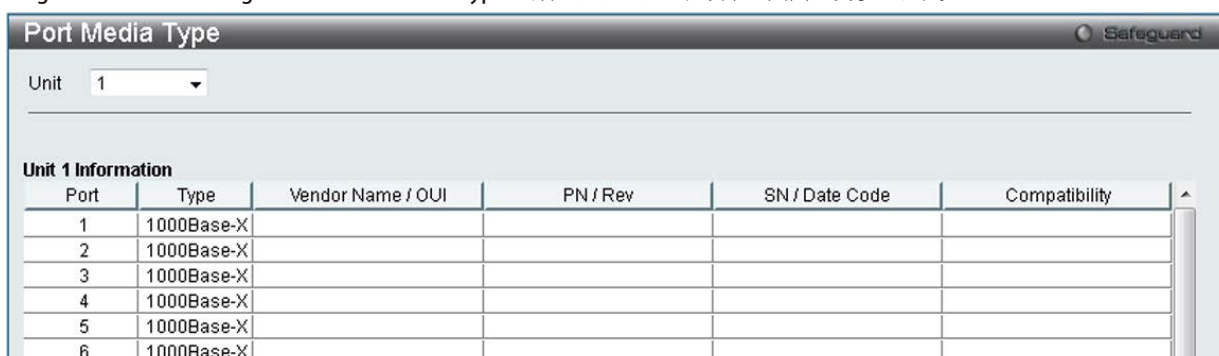


図 6-13 Port Media Type 画面

画面には以下の項目があります。

| 項目 | 説明 |
|-------------------|--------------------------------|
| Unit | 表示するユニットを指定します。 |
| Port | メディアタイプを表示するポートです。 |
| Type | ポートメディアのタイプです。 |
| Vendor Name / OUI | ベンダ名、OUI (MAC アドレス) について表示します。 |
| PN / Rev | パーツ番号、バージョンについて表示します。 |
| SN / Date Code | シリアル番号、日付について表示します。 |
| Compatibility | 互換性について表示します。 |

Port Auto Negotiation Information (オートネゴシエーション情報)

以下の画面ではオートネゴシエーションの詳しい情報を表示します。

System Configuration > Port Configuration > Port Auto Negotiation 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。:

| Port | AN | RS | CS | CB | CAB | CRB | RFA | RFR |
|------|---------|----|---------------|---------------|---------------|---------------|-----|-----|
| 01 | Enabled | | Complete | 10M_Half,1... | 10M_Half,1... | 10M_Half,1... | | |
| 02 | Enabled | | Configurin... | 10M_Half,1... | 10M_Half,1... | | | |
| 03 | Enabled | | Configurin... | 10M_Half,1... | 10M_Half,1... | | | |
| 04 | Enabled | | Configurin... | 10M_Half,1... | 10M_Half,1... | | | |
| 05 | Enabled | | Configurin... | 10M_Half,1... | 10M_Half,1... | | | |
| 06 | Enabled | | Configurin... | 10M_Half,1... | 10M_Half,1... | | | |
| 07 | Enabled | | Configurin... | 10M_Half,1... | 10M_Half,1... | | | |
| 08 | Enabled | | Configurin... | 10M_Half,1... | 10M_Half,1... | | | |
| 09 | Enabled | | Configurin... | 10M_Half,1... | 10M_Half,1... | | | |
| 10 | Enabled | | Configurin... | 10M_Half,1... | 10M_Half,1... | | | |
| 11 | Enabled | | Configurin... | 10M_Half,1... | 10M_Half,1... | | | |
| 12 | Enabled | | Configurin... | 10M_Half,1... | 10M_Half,1... | | | |

図 6-14 Port Auto Negotiation Information 画面

設定対象となる項目は以下の通りです。

| 項目 | 説明 |
|------|-----------------|
| Unit | 表示するユニットを選択します。 |

Jumbo Frame Settings (ジャンボフレームの有効化)

ジャンボフレームにより、同じデータを少ないフレームで転送することができます。ジャンボフレームは、1518 バイト以上のペイロードを持つイーサネットフレームです。本スイッチは最大 13312 バイトまでのジャンボフレームをサポートします。

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

| Port | Jumbo Frame State |
|------|-------------------|
| 1 | Enabled |
| 2 | Enabled |
| 3 | Enabled |

図 6-15 Jumbo Frame Settings 画面

本画面には次の項目があります。

| 項目 | 説明 |
|-----------------------------|--|
| Jumbo Frame Global Settings | |
| Jumbo Frame | ジャンボフレームを扱うかどうかを設定します。無効時の最大フレームサイズは 1536 バイトです。 <ul style="list-style-type: none"> • Enabled - デバイスでジャンボフレームを有効に設定します。最大フレームサイズは 13312 バイトです。 • Disabled - デバイスでジャンボフレームを無効に設定します。(初期値) |
| Jumbo Frame Port Settings | |
| Unit | 設定するユニットを選択します。 |
| From Port/To Port | 本設定に使用される適切なポート範囲を選択します。 |
| Status | プルダウンメニューを使用してポートのジャンボフレーム機能を「Enabled」(有効)/「Disabled」(無効)にします。 |

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

EEE Settings (EEE 設定) (H/W バージョン B1 のみ)

Energy Efficient Ethernet (EEE) は IEEE 802.3az によって定義され、パケットの送受信がない時に、スイッチの電力消費を抑える設計になっています。

注意 ハードウェアバージョン A1/A2 の機器には EEE 機能は実装されていません。

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

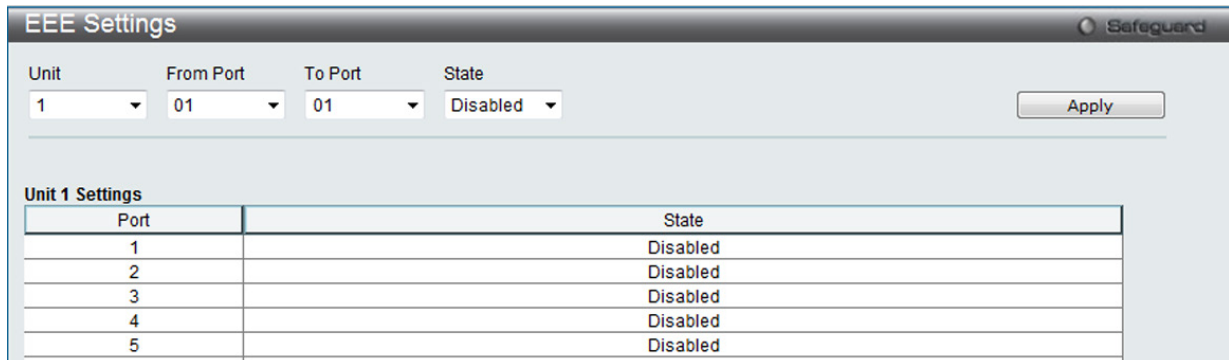


図 6-16 EEE Settings 画面

画面には以下の項目があります。

| 項目 | 説明 |
|-------------------|--|
| Unit | ポート設定を表示するユニットを設定します。 |
| From Port/To Port | EEE を設定するポートの最初 / 最後の番号を設定します。 |
| State | ポートのステータス (「Enabled」(有効) または 「Disabled」(無効)) を指定します。 |

「Apply」ボタンをクリックすると設定が更新されます。

PoE Configuration (PoE 設定) (DGS-3420-28PC/52P のみ)

DGS-3420-28PC および DGS-3420-52P は、IEEE 802.3af と 802.3at 規格で定義される PoE (Power over Ethernet) をサポートしており、すべてのポートが 30W までの PoE をサポートしています。カテゴリ 5 または カテゴリ 3 の UTP イーサネットケーブル経由で受電機器に 48VDC の電力を供給します。スイッチは標準の PSE (Power Source over Ethernet) のピン配列 Alternative A に従い、電源出力は 1、2、3 および 6 番ピンで行われます。スイッチは、弊社の IEEE 802.3af 準拠製品すべてに給電することができます。

スイッチは以下の PoE 給電機能を持ちます。

- 自動検出機能により受電機器の接続を認識し、自動的に給電します。
- 自動無効化機能は、以下の 2 つの条件下で動作します。
 - 使用電力の合計がシステムの供給電力の上限値 (Power Limit) を超えた場合。
 - ポートの使用電力がそのポートの供給電力の上限値 (Power Limit) を超えた場合。
- ショートが発生した場合、アクティブ回路保護機能によりそのポートを無効にします。他のポートは有効のままです。

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

| クラス | PD の最大使用電力 | クラス | PSE の最大出力電力 |
|-----|------------|-------|-------------|
| 0 | 12.95W | 0 | 15.4W |
| 1 | 3.84W | 1 | 4W |
| 2 | 6.49W | 2 | 7W |
| 3 | 12.95W | 3 | 15.4W |
| 4 | 29.5 W | ユーザ定義 | 35W |

スイッチの PoE の設定は **System Configuration > PoE** で行います。「PoE System Settings」画面では、PoE システムの電力制御と電力切断方法を設定します。PoE システムの電力制御を行う場合は、Power Limit の項目に 37W から 760W の間で数値を入力します。消費電力の合計が設定値を超えた場合は、PoE コントローラ (PSE) は電力のオーバーロードを避けるために電力供給を停止します。

PoE System Settings (PoE システムの設定)

PoE 機能の設定を行うためには、System Configuration > PoE > PoE System Settings の順にメニューを選択し、以下の画面を表示します。

図 6-17 PoE System Settings 画面

以下の項目を使用します。

| 項目 | 説明 |
|-------------------------|---|
| Unit | 設定するユニットを選択します。「All」を選択すると、すべてのユニットを選択します。 |
| Power Limit (37-760) | スイッチの給電機器から PoE ポート群に供給可能な電力の上限値。DGS-3420-28PC および DGS-3420-52P に 37-740W 間の電力制限を設定できます。初期値は 740W です。 |
| Power Disconnect Method | PoE コントローラは、「Deny Next Port」または「Deny Low Priority Port」によって、供給可能な電力の上限値の超過を防ぎ、スイッチの給電レベルを一定内に保ちます。プルダウンメニューから電力の停止方法を選択します。電力停止方法の初期値は「Deny Next Port」です。 <ul style="list-style-type: none"> Deny Next Port - スイッチが給電できる最大電力に到達した場合には、優先度に関わらず、新規に接続された PD に給電しません。未使用電力の最大は 19W です。(初期値) Deny Low Priority Port - スイッチが給電できる最大電力に到達した場合に新規の PD が接続された場合は、ポート優先度の最も低いポートを切断し、高優先度でクリティカルなポートに給電します。 |
| Legacy PD | プルダウンメニューを使用して、旧型の PD 信号の検知を「Enabled」(有効) / 「Disabled」(無効) にします。 |

「Apply」ボタンをクリックし、設定内容を適用します。

注意 リダンダント電源 (RPS) のないスイッチの電力制限は 390W です。ユーザが DGS-3420-28PC と DGS-3420-52P に対して DPS-700 などの RPS を追加する場合、Power Limit には 760W を設定する必要があります。

PoE Port Settings (PoE ポート設定)

デバイスの各ポートに PoE 設定を行います。

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

図 6-18 PoE Port Settings 画面

以下のパラメータを使用します。

| パラメータ | 説明 | | | | | | | | | | | | | | | | | | | | | | | | |
|---------------------|--|-----|-------------|---|---------------|---|--------------|---|--------------|---|---------------|---|--------|-----|-------------|---|---------|---|--------|---|--------|---|---------|-------|---------|
| Unit | 設定するユニットを選択します。 | | | | | | | | | | | | | | | | | | | | | | | | |
| From Port / To Port | プルダウンメニューから PoE 機能を有効または無効にするポート範囲を選択します。 | | | | | | | | | | | | | | | | | | | | | | | | |
| State | ポートの PoE 機能を「Enabled」(有効) / 「Disabled」(無効) にします。 | | | | | | | | | | | | | | | | | | | | | | | | |
| Time Range | 設定した PoE ポートにタイムレンジを選択します。タイムレンジを設定すると、指定期間だけ電力が供給されます。 | | | | | | | | | | | | | | | | | | | | | | | | |
| Priority | PoE ポートの優先度を指定します。ポート優先度はシステムがポートへの電力の供給を試みる優先度を決定します。ポート優先度には、高い順に「Critical」、「High」、「Low」の 3 つのレベルがあります。複数のポートに同じ優先レベルがたまたまある場合、ポート ID が優先度を決定するのに使用されます。低いポート ID ほど高い優先度を持ちます。優先度設定はポートに電力を供給する順番に影響します。「PoE System Settings」画面で停止方法に「Deny Low Priority Port」が設定されているかどうかにかかわらず、ポートへの電力供給を管理するためにシステムは各ポートの優先度を使用します。 | | | | | | | | | | | | | | | | | | | | | | | | |
| Power Limit | <p>1 ポートあたりの電力制限を設定します。ポートが電力制限を超過していると、シャットダウンされます。IEEE 802.3af/802.3at に基づいて、様々な PD クラスと電力消費の範囲があります。</p> <table border="1"> <thead> <tr> <th>クラス</th> <th>PD の電力消費の範囲</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>0.44 ~ 12.95W</td> </tr> <tr> <td>1</td> <td>0.44 ~ 3.84W</td> </tr> <tr> <td>2</td> <td>3.84 ~ 6.49W</td> </tr> <tr> <td>3</td> <td>6.49 ~ 12.95W</td> </tr> <tr> <td>4</td> <td>29.5 W</td> </tr> </tbody> </table> <p>これらの 5 つのクラスに対してポートに適用可能な電力の制限値は以下の通りです。各クラスの電力制限はそのクラスの電力範囲よりも若干大きくなっています。これはケーブル上の電力損失も考慮に入れているためです。そのため、標準値は以下のようになります。</p> <table border="1"> <thead> <tr> <th>クラス</th> <th>PSE の最大出力電力</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>15400mW</td> </tr> <tr> <td>1</td> <td>4000mW</td> </tr> <tr> <td>2</td> <td>7000mW</td> </tr> <tr> <td>3</td> <td>15400mW</td> </tr> <tr> <td>ユーザ定義</td> <td>35000mW</td> </tr> </tbody> </table> | クラス | PD の電力消費の範囲 | 0 | 0.44 ~ 12.95W | 1 | 0.44 ~ 3.84W | 2 | 3.84 ~ 6.49W | 3 | 6.49 ~ 12.95W | 4 | 29.5 W | クラス | PSE の最大出力電力 | 0 | 15400mW | 1 | 4000mW | 2 | 7000mW | 3 | 15400mW | ユーザ定義 | 35000mW |
| クラス | PD の電力消費の範囲 | | | | | | | | | | | | | | | | | | | | | | | | |
| 0 | 0.44 ~ 12.95W | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | 0.44 ~ 3.84W | | | | | | | | | | | | | | | | | | | | | | | | |
| 2 | 3.84 ~ 6.49W | | | | | | | | | | | | | | | | | | | | | | | | |
| 3 | 6.49 ~ 12.95W | | | | | | | | | | | | | | | | | | | | | | | | |
| 4 | 29.5 W | | | | | | | | | | | | | | | | | | | | | | | | |
| クラス | PSE の最大出力電力 | | | | | | | | | | | | | | | | | | | | | | | | |
| 0 | 15400mW | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | 4000mW | | | | | | | | | | | | | | | | | | | | | | | | |
| 2 | 7000mW | | | | | | | | | | | | | | | | | | | | | | | | |
| 3 | 15400mW | | | | | | | | | | | | | | | | | | | | | | | | |
| ユーザ定義 | 35000mW | | | | | | | | | | | | | | | | | | | | | | | | |

「Apply」ボタンをクリックし、設定内容を適用します。PoE 設定が行われたすべてのポートの状態は、上記画面下半分のテーブルに表示されます。

Serial Port Settings (シリアルポート設定)

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

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

図 6-19 Serial Port Settings 画面

画面には次の項目があります。

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

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

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

Warning Temperature Settings (警告温度設定)

システムの警告温度パラメータを設定します。

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

図 6-20 Warning Temperature Settings 画面

画面には次の項目があります。

| 項目 | 説明 |
|---------------------------|----------------------------|
| Traps State | 警告温度設定のトラップ状態を有効または無効にします。 |
| Log State | 警告温度設定のログ状態を有効または無効にします。 |
| High Threshold (-500~500) | 警告温度設定の上のしきい値を入力します。 |
| Low Threshold (-500~500) | 警告温度設定の下のしきい値を入力します。 |

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

System Log Configuration (システムログ構成)

System Log Settings (システムログ設定)

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

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

図 6-21 System Log Settings 画面

画面には次の項目があります。

| 項目 | 説明 |
|------------|---|
| System Log | システムログ機能を「Enabled」(有効) または「Disabled」(無効) にします。 |
| Save Mode | プルダウンメニューよりフラッシュメモリにスイッチのログを保存する方法を指定します。3つのオプションがあります。 <ul style="list-style-type: none"> On Demand - 手動でスイッチに、ログファイルを保存します。「Save」フォルダを使用して保存します。 Time Interval - 本項目横にある欄にログを保存する間隔 (1-65535) (分) を設定します。 Log Trigger - スイッチにログイベントが発生すると、スイッチにログファイルを保存します。 |

1. 「System Log」を「Enabled」(有効) にし、「Apply」ボタンをクリックします。
2. プルダウンメニューよりフラッシュメモリにスイッチのログを保存する方法を指定します。「Time Interval」を選択した場合は、横にある欄にログを保存する間隔を入力します。
3. 設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

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

システムログはイベントの記録と管理、エラーと情報のメッセージをレポートします。本スイッチは指定した4台までのSyslogサーバにSyslogメッセージを送信できます。

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

図 6-22 System Log Server Settings 画面

本画面には次の項目があります。

| 項目 | 説明 |
|------------------------------|--|
| Server ID | Syslog サーバ設定のインデックス (1-4) を設定します。 |
| Severity | 送信されるメッセージレベルをプルダウンメニューから選択します。選択したレベル以上のメッセージをすべて送信します。オプションは Emergency (0)、Alert (1)、Critical (2)、Error (3)、Warning (4)、Notice (5)、Informational (6) および Debug (7) です。 |
| Server IPv4 Address | ログを記録するサーバの IPv4 アドレスを設定します。 |
| Server IPv6 Address | ログを記録するサーバの IPv6 アドレスを設定します。 |
| Facility | オペレーティングシステムデーモンおよびプロセスでファシリティ値を割り当てている場合に設定します。Local 0、Local 1、Local 2、Local 3、Local 4、Local 5、Local 6、または Local 7 を選択します。 |
| UDP Port (514 or 6000-65535) | ログを送信するサーバの UDP ポートを設定します。514 または 6000-65535 が設定できます。初期値は 514 です。 |
| Status | 「Enabled」(有効) または「Disabled」(無効) を選択します。 |

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

エントリの変更

1. 編集する場合は、該当エントリ横の「Edit」ボタンをクリックして以下の画面を表示します。

図 6-23 System Log Server Settings 画面 - Edit

2. 項目を入力後、「Apply」ボタンをクリックします。

エントリの削除

削除するエントリ横の「Delete」ボタンをクリックし、デバイスのエントリを削除します。または、「Delete All」ボタンをクリックして、設定したすべてのサーバを削除します。

System Log (Syslog ログ)

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

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

図 6-24 System Log 画面

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

| 項目 | 説明 |
|----------|---|
| Log Type | プルダウンメニューで表示するログタイプを選択します。 <ul style="list-style-type: none"> Severity - これを選択する場合、次のチェックも行う必要があります。次にチェックするのは Emergency、Alert、Critical、Error、Warning、Notice、Informational および Debug です。ログ内の全情報を単に参照するには、「All」オプションを選択します。特定のモジュールを検索するためには、モジュール名を入力します。 Module List - これを選択する場合、手動でモジュール名を入力する必要があります。利用可能なモジュールは、MSTP、DHCPv6_CLIENT、DHCPv6_RELAY、ERPS、ERROR_LOG、CFM_EXT、および DHCPv6_SERVER です。 Attack Log - すべての攻撃が表示されます。プルダウンメニューからユニットを選択すると、そのユニットの結果を表示します。 |
| Index | エントリが加わるごとに 1 増加します。新しいエントリ順に表示されます。 |
| Time | スイッチの最後の再起動から経過した時間 (日、時、分、秒) を表示します。 |
| Level | ログエントリのレベルを表示します。 |
| Log Text | イベントの内容を表示します。 |

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

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

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

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

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

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

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

図 6-25 System Log & Trap Settings 画面

本画面には次の項目があります。

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

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

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

System Severity Settings (システムセバリティ設定)

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

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

| System Severity | Severity Level |
|-----------------|-----------------|
| Trap | Information (6) |
| Log | Information (6) |

図 6-26 System Severity Settings 画面

プルダウンメニューを使用して、以下の項目の設定を行います。

| 項目 | 説明 |
|-----------------|---|
| System Severity | 「Severity Type」で指定したレベルのアラートが発生した時に実行するアクションを選択します。 <ul style="list-style-type: none"> Log - 分析のためにスイッチのログに設定した「Severity Level」のアラートを送信します。 Trap - 分析のために SNMP エージェントに送信します。 All - 分析のために SNMP エージェントとスイッチのログに選択したアラートタイプを送信します。 |
| Severity Level | 送信されるメッセージレベルをプルダウンメニューから選択します。オプションは Emergency (0)、Alert (1)、Critical (2)、Error (3)、Warning (4)、Notice (5)、Informational (6) および Debug (7) です。 |

「Apply」ボタンをクリックして、システムのログレベル設定を適用します。

Time Range Settings (タイムレンジ設定)

各機能 (ACL など) が作用する期間 (タイムレンジ) を設定します。スイッチのアクセスプロファイル設定が有効な場合、アクセスプロファイル機能を実行する期間 (開始点と終了点) を一週間の特定の曜日によって決定します。

例えば、管理者は週土日にインターネットの閲覧を許可し、一方平日はインターネットの閲覧を拒否するようなタイムベース ACL を設定することができます。64 個のタイムレンジを入力することができます。

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

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

図 6-27 Time Range Settings 画面

以下の項目を設定することができます。

| 項目 | 説明 |
|------------------|---|
| Range Name | タイムレンジを識別するために使用する名前を半角英数字 32 文字以内で入力します。このレンジ名はアクセスプロファイルテーブルで使用され、このタイムレンジで有効であるアクセスプロファイルと関連するルールを識別します。 |
| Hours (HH MM SS) | プルダウンメニューを使用し、タイムレンジの時刻を以下の項目で設定します。 <ul style="list-style-type: none"> Start Time - 開始時刻を時間、分、秒 (24 時形式) で指定します。 End Time - 終了時刻を時間、分、秒 (24 時形式) で指定します。 |
| Weekdays | チェックボックスを使用し、タイムレンジを有効にする曜日を選択します。「Select All Days」をチェックすると、すべての曜日を設定します。 |

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

エントリの削除

削除するエントリ横の「Delete」ボタンをクリックします。

Port Group Settings (ポートグループ設定)

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

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

図 6-28 Port Group Settings 画面

以下の項目を設定することができます。

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

「Apply」 ボタンをクリックして行った変更を適用します。

エントリの削除

削除するエントリ横の「Delete」 ボタンをクリックします。

Time Settings (時刻設定)

スイッチに時刻を設定します。

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

図 6-29 Time Settings 画面

以下の項目を使用して設定、表示を行います。

| 項目 | 説明 |
|-------------------|--|
| Date (DD/MM/YYYY) | システムクロックの更新を行うために現在の年月日を入力します。項目のフォーマットは日 / 月 / 年です。 |
| Time (HH:MM:SS) | 現在のシステム時刻を時 : 分 : 秒 (24 時間制) で設定します。例えば午後 9 時であれば 21:00:00 と指定します。 |

「Apply」 ボタンをクリックし、デバイスに時刻設定を適用します。

User Accounts Settings (ユーザアカウントの設定)

スイッチはユーザ権限の制御を行うことができます。ユーザパスワードとアクセス権限を含むユーザアカウントを設定します。以下の手順でユーザアカウント情報を設定します。

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

User Accounts Settings

Add User Accounts

User Name: Password:

Access Right: Confirm Password:

Encryption:

Note: User Name should be less than 16 characters. Password should be less than 16 characters or 35 characters.

Total Entries: 4

| User Name | Access Right | Old Password | New Password | Confirm Password | Encryption |
|-----------|--------------|--------------|--------------|------------------|---|
| Ouser | Operator | ***** | ***** | ***** | <input type="button" value="Edit"/> <input type="button" value="Delete"/> |
| Puser | Power_User | ***** | ***** | ***** | <input type="button" value="Edit"/> <input type="button" value="Delete"/> |
| Uuser | User | ***** | ***** | ***** | <input type="button" value="Edit"/> <input type="button" value="Delete"/> |
| manager | Admin | ***** | ***** | ***** | <input type="button" value="Edit"/> <input type="button" value="Delete"/> |

図 6-30 User Accounts Settings 画面

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

| 管理 | Admin | Operator | Power User | User |
|---------------------------|----------|--------------|--------------|--------|
| コンフィグレーション設定 | 読み / 書き可 | 読み / 書き (一部) | 読み / 書き (一部) | 不可 |
| ネットワークモニタリング | 読み / 書き可 | 読み / 書き可 | 読み出しのみ | 読み出しのみ |
| コミュニティ名とトラップステーション | 読み / 書き可 | 読み出しのみ | 読み出しのみ | 読み出しのみ |
| ファームウェアとコンフィグレーションファイルの更新 | 読み / 書き可 | 不可 | 不可 | 不可 |
| システムユーティリティ | 読み / 書き可 | 読み出しのみ | 読み出しのみ | 読み出しのみ |
| リセット (工場出荷状態へ) | 読み / 書き可 | 不可 | 不可 | 不可 |
| ユーザアカウント管理 | | | | |
| ユーザアカウントの登録、更新、変更 | 読み / 書き可 | 不可 | 不可 | 不可 |
| ユーザアカウントの確認 | 読み / 書き可 | 不可 | 不可 | 不可 |

User Accounts 画面には次の項目があります。

| 項目 | 説明 |
|------------------|--|
| User Name | ユーザ名を定義します。(半角英数字 15 文字以内) |
| Access Right | ユーザのアクセス権限 (Admin、Operator、Power User および User) を指定します。 |
| Encryption | 本ボックスをチェックして、アカウントに適用する暗号化タイプ (Plain Text または SHA-1) を指定します。 |
| Password | ユーザアカウントに対するパスワードを設定します。 |
| Confirm Password | ユーザパスワードの確認のために再度入力します。 |

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

System Configuration (スイッチの主な設定)

ユーザアカウントの編集

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

| User Name | Access Right | Old Password | New Password | Confirm Password | Encryption |
|-----------|--------------|----------------------|----------------------|----------------------|-------------|
| Ouser | Operator | ***** | ***** | ***** | |
| Puser | Power_User | ***** | ***** | ***** | |
| User | User | ***** | ***** | ***** | |
| manager | Admin | <input type="text"/> | <input type="text"/> | <input type="text"/> | (Default) v |

図 6-31 User Accounts Settings 画面 - 編集

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

注意 パスワードを忘れてしまった場合やパスワード不正の場合は、[467 ページの「付録 F パスワードのリカバリ手順」](#)を参照してください。本問題を解決する手順が記載されています。

エントリの削除

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

注意 パスワードを忘れてしまった場合やパスワード不正の場合は、本マニュアル終わりにある [467 ページの「付録 F パスワードのリカバリ手順」](#)を参照してください。これは、この問題を解決するように必要な手順を案内します。

注意 ユーザ名とパスワードは 16 文字以内とします。

Command Logging Settings (コマンドログ設定)

コマンドログ設定を有効または無効にします。

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

Command Logging State Enabled Disabled

図 6-32 Command Logging Settings 画面

以下の項目を設定することができます。

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

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

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

Stacking (スタッキング設定)

本スイッチは、スイッチのスタックをサポートしています。これらは、12個のスイッチを1つに結合し、Telnet、GUI インタフェース (Web)、コンソールポートまたは SNMP 経由で1つの IP アドレスから管理することができます。

本シリーズの各スイッチは、2個のスタックポートを搭載しており、他のデバイスとの接続やそれらのスタックに使用されます。

- Duplex Chain - 図6-33のように、Duplex Chain トポロジはチェーン・リンク形式でスイッチをスタックします。この方法を使用すると、一方向のデータ転送だけが可能となります。そして、に1カ所中断が発生すると、データ転送は明らかに影響を受けます。
- Duplex Ring - 図6-34のように、Duplex Ring は、データが双方向に転送できるようにリングまたは円の形式でスイッチをスタックします。このトポロジは、リングに1カ所中断が発生しても、データはスタック内のスイッチ間のスタックケーブル経由で転送されるため高い冗長性を実現できます。

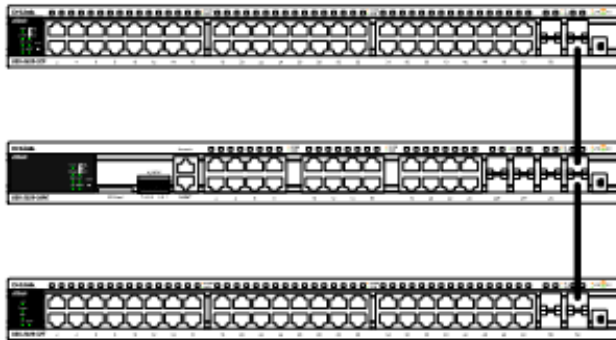


図 6-33 Duplex Chain でスタックされているスイッチ画面

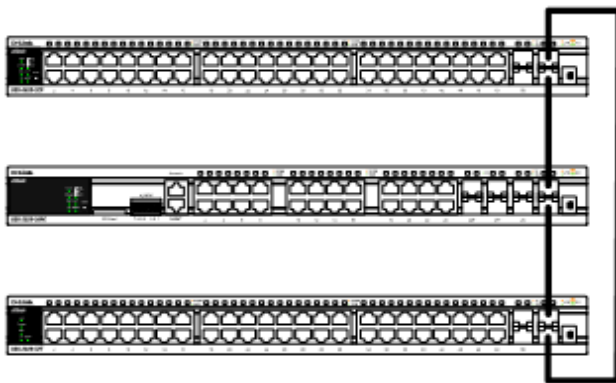


図 6-34 Duplex Ring でスタックされているスイッチ画面

各トポロジにおいて、各スイッチはスイッチスタックにおける役割を果たします。各スイッチには役割を設定でき、スイッチスタック機能により自動的に決定することもできます。

スイッチをスタックする場合に、3つの役割があります。

- プライマリマスタ

プライマリマスタは、スタックのリーダーです。スタックの通常操作、モニタ操作、およびトポロジの実行をメンテナンスします。本スイッチは、スイッチスタック内にあるスイッチにスタックユニット番号の割り当て、コンフィギュレーションの同期、コマンドの送信を行います。プライマリマスタには、スタックを物理的に構成する前、またはすべての優先度が同じである場合には最も数字の低い MAC アドレスを持つスイッチに決定します。また、スタックが自動的に決定される前に、最も高い優先度（低い番号ほど優先度は高くなります。）を本スイッチに割り当てることで手動で設定することができます。プライマリマスタは、スイッチの前面パネルの一番右にある LED によって Box ID と「H」が表示されます。

- バックアップマスタ

バックアップマスタは、プライマリマスタに対するバックアップであり、プライマリマスタが故障、またはスタックから取り外される場合に、プライマリマスタの機能を引き継ぎます。また、スタック内で隣接するスイッチの状態をモニタし、プライマリマスタによって割り当てられたコマンドを実行して、プライマリマスタの動作状態をモニタします。バックアップマスタは、スタックを物理的に構成する前、またはすべての優先度が同じである場合には2番目に数字の低いMACアドレスに決定します。また、スタックが自動的に決定される前に、2番目に高い優先度（低い番号ほど優先度は高くなります。）を本スイッチに割り当てることで手動で設定することができます。バックアップマスタは、物理的にスイッチの前面パネルの一番右にある7個のセグメント LED によって Box ID と「h」が表示されます。

・スレーブ

スレーブスイッチは、残りのスイッチスタックを構成します。プライマリマスタまたはバックアップマスタスイッチではありません。プライマリマスタおよびバックアップマスタが故障、またはスタックから取り外される場合に、それらの機能を引き継ぎます。スレーブスイッチは、マスタに要求された操作を実行して、スタックとスタックトポロジにある近接スイッチの状態をモニタします。さらに、バックアップマスタがプライマリマスタになるとバックアップマスタのコマンドに従います。スレーブスイッチは、バックアップマスタがプライマリマスタに移行する場合、バックアップマスタが故障、またはスイッチから取り外される場合に、セルフチェックを行い、自身がバックアップマスタになるかどうかを決定します。プライマリマスタとバックアップマスタの両方が故障、またはスイッチから取り外される場合、プライマリマスタになるかどうか決定します。これらの役割は、はじめに優先度によって決定され、さらに優先度が同じである場合は、最も低い MAC アドレスによって決定されます。

スイッチが希望したトポロジで構成されると、スタックは機能する状態に到達するまでに 3 つの過程を経由します。

- ・初期化状態 - これは、スタックの最初の状態で、ランタイムコードが設定および初期化され、システムは各スイッチが適切に機能していることを検証するために周辺機器の診断を行います。
- ・マスタ選出状態 - コードがロードされ、初期化されると、スタックはマスタ選出状態になり、使用されるトポロジのタイプを検出し、プライマリマスタ、バックアップマスタの順に選出します。
- ・同期状態 - プライマリマスタとバックアップマスタが確立すると、プライマリマスタがスイッチにスタックユニット番号を割り当て、すべてのスイッチに構成を同期させ、プライマリマスタの構成に基づき、残りのスイッチにコマンドを送信します。

これらの手順が終了すると、スイッチスタックは正常な操作モードに入ります。

スタックスイッチのスワップ

スイッチのスタック機能は、動作中のスタック内またはスタック外のスイッチの「ホットスワップ」をサポートしています。いくつかの簡単な条件により、電源オフやスタック内のスイッチ間のデータ転送に大きな影響を与えずに、スタックからのスイッチの取り外しやスタックへの追加を行うことができます。

スイッチが動作中のスタックに「ホットインサート」される場合、設定された優先度や MAC アドレスなど新たに追加されたコンフィグレーションによって、新しいスイッチはプライマリマスタ、バックアップマスタまたはスレーブとなる可能性があります。しかし、共に以前の選出過程を経て、その結果、プライマリマスタとバックアップマスタを持った 2 つのスタックが追加されると、新しいプライマリマスタが、優先度または MAC アドレスに基づいて、既存のプライマリマスタから選出されます。このプライマリマスタは、ホットインサートされた新しいスイッチすべてにプライマリマスタの全役割を引き継ぎます。この過程は、検出処理が完了するまで 1.5 秒ごとにスイッチスタックを通して循環するディスカバリパケットを使用して行われます。

「ホットリムーブ」の動作は、スタックが既に動作している場合にスタックからデバイスを取り外すことを意味します。ホットリムーブは、指定した間にデバイスからハートビートパケットを受信しない場合、またはスタックポートの中の 1 つのリンクがダウンした場合に、スタックによって検出されます。デバイスが一度取り外されると、残りのスイッチは、スタックトポロジデータベースを更新し、変更を反映します。スタックから 3 つの役割（プライマリマスタ、バックアップマスタ、またはスレーブ）のどれか 1 つが取り外される場合には、異なる過程がそれぞれの特定デバイス取り外しに発生します。

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

バックアップマスタがホットリムーブされると、新しくバックアップマスタが前述の選出過程を経由して選ばれます。スタック内のスイッチは、取り外されたユニットの ARP などのダイナミックに学習されたデータベースをクリアします。その後、データベース同期がスタックによって完了した際に、バックアップマスタはプライマリマスタのバックアップを開始します。

プライマリマスタが取り外されると、バックアップマスタはプライマリマスタの役割を引き受けて、新しいバックアップマスタが選出過程を経て選ばれます。スタック内のスイッチは、取り外されたユニットの ARP などのダイナミックに学習されたデータベースをクリアします。新しいプライマリマスタは、スタックとネットワーク内の矛盾を避けるために、前のプライマリマスタの MAC と IP アドレスを引き継ぎます。

プライマリマスタとバックアップマスタの両方が取り外される場合、選出過程では、直ちに処理を行い、新しいプライマリマスタとバックアップマスタを決定します。スタック内のスイッチは、取り外されたユニットの ARP などのダイナミックに学習されたデータベースをクリアします。スタティックなスイッチ構成は、スタックに存在するスイッチに関するデータベースに残りますが、それらの機能には影響されません。

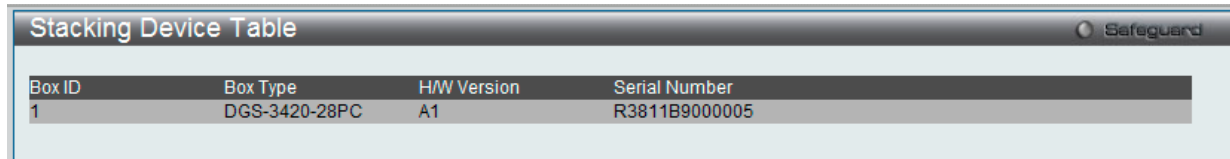
注意

スタックが検出過程にある時、Box ID の矛盾があると、そのデバイスは特別なスタンドアロントポロジモードに入ります。ユーザはデバイス情報の取得、Box ID の設定、保存、および再起動だけ行うことができます。すべてのスタックポートが無効とされ、エラーメッセージがスタック内の各デバイスのローカルコンソールポートに生成されます。ユーザは、Box ID を再設定し、スタックを再起動する必要があります。

Stacking Device Table (スタックデバイステーブル)

スイッチスタック内の現在のデバイスを表示します。

System Configuration > Stacking > Stacking Device 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。



| Box ID | Box Type | H/W Version | Serial Number |
|--------|---------------|-------------|---------------|
| 1 | DGS-3420-28PC | A1 | R3811B9000005 |

図 6-35 Stacking Device Table 画面

Stacking Mode Settings (スタックモード設定)

スタック処理を開始するためには、はじめに、以下の画面を使用して、デバイスのスタック機能を有効にする必要があります。

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

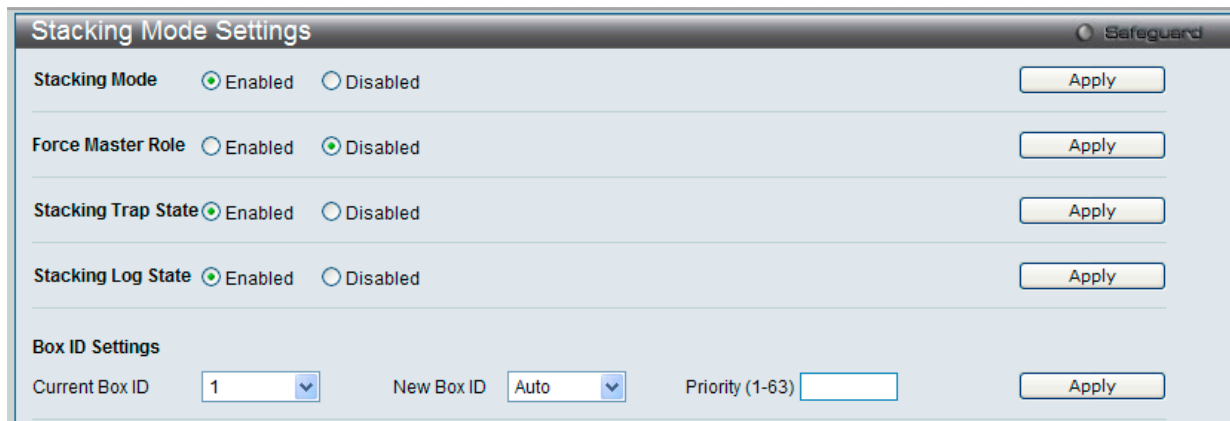


図 6-36 Stacking Mode Settings 画面

設定および表示する項目は以下の通りです。

| 項目 | 説明 |
|---------------------|---|
| Stacking Mode | 初期値では「Disabled」(無効)になっています。 |
| Force Master Role | ラジオボタンを使用して機能を「Enabled」(有効)/「Disabled」(無効)にします。新しいデバイスが現在のスタックポートに追加した際にマスターロールが変更されないことを保証するために使用されます。「Enabled」(有効)を選択すると、スタックが安定した後にマスタの優先度は0になります。 |
| Stacking Trap State | スタックにトラップを送信します。 |
| Stacking Log State | スタックにログを送信します。 |
| Current Box ID | スタックにおけるスイッチの現在のボックス番号を選択します。 |
| New Box ID | 「Current Box ID」で選択したスタック内のスイッチに新しくボックス番号(1-12)を指定します。「Auto」はスイッチスタック内のスイッチに自動的にボックス番号を割り当てます。 |
| Priority (1-63) | スイッチの優先度番号を表示します。低い値ほど高いプライオリティを示します。スタック内で最も低い優先度番号を持つボックス(スイッチ)が、プライマリマスタです。プライマリマスタスイッチは、スイッチスタックにおけるアプリケーションを設定するために使用されます。 |

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

第7章 Management (スイッチの管理)

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

| サブメニュー | 説明 | 参照ページ |
|---|--|---------------------|
| ARP (ARP 設定) | スタティック ARP、プロキシ ARP、ARP テーブルを設定します。次のメニューがあります。 Static ARP Settings (スタティック ARP 設定)、Proxy ARP Settings (プロキシ ARP 設定)、 ARP Table (ARP テーブルの参照) | 71 |
| Gratuitous ARP (Gratuitous ARP の設定) | Gratuitous ARP の設定をします。次のメニューがあります。 Gratuitous ARP Global Settings (Gratuitous ARP グローバル設定)、Gratuitous ARP Settings (Gratuitous ARP 設定) | 73 |
| IPv6 Neighbor Settings (IPv6 Neighbor 設定) | IPv6 Neighbor の設定を行います。 | 74 |
| IP Interface (IP インタフェース設定) | スイッチの IP インタフェース設定を行います。次のメニューがあります。 System IP Address Settings (IP アドレス設定)、Interface Settings (インタフェース設定)、 Loopback Interface Settings (ループバックインタフェース設定) | 75 |
| Management Settings (管理設定) | CLI ページング、DHCP 自動設定などの管理設定を行います。 | 81 |
| Out of Band Management Settings (アウトバンド管理設定) | RJ-45 のアウトバンド管理の詳細を設定します。 | 82 |
| Session Table (セッションテーブル) | スイッチが最後に起動してからの管理セッションを表示します。 | 82 |
| Single IP Management (シングル IP マネジメント設定) | シングル IP マネジメント機能を設定します。次のメニューがあります。 Single IP Settings (シングル IP 設定)、Firmware Upgrade (ファームウェア更新)、 Configuration File Backup/ Restore (コンフィギュレーションファイルの更新)、Upload Log File (ログファイルのアップロード) | 83 |
| SNMP Settings (SNMP 設定) | SNMP 設定を行います。次のメニューがあります。 SNMP Global Settings (SNMP グローバル設定)、SNMP Trap Settings (SNMP トラップ設定)、 SNMP Link Change Traps Settings (SNMP リンクチェンジトラップ設定)、SNMP View Table Settings (SNMP ビューテーブル)、SNMP Community Table Settings (SNMP コミュニティ テーブル設定)、SNMP Group Table Settings (SNMP グループテーブル)、SNMP Engine ID Settings (SNMP エンジン ID 設定)、SNMP User Table Settings (SNMP ユーザテーブル設定)、 SNMP Host Table Settings (SNMP ホストテーブル設定)、SNMP v6Host Table Settings (SNMP v6 ホストテーブル設定)、RMON Settings (RMON 設定)、SNMP Community Encryption Settings (SNMP コミュニティ暗号化設定)、SNMP Community Masking Settings (SNMP コ ミュニティマスク設定) | 92 |
| Telnet Settings (Telnet 設定) | スイッチに Telnet 設定をします。 | 101 |
| Web Settings (Web 設定) | スイッチに Web ステータスを設定します。 | 101 |
| Power Saving (省電力設定) | リンクダウン状態のポートの電源をオフにしてスイッチへの電力を節約します。 | 102 |

ARP (ARP 設定)

Static ARP Settings (スタティック ARP 設定)

ARP (Address Resolution Protocol) は、IP アドレスを物理的なアドレスに変換する TCP/IP プロトコルです。ここでは特定のデバイスに対する ARP 情報を参照、編集および削除することができます。

スタティックエントリを ARP テーブルに定義します。スタティックエントリを定義する場合、継続的なエントリを入力し、IP アドレスを MAC アドレスに変換するために使用します。以下の手順で ARP 情報を定義します。

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

図 7-1 Static ARP Settings 画面

「Static ARP Settings」画面には次の項目があります。

| 項目 | 説明 |
|---|---|
| Global Settings | |
| ARP Aging Time (0-65535) | ARP エントリのエージングタイム (分)。この時間が経過すると、エントリはテーブルから削除されます。範囲は 0-65535 (分) です。初期値は 20 (分) です。 |
| Add Static ARP Entry | |
| IP Address | MAC アドレスとスタティックに結びつける IP アドレスを設定します。 |
| MAC Address | ARP テーブルで IP アドレスとスタティックに結びつける MAC アドレスを設定します。 |
| スタティック ARP リスト | |
| ユーザがスタティックに設定した IP アドレスと MAC アドレスの対応エントリを表示します。 | |

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

Static ARP List のエントリの編集

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

図 7-2 Static ARP Settings 画面

2. 「MAC Address」を編集します。
3. 「Apply」ボタンをクリックします。

Static ARP List のエントリの削除

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

Proxy ARP Settings (プロキシ ARP 設定)

プロキシ ARP 機能に関する基本設定を参照および編集します。

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

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

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

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

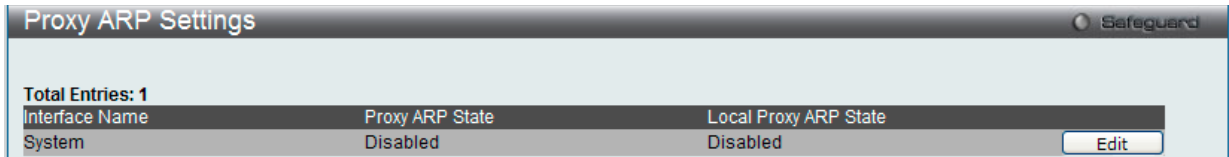


図 7-3 Proxy ARP Settings 画面

エントリの編集

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



図 7-4 Static ARP Settings 画面

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

初期値では、「Proxy ARP State」と「Local Proxy ARP State」の両方とも無効です。

ARP Table (ARP テーブルの参照)

スイッチ上の現在の ARP エントリを表示します。

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

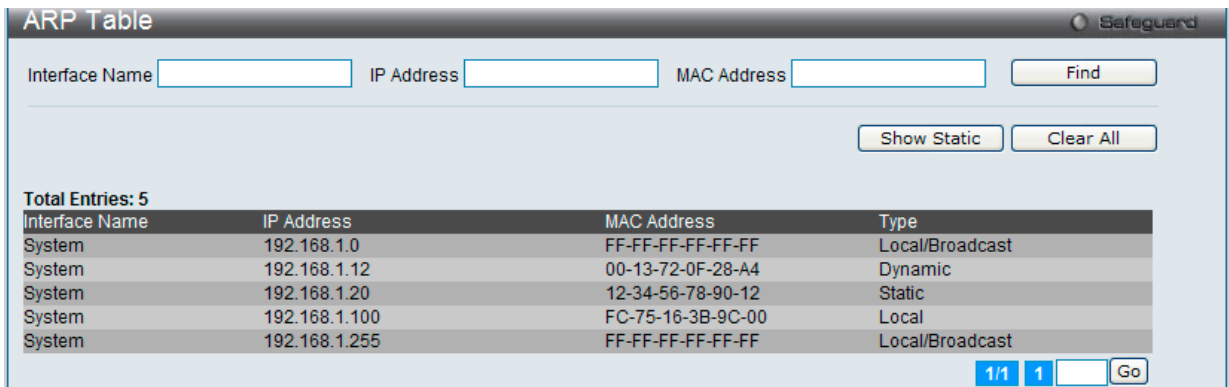


図 7-5 ARP Table 画面

設定対象となる項目は以下の通りです。

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

特定の ARP エントリを検索するためには、画面の上の「Interface Name」または「IP Address」を入力し、「Find」ボタンをクリックします。

スタティック ARP エントリを表示する場合は、「Show Static」ボタンをクリックします。

ARP テーブルをクリアする場合は、「Clear All」ボタンをクリックします。

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

Gratuitous ARP (Gratuitous ARP の設定)

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

Gratuitous ARP のグローバル設定を行います。

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

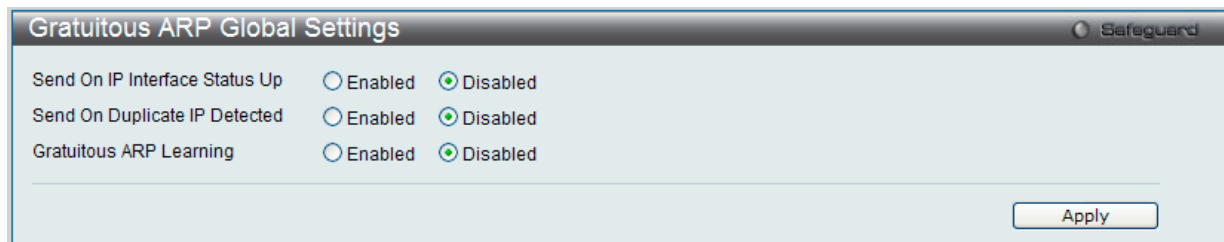


図 7-6 Gratuitous ARP Global Settings 画面

以下の項目を使用して、設定します。

| 項目 | 説明 |
|--------------------------------|---|
| Send On IP Interface Status Up | IP インタフェースの起動中に、Gratuitous ARP リクエストの送信を有効または無効にします。これは、自動的にインタフェースの IP アドレスを他のノードにアナウンスするために使用されます。初期値は無効で、Gratuitous ARP パケットだけがブロードキャストされます。 |
| Send On Duplicate IP Detected | 重複した IP アドレスが検知された場合の Gratuitous ARP リクエストパケットの送信を有効または無効にします。初期値は無効です。検出された重複 IP アドレスは、システム自身の IP アドレスに一致する IP アドレスによって送信された ARP リクエストパケットをシステムが受信したことを意味します。この場合、システムは、誰かがシステムと重複する IP アドレスを使用していることがわかります。この IP アドレスのホストを正しくするために、システムはこの重複 IP アドレスに Gratuitous ARP リクエストパケットを送信することができます。 |
| Gratuitous ARP Learning | システムは、通常、システムの IP アドレスに一致している MAC アドレスを求める ARP 応答パケットが正常な ARP リクエストパケットを学習するだけです。受信した Gratuitous ARP パケットに基づいて、ARP キャッシュの更新を有効または無効にします。Gratuitous ARP パケットはパケットがクエリである IP と同じ送信元 IP アドレスによって送信されます。初期値は無効です。 |

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

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

Gratuitous ARP Settings (Gratuitous ARP 設定)

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

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

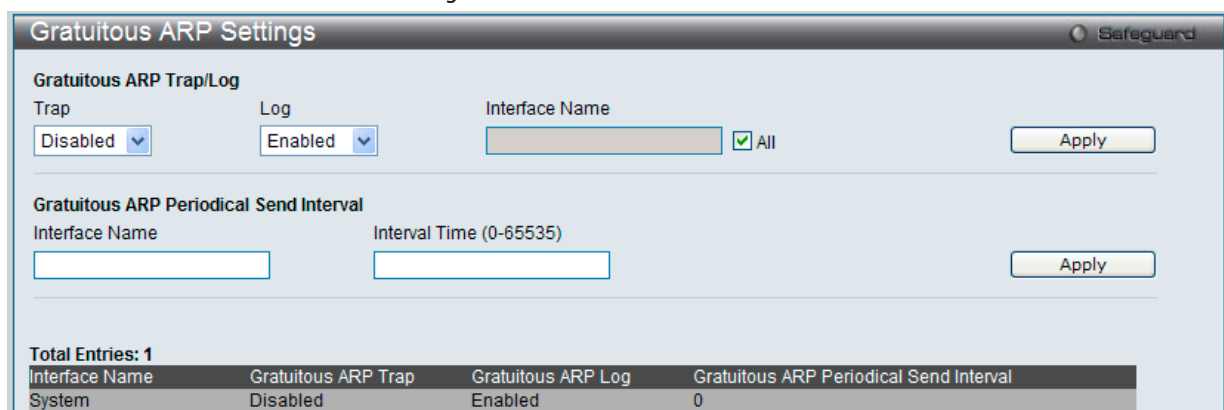


図 7-7 Gratuitous ARP Settings 画面

以下の項目を使用して設定します。

| 項目 | 説明 |
|---|--|
| Gratuitous ARP Trap/Log | |
| Trap | スイッチは、IP の重複イベントをトラップし、管理者に通知します。初期値ではトラップは無効です。 |
| Log | スイッチは、IP の重複イベントのログを取得し、管理者に通知します。初期値ではログは有効です。 |
| Interface Name | レイヤ 3 インタフェース名を入力します。「All」を選択して全インタフェース上の Gratuitous ARP トラップを有効または無効にします。 |
| Gratuitous ARP Periodical Send Interval | |
| Interface Name | 編集するインタフェース名を表示します。 |

| 項目 | 説明 |
|-------------------------|---|
| Interval Time (0-65535) | 定期的に Gratuitous ARP を送信する間隔 (秒) を入力します。0 は Gratuitous ARP リクエストが定期的に送信されないことを意味します。初期値は 0 (秒) です。 |

「Gratuitous ARP Trap/Log」セクションにある「Apply」ボタンをクリックしてこのセクションで行った変更を適用します。

「Gratuitous ARP Periodical Send Interval」セクションにある「Apply」ボタンをクリックして行った変更を適用します。

IPv6 Neighbor Settings (IPv6 Neighbor 設定)

スイッチの IPv6 Neighbor 設定を行います。

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

図 7-8 IPv6 Neighbor Settings 画面

スイッチの現在の IPv6 Neighbor 設定が下部に表示されます。

IPv6 Neighbor の新規登録

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

エントリの検索

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

エントリの削除

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

以下の項目が表示、または設定変更に使えます。

| 項目 | 説明 |
|------------------------|---|
| Interface Name | IPv6 Neighbor 名を入力します。スイッチにおける現在の全インタフェースに対して検索するには、画面の中央部分にある 2 個目の「Interface Name」欄で「All」を選択し、「Find」ボタンをクリックします。また、「Hardware」オプションを選択して、ハードウェアテーブルに書かれたすべての Neighbor キャッシュエントリを表示します。 |
| Neighbor IPv6 Address | Neighbor の IPv6 アドレスを入力します。 |
| Link Layer MAC Address | リンクレイヤの MAC アドレスを入力します。 |
| State | 「All」、「Address」、「Static」または「Dynamic」を指定します。「Address」を選択すると、「State」オプション横にあるスペースに IP アドレスを入力できるようになります。 |

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

IP Interface (IP インタフェース設定)

IP 設定を変更します。

ネットワーク接続前に IP アドレスをコンソールより設定する必要があります。Web マネージャはスイッチの現在の IP 設定が表示します。

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

System IP Address Settings (IP アドレス設定)

スイッチの IP アドレス設定を変更します。

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

図 7-9 System IP Address Settings 画面

スイッチの現在の IP 設定が表示されます。

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

1. 画面先頭のメニューから「Static」を選択します。
2. 適切な「IP Address」と「Subnet Mask」を入力します。
3. 異なるサブネットから本スイッチにアクセスする場合は、「Gateway」の IP アドレスを入力します。同じサブネットからスイッチを管理する場合は、この項目内は初期値 (0.0.0.0) のままにします。
4. 本スイッチに VLAN 設定をしていない場合は、初期設定の「Management VLAN Name」を使用できます。本スイッチは、購入時に VLAN 「default」が設定されていて、すべてのポートが所属しています。既に VLAN 設定をしている場合は、本スイッチにアクセスするためには、管理ステーションに接続しているポートが所属している VLAN の名称を入力します。
5. 設定が行われていない場合は、「Interface Admin State」プルダウンメニューから「Enabled」(有効)を選択します。

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

プロトコルは以下の通りです。

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

Management (スイッチの管理)

| 項目 | 説明 |
|-------|---|
| BOOTP | 電源が投入されるとスイッチは BOOTP ブロードキャストリクエストを送信します。BOOTP プロトコルを使用して BOOTP サーバが IP アドレス、ネットワークマスクおよびデフォルトゲートウェイを割り当てます。本オプションが選択すると、スイッチは初期設定や以前に登録された設定を使用する前に、BOOTP サーバにアクセスしこれらの情報を取得します。 |

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

以下の表は「System」インタフェースに関する項目について説明します。

| 項目 | 説明 |
|-----------------------|---|
| Interface Name | System インタフェース名が表示されます。 |
| Management VLAN Name | System インタフェースに所属する VLAN 名のエントリを許可します。 |
| Interface Admin State | 「Enabled」(有効)/「Disabled」(無効)にします。IP アドレスを設定する場合は、「Enabled」を設定する必要があります。 |
| IP Address | IP インタフェースに割り当てる IPv4 アドレスを入力します。本スイッチの IP アドレスの初期値は 10.90.90.90 です。 |
| Subnet Mask | 本スイッチのサブネットを指定します。入力形式：xxx.xxx.xxx.xxx (x は 0～255 の数字)。クラス A ネットワークには 255.0.0.0、クラス B ネットワークには 255.255.0.0、クラス C ネットワークには 255.255.255.0 を入力します。カスタムサブネットマスクも入力できます。 |
| Gateway | 所属するサブネット外の宛先アドレスを持つパケットの送信先。通常 IP ゲートウェイの役割をするルータやホストのアドレスを指定します。ご使用のネットワークがイントラネットの一部でない場合、またはローカルネットワーク外からのスイッチへのアクセスを許可しない場合は、本項目はそのままとします。 |

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

Interface Settings (インタフェース設定)

スイッチの IP インタフェース設定を行います。

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

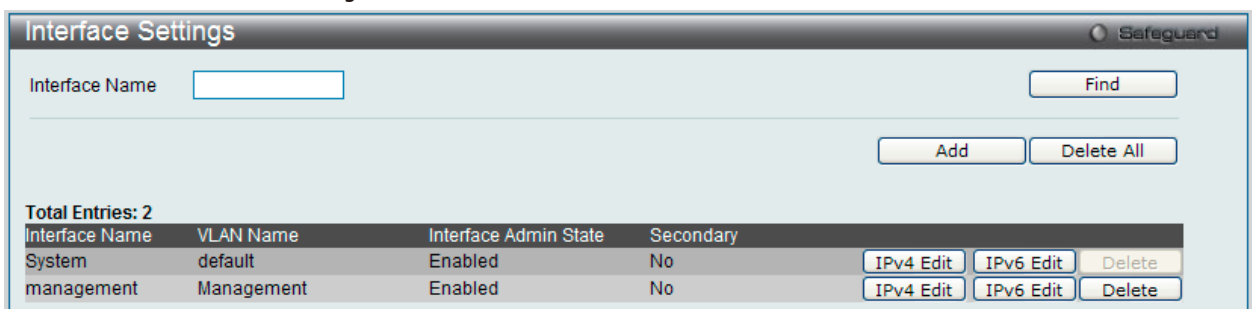


図 7-10 Interface Settings 画面

スイッチの現在の IP インタフェース設定が表示されます。

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

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

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

「Delete」ボタンをクリックして、指定エントリを削除します。

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

IP インタフェースの追加

- 「Add」ボタンをクリックして以下の画面を表示します。

図 7-11 IPv4 Interface Settings 画面

- 以下の項目を設定します。

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

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

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

IPv4 インタフェースの編集

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

図 7-12 IPv4 Interface Settings 画面 - Edit

- 以下の項目を設定します。

| 項目 | 説明 |
|-----------------------|--|
| IP MTU (512-1712) | 使用する IP レイヤの MTU 値を入力します。値は 512-1712 の範囲です。初期値は 1500 です。 |
| IP Directed Broadcast | IP ダイレクトブロードキャストオプションを選択します。指定インタフェースで IP ダイレクトブロードキャストを有効 / 無効にします。 |
| Get IP From | このインタフェースが IP アドレスを取得するのに使用する方式 (Static、DHCP、BOOTP) を指定します。 |
| Interface Name | 編集するインタフェース名が表示されます。 |
| IPv4 Address | 使用する IPv4 アドレスを入力します。 |
| Subnet Mask | 使用する IPv4 サブネットを入力します。 |
| VLAN Name | 使用する VLAN 名を入力します。 |

| 項目 | 説明 |
|--------------------------|---|
| IPv4 State | IPv4 の状態を有効または無効にします。 |
| Interface Admin State | インタフェースの管理を有効または無効にします。 |
| DHCP Option 12 State | プルダウンメニューを使用して「DHCPDISCOVER」「DHCPREQUEST」メッセージ内への Option12 の挿入を有効/無効を設定します。 |
| DHCP Option 12 Host Name | 「DHCPDISCOVER」「DHCPREQUEST」メッセージ内へ挿入するホスト名を入力します。 |

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

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

IPv6 インタフェースの編集

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

The screenshot shows the 'IPv6 Interface Settings' configuration page. It is divided into several sections:

- IPv6 Interface Settings:** Includes fields for Interface Name (System), IPv6 State (Enabled), Interface Admin State (Enabled), IPv6 Network Address (with a hint '(e.g.: 3710::1/64)'), Prefix Name (Max: 12 characters), DHCPv6 Client PD State (Disabled), DHCPv6 Client PD Prefix Name (Max: 12 characters), and DHCPv6 Client (Disabled). There is an 'Apply' button at the end of this section.
- NS Retransmit Time Settings:** Includes NS Retransmit Time (0-4294967295) set to 0 ms, with an 'Apply' button.
- Automatic Link Local State Settings:** Includes Automatic Link Local Address set to Disabled, with an 'Apply' button.
- Router Advertisement Settings:** Includes State (Disabled), Reachable Time (0-3600000) set to 1200000, Hop Limit (0-255) set to 64, Other Configuration Flag (Disabled), Max Router AdvInterval (4-1800) set to 600 sec, Life Time (0-9000) set to 1800 sec, Retransmit Time (0-4294967295) set to 0 ms, Managed Flag (Disabled), and Min Router AdvInterval (3-1350) set to 198 sec. There is an 'Apply' button at the end of this section.

At the bottom, there are links for 'View All IPv6 Address' and 'View Neighbor Discover', and a '<<Back' button.

図 7-13 IPv6 Interface Settings 画面 - Edit

- 以下の項目を使用して設定を行います。

| 項目 | 説明 |
|-------------------------------------|--|
| IP Interface Settings | |
| Interface Name | IPv6 インタフェースの名前が表示されます。 |
| IPv6 State | プルダウンメニューを使って IPv6 ステートの有効/無効を指定します。 |
| Interface Admin State | プルダウンメニューを使用して、管理者ステートを「Enabled」(有効)または「Disabled」(無効)とします。 |
| IPv6 Network Address | ネイバのグローバル/ローカルリンクアドレスを入力できます。 |
| Prefix Name | IPv6 プリフィクス名を指定します。 |
| DHCPv6 Client PD State | DHCPv6 クライアントの PD を有効/無効を指定します。 |
| DHCPv6 Client PD Prefix Name | DHCPv6 クライアントの PD プリフィクス名を指定します。 |
| DHCPv6 Client | DHCPv6 クライアントを有効/無効を指定します。 |
| NS Retransmit Time Settings | |
| NS Retransmit Time (0-4294967295) | ローカルネットワークに送信する Neighbor Solicitation パケットを生成する間隔 (秒) を設定します。これは「config ipv6 nd ra」コマンドの RA 再送信時間と同等の値になり、RA の項目に同期されます。0-4294967295 (ミリ秒) の範囲から指定します。 |
| Automatic Link Local State Settings | |
| Automatic Link Local Address | 本機能を有効/無効にします。有効にすると、IPv6 Link-Local アドレスを自動的に作成します。 |
| Router Advertisement Settings | |
| State | ルータの通知状態を有効または無効にします。 |

| 項目 | 説明 |
|---------------------------------|--|
| Life Time (0-9000) | デフォルトルータとしてのルータの寿命 (秒) を 0-9000 (秒) で指定します。 |
| Reachable Time (0-3600000) | 到達性の確認を受け取った後に、ノードが隣接しているノードを到達可能と見なすまでの時間 (ミリ秒) を指定します。 |
| Retransmit Time (0-4294967295) | ルータ通知メッセージの再送の間隔 (ミリ秒) を指定します。ルータ通知パケットがホストにそれを渡します。 |
| Hop Limit (0-255) | この RA メッセージを受信するホストに送信されるパケットのために IPv6 ヘッダ内の「hop_limit」フィールドの初期値を指定します。 |
| Managed Flag | <ul style="list-style-type: none"> Enabled - この RA を受信するホストは、ステートレスアドレス設定から取得したアドレスに加え、アドレス取得のためにステートフルアドレス設定プロトコルを使用する必要があります。 Disabled - アドレス取得のためにステートフルアドレス設定を使用した RA の受信を停止します。 |
| Other Configuration Flag | <ul style="list-style-type: none"> Enabled - この RA を受信するホストは、ステートレスアドレス設定から取得したアドレスに加え、アドレス取得のためにステートフルアドレス設定プロトコルを使用する必要があります。 Disabled - アドレス取得のためにステートフルアドレス設定を使用した RA の受信を停止します。 |
| Min Router AdvInterval (3-1350) | インタフェースから求められていないマルチキャスト通知が送信される最小時間 (秒) を入力します。本エントリは、3(秒) より大きくし、MaxRtrAdvInterval の 3/4 より大きくしないでください。初期値 : 0.33 * MaxRtrAdvInterval |
| Max Router Advinterval (4-1800) | インタフェースから求められていないマルチキャスト通知が送信される最大時間 (秒) を入力します。4-1800 (秒) で指定します。初期値は 600 (秒) です。 |

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

「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

「[View All IPv6 Address](#)」リンクをクリックして、現在の全 IPv6 アドレスを参照します。

「[View Neighbor Discover](#)」リンクをクリックして、すべての Neighbor 検出情報エントリを参照します。

IPv6 アドレスの参照

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

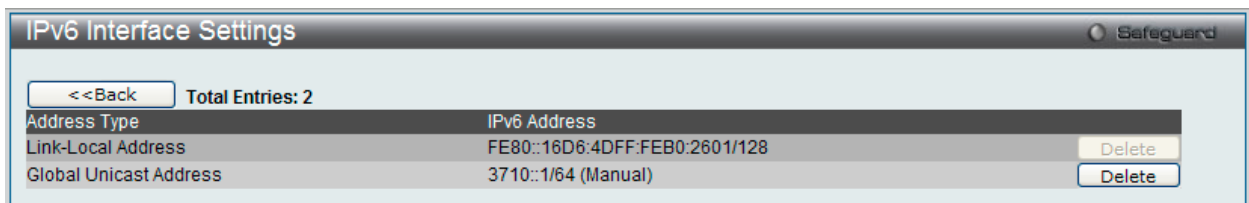


図 7-14 IPv6 Interface Settings 画面

「<<Back」をボタンをクリックして前のページに戻ります。

Neighbor の参照

1. 「[View Neighbor Discover](#)」リンクをクリックすると、以下の画面が表示されます。

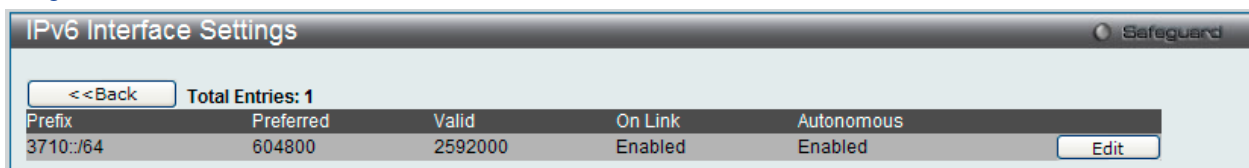


図 7-15 IPv6 Interface Settings 画面

Neighbor の編集

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

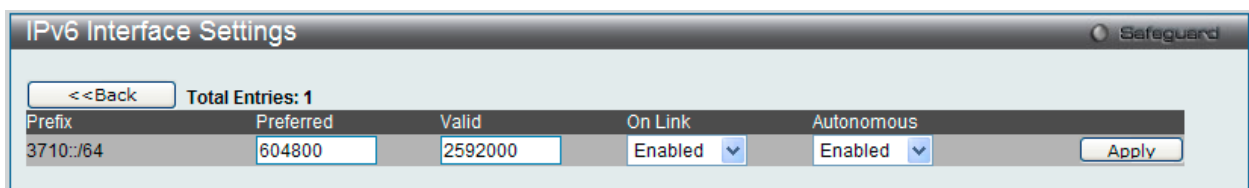


図 7-16 IPv6 Interface Settings 画面 - Edit

2. 設定変更後、「Apply」ボタンをクリックします。

「<<Back」をボタンをクリックして前のページに戻ります。

IPv6 インタフェースの削除

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

Loopback Interface Settings (ループバックインタフェース設定)

ループバックインタフェースを設定します。ループバックインタフェースは、それを無効または削除するまで通常アクティブな論理 IP インタフェースで、どんな物理インタフェースの状態からも独立しています。

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

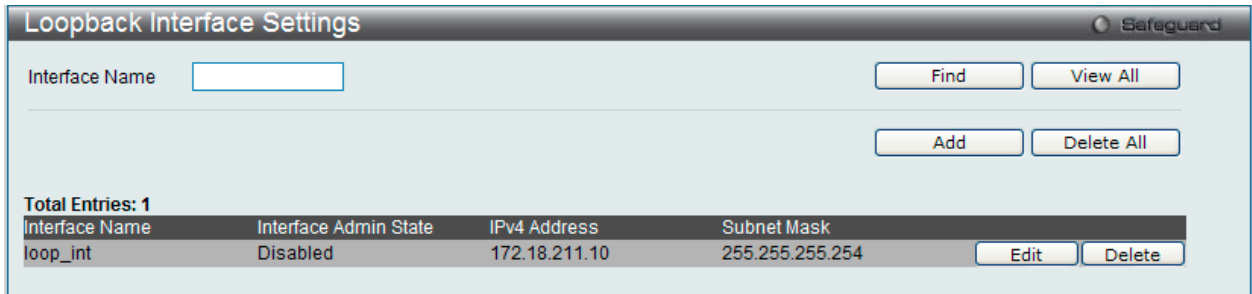


図 7-17 Loopback Interface Settings

以下の項目が表示、または設定変更に使えます。

| 項目 | 説明 |
|----------------|-----------------|
| Interface Name | インタフェース名を入力します。 |

インタフェースの検索

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

ループバックインタフェースの追加、編集

- 「Add」(追加) または 「Edit」(編集) ボタンをクリックして、以下の画面を表示します。

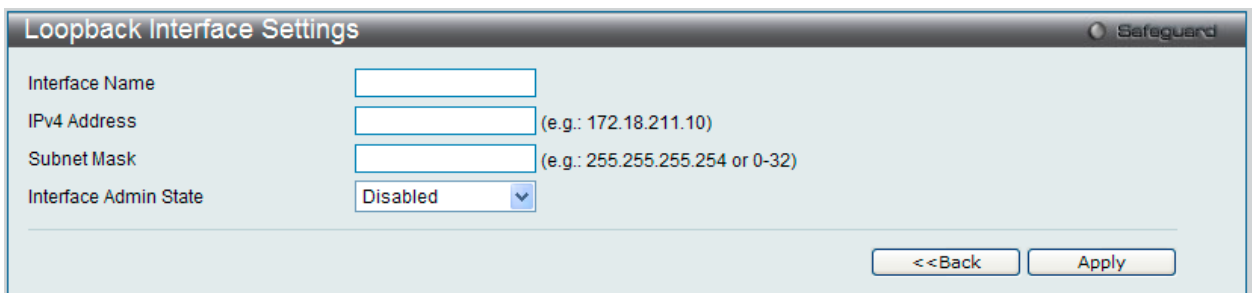


図 7-18 Loopback Interface Settings - Add/Edit 画面

以下の項目が表示、または設定変更に使えます。

| 項目 | 説明 |
|-----------------------|--|
| Interface Name | ループバックインタフェース名 注意 ループバック IP インタフェースには通常の IP インタフェースと共に同じネームドメイン空間を持つため、名前は通常の IP インタフェースと重複することはできません。 |
| IPv4 Address | ループバックインタフェース用に 32 ビットの IPv4 アドレスを入力します。 |
| Subnet Mask | ループバックインタフェースに割り当てるサブネットマスクを入力します。 |
| Interface Admin State | プルダウンメニューを使用して、ループバックインタフェースを「Enabled」(有効)/「Disabled」(無効)にします。 |

- 該当項目を入力後、「Apply」ボタンをクリックし、設定内容を適用します。

「<<Back」ボタンをクリックし、変更を破棄して前のページに戻ります。

インタフェースの削除

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

Management Settings (管理設定)

本スイッチの管理設定を行います。

コマンドラインインターフェースを使用する場合、コンソールの制限を超えた複数ページのスクロールを停止することができます。また、本画面で本スイッチ DHCP 自動設定機能を有効にします。「Enabled」の時、本スイッチは TFTP サーバからコンフィグレーションファイルを受信して、起動時に自動的に DHCP クライアントになるように設定します。この方法を使用するためには、DHCP サーバは TFTP サーバに IP アドレスと DHCP リプライパケット内の設定ファイル名情報を渡すように設定する必要があります。TFTP サーバを起動し、スイッチからリクエストを受信する時、そのベースディレクトリ内に構成ファイルを保管しておく必要があります。クライアントが使用するための設定ファイルに関する詳しい情報は、DHCP サーバまたは TFTP サーバソフトウェアの手順を参照してください。さらに、本マニュアルの「Tools」セクションの「Upload Log File」画面に関する説明を参照ください。

本スイッチが DHCP 自動設定を完了できない場合は、スイッチのメモリ内にある以前に保存したコンフィグレーションが使用されます。

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

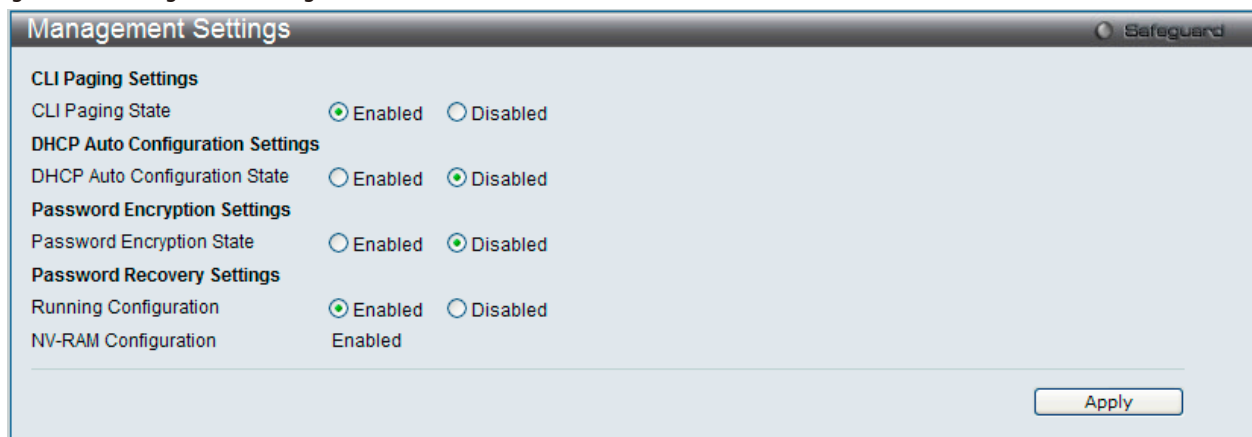


図 7-19 Management Settings 画面

2. 以下の項目を設定します。

| 項目 | 説明 |
|-------------------------------|---|
| CLI Paging State | コマンドラインインターフェースのページング機能はコンソールの終わりで各ページを停止します。これはコンソールの制限を超えた複数ページのスクロールを停止することができます。初期値では CLI ページング機能は有効です。無効にするためには「Disabled」ボタンをクリックします。 |
| DHCP Auto Configuration State | スイッチの DHCP 自動設定機能を有効または無効にします。「Enabled」の時、本スイッチは TFTP サーバからコンフィグレーションファイルを受信して、起動時に自動的に DHCP クライアントになるように設定します。この方法を使用するためには、DHCP サーバは TFTP サーバに IP アドレスと DHCP リプライパケット内の設定ファイル名情報を渡すように設定する必要があります。TFTP サーバを起動し、スイッチからリクエストを受信する時、そのベースディレクトリ内に構成ファイルを保管しておく必要があります。 |
| Password Encryption State | パスワードの暗号化はコンフィグレーションファイル内のパスワード設定を暗号化します。初期値ではパスワードの暗号化は「Disabled」(無効)になっています。パスワードの暗号化を有効にするためには「Enabled」ボタンをクリックします。 |
| Running Configuration | 「Password Recovery」オプションにおける動作中のコンフィグレーションを有効または無効にすることができます。有効にすると、動作中のコンフィグレーションのパスワードリカバリの実行を可能とします。 |

「Apply」ボタンをクリックして行った変更を適用します。

Out of Band Management Settings (アウトバンド管理設定)

アウトバンド管理ポートを設定します。

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

図 7-20 Out of Band Management Settings 画面

2. 以下の項目を設定します。

| 項目 | 説明 |
|-------------|---------------------------|
| IP Address | 使用する IP アドレスを入力します。 |
| Subnet Mask | 使用するサブネットを入力します。 |
| Gateway | 使用するゲートウェイ IP アドレスを入力します。 |
| Status | アウトバンド管理の状態を有効または無効にします。 |
| Link Status | リンクステータスを表示します。 |

「Apply」 ボタンをクリックして行った変更を適用します。

Session Table (セッションテーブル)

スイッチが最後に起動してからの管理セッションを表示します。

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

| ID | Live Time | From | Level | Name |
|----|--------------|-------------|-------|-----------|
| 8 | 00:01:24.110 | Serial Port | 1 | Anonymous |

図 7-21 Session Table 画面

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

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

シングル IP マネジメント (SIM) の概要

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

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

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

- SIM はスイッチのオプション機能であり、CLI または Web インタフェース経由で簡単に有効 / 無効にできます。また、SIM グループはご使用のネットワーク内でスイッチの操作に影響を与えることはありません。
- SIM には 3 つのクラスのスイッチがあります。Commander Switch (CS) はグループのマスタスイッチ、Member Switch (MS) は CS によって SIM グループのメンバとして認識されるスイッチ、Candidate Switch (CaS) は SIM グループに物理的にリンクはしているが、SIM グループのメンバとして認識されていないスイッチです。
- 1 つの SIM グループには、Commander Switch (CS) を 1 つだけ持つことができます。
- 特定の SIM グループ内のすべてのスイッチは、同じ IP サブネット（ブロードキャストドメイン）内にある必要があります。ルータを越えた位置にあるメンバの設定はできません。
- 1 つの SIM グループには、Commander Switch (番号 : 0) を含めず、最大 32 台のスイッチ (番号 : 1-32) が所属できます。
- 同じ IP サブネット（ブロードキャストドメイン）内の SIM グループ数に制限はありませんが、各スイッチは、1 つの SIM グループにしか所属することができません。
- マルチプル VLAN が設定されていると、SIM グループはスイッチ上のデフォルト VLAN だけを使用します。
- SIM は SIM をサポートしていないデバイスを經由することができます。そのため CS から 1 ホップ以上はなれたスイッチを管理することができます。

SIM グループは 1 つのエンティティとして管理されるスイッチのグループです。SIM スイッチは 3 つの異なる役割を持っています。

1. Commander Switch (CS) - グループの管理用デバイスとして手動で設定されるスイッチで、以下の特長を持っています。
 - IP アドレスを 1 つ持つ。
 - 他のシングル IP グループの CS や MS ではない。
 - マネジメント VLAN 経由で MS に接続する。
2. Member Switch (MS) - シングル IP グループに所属するスイッチで、CS からアクセスが可能です。MS は以下の特徴を持ちます。
 - 他のシングル IP グループの CS や MS ではない。
 - CS マネジメント VLAN 経由で CS に接続する。
3. Candidate Switch (CaS) - SIM グループに参加する準備が整っているが、まだ MS ではないスイッチです。CaS を SIM グループ内の MS として、本スイッチの機能を使用して手動で登録することが可能です。CaS として登録されたスイッチは、SIM グループには所属せず、以下の特長を持っています。
 - 他のシングル IP グループの CS や MS ではない。
 - CS マネジメント VLAN 経由で CS に接続する。

上記の役割には、以下のルールを適用します。

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

SIM グループの CS として運用するスイッチを 1 台登録した後、スイッチを手動によりグループに追加して MS とします。CS はその後 MS へのアクセスのためにインバンドエントリーポイントとして動作します。CS の IP アドレスがグループのすべての MS への経路になり、CS の管理パスワードや認証によって、SIM グループのすべての MS へのアクセスを制御します。

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

CS が MS に遷移すると、自動的に CS が所属する最初の SNMP コミュニティ（リード権 / ライト権、リード権だけを含む）のメンバになります。しかし、自身の IP アドレスを持つ MS は、グループ内の他のスイッチ（CS を含む）が所属していない SNMP コミュニティに加入することができます。

Single IP Settings (シングル IP 設定)

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

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

図 7-22 Single IP Settings 画面 (CaS 無効状態)

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

図 7-23 Single IP Settings 画面 (CS 有効状態)

3. 「Apply」ボタンをクリックして、設定を有効にします。

以下の項目が使用できます。

| 項目 | 説明 |
|----------------------------|---|
| SIM State | プルダウンメニューから「Enabled」(有効)または「Disabled」(無効)を選択します。「Disabled」を選択すると、スイッチのすべての SIM 機能が無効になります。初期値は「Disabled」です。 |
| Role State | プルダウンメニューからスイッチの SIM での役割を選択します。以下の 2 つから選択できます。 <ul style="list-style-type: none"> • Candidate - Candidate Switch (CaS) は SIM グループメンバではありませんが、Commander スイッチに接続しています。本スイッチの SIM 機能の初期設定です。 • Commander - Commander Switch (CS)。ユーザは CS に他のスイッチを参加させて SIM グループを作成します。このオプションを選択すると、本スイッチは SIM 機能対象のスイッチとして設定されます。 |
| Group Name | SIM グループ名を入力します。 |
| Discovery Interval (30-90) | スイッチが Discovery パケットを送信する Discovery プロトコル送信間隔 (秒) を設定します。CS スイッチに情報が送られてくると、接続する他のスイッチ (MS、CaS) の情報が CS に組み込まれます。値は 30-90 (秒) の間から指定します。初期値は 30 (秒) です。 |
| Hold Time Count (100-255) | 他のスイッチが「Discovery Interval」の間隔で送信してきた情報をスイッチが保持する時間 (秒) を指定します。値は 100-255 (秒) の間から指定します。初期値は 100 (秒) です。 |

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

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

Topology (トポロジ)

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

Management > Single IP Management > Topology の順にメニューをクリックします。

サーバ上で Java Runtime Environment が起動し、以下の画面が表示されます。

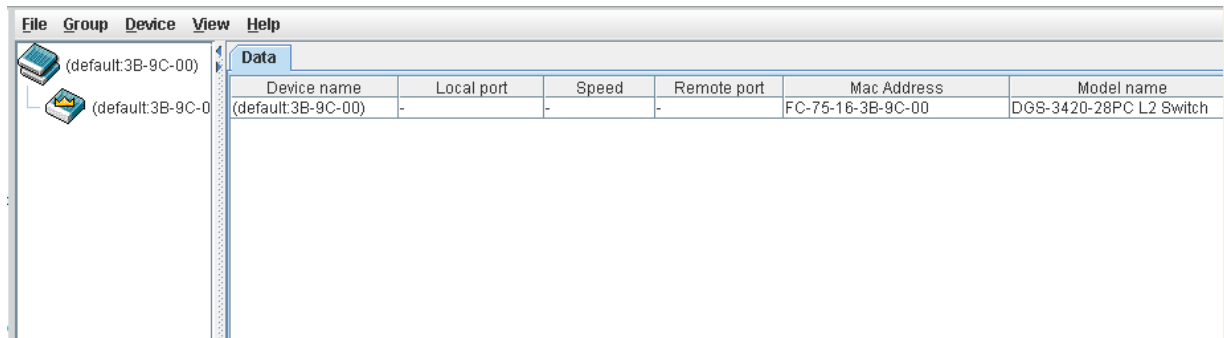


図 7-24 トポロジ画面

トポロジ画面の「Data」タブには以下の情報が表示されます。

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

トポロジマップの表示

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

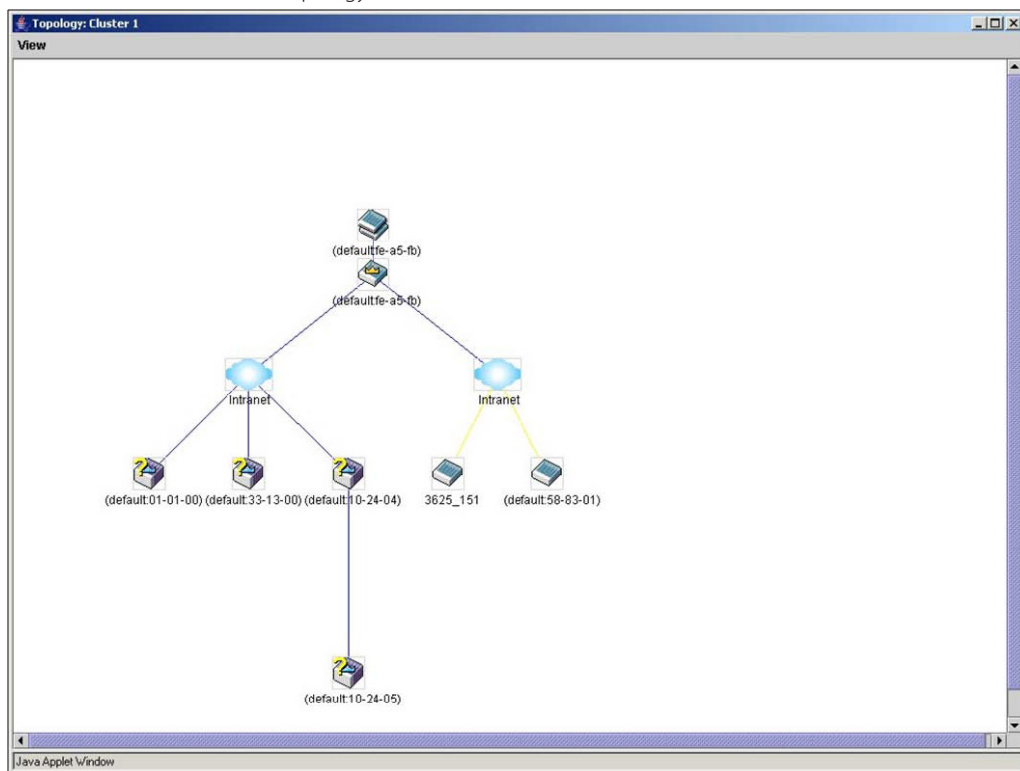













図 7-25 Topology 画面

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

本画面で表示されるアイコンは以下の通りです。

Management (スイッチの管理)

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

ツールヒント

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

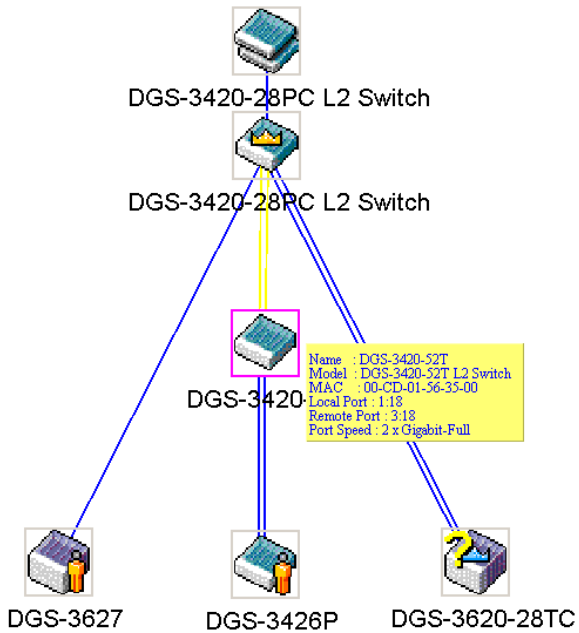


図 7-26 ツールヒントを利用したデバイス情報の表示

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

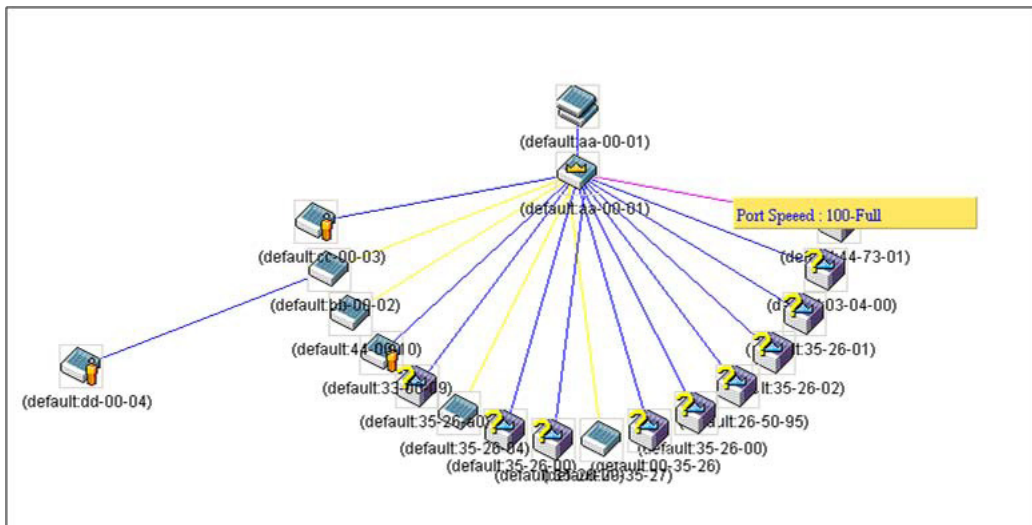


図 7-27 ツールヒントを利用したポート速度の表示

右クリックメニュー

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

グループアイコン

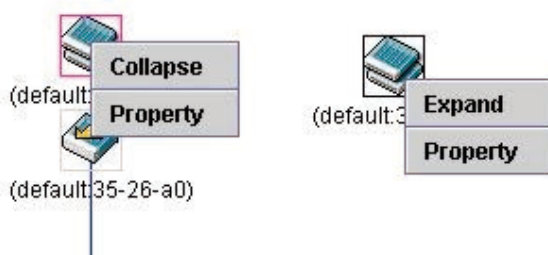


図 7-28 グループアイコン上での右クリック

以下のオプションが表示されます。

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

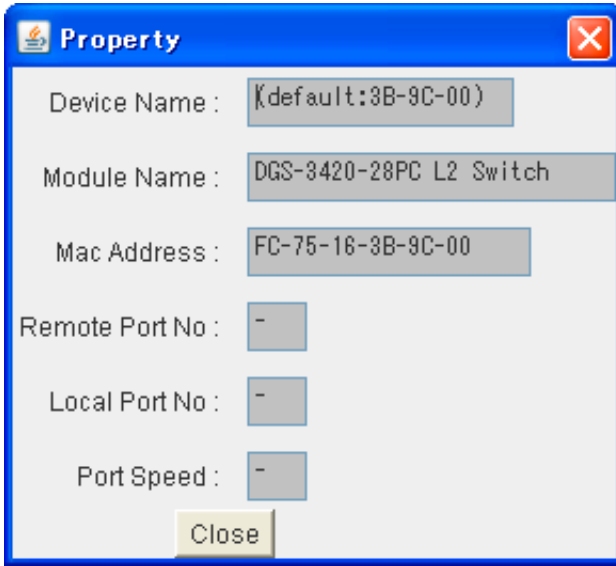


図 7-29 Property 画面

画面には以下の情報が表示されます。

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

「Close」ボタンをクリックし、「Property」画面を閉じます。

Commander スイッチアイコン

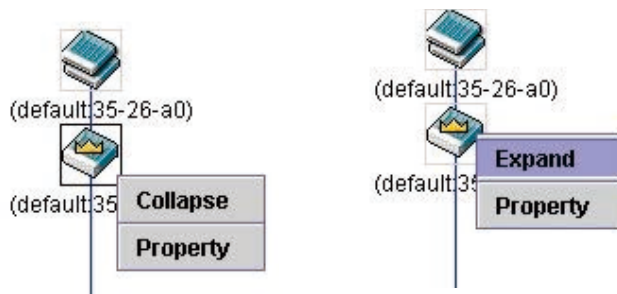


図 7-30 Commander スイッチアイコン上での右クリック

以下のオプションが表示されます。

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

Member スイッチアイコン

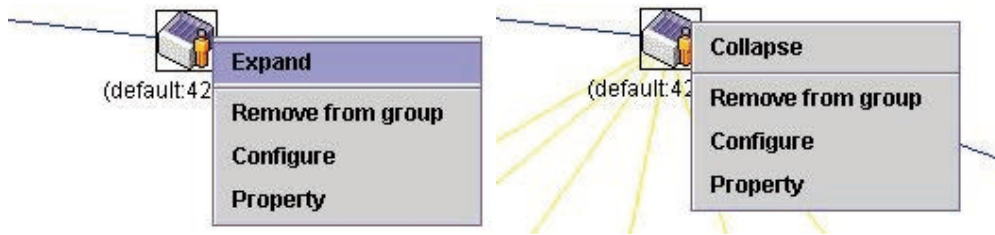


図 7-31 Member スイッチアイコン上での右クリック

以下のオプションが表示されます。

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

Candidate スイッチアイコン

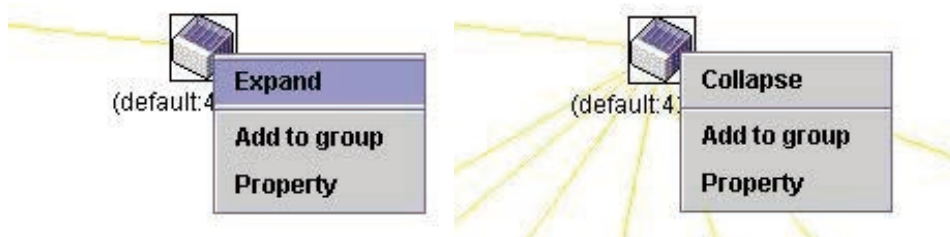


図 7-32 Candidate スイッチアイコン上での右クリック

以下のオプションが表示されます。

- Collapse – グループのアイコンを折りたたみ、1つのアイコンに代表させます。
- Expand – グループのアイコンを展開し、隠れているすべてのアイコンを表示させます。
- Add to group – CaS をグループに追加します。このオプションを選択すると、以下のパスワード入力画面が表示され、CaS スイッチを SIM グループに追加するための認証を行います。パスワードを入力して「OK」ボタンをクリックするか、「Cancel」ボタンをクリックして画面を閉じます。



図 7-33 Input password ダイアログボックス

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

メニューバー

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



File Group Device View Help

図 7-34 トポロジビュー内のメニューバー

メニューバーには以下の5つのメニューが存在します。

「File」メニュー

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

「Group」メニュー

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

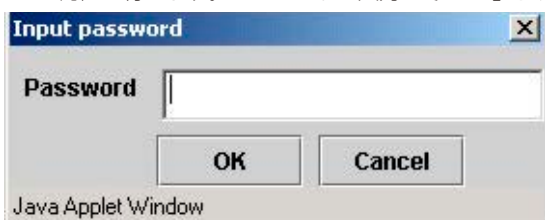


図 7-35 Input password ダイアログボックス

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

「Device」メニュー

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

「View」メニュー

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

「Help」メニュー

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

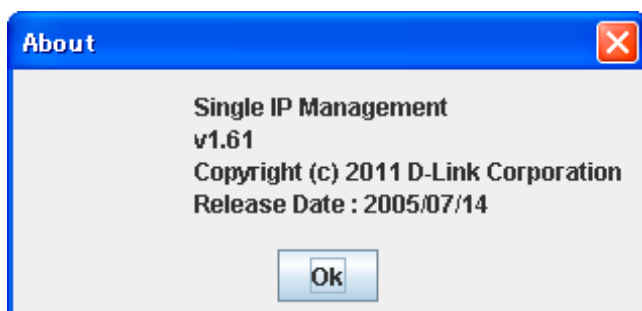


図 7-36 About ダイアログボックス

Firmware Upgrade (ファームウェア更新)

CS から MS へのファームウェアの更新を行います。

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

図 7-37 Firmware Upgrade 画面

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

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

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

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

図 7-38 Configuration File Backup/Restore 画面

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

Upload Log File (ログファイルのアップロード)

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

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

図 7-39 Upload Log File 画面

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

SNMP Settings (SNMP 設定)

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

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

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

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

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

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

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

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

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

トラップ

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

MIB

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

本スイッチシリーズは、スイッチの環境に合わせた柔軟性のある SNMP 管理機能を採用しています。SNMP 管理機能は、ネットワークの要求やネットワーク管理者の好みに合わせてカスタマイズすることができます。SNMP バージョンの選択は、「SNMP V3」メニューから行うことができます。

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

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

SNMP Global Settings (SNMP グローバル設定)

SNMP グローバルステート設定を有効または無効にします。

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

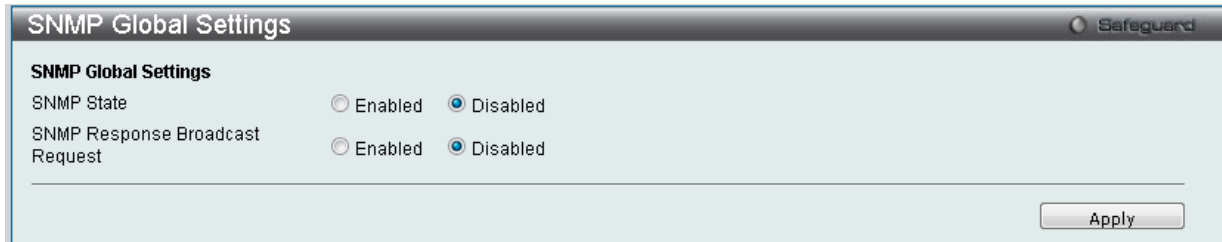


図 7-40 SNMP Global Settings 画面

2. 以下の項目を設定します。

| 項目 | 説明 |
|---------------------------------|---|
| SNMP State | SNMP 機能を使用するためには本オプションを有効にします。 |
| SNMP Response Broadcast Request | 「SNMP Response Broadcast Request」オプションを有効 / 無効にします。 |

「Apply」ボタンをクリックして行った変更を適用します。

SNMP Trap Settings (SNMP トラップ設定)

スイッチの SNMP 機能のトラップ設定を有効または無効にします。

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



図 7-41 SNMP Traps Settings 画面

2. 以下の項目を設定します。

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

「Apply」ボタンをクリックして行った変更を適用します。

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

SNMP リンクチェンジトラップを設定します。

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

図 7-42 SNMP Linkchange Traps Settings 画面

2. 以下の項目を設定します。

| 項目 | 説明 |
|---------------------|-------------------------------|
| Unit | 設定するユニットを選択します。 |
| From Port / To Port | 使用する開始 / 終了ポートを選択します。 |
| State | SNMP リンクチェンジトラップを有効または無効にします。 |

「Apply」ボタンをクリックして行った変更を適用します。

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

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

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

図 7-43 SNMP View Table Settings 画面

エントリの削除

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

エントリの新規作成

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

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

以下の項目が使用されます。

| 項目 | 説明 |
|-----------|---|
| View Name | 32 文字までの半角英数字を入力します。新しい SNMP ビューを登録し、識別する際に使用します。 |

| 項目 | 説明 |
|-------------|--|
| Subtree OID | ビューの OID (Object Identifier) サブツリーを入力します。OID は、オブジェクトツリー (MIB ツリー) が SNMP マネージャによってアクセス可能な範囲かどうかを識別します。 |
| View Type | 「Subtree OID」で指定した OID が、SNMP マネージャがアクセス可能な範囲であるかを指定します。 <ul style="list-style-type: none"> • Included - アクセス可能になります。 • Excluded - アクセス不可能になります。 |

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

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

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

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

エントリの設定

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

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

図 7-44 SNMP Community Table Settings 画面

以下の項目が使用されます。

| 項目 | 説明 |
|----------------|---|
| Community Name | 32 文字までの半角英数字を入力し、SNMP コミュニティメンバを識別します。本コミュニティ名は、リモートの SNMP マネージャが、スイッチの SNMP エージェント内の MIB オブジェクトにアクセスする際にパスワードのように使用します。 |
| View Name | 32 文字までの半角英数字を入力します。本値は、リモート SNMP マネージャがアクセスすることのできる MIB グループの定義に使用します。View Name は「SNMP View Table」に存在する必要があります。 |
| Access Right | <ul style="list-style-type: none"> • Read Only - 指定した「Community Name」を使用する SNMP コミュニティメンバは、スイッチの MIB の内容について読み出しのみ可能となります。 • Read Write - 指定した「Community Name」を使用する SNMP コミュニティメンバは、スイッチの MIB の内容について読み出し、および書き込みが可能です。 |

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

エントリの削除

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

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

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

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

| Group Name | Read View Name | Write View Name | Notify View Name | User-based Security Model | Security Level | |
|---------------|----------------|-----------------|------------------|---------------------------|----------------|--------|
| public | CommunityV... | | CommunityV... | SNMPv1 | NoAuthNoPriv | Delete |
| public | CommunityV... | | CommunityV... | SNMPv2 | NoAuthNoPriv | Delete |
| initial | restricted | | restricted | SNMPv3 | NoAuthNoPriv | Delete |
| private | CommunityV... | CommunityV... | CommunityV... | SNMPv1 | NoAuthNoPriv | Delete |
| private | CommunityV... | CommunityV... | CommunityV... | SNMPv2 | NoAuthNoPriv | Delete |
| test_group | read_test_... | write_test... | notify_tes... | SNMPv1 | NoAuthNoPriv | Delete |
| test_commu... | view_test | | view_test | SNMPv1 | NoAuthNoPriv | Delete |
| test_commu... | view_test | | view_test | SNMPv2 | NoAuthNoPriv | Delete |

図 7-45 SNMP Group Table Settings 画面

エントリの削除

削除するエントリの行の「Delete」ボタンをクリックします。

エントリの新規登録

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

以下の項目が使用されます。

| 項目 | 説明 |
|---------------------------|---|
| Group Name | 32 文字までの半角英数字を入力します。SNMP ユーザのグループの識別に使用します。 |
| Read View Name | SNMP メッセージを要求する SNMP グループ名を入力します。 |
| Write View Name | スイッチの SNMP エージェントに書き込み権限を与える SNMP グループ名を入力します。 |
| Notify View Name | スイッチの SNMP エージェントによるトラップメッセージを送信する SNMP グループ名を入力します。 |
| User-based Security Model | <ul style="list-style-type: none"> SNMPv1 - SNMP バージョン 1 が使用されます。 SNMPv2 - SNMP バージョン 2c が使用されます。SNMP バージョン 2 は集中型、分散型どちらのネットワーク管理にも対応します。SNMP バージョン 1 と比較して SMI (Structure of Management Information) およびセキュリティ機能において強化されています。 SNMPv3 - SNMP バージョン 3 が使用されます。ネットワーク上で認証とパケットの暗号化を併用することにより、デバイスへの安全なアクセスを提供します。 |
| Security Level | セキュリティレベル設定は SNMP バージョン 3 にのみ適用されます。 <ul style="list-style-type: none"> NoAuthNoPriv - 認証なし。スイッチとリモート SNMP マネージャ間の暗号化パケットの送信もないことを示します。 AuthNoPriv - 認証あり。スイッチとリモート SNMP マネージャ間の暗号化パケットの送信がないことを示します。 AuthPriv - 認証あり。スイッチとリモート SNMP マネージャ間のパケットも暗号化されて送信されることを示します。 |

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

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

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

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

図 7-46 SNMP Engine ID Settings 画面

以下の項目を使用します。

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

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

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

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

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

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

図 7-47 SNMP User Table Settings 画面

エントリの削除

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

エントリの新規登録

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

上記画面中の項目を以下に示します。

| 項目 | 説明 |
|--------------------|---|
| User Name | 32 文字までの半角英数字。SNMP ユーザを識別します。 |
| Group Name | 作成した SNMP グループが SNMP メッセージを要求するために使用される名前です。 |
| SNMP Version | <ul style="list-style-type: none"> V1 - SNMP バージョン 1 が使用されています。 V2 - SNMP バージョン 2 が使用されています。 V3 - SNMP バージョン 3 が使用されています。 |
| SNMP V3 Encryption | SNMP V3 に対して暗号化を有効にします。本項目は「SNMP Version」で「V3」を選択した場合に有効になります。 <ul style="list-style-type: none"> None - ユーザ認証は使用しません。 Key - HMAC-MD5 アルゴリズムまたは HMAC-SHA-96 アルゴリズムレベルのユーザ認証を行います。 Password - HMAC-SHA-96 アルゴリズムレベルのパスワードか HMAC-MD5-96 パスワードによる認証を行います。 |

Management (スイッチの管理)

| 項目 | 説明 |
|-------------------------------|---|
| Auth-Protocol by Password/Key | 本項目は「SNMP Version」で「V3」を選択され、「SNMP V3 Encryption」で「Password」または「Key」を選択した場合に有効になります。本項目を選択後、「Password」/「Key」にパスワードを入力します。 <ul style="list-style-type: none"> MD5 - HMAC-MD5-96 認証レベルが使用されます。 SHA - HMAC-SHA 認証プロトコルが使用されます。 |
| Priv-Protocol by Password/Key | 本項目は「SNMP Version」で「V3」を選択され、「SNMP V3 Encryption」で「Password」または「Key」を選択した場合に有効になります。 <ul style="list-style-type: none"> None - 認証プロトコルは使用されていません。 DES - CBC-DES (DES-56) 標準に基づく DES 56 ビット暗号化方式が使用されています。本項目を選択後、「Password」/「Key」にパスワード（半角英数字 8-16 文字）を入力します。 |

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

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

IPv4 用の SNMP トラップの送信先を設定します。

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

図 7-48 SNMP Host Table Settings 画面

エントリの新規登録

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

以下の項目を設定します。

| 項目 | 説明 |
|-------------------------------------|--|
| Host IP Address | スイッチの SNMP ホストとなるリモート管理ステーション（トラップの送信先）の IP アドレスを入力します。 |
| User-based Security Model | <ul style="list-style-type: none"> SNMPv1 - SNMP バージョン 1 が使用されます。 SNMPv2c - SNMP バージョン 2c が使用されます。 SNMPv3 - SNMP バージョン 3 が使用されます。 |
| Security Level | <ul style="list-style-type: none"> NoAuthNoPriv - NoAuth-NoPriv セキュリティレベルが使用されます。 AuthNoPriv - Auth-NoPriv セキュリティレベルが使用されます。 AuthPriv - Auth-Priv セキュリティレベルが使用されます。 |
| Community String / SNMPv3 User Name | コミュニティ名または SNMP V3 ユーザ名を入力します。 |

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

エントリの削除

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

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

IPv6 用の SNMP トラップの送信先を設定します。

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

図 7-49 SNMP v6Host Table Settings 画面

エントリの新規登録

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

以下の項目を設定します。

| 項目 | 説明 |
|---------------------------------------|--|
| Host IPv6 Address | スイッチの SNMP ホストとなるリモート管理ステーション (トラップの送信先) の IPv6 アドレスを入力します。 |
| User-based Security Model | <ul style="list-style-type: none"> SNMPv1 - SNMP バージョン 1 が使用されます。 SNMPv2c - SNMP バージョン 2c が使用されます。 SNMPv3 - SNMP バージョン 3 が使用されます。 |
| Security Level | <ul style="list-style-type: none"> NoAuthNoPriv - NoAuth-NoPriv セキュリティレベルが使用されます。 AuthNoPriv - Auth-NoPriv セキュリティレベルが使用されます。 AuthPriv - Auth-Priv セキュリティレベルが使用されます。 |
| Community String/ SNMPv3 User Name | コミュニティ名または SNMP V3 ユーザ名を入力します。 |

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

エントリの削除

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

RMON Settings (RMON 設定)

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

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

図 7-50 RMON Settings 画面

以下の項目を設定します。

| 項目 | 説明 |
|-------------------------|--|
| RMON Rising Alarm Trap | RMON 上昇アラームトラップ機能を使用するためには本オプションを有効にします。 |
| RMON Falling Alarm Trap | RMON 下降アラームトラップ機能を使用するためには本オプションを有効にします。 |

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

SNMP Community Encryption Settings (SNMP コミュニティ暗号化設定)

SNMP コミュニティ名の暗号化状態を有効または無効にします。

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

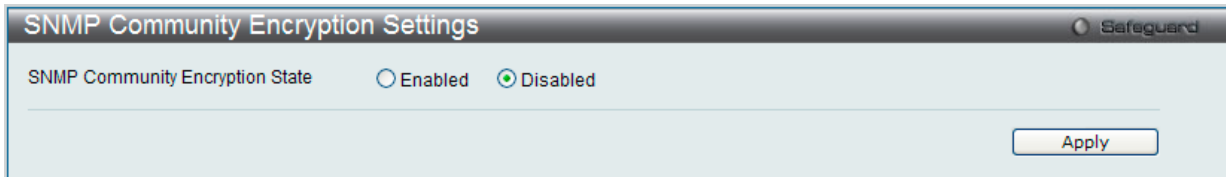


図 7-51 SNMP Community Encryption Settings 画面

以下の項目を設定します。

| 項目 | 説明 |
|---------------------------------|--|
| SNMP Community Encryption State | ラジオボタンを使用して暗号化を「Enabled」(有効) / 「Disabled」(無効)にします。 |

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

SNMP Community Masking Settings (SNMP コミュニティマスク設定)

SNMP コミュニティ名を作成するためのセキュリティ方式を選択します。ただし、コミュニティ名の暗号化の有無は、SNMP コミュニティ暗号化状態に従います。

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

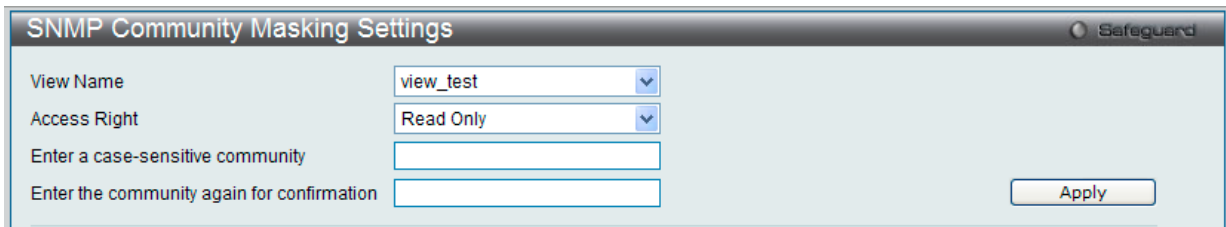


図 7-52 SNMP community Masking Settings 画面

以下の項目を設定します。

| 項目 | 説明 |
|--|---|
| View Name | プルダウンメニューを使用して、MIB ビュー名を選択します。 |
| Access Right | コミュニティ名を使用するユーザのアクセス権を選択します。利用可能なオプションは、「Read Only」と「Read Write」です。 |
| Enter a case-sensitive community | コミュニティ名 (大文字小文字区別あり) を入力します。 |
| Enter the community again for confirmation | 確認のために、再度コミュニティ名を入力します。 |

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

Telnet Settings (Telnet 設定)

スイッチに Telnet 設定をします。

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

図 7-53 Telnet Settings 画面

以下の項目を使用して設定、表示を行います。

| 項目 | 説明 |
|---------------------------|---|
| Telnet Settings | |
| Telnet State | Telnet 設定は初期値で「Enabled」(有効)です。Telnet 経由のシステム設定を許可しない場合は、「Disabled」(無効)を選択します。 |
| Port (1-65535) | スイッチの Telnet 管理に使用される TCP ポート番号。Telnet プロトコルに通常使用される TCP ポートは 23 です。 |
| Telnet Source IP Settings | |
| Interface Name | 「Telnet Source IP Settings」のインタフェース名を入力します。 |
| IPv4 Address | 「Telnet Source」の IPv4 アドレスを入力します。 |
| IPv6 Address | 「Telnet Source」の IPv6 アドレスを入力します。 |

「Apply」ボタンをクリックし、Telnet 設定を適用します。

「Clear IP Address」ボタンをクリックすると入力した IP アドレスが消去されます。

Web Settings (Web 設定)

スイッチに Web ステータスを設定します。

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

図 7-54 Web Settings 画面

以下の項目を使用して設定、表示を行います。

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

「Apply」ボタンをクリックし、Web 設定を適用します。

Power Saving (省電力機能)

本スイッチはスイッチの電源を節電する機能 (D-Link Green) テクノロジーを実装しています。

LED State Settings (LED 設定)

ポート LED の状態について設定します。

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

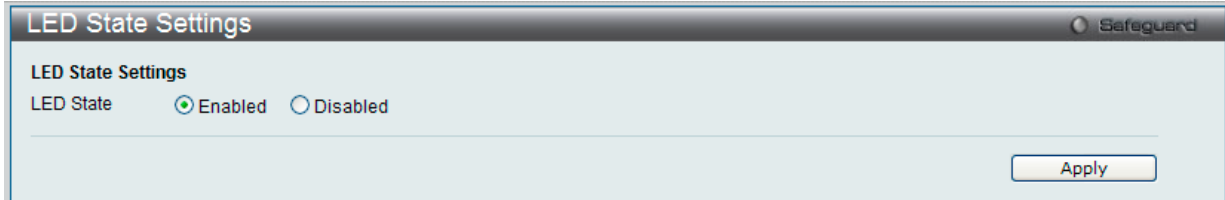


図 7-55 LED State Settings 画面

以下の項目が使用されます。

| 項目 | 説明 |
|-----------|-------------------------|
| LED State | ポート LED の有効 / 無効を選択します。 |

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

Power Saving Settings (省電力設定)

スイッチの内蔵電源を節電する機能を実装しています。省電力機能を使用する時間を設定します。

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

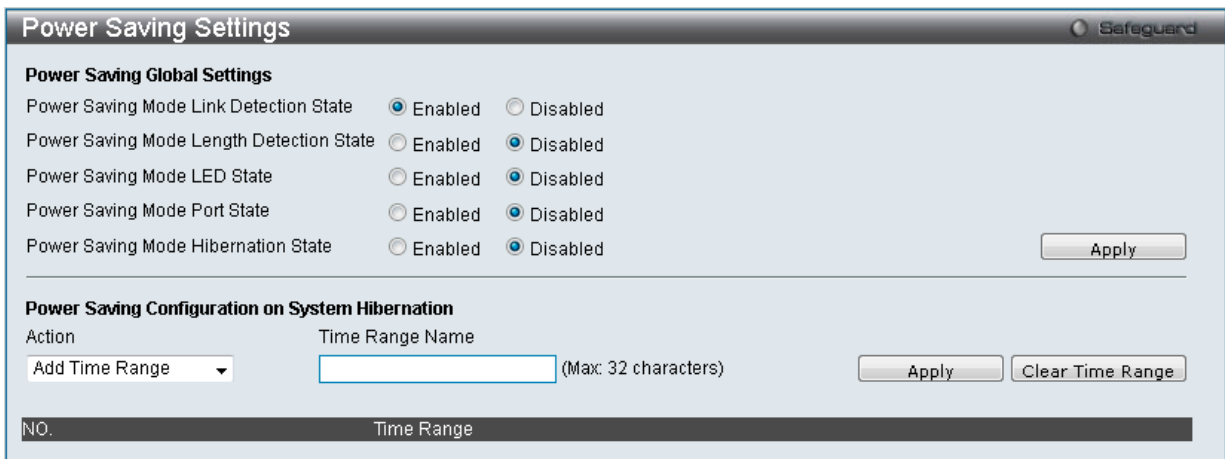


図 7-56 Power Saving Settings 画面

以下の項目が使用されます。

| 項目 | 説明 |
|--|---|
| Power Saving Global Settings | |
| Power Saving Mode Link Detection State | リンク検知の有効 / 無効を設定します。有効の場合、リンクダウンしているポートへの電力供給は行われず、スイッチの電力消費を抑えます。ポートがリンクアップしている場合は通常通り動作します。 |
| Power Saving Mode Length Detection State | ケーブル長検知の有効 / 無効を設定します。有効の場合、スイッチは自動的にケーブルの長さを検知しトラフィックに必要な電力をポートへの供給します。 |
| Power Saving Mode LED State | LED の有効 / 無効を設定します。有効の場合、設定した時間内にポート LED は点灯されません。 |
| Power Saving Mode Port State | ポート起動の有効 / 無効を設定します。有効の場合、設定した時間内ポートはシャットダウンされます。 |
| Power Saving Mode Hibernation State | スイッチ休止の有効 / 無効を設定します。有効の場合、設定した時間内スイッチは低電力モードに移行し、アイドル状態となり全ポート / 全ネットワーク機能 (telnet、ping、その他) はシャットダウンされます。RS232 ポートを使用したコンソール機能のみ有効です。スイッチに PoE 給電機能がある場合も、ポートに電力は給電されません。 |
| Power Saving Configuration on System Hibernation | |
| Action | スケジュールの追加 / 削除を行います。 |
| Time Range Name | スケジュール名を設定します。 |

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

全エントリを削除する際は、「Clear Time Range」ボタンをクリックします。

Power Saving LED Settings (LED 省電力設定)

ポート LED 省電力機能の設定を行います。

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

図 7-57 Power Saving LED Settings 画面

以下の項目が使用されます。

| 項目 | 説明 |
|-----------------|----------------------|
| Action | スケジュールの追加 / 削除を行います。 |
| Time Range Name | スケジュール名を設定します。 |

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

Power Saving Port Settings (ポート省電力設定)

ポート省電力機能の設定を行います。

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

図 7-58 Power Saving Port Settings 画面

以下の項目が使用されます。

| 項目 | 説明 |
|---------------------|----------------------|
| Unit | 設定するユニットを選択します。 |
| From Port / To Port | 設定するポート範囲を選択します。 |
| Action | スケジュールの追加 / 削除を行います。 |
| Time Range Name | スケジュール名を設定します。 |

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

第 8 章 L2 Features (L2 機能の設定)

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

以下は L2 Features サブメニューの説明です。

必要に応じて、設定 / 変更 / 修正を行ってください。

| サブメニュー | 説明 | 参照ページ |
|---|--|---------------------|
| VLAN (VLAN 設定) | 802.1Q スタティック VLAN 設定を行います。以下のメニューがあります。 802.1Q VLAN Settings (802.1Q VLAN 設定)、802.1v Protocol VLAN (802.1v プロトコル VLAN)、Asymmetric VLAN Settings (Asymmetric VLAN 設定)、GVRP (GVRP の設定)、MAC-based VLAN Settings (MAC ベース VLAN 設定)、Private VLAN Settings (プライベート VLAN 設定)、PVID Auto Assign Settings (PVID 自動割り当て設定)、Subnet VLAN (サブネット VLAN)、VLAN Precedence Settings (VLAN 優先度設定)、Voice VLAN (音声 VLAN)、VLAN Trunk Settings (VLAN トランク設定)、Browse VLAN (VLAN の参照)、Show VLAN Ports (VLAN ポートの参照) | 111 |
| QinQ (QinQ 設定) | Q-in-Q 機能を有効または無効にします。次のメニューがあります。 QinQ Settings (QinQ 設定)、VLAN Translation Settings (VLAN 変換機能の設定) | 129 |
| Layer 2 Protocol Tunneling Settings (レイヤ 2 プロトコルトンネリング設定) | レイヤ 2 プロトコルトンネリング機能を設定します。 | 134 |
| Spanning Tree (スパニングツリーの設定) | スパニングツリープロトコルの設定を行います。以下のメニューがあります。 STP Bridge Global Settings (STP ブリッジグローバル設定)、STP Port Settings (STP ポートの設定)、MST Configuration Identification (MST の設定)、STP Instance Settings (STP インスタンス設定)、MSTP Port Information (MSTP ポート情報) | 135 |
| Link Aggregation (ポートトラッキングの設定) | ポートトラッキング設定を行います。以下のメニューがあります。 Port Trunking Settings (ポートトラッキング設定)、LACP Port Settings (LACP ポートの設定) | 143 |
| FDB (FDB 設定) | スタティック FDB、MAC アドレスエイジングタイム、MAC アドレステーブルなどを設定します。以下のメニューがあります。 Static FDB Settings (スタティック FDB の設定)、MAC Notification Settings (MAC 通知設定)、MAC Address Aging Time Settings (MAC アドレスエイジングタイムの設定)、MAC Address Table (MAC アドレステーブル)、ARP & FDB Table (ARP と FDB テーブル) | 146 |
| L2 Multicast Control (L2 マルチキャストコントロール) | IGMP プロキシ、MLD プロキシ、IGMP Snooping、MLD Snooping の設定を行います。以下のメニューがあります。 IGMP Proxy (IGMP プロキシ)、IGMP Snooping (IGMP Snooping の設定)、MLD Proxy (MLD プロキシ)、MLD Snooping (MLD Snooping 設定)、Multicast VLAN (マルチ VLAN)、IP Multicast VLAN Replication (IP マルチキャスト VLAN レプリケーション) | 151 |
| Multicast Filtering (マルチキャストフィルタリング) | マルチキャストフィルタリングの設定を行います。以下のメニューがあります。 IPv4 Multicast Filtering (IPv4 マルチキャストフィルタリング)、IPv6 Multicast Filtering (IPv6 マルチキャストフィルタリング)、Multicast Filtering Mode (マルチキャストフィルタリングモード) | 179 |
| ERPS Settings (イーサネットリングプロテクション設定) | イーサネットリングプロテクション設定を有効にします。 | 188 |
| LLDP (LLDP 設定) | LLDP 設定を行います。以下のメニューがあります。 LLDP (LLDP 設定)、LLDP-MED (LLDP-MED 設定) | 191 |
| NLB FDB Settings (NLB FDB 設定) | NLB 機能を設定します。 | 200 |
| PTP (PTP の設定) | PTP システムを設定します。以下のメニューがあります。 PTP Global Settings (PTP グローバル設定)、PTP Port Settings (PTP ポート設定)、PTP Boundary Clock Settings (PTP 境界クロック設定)、PTP Boundary Port Settings (PTP 境界ポート設定)、PTP Peer to Peer Transparent Port Settings (PTP ピアツーピア透過ポート設定)、PTP Clock Information (PTP クロック情報の表示)、PTP Port Information (PTP ポート情報)、PTP Foreign Master Records Port Information (PTP 外部マスタレコードのポート情報) | 201 |

VLAN について

IEEE 802.1p プライオリティについて

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

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

プライオリティタグは、0 から 7 までの値で示され、0 が最も低い優先度、7 が最も高い優先度を表します。一般的に、7 番のプライオリティタグは、少しの遅延にも影響されやすい音声や映像に関わるデータに対して、またはデータ転送速度が保証されているような特別なユーザに対して使用されます。

本スイッチでは、プライオリティタグ付きのパケットをご使用のネットワークでどのように扱うかを細かく調整することができます。プライオリティタグ付きのデータをキューの使用によって管理することにより、ご使用のネットワークのニーズに合わせて優先度を設定できます。1 つのキューに複数の異なるタグを使用したパケットを関連付ける方が効果のある場合もありますが、一般的には最高の優先度のキュー（キュー 7）には、プライオリティレベル 7 のパケットに割り当てていただくことをお勧めします。プライオリティを与えられないパケットはキュー 0 に割り当てられ、最も低い送信優先度となります。

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

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

VLAN とは

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

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

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

本スイッチシリーズにおける VLAN について

どんな方法でエンドノードの識別を行い、エンドノードに VLAN メンバシップを割り当てたとしても、VLAN 間にルーティング機能を持つネットワークデバイスが存在しない限り、パケットは VLAN に所属しないポートに送信されることはありません。

本スイッチシリーズは IEEE 802.1Q 標準で規定する VLAN とポートベース VLAN をサポートします。ポートタグ取り機能は、パケットヘッダから 802.1Q タグを取り外すことにより、タグを理解しないデバイスとの互換性を保ちます。

スイッチの初期状態では、すべてのポートに「default」と名付けられた 802.1Q VLAN が割り当てられています。「default」VLAN の VID は 1 です。必要性があれば、ポートベース VLAN のメンバポートの重複は許されています。

IEEE 802.1Q VLAN

用語の説明

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

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

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

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

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

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

IEEE 802.1Q 標準規格の主な機能は以下の通りです。

- フィルタリングによりパケットを VLAN に割り当てます。
- 全体で 1 つのスパンニングツリーが構成されていると仮定します。
- 1 レベルのタグ付けによるタグ付けを行います。
- 802.1Q VLAN のパケット転送
- パケットの転送は以下の 3 つの種類のルールに基づいて決定されます。:
 - インGRESルール - 受け取ったパケットがどの VLAN に所属するかの分類に関するルール。
 - ポート間のフォワーディングルール - 転送するかしないかを決定します。
 - イーGRESルール - パケットが送信される時にタグ付きかタグなしかを決定します。

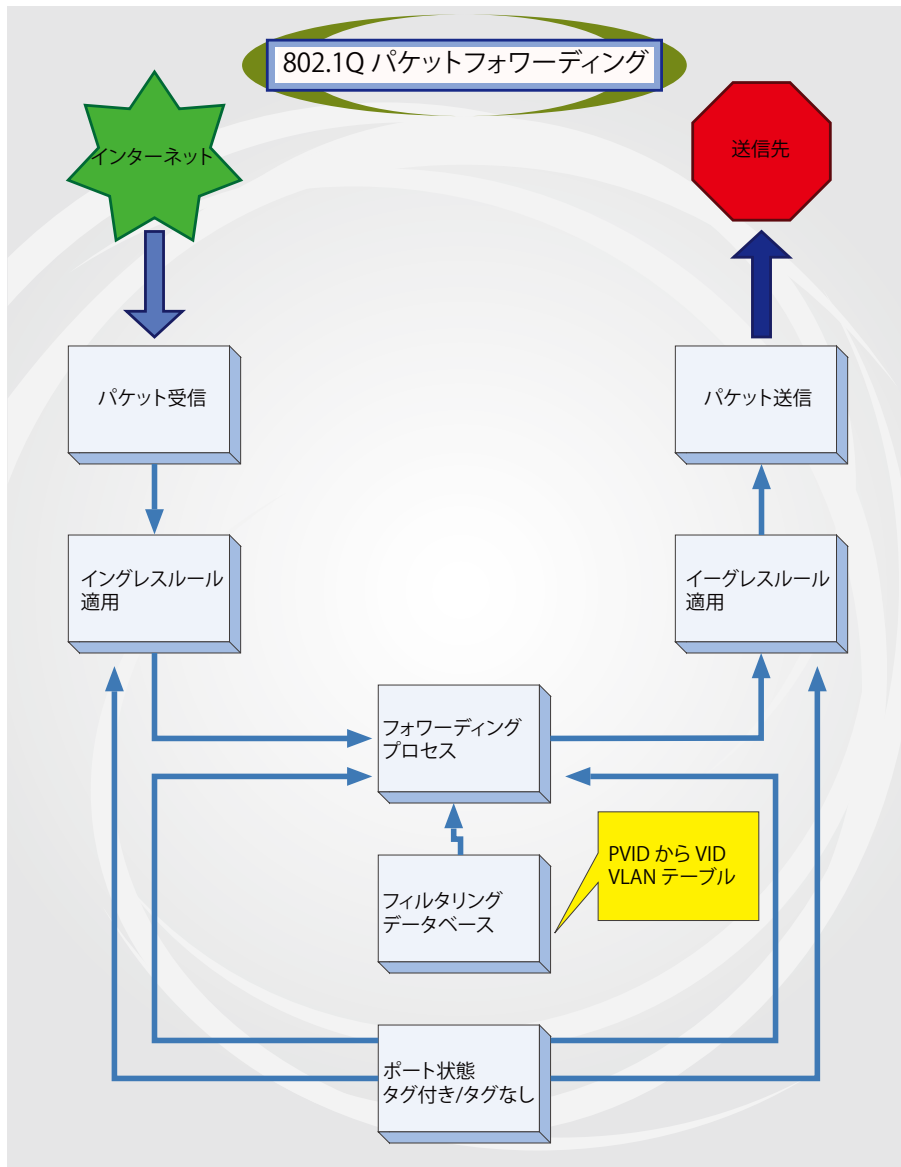


図 8-1 IEEE 802.1Q パケットフォワーディング

802.1Q VLAN タグ

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

IEEE 802.1Q タグ

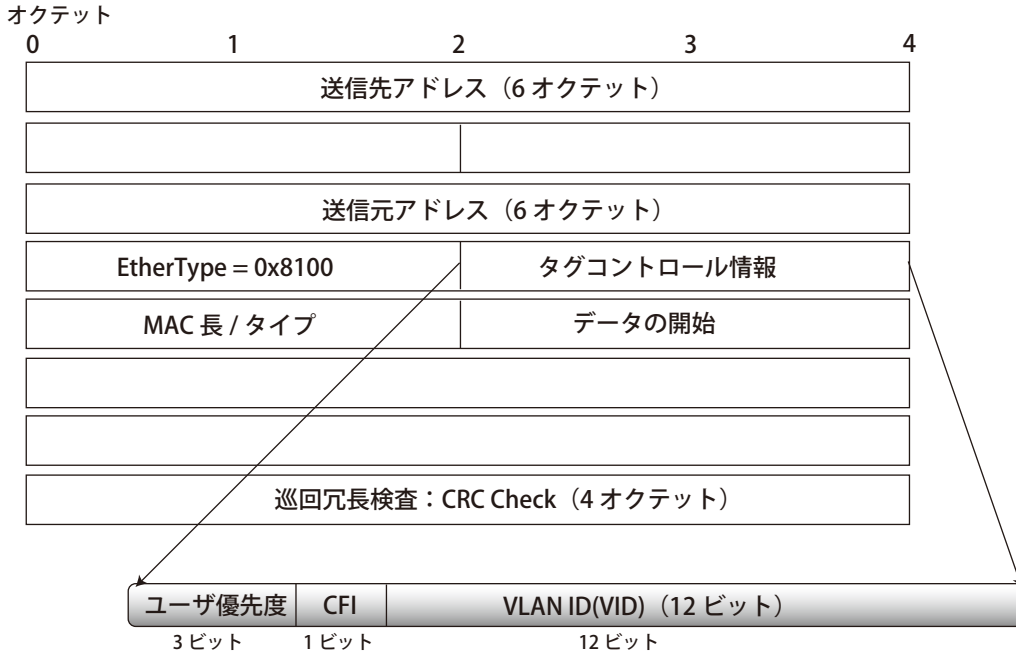


図 8-2 IEEE 802.1Q タグ

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

IEEE 802.1Q タグへの追加

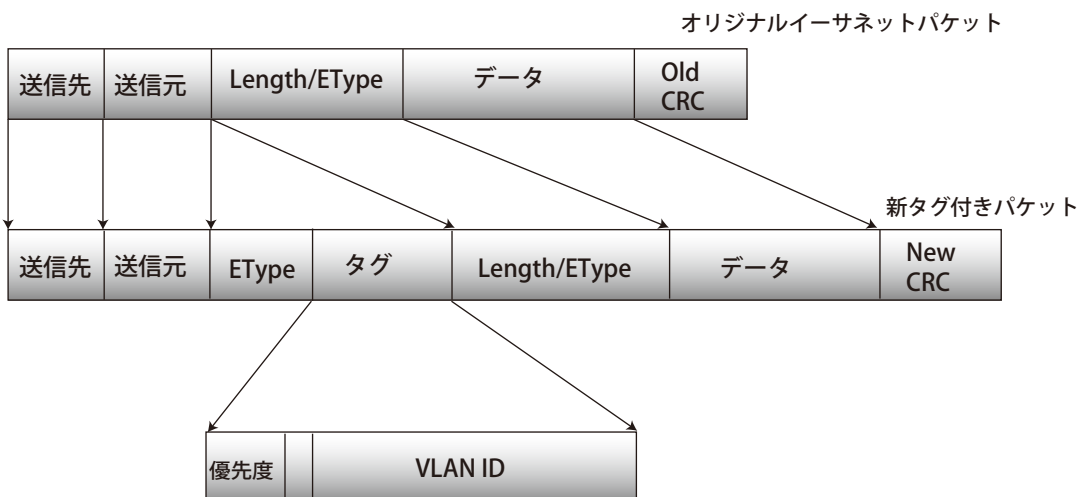


図 8-3 IEEE 802.1Q タグの挿入

ポート VLAN ID

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

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

802.1Q VLAN が採用される以前は、ポートベースや MAC ベースの VLAN が主流でした。これらの VLAN でのパケット送信はポート VLAN ID (PVID) を元に行われます。あるポートで受信したタグなしパケットには、そのポートの PVID を割り当てて、パケットの宛先アドレス (スイッチのフォーワーディングテーブルで参照) へと送信されます。

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

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

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

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

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

タグ付きとタグなし

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

タグ付きのポートは受信、送信するすべてのパケットのヘッダに、VID、プライオリティ、そしてそのほかの VLAN 情報を埋め込みます。パケットが既にタグ付けされていたなら、VLAN 情報を完全に保つためにポートはパケットを変更しません。ネットワーク上の他の 802.1Q 対応デバイスも、タグの VLAN 情報を使用してパケットの転送を決定します。

タグなしのポートは、受信、送信するすべてのパケットから 802.1Q タグを削除します。パケットに 802.1Q VLAN タグがなければ、ポートはパケットを変更しません。つまり、タグなしのポートが受信して、転送したすべてのパケットは 802.1Q VLAN 情報をまったく持ちません。PVID はスイッチの内部で使用されるだけです。タグなしはパケットを 802.1Q 対応のデバイスから、非対応のデバイスにパケットを送信するのに使用します。

イングレスフィルタリング

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

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

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

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

デフォルト VLAN

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

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

注意 スイッチ上に 1 つも VLAN が設定されていない場合、すべてのパケットがすべての送信先ポートへと転送されます。宛先アドレスが不明なパケットはすべてのポートに送信されます。ブロードキャストパケットやマルチキャストパケットも、すべてのポートに大量に送信されます。

VLAN の設定例を以下に示します。

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

ポートベース VLAN

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

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

VLAN セグメンテーション

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

VLAN (VLAN 設定)

802.1Q VLAN Settings (802.1Q VLAN 設定)

802.1Q VLAN を設定します。

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

VLAN リストの表示

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

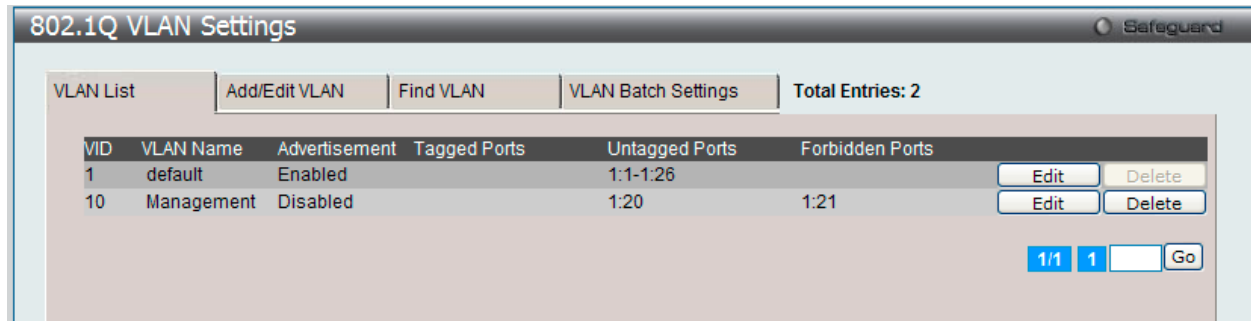


図 8-4 802.1Q VLAN Settings - VLAN List タブ画面

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

エントリの削除

対象のエントリの行の「Delete」ボタンをクリックします。

新規 / 既存の 802.1Q VLAN の登録

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

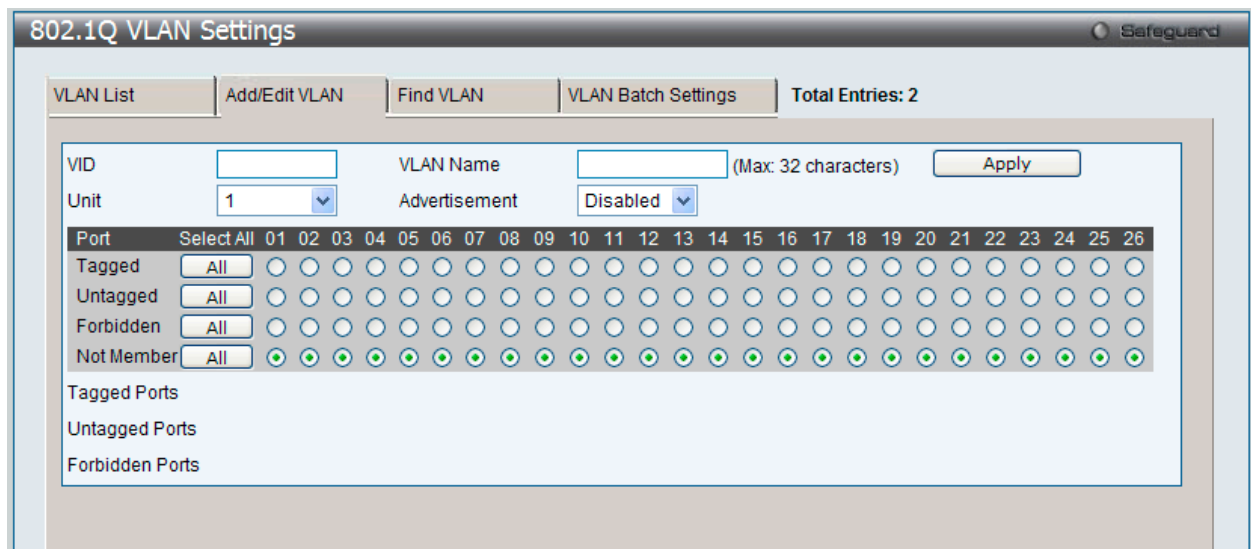


図 8-5 802.1Q VLAN Settings - Add/Edit VLAN タブ画面 (Add)

802.1Q VLAN の編集

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

図 8-6 802.1Q VLAN Settings - Add/Edit VLAN タブ画面 (Edit)

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

「Add/Edit VLAN」タブには以下の項目が含まれます。

| 項目 | 内容 |
|---------------|--|
| VID | VLAN ID の定義、または定義済みの VLAN の VLAN ID を表示します。VLAN は VID または VLAN 名で識別されます。 |
| VLAN Name | VLAN 名の定義、または VLAN 名の編集をします。ユーザ定義の VLAN 名を定義します。(半角英数字 32 文字以内) |
| Unit | 設定するユニットを選択します。 |
| Advertisement | 「Enabled」(有効) にすると、外部ソースに GVRP パケットを送信し、既存の VLAN に加わる可能性があることを通知します。 |
| Port | 各ポートを以下の通り VLAN のメンバとして定義します。 <ul style="list-style-type: none"> Tagged - ポートを 802.1Q タグ付きとして定義します。タグ付きとするポートのボックスをチェックします。 Untagged - ポートを 802.1Q タグなしとして定義します。タグなしとするポートのボックスをチェックします。 Forbidden - ポートを VLAN のメンバとならないことを定義し、ダイナミックにポートが VLAN のメンバになることを禁止します。 Not Member - 各ポートが VLAN メンバでないことを定義します。 Select All - 「All」ボタンをクリックし、すべてのポートを選択します。 |

「Apply」ボタンをクリックし、デバイスに VLAN 設定を適用します。

VLAN の検索

「Find VLAN」タブをクリックします。以下の画面が表示されます。

図 8-7 802.1Q VLAN Settings - Find VLAN タブ画面

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

802.1Q VLAN バッチの作成

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

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

以下の項目を使用して設定します。

| 項目 | 説明 |
|---------------------------|---|
| VID List (e.g.: 2-5) | VID の範囲 (1-4094) を指定します。続いて、「Add」、「Delete」または「Config」をボタンをクリックし、指定した VID List を追加、削除または編集します。 |
| Advertisement | 本機能を「Enabled」(有効) にすると、スイッチは GVRP パケットを送信し、VLAN に参加できることを通知します。 |
| Port List (e.g.: 1:1-1:5) | VLAN のメンバとして追加または削除するポートまたはポート範囲を指定します。 指定ポートに行う操作を指定します。 <ul style="list-style-type: none"> • Add - VLAN のメンバとして追加します。 • Delete - VLAN のメンバとして削除します。 • config - 指定ポートに以下の設定を行います。 <ul style="list-style-type: none"> - Tagged - ポートを 802.1Q タグ付きとして定義します。 - Untagged - ポートを 802.1Q タグなしとして定義します。 - Forbidden - ポートを VLAN のメンバではないポートとして定義します。動的に VLAN メンバになることが禁じられます。 |

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

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

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

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

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

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

注意 SNAP フレームの OUI が 0x080007 のフレームはサポートしていません。

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

図 8-9 802.1v Protocol Group Settings 画面

テーブルの下半分は定義済みのすべてのグループを表示します。

以下の項目を使用して、設定します。

| 項目 | 説明 |
|--------------------------------------|---|
| Add Protocol VLAN Group | |
| Group ID (1-16) | グループの ID 番号を 1-16 の範囲から指定します。 |
| Group Name | 新しいプロトコル VLAN グループの識別に使用します。32 文字までの半角英数字を入力します。 |
| Add Protocol for Protocol VLAN Group | |
| Group ID | チェックを入れグループの ID 番号を指定します。 |
| Group Name | 新しいプロトコル VLAN グループの識別に使用します。32 文字までの半角英数字を入力します。 |
| Protocol | 本機能は、関連するプロトコルのタイプを検出するためにパケットヘッダのタイプオクテットを検証することで、パケットをプロトコルで定義された VLAN にマップします。 プルダウンメニューを使用して、Ethernet II、IEEE802.3 LLC および IEEE802.3 SNAP から選択します。 |
| Protocol Value (0-FFFF) | グループに対してプロトコル値を入力します。プロトコル値は、指定されたフレームタイプのプロトコルを識別するために使用されます。入力形式は 0x0 から 0xffff です。オクテット文字列は、フレームタイプによって、以下に示す値の 1 つを持っています。 <ul style="list-style-type: none"> • ethernet II - 16 ビット (2 オクテット) の 16 進数です。例えば、IPv4 は 800、IPv6 は 86dd、ARP は 806 などです。 • IEEE802.3 SNAP - 16 ビット (2 オクテット) の 16 進数です。 • IEEE802.3 LLC - 2 オクテットの IEEE 802.2 Link Service Access Point(LSAP) ペアです。はじめのオクテットは、Destination Service Access Point (DSAP) のための値であり、2 番目のオクテットは送信元のための値です。 |

注意 SNAP フレームの OUI が 0x080007 のフレームはサポートしていません。

プロトコル VLAN グループの新規追加

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

プロトコル VLAN グループの編集

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

図 8-10 802.1v Protocol Group Settings 画面 - Edit

2. 項目を編集し、エントリの「Apply」ボタンをクリックします。

プロトコル VLAN グループの削除

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

プロトコル VLAN グループのプロトコル設定

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

プロトコル VLAN グループのプロトコルの削除

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

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

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

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

図 8-11 802.1v Protocol VLAN Settings 画面

以下の項目を使用して、設定します。

| 項目 | 説明 |
|-----------------------|---|
| Add New Protocol VLAN | |
| Group ID | 対応するボタンをチェックし、プルダウンメニューから定義済みの Group ID を選択します。 |
| Group Name | 対応するボタンをチェックし、プルダウンメニューから定義済みの Group Name を選択します。 |

L2 Features (L2機能の設定)

| 項目 | 説明 |
|-----------------------|---|
| VID (1-4094) | 対応するボタンをチェックし、VIDを入力します。これはVLAN名と共に、ユーザが作成するVLANを識別するために使用するIDです。 |
| VLAN Name | 対応するボタンをチェックし、VLAN Nameを入力します。これは、VLAN IDと共に、ユーザが作成するVLANを識別するために使用するVLAN名です。 |
| 802.1p Priority | <p>スイッチに設定済みの802.1pデフォルトプライオリティ（パケットが送られるCoSキューを決定するために使用）の設定を書き換える場合に使用します。本項目を選択すると、スイッチが受信したパケット内の本プライオリティに一致するパケットは、既に指定したCoSキューに送られます。</p> <p>本画面で設定した基準に一致するパケットが、指定されたCoSキューに送られる前に、パケットの802.1pデフォルトプライオリティを、「Priority (0-7)」に指定した値に書き換える場合に対応するボックスをクリックします。指定しない場合は、パケットは送出される前に、入力用の802.1pユーザプライオリティを元の値に書き換えられます。</p> <p>プライオリティキュー、CoSキューおよび802.1pマッピングについての詳細な情報については、本マニュアルの 221 ページの「第10章 QoS (QoS機能の設定)」 を参照してください。</p> |
| Port List (e.g.: 1-6) | 本項目にポート番号を入力することで特定のポートを選択するか、または「All Ports」をチェックします。 |
| Protocol VLAN Table | |
| Search Port List | 定義済みの全ポートリスト設定を検索し、テーブルの下半分の結果を表示します。 |

プロトコル VLAN ポートの新規設定

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

プロトコル VLAN ポートの設定編集

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

図 8-12 802.1v Protocol VLAN Settings 画面 - Edit

2. 項目を編集し、エントリの「Apply」ボタンをクリックします。

プロトコル VLAN ポートの削除

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

ポートリストの検索

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

定義済み全ポートリストの表示

「Show All」ボタンをクリックします。

すべての設定リストのクリア

「Delete All」ボタンをクリックします。

Asymmetric VLAN Settings (Asymmetric VLAN 設定)

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

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

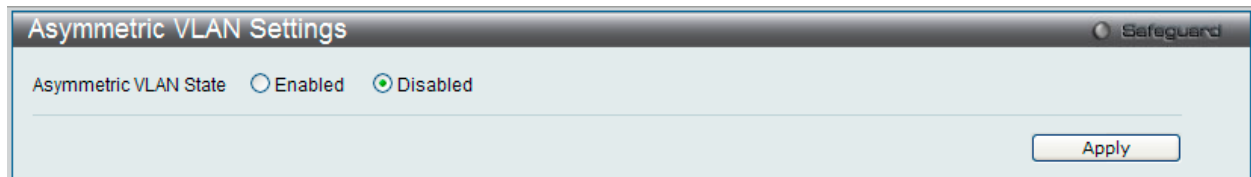


図 8-13 Asymmetric VLAN Settings 画面

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

GVRP (GVRP の設定)

GVRP Global Settings (GVRP グローバル設定)

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

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

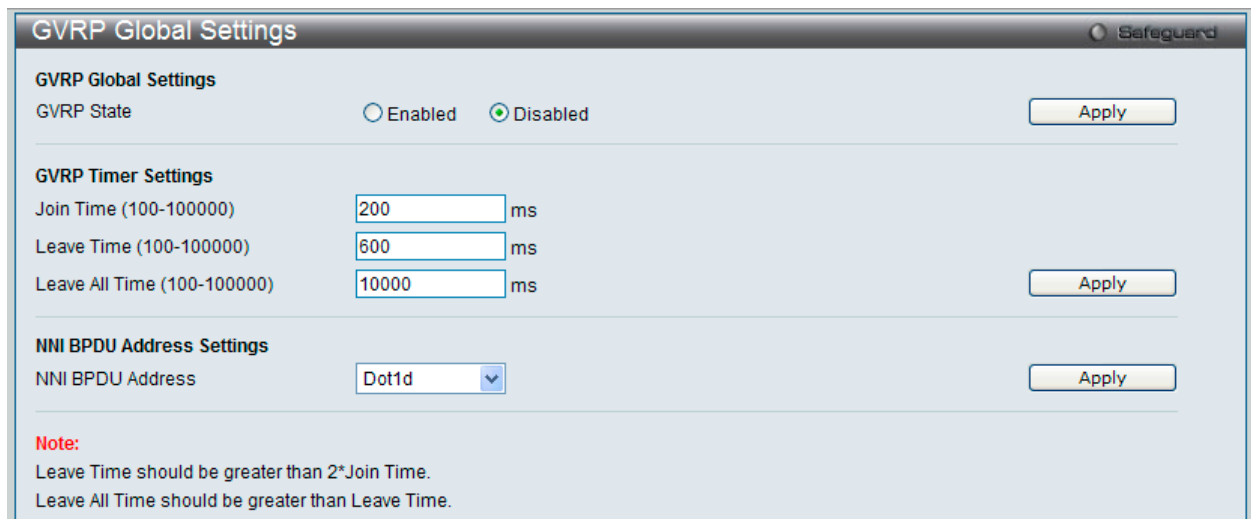


図 8-14 GVRP Global Settings 画面

本画面には次の項目があります。

| 項目 | 説明 |
|---------------------------|--|
| GVRP Global Settings | |
| GVRP State | GVRP 状態を有効または無効にして「Apply」ボタンをクリックします。 <ul style="list-style-type: none"> Enabled - デバイスで GVRP を有効に設定します。 Disabled - デバイスで GVRP を無効に設定します。(初期値) |
| GVRP Timer Settings | |
| Join Time | Join Time (ミリ秒) を入力します。 |
| Leave Time | Leave Time (ミリ秒) を入力します。 |
| Leave All Time | Leave All Time (ミリ秒) を入力します。 |
| NNI BPDU Address Settings | |
| NNI BPDU Address | サービス提供サイトにおける GVRP の BPDU プロトコルアドレスを決定します。802.1d GVRP アドレス、802.1ad サービスプロバイダの GVRP アドレスを使用します。 |

「Apply」ボタンをクリックし、デバイスに GVRP 設定を適用します。

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

GVRP Port Settings (GVRP ポート設定)

GVRP ポートパラメータを設定します。

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

| Unit | From Port | To Port | PVID (1-4094) | GVRP | Ingress Checking | Acceptable Frame Type |
|------|-----------|---------|---------------|----------|------------------|-----------------------|
| 1 | 01 | 01 | | Disabled | Enabled | All |

| Unit 1 Settings | | | | |
|-----------------|------|----------|------------------|-----------------------|
| Port | PVID | GVRP | Ingress Checking | Acceptable Frame Type |
| 1 | 1 | Disabled | Enabled | All |
| 2 | 1 | Disabled | Enabled | All |
| 3 | 1 | Disabled | Enabled | All |
| 4 | 1 | Disabled | Enabled | All |
| 5 | 1 | Disabled | Enabled | All |
| 6 | 1 | Disabled | Enabled | All |
| 7 | 1 | Disabled | Enabled | All |
| 8 | 1 | Disabled | Enabled | All |
| 9 | 1 | Disabled | Enabled | All |
| 10 | 1 | Disabled | Enabled | All |
| 11 | 1 | Disabled | Enabled | All |
| 12 | 1 | Disabled | Enabled | All |

図 8-15 GVRP Port Settings 画面

本画面には次の項目があります。

| 項目 | 説明 |
|----------------------|---|
| Unit | 設定するユニットを選択します。 |
| From Port / To Port | ポートベース VLAN に含まれるポートの範囲を指定します。 |
| PVID (1-4094) | PVID を VLAN に手動で割り当てます。スイッチには初期状態ですべてのポートが default VLAN (VID=1) に割り当てられています。PVID はポートが送信時にタグなしパケットにタグ付けをしたり、受信時にフィルタリングをするためのものです。 |
| GVRP | GVRP が各ポートを動的に VLAN メンバにするかどうかを設定します。 <ul style="list-style-type: none"> Enabled - 選択したポートで GVRP を有効に設定します。 Disabled - 選択したポートで GVRP を無効に設定します。(初期値) |
| Ingress Checking | Ingress フィルタリングの有効/無効を設定します。デバイスで Ingress チェックを有効にするかを設定します。 <ul style="list-style-type: none"> Enabled - デバイスで Ingress チェックを有効に設定します。Ingress チェックにより、受信したタグ付きパケットの VID とポートに割り当てられた PVID を比較します。PVID が異なっていれば、ポートはパケットを破棄します。(初期値) Disabled - Ingress チェックを無効に設定します。 |
| Acceptable FrameType | ポートが受け入れるフレームの種類を設定します。 <ul style="list-style-type: none"> Tagged Only - タグ付きフレームのみポートは受け入れます。 All - タグ付き、タグなし両方のフレームをポートは受け入れます。(初期値) |

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

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

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

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

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

図 8-16 MAC-based VLAN Settings 画面

以下の項目を使用して設定します。

| 項目 | 説明 |
|-------------|--|
| MAC Address | ユニキャスト MAC アドレスを入力します。 |
| VLAN ID | VLAN ID を入力します。 |
| VLAN Name | 作成済みの VLAN の VLAN 名を指定します。 |
| Priority | プルダウンメニューを使用してタグなしパケットに割り当てる優先度を選択します。 |

エントリの新規登録

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

エントリの検索

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

エントリの削除

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

エントリの参照

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

Private VLAN Settings (プライベート VLAN 設定)

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

Isolated VLAN

Isolated VLAN は、ポートに接続しているすべてのホストがレイヤ 2 で隔離されるという異なる特性を持つセカンダリ VLAN です。そのため、Isolated VLAN の第一の長所は、プライベート VLAN に基づいた設計は 2 つの VLAN 識別子を使用するだけでポートの分離を行い、多くのエンドユーザにサービスを提供することができるということです。プライベート VLAN は、1 つの Isolated VLAN のみをサポートしています。

Community VLAN

コミュニティ VLAN は、信頼関係を持つエンドデバイスの特定の「コミュニティ」に接続するポートグループに関連付けるセカンダリ VLAN です。プライベート VLAN ドメインには、複数の異なるコミュニティ VLAN が存在することができます。

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

プライベート VLAN のパラメータを設定します。

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

図 8-17 Private VLAN Settings 画面

以下の項目を使用して設定します。

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

エントリの新規登録

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

エントリの検索

「Find Private VLAN」セクションで「VLAN Name」または「VID」を入力し、「Find」ボタンをクリックします。結果は画面下のテーブルに表示されます。「View All」ボタンをクリックすると、すべての定義済みエントリを表示します。

エントリの削除

削除するエントリの「Delete」ボタンをクリックします。

エントリの編集

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

図 8-18 Private VLAN Settings 画面 - Edit

以下の項目を使用して設定します。

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

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

[View Private VLAN List](#) リンクをクリックすると前の画面に戻ります。

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

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

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

図 8-19 PVID Auto Assign Settings 画面

「Apply」ボタンをクリックし、デバイスに設定を適用します。

Subnet VLAN (サブネット VLAN)

Subnet VLAN Settings (サブネット VLAN 設定)

サブネット VLAN エントリは IP サブネットベースの VLAN クラシフィケーションルールです。ポートにタグなしまたはプライオリティタグを持つ IP パケットを受信すると、送信元 IP アドレスがサブネット VLAN エントリへの照合のために使用されます。エントリのサブネットに送信元 IP があると、パケットはこのサブネットのために定義された VLAN に分類されます。

サブネット VLAN のパラメータを設定します。

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

図 8-20 Subnet VLAN Settings 画面

以下の項目を使用して設定します。

| 項目 | 説明 |
|----------------------|--|
| VLAN Name | VLAN 名を入力します。 |
| VID | VID 値のリストを入力します。 |
| IPv4 Network Address | 使用する IPv4 アドレスを入力します。「/」表記を使用してサブネットマスクを含めることを忘れないでください。 |
| IPv6 Network Address | 使用する IPv6 アドレスを入力します。「/」表記を使用してサブネットマスクを含めることを忘れないでください。 |
| Priority | 使用するサブネット VLAN 優先度値を指定します。「None」、0-7 からオプションを選択します。 |
| VID List | VLAN ID のリストを入力します。 |

エントリの新規登録

「Add Subnet VLAN」セクションでサブネット VLAN に登録する「VLAN Name」/「VID」、「IPv4 Network Address」/「IPv6 Network Address」または「Priority」を指定後、「Add」ボタンをクリックします。

エントリの検索

「Find Subnet VLAN」セクションで「VLAN Name」/「VID」、「IPv4 Network Address」/「IPv6 Network Address」または「Priority」を指定後、「Find」ボタンをクリックします。結果は画面下のテーブルに表示されます。「View All」ボタンをクリックすると、すべての定義済みエントリを表示します。

エントリの削除

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

VLAN Precedence Settings (VLAN 優先度設定)

VLAN 優先度を設定します。

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

| Unit | From Port | To Port | VLAN Precedence |
|------|-----------|---------|-----------------|
| 1 | 01 | 01 | MAC-based VLAN |

| Unit 1 Settings | |
|-----------------|-----------------|
| Port | VLAN Precedence |
| 1 | MAC-based VLAN |
| 2 | MAC-based VLAN |
| 3 | MAC-based VLAN |
| 4 | MAC-based VLAN |
| 5 | MAC-based VLAN |
| 6 | MAC-based VLAN |

図 8-21 VLAN Precedence Settings 画面

以下の項目を使用して設定します。

| 項目 | 説明 |
|---------------------|--|
| Unit | 設定するユニットを選択します。 |
| From Port / To Port | 使用する開始 / 終了ポートを選択します。 |
| VLAN Precedence | プルダウンメニューを使用して優先する VLAN (「MAC-based VLAN」または「Subnet VLAN」) を選択します。 |

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

Voice VLAN (音声 VLAN)

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

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

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

音声 VLAN をグローバルに有効 / 無効にします。

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

図 8-22 Voice VLAN Global Settings 画面

以下の項目を使用して設定します。

| 項目 | 説明 |
|--------------------|--|
| Voice VLAN State | 音声 VLAN の状態を有効 / 無効にします。 |
| Voice VLAN Name | 音声 VLAN 名を指定します。 |
| Voice VID (1-4094) | 音声 VLAN の VLAN ID を指定します。 |
| Priority | 音声 VLAN の優先度 (0-7) を指定します。優先度の初期値は 5 です。 |

L2 Features (L2機能の設定)

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

音声 VLAN の有効化

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

音声 VLAN のパラメータ設定

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

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

ポートの音声 VLAN 情報を表示します。

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

| Unit | From Port | To Port | State | Mode |
|------|-----------|---------|----------|------|
| 1 | 01 | 01 | Disabled | Auto |

| Unit 1 Settings | | |
|-----------------|----------|------|
| Port | State | Mode |
| 1 | Disabled | Auto |
| 2 | Disabled | Auto |
| 3 | Disabled | Auto |
| 4 | Disabled | Auto |
| 5 | Disabled | Auto |

図 8-23 Voice VLAN Port Settings 画面

以下の項目を使用して設定します。

| 項目 | 説明 |
|---------------------|-----------------------------------|
| Unit | 設定するユニットを選択します。 |
| From Port / To Port | 表示するポート範囲を選択します。 |
| State | ポートの状態を設定します。 |
| Mode | ポートのモード (Auto または Manual) を設定します。 |

「Apply」ボタンをクリックして行った変更を適用します。

Voice VLAN OUI Settings (音声 VLAN OUI 設定)

ユーザ定義の音声トラフィックの OUI を設定します。

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

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

| OUI Address | Mask | Description | Edit | Delete |
|-------------------|-------------------|-------------|------|--------|
| 00-01-E3-00-00-00 | FF-FF-FF-00-00-00 | Siemens | Edit | Delete |
| 00-03-6B-00-00-00 | FF-FF-FF-00-00-00 | Cisco | Edit | Delete |
| 00-09-6E-00-00-00 | FF-FF-FF-00-00-00 | Avaya | Edit | Delete |
| 00-0F-E2-00-00-00 | FF-FF-FF-00-00-00 | Huawei&3COM | Edit | Delete |
| 00-60-B9-00-00-00 | FF-FF-FF-00-00-00 | NEC&Philips | Edit | Delete |
| 00-D0-1E-00-00-00 | FF-FF-FF-00-00-00 | Pingtel | Edit | Delete |
| 00-E0-75-00-00-00 | FF-FF-FF-00-00-00 | Veritel | Edit | Delete |

図 8-24 Voice VLAN OUI Settings 画面

以下の項目を使用して設定します。

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

「Apply」 ボタンをクリックして行った変更を適用します。

エントリの削除

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

エントリの編集

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

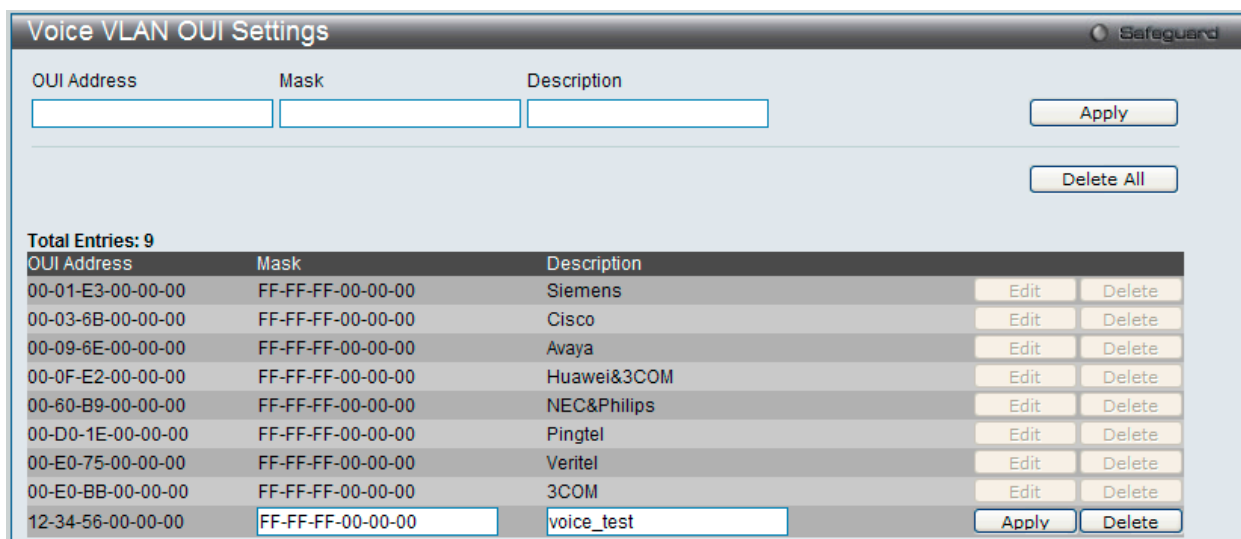


図 8-25 Voice VLAN OUI Settings 画面 - Edit

2. 項目を編集し、エントリの「Apply」ボタンをクリックします。

Voice VLAN Device (音声 VLAN デバイス)

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

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

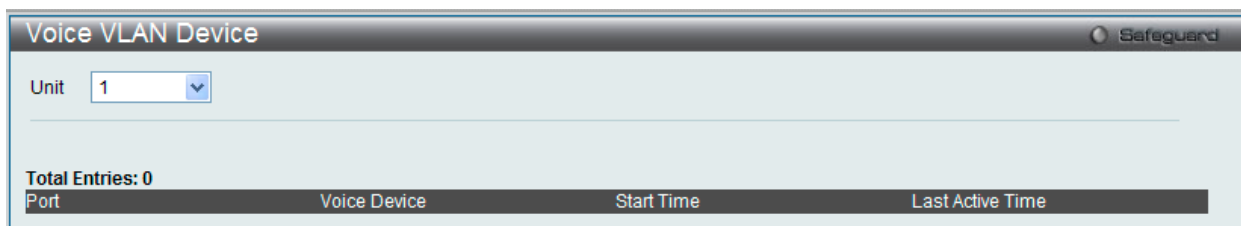


図 8-26 Voice VLAN Device 画面

以下の項目を使用して設定します。

| 項目 | 説明 |
|------|-----------------|
| Unit | 表示するユニットを選択します。 |

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

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

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

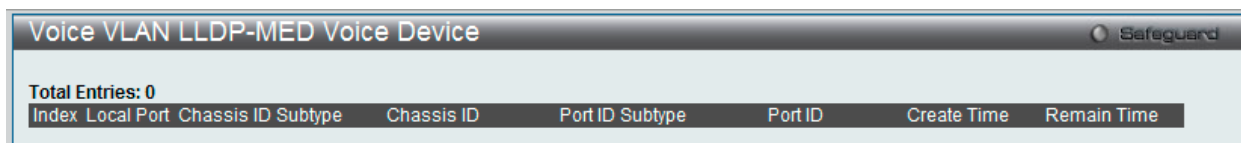


図 8-27 Voice VLAN LLDP-MED Voice Device 画面

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

VLAN Trunk Settings (VLAN トランク設定)

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

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

以下の図例を参照してください。

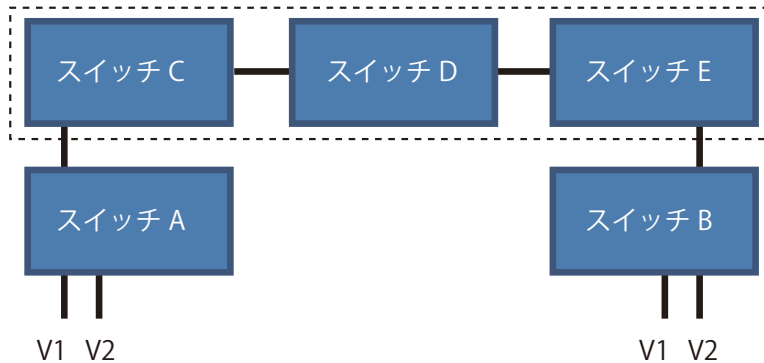


図 8-28 VLAN トランクの例題

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

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

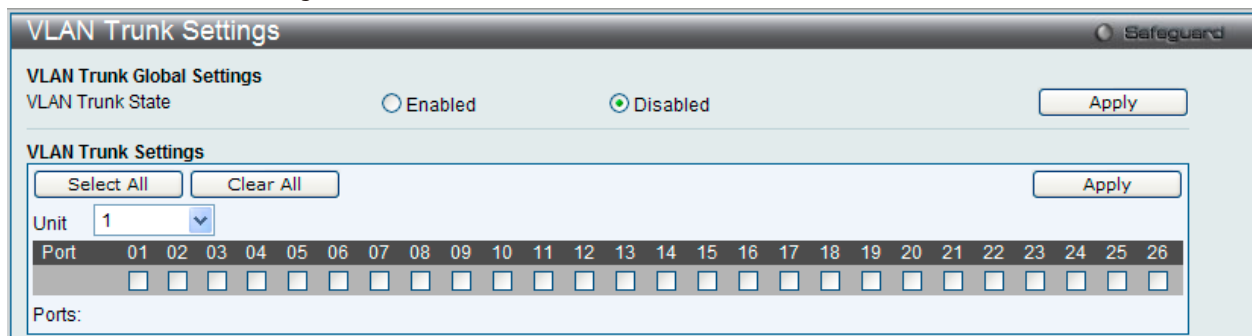


図 8-29 VLAN Trunk Settings 画面

本画面には次の項目があります。

| 項目 | 説明 |
|-------------------------|-----------------------------------|
| Unit | 設定するユニットを選択します。 |
| VLAN Trunk Global State | VLAN トランキングのグローバルな状態を有効または無効にします。 |
| Ports | 設定するポートを指定します。 |

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

「Select All」ボタンをクリックすると、全ポートが設定に使用されます。
「Clear All」ボタンをクリックすると、全ポートの設定がクリアされます。

Browse VLAN (VLAN の参照)

本画面では、スイッチの各ポートの VLAN ステータスを VLAN ごとに表示します。

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

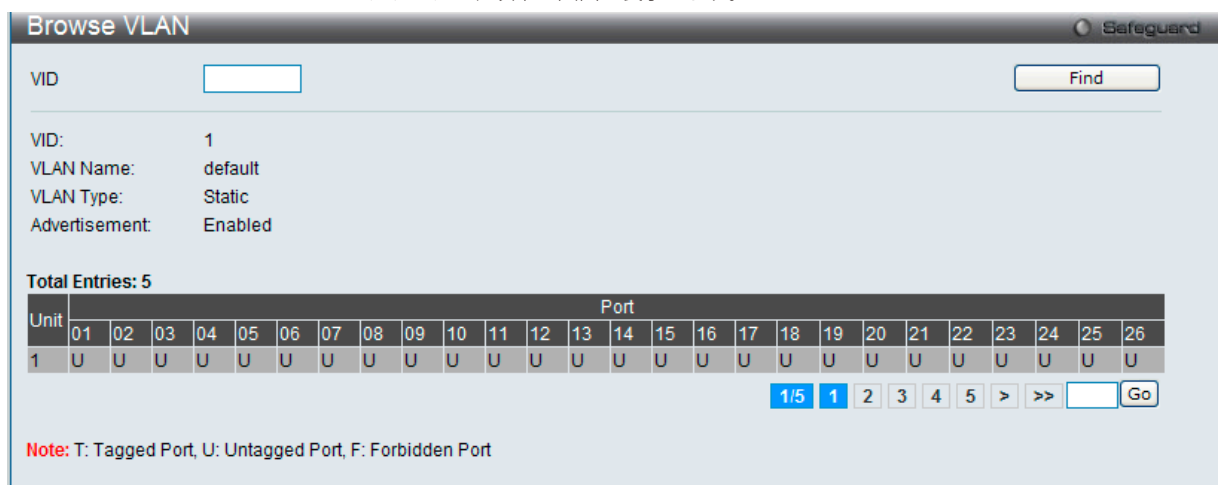


図 8-30 Browse VLAN 画面

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

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

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

Show VLAN Ports (VLAN ポートの参照)

スイッチの VLAN ポートを VID ごとに表示します。

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

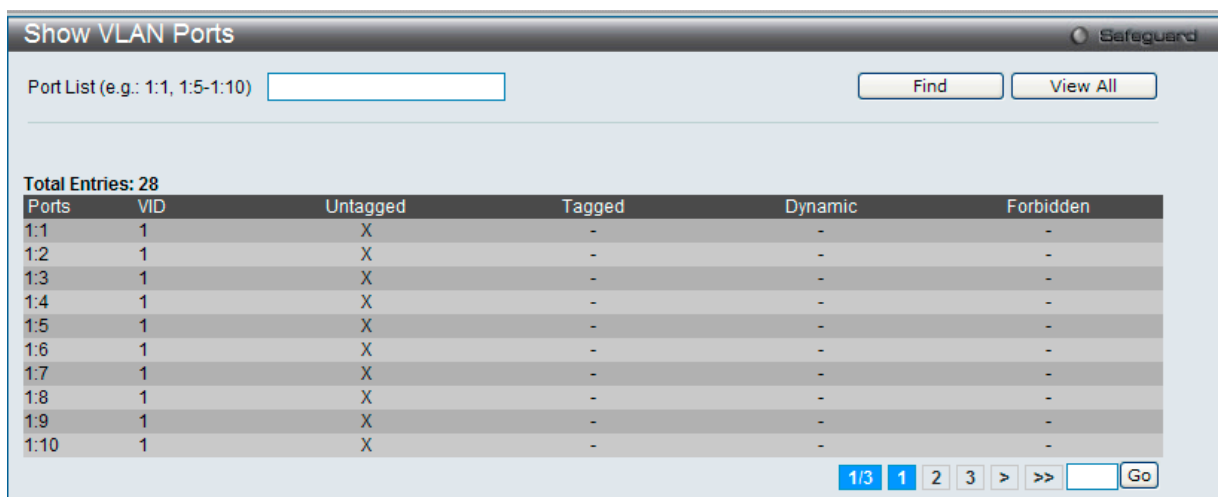


図 8-31 Show VLAN Ports 画面

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

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

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

QinQ (QinQ 設定)

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

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

以下に QinQ VLAN タグ付きパケットの例を示します。

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

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

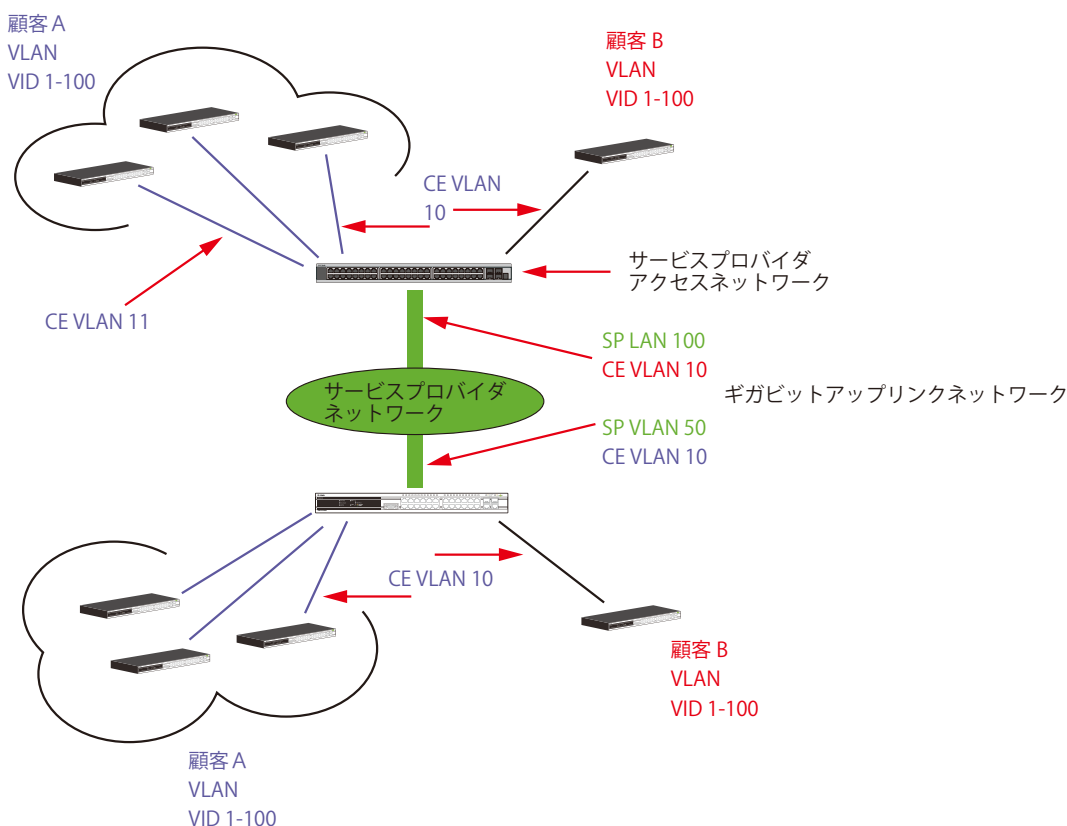


図 8-32 QinQ VLAN を使用したネットワーク例

上の図例では、サービスプロバイダ・アクセスネットワーク・スイッチ (プロバイダのエッジスイッチ) は顧客 A と顧客 B という特定の顧客に対して異なる SPVID を持つ QinQ VLAN を設定しているデバイスです。CEVLAN (Customer VLAN) 10 は、サービスプロバイダ・アクセスネットワーク上で顧客 A には SPVID 100 を、顧客 B には SPVID 200 をタグ付けされるので、サービスプロバイダのネットワーク上では 2 つの VLAN に属していることになります。

このように、顧客は通常の VLAN を保持しながら、サービスプロバイダは、複数の顧客の VLAN を 1 つの SP VLAN によって分割することができ、サービスプロバイダのスイッチ上でのトラフィックとルーティングのプロセスを調整します。これらの情報はサービスプロバイダのメインのネットワークに送られ、1 セットのプロトコルと 1 つのルーティング動作を持つ 1 つの VLAN として認識されます。

QinQ VLAN 使用時のルール

QinQ VLAN を使用するために、以下のルールがあります。

1. いくつかのルールを QinQ VLAN の処理の実行に適用します。
2. ポートは UNI ポートまたは NNI ポートとして設定されます。ギガビットポートとして UNI および NNI の両方を設定することができます。
3. プロバイダのエッジスイッチには SPVID タグが追加されるため、1522 バイト以上のフレームに対応する必要があります。
4. UNI ポートをサービスプロバイダ VLAN のタグなし、またはタグ付きポートとすることができます。NNI ポートをサービスプロバイダ VLAN のタグ付きポートとすることができます。
5. スイッチには QinQ VLAN と通常の VLAN は混在できません。一度 VLAN を変更すると、すべてのアクセスコントロールリストがクリアになり、再設定が必要となります。
6. QinQ VLAN が有効とされると、GVRP は QinQ VLAN で動作できます。
7. CPU から UNI ポートに送信されたすべてのパケットはタグ取りされるか、交換されます。
8. スイッチが QinQ VLAN モードにある場合、以下の機能は使用できなくなります。:
 - ゲスト VLAN
 - Web ベースのアクセス制御
 - IP マルチキャストルーティング
 - 通常の 802.1Q VLAN 機能

QinQ Settings (QinQ 設定)

QinQ のパラメータを設定します。

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

図 8-33 QinQ Settings 画面

以下の項目を使用して設定します。

| 項目 | 説明 |
|--------------------|---|
| QinQ State | QinQ 機能をグローバルに「Enabled」(有効)または「Disabled」(無効)にします。 |
| Inner TPID | SP-VLAN タグに Inner TPID を入力します。 |
| Unit | 設定するユニットを選択します。 |
| From Port/To Port | 設定に使用するポート範囲を選択します。 |
| Role | 役割 (UNI または NNI) を選択します。 <ul style="list-style-type: none"> • UNI - UNI (user-network interface) を選択すると、指定ユーザと指定ネットワーク間の通信が行われることを示します。 • NNI - NNI (network-to-network interface) を選択すると、指定した 2 つのネットワーク間で通信が行われることを示します。 |
| Missdrop | このオプションは、C-VLAN ベースの SP-VLAN 割り当ての Missdrop を有効または無効にします。 <ul style="list-style-type: none"> • Enabled - QinQ プロファイルにおけるどんな指定ルールにも一致しないパケットは廃棄されます。 • Disabled - パケットは転送され、受信ポートの PVID に割り当てられます。 |
| Outer TPID | SP-VLAN タグに Outer TPID を入力します。 |
| Use Inner Priority | S-VLAN タグの優先度として C-VLAN タグの優先度を使用するかどうかを指定します。初期値では設定は無効です。 |
| Add Inner Tag | 「Disabled」のチェックを外して、「Inner Tag」が追加されるエントリを入力します。初期値では無効です。 |

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

VLAN Translation Settings (VLAN 変換機能の設定)

C-VLAN と SP-VLAN 間の変換関係を追加します。

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

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

| Unit | From Port | To Port | CVID (1, 5-7) | Action | SVID (1-4094) | Priority |
|------|-----------|---------|---------------|--------|---------------|----------|
| 1 | 01 | 01 | | Add | | None |

Total Entries: 2

| Port | CVID | SVID | Action | Priority |
|------|------|------|--------|----------|
| 1:3 | 5 | 10 | Add | - |
| 1:4 | 5 | 10 | Add | - |

図 8-34 VLAN Translation Settings 画面

以下の項目を使用して、設定および表示を行います。

| 項目 | 説明 |
|---------------------|--|
| Unit | 設定するユニットを選択します。 |
| From Port / To Port | 設定に使用するポート範囲を選択します。 |
| CVID (1, 5-7) | 照合する C-VLAN ID を指定します。 |
| Action | <ul style="list-style-type: none"> Add - C- タグの前に S- タグを追加します。 Replace - オリジナルの C- タグを S- タグに置き換えます。 |
| SVID (1-4094) | SP-VLAN ID を入力します。 |
| Priority | S- タグの優先度を選択します。 |

「Apply」 ボタンをクリックし、新しいエントリを追加します。

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

エントリの編集

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

| Unit | From Port | To Port | CVID (1, 5-7) | Action | SVID (1-4094) | Priority |
|------|-----------|---------|---------------|--------|---------------|----------|
| 1 | 01 | 01 | | Add | | None |

Total Entries: 2

| Port | CVID | SVID | Action | Priority |
|------|------|------|--------|----------|
| 1:3 | 5 | 10 | Add | None |
| 1:4 | 5 | 10 | Add | - |

図 8-35 VLAN Translation Settings 画面 - Edit

エントリの削除

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

VLAN Translation Port Mapping Settings (VLAN 変換ポートのマッピング設定)

ポートの QinQ S-VLAN 割り当てのルールを設定します。これらのルールは QinQ プロファイルに含まれます。1 つの QinQ プロファイルをポートに追加できます。この設定は QinQ モードが無効の場合には有効になりません。

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

図 8-36 VLAN Translation Port Mapping Settings 画面

以下の項目を使用して、設定および表示を行います。

| 項目 | 説明 |
|--------------------------------|---------------------------------------|
| Unit | 設定するユニットを選択します。 |
| From Port / To Port | 設定に使用するポート範囲を選択します。 |
| VLAN Translation Profile (1-4) | VLAN 変換プロファイル番号を入力します。 |
| Action | 適用する操作を選択します。「Add」または「Delete」を選択できます。 |

「Apply」ボタンをクリックして行った変更を適用します。

VLAN Translation Profile List (VLAN 変換プロファイルリスト)

VLAN 変換プロファイルリストを設定します。

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

図 8-37 VLAN Translation Profile List 画面

以下の項目を使用して、設定および表示を行います。

| 項目 | 説明 |
|------------------|-----------------|
| Profile ID (1-4) | プロファイル番号を入力します。 |

「Apply」ボタンをクリックして行った変更を適用します。

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

「Add QinQ Profile」ボタンをクリックして、新しいエンTRIES QinQ プロファイルを追加します。

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

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

QinQ プロファイルの登録

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

図 8-38 VLAN Translation Profile List 画面 - Add

以下の項目を使用して、設定および表示を行います。

| 項目 | 説明 |
|---------------------|--|
| Profile ID (1-4) | 設定するプロファイル ID 番号を指定します。 |
| Rule ID (1-128) | プロファイルに追加するルール ID を指定します。 |
| Action | <ul style="list-style-type: none"> • Add - C-VLAN タグの前に割り当てられた SP-VLAN にタグを追加するします。S-TAG がパケットにないとこのルールは実施されません。 • Replace - タグ内の C-VLAN を SP VLAN と交換することを示すアクションを選択します。パケットに C-TAG がパケットにないとこのルールは実施されません。 |
| SVID (1-4094) | 一致するパケットに割り当てられるように SP-VLAN ID を指定します。 |
| Priority | SP-VLAN の優先度を指定します。優先度を指定しない場合はポート優先度の初期値を使用します。 |
| Source MAC | 送信元 MAC アドレスを指定します。 |
| Source Mask | 送信元 MAC アドレスマスクを指定します。 |
| Destination MAC | 送信先 MAC アドレスを指定します。 |
| Destination Mask | 送信先 MAC アドレスマスクを指定します。 |
| Source IP | 送信元 IPv4 アドレスまたは IPv4 サブネットを指定します。 |
| Source IP Mask | 送信元 IPv4 アドレスマスクを指定します。 |
| Destination IP | 送信先 IPv4 アドレスまたは IPv4 サブネットを指定します。 |
| Destination IP Mask | 送信先 IPv4 アドレスマスクを指定します。 |
| L4 Source Port | L4 送信元ポート ID を指定します。 |
| L4 Destination Port | L4 送信先ポート ID を指定します。 |
| Outer VID List | パケットの Outer VID 範囲を指定します。 |
| 802.1p | パケットの 802.1p 優先度を指定します。 |
| IP Protocol | 使用する IP プロトコルを指定します。 |

「Apply」 ボタンをクリックして行った変更を適用します。

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

QinQ VLAN 変換ルール情報の参照

「Show Match」 ボタンをクリックして以下の画面を表示します。

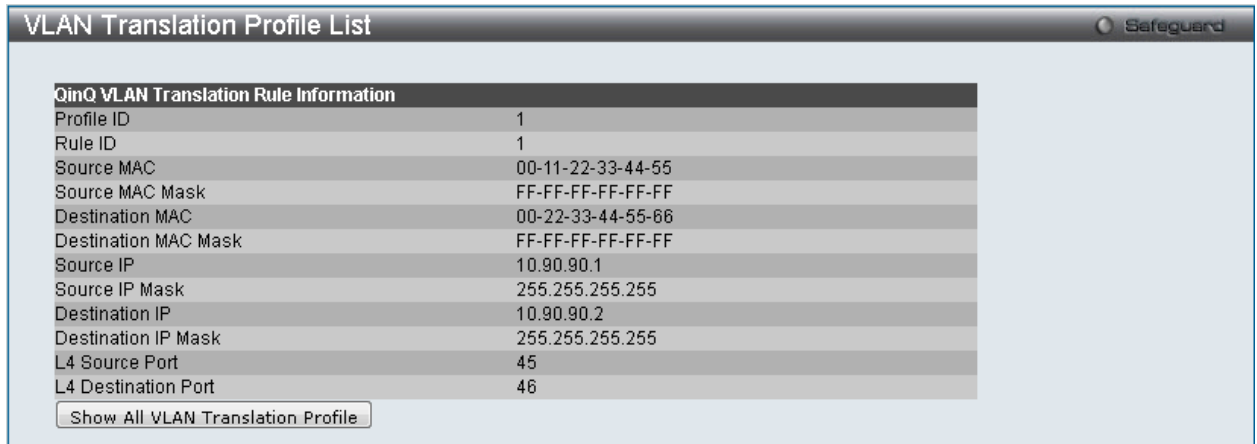


図 8-39 VLAN Translation Profile List 画面 - Show Match

「Show All VLAN Translation Profile」 ボタンをクリックして前の画面に戻ります。

Layer 2 Protocol Tunneling Settings (レイヤ 2 プロトコルトンネリング設定)

レイヤ 2 プロトコルトンネリングポートを設定します。

L2 Features > Layer 2 Protocol Tunneling Settings の順にメニューをクリックし、以下の画面を表示します。

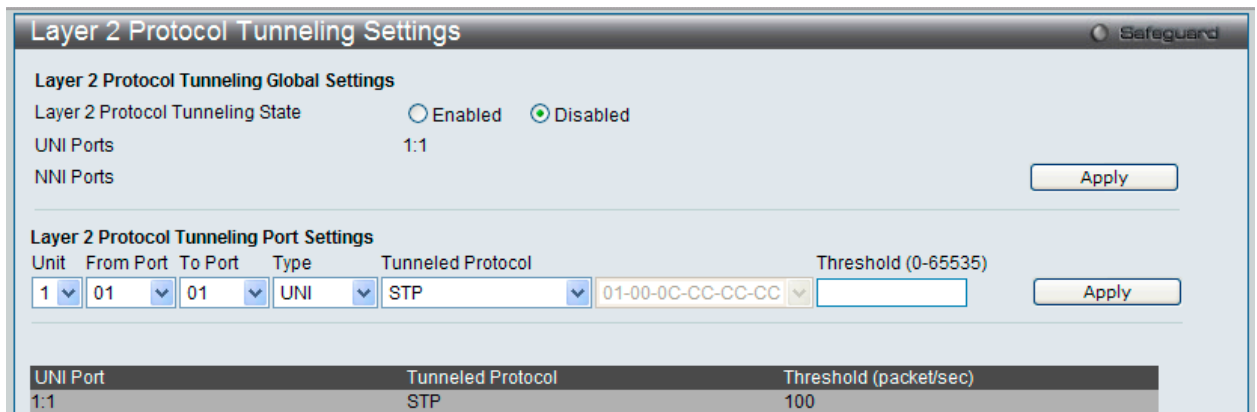


図 8-40 Layer 2 Protocol Tunneling Settings 画面

以下の項目を使用して、設定および表示を行います。

| 項目 | 説明 |
|----------------------------------|--|
| Layer 2 Protocol Tunneling State | レイヤ 2 プロトコルトンネリング状態を有効または無効にします。 |
| Unit | 設定するユニットを選択します。 |
| From Port / To Port | 設定に使用するポート範囲を選択します。 |
| Type | ポートタイプを指定します。UNI、NNI、および None (なし) が選択可能です。初期値は「None」です。 |
| Tunneled Protocol | 「Type」で「UNI」を選択した場合、このプルダウンメニューでは以下のオプションを表示します。 <ul style="list-style-type: none"> STP - これらの UNI で受信した BPDU をトンネルします。 GVRP - これらの UNI で受信した GVRP PDU をトンネルします。 Protocol MAC - これらの UNI ポートでトンネルする L2 プロトコルパケットの送信先 MAC アドレスを指定します。現時点では、MAC アドレスは、01-00-0C-CC-CC-CC または 01-00-0C-CC-CC-CD です。 All - すべてをサポートします。 |
| Threshold (0-65535) | この UNI ポートで受け入れるパケット / 秒の破棄しきい値を入力します。プロトコルのしきい値を超過すると、ポートは PDU を破棄します。値の範囲は 0-65535 (パケット / 秒) です。値 0 は無制限であることを意味します。初期値は 0 です。 |

「Apply」 ボタンをクリックして各セクションで行った変更を適用します。

Spanning Tree (スパンニングツリーの設定)

本スイッチは3つのバージョンのスパンニングツリープロトコル (802.1D-1998 STP、802.1D-2004 Rapid STP、および 802.1Q-2005 MSTP) をサポートしています。ネットワーク管理管理者間では 802.1D-1998 STP が最も一般的なプロトコルとして認識されていると思います。しかし、D-Link のマネジメントスイッチにも 802.1D-2004 RSTP と 802.1Q-2005 MSTP は導入されており、それらの技術について、以下に簡単に紹介します。また、802.1D-1998 STP、802.1D-2004 RSTP および 802.1Q-2005 MSTP の設定方法についても記述します。

802.1Q-2005 MSTP

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

MSTI ID (MST インスタンス ID) はこれらのインスタンスをクラス分けします。MSTP では、複数のスパンニングツリーを CIST (Common and Internal Spanning Tree) で接続します。CIST は自動的に各 MSTP リージョンとその最大範囲を決定し、1つのスパンニングツリーを構成する1つの仮想ブリッジのように見せかけます。そのため、異なる VLAN を割り当てられたフレームは、定義した VLAN や各スパンニングツリー内の管理エラーに関係なく、フレームの単純で完全な処理を続けながら、ネットワーク上の管理用に設定されたリージョン中の異なるデータ経路を通ります。

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

1. 32文字までの半角英数字で定義された「Configuration 名」。「MST Configuration Identification」画面中の「Configuration Name」で設定します。
2. 「Configuration Revision 番号」(「MST Configuration Identification」画面内の「Revision Level」)。
3. 4094 エレメントテーブル (「MST Configuration Identification」画面内の「VID List」)。

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

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

802.1D-2004 Rapid Spanning Tree

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

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

ポートの状態遷移

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

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

ポート状態の比較

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

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

Edge Port

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

P2P Port

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

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

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

2 つのレベルで動作するスパンニングツリープロトコル

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

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

STP ブリッジグローバルパラメータを設定します。

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

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

図 8-41 STP Bridge Global Settings 画面 : RSTP (初期値)

図 8-42

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



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

Bridge Max Age $\leq 2 \times$ (Bridge Forward Delay - 1 秒)

Bridge Max Age $\leq 2 \times$ (Bridge Hello Time + 1 秒)

設定には以下の項目が使用されます。

| 項目 | 説明 |
|-----------------------------|--|
| STP Global Settings | |
| STP State | STP をグローバルに「Enabled」(有効) / 「Disabled」(無効) にします。 |
| STP New Root Trap | 新しいルートトラップの送信を「Enabled」(有効) / 「Disabled」(無効) にします。 |
| STP Topology Change Trap | トポロジ変更トラップの送信を「Enabled」(有効) / 「Disabled」(無効) にします。 |
| STP Version | スイッチで使用する STP のバージョンをプルダウンメニューから選択します。 <ul style="list-style-type: none"> • STP - スイッチ上で STP がグローバルに使用されます。 • RSTP - スイッチ上で RSTP がグローバルに使用されます。 • MSTP - スイッチ上で MSTP がグローバルに使用されます。 |
| Forwarding BPDU | 「Enabled」(有効) または「Disabled」(無効) にします。「Enabled」にすると、STP BPDU パケットが他のネットワークデバイスから送信されます。初期値は「Enabled」です。 |
| Bridge Max Age (6-40) | 本項目は、古い情報がネットワーク内の冗長パスを永遠に循環し、新しい有効な情報の伝播を妨げるのを防ぐために設定します。ルートブリッジによりセットされるこの値は、スイッチと他の Bridged LAN (ブリッジで相互接続された LAN) 内のデバイスが持っているスパニングツリー設定値が矛盾していないかを確認するための値です。本値が経過した時にルートブリッジからの BPDU パケットが受信されていないければ、スイッチは自分で BPDU パケットを送信し、ルートブリッジになる許可を得ようとします。この時点でスイッチのブリッジ識別番号が一番小さければ、スイッチはルートブリッジになります。6-40 (秒) の範囲から値を指定します。初期値は 20 (秒) です。 |
| Bridge Hello Time (1-2) | ルートブリッジは、他のスイッチに自分がルートブリッジであることを示すために BPDU パケットを 2 回送信します。本値は、1 回目の送信と 2 回目の送信の間隔です。STP または RSTP が「STP Version」で選択された場合にだけ本項目は表示されます。MSTP に対して、Hello Time はポートごとに設定される必要があります。詳しくは「STP ポート設定」セクションを参照してください。1-2 秒で指定します。初期値は 2 (秒) です。 |
| Bridge Forward Delay (4-30) | スイッチ上のすべてのポートは、Blocking 状態から Forwarding 状態に移行する間に本値で指定した時間 Listening 状態を保ちます。4-30 (秒) の範囲から指定します。初期値は 15 (秒) です。 |
| Tx Hold Count (1-10) | Hello パケットの最大送信回数を指定します。1-10 の範囲から指定します。初期値は 6 です。 |
| Max Hops (6-40) | スイッチが送信した BPDU パケットが破棄される前のスパニングツリー範囲内のデバイス間のホップ数を設定します。値が 0 に到達するまで、各スイッチは 1 つずつホップカウントを減らしていきます。スイッチは、その後 BPDU パケットを破棄し、ポートに保持していた情報を解放します。ホップカウントは 6-40 で指定します。初期値は 20 です。 |
| NNI BPDU Address | サービス提供サイトにおける GVRP の BPDU プロトコルアドレスを決定します。「Dot1d」(802.1d GVRP アドレス)、「Dot1ad」(802.1ad サービスプロバイダの GVRP アドレス)、またはユーザ定義のマルチキャストアドレスを使用します。ユーザ定義アドレスの範囲は 0180C2000000-0180C2FFFFFF です。 |

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

STP Port Settings (STP ポートの設定)

STP をポートごとに設定します。

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

| Port | External Cost | Edge | P2P | Port STP | Restricted Role | Restricted TCN | Forward BPDU | Hello Time |
|------|---------------|----------|----------|----------|-----------------|----------------|--------------|------------|
| 1 | Auto/200000 | False/No | Auto/Yes | Enabled | False | False | Disabled | 2/2 |
| 2 | Auto/200000 | False/No | Auto/Yes | Enabled | False | False | Disabled | 2/2 |
| 3 | Auto/200000 | False/No | Auto/Yes | Enabled | False | False | Disabled | 2/2 |
| 4 | Auto/200000 | False/No | Auto/Yes | Enabled | False | False | Disabled | 2/2 |
| 5 | Auto/200000 | False/No | Auto/Yes | Enabled | False | False | Disabled | 2/2 |
| 6 | Auto/200000 | False/No | Auto/Yes | Enabled | False | False | Disabled | 2/2 |
| 7 | Auto/200000 | False/No | Auto/Yes | Enabled | False | False | Disabled | 2/2 |
| 8 | Auto/200000 | False/No | Auto/Yes | Enabled | False | False | Disabled | 2/2 |
| 9 | Auto/200000 | False/No | Auto/Yes | Enabled | False | False | Disabled | 2/2 |

図 8-43 STP Port Settings 画面



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

設定には以下の項目が使用されます。

| 項目 | 説明 |
|------------------------|---|
| Unit | 設定するユニットを選択します。 |
| From/ To Port | 設定対象のポート範囲を指定します。 |
| External Cost (0=Auto) | 設定対象のポートに対し、パケット送信のためのコストを表すメトリックを定義します。ポートコストは、自動設定、あるいは手動でメトリック値を指定できます。初期値は 0 (自動) です。 <ul style="list-style-type: none"> 0 - 0 を指定すると、指定したポートに対して、最適なパケット送信速度を自動的に設定します。デフォルトポートコスト：100Mbps ポートの場合は 200000、ギガビットポートの場合は 20000。 1-200000000 の範囲から指定 - 小さい数字を指定すると、パケット送出ポートとして選出される確率が上がります。 |
| Migrate | RSTP モードで動作中に、「Yes」を選択すると、選択されたポートは RSTP BPDU を送信します。 |
| Edge | <ul style="list-style-type: none"> True - 選択されたポートはエッジポートとして指定されます。エッジポートはループを発生しません。しかし、トポロジの変更によってループ発生の可能性が生じると、エッジポートはエッジポートとしての資格を失います。エッジポートは通常 BPDU パケットを受け取りません。しかし、BPDU パケットが受信されると、そのポートはエッジポートの資格を失います。 False - そのポートにエッジポートの資格がないことを示しています。 「Auto」オプションが利用可能です。 |
| P2P | <ul style="list-style-type: none"> True - 選択されたポートは P2P ポートとして指定されます。P2P ポートはエッジポートと似ていますが、全二重モードでのみ稼動する点で異なります。RSTP の特長として、エッジポート同様、P2P ポートは迅速に Forwarding 状態に遷移します。 False - そのポートに P2P ポートの資格がないことを示しています。 Auto - ポートはいつでも可能な時に (True を指定した時と同様に) P2P ポートとして稼動します。ポートの資格を失う時 (例えば、半二重モードを指定された時など)、自動的に False を指定した時と同様になります。(初期値) |
| Port STP | ポートの STP を「Enabled」(有効) / 「Disabled」(無効) にします。初期値は「Enabled」です。 |
| Restricted Role | 「True」と「False」を切り替えます。True に設定すると、ポートはルートポートになるように選択されることはありません。初期値は「False」です。 |
| Restricted TCN | TCN (Topology Change Notification) は、ブリッジがトポロジ変更を合図するためにルートポートに送出する簡単な BPDU です。Restricted TCN は「True」と「False」間で切り変わります。「True」に設定すると、受信した TCN とトポロジ変更を他のポートへ伝搬することを停止します。初期値は「False」です。 |
| Forward BPDU | プルダウンメニューから STP が無効の場合の BPDU パケットのフラッドを「Enabled」(有効)、「Disabled」(無効) にします。「Enabled」を選択すると、選択されたポートは他のネットワークデバイスから来る BPDU パケットの転送を行うようになります。 |

「Apply」ボタンをクリックし、設定を有効にします。



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

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

これらの設定は、前述の「STP Bridge Global Settings」メニューで行います。

MST Configuration Identification (MST の設定)

スイッチ上で MST インスタンスの設定を行います。本設定は MSTI (マルチプルスパニングツリーインスタンス) を識別するためのものです。スイッチは初期状態で 1 つの CIST (Common Internal Spanning Tree) を持ちます。ユーザはその項目を変更できますが、MSTI ID の変更や削除は行うことができません。

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

図 8-44 MST Configuration Identification 画面

上記画面には以下の項目が含まれます。

| 項目 | 説明 |
|--------------------------|---|
| Configuration Name | 各 MSTI (Multiple Spanning Tree Instance) を識別するためにスイッチに名前を設定します。名前が設定されていない場合、MSTP が動作しているデバイスの MAC アドレスが表示されます。 |
| Revision Level (0-65535) | スイッチ上に設定された MSTP リージョンの値を設定します。Configuration Name に同期しています。0 から 65535 の範囲で設定します。初期値は 0 です。 |
| MSTI ID (1-64) | 新規の MSTI ID を 1-64 の範囲から指定します。 |
| Type | MSTI 設定の変更方法を指定します。2 つのタイプから選択します。 <ul style="list-style-type: none"> • Add VID - MSTI ID に「VID List」で指定する VID を追加します。 • Remove VID - MSTI ID から「VID List」で指定する VID を削除します。 |
| VID List | スイッチに登録済みの VLAN の中から VID の範囲を指定します。指定できる VID の範囲は 1 から 4094 までです。 |

「Apply」ボタンをクリックし、デバイスに MST 設定を適用します。

エントリの編集

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

図 8-45 MST Configuration Identification 画面 - Edit

2. 「MST Configuration Identification Settings」セクションに現在の設定が表示されます。設定変更後、「Apply」ボタンをクリックします。

エントリの削除

削除するエントリ横の「Delete」ボタンをクリックします。

STP Instance Settings (STP インスタンス設定)

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

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

図 8-46 STP Instance Settings 画面

本画面には以下の情報があります。

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

「Apply」ボタンをクリックし、新しいプライオリティ設定を適用します。

エントリの編集

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

図 8-47 STP Instance Settings 画面 - Edit

2. 「STP Priority Settings」セクションに現在の設定が表示されます。設定変更後、「Apply」ボタンをクリックし、設定を適用します。

エントリの詳細情報の参照

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

図 8-48 MST Configuration Identification 画面 - View

2. STP インスタンスの状態が表示されます。

MSTP Port Information (MSTP ポート情報)

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

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

図 8-49 MSTP Port Information 画面

指定ポートの MSTP 設定の参照

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

指定ポートの MSTI インスタンス設定の編集

1. 特定の MSTI インスタンス設定を編集する場合は、編集する MSTI の「Edit」ボタンをクリックし、以下の画面を表示します。

MSTP Port Information Safeguard

Unit: 1 Port: 02 Find

MSTP Port Settings

Instance ID: 0 Internal Path Cost (1-200000000): 20000 Priority: 128 Apply

Port 2 Settings

| MSTI | Designated Bridge | Internal Path Cost | Priority | Status | Role | |
|------|-------------------|--------------------|----------|------------|------------|------|
| 0 | 0000fc75163b9c00 | 20000 | 128 | Forwarding | Designated | Edit |
| 2 | N/A | 200000 | 128 | Forwarding | NonStp | Edit |

図 8-50 MSTP Port Information 画面 - Edit

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

以下の項目を設定または参照できます。

| 項目 | 説明 |
|----------------------------------|---|
| Unit | 設定するユニットを選択します。 |
| Port | 適用するポートを選択します。 |
| Instance ID | 設定済みインスタンスの MSTI ID (0-64)。0 は CIST を意味します (初期値は MSTI)。 |
| Internal Path Cost (1-200000000) | インタフェースを STP インスタンスで選択する場合、指定ポートにパケットを転送する相対的なコストを設定します。 <ul style="list-style-type: none"> 0 (Auto) - インタフェースに自動的に最適な最速のルートを設定します。(初期値) 値 1-200000000 - ループが発生した場合、この範囲で指定した値を使用した最短のルートを設定します。コストが小さいほど高速で伝送されます。 |
| Priority | ポートインタフェースのプライオリティ (0-240) までの値を指定します。高いプライオリティほど、パケットの転送は優先されます。値が低いほどプライオリティは高くなります。 |

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

Link Aggregation (ポートトランキングの設定)

ポートトランクグループについて

ポートトランクグループは、多くのポートを結合して1つの広帯域のデータパイプラインとして利用する機能です。本スイッチは各グループ2個から8個のポートを束ねた最大32個のポートトランクグループをサポートしています。

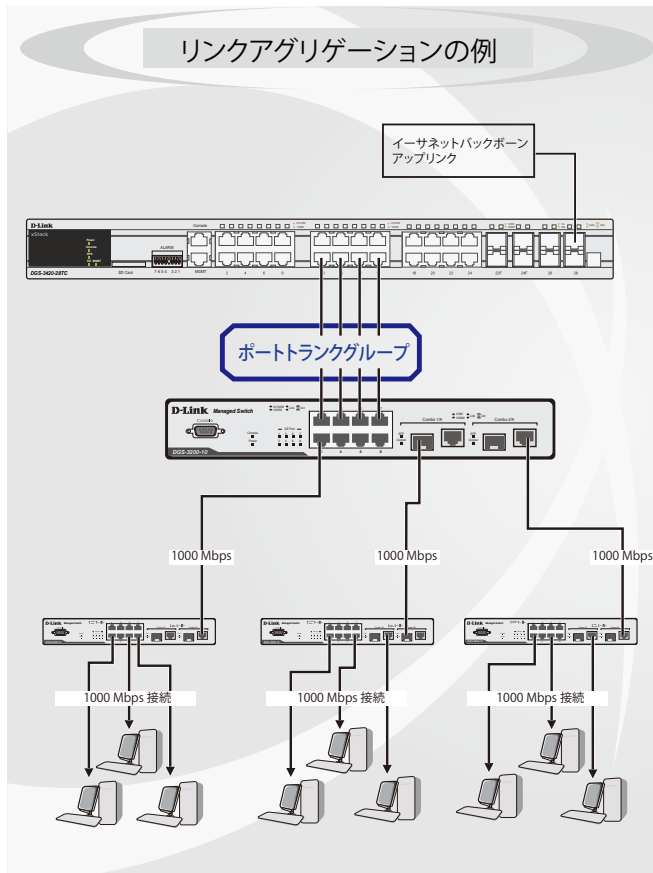


図 8-51 ポートトランクグループの例

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

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

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

本スイッチでは、2から8のリンク（ポート）で構成する最大32個のリンクアグリゲーショングループをサポートします。各ポートは1つのリンクアグリゲーショングループにだけ所属できます。

1つのグループ内の全ポートは同じVLANに属し、それぞれのスパンニングツリープロトコル（STP）ステータス、スタティックマルチキャスト、トラフィックコントロール、トラフィックセグメンテーション、および802.1p デフォルトプライオリティの設定は同じである必要があります。また、ポートロック、および802.1Xは有効化されてはなりません。さらに、集約するリンクはすべて同じ速度で、全二重モードで設定されている必要があります。

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

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

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

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

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

Port Trunking Settings (ポートトランキング設定)

スイッチにポートトランクを設定します。

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

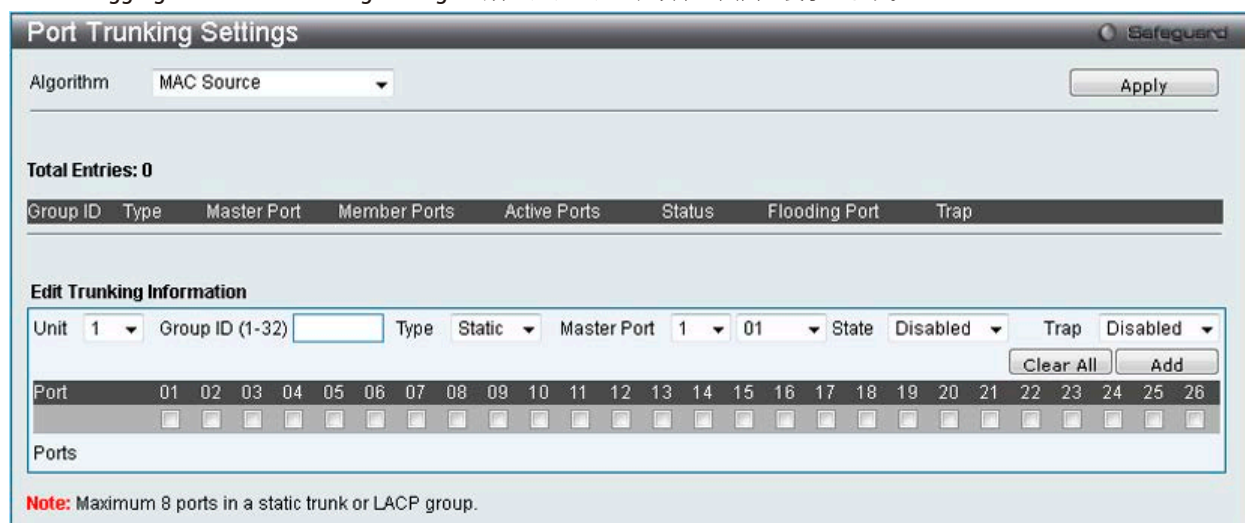


図 8-52 Port Trunking Settings 画面

本画面には次の項目があります。

| 項目 | 説明 |
|---------------------------|---|
| Algorithm | ポートトランクグループを構成するポートのトラフィックハッシュアルゴリズムを選択します。「MAC Source」、「MAC Destination」、「MAC Source Destination」、「IP Source」、「IP Destination」、「IP Source Dest」、「L4 Port Source」、「L4 Port Destination」、「L4 Source Dest」から指定してください。 |
| Group ID | グループの ID 番号が表示されます。 |
| Type | トランキンググループの種類が表示されます。 |
| Member Ports | トランキンググループのメンバポートが表示されます。 |
| Master Port | トランキンググループのマスタポートが表示されます。 |
| Active Ports | 現在パケットの送出を行っているポートが表示されます。 |
| State | ポートトランキンググループを「Enabled」(有効) または「Disabled」(無効) が表示されます。 |
| Flooding Ports | トランクグループ内でフラッディングが発生しているポートが表示されます。 |
| Trap | Trap の状況を表示します。 |
| Edit Trunking Information | |
| Unit | 設定するユニットを指定します。 |
| Group ID (1-32) | グループの ID 番号を 1-32 の範囲から指定します。 |
| Type | トランキンググループの種類を設定します。「Static」または「LACP」から選択します。 LACP (Link Aggregation Control Protocol) を選択すると、ポートトランキンググループ内でのリンクの自動検出を行います。 |
| Master Port | トランキンググループのマスタポートを選択します。 |
| State | ポートトランキンググループを「Enabled」(有効) または「Disabled」(無効) にします。これは、診断、迅速に帯域が集中するネットワークデバイスの迅速な分離する場合、または自動制御下でない独立したバックアップアグリゲーショングループを持つ場合に有益です。 |
| Trap | Trap の有効 / 無効を指定します。 |

ポートトランキンググループの設定

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

ポートトランクグループの編集

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

図 8-53 Port Trunking 画面 - Edit

2. 項目を編集後「Apply」ボタンをクリックします。

ポートトランキンググループの削除

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

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

LACP Port Settings (LACP ポートの設定)

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

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

図 8-54 LACP Port Settings 画面

以下の項目を使用して設定を行います。

| 項目 | 説明 |
|---------------------|---|
| Unit | 設定するユニットを選択します。 |
| From Port / To Port | 設定対象のポート範囲を指定します。 |
| Activity | <ul style="list-style-type: none"> Active - Active ポートは LACP 制御フレームの処理と送信を行います。これにより LACP 準拠のデバイス同士はネゴシエーションとリンクの集約を行い、グループは必要に応じて動的に変更されます。グループへのポート追加、または削除などのグループの変更を行うためには、少なくともどちらかのデバイスで LACP ポートを「Active」に設定する必要があります。また、両方のデバイスは LACP をサポートしている必要があります。 Passive - Passive ポートは自分から LACP 制御フレームの送信を行いません。リンクするポートグループがネゴシエーションを行い、動的にグループの変更を行うためには、接続のどちらか一端が Active な LACP ポートである必要があります。(初期値) |

「Apply」ボタンをクリックし、デバイスに LACP 設定を適用します。

FDB (FDB 設定)

Static FDB Settings (スタティック FDB の設定)

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

スイッチにスタティックなユニキャストフォワーディングを設定します。

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

図 8-55 Unicast Static FDB Settings 画面

以下の項目を使用して設定を行います。

| 項目 | 説明 |
|-------------|--|
| VLAN Name | ラジオボタンをクリックし、関連するユニキャスト MAC アドレスが存在する VLAN 名を入力します。 |
| VLAN List | ラジオボタンをクリックし、関連するユニキャスト MAC アドレスが存在する VLAN リストを入力します。 |
| MAC Address | パケットがスタティックに送信される宛先の MAC アドレス。ユニキャスト MAC アドレスを指定します。 |
| Port/Drop | 上記 MAC アドレスのあるポート番号を指定します。また、本オプションはユニキャストのスタティックな FDB から MAC アドレスを破棄します。 <ul style="list-style-type: none"> Port - 上記 MAC アドレスのあるポート番号を指定します。「ユニット ID: ポート番号」(例 1:5) または「ポート番号」(例 5) という形式とします。ポート番号だけを入力する場合、ユニット番号の初期値は 1 となります。 Drop - ユニキャストのスタティックな FDB から MAC アドレスを破棄します。 |

「Apply」ボタンをクリックして設定を適用します。

エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。

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

スイッチにスタティックなマルチキャストフォワーディングを設定します。

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

The screenshot shows the 'Multicast Static FDB Settings' window. It includes input fields for 'VID', 'Multicast MAC Address', and a 'Unit' dropdown menu. There are 'Clear All' and 'Apply' buttons. A port selection table has two rows: 'None' and 'Egress', each with 'All' buttons and radio buttons for ports 01-26. Below the table, 'Egress Ports' is set to '1:20'. A table at the bottom lists 'Total Entries: 1' with columns for VID, MAC Address, Mode, and Egress Ports, showing a single entry with VID 10, MAC Address 01-00-5E-00-00-01, Mode Static, and Egress Ports 1:20. 'Edit' and 'Delete' buttons are next to the entry.

図 8-56 Multicast Static FDB Setting 画面

以下の項目を使用して設定を行います。

| 項目 | 説明 |
|-----------------------|---|
| VID | 指定の Multicast MAC アドレスが属する VLAN の VLAN ID。 |
| Multicast MAC Address | マルチキャストパケットの送信先 MAC アドレス。マルチキャスト MAC アドレスを指定します。宛先 MAC アドレスの形式は「01-xx-xx-xxxxxx」です、「01-00-5E-xx-xx-xx」は除く必要があります。本機能は、「01-00-5E-xx-xx-xx」を持つ宛先 MAC アドレスをサポートしていません。 |
| Unit | 設定するユニットを選択します。 |
| Port | スタティックマルチキャストグループのメンバとなるポート、および GMRP によって動的にグループに参加させるポート、参加させないポートを選択します。オプションは以下の通りです。 <ul style="list-style-type: none"> None - ダイナミックにマルチキャスト参加を行います。指定すると、ポートはスタティックマルチキャストグループのメンバにはなりません。「All」ボタンをクリックするとすべてのポートを選択します。 Egress - ポートはマルチキャストグループのスタティックメンバとなります。「All」ボタンをクリックするとすべてのポートを選択します。 |

「Apply」ボタンをクリックして設定を適用します。

エントリの編集

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

This screenshot is similar to the previous one but shows the 'Edit' button highlighted with a yellow box. The input fields are now populated with the values: VID: 10, Multicast MAC Address: 01-00-5E-00-00-01, Unit: 1. The 'Egress Ports' field also shows '1:20'. The table at the bottom has the 'Edit' button highlighted.

図 8-57 Multicast Static FDB Setting 画面

2. 項目を編集後「Apply」ボタンをクリックします。

エントリの削除

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

MAC Notification Settings (MAC 通知設定)

MAC Notification (通知) は、学習によりフォワーディングデータベースに記録された MAC アドレスの監視を行うために使用します。スイッチの MAC 通知をグローバルに設定します。また、スイッチの各ポートに MAC 通知を設定します。

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

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

図 8-58 MAC Notification Settings 画面

以下の項目を使用して設定を行います。

| 項目 | 説明 |
|----------------------------------|---|
| MAC Notification Global Settings | |
| State | スイッチ上の MAC 通知をグローバルに「Enabled」(有効) / 「Disabled」(無効) にします。初期値は「Disabled」です。 |
| Interval (1-2147483647) | 通知を行う間隔 (秒)。初期値: 1 (秒) |
| History Size (1-500) | 通知に使用するヒストリログの最大エントリ数 (最大 500 エントリ)。初期値: 1 |
| MAC Notification Port Settings | |
| Unit | 設定するユニットを選択します。 |
| From Port / To Port | プルダウンメニューを使用して MAC 通知を有効にするポート範囲を指定します。 |
| State | 指定したポートの MAC 通知設定を「Enabled」(有効) / 「Disabled」(無効) にします。初期値は「Disabled」です。 |

各セクションの「Apply」ボタンをクリックして行った変更を適用します。

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

スイッチに MAC アドレスエイジングタイムを設定します。

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

図 8-59 MAC Address Aging Time Settings 画面

以下の項目を使用して設定、表示を行います。

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

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

MAC Address Table (MAC アドレステーブル)

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

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

The screenshot shows the 'MAC Address Table' configuration interface. At the top, there are search filters: Unit (1), Port (01), VLAN Name, VID List, MAC Address (00-00-00-00-00), and Security (unchecked). Below these are 'Find' and 'Clear Dynamic Entries' buttons. A 'View All Entries' and 'Clear All Entries' button is also present. The main part of the interface is a table with 6 entries. Each entry has an 'Add to Static MAC table' button. The table columns are VID, VLAN Name, MAC Address, Port, Type, and Status.

| VID | VLAN Name | MAC Address | Port | Type | Status |
|-----|-----------|-------------------|------|---------|---------|
| 1 | default | 00-13-72-0F-28-A4 | 1:2 | Dynamic | Forward |
| 1 | default | 00-24-A5-4E-C9-C2 | 1:2 | Dynamic | Forward |
| 1 | default | 00-A0-B0-A3-6C-BA | 1:2 | Dynamic | Forward |
| 1 | default | 12-34-56-78-90-12 | 1:3 | Static | Forward |
| 1 | default | 14-FE-B5-E6-8A-B4 | 1:2 | Dynamic | Forward |
| 1 | default | FC-75-16-3B-9C-00 | CPU | Self | Forward |

図 8-60 MAC Address Table 画面

以下の項目を使用して、設定および表示を行います。

| 項目 | 説明 |
|-------------|--|
| Unit | 設定するユニットを選択します。 |
| Port | 以下の MAC アドレスと関連付けられるポート。 |
| VLAN Name | 参照するフォワーディングテーブルの VLAN 名を入力します。 |
| VID List | 参照するフォワーディングテーブルの VLAN リストを入力します。 |
| MAC Address | 参照するフォワーディングテーブルの MAC アドレスを入力します。 |
| Security | チェックすると、セキュリティモジュールによって作成される FDB エントリを表示します。 |

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

エントリの検索

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

ダイナミックエントリの削除

「Clear Dynamic Entries」ボタンをクリックして、アドレステーブルのすべてのダイナミックエントリを削除します。

エントリの表示

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

全エントリの削除

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

エントリの追加

「Add to Static MAC table」ボタンをクリックして、スタティックテーブルに指定エントリを追加します。

ARP & FDB Table (ARP と FDB テーブル)

ARP と FDB テーブルのパラメータを検索します。

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

The screenshot shows the 'ARP & FDB Table' configuration interface. At the top, there are search criteria: Unit (1), Port (01), MAC Address (00-00-00-00-00-00), and IP Address. Search buttons include 'Find by Port', 'Find by MAC', 'Find by IP Address', and 'View All Entries'. Below the search area, a table displays 'Total Entries: 1' with the following data:

| Interface | IP Address | MAC Address | VLAN Name | Port |
|-----------|--------------|-------------------|-----------|------|
| System | 192.168.1.12 | 00-13-72-0F-28-A4 | default | 1:1 |

An 'Add to IP MAC Port Binding Table' button is located to the right of the table entry.

図 8-61 ARP & FDB Table 画面

以下の項目を使用して、設定および表示を行います。

| 項目 | 説明 |
|-------------|--------------------------|
| Unit | 設定するユニットを選択します。 |
| Port | この設定に使用するポート番号を選択します。 |
| MAC Address | 本設定に使用する MAC アドレスを指定します。 |
| IP Address | 本設定に使用する IP アドレスを入力します。 |

エントリの検索 (ポートベース)

「Find by Port」ボタンをクリックして、選択したポート番号に基づく特定のエントリを検出します。

エントリの検索 (MAC ベース)

「Find by MAC」ボタンをクリックして、入力した MAC アドレスに基づく特定のエントリを検出します。

エントリの検索 (IP アドレスベース)

「Find by IP Address」ボタンをクリックして、入力した IP アドレスに基づく特定のエントリを検出します。

エントリの表示

「View All Entries」ボタンをクリックして、すべてのエントリを表示します。

エントリの追加

「Add to IP MAC Port Binding Table」ボタンをクリックして、IP MAC ポートバインディングテーブルに指定エントリを追加します。

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

IGMP Proxy (IGMP プロキシ)

IGMP プロキシは、IGMP フォワーディングに基づいてアップストリームでは IGMP のホスト部分を、ダウンストリームでは IGMP のルータ部分を実行して、エッジボックスなどのデバイスに VLAN を通過するマルチキャストトラフィックを複製します。これによりコアネットワークに送信される IGMP コントロールパケット数を削減します。

IGMP Proxy Settings (IGMP プロキシ設定)

IGMP プロキシの状態と IGMP プロキシのアップストリームインタフェースを設定します。

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

図 8-62 IGMP Proxy Settings 画面

以下の項目を使用して、設定および表示を行います。

| 項目 | 説明 |
|------------------------------------|---|
| IGMP Proxy Global Settings | |
| IGMP Proxy State | ラジオボタンを使用して IGMP プロキシのグローバル状態を「Enabled」(有効)/「Disabled」(無効)にします。 |
| IGMP Proxy Upstream Settings | |
| VLAN Name | 先頭のラジオボタンをチェックして、インタフェースの VLAN 名を入力します。 |
| VID | 先頭のラジオボタンをチェックして、インタフェースの VLAN ID を入力します。 |
| Source IP Address | 上流プロトコルのパケットの IP アドレスを入力します。指定しないと、ゼロ IP アドレスがプロトコルの送信元 IP アドレスとして使用されます。 |
| Unsolicited Report Interval (0-25) | Unsolicited レポート間隔。グループ内のメンバシップに関するホストの開始レポートの送信する間隔。初期値は 10 (秒) です。0 に設定すると、1 つのレポートパケットだけを送信することを意味します。 |
| Unit | 設定するユニットを選択します。 |
| Static Router Port | 本設定に含めるポートを選択します。 |

「Apply」ボタンをクリックして各セクションで行った変更を適用します。

「Select All」ボタンをクリックするとすべてのポートを選択します。

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

IGMP Proxy Downstream Settings (IGMP プロキシダウンストリーム設定)

IGMP プロキシのダウンストリームインタフェースを設定します。IGMP プロキシのダウンストリームインタフェースはIGMP Snooping が有効な VLAN である必要があります。

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

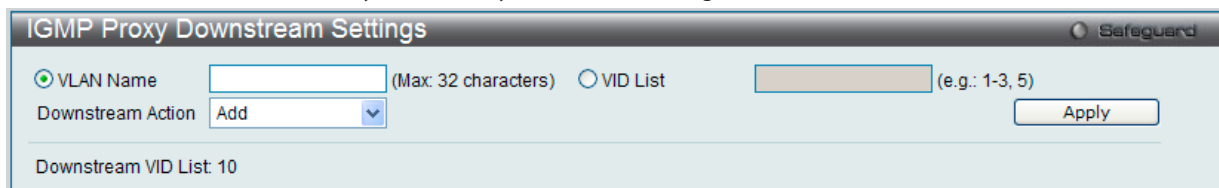


図 8-63 IGMP Proxy Downstream Settings 画面

以下の項目を使用して、設定および表示を行います。

| 項目 | 説明 |
|-------------------|--|
| VLAN Name | IGMP プロキシダウンストリームインタフェースに所属する VLAN 名を指定します。 |
| VID List | IGMP プロキシダウンストリームインタフェースに所属する VLAN のリストを指定します。 |
| Downstream Action | ダウンストリームインタフェースの「Add」(追加) または「Delete」(削除) を行います。 |

「Apply」 ボタンをクリックして行った変更を適用します。

IGMP Proxy Group (IGMP プロキシグループ)

IGMP プロキシグループ設定を参照します。

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

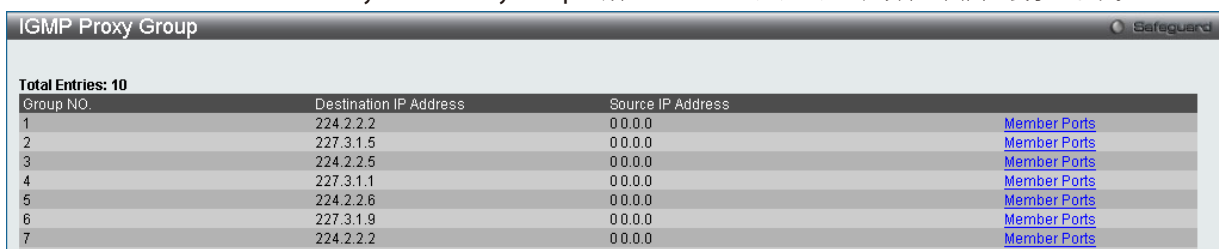


図 8-64 IGMP Proxy Group 画面

IGMP プロキシメンバポートの参照

「[Member Ports](#)」 リンクをクリックして、以下の画面が表示されます。

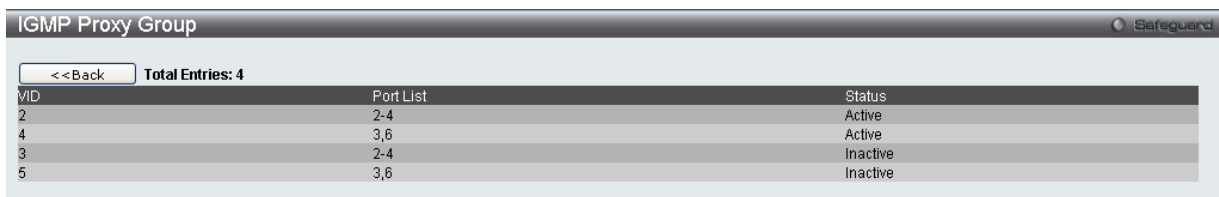


図 8-65 IGMP Proxy Group 画面

IGMP Snooping (IGMP Snooping の設定)

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

IGMP Snooping Settings (IGMP Snooping 設定)

IGMP Snooping 設定をグローバルに有効または無効にします。

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

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

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

図 8-66 IGMP Snooping Settings 画面

画面には以下の項目があります。

| 項目 | 説明 |
|-------------------------------|---|
| IGMP Snooping Global Settings | |
| IGMP Snooping State | IGMP Snooping 状態を有効または無効にします。 <ul style="list-style-type: none"> Enabled - デバイスで IGMP Snooping を有効にします。 Disabled - デバイスで IGMP Snooping を無効に設定します。(初期値) |
| Max Learned Entry Value | Data Driven 機能が学習するグループの最大エントリ数を指定します。この値は、1-960 である必要があります。 |

IGMP Snooping 機能の利用

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

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

IGMP Snooping 機能の詳細設定

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

図 8-67 IGMP Snooping Parameters Settings 画面

以下の項目を参照または編集することができます。

| 項目 | 説明 |
|-----------------------------------|---|
| VID | VLAN ID を表示します。VLAN 名と共に、IGMP Snooping 設定の対象となる VLAN を識別するために使用します。 |
| VLAN Name | IGMP Snooping クエリアを設定する VLAN 名を表示します。VLAN ID と共に、IGMP Snooping 設定を行う対象の VLAN を識別します。 |
| Rate Limit | スイッチが特定のポート / VLAN で処理できる IGMP 制御パケットのレートを表示します。レートはパケット / 毎秒で指定されます。制限レートを超過したパケットは破棄されます。 |
| Querier IP | ネットワークに IGMP クエリを送信するデバイスの IP アドレスを表示します。 |
| Query Interval (1-65535) | 一般的な IGMP クエリア送信間隔 (秒) を指定します。初期値は 125 (秒) です。 |
| Max Response Time (1-25) | メンバからのレポートを待つ最大時間を 1-25 (秒) で設定します。初期値は 10 (秒) です。 |
| Robustness Value (1-7) | 予想されるサブネット上のパケットの損失に応じてこの変数を調整します。Robustness Variable は以下の IGMP メッセージ間隔を計算して使用されます。1-7 の範囲から指定します。初期値は 2 です。 |
| Last Member Query Interval (1-25) | Group-Specific Query メッセージ (Leave Group メッセージに応じて送信されるものも含む) の最大送信間隔を指定します。この間隔はルータがグループのラストメンバの損失を検出するためにかかる時間をより減少するように低くします。初期値は 1 です。 |
| Data Driven Group Expiry Time | 使用する Data Driven グループの生存時間を指定します。エージングオプションが有効な場合のみ、本値は有効です。 |
| Proxy Reporting Source IP | プロキシレポートの送信元 IP アドレスを指定します。 |
| Proxy Reporting State | プルダウンメニューを使用して、本機能を「Enabled」(有効) / 「Disabled」(無効) にします。 |
| Querier State | クエリア状態を有効または無効にします。 <ul style="list-style-type: none"> Enabled - スイッチが IGMP クエリパケットを送信する IGMP クエリアとして選択されます。 Disabled - スイッチが IGMP クエリアとしての役目を果たしません。 |
| Fast Leave | IGMP Snooping の Fast Leave 機能を有効または無効にします。有効にすると、システムが IGMP Leave メッセージを受信するとメンバはすぐにグループから削除されます。 |
| State | 指定した VLAN への IGMP Snooping 機能を「Enabled」(有効) / 「Disabled」(無効) にします。初期値は無効です。 注意 スイッチに接続するレイヤ 3 ルータが IGMP プロキシ機能だけを提供し、マルチキャストルーティング機能を提供しない場合、この状態は無効に設定されます。そうでない場合、レイヤ 3 ルータをクエリアとして選択しないと、IGMP クエリパケットを送信しません。また、マルチキャストルーティングプロトコルパケットを送信しないため、ポートはルータポートとしてタイムアウトになります。 |
| Data Driven Learning State | IGMP Snooping グループの Data Driven Learning を有効または無効にします。Data Driven Learning が VLAN に対して有効な場合、スイッチがこの VLAN で IP マルチキャストトラフィックを受信すると、IGMP Snooping グループが作成されます。エントリの学習は IGMP メンバシップ登録ではなく、トラフィックによりアクティブになります。通常の IGMP Snooping エントリのために、IGMP プロトコルはエントリのエージングアウトを認めます。Data Driven エントリのために、エントリは、エージングタイマによってエージングアウトしないように指定されます。Data Driven Learning が有効で、Data Driven テーブルがフルではない場合、すべてのポートのマルチキャストフィルタリングモードは無視されます。つまり、マルチキャストパケットはルータポートに送信されます。Data Driven Learning テーブルがフルの場合、マルチキャストフィルタリングモードに従って、マルチキャストパケットは送信されます。Data Driven グループが作成され、IGMP メンバポートがその後学習されると、エントリは、通常の IGMP Snooping エントリになることに注意してください。エージングアウトメカニズムは、通常の IGMP Snooping エントリに追従します。 |
| Data Driven Learning Aged Out | エントリのエージングアウトを有効または無効に指定します。 |

| 項目 | 説明 |
|---------|--|
| Version | このポートに送信される IGMP パケットのバージョンを指定します。インタフェースが受信した IGMP パケットが指定のバージョンより高いバージョンを持つ場合、本パケットはルータポートから転送されるか、VLAN 内にフラッディングされます。 |

上記項目設定後、「Apply」ボタンをクリックして変更を有効にします。

前の画面に戻るためには、「<< Back」ボタンをクリックします。

IGMP Snooping ルータポート設定の変更

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

図 8-68 IGMP Snooping Router Ports Settings 画面

以下の項目を設定または表示します。

| 項目 | 説明 |
|-----------------------|---|
| Unit | 設定するユニットを選択します。 |
| Static Router Port | マルチキャストが有効なルータに接続するポート範囲を指定します。これは、宛先としてルータが持つすべてのパケットをプロトコルなどにかかわらず、マルチキャストが有効なルータに到達するように設定します。 |
| Forbidden Router Port | マルチキャストが有効なルータに接続しないポート範囲を指定します。これは、禁止ポートがルーティングパケットを送信しないように設定します。 |
| Dynamic Router Port | ダイナミックに設定されたルータポートを表示します。 |

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

「Select All」ボタンをクリックするとすべてのポートを選択します。

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

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

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

IGMP Snooping レート制限パラメータを設定します。

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

図 8-69 IGMP Snooping Rate Limit Settings 画面

以下の項目があります。

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

「Apply」ボタンをクリックして行った変更を適用します。

エントリの編集

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

図 8-70 IGMP Snooping Rate Limit Settings 画面

2. 指定エントリを編集して「Apply」ボタンをクリックします。

エントリの参照

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

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

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

スイッチの IGMP Snooping スタティックグループテーブルを参照します。IGMP Snooping 機能では、スイッチを通過する IGMP パケットからマルチキャストグループ IP アドレスと対応する MAC アドレスを読み取ることができます。

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

図 8-71 IGMP Snooping Static Group Settings 画面

以下の項目を設定または表示します。

| 項目 | 説明 |
|--------------|-----------------------|
| VLAN Name | マルチキャストグループの VLAN 名。 |
| VID List | マルチキャストグループの VID リスト。 |
| IPv4 Address | IPv4 アドレスを指定します。 |

エントリの参照

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

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

エントリの登録

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

エントリの削除

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

エントリの編集

「Edit」ボタンをクリックして、以下の画面を表示します。

図 8-72 IGMP Snooping Static Group Settings 画面

以下の項目を設定または表示します。

| 項目 | 説明 |
|-------|---|
| Unit | 設定するユニットを選択します。 |
| Ports | 個別に適切なポートを選択して、IGMP Snooping スタティックグループ設定に含めます。 |

「Apply」ボタンをクリックして行った変更を適用します。

「Select All」ボタンをクリックするとすべてのポートを選択します。

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

IGMP Router Port (ルータポート参照)

スイッチが現在ルータポートとして設定しているポートを表示します。

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

図 8-73 IGMP Router Port 画面

1. 画面上のVID(VLAN ID)を入力します。
2. 「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

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

コンソールまたは Web ベースの管理インタフェースで設定されたルータポートはスタティックルータポートとして「S」で表示されます。スイッチにダイナミックに設定されたルータポートは「D」と表示され、Forbidden ポートは「F」と表示されます。

IGMP Snooping Group (IGMP Snooping グループ)

スイッチのIGMP Snooping グループテーブルを参照します。IGMP Snooping 機能では、スイッチを通過するIGMPパケットからマルチキャストグループのIPアドレスと送信元のIPアドレスを読み取ることができます。

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

図 8-74 IGMP Snooping Group 画面

以下の項目があります。

| 項目 | 説明 |
|-------------------------|--|
| VLAN Name | マルチキャストグループのVLAN名。 |
| VID List (e.g.: 1, 4-6) | マルチキャストグループのVLAN ID リスト。 |
| Port List | マルチキャストグループを検索するのに使用されるポート番号を指定します。 |
| Group IPv4 Address | IPv4アドレスを指定します。 |
| Data Driven | IGMP Snooping グループの Data Driven Learning を有効または無効にします。 |

エントリの参照

画面左上の「VLAN Name」または「VID」を入力して「Find」ボタンをクリックすることにより、IGMP Snooping グループテーブルを検索することができます。「View All」ボタンをクリックして、すべての定義済みエントリを表示します。検索されたエントリは「IGMP Snooping Group Table」に表示されます。

Data Driven 情報のクリア

「Clear Data Driven」ボタンをクリックして、Data Driven 情報をクリアします。「Clear All Data Driven」ボタンをクリックして、すべての Data Driven 情報をクリアします。

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

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

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

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

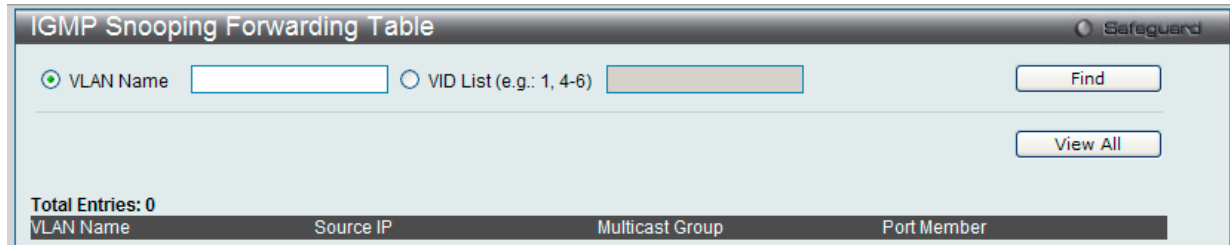


図 8-75 IGMP Snooping Forwarding Table 画面

以下の項目が表示されます。

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

エントリの参照

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

カウンタテーブルの参照

「Packet Statistics」リンクをクリックして、IGMP Snooping カウンタテーブルを参照します。

IGMP Snooping Counter (IGMP Snooping カウンタ)

スイッチの IGMP Snooping カウンタテーブルを参照します。

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

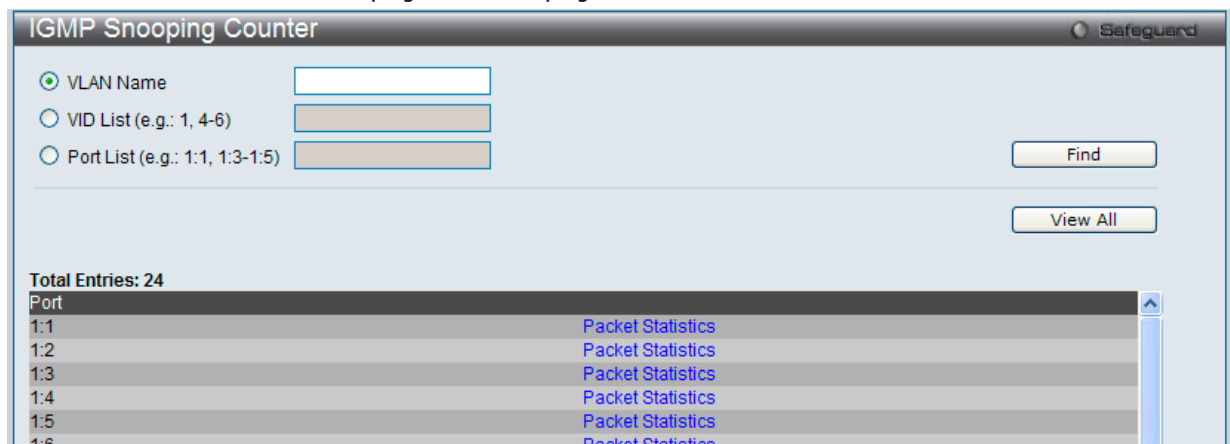


図 8-76 IGMP Snooping Counter 画面

以下の項目が表示されます。

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

エントリの参照

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

IGMP Snooping カウンタテーブルの参照

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

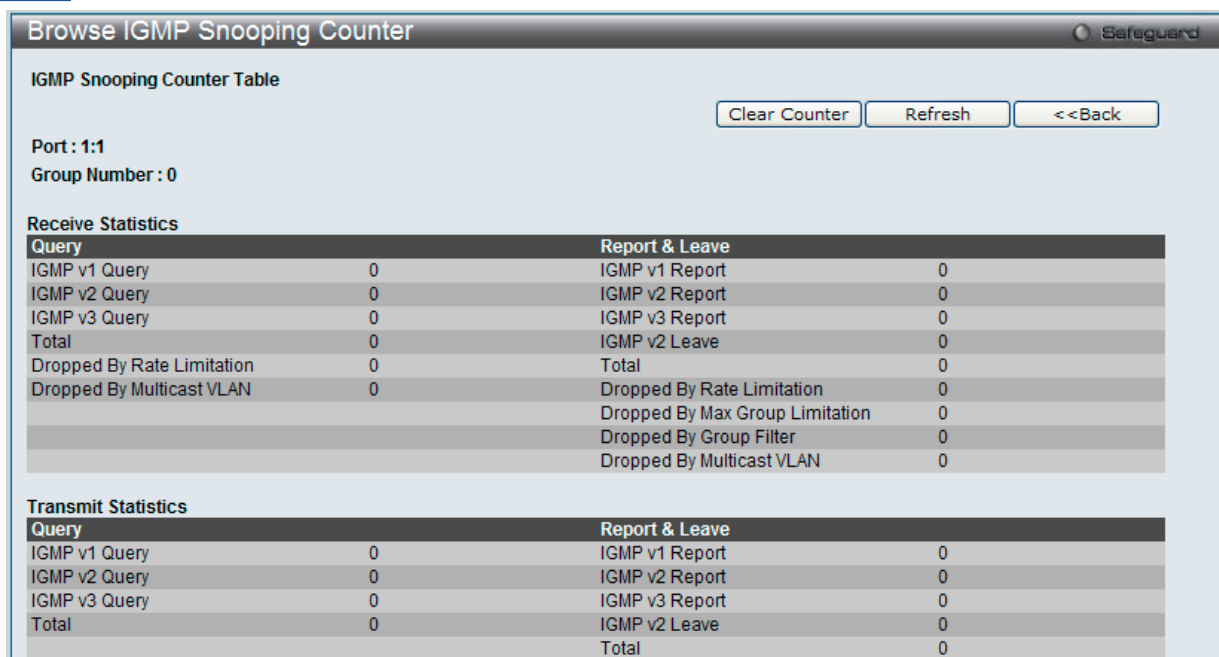


図 8-77 Browse IGMP Snooping Counter 画面

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

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

「<<Back」ボタンをクリックして前のページに戻ります。

IGMP Snooping Forward Lookup Mode Settings (IGMP Snooping フォワーディング検索モード設定)

IGMP Snooping フォワーディングモード設定を行います。

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

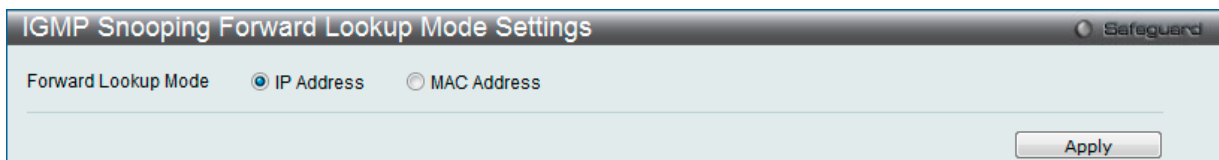


図 8-78 IGMP Snooping Forward Lookup Mode Settings 画面

設定対象となる項目は以下の通りです：

| 項目 | 説明 |
|---------------------|--|
| Forward Lookup Mode | 適切な IGMP Snooping 転送検索モードを選択します。 <ul style="list-style-type: none"> • IP Address - IP アドレスに基づいてマルチキャストフォワーディング検索を行います。 • MAC Address - MAC アドレスに基づいてマルチキャストフォワーディング検索を行います。 |

「Apply」ボタンをクリックして行った変更を適用します。

MLD Proxy (MLD プロキシ)

MLD プロキシはアップストリームインタフェースでホストの役割を果たします。MLD Report パケットはルータポートに送信されます。MLD プロキシはダウンストリームインタフェースでルータの役割を果たします。これによりコアネットワークに送信される MLD コントロールパケット数を削減します。

MLD Proxy Settings (MLD プロキシ設定)

MLD プロキシの状態と MLD プロキシのアップストリームインタフェースを設定します。

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

図 8-79 MLD Proxy Settings 画面

以下の項目が表示されます。

| 項目 | 説明 |
|------------------------------------|--|
| MLD Proxy Global Settings | |
| MLD Proxy State | MLD プロキシのグローバル状態を有効または無効にします。 |
| MLD Proxy Upstream Settings | |
| VLAN Name | 先頭のラジオボタンをチェックして、インタフェースの VLAN 名を入力します。 |
| VID | 先頭のラジオボタンをチェックして、インタフェースの VLAN ID を入力します。 |
| Source IP Address | アップストリームプロトコルパケットの IPv6 アドレスを入力します。指定しないと、ゼロ IP アドレスがプロトコルの送信元 IP アドレスとして使用されます。 |
| Unsolicited Report Interval (0-25) | Unsolicited レポート間隔。グループ内のメンバシップに関するホストの開始レポートの送信する間隔。初期値は 10 (秒) です。0 に設定されると、1 つのレポートパケットだけを送信することを意味します。 |
| Unit | 設定するユニットを選択します。 |
| Static Router Port | 設定に適用するスタティックルータポートを入力します。 |
| Dynamic Router Port | マルチキャストが有効なルータに接続するポートリストを表示します。 |

「Apply」 ボタンをクリックして各セクションで行った変更を適用します。

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

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

MLD Proxy Downstream Settings (MLD プロキシダウンストリーム設定)

MLD プロキシのダウンストリームインタフェースを設定します。MLD プロキシのダウンストリームインタフェースは MLD Snooping が有効な VLAN である必要があります。

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

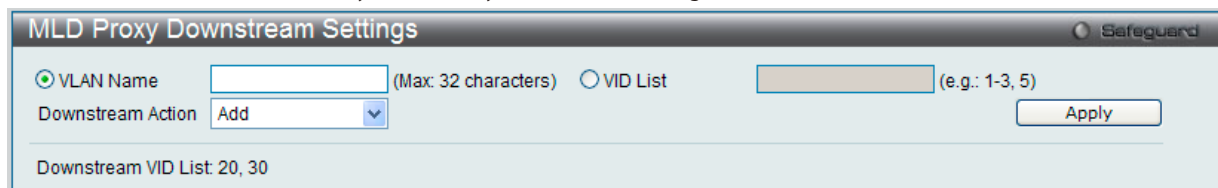


図 8-80 MLD Proxy Downstream Settings 画面

以下の項目が表示されます。

| 項目 | 説明 |
|-------------------|---|
| VLAN Name | MLD プロキシダウンストリームインタフェースに所属する VLAN 名を入力します。 |
| VID List | MLD プロキシダウンストリームインタフェースに所属する VID リストを入力します。 |
| Downstream Action | 適切な操作を選択します。 <ul style="list-style-type: none"> • Add - ダウンストリームインタフェースを追加します。 • Delete - ダウンストリームインタフェースを削除します。 |

「Apply」 ボタンをクリックして行った変更を適用します。

MLD Proxy Group (MLD プロキシグループ)

MLD プロキシグループ設定を参照します。

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

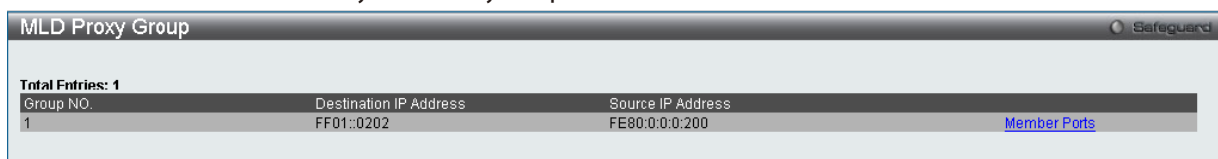


図 8-81 MLD Proxy Group 画面

MLD プロキシメンバポートの参照

「[Member Ports](#)」リンクをクリックすると、以下の画面が表示されます。

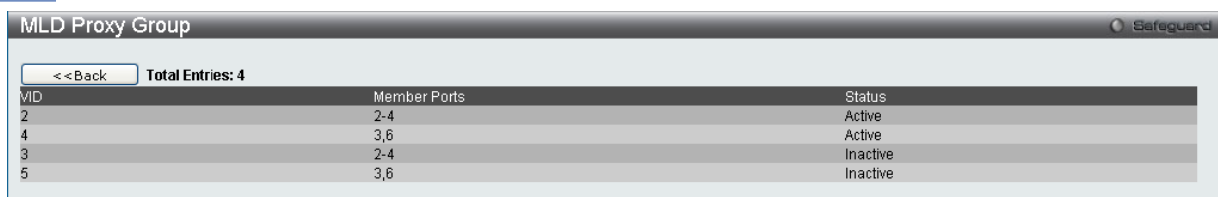


図 8-82 MLD Proxy Group 画面

MLD Snooping (MLD Snooping 設定)

Multicast Listener Discovery (MLD) Snooping は、IPv4 の IGMP Snooping と同じように使用される IPv6 機能です。マルチキャストデータを要求する VLAN に接続しているポートを検出するために使用されます。選択した VLAN 上のすべてのポートにマルチキャストトラフィックが流れる替わりに、MLD Snooping は、リクエストポートとマルチキャストの送信元によって生成する MLD クエリと MLD レポートを使用してデータを受信したいポートにのみマルチキャストデータを転送します。

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

MLD コントロールメッセージ

MLD Snooping バージョン 1 の実行には、デバイス間で 3 つのタイプのメッセージが送信されます。これらのメッセージは、130、131、132 および 143 にラベル付けされた ICMPv6 パケットヘッダによって定義されています。

1. Multicast Listener Query

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

2. Multicast Listener Report Version 1

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

3. Multicast Listener Done

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

4. Multicast Listener Report, Version 2

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

MLD Snooping Settings (MLD Snooping 設定)

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

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

MLD Snooping Settings Safeguard

MLD Snooping Global Settings

MLD Snooping State Enabled Disabled Apply

MLD Data Driven Learning Settings

Max Learned Entry Value (1-480) Apply

Total Entries: 2

| VID | VLAN Name | State | | |
|-----|-----------|----------|------------------------------------|-------------------|
| 1 | default | Disabled | Modify Router Port | Edit |
| 2 | PVLAN | Disabled | Modify Router Port | Edit |

1/1 1 Go

図 8-83 MLD Snooping Settings 画面

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

L2 Features (L2機能の設定)

画面には以下の項目があります。

| 項目 | 説明 |
|-----------------------------------|--|
| MLD Snooping Global Settings | |
| MLD Snooping State | ラジオボタンをクリックして MLD Snooping 状態を「Enabled」(有効) / 「Disabled」(無効) にします。 |
| MLD Data Driven Learning Settings | |
| Max Learned Entry Value | Data Driven 機能が学習するグループの最大エントリ数を指定します。この値は、1-480 である必要があります。 |

「Apply」 ボタンをクリックして各セクションで行った変更を適用します。

MLD Snooping のグローバル設定

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

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

MLD Snooping 機能の詳細設定

関連する VLAN エントリの「Edit」 ボタンをクリックして以下の画面を表示します。

図 8-84 MLD Snooping Parameters Settings 画面

以下の項目を参照または編集することができます。

| 項目 | 説明 |
|-----------------------------------|--|
| VID | VLAN 名と共に MLD Snooping 設定の編集を行う VLAN を識別するために使用する ID です。 |
| VLAN Name | VLAN ID と共に MLD Snooping 設定の編集を行う VLAN を識別するために使用する名称です。 |
| Rate Limit | スイッチが特定のポート /VLAN で処理できる MLD 制御パケットのレートを表示します。レートはパケット / 秒で指定されます。制限レートを超過したパケットは破棄されます。 |
| Querier IP | ネットワークに MLD クエリを送信するデバイスの IP アドレスを表示します。 |
| Querier Expiry Time | クエリアの有効時間を表示します。 |
| Query Interval (1-65535) | 一般的なクエリア送信間隔 (秒) を指定します。初期値は 125 (秒) です。 |
| Max Response Time (1-25) | リスナーからのからのレポートを待つ最大時間を 1-25 (秒) で設定します。初期値は 10 (秒) です。 |
| Robustness Value (1-7) | <p>予想されるサブネット上のパケットの損失に応じてこの変数を調整します。Robustness Variable は以下の MLD メッセージ間隔を計算して使用されます。1-7 の範囲から指定します。初期値は 2 です。</p> <ul style="list-style-type: none"> • Group Listener Interval - マルチキャストルータがネットワーク上のグループにリスナーがいないと判断するまでの時間。 • Other Querier Present Interval- マルチキャストルータがクエリアである他のマルチキャストルータがないと判断するまでの時間。 • Last Listener Query Count- ルータがグループにローカルリスナーがいないと見なす前に送信された Group-Specific Query 数。初期値は Robustness Variable の値です。 <p>サブネットが失われたと予想する場合には、この値を増やすことができます。</p> |
| Last Member Query Interval (1-25) | Group-Specific Query メッセージ (Leave Group メッセージに応じて送信されるものも含む) の最大送信間隔を指定します。この間隔はルータがグループのラストメンバの損失を検出するためにかかる時間をより減少するように低くします。 |
| Data Driven Group Expiry Time | 使用する Data Driven グループの生存時間を指定します。エージングオプションが有効な場合のみ、本値は有効です。 |
| Proxy Reporting Source IP | プロキシレポートの送信元 IPv6 アドレスを指定します。 |
| Proxy Reporting State | プルダウンメニューを使用して、本機能を「Enabled」(有効) / 「Disabled」(無効) にします。 |

| 項目 | 説明 |
|-------------------------------|--|
| Querier State | 有効または無効にして、スイッチを (MLD クエリパケットを送信する) MLD Querier または (MLD クエリパケットを送信しない) Non-Querier として指定します。初期値は無効です。 |
| Fast Done | MLD Snooping の Fast Done 機能を有効または無効にします。有効にすると、システムが MLD Leave メッセージを受信するとメンバはすぐにグループから削除されます。 |
| State | 指定した VLAN への MLD Snooping 機能を「Enabled」(有効) / 「Disabled」(無効) にします。初期値は無効です。 <ul style="list-style-type: none"> Enabled - スイッチが MLD クエリパケットを送信する MLD クエリアとして選択されます。 Disabled - スイッチは MLD クエリアとしての役目を果たしません。 |
| Data Driven Learning State | MLD Snooping グループの Data Driven Learning を有効または無効にします。Data Driven Learning が VLAN に対して有効な場合、スイッチがこの VLAN で IP マルチキャストトラフィックを受信すると、MLD Snooping グループが作成されます。つまり、エントリの学習は MLD メンバシップ登録ではなく、トラフィックによりアクティブになります。通常の MLD Snooping エントリのために、MLD プロトコルはエントリのエージングアウトを認めず、Data Driven エントリのために、エントリは、エージングアウトしないように指定されるか、またはエージングタイムによってエージングアウトするように指定されます。Data Driven Learning が有効で、Data Driven テーブルがフルではない場合、すべてのポートのマルチキャストフィルタリングモードは無視されます。つまり、すべてのマルチキャストパケットはルータポートに送信されます。Data Driven Learning テーブルがフルの場合、マルチキャストフィルタリングモードに従って、マルチキャストパケットは送信されます。Data Driven グループが作成され、MLD メンバポートが後で学習されると、エントリは、通常の MLD Snooping エントリになります。エージングアウトメカニズムは、通常 MLD Snooping エントリに追従します。 |
| Data Driven Learning Aged Out | エントリのエージングを有効または無効にします。初期値では「Disabled」(無効) になっています。 |
| Version | このポートに送信される MLD パケットのバージョンを指定します。インターフェースが受信した MLD パケットが指定のバージョンより高いバージョンを持つ場合、本パケットはルータポートから転送されるか、VLAN 内にフラディングされます。 |
| Querier Role | Query パケット送信についてのスイッチの動作を表示します。 <ul style="list-style-type: none"> Querier - スイッチが MLD Query パケットの送信を行います。 Non-Querier - スイッチが MLD Query パケットの送信を行いません。 本項目は「Querier State」と「State」で「Enabled」指定時には「Querier」と表示されます。 |

上記項目設定後、「Apply」ボタンをクリックして変更を有効にします。

「<<Back」ボタンをクリックし、変更を破棄して前のページに戻ります。

「Modify Router Port」リンクをクリックすると、エントリの編集をすることができます。

MLD Snooping ルータポートの設定

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

図 8-85 MLD Snooping Router Port Settings 画面

以下の項目を指定します。

| 項目 | 説明 |
|-----------------------|---|
| Unit | 設定するユニットを選択します。 |
| Static Router Port | マルチキャストが有効なルータに接続するポート範囲を指定します。これは、宛先としてルータが持つすべてのパケットをプロトコルなどにかかわらず、マルチキャストが有効なルータに到達するように設定します。 |
| Forbidden Router Port | マルチキャストが有効なルータに接続しないポート範囲を指定します。これは、禁止ポートがルーティングパケットを送信ないように設定します。 |

L2 Features (L2機能の設定)

| 項目 | 説明 |
|---------------------|---------------------------|
| Dynamic Router Port | ダイナミックに設定されたルータポートを表示します。 |

「Apply」 ボタンをクリックして行った変更を適用します。

「<<Back」 ボタンをクリックし、変更を破棄して前のページに戻ります。

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

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

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

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

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

The screenshot shows the 'MLD Snooping Rate Limit Settings' interface. At the top, there are two radio buttons: 'Port List' (selected) and 'VID List'. Below them are input fields for 'Port List' (with example '1:1, 2:3-2:4') and 'VID List' (with example '1, 3-4'). A 'Rate Limit (1-1000)' field is set to 'No Limit' with a checked checkbox. An 'Apply' button is visible. Below this is another section with 'Port List' and 'VID List' fields and a 'Find' button. A table titled 'Total Entries: 5' lists VID values (1, 10, 20, 30, 40) and their corresponding 'Rate Limit' (all 'No Limit'). Each row has an 'Edit' button.

図 8-86 MLD Snooping Rate Limit Settings 画面

以下の項目があります。

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

「Apply」 ボタンをクリックして行った変更を適用します。

エントリの参照

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

エントリの編集

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

This screenshot is similar to the previous one but shows the 'Edit' mode for the first entry (VID 1). The 'Rate Limit' field for VID 1 is highlighted with a blue border, and the 'No Limit' checkbox is now unchecked, indicating it is being modified. The 'Apply' button is visible next to the field.

図 8-87 MLD Snooping Rate Limit Settings 画面 - Edit

2. 指定エントリを編集して「Apply」 ボタンをクリックします。

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

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

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

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

図 8-88 MLD Snooping Static Group Settings 画面

以下の項目を設定または表示します。

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

エントリの参照

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

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

エントリの削除

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

エントリの登録

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

エントリの編集

「Edit」ボタンをクリックして、以下の画面を表示します。

図 8-89 MLD Snooping Static Group Settings 画面

「Unit」で設定するユニットを選択します。

「Select All」ボタンをクリックするとすべてのポートを選択します。

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

「Apply」ボタンをクリックして行った変更を適用します。

「<<Back」ボタンをクリックし、変更を破棄して前のページに戻ります。

MLD Router Port (ルータポート参照)

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

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

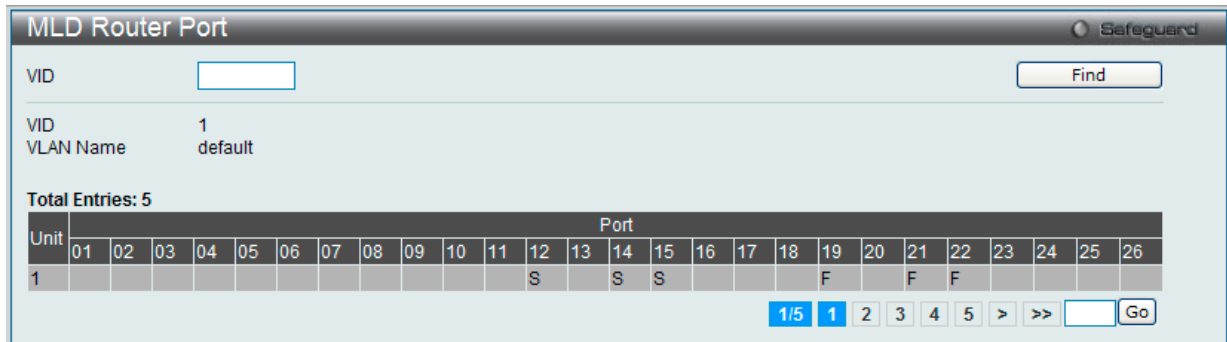


図 8-90 MLD Router Port 画面

1. 画面上の VID(VLAN ID) を入力します。
2. 「Find」 ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

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

注意

コンソールまたは Web ベースの管理インターフェースで設定されたルータポートはスタティックルータポートとして「S」で表示されます。スイッチにダイナミックに設定されたルータポートは「D」と表示され、Forbidden ポートは「F」と表示されます。

MLD Snooping Group (MLD Snooping グループ)

スイッチの MLD Snooping グループテーブルを参照します。MLD Snooping 機能では、スイッチを通過する MLD パケットからマルチキャストグループの IP アドレスと送信元の IP アドレスを読み取ることができます。MLD Snooping は、IPv4 の IGMP Snooping に相当する IPv6 の機能です。

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

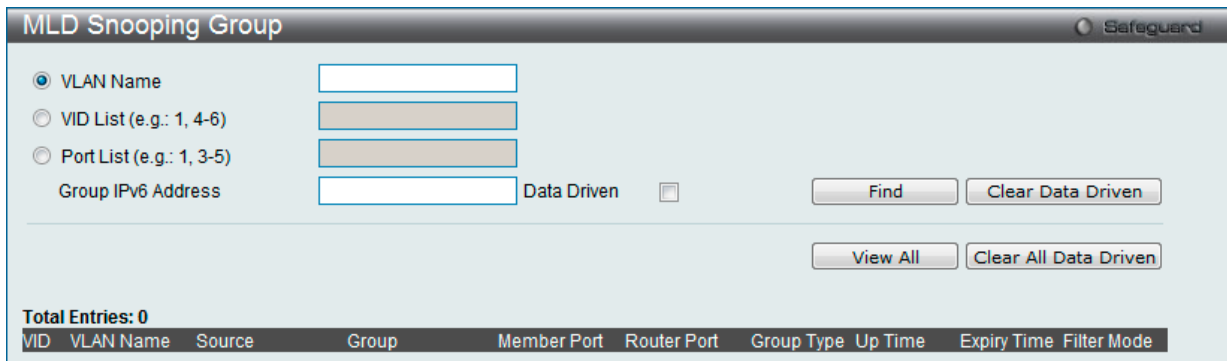


図 8-91 MLD Snooping Group 画面

MLD Snooping グループテーブルの参照

以下の項目を使用して、検索します。

| 項目 | 説明 |
|--------------------|---|
| VLAN Name | ラジオボタンをクリックして、マルチキャストグループの VLAN 名を入力します。 |
| VID List | ラジオボタンをクリックして、マルチキャストグループの VLAN リストを入力します。 |
| Port List | マルチキャストグループを検索するのに使用されるポート番号を指定します。 |
| Group IPv6 Address | 使用するグループ IPv6 アドレスを入力します。 |
| Data Driven | MLD Snooping グループの Data Driven Learning を有効または無効にします。初期値は「Enabled」です。 |

適切な情報を入力して、「Find」 ボタンをクリックします。検索されたエントリは「MLD Snooping Group Table」に表示されます。

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

エントリの削除

「Clear Data Driven」 ボタンをクリックして、Data Driven 情報をクリアします。

「Clear All Data Driven」 ボタンをクリックして、すべての Data Driven 情報をクリアします。

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

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

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

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

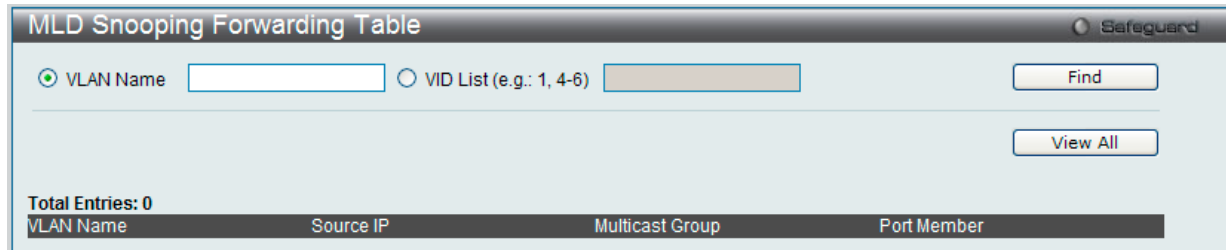


図 8-92 MLD Snooping Forwarding Table 画面

以下の項目を使用して検索します。

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

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

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

MLD Snooping Counter (MLD Snooping カウンタ)

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

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

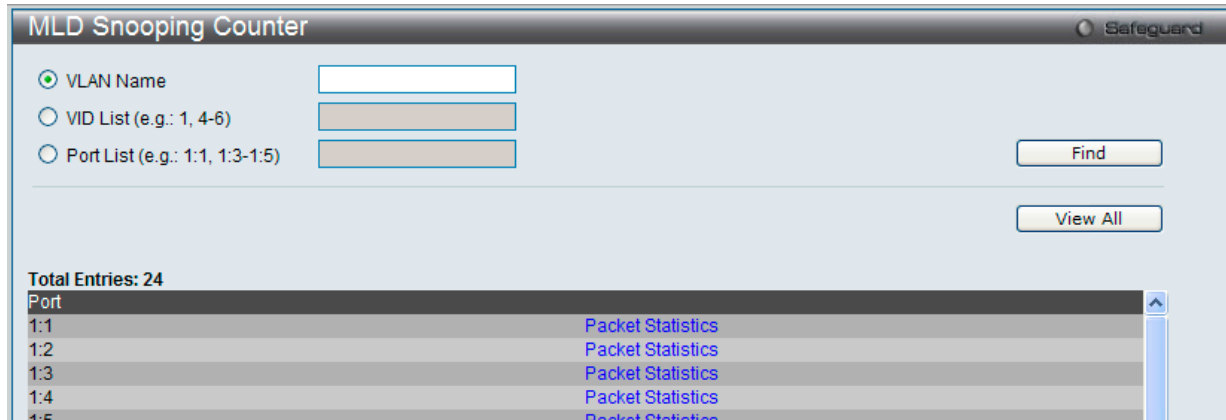


図 8-93 MLD Snooping Counter 画面

以下の項目が表示されます。

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

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

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

MLD Snooping カウンタテーブルの参照

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

Browse MLD Snooping Counter

MLD Snooping Counter Table

Port : 1:1
Group Number : 0

Clear Counter Refresh <<Back

Receive Statistics

| Query | Report & Done |
|----------------------------|---------------------------------|
| MLD v1 Query | MLD v1 Report |
| 0 | 0 |
| MLD v2 Query | MLD v2 Report |
| 0 | 0 |
| Total | MLD v1 Done |
| 0 | 0 |
| Dropped By Rate Limitation | Total |
| 0 | 0 |
| Dropped By Multicast VLAN | Dropped By Rate Limitation |
| 0 | 0 |
| | Dropped By Max Group Limitation |
| | 0 |
| | Dropped By Group Filter |
| | 0 |
| | Dropped By Multicast VLAN |
| | 0 |

Transmit Statistics

| Query | Report & Done |
|--------------|---------------|
| MLD v1 Query | MLD v1 Report |
| 0 | 0 |
| MLD v2 Query | MLD v2 Report |
| 0 | 0 |
| Total | MLD v1 Done |
| 0 | 0 |
| | Total |
| | 0 |

図 8-94 Browse MLD Snooping Counter 画面

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

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

「<<Back」ボタンをクリックして前のページに戻ります。

Multicast VLAN (マルチキャスト VLAN)

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

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

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

制限と条件：

1. マルチキャスト VLAN はエッジおよびエッジでないスイッチで実行することができます。
2. メンバポートとソースポートはマルチプル ISM VLAN で使用できます。しかし、特定のマルチキャスト VLAN では、メンバポートとソースポートを同じポートにはできませんのでご注意ください。
3. マルチキャスト VLAN はノーマルな 802.1Q VLAN とは排他的です。これは、802.1Q VLAN とマルチキャスト VLAN の VLAN ID(VID) と VLAN 名は同じにはできないことを意味します。VID または VLAN 名がどんな VLAN でも一度選択されると、別の VLAN に使用することはできません。
4. 設定された VLAN の通常の表示は設定されたマルチキャスト VLAN を表示しません。
5. 一度、マルチキャスト VLAN が有効になると、この VLAN に対応する IGMP Snooping 状態も有効になります。有効になったマルチキャスト VLAN の IGMP 機能を無効にすることはできません。
6. 1 つの IP マルチキャストアドレスを複数のマルチキャスト VLAN に追加することはできませんが、1 つのマルチキャスト VLAN に複数の範囲を追加することはできます。

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

プロファイルを追加し、指定したスイッチポートに受信するマルチキャストアドレスレポートを設定します。本機能は、受信するレポート数とスイッチに設定するマルチキャストグループ数を制限することができます。

特定のスイッチポートに到着するレポートを受信する (Permit) またはレポートを拒否する (Deny) IP アドレス /IP アドレス範囲を設定することができます。

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

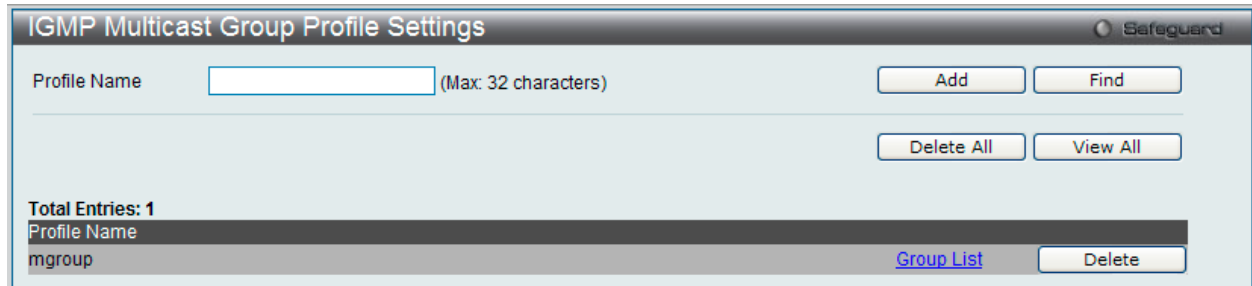


図 8-95 IGMP Multicast Group Profile Settings 画面

以下の項目を使用して設定します。

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

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

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

エントリの追加

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

エントリの削除

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

エントリの変更

1. 「Multicast Address List」欄の対応する「[Group List](#)」リンクをクリックし、以下の画面を表示します。



図 8-96 Multicast Group Profile Multicast Address Settings 画面

以下の項目が表示されます。

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

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

エントリの削除

該当するエントリの「Delete」 ボタンをクリックします。

「<<Back」 ボタンをクリックし、前のページに戻ります。

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

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

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

図 8-97 IGMP Snooping Multicast VLAN Settings 画面

以下の項目を使用して設定します。

| 項目 | 説明 |
|---------------------------------------|---|
| IGMP Multicast VLAN State | IGMP マルチキャスト VLAN 状態を有効または無効にします。 |
| IGMP Multicast VLAN Forward Unmatched | IGMP マルチキャスト VLAN フォワーディングの状態を有効または無効にします。 |
| IGMP Multicast VLAN Auto Assign VLAN | 右のマルチキャスト VLAN に対して IGMP 制御パケットの割り当てを有効または無効にします。「auto assign VLAN」を有効にすると、スイッチはグループをインGRESポートが所属するマルチキャスト VLAN プロファイルと照合します。一致があると、照合しているマルチキャスト VLAN をパケット VLAN として設定します。本機能が無効である場合、スイッチは VID チェックを行い、その後、グループが現在のプロファイルバインディングに一致しないと、このパケットを破棄します。 |
| VLAN Name | 使用する VLAN 名を入力します。 |
| VID (2-4094) | 使用する VID を指定します。 |
| Remap Priority | <ul style="list-style-type: none"> 0-7 - マルチキャスト VLAN に転送されるデータトラフィックに関連するリマップ優先度 (0-7)。 None - パケットの元の優先度が使用されます。(初期値) |
| Replace Priority | スイッチはパケットの優先度をリマップ優先度に基づいて変更します。リマップ優先度が設定される場合だけ、このフラグは有効になります。 |

「Apply」ボタンをクリックして各セクションで行った変更を適用します。

マルチキャスト VLAN の登録

- 「IGMP Multicast VLAN State」を「Enabled」(有効)を選択し、「Apply」ボタンをクリックします。
- 各項目を入力後、「Add」ボタンをクリックしてエントリを追加します。

エントリの削除

削除するエントリの「Delete」ボタンをクリックします。

マルチキャスト VLAN の変更

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

図 8-98 IGMP Snooping Multicast VLAN Settings 画面 - Edit

以下の項目を使用して設定します。

| 項目 | 説明 |
|-----------------------|--|
| VLAN Name | 定義済みのマルチキャスト VLAN 名を表示します。 |
| State | 選択した VLAN のマルチキャスト VLAN を「Enabled」(有効)または「Disabled」(無効)にします。 |
| Replace Source IP | IGMP Snooping 機能を使用すると、ホストが送信した IGMP レポートパケットは送信元ポートに転送されます。パケットの転送の前に、Join パケット内の送信元 IP アドレスはこの IP アドレスに変更されます。「Not Replaced」にチェックを入れると、送信元 IP アドレスはゼロ IP アドレスを使用します。 |
| Remap Priority | リマップの優先順位は、マルチキャスト VLAN に送信されるデータトラフィックに対応しています。 <ul style="list-style-type: none"> • 0-7 - マルチキャスト VLAN に転送されるデータトラフィックに関連するリマップ優先度 (0-7)。 • None - パケットの元の優先度が使用されます。(初期値) |
| Replace Priority | スイッチがリマップ優先順位に基づいてパケットの元の優先順位を変更します。本オプションは、リマップ優先順位を設定している場合にのみ有効です。 |
| Unit | 指定するユニットを選択します。 |
| Untagged Member Ports | マルチキャスト VLAN のタグなしメンバポートを指定します。 |
| Tagged Member Ports | マルチキャスト VLAN のタグ付きメンバポートを指定します。 |
| Untagged Source Ports | マルチキャストトラフィックがスイッチに入力しているタグなしソースポートを指定します。タグなしソースポートの PVID は、自動的にマルチキャスト VLAN に対して変更されます。ソースポートは 1 つのマルチキャスト VLAN に対してタグ付またはタグなしのいずれかとなり、つまり、両方のタイプは同じマルチキャスト VLAN のメンバとなることができません。 |
| Tagged Source Ports | マルチキャスト VLAN のタグ付きメンバとしてソースポートまたはソースポート範囲を指定します。 |

「Select All」ボタンをクリックするとすべてのポートを選択します。

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

「Apply」ボタンをクリックして行った変更を適用します。

「<<Back」ボタンをクリックし、変更を破棄して前のページに戻ります。

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

マルチキャスト VLAN グループリストの設定

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

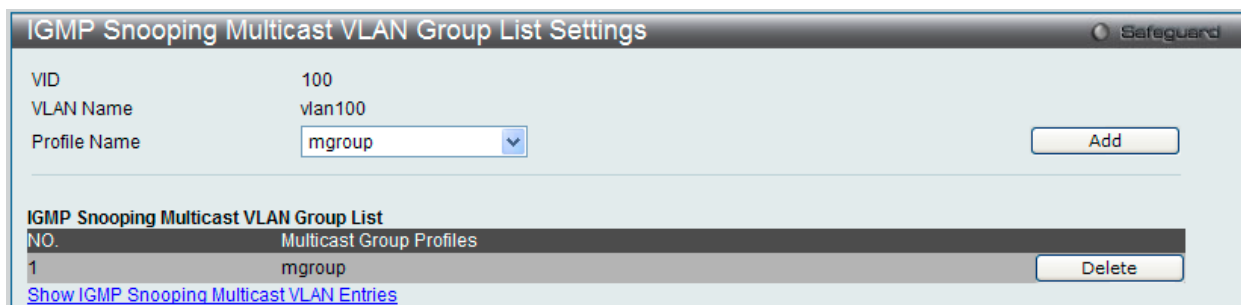


図 8-99 IGMP Snooping Multicast VLAN Group List Settings 画面

以下の項目を使用して設定します。

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

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

- プロファイル名を入力し、「Add」ボタンをクリックしてエントリを追加します。

マルチキャスト VLAN グループリストの削除

- マルチキャスト VLAN グループリストを削除する場合は、該当する行の「Delete」ボタンをクリックします。

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

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

プロファイルを追加し、指定したスイッチポートに受信するマルチキャストアドレスレポートを設定します。本機能は、受信するレポート数とスイッチに設定するマルチキャストグループ数を制限することができます。

特定のスイッチポートに到着するレポートを受信する (Permit) またはレポートを拒否する (Deny) IP アドレス /IP アドレス範囲を設定することができます。

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

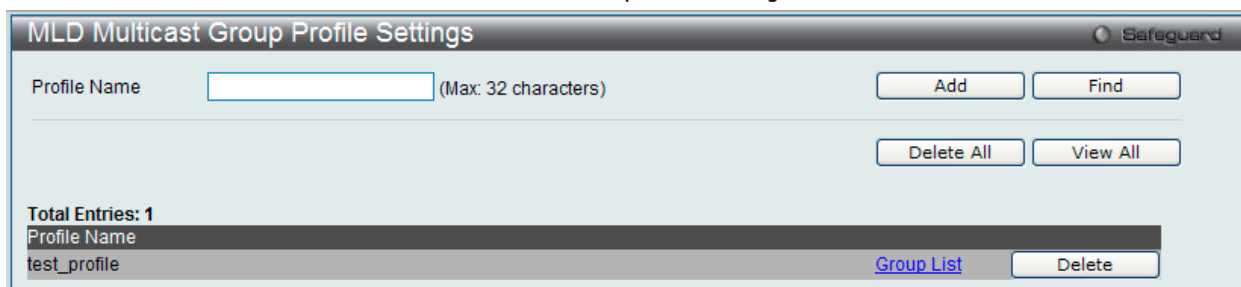


図 8-100 MLD Multicast Group Profile Settings 画面

以下の項目を使用して設定します。

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

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

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

エントリの追加

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

エントリの削除

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

エントリの変更

1. 「Multicast Address List」欄の対応する「[Group List](#)」リンクをクリックし、以下の画面を表示します。

図 8-101 Multicast Group Profile Multicast Address Settings 画面 - Edit

以下の項目が表示されます。

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

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

「<<Back」ボタンをクリックし、前のページに戻ります。

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

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

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

図 8-102 MLD Snooping Multicast VLAN Settings 画面

以下の項目を使用して設定します。

| 項目 | 説明 |
|--------------------------------------|--|
| MLD Multicast VLAN State | MLD マルチキャスト VLAN 状態を有効または無効にします。 |
| MLD Multicast VLAN Forward Unmatched | MLD multicast VLAN Forward Unmatched (MLD マルチキャスト VLAN フォワーディングの不一致) を有効または無効にします。 |
| MLD Multicast VLAN Auto Assign VLAN | 右のマルチキャスト VLAN に対して MLD 制御パケットの割り当てを有効または無効にします。「auto assign VLAN」を有効にすると、スイッチはグループをインGRESSポートが所属するすべてのマルチキャスト VLAN のプロファイルと照合します。一致があると、結果は「in profile」となり、照合しているマルチキャスト VLAN をパケット VLAN として設定します。本機能が無効である場合、スイッチは最初に VID をチェックします。グループがマルチキャスト VLAN に割り当てられる現在のプロフィールに一致しないと、スイッチはこのパケットを破棄します。 |
| VLAN Name | 使用する VLAN 名を入力します。 |
| VID | 使用する VID を指定します。 |
| Remap Priority | <ul style="list-style-type: none"> 0-7 - マルチキャスト VLAN に転送されるデータトラフィックに関連するリマップ優先度 (0-7)。 None - パケットの元の優先度が使用されます。(初期値) |
| Replace Priority | スイッチはパケットの優先度をリマップ優先度に基づいて変更します。リマップ優先度が設定される場合だけ、このフラグは有効になります。 |

「Apply」ボタンをクリックして各セクションで行った変更を適用します。

マルチキャスト VLAN の登録

1. 「MLD Multicast VLAN State」を「Enabled」(有効)を選択し、「Apply」ボタンをクリックします。
2. 各項目を入力後、「Add」ボタンをクリックしてエントリを追加します。

マルチキャスト VLAN の変更

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

図 8-103 MLD Snooping Multicast VLAN Settings 画面 - Edit

以下の項目を使用して設定します。

| 項目 | 説明 |
|-----------------------|--|
| VLAN Name | 定義済みのマルチキャスト VLAN 名を表示します。 |
| State | 選択した VLAN のマルチキャスト VLAN を「Enabled」(有効)または「Disabled」(無効)にします。 |
| Replace Source IP | MLD Snooping 機能を使用すると、ホストが送信した MLD レポートパケットは送信元ポートに転送されます。パケットの転送の前に、Join パケット内の送信元 IP アドレスはこの IP アドレスに変更されます。「Not Replaced」にチェックを入れると、送信元 IP アドレスはゼロ IP アドレスを使用します。 |
| Remap Priority | リマップの優先順位は、マルチキャスト VLAN に送信されるデータトラフィックに対応しています。 <ul style="list-style-type: none"> • 0-7 - マルチキャスト VLAN に転送されるデータトラフィックに関連するリマップ優先度 (0-7)。 • None - 「none」が指定されると、パケットの元の優先度が使用されます。(初期値) |
| Replace Priority | 選択すると、スイッチがリマップ優先順位に基づいてパケットの元の優先順位を変更します。本オプションは、リマップ優先順位を設定している場合のみ有効です。 |
| Unit | 指定するユニットを選択します。 |
| Untagged Member Ports | マルチキャスト VLAN のタグなしメンバポートを指定します。 |
| Tagged Member Ports | マルチキャスト VLAN のタグ付きメンバポートを指定します。 |
| Untagged Source Ports | マルチキャストトラフィックがスイッチに入力しているタグなしソースポートを指定します。タグなしソースポートの PVID は、自動的にマルチキャスト VLAN に対して変更されます。ソースポートは 1 つのマルチキャスト VLAN に対してタグ付けまたはタグなしのいずれかとなり、つまり、両方のタイプは同じマルチキャスト VLAN のメンバとなることができません。 |
| Tagged Source Ports | マルチキャスト VLAN のタグ付きメンバとしてソースポートまたはソースポート範囲を指定します。 |

「Select All」ボタンをクリックするとすべてのポートを選択します。

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

「<<Back」ボタンをクリックし、変更を破棄して前のページに戻ります。

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

マルチキャスト VLAN グループリストの設定

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

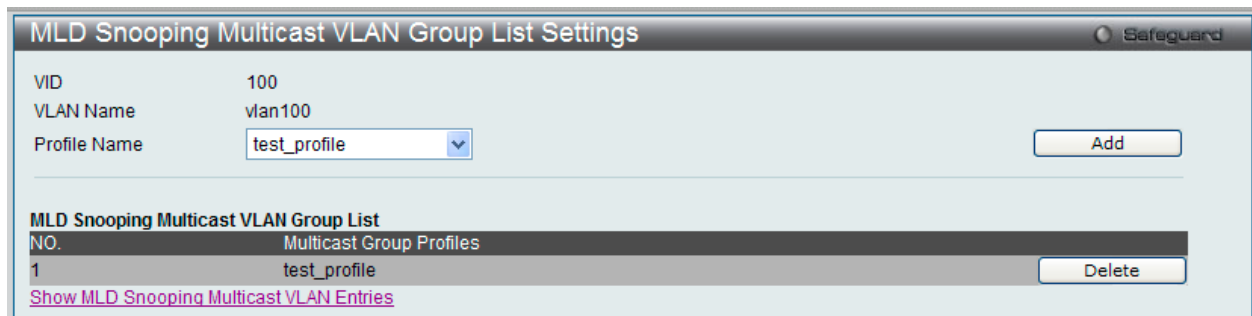


図 8-104 MLD Snooping Multicast VLAN Group List Settings 画面

以下の項目を使用して設定します。

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

- プロファイル名を入力し、「Add」ボタンをクリックしてエントリを追加します。

マルチキャスト VLAN グループリストの削除

- マルチキャスト VLAN グループリストを削除する場合は、該当する行の「Delete」ボタンをクリックします。

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

IP Multicast VLAN Replication (IP マルチキャスト VLAN レプリケーション)

一般に、スイッチがどのマルチキャストルーティングプロトコルもサポートしない場合、VLAN を経由したマルチキャストデータの転送はできません。IP マルチキャスト VLAN レプリケーションは、マルチキャストプロトコルをサポートせずに実行できます。希望のソーストラフィックと対応する外向きメンバを設定する必要があります。

IP Multicast VLAN Replication Global Settings (IP マルチキャスト VLAN レプリケーションのグローバル設定)

IP マルチキャスト VLAN のレプリケーションパラメータを設定します。

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

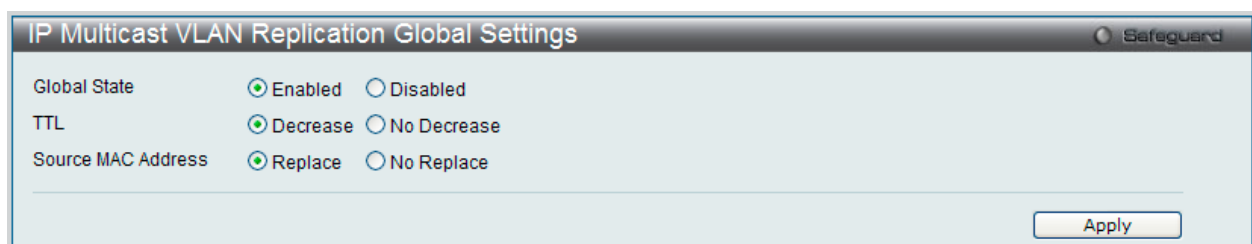


図 8-105 IP Multicast VLAN Replication Global Settings 画面

以下の項目を使用して設定します。

| 項目 | 説明 |
|--------------------|--|
| Global State | グローバル状態を有効または無効にします。 |
| TTL | パケット内の TTL (Time to live) 値に対して「Decrease」(減らす) または「No decrease」(減らさない) を選択します。 |
| Source MAC Address | パケットの送信元 MAC アドレスの交換の有無を選択します。 |

「Apply」ボタンをクリックして行った変更を適用します。

IP Multicast VLAN Replication Settings (IP マルチキャスト VLAN レプリケーション設定)

IP マルチキャスト VLAN のレプリケーションテーブルの追加または参照を行います。

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

図 8-106 IP Multicast VLAN Replication Settings 画面

以下の項目を使用して設定します。

| 項目 | 説明 |
|------------|-----------------------------|
| Entry Name | マルチキャストレプリケーションエントリ名を入力します。 |

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

「Find by Hardware」をクリックしてハードウェアに基づいてエントリを検索します。

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

「Source」の下にある「Edit」ボタンをクリックして、指定エントリを編集します。

「Destination」の下にある「Edit」ボタンをクリックして、指定エントリを編集します。

「Delete」ボタンをクリックして、指定エントリを削除します。

送信元エントリの変更

「Source」の下にある「Edit」ボタンをクリックして、以下の画面を表示します。

図 8-107 IP Multicast VLAN Replication Source Settings 画面

以下の項目を使用して設定します。

| 項目 | 説明 |
|------------------------|---|
| Entry Name | IP マルチキャスト VLAN レプリケーションソースエントリ名が表示されます。 |
| VID / VLAN Name | 「VLAN Name」、「VID」または「Group」を選択して、値を入力します。 |
| Action | 適用する操作を選択します。 |
| Multicast Address List | マルチキャストアドレスリストを入力します。 |
| Source Address | 送信元アドレスを入力します。 |

「Apply」ボタンをクリックして行った変更を適用します。

「<<Back」ボタンをクリックし、変更を破棄して前のページに戻ります。

送信先エントリの変更

「Destination」の下にある「Edit」ボタンをクリックして、以下の画面を表示します。

図 8-108 IP Multicast VLAN Replication Destination Settings 画面

以下の項目を使用して設定します。

| 項目 | 説明 |
|-----------------|---|
| Entry Name | IP マルチキャスト VLAN レプリケーション宛先エントリ名が表示されます。 |
| VID / VLAN Name | 「VLAN Name」、「VID」または「Group」を選択して、値を入力します。 |
| Action | 適用する操作を選択します。 |
| Port List | ポートリストを指定します。 |

「Apply」ボタンをクリックして行った変更を適用します。

「<<Back」ボタンをクリックし、変更を破棄して前のページに戻ります。

Multicast Filtering (マルチキャストフィルタリング)

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

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

指定したスイッチポートにマルチキャストアドレスレポートを受信するプロファイルを追加します。本機能は、受信するレポート数とスイッチに設定するマルチキャストグループ数を制限することができます。特定のスイッチポートに到着するレポートを受信する (Permit) またはレポートを拒否する (Deny) IPv4 アドレス / IPv4 アドレス範囲を設定することができます。

L2 Features > Multicast Filtering > IPv4 Multicast Filtering > IPv4 Multicast Profile Settings の順にメニューをクリックし、以下の画面を表示します。

図 8-109 IPv4 Multicast Profile Settings 画面

以下の項目を使用して設定します。

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

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

エントリの登録

各項目を入力後、「Add」ボタンをクリックしてエントリを追加します。

エントリの編集

1. 「Edit」 ボタンをクリックして、以下の画面を表示します。

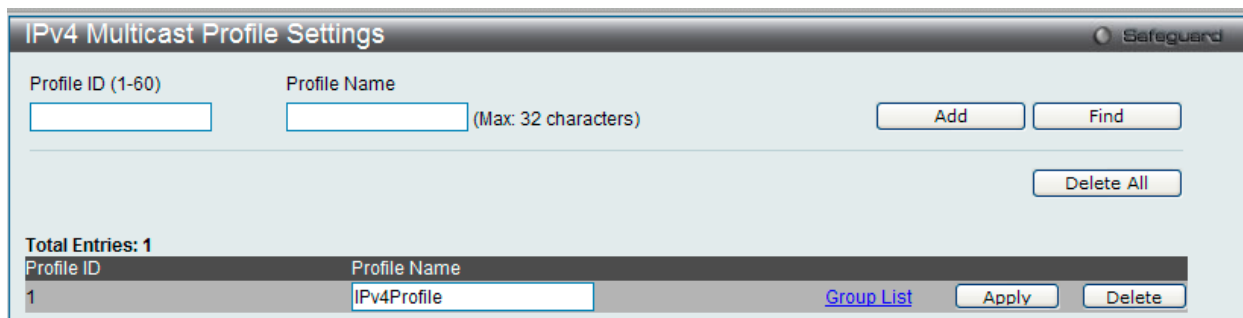


図 8-110 IPv4 Multicast Profile Settings 画面 - Edit

2. 指定エントリ名を編集し、「Apply」 ボタンをクリックします。

エントリの削除

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

マルチキャストグループリストの設定

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

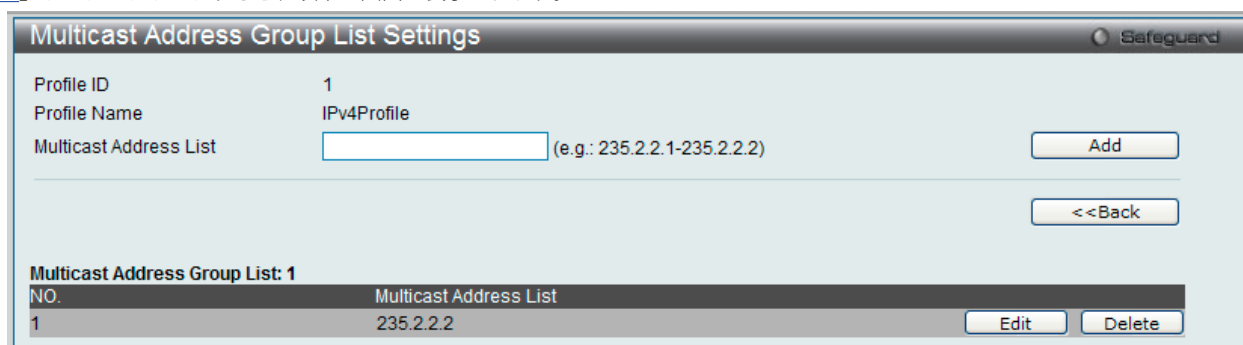


図 8-111 Multicast Address Group List Settings 画面

以下の項目を使用して設定します。

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

エントリの登録

各項目を入力後、「Add」 ボタンをクリックしてエントリを追加します。「<<Back」 ボタンをクリックし、変更を破棄して前のページに戻ります。

エントリの編集

1. 「Edit」 ボタンをクリックして、以下の画面を表示します。

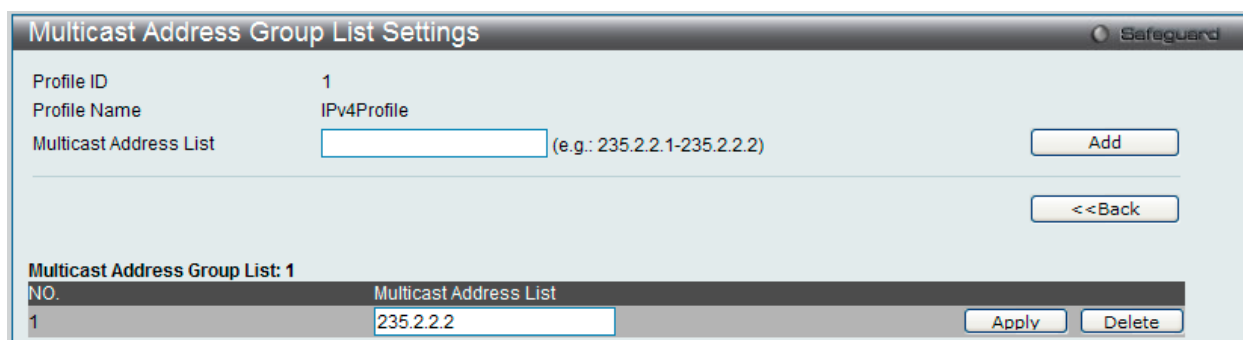


図 8-112 IPv4 Multicast Profile Settings 画面 - Edit

2. 指定エントリを編集して「Apply」 ボタンをクリックします。

エントリの削除

「Delete」 ボタンをクリックして、指定エントリを削除します。

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

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

L2 Features > Multicast Filtering > IPv4 Multicast Filtering > IPv4 Limited Multicast Range Settings の順にメニューをクリックし、以下の画面を表示します。

The screenshot shows the 'IPv4 Limited Multicast Range Settings' configuration window. It features three rows of input fields for 'Ports' (with examples like 1:1, 1:4-1:5), 'Access' (set to 'Permit'), and 'Profile ID' (set to '1'). Below these fields are 'Add', 'Delete', and 'Find' buttons. A table at the bottom displays 'Total Entries: 3' with columns for VID, Access State, and Profile ID. The table contains three rows, all with 'Permit' as the Access State. A pagination control at the bottom right shows '1/1' and a 'Go' button.

図 8-113 IPv4 Limited Multicast Range Settings 画面

制限する IP マルチキャストの範囲に含まれるスイッチポートを設定します。

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

| 項目 | 説明 |
|----------------|---|
| Ports/VID List | マルチキャストアドレスフィルタ機能を追加または削除するポート範囲またはVLAN IDを指定します。 |
| Access | 以下のオプションの一つを選択します。 <ul style="list-style-type: none"> Permit - 指定したポートまたはVIDに一致するパケットを許可することを指定します。 Deny - 指定したポートまたはVIDに一致するパケットを破棄することを指定します。 |

「Apply」ボタンをクリックし、設定を適用します。

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

| 項目 | 説明 |
|---------------------------|---|
| Ports | マルチキャストアドレスフィルタ機能を追加または削除するポート範囲を指定します。 |
| Profile ID / Profile Name | プルダウンメニューを使用して、指定したポート範囲に(から)追加または削除するプロファイルIDまたはプロファイル名を選択します。 |
| Access | プルダウンメニューを使用して、以下のオプションの一つを選択します <ul style="list-style-type: none"> Permit - プロファイル内に指定されているアドレスに一致するパケットを許可します。 Deny - プロファイル内に指定されているアドレスに一致するパケットを破棄します。 |

新しいマルチキャストアドレス範囲の追加

適切な情報を入力し、「Add」ボタンをクリックします。

マルチキャストアドレス範囲の削除

情報を入力し、「Delete」ボタンをクリックします。

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

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

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

学習されるマルチキャストグループの最大数をスイッチのポートに設定します。

L2 Features > Multicast Filtering > IPv4 Multicast Filtering > IPv4 Max Multicast Group Settings の順にメニューをクリックし、以下の画面を表示します。

図 8-114 IPv4 Max Multicast Group Settings 画面

以下の項目を使用して、設定します。

| 項目 | 説明 |
|-------------------|--|
| Ports / VID List | 本設定に使用される適切なポートまたは VLAN ID を選択します。 |
| Max Group (1-960) | マルチキャストグループの最大数を指定します。範囲は 1-960 です。「Infinite」ボックスをチェックしない場合、ここに最大グループ数を入力します。 |
| Infinite | 「Infinite」(制限なし) を有効または無効にします。 |
| Action | ルールに適切な操作を選択します。 <ul style="list-style-type: none"> Drop - 破棄の動作を行います。 Replace - 交換の動作を行います。 |

エントリの追加

適切な情報を入力し「Apply」ボタンをクリックします。

エントリの参照

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

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

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

指定したスイッチポートにマルチキャストアドレスレポートを受信するプロファイルを追加します。本機能は、受信するレポート数とスイッチに設定するマルチキャストグループ数を制限することができます。特定のスイッチポートに到着するレポートを受信する (Permit) またはレポートを拒否する (Deny) IPv6 アドレス / IPv6 アドレス範囲を設定することができます。

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

IPv6 マルチキャストプロファイルの追加、削除、または設定を行います。

L2 Features > Multicast Filtering > IPv6 Multicast Filtering > IPv6 Multicast Filtering Profile Settings の順にメニューをクリックし、以下の画面を表示します。

図 8-115 IPv6 Multicast Profile Settings 画面

以下の項目を使用して設定します。

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

エントリの登録

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

エントリの参照

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

エントリの編集

1. 「Edit」ボタンをクリックして、以下の画面を表示します。

図 8-116 IPv6 Multicast Profile Settings 画面 - Edit

2. 指定エントリを編集して「Apply」ボタンをクリックします。

エントリの削除

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

マルチキャストグループリストの設定

「Group List」リンクをクリックすると、以下の画面が表示されます。

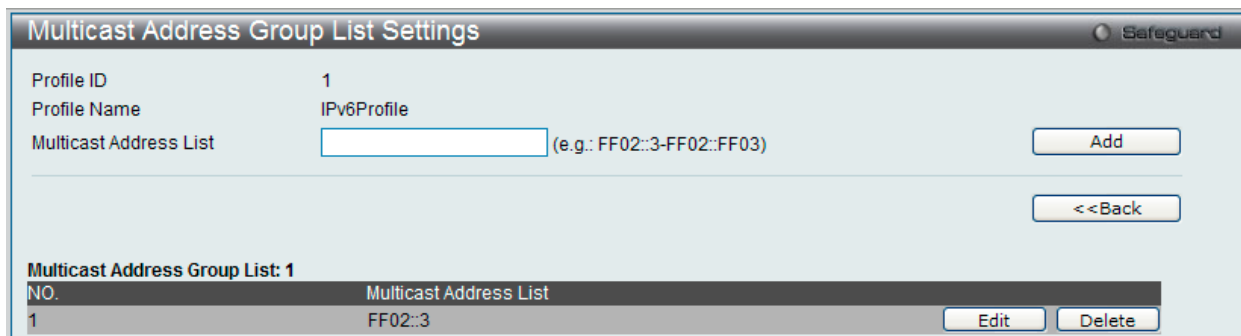


図 8-117 Multicast Address Group List Settings 画面

以下の項目を使用して設定します。

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

エントリの登録

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

「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

エントリの編集

1. 「Edit」ボタンをクリックして、以下の画面を表示します。

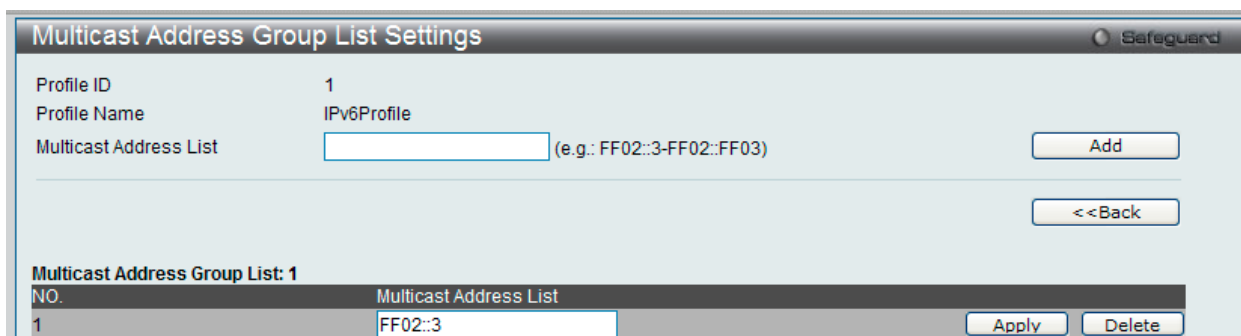


図 8-118 Multicast Address Group List Settings 画面 - Edit

2. 指定エントリを編集して「Apply」ボタンをクリックします。

エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。

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

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

L2 Features > Multicast Filtering > IPv6 Multicast Filtering > IPv6 Limited Multicast Range Settings の順にメニューをクリックし、以下の画面を表示します。

| VID | Access State | Profile ID |
|-----|--------------|------------|
| 1 | Deny | |
| 10 | Deny | |
| 20 | Deny | |
| 30 | Deny | |
| 40 | Deny | |
| 50 | Deny | |
| 100 | Deny | |

図 8-119 IPv6 Limited Multicast Range Settings 画面

制限する IP マルチキャストの範囲に含まれるスイッチポートを設定します。

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

| 項目 | 説明 |
|---------------|--|
| Ports/MD List | マルチキャストアドレスフィルタ機能を追加または削除するポート範囲または VID を指定します。 |
| Access | プルダウンメニューを使用して、以下のオプションの一つを選択します。 <ul style="list-style-type: none"> Permit - 指定したポートまたは VID に一致するパケットを許可することを指定します。 Deny - 指定したポートまたは VID に一致するパケットを破棄することを指定します。 |

「Apply」 ボタンをクリックし、設定を適用します。

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

| 項目 | 説明 |
|------------------|---|
| Ports / VID List | マルチキャストアドレスフィルタ機能を追加または削除するポート範囲または VID を指定します。 |
| Profile ID | プルダウンメニューを使用して、指定したポート範囲に (から) 追加または削除するプロファイル ID を選択します。 |
| Access | プルダウンメニューを使用して、以下のオプションの一つを選択します <ul style="list-style-type: none"> Permit - プロファイル内に指定されているアドレスに一致するパケットを許可します。 Deny - プロファイル内に指定されているアドレスに一致するパケットを破棄します。 |

新しいマルチキャストアドレス範囲の追加

適切な情報を入力し、「Add」 ボタンをクリックします。

マルチキャストアドレス範囲の削除

情報を入力し、「Delete」 ボタンをクリックします。

エントリの検索

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

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

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

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

L2 Features > Multicast Filtering > IPv6 Multicast Filtering > IPv6 Max Multicast Group Settings の順にメニューをクリックし、以下の画面を表示します。

図 8-120 IPv6 Max Multicast Group Settings 画面

以下の項目を使用して設定します。

| 項目 | 説明 |
|-------------------|---|
| Ports / VID List | 本設定に使用される適切なポート範囲または VID を選択します。 |
| Max Group (1-480) | マルチキャストグループの最大数を指定します。範囲は 1-480 です。「Infinite」ボックスをチェックしない場合、ここに最大グループ数を入力します。 |
| Infinite | 「Infinite」(制限なし) を有効または無効にします。 |
| Action | ルールに適切な操作を選択します。「Drop」を選択すると破棄の動作を行い、「Replace」を選択すると交換の動作を行います。 |

エントリの登録

適切な情報を入力し「Apply」ボタンをクリックします。

エントリの検索

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

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

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

マルチキャストフィルタリングモードを設定します。

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

| VLAN ID | VLAN Name | Multicast Filter Mode |
|---------|--------------|-----------------------------|
| 1 | default | Forward Unregistered Groups |
| 10 | Management | Forward Unregistered Groups |
| 20 | test_private | Forward Unregistered Groups |
| 30 | super_vlan | Forward Unregistered Groups |
| 40 | sub_vlan | Forward Unregistered Groups |
| 50 | VLAN100 | Forward Unregistered Groups |
| 100 | vlan100 | Forward Unregistered Groups |

図 8-121 Multicast Filtering Mode 画面

以下の項目を使用して設定します。

| 項目 | 説明 |
|--------------------------|--|
| VLAN Name/VID List | フィルタリングが適用される VLAN を指定します。「All」をチェックするとすべての VLAN にフィルタリングが適用されます。 |
| Multicast Filtering Mode | 指定した VLAN ポートに転送されるマルチキャストパケットを受信した時の動作を指定します。 <ul style="list-style-type: none"> Forward All Groups - 指定ポート VLAN にすべてのマルチキャストパケットを転送します。 Forward Unregistered Groups - 宛先が未登録のマルチキャストグループであるマルチキャストパケットは、上記指定ポート範囲に転送されます。 Filter Unregistered Groups - 宛先が登録済みのマルチキャストグループであるマルチキャストパケットは、上記指定ポート範囲に転送されます。 |

「Apply」ボタンをクリックして行った変更を適用します。

エントリの検索

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

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

ERPS Settings (イーサネットリングプロテクション設定)

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

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

G.8032 の用語と概念

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

スイッチの ERPS 機能を有効にします。



ERPS を有効にする前に、STP と LBD をリングポートで無効にする必要があります。R-APS VLAN の作成前およびリングポート、RPL ポート、RPL オーナの設定前に ERPS を有効にすることはできません。

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

図 8-122 ERPS Settings 画面

設定対象となる項目は以下の通りです。

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

エントリの追加

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

詳細情報の参照

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

| ERPS Settings | | |
|-------------------------|-----------------|-----|
| ERPS Information | | |
| R-APS VLAN | 1 | |
| Ring Status | Disabled | |
| Admin West Port | Virtual Channel | |
| Operational West Port | | |
| Admin East Port | Virtual Channel | |
| Operational East Port | | |
| Admin RPL Port | None | |
| Operational RPL Port | None | |
| Admin RPL Owner | Disabled | |
| Operational RPL Owner | Disabled | |
| Protected VLAN(s) | | |
| Ring MEL (0-7) | 1 | |
| Holdoff Time (0-10000) | 0 | ms |
| Guard Time (10-2000) | 500 | ms |
| WTR Time (5-12) | 5 | min |
| Revertive | Enabled | |
| Current Ring State | - | |

Edit <<Back

図 8-123 ERPS Settings 画面 - ERPS Information

エントリの編集

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

| ERPS Settings | | |
|-------------------------------|--|---|
| ERPS Information | | |
| R-APS VLAN | 10 | |
| Ring Status | Disabled <input type="checkbox"/> | |
| Admin West Port | Unit 1 <input type="checkbox"/> Virtual Channel <input type="checkbox"/> | |
| Operational West Port | | |
| Admin East Port | Unit 1 <input type="checkbox"/> Virtual Channel <input type="checkbox"/> | |
| Operational East Port | | |
| Admin RPL Port | None <input type="checkbox"/> | |
| Operational RPL Port | None | |
| Admin RPL Owner | Disabled <input type="checkbox"/> | |
| Operational RPL Owner | Disabled | |
| Protected VLAN(s) (e.g.: 4-6) | <input type="text"/> <input type="checkbox"/> | <input checked="" type="radio"/> Add <input type="radio"/> Delete |
| Ring MEL (0-7) | 1 <input type="checkbox"/> | |
| Holdoff Time (0-10000) | 0 <input type="checkbox"/> | ms |
| Guard Time (10-2000) | 500 <input type="checkbox"/> | ms |
| WTR Time (5-12) | 5 <input type="checkbox"/> | min |
| Revertive | Enabled <input type="checkbox"/> | |
| Current Ring State | - | |

Apply <<Back

図 8-124 ERPS Settings 画面 - Edit

L2 Features (L2機能の設定)

設定対象となる項目は以下の通りです。

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

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

「<<Back」をボタンをクリックして前のページに戻ります。

サブリング情報の参照

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

図 8-125 ERPS Sub-Ring Settings 画面

- 以下の項目を使用して設定します。

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

- 「Apply」ボタンをクリックして行った変更を適用します。

「<<Back」をボタンをクリックして前のページに戻ります。

エントリの削除

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

「Clear All」ボタンをクリックすると、本画面のすべての設定がクリアされます。

LLDP (LLDP 設定)

LLDP (Link Layer Discovery Protocol) は、IEEE 802 ネットワークに接続しているステーションから同じ IEEE 802 ネットワークに接続している他のステーションに通知を出します。本システムが提供する主な機能は、ステーションまたは本機能の管理を提供するエンティティの管理アドレスと、管理エンティティが要求する IEEE 802 ネットワークに接続するステーションの接続点の識別子を組み合わせることです。

本プロトコルによって送信される情報は、受信先によって標準の管理情報ベース (MIB) に格納されるため、SNMP (Simple Network Management Protocol) などの管理プロトコルを使用したネットワーク管理システム (NMS) からその情報にアクセスできるようになります。

LLDP (LLDP 設定)

LLDP Global Settings (LLDP グローバル設定)

LLDP グローバルパラメータを設定します。

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

| LLDP Global Settings | |
|-------------------------------------|--|
| LLDP State | <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled <input type="button" value="Apply"/> |
| LLDP Forward Message | <input type="radio"/> Enabled <input checked="" type="radio"/> Disabled <input type="button" value="Apply"/> |
| Message TX Interval (5-32768) | <input type="text" value="30"/> sec |
| Message TX Hold Multiplier (2-10) | <input type="text" value="4"/> |
| LLDP Reinit Delay (1-10) | <input type="text" value="2"/> sec |
| LLDP TX Delay (1-8192) | <input type="text" value="2"/> sec |
| LLDP Notification Interval (5-3600) | <input type="text" value="5"/> sec <input type="button" value="Apply"/> |
| LLDP System Information | |
| Chassis ID Subtype | MAC Address |
| Chassis ID | 14-D6-4D-B0-26-00 |
| System Name | |
| System Description | Gigabit Ethernet Switch |
| System Capabilities | Repeater, Bridge |

図 8-126 LLDP Global Settings 画面

以下の項目を設定できます。

| 項目 | 説明 |
|-------------------------------------|---|
| LLDP State | スイッチにおける LLDP 機能を「Enabled」(有効) または「Disabled」(無効) にします。 |
| LLDP Forward Message | 同じ IEEE 802 ネットワークに割り当てられた他のステーションに通知するために LLDP 機能のメッセージ転送を「Enabled」(有効) または「Disabled」(無効) にします。 <ul style="list-style-type: none"> Enabled - 同一のポート VLAN を持つすべてのポートに LLDP パケットをフラッドして、同じ IEEE 802 LAN に接続している他のコンピュータに通知します。 Disabled - 本機能が各ポートにおいて LLDP パケットのメッセージ転送を制御します。 |
| Message TX Interval (5-32768) | アクティブなポートが通知を再送する方法を制御します。パケット伝送間隔を変更するために、5-32768 (秒) の範囲で値を入力します。 |
| Message TX Hold Multiplier (2-10) | LLDP スイッチに使用される乗数を変更することで LLDP Neighbor に LLDP 通知を作成して送信する有効期間 (TTL : Time-to-Live) を計算します。指定通知の TTL (time-to-Live) の期限が来ると、通知データは Neighbor スイッチの MIB から削除されます。 |
| LLDP Reinit Delay (1-10) | LLDP ポートが LLDP 無効にするコマンドを受け取った後、再初期化を行う前に待機する時間です。1-10 (秒) から値を入力します。 |
| LLDP Tx Delay (1-8192) | LLDP MIB コンテンツの変更のために、LLDP ポートが連続した LLDP 通知の送信を遅らせる最短時間 (遅延間隔) を変更します。LLDP TX Delay を変更するために、1-8192 (秒) から値を入力します。 |
| LLDP Notification Interval (5-3600) | LLDP データ変更が LLDP Neighbor からポートに受信した通知の中に検出される場合、定義済みの SNMP トラップレシーバに変更通知を送信する時に使用されます。5-3600 (秒) から値を入力します。 |

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

LLDP Port Settings (LLDP ポート設定)

LLDP ポートパラメータを設定します。

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

| Port ID | Notification | Admin Status | IPv4 (IPv6) Address |
|---------|--------------|--------------|---------------------|
| 1 | Disabled | TX and RX | |
| 2 | Disabled | TX and RX | |
| 3 | Disabled | TX and RX | |

図 8-127 LLDP Port Settings 画面

以下の項目を設定できます。

| 項目 | 説明 |
|-------------------|---|
| Unit | 設定するユニットを選択します。 |
| From Port/To Port | プルダウンメニューを使用して設定するポート範囲を指定します。 |
| Notification | プルダウンメニューを使用して LLDP 通知を「Enabled」(有効)または「Disabled」(無効)にします。本機能は SNMP トラップを制御し、無効にするとトラップを実行しません。 |
| Admin Status | 本機能はローカル LLDP エージェントを制御し、ポートで LLDP フレームの送受信を行うことができるようになります。通知のステータスを選択します。 <ul style="list-style-type: none"> TX - ローカル LLDP エージェントは LLDP フレームを送信します。 RX - ローカル LLDP エージェントは LLDP フレームを受信します。 TX and RX - ローカル LLDP エージェントは LLDP フレームの送受信両方を行います。(初期値) Disabled - ローカル LLDP エージェントは、LLDP フレームの送受信を行いません。 |
| Subtype | 送信される IP アドレス情報 (IPv4 / IPv6) のタイプを選択します。 |
| Action | ポートベースの管理アドレス機能を「Enabled」(有効)または「Disabled」(無効)にします。 |
| Address | 通知するエンティティの管理アドレスを入力します。 |

「Apply」ボタンをクリックし、変更を有効にします。

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

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

LLDP 管理アドレスを参照します。

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

| Subtype | Address | IF Type | OID | Advertising Ports |
|---------|---------------|---------|-------------------------|-------------------|
| IPv4 | 10.10.10.1 | Ifindex | 1.3.6.1.4.1.171.10.1... | |
| IPv4 | 192.168.1.100 | Ifindex | 1.3.6.1.4.1.171.10.1... | |
| IPv6 | 3710::1 | Ifindex | 1.3.6.1.4.1.171.10.1... | |

図 8-128 LLDP Management Address List 画面

以下の項目を設定できます。

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

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

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

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

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

本スイッチにおけるベーシック TLV 設定を有効にします。

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

| Port | Port Description | System Name | System Description | System Capabilities |
|------|------------------|-------------|--------------------|---------------------|
| 1 | Disabled | Disabled | Disabled | Disabled |
| 2 | Disabled | Disabled | Disabled | Disabled |
| 3 | Disabled | Disabled | Disabled | Disabled |
| 4 | Disabled | Disabled | Disabled | Disabled |

図 8-129 LLDP Basic TLVs Settings 画面

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

以下の項目を設定できます。

| 項目 | 説明 |
|---------------------|--|
| Unit | 設定するユニットを選択します。 |
| From Port/To Port | 設定するポート範囲を指定します。 |
| Port Description | ポート説明を「Enabled」(有効) / 「Disabled」(無効) にします。 |
| System Name | システム名を「Enabled」(有効) / 「Disabled」(無効) にします。 |
| System Description | システム説明を「Enabled」(有効) / 「Disabled」(無効) にします。 |
| System Capabilities | システムケーパビリティを「Enabled」(有効) / 「Disabled」(無効) にします。 |

「Apply」ボタンをクリックし、変更を有効にします。

LLDP Dot1 TLVs Settings (LLDP Dot1 TLV 設定)

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

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

| Port | PVID State | Port and Protocol VID State | VID | VLAN Name State | VID | Protocol Identity State | Protocol Identity |
|------|------------|-----------------------------|-----|-----------------|-----|-------------------------|-------------------|
| 1 | Disabled | Disabled | | Disabled | | Disabled | |
| 2 | Disabled | Disabled | | Disabled | | Disabled | |
| 3 | Disabled | Disabled | | Disabled | | Disabled | |
| 4 | Disabled | Disabled | | Disabled | | Disabled | |
| 5 | Disabled | Disabled | | Disabled | | Disabled | |
| 6 | Disabled | Disabled | | Disabled | | Disabled | |
| 7 | Disabled | Disabled | | Disabled | | Disabled | |

図 8-130 LLDP Dot1 TLVs Settings 画面

以下の項目が使用できます。

| 項目 | 説明 |
|----------------------------|---|
| Unit | 設定するユニットを選択します。 |
| From Port/To Port | 設定するポート範囲を指定します。 |
| Dot1 TLV PVID | Dot1 TLV PVID の通知を「Enabled」(有効) / 「Disabled」(無効) にします。 |
| Dot1 TLV Protocol VLAN | プロトコル VLAN ID の通知を「Enabled」(有効) / 「Disabled」(無効) にします。本オプションの有効後、次のプルダウンメニューで「VLAN Name」、「VID List」または「All」を選択することができます。これを選択後に、対象となるプロトコル VLAN を右の欄で指定します。 <ul style="list-style-type: none"> VLAN Name - VLAN 名を指定します。 VLAN ID - VLAN ID を指定します。 All - すべてを対象とします。 |
| Dot1 TLV VLAN | Dot1 TLV VLAN の有効/無効、および設定を行います。本オプションの有効後、次のプルダウンメニューで「VLAN Name」、「VID List」または「All」を選択することができます。これを選択後に、対象となるプロトコル VLAN を右の欄で指定します。 <ul style="list-style-type: none"> VLAN Name - VLAN 名を指定します。 VLAN ID - VLAN ID を指定します。 All - すべてを対象とします。 |
| Dot1 TLV Protocol Identity | プロトコル識別子の通知を「Enabled」(有効) / 「Disabled」(無効) にします。次に対象とするプロトコルを「EAPOL」、「LACP」、「GVRP」、「STP」または「All」から選択します。 |

「Apply」ボタンをクリックし、変更を有効にします。

LLDP Dot3 TLVs Settings (LLDP Dot3 TLV 設定)

個別のポートやポートグループが送信する LLDP 通知から IEEE 802.3 規定のポート VLAN ID TLV データタイプを除外するように設定します。

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

| Port | MAC / PHY Configuration Status | Link Aggregation | Maximum Frame Size | Power Via MDI |
|------|--------------------------------|------------------|--------------------|---------------|
| 1 | Disabled | Disabled | Disabled | Disabled |
| 2 | Disabled | Disabled | Disabled | Disabled |
| 3 | Disabled | Disabled | Disabled | Disabled |
| 4 | Disabled | Disabled | Disabled | Disabled |
| 5 | Disabled | Disabled | Disabled | Disabled |
| 6 | Disabled | Disabled | Disabled | Disabled |
| 7 | Disabled | Disabled | Disabled | Disabled |

図 8-131 LLDP Dot3 TLVs Settings 画面

以下の項目を設定できます。

| 項目 | 説明 |
|------------------------------|---|
| Unit | 設定するユニットを選択します。 |
| From Port/To Port | 設定するポート範囲を指定します。 |
| MAC/PHY Configuration Status | スイッチの MAC または PHY 状態の通知を「Enabled」(有効) / 「Disabled」(無効) にします。本 TLV のオプションデータタイプは、LLDP エージェントが「MAC/PHY configuration/status TLV」を送信する必要があることを示します。このタイプは、IEEE 802.3 リンクの 2 つの終端が異なる速度設定で、何らかの限定的な接続性を確立することが可能であることを示しています。情報には、ポートがオートネゴシエーション機能をサポートしているかどうか、機能が有効であるかどうか、自動通知機能、および操作可能な MAU タイプが含まれます。初期値は無効です。 |
| Link Aggregation | スイッチのリンクアグリゲーション状態の通知を「Enabled」(有効) / 「Disabled」(無効) にします。これは、LLDP エージェントが「Link Aggregation TLV」を送信する必要があることを示します。このタイプは IEEE 802.3 MAC における現在のリンクアグリゲーションステータスを示します。情報には、ポートがリンクアグリゲーションができるかどうか、ポートが集約した 1 つのリンクにまとめられるかどうか、および束ねられたポートの ID が含まれる必要があります。初期値は無効です。 |
| Maximum Frame Size | 最大フレームサイズの通知を「Enabled」(有効) / 「Disabled」(無効) にします。LLDP エージェントが「Maximum-frame-size TLV」を送信する必要があることを示します。初期値は無効です。 |
| Power Via MDI | プルダウンメニューを使用して、LLDP エージェントが MDI TLV を通じた電力供給の有無を指定します。3 つの IEEE 802.3 PMD インプリメンテーション (10BASE-T、100BASE-TX および 1000BASE-T) により、接続されている電力が未供給のシステムに対してリンクを通じて供給されます。MDI TLV 経由の電力供給により、ネットワーク管理が通知を行い、送信する IEEE 802.3 LAN ステーション MDI 電力のサポート機能を検出します。初期値は無効です。 |

「Apply」ボタンをクリックし、変更を有効にします。

LLDP Statistics System (LLDP 統計情報システム)

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

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

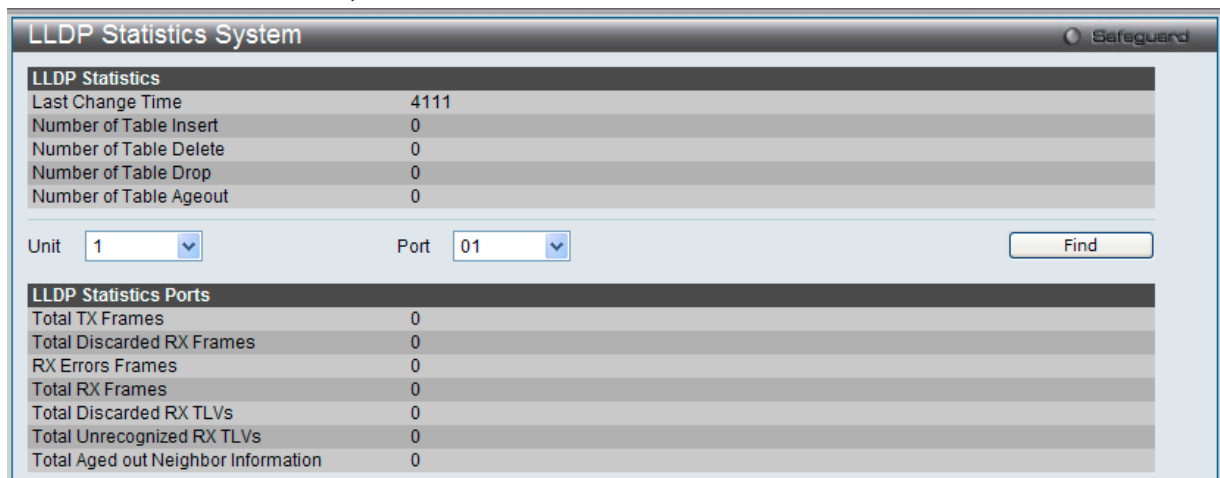


図 8-132 LLDP Statistics System 画面

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

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

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

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

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

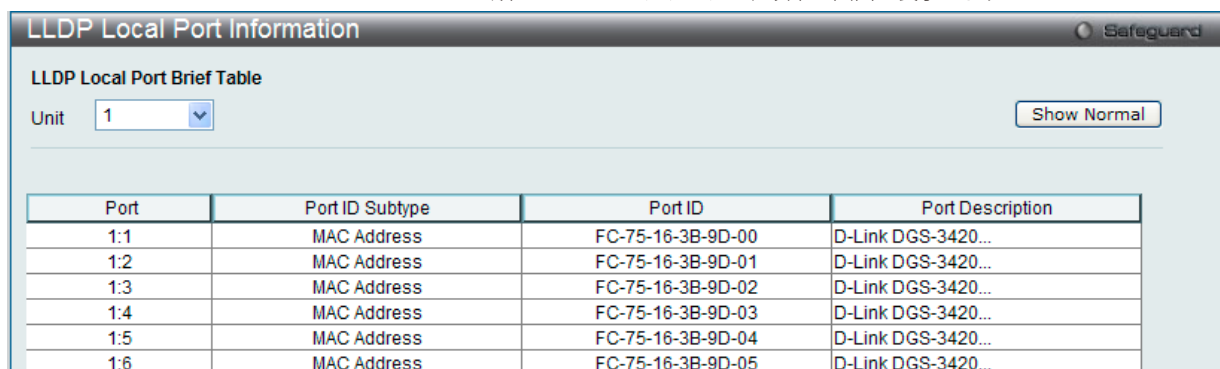


図 8-133 LLDP Local Port Information 画面 - Brief

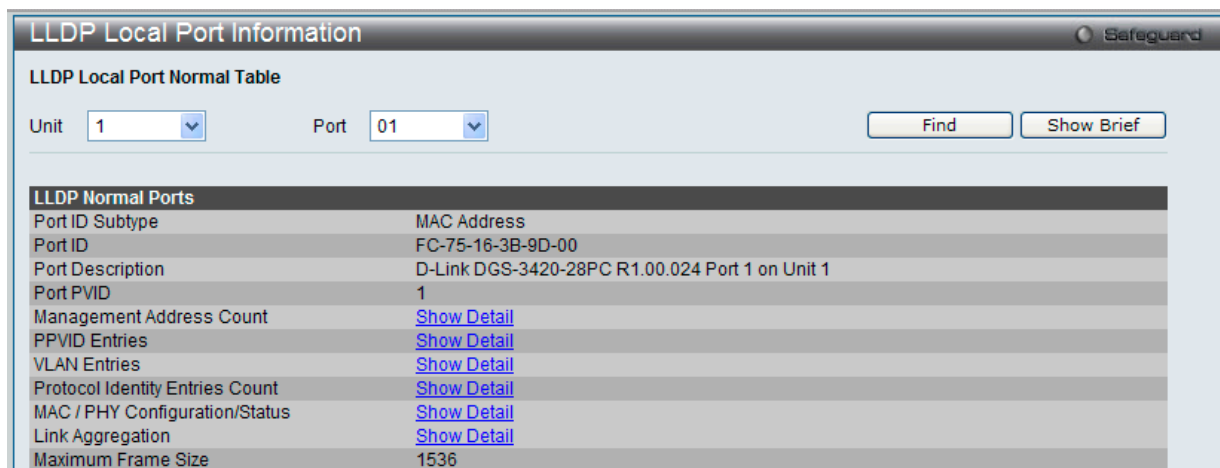
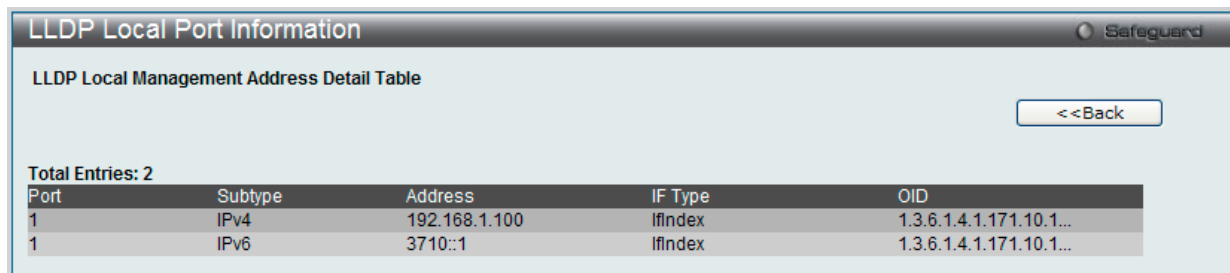


図 8-134 LLDP Local Port Information 画面 - Normal

ユニット番号およびポート番号を選択し、「Find」ボタンをクリックして指定エントリを表示します。

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



| Port | Subtype | Address | IF Type | OID |
|------|---------|---------------|---------|-------------------------|
| 1 | IPv4 | 192.168.1.100 | ifindex | 1.3.6.1.4.1.171.10.1... |
| 1 | IPv6 | 3710::1 | ifindex | 1.3.6.1.4.1.171.10.1... |

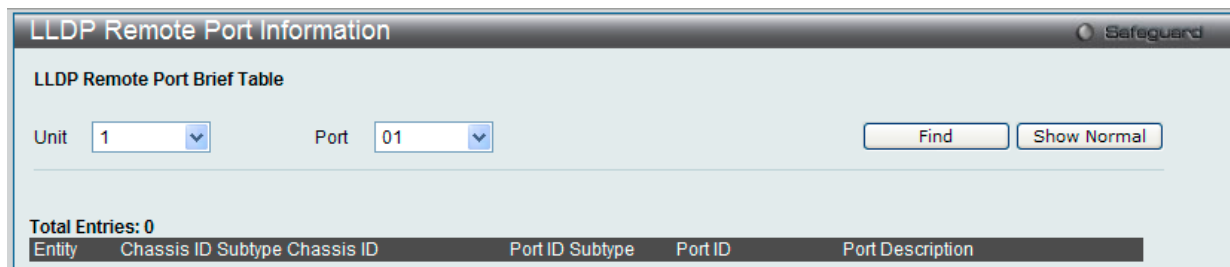
図 8-135 LLDP Local Port Information 画面 - Detail

「<<Back」ボタンをクリックして前のページに戻ります。

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

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

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

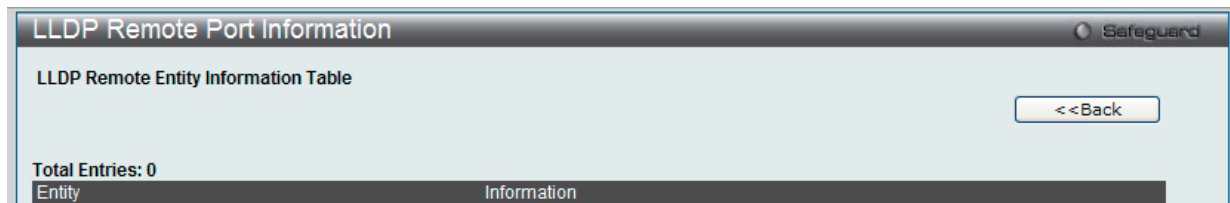


| Entity | Chassis ID Subtype | Chassis ID | Port ID Subtype | Port ID | Port Description |
|------------------|--------------------|------------|-----------------|---------|------------------|
| Total Entries: 0 | | | | | |

図 8-136 LLDP Remote Port Information 画面 - Brief

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

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



| Entity | Information |
|------------------|-------------|
| Total Entries: 0 | |

図 8-137 LLDP Remote Port Information 画面 - Normal

「<<Back」ボタンをクリックして前のページに戻ります。

LLDP-MED (LLDP-MED 設定)

LLDP-MED (Media-Endpoint-Discovery) は、専門的なケーパビリティと LLDP-MED 規格に準拠した機能を持つネットワークエッジに高度な機能をサポートするために LLDP 業界標準を拡張したものです。

LLDP-MED System Settings (LLDP-MED システム設定)

LLDP-MED のログ状態と「Fast Start Repeat Count」(ファストスタート実行回数) の設定と LLDP MED システム情報の表示を行います。

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

図 8-138 LLDP-MED System Settings 画面

以下の項目が使用できます。

| 項目 | 説明 |
|--------------------------------|---|
| LLDP-MED Log State | ラジオボタンを使用して LLDP-MED のログ状態を「Enabled」(有効) / 「Disabled」(無効) にします。 |
| Fast Start Repeat Count (1-10) | ファストスタート実行回数 (1-10) を入力します。LLDP MED ケイパビリティの TLV が存在する LLDP リモートシステム MIB と関連しない MSAP 識別子で検出される場合、アプリケーションレイヤはファストスタートメカニズムを開始し、「medFastStart」 タイマを「medFastStartRepeatCount」回数 1 に設定します。初期値は 4 です。 |

「Apply」 ボタンをクリックして各セクションで行った変更を適用します。

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

LLDP-MED TLV の送信を有効または無効にします。

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

| Port | NTCS | Capabilities | Network Policy | Power Pse | Inventory |
|------|----------|--------------|----------------|-----------|-----------|
| 1 | Disabled | Disabled | Disabled | Disabled | Disabled |
| 2 | Disabled | Disabled | Disabled | Disabled | Disabled |

図 8-139 LLDP-MED Port Settings 画面

以下の項目が使用できます。

| 項目 | 説明 |
|---------------------|--|
| Unit | 設定するユニットを選択します。 |
| From Port / To Port | 設定するポート範囲を指定します。 |
| NTCS | NTCS (トポロジ変更状態の通知) を有効または無効にします。 |
| State | 「LLDP-MED TLV」の送信を有効または無効にします。また、LLDP エージェントが送信すべき TLV タイプをチェックします。TLV タイプは Capabilities、Network Policy、Power Pse、および Inventory です。「All」を選択すると、すべての TLV タイプを選択します。 |
| Capabilities | この TLV タイプは、LLDP エージェントが「LLDP-MED capabilities TLV」を送信する必要があることを示します。LLDP-MED PDU を送信する場合、この TLV タイプを有効にする必要があります。そうでないと、このポートは LLDP-MED PDU を送信することができません。 |

| 項目 | 説明 |
|----------------|---|
| Network Policy | このTLV タイプは、LLDP エージェントが「LDP-MED network policy TLV」を送信する必要があることを示します。 |
| Inventory | このTLV タイプは、LLDP エージェントが「LLDP-MED inventory TLV」を送信する必要があることを示します。 |
| All | このオプションを選択すると、設定に「Capabilities」、「Network Policy」および「Inventory」を含めます。 |

「Apply」 ボタンをクリックして行った変更を適用します。

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

外向きの LLDP-MED 通知を組み込むためにポートごとの現在の情報を表示します。

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

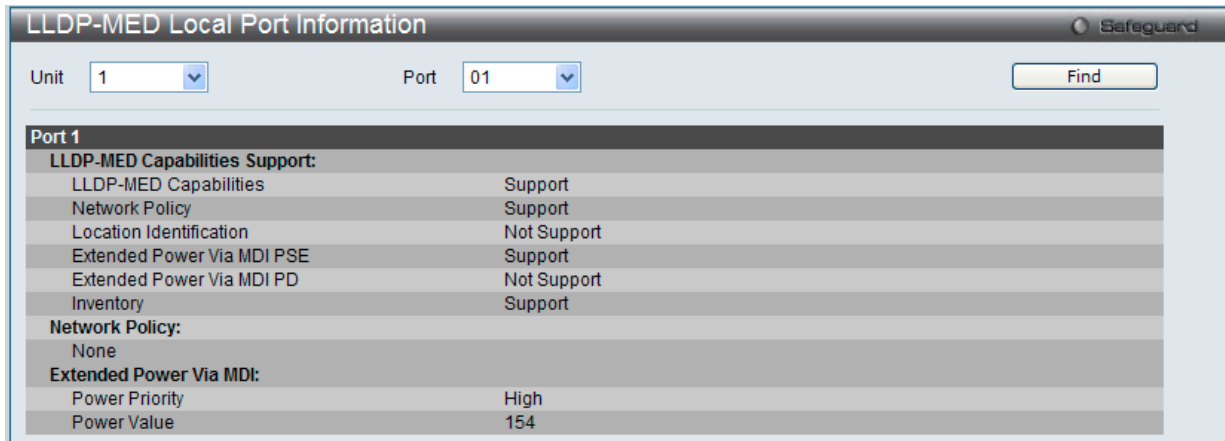


図 8-140 LLDP-MED Local Port Information 画面

「Unit」 および 「Port」 を選択し、「Find」 ボタンをクリックして、特定ポートの統計情報を参照します。

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

Neighbor デバイスのパラメータから学習した情報を表示します。

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

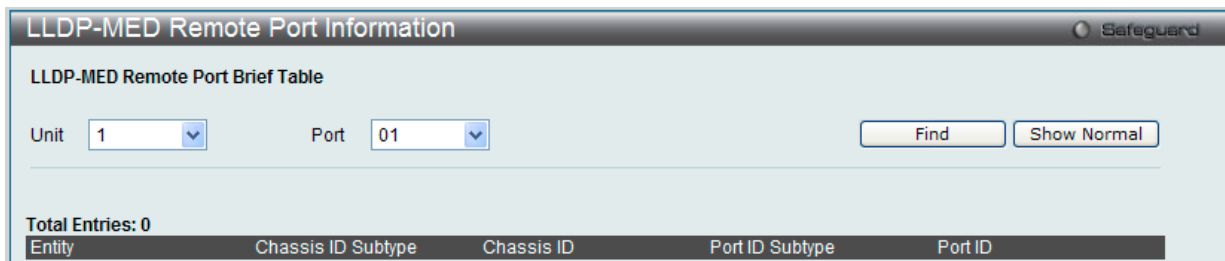


図 8-141 LLDP-MED Remote Port Information 画面 - Brief

ユニットおよびポート番号を選択し、「Find」 ボタンをクリックして、特定ポートの統計情報を参照します。

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

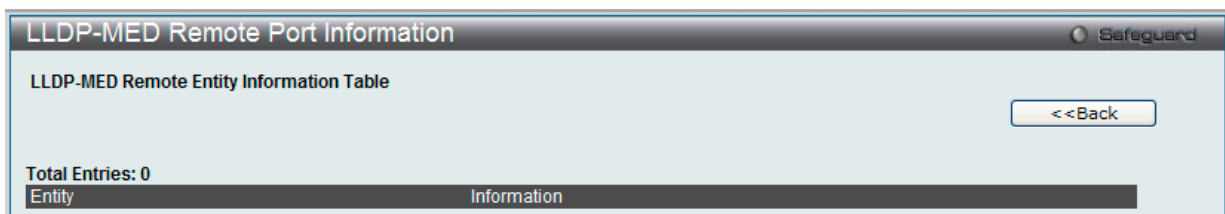


図 8-142 LLDP-MED Remote Port Information 画面 - Normal

「<<Back」 ボタンをクリックして前のページに戻ります。

NLB FDB Settings (NLB FDB 設定)

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

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

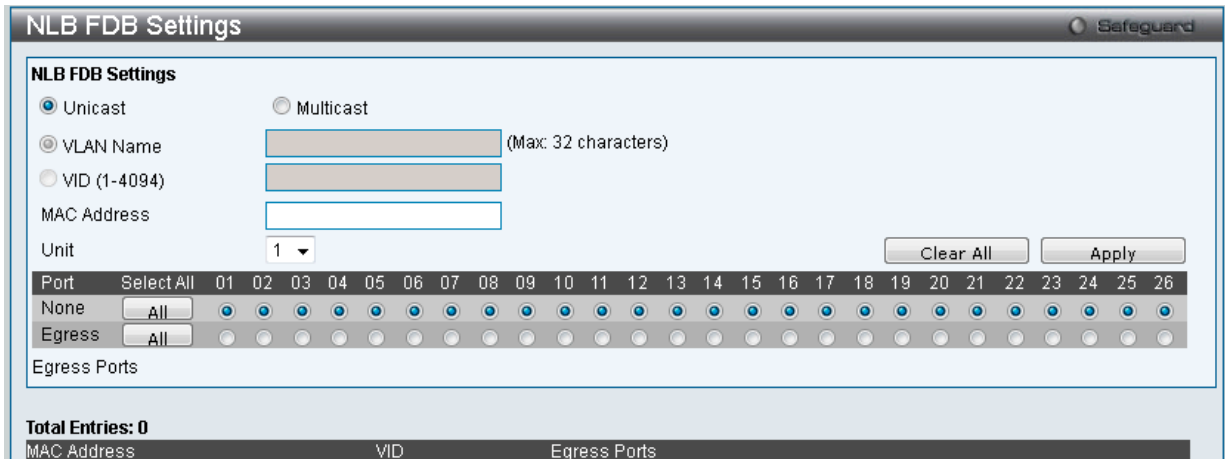


図 8-143 NLB FDB Settings 画面

以下の項目が設定可能です。

| 項目 | 説明 |
|--------------|--|
| Unicast | NLB ユニキャスト FDB エントリを作成します。 |
| Multicast | NLB マルチキャスト FDB エントリを作成します。 |
| VLAN Name | ラジオボタンをクリックして、作成される NLB マルチキャスト FDB エントリの VLAN 名を入力します。 |
| VID (1-4094) | ラジオボタンをクリックして、VLAN ID を入力します。 |
| MAC Address | 作成される NLB マルチキャスト FDB エントリの MAC アドレスを入力します。 |
| Unit | 設定するユニットを選択します。 |
| Port | 指定した NLB マルチキャスト FDB エントリに使用するフォワーディングポートを選択します。 <ul style="list-style-type: none"> None - ポートはフォワーディングポートではありません。「All」ボタンをクリックするとすべてのポートを選択します。 Egress - ポートはフォワーディングポートです。「All」ボタンをクリックするとすべてのポートを選択します。 |

「Apply」ボタンをクリックして行った変更を適用します。

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

エントリの編集

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

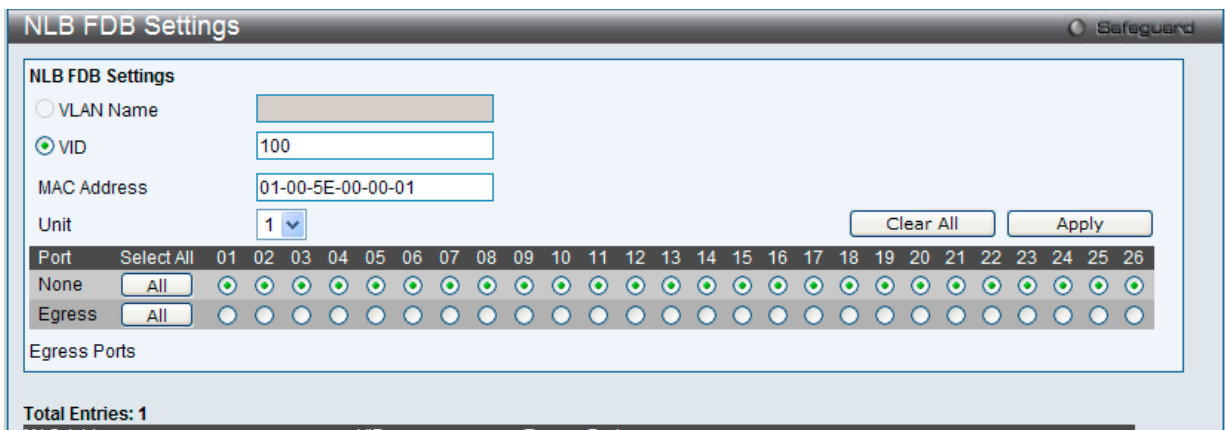


図 8-144 NLB FDB Settings 画面 - Edit

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

エントリの削除

削除するエントリの「Delete」ボタンをクリックします。

PTP (PTP の設定)

PTP (Precision Time Protocol : 高精度時刻同期方式) システムは、イーサネットネットワークを通して 1 マイクロ秒未満の精度で配信されるクロックに同期することができます。

PTP は、システムにおいて正確なクロックの同期を可能にする技術です。PTP はイーサネットおよび UDP を含むマルチキャストメッセージ送信をサポートするローカルエリアネットワークで通信するシステムに適切です。PTP により、様々な固有の精度、解像度、および安定性のクロックを含む異種システムはグラントマスタクロックへ同期が可能となります。

同期は 2 つの処理に分けられます。ベストマスタクロック (BMC : Best Master Clock) アルゴリズムは、すべてのローカルポートの PTP 状態 (マスタ / スレーブ) を決定します。同期アルゴリズムはマスタとスレーブクロック間のクロックオフセットを計算します。イベントメッセージの伝搬時間を計算するために、2 つのメカニズム (Delay Request-response Mechanism および Peer Delay Mechanism) があります。

PTP システムには、3 つ PTP デバイスタイプ (境界クロック、エンドツーエンド透過クロック、およびピアツーピア透過クロック) があります。境界クロックのみベストマスタクロックの選択に参加できます。

注意 PTP 機能は、単体利用の場合のみサポートしている機能です。スタック構成時にはご使用になれませんのでご注意ください。

PTP Global Settings (PTP グローバル設定)

PTP 機能をグローバルに設定します。

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

図 8-145 PTP Global Settings 画面

以下の項目が設定可能です。

| 項目 | 説明 |
|---------------------------------|--|
| PTP State | プルダウンメニューを使用して、PTP 状態を「Enabled」(有効)/「Disabled」(無効)にします。 |
| PTP Mode | スイッチの PTP タイプを選択します。スイッチには、3 つ PTP デバイスタイプ、「Boundary」(境界)、「P2P Transparent」(ピアツーピア透過)、および「E2E Transparent」(エンドツーエンド透過)があります。初期値は「E2E Transparent」です。 |
| PTP Transport Protocol | 通信パスに使用する送信プロトコルを選択します。初期値は UDP です。 |
| Unit | 設定するユニットを選択します。 |
| PTP Clock Domain Number (0-127) | ローカルクロックのドメイン属性を入力します。すべての PTP メッセージ、データセット、ステートマシン、およびその他すべての PTP エンティティがいつも特定のドメイン番号に関連付けられます。範囲は 0-127 です。初期値は 0 です。個別に PTP を実行するスタックシステムでは、各ユニットは同じドメインまたは異なるドメインで動作することができます。 |
| PTP Clock Domain Name | 指定したドメイン番号に対してドメイン名を入力します。 |

「Apply」 ボタンをクリックして各セクションで行った変更を適用します。

PTP Port Settings (PTP ポート設定)

PTP の状態をポートごとに設定します。

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

| Unit | From Port | To Port | State |
|------|-----------|---------|----------|
| 1 | 01 | 01 | Disabled |

| Port | State |
|------|----------|
| 1 | Disabled |
| 2 | Disabled |
| 3 | Disabled |
| 4 | Disabled |
| 5 | Disabled |

図 8-146 PTP Port Settings 画面

以下の項目が設定可能です。

| 項目 | 説明 |
|---------------------|--|
| Unit | 設定するユニットを選択します。 |
| From Port / To Port | この設定に使用するポート範囲を選択します。 |
| State | プルダウンメニューを使用して、指定ポートの PTP 状態を「Enabled」(有効)/「Disabled」(無効)にします。 |

「Apply」ボタンをクリックして行った変更を適用します。

PTP Boundary Clock Settings (PTP 境界クロック設定)

PTP 境界クロックの属性を設定します。実行するためには少なくとも 1 つ設定する必要があります。

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

図 8-147 PTP Boundary Clock Settings 画面

以下の項目が設定可能です。

| 項目 | 説明 |
|--------------------|---|
| Priority 1 (0-255) | ベストマスタクロックアルゴリズムの実行に使用します。低い値ほど優先度が高くなります。範囲は 0-255 です。0 は最も高い優先度を示します。 |
| Priority 2 (0-255) | ベストマスタクロックアルゴリズムの実行に使用します。低い値ほど優先度が高くなります。BMC アルゴリズムの操作が、Priority1 の値、クロックのクラス、およびクロックの精度に基づいたクロックの指示に失敗した場合、Priority2 は他のデバイスより低い値を作成することができます。範囲は 0-255 です。0 は最も高い優先度を示します。 |

「Apply」ボタンをクリックして行った変更を適用します。

PTP Boundary Port Settings (PTP 境界ポート設定)

PTP 境界クロックの属性を設定します。PTP デバイスが境界タイプである場合に、本設定は機能します。

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

| Port | DM | AI | CART | SI | EDRI | PDRI |
|------|-----|----|------|------|------|------|
| 1 | E2E | 2 | 3 | 1.00 | 0 | 1 |
| 2 | E2E | 2 | 3 | 1.00 | 0 | 1 |
| 3 | E2E | 2 | 3 | 1.00 | 0 | 1 |
| 4 | F2F | 2 | 3 | 1.00 | 0 | 1 |

図 8-148 PTP Boundary Port Settings 画面

以下の項目が設定可能です。

| 項目 | 説明 |
|---------------------------------|---|
| Unit | 設定するユニットを選択します。 |
| From Port / To Port | この設定に使用するポート範囲を選択します。 |
| Announce Interval (1-16) | ラジオボタンをクリックし、連続するアナウンスメッセージ間の平均時間を入力します。アナウンス間隔として参照されます。IEEE 1588 プロトコルに従い、アナウンス間隔の値は底を 2 とする測定時間 (秒) の対数として表示されます。入力値は 1、2、4、8、または 16 とします。無効な数字が入力されると、それより大きくて最も近い値に自動的に調整されます。初期値は 2 (秒) です。 |
| Announce Receipt Timeout (2-10) | ラジオボタンをクリックして、ANNOUNCE_RECEIPT_TIMEOUT_EXPIRES イベントの発生前にアナウンスメッセージを受信せずに通過すべきアナウンス間隔を入力します。アナウンス間隔値の乗数は、アナウンス受信のタイムアウトの間隔に一致します。範囲は 2-10 です。 |
| Delay Mechanism | プルダウンメニューを使用して、イベントメッセージの伝搬遅延時間を測定するメカニズムを指定します。 <ul style="list-style-type: none"> E2E - ポートは Delay Request-response Mechanism を使用します。(初期値) P2P - Peer Delay Mechanism を使用します。 |
| Delay Request Interval (0-5) | スレーブがマスタ上の指定ポートに送信する連続する遅延要求メッセージの許容される間隔の平均を入力します。この間隔の平均は、マスタによって決定されて、通知されます。 |
| Pdelay Request Interval (1-32) | 連続する Pdelay_Request メッセージの許容される間隔の平均を入力します。 |
| Synchronization Interval (1-2) | 連続する Sync メッセージ間隔の平均を入力します。syncInterval と呼ばれます。Half Second をチェックして、syncInterval に 0.5 秒を設定します。 |

「Apply」ボタンをクリックして行った変更を適用します。

PTP Peer to Peer Transparent Port Settings (PTP ピアツーピア透過ポート設定)

P2P 透過クロックの Pdelay Request Interval を設定します。

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

| Unit | From Port | To Port | Pdelay Request Interval (1-32) |
|------|-----------|---------|--------------------------------|
| 1 | 01 | 01 | 1 sec |

| Port | Pdelay Request Interval |
|------|-------------------------|
| 1 | 1 |
| 2 | 1 |
| 3 | 1 |
| 4 | 1 |
| 5 | 1 |
| 6 | 1 |
| 7 | 1 |
| 8 | 1 |
| 9 | 1 |
| 10 | 1 |

図 8-149 PTP Peer to Peer Transparent Port Settings 画面

以下の項目が設定可能です。

| 項目 | 説明 |
|--------------------------------|---|
| Unit | 設定するユニットを選択します。 |
| From Port / To Port | この設定に使用するポート範囲を選択します。 |
| Pdelay Request Interval (1-32) | 連続する Pdelay_Request メッセージの許容される間隔の平均を入力します。 |

「Apply」ボタンをクリックして行った変更を適用します。

PTP Clock Information (PTP クロック情報の表示)

PTP クロックのアクティブな属性を表示します。PTP の状態が「PTP Global Settings」画面で無効にされると、PTP クロック ID は「0000000000000000」と表示されます。

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

図 8-150 PTP Clock Information 画面

PTP Port Information (PTP ポート情報)

スイッチにおいて特別である PTP ポートのアクティブな属性を表示します。

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



図 8-151 PTP Port Information 画面

PTP Foreign Master Records Port Information (PTP 外部マスタレコードのポート情報)

境界クロックの特定ポートにおける現在の外部マスタレコードを表示します。

L2 Features > PTP > PTP Foreign Master Records Port Information の順にメニューをクリックし、以下の画面を表示します：

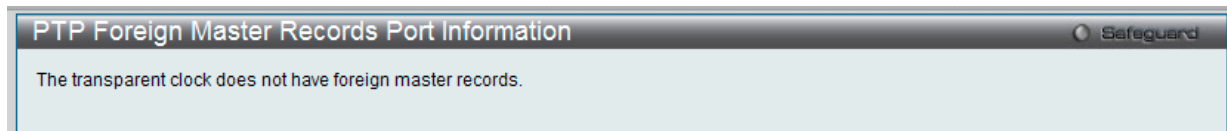


図 8-152 PTP Foreign Master Records Port Information 画面

第9章 L3 Features (レイヤ3機能の設定)

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

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

| サブメニュー | 説明 | 参照ページ |
|--|---|---------------------|
| IPv4 Static/Default Route Settings (IPv4 スタティック / デフォルトルート設定) | IPv4 スタティック / デフォルトルートの設定を行います。 | 207 |
| IPv4 Route Table (IPv4 ルートテーブル) | IPv4 ルーティングテーブルの外部経路情報を参照します。 | 208 |
| IPv6 Static/Default Route Settings (IPv6 スタティック / デフォルトルート設定) | IPv6 スタティック / デフォルトルートの設定を行います。 | 208 |
| IPv6 Route Table (IPv6 ルートテーブル) | IPv6 ルーティングテーブルの外部経路情報を参照します。 | 209 |
| Policy Route Settings (ポリシールート設定) | ポリシーベースルーティングは、指定したデバイスにインターネットへの最適な経路を与えます。 | 210 |
| IP Forwarding Table (IP フォワーディングテーブル) | 直接接続するすべての IP 情報を参照します。 | 212 |
| Route Preference Settings (ルート優先度設定) | ルート優先度の設定を行います。 | 212 |
| Route Redistribution Settings (ルート再配送設定) | OSPF または RIP が動作するネットワーク上のルータに OSPF と RIP 間のルーティング情報を再配送する設定を行います。 | 213 |
| IP Tunnel (IP トンネル) | IP トンネルを設定します。以下のメニューがあります。 IP Tunnel Settings (IP トンネル設定)、IP Tunnel GRE Settings (IP トンネル GRE 設定) | 214 |
| RIP (RIP 設定) | RIP の設定を行います。以下のメニューがあります。 RIP Settings (RIP 設定)、RIPng (RIPng 設定) | 216 |
| VRRP (VRRP 設定) | VRRP (Virtual Routing Redundancy Protocol) は、LAN 上の VRRP ルータの 1 つに仮想ルータとしての役割を動的に割り当てる機能です | 221 |

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

本スイッチはIPv4 アドレッシングのためにスタティックルーティング機能をサポートしています。IPv4 には最大 256 個のスタティックルートエントリを作成することができます。

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

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

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

図 9-1 IPv4 Static/Default Route Settings 画面

画面には以下の項目が表示されます。

| 項目 | 説明 |
|----------------|---|
| IP Address | スタティックルートに割り当てる IPv4 アドレスを入力します。「Default」をチェックすると、デフォルトルートに割り当てられます。 |
| Netmask | 対応するサブネットマスクを入力します。 |
| IP Tunnel Name | 「IP Tunnel」にチェックを入れ使用する IP トンネルの名前を指定します。 |
| Gateway | 対応するゲートウェイ IP アドレスを入力します。 |
| Metric | テーブルに入力した IP インタフェースのメトリック値を示します。1-65535 の範囲の値です。 |
| Backup State | Primary、Backup、または Weight から選択します。 各 IP アドレスは 1 つのプライマリルートを持っており、一方、他のルートはバックアップ状態に割り当てられる必要があります。プライマリルートに障害が発生すると、スイッチはルートが回復するまでルーティングテーブルが学習した順番に従ってバックアップルートを試みます。スタティックおよびデフォルトルートが設定されるバックアップ状態を示します。 |
| Null Interface | ネクストホップとして Null インタフェースを有効または無効にします。Null インタフェースはトラフィックをフィルタする別の方法を提供します。Null インタフェースに送信されるパケットはスイッチに破棄されます。 |

「Apply」ボタンをクリックして行った変更を適用します。

エントリの削除

対象のエントリの行の「Delete」ボタンをクリックします。

IPv4 Route Table (IPv4 ルートテーブル)

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

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

図 9-2 IPv4 Route Table 画面

画面には以下の項目が表示されます。

| 項目 | 説明 |
|-----------------|--|
| Network Address | 表示するルートの宛先ネットワークアドレスを指定します。 |
| IP Address | 表示するルートの宛先 IP アドレスを指定します。ルートに最も長く一致するプレフィックスが表示されます。 |
| RIP | RIP ルートだけを表示します。 |
| Hardware | チップに記述されているルートだけを表示します。 |

「Find」 ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

複数ページが存在する場合は、ページ番号を入力後、「Go」 ボタンをクリックして、特定のページへ移動します。

IPv6 Static/Default Route Settings (IPv6 スタティック / デフォルトルート設定)

IPv6 アドレスのスタティックエントリは IPv6 形式のアドレスで本スイッチのルーティングテーブルに入力します。

L3 Features > IPv6 Static/Default Route Settings の順にメニューをクリックし、以下の画面を表示します。

図 9-3 IPv6 Static/Default Route Settings 画面

画面には以下の項目が表示されます。

| 項目 | 説明 |
|----------------------------|---|
| IPv6 Address/Prefix Length | ルートの宛先ネットワークを入力するか、「Default」をチェックしてデフォルトルートに割り当てます。 |
| IP Tunnel Name | 「IP Tunnel」をチェックして、使用する IP トンネル名を入力します。 |
| Interface Name | スタティック IPv6 ルートが作成される IP インタフェース名を指定します。 |
| Nexthop Address | IPv6 形式におけるネクストホップゲートウェイアドレスに対応する IPv6 アドレスを指定します。 |
| Metric (1-65535) | IPv6 インタフェースのメトリック値を指定します。スイッチと上記 IPv6 アドレス間のルータの数を表します。範囲は 1-65535 です。 |

| 項目 | 説明 |
|--------------|--|
| Backup State | 各 IPv6 アドレスは1つのプライマリルートを持っており、一方、他のルートはバックアップ状態に割り当てられる必要があります。プライマリルートに障害が発生すると、スイッチはルートが回復するまでルーティングテーブルが学習した順番に従ってバックアップルートを試します。IPv6 が設定されるバックアップ状態を示します。「Primary」または「Backup」を指定します。 |

「Apply」 ボタンをクリックして行った変更を適用します。

エントリの削除

テーブル内の削除するエントリの「Delete」 ボタンをクリックします。すべてのエントリを削除するためには、「Delete All」 ボタンをクリックします。

IPv6 Route Table (IPv6 ルートテーブル)

現在の IPv6 ルーティングテーブルを表示します。

L3 Features > IPv6 Route Table の順にメニューをクリックし、以下の画面を表示します。

図 9-4 IPv6 Route Table 画面

画面には以下の項目が表示されます。

| 項目 | 説明 |
|----------------------------|---------------------------------------|
| IPv6 Address/Prefix Length | チェックを行い、ルートの IPv6 宛先ネットワークアドレスを入力します。 |
| IPv6 Address | チェックを行い、IPv6 アドレスを入力します。 |
| RIPng | RIPng ルートエントリを表示します。 |
| Hardware | ハードウェアテーブルに記述されているルートだけを表示します。 |

「Find」 ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

複数ページが存在する場合は、ページ番号を入力後、「Go」 ボタンをクリックして、特定のページへ移動します。

Policy Route Settings (ポリシールート設定)

ポリシーベースルーティングは、指定したデバイスにインターネットへの最適な経路を与えるためにスイッチに使用される方法です。アクセスプロファイル機能と連携して使用される場合、スイッチはデバイスから送信されたトラフィックについてアクセスプロファイル機能を使用して識別し、ご使用のネットワークの通常のルーティング体系よりもインターネットにより直接的に接続するネクストホップルータに転送します。

下の図は例です。

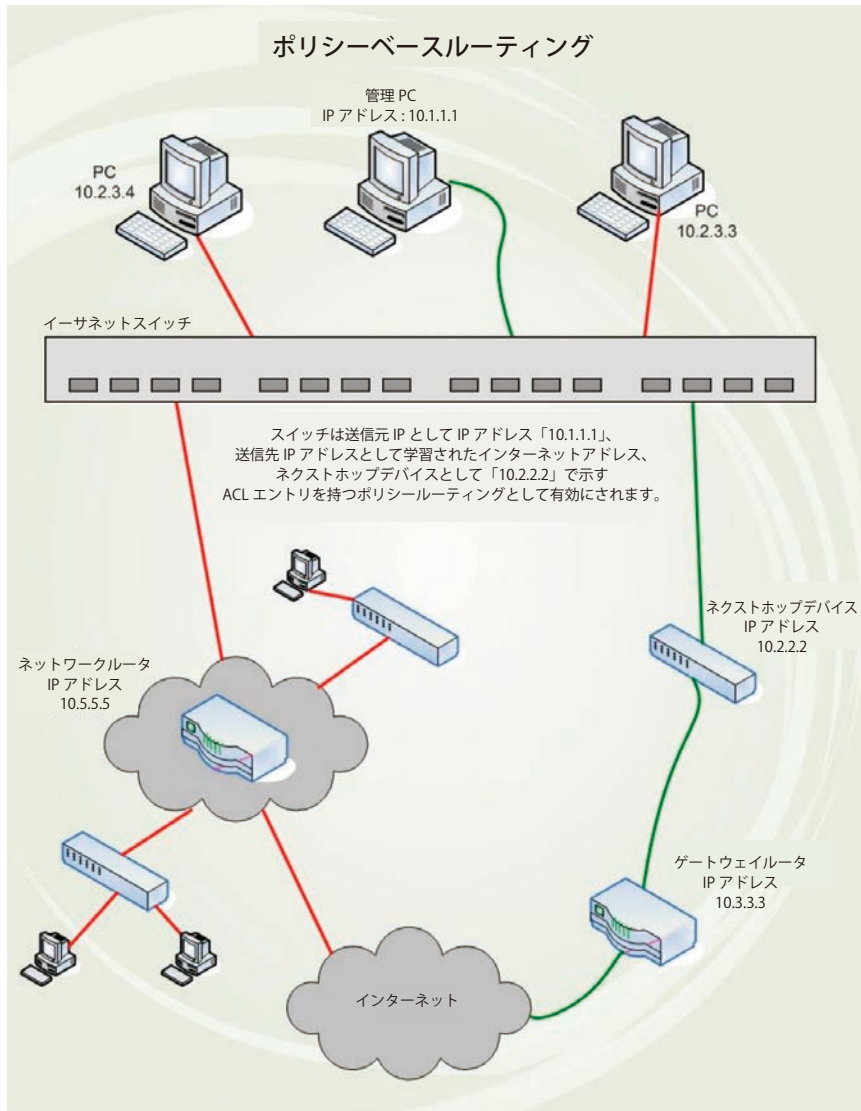


図 9-5 ポリシーベースルート例

IP アドレス「10.1.1.1」の PC が会社のマネージャに所属し、他の PC が従業員に所属しているとします。ネットワーク管理者は、ポリシールーティングスイッチをゲートウェイルータ「10.3.3.3」に直接接続しているネクストホップデバイス「10.2.2.2」を使用してインターネットにより直接的な接続を行うように設定し、ネットワークトラフィックを回避することを望みます。このようにノーマルなネットワークとそのトラフィックを避けることができます。これを実行するためには、スイッチのアクセスプロファイル機能を使用し、適切な情報に従って送信元 IP アドレスとして IP アドレス「10.1.1.1」を、送信先 IP アドレスとして (ルーティングプロトコル経由で学習した) インターネットアドレスを PC に設定する必要があります。次に、管理者は「Policy Route」画面で設定を行い、アクセスプロファイルとその関連ルールを有効にし、さらにネクストホップルータの IP アドレス「10.2.2.2」を設定します。最後にポリシールートエントリを有効にします。

設定を完了すると、アクセスプロファイル機能を使用して IP アドレスを識別し、ポリシーベースルートがあることを認知します。その後、ゲートウェイルータにパケットをリレーする指定のネクストホップルータに対して情報をフォワードします。このようにしてインターネットへの新しい経路が設定されます。

本機能の実行には以下の制限および注意があります。

1. アクセスプロファイルはルールに従ってはじめて作成される必要があります。管理者がアクセスプロファイルなしで本機能を有効にしようとすると、エラーメッセージが表示されます。
2. アクセスプロファイルが Deny に設定されると、パケットは破棄され、ネクストホップルータにフォワードされません。
3. 管理者が設定済みのポリシールートに直接リンクするルールまたはプロファイルを削除すると、エラーメッセージが直ちに現れます。

ポリシールート機能を設定するためには、**L3 Features > Policy Route Settings** の順にメニューをクリックし、以下の画面を表示します。

図 9-6 Policy Route Settings 画面

「Add」ボタンをクリックして、入力した情報に基づいて新しいエントリを追加します。

「Edit」ボタンをクリックして、指定エントリを編集します。

「Delete」ボタンをクリックして、指定エントリを削除します。

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

エントリの編集

ポリシールートの編集をするためには、「Edit」ボタンをクリックして以下の画面を表示します。

図 9-7 Policy Route Settings 画面 - Edit

以下の項目を設定します。

| 項目 | 説明 |
|-----------------------|--|
| Policy Route Name | ポリシールートを識別するために使用する名前を半角英数字 32 文字以内で入力します。 |
| Profile ID (1-6) | 作成済みのアクセスプロファイルの Profile ID 番号を入力します。これはパケットを以下に続くこのポリシールートとして識別するために使用されます。このアクセスプロファイルはアクセスルールに従っており、このポリシールートの作成前に作成される必要があります。 |
| Access ID (1-256) | 作成済みのアクセスプロファイルの Access ID 番号を入力します。これはパケットを以下に続くこのポリシールートとして識別するために使用されます。このアクセスルールはアクセスプロファイルに従っており、このポリシールートの作成前に作成される必要があります。 |
| Next Hop IPv4 Address | インターネットに接続しているゲートウェイルータも直接接続しているネクストホップルータの IP アドレスを入力します。 |
| State | プルダウンメニューを使用して、ポリシールートを「Enabled」（有効）または「Disabled」（無効）にします。 |
| Route Preference | 「Route Preference（ルート優先度）」を使用します。オプションを「Default」または「BPR」から選択します。 |

「Apply」ボタンをクリックして行った変更を適用します。

「<<Back」ボタンをクリックし、変更を破棄して前のページに戻ります。

IP Forwarding Table (IP フォワーディングテーブル)

IP フォワーディングテーブルは直接接続するすべての IP 情報を保存しています。ここでは直接接続するすべての IP 情報を参照します。

L3 Features > IP Forwarding Table をクリックし、以下の画面を表示します。

図 9-8 IP Forwarding Table 画面

エントリの参照

「IP Address」、「Interface Name」または「Port」ラジオボタンをクリックして、情報を入力し、「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

Route Preference Settings (ルート優先度設定)

ルート優先度を設定します。小さい優先度値を持つルートほど高いプライオリティを持ちます。ローカルルートの優先度は 0 に固定されています。

L3 Features > Route Preference Settings の順にメニューをクリックし、以下の画面を表示します。

図 9-9 Route Preference Settings 画面

以下の項目が設定、表示に使用されます。

| 項目 | 説明 |
|-----------------|---|
| Static (1-999) | 1 から 999 の範囲から、Static のルート優先度を指定します。初期値は 60 です。 |
| Default (1-999) | デフォルトルートの優先度値を設定します。初期値は 1 です。 |
| RIP | RIP ルートに優先度値を設定します。初期値は 100 です。 |

「Apply」ボタンをクリックし、設定を有効にします。

Route Redistribution (ルート再配布)

Route Redistribution Settings (ルート再配布設定)

1つのルーティングプロトコルから別のルーティングプロトコルまでルーティング情報を再配布するように設定します。

L3 Features > Route Redistribution > Route Redistribution 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。

| Source Protocol | Destination Protocol | Type | Metric | Edit | Delete |
|-----------------|----------------------|------|--------|------|--------|
| Static | RIP | All | 1 | Edit | Delete |
| Local | RIP | All | 2 | Edit | Delete |

図 9-10 Route Redistribution Settings 画面

以下の項目が使用されます。

| 項目 | 説明 |
|----------------------|--------------------------------|
| Destination Protocol | プルダウンメニューを使用して送信先のプロトコルを選択します。 |
| Source Protocol | プルダウンメニューを使用して送信元のプロトコルを選択します。 |
| Metric (0-16) | 再配布ルートに RIP メトリックを指定します。 |

「Apply」 ボタンをクリックして各セクションで行った変更を適用します。

エントリの編集

1. 編集するポートの「Edit」 ボタンをクリックし、以下の画面を表示します。

| Source Protocol | Destination Protocol | Type | Metric | Edit | Delete |
|-----------------|----------------------|------|--------|------|--------|
| Static | RIP | All | 1 | Edit | Delete |

図 9-11 Route Redistribution Settings 画面 - Edit

2. 項目を編集し、エントリの「Apply」 ボタンをクリックします。

エントリの削除

削除するエントリの「Delete」 ボタンをクリックします。

IPv6 Route Redistribution Settings (IPv6 ルート再配布設定)

IPv6 について 1つのルーティングプロトコルから別のルーティングプロトコルまでルーティング情報を再配布するように設定します。

L3 Features > Route Redistribution > IPv6 Route Redistribution 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。

| Source Protocol | Destination Protocol | Type | Metric | Edit | Delete |
|-----------------|----------------------|------|--------|------|--------|
| Local | RIPng | All | 1 | Edit | Delete |
| Static | RIPng | All | 2 | Edit | Delete |

図 9-12 IPv6 Route Redistribution Settings 画面

以下の項目が使用されます。

| 項目 | 説明 |
|----------------------|--------------------------------|
| Destination Protocol | プルダウンメニューを使用して送信先のプロトコルを選択します。 |
| Source Protocol | プルダウンメニューを使用して送信元のプロトコルを選択します。 |
| Type | プロトコルの種類を指定します。 |
| Metric | 再配布ルートに RIP メトリックを指定します。 |

「Apply」 ボタンをクリックして各セクションで行った変更を適用します。

IP Tunnel (IP トンネル)

IP Tunnel Settings (IP トンネル設定)

IP トンネルを設定します。

L3 Features > IP Tunnel > IP Tunnel Settings の順にメニューをクリックして以下の画面を表示します。

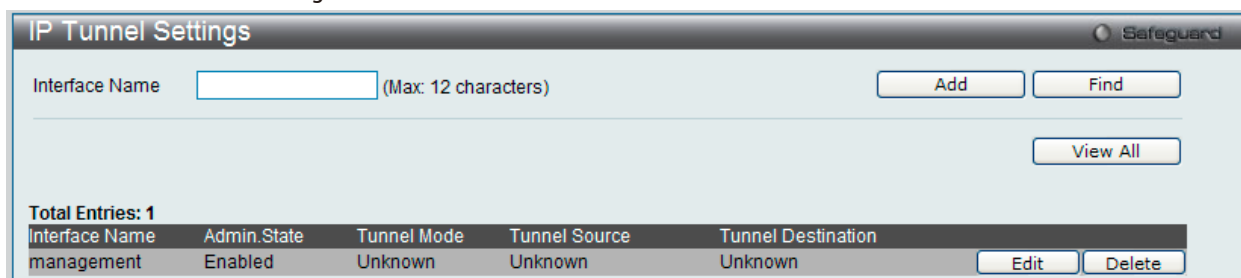


図 9-13 IP Tunnel Settings 画面

以下の項目が使用されます。

| 項目 | 説明 |
|----------------|-------------------------|
| Interface Name | IP トンネルのインタフェース名を入力します。 |

エントリの登録

「Add」ボタンをクリックして、入力した情報に基づいて新しいエントリを追加します。

エントリの検索

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。「View All」ボタンをクリックして、すべての定義済みエントリを表示します。

エントリの削除

テーブル内の削除するエントリの「Delete」ボタンをクリックします。すべてのエントリを削除するためには、「Delete All」ボタンをクリックします。

エントリの編集

1. 編集するポートの「Edit」ボタンをクリックし、以下の画面を表示します。

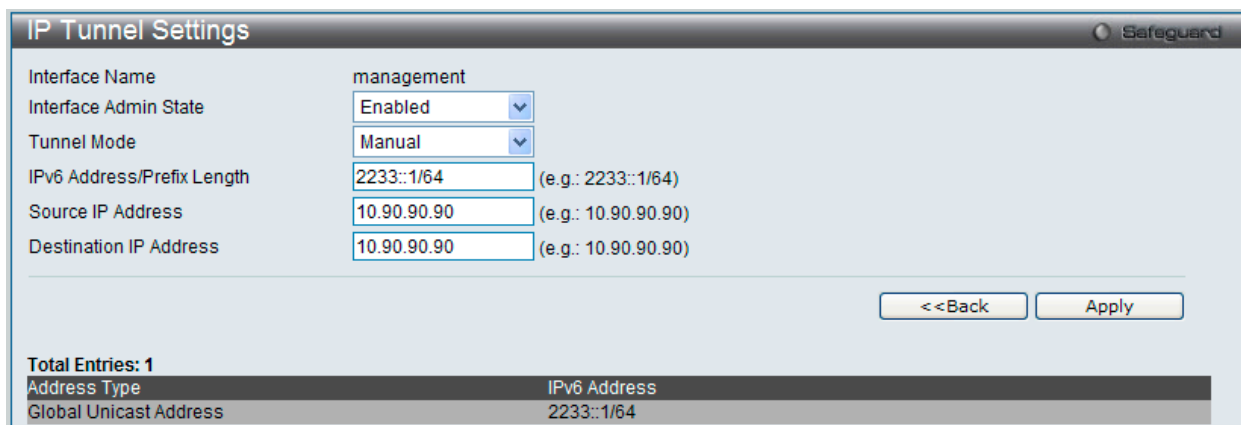


図 9-14 IP tunnel Settings - Edit 画面

以下の項目が使用されます。

| 項目 | 説明 |
|----------------------------|--|
| Interface Admin State | プルダウンメニューを使用して、「Interface Admin State」を「Enabled」(有効)/「Disabled」(無効)にします。 |
| Tunnel Mode | プルダウンメニューを使用してトンネルモードを選択します。None、Manual、6to4、および ISATAP から選択できます。 |
| IPv6 Address/Prefix Length | IPv6 アドレスネットワークアドレスを入力します。 |
| Source IP Address | 送信元 IP アドレスを指定します。 |
| Destination IP Address | 送信先 IP アドレスを指定します。 |

2. 項目を編集し、エントリの「Apply」ボタンをクリックします。

「<<Back」ボタンをクリックして前のページに戻ります。

IP Tunnel GRE Settings (IP トンネル GRE 設定)

スイッチにおいて既存のトンネルを GRE トンネル (IPv6/IPv4-in-IPv4 または IPv6/IPv4-in-IPv6) として設定します。このトンネルが以前に別のモードで設定されていると、トンネルの情報はデータベースにまだ存在します。しかし、トンネルの以前の情報が有効かどうかは、現在のモードに依存します。

GRE トンネルは、単にサイト内またはサイト間で使用できる point-to-point トンネルです。

GRE IPv6/IPv4-in-IPv4 トンネルを設定する場合、送信プロトコルが IPv4 プロトコルであるため、送信元と送信先アドレスの双方とも IPv4 アドレスである必要があります。送信元と送信先アドレスタイプが一致していないと、GRE トンネルは動作しません。

GRE IPv6/IPv4-in-IPv4 トンネルを設定する場合、送信プロトコルが IPv6 プロトコルであるため、送信元と送信先アドレスの双方とも IPv6 アドレスである必要があります。送信元と送信先アドレスタイプが一致していないと、GRE トンネルは動作しません。

L3 Features > IP Tunnel > IP Tunnel GRE Settings の順にメニューをクリックして以下の画面を表示します：

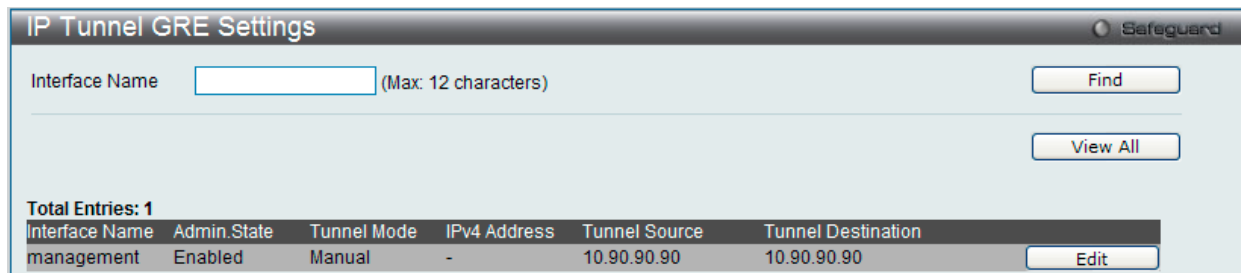


図 9-15 IP Tunnel GRE Settings 画面

以下の項目が使用されます。

| 項目 | 説明 |
|----------------|-------------------------|
| Interface Name | IP トンネルのインタフェース名を入力します。 |

エントリの検索

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

「View All」ボタンをクリックして、すべての定義済みエントリを表示します。

エントリの編集

1. 編集するポートの「Edit」ボタンをクリックし、以下の画面を表示します。

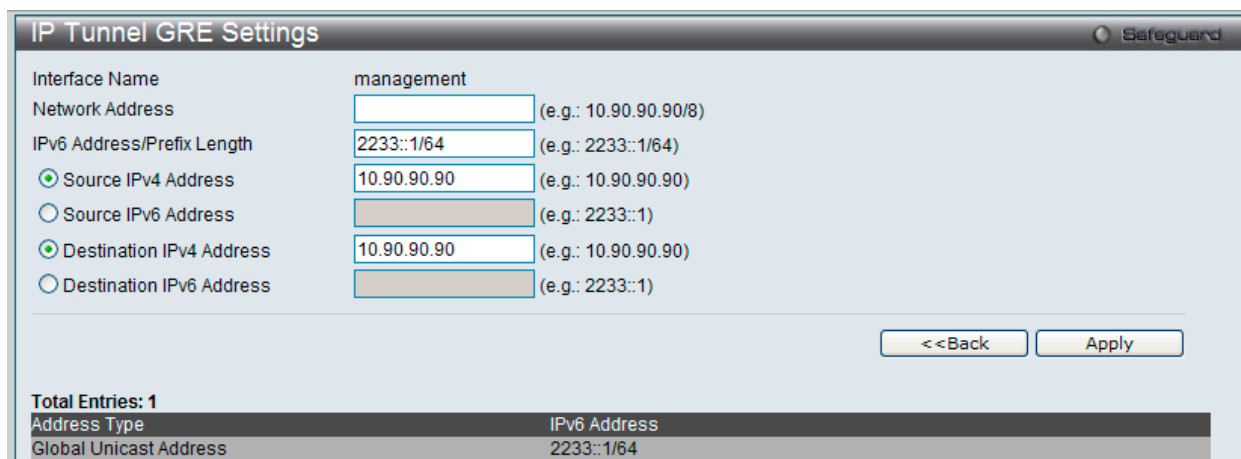


図 9-16 IP tunnel GRE Settings - Edit 画面

以下の項目が使用されます。

| 項目 | 説明 |
|----------------------------|---|
| Network Address | GRE トンネルインタフェースに割り当てた IPv4 アドレスを入力します。IPv4 アドレスが設定される場合、IPv4 の処理はこの IPv4 トンネルインタフェースで有効となります。この IPv4 アドレスはトンネルの送信元または送信先の IPv4 アドレスには接続していません。 |
| IPv6 Address/Prefix Length | GRE トンネルインタフェースに割り当てた IPv6 アドレスを入力します。IPv6 アドレスが設定される場合、IPv4 の処理はこの IPv6 トンネルインタフェースで有効となります。この IPv6 アドレスはトンネルの送信元または送信先の IPv6 アドレスには接続していません。 |
| Source IPv4 Address | ラジオボタンをクリックして、GRE トンネルインタフェースの送信元 IPv4 アドレスを入力します。これは、このトンネルの packets に送信元アドレスとして使用されます。使用するアドレスタイプは送信プロトコルに依存します。送信元と送信先の両方で使用されるアドレスタイプが一致していないと、GRE トンネルは動作しません。 |

| 項目 | 説明 |
|--------------------------|---|
| Source IPv6 Address | ラジオボタンをクリックして、GRE トンネルインタフェースの送信元 IPv6 アドレスを入力します。これは、このトンネルの packets に送信元アドレスとして使用されます。使用するアドレスタイプは送信プロトコルに依存します。送信元と送信先の両方で使用されるアドレスタイプが一致していないと、GRE トンネルは動作しません。 |
| Destination IPv4 Address | ラジオボタンをクリックして、GRE トンネルインタフェースの送信先 IPv4 アドレスを入力します。これは、このトンネルの packets に送信先アドレスとして使用されます。使用するアドレスタイプは送信プロトコルに依存します。送信元と送信先の両方で使用されるアドレスタイプが一致していないと、GRE トンネルは動作しません。 |
| Destination IPv6 Address | ラジオボタンをクリックして、GRE トンネルインタフェースの送信先 IPv6 アドレスを入力します。これは、このトンネルの packets に送信先アドレスとして使用されます。使用するアドレスタイプは送信プロトコルに依存します。送信元と送信先の両方で使用されるアドレスタイプが一致していないと、GRE トンネルは動作しません。 |

2. 項目を編集し、エントリの「Apply」ボタンをクリックします。

「<<Back」をボタンをクリックして前のページに戻ります。

RIP (RIP 設定)

RIP (Routing Information Protocol) は、距離ベクトル型のルーティングプロトコルです。RIP を使用するデバイスには、RIP アクティブが稼働しているものと RIP パッシブが稼働しているものの 2 種類があります。RIP アクティブのデバイスは、RIP メッセージを使用して他のデバイスに対してルートの通知 (Advertise) を行います。一方、パッシブのデバイスはこれらのメッセージをリスンするだけです。アクティブデバイスが送信する RIP メッセージに基づき、アクティブ、パッシブ両方のルーティングテーブルが更新されます。アクティブ側になることができるのはルータだけです。

RIP を使用するルータは、30 秒ごとにネットワークアドレスと距離情報 (通知ルータとリモートネットワークの間のルータの数 (ホップ) で表現) を含むルーティングアップデートをブロードキャストします。

RIP では、距離を 1 つのネットワークから他のネットワークへのホップ数 (整数) で計ります。直接接続されるネットワークに接続するルータを 1 ホップ、そのルータを経由して到達する次のルータが 2 ホップと数えられます。送信元から宛先の間ルータの数が増えるほど、RIP での距離 (またはホップカウント) は大きくなります。

ネットワークのパフォーマンスと安定性を高めるために使用されるルーティングテーブルの更新プロセスには、いくつかのルールがあります。ルータは新しいルートを学習した際、そのルートと同じホップカウント (コスト) のルートが既にテーブル内にあれば、更新を行いません。つまり、学習されたルートは、小さいホップカウントを持つルートが学習されるまで保持されます。

学習されたルートがルーティングテーブルに組み込まれる時、タイマが始動します。このタイマは、そのルートが通知される度に、再始動します。もし、ルートが一定期間 (通常は 180 秒) 通知されなければ、そのルートはルーティングテーブルから削除されます。

RIP は、ループ検出を行うための明示的な方法を持ちません。しかし、ルータが権限のないルータから間違ったルートを学習するのを防ぐための認証メカニズムを多く使用しています。

安定性を高めるため、RIP が使用するホップカウントには、低い値の最大値が設けられています。16 ホップは無限大 (ネットワーク到達不可能) として定義されています。言い換えると、ローカルルータは、送信元から 16 ルータ以上離れたネットワークへは、到達不可能であると見なすということです。

RIP メッセージのネットワークでの伝播が比較的遅いため、RIP は収束 (矛盾、到達不可能、またはループ状態のルートをルーティングテーブルから削除する) に時間がかかると指摘されています。

収束に時間がかかるという問題については、スプリットホライズンによって解決を図っています。スプリットホライズンは、あるルートを通知する際に、そのルートを学習したインタフェースからは通知しないという原則で成り立ちます。これにより一時的なルーティングループの発生を抑えることができます。

ホールドダウンという方法を使用して、ルータが新しいルートアップデートを受信後、新規のルートアップデートをある期間 (通常は 60 秒) 無視するようにすることもできます。これにより、ネットワーク上のすべてのルータがアップデートメッセージを受信できるようになります。

ルータは、「ポイズンリバース」という手法により、ルートの通知に無限大のホップカウント (16) を付加します。この方法は通常トリガーアップデートと組み合わせて使用され、到達不可のネットワークのアップデートメッセージを受信すると、ルータは直ちにブロードキャストを行うようにします。

RIP バージョン 1 メッセージフォーマット

RIP メッセージには、Routing information message と Information request の 2 種類があります。どちらも同じ形式を使用しています。

コマンドフィールドには、以下の表に示すオペレーションが指定されます。

| コマンド | 意味 |
|------|---------------------------------------|
| 1 | 一部またはすべてのルーティング情報のリクエスト |
| 2 | 送信元のルーティングテーブルからのネットワークと距離の情報を含むレスポンス |
| 3 | トレースモードオン (サポートなし) |
| 4 | トレースモードオフ (サポートなし) |
| 5 | Sun Microsystems 専用領域 |
| 9 | アップデート・リクエスト |
| 10 | アップデート・レスポンス |
| 11 | アップデート・アクノリッジメント (確認) |

RIP コマンドコード

「Version」フィールドには、プロトコルのバージョン (ここでは 1) が格納され、パケットの受信者は RIP のどのバージョンのパケットが送信されたかを知ることができます。

RIP1 メッセージ

RIP は、TCP/IP のみに限定されるわけではありません。RIP では、宛先ネットワークアドレスとして 14 オクテットまでのフィールドが確保されています (IP 使用の場合は、残りの 10 オクテットはゼロ)。他のネットワークプロトコルスイートはアドレスファミリ識別子フィールドに指定されます (IP の値は 2)。これにより、アドレスフィールドの解釈の仕方が決定されます。

RIP では、IP アドレス 0.0.0.0 がデフォルトルートとして指定されています。

ルータのホップ数で測る距離は、「Distance to Source Network」および「Distance to Destination Network」フィールドに格納されます。

RIP1 ルートの解釈

RIP は、クラス分けされるアドレスに使用されるように設計され、明示的なサブネットマスクは使用されません。バージョン 1 の拡張機能では、ルータがサブネットアドレスの交換を行う仕様になっていますが、これは、ネットワークが使用するサブネットマスクとアドレスが使用するサブネットマスクが同じである場合のみ適用されます。このため RIP バージョン 1 ではクラスのないアドレスを伝播できません。

RIP バージョン 1 を使用するルータは、各 IP インタフェースの異なるアップデートメッセージを接続するインタフェースに送信します。ルータのネットワークと同じサブネットマスクを使用するインタフェースは、サブネット化されたルートを持ちますが、他のインタフェースは持ちません。その場合、ルータはネットワークへのルートを一つだけ通知します。

RIP バージョン 2 の拡張機能

RIP バージョン 2 は、明示的なサブネットマスクを含みます。そのため、可変長のサブネットアドレスや CIDR 表記のクラスレスアドレスを使用することができます。さらに、明示的なネクストホップを含むため、収束までの速度が上がり、ルーティングループの発生を防止します。

RIP2 メッセージフォーマット

RIP2 で使用するメッセージフォーマットは RIP1 フォーマットの拡張版です。

RIP バージョン 2 では、さらに 16 ビットのルートタグが付加されています。ルートタグは維持され、またルータアップデートと共に送信されます。ルートの基点を識別するために使用されます。

RIP2 のバージョンは、RIP1 と同じオクテットを使用するため、1 つのルータ上で両方のバージョンを同時に使用することも可能です。

RIP Settings (RIP 設定)

1 つ以上の IP インタフェースに RIP 設定を行います。

L3 Features > RIP > RIP 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。RIP の設定を行ったインタフェースのリストが表示されます。

図 9-17 RIP Settings 画面

以下の項目があります。

| 項目 | 説明 |
|-----------------------------------|--|
| RIP State | RIP の状態を有効または無効にします。状態が無効にされると、RIP パケットは、インタフェースによって送受信されません。このインタフェースで設定されたネットワークは RIP データベースにはありません。 |
| Update Time (5-65535) | RIP アップデートを送信するレートを入力します。 |
| Timeout Time (5-65535) | RIP ルートが無効であると判断する時間を入力します。 |
| Garbage Collection Time (5-65535) | RIP ルートがルーティングテーブルから削除されないで保持される時間を入力します。 |
| Interface Name | 本設定に使用 IP インタフェース名を指定します。 |

「Apply」 ボタンをクリックして行った変更を適用します。

「Find」 ボタンをクリックして、指定したエントリを検索します。

「View All」 ボタンをクリックして、すべてのエントリを表示します。

エントリの編集

1. 「Edit」 ボタンをクリックすると、以下の画面が表示されます。

図 9-18 RIP Settings 画面 – Edit 画面

RIP インタフェースの設定に使用する項目は以下の通りです。

| 項目 | 説明 |
|----------------|---|
| Interface Name | 設定するインタフェース名が表示されます。 |
| TX Mode | 「Disabled」、「v1 Only」、「v1 Compatible」、「v2 Only」から選択します。ここで指定する RIP プロトコルのバージョンで RIP パケットを送出します。「Disabled」を指定すると、RIP パケットの送信をしません。 |
| RX Mode | 「Disabled」、「v1 Only」、「v2 Only」、「v1 or v2」から選択します。ここで指定する RIP プロトコルのバージョンが受信した RIP パケットの解釈に使用されます。「Disabled」を指定すると、RIP パケットの受信をしません。 |

| 項目 | 説明 |
|----------------|--|
| State | RIP インタフェースとしての使用を「Enabled」(有効) / 「Disabled」(無効) にします。状態が無効にされると、RIP パケットは、インタフェースによって送受信されません。このインタフェースで設定されたネットワークは RIP データベースにはありません。 |
| Authentication | ネットワーク上のルータがテーブルの交換の際に認証を行うかどうかを指定します。認証状態を有効にした場合、提供されたスペースで使用するパスワードを入力します。 |

2. 項目を編集後「Apply」ボタンをクリックします。

「<<Back」ボタンをクリックして前のページに戻ります。

RIPng (RIPng 設定)

スイッチは、RIPng (Routing Information Protocol next generation) をサポートしています。RIPng は、ルートを計算するのに使用するルーティング情報を交換するルーティングプロトコルであり、IPv6 ベースのネットワーク用です。

RIPng Global Settings (RIPng グローバル設定)

本画面では、RIPng の設定を行います。

L3 Features > RIP > RIPng > RIPng Global Settings の順にメニューをクリックして以下の画面を表示します。

図 9-19 RIPng Global Settings 画面

以下の項目を使用します。

| 項目 | 説明 |
|-----------------------------------|---|
| RIPng State | ラジオボタンを使用して RIPng を「Enabled」(有効) / 「Disabled」(無効) にします。初期値は「Disabled」です。 |
| Method | プルダウンメニューを使用して「No Horizon」、「Split Horizon」、および「Poison Reverse」から選択します。 <ul style="list-style-type: none"> No Horizon - どのホライズンも使用しません。 Split Horizon - 基本的なスプリットホライズンを使用します。これは初期設定です。 Poison Reverse - ポイズンリバースを持つスプリットホライズンを使用します。 |
| Update Time (5-65535) | アップデートタイムの値 (秒) を入力します。 |
| Expire Time (1-65535) | 期限終了タイムの値 (秒) を入力します。 |
| Garbage Collection Time (1-65535) | ガーベージコレクションタイムの値 (秒) を入力します。 |

「Apply」ボタンをクリックして行った変更を適用します。

RIPng Interface Settings (RIPng インタフェース設定)

本画面では、RIPng インタフェースの設定を行います。

L3 Features > RIP > RIPng > RIPng Interface Settings の順にメニューをクリックして以下の画面を表示します。

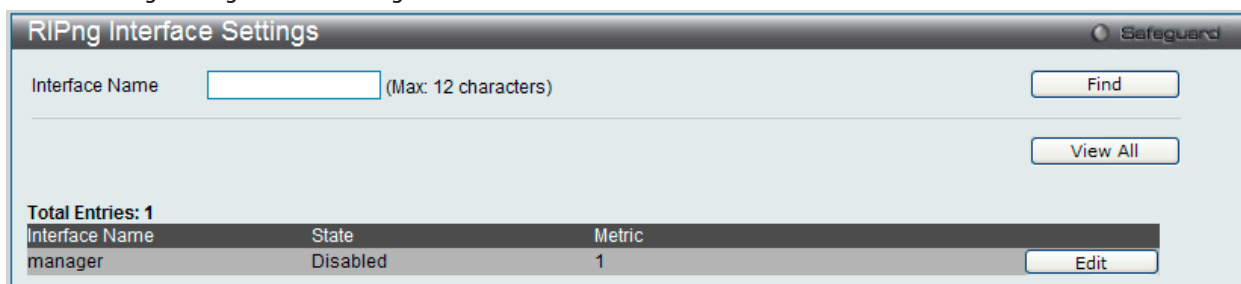


図 9-20 RIPng Interface Settings 画面

以下の項目を使用します。

| 項目 | 説明 |
|----------------|--------------------------|
| Interface Name | RIPng 設定のインタフェース名を入力します。 |

「Find」ボタンをクリックして、入力したインタフェースを検出します。

「View All」ボタンをクリックして、本スイッチに定義済みの全インタフェースを表示します。

エントリの編集

1. 編集するエントリの「Edit」ボタンをクリックして以下の画面を表示します。

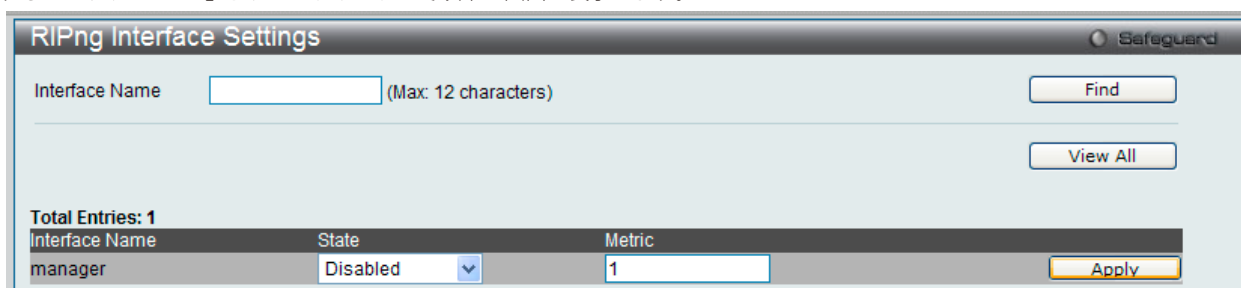


図 9-21 RIPng Interface Settings 画面 - Edit

2. 項目を編集後「Apply」ボタンをクリックします。

VRRP (VRRP 設定)

VRRP (Virtual Routing Redundancy Protocol) は、LAN 上の VRRP ルータの 1 つに仮想ルータとしての役割を動的に割り当てる機能です。VRRP ルータのうち、仮想ルータと対向する IP アドレスの制御を行うものをマスタールータと呼び、このルータが本 IP アドレス向けのパケットを送出します。また、エンドホストは LAN 上の仮想ルータの IP アドレスをデフォルトのファーストホップとして使用できます。VRRP 機能を使用して、管理者はすべてのエンドホストにダイナミックルーティングやルート検出プロトコルの設定を行わなくても、デフォルトパスコストを取得することができます。

LAN 上に静的に設定されたデフォルトルートは、障害発生箇所となる傾向があります。VRRP 機能はこの障害を回避するために、選出プロトコルを使用して LAN 上の VRRP ルータの 1 つに仮想ルータとしての役割を割り当てるよう設計されています。仮想ルータがダウンすると、選出プロトコルが優先度の最も高い仮想ルータを選び、LAN 上のマスタールータに任命します。これによりダウンした箇所に関係なく、リンクとコネクションはその状態を保つことができます。

VRRP では、1 台の物理的ルータの代わりに、物理的ルータのグループから構成される仮想ルータを導入します。仮想ルータは 2 台以上の物理ルータから構成され、その中で実際に稼動するのは 1 台のみです。その仮想ルータの中で実際に稼動しているルータが停止した場合、自動的に別のルータに切り替わり稼動を開始します。実際に稼動している物理ルータをマスタールータと呼び、マスタールータ異常時に備えて待機している物理ルータをバックアップルータと呼びます。

スイッチに仮想ルータ用の VRRP 機能を設定するためには、IP インタフェースが存在し、その IP アドレスが VLAN に所属している必要があります。VRRP 用 IP インタフェースはスイッチの VLAN (IP インタフェース) ごとに設定します。VRRP 機能が正しく動作するために、同じ VRRP グループ内の VRRP ルータは、同じ設定内容を持つ必要があります。

VRRP Global Settings (VRRP グローバル設定)

スイッチの VRRP 機能をグローバルに有効にします。

L3 Features > VRRP > VRRP Global Settings の順にメニューをクリックし、以下の画面を表示します。

図 9-22 VRRP Global Settings 画面

以下の項目を使用して設定を行います。

| 項目 | 説明 |
|-------------------------|--|
| VRRP State | スイッチの VRRP 機能をグローバルに「Enabled」(有効) / 「Disabled」(無効) にします。初期値は「Disabled」です。 |
| Non-owner Response Ping | 「Enabled」(有効) にすると、仮想 IP アドレスが他のホストに ping を行い、接続性を確認することができます。初期値は「Disabled」(無効) です。 |

「Apply」ボタンをクリックし、設定を有効にします。

VRRP Virtual Router Settings (VRRP 仮想ルータ設定)

VRRP 仮想ルータ設定を行います。

L3 Features > VRRP > VRRP Virtual Router Settings の順にメニューをクリックし、以下の画面でスイッチの仮想ルータの設定内容を参照します。

図 9-23 VRRP Virtual Router Settings 画面

インタフェースの仮想ルータの状態を指定します。

| 項目 | 説明 |
|----------------|--|
| Interface Name | VRRP エントリを作成するのに使用する IP インタフェース名を指定します。この IP インタフェースには VLAN が割り当てられている必要があります。 |

| 項目 | 説明 |
|--------------------------------|---|
| VRID (1-255) | 使用する仮想ルータの ID を指定します。本グループに参加するルータには同じ VRID 値が割り当てられる必要があります。スイッチの他の VRRP グループとは異なる値を入力します。 |
| IP Address | 使用するルータの IP アドレスを指定します。本 IP アドレスは、エンドホストに静的に割り当てられるデフォルトゲートウェイのアドレスでもあります。同じグループに属するルータには、同じ値を設定する必要があります。 |
| State | VRRP IP インタフェースを「Enabled」(有効) / 「Disabled」(無効) にします。 |
| Priority (1-254) | 仮想ルータのマスター選出のプライオリティを指定します。 |
| Advertisement Interval (1-255) | VRRP メッセージパケットの送出間隔(秒)。本値はグループ内で同じものが設定されている必要があります。初期値は1(秒)です。 |
| Preempt Mode | より高いプライオリティのバックアップルータが、より低いプライオリティのマスターから役割を取り戻すかどうかを制御します。初期値は「True」です。 <ul style="list-style-type: none"> • True - 高いプライオリティのバックアップルータはマスタールータに代わります。 • False - 高いプライオリティのバックアップルータはマスターに代わることはできません。本設定はグループ内で統一させる必要があります。 |
| Critical IP Address | 本仮想ルータから、インターネットやクリティカルなネットワークへ最も直接的なルートを提供する物理デバイスの IP アドレスを入力します。本アドレスは、ネットワーク上のデバイスの物理アドレスである必要があります。仮想ルータから本 IP アドレスへの接続がダウンすると、仮想ルータは自動的にダウンします。この場合、VRRP グループ内のバックアップルータから新しいマスターが選出されます。VRRP グループ内の別のルータには異なる Critical IP Address を指定できます。それによりインターネットやクリティカルなネットワークに複数のルートを定義することができます。 |
| Checking Critical IP | クリティカルな IP アドレスのステータス (Active または Inactive) をチェックする状態を指定します。 |

「Add」ボタンをクリックして、新しいエントリを追加します。

エントリの編集

1. 「Edit」ボタンをクリックすると、以下の画面が表示されます。

VRRP Virtual Router Settings

Interface Name: System VRID (1-255): 1

IP Address: 10.90.90.90 State: Disabled

Priority (1-254): 255 Advertisement Interval (1-255): 1 sec

Preempt Mode: True Critical IP Address: 10.2.2.2

Checking Critical IP: Disabled [Apply]

VRRP Virtual Router Detail Information

| | | | |
|----------------------|-------------------|------------------------|-------------------|
| Interface Name | System | Authentication Type | No Authentication |
| VRID | 1 | Virtual IP Address | 10.90.90.90 |
| Virtual MAC Address | 00-00-5E-00-01-01 | Virtual Router State | Initialize |
| State | Disabled | Priority | 255 |
| Master IP Address | 10.90.90.90 | Critical IP Address | 10.2.2.2 |
| Checking Critical IP | Disabled | Advertisement Interval | 1 sec |
| Preempt Mode | True | Virtual Router Up Time | 0 centi-sec |

[<<Back]

図 9-24 VRRP Virtual Router Settings – Edit 画面

2. エントリの編集を行い、「Apply」ボタンをクリックします。

エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。「Delete All」ボタンをクリックして、表示されたすべてのエントリを削除します。

「<<Back」をボタンをクリックして前のページに戻ります。

VRRP Authentication Settings (VRRP 認証設定)

インタフェースにおける仮想ルータの認証設定を行います。

L3 Features > VRRP > VRRP Authentication Settings の順にメニューをクリックし、以下の画面を表示します。

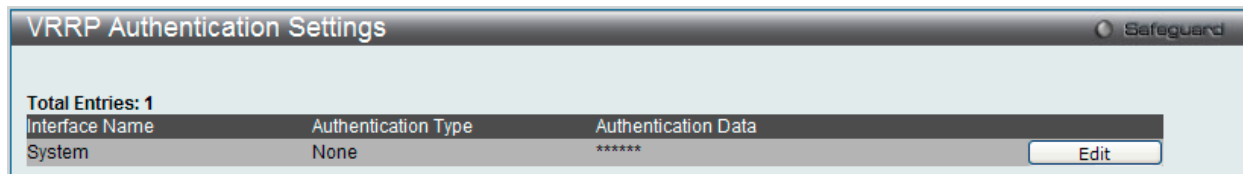


図 9-25 VRRP Authentication Settings 画面

1. 「Edit」ボタンをクリックすると、以下の画面が表示されます。

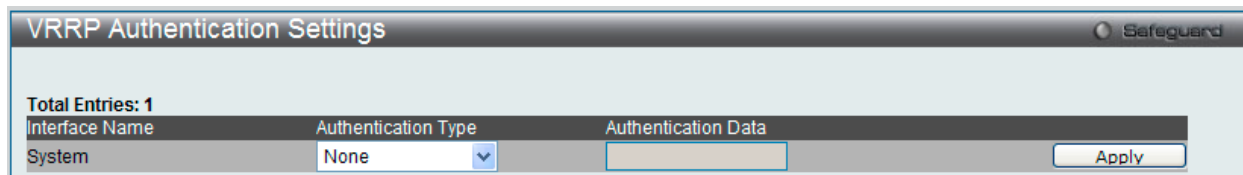


図 9-26 VRRP Authentication Settings – Edit 画面

以下の項目が表示されます。

| 項目 | 説明 |
|---------------------|---|
| Interface Name | VRRP 認証情報を設定する IP インタフェース名です。 |
| Authentication Type | VRRP 認証タイプを指定します。「None」、「Simple」または「IP」を選択します。 <ul style="list-style-type: none"> • None - VRRP プロトコル交換は認証されないことを意味します。 • Simple - Authentication フィールドへのシンプルパスワード設定が必要になります。ルータが受信した VRRP メッセージを照合するデータフィールド。2つのパスワードが正確に一致しない場合、パケットは破棄されます。 • IP- ルータが受信した VRRP メッセージを照合する認証のために IP 設定が必要になります。2つの値が正確に一致しない場合、パケットは破棄されます。 |
| Authentication Data | 本欄は、「Authentication Type」欄で「Simple」または「IP」が指定されている場合に有効です。「Simple」と「IP」認証アルゴリズムで使用する認証データを指定します。同じ IP インタフェースに所属する全ルータが同じ設定を行う必要があります。 <ul style="list-style-type: none"> • Simple - ルータが受信した VRRP パケットを識別するために 8 文字以内の半角英数字を入力します。 • IP - ルータが受信した VRRP パケットを照合するために 16 文字以内の半角英数字を入力します。 |

2. エントリの編集を行い、「Apply」ボタンをクリックします。

第 10 章 QoS (QoS 機能の設定)

以下は QoS サブメニューの説明です。
必要に応じて、設定 / 変更 / 修正を行ってください。

| サブメニュー | 説明 | 参照ページ |
|--|--|---------------------|
| 802.1p Settings (802.1p 設定) | ポート単位にプライオリティを割り当てます。以下のメニューがあります。 802.1p Default Priority Settings (ポートへのパケットプライオリティの割り当て)、802.1p User Priority Settings (802.1p ユーザプライオリティ) | 226 |
| Bandwidth Control (帯域幅の設定) | 送信と受信のデータレートを制限します。以下のメニューがあります。 Bandwidth Control Settings (帯域幅の設定)、Queue Bandwidth Control Settings (キュー帯域幅制御の設定) | 227 |
| Traffic Control Settings (トラフィックコントロールの設定) | ストームコントロールの有効 / 無効の設定、およびマルチキャスト、ブロードキャストストームのしきい値を調整します。 | 229 |
| DSCP (DSCP 設定) | DSCP の設定を行います。以下のメニューがあります。 DSCP Trust Settings (DSCP トラスト設定)、DSCP Map Settings (DSCP マップ設定) | 231 |
| HOL Blocking Prevention (HOL ブロッキング防止) | HOL ブロッキング防止機能を有効または無効にします。 | 232 |
| Scheduling Settings (スケジューリングの設定) | QoS スケジューリングを設定します。以下のメニューがあります。 QoS Scheduling (QoS スケジュール作成)、QoS Scheduling Mechanism (QoS スケジュールメカニズム設定) | 232 |
| WRED (WRED 設定) | WRED の状態とそのポート設定を行います。 | 234 |

本スイッチシリーズは、802.1p プライオリティキューイング QoS(Quality of Service) をサポートしています。以下の項では QoS の機能と、802.1p プライオリティキューイングを利用するメリットについて説明します。

QoS の長所

QoS は IEEE 802.1p 標準で規定される技術で、ネットワーク管理者に、VoIP (Voice-over Internet Protocol)、Web 閲覧用アプリケーション、ファイルサーバアプリケーション、またはビデオ会議などの広帯域を必要とする、または高い優先順位を持つ重要なサービスのために、帯域を予約する方法を提供します。より大きい帯域を作成可能だけでなく他の重要度の低いトラフィックを制限することで、ネットワークが必要以上の帯域を使用しないようにします。スイッチは各物理ポートで受信した様々なアプリケーションからのパケットをプライオリティに基づき独立したハードウェアキューに振り分けます。以下の図に、802.1p プライオリティキューイングがどのように本スイッチに実装されているかを示しています。

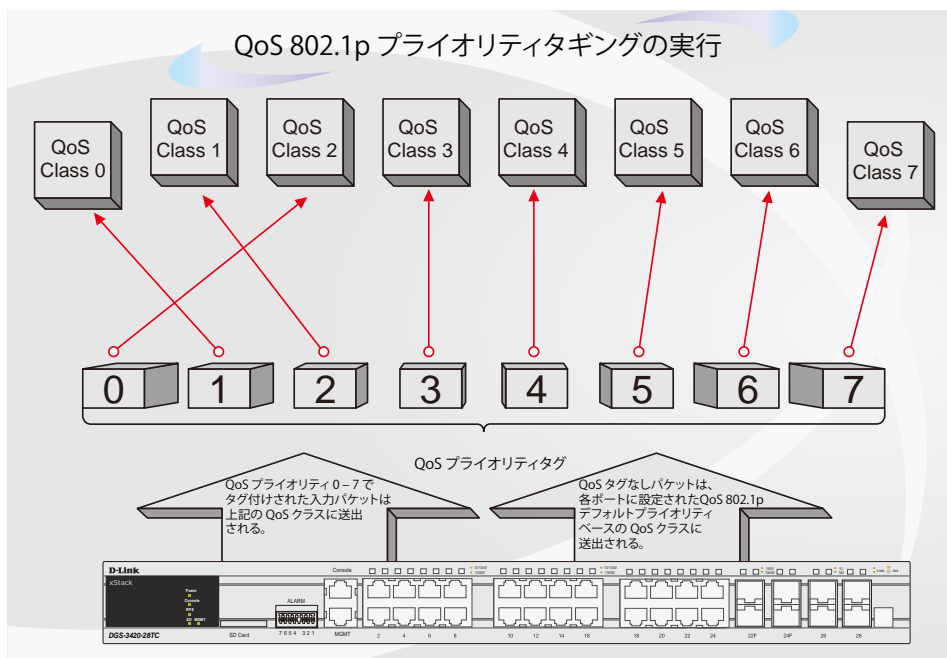


図 10-1 スイッチ上での QoS マッピングの例

上の図は本スイッチのプライオリティの初期設定です。クラス-7は、スイッチ上における7つのプライオリティキューの中で、最も高い優先権を持っています。QoS を実行するためには、ユーザはスイッチに対し、パケットのヘッダに適切な識別タグが含まれているかを確認するように指示する必要があります。そして、ユーザはそれらのタグ付きパケットをスイッチ上の指定されたキューに送り、優先順序に従って送出するようにします。

例えば、遠隔地に設置した2台のコンピュータ間でビデオ会議を行うとします。管理者は Access Profile コマンドを使用して、送信するビデオパケットにプライオリティタグを付加します。次に受信側ではスイッチにそのタグの確認するよう指示を行い、タグ付きパケットを受信したら、それをスイッチのクラスキューに関連付けを行うようにします。また、管理者はこのキューに優先順位を与え、他のパケットが送出されるよりも前に送信されるように設定を行います。この結果、このサービス用のパケットは、できるだけ早く送信され、キューが最優先されることにより、中断されことなくパケットを受け取ることができるため、このビデオ会議用に帯域を最適化することが可能になります。

QoS について

本スイッチには、4つのプライオリティキューがあります。プライオリティキューには、最高レベルの7番(クラス7)から最低レベルの0番(クラス0)まであります。IEEE 802.1pに規定される8つのプライオリティタグはスイッチのプライオリティタグと以下のように関連付けされます。

- ・ プライオリティ 0 は、スイッチの Q2 キューに割り当てられます。
- ・ プライオリティ 1 は、スイッチの Q0 キューに割り当てられます。
- ・ プライオリティ 2 は、スイッチの Q1 キューに割り当てられます。
- ・ プライオリティ 3 は、スイッチの Q3 キューに割り当てられます。
- ・ プライオリティ 4 は、スイッチの Q4 キューに割り当てられます。
- ・ プライオリティ 5 は、スイッチの Q5 キューに割り当てられます。
- ・ プライオリティ 6 は、スイッチの Q6 キューに割り当てられます。
- ・ プライオリティ 7 は、スイッチの Q7 キューに割り当てられます。

Strict (絶対優先)のプライオリティベースのスケジューリングでは、優先度の高いキューに属するパケットから送信されます。優先度の高いキューが複数ある場合は、プライオリティタグに従って送信されます。高プライオリティのキューが空である時にだけプライオリティの低いパケットは送信されます。

重み付けラウンドロビンキューイングでは、各プライオリティキューから送信されるパケットの数は、指定された重み付けによって決定されます。A から H までの 8 つある CoS キューに、8 から 1 までの重み付けを設定したとすると、パケットは以下の順に送信されます。: A1, B1, C1, D1, E1, F1, G1, H1, A2, B2, C2, D2, E2, F2, G2, A3, B3, C3, D3, E3, F3, A4, B4, C4, D4, E4, A5, B5, C5, D5, A6, B6, C6, A7, B7, A8, A1, B1, C1, D1, E1, F1, G1, H1。

重み付けラウンドロビンキューイングでは、各QoSキューが同じ重み付けを持つならば、各QoSキューのパケット送信の機会はラウンドロビンキューイングのように、全く同じになります。また、あるCoSの重み付けとして0を設定すると、そのCoSから送信するパケットがなくなるまでパケットを処理します。0以外の値を持つ他のCoSキューでは、重み付けラウンドロビンの規則により、重みに従って送信を行います。

本スイッチは、スイッチ上の各ポートに8つのプライオリティキュー(と8つのCoS)を持っています。

802.1p Settings (802.1p 設定)

802.1p Default Priority Settings (ポートへのパケットプライオリティの割り当て)

本スイッチは、各ポートにデフォルトの 802.1p プライオリティを割り当てることができます。

本画面では、スイッチのそれぞれのポートにデフォルトの 802.1p プライオリティを割り当てて、受信したタグなしパケットに 802.1p プライオリティタグを挿入します。プライオリティと有効なプライオリティタグは、最低の 0 から最高の 7 まで指定できます。有効なプライオリティは、RADIUS に割り当てられた実際のプライオリティを示しています。RADIUS が割り当てた値が指定した制限を超えると、値はデフォルトプライオリティに設定されます。例えば、RADIUS が制限値に 8、デフォルトプライオリティに 0 を割り当てている場合、有効なプライオリティは 0 になります。

QoS > 802.1p Settings > 802.1p Default Priority Settings の順にクリックし、以下の画面を表示します。

| Port | Priority | Effective Priority |
|------|----------|--------------------|
| 1 | 0 | 0 |
| 2 | 0 | 0 |
| 3 | 0 | 0 |
| 4 | 0 | 0 |
| 5 | 0 | 0 |
| 6 | 0 | 0 |
| 7 | 0 | 0 |
| 8 | 0 | 0 |
| n | n | n |

図 10-2 802.1p Default Priority Settings 画面

新しいデフォルトプライオリティを実行するためには、はじめに「From」、「To」プルダウンメニューでポート範囲を選択し、「Priority」プルダウンメニューで値 0 から 7 を選択します。「Apply」ボタンをクリックして行った変更を適用します。

本画面には以下の項目があります。

| 項目 | 説明 |
|---------------------|------------------------------|
| Unit | 設定するユニットを選択します。 |
| From Port / To Port | 使用する開始 / 終了ポートを選択します。 |
| Priority | プルダウンメニューを使用して、0-7 の値を選択します。 |

「Apply」ボタンをクリックして行った変更を適用します。

802.1p User Priority Settings (802.1p ユーザプライオリティ)

スイッチは各 802.1p プライオリティにユーザプライオリティを割り当てることができます。

QoS > 802.1p Settings > 802.1p User Priority Settings の順にクリックし、以下の画面を表示します。

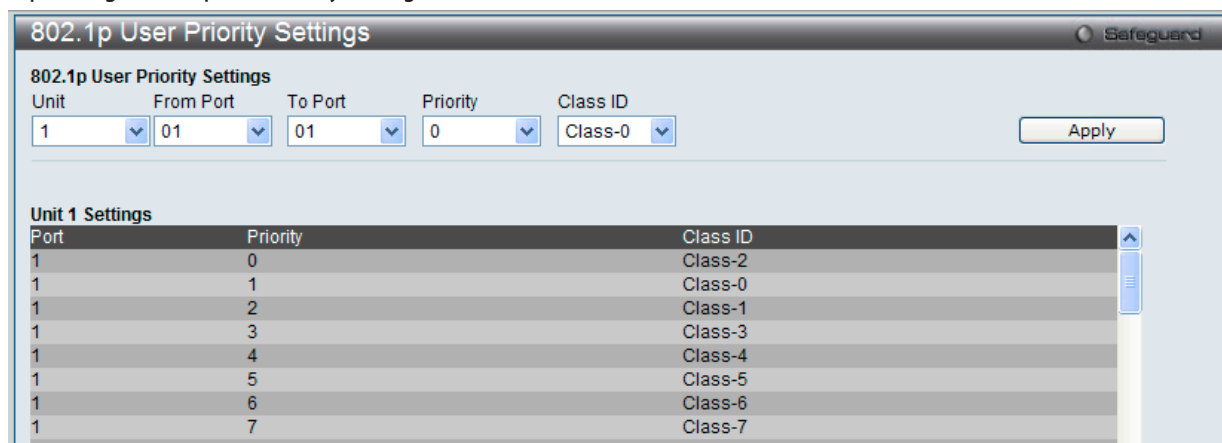


図 10-3 802.1P User Priority Settings 画面

スイッチのポートグループにプライオリティを割り当てると、本画面のプルダウンメニューを使用して 802.1p プライオリティの 8 レベルのそれぞれに対してクラスを設定することができます。ユーザプライオリティのマッピングは最後のページで設定したデフォルトプライオリティに対するだけでなく、802.1p タグを持つすべての入力パケットに対しても行われます。

本画面には以下の項目があります。

| 項目 | 説明 |
|---------------------|--|
| Unit | 設定するユニットを選択します。 |
| From Port / To Port | 設定対象のポート範囲を指定します。 |
| Priority | キューに割り当てられるプライオリティを表示します。 |
| Class ID | プライオリティを割り当てるクラス (キュー) を設定します。「Class-0」(クラス 0) は最も低い優先度のキューで、「Class-3」(クラス 7) が最も高くなります。 |

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

Bandwidth Control (帯域幅の設定)

帯域制御の設定を行うことにより、すべての選択ポートに対して、送信と受信のデータレートを制限することができます。

Bandwidth Control Settings (帯域幅の設定)

「Effective RX Rate」は設定した速度に一致しない場合にスイッチポートの実際の帯域幅を表示します。これは、通常 RADIUS サーバをなどの高優先度を持つリソースが割り当てた速度を表示します。

QoS > Bandwidth Control > Bandwidth Control Settings の順にメニューをクリックし、以下の画面を表示します。



図 10-4 Bandwidth Control Settings 画面

QoS (QoS機能の設定)

以下の項目を設定または表示できます。

| 項目 | 説明 |
|---------------------|---|
| Unit | 設定するユニットを選択します。 |
| From Port / To Port | 設定対象のポート範囲を指定します。 |
| Type | RX (受信)、TX (送信) および Both (両方) から選択します。帯域上限を受信、送信、送受信の両方のいずれに適用するのかが設定します。 |
| No Limit | <p>選択ポートに対する帯域制限を設定します。</p> <ul style="list-style-type: none"> Enabled - ポートで帯域制限を行いません。 Disabled - ポートで帯域制限を行います。(初期値) <p>注意 設定値がポート速度より大きいと、帯域幅制限の意味がなくなります。</p> |
| Rate (8-1024000) | 選択ポートのデータ速度の上限値 (Kbit/秒) を指定します。値は 8 から 1024000 の間で速度を指定します。 |
| Effective RX | RADIUS サーバが RX の帯域幅を割り当てると、それは有効な RX 帯域幅となります。RADIUS サーバを使用した認証は、ポートごとかユーザごとに行われます。ユーザごとの認証のために、指定ポートに複数ユーザが割り当てられていると、割り当てられる RX 帯域幅が複数あります。最終的な RX 帯域幅は、これら複数の RX 帯域幅の中で最も大きいものとなります。 |
| Effective TX | RADIUS サーバが TX の帯域幅を割り当てると、それは有効な TX 帯域幅となります。RADIUS サーバを使用した認証は、ポートごとかユーザごとに行われます。ユーザごとの認証のために、指定ポートに複数ユーザが割り当てられていると、割り当てられる TX 帯域幅が複数あります。最終的な TX 帯域幅は、これら複数の TX 帯域幅の中で最も大きいものとなります。 |

「Apply」 ボタンをクリックし、選択ポートの帯域制御を設定します。設定の結果は、画面下部の「Bandwidth Control Table」に表示されます。

Queue Bandwidth Control Settings (キュー帯域幅制御の設定)

キューの帯域幅を設定します。

QoS > Bandwidth Control > Queue Bandwidth Control Settings の順にメニューをクリックし、以下の画面を表示します。

The screenshot shows the 'Queue Bandwidth Control Settings' window. At the top, there are dropdown menus for 'Unit' (set to 1), 'From Port' (01), 'To Port' (01), 'From Queue' (0), and 'To Queue' (0). There are input fields for 'Min Rate (8-102400000)' and 'Max Rate (8-102400000)', both with 'No Limit' checked. An 'Apply' button is visible. Below the configuration fields, there are three sections for 'Queue Bandwidth Control Table On Port 1', 'Port 2', and 'Port 3'. Each section contains a table with columns 'Queue', 'Min Rate (Kbit/sec)', and 'Max Rate (Kbit/sec)'. All entries in these tables are 'No Limit'.

図 10-5 Queue Bandwidth Control Settings 画面

以下の項目を設定または表示できます。

| 項目 | 説明 |
|------------------------|--|
| Unit | 設定するユニットを選択します。 |
| From Port / To Port | この設定に使用するポート範囲を選択します。 |
| From Queue / To Queue | この設定に使用するキュー範囲を選択します。 |
| Min Rate (8-102400000) | ポートが受信できるパケット制限 (Kbps) を指定します。「No Limit」をチェックすると指定キューが受信するパケットにレート制限がなくなります。 |
| Max Rate (8-102400000) | キューの最大レートを入力します。「No Limit」オプションを選択すると、レート制限はなくなります。 |

「Apply」 ボタンをクリックして行った変更を適用します。

注意 キュー帯域幅制御の最小粒度は 64Kbps です。システムは自動的に 64 倍の数に調整します。

Traffic Control Settings (トラフィックコントロールの設定)

コンピュータネットワーク上にはマルチキャストパケットやブロードキャストパケットなどのパケットが正常な状態でも絶えずあふれています。このトラフィックはネットワーク上の端末の不良や、故障したネットワークカードなどのように誤動作しているデバイスによって増加することもあります。そのため、スイッチのスループットに関する問題が発生し、その結果、ネットワークの全体的なパフォーマンスにも影響する可能性があります。このパケットストームを調整するために、本スイッチは状況を監視し、制御します。

パケットストームを監視し、ユーザが指定したしきい値レベルを基に非常に多くのパケットがネットワークであふれているどうかを判断します。パケットストームが検出されると本スイッチはパケットストームが緩和されるまで受信したパケットを破棄します。この方法を使用するためには以下の画面の「Action」欄の「Drop」オプションを設定します。

トラフィックコントロールに設定したポートで本時間経過後もパケットストームが続くようであれば、そのポートは「Shutdown Forever」(永久シャットダウン)モードに遷移し、トラップレシーバに送信する警告メッセージを生成します。一度「Shutdown Forever」モードに入ると、本ポートを回復する方法は、**System Configuration > Port Configuration > Port Settings**画面で手動により有効状態に戻すか、または「Traffic Auto Recover Time」欄に設定した時間経過後自動的に回復します。無効なポートを選択して、「Status」を「Enabled」ステータスに戻します。このようなストームコントロール機能を利用するためには、次に示す画面の「Action」フィールドで「Shutdown」オプションを選択してください。この画面を使用して、ストームコントロールの有効/無効や、マルチキャストおよびブロードキャストのしきい値の調整を行います。

QoS > Traffic Control Settings の順にクリックし、以下の画面を表示します。

| Port | Traffic Control Type | Action | Broadcast | Multicast | Unicast | Countdown | Interval | Shutdown Forever |
|------|----------------------|--------|-----------|-----------|---------|-----------|----------|------------------|
| 1 | None | Drop | 131072 | 131072 | 131072 | 0 | 5 | |
| 2 | None | Drop | 131072 | 131072 | 131072 | 0 | 5 | |
| 3 | None | Drop | 131072 | 131072 | 131072 | 0 | 5 | |
| 4 | None | Drop | 131072 | 131072 | 131072 | 0 | 5 | |

図 10-6 Traffic Control Settings 画面

本画面には次の項目があります。

| 項目 | 説明 |
|--------------------------|---|
| Traffic Control Settings | |
| Unit | 設定するユニットを選択します。 |
| From Port / To Port | ストームコントロールを表示するポート範囲を設定します。 |
| Action | <p>トラフィックコントロールの方法をプルダウンメニューで指定します。以下の方法を指定できます。</p> <ul style="list-style-type: none"> Drop – スwitchのハードウェアによるトラフィックコントロールを行います。選択すると、switchのハードウェアが指定したしきい値に基づくパケットストームの検知を行い、パケットストームが発生すると、状態が改善するまでパケットの廃棄を行います。 Shutdown – switchのソフトウェアによるトラフィックコントロールにより、トラフィックストームの発生を検知します。ストームが検出されると、switchはスパンニングツリーの保持に必要である STP BPDU パケットを除くすべてのトラフィックの入力に対して、ポートをシャットダウンします。カウントタイム経過後もパケットストームが続くようであれば、そのポートは「Shutdown Forever」(永久シャットダウン)モードに遷移し、5分後自動的にポートが回復するまで操作できません。本ポートを通常の状態に戻すには、System Configuration > Port Configuration > Port Settings画面で、無効になっているポートを手動で有効状態に戻します。本オプションを選択する際は、switchのチップからパケットカウントを受け取ってパケットストームの発生を検知するために必要な「Time Interval」の設定も必要となります。 |
| Countdown (0 or 3-30) | 本値はswitchがトラフィックストームが発生中のポートをシャットダウンするまでに待機する時間(分)を表します。本値は、「Action」で「Shutdown」を指定し、ハードウェアによるトラフィックコントロールを行わない場合に有効です。0、3-30(分)が指定できます。「Disabled」をチェックして、ストームを削除すると直ちにポートはシャットダウンされます。 |

QoS (QoS機能の設定)

| 項目 | 説明 |
|-------------------------------------|--|
| Time Interval (5-600) | スイッチのチップからトラフィックコントロール機能に送信する、マルチキャストおよびブロードキャストパケットカウントの送信間隔を指定します。このパケットカウントにより、いつ入力パケットがしきい値を超過したかの検出が行われます。値の範囲は 5-600 で、初期値は 5 (秒) です。 |
| Threshold (0-255000) | トラフィックコントロール機能を起動させるトリガーとなる、1 秒あたりの最大パケット数。設定可能なしきい値の範囲は 0-255000 です。初期値は 131072 パケット / 秒です。 |
| Traffic Control Type | 検知の対象となるストームの種類を選択します。 Broadcast、Multicast、Unknown Unicast、Broadcast + Multicast、Broadcast + Unknown Unicast、Multicast + Unknown Unicast、Broadcast + Multicast + Unknown Unicast、または None |
| Broadcast (0-255000) | ストームトラフィック判断のトリガとなる「ブロードキャスト数 / 秒」を指定します。0 から 255000 で指定できます。 |
| Multicast (0-255000) | ストームトラフィック判断のトリガとなる「マルチキャスト数 / 秒」を指定します。0 から 255000 で指定できます。 |
| Unicast (0-255000) | ストームトラフィック判断のトリガとなる「ユニキャスト数 / 秒」を指定します。0 から 255000 で指定できます。 |
| Traffic Trap Settings | トラフィックコントロール機能によるトラフィックストームの扱いを指定します。 <ul style="list-style-type: none"> • None - トラフィックコントロールメカニズムの動作に関わらず、ストームトラップメッセージを送信しません。 • Storm Occurred - ストームトラップ発生時にストームトラップ警告メッセージを送信します。 • Storm Cleared - スイッチがストームトラップを消失させた時ストームトラップメッセージを送信します。 • Both - ストームトラップ発生時と消失時にストームトラップメッセージを送信します。 本機能は、ハードウェアモード中(「Action」で「Drop」が選択された時)は実行できません。 |
| Traffic Log Settings | プルダウンメニューを使用して、本機能を「Enabled」(有効)/「Disabled」(無効)にします。ログ状態が有効な場合、ストームが発生した場合やストームがクリアされた場合にトラフィックコントロール状態がログに出力されます。ログ状態が無効な場合、トラフィックコントロールイベントはログに出力されません。 |
| Traffic Auto Recover Time (0-65535) | ポートがシャットダウンからの自動回復を許可する時間を入力します。初期値は 0 で、自動回復モードが無効で、永久にシャットダウンするということを意味します。ポートをフォワーディング状態に戻すためには、 System Configuration > Port Configuration > Port Settings 画面で手動の設定が必要です。 |

注意 トラフィックコントロールは、リンクアグリゲーション (ポートトランッキング) が設定されたポートに対しては行うことができません。

注意 「Shutdown Forever」モードのポートは、スイッチの CPU に BPDU 送信を行いますが、「Spanning Tree」画面では「Discarding」状態として表示されます。

注意 「Shutdown Forever」モードのポートは、ユーザがポートの復旧を行うまでの間はリンクダウン状態として表示されます。

注意 最小のストームコントロールしきい値のグラニュラリティは 0 です。

DSCP (DSCP 設定)

DSCP Trust Settings (DSCP トラスト設定)

本スイッチにおけるポートへの DSCP トラスト設定機能を有効にします。ポートが DSCP トラストモードにある場合、スイッチはデフォルトポートプライオリティの代わりに DSCP Map を使用してプライオリティタグをタグなしパケットに挿入します。

QoS > DSCP > DSCP Trust 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。

| Port | DSCP Trust |
|------|------------|
| 1 | Disabled |
| 2 | Disabled |
| 3 | Disabled |
| 4 | Disabled |
| 5 | Disabled |
| 6 | Disabled |

図 10-7 DSCP Trust Settings 画面

「Unit」で設定するユニット、「From Port」および「To Port」で有効にするポートを選択し、その「State」を選択して「Apply」ボタンをクリックします。

DSCP Map Settings (DSCP マップ設定)

本スイッチにおける DSCP マップ設定機能を有効にします。ポートが DSCP トラストモードの場合、キューへの DSCP マッピングでパケットの優先値は決定します (スケジューリングキューも決定する)。「DSCP-to-DSCP」マッピングはパケットがポートに入る時に、パケットの DSCP を交換する機能です。新しい DSCP に基づきパケットのプロセスは残ります。初期値では DSCP は同じ DSCP にマッピングされます。

QoS > DSCP > DSCP Map 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。

| Port | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|------|-----|------|-------|-------|-------|-------|-------|-------|
| 1 | 0-7 | 8-15 | 16-23 | 24-31 | 32-39 | 40-47 | 48-55 | 56-63 |
| 2 | 0-7 | 8-15 | 16-23 | 24-31 | 32-39 | 40-47 | 48-55 | 56-63 |
| 3 | 0-7 | 8-15 | 16-23 | 24-31 | 32-39 | 40-47 | 48-55 | 56-63 |
| 4 | 0-7 | 8-15 | 16-23 | 24-31 | 32-39 | 40-47 | 48-55 | 56-63 |

図 10-8 DSCP Map Settings - DSCP Priority 画面

QoS > DSCP > DSCP Map Settings の順にメニューをクリックし、「DSCP Map」のメニューから「DSCP DSCP」を選択すると以下の画面を表示します。

| Port 1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|--------|----|----|----|----|----|----|----|----|----|----|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 1 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 |
| 2 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 |
| 3 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 |
| 4 | 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 |

図 10-9 DSCP Map Settings DSCP to DSCP 画面

本画面には以下の項目があります。

| 項目 | 説明 |
|-------------------|---|
| Unit | 設定するユニットを指定します。 |
| From Port/To Port | 設定の対象となるポートを指定します。 |
| DSCP Map | プルダウンメニューを使用して、DSCP マップ (DSCP Priority、DSCP DSCP) を選択します。 |
| DSCP List (0-63) | DSCP リストの値を入力します。0 から 63 の範囲で設定します。 |
| Priority | スイッチに設定済みの 802.1p デフォルトプライオリティ (パケットが送られる CoS キューを決定するために使用) の設定を書き換える場合に使用します。本フィールドを選択すると、スイッチが受信したパケットの中の、本プライオリティに一致するパケットは、既に指定した CoS キューに送られます。 |
| DSCP (0-63) | DSCP 値を入力します。これは、「DSCP MAP」で「DSCP DSCP」を選択した場合にのみ表示されます。 |
| Port | プルダウンメニューでポートを選択します。 |

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

HOL Blocking Prevention (HOL ブロッキング防止)

HOL (Head of Line) ブロッキングはブロードキャストまたはマルチキャストパケットの送信先ポートの1つが使用中である場合に発生します。スイッチはバッファにこのパケットを保持し、一方他の送信先ポートは使用中でなくてもパケットを送信しません。HOL ブロッキング防止機能は、より低い待ち時間と、より高い性能を持つために、使用中のポートを無視して、直接パケットを転送します。HOL ブロッキング防止機能を有効または無効にします。

QoS > HOL Blocking Prevention の順にクリックし、以下の画面を表示します。

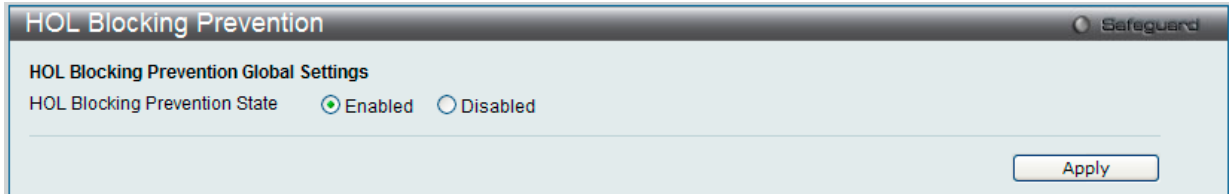


図 10-10 HOL Blocking Prevention 画面

HOL ブロッキング防止のグローバル設定を有効または無効にします。

本画面には以下の項目があります。

| 項目 | 説明 |
|-------------------------------|-----------------------------------|
| HOL Blocking Prevention State | HOL ブロッキング防止のグローバル設定を有効または無効にします。 |

「Apply」 ボタンをクリックして行った変更を適用します。

Scheduling Settings (スケジューリング設定)

QoS Scheduling (QoS スケジューリング作成)

スイッチで利用可能な 8 個のハードウェアキューの 1 つに入力パケットの 802.1p ユーザプライオリティに基づいてポートごとに入力パケットを照合する方法を設定します。

QoS > Scheduling Settings > QoS Scheduling の順にメニューをクリックし、以下の画面を表示します。

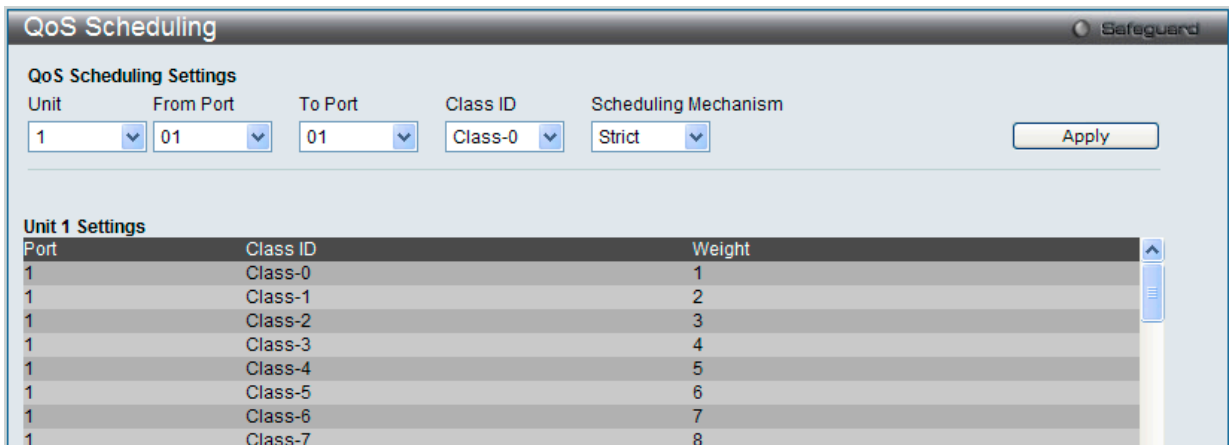


図 10-11 QoS Scheduling 画面

本画面には以下の項目があります。

| 項目 | 説明 |
|----------------------|---|
| Unit | 設定するユニットを選択します。 |
| From Port / To Port | 設定対象のポート (範囲) を指定します。 |
| Class ID | QoS パラメータに設定するクラス ID を 0 から 7 の範囲で指定します。 |
| Scheduling Mechanism | <ul style="list-style-type: none"> Strict - 上位の CoS キューからトラフィックを処理します。上位キューの送信が完了するまで下位キューからはパケットは送信されません。 Weight - プライオリティのサービスクラスで配分されたパケットを重み付けされたラウンドロビン (WRR) アルゴリズムによって処理します。 |

「Apply」 ボタンをクリックして行った変更を適用します。

QoS Scheduling Mechanism (QoS スケジュールメカニズム設定)

QoS のカスタマイズは、スイッチのハードウェアキューに使用する出力スケジュールを変更することにより実行できます。QoS 設定の変更は、どのような変更であっても気をつけて行う必要がありますが、特に優先度の低いキューでのネットワークトラフィックへの影響に注意が必要です。スケジュールの変更により、許容範囲外のパケットロスや重大な伝送遅延が発生することがあります。不適切な QoS 設定により急激なボトルネックが引き起こされる場合があるため、本設定をカスタマイズする際、特にトラフィックのピーク時には、ネットワークパフォーマンスをモニタしながら行うことが重要です。

QoS > Scheduling Settings > QoS Scheduling Mechanism の順にクリックし、以下の画面を表示します。

| QoS Scheduling Mechanism Settings | | | |
|--------------------------------------|-----------|---------|----------------------|
| Unit | From Port | To Port | Scheduling Mechanism |
| 1 | 01 | 01 | Strict |
| <input type="button" value="Apply"/> | | | |
| Unit 1 Settings | | | |
| Port | Mode | | |
| 1 | Strict | | |
| 2 | Strict | | |
| 3 | Strict | | |
| 4 | Strict | | |
| 5 | Strict | | |
| 6 | Strict | | |
| 7 | Strict | | |
| 8 | Strict | | |

図 10-12 Scheduling Profile Settings 画面

本画面には以下の項目があります。

| 項目 | 説明 |
|----------------------|---|
| Unit | 設定するユニットを選択します。 |
| From Port / To Port | 設定対象のポート (範囲) を指定します。 |
| Scheduling Mechanism | 2つのスケジューリングメカニズムの1つを選択します。 <ul style="list-style-type: none"> • Strict - 上位の CoS キューからトラフィックを処理します。上位キューの送信が完了するまで下位キューからはパケットは送信されません。 • Weight Round Robin - プライオリティ CoS で配分されたパケットを重み付けされたラウンドロビン (WRR) アルゴリズムによって処理します。 |

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

注意 キューに割り当てる 0 から 7 の番号は IEEE 802.1p プライオリティタグの番号を表しています。ポート番号の指定ではない点にご注意ください。

WRED (WRED 設定)

WRED Port Settings (WRED ポート設定)

WRED の状態とそのポート設定を行います。

QoS > WRED > WRED Port Settings の順にメニューをクリックし、以下の画面を表示します。

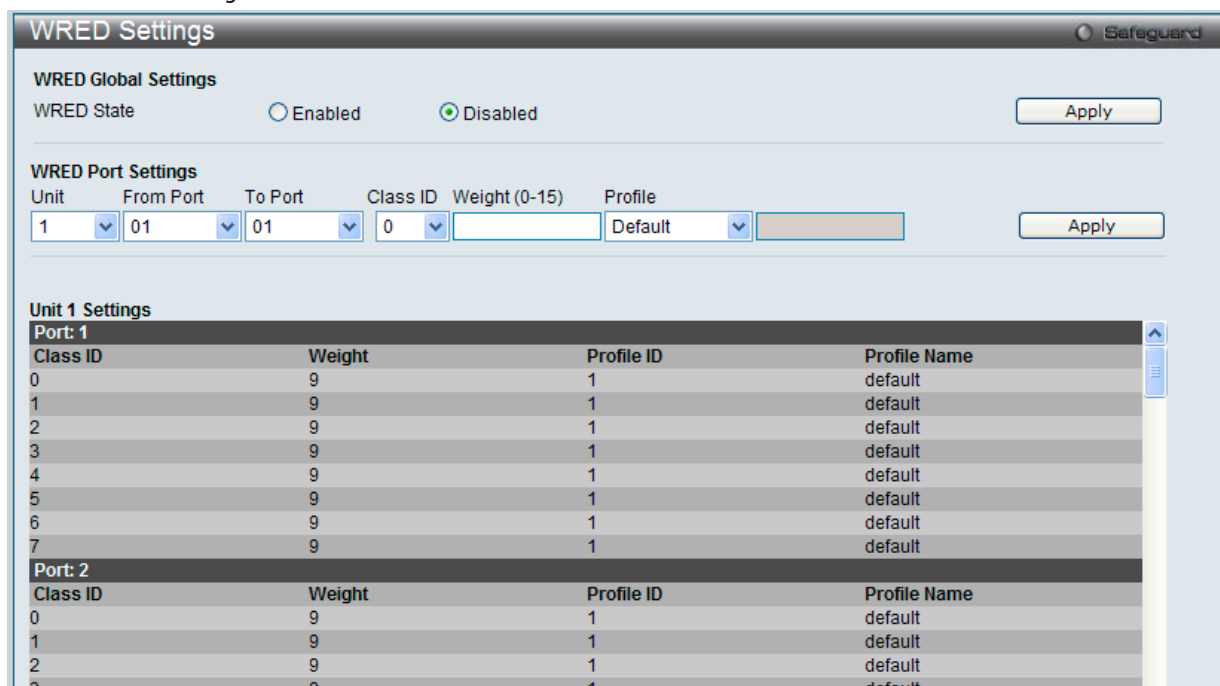


図 10-13 WRED Settings 画面

本画面には以下の項目があります。

| 項目 | 説明 |
|----------------------|--|
| WRED Global Settings | |
| WRED State | WRED グローバル状態を有効または無効にします。 |
| WRED Port Settings | |
| Unit | 設定するユニットを選択します。 |
| From Port / To Port | この設定に使用するポート範囲を選択します。 |
| Class ID | プルダウンメニューを使用してハードウェアの優先度を選択します。 |
| Weight (0-15) | 通常のキューサイズ計算における重み付けを指定します。 |
| Profile | プルダウンメニューを使用して、WRED ポートとキューに使用するプロファイルを選択します。 <ul style="list-style-type: none"> Default - 使用するプロファイルの初期値を指定します。 Profile ID - 選択して、使用するプロファイル ID を指定します。 Profile Name - 選択して、使用するプロファイル名を指定します。 |

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

WRED Profile Settings (WRED プロファイル設定)

WRED プロファイル設定を行います。

QoS > WRED > WRED Profile Settings の順にメニューをクリックし、以下の画面を表示します。

WRED Profile Settings

Create WRED Profile

Profile ID (2-128) Profile Name (Max: 32 characters)

Add Delete Delete All

Configure WRED Profile

Profile Packet Type Packet Colour Min Threshold (0-100) Max Threshold (0-100) Max Drop Rate (0-100)

Default TCP Green 50 100 50

Apply

WRED ProfileTable

Profile

Default Find

Total Current Profile Number: 1

| WRED Profile ID: 1 | Profile Name: default | | |
|--------------------|-----------------------|---------------|---------------|
| Packet Type | Min-Threshold | Max-Threshold | Max-Drop-Rate |
| TCP-Green | 50 | 100 | 50 |
| TCP-Yellow | 50 | 100 | 50 |
| TCP-Red | 50 | 100 | 50 |
| Non-TCP-Green | 50 | 100 | 50 |
| Non-TCP-Yellow | 50 | 100 | 50 |
| Non-TCP-Red | 50 | 100 | 50 |

図 10-14 WRED Profile Settings 画面

本画面には以下の項目があります。

| 項目 | 説明 |
|------------------------|--|
| Create WRED Profile | |
| Profile ID (2-128) | 追加または削除する WRED プロファイル ID を入力します。 |
| Profile Name | 追加または削除する WRED プロファイル名を入力します。 |
| Configure WRED Profile | |
| Profile | プルダウンメニューを使用して、WRED ポートとキューに使用するプロファイルを選択します。 <ul style="list-style-type: none"> Default - 使用するプロファイルの初期値を指定します。 Profile ID - 選択して、使用するプロファイル ID を指定します。 Profile Name - 選択して、使用するプロファイル名を指定します。 |
| Packet Type | 破棄するパケットタイプ (TCP または Non-TCP) を選択します。 |
| Packet Colour | 破棄するパケットカラー (Green、Yellow または Red) を選択します。 |
| Min Threshold (0-100) | 使用するしきい値 (最小) を入力します。キューサイズがこの値より高いと、カラー「Yellow」が割り当てられます。キューサイズがこの値より低いと、カラー「Green」が割り当てられ、破棄されないことを保証されます。「Yellow」パケットの動作は、このカラーのプロファイル設定に依存します。 |
| Max Threshold (0-100) | 使用するしきい値 (最大) を入力します。キューサイズがこの値より低いと、カラー「Yellow」が割り当てられます。キューサイズがこの値より高いと、カラー「Red」が割り当てられ、破棄されます。「Yellow」パケットの動作は、このカラーのプロファイル設定に依存します。 |
| Max Drop Rate (0-100) | 最大の破棄レートの値を入力します。 |

「Add」ボタンをクリックして、入力した情報に基づいて新しいエントリを追加します。

「Delete」ボタンをクリックして、入力した情報に基づいてエントリを削除します。

「Delete All」ボタンをクリックして、表示されたすべてのエントリを削除します。

「Apply」ボタンをクリックして行った変更を適用します。

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

第 11 章 ACL (ACL 機能の設定)

ACL メニューを使用し、本スイッチにアクセスプロファイルおよびルールを設定を行うことができます。

以下は、ACL サブメニューの説明です。
必要に応じて、設定 / 変更 / 修正を行ってください。

| サブメニュー | 説明 | 参照ページ |
|---|--|---------------------|
| ACL Configuration Wizard (ACL 設定ウィザード) | ウィザードを使用してアクセスプロファイルとルールを作成します。 | 236 |
| Access Profile List (アクセスプロファイルリスト) | パケットヘッダに含まれる情報に基づくパケット転送可否の基準を設定するプロファイルを設定します。 | 238 |
| CPU Access Profile List (CPU アクセスプロファイルリスト) | CPU インタフェースフィルタリング機能を設定します。 | 255 |
| ACL Finder (ACL 検索) | ACL エントリを検索します。 | 270 |
| ACL Flow Meter (ACL フローメータ) | フローごとの帯域幅制御設定を行います。 | 271 |
| Egress Access Profile List (Egress アクセスプロファイルリスト) | フローごとのパケット処理を実行します。 | 275 |
| Egress ACL Flow Meter (Egress ACL フローメータリング) | Egress アクセスプロファイルおよびルールに基づいてパケットフローベースのメータリングを設定します。 | 288 |

ACL Configuration Wizard (ACL 設定ウィザード)

ACL 設定ウィザードは、必要なアドレスやサービスタイプおよび操作を簡単に入力することで自動的にアクセスプロファイルと ACL ルールを作成します。管理者の多くの時間を節約します。

ACL > ACL Configuration Wizard の順にメニューをクリックし、以下の画面を表示します。

図 11-1 ACL Configuration Wizard 画面

1. ACL の種類 (Normal または CPU) を選択します。「Normal」を選択すると、スイッチのインタフェースの 1 つに受信したパケットに適用される ACL ルールを作成します。「CPU」を選択すると、スイッチに送信されるパケットにだけ適用される ACL ルールを作成します。
2. Profile ID (1-6) と Access ID (1-256) を割り当てるか、またはこれを自動的に行うために「Auto Assign」欄をチェックします。
3. 範囲を From (Any、MAC Address、IPv4 Address または IPv6) と To (Any、MAC Address、IPv4 Address) から選択します。
4. 「Action」を「Permit」、「Deny」または「Mirror」から選択します。
5. 「Option」を「Change IP Priority」、「Replace DSCP」または「Replace ToS Precedence」から選択し、隣接している欄に 0-7 の値を入力します。
6. 新しい ACL ルール用のポートを「Ports」横の欄に入力し、「Apply」ボタンをクリックして設定を適用します。

以下の項目を使用して、設定を行います。

| 項目 | 説明 |
|-------------------|---|
| Type | プルダウンメニューを使用して以下の ACL ルールタイプを選択します。 <ul style="list-style-type: none"> • Normal - ノーマル ACL ルールを作成します。 • CPU - CPU ACL ルールを作成します。 • Egress - Egress ACL ルールを作成します。 |
| Profile Name | 「Normal」タイプルールを選択後、新しいルールに対するプロファイル名を入力します。 |
| Profile ID (1-6) | 新しいルールに対するプロファイル ID を入力します。 |
| Access ID (1-256) | 新しいルールに対するアクセス ID を入力します。「Auto Assign」オプションを選択すると、このルールに対して自動的に未使用のアクセス ID を割り当てます。 |
| From / To | 以下の 4 つの異なるカテゴリに適用するためにこのルールを作成します。 <ul style="list-style-type: none"> • Any - あらゆる開始カテゴリをこのルールに含めます。 • MAC Address - このルールに MAC アドレス範囲を入力します。 • IPv4 Address - このルールに IPv4 アドレス範囲を入力します。 • IPv6 - このルールに IPv6 アドレス範囲を入力します。 |
| Action | <ul style="list-style-type: none"> • Permit- スイッチはアクセスプロファイルに一致するパケットの送信を、以下のフィールドで設定する追加のルールに従って行います。 • Deny- スイッチはアクセスプロファイルに一致するパケットを送信せずにフィルタリングします。 • Mirror- スイッチはアクセスプロファイルに一致するパケットをミラーポートセクションで定義したポートにミラーリングします。ポートミラーリングが有効で、ターゲットポートが設定されている必要があります。 |
| Option | 「Permit」アクション選択後、以下のオプションの 1 つを選択します。 <ul style="list-style-type: none"> • Change 1p Priority - 802.1p プライオリティ値を入力します。 • Replace DSCP - DSCP 値を入力します。 • Replace ToS Precedence - ToS 優先度値を入力します。 |
| Apply To | このルールに適用するオブジェクトの選択または入力を行います。 <ul style="list-style-type: none"> • Ports - ポート番号またはポート範囲を入力します。 • VLAN Name - VLAN 名を入力します。 • VLAN ID - VID を入力します。 |

「Apply」ボタンをクリックして行った変更を適用します。

注意 スイッチはユーザが入力するすべての項目をカバーするために最小限のマスクを使用しますが、余分なビットまで同時にマスクする可能性があります。ACL プロファイルとルールを最適化するためには、手動設定を行ってください。

Access Profile List (アクセスプロファイルリスト)

アクセスプロファイルを使用することにより、それぞれのパケットヘッダに含まれる情報に基づくパケット転送可否の基準を設定することができます。スイッチは、4つのプロファイルタイプ（イーサネット ACL、IPv4 ACL、IPv6 ACL およびパケットコンテンツ ACL）をサポートしています。

アクセスプロファイルの作成は2段階に分かれます。はじめにフレームのどの部分を調べるのか、送信元 MAC アドレスか、受信先 IP アドレスか、などを決定します。次に、そのフレームに対してどのような処理を行うのかという基準になる値を入力します。詳しくは以下で説明します。

スイッチに現在定義済みのアクセスプロファイルを表示できます。

ACL > Access Profile List の順にメニューをクリックし、以下の画面を表示します。

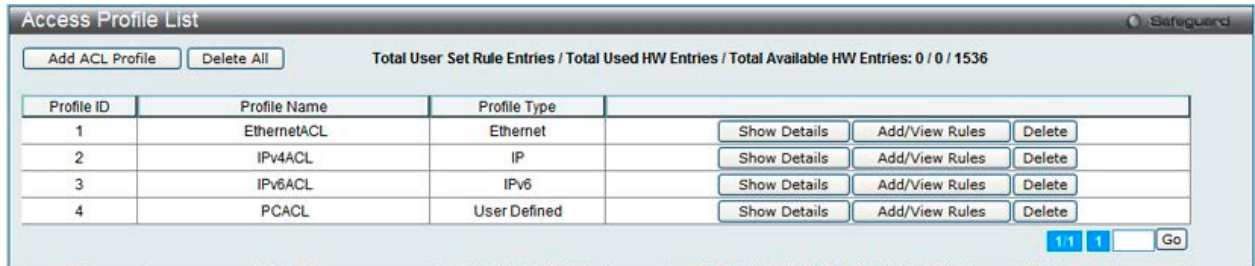


図 11-2 Access Profile List 画面

| 項目 | 説明 |
|-----------------|--|
| Add ACL Profile | アクセスプロファイルリストにエントリを追加します。 |
| Delete All | テーブルからすべてのアクセスプロファイルを削除します。 |
| Show Details | 指定プロファイル ID エントリに関する情報を表示します。 |
| Add/View Rules | 指定プロファイル ID の ACL ルールの参照または追加を行います。 |
| Delete | 指定エントリを削除します。 |
| Go | 複数ページが存在する場合は、ページ番号を入力後、クリックして、特定のページへ移動します。 |

「Add Access Profile」画面には 4 種類あります。:

イーサネット (MAC アドレスベース) プロファイル設定用、IPv6 アドレスベースプロファイル設定用、IPv4 アドレスベースプロファイル設定用およびパケットコンテンツマスクプロファイル設定用です。

アクセスプロファイルリストの作成 (Ethernet)

イーサネット用のアクセスプロファイルを作成し、プロファイルにルールを作成します。

ACL > Access Profile List の順にメニューをクリックし、以下の画面を表示します。

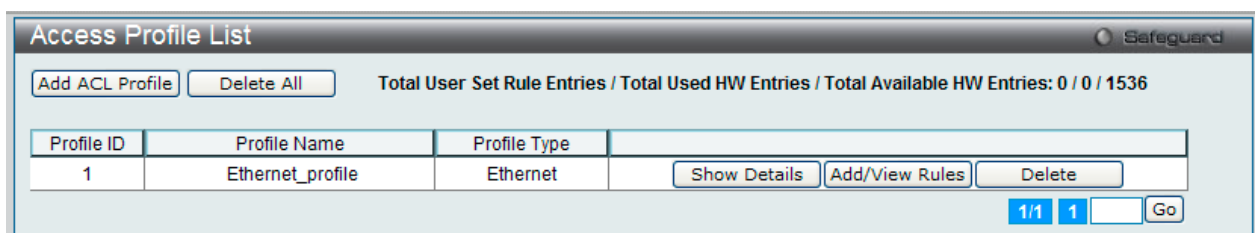


図 11-3 Access Profile List 画面

エントリの削除

エントリを削除するためには、エントリ横の「Delete」ボタンをクリックします。すべてのアクセスプロファイルを削除するためには、「Delete All」ボタンをクリックします。

エントリの追加

「Access Profile List」にエントリを追加するには、「Add ACL Profile」ボタンをクリックし、以下の画面を表示します。

イーサネットの「Add ACL Profile」画面

The screenshot shows the 'Add ACL Profile' configuration interface. At the top, there are fields for 'Profile ID (1-6)' (set to 1) and 'Profile Name' (set to EthernetACL). Under 'Select ACL Type', 'Ethernet ACL' is selected with a radio button, and 'Tagged' is selected in a dropdown menu. There are also radio buttons for 'IPv4 ACL' and 'Packet Content ACL', and a 'Select' button. Below this, a header bar highlights 'MAC Address', 'VLAN', and '802.1p' in red, and 'Ethernet Type' and 'Payload' in grey. The main content area contains checkboxes and input fields for 'Source MAC Mask', 'Destination MAC Mask', 'VLAN', 'VLAN Mask (0-FFF)', '802.1p', and 'Ethernet Type'. At the bottom, there are '<<Back' and 'Create' buttons.

図 11-4 Add ACL Profile - Ethernet ACL 画面

「Profile ID」でプロファイル番号を 1-1024 から選択し、「Select ACL Type」で「Ethernet ACL」をチェック後、「Select」ボタンをクリックすることで画面を切り替えることができます。画面上部のボックスをクリックすると、赤色に変わり、設定用項目が表示されます。

以下の項目を Ethernet ACL タイプに設定します。

| 項目 | 説明 |
|--|---|
| Profile ID (1-6) | プロファイル設定のための固有の識別番号を指定します。1 から 6 が指定できます。 |
| Profile Name | 作成したプロファイルにプロファイル名を入力します。 |
| Select ACL Type | Ethernet (MAC アドレス)、IPv4 アドレス、IPv6 アドレスまたはパケットコンテンツからプロファイルのタイプを指定します。Type の変更に伴いメニューも変わります。ここでは、「Ethernet ACL」を選択します。 ・ Ethernet ACL - パケットヘッダのレイヤ 2 部分を検証します。 |
| 以下のオプションを指定すると各フレームヘッダのプロトコルタイプを調べます。転送基準にどのようなプロトコルを含めるかを指定します。 | |
| MAC Address | <ul style="list-style-type: none"> Source MAC Mask - 送信元 MAC アドレスをマスクする MAC アドレスを指定します。例: FF-FF-FF-FF-FF-FF Destination MAC Mask - 送信先 MAC アドレスをマスクする MAC アドレスを指定します。例: FF-FF-FF-FF-FF-FF |
| 802.1Q VLAN | <ul style="list-style-type: none"> パケットヘッダの 802.1Q VLAN 識別子を調べて、部分的もしくは全体を転送基準として使用します。 VLAN - VLAN マスクを指定します。 VLAN Mask (0-FFF) - VLAN マスクを指定します。 |
| 802.1p | 各パケットヘッダの 802.1p プライオリティを調べて、部分的または全体を転送基準として使用します。 |
| Ethernet Type | フレームヘッダでイーサネットタイプの値を調べます。 |

「Create」ボタンをクリックし、プロファイルを作成します。

「<<Back」ボタンをクリックし、変更を破棄して前のページに戻ります。

作成したプロファイルの詳細の参照

「Access Profile List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

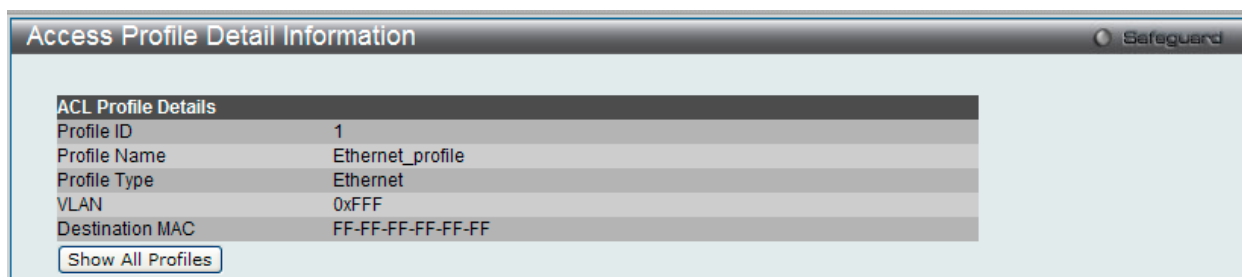


図 11-5 Access Profile Detail Information - Ethernet 画面

「Show All Profiles」ボタンをクリックすると、「Access Profile List」画面に戻ります。

作成したアクセスプロファイルに対するルールの設定手順 (Ethernet) :

Ethernet アクセスルールの設定

1. 「Access Profile List」画面を表示します。

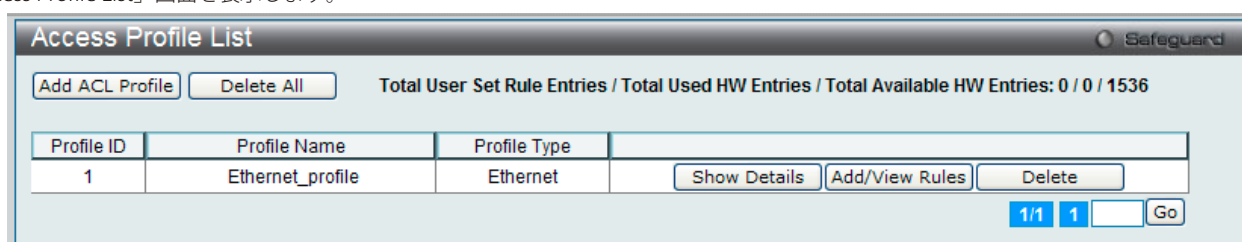


図 11-6 Access Profile List 画面

2. Ethernet エントリの「Add/View Rules」ボタンをクリックし、以下の画面を表示します。

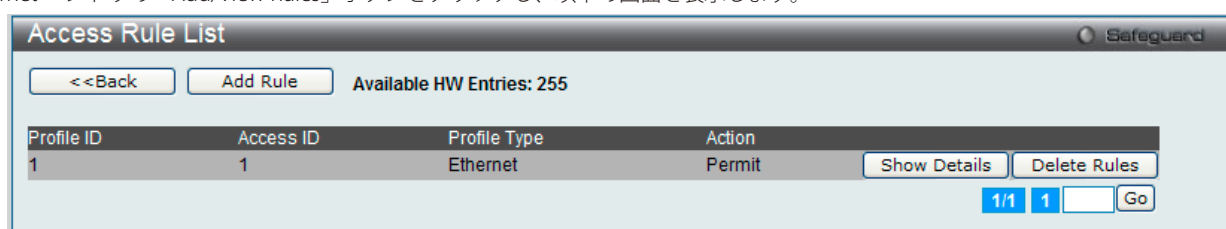


図 11-7 Access Rule List - Ethernet 画面

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。「<<Back」ボタンをクリックし、前のページに戻ります。

作成したルールの削除

該当の「Delete Rules」ボタンをクリックします。

ルールの新規作成

ルールを作成するためには、「Add Rule」ボタンをクリックし、以下の画面を表示します。

図 11-8 Add Access Rule - Ethernet 画面

Ethernet のアクセスルールを設定するためには以下の項目を設定して、「Apply」ボタンをクリックします。

| 項目 | 説明 |
|------------------------------|--|
| Rule Detail | |
| Access ID (1-256) | プロファイル設定のための固有の識別番号を指定します。1 から 256 が指定できます。 • Auto Assign - 本項目をチェックするとスイッチは自動的に作成されるルールに Access ID を割り当てます。 |
| VLAN Name | 設定済みの VLAN 名を入力します。スイッチはパケットヘッダの VLAN を確認し、その結果をパケット送信の基準 (または基準の一部) とします。 |
| VLAN ID | VLAN ID 番号を指定します。 |
| VLAN Mask (0-FFFF) | VLAN マスクを指定します。 |
| Source MAC Address | 送信元 MAC アドレスの MAC アドレスマスクを指定します。 |
| Source MAC Address Mask | 送信元 MAC アドレスの MAC アドレスマスクを 16 進数形式で指定します。 |
| Destination MAC Address | 送信先 MAC アドレスの MAC アドレスマスクを入力します。 |
| Destination MAC Address Mask | 送信先 MAC アドレスの MAC アドレスマスクを 16 進数形式で入力します。 |
| 802.1p (0-7) | 802.1p プライオリティ値を 0-7 で入力します。アクセスプロファイルをこの値を持つパケットに適用します。 |
| Ethernet Type (0-FFFF) | アクセスプロファイルが適用されるパケットヘッダの 802.1Q イーサネットタイプの値を 16 進数 (hex 0x0-0xffff) で指定します。イーサネットタイプは次の形式で指定します。: hex 0x0-0xffff (a-f の半角英文字、と 0-9999 の数字を使用します。) |
| Rule Action | |
| Action | <ul style="list-style-type: none"> Permit - スイッチはアクセスプロファイルに一致するパケットの送信を、以下のフィールドで設定する追加のルールに従って行います。 Deny - スイッチはアクセスプロファイルに一致するパケットを送信せずにフィルタリングします。 Mirror - スイッチはアクセスプロファイルに一致するパケットを「Port Mirroring」画面で定義したポートにミラーリングします。ポートミラーリングが有効で、ターゲットポートが設定されている必要があります。 |
| Priority (0-7) | スイッチにより設定された 802.1p デフォルトプライオリティを上書きしたい場合に指定します。このプライオリティにより転送されたパケットがどの CoS キューを使用するかが決まります。この欄を指定するとパケットはこのプライオリティを割り当てられ、対応した CoS キューに転送されます。指定しない場合は、パケットは送出される前に、入力用の 802.1p ユーザプライオリティを元の値に書き換えられます。プライオリティキュー、CoS キューおよび 802.1p マッピングについての詳細な情報については、本マニュアルの 221 ページの「第 10 章 QoS (QoS機能の設定)」 を参照してください。 |
| Replace Priority | 条件に合ったパケットの DSCP 値は指定した値に入れ替わります。 |

ACL (ACL機能の設定)

| 項目 | 説明 |
|------------------------------|---|
| Replace DSCP (0-63) | スイッチは本画面で指定した基準に一致するパケットの DSCP をチェックボックスの右側のフィールド内に指定した値に書き換えます。ACL ルールがプライオリティと IPv4 パケットの両方を変更するために追加されても、チップの制限のためそれらの一方しか変更できません。プライオリティと DSCP の両方が変更されるように設定されている場合は、現在のプライオリティを変更します。 |
| Replace ToS Precedence (0-7) | 出力パケットの IP 優先度が新しい値に変更されます。操作の優先度なしで使用すると、デフォルト TC にパケットは送信されます。 |
| Time Range Name | チェックボックスをクリックし、「Time Range」画面に設定済みのタイムレンジ設定名を入力します。このアクセスルールをスイッチで実行する場合、ここに特定の時間を設定します。 |
| Counter | 「Counter」機能を「Enabled」(有効) / 「Disabled」(無効) にします。カウンタ機能は、アクセスルールに一致するパケット数を記録するために使用されます。本機能はオプションです。初期値は無効です。 |
| Mirror Group ID (1-4) | 「Action」で「Mirror」を選択した場合に、ミラーグループ ID を指定します。 |
| Ports / VLAN Name / VLAN ID | このルールに適用するオブジェクトの選択または入力を行います。 <ul style="list-style-type: none">Ports - ポート番号またはポート範囲を入力します。ポートの範囲を指定する際には、本画面中の「Access ID」フィールドの「Auto assign」チェックボックスを選択しておく必要があります。選択しないと、エラーメッセージが表示され、アクセスルールの設定が行われません。VLAN Name - VLAN 名を入力します。VLAN ID - VID を入力します。 |

「Apply」ボタンをクリックして行った変更を適用します。

「<<Back」ボタンをクリックし、変更を破棄して前のページに戻ります。

作成したルールの詳細の参照

「Access Rule List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

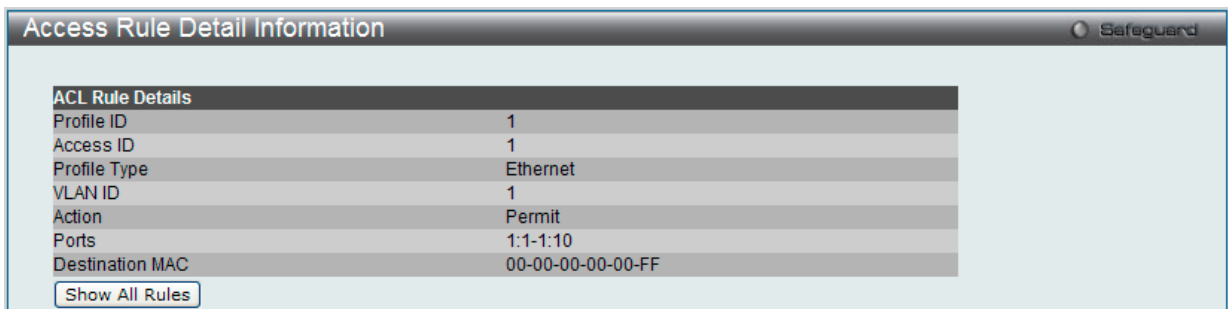


図 11-9 Access Rule Detail Information - Ethernet 画面

「Show All Rules」ボタンをクリックすると、「Access Rule List」画面に戻ります。

アクセスプロファイルリストの作成 (IPv4)

アクセスプロファイルを作成し、プロファイルにルールを作成します。

ACL > Access Profile List の順にメニューをクリックし、以下の画面を表示します。1つのアクセスプロファイルが説明のために作成されています。

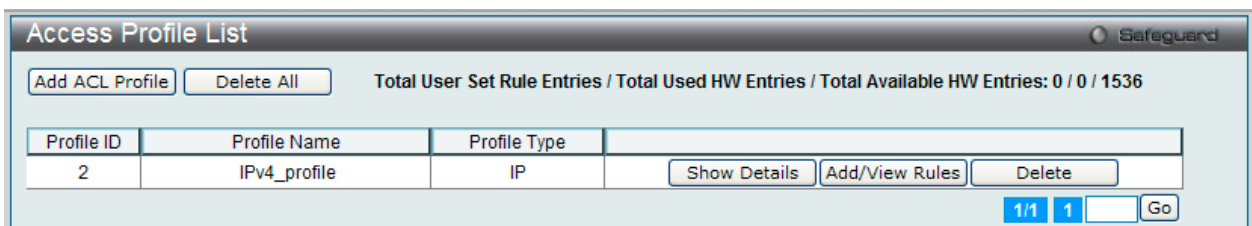


図 11-10 Access Profile List 画面

エントリの削除

エントリを削除するためには、エントリ横の「Delete」ボタンをクリックします。すべてのアクセスプロファイルを削除するためには、「Delete All」ボタンをクリックします。

エントリの追加

「Access Profile List」にエントリを追加するには、「Add ACL Profile」ボタンをクリックし、以下の画面を表示します。

IPv4 の「Add ACL Profile」画面

図 11-11 Add ACL Profile - IPv4 ACL 画面

「Profile ID」でプロファイル番号を 1-6 から選択し、「Select ACL Type」で「IPv4 ACL」をチェック後、隣接する欄で設定するフレームヘッダ（ICMP、IGMP、TCP、UDP、Protocol ID）選択して「Select」ボタンをクリックします。画面上部のボックスをクリックすると、赤色に変わり、設定用項目が表示されます。

以下の項目を IPv4 ACL タイプに設定します。

| 項目 | 説明 |
|--|--|
| Profile ID | プロファイル設定のための固有の識別番号を指定します。1 から 6 が指定できます。 |
| Profile Name | 作成したプロファイルにプロファイル名を入力します。 |
| Select ACL Type | Ethernet (MAC アドレス)、IPv4 アドレス、IPv6 アドレスまたはパケットコンテンツの中からプロファイルのベースを指定します。Type の変更に伴いメニューも変わります。ここでは「IPv4 ACL」を選択します。 ・ IPv4 ACL - フレームヘッダの IPv4 アドレスを検証します。 |
| 以下のオプションを指定すると各フレームヘッダのプロトコルタイプを調べます。転送基準にどのようなプロトコルを含めるかを指定します。 | |
| 802.1Q VLAN | パケットヘッダの 802.1Q VLAN 識別子を調べて、部分的もしくは全体を転送基準として使用します。 ・ VLAN - VLAN マスクを指定します。 ・ VLAN Mask (0-FFF) - VLAN マスクを指定します。 |
| IPv4 DSCP | 各パケットヘッダの DiffServ コードを調べて、部分的もしくは全体を転送基準として使用します。 |
| IPv4 Address | ・ Source IP Mask - 送信元 IP アドレスをマスクする IP アドレスを指定します。 ・ Destination IP Mask - 送信先 IP アドレスをマスクする IP アドレスを指定します。 |
| ICMP | 各パケットのフレームヘッダの「Internet Control Message Protocol」(ICMP) 項目を調べます。アクセスプロファイルが適用するタイプ（「ICMP Type」または「ICMP Code」）を選択します。 ・ ICMP Type - アクセスプロファイルを ICMP Type 値に適用します。 ・ ICMP Code - アクセスプロファイルを ICMP Code に適用します。 |
| IGMP | それぞれのフレームヘッダの「Internet Group Management Protocol」(IGMP) 項目を調べます。アクセスプロファイルが適用するタイプ「IGMP Type」を選択します。 |
| TCP | 転送基準となる受信したパケットの TCP ポート番号を使用します。TCP を選ぶと送信元ポートマスク (source port mask) と (または) 送信先ポートマスク (dest port mask) を指定する必要があります。 - Source Port Mask (0-FFFF) - フィルタリングしたい送信元ポートをマスクする TCP ポートを 16 進数 (hex 0x0-0xffff) で指定します。 - Destination Port Mask (0-FFFF) - フィルタリングしたい送信先ポートをマスクする TCP ポートを 16 進数 (hex 0x0-0xffff) で指定します。 - TCP Flag Bits - フィルタするフラグビットを指定します。フラグビットはパケットがどのような振る舞いをするかを決定するパケットの一部です。パケットのフラグビットでフィルタリングするには「TCP」項目のフラグビットに一致する内容のボックスをチェックします。URG (urgent)、ACK (acknowledgement)、PSH (push)、RST (reset)、SYN (synchronize)、FIN (finish) または Check All (すべて) を選ぶことができます。 |

ACL (ACL機能の設定)

| 項目 | 説明 |
|-------------|---|
| UDP | 転送基準となる受信したパケットのUDPポート番号を使用します。UDPを選ぶと送信元ポートマスク (source port mask) と (もしくは) 送信先ポートマスク (dest port mask) を指定する必要があります。 <ul style="list-style-type: none">- Source Port Mask (0-FFFF) - フィルタリングしたい送信元ポートをマスクする UDP ポートを 16 進数 (hex 0x0-0xffff) で指定します。例: 255.255.255.255- Destination Port Mask (0-FFFF) - フィルタリングしたい送信先ポートをマスクする UDP ポートを 16 進数 (hex 0x0-0xffff) で指定します。例: 255.255.255.255 |
| Protocol ID | マスクしたいパケットヘッダの Protocol ID Mask (0-FF) を指定します。「User Define」マスクは 16 進数 (0-FFFFFFF) で指定します。 |

「Create」ボタンをクリックし、設定を適用します。

「<<Back」ボタンをクリックし、変更を破棄して前のページに戻ります。

作成したプロファイルの詳細の参照

作成したプロファイルの詳細を参照するには、「Access Profile List」画面の該当エントリの「Show Details」ボタンをクリックし、以下の画面を表示します。



図 11-12 Access Profile Detail Information - IPv4 画面

「Show All Profiles」ボタンをクリックすると、「Access Profile List」画面に戻ります。

作成したアクセスプロファイルに対するルールの設定手順 (IPv4) :

IPv4 アクセスルールの設定

1. 「Access Profile List」画面を表示します。

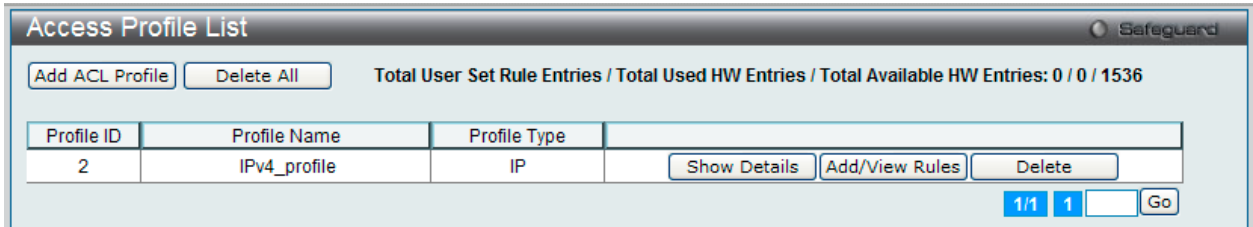


図 11-13 Access Profile List 画面

2. 「Access Profile List」画面を表示し、IPv4 エントリの「Add/View Rules」ボタンをクリックし、以下の画面を表示します。

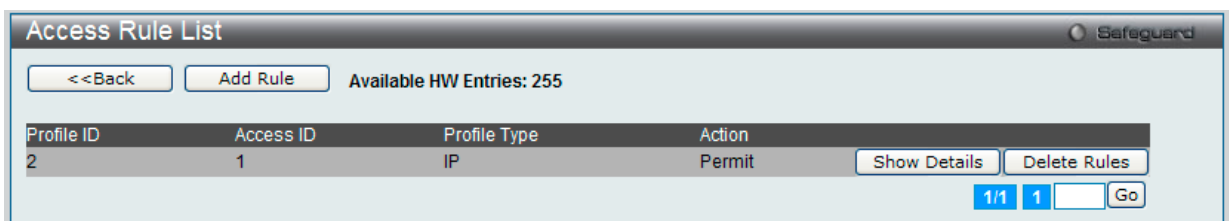


図 11-14 Access Rule List - IPv4 画面

「<<Back」ボタンをクリックして前のページに戻ります。

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

ルールの削除

該当の「Delete Rules」ボタンをクリックします。

ルールの新規作成

新しいルールを作成するには、「Add Rule」ボタンをクリックし、以下の画面を表示します。

Add Access Rule Safeguard

Profile Information

| | | | |
|--------------|----|--------------|--------------|
| Profile ID | 2 | Profile Name | IPv4_profile |
| Profile Type | IP | DSCP | Yes |

Rule Detail
(Keep the input field blank to specify that the corresponding option does not matter).

Access ID (1-256) Auto Assign

DSCP (e.g.: 0-63)

Rule Action

Action

Priority (0-7)

Replace Priority

Replace DSCP (0-63)

Replace ToS Precedence (0-7)

Time Range Name

Counter

Mirror Group ID (1-4)

図 11-15 Add Access Rule - IPv4 画面

以下の項目を設定します。

| 項目 | 説明 |
|-----------------------------|---|
| Rule Detail | |
| Access ID (1-256) | プロファイル設定のための固有の識別番号を指定します。1 から 256 が指定できます。 • Auto Assign - 本項目をチェックするとスイッチは自動的に作成されるルールに Access ID を割り当てます。 |
| VLAN Name | 設定済みの VLAN 名を入力します。スイッチはパケットヘッダの VLAN を確認し、その結果をパケット送信の基準 (または基準の一部) とします。 |
| VLAN ID(1-4094) | VLAN ID を入力します。「Mask」(0-FFF) にマスク値を入力します。 |
| VLAN Mask (0-FFFF) | VLAN マスクを指定します。 |
| Source IP Address | 送信元の IP アドレスの IP アドレスを入力します。 |
| Source IP Address Mask | 送信元の IP アドレスの IP アドレスマスクを入力します。 |
| Destination IP Address | 宛先 IP アドレスの IP アドレスを入力します。 |
| Destination IP Address Mask | 送信先 IP アドレスの IP アドレスマスクを入力します。 |
| DSCP | DSCP 値 (0-63) を指定すると各パケットヘッダの DiffServ コードを調べて、部分的または全体を転送基準として使用します。 |
| ICMP | 各パケットのフレームヘッダの「Internet Control Message Protocol」(ICMP) 項目を調べます。アクセスプロファイルが適用するタイプ (「ICMP Type」または「ICMP Code」) を選択します。 • Type - アクセスプロファイルを ICMP Type 値に適用します。 • Code - アクセスプロファイルを ICMP Code に適用します。 |
| IGMP | それぞれのフレームヘッダの「Internet Group Management Protocol」(IGMP) 項目を調べます。アクセスプロファイルが適用するタイプ「IGMP Type」を選択します。 |

ACL (ACL機能の設定)

| 項目 | 説明 |
|------------------------------|--|
| TCP | <p>転送基準となる受信したパケットのTCPポート番号を使用します。TCPを選ぶと送信元ポートマスク (source port mask) と (または) 送信先ポートマスク (dest port mask) を指定する必要があります。</p> <ul style="list-style-type: none"> - TCP Source Port (0-65535) - フィルタリングしたい送信元ポートを指定します。 - TCP Source Port Mask (0-FFFF) - フィルタリングしたい送信元ポートをマスクするTCPポートを16進数で指定します。 - TCP Destination Port (0-65535) - フィルタリングしたい送信先ポートを指定します。 - TCP Destination Port Mask (0-FFFF) - フィルタリングしたい送信先ポートをマスクするTCPポートを16進数で指定します。 - Flag Bits - フィルタするフラグビットを指定します。フラグビットはパケットがどのような振る舞いをするかを決定するパケットの一部です。パケットのフラグビットでフィルタリングするには「TCP」項目のフラグビットに一致する内容のボックスをチェックします。URG (urgent)、ACK (acknowledgement)、PSH (push)、RST (reset)、SYN (synchronize)、FIN (finish) を選ぶことができます。 |
| UDP | <p>転送基準となる受信したパケットのUDPポート番号を使用します。UDPを選ぶと送信元ポートマスク (source port mask) と (または) 送信先ポートマスク (dest port mask) を指定する必要があります。</p> <ul style="list-style-type: none"> - UDP Source Port (0-65535) - フィルタリングしたい送信元ポートを指定します。 - UDP Source Port Mask (0-FFFF) - フィルタリングしたい送信元ポートをマスクするUDPポートを16進数 (hex 0x0-0xffff) で指定します。 - UDP Destination Port (0-65535) - フィルタリングしたい送信先ポートを指定します。 - UDP Destination Port Mask (0-FFFF) - フィルタリングしたい送信先ポートをマスクするUDPポートを16進数 (hex 0x0-0xffff) で指定します。 |
| Protocol ID | マスクしたいパケットヘッダのProtocol ID Maskを指定します。0-255の値を入力します。 |
| User | マスクしたいパケットヘッダのProtocol ID Maskを16進数 (0-FFFFFFFF) で指定します。 |
| User Mask (0-FFFFFFFF) | マスクしたいパケットヘッダのProtocol ID Maskを16進数 (0-FFFFFFFF) で指定します。 |
| Rule Action | |
| Action | <ul style="list-style-type: none"> • Permit - アクセスプロファイルに一致したパケットを転送します。この時、新しいルールが追加されることがあります (以下参照)。 • Deny - アクセスプロファイルに一致したパケットは転送せずにフィルタリングします。 • Mirror - アクセスプロファイルに一致するパケットを「Port Mirroring」画面で定義したポートにミラーリングします。ポートミラーリングが有効で、ターゲットポートに設定されている必要があります。 |
| Priority (0-7) | <p>スイッチにより設定された802.1pデフォルトプライオリティを上書きしたい場合に指定します。このプライオリティにより転送されたパケットがどのCoSキューを使用するかが決まります。この欄を指定するとパケットはこのプライオリティを割り当てられ、対応したCoSキューに転送されます。指定しない場合は、パケットは送出される前に、入力用の802.1pユーザプライオリティを元の値に書き換えられます。プライオリティキュー、CoSキューおよび802.1pマッピングについての詳細な情報については、本マニュアルの 221 ページの「第10章 QoS (QoS機能の設定)」 を参照してください。</p> |
| Replace Priority | 条件に合ったパケットのDSCP値は指定した値に入れ替わります。 |
| Replace DSCP (0-63) | <p>スイッチはここで指定した基準に一致するパケットのDSCPをボックスの右側の欄内に指定した値に書き換えます。ACLルールがプライオリティとIPv4パケットの両方を変更するのに追加されても、チップの制限のためそれら的一方しか変更できません。プライオリティとDSCPの両方を変更するように設定している場合は、現在のプライオリティを変更します。</p> |
| Replace ToS Precedence (0-7) | 出力パケットのIP優先度が新しい値に変更されます。操作の優先度なしで使用すると、デフォルトTCにパケットは送信されます。 |
| Time Range Name | <p>チェックボックスをクリックし、「Time Range」画面に設定済みのタイムレンジ設定名を入力します。このアクセスルールをスイッチで実行する場合、ここに特定の時間を設定します。</p> |
| Counter | <p>「Counter」機能を「Enabled」(有効) / 「Disabled」(無効) にします。カウンタ機能は、アクセスルールに一致するパケット数を記録するために使用されます。本機能はオプションです。初期値は無効です。</p> |
| Mirror Group ID (1-4) | 「Action」で「Mirror」を選択した場合に、ミラーグループIDを指定します。 |
| Ports / VLAN Name / VLAN ID | <p>このルールに適用するオブジェクトの選択または入力を行います。</p> <ul style="list-style-type: none"> • Ports - ポート番号またはポート範囲を入力します。ポートの範囲を指定する際には、本画面中の「Access ID」フィールドの「Auto assign」チェックボックスを選択しておく必要があります。選択しないと、エラーメッセージが表示され、アクセスルールの設定が行われません。 • VLAN Name - VLAN名を入力します。 • VLAN ID - VIDを入力します。 |

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

「<<Back」ボタンをクリックし、変更を破棄して前のページに戻ります。

作成したルールの詳細の参照

「Access Rule List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

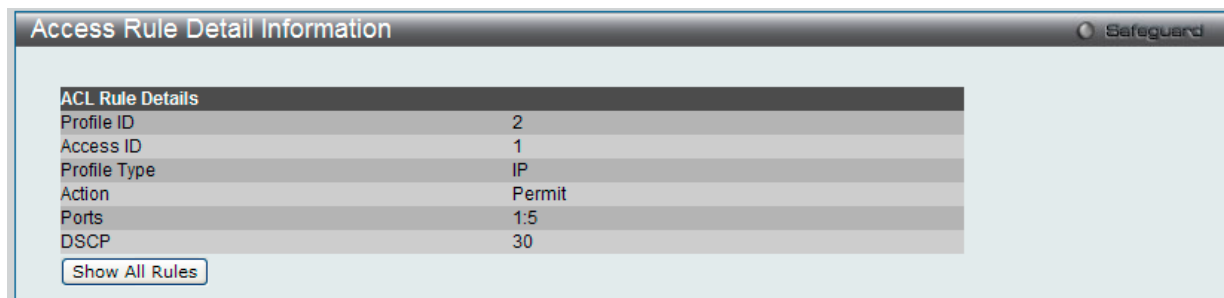


図 11-16 Access Rule Detail Information - IP 画面

「Show All Rules」ボタンをクリックすると、「Access Rule List」画面に戻ります。

アクセスプロファイルリストの作成 (IPv6)

アクセスプロファイルを作成し、プロファイルにルールを作成します。

ACL > Access Profile List の順にメニューをクリックし、以下の画面を表示します。1つのアクセスプロファイルが説明のために作成されています。

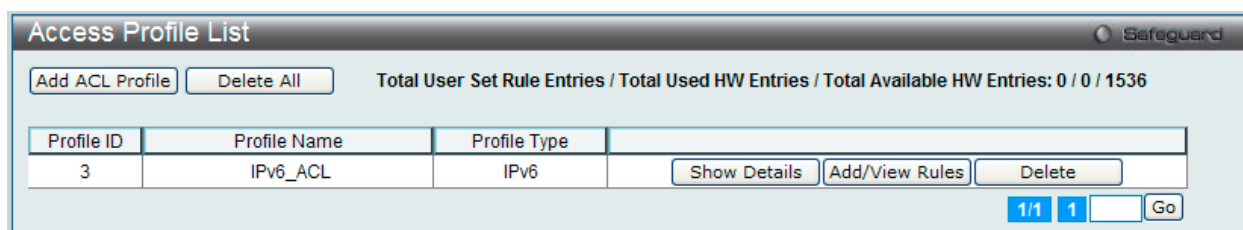


図 11-17 Access Profile List 画面

エントリの削除

エントリの削除は、エントリ横の「Delete」ボタンをクリックします。すべてのアクセスプロファイルの削除は、「Delete All」ボタンをクリックします。

エントリの追加

「Access Profile List」にエントリを追加するには、「Add ACL Profile」で「IPv6 ACL」ボタンをチェック後、隣接する欄で設定するフレームヘッダ（TCP または UDP）を選択して「Select」ボタンをクリックします。

IPv6 の「Add ACL Profile」画面

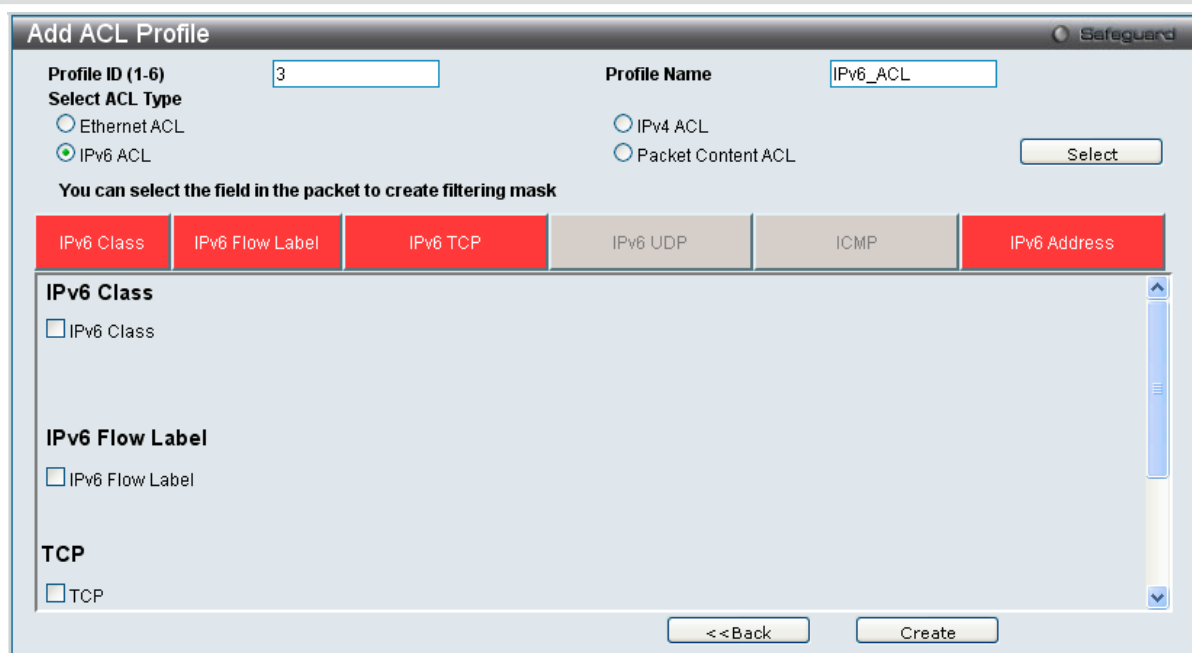


図 11-18 Add ACL Profile - IPv6 ACL 画面

「Profile ID」でプロファイル番号を 1-6 から選択し、「Select ACL Type」をチェック後、「Select」ボタンをクリックすることで画面を切り替えることができます。画面上部のボックスをクリックすると、赤色に変わり、設定用項目が表示されます。

ACL (ACL機能の設定)

以下の項目を IPv6 ACL タイプに設定します。

| 項目 | 説明 |
|--|---|
| Profile ID | プロファイル設定のための固有の識別番号を指定します。1 から 6 を指定できます。 |
| Select ACL Type | Ethernet (MAC アドレス)、IPv4 アドレス、IPv6 アドレスまたはパケットコンテンツの中からプロファイルのベースを指定します。Type の変更に伴いメニューも変わります。ここでは「IPv6 ACL」を選択します。 <ul style="list-style-type: none">IPv6 ACL - フレームヘッダの IPv6 アドレスを検証します。 |
| 以下のオプションを指定すると各フレームヘッダのプロトコルタイプを調べます。転送基準にどのようなプロトコルを含めるかを指定します。 | |
| IPv6 Class | この項目を選ぶと IPv6 ヘッダの「Class」を調べます。「Class」は IPv4 における「Type of Service」(ToS)、「Precedence bits」のようなパケットヘッダの一部です。 |
| IPv6 Flow Label | この項目を選ぶと IPv6 ヘッダの「flow label」を調べます。「flow label」は送信元で順番につけられる QoS やリアルタイムサービスパケットのためのデフォルトではない項目です。 |
| IPv6 TCP | <ul style="list-style-type: none">TCP - TCP トラフィックに適用するルールを指定します。Source Port Mask (0-FFFF) - TCP 送信元ポートマスクを指定します。Destination Port Mask (0-FFFF) - TCP 宛先ポートマスクを指定します。 |
| IPv6 UDP | <ul style="list-style-type: none">UDP - ルールを UDP トラフィックに適用するように指定します。Source Port Mask (0-FFFF) - UDP 送信元ポートマスクを指定します。Destination Port Mask (0-FFFF) - UDP 宛先ポートマスクを指定します。 |
| ICMP | 各パケットのフレームヘッダの「Internet Control Message Protocol」(ICMP) 項目を調べます。アクセスプロファイルが適用するタイプ(「ICMP Type」または「ICMP Code」)を選択します。 <ul style="list-style-type: none">ICMP Type - アクセスプロファイルを ICMP Type 値に適用します。ICMP Code - アクセスプロファイルを ICMP Code に適用します。 |
| IPv6 Address | <ul style="list-style-type: none">IPv6 Source Address - 対応するボックスをチェックして、送信元 IPv6 アドレスをマスクする IP アドレスを指定します。IPv6 Destination Address - 対応するボックスをチェックして、送信先 IPv6 アドレスをマスクする IP アドレスを指定します。 |

「Create」ボタンをクリックし、設定を適用します。

「<<Back」ボタンをクリックし、変更を破棄して前のページに戻ります。

作成したプロファイルの詳細の参照

作成したプロファイルの詳細を参照する場合は、「Access Profile List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

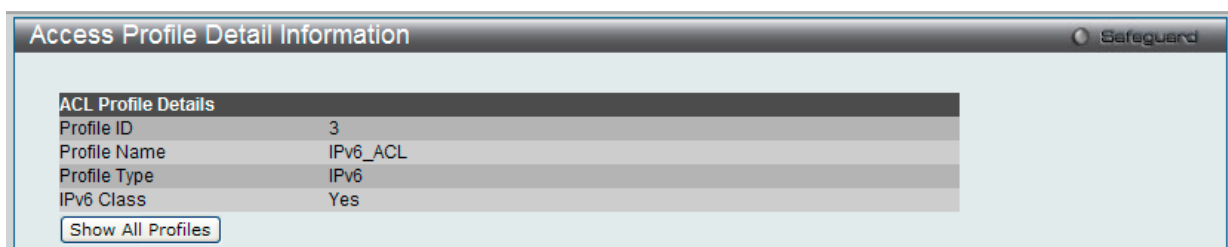


図 11-19 Access Profile Detail Information - IPv6 ACL 画面

「Show All Profiles」ボタンをクリックすると、「Access Profile List」画面に戻ります。

作成したアクセスプロファイルに対するルールの設定手順 (IPv6) :

IPv6 アクセスルールの設定

1. 「Access Profile List」画面を表示します。

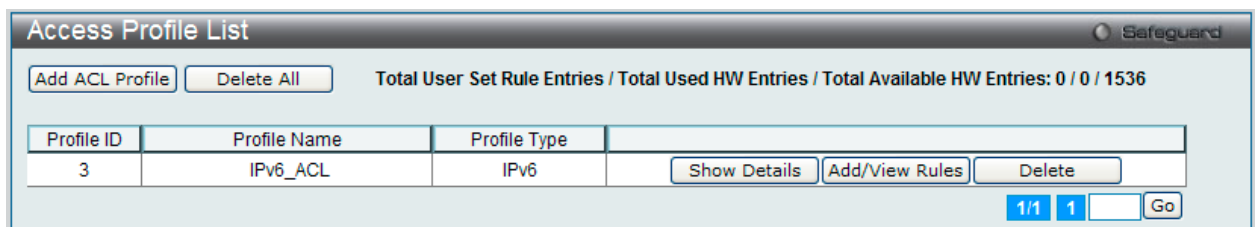


図 11-20 Access Profile List 画面

2. 「Access Profile List」画面を表示し、IPv6 エントリの「Add/View Rules」ボタンをクリックして以下の画面を表示します。

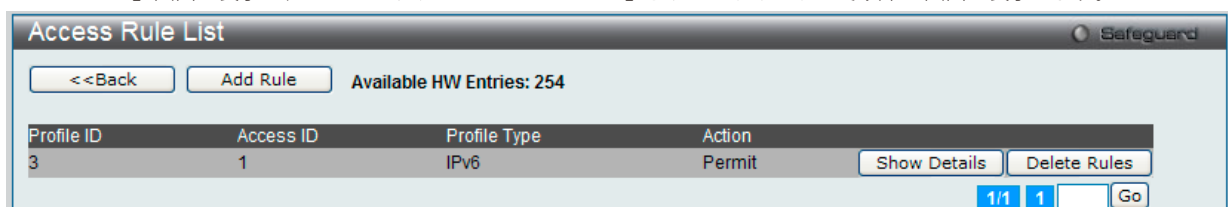


図 11-21 Access Rule List - IPv6 画面

「<<Back」ボタンをクリックして前のページに戻ります。

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

作成済みのルールの削除

該当の「Delete Rules」ボタンをクリックします。

ルールの新規登録

新しいルールを作成するためには、「Add Rule」ボタンをクリックします。

図 11-22 Add Access Rule - IPv6 画面

以下の項目を設定します。

| 項目 | 説明 |
|-------------------------------|--|
| Rule Detail | |
| Access ID (1-256) | プロファイル設定のための固有の識別番号を指定します。1 から 256 が指定できます。 • Auto Assign - 本項目をチェックするとスイッチは自動的に作成されるルールに Access ID を割り当てます。 |
| Class | クラスを入力し、IPv6 ヘッダの「Class」フィールドを調べます。本フィールドは IPv4 における「Type of Service (ToS)」、「Precedence bits」フィールドのようなパケットヘッダの一部です。 |
| Flow Label | IPv6 フローラベルマスクを指定します。0-FFFFFF の範囲で指定します。 |
| IPv6 Source Address | IPv6 送信元アドレスの IPv6 アドレスを入力します。 |
| IPv6 Source Address Mask | IPv6 送信元サブマスクを指定します。送信元 IPv6 アドレスの最後の 44 ビット (LSB) のフィルタリングのみを行います。 |
| IPv6 Destination Address | 送信先 IPv6 アドレスの IP アドレスを入力します。 |
| IPv6 Destination Address Mask | 送信先 IPv6 アドレスの IP アドレスマスクを入力します。 |
| TCP | <ul style="list-style-type: none"> • TCP Source Port (0-65535) - IPv6 L4 TCP 送信元ポートサブマスクを指定します。 • TCP Source Port Mask (0-FFFF) - フィルタリングしたい送信元ポートをマスクする TCP ポートを 16 進数で指定します。 • TCP Destination Port (0-65535) - IPv6 L4 TCP 送信先ポートサブマスクを指定します。 • TCP Destination Port Mask (0-FFFF) - フィルタリングしたい送信先ポートをマスクする TCP ポートを 16 進数で指定します。 |

ACL (ACL機能の設定)

| 項目 | 説明 |
|------------------------------|--|
| UDP | <ul style="list-style-type: none"> UDP Source Port (0-65535) - IPv6 L4 UDP 送信元ポートサブマスクを指定します。 UDP Source Port Mask (0-FFFF) - フィルタリングしたい送信元ポートをマスクする UDP ポートを 16 進数で指定します。 UDP Destination Port (0-65535) - IPv6 L4 UDP 送信先ポートサブマスクを指定します。 UDP Destination Port Mask (0-FFFF) - フィルタリングしたい送信先ポートをマスクする UDP ポートを 16 進数で指定します。 |
| ICMP | <p>各パケットのフレームヘッダの「Internet Control Message Protocol」(ICMP) 項目を調べます。アクセスプロファイルが適用するタイプ (「ICMP Type」または「ICMP Code」) を選択します。</p> <ul style="list-style-type: none"> Type - アクセスプロファイルを ICMP Type 値に適用します。 Code - アクセスプロファイルを ICMP Code に適用します。 |
| Rule Action | |
| Action | <ul style="list-style-type: none"> Permit - アクセスプロファイルに一致したパケットを転送します。この時、新しいルールが追加されることがあります (以下参照)。 Deny - アクセスプロファイルに一致したパケットは転送せずにフィルタリングします。 Mirror - アクセスプロファイルに一致するパケットを「Port Mirroring」画面で定義したポートにミラーリングします。ポートミラーリングが有効で、ターゲットポートに設定されている必要があります。 |
| Priority (0-7) | <p>スイッチにより設定された 802.1p デフォルトプライオリティを上書きしたい場合に指定します。このプライオリティにより転送されたパケットがどの CoS キューを使用するかが決まります。この欄を指定するとパケットはこのプライオリティを割り当てられ、対応した CoS キューに転送されます。指定しない場合は、パケットは送出される前に、入力用の 802.1p ユーザプライオリティを元の値に書き換えられます。プライオリティキュー、CoS キューおよび 802.1p マッピングについての詳細な情報については、本マニュアルの 221 ページの「第 10 章 QoS (QoS 機能の設定)」 を参照してください。</p> |
| Replace Priority | 条件に合ったパケットの DSCP 値は指定した値に入れ替わります。 |
| Replace DSCP (0-63) | <p>スイッチは本画面で指定した基準に一致するパケットの DSCP をチェックボックスの右側のフィールド内に指定した値に書き換えます。ACL ルールがプライオリティと IPv4 パケットの両方を変更するために追加されても、チップの制限のためそれらの一方しか変更できません。プライオリティと DSCP の両方が変更されるように設定されている場合は、現在のプライオリティを変更します。</p> |
| Replace ToS Precedence (0-7) | 出力パケットの IP 優先度が新しい値に変更されます。操作の優先度なしで使用すると、デフォルト TC にパケットは送信されます。 |
| Time Range Name | <p>チェックボックスをクリックし、「Time Range」画面に設定済みのタイムレンジ設定名を入力します。このアクセスルールをスイッチで実行する場合、ここに特定の時間を設定します。</p> |
| Counter | <p>「Counter」機能を「Enabled」(有効) / 「Disabled」(無効) にします。カウンタ機能は、アクセスルールに一致するパケット数を記録するために使用されます。本機能はオプションです。初期値は無効です。</p> |
| Mirror Group ID (1-4) | 「Action」で「Mirror」を選択した場合に、ミラーグループ ID を指定します。 |
| Ports / VLAN Name / VLAN ID | <p>このルールに適用するオブジェクトの選択または入力を行います。</p> <ul style="list-style-type: none"> Ports - ポート番号またはポート範囲を入力します。ポートの範囲を指定する際には、本画面中の「Access ID」フィールドの「Auto assign」チェックボックスを選択しておく必要があります。選択しないと、エラーメッセージが表示され、アクセスルールの設定が行われません。 VLAN Name - VLAN 名を入力します。 VLAN ID - VID を入力します。 |

IPv6 のアクセスルールを設定するためには、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

「<<Back」ボタンをクリックし、変更を破棄して前のページに戻ります。

作成したルールの詳細の参照

「Access Rule List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

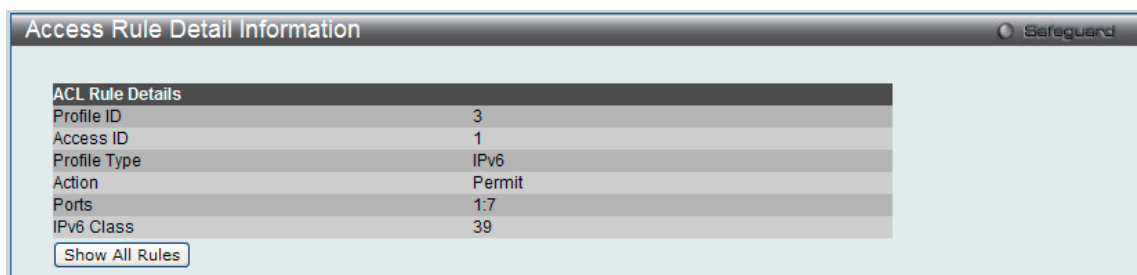


図 11-23 Access Rule Detail Information - IPv6 画面

「Show All Rules」ボタンをクリックすると、「Access Rule List」画面に戻ります。

アクセスプロファイルリストの作成 (パケットコンテンツ)

アクセスプロファイルを作成し、プロファイルにルールを作成します。

ACL > Access Profile List の順にメニューをクリックし、以下の画面を表示します。1つのアクセスプロファイルが説明のために作成されています。

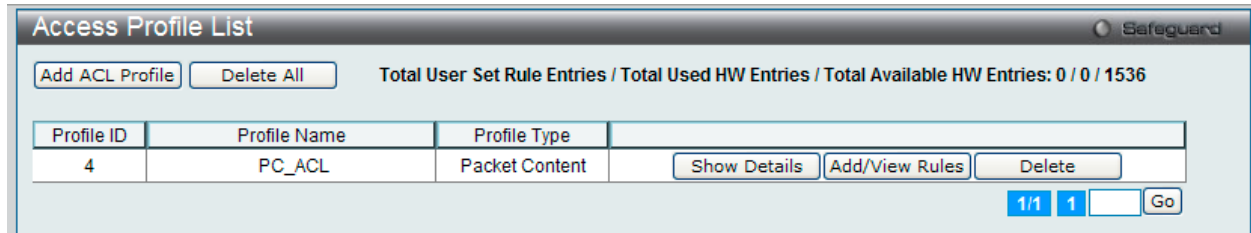


図 11-24 Access Profile List 画面

エントリの削除

エントリを削除するためには、エントリ横の「Delete」ボタンをクリックします。すべてのアクセスプロファイルを削除するためには、「Delete All」ボタンをクリックします。

エントリの追加

「Access Profile List」にエントリを追加するには、「Add ACL Profile」ボタンをクリックし、以下の画面を表示します。

パケットコンテンツの「Add ACL Profile」画面

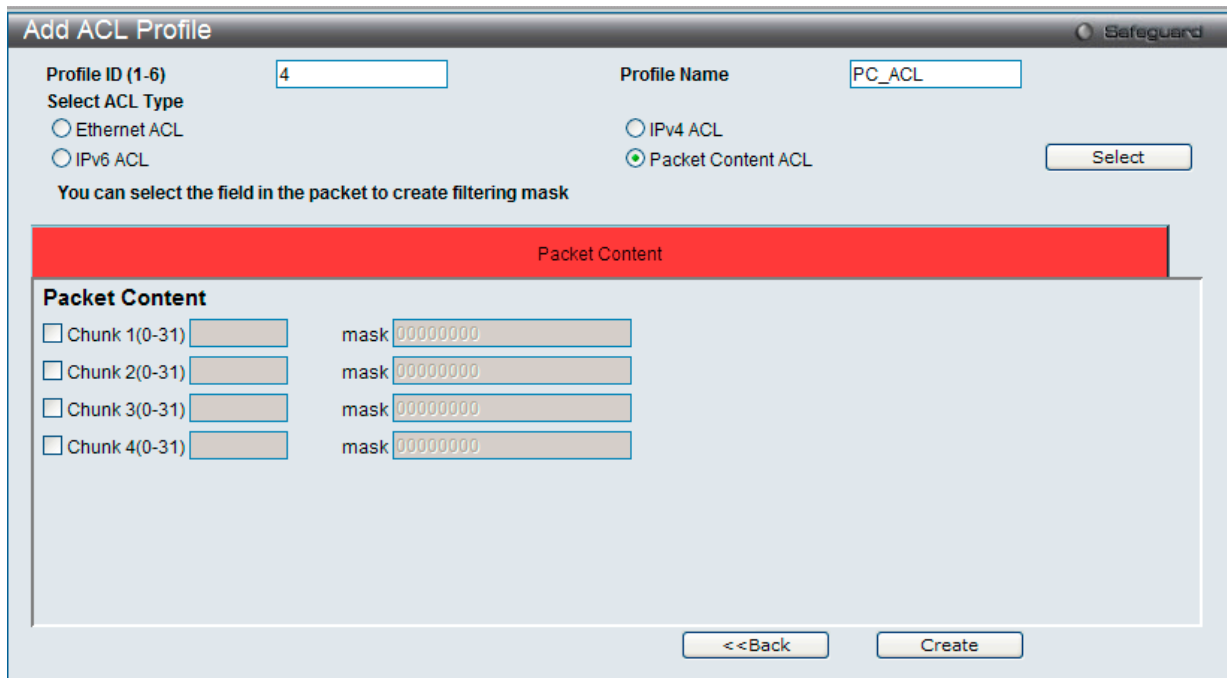


図 11-25 Add ACL Profile 画面 - パケットコンテンツ

「Profile ID」でプロファイル番号を 1-6 から選択し、「Select ACL Type」で「Packet Content ACL」をチェック後、「Select」ボタンをクリックします。画面上部のボックスをクリックすると、赤色に変わり、設定用項目が表示されます。

以下の項目をパケットコンテンツタイプに設定します。

| 項目 | 説明 |
|-----------------|--|
| Profile ID | プロファイル設定のための固有の識別番号を指定します。1 から 6 を指定できます。 |
| Select ACL Type | Ethernet (MAC アドレス)、IPv4 アドレス、IPv6 アドレスまたはパケットコンテンツの中からプロファイルのベースを指定します。Type の変更に伴いメニューも変わります。ここでは「IPv6 ACL」を選択します。 <ul style="list-style-type: none"> Packet Content - フレームヘッダのパケットコンテンツを検証します。 |

| 項目 | 説明 | | | | | | | | | | | | | | |
|-----------------------|---|-------------------|--------|---------------------------|---------------------------|---------------------------|---------|---------|-----------------------|-------------------|-------------------|----|---------------------------|---------------------------|---------------------------|
| Packet Content | <p>パケットコンテンツは、同時にパケット内の4個のオフセットチャンクと、そのフレームコンテンツとオフセットを検証できます。設定可能な4個のチャンクオフセットとマスクがあります。チャンクマスクは4バイトを示します。</p> <p>以下で説明するように、32個の定義済みオフセットチャンクから4つのオフセットチャンクを選択することができます。offset_chunk_1、offset_chunk_2、offset_chunk_3、offset_chunk_4</p> <table border="1"> <thead> <tr> <th>chunk0</th> <th>chunk1</th> <th>chunk2</th> <th>……</th> <th>chunk29</th> <th>chunk30</th> <th>chunk31</th> </tr> </thead> <tbody> <tr> <td>B126, B127, B0, B1</td> <td>B2, B3, B4, B5</td> <td>B6, B7, B8, B9</td> <td>……</td> <td>B114, B115, B116, B117</td> <td>B118, B119, B120, B121</td> <td>B122, B123, B124, B125</td> </tr> </tbody> </table> <p>例題： offset_chunk_1 0 0xfffffff はパケットバイトオフセット 126,127,0,1 に一致します。 offset_chunk_1 0 0x0000ffff はパケットバイトオフセット 0,1 に一致します。</p> <p>注意 一度に、1個のパケットコンテンツマスクプロファイルしか作成できません。</p> <p>D-Link xStack スイッチファミリは、高度なパケットコンテンツマスク（またはパケットコンテンツアクセスコントロールリスト -ACL として知られる）機能を使用して、現在広く蔓延する ARP Spoofing などの一般的なネットワーク攻撃を効果的に軽減することができます。このため、パケットコンテンツ ACL が異なるプロトコル層におけるパケットのどんな指定コンテンツも検証できます。</p> | chunk0 | chunk1 | chunk2 | …… | chunk29 | chunk30 | chunk31 | B126, B127, B0, B1 | B2, B3, B4, B5 | B6, B7, B8, B9 | …… | B114, B115, B116, B117 | B118, B119, B120, B121 | B122, B123, B124, B125 |
| chunk0 | chunk1 | chunk2 | …… | chunk29 | chunk30 | chunk31 | | | | | | | | | |
| B126, B127, B0, B1 | B2, B3, B4, B5 | B6, B7, B8, B9 | …… | B114, B115, B116, B117 | B118, B119, B120, B121 | B122, B123, B124, B125 | | | | | | | | | |

「Select」ボタンをクリックし、ACLタイプを選択します。

「Create」ボタンをクリックし、プロファイルを追加します。

「<<Back」ボタンをクリックし、変更を破棄して前のページに戻ります。

作成したプロファイルの詳細の参照

作成したプロファイル設定を参照するためには、「Access Profile List」画面の対応する「Show Details」ボタンをクリックし、以下の画面を表示します。



図 11-26 Access Profile Detail Information 画面 - パケットコンテンツ

「Show All Profiles」ボタンをクリックすると、「Access Profile List」画面に戻ります。

注意 ARP(Address Resolution Protocol) は、ホストのハードウェアアドレス (MAC アドレス) を検索するための標準規格です。しかし、LAN を攻撃する（つまり、ARP スプーフィング攻撃）ために容易に利用できるため、ARP は被害を受けやすいという弱点があります。ARP プロトコルの動作方法、および ARP Spoofing 攻撃を防ぐために D-Link 独自のパケットコンテンツ ACL を使用する方法について本マニュアル最後にある [467 ページの「付録 F パスワードのリカバリ手順」](#) を参照してください。

作成したアクセスプロファイルに対するルールの設定手順 (パケットコンテンツ) :

パケットコンテンツアクセスルールの設定

1. 「Access Profile List」画面を表示します。

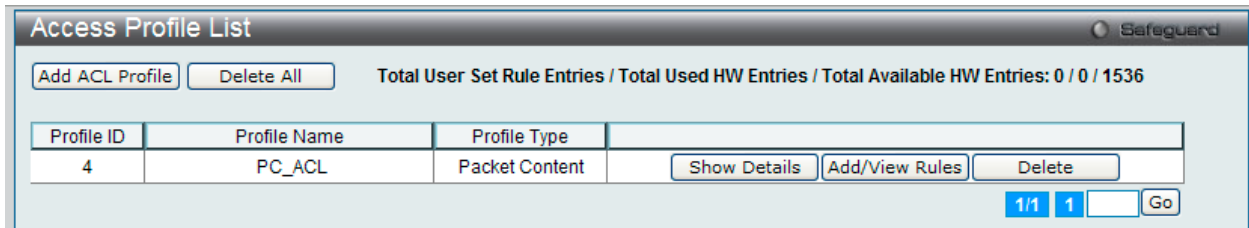


図 11-27 Access Profile List 画面

2. 「Access Profile List」画面を表示し、パケットコンテンツエントリの「Add/View Rules」ボタンをクリックして以下の画面を表示します。

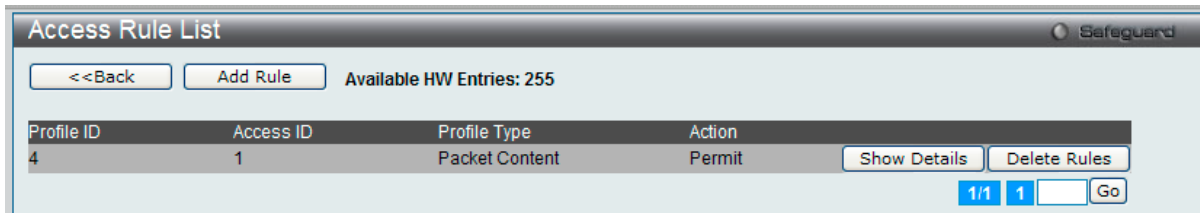


図 11-28 Access Rule List 画面 - パケットコンテンツ

「<<Back」ボタンをクリックして前のページに戻ります。

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

既に作成したルールの削除

該当の「Delete Rules」ボタンをクリックします。

ルールの新規作成

新しいルールを作成するためには、「Add Rule」ボタンをクリックし、以下の画面を表示します。

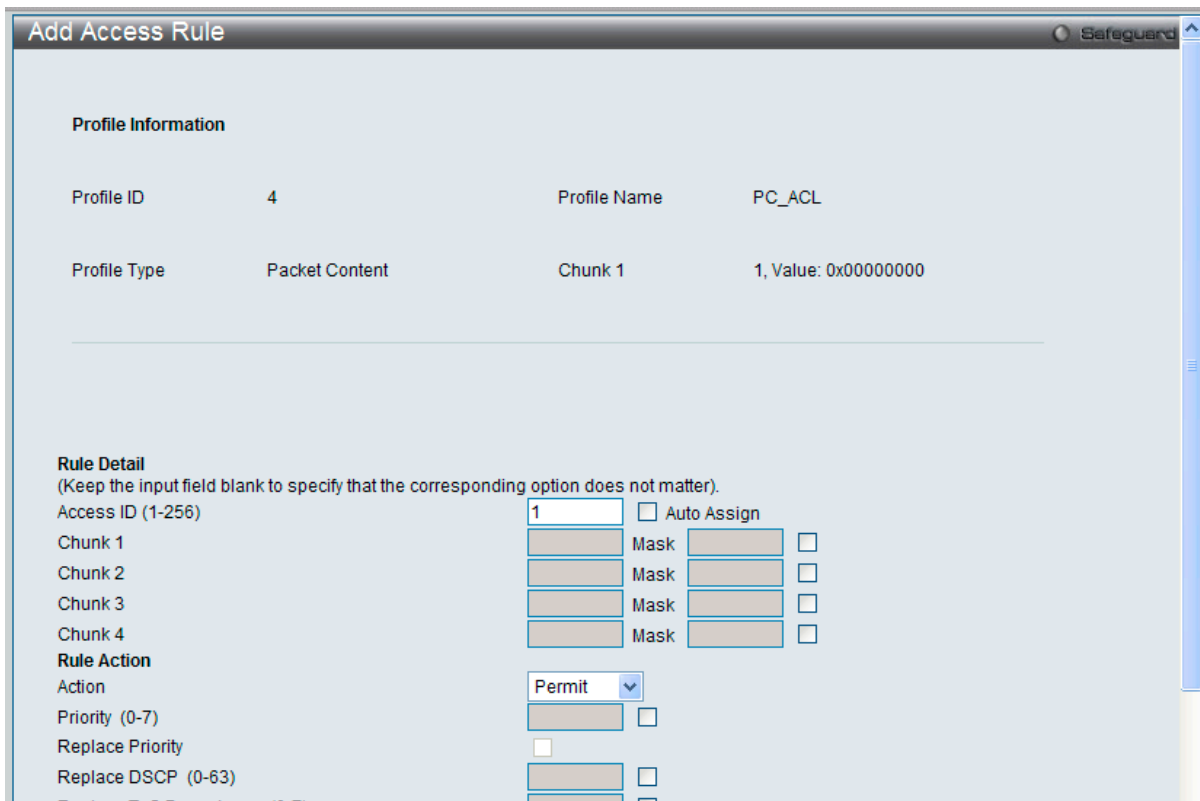


図 11-29 Add Access Rule 画面 - パケットコンテンツ

ACL (ACL機能の設定)

以下の項目を設定します。

| 項目 | 説明 |
|------------------------------|---|
| Rule Detail | |
| Access ID (1-256) | プロファイル設定のための固有の識別番号を指定します。1 から 256 が指定できます。 • Auto Assign - 本項目をチェックするとスイッチは自動的に作成されるルールに Access ID を割り当てます。 |
| Chunk | 本項目の設定により、スイッチは指定したオフセット値で始まるバケットヘッダをマスクします。 |
| Rule Action | |
| Action | <ul style="list-style-type: none"> Permit - アクセスプロファイルに一致したパケットを転送します。この時、新しいルールが追加されることがあります (以下参照)。 Deny - アクセスプロファイルに一致したパケットは転送せずにフィルタリングします。 Mirror - アクセスプロファイルに一致するパケットを「Port Mirroring」画面で定義したポートにミラーリングします。ポートミラーリングが有効で、ターゲットポートに設定されている必要があります。 |
| Priority (0-7) | スイッチにより設定された 802.1p デフォルトプライオリティを上書きしたい場合に指定します。このプライオリティにより転送されたパケットがどの CoS キューを使用するかが決まります。この欄を指定するとパケットはこのプライオリティを割り当てられ、対応した CoS キューに転送されます。指定しない場合は、パケットは送出される前に、入力用の 802.1p ユーザプライオリティを元の値に書き換えられます。プライオリティキュー、CoS キューおよび 802.1p マッピングについての詳細な情報については、本マニュアルの 221 ページの「第 10 章 QoS (QoS 機能の設定)」 を参照してください。 |
| Replace Priority | 条件に合ったパケットの DSCP 値は指定した値に入れ替わります。 |
| Replace DSCP (0-63) | スイッチは本画面で指定した基準に一致するパケットの DSCP をチェックボックスの右側のフィールド内に指定した値に書き換えます。ACL ルールがプライオリティと IPv4 パケットの両方を変更するために追加されても、チップの制限のためそれらの一方しか変更できません。プライオリティと DSCP の両方が変更されるように設定されている場合は、現在のプライオリティを変更します。 |
| Replace ToS Precedence (0-7) | 出力パケットの IP 優先度が新しい値に変更されます。操作の優先度なしで使用すると、デフォルト TC にパケットは送信されます。 |
| Time Range Name | チェックボックスをクリックし、「Time Range」画面に設定済みのタイムレンジ設定名を入力します。このアクセスルールをスイッチで実行する場合、ここに特定の時間を設定します。 |
| Counter | 「Counter」機能を「Enabled」(有効) / 「Disabled」(無効) にします。カウンタ機能は、アクセスルールに一致するパケット数を記録するために使用されます。本機能はオプションです。初期値は無効です。 |
| Mirror Group ID (1-4) | 「Action」で「Mirror」を選択した場合に、ミラーグループ ID を指定します。 |
| Ports / VLAN Name / VLAN ID | このルールに適用するオブジェクトの選択または入力を行います。 <ul style="list-style-type: none"> Ports - ポート番号またはポート範囲を入力します。ポートの範囲を指定する際には、本画面中の「Access ID」フィールドの「Auto assign」チェックボックスを選択しておく必要があります。選択しないと、エラーメッセージが表示され、アクセスルールの設定が行われません。 VLAN Name - VLAN 名を入力します。 VLAN ID - VID を入力します。 |

パケットコンテンツマスクのアクセスルールを設定するためには、必ず「Apply」ボタンをクリックし、設定内容を適用してください。「<<Back」ボタンをクリックし、変更を破棄して前のページに戻ります。

作成したルールの詳細の参照

「Access Rule List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

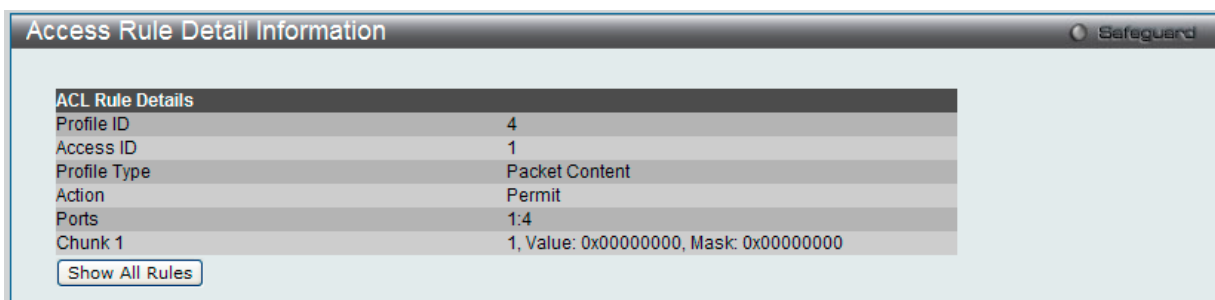


図 11-30 Access Rule Detail Information - パケットコンテンツ画面

「Show All Rules」ボタンをクリックすると、「Access Rule List」画面に戻ります。

CPU Access Profile List (CPU アクセスプロファイルリスト)

チップセットの制限やスイッチのセキュリティの必要性などから、本スイッチは、CPU インタフェースフィルタリング機能を持っています。この追加機能によって CPU インタフェース向けのパケットアクセスルールリストの作成が可能になり、動作時のセキュリティが高くなります。既に説明したアクセスプロファイル機能と似た方法で CPU インタフェースフィルタリングは CPU に到達するイーサネット、IP およびパケットコンテンツマスクのパケットヘッダを調べて、ユーザ設定に基づきそれらを転送もしくはフィルタリングします。そして CPU フィルタリングの追加機能として、CPU フィルタリングでは多彩なルールのリストをあらかじめ用意しておき、必要に応じてグローバルに有効 / 無効を設定することができます。

注意 CPU インタフェースフィルタリングは、プロトコル変換または管理アクセスなど直接スイッチへのトラフィックアクセスを制御するのに使用されます。CPU インタフェースフィルタリングルールは正常な L2/3 トラフィックの送信には影響ありません。しかし、不適当な CPU インタフェースフィルタリングルールによって、ネットワークは不安定になる可能性があります。

CPU 用のアクセスプロファイルの作成は2段階に分かれます。はじめにフレームのどの部分を調べるのか、送信元 MAC アドレスか、送信先 IP アドレスか、などを決定します。次に、そのフレームに対してどのような処理を行うのかという基準になる値を入力します。詳しくは以下で2つに分けて説明します。

動作状態を変更するためには、ラジオボタンを使用して、CPU インタフェースフィルタリング機能をグローバルに「Enabled」(有効)または「Disabled」(無効)にします。

「Enabled」を選択するとスイッチは CPU パケットを詳しく調べます。「Disabled」にするとこの動作は行われません。

ACL > CPU Access Profile List の順にメニューをクリックし、以下の画面を表示します。

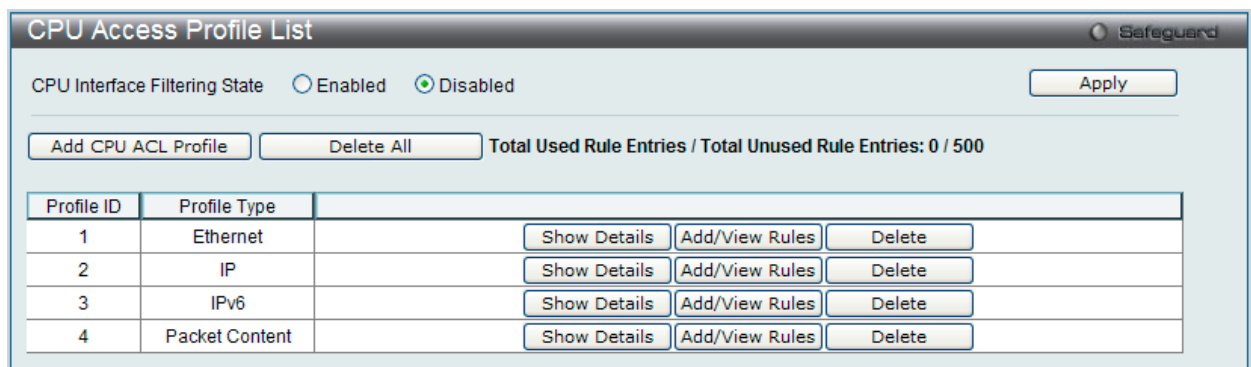


図 11-31 CPU Access Profile List 画面

| 項目 | 説明 |
|-------------------------------|--|
| CPU Interface Filtering State | CPU インタフェースフィルタリング状態を有効または無効にします。「Apply」ボタンをクリックして行った変更を適用します。 |
| Add CPU ACL Profile | CPU ACL リストにエンTRIESを追加します。 |
| Delete All | テーブルからすべてのアクセスプロファイルを削除します。 |
| Show Details | 指定プロファイル ID エントリに関する情報を表示します。 |
| Add/View Rules | 指定プロファイル ID 内の CPU ACL ルールの参照または追加を行います。 |
| Delete | 指定エンTRIESを削除します。 |

「Add CPU ACL Profile」画面には 4 種類あります。:

イーサネット (MAC アドレスベース) プロファイル設定用、IPv6 アドレスベースプロファイル設定用、IPv4 アドレスベースプロファイル設定用およびパケットコンテンツマスクプロファイル設定用です。

CPU アクセスプロファイルの作成 (Ethernet)

CPU アクセスプロファイルを作成し、プロファイルにルールを作成します。

以下の画面では、ラジオボタンを使用し、「CPU Interface Filtering State」をグローバルに有効または無効にし、動作状態の変更をします。

ACL > CPU Access Profile List の順でメニューをクリックし、以下の画面を表示します。



図 11-32 CPU Access Profile List 画面

スイッチに作成した CPU アクセスプロファイルリストを表示します。各タイプに1つのアクセスプロファイルが説明のために作成されています。「CPU Interface Filtering State」に「Enabled」を選択すると、スイッチは CPU パケットを詳しく調べます。また、「Disabled」を選択すると、調べません。

エントリの設定の参照

該当の「Show Details」ボタンをクリックします。

CPU Access Profile List のエントリの削除

エントリを削除するためには、エントリ横の「Delete」ボタンをクリックします。すべてのエントリを削除するためには、「Delete All」ボタンをクリックします。

CPU アクセスプロファイルリストの新規登録

「Add CPU ACL Profile」ボタンをクリックし、以下の画面を表示します。

イーサネットの「Add CPU ACL Profile」画面

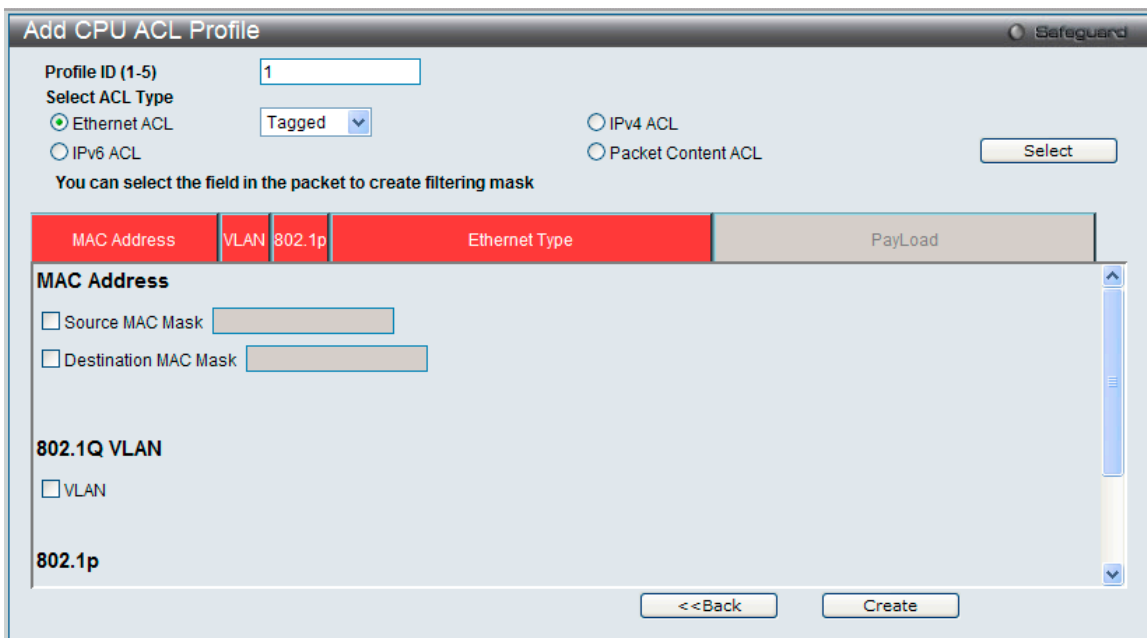


図 11-33 Add CPU ACL Profile - Ethernet 画面

「Add CPU ACL」画面で「Select Profile ID」（プロファイル ID）を指定し、「Select All Type」（ACL タイプ）に「Ether ACL」を選択して「Select」ボタンをクリックします。画面上部のボックスをクリックすると赤色に変わり、設定用項目が表示されます。

以下の項目を設定します。

| 項目 | 説明 |
|--|---|
| Select Profile ID | プロファイルのための固有の識別番号を指定します。1 から 5 が指定できます。 |
| Select ACL Type | Ethernet (MAC アドレス)、IPv4 アドレス、IPv6 アドレス、または Packet Content の中からプロファイルのベースを指定します。Type の変更に伴いメニューも変わります。ここでは「Ethernet」を選択します。 • Ethernet - パケットヘッダのレイヤ 2 部分を対象にします。 |
| 以下のオプションを指定すると各フレームヘッダのプロトコルタイプを調べます。基準にどのようなプロトコルを含めるかを指定します。 | |
| MAC Address | <ul style="list-style-type: none"> Source MAC Mask - 送信元 MAC アドレスをマスクする MAC アドレスを指定します。 Destination MAC Mask - 送信先 MAC アドレスをマスクする MAC アドレスを指定します。 |
| 802.1Q VLAN | パケットヘッダの 802.1Q VLAN 識別子を調べて、部分的もしくは全体を転送基準として使用します。 • VLAN Mask (0-FFF) - VLAN マスクを指定します。 |
| 802.1p | アクセスルールを設定する 802.1p プライオリティ値を指定できるようになります。 |
| Ethernet Type | 各フレームヘッダの Ethernet Type 値を調べます。 |

「Create」 ボタンをクリックし、このエントリをスイッチに保存します。

作成したプロファイルの詳細の参照

「CPU Access Profile List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

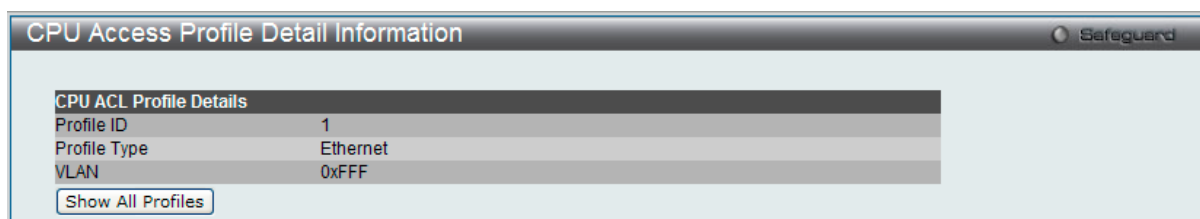


図 11-34 CPU Access Profile Detail Information - Ethernet 画面

「Show All Profiles」ボタンをクリックすると、「CPU Access Profile List」画面に戻ります。

作成した CPU アクセスプロファイルに対するルールの設定手順 (Ethernet)

Ethernet アクセスルールの設定

1. 「CPU Access Profile List」画面を表示します。



図 11-35 CPU Access Profile List 画面

2. 「CPU Access Profile List」画面を表示し、イーサネットエントリの「Add/View Rules」ボタンをクリックして以下の画面を表示します。

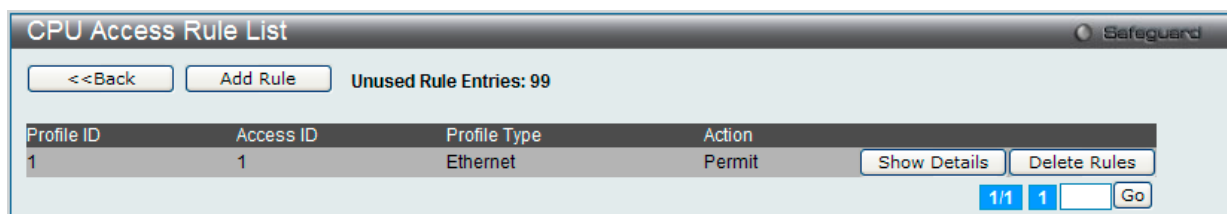


図 11-36 CPU Access Rule List - Ethernet 画面

「Show Details」ボタンをクリックし、作成した指定ルールに関する詳しい情報を表示します。

「Delete Rules」ボタンをクリックして、指定エントリを削除します。

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

既に作成したルールの削除

該当の「Delete Rules」ボタンをクリックします。

新しいルールの作成

「Add Rule」 ボタンをクリックし、以下の画面を表示します。

図 11-37 Add Access Rule - Ethernet 画面

以下の項目を設定します。

| 項目 | 説明 |
|-------------------------|---|
| Rule Detail | |
| Access ID (1-100) | それぞれのルールに固有の番号を指定します。1 から 100 が指定できます。 • Auto Assign - 選択すると、作成中のルールに自動で Access ID を割り当てます。 |
| VLAN Name | 設定済みの VLAN 名を入力します。スイッチはパケットヘッダの VLAN を確認し、その結果をパケット送信の基準 (または基準の一部) とします。 |
| VLAN ID | 設定済みの VLAN ID を入力します。スイッチはパケットヘッダの VLAN を確認し、その結果をパケット送信の基準 (または基準の一部) とします。 |
| Source MAC Address | 送信元 MAC アドレスの MAC アドレスマスクを指定します。 |
| Destination MAC Address | 送信先 MAC アドレスの MAC アドレスマスクを入力します。 |
| 802.1p (0-7) | アクセスプロファイルは、ここで指定する 802.1p プライオリティ値 (0-7) を持つパケットにのみ適用されます。 |
| Ethernet Type (0-FFFF) | アクセスプロファイルが適用されるパケットヘッダの 802.1Q イーサネットタイプの値を 16 進数 (hex 0x0-0xffff) で指定します。イーサネットタイプは次の形式で指定します。: hex 0x0-0xffff (a-f の半角英文字、と 0-9999 の数字を使用します。) |
| Rule Action | |
| Action | <ul style="list-style-type: none"> Permit - アクセスプロファイルにマッチしたパケットを転送します。この時新しいルールが追加されることがあります (以下参照)。 Deny - Deny - スイッチはアクセスプロファイルに一致するパケットを送信せずにフィルタリングします。 |
| Time Range Name | チェックボックスをクリックし、「Time Range」画面に設定済みのタイムレンジ設定名を入力します。このアクセスルールをスイッチで実行する場合、ここに特定の時間を設定します。 |
| Ports | 設定するポート範囲を指定します。 |

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

作成したルールの詳細の参照

「CPU Access Rule List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

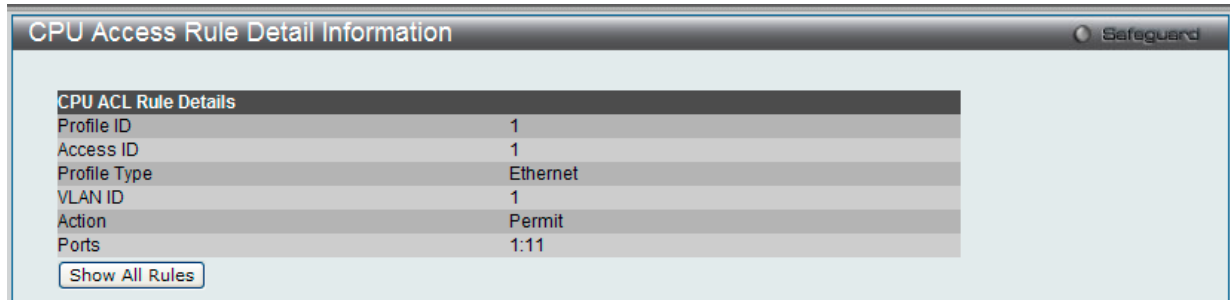


図 11-38 CPU Access Rule Detail Information - Ethernet 画面

「Show All Rules」ボタンをクリックすると、「CPU Access Rule List」画面に戻ります。

CPU アクセสプロファイルの作成 (IPv4)

CPU アクセスプロファイルを作成し、プロファイルにルールを作成します。

以下の画面では、ラジオボタンを使用し、CPU Interface Filtering State をグローバルに有効または無効にし、動作状態の変更をします。

ACL > CPU Access Profile List の順でメニューをクリックし、以下の画面を表示します。



図 11-39 CPU Access Profile List 画面

スイッチに作成した CPU アクセスプロファイルリストを表示します。1つのアクセスプロファイルが説明のために作成されています。「CPU Interface Filtering State」に「Enabled」を選択すると、スイッチは CPU パケットを詳しく調べます。また、「Disabled」を選択すると、調べません。

エントリの設定の参照

該当の「Show Details」ボタンをクリックします。

CPU Access Profile List のエントリの削除

エントリを削除するためには、エントリ横の「Delete」ボタンをクリックします。すべてのエントリを削除するためには、「Delete All」ボタンをクリックします。

CPU アクセスプロファイルリストの新規登録

「Add CPU ACL Profile」ボタンをクリックし、以下の画面を表示します。

IPv4 の「Add CPU ACL Profile」画面

図 10-38 Add CPU ACL Profile - IPv4 画面

「Add CPU ACL」画面で「Select Profile ID」（プロファイル ID）を指定し、「Select All Type」（ACL タイプ）に「IPv4 ACL」を選択します。さらに、隣接する欄で設定するフレームヘッダ（ICMP、IGMP、TCP、UDP、Protocol ID）を指定して「Select」ボタンをクリックします。画面上部のボックスをクリックすると赤色に変わり、設定用項目が表示されます。

以下の項目を IP（IPv4）フィルタに設定できます。

| 項目 | 説明 |
|--|---|
| Select Profile ID | プロファイルのための固有の識別番号を指定します。1 から 5 が指定できます。 |
| Select ACL Type | Ethernet（MAC アドレス）、IPv4 アドレス、IPv6 アドレス、または Packet Content の中からプロファイルのベースを指定します。Type の変更に伴いメニューも変わります。ここでは「IPv4」を選択します。 ・ IPv4 - フレームヘッダの IP アドレスを対象にします。 |
| 以下のオプションを指定すると各フレームヘッダのプロトコルタイプを調べます。基準にどのようなプロトコルを含めるかを指定します。 | |
| 802.1Q VLAN | パケットヘッダの 802.1Q VLAN 識別子を調べて、部分的もしくは全体を転送基準として使用します。 ・ VLAN - VLAN マスクを指定します。 ・ VLAN Mask (0-FFF) - VLAN マスクを指定します。 |
| IPv4 DSCP | このオプションを指定すると各パケットヘッダの DiffServ コードを調べて、部分的もしくは全体を転送基準として使用します。 |
| IPv4 Address | 転送決定の基準として使用されます。 ・ Source IP Mask - 送信元 IP アドレスをマスクする IP アドレスを指定します。例: 255.255.255.255 ・ Destination IP Mask - 送信先 IP アドレスをマスクする IP アドレスを指定します。例: 255.255.255.255 |
| Protocol: 各フレームヘッダのプロトコルタイプを調べます。転送基準にどのようなプロトコルを含めるかを指定します。 | |
| ICMP | それぞれのフレームヘッダの「Internet Control Message Protocol」（ICMP）項目を調べます。アクセスプロファイルが適用するタイプ（「ICMP Type」または「ICMP Code」）を選択します。 |
| IGMP | それぞれのフレームヘッダの「Internet Group Management Protocol」（IGMP）項目を調べます。アクセスプロファイルが適用するタイプ「IGMP Type」を選択します。 |
| TCP | 転送基準となる受信したパケットの TCP ポート番号を使用します。TCP を選ぶと送信元ポートマスク (source port mask) と（もしくは）送信先ポートマスク (dest port mask) を指定する必要があります。 - Source Port Mask (0-FFFF) - フィルタリングしたい送信元ポートをマスクする TCP ポートを 16 進数 (hex 0x0-0xffff) で指定します。 - Destination Port Mask (0-FFFF) - フィルタリングしたい送信先ポートをマスクする TCP ポートを 16 進数 (hex 0x0-0xffff) で指定します。 - TCP Flag Bits - フィルタするフラグビットを指定します。フラグビットはパケットがどのような振る舞いをするかを決定するパケットの一部です。パケットのフラグビットでフィルタリングするには TCP 項目のフラグビットに一致する内容のボックスをチェックします。URG (urgent)、ACK (acknowledgement)、PSH (push)、RST (reset)、SYN (synchronize)、FIN (finish)、または Check All (すべて) を選ぶことができます。 |

| 項目 | 説明 |
|-------------|--|
| UDP | <p>転送基準となる受信したパケットのUDPポート番号を使用します。UDPを選ぶと送信元ポートマスクと(または)送信先ポートマスクを指定する必要があります。</p> <ul style="list-style-type: none"> Source Port Mask (0-FFFF) - フィルタリングする送信元ポートをマスクするUDPポートを16進数(hex 0x0-0xffff)で指定します。 Destination Port Mask (0-FFFF) - フィルタリングする送信先ポートをマスクするTCPポートを16進数(hex 0x0-0xffff)で指定します。 |
| Protocol ID | <p>Protocol ID Maskをチェックし、マスクするパケットヘッダのprotocol IDを定義する値を指定します。</p> <ul style="list-style-type: none"> Protocol ID Mask (0-FF) - IPヘッダの後のマスクオプションに定義する値を指定します。 User Define (0-FFFFFFF) - ユーザ定義のレイヤ4パートマスク値を指定します。 |

「Create」ボタンをクリックし、このエントリをスイッチに保存します。

「<<Back」ボタンをクリックし、変更を破棄して前のページに戻ります。

作成したプロファイルの詳細の参照

「CPU Access Profile List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。



図 11-40 CPU Access Profile Detail Information - IP (IPv4) 画面

「Show All Profiles」ボタンをクリックすると、「CPU Access Profile List」画面に戻ります。

作成したCPUアクセスプロファイルに対するルールの設定手順 (IP) :

IP アクセッスルールの設定

1. 「CPU Access Profile List」画面を表示します。



図 11-41 CPU Access Profile List 画面

2. 「CPU Access Profile List」画面を表示し、IP エントリの「Add/View Rules」ボタンをクリックして以下の画面を表示します。

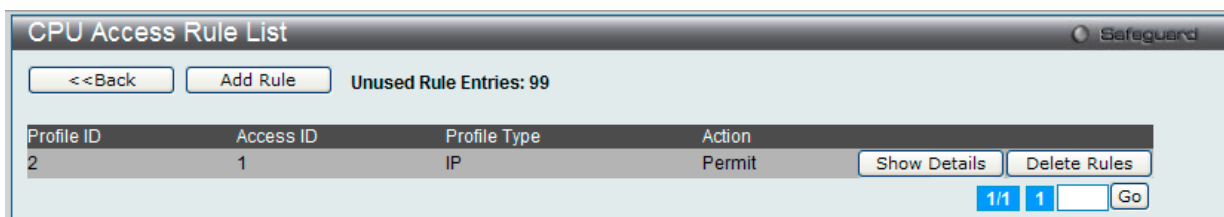


図 11-42 CPU Access Rule List - IP 画面

既に作成したルールの削除

該当の「Delete Rules」ボタンをクリックします。

ルールの新規登録

「Add Rule」 ボタンをクリックします。

図 11-43 Add Access Rule - IP 画面

以下の項目を設定します。

| 項目 | 説明 |
|------------------------|--|
| Rule Detail | |
| Access ID (1-100) | それぞれのルールに固有の番号を指定します。1 から 100 が指定できます。 • Auto Assign - 選択すると、作成中のルールに自動で Access ID を割り当てます。 |
| IGMP | それぞれのフレームヘッダの「Internet Group Management Protocol」(IGMP) 項目を調べます。アクセスプロファイルが適用するタイプ「IGMP Type」を選択します。 |
| VLAN Name | 設定済みの VLAN 名を入力します。スイッチはパケットヘッダの VLAN を確認し、その結果をパケット送信の基準 (または基準の一部) とします。 |
| VLAN ID | 設定済みの VLAN ID を入力します。スイッチはパケットヘッダの VLAN を確認し、その結果をパケット送信の基準 (または基準の一部) とします。 |
| Source IP Address | 送信元の IP アドレスの IP アドレスを入力します。 |
| Destination IP Address | 宛先 IP アドレスの IP アドレスを入力します。 |
| TCP | 転送基準となる受信したパケットの TCP ポート番号を使用します。TCP を選ぶと送信元ポートマスク (source port mask) と (または) 送信先ポートマスク (dest port mask) を指定する必要があります。 - TCP Source Port Mask (0-FFFF) - フィルタリングしたい送信元ポートをマスクする TCP ポートを 16 進数で指定します。 - TCP Destination Port Mask (0-FFFF) - フィルタリングしたい送信先ポートをマスクする TCP ポートを 16 進数で指定します。 - Flag Bits - フィルタするフラグビットを指定します。フラグビットはパケットがどのような振る舞いをするかを決定するパケットの一部です。パケットのフラグビットでフィルタリングするには「TCP」項目のフラグビットに一致する内容のボックスをチェックします。URG (urgent)、ACK (acknowledgement)、PSH (push)、RST (reset)、SYN (synchronize)、FIN (finish) を選ぶことができます。 |
| UDP | 転送基準となる受信したパケットの UDP ポート番号を使用します。UDP を選ぶと送信元ポートマスク (source port mask) と (または) 送信先ポートマスク (dest port mask) を指定する必要があります。 - UDP Source Port Mask - フィルタリングしたい送信元ポートをマスクする UDP ポートを 16 進数 (hex 0x0-0xffff) で指定します。 - UDP Destination Port Mask (0-FFFF) - フィルタリングしたい送信先ポートをマスクする UDP ポートを 16 進数 (hex 0x0-0xffff) で指定します。 |
| Protocol ID | マスクしたいパケットヘッダの Protocol ID Mask を指定します。0-255 の値を入力します。 |

| 項目 | 説明 |
|-----------------|--|
| User | マスクしたいパケットヘッダの Protocol ID Mask を 16 進数 (0-FFFFFFF) で指定します。 |
| DSCP | 各パケットヘッダの DiffServ コードを調べて、部分的もしくは全体を転送基準として使用します。 |
| ICMP | 各フレームヘッダの Internet Control Message Protocol(ICMP) フィールドを調べます。 |
| Rule Action | |
| Action | <ul style="list-style-type: none"> Permit - アクセスプロファイルに一致したパケットを転送します。この時新しいルールが追加されることがあります (以下参照)。 Deny - アクセスプロファイルに一致したパケットは転送せずにフィルタリングします。 |
| Time Range Name | チェックボックスをクリックし、「Time Range」画面に設定済みのタイムレンジ設定名を入力します。このアクセスルールをスイッチで実行する場合、ここに特定の時間を設定します。 |
| Ports | 設定するポート範囲を指定します。 |

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

作成したルールの詳細の参照

「CPU Access Rule List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

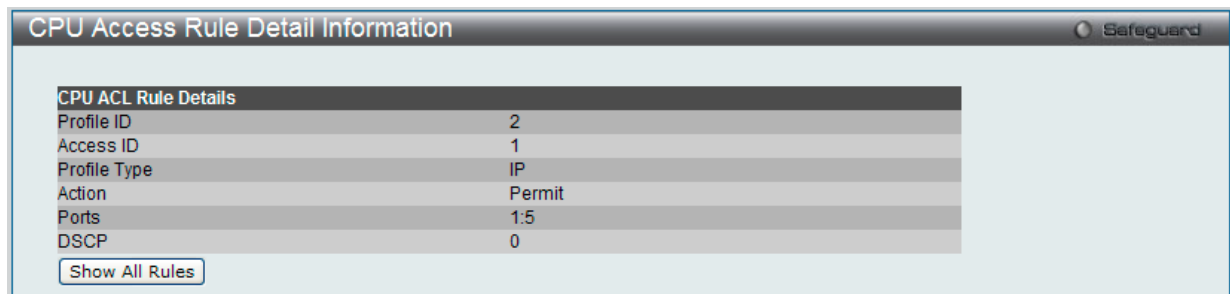


図 11-44 CPU Access Rule Detail Information - IP 画面

「Show All Rules」ボタンをクリックすると、「CPU Access Rule List」画面に戻ります。

CPU アクセスプロファイルの作成 (IPv6)

CPU アクセスプロファイルを作成し、プロファイルにルールを作成します。

以下の画面では、ラジオボタンを使用し、CPU Interface Filtering State をグローバルに有効または無効にし、動作状態の変更をします。

ACL > CPU Access Profile List の順でメニューをクリックし、以下の画面を表示します。



図 11-45 CPU Access Profile List 画面

スイッチに作成した CPU アクセスプロファイルリストを表示します。1つのアクセスプロファイルが説明のために作成されています。「CPU Interface Filtering State」に「Enabled」を選択すると、スイッチは CPU パケットを詳しく調べます。また、「Disabled」を選択すると、調べません。

エントリの設定の参照

該当の「Show Details」ボタンをクリックします。

CPU Access Profile List のエントリの削除

エントリを削除するためには、エントリ横の「Delete」ボタンをクリックします。すべてのエントリを削除するためには、「Delete All」ボタンをクリックします。

CPU アクセスプロファイルリストの新規登録

「Add CPU ACL Profile」 ボタンをクリックし、以下の画面を表示します。

IPv6 の「Add CPU ACL Profile」画面

図 11-46 Add CPU ACL Profile - IPv6 画面

「Add CPU ACL」画面で「Select Profile ID」（プロファイル ID）を指定し、「Select All Type」（ACL タイプ）に「IPv6 ACL」を選択して「Select」ボタンをクリックします。画面上部のボックスをクリックすると赤色に変わり、設定用項目が表示されます。

以下の項目を IP（IPv6）フィルタに設定できます。

| 項目 | 説明 |
|--|---|
| Select Profile ID | プロファイルのための固有の識別番号を指定します。1 から 5 が指定できます。 |
| Select ACL Type | Ethernet（MAC アドレス）、IPv4 アドレス、IPv6 アドレス、または Packet Content の中からプロファイルのベースを指定します。Type の変更に伴いメニューも変わります。ここでは、「IPv6」を選択します。 ・ IPv6 - フレームヘッダの IP アドレスを対象にします。 |
| 以下のオプションを指定すると各フレームヘッダのプロトコルタイプを調べます。基準にどのようなプロトコルを含めるかを指定します。 | |
| IPv6 Class | この項目を選ぶと IPv6 ヘッダの「Class」項目を調べます。「Class」項目は IPv4 における Type of Service (ToS)、「Precedence bits」項目のようなパケットヘッダの一部です。 |
| IPv6 Flow Label | この項目を選ぶと IPv6 ヘッダの「flow label」を調べます。「flow label」は送信元で順番につけられる QoS やリアルタイムサービスパケットのためのデフォルトではない項目です。 |
| IPv6 Address | <ul style="list-style-type: none"> IPv6 Source Mask - 送信元アドレスとして使用する IPv6 アドレスを入力します。 IPv6 Destination Mask - 宛先アドレスとして使用する IPv6 アドレスを入力します。 <p>注意 いかなる場合も、IPv6 Class と IPv6 Flow Label は共に選択し、IPv6 アドレスは単体で選択します。</p> |

「create」ボタンをクリックし、このエントリをスイッチに保存します。

作成したプロファイルの詳細の参照

「CPU Access Profile List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

図 11-47 CPU Access Profile Detail Information - IPv6 画面

「Show All Profiles」ボタンをクリックすると、「CPU Access Profile List」画面に戻ります。

作成した CPU アクセスプロファイルに対するルールの設定手順 (IPv6) :

IPv6 アクセスルールの設定

1. 「CPU Access Profile List」画面を表示します。

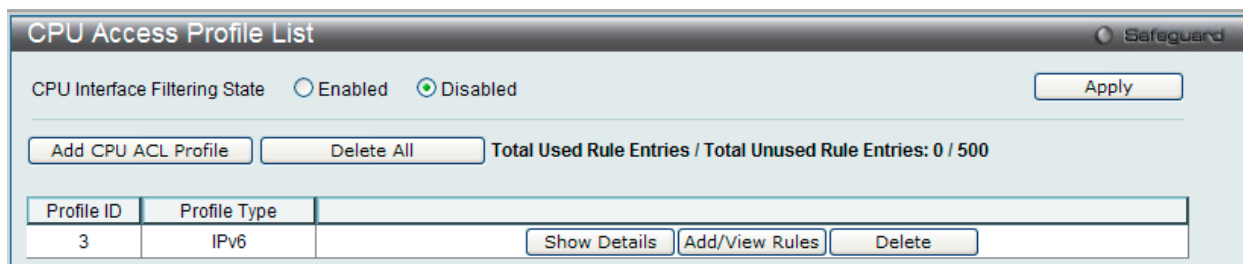


図 11-48 CPU Access Profile List 画面

2. 「CPU Access Profile List」画面を表示し、IPv6 エントリの「Add/View Rules」ボタンをクリックして以下の画面を表示します。

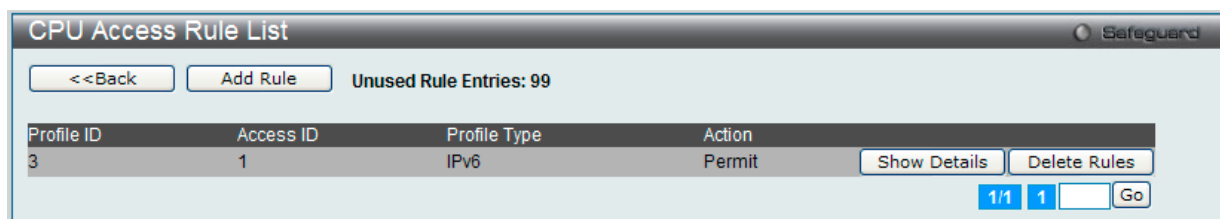


図 11-49 CPU Access Rule List - IPv6 画面

既に作成したルールの削除

「Show All Rules」ボタンをクリックすると、「CPU Access Rule List」画面に戻ります。該当の「Delete Rules」ボタンをクリックします。

ルールの新規登録

「Add Rule」ボタンをクリックし、以下の画面を表示します。

図 11-50 Add Access Rule - IPv6 画面

ACL (ACL機能の設定)

以下の項目を設定します。

| 項目 | 説明 |
|--------------------------|--|
| Rule Detail | |
| Access ID (1-100) | それぞれのルールに固有の番号を指定します。1 から 100 が指定できます。 • Auto Assign - 選択すると、作成中のルールに自動で Access ID を割り当てます。 |
| Class | クラスを入力し、IPv6 ヘッダの「Class」フィールドを調べます。本フィールドは IPv4 における「Type of Service(ToS)」、「Precedence bits」フィールドのようなパケットヘッダの一部です。 |
| Flow Label | この項目を選ぶと IPv6 ヘッダの flow label 項目を調べます。flow label 項目は送信元で順番につけられる QoS やリアルタイムサービスパケットのためのデフォルトではない項目です。 |
| IPv6 Source Address | IPv6 送信元アドレスの IPv6 アドレスを入力します。 |
| IPv6 Destination Address | IPv6 送信先アドレスの IPv6 アドレスを入力します。 |
| Rule Action | |
| Action | • Permit - アクセスプロファイルにマッチしたパケットを転送します。この時新しいルールが追加されることがあります（以下参照）。 • Deny - アクセスプロファイルに一致したパケットは転送せずにフィルタリングします。 |
| Time Range Name | チェックボックスをクリックし、「Time Range」画面に設定済みのタイムレンジ設定名を入力します。このアクセスルールをスイッチで実行する場合、ここに特定の時間を設定します。 |
| Ports | 設定するポート範囲を指定します。 |

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

作成したルールの詳細の参照

「CPU Access Rule List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

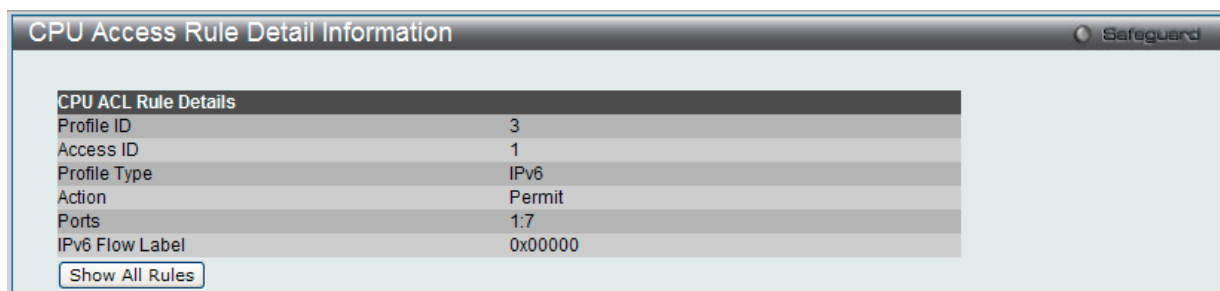


図 11-51 CPU Access Rule Detail Information - IPv6 画面

「Show All Rules」ボタンをクリックすると、「CPU Access Rule List」画面に戻ります。

CPU アクセスプロファイルの作成 (パケットコンテンツ)

CPU アクセスプロファイルを作成し、プロファイルにルールを作成します。

以下の画面では、ラジオボタンを使用し、「CPU Interface Filtering State」をグローバルに有効または無効にし、動作状態の変更をします。

ACL > CPU Access Profile List の順でメニューをクリックし、以下の画面を表示します。

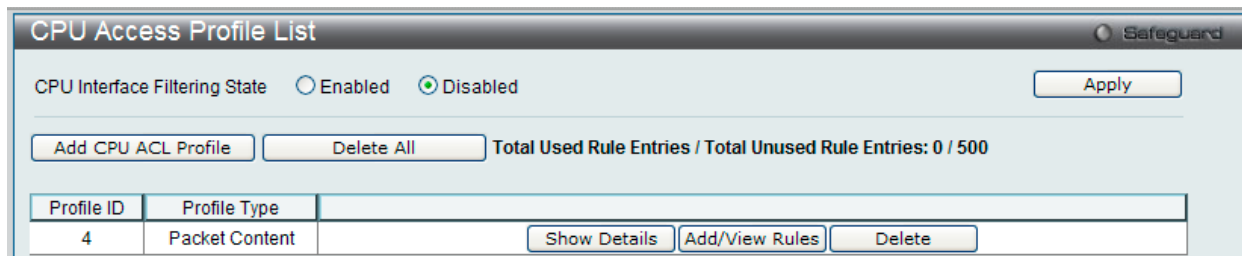


図 11-52 CPU Access Profile List 画面

本画面は、スイッチに作成した CPU アクセスプロファイルリストを表示します。各タイプに 1 つのアクセスプロファイルが説明のために作成されています。「Enabled」を選択すると、スイッチは CPU パケットを詳しく調べます。また、「CPU Interface Filtering State」に「Disabled」を選択すると、調べません。

エントリの設定の参照

該当の「Show Details」ボタンをクリックします。

CPU Access Profile List のエントリの削除

エントリを削除するためには、エントリ横の「Delete」ボタンをクリックします。すべてのエントリを削除するためには、「Delete All」ボタンをクリックします。

CPU アクセスプロファイルリストの新規登録

「Add CPU ACL Profile」ボタンをクリックし、以下の画面を表示します。

パケットコンテンツの「Add CPU ACL Profile」画面

図 11-53 Add CPU ACL Profile - Packet Content 画面

「Add CPU ACL」画面で「Select Profile ID」（プロファイル ID）を指定し、「Select All Type」（ACL タイプ）に「Packet Content ACL」を選択して「Select」ボタンをクリックします。画面上部のボックスをクリックすると赤色に変わり、設定用項目が表示されます。

以下の項目を Packet Content フィルタに設定できます。

| 項目 | 説明 |
|-------------------|---|
| Select Profile ID | プロファイルのための固有の識別番号を指定します。1 から 5 が指定できます。 |
| Select ACL Type | Ethernet（MAC アドレス）、IPv4 アドレス、IPv6 アドレス、または Packet Content の中からプロファイルのベースを指定します。Type の変更に伴いメニューも変わります。ここでは「Packet Content」を選択します。 <ul style="list-style-type: none"> Packet Content - パケットヘッダの内容をマスクして隠します。 |
| Packet Content | 1個のパケット内で最大5個のパケットコンテンツオフセットチャンクを同時に検証し、そのフレームコンテンツオフセット、マスクおよびレイヤを規定することができます。5個のパケットコンテンツチャンクオフセットが設定できます。パケットコンテンツチャンクマスクは4バイトを示します。最大5個までパケットコンテンツオフセットチャンクを選択することが可能です。 パケットヘッダにマスクを開始するオフセットを指定します。 <ul style="list-style-type: none"> Offset 0-15 - 16 進数でパケットの最初から 15 バイト目までのマスクを指定します。 Offset 16-31 - 16 進数でパケットの 16 バイト目から 31 バイト目までのマスクを指定します。 Offset 32-47 - 16 進数でパケットの 32 バイト目から 47 バイト目までのマスクを指定します。 Offset 48-63 - 16 進数でパケットの 48 バイト目から 63 バイト目までのマスクを指定します。 Offset 64-79 - 16 進数でパケットの 64 バイト目から 79 バイト目までのマスクを指定します。 <p>注意 作成できるパケットコンテンツマスクプロファイルは1つだけです。本スイッチは、高度なパケットコンテンツマスク（またはパケットコンテンツアクセスコントロールリスト -ACL として知られる）機能を使用して、ARP Spoofing などの一般的なネットワーク攻撃を効果的に軽減することができます。このため、パケットコンテンツ ACL が異なるプロトコル層におけるパケットのどんな指定コンテンツも検証できます。</p> |

「Create」ボタンをクリックし、このエントリをスイッチに保存します。

作成したプロファイルの詳細の参照

「CPU Access Profile List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

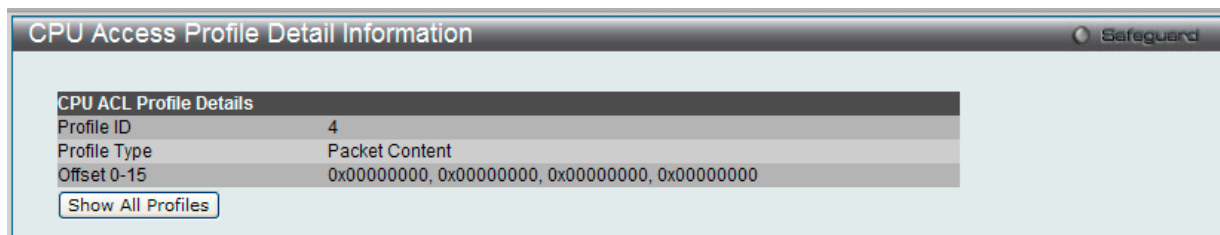


図 11-54 CPU Access Profile Detail Information - Packet Content 画面

「Show All Profiles」ボタンをクリックすると、「CPU Access Profile List」画面に戻ります。

作成した CPU アクセスプロファイルに対するルールの設定手順 (Packet Content) :

Packet Content アクセスルールの設定

1. 「CPU Access Profile List」画面を表示します。



図 11-55 CPU Access Profile List 画面

2. 「CPU Access Profile List」画面を表示し、Packet Content エントリの「Add/View Rules」ボタンをクリックして以下の画面を表示します。

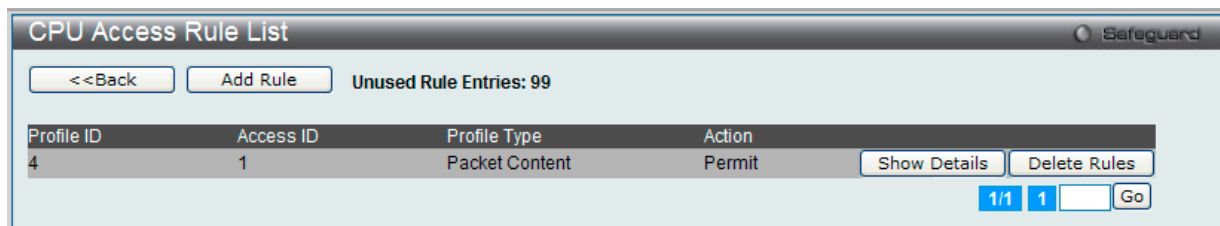


図 11-56 CPU Access Rule List - Packet Content 画面

作成済みのルールの削除

該当の「Delete Rules」ボタンをクリックします。

ルールの新規作成

「Add Rule」ボタンをクリックします。

図 11-57 Add Access Rule - Packet Content 画面

| 項目 | 説明 |
|-------------------|--|
| Rule Detail | |
| Access ID (1-100) | それぞれのルールに固有の番号を指定します。1 から 100 が指定できます。 <ul style="list-style-type: none"> Auto Assign - 選択すると、作成中のルールに自動で Access ID を割り当てます。 |
| Offset | パケットヘッダにマスクを開始するオフセットを指定します。 <ul style="list-style-type: none"> Offset 0-15 - 16 進数でパケットの最初から 15 バイト目までのマスクを指定します。 Offset 16-31 - 16 進数でパケットの 16 バイト目から 31 バイト目までのマスクを指定します。 Offset 32-47 - 16 進数でパケットの 32 バイト目から 47 バイト目までのマスクを指定します。 Offset 48-63 - 16 進数でパケットの 48 バイト目から 63 バイト目までのマスクを指定します。 Offset 64-79 - 16 進数でパケットの 64 バイト目から 79 バイト目までのマスクを指定します。 |
| Rule Action | |
| Action | <ul style="list-style-type: none"> Permit - アクセスプロファイルにマッチしたパケットを転送します。この時新しいルールが追加されることがあります (以下参照)。 Deny - アクセスプロファイルに一致したパケットは転送せずにフィルタリングします。 |
| Time Range Name | チェックし、「Time Range」画面に設定済みのタイムレンジ設定名を入力します。このアクセスルールをスイッチで実行する場合、ここに特定の時間を設定します。 |
| Ports | 設定するポート範囲を指定します。 |

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

作成したルールの詳細の参照

「CPU Access Rule List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

図 11-58 CPU Access Rule Detail Information - Packet Content 画面

「Show All Rules」ボタンをクリックすると、「CPU Access Rule List」画面に戻ります。

「<<Back」ボタンをクリックし、変更を破棄して前のページに戻ります。

ACL Finder (ACL 検索)

ACL ルール検索を使用して、特定のポートに割り当てられたすべてのルールを確認し、すばやく既存のルールを編集します。

ACL > ACL Finder の順にメニューをクリックし、以下の画面を表示します。

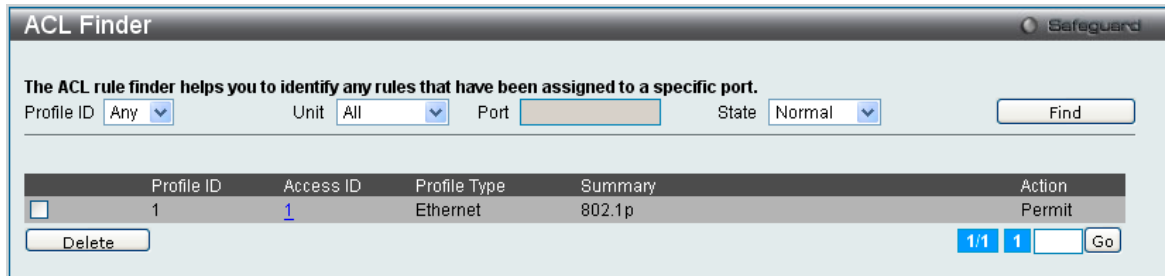


図 11-59 ACL Finder 画面

本画面には以下の項目があります。

| 項目 | 説明 |
|------------|---|
| Profile ID | ルールの特定ののために ACL ルール検索でプロファイル ID を選択します。 |
| Unit | 設定するユニットを選択します。 |
| Port | ルールの特定ののために ACL ルール検索でポート番号を入力します。 |
| State | プルダウンメニューを使用して状態を選択します。 <ul style="list-style-type: none"> Normal - 通常の ACL ルールを検索します。 CPU - CPU ACL ルールを検索します。 Egress - Egress ACL ルールを検索します。 |

定義済みの ACL エントリの検索

エントリを検索するためには、「Profile ID」でプロファイル ID を、「Port」で参照するポートを指定し、さらに「State」を定義して、「Find」ボタンをクリックします。画面下半分のテーブルにエントリは表示されます。

エントリの削除

削除するエントリのラジオボタンをチェックし、「Delete」ボタンをクリックします。

プロファイルの参照

参照するエントリの「[Access ID](#)」のリンクをクリックします。

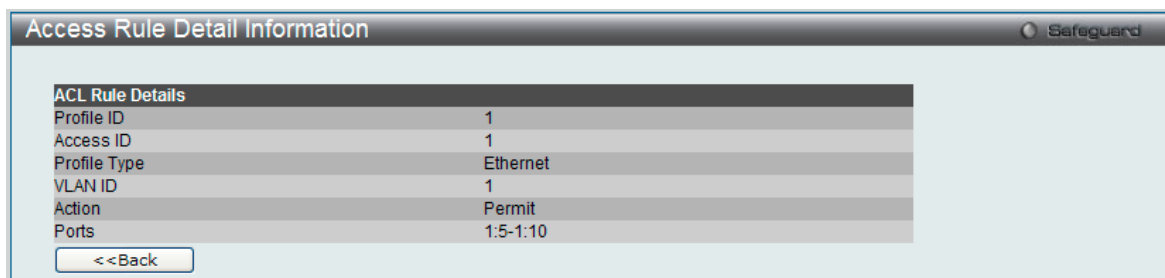


図 11-60 Access Rule Detail Information 画面

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

ACL Flow Meter (ACL フローメータ)

ACL フローメータを設定する前に、ユーザが知っておく必要がある頭文字語および項目のリストは次の通りです。

trTCM - Two Rate Three Color Marker. これは、srTCM と共にメータリングおよびパケットフローをマーキングするためにスイッチで可能な 2 つの方式です。trTCM が IP フローを計測し、2 つのレート (CIR および PIR) に基づいて、色でマークします。

CIR - Committed Information Rate. trTCM と srTCM の両方に共通で、CIR は IP パケットのバイト数を計測します。IP パケットのバイト数は、リンクする特定のヘッダではなく、IP ヘッダのサイズを取得することで計測します。trTCM に関しては、パケットフローは、CIR を超過していない場合に緑色でマークされ、CIR を超過している場合に黄色でマークされます。設定される CIR のレートは PIR のレートを超過してはなりません。また、CBS および PBS フィールドを使用して予期しないパケットバーストのために CIR を設定することができます。

- **CBS** - Committed Burst Size. バイト数を計測する場合、CBS は、CIR に関連して、パケットサイズの正常な境界を越えているパケットを特定するために使用されます。IP フローで予想される最も大きい IP パケットを受け入れるために、CBS を設定する必要があります。

PIR - Peak Information Rate. このレートは IP パケットのバイト数で計測されます。IP パケットのバイト数は、リンクする特定のヘッダではなく、IP ヘッダのサイズを取得することで計測します。パケットフローが PIR を超過すると、そのパケットフローは赤でマークされます。CIR のレートと同じかそれ以上になるように PIR を設定する必要があります。

- **PBS** - Peak Burst Size. バイト数を計測する場合、PBS は、PIR に関連して、パケットサイズの正常な境界を越えているパケットを特定するために使用されます。IP フローで予想される最も大きい IP パケットを受け入れるために、PBS を設定する必要があります。

srTCM - Single Rate Three Color Marker. これは、trTCM と共にメータリングおよびパケットフローをマーキングするためにスイッチで可能な 2 つの方式です。srTCM は、設定された CBS と EBS に基づいて IP パケットフローをマークします。CBS に到達しないパケットフローは、緑色にマークされ、EBS ではなく CBS を超過している場合、黄色にマークされ、EBS を超過している場合、赤色にマークされます。

CBS - Committed Burst Size. バイト数を計測する場合、CBS は、CIR に関連して、パケットサイズの正常な境界を越えているパケットを特定するために使用されます。IP フローで予想される最も大きい IP パケットを受け入れるために、CBS を設定する必要があります。

EBS - Excess Burst Size. バイト数を計測する場合、EBS は、CIR に関連して、パケットサイズの正常な境界を越えているパケットを特定するために使用されます。EBS は、CBS と同じかさらに大きいレートに設定されます。

DSCP - Differentiated Services Code Point. 色が追加されるパケットヘッダの部分。入力パケットの「DSCP」フィールドを変更することが可能です。ACL フローメータ機能により、入力パケットのレートに基づいて IP パケットフローにカラーコードを付加することができます。以前に説明した通り、2 つのフローメータリングのタイプ (trTCM および srTCM) を選択することができます。パケットフローがカラーコードに置かれる時、その色分けされたレートを超過したパケットで何をすべきかを定めることができます。

緑 - IP フローが緑色のモードである時、設定可能なパラメータは、パケットがその「DSCP」フィールドを変更できる「Conform」フィールドにて設定されます。これは ACL フローメータ機能で許容できるフローレートです。

黄 - IP フローが黄色のモードである時、設定可能なパラメータは、「Exceed」フィールドにて設定されます。超過したパケットを「Permit」(許可) または「Drop」(廃棄) するかを選択します。パケットの「DSCP」フィールドを変更ために選択します。

赤 - IP フローが赤色のモードである時、設定可能なパラメータは、「Violate」フィールドにて設定されます。

超過したパケットを「Permit」(許可) または「Drop」(廃棄) するかを選択します。パケットの「DSCP」フィールドを変更ために選択します。

また、「Counter」を指定することによって超過パケットをカウントできるように選択することができます。

「Counter」を有効にすると、アクセスプロファイル内のカウンタ設定は無効になります。どんな指定時間においても 1 つのフローメータに対して 2 つのカウンタのみ有効になります。

ACL > ACL Flow Meter の順にメニューをクリックし、以下の画面を表示します。

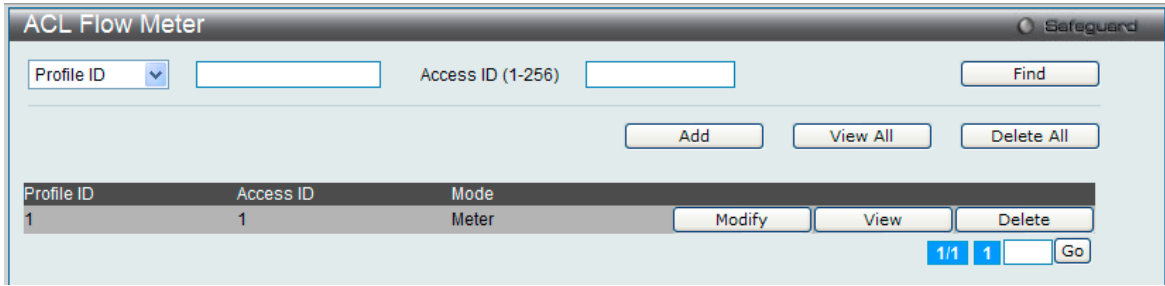


図 11-61 ACL Flow Meter 画面

以下の項目を使用して設定を行います。

| 項目 | 説明 |
|--------------|--|
| Profile ID | ACL フローメータリングパラメータを設定する定義済みプロファイル ID を指定します。 |
| Profile Name | ACL フローメータリングパラメータを設定する定義済みプロファイル名を指定します。 |
| Access ID | ACL フローメータリングパラメータを設定する定義済みアクセス ID を指定します。 |

入力後、「Find」ボタンをクリックします。情報が画面下半分に表示されます。

エントリの削除

対応する「Delete」ボタンをクリックします。すべてのエントリを削除するためには、「Delete All」ボタンをクリックします。

エントリの追加

「Add」ボタンをクリックし、以下の画面を表示します。

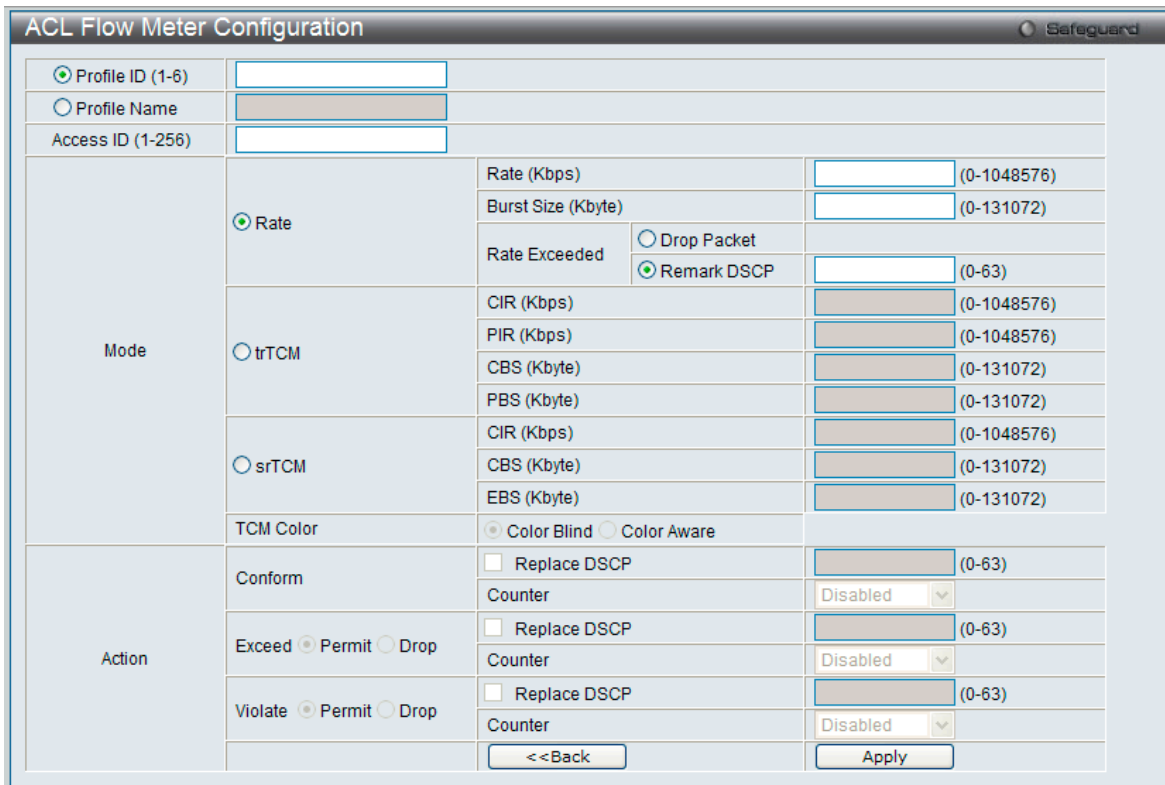


図 11-62 ACL Flow Meter Configuration 画面 - Add

以下の項目を使用して、設定を行います。

| 項目 | 説明 |
|--------------------|--|
| Profile ID | プルダウンメニューから、フローメータリングを設定する定義済みのプロファイル ID を指定します。 |
| Profile Name | フローメータに対するプロファイル名を入力します。 |
| Access ID (1-1024) | ACL フローメータリングを設定する定義済みアクセス ID を 1-1024 の範囲で指定します。 |
| Mode | <p>Rate - シングルレート 2 カラーモードのレートを指定します。</p> <ul style="list-style-type: none"> Rate - フローに規定する帯域幅を Kbps 単位で指定します。 Burst Size - シングルレート 2 カラーモードにバーストサイズを指定します。単位は Kbps です。 Rate Exceeded - シングルレート 2 カラーモードでコミットレートを超過したパケットへの操作を指定します。以下の一つの動作が行われます。: <ul style="list-style-type: none"> - Drop Packet - パケットを直ちに破棄します。 - Remark DSCP - 特定の DSCP をパケットにマークをつけます。高い優先度を持つパケットが破棄されるように設定されます。 <p>trTCM - 「2 レート 3 カラーモード」を指定します。</p> <ul style="list-style-type: none"> CIR - コミット情報レートの値を入力します。単位は Kbps です。CIR は PIR 以下である必要があります。 PIR - ピーク情報レートを指定します。単位は Kbps です。PIR は CIR 以上である必要があります。 CBS - 「コミットバーストサイズ」の値を入力します。単位は Kbps です。 PBS - ピークバーストサイズの値を入力します。単位は Kbps です。 <p>srTCM - 「シングルレート 3 カラーモード」を指定します。</p> <ul style="list-style-type: none"> CIR - コミット情報レートの値を入力します。単位は Kbps です。 CBS - 「コミットバーストサイズ」の値を入力します。単位は Kbps です。 EBS - 「超過バーストサイズ」を指定します。単位は Kbps です。 |
| Action | <p>Conform - 本フィールドは緑色のパケットフローを表します。緑色のパケットフローは、DSCP フィールドを本フィールドで指定された値に書き換える可能性があります。また、「Counter」パラメータを使用することで緑色のパケットをカウントするように選択することができます。</p> <ul style="list-style-type: none"> Replace DSCP - 緑色のフローにあるパケットが本パラメータを使用し、DSCP 値を入力することで、DSCP 値を書き換えることが可能です。 Counter - 緑色のフローにおいて指定された ACL エントリのパケットカウンタを有効または無効にします。 <p>Un-conform - 不適合 (黄色または赤) パケットの DSCP を変更します。</p> <ul style="list-style-type: none"> Replace DSCP - 赤色のフローにあるパケットが本パラメータを使用し、DSCP 値を入力することで、DSCP 値を書き換えることが可能です。 <p>Exceed - 本フィールドは黄色のパケットフローを表します。黄色のパケットフローは超過パケットを許可または廃棄します。これらのパケットの「DSCP」フィールドを割り当てられたフィールドに新しい DSCP 値を入れることで交換することができます。</p> <ul style="list-style-type: none"> Counter - 黄色のフローにおいて指定された ACL エントリのパケットカウンタを有効または無効にします。 <p>Violate - 本フィールドは赤色のパケットフローを表します。赤色のパケットフローは超過パケットを許可または廃棄します。これらのパケットの「DSCP」フィールドを割り当てられたフィールドに新しい DSCP 値を入れることで交換することができます。</p> <ul style="list-style-type: none"> Counter - 赤色のフローにおいて指定された ACL エントリのパケットカウンタを有効または無効にします。 |

「Apply」ボタンをクリックして、設定を適用します。

「ACL Flow Meter」画面に戻るためには、「<<Back」ボタンをクリックします。

エントリの変更

対応する「Modify」ボタンをクリックし、以下の画面を表示します。

図 11-63 ACL Flow Meter Configuration 画面 - Modify

以下の項目を使用して、設定を行います。

| 項目 | 説明 |
|------|--|
| Mode | <p>Rate - シングルレート 2 カラーモードのレートを指定します。</p> <ul style="list-style-type: none"> Rate - フローに規定する帯域幅を Kbps 単位で指定します。 Burst Size - シングルレート 2 カラーモードにバーストサイズを指定します。単位は Kbps です。 Rate Exceeded - シングルレート 2 カラーモードでコミットレートを超過したパケットへの操作を指定します。以下の一つの動作が行われます。: <ul style="list-style-type: none"> Drop Packet - パケットを直ちに破棄します。 Remark DSCP - 特定の DSCP をパケットにマークをつけます。高い優先度を持つパケットが破棄されるように設定されます。 |

「Apply」ボタンをクリックして、設定を適用します。

「ACL Flow Meter」画面に戻るためには、「<<Back」ボタンをクリックします。

エントリの参照

すべてのエントリを参照するためには、「View All」ボタンをクリックします。

エントリを参照するためには、対応する「View」ボタンをクリックし、以下の画面を表示します。

図 11-64 ACL Flow Meter Display 画面

「ACL Flow Meter」画面に戻るためには、「<<Back」ボタンをクリックします。

Egress Access Profile List (Egress アクセスプロファイルリスト)

Egress ACL は、スイッチから送出される場合に、フローごとのパケット処理を実行します。スイッチは、3つのプロファイルタイプ（イーサネット ACL、IPv4 ACL、および IPv6 ACL）をサポートしています。

ACL > Egress Access Profile List の順にメニューをクリックし、以下の画面を表示します。

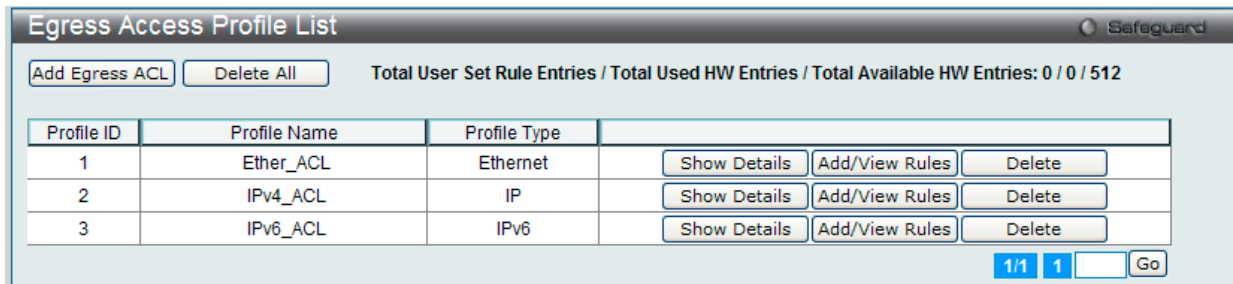


図 11-65 Egress Access Profile List 画面

| 項目 | 説明 |
|--------------------|--|
| Add Egress Profile | Egress アクセスプロファイルリストにエンTRIESを追加します。 |
| Delete All | テーブルからすべてのアクセスプロファイルを削除します。 |
| Show Details | 指定プロファイル ID エントリに関する情報を表示します。 |
| Add/View Rules | 指定プロファイル ID の ACL ルールの参照または追加を行います。 |
| Delete | 指定エンTRIESを削除します。 |
| Go | 複数ページが存在する場合は、ページ番号を入力後、クリックして、特定のページへ移動します。 |

アクセスプロファイルリストの作成 (Ethernet)

イーサネット用のアクセスプロファイルを作成し、プロファイルにルールを作成します。

ACL > Egress Access Profile List の順にメニューをクリックし、以下の画面を表示します。

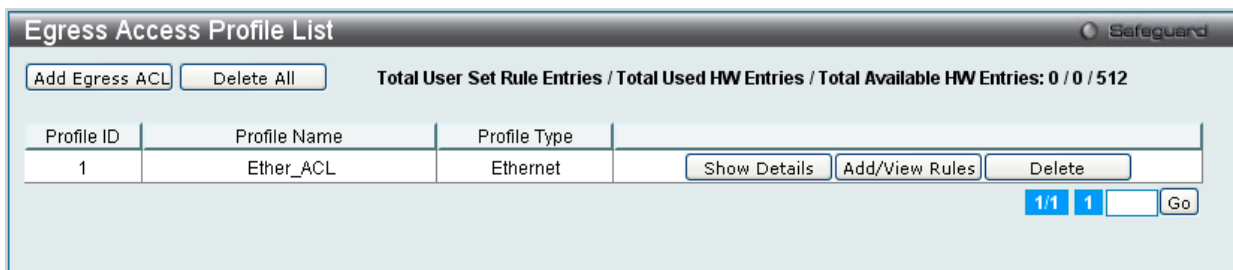


図 11-66 Egress Access Profile List 画面

エンTRIESの削除

エンTRIESを削除するためには、エンTRIES横の「Delete」ボタンをクリックします。すべてのアクセスプロファイルを削除するためには、「Delete All」ボタンをクリックします。

エントリの追加

「Access Profile List」にエントリを追加するには、「Add Egress ACL」ボタンをクリックし、以下の画面を表示します。

イーサネットの「Add ACL Profile」画面

図 11-67 Add Egress ACL Profile - Ethernet ACL 画面

「Profile ID」でプロファイル番号を 1-4 から選択し、「Select ACL Type」で「Ethernet ACL」をチェック後、「Select」ボタンをクリックすることで画面を切り替えることができます。画面上部のボックスをクリックすると、赤色に変わり、設定用項目が表示されます。

以下の項目を Ethernet ACL タイプに設定します。

| 項目 | 説明 |
|--|---|
| Profile ID | プロファイル設定のための固有の識別番号を指定します。1 から 4 が指定できます。 |
| Profile Name | 作成したプロファイルにプロファイル名を入力します。 |
| Select ACL Type | Ethernet (MAC アドレス)、IPv4 アドレス、または IPv6 アドレスからプロファイルのタイプを指定します。Type の変更に伴いメニューも変わります。ここでは、「Ethernet ACL」を選択します。 ・ Ethernet ACL - パケットヘッダのレイヤ 2 部分を検証します。 |
| 以下のオプションを指定すると各フレームヘッダのプロトコルタイプを調べます。転送基準にどのようなプロトコルを含めるかを指定します。 | |
| MAC Address | <ul style="list-style-type: none"> Source MAC Mask - 送信元 MAC アドレスをマスクする MAC アドレスを指定します。例: FF-FF-FF-FF-FF-FF Destination MAC Mask - 送信先 MAC アドレスをマスクする MAC アドレスを指定します。例: FF-FF-FF-FF-FF-FF |
| 802.1Q VLAN | パケットヘッダの 802.1Q VLAN 識別子を調べて、部分的もしくは全体を転送基準として使用します。 <ul style="list-style-type: none"> VLAN - VLAN マスクを指定します。 VLAN Mask (0-FFF) - VLAN マスクを指定します。 |
| 802.1p | 各パケットヘッダの 802.1p プライオリティを調べて、部分的または全体を転送基準として使用します。 |
| Ethernet Type | フレームヘッダでイーサネットタイプの値を調べます。 |

「Create」ボタンをクリックし、プロファイルを作成します。

「<<Back」ボタンをクリックし、変更を破棄して前のページに戻ります。

作成したプロファイルの詳細の参照

「Access Profile List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

図 11-68 Egress Access Profile Detail Information - Ethernet 画面

「Show All Profiles」ボタンをクリックすると、「Egress Access Profile List」画面に戻ります。

作成したアクセスプロファイルに対するルールの設定手順 (Ethernet) :

Ethernet アクセスルールの設定

1. 「Access Profile List」画面を表示します。

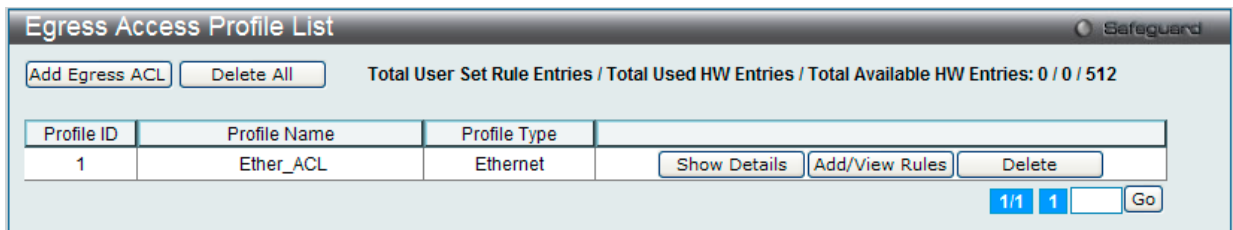


図 11-69 Egress Access Profile List 画面

2. Ethernet エントリの「Add/View Rules」ボタンをクリックし、以下の画面を表示します。

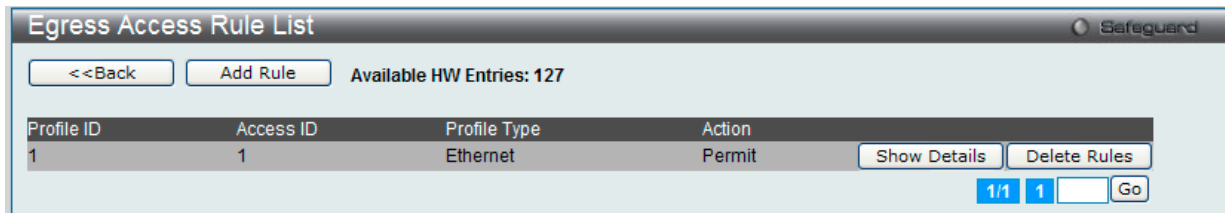


図 11-70 Egress Access Rule List - Ethernet 画面

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。「<<Back」ボタンをクリックし、前のページに戻ります。

作成したルールの削除

該当の「Delete Rules」ボタンをクリックします。

ルールの新規作成

ルールを作成するためには、「Add Rule」ボタンをクリックし、以下の画面を表示します。

図 11-71 Add Access Rule - Ethernet 画面

ACL (ACL機能の設定)

Ethernet のアクセスルールを設定するためには以下の項目を設定して、「Apply」ボタンをクリックします。

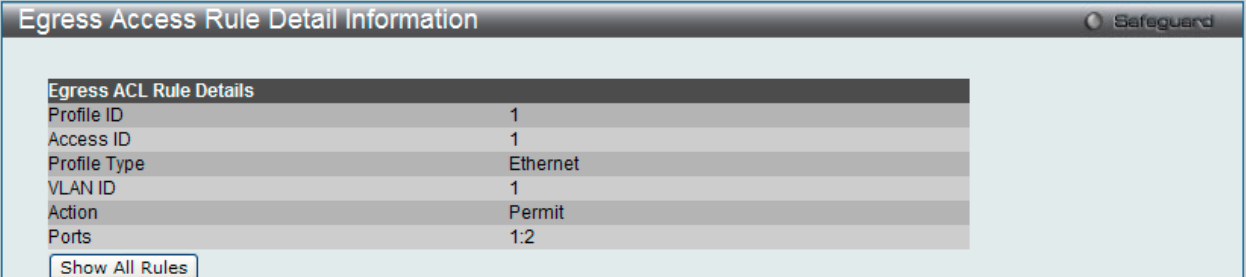
| 項目 | 説明 |
|------------------------------|--|
| Rule Detail | |
| Access ID (1-128) | プロファイル設定のための固有の識別番号を指定します。1 から 128 が指定できます。 • Auto Assign - 本項目をチェックするとスイッチは自動的に作成されるルールに Access ID を割り当てます。 |
| VLAN Name | 設定済みの VLAN 名を入力します。スイッチはパケットヘッダの VLAN を確認し、その結果をパケット送信の基準 (または基準の一部) とします。 |
| VLAN ID | VLAN ID 番号を指定します。 |
| VLAN Mask (0-FFFF) | VLAN マスクを指定します。 |
| Source MAC Address | 送信元 MAC アドレスの MAC アドレスマスクを指定します。 |
| Source MAC Address Mask | 送信元 MAC アドレスの MAC アドレスマスクを 16 進数形式で指定します。 |
| Destination MAC Address | 送信先 MAC アドレスの MAC アドレスマスクを入力します。 |
| Destination MAC Address Mask | 送信先 MAC アドレスの MAC アドレスマスクを 16 進数形式で入力します。 |
| 802.1p (0-7) | 802.1p プライオリティ値を 0-7 で入力します。アクセスプロファイルをこの値を持つパケットに適用します。 |
| Ethernet Type (0-FFFF) | アクセスプロファイルが適用されるパケットヘッダの 802.1Q イーサネットタイプの値を 16 進数 (hex 0x0-0xffff) で指定します。イーサネットタイプは次の形式で指定します。: hex 0x0-0xffff (a-f の半角英文字、と 0-9999 の数字を使用します。) |
| Rule Action | |
| Action | <ul style="list-style-type: none"> Permit - スイッチはアクセスプロファイルに一致するパケットの送信を、以下のフィールドで設定する追加のルールに従って行います。 Deny - スイッチはアクセスプロファイルに一致するパケットを送信せずにフィルタリングします。 Mirror - スイッチはアクセスプロファイルに一致するパケットを「Port Mirroring」画面で定義したポートにミラーリングします。ポートミラーリングが有効で、ターゲットポートが設定されている必要があります。 |
| Priority (0-7) | スイッチが設定した 802.1p デフォルトプライオリティを上書きしたい場合に指定します。このプライオリティにより転送されたパケットがどの CoS キューを使用するかが決まります。この欄を指定するとパケットはこのプライオリティを割り当てられ、対応した CoS キューに転送されます。指定しない場合は、パケットは送出される前に、入力用の 802.1p ユーザプライオリティを元の値に書き換えられます。プライオリティキュー、CoS キューおよび 802.1p マッピングについての詳細な情報については、本マニュアルの 221 ページの「第 10 章 QoS (QoS 機能の設定)」 を参照してください。 |
| Replace Priority | 条件に合ったパケットの DSCP 値は指定した値に入れ替わります。 |
| Replace DSCP (0-63) | スイッチは本画面で指定した基準に一致するパケットの DSCP をチェックボックスの右側のフィールド内に指定した値に書き換えます。ACL ルールがプライオリティと IPv4 パケットの両方を変更するために追加されても、チップの制限のためそれらの一方しか変更できません。プライオリティと DSCP の両方が変更されるように設定されている場合は、現在のプライオリティを変更します。 |
| Time Range Name | チェックボックスをクリックし、「Time Range」画面に設定済みのタイムレンジ設定名を入力します。このアクセスルールをスイッチで実行する場合、ここに特定の時間を設定します。 |
| Counter | 「Counter」機能を「Enabled」(有効) / 「Disabled」(無効) にします。カウンタ機能は、アクセスルールに一致するパケット数を記録するために使用されます。本機能はオプションです。初期値は無効です。 |
| Ports | ポートの範囲を指定する際には、本画面中の「Access ID」フィールドの「Auto assign」チェックボックスを選択しておく必要があります。選択しないと、エラーメッセージが表示され、アクセスルールの設定が行われません。 |
| Port Group ID | アクセスルールに適用するポートグループ ID を指定します。 |
| Port Group Name | アクセスルールに適用するグループ名を指定します。 |
| VLAN Name | アクセスルールに適用する VLAN 名を指定します。 |
| VLAN ID | アクセスルールに適用する VLAN ID を指定します。 |

「<<Back」ボタンをクリックし、変更を破棄してと前のページに戻ります。

「Apply」ボタンをクリックして行った変更を適用します。

作成したプロファイルの詳細の参照

「Access Profile List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。



| Egress ACL Rule Details | |
|-------------------------|----------|
| Profile ID | 1 |
| Access ID | 1 |
| Profile Type | Ethernet |
| VLAN ID | 1 |
| Action | Permit |
| Ports | 1:2 |

Show All Rules

図 11-72 Egress Access Profile Detail Information - Ethernet 画面

「Show All Profiles」ボタンをクリックすると、「Access Profile List」画面に戻ります。

アクセスプロファイルリストの作成 (IPv4)

アクセスプロファイルを作成し、プロファイルにルールを作成します。

ACL > Egress Access Profile List の順にメニューをクリックし、以下の画面を表示します。1つのアクセスプロファイルが説明のために作成されています。

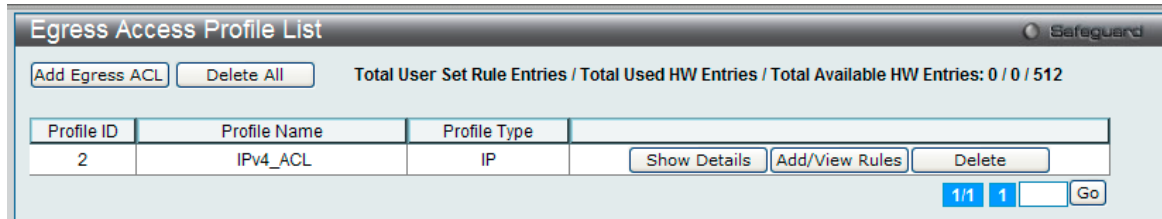


図 11-73 Egress Access Profile List 画面

エントリの削除

エントリを削除するためには、エントリ横の「Delete」ボタンをクリックします。すべてのアクセスプロファイルを削除するためには、「Delete All」ボタンをクリックします。

エントリの追加

「Access Profile List」にエントリを追加するには、「Add ACL Profile」ボタンをクリックし、以下の画面を表示します。

IPv4 の「Add ACL Profile」画面

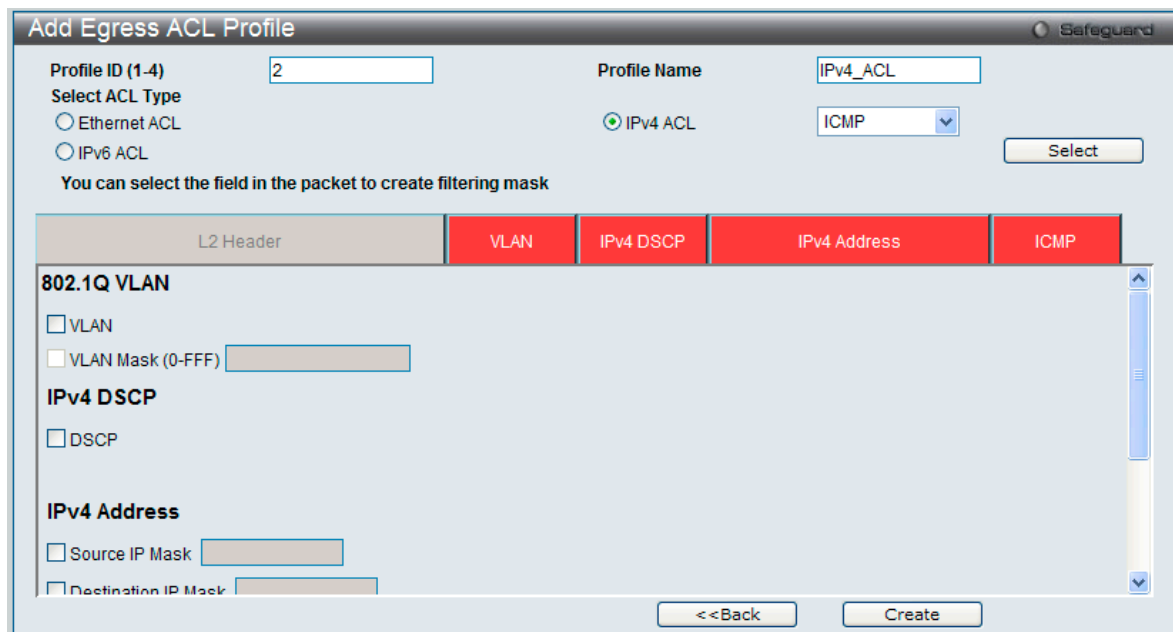


図 11-74 Add Egress ACL Profile - IPv4 ACL 画面

「Profile ID」でプロファイル番号を 1-4 から選択し、「Select ACL Type」で「IPv4 ACL」をチェック後、隣接する欄で設定するフレームヘッダ (ICMP、IGMP、TCP、UDP、Protocol ID) 選択して「Select」ボタンをクリックします。画面上部のボックスをクリックすると、赤色に変わり、設定用項目が表示されます。

ACL (ACL機能の設定)

以下の項目を IPv4 ACL タイプに設定します。

| 項目 | 説明 |
|--|--|
| Profile ID | プロファイル設定のための固有の識別番号を指定します。1 から 4 が指定できます。 |
| Profile Name | 作成したプロファイルにプロファイル名を入力します。 |
| Select ACL Type | Ethernet (MAC アドレス)、IPv4 アドレス、IPv6 アドレスまたはパケットコンテンツの中からプロファイルのベースを指定します。Type の変更に伴いメニューも変わります。ここでは「IPv4 ACL」を選択します。 <ul style="list-style-type: none"> IPv4 ACL - フレームヘッダの IPv4 アドレスを検証します。 |
| 以下のオプションを指定すると各フレームヘッダのプロトコルタイプを調べます。転送基準にどのようなプロトコルを含めるかを指定します。 | |
| 802.1Q VLAN | パケットヘッダの 802.1Q VLAN 識別子を調べて、部分的もしくは全体を転送基準として使用します。 <ul style="list-style-type: none"> VLAN - VLAN マスクを指定します。 VLAN Mask (0-FFF) - VLAN マスクを指定します。 |
| IPv4 DSCP | 各パケットヘッダの DiffServ コードを調べて、部分的もしくは全体を転送基準として使用します。 |
| IPv4 Address | <ul style="list-style-type: none"> Source IP Mask - 送信元 IP アドレスをマスクする IP アドレスを指定します。 Destination IP Mask - 送信先 IP アドレスをマスクする IP アドレスを指定します。 |
| ICMP | 各パケットのフレームヘッダの「Internet Control Message Protocol」(ICMP) 項目を調べます。アクセスプロファイルが適用するタイプ (「ICMP Type」または「ICMP Code」) を選択します。 <ul style="list-style-type: none"> ICMP Type - アクセスプロファイルを ICMP Type 値に適用します。 ICMP Code - アクセスプロファイルを ICMP Code に適用します。 |
| IGMP | それぞれのフレームヘッダの「Internet Group Management Protocol」(IGMP) 項目を調べます。アクセスプロファイルが適用するタイプ「IGMP Type」を選択します。 |
| TCP | 転送基準となる受信したパケットの TCP ポート番号を使用します。TCP を選ぶと送信元ポートマスク (source port mask) と (または) 送信先ポートマスク (dest port mask) を指定する必要があります。 <ul style="list-style-type: none"> Source Port Mask (0-FFFF) - フィルタリングしたい送信元ポートをマスクする TCP ポートを 16 進数 (hex 0x0-0xffff) で指定します。 Destination Port Mask (0-FFFF) - フィルタリングしたい送信先ポートをマスクする TCP ポートを 16 進数 (hex 0x0-0xffff) で指定します。 TCP Flag Bits - フィルタするフラグビットを指定します。フラグビットはパケットがどのような振る舞いをするかを決定するパケットの一部です。パケットのフラグビットでフィルタリングするには「TCP」項目のフラグビットに一致する内容のボックスをチェックします。URG (urgent)、ACK (acknowledgement)、PSH (push)、RST (reset)、SYN (synchronize)、FIN (finish) または Check All (すべて) を選ぶことができます。 |
| UDP | 転送基準となる受信したパケットの UDP ポート番号を使用します。UDP を選ぶと送信元ポートマスク (source port mask) と (もしくは) 送信先ポートマスク (dest port mask) を指定する必要があります。 <ul style="list-style-type: none"> Source Port Mask (0-FFFF) - フィルタリングしたい送信元ポートをマスクする UDP ポートを 16 進数 (hex 0x0-0xffff) で指定します。例: 255.255.255.255 Destination Port Mask (0-FFFF) - フィルタリングしたい送信先ポートをマスクする UDP ポートを 16 進数 (hex 0x0-0xffff) で指定します。例: 255.255.255.255 |
| Protocol ID | マスクしたいパケットヘッダの Protocol ID Mask (0-FF) を指定します。 <ul style="list-style-type: none"> User Define - レイヤ 4 パートマスクを指定します。 |

「Create」ボタンをクリックし、設定を適用します。

「<<Back」ボタンをクリックし、変更を破棄して前のページに戻ります。

作成したプロファイルの詳細の参照

作成したプロファイルの詳細を参照するには、「Egress Access Profile List」画面の該当エントリの「Show Details」ボタンをクリックし、以下の画面を表示します。



図 11-75 Egress Access Profile Detail Information - IPv4 画面

「Show All Profiles」ボタンをクリックすると、「Egress Access Profile List」画面に戻ります。

作成したアクセスプロファイルに対するルールの設定手順 (IPv4) :

IPv4 アクセスルールの設定

1. 「Egress Access Profile List」画面を表示します。

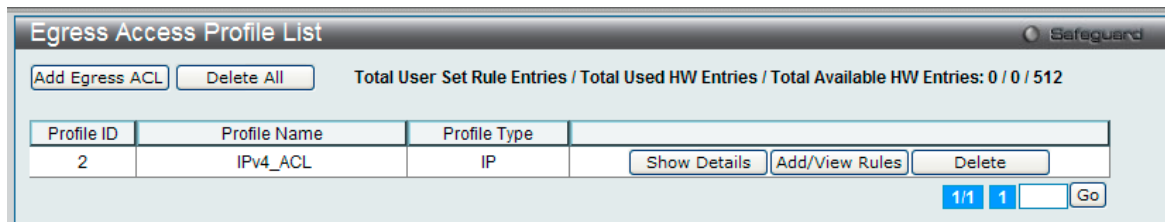


図 11-76 Egress Access Profile List 画面

2. 「Egress Access Profile List」画面を表示し、IPv4 エントリの「Add/View Rules」ボタンをクリックし、以下の画面を表示します。

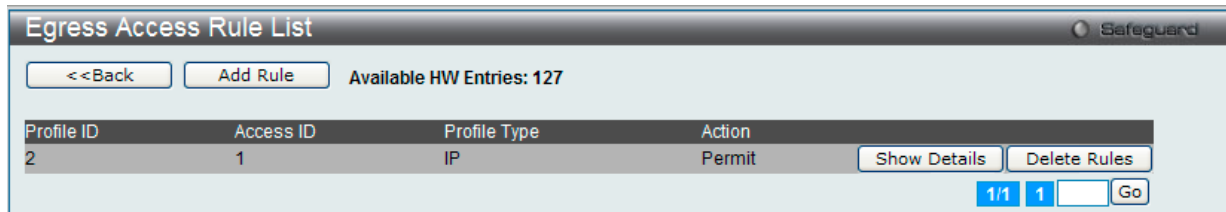


図 11-77 Egress Access Rule List - IPv4 画面

「<<Back」ボタンをクリックして前のページに戻ります。

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

ルールの削除

該当の「Delete Rules」ボタンをクリックします。

ルールの新規作成

新しいルールを作成するには、「Add Rule」ボタンをクリックし、以下の画面を表示します。

図 11-78 Add Egress Access Rule - IPv4 画面

ACL (ACL機能の設定)

以下の項目を設定します。

| 項目 | 説明 |
|-----------------------------|---|
| Rule Detail | |
| Access ID (1-128) | プロファイル設定のための固有の識別番号を指定します。1 から 128 が指定できます。 • Auto Assign - 本項目をチェックするとスイッチは自動的に作成されるルールに Access ID を割り当てます。 |
| VLAN Name | 設定済みの VLAN 名を入力します。スイッチはパケットヘッダの VLAN を確認し、その結果をパケット送信の基準 (または基準の一部) とします。 |
| VLAN ID(1-4094) | VLAN ID を入力します。「Mask」 (0-FFF) にマスク値を入力します。 |
| VLAN Mask (0-FFFF) | VLAN マスクを指定します。 |
| Source IP Address | 送信元の IP アドレスの IP アドレスを入力します。 |
| Source IP Address Mask | 送信元の IP アドレスの IP アドレスマスクを入力します。 |
| Destination IP Address | 宛先 IP アドレスの IP アドレスを入力します。 |
| Destination IP Address Mask | 送信先 IP アドレスの IP アドレスマスクを入力します。 |
| DSCP | DSCP 値 (0-63) を指定すると各パケットヘッダの DiffServ コードを調べて、部分的または全体を転送基準として使用します。 |
| ICMP | 各パケットのフレームヘッダの「Internet Control Message Protocol」 (ICMP) 項目を調べます。アクセスプロファイルが適用するタイプ (「ICMP Type」または「ICMP Code」) を選択します。 • Type - アクセスプロファイルを ICMP Type 値に適用します。 • Code - アクセスプロファイルを ICMP Code に適用します。 |
| IGMP | それぞれのフレームヘッダの「Internet Group Management Protocol」 (IGMP) 項目を調べます。アクセスプロファイルが適用するタイプ「IGMP Type」を選択します。 |
| TCP | 転送基準となる受信したパケットの TCP ポート番号を使用します。TCP を選ぶと送信元ポートマスク (source port mask) と (または) 送信先ポートマスク (dest port mask) を指定する必要があります。 - TCP Source Port (0-65535) - フィルタリングしたい送信元ポートを指定します。 - TCP Source Port Mask (0-FFFF) - フィルタリングしたい送信元ポートをマスクする TCP ポートを 16 進数で指定します。 - TCP Destination Port (0-65535) - フィルタリングしたい送信先ポートを指定します。 - TCP Destination Port Mask (0-FFFF) - フィルタリングしたい送信先ポートをマスクする TCP ポートを 16 進数で指定します。 - Flag Bits - フィルタするフラグビットを指定します。フラグビットはパケットがどのような振る舞いをするかを決定するパケットの一部です。パケットのフラグビットでフィルタリングするには「TCP」項目のフラグビットに一致する内容のボックスをチェックします。URG (urgent)、ACK (acknowledgement)、PSH (push)、RST (reset)、SYN (synchronize)、FIN (finish) を選ぶことができます。 |
| UDP | 転送基準となる受信したパケットの UDP ポート番号を使用します。UDP を選ぶと送信元ポートマスク (source port mask) と (または) 送信先ポートマスク (dest port mask) を指定する必要があります。 - UDP Source Port (0-65535) - フィルタリングしたい送信元ポートを指定します。 - UDP Source Port Mask (0-FFFF) - フィルタリングしたい送信元ポートをマスクする UDP ポートを 16 進数 (hex 0x0-0xffff) で指定します。 - UDP Destination Port (0-65535) - フィルタリングしたい送信先ポートを指定します。 - UDP Destination Port Mask (0-FFFF) - フィルタリングしたい送信先ポートをマスクする UDP ポートを 16 進数 (hex 0x0-0xffff) で指定します。 |
| Protocol ID | マスクしたいパケットヘッダの Protocol ID Mask を指定します。0-255 の値を入力します。 |
| Rule Action | |
| Action | <ul style="list-style-type: none"> Permit - アクセスプロファイルに一致したパケットを転送します。この時、新しいルールが追加されることがあります (以下参照)。 Deny - アクセスプロファイルに一致したパケットは転送せずにフィルタリングします。 Mirror - アクセスプロファイルに一致するパケットを「Port Mirroring」画面で定義したポートにミラーリングします。ポートミラーリングが有効で、ターゲットポートに設定されている必要があります。 |
| Priority (0-7) | スイッチにより設定された 802.1p デフォルトプライオリティを上書きしたい場合に指定します。このプライオリティにより転送されたパケットがどの CoS キューを使用するかが決まります。この欄を指定するとパケットはこのプライオリティを割り当てられ、対応した CoS キューに転送されます。指定しない場合は、パケットは送出される前に、入力用の 802.1p ユーザプライオリティを元の値に書き換えられます。プライオリティキュー、CoS キューおよび 802.1p マッピングについての詳細な情報については、本マニュアルの 221 ページの「第 10 章 QoS (QoS 機能の設定)」 を参照してください。 |
| Replace DSCP(0-63) | スイッチは本画面で指定した基準に一致するパケットの DSCP をチェックボックスの右側のフィールド内に指定した値に書き換えます。ACL ルールがプライオリティと IPv4 パケットの両方を変更するために追加されても、チップの制限のためそれらの一方しか変更できません。プライオリティと DSCP の両方が変更されるように設定されている場合は、現在のプライオリティを変更します。 |
| Time Range Name | チェックボックスをクリックし、「Time Range」画面に設定済みのタイムレンジ設定名を入力します。このアクセスルールをスイッチで実行する場合、ここに特定の時間を設定します。 |
| Counter | 「Counter」機能を「Enabled」(有効) / 「Disabled」(無効) にします。カウンタ機能は、アクセスルールに一致するパケット数を記録するために使用されます。本機能はオプションです。初期値は無効です。 |

| 項目 | 説明 |
|-----------------|--|
| Ports | ポートの範囲を指定する際には、本画面中の「Access ID」フィールドの「Auto assign」チェックボックスを選択しておく必要があります。選択しないと、エラーメッセージが表示され、アクセスルールの設定が行われません。「All Ports」をチェックすると、スイッチのすべてのポートを選択できます。 |
| Port Group ID | アクセスルールに適用するポートグループ ID を指定します。 |
| Port Group Name | アクセスルールに適用するグループ名を指定します。 |
| VLAN Name | アクセスルールに適用する VLAN 名を指定します。 |
| VLAN ID | アクセスルールに適用する VLAN ID を指定します。 |

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
「<<Back」ボタンをクリックし、変更を破棄して前のページに戻ります。

作成したルールの詳細の参照

「Access Rule List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

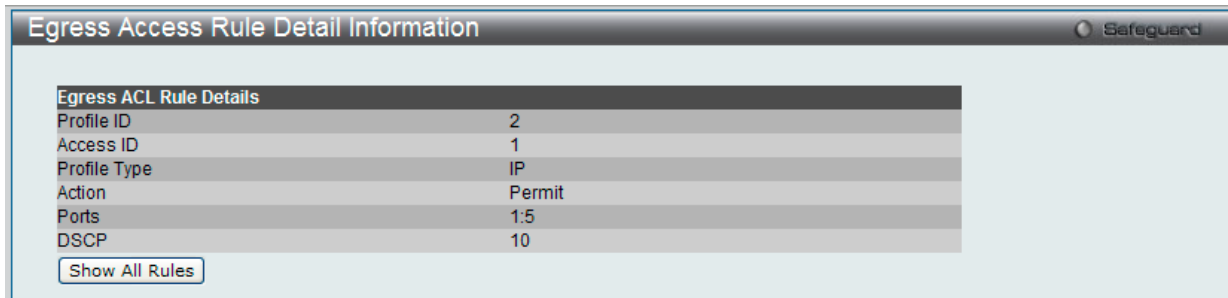


図 11-79 Egress Access Rule Detail Information - IP 画面

「Show All Rules」ボタンをクリックすると、「Access Rule List」画面に戻ります。

アクセスプロファイルリストの作成 (IPv6)

アクセスプロファイルを作成し、プロファイルにルールを作成します。

ACL > Egress Access Profile List の順にメニューをクリックし、以下の画面を表示します。1つのアクセスプロファイルが説明のために作成されています。

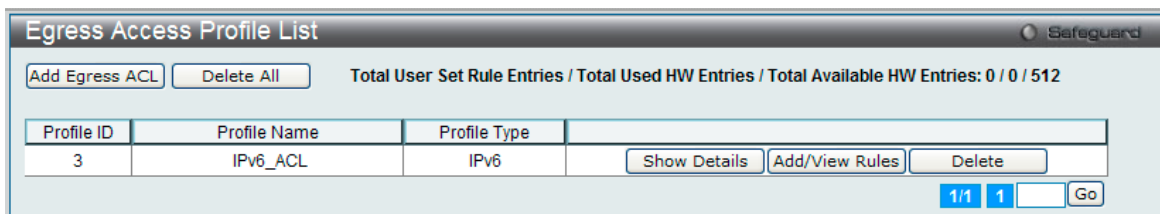


図 11-80 Egress Access Profile List 画面

エントリの削除

エントリの削除は、エントリ横の「Delete」ボタンをクリックします。すべてのアクセスプロファイルの削除は、「Delete All」ボタンをクリックします。

エントリの追加

「Access Profile List」にエントリを追加するには、「Add ACL Profile」で「IPv6 ACL」ボタンをチェック後、隣接する欄で設定するフレームヘッダ（TCP または UDP）を選択して「Select」ボタンをクリックします。

IPv6 の「Add ACL Profile」画面

図 11-81 Add Egress ACL Profile - IPv6 ACL 画面

「Profile ID」でプロファイル番号を 1-6 から選択し、「Select ACL Type」をチェック後、「Select」ボタンをクリックすることで画面を切り替えることができます。画面上部のボックスをクリックすると、赤色に変わり、設定用項目が表示されます。

以下の項目を IPv6 ACL タイプに設定します。

| 項目 | 説明 |
|--|---|
| Profile ID | プロファイル設定のための固有の識別番号を指定します。1 から 4 を指定できます。 |
| Select ACL Type | Ethernet (MAC アドレス)、IPv4 アドレス、IPv6 アドレスまたはパケットコンテンツの中からプロファイルのベースを指定します。Type の変更に伴いメニューも変わります。ここでは「IPv6 ACL」を選択します。 • IPv6 ACL - フレームヘッダの IPv6 アドレスを検証します。 |
| 以下のオプションを指定すると各フレームヘッダのプロトコルタイプを調べます。転送基準にどのようなプロトコルを含めるかを指定します。 | |
| IPv6 Class | この項目を選ぶと IPv6 ヘッダの「Class」を調べます。「Class」は IPv4 における「Type of Service」(ToS)、「Precedence bits」のようなパケットヘッダの一部です。 |
| IPv6 Flow Label | この項目を選ぶと IPv6 ヘッダの「flow label」を調べます。「flow label」は送信元で順番につけられる QoS やリアルタイムサービスパケットのためのデフォルトではない項目です。 |
| TCP | <ul style="list-style-type: none"> • TCP - TCP トラフィックに適用するルールを指定します。 • Source Port Mask (0-FFFF) - TCP 送信元ポートマスクを指定します。 • Destination Port Mask (0-FFFF) - TCP 宛先ポートマスクを指定します。 |
| UDP | <ul style="list-style-type: none"> • UDP - ルールを UDP トラフィックに適用するように指定します。 • Source Port Mask (0-FFFF) - UDP 送信元ポートマスクを指定します。 • Destination Port Mask (0-FFFF) - UDP 宛先ポートマスクを指定します。 |
| IPv6 Address | <ul style="list-style-type: none"> • IPv6 Source Address - 対応するボックスをチェックして、IPv6 アドレスマスク (例 FFFF:FFFF::FFFF) を入力することで送信元 IPv6 アドレスのマスクアドレスを指定します。 • IPv6 Destination Address - 対応するボックスをチェックして、IPv6 アドレスマスク (例 FFFF:FFFF::FFFF) を入力することで送信先 IPv6 アドレスのマスクアドレスを指定します。 |

「Create」ボタンをクリックし、設定を適用します。

「<<Back」をボタンをクリックし、変更を破棄して前のページに戻ります。

作成したプロファイルの詳細の参照

作成したプロファイルの詳細を参照する場合は、「Access Profile List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

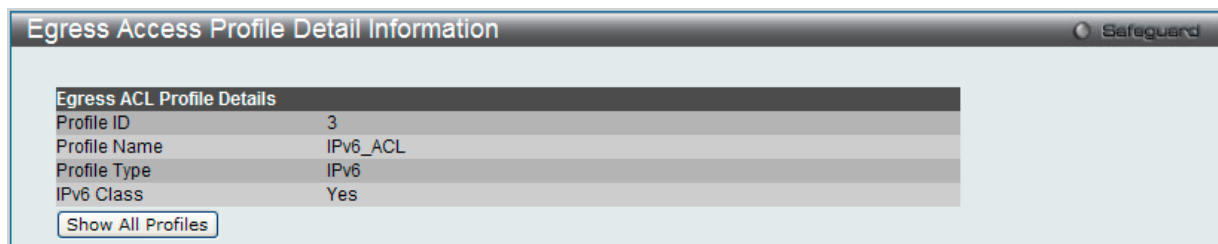


図 11-82 Egress Access Profile Detail Information - IPv6 ACL 画面

「Show All Profiles」ボタンをクリックすると、「Access Profile List」画面に戻ります。

作成したアクセスプロファイルに対するルールの設定手順 (IPv6) :

IPv6 アクセスルールの設定

1. 「Egress Access Profile List」画面を表示します。

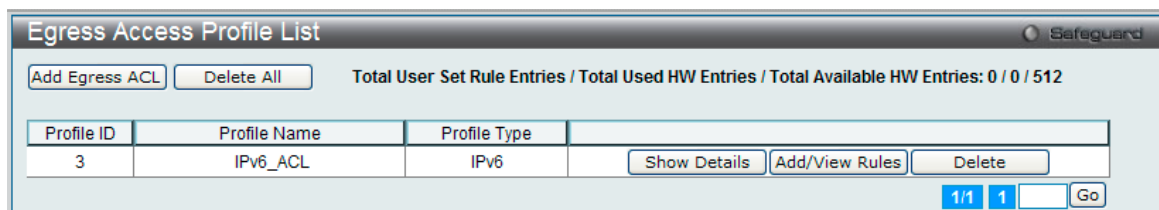


図 11-83 Egress Access Profile List 画面

2. 「Access Profile List」画面を表示し、IPv6 エントリの「Add/View Rules」ボタンをクリックして以下の画面を表示します。

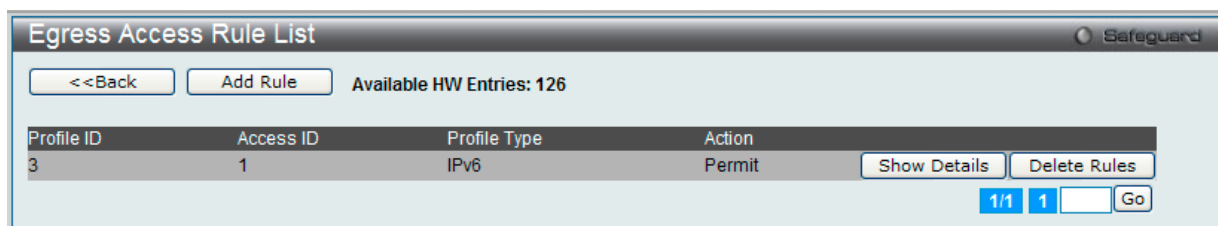


図 11-84 Egress Access Rule List - IPv6 画面

「<<Back」ボタンをクリックして前のページに戻ります。

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

作成済みのルールの削除

該当の「Delete Rules」ボタンをクリックします。

ルールの新規登録

新しいルールを作成するためには、「Add Rule」ボタンをクリックします。

図 11-85 Add Egress Access Rule - IPv6 画面

以下の項目を設定します。

| 項目 | 説明 |
|-------------------------------|--|
| Rule Detail | |
| Access ID (1-128) | プロファイル設定のための固有の識別番号を指定します。1 から 128 が指定できます。 • Auto Assign - 本項目をチェックするとスイッチは自動的に作成されるルールに Access ID を割り当てます。 |
| Class | クラスを入力し、IPv6 ヘッダの「Class」フィールドを調べます。本フィールドは IPv4 における「Type of Service(ToS)」、 「Precedence bits」フィールドのようなパケットヘッダの一部です。 |
| Flow Label | IPv6 フローラベルマスクを指定します。0-FFFFFF の範囲で指定します。 |
| IPv6 Source Address | IPv6 送信元アドレスの IPv6 アドレスを入力します。 |
| IPv6 Source Address Mask | IPv6 送信元サブマスクを指定します。送信先 IPv6 アドレスの最後の 44 ビット (LSB) のフィルタリングのみを行います。 |
| IPv6 Destination Address | IPv6 送信先アドレスの IPv6 アドレスを入力します。 |
| IPv6 Destination Address Mask | IPv6 送信先サブマスクを指定します。送信先 IPv6 アドレスの最後の 44 ビット (LSB) のフィルタリングのみを行います。 |
| TCP | <ul style="list-style-type: none"> • TCP Source Port (0-65535) - IPv6 L4 TCP 送信元ポートサブマスクを指定します。 • TCP Source Port Mask (0-FFFF) - フィルタリングしたい送信元ポートをマスクする TCP ポートを 16 進数で指定します。 • TCP Destination Port (0-65535) - IPv6 L4 TCP 送信先ポートサブマスクを指定します。 • TCP Destination Port Mask (0-FFFF) - フィルタリングしたい送信先ポートをマスクする TCP ポートを 16 進数で指定します。 |
| UDP | <ul style="list-style-type: none"> • UDP Source Port (0-65535) - IPv6 L4 UDP 送信元ポートサブマスクを指定します。 • UDP Source Port Mask (0-FFFF) - フィルタリングしたい送信元ポートをマスクする UDP ポートを 16 進数で指定します。 • UDP Destination Port (0-65535) - IPv6 L4 UDP 送信先ポートサブマスクを指定します。 • UDP Destination Port Mask (0-FFFF) - フィルタリングしたい送信先ポートをマスクする UDP ポートを 16 進数で指定します。 |
| Rule Action | |
| Action | <ul style="list-style-type: none"> • Permit - アクセスプロファイルに一致したパケットを転送します。この時、新しいルールが追加されることがあります (以下参照)。 • Deny - アクセスプロファイルに一致したパケットは転送せずにフィルタリングします。 • Mirror - アクセスプロファイルに一致するパケットを「Port Mirroring」画面で定義したポートにミラーリングします。ポートミラーリングが有効で、ターゲットポートに設定されている必要があります。 |

| 項目 | 説明 |
|---------------------|---|
| Priority (0-7) | スイッチにより設定された 802.1p デフォルトプライオリティを上書きしたい場合に指定します。このプライオリティにより転送されたパケットがどの CoS キューを使用するかが決まります。この欄を指定するとパケットはこのプライオリティを割り当てられ、対応した CoS キューに転送されます。指定しない場合は、パケットは送出される前に、入力用の 802.1p ユーザプライオリティを元の値に書き換えられます。プライオリティキュー、CoS キューおよび 802.1p マッピングについての詳細な情報については、本マニュアルの 221 ページの「第 10 章 QoS (QoS 機能の設定)」 を参照してください。 |
| Replace DSCP (0-63) | スイッチは本画面で指定した基準に一致するパケットの DSCP をボックスの右側の欄に指定した値に書き換えます。ACL ルールがプライオリティと IPv4 パケットの両方を変更するために追加されても、チップの制限のためそれらの一方しか変更できません。プライオリティと DSCP の両方が変更されるように設定されている場合は、現在のプライオリティを変更します。 |
| Time Range Name | チェックボックスをクリックし、「Time Range」画面に設定済みのタイムレンジ設定名を入力します。このアクセスルールをスイッチで実行する場合、ここに特定の時間を設定します。 |
| Counter | 「Counter」機能を「Enabled」(有効) / 「Disabled」(無効) にします。カウンタ機能は、アクセスルールに一致するパケット数を記録するために使用されます。本機能はオプションです。初期値は無効です。 |
| Ports | ポートの範囲を指定する際には、本画面中の「Access ID」フィールドの「Auto assign」チェックボックスを選択しておく必要があります。選択しないと、エラーメッセージが表示され、アクセスルールの設定が行われません。「All Ports」をチェックすると、スイッチのすべてのポートを選択できます。 |
| Port Group ID | アクセスルールに適用するポートグループ ID を指定します。 |
| Port Group Name | アクセスルールに適用するグループ名を指定します。 |
| VLAN Name | アクセスルールに適用する VLAN 名を指定します。 |
| VLAN ID | アクセスルールに適用する VLAN ID を指定します。 |

IPv6 のアクセスルールを設定するためには、必ず「Apply」ボタンをクリックし、設定内容を適用してください。
 「<<Back」ボタンをクリックし、変更を破棄して前のページに戻ります。

作成したルールの詳細の参照

「Egress Access Rule List」画面の該当エントリの「Show Details」ボタンをクリックして以下の画面を表示します。

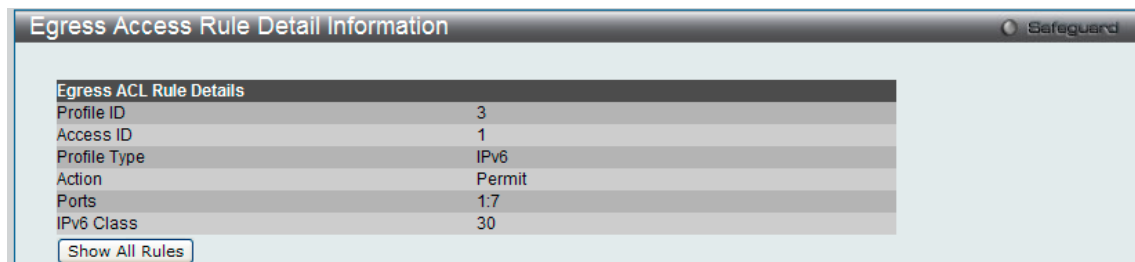


図 11-86 Egress Access Rule Detail Information - IPv6 画面

「Show All Rules」ボタンをクリックすると、「Egress Access Rule List」画面に戻ります。

Egress ACL Flow Meter (Egress ACL フローメータリング)

Egress アクセスプロファイルおよびルールに基づいてパケットフローベースのメータリングを設定します。

ACL > Egress ACL Flow Meter の順にメニューをクリックし、以下の画面を表示します。

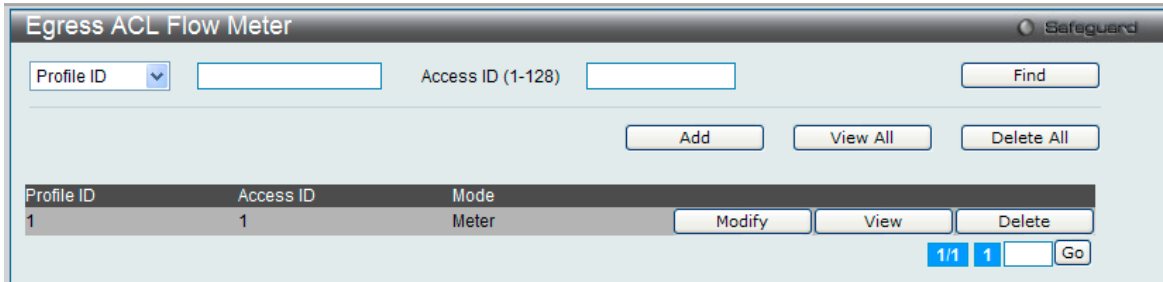


図 11-87 Egress ACL Flow Meter 画面

以下の項目を使用して設定を行います。

| 項目 | 説明 |
|-------------------|--|
| Profile ID | ACL フローメータリングパラメータを設定する定義済みプロファイル ID を指定します。 |
| Profile Name | ACL フローメータリングパラメータを設定する定義済みプロファイル名を指定します。 |
| Access ID (1-128) | ACL フローメータリングパラメータを設定する定義済みアクセス ID を指定します。 |

入力後、「Find」ボタンをクリックします。情報が画面下半分に表示されます。

エントリの削除

対応する「Delete」ボタンをクリックします。すべてのエントリを削除するためには、「Delete All」ボタンをクリックします。

エントリの追加

「Add」ボタンをクリックし、以下の画面を表示します。

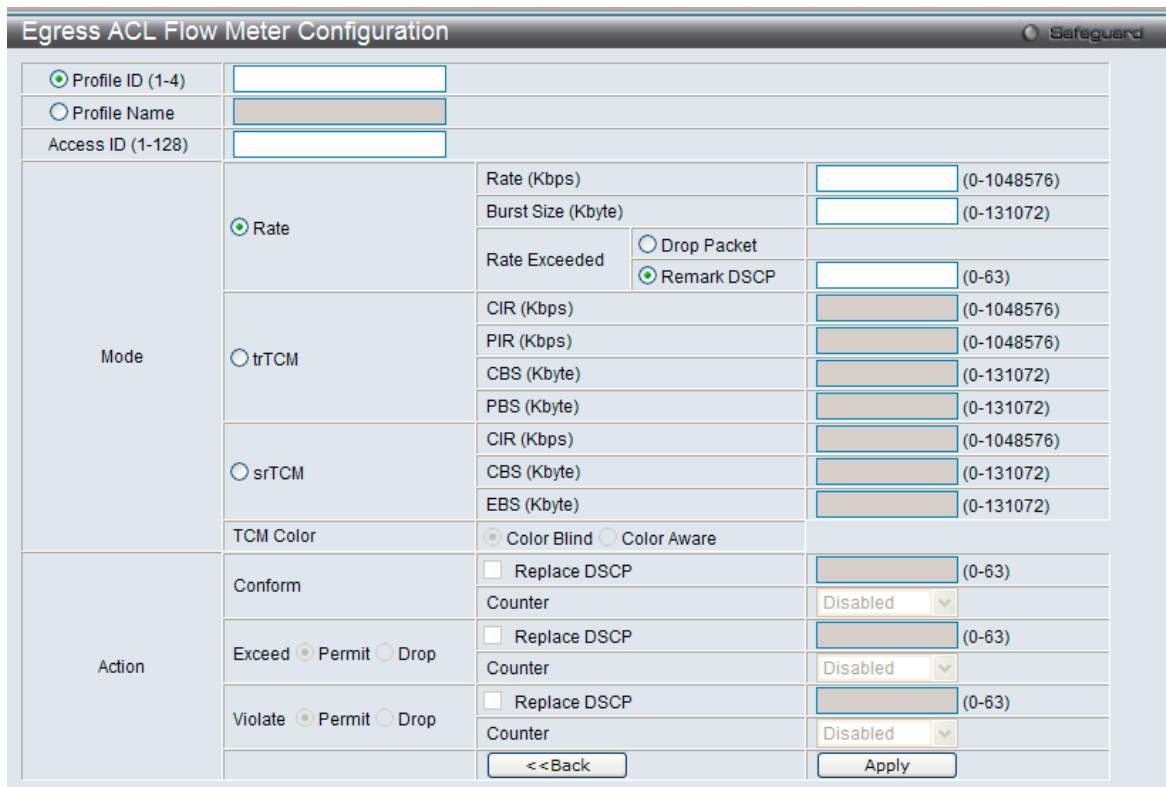


図 11-88 Egress ACL Flow Meter Configuration 画面 - Add

以下の項目を使用して、設定を行います。

| 項目 | 説明 |
|-------------------|--|
| Profile ID | プルダウンメニューから、フローメータリングを設定する定義済みのプロファイル ID を指定します。 |
| Profile Name | フローメータに対するプロファイル名を入力します。 |
| Access ID (1-128) | ACL フローメータリングを設定する定義済みアクセス ID を 1-128 の範囲で指定します。 |
| Mode | <p>Rate - シングルレート 2 カラーモードのレートを指定します。</p> <ul style="list-style-type: none"> Rate - フローに規定する帯域幅を Kbps 単位で指定します。 Burst Size - シングルレート 2 カラーモードにバーストサイズを指定します。単位は Kbps です。 Rate Exceeded - シングルレート 2 カラーモードでコミットレートを超過したパケットへの操作を指定します。以下の一つの動作が行われます。: <ul style="list-style-type: none"> - Drop Packet - パケットを直ちに破棄します。 - Remark DSCP - 特定の DSCP をパケットにマークをつけます。高い優先度を持つパケットが破棄されるように設定されます。 <p>trTCM - 「2 レート 3 カラーモード」を指定します。</p> <ul style="list-style-type: none"> CIR - コミット情報レートの値を入力します。単位は Kbps です。CIR は PIR 以下である必要があります。 PIR - ピーク情報レートを指定します。単位は Kbps です。PIR は CIR 以上である必要があります。 CBS - 「コミットバーストサイズ」の値を入力します。単位は Kbps です。 PBS - ピークバーストサイズの値を入力します。単位は Kbps です。 <p>srTCM - 「シングルレート 3 カラーモード」を指定します。</p> <ul style="list-style-type: none"> CIR - コミット情報レートの値を入力します。単位は Kbps です。 CBS - 「コミットバーストサイズ」の値を入力します。単位は Kbps です。 EBS - 「超過バーストサイズ」を指定します。単位は Kbps です。 |
| Action | <p>Conform - 本フィールドは緑色のパケットフローを表します。緑色のパケットフローは、DSCP フィールドを本フィールドで指定された値に書き換える可能性があります。また、「Counter」パラメータを使用することで緑色のパケットをカウントするように選択することができます。</p> <ul style="list-style-type: none"> Replace DSCP - 緑色のフローにあるパケットが本パラメータを使用し、DSCP 値を入力することで、DSCP 値を書き換えることが可能です。 Counter - 緑色のフローにおいて指定された ACL エントリのパケットカウンタを有効または無効にします。 <p>Un-conform - 不適合 (黄色または赤) パケットの DSCP を変更します。</p> <ul style="list-style-type: none"> Replace DSCP - 赤色のフローにあるパケットが本パラメータを使用し、DSCP 値を入力することで、DSCP 値を書き換えることが可能です。 <p>Exceed - 本フィールドは黄色のパケットフローを表します。黄色のパケットフローは超過パケットを許可または廃棄します。これらのパケットの「DSCP」フィールドを割り当てられたフィールドに新しい DSCP 値を入れることで交換することができます。</p> <ul style="list-style-type: none"> Counter - 黄色のフローにおいて指定された ACL エントリのパケットカウンタを有効または無効にします。 <p>Violate - 本フィールドは赤色のパケットフローを表します。赤色のパケットフローは超過パケットを許可または廃棄します。これらのパケットの「DSCP」フィールドを割り当てられたフィールドに新しい DSCP 値を入れることで交換することができます。</p> <ul style="list-style-type: none"> Counter - 赤色のフローにおいて指定された ACL エントリのパケットカウンタを有効または無効にします。 |

「Apply」ボタンをクリックして、設定を適用します。

「Egress ACL Flow Meter」画面に戻るためには、「<<Back」ボタンをクリックします。

エントリの変更

対応する「Modify」ボタンをクリックし、以下の画面を表示します。

図 11-89 Egress ACL Flow Meter Configuration 画面 - Modify

以下の項目を使用して、設定を行います。

| 項目 | 説明 |
|------|--|
| Mode | <p>Rate - シングルレート 2 カラーモードのレートを指定します。</p> <ul style="list-style-type: none"> Rate - フローに規定する帯域幅を Kbps 単位で指定します。 Burst Size - シングルレート 2 カラーモードにバーストサイズを指定します。単位は Kbps です。 Rate Exceeded - シングルレート 2 カラーモードでコミットレートを超過したパケットへの操作を指定します。以下の一つの動作が行われます。： <ul style="list-style-type: none"> Drop Packet - パケットを直ちに破棄します。 Remark DSCP - 特定の DSCP をパケットにマークをつけます。高い優先度を持つパケットが破棄されるように設定されます。 |

「Apply」ボタンをクリックして、設定を適用します。

「Egress ACL Flow Meter」画面に戻るためには、「<<Back」ボタンをクリックします。

エントリの参照

すべてのエントリを参照するためには、「View All」ボタンをクリックします。

エントリを参照するためには、対応する「View」ボタンをクリックし、以下の画面を表示します。

図 11-90 Egress ACL Flow Meter Display 画面

「Egress ACL Flow Meter」画面に戻るためには、「<<Back」ボタンをクリックします。

第 12 章 Security (セキュリティ機能の設定)

本セクションではユーザアカウントを含むデバイスのセキュリティの設定について解説します。

以下は Security サブメニューの説明です。

必要に応じて、設定 / 変更 / 修正を行ってください。

| サブメニュー | 説明 | 参照ページ |
|--|--|---------------------|
| 802.1X (802.1X 設定) | 802.1X 認証を設定します。以下のメニューがあります。 802.1X Global Settings (802.1X グローバル設定)、802.1X Port Settings (802.1X ポート設定)、802.1X User Settings (802.1X ユーザ設定)、Guest VLAN (ゲスト VLAN の設定)、Authenticator State (オーセンティケータの状態)、Authenticator Statistics (オーセンティケータ統計情報)、Authenticator Session Statistics (オーセンティケータセッション統計情報)、Authenticator Diagnostics (オーセンティケータ診断)、Initialize Port-based Port(s) (初期化ポート - ポートベース)、Initialize Host-based Port(s) (初期化ポート - ホストベース)、Reauthenticate Port-based Port(s) (再認証ポート - ポートベース)、Reauthenticate Host-based Port(s) (再認証ポート - ホストベース) | 293 |
| RADIUS (RADIUS 設定) | RADIUS サーバの設定を行います。以下のメニューがあります。 Authentication RADIUS Server Settings (認証 RADIUS サーバ設定)、RADIUS Accounting Setting (RADIUS アカウンティング設定)、RADIUS Authentication (RADIUS 認証)、RADIUS Account Client (RADIUS アカウンティングクライアント) | 306 |
| IP-MAC-Port Binding (IMPB: IP-MAC-ポートバインディング) | IP アドレス、MAC アドレスおよびポートを結合し、レイヤ間通信を行います。以下のメニューがあります。 IMPB Global Settings (IMPB グローバル設定)、IMPB Port Settings (IMPB ポート設定)、IMPB Entry Settings (IMPB エントリ設定)、MAC Block List (MAC ブロックリスト)、DHCP Snooping (DHCP Snooping 設定)、ND Snooping (ND Snooping 設定) | 310 |
| MAC-based Access Control (MAC ベースアクセスコントロール) | MAC アドレス認証機能を設定します。以下のメニューがあります。 MAC-based Access Control Settings (MAC ベースアクセスコントロール設定)、MAC-based Access Control Local Settings (MAC ベースアクセスコントロール ローカル設定)、MAC-based Access Control Authentication State (MAC ベースアクセスコントロールの認証状態) | 316 |
| Web-based Access Control (WAC) (Web ベースのアクセス制御) | Web ベースアクセスコントロールを設定します。以下のメニューがあります。 WAC Global Settings (WAC グローバル設定)、WAC User Settings (WAC ユーザ設定)、WAC Port Settings (WAC ポート設定)、WAC Authentication State (WAC 認証状態)、WAC Customize Page (WAC カスタマイズページ設定) | 320 |
| Japanese Web-based Access Control (JWAC: JWAC 設定) | JWAC の有効化および設定をします。以下のメニューがあります。 JWAC Global Settings (JWAC グローバル設定)、JWAC Port Settings (JWAC ポート設定)、JWAC User Settings (JWAC ユーザ設定)、JWAC Authentication State (JWAC 認証状態)、JWAC Customize Page Language (JWAC 画面言語のカスタマイズ)、JWAC Customize Page (JWAC 画面のカスタマイズ) | 326 |
| Compound Authentication (コンパウンド認証) | コンパウンド認証方式を設定します。以下のメニューがあります。 Compound Authentication Settings (コンパウンド認証設定)、Compound Authentication Guest VLAN Settings (コンパウンド認証ゲスト VLAN の設定)、Compound Authentication MAC Format Settings (コンパウンド認証 MAC 形式設定) | 331 |
| IGMP Access Control Settings (IGMP アクセスコントロール設定) | 各ポートに IGMP 認証 (IGMP アクセスコントロール) を設定することができます。 | 333 |
| Port Security (ポートセキュリティ) | ダイナミックな MAC アドレス学習をロックします。以下のメニューがあります。 Port Security Settings (ポートセキュリティの設定)、Port Security VLAN Settings (ポートセキュリティ VLAN 設定)、Port Security Entries (ポートセキュリティエントリ) | 334 |
| ARP Spoofing Prevention Settings (ARP Spoofing 防止設定) | パケットコンテンツ ACL を使用して、ARP スプーフィング攻撃を防止します。 | 338 |
| BPDU Attack Protection (BPDU アタック防止設定) | ポートに BPDU 防止機能を設定します。 | 339 |
| Loopback Detection Settings (ループバック検知設定) | ループバック検知機能の設定を行います。 | 340 |
| Traffic Segmentation Settings (トラフィックセグメンテーション設定) | ポートのトラフィックフローを制限します。 | 341 |
| NetBIOS Filtering Setting (NetBIOS フィルタリング設定) | NetBIOS フィルタ設定を行います。 | 341 |
| DHCP Server Screening (DHCP サーバスクリーニング) | 不正な DHCP サーバへのアクセスを拒否します。以下のメニューがあります。 DHCP Server Screening Port Settings (DHCP サーバスクリーニング設定)、DHCP Offer Permit Entry Settings (DHCP オファー許可エントリ設定) | 343 |

Security(セキュリティ機能の設定)

| サブメニュー | 説明 | 参照ページ |
|---|---|---------------------|
| Access Authentication Control (アクセス認証コントロール) | TACACS/XTACACSTACACS+/RADIUS 認証の設定を行います。以下のメニューがあります。 Enable Admin (管理者レベルの認証)、Authentication Policy Settings (認証ポリシー設定)、 Application Authentication Settings (アプリケーションの認証設定)、Authentication Server Group Settings (認証サーバグループ設定)、Authentication Server Settings (認証サーバ設定)、 Login Method Lists Settings (ログインメソッドリスト)、Enable Method Lists Settings (メソッ ドリストの有効化)、Local Enable Password Settings (ローカルユーザパスワード設定) | 346 |
| SSL Settings (Secure Socket Layer の設定) | 証明書の設定、暗号スイートの設定を行います。 | 356 |
| SSH (Security Shell の設定) | SSH サーバ、SSH アルゴリズム、SSH ユーザ認証の設定を行います。以下のメニューがあり ます。SSH Settings (SSH サーバ設定)、SSH Authentication Method and Algorithm Settings (SSH 認証モードとアルゴリズム設定)、SSH User Authentication List (SSH ユーザ認証リスト) | 359 |
| DoS Attack Prevention Settings (DoS 攻撃防止設定) | 各 DoS 攻撃に対して防御設定を行います。 | 362 |
| Trusted Host Settings(トラストホスト) | リモートのスイッチ管理用トラストホストを設定します。 | 363 |
| Safeguard Engine Settings (セーフガードエンジン) | セーフガードエンジンの設定を行います。 | 364 |
| SFTP Server Settings (SFTP サーバ設定) | SFTP 機能を設定します。「SFTP over SSH2」はすべてのファイル操作に安全性を提供するセキュ アなファイル送信プロトコルです。 | 365 |

802.1X (802.1X 設定)

Port Access Entity (ポートアクセスエンティティ)

802.1X ポートベースおよび MAC ベースのアクセスコントロール

IEEE 802.1X 標準規格は、クライアント・サーバベースのアクセスコントロールモデルの使用により、特定の LAN 上の様々な有線 / 無線デバイスへのアクセスを行う場合にユーザ認証を行うセキュリティ方式です。本方式は、ネットワークへアクセスするユーザを認証するために RADIUS サーバを使用し、EAPOL (Extensible Authentication Protocol over LAN) と呼ばれるパケットをクライアント・サーバ間で中継することにより実現します。以下の図は基本的な EAPOL パケットの構成を示しています。

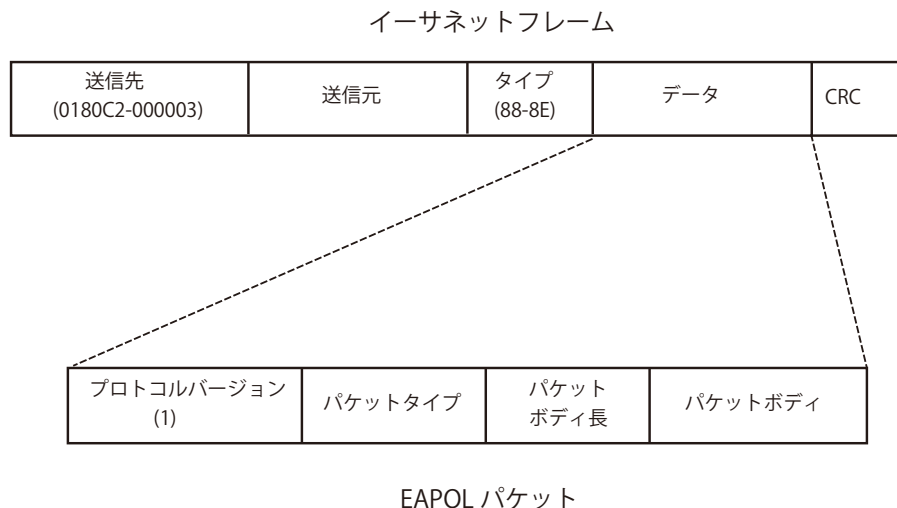


図 12-1 EAPOL パケット

本方法を使用すると、未認証のデバイスが接続ポート経由で LAN に接続することを制限できます。EAPOL パケットは、承認が与えられるまでの間指定ポート経由で送受信される唯一のトラフィックです。802.1X アクセスコントロール方式は 3 つの役割を持っており、それぞれがアクセスコントロールセキュリティ方法の作成、状態の保持および動作のために必要不可欠です。

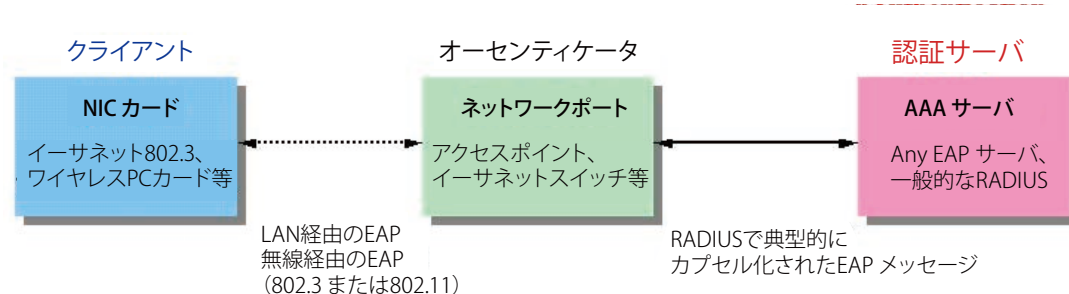


図 12-2 802.1X の 3 つの要素

以下の項では、クライアント、オーセンティケータ、および認証サーバのそれぞれの役割について詳しく説明します。

認証サーバ

認証サーバはクライアントやオーセンティケータと同じネットワークに接続されるリモートデバイスです。認証サーバ上では RADIUS サーバプログラムを実行し、またそのサーバのデータがオーセンティケータ側（スイッチ）に正しく登録されている必要があります。スイッチポートに接続しているクライアントは、LAN 上のスイッチが提供するサービスを受ける前に、認証サーバ（RADIUS）による認証を受ける必要があります。認証サーバは、RADIUS サーバとクライアントの間で EAPOL パケットを通じて信頼できる情報を交換し、そのクライアントの LAN やスイッチのサービスに対するアクセス許可の有無をスイッチに通知します。このように、認証サーバの役割は、ネットワークにアクセスを試みるクライアントの身元を保証することです。

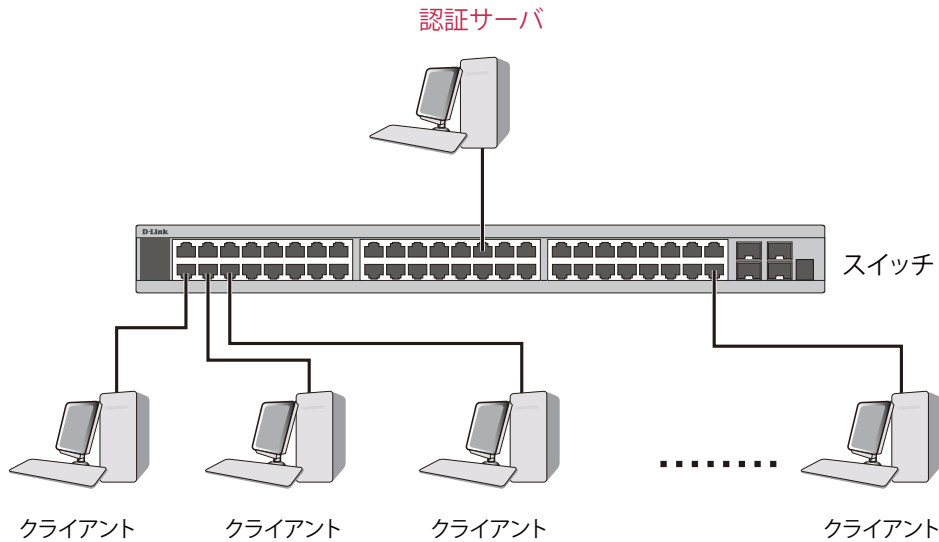


図 12-3 認証サーバ

オーセンティケータ

オーセンティケータ（スイッチ）は、認証サーバとクライアントの間を取り持つ、仲介の役割を果たします。802.1X を使用する場合、オーセンティケータサーバには 2 つの目的があります。1 つ目の目的は、クライアントに EAPOL パケットを通して認証情報を提出するよう要求することです。EAPOL パケットはクライアントにアクセスが許可される前にオーセンティケータを通過することのできる唯一の情報です。2 つ目の目的はクライアントから収集した情報を、認証サーバに確認してもらい、その結果をクライアントに伝達することです。

スイッチをオーセンティケータとして正しく設定するためには、以下の 3 つの手順を実行する必要があります。

1. 802.1X 機能を有効にします。(Security > 802.1X > 802.1X Settings)
2. 対象ポートに 802.1X の設定を行います。(Security > 802.1X > 802.1X Port Settings)
3. スwitchに RADIUS サーバの設定を行います。(Security > RADIUS > Authentication RADIUS Server Settings)

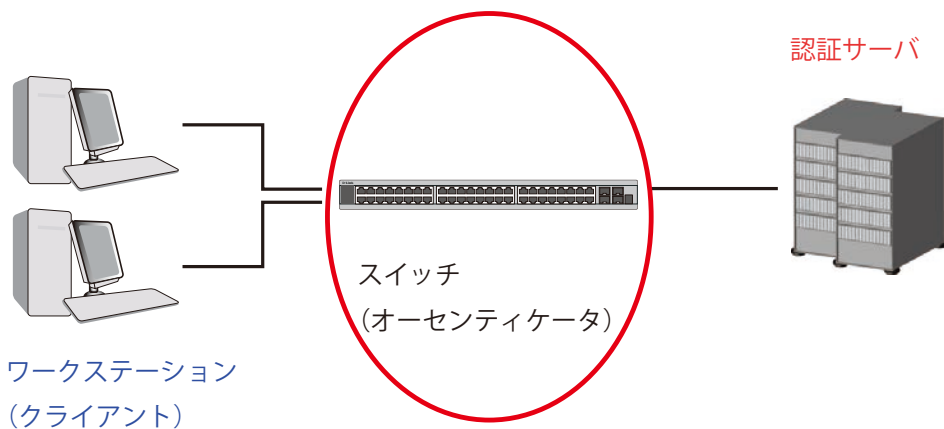


図 12-4 オーセンティケータ

クライアント

クライアントとは、簡単に言うと LAN やスイッチが提供するサービスへのアクセスを希望するワークステーションです。クライアントとなるワークステーションでは、802.1X プロトコルに準拠したソフトウェアが起動している必要があります。Windows XP 使用の場合には、OS 内に既にそのようなソフトウェアが組み込まれています。それ以外の場合には、802.1X クライアントソフトウェアを別途用意する必要があります。クライアントは EAPOL パケットを使用して LAN へのアクセスを要求し、またスイッチからの要求に対しても応答します。

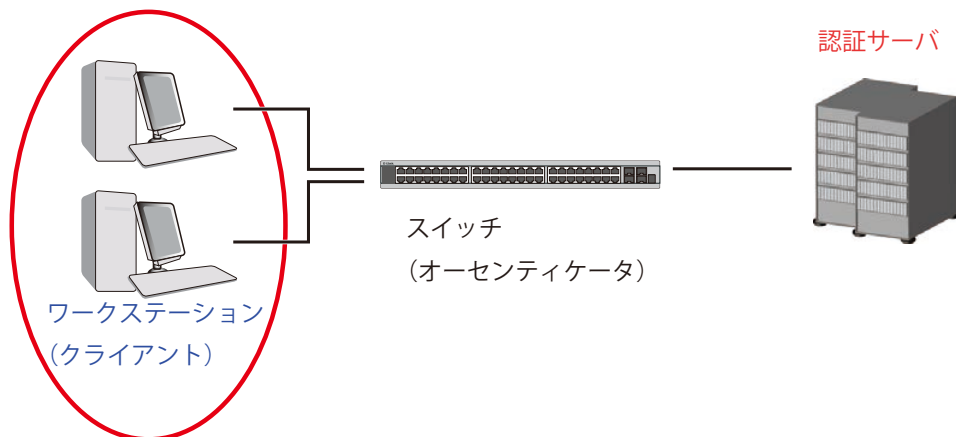


図 12-5 クライアント

認証プロセス

これらの3つの要素により、802.1X プロトコルはネットワークへのアクセスを試みるユーザの認証を安定的かつ安全に行います。認証に成功する前は、EAPOL トラフィックのみが特定ポートの通過を許可されます。このポートは、有効なユーザ名とパスワード (802.1X の設定で MAC アドレスも指定されている場合は MAC アドレスも) を持つクライアントがアクセス権を取得してポートのロックが解除されるまで、ロック状態を保ちます。ロックが解除されると、通常のトラフィックがポートを通過できるようになります。D-Link が実装する 802.1X では以下の2種類のアクセスコントロールが選択できます。

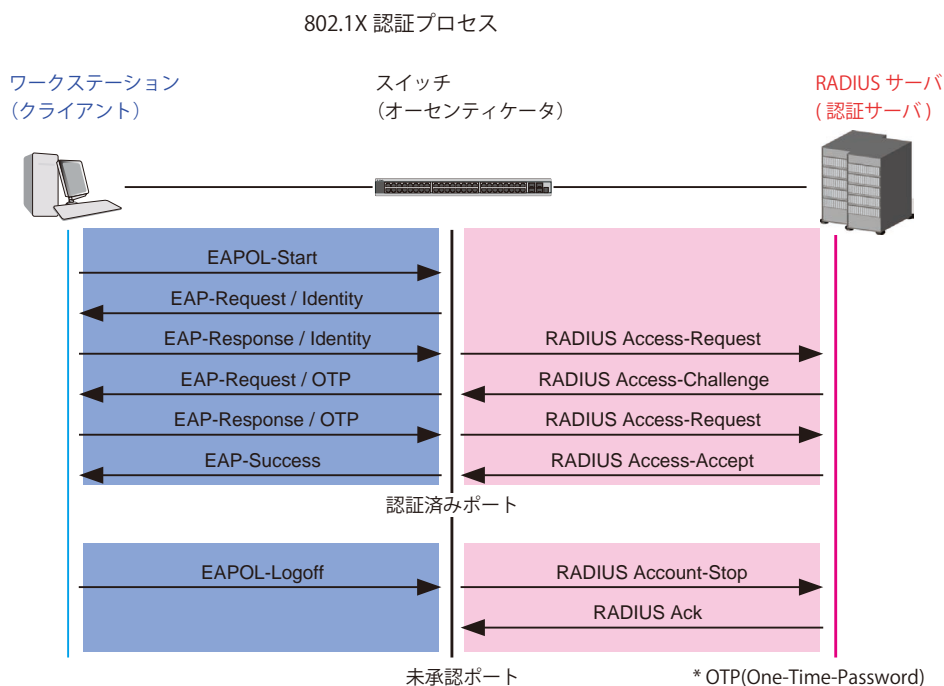


図 12-6 802.1X 認証プロセス

本スイッチの 802.1X 機能では、以下の2つのタイプのアクセスコントロールから選択することができます。

- 1. ポートベースのアクセスコントロール**
本方式では、1人のユーザがリモートの RADIUS サーバにポートごとの認証をリクエストし、残りのユーザも同じポートをアクセスできるようにします。
- 2. MAC ベースのアクセスコントロール**
本方式では、スイッチは自動的に各ポートに対して 448 件までの MAC アドレスを自動的に学習してリストに追加します。スイッチはリモート RADIUS サーバを使用して、ネットワークへのアクセスを許可する前に各 MAC アドレスの認証を行います。

ポートベースのネットワークアクセスコントロール

802.1X 開発の本来の目的は、LAN 上で Point to Point プロトコルの機能を利用することでした。インフラストラクチャのように単一の LAN セグメントが 2 個以上のデバイスを持たない場合、どちらかがブリッジポートとなります。ブリッジポートは、リンクのリモートエンドにあるアクティブなデバイスの接続を示すイベントや、アクティブなデバイスが非アクティブ状態に遷移することを示すイベントの検知を行います。これらのイベントをポートの認証状態の制御に利用し、ポートでの認証が行わない場合に接続デバイスの認証プロセスを開始します。これをポートベースのアクセスコントロールと呼びます。

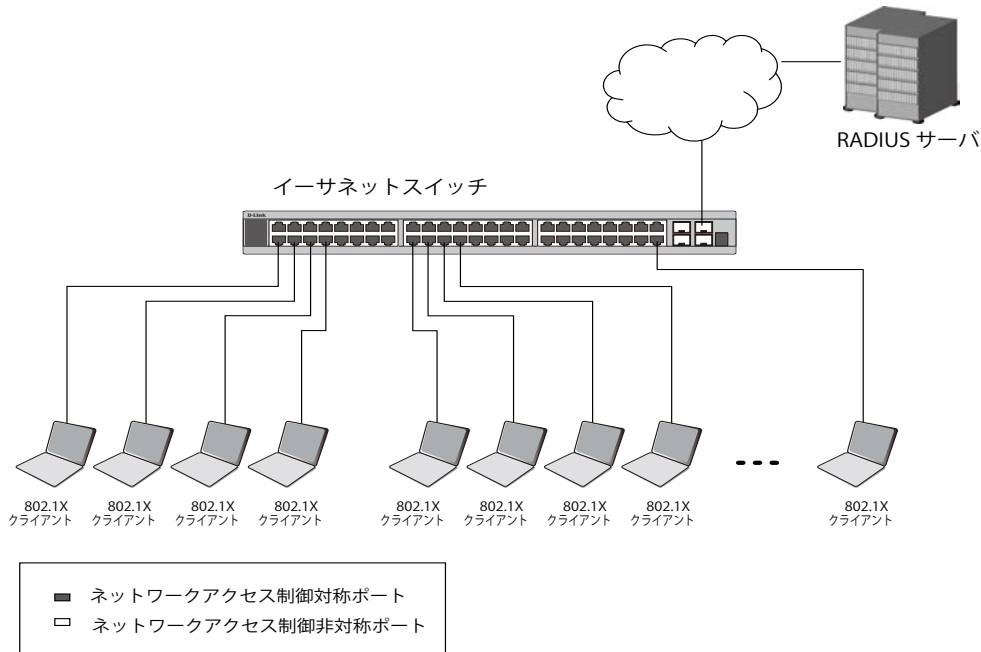


図 12-7 典型的なポートベースアクセスコントロールのネットワーク構成例

一度接続デバイスが認証に成功すると、ポートは Authorized（認証済み）状態になり、ポートが未認証になるようなイベントが発生するまでポート上のすべてのトラフィックはアクセスコントロール制限の対象となりません。そのため、ポートが 1 台以上のデバイスが所属する共有 LAN セグメントに接続される場合、接続デバイスの 1 つが認証に成功すると共有セグメント上のすべての LAN に対して事実上アクセスを許可することになります。このような状態のセキュリティは明らかに脆弱であると言えます。

MAC ベースのネットワークアクセスコントロール

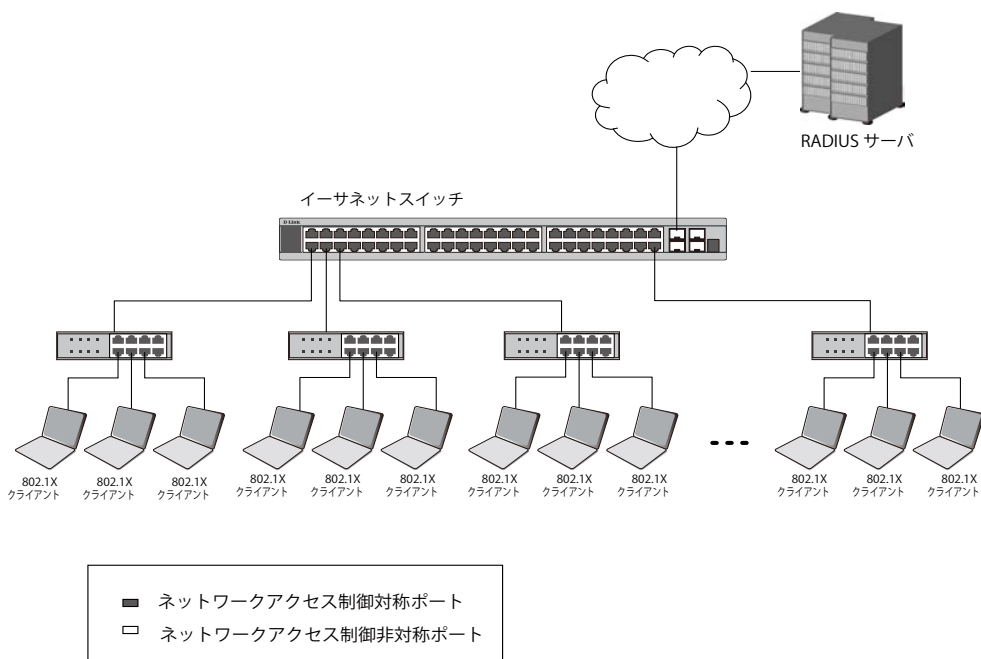


図 12-8 典型的な MAC ベースアクセスコントロールのネットワーク構成例

共有 LAN セグメント内で 802.1X を活用するためには、LAN へのアクセスを希望する各デバイスに「仮想」ポートを定義する必要があります。するとスイッチは共有 LAN セグメントに接続する 1 つの物理ポートを、異なる論理ポートの集まりであると認識し、それら仮想ポートを EAPOL の交換と認証状態に基づいて別々に制御します。スイッチは接続する各デバイスの MAC アドレスを学習し、それらのデバイスがスイッチ経由で LAN と通信するための仮想ポートを確立します。

802.1X Global Settings (802.1X グローバル設定)

802.1X グローバルパラメータを設定します。

Security > 802.1X > 802.1X Global Settings の順にメニューをクリックし、以下の画面を表示します。

図 12-9 802.1X Global Settings 画面

以下の項目を使用して設定を行います。

| 項目 | 説明 |
|-------------------------|--|
| Authentication Mode | 802.1X 機能を「Disabled」、「Port-based」または「MAC-based」から選択します。 |
| Authentication Protocol | 認証プロトコルを「Local」または「RADIUS EAP」から選択します。 |
| Forward EAPOL PDU | これは、EAPOL PDU の転送を制御するグローバル設定です。802.1X 機能をグローバルまたはポートに無効とした場合に、802.1X forward PDU がグローバルおよびポートに有効にされると、ポートに受信した EAPOL パケットは同じ VLAN 内で (グローバルまたはそのポートに対して) 802.1X forward PDU が有効で 802.1X が無効であるポートにフラッドします。初期値は無効です。 |
| Max Users | ユーザの最大数を指定します。最大ユーザ数は 448 です。「No Limit」をチェックすると、ユーザ制限はなくなります。 |
| RADIUS Authorization | 認可設定の受け入れを有効または無効にします。802.1X の RADIUS における許可を有効にする場合、グローバルな認可ネットワークが有効になると、RADIUS サーバに割り当てられる認可データが許可されます。 |

「Apply」ボタンをクリックして行った変更を適用します。

802.1X Port Settings (802.1X ポート設定)

802.1X のオーセンティケータ設定を行います。

Security > 802.1X > 802.1X Port Settings の順にメニューをクリックし、以下の画面を表示します。

図 12-10 802.1X Port Settings 画面

以下の項目を使用して設定を行います。

| 項目 | 説明 |
|---------------------|---|
| Unit | 設定するユニットを選択します。 |
| From Port / To Port | 設定するポート範囲を指定します。 |
| QuietPeriod | クライアントの認証交換に失敗した後、スイッチが静止状態のままクライアントとの通信を拒否する期間 (秒)。初期値は 60 (秒) です。 |

Security(セキュリティ機能の設定)

| 項目 | 説明 |
|-------------------|---|
| SuppTimeout | オーセンティケータとクライアント間の交換でクライアントに EAP-Request を送信した後、応答を待つ時間。初期値は 30 (秒) です。IEEE-802.1X-2001 P47 の SuppTimeout で定義されています。サブリカントがタイムアウトになった際に aWhile タイマを初期化する値です。初期値は 30 (秒) です。しかし、現在の認証交換に関連するチャレンジのタイプが異なるタイムアウト値を要求する場合 (例えば、チャレンジがユーザ側の操作を必要とする場合)、タイムアウト値はそれに基づいて調整されます。1-65535 (秒) の範囲の任意の値に設定することができます。 |
| ServerTimeout | オーセンティケータが認証サーバ間の交換でオーセンティケータが Access-Request を送信した後、応答を待つ時間。初期値は 30 (秒) です。 |
| MaxReq | 認証セッションのタイムアウト前にスイッチからクライアントへの EAPOL-Request パケットの最大再送回数。初期値は 2 です。IEEE-802.1X-2001 P47 の MaxReq で定義されています。認証セッションのタイムアウト前にスイッチからクライアントへの EAPOL-Request パケットの最大再送回数。初期値は 2 です。1-10 までの範囲の任意の値を設定できます。 |
| TxPeriod | オーセンティケータ PAE 状態マシンの TxPeriod の時間を指定します。本値がクライアントへの EAP Request/Identity パケットの送信間隔となります。初期値は 30 (秒) です。 |
| ReAuthPeriod | クライアントの再認証間隔を定義する 0 (秒) 以外の定数。初期値は 3600 (秒) です。 |
| ReAuthentication | このポート上で通常の再認証を行うかどうか指定します。初期値は「Disabled」です。 |
| Port Control | ポートの認証状態を制御できます。 <ul style="list-style-type: none"> ForceAuthorized - 802.1X を無効にし、認証情報の交換を要求せずにポートを Authorized 状態にします。この時ポートではクライアントの 802.1X ベースの認証を行うことなく、通常のトラフィックの送受信が可能になります。 ForceUnauthorized - 対象ポートは Unauthorized 状態を貫き、すべてのクライアントからの認証要求を無視します。スイッチはインタフェースを通したクライアントの認証サービスを行いません。 Auto - 802.1X を有効にし、Unauthorized 状態を開始し、ポートにおいて EAPOL フレームのみの送受信を許可します。認証プロセスは、ポートのリンク状態が Down から Up に遷移した時、または EAPOL-start フレームが受信された時に開始されます。スイッチはクライアントの ID を要求し、クライアントと認証サーバとの間で認証メッセージの中継を開始します。(初期値) |
| Capability | ポートに 802.1X オーセンティケータの設定を適用するために使用します。Authenticator が設定をポートに適用するのを選択してください。 <ul style="list-style-type: none"> Authenticator - ユーザは認証プロセスを通過するとネットワークにアクセス可能になります。 None - 指定ポートは 802.1X 認証機能によって制御されません。 |
| Direction | 管理制御するトラフィックの方向 (Both または In) を指定します。 <ul style="list-style-type: none"> Both - 指定したポートでの入力、出力トラフィックの両方が制御対象となります。 In - 最初の欄に指定したポートへの入力トラフィックのみ制御対象となります。 |
| Forward EAPOL PDU | これは、EAPOL PDU の転送を制御するポートベースの設定です。802.1X 機能をグローバルまたはポートに無効とした場合に、802.1X forward PDU がグローバルおよびポートに有効にされると、ポートに受信した EAPOL パケットは同じ VLAN 内で (グローバルまたはそのポートに対して) 802.1X forward PDU が有効で 802.1X が無効であるポートにフラッドします。初期値は無効です。 |
| Max User | ユーザの最大数を指定します。最大ユーザ数は 448 です。初期値は 16 です。 |

「Refresh」 ボタンをクリックして、テーブルを更新して新しいエントリを表示します。

「Apply」 ボタンをクリックして行った変更を適用します。

802.1X User Settings (802.1X ユーザ設定)

スイッチのローカルデータベースに様々な 802.1X ユーザを設定します。

Security > 802.1X > 802.1X User Settings の順にメニューをクリックし、以下の画面を表示します。

図 12-11 802.1X User Settings 画面

以下の項目を使用して設定を行います。

| 項目 | 説明 |
|------------------|---------------------------|
| 802.1X User | 802.1X ユーザのユーザ名を入力します。 |
| Password | 802.1X ユーザのパスワードを入力します。 |
| Confirm Password | 802.1X ユーザのパスワードを再度入力します。 |

「Apply」 ボタンをクリックして行った変更を適用します。

「Delete」 ボタンをクリックして、指定エントリを削除します。

注意 802.1X ユーザ名とパスワードは 16 文字以内とします。

Guest VLAN (ゲスト VLAN の設定)

802.1X セキュリティが有効であるネットワークでは、Windows 98 やそれより以前の OS が動作するコンピュータのように適切な 802.1X ソフトウェアの欠落や互換性のないデバイス、またはゲストが限定した権限でネットワークに接続するために 802.1X をサポートしていないデバイスにも限られた範囲でアクセスできる必要があります。本スイッチは、ゲスト 802.1X VLAN 機能を搭載しています。この VLAN には制限付きのアクセス権があり、他の VLAN とは分かれています。

ゲスト 802.1X VLAN を実行するためには、はじめにネットワークに制限付き 802.1X ゲスト VLAN を作成し、この VLAN を有効にします。次に管理者は、ゲスト VLAN 内のスイッチにアクセスするゲストアカウントを作成します。スイッチへはじめてエントリする際には、スイッチにアクセスするクライアントは、リモート RADIUS サーバまたはフル操作が可能な VLAN 内に設置されているスイッチのローカル認証により認証される必要があります。

認証され、Authenticator が VLAN プレースメント情報を処理した場合、クライアントはフル操作が可能なターゲット VLAN にアクセスを許可され、通常のスイッチ機能がクライアントにサービスを開始します。Authenticator がターゲットの VLAN プレースメント情報を持たない場合、クライアントは元の VLAN に戻されます。クライアントが Authenticator によって認証を拒否されたら、制限付き権限を持つゲスト VLAN に置かれます。以下でゲスト VLAN プロセスについて説明します。

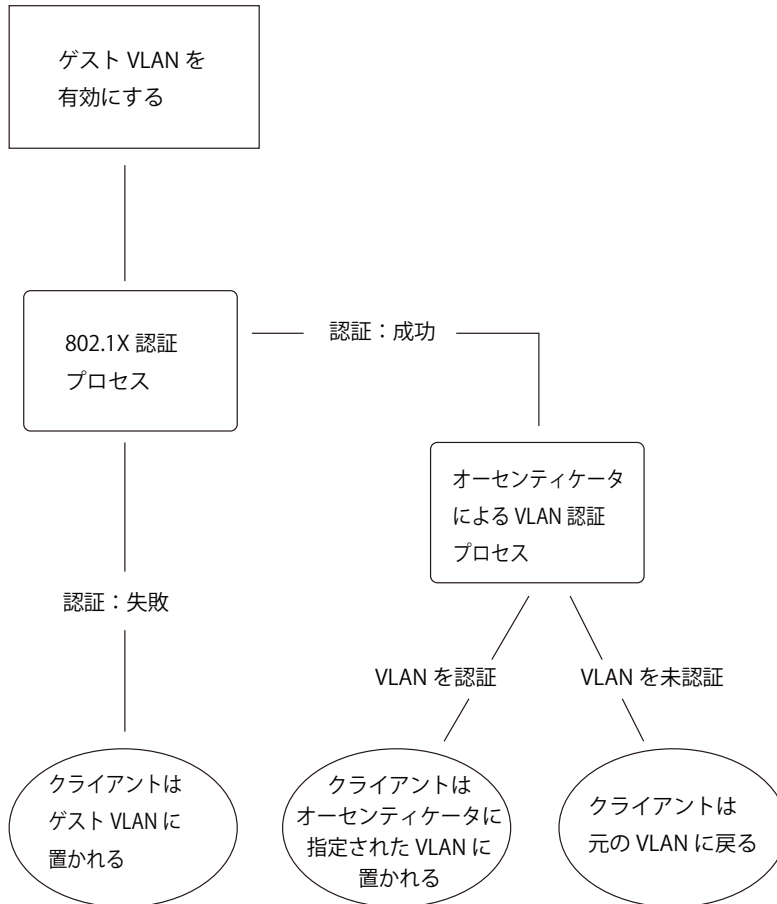


図 12-12 ゲスト VLAN 認証プロセス画面

ゲスト VLAN を使用する場合の制限事項

1. ゲスト VLAN はポートベースの VLAN にのみ対応しています。MAC ベースの VLAN では、本プロセスは行われません。
2. ゲスト VLAN をサポートするポートで GVRP を有効化することはできません。また、GVRP が有効であるポートでゲスト VLAN はサポートできません。
3. ポートはゲスト VLAN とスタティック VLAN の両方に所属することはできません。
4. クライアントがターゲット VLAN に所属を許可されると、ゲスト VLAN にはアクセスできなくなります。
5. ポートが複数の VLAN に所属している場合、ゲスト VLAN には所属できません。

ゲスト VLAN 設定

ゲスト VLAN を設定します。

注意 ゲスト VLAN を設定するためには、ここでゲスト VLAN ステータスを有効にできる VLAN をあらかじめ設定しておく必要があります。

Security > 802.1X > Guest VLAN の順にクリックし、以下の画面を表示します。

図 12-13 Guest VLAN Settings 画面

以下の項目によりゲスト VLAN を有効にすることができます。

| 項目 | 説明 |
|-----------|--|
| VLAN Name | ゲスト 802.1X VLAN にする定義済みの VLAN 名を入力します。 |
| Unit | 設定するユニットを指定します。 |
| Ports | ゲスト 802.1X VLAN を有効にするポートを設定します。「All」ボタンをクリックするとすべてのポートを選択します。 |

「Apply」ボタンをクリックし、設定を有効にします。正しく設定されるとゲスト VLAN 名と対象のポートが画面の下部に表示されます。

「Delete」ボタンをクリックして、入力した情報に基づいて指定エントリを削除します。

Authenticator State (オーセンティケータの状態)

オーセンティケータの状態を表示します。「Authentication State」が「802.1X Global Settings」画面で有効な場合に表示されます。

Security > 802.1X > Authenticator State の順にメニューをクリックし、以下の画面を表示します。

図 12-14 Authenticator State 画面

設定対象となる項目は以下の通りです。

| 項目 | 説明 |
|------|--------------------------------|
| Unit | 表示するユニットを選択します。 |
| Port | プルダウンメニューを使用して表示するポート範囲を指定します。 |

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

「Refresh」ボタンをクリックして、テーブルを更新して新しいエントリを表示します。

Authenticator Statistics (オーセンティケータ統計情報)

オーセンティケータの統計情報を表示します。「Authentication State」が「802.1X Global Settings」画面で有効な場合に表示されます。

Security > 802.1X > Authenticator Statistics の順にメニューをクリックし、以下の画面を表示します。



図 12-15 Authenticator Statics 画面

設定対象となる項目は以下の通りです。

| 項目 | 説明 |
|------|--------------------------------|
| Unit | 表示するユニットを選択します。 |
| Port | プルダウンメニューを使用して表示するポート範囲を指定します。 |

「Apply」ボタンをクリックして行った変更を適用します。

Authenticator Session Statistics (オーセンティケータセッション統計情報)

オーセンティケータセッションの統計情報を表示します。「Authentication State」が「802.1X Global Settings」画面で有効な場合に表示されます。

Security > 802.1X > Authenticator Session Statistics の順にメニューをクリックし、以下の画面を表示します。

| Index | Octets RX | Octets TX | Frames RX | |
|-------|-----------|-----------|-----------|--|
| 1 | null | null | null | |
| 2 | null | null | null | |
| 3 | null | null | null | |
| 4 | null | null | null | |
| 5 | null | null | null | |
| 6 | null | null | null | |
| 7 | null | null | null | |
| 8 | null | null | null | |
| 9 | null | null | null | |
| 10 | null | null | null | |

図 12-16 Authenticator Session Statistics 画面

設定対象となる項目は以下の通りです。

| 項目 | 説明 |
|------|--------------------------------|
| Unit | 表示するユニットを選択します。 |
| Port | プルダウンメニューを使用して表示するポート範囲を指定します。 |

「Apply」ボタンをクリックして行った変更を適用します。

Authenticator Diagnostics (オーセンティケータ診断)

オーセンティケータ診断情報を表示します。「Authentication State」が「802.1X Global Settings」画面で有効な場合に表示されます。

Security > 802.1X > Authenticator Diagnostics の順にメニューをクリックし、以下の画面を表示します。

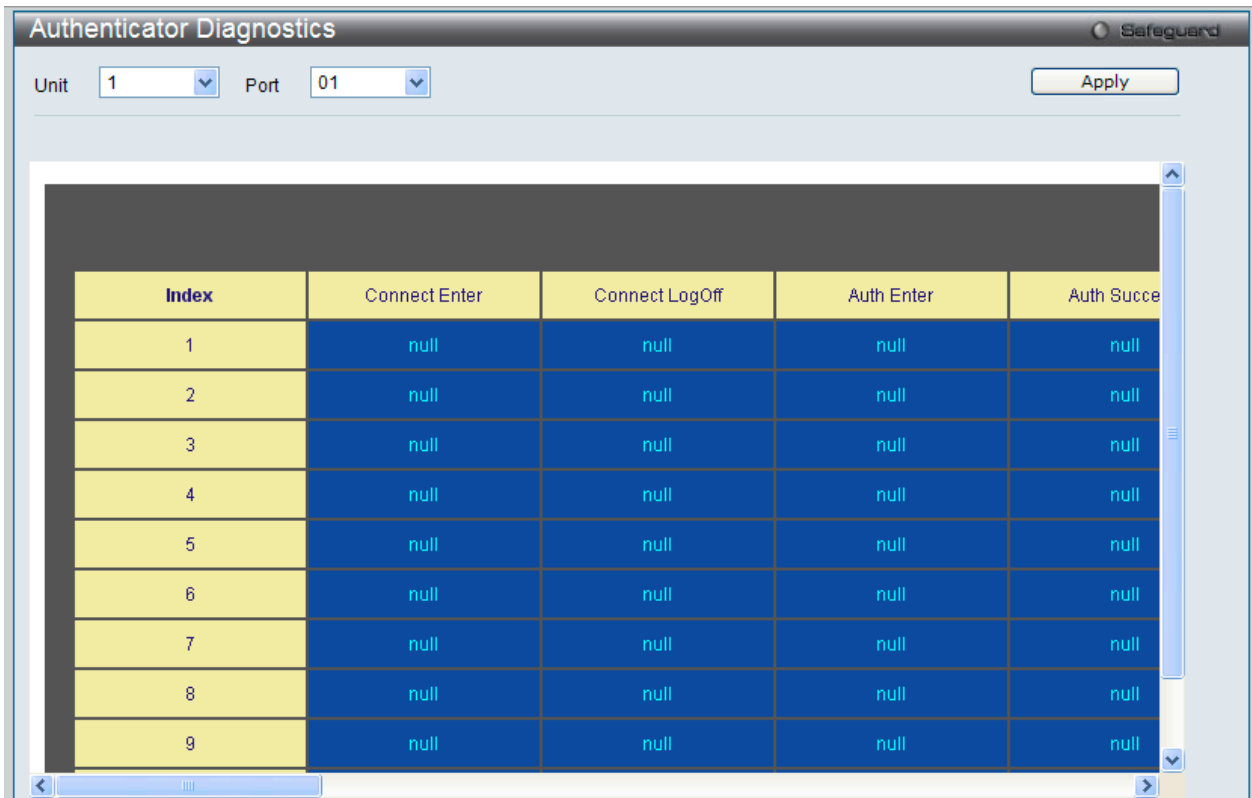


図 12-17 Authenticator Diagnostics 画面

設定対象となる項目は以下の通りです。

| 項目 | 説明 |
|------|--------------------------------|
| Unit | 表示するユニットを選択します。 |
| Port | プルダウンメニューを使用して表示するポート範囲を指定します。 |

「Apply」ボタンをクリックして行った変更を適用します。

Initialize Port-based Port(s) (初期化ポート - ポートベース)

ポートベースポートの 802.1X 認証ステートマシンを初期化します。また、現在の初期化されているポートベースポートを表示します。「Authentication State」が「802.1X Global Settings」画面で有効な場合に表示されます。

Security > 802.1X > Initialize Port-based Port(s) の順にメニューをクリックし、以下の画面を表示します：

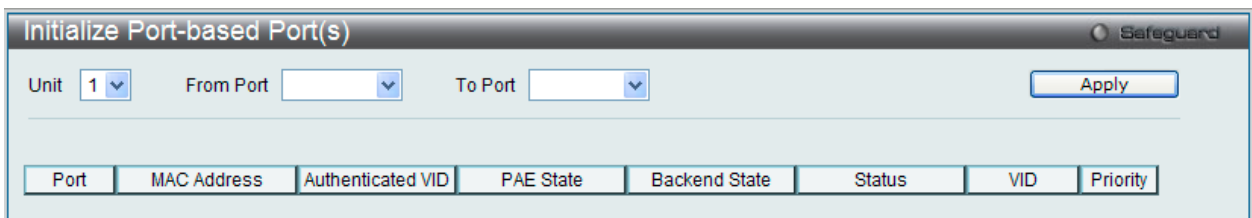


図 12-18 Initialize Port-based Port(s) 画面

設定対象となる項目は以下の通りです。

| 項目 | 説明 |
|---------------------|--------------------------------|
| Unit | 表示するユニットを選択します。 |
| From Port / To Port | プルダウンメニューを使用して表示するポート範囲を指定します。 |

「Apply」ボタンをクリックして行った変更を適用します。

Initialize Host-based Port(s) (初期化ポート - ホストベース)

ホストベースポートの 802.1X 認証ステートマシンを初期化します。また、現在の初期化されているポート（ホストベース）を表示します。「Authentication State」が「802.1X Global Settings」画面で有効な場合に表示されます。

Security > 802.1X > Initialize Host-based Port(s) の順にメニューをクリックし、以下の画面を表示します。

図 12-19 Initialize Host-based Port(s) 画面

設定対象となる項目は以下の通りです。

| 項目 | 説明 |
|---------------------|--|
| Unit | 表示するユニットを選択します。 |
| From Port / To Port | プルダウンメニューを使用して表示するポート範囲を指定します。 |
| MAC Address | もしあれば、対応するポートに接続されたスイッチの MAC アドレスを入力します。 |

「Apply」ボタンをクリックして行った変更を適用します。

Reauthenticate Port-based Port(s) (再認証ポート - ポートベース)

現在の再認証ポート（ポートベース）を表示します。「Authentication State」が「802.1X Global Settings」画面で有効な場合に表示されます。

Security > 802.1X > Reauthenticate Port-based Port(s) の順にメニューをクリックし、以下の画面を表示します。

図 12-20 Reauthenticate Port-based Port(s) 画面

設定対象となる項目は以下の通りです。

| 項目 | 説明 |
|---------------------|--------------------------------|
| Unit | 表示するユニットを選択します。 |
| From Port / To Port | プルダウンメニューを使用して表示するポート範囲を指定します。 |

「Apply」ボタンをクリックして行った変更を適用します。

Reauthenticate Host-based Port(s) (再認証ポート - ホストベース)

現在の再認証ポート（ホストベース）を表示します。「Authentication State」が「802.1X Global Settings」画面で有効な場合に表示されます。

Security > 802.1X > Reauthenticate Host-based Port(s) の順にメニューをクリックし、以下の画面を表示します。

図 12-21 Reauthenticate Host-based Port(s)

設定対象となる項目は以下の通りです。

| 項目 | 説明 |
|---------------------|--------------------------------|
| Unit | 表示するユニットを選択します。 |
| From Port / To Port | プルダウンメニューを使用して表示するポート範囲を指定します。 |
| MAC Address | チェックを行い、MAC アドレスを入力します。 |

「Apply」ボタンをクリックして行った変更を適用します。

RADIUS (RADIUS 設定)

Authentication RADIUS Server Settings (認証 RADIUS サーバ設定)

スイッチの RADIUS 機能は中央集中型のユーザ管理を容易にし、またスニффイングやハッカーからの攻撃から保護します。

Security > RADIUS > Authentication RADIUS Server の順にメニューをクリックし、以下の画面を表示します。

図 12-22 Authentic RADIUS Server Settings 画面

本画面は 2 つのメインセクションに分かれています。上のセクションでは、管理者が RADIUS サーバ設定を行い、下のセクションではシステムに現在設定されている RADIUS サーバの設定を表示します。

使用される項目の説明は以下の通りです。

| 項目 | 説明 |
|-------------------------------|---|
| Index | 「1」、「2」、「3」、「select the IPv4 Address」から設定を行う RADIUS サーバを選択します。 |
| IPv4 Address | RADIUS サーバの IP アドレスを入力します。 |
| IPv6 Address | RADIUS サーバの IPv6 アドレスを入力します。 |
| Authentication Port (1-65535) | スイッチと RADIUS サーバ間で RADIUS 認証データを送信するために使用される RADIUS 認証サーバの UDP ポート番号を指定します。初期値は 1812 です。 |
| Accounting Port (1-65535) | スイッチと RADIUS サーバ間で RADIUS アカウンティング統計情報を送信するために使用される RADIUS 認証サーバの UDP ポート番号を指定します。初期値は 1813 です。 |
| Timeout (1-255) | RADIUS サーバのエージングタイム (秒) を設定します。 |
| Retransmit (1-20) | RADIUS サーバの送信回数を設定します。 |
| Key | RADIUS サーバと同じキーを入力します。 |
| Confirm Key | RADIUS サーバと同じキーを確認のために再度入力します。 |

「Apply」ボタンをクリックして行った変更を適用します。

エントリの編集

1. 編集するエントリの「Edit」ボタンをクリックして、以下の画面を表示します。

| Index | IP Address | Auth-Port | Acct-Port | Timeout | Retransmit | Key | Edit | Delete |
|-------|-------------|-----------|-----------|---------|------------|-------|------|--------|
| 1 | 10.90.90.90 | 1812 | 1813 | 5 | 2 | ***** | | |
| 2 | | | | | | | | |
| 3 | | | | | | | | |

図 12-23 Authentic RADIUS Server Settings 画面 - Edit

2. エントリの編集後、「Apply」ボタンをクリックします。

エントリの削除

削除するエントリの「Delete」ボタンをクリックします。

RADIUS Authentication (RADIUS 認証)

RADIUS 認証プロトコルでクライアント側の RADIUS 認証クライアントの動作に関連する情報を表示します。

Security > RADIUS > RADIUS Authentication をクリックし、以下の画面を表示します。

| ServerIndex | InvalidServerAddr | Identifier | AuthServerAddr | ServerPortNumber | RoundTripTime |
|-------------|-------------------|------------|----------------|------------------|---------------|
| 1 | 0 | | 10.90.90.90 | 1812 | 0 |
| 2 | 0 | | | 0 | 0 |
| 3 | 0 | | | 0 | 0 |

図 12-24 RADIUS Authentication 画面

統計情報の更新間隔を 1s から 60s (s : 秒) で選択します。初期値は 1s (1 秒) です。現在の統計情報をクリアするためには左上角の「Clear」ボタンをクリックします。以下の情報が表示されます。

| 項目 | 説明 |
|-------------------|--|
| ServerIndex | クライアントが暗号鍵を共有している各 RADIUS 認証サーバに割り当てられた識別子の番号。 |
| InvalidServerAddr | 不明なアドレスから受信した RADIUS Access-Response パケット数。 |
| Identifier | RADIUS 認証クライアントの NAS 識別子。(MIB II の sysName と同じである必要はありません。) |
| AuthServerAddr | クライアントが暗号鍵を共有している RADIUS 認証サーバを一覧にしているテーブル。 |
| ServerPortNumber | クライアントがこのサーバにリクエストを送信するために使用する UDP ポート。 |
| RoundTripTime | 最も最近 RADIUS 認証サーバから送信された Access-Reply/Access-Challenge と Access-Request の間隔 (1/100 秒単位)。 |
| AccessRequests | サーバに送信された RADIUS Access-Request パケット数。再送信は含まれません。 |
| AccessRetrans | 本 RADIUS 認証サーバに再送信された RADIUS Access-Request パケット数。 |
| AccessAccepts | 本サーバから受信した RADIUS Access-Accept パケット数 (有効 / 無効パケット)。 |
| AccessRejects | 本サーバより受信した RADIUS Access-Reject パケット数 (有効 / 無効パケット)。 |
| AccessChallenges | 本サーバより受信した RADIUS Access-Challenge パケット数 (有効 / 無効パケット)。 |
| AccessResponses | 本サーバより受信した不正な形式の RADIUS Access-Response パケット数。不正形式のパケットには不正な長さのパケットも含まれます。不正認証、署名属性、または不明なタイプは不正な Access Responses としては含まれません。 |
| BadAuthenticators | 本サーバより受信した不正認証や署名属性 RADIUS Access-Response パケット数。 |
| PendingRequests | まだタイムアウトになっていない、またはレスポンスを受信していないこのサーバ行きの RADIUS Access-Request パケット数。この変数は Access-Request が送信されると 1 つ増加し、Access-Accept、Access-Reject または Access-Challenge の受信、タイムアウトまたは再転送時に 1 つ減少します。 |
| Timeouts | 本サーバへの認証タイムアウト数。タイムアウトの後、クライアントは同じサーバにリトライするか、異なるサーバに送信するか、または送信を終了します。同じサーバへのリトライはタイムアウトと同様に再転送としてカウントされます。異なるユーザへの送信はタイムアウトと同様に Request としてカウントされます。 |
| UnknownTypes | 本サーバから認証ポートに受信した不明なタイプの RADIUS パケット数。 |
| PacketsDropped | 本サーバから認証ポートに受信し、何らかの理由で破棄した RADIUS パケット数。 |

RADIUS Account Client (RADIUS アカウンティングクライアント)

RADIUS Accounting クライアントを管理するために使用する管理オブジェクトとそれらに関連した現在の統計情報を表示します。

Security > RADIUS > RADIUS Accounting Client をクリックし、以下の画面を表示します。

| ServerIndex | InvalidServerAddr | Identifier | |
|-------------|-------------------|------------|--|
| 1 | 0 | | |
| 2 | 0 | | |
| 3 | 0 | | |

図 12-25 RADIUS Accounting Client 画面

統計情報を更新するためには更新間隔を 1s ~ 60s (s は秒) から指定します。初期値は 1 (秒) です。現在の統計情報をクリアするためには左上の「Clear」ボタンをクリックします。以下の情報が表示されます。

| 項目 | 説明 |
|--------------------|--|
| ServerIndex | クライアントが暗号鍵を共有する RADIUS Accounting サーバの IP アドレス。 |
| InvalidServerAddr | 不明なアドレスから受信した RADIUS Accounting-Response パケット数。 |
| Identifier | RADIUS アカウンティングクライアントの NAS 識別子。(MIB II の sysName と同じである必要はありません。) |
| ServerAddress | クライアントが暗号鍵を共有している RADIUS アカウンティングサーバを一覧にしているテーブル。 |
| ServerPortNumber | クライアントがこのサーバにリクエストを送信するために使用する UDP ポート。 |
| RoundTripTime | RADIUS アカウンティングサーバからクライアントに送信される最も新しい Accounting-Response と Accounting-Request の間隔。 |
| Requests | 送信された RADIUS Accounting-Request パケット数。これは再転送のパケット数は含まれていません。 |
| Retransmissions | RADIUS アカウンティングサーバに再送された RADIUS Accounting-Request 数。再送には、同じものが残るような Identifier および Acct-Delay が更新されるといったリトライも含まれます。 |
| Responses | 本サーバから Accounting ポートに受信した RADIUS パケット数。 |
| MalformedResponses | このサーバから受信した不正な形式の RADIUS Accounting-Response パケット数。Malformed packets には不正な長さのパケットが含まれます。認証エラーや不明なタイプは不正な accounting responses としては含まれません。 |
| BadAuthenticators | このサーバから受信した不正な認証を含む RADIUS Accounting-Response パケット数。 |
| PendingRequests | まだタイムアウトになっていない、またはレスポンスを受信していないサーバ行きの RADIUS Accounting-Request パケット数。この変数は Accounting-Request が送信された時に 1 つ加算し、Accounting-Response の受信、タイムアウトまたは再転送時に 1 つ減少します。 |
| Timeouts | このサーバへの Accounting タイムアウト数。タイムアウトの後、クライアントは同じサーバにリトライするか、異なるサーバに送信するか、または送信を終了します。同じサーバへのリトライはタイムアウトと同様に再転送としてカウントされます。異なるユーザへの送信はタイムアウトと同様に Accounting-Request としてカウントされます。 |
| UnknownTypes | このサーバから Accounting ポートに受信した不明なタイプの RADIUS パケット数。 |
| PacketsDropped | このサーバから Accounting ポートに受信し、何らかの理由で破棄した RADIUS パケット数。 |

IP-MAC-Port Binding (IMPB: IP-MAC-ポートバインディング)

IP ネットワークレイヤ (IP レベル) では IPv4/IPv6 のアドレスを使用し、イーサネットリンクレイヤ (データリンクレベル) では MAC アドレスを使用します。これらの 2 つのアドレスタイプを結合させることにより、レイヤ間のデータ転送を可能にします。IP-MAC-ポートバインディングの第一の目的は、スイッチにアクセスする認可ユーザ数を制限することです。IP/MAC アドレスのペアを、事前に設定したデータベースと比較を行うことで、認証クライアントはスイッチのポートアクセスできるようになります。また、DHCP Snooping を有効にすると、スイッチは、DHCP パケットを検索し、IMPB ホワイトリストにそれらを保存することで自動的に IP/MAC アドレスのペアを学習します。未認証ユーザが IP-MAC バインディングが有効なポートにアクセスしようとすると、システムはアクセスをブロックして、パケットを廃棄します。xStack® DGS-3420 スイッチシリーズでは、アクティブ、インアクティブエントリは同じデータベースを使用します。IPv4/IPv6 最大エントリ数は 510/511 です。認証クライアントのリストは、CLI または Web により手動で作成できます。

本機能はポートベースであるため、ポートごとに本機能を有効/無効にすることができます。

IMPB Global Settings (IMPB グローバル設定)

スイッチのグローバルな IP-MAC-ポートバインディング設定 (トラップログステータスおよび DHCP Snoop ステータス) を有効または無効にするのに使用します。「Trap/Log」欄では、IP-MAC-ポートバインディングのトラップログメッセージ送信を有効または無効にします。有効にすると、スイッチはスイッチに設定された IP-MAC バインディング - ポートに一致しない ARP/IP パケットを受信した場合に、SNMP エージェントとスイッチログにトラップログメッセージを送信します。

Security > IP-MAC-Port Binding (IMPB) > IMPB Global Settings の順にメニューをクリックして、以下の画面を表示します。

図 12-26 IMPB Global Settings 画面

以下の項目を使用して、設定または編集を行います。

| 項目 | 説明 |
|--|--|
| Roaming State | IMPB ローミングを有効/無効にします。 IMPB ローミングが有効の場合、指定ポートの DHCP/ND スヌーピングを通して学習した認証 MAC アドレスは、①同じ IP と MAC アドレスに属する新しい DHCP プロセスの場合と、②同じ IP アドレスと MAC アドレスに属する新しい DAD プロセスの場合に、DHCP ポートを変更することができます。 |
| Trap/Log | IP-MAC バインディングのトラップログメッセージ送信を有効または無効にします。有効にすると、スイッチはスイッチに設定された IP-MAC バインディングに一致しない ARP パケットを受信した場合に、SNMP エージェントとスイッチログにトラップログメッセージを送信します。初期値は「Disabled」です。 |
| DHCP Snooping (IPv4) | IP-MAC-ポートバインディングの DHCP Snooping (IPv4) オプションを「Enabled」(有効)または「Disabled」(無効)にします。初期値は「Disabled」です。 |
| DHCP Snooping (IPv6) | IP-MAC-ポートバインディングの DHCP Snooping (IPv6) オプションを「Enabled」(有効)または「Disabled」(無効)にします。初期値は「Disabled」です。 |
| ND Snooping | スイッチの ND snooping を「Enabled」(有効)/「Disabled」(無効)にします。初期値は「Disabled」です。 |
| Recover Learning Ports | 学習状態を回復するポート番号を選択します。「All」をチェックすると、すべての学習ポートのリカバリを行います。 |
| Download and Upload Address Binding Snooping Entry | |
| File Name | 本オプションは「DHCPv4」スヌーピングバインディングエントリを TFTP を使用してアップロード/ダウンロードします。TFTP サーバにファイルパスを入力、または「Browse(参照)」ボタンからファイルを指定します。「Download」をクリックするとダウンロードを開始します。「Upload」をクリックするとアップロードを開始します。 |

| 項目 | 説明 |
|--|---|
| Address Binding DHCP Snooping Entry File | 本オプションは「DHCPv4」スヌーピングバインディングエントリの保存に使用します。ファイル名を入力します。本機能は SD カードなどの外部メモリをサポートする機器のみに対応します。 |
| Auto Save | 自動保存機能について有効/無効に設定します。 |
| Save DHCP Snooping Binding Entry | スヌーピングバインディングエントリを手動で保存します。「Save」をクリックします。 |

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

IMPB Port Settings (IMPB ポート設定)

ポートベースで IP-MAC- ポートバインディング設定を行います。

Security > IP-MAC-Port Binding (IMPB) > IMPB Port Settings の順にメニューをクリックし、以下の画面を表示します。

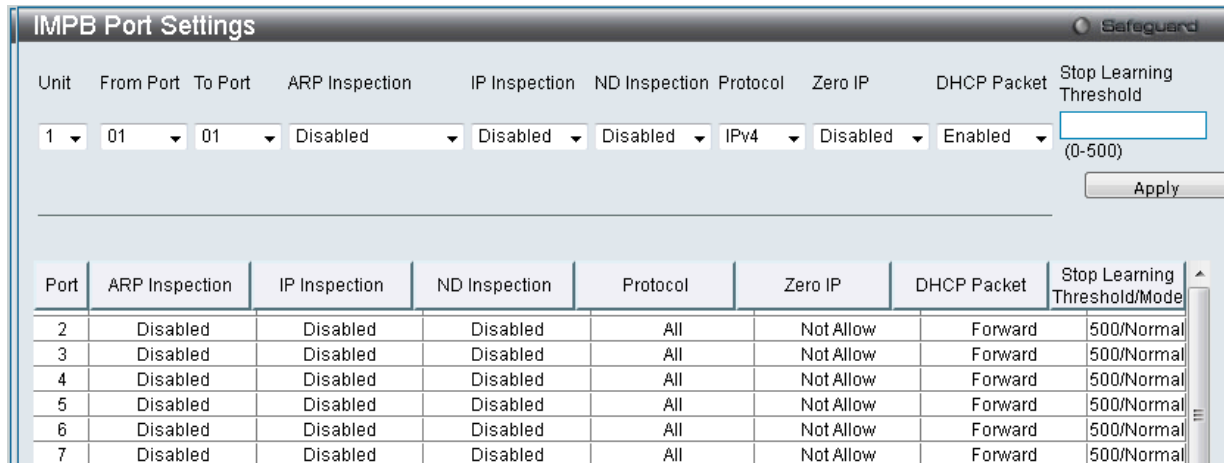


図 12-27 IMPB Port Settings 画面

以下の項目を使用して、設定または編集を行います。

| 項目 | 説明 |
|-------------------------|---|
| Unit | 設定するユニットを選択します。 |
| From Port/To Port | IP-MAC- ポートバインディングを設定する対象のポートを指定します。 |
| ARP Inspection | ARP 検証機能が有効な場合、正しい ARP パケットは転送され一方不正なパケットは破棄されます。 <ul style="list-style-type: none"> Disabled - ARP 検証機能を無効にします。 Enabled (Strict) - 本モードはハードウェアによる MAC アドレスの学習を無効にします。本モードでは、正しい ARP または IP パケットが検出されるまで、すべてのパケットが初期値で破棄されます。本モードを有効にすると、スイッチはポートの破棄 FDB エントリの記載を停止します。正しいパケットを検出した場合は、スイッチは FDB エントリを記載する必要があります。 Enabled (Loose) - 本モードでは、不正な ARP またはブロードキャスト IP パケットが検出されるまで、初期値ですべてのパケットを転送します。初期値は「Disabled」(無効)です。 |
| IP Inspection | ARP と IP 検証の両方を有効にすると、すべての IP パケットがチェックされます。正しい IP パケットは転送され、一方不正なパケットは破棄されます。IP 検証が有効で、ARP 検証が無効である場合、IP でない全パケット (例 L2 パケット、または ARP) が初期値で送信されます。初期値は「Disabled」(無効)です。 |
| Protocol | プルダウンメニューを使用してプロトコルレベル (IPv4、IPv6 または All) を選択します。 |
| Zero IP | プルダウンメニューを使用して、本機能を「Enabled」(有効) / 「Disabled」(無効) にします。「Allow zero IP」を設定すると、ステートが 0.0.0.0 送信元 IP の ARP パケットを許容します。 |
| DHCP Packet | 初期設定では、ブロードキャスト DA の DHCP パケットをフラッドします。無効にすると、指定ポートが受信したブロードキャスト DHCP パケットは、「strict」モードでは転送されません。本設定は、CPU がトラップした DHCP パケットをソフトウェアが転送する必要がある時、DHCP Snooping で有効である場合に効果があります。本設定はこの状況における転送の実行を制御します。 |
| Stop Learning Threshold | ポートにおいてブロックされるエントリ数を表示します。初期値は 500 です。 |

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

IMPB Entry Settings (IMPB エントリ設定)

スイッチにスタティック IP-MAC- ポートバインディングエントリを作成します。

Security > IP-MAC-Port Binding (IMPB) > IMPB Entry Settings の順にメニューをクリックし、以下の画面を表示します。

図 12-28 IMPB Entry Settings 画面

以下の項目を使用して、設定または編集を行います。

| 項目 | 説明 |
|--------------|---|
| IPv4 Address | チェックして MAC アドレスにバインドする IP アドレスを入力します。 |
| IPv6 Address | チェックして MAC アドレスにバインドする IPv6 アドレスを入力します。 |
| MAC Address | IP アドレスとバインドする MAC アドレスを入力します。 |
| Ports | 本 IP-MAC バインディングエントリ (IP アドレス + MAC アドレス) を設定する対象のポートを指定します。「All Ports」を選択すると、スイッチのすべてのポートに設定します。 |

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

エントリの追加

- 「IPv4 Address」または「IPv6 Address」をチェック後、「MAC Address」および「Ports」にバインドする IP アドレス、MAC アドレスおよびポートを入力します。
- 「Apply」ボタンをクリックします。

エントリの編集

- 編集するエントリの「Edit」ボタンをクリックし、以下の画面を表示します。

図 12-29 IMPB Entry Settings 画面 - Edit

- 項目を編集し、エントリの「Apply」ボタンをクリックします。

エントリの検索

検索する項目を入力し、「Find」ボタンをクリックします。

すべてのエントリの表示

「View All」ボタンをクリックします。

エントリの削除

エントリの「Delete」ボタンをクリックします。すべてのエントリを削除する場合は、「Delete All」ボタンをクリックします。

MAC Block List (MAC ブロックリスト)

IP-MAC バインディング機能によりブロックされた未承認のデバイスを参照します。

Security > IP-MAC-Port Binding (IMPB) > MAC Block List の順にメニューをクリックして、以下の画面を表示します。

図 12-30 MAC Block List 画面

以下の項目を使用して、設定または編集を行います。

| 項目 | 説明 |
|-------------|--------------------------------|
| VLAN Name | 検出または削除する VLAN の VLAN 名を入力します。 |
| MAC Address | 検出または削除する MAC アドレスを入力します。 |

VIP-MAC バインディング機能によりブロックされた未承認デバイスの検索

「VLAN ID」と「MAC Address」を入力し、「Find」ボタンをクリックします。

エントリの削除

対象のエントリの行の「Delete」ボタンをクリックします。テーブル内のすべてのエントリを削除するためには、「Delete All」ボタンをクリックします。

エントリの表示

すべてのエントリを表示するためには、「View All」ボタンをクリックします。

DHCP Snooping (DHCP Snooping 設定)

DHCP Snooping Maximum Entry Settings (DHCP Snooping 最大エントリ設定)

DHCP Snooping の最大エントリをポートに設定します。

Security > IP-MAC-Port Binding (IMPB) > DHCP Snooping > DHCP Snooping Maximum Entries の順にクリックして、以下の画面を表示します。

図 12-31 DHCP Snooping Maximum Entry Settings 画面

以下の項目を使用して、設定または編集を行います。

| 項目 | 説明 |
|---------------------------|---|
| Unit | 設定するユニットを選択します。 |
| From Port / To Port | 使用するポート範囲を選択します。 |
| Maximum Entry (1-50) | 最大エントリ数を入力します。「No limit」をチェックすると学習するエントリの最大数に制限がなくなります。 |
| Maximum IPv6 Entry (1-50) | IPv6 DHCP Snooping の最大エントリ数を入力します。「No limit」をチェックすると学習するエントリの最大数に制限がなくなります。 |

「Apply」ボタンをクリックして行った変更を適用します。

DHCP Snooping Entry (DHCP Snooping エントリ)

特定ポートのダイナミックエントリを表示します。

Security > IP-MAC-Port Binding (IMPB) > DHCP Snooping > DHCP Snooping Entry の順にクリックして、以下の画面を表示します。

図 12-32 DHCP Snooping Entry 画面

以下の項目を使用して、設定または編集を行います。

| 項目 | 説明 |
|-------|---|
| Unit | 設定するユニットを選択します。 |
| Port | プルダウンメニューで希望するポートを選択します。 |
| Ports | DHCP Snooping エントリを表示するポートを指定します。 <ul style="list-style-type: none"> All Port - すべてのポートの全エントリを選択します。 IPv4 - IPv4 DHCP Snooping が学習したエントリを選択します。 IPv6 - IPv6 DHCP Snooping が学習したエントリを選択します。 |

特定ポートの設定の表示

ポート番号を入力して「Find」ボタンをクリックします。

すべてのエントリの表示

「View All」ボタンをクリックします。

エントリの削除

「Clear」ボタンをクリックします。

ND Snooping (ND Snooping 設定)

ND Snooping Maximum Entry Settings (ND Snooping 最大エントリ設定)

ND Snooping の最大エントリをポートに設定します。

Security > IP-MAC-Port Binding (IMPB) > ND Snooping > ND Snooping Maximum Entry Settings の順にメニューをクリックし、以下の画面を表示します。

図 12-33 ND Snooping Maximum Entry Setting 画面

以下の項目を使用して、設定または編集を行います。

| 項目 | 説明 |
|----------------------|---|
| Unit | 設定するユニットを選択します。 |
| From Port / To Port | プルダウンメニューを使用して、ND Snooping を使用して学習可能な最大エントリ数の制限を必要とするポート範囲を指定します。 |
| Maximum Entry (1-50) | 最大エントリ数を入力します。「No limit」をチェックすると学習するエントリの最大数に制限がなくなります。 |

「Apply」ボタンをクリックして行った変更を適用します。

ND Snooping Entry (ND Snooping エントリ)

指定ポートのダイナミックエントリを表示します。

Security > IP-MAC-Port Binding (IMPB) > ND Snooping > ND Snooping Entry の順にメニューをクリックし、以下の画面を表示します。

図 12-34 ND Snooping Entry 画面

以下の項目を使用して、設定または編集を行います。

| 項目 | 説明 |
|-------|--|
| Unit | 設定するユニットを選択します。 |
| Port | プルダウンメニューで希望するポートを選択します。 |
| Ports | ND Snooping エントリのポートを指定します。「All Port」を選択すると、すべてのポートの全エントリを選択します。 |

「Find」ボタンをクリックして、選択したポート番号に基づいて指定エントリを検出します。

「Clear」ボタンをクリックして、本欄に入力したすべてのエントリをクリアします。

「View All」ボタンをクリックして、すべての定義済みエントリを表示します。

MAC-based Access Control (MAC ベースアクセスコントロール)

MAC ベースアクセスコントロールは、ポートまたはホストを使用してアクセスを認証および認可する方式です。本方式では、ポートベースの MAC にはポートアクセス権を決定し、一方ホストベースの MAC には MAC アクセス権を決定します。ネットワークへのアクセスを許可する前に MAC ユーザが認証される必要があります。

本スイッチは、ローカル認証とリモート RADIUS サーバ認証の両方の方法をサポートしています。MAC ベースアクセスコントロールでは、ローカルデータベースまたは RADIUS サーバデータベース内の MAC ユーザ情報が認証のために検索されます。認証結果に基づいて、ユーザは異なるレベルの許可を取得します。

MAC ベースアクセスコントロールに関する注意

MAC ベースアクセスコントロールに関するいくつかの制限と規則があります。

1. 本機能がポートで有効になると、スイッチはそのポートの FDB をクリアします。
2. ポートが、ゲスト VLAN ではない VLAN で MAC アドレスをクリアする権利を認められている場合、そのポート上の他の MAC アドレスは、アクセスのために認証されている必要があり、そうでない場合、スイッチにブロックされます。
3. リンクアグリゲーション、およびポートセキュリティが有効なポートは、MAC ベースアクセスコントロールを有効にすることはできません。
4. GVRP 認証が有効なポートをゲスト VLAN で有効にすることはできません。

MAC-based Access Control Settings (MAC ベースアクセスコントロール設定)

スイッチの MAC ベースアクセスコントロール機能にパラメータを設定します。動作状態、認証方式、RADIUS パスワードの設定、およびスイッチの MAC ベースアクセスコントロール機能に関連するゲスト VLAN 設定の参照を行います。また、ポートの MAC ベースアクセスコントロール機能を有効または無効にします。以前に記述した他の機能で有効とされているポートは、MAC ベースアクセスコントロールを使用できないことにご注意ください。

Security > MAC-based Access Control (MAC) > MAC-based Access Control Settings の順にメニューをクリックし、以下の画面を表示します。

図 12-35 MAC-based Access Control Settings 画面

以下の項目を参照、または設定可能です。

| 項目 | 説明 |
|--|---|
| MAC-based Access Control Global Settings | |
| MAC-based access control State | 「Enabled」(有効)または「Disabled」(無効)を選択し、スイッチの MAC ベースアクセスコントロールをグローバルに設定します。 |

| 項目 | 説明 |
|----------------------|--|
| Method | 認証 MAC アドレスがポートにある場合、認証タイプをプルダウンメニューで選択します。認証タイプは以下の通りです。 <ul style="list-style-type: none"> Local - MAC ベースアクセスコントロールのオーセンティケータとしてローカルに設定された MAC アドレスデータベースを利用します。この MAC アドレスリストは、「MAC-Based Access Control Local Database Settings」画面で設定します。 RADIUS - MAC ベースアクセスコントロールのオーセンティケータとしてリモート RADIUS サーバを利用します。MAC リストははじめに RADIUS サーバに設定されている必要があり、サーバの設定もスイッチに設定されている必要があることにご注意ください。 |
| RADIUS Authorization | RADIUS 認証を有効または無効にします。 |
| Local Authorization | ローカル認証を有効または無効にします。 |
| Log State | プルダウンメニューを使用して、ログの状態を「Enabled」(有効)/「Disabled」(無効)にします。 |
| Password Type | プルダウンメニューを使用してパスワードタイプを選択します。利用可能なオプションは「Manual String」および「Client MAC Address」です。 |
| Password | 認証リクエストのパケットを送信するために使用する RADIUS サーバのパスワードを入力します。初期値は「default」です。 |
| Trap State | プルダウンメニューから MAC ベースアクセスコントロール用のトラップの送信を「Enabled」(有効)または「Disabled」(無効)にします。 |
| Max User (1-4000) | スイッチの最大ユーザ数を指定します。「No Limit」を選択すると、ユーザの最大数の設定を行いません。 |
| Guest VLAN Settings | |
| VLAN Name | 本機能に使用される設定済みのゲスト VLAN 名を入力します。 |
| VID | 先頭のラジオボタンをクリックしてゲスト VLAN ID を入力します。 |
| Member Ports | ゲスト VLAN に設定するポートリストを入力します。 |
| Port Settings | |
| Unit | 設定するユニットを選択します。 |
| From Port / To Port | プルダウンメニューを使用して MAC ベースアクセスコントロールに設定するポート範囲を指定します。 |
| State | 本画面の「Port Settings」セクションで選択したポートまたはポート範囲の MAC ベースアクセスコントロール有効または無効にします。 |
| Aging Time (1-1440) | 1-1440(分)の範囲で指定します。初期値は 1440 です。エージングタイムを無効にするためには、「Infinite」オプションを選択します。 |
| Block Time (0-300) | 1-300(秒)の範囲で指定します。初期値は 300 です。 |
| Max User (1-4000) | 本設定に使用する最大ユーザ数を指定します。「No Limit」を選択すると、本ルールにユーザの制限はなくなります。 |

「Apply」ボタンをクリックして各セクションで行った変更を適用します。

「Delete」ボタンをクリックして、入力した情報に基づいて指定エントリを削除します。

MAC-based Access Control Local Settings (MAC ベースアクセスコントロール ローカル設定)

スイッチに対して認証されるターゲット VLAN と MAC アドレスリストを設定します。MAC アドレスのクエリが本テーブルに一致すると、MAC アドレスは、関連する VLAN に置かれます。スイッチ管理者は、ここで設定された local 方式を使用して、認証する最大 1024 個の MAC アドレスを入力することができます。

Security > MAC-based Access Control (MAC) > MAC-based Access Control Local Settings をクリックし、以下の画面を表示します。

図 12-36 MAC-based Access Control Local Settings 画面

以下の項目を使用して、設定または編集を行います。

| 項目 | 説明 |
|--------------|--------------------------------|
| MAC Address | ローカル認証リストに追加する MAC アドレスを入力します。 |
| VLAN Name | MAC アドレスに対応する VLAN 名を入力します。 |
| VID (1-4094) | MAC アドレスに対応する VLAN ID を入力します。 |

MAC アドレスリストへの新規登録

MAC アドレスをローカル認証リストに追加するためには、「MAC Address」と「VLAN Name」/「VID」に MAC アドレスとターゲット VLAN 名 / VLAN ID をそれぞれ入力し、「Add」ボタンをクリックします。

MAC アドレスリストの検出

「Find by MAC」ボタンをクリックして、入力した MAC アドレスに基づく特定のエントリを検出します。また、「Find by VLAN」ボタンをクリックして、入力した VLAN 名または VLAN ID に基づく特定のエントリを検出します。

MAC アドレスリストの参照

「View All」ボタンをクリックして、すべての定義済みエントリを表示します。

MAC アドレスエントリの削除

「Delete by MAC」ボタンをクリックして、入力した MAC アドレスに基づいて指定エントリを削除します。または、「Delete by VLAN」ボタンをクリックして、入力した VLAN 名または VLAN ID に基づいて指定エントリを削除します。

MAC アドレスリストの変更

選択した MAC アドレスの VLAN 名を変更するためには、「Edit by Name」ボタンをクリックし、以下の画面を表示します。

図 12-37 Edit by VLAN Name 画面

選択した MAC アドレスの VID 変更するためには、「Edit by ID」ボタンをクリックします。

図 12-38 Edit by VID 画面

複数ページが存在する場合は、ページ番号を入力後、「Go」ボタンをクリックして、特定のページへ移動します。

MAC-based Access Control Authentication State (MAC ベースアクセスコントロールの認証状態)

MAC ベースアクセスコントロールの認証情報を表示します。

Security > MAC-based Access Control (MAC) > MAC-based Access Control Authentication State をクリックし、以下の画面を表示します。

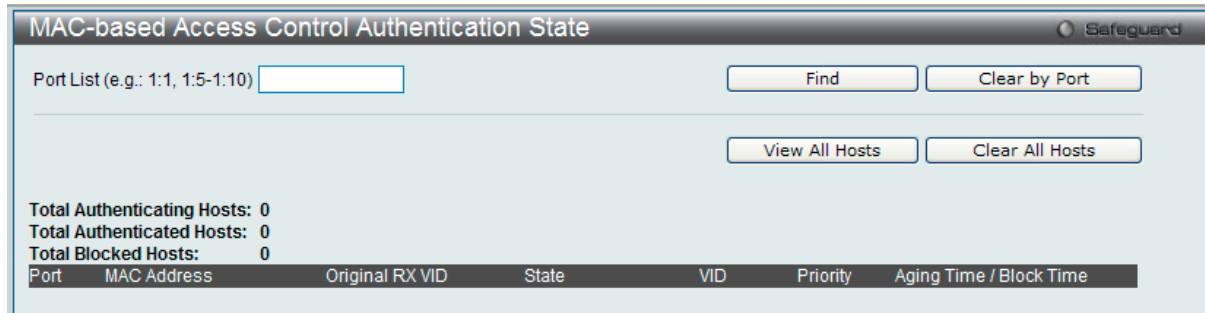


図 12-39 MAC-based Access Control Authentication State

以下の項目を使用して、設定または編集を行います。

| 項目 | 説明 |
|-----------|-----------------------|
| Port List | 本設定に使用するポートリストを指定します。 |

MAC ベースアクセスコントロールの認証状態の情報を表示するためには、ポート番号を入力し、「Find」ボタンをクリックします。

「Clear by Port」ボタンをクリックして、入力したポートにリンクするすべての情報をクリアします。

「View All Hosts」ボタンをクリックして、すべての定義済みホストを表示します。

「Clear All Hosts」ボタンをクリックして、すべての定義済みホストをクリアします。

Web-based Access Control (WAC) (Web ベースのアクセス制御)

Web ベース認証のログインは、スイッチを経由してインターネットにアクセスを試みる場合に、ユーザを認証するように設計された機能です。認証処理には HTTP または HTTPS プロトコルを使用します。Web ブラウザ経由で Web ページ (例: <http://www.dlink.com>) の閲覧を行う場合に、スイッチは認証段階に進みます。スイッチは、HTTP または HTTPS パケットを検出し、このポートが未認証である場合に、ユーザ名とパスワードの画面を表示して、ユーザに問い合わせます。認証処理を通過するまで、ユーザはインターネットにアクセスすることはできません。

スイッチは、認証サーバとなってローカルデータベースに基づく認証を行うか、または RADIUS クライアントとなってリモート RADIUS サーバと共に RADIUS プロトコルを介する認証処理を実行します。Web へのアクセスを試みることによって、クライアントユーザは WAC の認証処理を開始します。

D-Link の WAC の実行には、WAC 機能が排他的に使用し、スイッチの他のモジュールに知られていない仮想 IP を使用します。実際は、スイッチの他の機能への影響を避ける場合にだけ、WAC は仮想 IP アドレスを使用してホストとの通信を行います。そのため、すべての認証要求を仮想 IP アドレスに送信し、スイッチの物理インタフェースの IP アドレスには送信しないようする必要があります。

ホスト PC が仮想 IP 経由で WAC スイッチと通信する場合、仮想 IP は、スイッチの物理的な IPIF (IP インタフェース) アドレスに変換されて通信を可能にします。ホスト PC と他のサーバの IP 構成は WAC の仮想 IP に依存しません。仮想 IP は、ICMP パケットまたは ARP リクエストに応答しません。つまり、仮想 IP は、スイッチの IPIF (IP インタフェース) と同じサブネット、またはホスト PC のサブネットと同じサブネットには設定することはできません。

認証済みおよび認証中のホストから仮想 IP に送信されるすべてのパケットがスイッチの CPU にトラップされるため、仮想 IP が他のサーバまたは PC と同じであると、WAC が有効なポートに接続するホストは、IP アドレスを実際に所有しているサーバまたは PC とは通信できません。ホストがサーバまたは PC にアクセスする必要がある場合、仮想 IP をサーバまたは PC の 1 つと同じにすることはできません。ホスト PC がプロキシを使用して Web にアクセスする場合、PC のユーザは、認証を適切に実行するために、プロキシ設定の例外として仮想 IP を加える必要があります。仮想 IP を指定するかどうかに関わらず、ユーザはスイッチのシステム IP を経由して WAC ページにアクセスします。仮想 IP を指定しない場合、認証中の Web のリクエストは、スイッチのシステム IP にリダイレクトされます。

スイッチの WAC の実行は、ユーザ定義のポート番号により HTTP または HTTPS プロトコルのいずれかに対して TCP ポートを設定できることを特徴としています。HTTP か HTTPS に対するこの TCP ポートは、認証処理のために CPU にトラップされる HTTP か HTTPS パケットを識別するためやログインページにアクセスするために使用されます。指定しない場合、HTTP に対するポート番号の初期値は 80、HTTPS に対するポート番号の初期値は 443 となります。プロトコルも指定されないと、プロトコルの初期値は HTTP になります。

以下の図は、Web 認証処理を成功させるために通過する基本的な 6 段階を示しています。

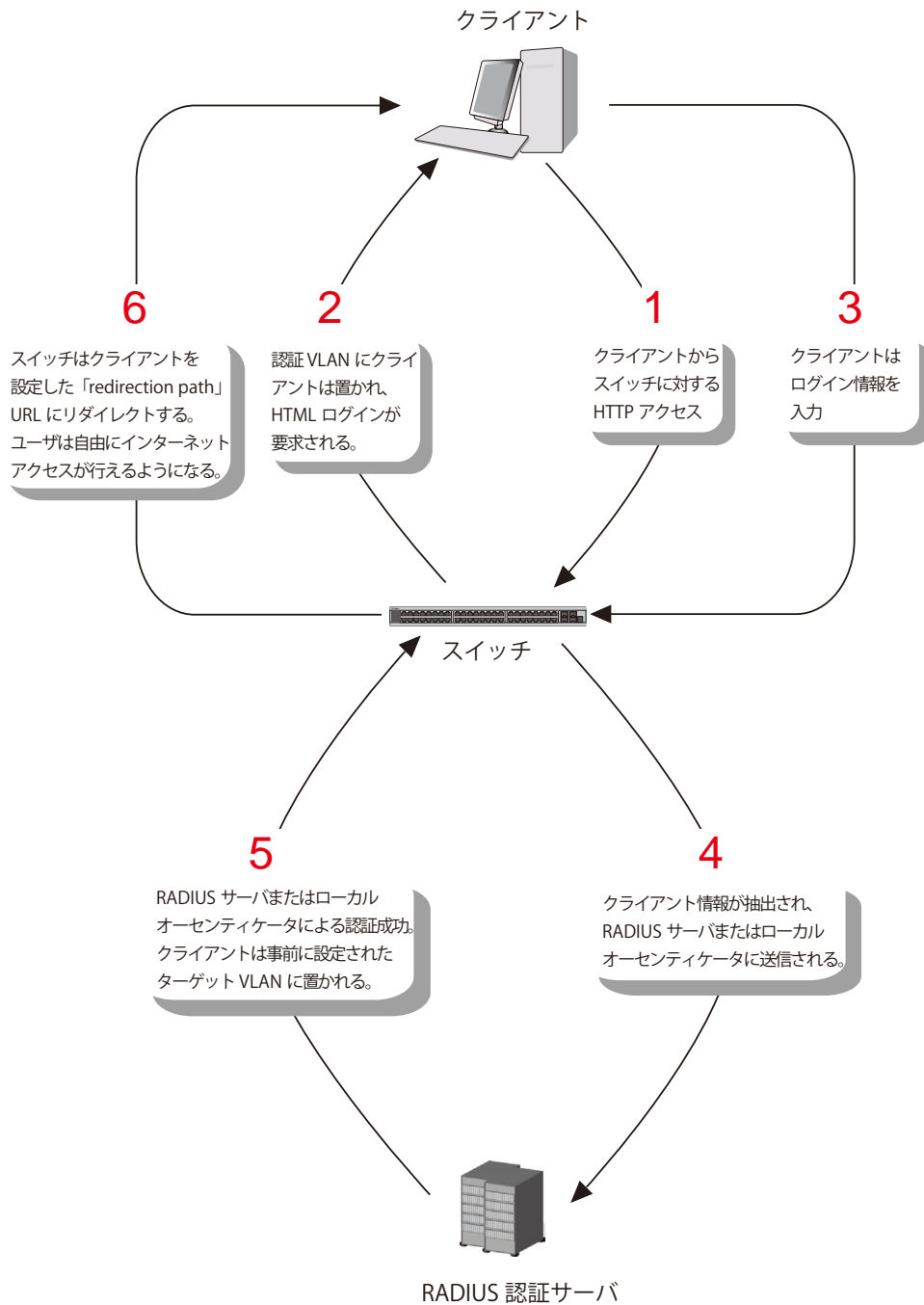


図 12-40 Web 認証プロセス画面

条件および制限

Web ベースアクセスコントロールにはいくつかの制限と規則があります。

1. クライアントが IP アドレス取得のために DHCP を使用している場合、認証 VLAN はクライアントが IP アドレス取得を行えるように、DHCP サーバまたは DHCP リレー機能を持つ必要があります。
2. アクセスプロファイル機能のように、スイッチ上に存在する機能の中には HTTP パケットをフィルタしてしまうものがあります。ターゲット VLAN にフィルタ機能の設定を行う際には、HTTP パケットがスイッチにより拒否されないように、十分に注意してください。
3. 認証に RADIUS サーバを使用する場合、Web 認証を有効にする前に、ターゲット VLAN を含む必要なパラメータを入力して RADIUS サーバの設定を行います。

注意 WAC/JWAC 認証では、System インタフェースがアップ状態である必要があります。

WAC Global Settings (WAC グローバル設定)

MAC ベースアクセスコントロール機能をスイッチに設定します。

Security > Web-based Access Control (WAC) > WAC Global Settings をクリックし、以下の画面を表示します。

図 12-41 WAC Global Settings 画面

以下の項目を使用して、設定を行います。

| 項目 | 説明 |
|------------------------|---|
| WAC Global Settings | |
| WAC Global State | Web 認証機能を「Enable」(有効) / 「Disable」(無効) にします。 |
| WAC Settings | |
| Virtual IP | 仮想 IP アドレスを入力します。このアドレスは WAC にだけ使用され、スイッチの他のモジュールには知られません。 |
| Virtual IPv6 | 仮想 IPv6 アドレスを入力します。このアドレスは WAC にだけ使用され、スイッチの他のモジュールには知られません。 |
| Redirection Path | 認証に成功し、ターゲット VLAN に割り当てられたユーザを導く Web サイトの URL を入力します。 |
| Clear Redirection Path | リダイレクションパスのクリアを有効または無効にします。 |
| RADIUS Authorization | RADIUS 認証を有効または無効にします。 |
| Local Authorization | ローカル認証を有効または無効にします。 |
| Method | Web ベースアクセスコントロールのオーセンティケータを選択します。 <ul style="list-style-type: none"> Local - スイッチを経由してネットワークにアクセスを行うユーザの認証方法として、スイッチでのローカル認証を行う場合に指定します。後に示す「WAC User Settings」画面 (Security > Web-based Access Control (WAC) > WAC User Settings) を使用して設定する、スイッチへのアクセス用のユーザ名とパスワードがローカルで参照するデータベースとなります。 RADIUS - スイッチを経由してネットワークにアクセスを行うユーザの認証方法として、リモート RADIUS サーバを使用する場合に指定します。管理者は、この RADIUS サーバを「Authentication RADIUS Server Settings」画面 (Security > RADIUS > Authentication RADIUS Server Settings) を使用して、事前に設定しておく必要があります。 |
| HTTP(S) Port (1-65535) | HTTP ポート番号を入力します。ポートの初期値は 80 です。 <ul style="list-style-type: none"> HTTP - TCP ポートが WAC HTTP プロトコルを実行します。初期値は 80 です。HTTP ポートは TCP ポート 443 で動作しません。 HTTPS - TCP ポートは WAC HTTPS プロトコルを実行します。初期値は 443 です。HTTPS は TCP ポート 80 で動作しません。 |

「Apply」 ボタンをクリックし、設定を有効にします。

注意

認証に成功すると、クライアントは事前に設定したサイトへ誘導されます。このサイトが開かなくても「Fail」メッセージが表示されない場合は、そのクライアントは既に認証されています。その場合はブラウザの画面を更新するか、他の Web サイトへ接続してみてください。

WAC User Settings (WAC ユーザ設定)

Web 認証用ローカルデータベースのユーザアカウントの参照および設定を行います。

Security > Web-based Access Control (WAC) > WAC User Settings をクリックし、以下の設定用画面を表示します。

WAC User Settings Safeguard

Create User

User Name VLAN Name VID (1-4094) Password Confirm Password

Note: WAC User and Password should be less than 16 characters.

Total Entries: 1

| User Name | VLAN Name | VID | Old Password | New Password | Confirm Password |
|-----------|-----------|-----|--------------|--------------|------------------|
| user1 | default | 1 | ***** | | |

図 12-42 User Account Settings 画面

以下の項目を使用して、設定を行います。

| 項目 | 説明 |
|------------------|---|
| User Name | 本プロセスを通して Web にアクセスを希望するユーザのユーザ名を 15 文字までの半角英数字で指定します。本項目は、オーセンティケータに「Local」を指定した場合、入力が必要です。 |
| VLAN Name | 先頭のラジオボタンをクリックして VLAN 名を入力します。 |
| VID (1-4094) | 先頭のラジオボタンをクリックして VLAN ID を入力します。 |
| Password | 上記ユーザ用に管理者が指定するパスワードを半角英数字で指定します。大文字、小文字は区別されます。本欄は、Web ベースのオーセンティケータに「Local」を選択した場合に管理者が使用します。 |
| Confirm Password | 確認のために再度同じパスワードを入力します。 |

「Apply」ボタンをクリックして行った変更を適用します。

VLAN 名の編集

1. 編集するエントリの「Edit VLAN Name」ボタンをクリックして、以下の画面を表示します。

WAC User Settings Safeguard

Create User

User Name VLAN Name VID (1-4094) Password Confirm Password

Note: WAC User and Password should be less than 16 characters.

Total Entries: 1

| User Name | VLAN Name | VID | Old Password | New Password | Confirm Password |
|-----------|-----------|-----|--------------|--------------|------------------|
| user1 | default | 1 | | | |

図 12-43 User Account Settings 画面 - Edit VLAN Name

2. VLAN 名を編集して「Apply」ボタンをクリックします。

VLAN ID の編集

1. 編集するエントリの「Edit VID」ボタンをクリックして、以下の画面を表示します。

図 12-44 User Account Settings 画面 - Edit VID

2. VLAN ID を編集して「Apply」ボタンをクリックします。

エントリの削除

「Clear VLAN」ボタンをクリックして、指定エントリから VLAN 情報を削除します。

「Delete」ボタンをクリックして、指定エントリを削除します。「Delete All」ボタンをクリックして、表示されたすべてのエントリを削除します。

注意 WAC ユーザ名とパスワードは 16 文字以内とします。

WAC Port Settings (WAC ポート設定)

Web 認証のためポート設定の表示またはポート設定を行います。

Security > Web-based Access Control (WAC) > WAC Port Settings をクリックし、以下の設定用画面を表示します。

図 12-45 WAC Port Settings 画面

以下の項目を使用して、設定を行います。

| 項目 | 説明 |
|---------------------|--|
| Unit | 設定するユニット番号を選択します。 |
| From Port / To Port | プルダウンメニューを使用して WAC ポートとして有効にするポート範囲を指定します。 |
| Aging Time (1-1440) | 認証ホストが認証状態を保つ時間を指定します。0-1440(分)の範囲で指定します。0 は、認証ホストがポート上でエージングしないことを示しています。初期値は 1440 分(24 時間)です。 |
| State | プルダウンメニューを使用して WAC ポートとして設定するポートを有効にします。 |
| Idle Time (1-1440) | 本設定時間にトラフィックがない場合、ホストは未認証状態に戻ります。0-1440(分)の範囲で指定します。0 を指定すると、ポート上の認証ホストのアイドル状態がチェックされません。初期値は「infinite」です。 |
| Block Time (0-300) | 認証に失敗した後にホストがブロック状態を維持する期間を指定します。1-300(秒)の範囲で指定します。初期値は 60(秒)です。 |

「Apply」ボタンをクリックして行った変更を適用します。

WAC Authentication State (WAC 認証状態)

Web 認証用のホストの表示および削除を行います。

Security > Web-based Access Control (WAC) > WAC Authentication Settings をクリックし、以下の設定用画面を表示します。

図 12-46 WAC Authentication State 画面

以下の項目を使用して、設定を行います。

| 項目 | 説明 |
|----------------|--|
| Port List | ポート範囲を選択し、適切なチェックボックス（「Authenticated」（認証済み）、「Authenticating」（認証中）、および「Blocked」（破棄））を選択します。 |
| Authenticated | ポートに対して認証済みユーザのすべてをクリアします。 |
| Authenticating | ポートに対して認証中ユーザのすべてをクリアします。 |
| Blocked | ポートに対してブロックされたユーザすべてをクリアします。 |

「Find」 ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

「Clear by Port」 ボタンをクリックして、入力したポートリストに基づくエントリを削除します。

「View All Hosts」 ボタンをクリックして、すべての定義済みホストを表示します。

「Clear All Hosts」 ボタンをクリックして、表示されたすべてのエントリを削除します。

WAC Customize Page (WAC カスタマイズページ設定)

認証ページの項目をカスタマイズします。

Security > Web-based Access Control (WAC) > WAC Customize Page の順にメニューをクリックし、以下の画面を表示します。

図 12-47 WAC Customize Page 画面

WAC ページの設定を行うためにはこの画面の WAC 認証情報をすべて入力して「Apply」 ボタンをクリックして行った変更を適用します。

「Set to default」 ボタンをクリックして、全項目を初期設定に復元します。

「Edit」 ボタンをクリックして、項目を編集します。

Japanese Web-based Access Control (JWAC : JWAC 設定)

JWAC Global Settings (JWAC グローバル設定)

スイッチにおける JWAC (Japanese Web-based Access Control) の有効化および設定をします。

JWAC と Web 認証が相互に排他的な機能であり、それらを同時に使用することができませんのでご注意ください。JWAC 機能を使用するためには、PC ユーザは、2 段階の認証を通過する必要があります。最初のステップは、検疫サーバで検疫を行い、2 番目のステップでユーザ認証が行われます。2 番目のステップは、ホストが認証を通過した後にポートの VLAN メンバシップ変更がないという点を除き、Web 認証に似ています。RADIUS サーバは、802.1X コマンドセットによって定義されたサーバ設定を共有します。

注意 JWAC/JWAC 認証では、System インタフェースがアップ状態である必要があります。

Security > Japanese Web-based Access Control (JWAC) > JWAC Global Settings の順にメニューをクリックし、以下の画面を表示します。

図 12-48 JWAC Global Settings 画面

以下の項目を設定可能です。

| 項目 | 説明 |
|-------------------------|---|
| JWAC Global Settings | |
| JWAC State | JWAC 機能を「Enabled」(有効) / 「Disabled」(無効) にします。設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。 |
| JWAC Settings | |
| Virtual IPv4 | 未認証ホストからの認証リクエストを受け入れるために使用する JWAC 仮想 IP アドレスを入力します。これは未認証ホストから認証リクエストを受け入れるために使用する JWAC の仮想 IP アドレスです。この IP に送信されたリクエストだけが正しい応答を取得します。 注意 この IP は、ARP リクエストまたは ICMP パケットには応答しません。 |
| IPv4 Virtual URL | 使用する仮想 URL を入力します。 |
| UDP Filtering | JWAC UDP フィルタリングを「Enabled」(有効) / 「Disabled」(無効) にします。本項目を「Enabled」にすると、DHCP と DNS を除く未認証ホストからの UDP と ICMP パケットは破棄されます。 JWAC 認証中の ping パケットが通過する時間は 0 から 30 です。 |
| Port Number (1-65535) | JWAC スイッチがリッスンし、認証プロセスを終了するために使用する TCP ポートを指定します。 |
| Forcible Logout | JWAC Forcible Logout を「Enabled」(有効) / 「Disabled」(無効) にします。「Enabled」の場合、認証ホストから JWAC スイッチに TTL=1 を持つ ping パケットはログアウトリクエストと見なされ、ホストは未認証状態に戻ります。 |
| Authentication Protocol | JWAC に使用される RADIUS プロトコルを指定し、RADIUS 認証を完了します。オプションには Local、EAP MD5、PAP、CHAP、MS CHAP、および MS CHAPv2 があります。 |
| Redirected State | JWAC リダイレクト機能を「Enabled」(有効) / 「Disabled」(無効) にします。リダイレクト検疫サーバが「Enabled」な場合、ランダムな URL にアクセスしようとする、未認証ホストは検疫サーバにリダイレクトされます。リダイレクト先に JWAC Login Page を指定した場合、未認証ホストは、スイッチの JWAC Login Page にリダイレクトされ、Web 認証画面に移行します。リダイレクトが無効な場合、未認証ユーザは検疫サーバへのアクセスと未認証ホストからの JWAC Login Page だけが許可され、他のすべての Web アクセスは拒否されます。 注意 Quarantine Server (検疫サーバ) へのリダイレクトを有効にする場合、はじめに検疫サーバを設定する必要があります。 |
| Redirect Destination | 未認証ホストが Quarantine Server または JWAC Login Page にリダイレクトされる前にリダイレクトされる宛先を指定します。 |

| 項目 | 説明 |
|----------------------------|---|
| Redirect Delay Time (0-10) | 未認証ホストが Quarantine Server または JWAC Login Page にリダイレクトされる場合の遅延時間 0-10 (秒) を指定します。0 はリダイレクトの遅延がないことを示します。 |
| RADIUS Authorization | RADIUS 認証を有効または無効にします。 |
| Local Authorization | ローカル認証を有効または無効にします。 |
| Quarantine Server Settings | |
| Error Timeout (5-300) | Quarantine Server のエラータイムアウトを設定します。Quarantine Server モニタが有効な場合、JWAC スイッチは、定期的に検疫が問題なく動作するかどうかをチェックします。スイッチが設定された時間に Quarantine Server から応答を受信しないと、スイッチは適切に動作していないと見なします。5-300 (秒) で指定します。 |
| Monitor | JWAC Quarantine Server モニタを「Enabled」(有効) / 「Disabled」(無効) にします。Quarantine Server モニタが有効な場合、JWAC スイッチは、定期的に検疫が問題なく動作するかどうかをチェックします。Quarantine Server を検出できない場合、リダイレクト Quarantine Server を有効にし、リダイレクトする先を Quarantine Server として設定することによりすべての未認証 HTTP リクエストを JWAC Login Page にリダイレクトします。 |
| URL | JWAC Quarantine Server の URL を指定します。リダイレクトが有効で、リダイレクトの宛先が Quarantine Server であると、未認証ホストが HTTP リクエストパケットをランダムな Web サーバに送信する場合、スイッチは、この HTTP パケットを処理し、設定された URL を持つ Quarantine Server へのアクセスを許可するためにホストにメッセージを送り返します。コンピュータが指定 URL に接続している場合、Quarantine Server は、PC ユーザにユーザ名とパスワードの入力を要求し、認証処理を終了します。 |
| Update Server Settings | |
| Update Server IP | 更新用サーバの IP アドレスを指定します。 |
| Mask | サーバ IP アドレスのネットマスクを指定します。 |
| Port | 更新サーバが使用するポート番号を選択します。 |

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

JWAC Port Settings (JWAC ポート設定)

スイッチに JWAC ポート設定を行います。

Security > Japanese Web-based Access Control (JWAC) > JWAC Port Settings の順にメニューをクリックし、以下の画面を表示します。

| Port | State | Aging Time | Idle Time | Block Time | Max Host |
|------|----------|------------|-----------|------------|----------|
| 1 | Disabled | 1440 | Infinite | 60 | 100 |
| 2 | Disabled | 1440 | Infinite | 60 | 100 |
| 3 | Disabled | 1440 | Infinite | 60 | 100 |
| 4 | Disabled | 1440 | Infinite | 60 | 100 |
| 5 | Disabled | 1440 | Infinite | 60 | 100 |

図 12-49 JWAC Port Settings 画面

スイッチの各ポートに JWAC を設定するためには、以下の項目を設定します。

| 項目 | 説明 |
|---------------------------------|---|
| Unit | 設定するユニットを選択します。 |
| From Port / To Port | JWAC ポートとして有効になるポート範囲を選択します。 |
| State | プルダウンメニューを使用して JWAC ポートとして設定するポートを有効にします。 |
| Max Authenticating Host (0-100) | 同時に各ポートに許可される認証処理を試みるホストの最大数を指定します。初期値は 100 です。 |
| Aging Time (1-1440) | 認証ホストが認証状態を保つ時間を指定します。「Infinite」をチェックすると、認証ホストはポートにエージングを行いません。初期値は 1440 です。 |
| Block Time (0-300) | 認証を通過することに失敗した場合にホストがブロックされる時間を指定します。0-300 (秒) で指定します。初期値は 60 です。 |
| Idle Time (1-1440) | 本設定時間にトラフィックがない場合、ホストは未認証状態に戻ります。値を変更するには「Infinite」のチェックを外して 0-1440 (分) で指定します。「Infinite」を指定すると、ポート上の認証ホストのアイドル状態をチェックしません。初期値は「infinite」です。0 を指定すると、ポート上の認証ホストのアイドル状態がチェックされません。 |
| Authentication Mode | 「Host-based」(ホストベース) または 「Port-based」(ポートベース) を指定します。 |

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

JWAC User Settings (JWAC ユーザ設定)

スイッチのローカルデータベースに JWAC ユーザを設定します。

Security > Japanese Web-based Access Control (JWAC) > JWAC User Settings をクリックし、以下の画面を表示します。

図 12-50 JWAC User Settings 画面

スイッチが JWAC にユーザアカウント設定をするためには、以下の項目を入力後、「Add」ボタンをクリックします。

以下の項目を設定します。

| 項目 | 説明 |
|----------------------|--|
| User Name | 半角英数字 15 文字以内でユーザ名を入力します。 |
| New Password | 管理者が選択ユーザのために設定するパスワードを英数字（大文字小文字の区別あり）で入力します。 |
| Confirm New Password | 上記で入力したパスワードを再度入力します。 |
| VID(1-4094) | VLAN ID 番号（1-4094）を入力します。 |

エントリの削除

削除するエントリの「Delete」ボタンをクリックします。画面下部に表示されている現在の JWAC ユーザ設定を削除するためには、「Delete All」ボタンをクリックします。

エントリの変更

1. 変更するエントリの「Edit」ボタンをクリックして以下の画面を表示します。

図 12-51 JWAC User Settings 画面 - Edit

2. エントリを編集して「Apply」ボタンをクリックします。

注意 ユーザ名とパスワードは 16 文字以内とします。

JWAC Authentication State (JWAC 認証状態)

スイッチにおける JWAC の認証情報を表示します。

Security > Japanese Web-based Access Control (JWAC) > JWAC Authentication State をクリックし、以下の画面を表示します。

図 12-52 JWAC Authentication State 画面

以下の項目を設定します。

| 項目 | 説明 |
|----------------|--|
| Port List | ポートまたはポート範囲を指定します。 |
| Authenticated | 本ボックスをクリックして、認証されたクライアントホストだけをクリアします。 |
| Authenticating | 本ボックスをクリックして、認証中のクライアントホストだけをクリアします。 |
| Blocked | 本ボックスをクリックして、認証エラーのために一時的にブロックされたクライアントホストだけをクリアします。 |

「Find」 ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

「Clear」 ボタンをクリックして、入力したポートリストに基づくエントリを削除します。

「View All Hosts」 ボタンをクリックして、すべての定義済みホストを表示します。

「Clear All Hosts」 ボタンをクリックして、表示されたすべてのエントリを削除します。

JWAC Customize Page Language (JWAC 画面言語のカスタマイズ)

JWAC 画面言語の設定を行います。現在のファームウェアは英語および日本語をサポートしています。

Security > Japanese Web-based Access Control (JWAC) > JWAC Customize Page Language の順にメニューをクリックし、以下の画面を表示します。

図 12-53 JWAC Customize Page Language 画面

以下の項目を設定します。

| 項目 | 説明 |
|-------------------------|--|
| Customize Page Language | ラジオボタンを使用して「English」または「Japanese」を選択します。 |

JWAC 画面に使用する言語を設定するためには、「English」または「Japanese」のボタンをクリックし、「Apply」 ボタンをクリックして、変更を保存します。

JWAC Customize Page (JWAC 画面のカスタマイズ)

JWAC 画面の設定を行います。

Security > Japanese Web-based Access Control (JWAC) > JWAC Customize Page の順にメニューをクリックし、以下の画面を表示します。

English Japanese

Current Status: Un-Authenticated

Authentication Logi

User Name

Password

Enter Clear

Logout From The N

Logout

Notification

Set to default Apply

図 12-54 JWAC Customize Page 画面 (English)

English Japanese

認証状態:未認証

社内LAN認証ログイ

ユーザID

パスワード

Enter Clear

社内LAN認証ログア

Logout

Notification

Set to default Apply

図 12-55 JWAC Customize Page 画面 (Japanese)

JWAC 認証情報を入力して、JWAC 画面の設定を行います。最初の欄に認証名を入力し、「Apply」ボタンをクリックします。次にユーザ名とパスワードを入力し、「Enter」ボタンをクリックします。

Compound Authentication (コンパウンド認証)

新しいネットワークでは多くの認証方式を採用しています。

Compound Authentication Settings (コンパウンド認証設定)

スイッチポートに認可ネットワーク状態の設定およびコンパウンド認証方式の設定を行います。

Security > Compound Authentication > Compound Authentication Settings の順にメニューをクリックし、以下の画面を表示します。

| Port | Authentication Methods | Authorized Mode | Authentication VLAN |
|------|------------------------|-----------------|---------------------|
| 1 | None | Host-based | |
| 2 | None | Host-based | |
| 3 | None | Host-based | |
| 4 | None | Host-based | |
| 5 | None | Host-based | |
| 6 | None | Host-based | |

図 12-56 Compound Authentication Settings 画面

スイッチの各ポートにコンパウンド認証を設定するには、以下の項目を指定します。

| 項目 | 説明 |
|--------------------------------|---|
| Authorization Attributes State | 認可ネットワーク状態を有効または無効にします。 |
| Authentication Server Failover | 認証サーバのフェイルオーバー機能を設定します。 <ul style="list-style-type: none"> Local - スイッチは、クライアントを認証するためにローカルデータベースを使用します。クライアントがローカル認証に失敗すると、クライアントは認証に失敗したとみなされます。 Permit - クライアントは、認証なしで通信可能となります。ゲスト VLAN が有効であると、クライアントはゲスト VLAN にとどまり、そうでない場合、オリジナルの VLAN にとどまります。 Block - クライアントは認証されず、ブロックされます。(初期値) |
| Unit | 設定するユニットの番号を選択します。 |
| From Port / To Port | コンパウンド認証ポートとして設定するポート範囲を指定します。 |
| Authentication Methods | コンパウンド認証方式には以下のオプションがあります。 <ul style="list-style-type: none"> None - すべてのコンパウンド認証方式を無効にします。 Any (MAC, 802.1X, JWAC or WAC) - これらのうちいずれかの認証方式を通過すると接続を許可します。本モードでは、1つのポートに対し一度に MAC アドレス認証、802.1X、および WAC/JWAC 認証を有効にします。各セキュリティモジュールがポートに対して有効か否かはそのシステムの状態に依存します。WAC と JWAC のシステム状態は相互に排他的であるため、1つのポートに対して、どちらか1つだけが有効になります。 802.1X+IMPB - はじめに 802.1X 認証を行い、次に IP-MAC- ポートバインディング認証を行います。両方の認証方式を通過する必要があります。 IMPB+JWAC - はじめに IP-MAC- ポートバインディング認証を行い、次に JWAC 認証を行います。両方の認証方式を通過する必要があります。 IMPB+WAC - はじめに IP-MAC- ポートバインディング認証を行い、次に WAC 認証を行います。両方の認証方式を通過する必要があります。 MAC+IMPB - はじめに MAC 認証を行い、次に IP-MAC- ポートバインディング認証を行います。両方の認証方式を通過する必要があります。 |
| Authorized Mode | 「Host-based」または「Port-based」を選択します。 <ul style="list-style-type: none"> Port-based - 対応するホストの1つが認証を通過すると、同じポート上のホストはすべてネットワークへの接続が許可されます。認証に失敗するとこのポートは続いて次の認証方式を実行します。 Host-based - ユーザは個別に認証されます。 |
| VID List | VLAN ID リストを指定します。 |
| State | 認証 VLAN として特定の VID リストを割り当てまたは削除します。 |

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

注意 Compound 認証と DHCP スヌーピングは同じポートでは、動作できません。

Compound Authentication Guest VLAN Settings (コンパウンド認証ゲスト VLAN の設定)

ポートをゲスト VLAN に割り当て、または削除することができます。

Security > Compound Authentication > Compound Authentication Guest VLAN Settings の順にメニューをクリックし、以下の画面を表示します。

図 12-57 Compound Authentication Guest VLAN Settings 画面

以下の項目を使用して、ゲスト VLAN の設定をします。

| 項目 | 説明 |
|-------------------------|---|
| VLAN Name | VLAN をゲスト VLAN として割り当てます。必ず定義済みのスタティック VLAN を割り当てます。 |
| VID (1-4094) | VLAN ID をゲスト VLAN に割り当てます。この VLAN ID には、必ず定義済みのスタティック VLAN に割り当てます。 |
| Port List (e.g.: 1,6-9) | 設定するポート範囲を指定します。または、「All Ports」のチェックボタンをチェックしてすべてのポートを一度に設定します。 |
| Action | プルダウンメニューを使用して操作する機能を選択します。 <ul style="list-style-type: none"> • Create VLAN - VLAN を作成します。 • Add Ports - ポートを追加します。 • Delete Ports - ポートを削除します。 |

「Apply」ボタンをクリックし、ゲスト VLAN を実行します。正しく設定されるとゲスト VLAN 名と対象のポートが画面の下部に表示されます。

「Delete」ボタンをクリックして、指定エントリを削除します。

Compound Authentication MAC Format Settings (コンパウンド認証 MAC 形式設定)

RADIUS サーバ経由の認証ユーザ名に使用される MAC アドレス形式を設定します。

Security > Compound Authentication > Compound Authentication MAC Format Settings の順にメニューをクリックし、以下の画面を表示します。

Compound Authentication MAC Format Settings 画面

設定対象となる項目は以下の通りです。

| 項目 | 説明 |
|------------------|--|
| Case | RADIUS 認証ユーザ名の形式を選択します。 <ul style="list-style-type: none"> • Lowercase - RADIUS 認証名を「aa-bb-cc-dd-ee-ff」という小文字の形式を使用します。 • Uppercase - RADIUS 認証名を「AA-BB-CC-DD-EE-FF」という大文字の形式を使用します。 |
| Delimiter | プルダウンメニューを使用して区切り文字を選択します。 <ul style="list-style-type: none"> • Hyphen - 「-」を使用して、「AA-BB-CC-DD-EE-FF」という形式にします。 • Colon - 「:」を使用して、「AA:BB:CC:DD:EE:FF」という形式にします。 • Dot - 「.」を使用して、「AA.BB.CC.DD.EE.FF」という形式にします。 • None - 区切り文字を使用しないで、「AABBCCDDEEFF」という形式にします。 |
| Delimiter Number | プルダウンメニューを使用して区切り数字を選択します。 <ul style="list-style-type: none"> • 1 - 1 つの区切りを使用して、「AABBCC.DDEEFF」という形式にします。 • 2 - 2 つの区切りを使用して、「AABB.CCDD.EEFF」という形式にします。 • 5 - 複数の区切りを使用して、「AA.BB.CC.DD.EE.FF」という形式にします。 |

「Apply」ボタンをクリックして行った変更を適用します。

IGMP Access Control Settings (IGMP アクセスコントロール設定)

本製品の各ポートに IGMP 認証 (IGMP アクセスコントロール) を設定することができます。本製品の認証状態が有効で IGMP の join リクエストを受信すると、RADIUS サーバに接続リクエストを送信して認証を行います。

IGMP 認証では IGMP レポートを以下のように処理します。ホストが希望するマルチキャストグループに join メッセージを送信する場合、本製品は、そのマルチキャストグループ / ポートを学習する前に認証を行う必要があります。本製品は、Access-Request (認証リクエスト) とホストの MAC、スイッチポート番号、スイッチ IP、およびマルチキャストグループ IP を含む情報を認証サーバに送信します。認証サーバが Access-Accept (アクセス許可) を返した場合、本製品はマルチキャストグループ / ポートを学習します。認証サーバが Access-Reject (アクセス拒否) を返した場合は、本製品はマルチキャストグループ / ポートを学習せず、パケットの処理を行いません。エントリ (ホスト MAC、スイッチポート番号、およびマルチキャストグループ IP) は認証エラーリストに入ります。T1 タイム後に認証サーバから何の応答もない場合、本製品はサーバに Access-Request (認証リクエスト) を再送信します。本製品が N1 タイム後に何の応答も受信しない場合、認証結果は拒否であり、エントリ (ホスト MAC、スイッチポート番号、およびマルチキャストグループ IP) は認証エラーリストに入ります。一般的に、マルチキャストグループ / ポートが学習済みの場合、再度認証が行われることはなく当該のパケットは通常のものとして処理されます。

IGMP 認証では IGMP leave を以下のように処理します。ホストが指定のマルチキャストグループに leave メッセージを送信する場合、本製品はグループ離脱の通常処理を行い、その後アカウンティングサーバに Accounting-Request (アカウンティングリクエスト) を送信して通知します。T2 タイム後にアカウンティングサーバから応答がない場合、本製品はサーバに Accounting-Request (アカウンティングリクエスト) を再送信します。リトライ時間の最大値は N2 です。

Security > IGMP Access Control Settings の順にクリックし、以下の画面を表示します。

図 12-58 IGMP Access Control Settings 画面

本画面には以下の項目があります。

| 項目 | 説明 |
|-------------------|---|
| Unit | 設定するユニットを指定します。 |
| From Port/To Port | 設定の対象となるポートを指定します。 |
| State | 指定ポートの RADIUS 認証機能を有効、または無効にします。 Disable - 指定ポートのアカウンティングも認証も無効となります。 Auth_accounting - クライアント認証後に RADIUS サーバへアカウンティングメッセージが送信されます。(初期値) Auth_only - クライアント認証後に RADIUS サーバへアカウンティングメッセージが送信されません。 Accounting_only - クライアント認証の有無に関わらず、クライアントがグループに加入すると RADIUS サーバへアカウンティングメッセージが送信されます。 |

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

Port Security (ポートセキュリティ)

Port Security Settings (ポートセキュリティの設定)

ポートやポート範囲を指定して、ダイナミックな MAC アドレス学習をロックすることにより、MAC アドレスフォワーディングテーブルへ、新しいソース MAC アドレスが追加されないよう設定することができます。「Admin State」のプルダウンメニューで「Enabled」を選択し、「Apply」ボタンをクリックするとポートをロックできます。

ポートセキュリティは、ポートのロックを行う前にスイッチが（ソース MAC アドレスを）認識していない不正なコンピュータが、ロックしたポートに接続してネットワークへのアクセスを行わないようにするための機能です。

Security > Port Security > Port Security Settings の順にクリックし、以下の画面を表示します。

図 12-59 Port Security Settings 画面

本画面には次の項目があります。

| 項目 | 説明 |
|---------------------------------|---|
| Port Security Trap/Log Settings | スイッチのポートセキュリティトラップとログ設定を「Enabled」(有効)または「Disabled」(無効)にします。 |
| System Maximum Address (1-3328) | システムの最大アドレス数を入力します。 |
| Unit | ポートセキュリティ項目を表示するユニット番号を選択します。 |
| From Port / To Port | ポートセキュリティ項目を表示するポート範囲を選択します。 |
| Admin State | ポートセキュリティの有効/無効をプルダウンメニューで指定します。「Enabled」にすると、該当ポートは MAC アドレステーブルがロックされます。 |
| Lock Address Mode | プルダウンメニューでスイッチの選択ポートグループに対して MAC アドレステーブルのロック動作の詳細を指定します。オプションは以下の通りです。 <ul style="list-style-type: none"> Permanent – ロックされたアドレスは、エージングタイム経過後に削除されません。 Delete On Timeout – ロックされたアドレスは、エージングタイム経過後に削除されます。 Delete On Reset – ロックされたアドレスはリセットか再起動されるまで削除されません。 |
| Max Learning Address (0-3328) | 本ポートが学習できるポートセキュリティエントリの最大数を指定します。 |

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

エントリの編集

1. 編集するエントリの「Edit」ボタンをクリックして、以下の画面を表示します。

Port Security Settings Safeguard

Port Security Trap/Log Settings Enabled Disabled

Port Security System Settings

System Maximum Address (1-3328) No Limit

Unit From Port To Port Admin State Lock Address Mode Max Learning Address (0-3328)

1 01 01 Disabled Delete on Reset 32

Port Security Port Table

| Port | Admin State | Lock Address Mode | Max Learning Address | | |
|------|-------------|-------------------|----------------------|--------------------------------------|---|
| 1 | Disabled | DeleteOnReset | 32 | <input type="button" value="Apply"/> | <input type="button" value="View Details"/> |
| 2 | Disabled | DeleteOnReset | 32 | <input type="button" value="Edit"/> | <input type="button" value="View Details"/> |
| 3 | Disabled | DeleteOnReset | 32 | <input type="button" value="Edit"/> | <input type="button" value="View Details"/> |

図 12-60 Port Security Settings 画面 - Edit

2. 指定エントリを編集して「Apply」ボタンをクリックします。

指定エントリの参照

「View Detail」ボタンをクリックし、以下の画面を表示します。

Port Security Port-VLAN Settings Safeguard

Port 1:1

VLAN Name

VID List (e.g.: 1, 4-6)

Max Learning Address (0-3328) No Limit

Port Security Port-VLAN Table

| VLAN Name | Max Learning Address | |
|-----------|----------------------|-------------------------------------|
| default | 100 | <input type="button" value="Edit"/> |

図 12-61 Port Security Port-VLAN Settings 画面

本画面には次の項目があります。

| 項目 | 説明 |
|-------------------------------|---|
| VLAN Name | ラジオボタンをクリックして VLAN 名を入力します。 |
| VID List | ラジオボタンをクリックして VLAN ID リストを入力します。 |
| Max Learning Address (0-3328) | VLAN が学習できるポートセキュリティエントリの最大数を指定します。「0」は、本 VLAN でユーザの認証は行われなことを意味します。設定が VLAN ポートで現在学習したエントリ数より小さいと、コマンドは拒否されます。「No Limit」をチェックすると、VLAN が学習できるポートセキュリティエントリの最大数を制限しません。初期値は「No Limit」です。 |

エントリの編集

1. 編集するエントリの「Edit」ボタンをクリックして、以下の画面を表示します。

Port Security Port-VLAN Settings Safeguard

Port 1:1

VLAN Name

VID List (e.g.: 1, 4-6)

Max Learning Address (0-3328) No Limit

Port Security Port-VLAN Table

| VLAN Name | Max Learning Address | |
|-----------|----------------------|--|
| default | 100 | <input type="checkbox"/> No Limit <input type="button" value="Apply"/> |

図 12-62 Port Security Port-VLAN Settings 画面 - Edit

2. 指定エントリを編集して「Apply」ボタンをクリックします。

「<<Back」ボタンをクリックし、変更を破棄して前のページに戻ります。

Port Security VLAN Settings (ポートセキュリティ VLAN 設定)

指定 VLAN で学習されるポートセキュリティエントリの最大数を指定します。

Security > Port Security > Port Security VLAN Settings の順にクリックし、以下の画面を表示します。

図 12-63 Port Security VLAN Settings 画面

本画面には次の項目があります。

| 項目 | 説明 |
|-------------------------------|--|
| VLAN Name | VLAN 名を入力します。 |
| VID List | VLAN リストを指定します。 |
| Max Learning Address (0-3328) | VLAN が学習できるポートセキュリティエントリの最大数を指定します。「No Limit」をチェックすると、VLAN が学習できるポートセキュリティエントリの最大数を制限しません。 |

「Apply」ボタンをクリックして行った変更を適用します。

エントリの編集

1. 編集するエントリの「Edit」ボタンをクリックして、以下の画面を表示します。

図 12-64 Port Security VLAN Settings 画面 - Edit

2. 指定エントリを編集して「Apply」ボタンをクリックします。

Port Security Entries (ポートセキュリティエントリ)

スイッチが学習して転送データベースに登録したポートセキュリティエントリからエントリを削除します。

Security > Port Security > Port Security Entries の順にメニューをクリックし、以下の画面を表示します。

| VID | MAC Address | Port | Lock Mode | |
|-----|-------------------|------|---------------|--------|
| 1 | 00-13-72-0F-28-A4 | 1:2 | DeleteOnReset | Delete |
| 1 | 00-24-A5-4E-C9-C2 | 1:2 | DeleteOnReset | Delete |
| 1 | 14-FE-B5-E6-8A-B4 | 1:2 | DeleteOnReset | Delete |

図 12-65 Port Security Entries 画面

この画面では以下の情報を表示できます。

| 項目 | 説明 |
|-------------|--|
| VLAN Name | スイッチの転送データベーステーブルに登録されているエントリの VLAN 名です。 |
| VID List | スイッチの転送データベーステーブルに登録されているエントリの VLAN ID です。 |
| Port List | ポートセキュリティエントリ検索に使用するポート番号 (リスト) を入力します。「All」を選択すると、設定されているすべてのポートを表示します。 |
| MAC Address | スイッチの転送データベーステーブルに登録されているエントリの MAC アドレスです。 |
| Lock Mode | 転送データベーステーブルに登録されている MAC アドレスの種類です。 |

エントリの参照

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

「Show All」ボタンをクリックして、すべての定義済みエントリを表示します。

エントリのクリア

「Clear」ボタンをクリックして、入力した情報に基づいてすべてのエントリを削除します。

「Clear All」ボタンをクリックして、表示されたすべてのエントリを削除します。

エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。

ARP Spoofing Prevention Settings (ARP Spoofing 防止設定)

保護されたゲートウェイに対する MAC のなりすましを防止するためにスプーフィング防止エントリを設定します。エントリが作成されると、送信側 IP がエントリのゲートウェイ IP に一致するが、送信側 MAC フィールドまたは送信元 MAC フィールドがエントリのゲートウェイ MAC に一致しない ARP パケットは、システムによって破棄されます。

Security > ARP Spoofing Prevention Settings の順にメニューをクリックし、以下の画面を表示します。

図 12-66 ARP Spoofing Prevention Settings 画面

この画面では以下の情報を表示できます。

| 項目 | 説明 |
|---------------------|--|
| Gateway IP Address | ARP Spoofing を防止するのに使用するゲートウェイ IP アドレスを入力します。 |
| Gateway MAC Address | ARP Spoofing を防止するのに使用する MAC アドレスを指定します。 |
| Ports | 機能を適用するポート番号を選択します。また、「All Port」を選択するとスイッチのすべてのポートに本機能が適用されます。 |

「Gateway IP」(ゲートウェイの IP アドレス)、「Gateway MAC」(ゲートウェイの MAC アドレス) および「Port List」を入力し、「Apply」ボタンをクリックします。

エントリの編集

1. 編集するエントリの「Edit」ボタンをクリックして、以下の画面を表示します。

図 12-67 ARP Spoofing Prevention Settings 画面 - Edit

2. 指定エントリを編集して「Apply」ボタンをクリックします。

エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。「Delete All」ボタンをクリックして、表示されたすべてのエントリを削除します。

BPDU Attack Protection (BPDU アタック防止設定)

スイッチのポートに BPDU 防止機能を設定します。通常、BPDU 防止機能には 2 つの状態があります。1 つは正常な状態で、もう 1 つはアタック状態です。

アタック状態には、3 つのモード（破棄、ブロックおよびシャットダウン）があります。BPDU 防止が有効なポートは、STP BPDU パケットを受信するとアタック状態に入ります。そして、設定に基づいてアクションを行います。このように、BPDU 防止は STP が無効なポートにだけ有効にすることができます。

BPDU 防止では、「STP Port Settings」画面 (L2 Features > Spanning Tree > STP Port Settings) の「Forward BPDU」に設定したものより高い優先度を持っています。つまり、ポートが「STP Port Settings」画面の「Forward BPDU」に設定されており、BPDU 防止が有効であると、ポートは STP BPDU を転送しません。

BPDU 防止では、BPDU の処理を決定するために設定したレイヤ 2 プロトコルトンネルポートより高い優先度を持っています。つまり、ポートが L2 Features > Layer2 Protocol Tunneling Settings 画面の「Tunnel STP Port(s)」にレイヤ 2 プロトコルトンネルポートとして設定されていると、ポートは STP BPDU を転送します。しかし、ポートで BPDU 防止が有効であると、ポートは STP BPDU を転送しません。

Security > BPDU Attack Protection の順にメニューをクリックし、以下の画面を表示します。

図 12-68 BPDU Attack Protection 画面

以下の項目を使用して、設定します。

| 項目 | 説明 |
|------------------------------|--|
| BPDU Attack Protection State | BPDU アタック防止機能をグローバルに有効または無効にします。初期値は無効です。 |
| Trap State | トラップをいつ送信するか指定します。「None」、「Attack Detected」、「Attack Cleared」、または「Both」を選択します。初期値は「None」(なし) です。 |
| Log State | ログエントリをいつ送信するか指定します。「None」、「Attack Detected」、「Attack Cleared」、または「Both」を選択します。初期値は「Both」です。 |
| Recover Time (60-1000000) | BPDU 防止の自動復帰タイムを指定します。復帰タイムの初期値は 60 です。「Infinite」をチェックすると、自動復帰はしなくなります。 |
| Unit | 設定を使用するユニット番号を選択します。 |
| From Port / To Port | 設定を使用するポート範囲を選択します。 |
| State | 指定ポートに対してモードを有効または無効にします。 |
| Mode | BPDU 防止モードを指定します。 <ul style="list-style-type: none"> Drop - ポートがアタック状態に入るとすべての受信 BPDU パケットを破棄します。 Block - ポートがアタック状態に入るとすべてのパケット (BPDU と正常なパケットを含む) を破棄します。 Shutdown - ポートがアタック状態に入るとポートをシャットダウンします。(初期値) |

「Apply」 ボタンをクリックし、変更を有効にします。

Loopback Detection Settings (ループバック検知設定)

ループバック検知 (LBD) 機能は、特定のポートに生成されるループを検出するために使用されます。本機能は、CTP(Configuration Testing Protocol) パケットがスイッチにループバックすると、スイッチのポートを一時的にシャットダウンします。スイッチが CTP パケットをポートまたは VLAN から受信したことを検知すると、ネットワークにループバックが発生していると認識します。スイッチは、自動的にポートまたは VLAN をブロックして管理者にアラートを送信します。「Loopback Detection Recover Time」がタイムアウトになると、ループバック検知ポートは再起動 (Normal 状態へ遷移) を行います。ループバック検知機能はポート範囲に実行されます。

Security > Loopback Detection Settings の順にメニューをクリックし、以下の画面を表示します。

The screenshot shows the 'Loopback Detection Settings' interface. At the top, there's a title bar with 'Safeguard' on the right. Below it, the 'Loopback Detection Global Settings' section has a radio button for 'Loopback Detection State' set to 'Disabled'. There are 'Apply' buttons. The 'Loopback Detection Global Settings' section includes: 'Mode' (Port-based), 'Interval (1-32767)' (10 sec), 'Trap State' (None), 'Recover Time (0 or 60-1000000)' (60 sec), 'Log State' (Enabled), and 'Enabled VLANs (e.g.: 2-5)' (1-4094) with an 'All VLANs' checkbox. Below this is the 'Unit 1 Settings' section with a table:

| Unit | From Port | To Port | State |
|------|-----------|---------|----------|
| 1 | 01 | 01 | Disabled |

Below the table is the 'Unit 1 Settings' table:

| Port | Loopback Detection State | Loop Status |
|------|--------------------------|-------------|
| 1 | Disabled | Normal |
| 2 | Disabled | Normal |
| 3 | Disabled | Normal |

図 12-69 Loopback Detection Settings 画面

本画面には次の項目があります。

| 項目 | 説明 |
|--------------------------------|---|
| Loopback Detection State | ループバック検知機能を「Enabled」(有効)または「Disabled」(無効)にします。初期値は「Disabled」です。 |
| Mode | プルダウンメニューを使用して、「Port-based」と「VLAN-based」を切り替えます。 |
| Trap State | トラップを送信する状態を選択します。オプションは以下の通りです。 <ul style="list-style-type: none"> Loop Detected - ループ状態を検知すると、トラップを送信します。 Loop Cleared - ループ状態がクリアされると、トラップを送信します。 None - ループバック検知のトラップを送信しません。(初期値)。 Both - 検知およびクリアのトラップを両方送信します。 |
| Log State | プルダウンメニューを使用して、ループバック検知のログ状態を「Enabled」(有効) / 「Disabled」(無効)にします。 |
| Interval (1-32767) | デバイスがループバックイベントを検出するためにすべての CTP(Configuration Test Protocol) パケットを送信する間隔 (秒)。有効な範囲は 1-32767 (秒) です。初期値:10 (秒)。 |
| Recover Time (0 or 60-1000000) | ループが検知された場合にリカバリする時間 (秒) を指定します。指定時間に到達すると、スイッチはループをチェックします。ループが検知されないと、ポートが再度有効になります。0 または 60-1000000 (秒) に設定します。0 を指定すると、ループバックリカバリタイムは無効になります。初期値は 60 (秒) です。 |
| Enabled VLANs | VLAN のループバック検知を有効にします。設定する VLAN リストを指定します。すべての VLAN に適用する場合は、「All VLANs」にチェックを入れます。 |
| Unit | 設定を使用するユニット番号を選択します。 |
| From Port / To Port | プルダウンメニューで適用するポート範囲を選択します。 |
| State | プルダウンメニューで「Enabled」(有効)または「Disabled」(無効)を指定します。 |

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

注意

「Untag (タグなし)」時でも「VID 0」は CTP に「Tag Field」を付与されます。規定上「VID 0」は「Untag (タグなし)」として扱われますが、古い一部のハードウェア製品 (chipset 等) では破棄する場合がありますのでご注意ください。

NetBIOS Filtering Setting (NetBIOS フィルタリング設定)

ネットワークをまたいで通信するために、NetBIOS はインタフェースをプログラミングするアプリケーションで、アプリケーションが使用する多くの機能を提供します。NetBEUI (NetBIOS Enhanced User Interface) は、NetBIOS のためのデータリンク層フレーム構造として作成されました。NetBIOS トラフィックを送信するためのシンプルなメカニズムである NetBEUI は小規模の MS-DOS や Windows ベースのワークグループのために選択するプロトコルです。NetBIOS は、厳密には NetBEUI プロトコル内には含まれません。マイクロソフトは、RFC1001 と RFC1002 に NetBIOS over TCP/IP (NBT) を記述した国際規格を作成するために取り組みました。

NetBEUI プロトコルを使用する 2 台以上のコンピュータのネットワーク通信をブロックする場合、これらの種類のパケットをフィルタするために NetBIOS フィルタリングを使用することができます。

NetBIOS フィルタを有効にすると、スイッチは自動的に 1 つのアクセスプロファイルと 3 つのアクセスルールを作成します。ユーザが広範囲に NetBIOS フィルタを有効にすると、スイッチはもう 1 つずつアクセスプロファイルとアクセスルールを作成します。

Security > NetBIOS Filtering Setting の順にメニューをクリックし、以下の画面を表示します。

図 12-70 NetBIOS Filtering Settings 画面

以下の項目を使用して設定します。

| 項目 | 説明 |
|--|--|
| NetBIOS Filtering | |
| NetBIOS フィルタリング設定に含める適切なポートを選択します。 | |
| Unit | 設定するユニットを選択します。 |
| Ports | NetBIOS フィルタリング設定に含める適切なポートを簡単にチェックできます。 |
| Extensive NetBIOS Filtering Ports | |
| Extensive NetBIOS フィルタリング設定に含める適切なポートを選択します。Extensive NetBIOS は 802.3 (TCP/IP) における NetBIOS です。スイッチはこれが有効なポートでは 802.3 における NetBIOS フレームを拒否します。 | |
| Unit | 設定するユニットを選択します。 |
| Ports | Extensive NetBIOS フィルタリング設定に含める適切なポートを簡単にチェックできます。 |

「Apply」 ボタンをクリックして各セクションで行った変更を適用します。

「Select All」 ボタンをクリックすると設定用にすべてのポートを選択します。

「Clear All」 ボタンをクリックして、すべてのポートを削除します。

Traffic Segmentation Settings (トラフィックセグメンテーション設定)

トラフィックセグメンテーション機能は、(単一/複数) ポート間のトラフィックの流れを制限するために使用します。「トラフィックフローの分割」という方法は、「VLANによるトラフィック制限」に似ていますが、さらに制限的です。本機能によりマスタスイッチ CPU のオーバヘッドを増加させないようにトラフィックを操作することが可能です。

Security > Traffic Segmentation Settings の順にメニューをクリックし、以下の画面を表示します。

| Port | Forward Port List |
|------|-------------------|
| 1 | 1:1-1:26 |
| 2 | 1:1-1:26 |
| 3 | 1:1-1:26 |
| 4 | 1:1-1:26 |
| 5 | 1:1-1:26 |
| 6 | 1:1-1:26 |
| 7 | 1:1-1:26 |
| 8 | 1:1-1:26 |

図 12-71 Traffic Segmentation Settings 画面

以下の項目を使用して設定します。

| 項目 | 説明 |
|-------------------|---|
| Port List | トラフィックセグメンテーションを設定するポートを入力します。「All Ports」ボタンをクリックすると設定用にすべてのポートを選択します。 |
| Forward Port List | トラフィックセグメンテーション設定に含めるポートを入力します。「All Ports」ボタンをクリックすると設定用にすべてのポートを選択します。 |
| Unit | 設定するユニット番号を選択します。 |
| Port | トラフィックセグメンテーション設定に含めたポートを表示します。 |

「Apply」ボタンをクリックすると、転送ポートの組み合わせが入力され、設定内容がテーブルに反映されます。

DHCP Server Screening (DHCP サーバスクリーニング)

本機能では、ユーザはすべての DHCP サーバパケットを制限できるだけでなく、指定したどの DHCP クライアントからの DHCP サーバパケットも受信することが可能になります。この機能は 1 つ以上の DHCP サーバがネットワークに存在する場合に DHCP サービスを異なるクライアントグループと区別するのに役に立ちます。

初めて DHCP フィルタを有効にした時にアクセスプロファイルエントリとポートエントリごとのアクセスルールとその他のアクセスルールが作成されます。これらのルールは、すべての DHCP サーバパケットをブロックするのに使用します。さらに、DHCP エントリの許可のために、初めて DHCP クライアント MAC アドレスがクライアント MAC アドレスとして使用される時に、1 つのアクセスプロファイルと 1 つのアクセスルールエントリが作成されます。送信元 IP アドレスは DHCP サーバの IP アドレスと同じになります (UDP ポート番号は 68 です)。これらのルールは、ユーザが設定した特定のフィールドを持つ DHCP サーバパケットを許可するのに使用します。

DHCP サーバフィルタ機能が有効の場合、指定されたポートからのすべての DHCP サーバパケットはフィルタされます。

DHCP Server Screening Port Settings (DHCP サーバスクリーニング設定)

スイッチは DHCP サーバスクリーニング (不正な DHCP サーバへのアクセスを拒否する機能) をサポートしています。DHCP サーバフィルタ機能が有効の場合、指定されたポートからのすべての DHCP サーバパケットはフィルタされます。

Security > DHCP Server Screening > DHCP Screening Port Settings の順にメニューをクリックして画面を表示します。

The screenshot shows the configuration interface for DHCP Server Screening Port Settings. It includes the following elements:

- Global Settings:**
 - DHCP Server Screening Trap State: Enabled, Disabled
 - DHCP Server Screening Log State: Enabled, Disabled
 - Illegitimate Server Log Suppress Duration: 1 min, 5 mins, 30 mins
- Unit Settings:**
 - Unit: 1 (dropdown)
 - From Port: 01 (dropdown)
 - To Port: 01 (dropdown)
 - State: Disabled (dropdown)
- Unit 1 Settings Table:**

| Port | State |
|------|----------|
| 1 | Disabled |
| 2 | Disabled |
| 3 | Disabled |
| 4 | Disabled |
| 5 | Disabled |

図 12-72 DHCP Screening Port Settings 画面

本画面には次の項目があります。

| 項目 | 説明 |
|--------------------------------------|--|
| DHCP Server Screening Trap State | DHCP サーバのトラップフィルタを「Enabled」(有効) または「Disabled」(無効) にします。 |
| DHCP Server Screening Log State | DHCP サーバのログフィルタを「Enabled」(有効) または「Disabled」(無効) にします。 |
| Illegal Server Log Suppress Duration | 不正なサーバログの抑制時間を 1、5、または 30 分から選択します。 |
| Unit | 設定するユニットを選択します。 |
| From Port/To Port | 設定の対象となるポートを指定します。 |
| State | DHCP サーバスクリーニングを「Enabled」(有効) または「Disabled」(無効) にします。初期値は「Disabled」です。 |

設定後、「Apply」ボタンをクリックして設定を有効にします。

DHCP Offer Permit Entry Settings (DHCP オファー許可エントリ設定)

許可エントリの追加または削除を行います。

Security > DHCP Server Screening > DHCP Offer Permit Entry Settings の順にクリックし、画面を表示します。

図 12-73 DHCP Offer Permit Entry Settings 画面

本画面には次の項目があります。

| 項目 | 説明 |
|----------------------|---|
| Server IP Address | フィルタを通過させる DHCP サーバを指定します。 |
| Client's MAC Address | DHCP クライアントの MAC アドレスを指定します。ネットワーク上の正しい DHCP サーバが複数ある場合にだけ入力します。ネットワーク上に正しい DHCP サーバが 1 つしか存在しない場合は、入力することはできません。 |
| Ports | フィルタする DHCP サーバのポート番号を入力します。スイッチのすべてのポートを使用する場合は「All Ports」をチェックします。 |

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。「Delete」ボタンをクリックして、入力した情報に基づいて指定エントリを削除します。

Filter DHCPv6 Server (DHCPv6 サーバフィルタ設定)

DHCPv6 サーバフィルタ設定には指定ポートの DHCP サーバパケットを制限する目的と、事前に定義済みのサーバ IP アドレスとクライアント MAC アドレスの DHCP サーバパケットを許可する目的があります。これにより指定の DHCP クライアントに対応する DHCP サーバを制限することが可能です。この機能はネットワーク上に二つ以上の DHCP サーバが存在する場合に有効で、一つはプライベート IP アドレスを提供し、他はパブリックの IP アドレスを提供することができます。DHCP サーバポートフィルタを有効にすることでアクセスプロファイルとアクセスルールを各ポートにそれぞれ作成します。(UDP ポートは 67 と同等です。) ファイル内の制限されたコマンドは同じアクセスプロファイル内で共有されます。許可された DHCP エントリの追加にはアクセスプロファイルとアクセスルールが作成されます。ファイル内の制限されたコマンドは同じアクセスプロファイル内で共有されます。

Security > DHCP Server Screening > Filter DHCPv6 Server の順にメニューをクリックして画面を表示します。

図 12-74 Filter DHCPv6 Server 画面

本画面には次の項目があります。

| 項目 | 説明 |
|------------|------------------------------------|
| Log State | DHCP サーバフィルタイベントのログを有効 / 無効にします。 |
| Trap State | DHCP サーバフィルタイベントのトラップを有効 / 無効にします。 |

| 項目 | 説明 |
|----------------------------|---|
| Filter DHCPv6 Server State | DHCPv6 サーバフィルタを設定します。 <ul style="list-style-type: none"> Ports - 設定するポートリストを指定します。「All Ports」にチェックすると全ポートを設定します。 State - 「有効」「無効」を指定します。 |
| DHCPv6 Server Permit | DHCPv6 サーバの許可エントリを作成します。指定した送信元 IPv6 アドレスの DHCPv6 サーバパケットは指定ポートへ転送されます。 <ul style="list-style-type: none"> Source IP Address - フィルタ DHCPv6 サーバ転送リストに作成するエントリの送信元アドレスを指定します。 Ports - 設定に適用するポートリストを指定します。「All Ports」にチェックすると全ポートを設定します。 |

設定後、「Apply」ボタンをクリックして設定を有効にします。

Filter ICMPv6 (ICMPv6 フィルタ設定)

「Filter ICMPv6」ではスイッチの全 ICMPv6 RA ノードパケットの制限 (フィルタ) を設定します。全 ICMPv6 RA ノードパケットの制限 (フィルタ) 機能はスイッチ上、指定ポートの ICMPv6 RA 全ノードパケットを制限、または指定送信元からのトラストパケットを受信するために使用されます。不正なホストからの ICMPv6 RA 全ノードパケット送信からネットワークを守るために有効です。宛先アドレスが全ノードマルチキャストアドレス (FF02::1) の場合にフィルタを有効にする必要があります。

Security > DHCP Server Screening > Filter ICMPv6 の順にクリックし、画面を表示します。

The screenshot shows the 'Filter ICMPv6' configuration window. At the top right is a 'Safeguard' icon. The 'Log State' section has 'Enabled' selected. The 'Trap State' section has 'Disabled' selected. Below is the 'Filter ICMPv6 RA_All_Node State' section with a text input field, an 'All Ports' checkbox, and a 'State' dropdown menu set to 'Disabled'. The 'ICMPv6 RA_All_Node Permit' section has a 'Source IP Address' text input field, a 'Ports' text input field, and an 'All Ports' checkbox. At the bottom, there is a 'Total Entries: 1' section with a table listing one entry: 'Source IP Address: 3FF3::1' and 'Ports: 1:1-1:26'. Buttons for 'Apply' and 'Delete' are present throughout the interface.

図 12-75 Filter ICMPv6 画面

本画面には次の項目があります。

| 項目 | 説明 |
|---------------------------------|---|
| Log State | ICMPv6 RA All-nodes のログを有効 / 無効にします。有効にすると “Detected untrusted ICMPv6 All-nodes RA” が起動します。 |
| Trap State | ICMPv6 RA All-nodes のトラップを有効 / 無効にします。有効にすると “illegal ICMPv6 all-nodes RA is detected” が送信されます。「ICMPv6 RA all-nodes」サーバが無効の場合、送信されません。 |
| Filter ICMPv6 RA_All_Node State | ICMPv6 フィルタを設定します。 <ul style="list-style-type: none"> Ports - 設定するポートリストを指定します。「All Ports」にチェックすると全ポートを設定します。 State - 「有効」「無効」を指定します。 |
| ICMPv6 RA_All_Node Permit | DHCPv6 サーバの許可エントリを作成します。指定した送信元 IPv6 アドレスの DHCPv6 サーバパケットは指定ポートへ転送されます。 <ul style="list-style-type: none"> Source IP Address - フィルタ ICMPv6 RA All-nodes 転送リストに作成するエントリの送信元アドレスを指定します。 Ports - 設定に適用するポートリストを指定します。「All Ports」にチェックすると全ポートを設定します。 |

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

「Delete」ボタンをクリックして、入力した情報に基づいて指定エントリを削除します。

Access Authentication Control (アクセス認証コントロール)

TACACS/ XTACACS/ TACACS+/ RADIUS コマンドは、TACACS/ XTACACS/ TACACS+/ RADIUS プロトコルを使用してスイッチへの安全なアクセスを可能にします。ユーザがスイッチへのログインや、管理者レベルの特権へのアクセスを行おうとする時、パスワードの入力を求められます。TACACS/ XTACACS/ TACACS+/ RADIUS 認証がスイッチで有効になると、スイッチは TACACS/ XTACACS/ TACACS+/ RADIUS サーバと連絡し、ユーザの確認をします。確認が行われたユーザは、スイッチへのアクセスを許可されます。

現在 TACACS セキュリティプロトコルには異なるエンティティを持つ 3 つのバージョンが存在します。本スイッチのソフトウェアは TACACS の以下のバージョンをサポートします。

- TACACS (Terminal Access Controller Access Control System)
セキュリティのためのパスワードチェック、認証、およびユーザアクションの通知を、1 台またはそれ以上の集中型の TACACS サーバを使用して行います。パケットの送受信には UDP プロトコルを使用します。
- XTACACS (拡張型 TACACS)
TACACS プロトコルの拡張版で、TACACS プロトコルより多種類の認証リクエストとレスポンスコードに対応します。パケットの送受信に UDP プロトコルを使用します。
- TACACS+ (Terminal Access Controller Access Control System plus)
ネットワークデバイスの認証のために詳細なアクセス制御を提供します。TACACS+ は、1 台またはそれ以上の集中型のサーバを経由して認証コマンドを使用することができます。TACACS+ プロトコルは、スイッチと TACACS+ デモンの間のすべてのトラフィックを暗号化します。また、TCP プロトコルを使用して信頼性の高い伝達を行います。

TACACS/ XTACACS/ TACACS+/ RADIUS のセキュリティ機能が正常に動作するためには、スイッチ以外の認証サーバホストと呼ばれるデバイス上で認証用のユーザ名とパスワードを含む TACACS/ XTACACS/ TACACS+/ RADIUS サーバの設定を行う必要があります。スイッチがユーザにユーザ名とパスワードの要求を行う時、スイッチは TACACS/ XTACACS/ TACACS+/ RADIUS サーバにユーザ認証の問い合わせを行います。サーバは以下の 3 つのうちの 1 つの応答を返します。

- サーバは、ユーザ名とパスワードを認証し、ユーザにスイッチへの通常のアクセス権を与えます。
- サーバは、入力されたユーザ名とパスワードを受け付けず、スイッチへのアクセスを拒否します。
- サーバは、認証の問い合わせに応じません。この時点でスイッチはサーバからタイムアウトを受け取り、メソッドリスト中に設定された次の認証方法へと移行します。

本スイッチには TACACS、XTACACS、TACACS+、RADIUS の各プロトコル用に 4 つの認証サーバグループがあらかじめ組み込まれています。これらの認証サーバグループはスイッチにアクセスを試みるユーザの認証に使用されます。認証サーバグループ内に任意の順番で認証サーバホストを設定し、ユーザがスイッチへのアクセス権を取得する場合、1 番目の認証サーバホストに認証を依頼します。認証が行われなければ、リストの 2 番目のサーバホストに依頼し、以下同様の処理が続きます。実装されている認証サーバグループには、特定のプロトコルが動作するホストのみを登録できます。例えば TACACS 認証サーバグループは、TACACS 認証サーバホストのみを登録できます。

スイッチの管理者は、ユーザ定義のメソッドリストに 6 種類の異なる認証方法 (TACACS/ XTACACS/ TACACS+/ RADIUS/ local/ none) を設定できます。これらの方法は、任意に並べ替えることが可能で、スイッチ上での通常のユーザ認証に使用されます。リストには最大 8 つの認証方法を登録できます。ユーザがスイッチにアクセスしようすると、スイッチはリストの 1 番目の認証方法を選択して認証を行います。1 番目の方法で認証サーバホストを通過しても認証が返ってこなければ、スイッチはリストの次の方法を試みます。この手順は、認証が成功するか、拒否されるか、またはリストのすべての認証方法を試し終わるまで繰り返されます。

TACACS/XTACACS/TACACS+ または non (認証なし) のメソッド経由でユーザがデバイスへのログインに成功すると、「User」の権限のみが与えられます。ユーザが管理者レベルの権限に更新したい場合、「Enable Admin」コマンドを実行し、権限レベルを昇格させる必要があります。しかし、ユーザが RADIUS サーバまたはローカルな方法を経由してデバイスへのログインに成功すると、3 種類の権限レベルをユーザに割り当てることが可能であり、ユーザは「enable admin」コマンドを使用して、権限レベルを昇格させることはできません。

スイッチへのアクセス権を取得したユーザは、スイッチに通常ユーザのアクセス権を与えられています。理者特権レベルの権利を取得するためには、ユーザは「Enable Admin」画面にアクセスし、スイッチに管理者により事前に設定されているパスワードの入力が必要になります。本スイッチは TACACS+ サーバのユーザ権限の割り当てをサポートします。

注意 TACACS、XTACACS、TACACS+、RADIUS は独立したエンティティであり、互換性はありません。スイッチとサーバ間は、同じプロトコルを使用した全く同じ設定を行う必要があります。(例えば、スイッチに TACACS 認証を設定した場合、ホストサーバにも同様の設定を行います。)

Enable Admin (管理者レベルの認証)

本画面は、通常のユーザレベルとしてスイッチにログインした後、管理者レベルに昇格したい場合に使用します。スイッチにログインした後のユーザにはユーザレベルの権限のみが与えられています。管理者レベルの権限を取得するためには、本画面を開き、認証用パスワードを入力します。本機能における認証方法は、TACACS/XTACACS/TACACS+/RADIUS、ユーザ定義のサーバグループ、local enable(スイッチ上のローカルアカウント)または、認証なし(none)から選択できます。XTACACS と TACACS は Enable の機能をサポートしていないため、ユーザはサーバホスト上に特別なアカウントを作成し、ユーザ名「enable」、および管理者が設定するパスワードを登録する必要があります。本機能は認証ポリシーが「Disabled」(無効)である場合には実行できません。

Security > Access Authentication Control > Enable Admin の順にメニューをクリックし、以下の画面を表示します。

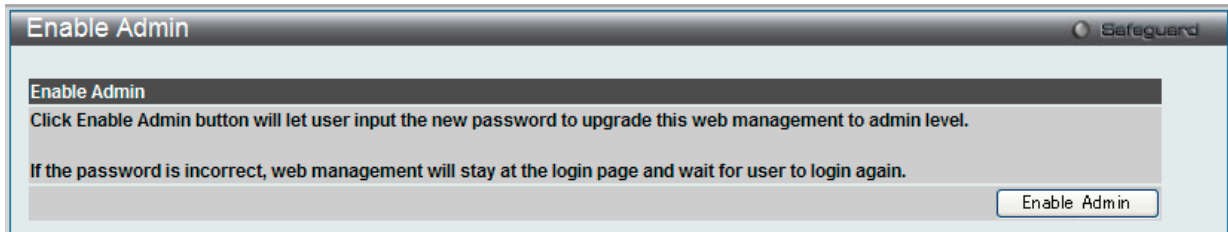


図 12-76 Enable Admin 画面

「Enable Admin」ボタンをクリックして以下のダイアログボックスを表示します。

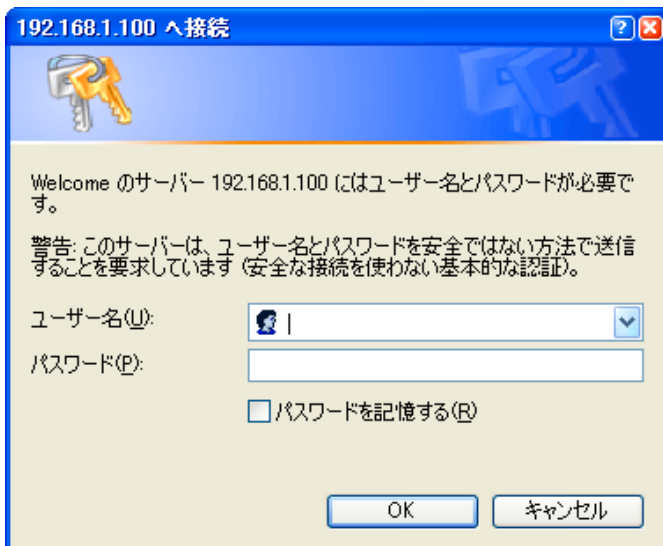


図 12-77 ユーザ名とパスワード入力ダイアログボックス

「ユーザー名」と「パスワード」を入力して「OK」ボタンをクリックします。「ユーザー名」と「パスワード」が承認されると、ユーザ権限は管理者特権レベルに変更されます。

Authentication Policy Settings (認証ポリシー設定)

スイッチにアクセスするユーザのために管理者が定義した認証ポリシーを有効にします。有効にすると、デバイスはログインメソッドリストをチェックし、ログイン時のユーザ認証に使用する認証方法を選択します。

Security > Access Authentication Control > Authentication Policy Settings の順にメニューをクリックし、以下の画面を表示します。

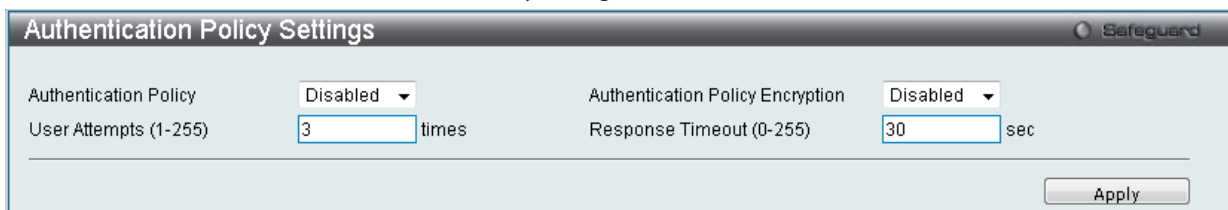


図 12-78 Authentication Policy Settings 画面

以下の項目を使用して設定を行います。

| 項目 | 説明 |
|----------------------------------|---|
| Authentication Policy | プルダウンメニューからスイッチの認証ポリシーを「Enabled」(有効)または「Disabled」(無効)に設定します。 |
| Authentication Policy Encryption | プルダウンメニューからスイッチの認証ポリシー暗号化を「Enabled」(有効)または「Disabled」(無効)に設定します。 |

Security (セキュリティ機能の設定)

| 項目 | 説明 |
|--------------------------|--|
| Response Timeout (0-255) | ユーザからの認証のレスポンスに対するスイッチの待ち時間を指定します。0-255 (秒) の範囲から指定します。初期値は 30 (秒) です。 |
| User Attempts (1-255) | ユーザが認証を試みることができる最大回数。指定回数認証に失敗すると、そのユーザはスイッチへのアクセスを拒否され、さらに認証を試みることができなくなります。CLI ユーザは、再度認証を行う前に 60 秒待つ必要があります。Telnet および Web ユーザはスイッチから切断されます。1-255 の範囲で指定します。初期値は 3 (回) です。 |

「Apply」 ボタンをクリックし、設定を有効にします。

Application Authentication Settings (アプリケーションの認証設定)

作成済みのメソッドリストを使用して、ユーザレベルおよび管理者レベル (Enable Admin) でログインする際に使用するスイッチの設定用アプリケーション (コンソール、Telnet、SSH、Web) を設定します。

Security > Access Authentication Control > Application Authentication Settings の順にクリックし、以下の画面を表示します。

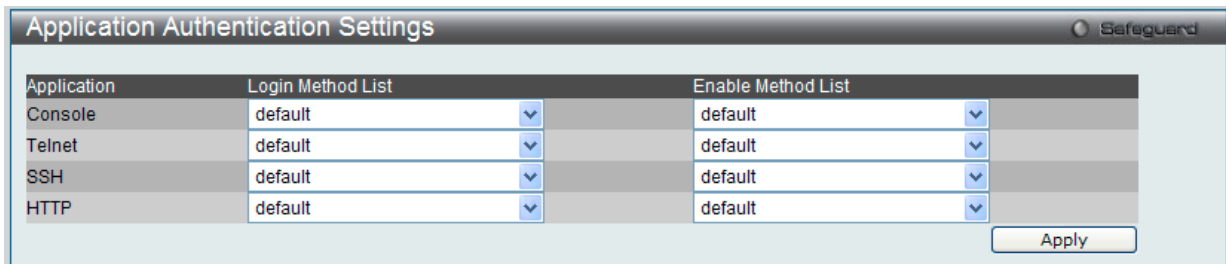


図 12-79 Application Authentication Settings 画面

以下の項目を使用して、設定を行います。

| 項目 | 説明 |
|--------------------|--|
| Application | スイッチ上の設定用アプリケーションをリスト表示しています。それぞれのアプリケーション (コンソール、Telnet、SSH、HTTP) を使用するユーザ認証用の「Login Method List」と「Enable Method List」を指定できます。 |
| Login Method List | プルダウンメニューを使用し、登録済みのメソッドリストから、ユーザレベルの通常ログインを行うアプリケーションに適用するリストを選択します。初期設定のメソッドリスト、またはユーザ定義のメソッドリストを選択できます。詳細な情報は、後述の「Login Method Lists Settings」画面を参照してください。 |
| Enable Method List | プルダウンメニューにより、登録済みのメソッドリストを使用してユーザレベルを管理者レベルに昇格させるアプリケーションを選択します。初期設定のメソッドリスト、またはユーザ定義のメソッドリストを選択できます。詳細な情報は、後述の「Login Method Lists Settings」画面を参照してください。 |

「Apply」 ボタンをクリックし、設定を有効にします。

Accounting Settings (アカウント設定)

RADIUS アカウントサービスの状態を設定します。

Security > Access Authentication Control > Accounting Settings の順にクリックし、以下の画面を表示します。

Accounting Settings Safeguard

Network: Disabled

Shell: Disabled

System: Disabled

Command Service Method List Name Settings

Administrator: None

Operator: None

Power User: None

User: None

Apply

Network: When enabled, the switch will send informational packets to a remote server when 802.1X, WAC and JWAC port access control events occur on the switch.

Shell: When enabled, the switch will send informational packets to a remote server when a user either logs in, logs out or times out on the switch, using the console, Telnet, or SSH.

System: When enabled, the switch will send informational packets to a remote server when system events occur on the switch, such as a system reset or system boot.

Command Accounting: It's the service for all administrator,operator,power user or user level commands.When it selects method list name,it specifies accounting service by the AAA user defined method list.When it selects none,the switch disables AAA command accounting services by specified command level.

図 12-80 Accounting Settings 画面

以下の項目を使用して、設定を行います。

| 項目 | 説明 |
|---------------|--|
| Network | 「RADIUS Only」が選択された場合、リモート RADIUS サーバに「Network」情報パケットを送信します。 「Method List Name」が選択された場合、作成されたメソッドリストを基に「Network」情報パケットを送信します。 |
| Shell | 「RADIUS Only」が選択された場合、リモート RADIUS サーバに「Shell」情報パケットを送信します。 「Method List Name」が選択された場合、作成されたメソッドリストを基に「Shell」情報パケットを送信します。 |
| System | 「RADIUS Only」が選択された場合、リモート RADIUS サーバに「System」情報パケットを送信します。 「Method List Name」が選択された場合、作成されたメソッドリストを基に「System」情報パケットを送信します。 |
| Administrator | 選択されると「Administrator」レベルのコマンドが有効になります。 |
| Operator | 選択されると「Operator」レベルのコマンドが有効になります。 |
| Power User | 選択されると「Power User」レベルのコマンドが有効になります。 |
| User | 選択されると「User」レベルのコマンドが有効になります。 |

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

Authentication Server Group Settings (認証サーバグループ設定)

本画面では、スイッチ上に認証サーバグループの設定を行います。サーバグループとは、TACACS/ XTACACS/ TACACS+/ RADIUS のサーバホストを、ユーザ定義のメソッドリスト使用の認証カテゴリにグループ分けしたものです。プロトコルによって、または定義済みのサーバグループに組み込むことによりグループ分けを行います。スイッチには4つの認証サーバグループがあらかじめ組み込まれています。これらは削除することができませんが、内容の変更は可能です。1つのグループにつき最大8個までの認証サーバホストを登録できます。

Security > Access Authentication Control > Authentication Server Group Settings の順にメニューをクリックし、以下の画面を表示します。

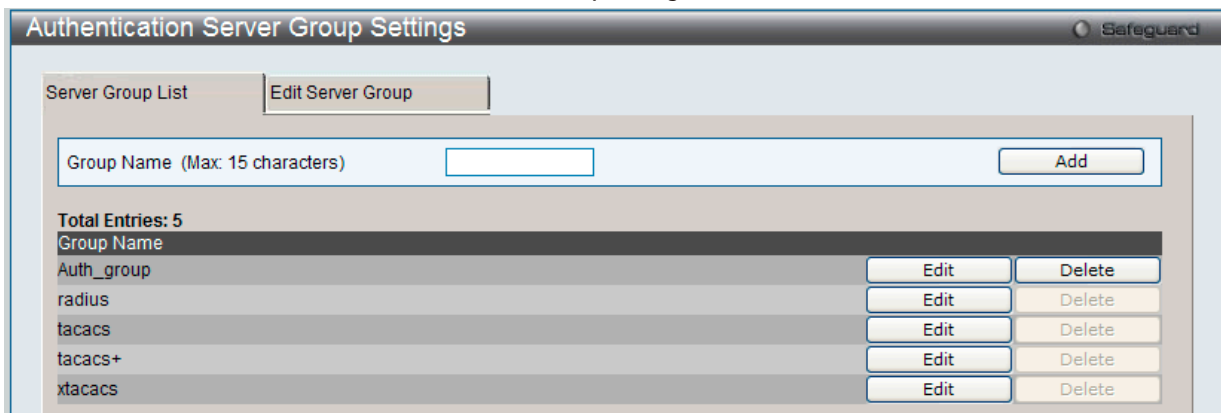


図 12-81 Authentication Server Group Settings 画面

スイッチの認証サーバグループを表示します。スイッチには4つの認証サーバグループが組み込まれています。これらは削除できませんが、内容の変更は可能です。

以下の項目を使用して、設定を行います。

| 項目 | 説明 |
|------------|-------------------|
| Group Name | 新規サーバグループ名を指定します。 |

新しいサーバグループを作成するためには、「Group Name」欄に名前を入力し、「Add」ボタンをクリックします。特定のグループを編集するためには、対応する「Edit」ボタンをクリックするか、またはこの画面の上の「Edit Server Group」タブをクリックし、以下の画面を表示します。

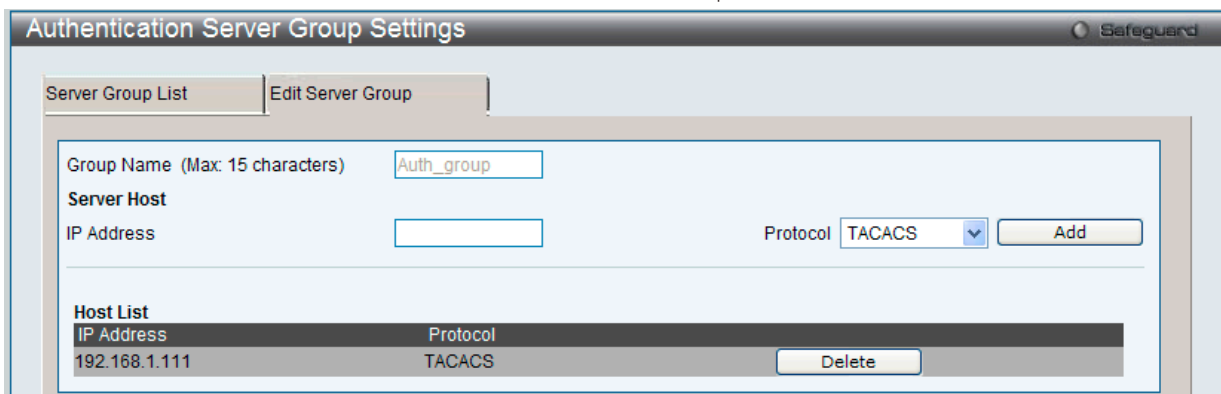


図 12-82 Authentication Server Group Settings (Edit) 画面

以下の項目を使用して、設定を行います。

| 項目 | 説明 |
|------------|--|
| Group Name | サーバグループ名を指定します。 |
| IP Address | サーバホストの IP アドレスを入力します。 |
| Protocol | プルダウンメニューを使用して、認証サーバホストの IP アドレスに割り当てるプロトコルを選択します。 |

リストに認証サーバホストを追加するためには、「Group Name」欄にホストの名称、「IP Address」フィールドにホストの IP アドレスを入力し、プルダウンメニューから認証サーバホストの IP アドレスに関連付けるプロトコルを指定します。その後「Add」ボタンをクリックすると、本認証サーバホストがグループに登録されます。エントリはこのタブの「Host List」に表示されます。

注意 認証サーバホストをリストに追加する前に、「Authentication Server Settings」画面にてホストの登録を行う必要があります。本機能を正しく動作させるためには、リモートの中央管理サーバ上でプロトコルを指定して認証サーバホストの設定を行う必要があります。

注意 あらかじめ組み込まれている4つのサーバグループには、同じTACACSデーモンが起動されているサーバホストのみを入れることができます。TACACS/ XTACACS/ TACACS+ プロトコルは別のエンティティで、互換性はありません。

Authentication Server Settings (認証サーバ設定)

本画面では、スイッチに TACACS/XTACACS/TACACS+/RADIUS セキュリティプロトコルに対応したユーザ定義の認証サーバホストを設定します。

ユーザが認証ポリシーを有効にしてスイッチにアクセスを試みると、スイッチはリモートホスト上の TACACS/XTACACS/TACACS+/RADIUS サーバホストに認証パケットを送信します。すると TACACS/XTACACS/TACACS+/RADIUS サーバホストはその要求を認証または拒否し、スイッチに適切なメッセージを返します。1つの物理ホスト上で複数の認証プロトコルを動作させることは可能ですが、TACACS/XTACACS/TACACS+/RADIUS は別のエンティティであり、互換性を持たないことに注意が必要です。サポート可能なサーバホストは最大 16 台です。

Security > Access Authentication Control > Authentication Server 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。

| IP Address | Protocol | Port | Timeout | Key | Retransmit |
|---------------|----------|------|---------|-------|------------|
| 192.168.1.111 | TACACS | 49 | 5 | ----- | 2 |

図 12-83 Authentication Server Settings 画面

以下の項目を使用して、設定を行います。

| 項目 | 説明 |
|-------------------|--|
| IP Address | 追加するリモートサーバホストの IP アドレス。 |
| Port (1-65535) | サーバホスト上で認証プロトコルに使用する仮想ポート番号 (1-65535)。ポート番号の初期値は、TACACS/XTACACS/TACACS+ サーバの場合は 49、RADIUS サーバの場合は 1812 です。独自の番号を設定してセキュリティを向上することも可能です。 |
| Protocol | サーバホストが使用するプロトコル。以下から選択します。 <ul style="list-style-type: none"> TACACS - ホストが TACACS プロトコルを使用している場合に選択します。 XTACACS - ホストが XTACACS プロトコルを使用している場合に選択します。 TACACS+ - ホストが TACACS+ プロトコルを使用している場合に選択します。 RADIUS - ホストが RADIUS プロトコルを使用している場合に選択します。 |
| Timeout (1-255) | スイッチが、サーバホストからの認証リクエストへの応答を待つ時間 (秒)。初期値は 5 (秒) です。 |
| Key | TACACS+ と RADIUS サーバの場合に指定する共有キー。254 文字までの半角英数字を入力します。 |
| Retransmit (1-20) | TACACS サーバからの応答がない場合に、デバイスが認証リクエストを再送する回数を入力します。 |

「Apply」ボタンをクリックし、サーバホストを追加します。

注意 1つの物理ホスト上で複数の認証プロトコルを動作させることは可能ですが、TACACS/XTACACS/TACACS+ は個別のエンティティであり、互換性を持たないことに注意が必要です。

エントリの編集

1. 編集するエントリの「Edit」ボタンをクリックして、以下の画面を表示します。

| IP Address | Protocol | Port | Timeout | Key | Retransmit |
|---------------|----------|------|---------|-----|------------|
| 192.168.1.111 | TACACS | 49 | 5 | 2 | Apply |

図 12-84 Authentication Server Settings 画面 - Edit

2. 指定エントリを編集して「Apply」ボタンをクリックします。

エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。

Login Method Lists Settings (ログインメソッドリスト)

本メニューでは、ユーザがスイッチにログインする際の認証方法を規定するユーザ定義または初期設定のログインメソッドリストを設定します。本メニューで設定した認証方法の順番が認証結果に影響します。例えば、ログインメソッドリストに TACACS-XTACACS-Local の順番で認証方法を指定すると、スイッチはまずサーバグループ内の 1 番目の TACACS ホストに認証リクエストを送信します。そのサーバホストから応答がない場合、2 番目の TACACS ホストに認証リクエストを送信します。このようにサーバグループ内のすべてのホストに順番に送信を試みても応答がない場合、スイッチは本メソッドリストの次の方法 (XTACACS) を試みます。それでも認証が行われなければ、スイッチ内に設定したローカルアカウントデータベースを使用して認証を行います。Local メソッドが使用される時、ユーザの権限はスイッチに設定されたローカルアカウントの権限に依存します。

これらの認証方法によって、認証に成功したユーザには「User」の権限のみが与えられます。ユーザが管理者レベルの権限を必要とするのであれば、「Enable Admin」画面にアクセスし、スイッチに管理者により事前に設定されているパスワードの入力が必要になります。

Security > Access Authentication Control > Login Method Lists Settings の順にメニューをクリックし、以下の画面を表示します。

| Method List Name | Priority 1 | Priority 2 | Priority 3 | Priority 4 | | |
|------------------|------------|------------|------------|------------|------|--------|
| default | local | ---- | ---- | ---- | Edit | Delete |
| loca_list | Auth_group | ---- | ---- | ---- | Edit | Delete |

図 12-85 Login Method Lists Settings 画面

スイッチには、あらかじめ削除できない Login Method List が登録されています。このリストの内容の変更は可能です。

Login Method List の新規登録

以下の項目を設定し、「Apply」ボタンをクリックします。

| 項目 | 説明 |
|---------------------|---|
| Method List Name | 15 文字までの半角英数字でメソッドリスト名を入力します。 |
| Priority 1, 2, 3, 4 | <p>本メソッドリストに追加する認証方法を最大 4 件まで指定します。</p> <ul style="list-style-type: none"> tacacs – リモートの TACACS サーバから TACACS プロトコルを使用してユーザ認証を行います。 xtacacs – リモートの XTACACS サーバから XTACACS プロトコルを使用してユーザ認証を行います。 tacacs+ – リモートの TACACS+ サーバから TACACS+ プロトコルを使用してユーザ認証を行います。 radius – リモートの RADIUS サーバから RADIUS プロトコルを使用してユーザ認証を行います。 server_group – スイッチ上に設定したユーザ定義のサーバグループを使用してユーザ認証を行います。 local – スイッチ上のローカルユーザアカウントデータベースを使用してユーザ認証を行います。 none – スイッチへアクセスするための認証を行います。 |

Login Method List の変更

1. 対応する「Edit」ボタンをクリックし、以下の画面を表示します。

| Method List Name | Priority 1 | Priority 2 | Priority 3 | Priority 4 | | |
|------------------|------------|------------|------------|------------|-------|--------|
| default | local | ---- | ---- | ---- | Edit | Delete |
| loca_list | Auth_grou | ---- | ---- | ---- | Apply | Delete |

図 12-86 Login Method Lists 画面 - Edit

2. 項目を編集し、「Apply」ボタンをクリックします。

ユーザ定義の Login Method List の削除

1. 削除対象のエントリの行の「Delete」ボタンをクリックします。

Enable Method Lists Settings (メソッドリストの有効化)

スイッチ上で認証メソッドを使用して、ユーザの権限をユーザレベルから管理者 (Admin) レベルに上げる際に利用するメソッドリストの設定を行います。通常のユーザレベルの権限を取得したユーザが管理者特権を得るためには、管理者が定義した方法により認証を受ける必要があります。最大 8 件の Enable Method List が登録でき、そのうちの 1 つは default Enable メソッドリストになります。本 default Enable メソッドリストは内容の変更はできますが、削除はできません。

本メニューで定義した認証方法の順番が認証結果に影響します。例えば、ログインメソッドリストに TACACS-XTACACS-Local の順番で認証方法を指定した場合、スイッチはまずサーバグループ内の 1 番目の TACACS ホストに対して、認証リクエストを送信します。認証が確認できなければ、2 番目の TACACS ホストに認証リクエストを送信します。このようにサーバグループ内のすべてのホストに順番に送信を試みても応答がない場合、スイッチは本メソッドリスト中の次の方法 (XTACACS) を試みます。それでも認証が行われなければ、スイッチ内に設定したローカル Enable パスワードを使用してユーザの認証を行います。

以上のいずれかの方法で認証されたユーザは、「Admin」(管理者) 権限を取得することができます。

注意 ローカル Enable パスワードの設定については [344 ページの「Local Enable Password Settings \(ローカルユーザパスワード設定\)」](#)の項を参照してください。

Security > Access Authentication Control > Enable Method Lists Settings の順にメニューをクリックし、以下の画面を表示します。

図 12-87 Enable Method Lists Settings 画面

以下の項目を使用して、Enable Method List の設定を行います。入力後、「Apply」ボタンをクリックします。

| 項目 | 説明 |
|---------------------|---|
| Method List Name | 15 文字までの半角英数字でメソッドリスト名を入力します。 |
| Priority 1, 2, 3, 4 | <p>本メソッドリストに追加する認証方法を最大 4 件まで指定します。</p> <ul style="list-style-type: none"> local_enable – スイッチ上のローカル Enable パスワードデータベースを使用してユーザ認証を行います。Local enable password は次セクションの 344 ページの「Local Enable Password Settings (ローカルユーザパスワード設定)」を参照し、設定してください。 none – スイッチへアクセスするための認証を行います。 radius – リモートの RADIUS サーバから RADIUS プロトコルを使用してユーザ認証を行います。 tacacs – リモートの TACACS サーバから TACACS プロトコルを使用してユーザ認証を行います。 xtacacs – リモートの XTACACS サーバから XTACACS プロトコルを使用してユーザ認証を行います。 tacacs+ – リモートの TACACS+ サーバから TACACS+ プロトコルを使用してユーザ認証を行います。 server_group – スイッチ上に設定したユーザ定義のサーバグループを使用してユーザ認証を行います。 |

メソッドリストの作成

- メソッドリスト名を「Method List Name」に入力し、認証方法を「Priority 1-4」に設定します。
- 「Apply」ボタンをクリックして設定を適用します。

ユーザ定義の Enable メソッドリストの削除

対象の行で「Delete」ボタンをクリックします。

メソッドリストの変更

1. 対応するメソッドリスト名の「Edit」ボタンをクリックし、以下の画面を表示します。

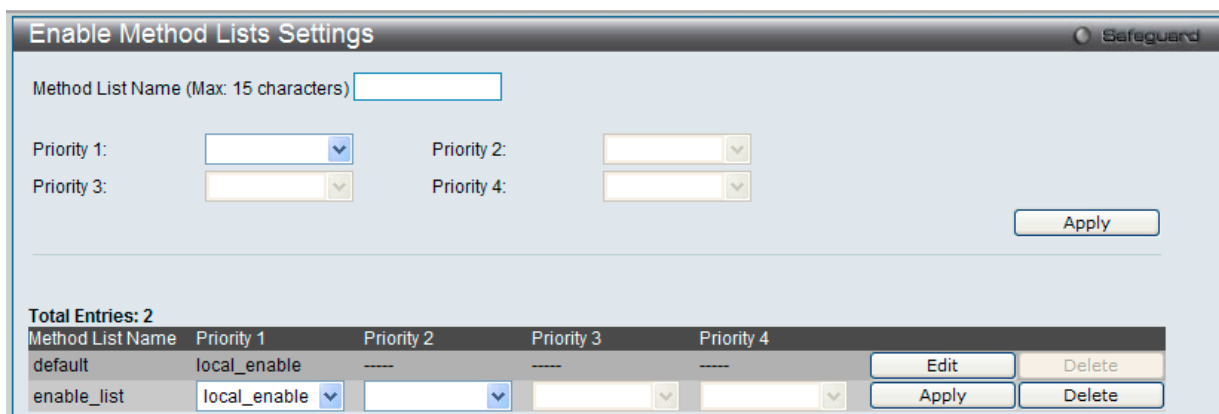


図 12-88 Enable Method Lists 画面 - Edit

2. 項目を編集後、エントリの「Apply」ボタンをクリックします。

Accounting Method Lists Settings (アカウントिंगメソッドリスト設定)

スイッチ上でアカウントिंगメソッドリストの作成を行います。

Security > Access Authentication Control > Accounting method Lists Settings の順にメニューをクリックし、以下の画面を表示します。

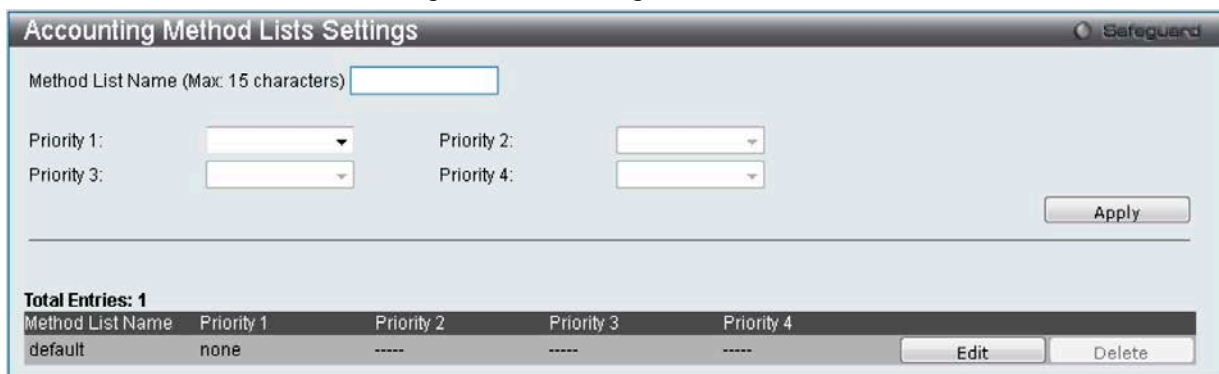


図 12-89 Accounting method Lists Settings 画面

以下の項目を使用して、「Accounting Method List」の設定を行います。

| 項目 | 説明 |
|---------------------|--|
| Method List Name | 15 文字までの半角英数字でメソッドリスト名を入力します。 |
| Priority 1, 2, 3, 4 | 本メソッドリストに追加する認証方法を最大 4 件まで指定します。 <ul style="list-style-type: none"> • none - アカウントिंगを必要としないパラメータです。 • radius - リモートの RADIUS サーバから RADIUS プロトコルを使用してユーザ認証を行います。 • tacacs+ - リモートの TACACS+ サーバから TACACS+ プロトコルを使用してユーザ認証を行います。 |

入力後、「Apply」ボタンをクリックします。

Local Enable Password Settings (ローカルユーザパスワード設定)

本画面では、「Enable Admin」コマンド用の Local Enable Password を設定します。ユーザがその権限をユーザレベルから管理者レベルに変更する際の認証方法に、「local_enable」を選択している場合、本画面でスイッチに登録したパスワードの入力が要求されます。

Security > Access Authentication Control > Local Enable Password Settings の順にメニューをクリックし、以下の画面を表示します。

図 12-90 Local Enable Password Settings 画面

以下の項目を使用して、Local Enable Password を設定します。入力が完了後、「Apply」ボタンをクリックします。

| 項目 | 説明 |
|-------------------------------|---|
| Encryption | パスワードに使用する暗号化タイプを指定します。 <ul style="list-style-type: none"> Plain Text - プレーンテキスト形式でパスワードを指定します。 SHA1 - SHA-1 暗号化形式でパスワードを指定します。 |
| Old Local Enable Password | 登録済みのパスワードがある場合は、新しいパスワードに変更するために入力します。 |
| New Local Enable Password | スイッチの管理者レベルでアクセスを試みるユーザの認証に使用する（新しい）パスワードを入力します。15文字までの半角英数字を使用します。 |
| Confirm Local Enable Password | 確認のため、上記の新パスワードを再度入力します。先に入力したものと異なると、エラーメッセージが表示されます。 |
| Local Enable | 「Encryption」オプションの1つを選択後に、使用するローカルパスワードを入力します。 |

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

Authentication Source IP Interface Settings (認証送信元 IP インタフェース設定)

本画面ではすべての送信 RADIUS パケットと TACACS パケットの送信元インタフェースの設定をします。

Security > Access Authentication Control > Authentication Source IP Interface Settings の順にメニューをクリックし、以下の画面を表示します。

図 12-91 Authentication Source IP Interface Settings 画面

以下の項目を使用して設定します。

| 項目 | 説明 |
|----------------|--|
| Interface Name | 送信 RADIUS パケットと TACACS パケットの送信元インタフェース名を指定します。 |
| IPv4 Address | 送信 RADIUS パケットと TACACS パケットの送信元 IPv4 アドレスを指定します。 |

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

SSL Settings (Secure Socket Layer の設定)

Secure Sockets Layer (SSL) とは、認証、デジタル署名および暗号化を使用して、ホストとクライアント間に安全な通信パスを提供するセキュリティ機能です。このセキュリティ機能は、認証セッションに使用する厳密な暗号パラメータ、特定の暗号化アルゴリズムおよびキー長を決定する、暗号スイートと呼ばれるセキュリティ文字列により実現しています。SSL は、以下の 3 つの段階で構成されます。

1. 鍵交換

暗号スイート文字列の最初の部分では、使用する公開鍵アルゴリズムを規定しています。本スイッチは、RSA (Rivest Shamir Adleman) 公開鍵アルゴリズムとデジタル署名アルゴリズム (DHE : DHE DSS Diffie-Hellman 公開鍵アルゴリズムとして指定) を使用します。本レベルは、鍵を交換して適合する相手を探し、暗号化のネゴシエーションを行うまでの認証を行って、次のレベルに進むというクライアント、ホスト間の最初のプロセスとなります。

2. 暗号化

暗号スイートの次の段階は、クライアントとホスト間で送受信するメッセージの暗号化を含む暗号化方式です。本スイッチは 2 種類の暗号化アルゴリズムをサポートしています。

- ストリーム暗号 - スイッチは 2 種類のストリーム暗号に対応します。1 つは 40 ビット鍵での RC4、もう 1 つは 128 ビット鍵での RC4 です。これらの鍵はメッセージの暗号化に使用され、最適な使用のためにはクライアントとホスト間で一致させる必要があります。
- CRC ブロック暗号 - CBC (Cipher Block Chaining : 暗号ブロック連鎖) とは、前に暗号化したブロックの暗号文を使用して現在のブロックの暗号化を行う方法です。本スイッチは、DES (Data Encryption Standard) で定義する 3 DES EDE 暗号化コードをサポートし、暗号文を生成します。

3. ハッシュアルゴリズム

暗号スイートの最後の段階では、メッセージ認証コードを決定するメッセージダイジェスト機能を規定します。このメッセージ認証コードは送信されたメッセージで暗号化され、整合性を提供し、リプレイアタックを防止します。本スイッチは、MD5 (Message Digest 5) と SHA (Secure Hash Algorithm) の 2 種類のハッシュアルゴリズムをサポートします。

これら 3 つのパラメータは、スイッチ上での 4 つの選択肢として独自に組み合わせられ、サーバとホスト間で安全な通信を行うための 3 層の暗号化コードを生成します。暗号スイートの中から 1 つ、または複数を組み合わせて実行することができますが、選択する暗号スイートによりセキュリティレベルや安全な接続時のパフォーマンスは変化します。暗号スイートに含まれる情報はスイッチには存在していないため、証明書と呼ばれるファイルを第三者機関からダウンロードする必要があります。この証明書ファイルがないと本機能をスイッチ上で実行することができません。証明書ファイルは、TFTP サーバを使用してスイッチにダウンロードできます。本スイッチは、SSLv3 および TLSv1/v2/v3 をサポートしています。SSL の他のバージョンは本スイッチとは互換性がないおそれがあり、クライアントからホストへの認証やメッセージ送信時に問題が発生する場合があります。

証明書のダウンロード (Download Certificate)

本画面では、SSL を使用するための証明書ファイルを TFTP サーバからダウンロードします。証明書ファイルは、ネットワーク上のデバイスを認証するために使われるデータであり、所有者の情報や認証のための鍵やデジタル署名などの情報が格納されています。SSL 機能を最大限に活用するためには、サーバとクライアントが一致した証明書ファイルを持つ必要があります。スイッチは、拡張子 ".der" を持つ証明書のみをサポートします。スイッチは証明書が既にロードされている形で発送されますが、ユーザの環境によっては、さらにダウンロードが必要になる場合があります。

暗号スイート

「SSL Configuration Settings」画面では、ネットワークマネージャが SSL を有効にしてスイッチに暗号スイートを設定できます。暗号スイートは認証セッションに使用する、正確な暗号のパラメータ、特定の暗号化アルゴリズム、および鍵のサイズを決定する文字列です。スイッチは SSL 機能のための 4 つの暗号スイートを持ち、初期設定ではすべてを有効にしていますが、特定の暗号スイートのみ有効にして、他のものを無効にすることも可能です。

SSL 機能が有効になると、Web の使用はできなくなります。SSL 機能を使用しながら Web ベースの管理を行うためには、Web ブラウザが SSL 暗号化をサポートし、<https://> で始まる URL を使用しなければなりません。(例 : <https://10.90.90.90>) これを守らないと、エラーが発生し、Web ベースの管理機能にアクセスできなくなります。

Security > SSL の順にメニューをクリックし、以下の画面を表示します。

図 12-92 SSL Settings 画面

SSL 機能の設定

「SSL Global Settings」セクションの項目を設定し、「Apply」ボタンをクリックします。

SSL 暗号スイート機能の設定

「SSL Ciphersuite Settings」セクションの項目を設定し、「Apply」ボタンをクリックします。

SSL 証明書のダウンロード

「SSL Certificate Download」セクションの項目を設定し、「Download」ボタンをクリックします。

| 項目 | 説明 |
|----------------------------------|---|
| SSL Global Settings | |
| SSL State | スイッチの SSL の「Enabled」(有効)、「Disabled」(無効)を指定します。初期値は「Disabled」です。 |
| SSL 3.0/TLS1.0/TLS1.1/ TLS1.2 | SSL/TLS の各バージョンについて「Enabled」(有効)、「Disabled」(無効)を指定します。 |
| Cache Timeout (60-86400) | クライアントとホストの間の SSL による新しい鍵交換の間隔を指定します。クライアントとホストが鍵交換を すると常に新しい SSL セッションが確立します。この値を長くすると SSL セッションによる特定のホストとの 再接続には主鍵が再利用されます。そのためネゴシエーション処理は速くなります。初期値は 600 (秒) です。 |
| SSL Ciphersuite Settings | |
| SSL Ciphersuite Settings | 各暗号スイートの「Enabled」(有効)、「Disabled」(無効)を指定します。 |
| SSL Certificate Download | |
| Server IP Address | 証明書のファイルがある TFTP サーバの IP アドレスを指定します。 |
| Certificate File Name | ダウンロードする証明書のパスとファイル名を指定します。ファイルには拡張子 ".der" が必要です。(例 c:/cert.der) |
| Key File Name | ダウンロードする鍵ファイルのパスとファイル名を指定します。ファイルには拡張子 ".der" が必要です。(例 c:/ pkey.der) |

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

注意 SSL の機能と構成に関するいくつかの機能は本スイッチの Web ベースマネジメントでは利用できません。

注意 SSL 機能が有効になると Web ベースマネジメントは無効になります。再度本スイッチにログオンするには URL の最初を <https://> で始まるアドレスを Web ブラウザのアドレスに指定してもエラーになり、認証はされません。

SSL Certification Settings (SSL 証明書設定)

SSL 証明書の設定を行います。

Security > SSL > SSL Certification Settings の順にメニューをクリックし、以下の画面を表示します。

図 12-93 SSL Certification Settings 画面

以下の項目を使用して、参照または設定を行います。

| 項目 | 説明 |
|-----------------------------|---|
| SSL Certification File Name | プルダウンメニューを使用して、SSL 証明書名を選択します。 |
| SSL CA Chain Configuration | スイッチにおける証明書のチェーンを入力します。「Default」ボタンをクリックすると、実装されている証明書を使用します。 |
| SSL Certificate File Name | 削除する SSL 証明書ファイル名を入力します。 |

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

「Delete」ボタンをクリックして、指定エントリを削除します。

SSH (Secure Shell の設定)

SSH (Secure Shell) は、安全性の低いネットワーク上で、安全なリモートログインと安全なネットワークサービスを実現するためのプログラムです。SSH は、リモートのホストコンピュータへの安全なログインや、リモートのエンドノードでの安全なコマンド実行メソッドを可能にし、信頼関係を結んでいないホスト間に暗号化と認証を利用した安全な通信を提供します。高度なセキュリティ機能を備えた SSH は、今日のネットワーク環境に必要不可欠なツールです。ネットワーク通信を脅かす数々のセキュリティハザードに対して、強力な監視者としての役割を担います。

リモート PC (SSH クライアント) とスイッチ (SSH サーバ) 間でセキュアな通信を行うための SSH プロトコルの設定は、以下の手順で行います。

1. **System Configuration > User Accounts** で管理者レベルのアクセス権を持つアカウントを作成します。本手順はスイッチに管理者レベルのユーザアカウントを作成する方法と同じで、パスワードの設定を含みます。本パスワードは、SSH プロトコルを使用した安全な通信経路が確立された後、スイッチにログインする際に使用します。
2. 「SSH User Authentication Lists」画面を使用して、ユーザアカウントを設定します。この時スイッチが SSH 接続の確立を許可する際のユーザの認証方法を指定します。この認証方法には、「Host-based」、「Password」、「Public Key」の 3 つがあります。
3. 「SSH Authentication Method and Algorithm Settings」画面を使用して、SSH クライアントとサーバ間で送受信するメッセージの暗号化、復号化に用いる暗号化アルゴリズムを設定します。
4. 最後に「SSH Settings」画面で、SSH を有効にします。

これらの手順が完了後、安全な帯域内の接続でスイッチの管理を行うために、リモート PC 上の SSH クライアントの設定を行います。

SSH Settings (SSH サーバ設定)

本画面は SSH サーバの設定および設定内容の確認に使用します。

Security > SSH > SSH Settings の順にメニューをクリックします。

図 12-94 SSH Settings 画面

以下の項目を使用して、SSH サーバの設定を行います。

| 項目 | 説明 |
|---|--|
| SSH Global Settings | |
| SSH Server State | スイッチ上で SSH 機能を「Enabled」(有効) / 「Disabled」(無効) にします。初期値は「Disabled」です。 |
| Max. Session (1-8) | 同時にスイッチに接続できる数を 1 から 8 の数字を設定します。初期値は 8 です。 |
| Connection Timeout (30-600) | 接続のタイムアウト時間を指定します。30 から 600 (秒) が指定できます。初期値は 120 (秒) です。 |
| Authfail Attempts (2-20) | ユーザが SSH サーバに対して認証を試みることができる回数を指定します。指定した回数を超えるとスイッチは接続を切り、ユーザは再度スイッチに接続する必要があります。2 から 20 が指定できます。初期値は 2 です。 |
| Rekey Timeout | スイッチが SSH 鍵の再交換を行う間隔をプルダウンメニューから選択します。「Never」、「10 min」、「30 min」、「60 min」です。初期値は「Never」(鍵再交換を行わない) です。 |
| TCP Port Number (1-65535) | SSH に使用する TCP 番号を入力します。初期値は 22 です。 |
| Bypass Login Screen State | SSH 鍵認証後、再びのユーザ名 / パスワードの認証要求を避けるために指定します。設定されると SSH 公共鍵を使用するログインユーザは初期権限レベルでコマンドを実行することができます。 |
| Download and Upload SSH Public Key | |
| File Name | TFTP プロトコルを使用してクライアントコンピュータの SSH 公共鍵をスイッチにダウンロードします。「Browse (参照)」をクリックして鍵ファイルの場所を指定し「Download」をクリックします。 |

| 項目 | 説明 |
|-----------------------|---|
| Upload SSH Public Key | 「Upload SSH Public Key」をクリックしFTP プロトコルを使用してスイッチのSSH 公開鍵をコンピュータにアップロードします。 |

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

SSH Authentication Method and Algorithm Settings (SSH 認証モードとアルゴリズム設定)

認証および暗号化に使用する SSH アルゴリズムの種類を設定します。アルゴリズムはカテゴリに分けてリスト表示され、各アルゴリズムは対応するチェックボックスを使用して有効、無効に設定できます。すべてのアルゴリズムは初期値で有効です。

Security > SSH > SSH Authentication mode and Algorithm Settings の順にメニューをクリックし、以下の画面を表示します。

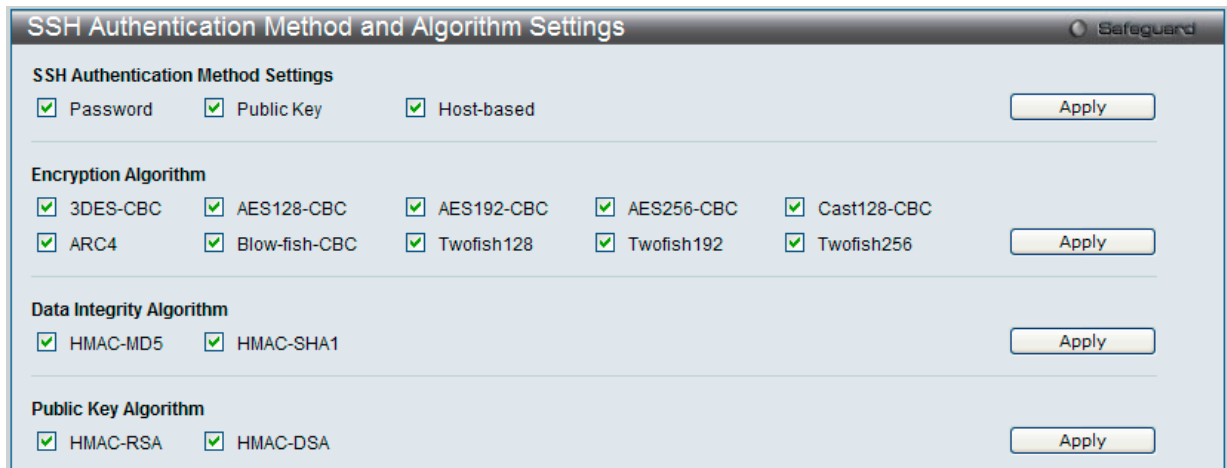


図 12-95 SSH Authentication Method and Algorithm Settings 画面

以下のアルゴリズムが設定できます。

| 項目 | 説明 |
|----------------------------------|---|
| SSH Authentication Mode Settings | |
| Password | スイッチにおける認証にローカルに設定したパスワードを使用する場合に「Enabled」(有効) にします。初期値は「Enabled」です。 |
| Public Key | スイッチにおける認証に SSH サーバに設定した公開鍵を使用する場合に「Enabled」(有効) にします。初期値は「Enabled」です。 |
| Host-based | 認証にホストコンピュータを使用する場合に「Enabled」(有効) にします。本項目は SSH 認証機能を必要とする Linux ユーザ向けに設定されます。ホストコンピュータには SSH プログラムがインストールされ、Linux OS が起動している必要があります。初期値は「Enabled」です。 |
| Encryption Algorithm | |
| 3DES-CBC | CBC 方式で 3DES 暗号化アルゴリズムを「Enabled」(有効) / 「Disabled」(無効) にします。初期値は「Enabled」です。 |
| Blow-fish-CBC | CBC 方式で Blowfish 暗号化アルゴリズムを「Enabled」(有効) / 「Disabled」(無効) にします。初期値は「Enabled」です。 |
| AES128-CBC | CBC 方式で AES128 暗号化アルゴリズムを「Enabled」(有効) / 「Disabled」(無効) にします。初期値は「Enabled」です。 |
| AES192-CBC | CBC 方式で AES192 暗号化アルゴリズムを「Enabled」(有効) / 「Disabled」(無効) にします。初期値は「Enabled」です。 |
| AES256-CBC | CBC 方式で AES256 暗号化アルゴリズムを「Enabled」(有効) / 「Disabled」(無効) にします。初期値は「Enabled」です。 |
| ARC4 | ARC4 暗号化アルゴリズムを「Enabled」(有効) / 「Disabled」(無効) にします。初期値は「Enabled」です。 |
| Cast128-CBC | CBC 方式で Cast128 暗号化アルゴリズムを「Enabled」(有効) / 「Disabled」(無効) にします。初期値は「Enabled」です。 |
| Twofish128 | Twofish128 暗号化アルゴリズムを「Enabled」(有効) / 「Disabled」(無効) にします。初期値は「Enabled」です。 |
| Twofish192 | Twofish192 暗号化アルゴリズムを「Enabled」(有効) / 「Disabled」(無効) にします。初期値は「Enabled」です。 |
| Twofish256 | Twofish256 暗号化アルゴリズムを「Enabled」(有効) / 「Disabled」(無効) にします。初期値は「Enabled」です。 |
| Data Integrity Algorithm | |
| HMAC-SHA1 | SHA1 (セキュアハッシュ) 暗号化アルゴリズムを使用した HMAC メカニズムを「Enabled」(有効) / 「Disabled」(無効) にします。初期値は「Enabled」です。 |
| HMAC-MD5 | MD5 (メッセージダイジェスト) 暗号化アルゴリズムを使用した HMAC メカニズムを「Enabled」(有効) / 「Disabled」(無効) にします。初期値は「Enabled」です。 |
| Public Key Algorithm | |
| HMAC-RSA | RSA 暗号化アルゴリズムを使用した HMAC メカニズムを「Enabled」(有効) / 「Disabled」(無効) にします。初期値は「Enabled」です。 |
| HMAC-DSA | DSA (デジタル署名) 暗号化アルゴリズムを使用した HMAC メカニズムを「Enabled」(有効) / 「Disabled」(無効) にします。初期値は「Enabled」です。 |

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

SSH User Authentication Lists (SSH ユーザ認証リスト)

SSH を使用してスイッチにアクセスを行うユーザの設定を行います。

Security > SSH > SSH User Authentication Lists の順にメニューをクリックし、以下の画面を表示します。

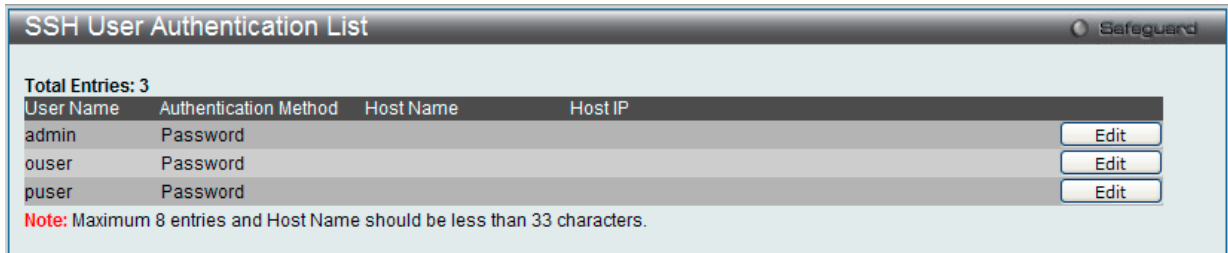


図 12-96 SSH User Authentication List 画面

上記画面例のユーザアカウントは **System Configuration > User Accounts** で既に設定されているものとします。SSH ユーザとしての項目を設定するためには、ユーザアカウントをあらかじめ登録しておく必要があります。

SSH ユーザの設定

SSH ユーザとしての項目を設定するためには、本画面で対応するエントリの「Edit」ボタンをクリックし、以下の画面を表示します。

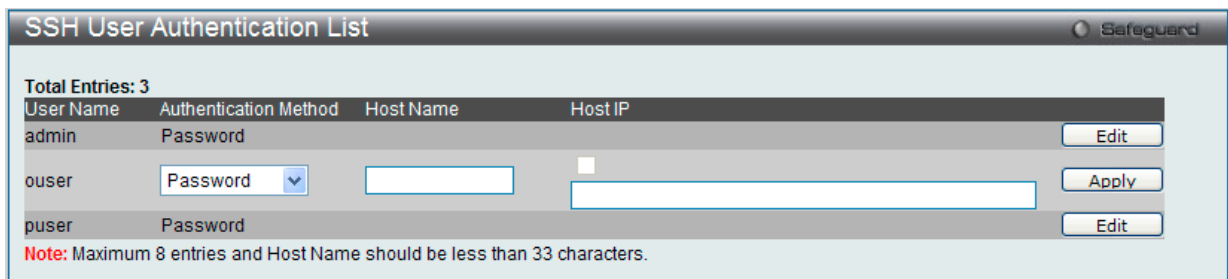


図 12-97 SSH User Authentication Lists 画面 - Edit

以下の項目を使用して、参照または設定を行います。

| 項目 | 説明 |
|-----------------------|---|
| User Name | SSH ユーザを識別するユーザ名を 15 文字までの半角英数字で指定します。本ユーザ名はスイッチにユーザアカウントとして登録済みである必要があります。 |
| Authentication Method | スイッチにアクセスを試みるユーザの認証モードを以下から指定します。 <ul style="list-style-type: none"> Host-Based - 認証用にリモート SSH サーバを使用する場合に選択します。本項目を選択すると、SSH ユーザ識別のために以下の情報を入力することが必要になります。 <ul style="list-style-type: none"> Host Name - リモート SSH ユーザを識別する 31 文字までの半角英数字を入力します。 Host IP - SSH ユーザの IP アドレスを入力します。 Password - 管理者定義のパスワードを使用して認証を行う場合に選択します。本項目を選択すると、スイッチは管理者にパスワードの入力（確認のため 2 回）を促します。 Public Key - SSH サーバ上の公開鍵を使用して認証を行う場合に選択します。 |
| Host Name | リモート SSH ユーザを識別する 32 文字までの半角英数字を入力します。本項目は「Auth. Mode」で「Host-Based」を選択した場合のみ入力が必要です。 |
| Host IP | SSH ユーザの IP アドレスを入力します。本項目は「Auth. Mode」で「Host-Based」を選択した場合のみ入力が必要です。 |

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

注意 SSH User Authentication Mode の項目を設定するためには、事前にユーザアカウントを登録しておく必要があります。スイッチのローカルユーザアカウント設定に関する詳しい情報に関しては、本マニュアルの [66 ページの「User Accounts Settings \(ユーザアカウントの設定\)」](#) を参照してください。

DoS Attack Prevention Settings (DoS 攻撃防止設定)

各 DoS 攻撃に対して防御設定を行います。パケット照合はハードウェアで行われます。特定タイプの攻撃に対しては、パケットの内容を特定パターンと照合します。

Security > DoS Attack Prevention Settings の順にメニューをクリックし、以下の画面を表示します。

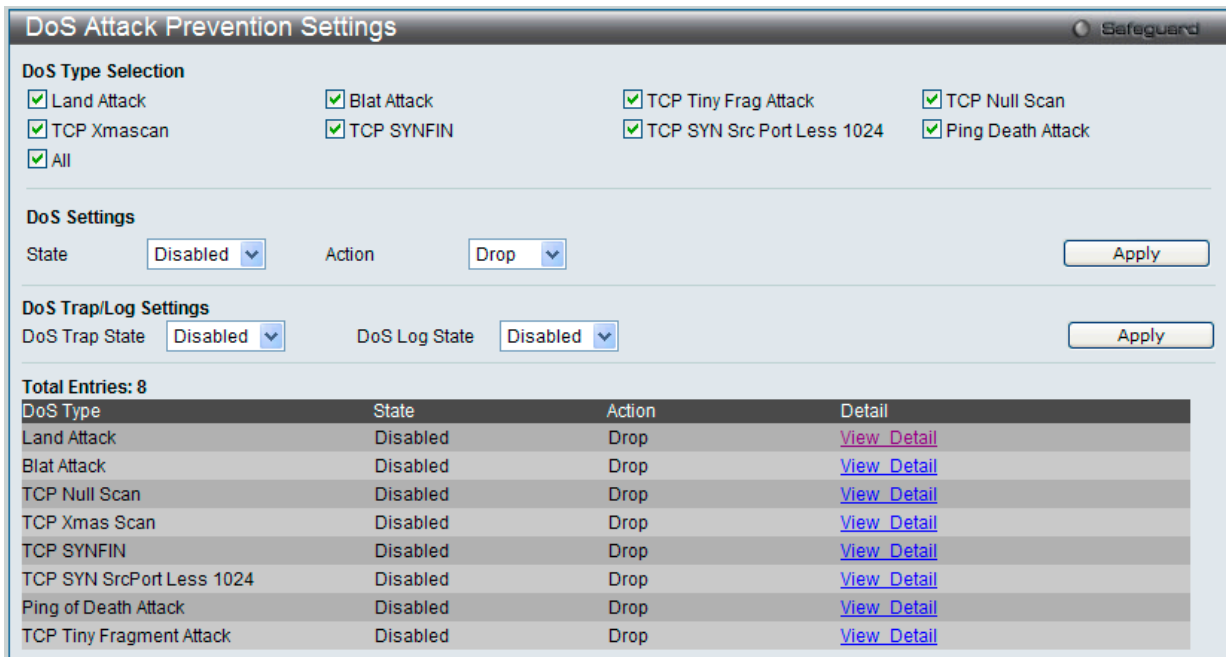


図 12-98 DoS Attack Prevention Settings 画面

設定および表示する項目は以下の通りです。

| 項目 | 説明 |
|-----------------------|---|
| DoS Type Selection | 適切な DoS 攻撃防御のタイプを選択します。 <ul style="list-style-type: none"> Land Attack - DoS 攻撃防止タイプに LAND 攻撃を指定します。 Blat Attack - DoS 攻撃防止タイプに BLAT 攻撃を指定します。 TCP Tiny Frag Attack - DoS 攻撃防止タイプに TCP Tiny Frag 攻撃を指定します。 TCP Null Scan - DoS 攻撃防止タイプに TCP Null Scan 攻撃を指定します。 TCP Xmascan - DoS 攻撃防止タイプに TCP Xmascan 攻撃を指定します。 TCP SYNFIN - DoS 攻撃防止タイプに TCP SYNFIN 攻撃を指定します。 TCP SYN Src Port Less 1024 - DoS 攻撃防止タイプに TCP SYN Source Port Less 1024 攻撃を指定します。 Ping Death Attack - DoS 攻撃防止タイプに Ping Death Attack 攻撃を指定します。 All - DoS 攻撃防止タイプにすべての攻撃を指定します。 |
| DoS Settings | |
| State | DoS 攻撃防止の状態を指定します。 <ul style="list-style-type: none"> Enabled - DoS 攻撃防止の状態を有効にします。 Disabled - DoS 攻撃防止の状態を無効にします。 |
| Action | DoS 攻撃防止機能により行われる操作を無効にします。 <ul style="list-style-type: none"> Drop - 一致する DoS 攻撃パケットをすべて破棄します。 |
| DoS Trap/Log Settings | |
| DoS Trap State | 本オプションは、DoS 防止トラップ状態を有効または無効にします。 |
| DoS Log State | DoS 防止ログ状態を有効または無効にします。 |

詳細情報の表示

「DoS Type」の横に表示される「[View Detail](#)」リンクをクリックすると、以下の画面が表示されます。



図 12-99 DoS Attack Prevention Detail 画面

「<<Back」をボタンをクリックして前のページに戻ります。

Trusted Host Settings (トラストホスト)

最大 30 個までのトラストホストのセキュアな IP アドレスが、リモートのスイッチ管理のために設定され、使用できます。1 個以上のトラストホストが使用可能な状態にあると、スイッチは直ちに指定 IP アドレスからのリモートアクセスのみ許可することにご注意ください。この機能を有効にする場合、はじめに現在使用している IP アドレスを入力してください。

Security > Trusted Host Settings の順にクリックし、以下の画面を表示します。

図 12-100 Trusted Host Settings 画面

以下の項目を使用して、参照または設定を行います。

| 項目 | 説明 |
|------------------|---------------------------------|
| IPv4 Address | IPv4 アドレスを入力してトラストホストリストに追加します。 |
| IPv6 Address | IPv6 アドレスを入力してトラストホストリストに追加します。 |
| Net Mask | ネットマスクを入力してトラストホストリストに追加します。 |
| Access Interface | トラストホストに許可するサービスを選択します。 |

「Add」ボタンをクリックして、入力した情報に基づいて新しいエントリを追加します。

エントリの編集

1. 編集するエントリの「Edit」ボタンをクリックして、以下の画面を表示します。

図 12-101 Trusted Host 画面 - Edit

2. 指定エントリを編集して「Apply」ボタンをクリックします。

エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。「Delete All」ボタンをクリックして、表示されたすべてのエントリを削除します。

Safeguard Engine Settings (セーフガードエンジン設定)

ネットワーク上の悪意のあるホストがスイッチに対して、パケットフラッディング (ARP ストーム) などを利用して、周期的に攻撃してくることがあります。これらの攻撃はスイッチに能力以上の負荷を加える可能性があります。このような問題を軽減するために、本スイッチのソフトウェアにセーフガードエンジン機能を付加しました。

セーフガードエンジンは、攻撃が行われている間、スイッチの稼働を最小化して、スイッチ全体の操作性を保ち、限られたリソース内で必要不可欠なパケットの送受信を可能にします。セーフガードエンジンには、Strict と Fuzzy の 2 つの操作モードがあります。「Strict」モードでは、スイッチが (a) 処理能力を超えた量のパケットを受信した場合、または (b) メモリ使用率が高すぎる場合には、「Exhausted」モードに遷移します。本モードでは、スイッチは算出された間隔で、すべての ARP と IP ブロードキャストパケットを廃棄します。スイッチは 5 秒おきにパケットフラッディングが発生していないかチェックをします。パケット数がしきい値を超えると、スイッチはまず、すべての入力 ARP および IP ブロードキャストパケットを 5 秒間停止させます。その 5 秒後に、スイッチは再びパケットの入力フローをチェックします。フラッディングが解消されていれば、スイッチは再びすべてのパケットを受信し始めます。逆に、まだフラッディングが認められれば、前回の 2 倍の時間 (10 秒)、すべての入力 ARP および IP ブロードキャストパケットを停止させます。パケットの停止時間は、最大時間 (320 秒) に達するまで倍増していき、それ以降は、通常の入力フローに戻るまで 320 秒で行われます。このしくみを以下に例示します。

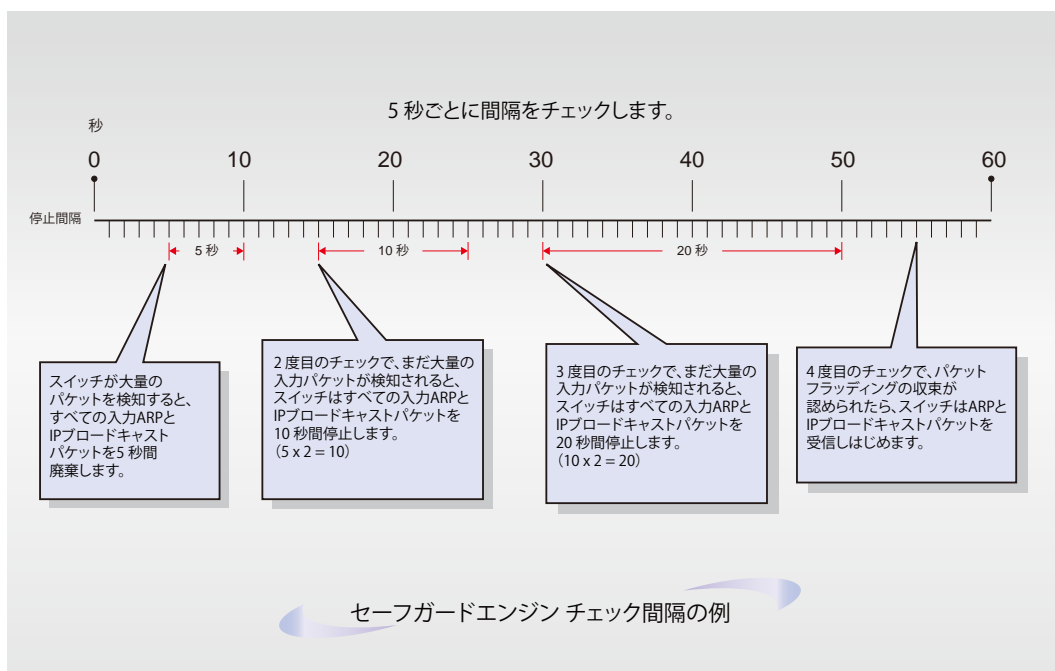


図 12-102 セーフガードエンジンの例

パケットのフラッディングの問題を軽減するためにすべての継続したチェック間隔に対してスイッチは、信頼できない IP アドレスからの受信 ARP および IP ブロードキャストパケットを破棄する時間を倍にします。上の例題では継続したパケットのフラッディング問題が 5 秒間隔で検出された場合は ARP および IP ブロードキャストパケットを破棄する時間を倍にしています。(最初の破棄 = 5 秒、2 回目の破棄 = 10 秒、3 回目の破棄 = 20 秒) パケットのフラッディングを検出しなくなると ARP および IP ブロードキャストパケットを破棄する間隔を 5 秒に戻してプロセスを再開します。

Fuzzy モードでは、一度セーフガードエンジンは Exhausted モードになると、パケットフローは本モード開始時の半分のレベルまで減少させます。Normal モードに戻ると、パケットを 25% ずつ増加させます。スイッチは、その後間隔をチェックし、スイッチのオーバーロードを避けるように動的に通常のパケットフローに戻します。

注意 セーフガードエンジンが有効の場合、本スイッチは FFP (Fast Filter Processor) メータリングテーブルを使用し、各トラフィックフロー (ARP、IP) に帯域を割り当て、CPU 使用率を制御することでトラフィックを制限します。これは、ネットワーク上のトラフィックのルーティング速度を制限します。

スイッチのセーフガードエンジン機能の有効化およびセーフガードエンジンの設定を行います。

Security > Safeguard Engine Settings の順にクリックし、以下の画面を表示します。

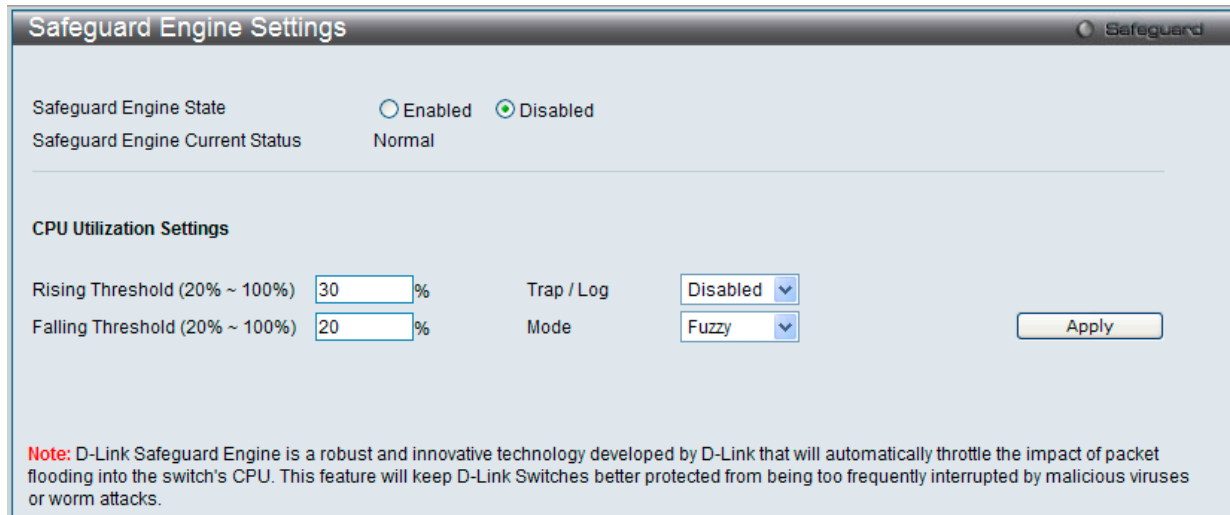


図 12-103 Safeguard Engine Settings 画面

セーフガードエンジンオプションの有効化

「Safeguard Engine State」を「Enabled」にします。

高度なセーフガードエンジン設定

以下の項目を設定し、「Apply」をクリックします。

| 項目 | 説明 |
|---------------------------------|--|
| Safeguard Engine State | セーフガードエンジン機能を「Enabled」(有効) / 「Disabled」(無効) にします。 |
| Safeguard Engine Current Status | 現在のセーフガードエンジンの状態を表示します。 |
| Rising Threshold (20% ~ 100%) | Safeguard Engine を有効にする前に許容可能な CPU 使用率のレベルを設定します。CPU 使用率がこのしきい値に到達すると、ここで設定した項目に基づいて、Exhausted モードに入ります。 |
| Falling Threshold (20% ~ 100%) | 許容可能な CPU 使用率のレベルを設定します。スイッチは CPU 使用率がこのしきい値に到達すると Safeguard Engine 状態から Normal モードに戻ります。 |
| Trap/Log | CPU 使用率が高くなりセーフガードエンジン機能が作動した際にデバイスの SNMP エージェントとスイッチのログにメッセージを送信する機能を「Enabled」(有効) / 「Disabled」(無効) にします。 |
| Mode | CPU 高使用率に到達した際に起動する Safeguard Engine のタイプを選択します。 <ul style="list-style-type: none"> Fuzzy - 本機能はすべてのトラフィックフローに対し平等に動的な帯域割り当てを行うことで CPU に対する IP と ARP トラフィックフローを最小化します。(初期値) Strict - 本機能はストームがおさまるまで本スイッチ行きではないすべての ARP パケットの受信をストップし、不必要なブロードキャスト IP パケットの受信をストップします。 |

SFTP Server Settings (SFTP サーバ設定)

本画面では SFTP 機能を設定します。「SFTP over SSH2」はすべてのファイル操作に安全性を提供するセキュアなファイル送信プロトコルです。SFTP サーバは SSH サーバのサブシステムとして動作します。SSH サーバは SFTP サーバを起動させる前に有効にする必要があります。

Security > SFTP Server Settings の順にクリックし、以下の画面を表示します。

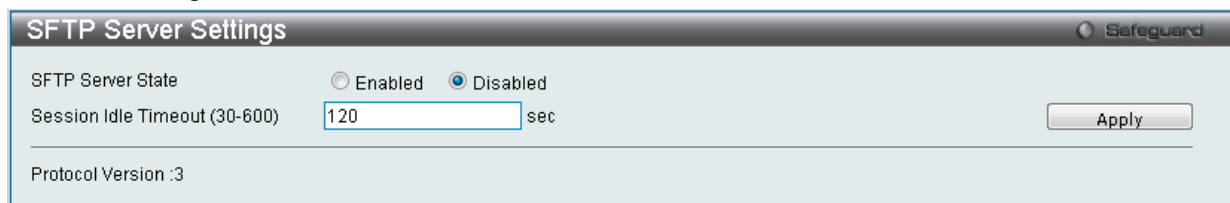


図 12-104 SFTP Server Settings 画面

以下の項目を使用して、参照または設定を行います。

| 項目 | 説明 |
|-------------------------------|--|
| SFTP Server State | SFTP サーバを有効 / 無効にします。 |
| Session Idle Timeout (30-600) | SFTP サーバセッションのアイドルタイムアウトの時間を指定します。30 から 600 (秒) の間で指定できます。初期値は 120 です。 |

「Add」ボタンをクリックして、設定を有効にします。

第 13 章 Network Application (ネットワークアプリケーション)

以下は Network Application サブメニューの説明です。
必要に応じて、設定 / 変更 / 修正を行ってください。

| サブメニュー | 説明 | 参照ページ |
|--|--|---------------------|
| DHCP (DHCP 設定) | DHCP リレーの設定を行います。以下のメニューがあります。 DHCP Relay (DHCP リレー)、DHCP Server (DHCP サーバ)、DHCPv6 Server (DHCPv6 サーバ設定)、DHCPv6 Relay (DHCPv6 リレー)、DHCP Local Relay Settings (DHCP ローカルリレー設定) | 367 |
| DNS (ドメインネームシステム) | DNS リレーの設定を行います。以下のメニューがあります。 DNS Relay (DNS リレー) | 386 |
| DNS Resolver (DNS リゾルバ) | DNS リゾルバの設定を行います。以下のメニューがあります。 DNS Resolver Global Settings (DNS リゾルバグローバル設定)、DNS Resolver Static Name Server Settings (DNS リゾルバスタティックネームサーバ設定)、DNS Resolver Dynamic Name Server Table (DNS リゾルバダイナミックネームサーバテーブル)、DNS Resolver Static Host Name Settings (DNS リゾルバスタティックホスト名設定)、DNS Resolver Dynamic Host Name Table (DNS リゾルバダイナミックホスト名テーブル) | 388 |
| RCP Server Settings (RCP サーバ設定) | RCP サーバの設定を行います。 | 390 |
| SMTP Settings (SMTP 設定) | スイッチのイベントを送信する SMTP サーバを設定します。 | 391 |
| SNTP (SNTP 設定) | 本製品に時刻設定をします。以下のメニューがあります。 SNTP Settings (SNTP 設定)、Time Zone Settings (タイムゾーン設定) | 393 |
| UDP (UDP 設定) | UDP 送信先ポートに応じて、特定のブロードキャストをサーバに送信します。以下のメニューがあります。 UDP Helper (UDP ヘルパー) | 396 |
| Flash File System Settings (フラッシュファイルシステム設定) | フラッシュファイルシステムを利用したファイル操作を行います。 | 398 |

DHCP (DHCP 設定)

DHCP Relay (DHCP リレー)

DHCP Relay Global Settings (DHCP リレーグローバル設定)

DHCP リレーグローバル設定の有効化および設定を行うことができます。

DHCP メッセージが中継される最大のホップ (ルータの) 数を「DHCP Relay Hops Count Limit」として、指定することができます。DHCP パケットは、受信パケット内のリレーホップカウントが、この設定以上になると破棄されます。値の範囲は 1-16 で、初期値は 4 です。「DHCP Relay Time Threshold」はスイッチが Boot Request パケットを送出する前に待つ最小の時間 (秒) です。パケットの「Seconds」の値が「DHCP Relay Time Threshold」の値より小さければ、そのパケットは廃棄されます。値の範囲は 0-65535 で初期値は 0 (秒) です。

Network Application > DHCP > DHCP Relay > DHCP Relay Global Settings の順にメニューをクリックし、以下の画面を表示します。DHCP リレーのグローバル設定を有効にして、設定を行います。

図 13-1 DHCP Relay Global Settings 画面

以下の項目が使用されます。

| 項目 | 説明 |
|--|---|
| DHCP Relay State | スイッチ上で DHCP リレーサービスを「Enabled」(有効) / 「Disabled」(無効) にします。初期値は「Disabled」です。 |
| DHCP Relay Hops Count Limit (1-16) | DHCP メッセージが中継されるルータホップの最大数 (1-16) を定義します。初期値は 4 です。 |
| DHCP Relay Time Threshold (0-65535) | DHCP パケットのルーティングを行うタイムリミットを 0-65535 (秒) で定義します。0 を指定すると、スイッチは DHCP パケットの「Seconds」内の値の処理を行いません。0 以外の値を指定すると、スイッチはその値を使用し、ホップカウントと併用しながら DHCP パケットの送出手続きを決定します。初期値は 0 です。 |
| DHCP Relay Agent Information Option 82 State | <p>スイッチ上で DHCP Agent Information Option 82 機能を「Enabled」(有効) / 「Disabled」(無効) にします。初期値は「Disabled」です。</p> <ul style="list-style-type: none"> Enabled - リレーエージェントは DHCP サーバとクライアント間で交わすメッセージに DHCP Relay Information (「Option 82」欄) を挿入 / 削除します。リレーエージェントが DHCP リクエストを受信すると、Option 82 情報と (設定があれば) リレーエージェントの IP アドレスをパケットに付加します。Option 82 情報が付加されたパケットは DHCP サーバに送信されます。Option 82 をサポートする DHCP サーバがパケットを受信すると、そのサーバは remote ID、circuit ID、またはそれらの両方を使用して IP アドレスを割り当て、単一の remote ID または circuit ID に割り当て可能な IP アドレス制限などのポリシーを適用できます。また、DHCP サーバは「Option-82」欄の値を DHCP reply の中にそのまま残します。DHCP サーバはスイッチが DHCP request を中継していた場合には、ユニキャストで reply を返します。スイッチは remote ID や circuit ID 欄を調べて、本来の Option-82 情報が insert されていたかを確認します。スイッチは「Option-82」欄を削除してからそのパケットを DHCP クライアントに接続されているスイッチポートに転送します。 Disabled - リレーエージェントは DHCP サーバとクライアント間で交換するメッセージへの DHCP Relay Information (「Option 82」欄) の挿入 / 削除を行いません。また、以下の Option 82 のチェックとポリシーの項目は無効になります。 |
| DHCP Relay Agent Information Option 82 Check | <p>スイッチのパケットの Option 82 項目の妥当性のチェックを行う機能を「Enabled」(有効) / 「Disabled」(無効) にします。</p> <ul style="list-style-type: none"> Enabled - リレーエージェントはパケットの「Option 82」項目の妥当性のチェックを行います。スイッチが DHCP クライアントから Option 82 項目を含むパケットを受信すると、スイッチはこれらのパケットは不正だとしてパケットを廃棄します。リレーエージェントは DHCP サーバから受信したパケットから不正なメッセージを削除します。 Disabled - リレーエージェントはパケットの「Option 82」項目の妥当性のチェックを行いません。 |

| 項目 | 説明 |
|--|---|
| DHCP Relay Agent Information Option 82 Policy | プルダウンメニューから「Replace」、「Drop」または「Keep」を選択します。初期値は「Replace」です。 <ul style="list-style-type: none"> Replace - DHCP クライアントから受信したパケット内の既存のリレー情報をスイッチの DHCP リレー情報に置き換えます。 Drop - DHCP クライアントから受信したパケット内に既にリレー情報があった場合はそのパケットを削除します。 Keep - DHCP クライアントから受信したパケット内の既存のリレー情報を保持します。 |
| DHCP Relay Agent Information Option 82 Remote ID | Remote ID を入力します。「Default」に設定すると、Remote ID としてスイッチの MAC アドレスを使用します。 |
| DHCP Relay Option 60 State | DHCP Relay Option 60 State 機能を有効または無効にします。 |
| DHCP Relay Option 61 State | DHCP Relay Option 61 State 機能を有効または無効にします。 |

「Apply」ボタンをクリックして設定内容を有効にします。

注意 スイッチが、DHCP クライアントから「Option-82」項目を含むパケットを受信し、チェック機能が「Enabled」(有効)になっている場合、スイッチはこのようなパケットは不正だとして、パケットを破棄します。しかし、場合によってはクライアント側で Option-82 情報が設定されることもあります。そのような状況では、チェック機能を無効にしてスイッチがパケットから Option-82 欄を破棄しないようにします。DHCP クライアントから受信したパケット内に既にリレー情報があった場合のスイッチの動作を「DHCP Agent Information Option 82 Policy」で指定します。

DHCP Relay Agent Information Option 82 の実装

config dhcp_relay option_82 コマンドは、スイッチの DHCP リレーエージェント Information Option 82 の設定を行う際に使用します。Circuit ID サブオプションおよび Remote ID サブオプションのフォーマットは以下の通りです。

注意 スタンドアロンスイッチの場合、サーキット ID のサブオプションのモジュールフィールドは常に 0 です。

サーキット ID のサブオプションフォーマット

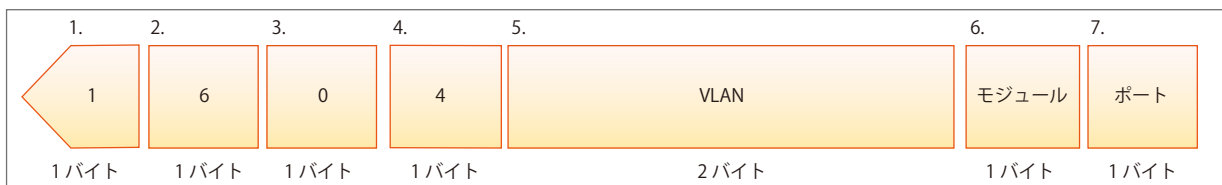


図 13-2 サーキット ID サブオプション形式

1. サブオプションタイプ
2. サブオプションタイプ長
3. Circuit ID タイプ
4. Circuit ID 長
5. VLAN: DHCP クライアントパケットを受信した VLAN
6. モジュール: スタンドアロンスイッチの場合は常に 0。スタックアップスイッチの場合は Unit ID。
7. ポート: DHCP クライアントパケットを受信したポート番号。ポート番号は 1 から始まります。

リモート ID のサブオプションフォーマット (初期値)

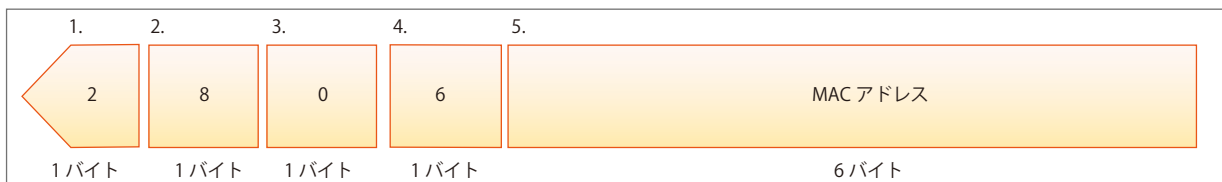


図 13-3 リモート ID サブオプション形式

1. サブオプションタイプ
2. サブオプション長
3. Remote ID タイプ
4. Remote ID 長
5. MAC アドレス: スイッチのシステム MAC アドレス

DHCP Relay Interface Settings (DHCP リレーインタフェース設定)

DHCP 情報をスイッチに中継するために、IP アドレスでサーバを設定します。以下の画面を使用して、DHCP サーバに直接接続するスイッチ上に定義済みの IP インタフェースを入力します。正しく入力を行い「Apply」ボタンをクリックすると、以下の画面の下部に位置する「DHCP Relay Interface Table」にリスト表示されます。スイッチの 1 つの IP インタフェースに対して 4 件までのサーバ IP アドレスを登録できます。

Network Application > DHCP > DHCP Relay > DHCP Relay Interface Settings の順にメニューをクリックし、以下の画面を表示します。

図 13-4 DHCP Relay Interface Settings 画面

以下の項目を使用して設定、表示を行います。

| 項目 | 説明 |
|-------------------|--|
| Interface Name | DHCP サーバに直接接続するスイッチの IP インタフェース |
| Server IP Address | DHCP サーバの IP アドレス。1 つの IP インタフェースに対して 4 件までの入力が可能です。 |

「Apply」ボタンをクリックして設定内容を有効にします。

DHCP リレーインタフェース設定の削除

削除するエントリの「Delete」ボタンをクリックします。

DHCP Relay Option 60 Server Settings (DHCP リレーオプション 60 サーバ設定)

DHCP リレーオプション 60 サーバのパラメータを設定します。

DHCP オプション 60 はベンダクラス識別子です。本機能が有効である場合、スイッチは、DHCP クライアントからのオプション 60 をチェックして、それを送信すべき DHCP サーバを決定します。本スイッチに転送ルールを設定することができます。

Network Application > DHCP > DHCP Relay > DHCP Relay Option 60 Server Settings の順にメニューをクリックし、以下の画面を表示します。

図 13-5 DHCP Relay Option 60 Server Settings 画面

以下の項目を使用して設定、表示を行います。

| 項目 | 説明 |
|-------------------|--|
| Server IP Address | DHCP リレーオプション 60 サーバのリレー IP アドレスを指定します。「Add」ボタンをクリックして、入力した情報に基づいて新しいエントリを追加します。 |
| Mode | DHCP リレーオプション 60 サーバのモードを選択します。「Apply」ボタンをクリックして行った変更を適用します。 |

エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。

「Delete All」ボタンをクリックして、表示されたすべてのエントリを削除します。

注意 オプション 60 に基づくパケットに一致しないサーバが発見された場合、リレーサーバはデフォルトリレーサーバによって判断されます。

DHCP Relay Option 60 Settings (DHCP リレーオプション 60 設定)

これは、DHCP リレーが DHCP オプション 60 を処理するかどうか決定します。

Network Application > DHCP > DHCP Relay > DHCP Relay Option 60 Settings の順にメニューをクリックし、以下の画面を表示します。

図 13-6 DHCP Relay Option 60 Settings 画面

以下の項目を使用して設定、表示を行います。

| 項目 | 説明 |
|-------------------|---|
| String | DHCP リレーオプション 60 文字列を入力します。同じリレーサーバに異なる文字列を指定でき、複数のリレーサーバに同じ文字列を指定できます。システムはすべてが一致しているサーバにパケットをリレーします。 |
| Server IP Address | DHCP リレーオプション 60 サーバの IP アドレスを入力します。 |
| Match Type | DHCP リレーオプション 60 サーバの一致タイプを入力します。 <ul style="list-style-type: none"> Exact Match - パケットにおけるオプション 60 の文字列が指定した文字列に完全に一致する必要があります。 Partial Match - パケットにおけるオプション 60 の文字列が指定した文字列に部分的にだけ一致する必要があります。 |
| IP Address | DHCP リレーオプション 60 の IP アドレスを入力します。 |

エントリの追加

「Add」ボタンをクリックして、入力した情報に基づいて新しいエントリを追加します。

エントリの参照

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

「Show All」ボタンをクリックして、すべての定義済みエントリを表示します。

エントリの削除

「Delete」ボタンをクリックして、入力した情報に基づいて指定エントリを削除します。

「Delete All」ボタンをクリックして、表示されたすべてのエントリを削除します。

DHCP Relay Option 61 Settings (DHCP リレーオプション 61 設定)

DHCP リレーオプション 61 のパラメータを設定します。

本機能が有効である場合、スイッチは、DHCP クライアントからのオプション 61 をチェックして、管理者が設定したオプション 61 ルールに基づいて、それを特定のサーバに送信するか、または破棄するかを決定します。

Network Application > DHCP > DHCP Relay > DHCP Relay Option 60 Settings の順にメニューをクリックし、以下の画面を表示します。

図 13-7 DHCP Relay Option 61 Settings 画面

以下の項目を使用して設定、表示を行います。

| 項目 | 説明 |
|------------------------------|---|
| DHCP Relay Option 61 Default | DHCP リレーオプション 61 デフォルトオプションを選択します。 <ul style="list-style-type: none"> Drop - パケットを破棄します。 Relay - IP アドレスにパケットをリレーします。デフォルトリレーサーバの IP アドレスを入力します。オプション 61 に基づくパケットに一致しないサーバが発見された場合、リレーサーバはデフォルトリレーサーバ設定によって判断されます。 |
| Client ID | <ul style="list-style-type: none"> MAC Address - クライアントのハードウェアアドレスであるクライアント ID。 String - 管理者によって指定されるクライアント ID。 |
| Relay Rule | <ul style="list-style-type: none"> Drop - パケットを破棄します。 Relay - IP アドレスにパケットをリレーします。 |

「Apply」ボタンをクリックして行った変更を適用します。

エントリの追加

「Add」ボタンをクリックして、入力した情報に基づいて新しいエントリを追加します。

エントリの削除

「Delete」ボタンをクリックして、入力した情報に基づいて指定エントリを削除します。

「Delete All」ボタンをクリックして、表示されたすべてのエントリを削除します。

DHCP Relay Port Settings (DHCP リレーポート設定)

DHCP リレー機能を各ポートで設定します。

Network Application > DHCP > DHCP Relay > DHCP Relay Port Settings の順にメニューをクリックし、以下の画面を表示します。

| Unit | From Port | To Port | State |
|------|-----------|---------|---------|
| 1 | 01 | 01 | Enabled |

| Unit 1 Settings | |
|-----------------|---------|
| Port | State |
| 1 | Enabled |
| 2 | Enabled |
| 3 | Enabled |
| 4 | Enabled |
| 5 | Enabled |
| 6 | Enabled |
| 7 | Enabled |
| 8 | Enabled |

図 13-8 DHCP Relay Settings 画面

以下の項目を使用して設定、表示を行います。

| 項目 | 説明 |
|---------------------|------------------------------|
| Unit | DHCP リレーを有効/無効にするユニットを指定します。 |
| From Port / To Port | DHCP リレーを有効/無効にするポートを指定します。 |
| State | ポートごとに DHCP リレーを有効/無効にします。 |

「Apply」ボタンをクリックして行った変更を適用します。

DHCP Server (DHCP サーバ)

DHCP (Dynamic Host Configuration Protocol) によってスイッチは、IP アドレス、サブネットマスク、デフォルトゲートウェイ、および他の IP パラメータをこの情報を要求するデバイスに発行することができます。DHCP が有効なデバイスが起動すると、ローカルなネットワークに割り当てられます。このデバイスは DHCP クライアントであり、有効にすると、IP パラメータが設定される前にネットワークにクエリメッセージを送信します。DHCP サーバがこのリクエストを受信すると、DHCP クライアントがローカル設定に利用する上記 IP 情報を含む応答をクライアントに返します。

ローカルに割り当てられたネットワークを利用するために、DHCP に関連する多くのパラメータを設定できます。これにより、割り当てた IP アドレスのリースタイム、DHCP プール内で許可されている IP アドレス範囲、ネットワークに同一のエントリを作成しないようにアドレスプール内の各 IP アドレスを排除する機能など自動 IP 設定を希望するクライアントの IP 設定をコントロールおよび制限します。また、DNS サーバまたはデフォルトルートの IP アドレスなどネットワークの別のデバイスに重要なデバイスの IP アドレスを割り当てることができます。

さらに、スタティック IP アドレスを必要とするネットワークメンテナンスに重要なデバイスの IP アドレスを同一に保つために、DHCP プール内の IP アドレスを指定した MAC アドレスに割り当てることができます。

DHCP Server Global Settings (DHCP サーバグローバル設定)

DHCP サーバグローバルパラメータを設定します。

Network Application > DHCP > DHCP Server > DHCP Server Global Settings の順にメニューをクリックし、以下の画面を表示します。

図 13-9 DHCP Server Global Settings 画面

以下のパラメータを設定できます。

| パラメータ | 説明 |
|------------------------|--|
| DHCP Server State | スイッチを DHCP サーバとしてグローバルに「Enabled」(有効) / 「Disabled」(無効) にします。 |
| Ping Packets (0-10) | 割り当て済みの IP アドレスを含むネットワークにスイッチが送信する ping パケットの数 (0-10) を指定します。ping リクエストが戻らない場合、その IP アドレスは、ローカルネットワークに対して固有であると見なされて、要求側クライアントに割り当てられます。0 は ping テストを行わないことを意味します。初期値は 2 パケットです。 |
| Ping Timeout (10-2000) | ping パケットがタイムアウトになる前に DHCP サーバが待つ時間を選択します。初期値は 100 です。 |

「Apply」ボタンをクリックして各セクションで行った変更を適用します。

DHCP Server Exclude Address Settings (DHCP サーバ除外アドレス設定)

DHCP 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。除外する複数のグループを定義するために本コマンドを繰り返して使用します。DHCP サーバは、DHCP プールサブネットにあるすべての IP アドレスを DHCP クライアントに割り当てることができるものとします。

Network Application > DHCP > DHCP Server > DHCP Server Exclude Address Settings の順にメニューをクリックし、以下の画面を表示します。

図 13-10 DHCP Server Exclude Address Settings 画面

以下の項目を使用して設定、表示を行います。

| 項目 | 説明 |
|---------------|-----------------------|
| Begin Address | 除外する開始 IP アドレスを指定します。 |
| End Address | 除外する終了 IP アドレスを指定します。 |

IP アドレスまたは IP アドレス範囲を設定するために、範囲の「Begin Address」(開始アドレス) と「End Address」(終了アドレス) を入力し、「Add」ボタンをクリックします。設定したアドレス範囲は以下の画面下半分に表示されます。

エントリの削除

「Delete All」ボタンをクリックして、表示されたすべてのエントリを削除します。

「Delete」ボタンをクリックして、指定エントリを削除します。

DHCP Server Pool Settings (DHCP サーバプール設定)

DHCP サーバプールの追加および削除を行います。

Network Application > DHCP > DHCP Server > DHCP Server Pool Settings の順にメニューをクリックし、以下の画面を表示します。

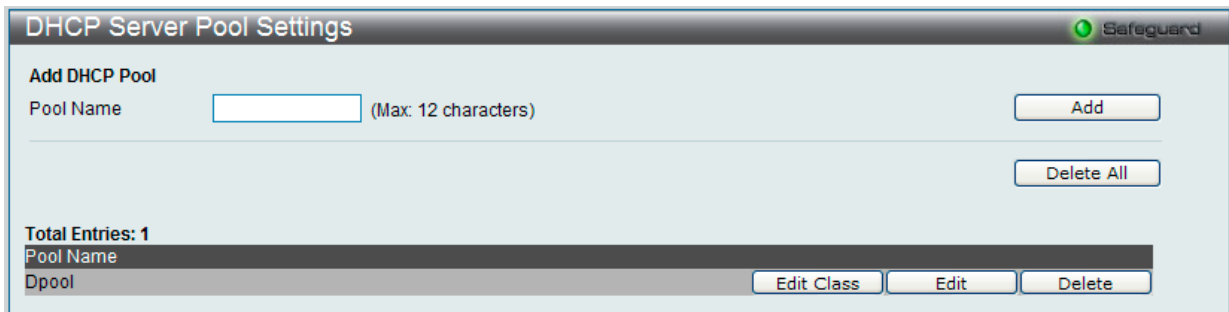


図 13-11 DHCP Server Pool Settings 画面

以下の項目を使用して設定、表示を行います。

| 項目 | 説明 |
|-----------|---------------------|
| Pool Name | DHCP サーバプール名を入力します。 |

はじめに「Pool Name」欄に名前(半角英数字 12 文字以内)を入力して、「Add」をクリックすることによって、プールを作成します。一度作成されると、対応する「Edit」ボタンをクリックして、プールの設定を編集することができます。

エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。「Delete All」ボタンをクリックして、表示されたすべてのエントリを削除します。

エントリの編集

1. 「Edit」ボタンをクリックすると、以下の画面が表示されます。

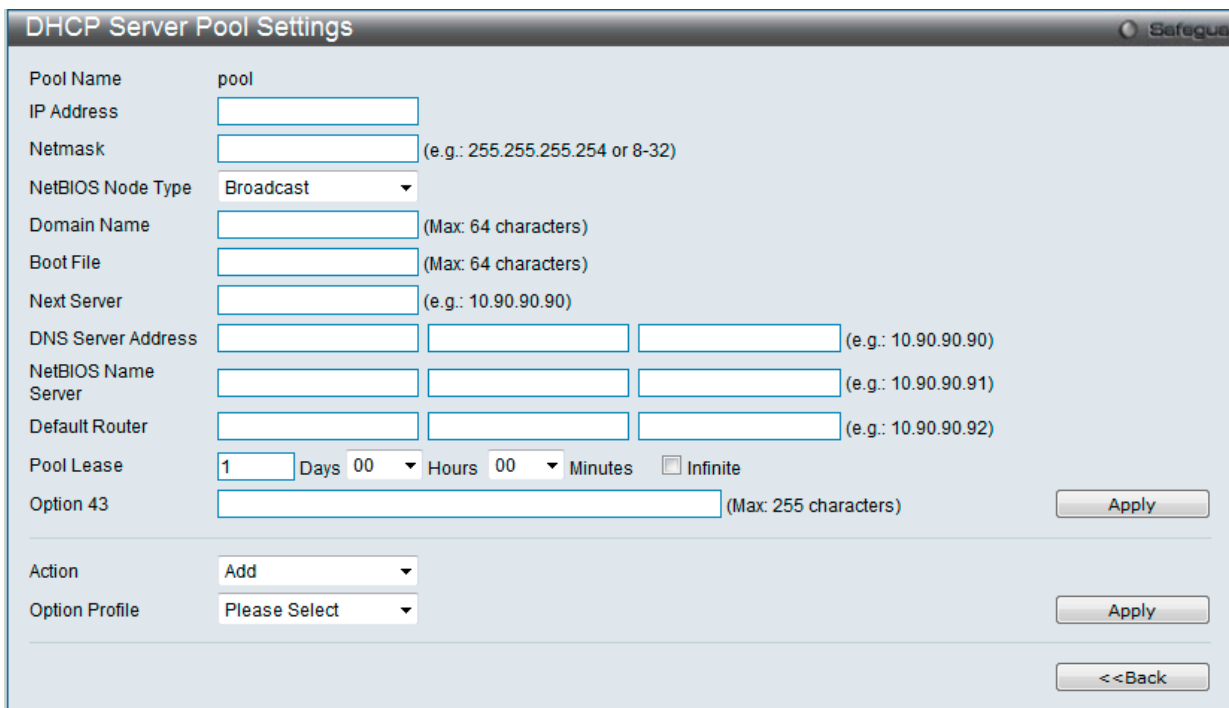


図 13-12 DHCP Server Pool Settings (Edit) 画面

以下の項目を使用して設定、表示を行います。

| 項目 | 説明 |
|-------------------|---|
| Pool Name | パラメータを調整する DHCP プール名を表示します。 |
| IP Address | プールのネットワークアドレスを入力します。 |
| Netmask | 上記フィールドに割り当てられたネットワークアドレスに対応するネットマスクを入力します。 |
| NetBIOS Node Type | マイクロソフト DHCP クライアントの NetBIOS のノードタイプを設定します。プルダウンメニューを使用して、4 つのノードタイプ (Broadcast、Peer to Peer、Mixed および Hybrid) から選択します。 |

| 項目 | 説明 |
|---------------------|---|
| Domain Name | クライアントのドメイン名を入力します。ここで設定したドメイン名は、クライアントにデフォルトドメイン名として使用されます。 |
| Boot File | ブートイメージのファイル名。ブートファイルは、クライアント用のブートイメージを保存するのに使用されます。通常、本イメージは、クライアントがロードするのに使用するオペレーティングシステムです。このオプションが二度同じプールに入力されると、2 番目のコマンドは最初のコマンドを上書きします。ブートファイルを指定しないと、ブートファイル情報はクライアントに提供されません。 |
| Next Server | ネクストサーバの IP アドレスを指定します。 |
| DNS Server Address | DNS サーバの IP アドレス。DHCP クライアントが使用可能である DNS サーバの IP アドレスを入力します。1 つのコマンドラインで最大 3 つの IP アドレスを指定できます。 |
| NetBIOS Name Server | WINS サーバの IP アドレス。WINS(Windows Internet Naming Service) は、マイクロソフト DHCP クライアントが通常グループ分けされているネットワーク内の IP アドレスにホスト名を関連付けるために使用する名前解決サービスです。1 つのコマンドラインで最大 3 つの IP アドレスを指定できます。 |
| Default Router | デフォルトルータの IP アドレス。DHCP クライアントにデフォルトルータの IP アドレスを入力します。1 つのコマンドラインで最大 3 つの IP アドレスを指定できます。 |
| Pool Lease | 初期値では、DHCP サーバに割り当てられる各 IP アドレスのリース期間 (アドレスが有効であることの時間) は 1 日です。 <ul style="list-style-type: none"> Days - リースする日 Hours - リースする時間 (時) Minutes - リースする時間 (分) 「Infinite」を指定すると無制限になります。 |
| Option 43 | 本オプションは、DHCP オプション 43 を追加、または削除するのに使用されます。DHCP サーバは、クライアントのリクエストパケット内のオプション 55 に従って、DHCP リレーに本オプションを含めることができます。ここで使用する DHCP オプション 43 の文字列を入力します。 |
| Action | オプションの動作を指定します。「Add (追加)」「Delete (削除)」から指定します。 |
| Option Profile | DHCP サーバプールと連動するオプションプロファイルを指定します。 |

2. エントリの編集を行い、「Apply」ボタンをクリックします。

「<<Back」ボタンをクリックし、変更を破棄して前のページに戻ります。

プールクラスの編集

「Edit Class」ボタンをクリックすると、以下の画面が表示されます。

The screenshot shows the 'DHCP Server Pool Class Settings' window. The 'Pool Name' is 'Dpool' and the 'Class Name' is 'DClass'. The 'Begin Address' and 'End Address' fields are empty, with examples '(e.g.: 20.0.0.20)' and '(e.g.: 20.0.0.50)' provided. There are '<<Back' and 'Add' buttons. Below, a table shows 'Total Entries: 1' with one entry: 'DClass' with 'Begin Address' '192.168.1...' and 'End Address' '192.168.1...'. There are 'Edit', 'Delete by Name', and 'Delete Address' buttons.

図 13-13 DHCP Server Pool Settings (クラスの編集) 画面

以下の項目を使用して設定、表示を行います。

| 項目 | 説明 |
|---------------|--|
| Class Name | ここで使用する DHCP クラス名を入力します。12 文字以内で指定します。 |
| Begin Address | DHCP プールに使用される開始 IP アドレスを指定します。 |
| End Address | DHCP プールに使用される終了 IP アドレスを指定します。 |

「Add」ボタンをクリックして、入力した情報に基づいて新しいエントリを追加します。

「<<Back」ボタンをクリックし、変更を破棄してと前のページに戻ります。

指定プールクラスの編集

「Edit」 ボタンをクリックして、指定エントリを編集します。



図 13-14 DHCP Server Pool Settings (クラスの編集) 画面

エントリの削除

名前に基づいて指定エントリを削除するには、「Delete By Name」ボタンをクリックします。

アドレスに基づいて指定エントリを削除するには、「Delete By Address」ボタンをクリックします。

DHCP Server Class Settings (DHCP サーバクラス設定)

DHCP サーバクラスを設定します。

Network Application > DHCP > DHCP Server > DHCP Server Class Settings の順にメニューをクリックし、以下の画面を表示します。

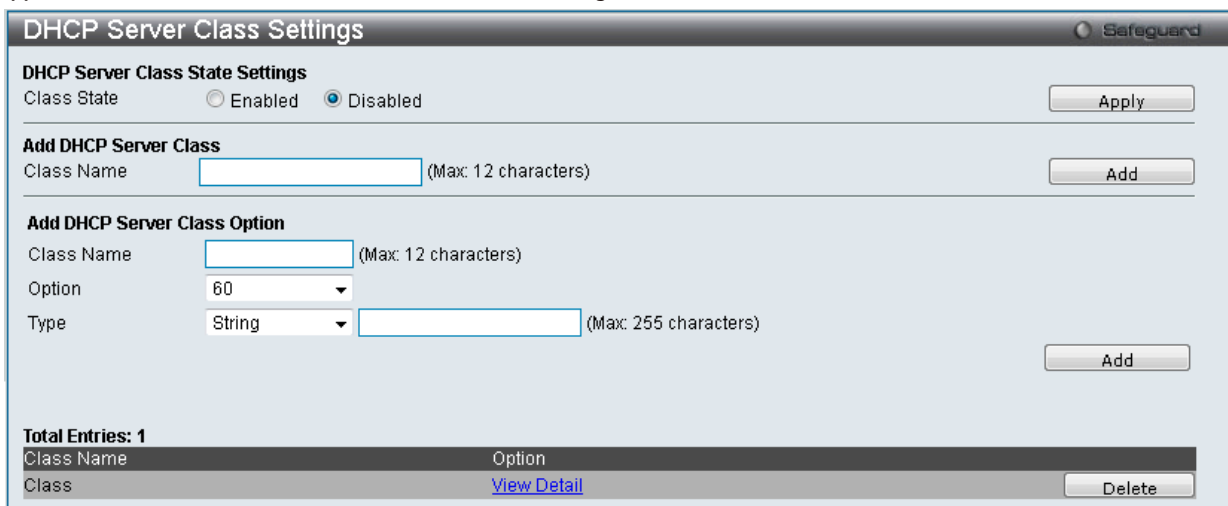


図 13-15 DHCP Server Class Settings 画面

以下の項目を使用して設定、表示を行います。

| 項目 | 説明 |
|-------------|-------------------------------------|
| Class State | DHCP サーバクラスの状態を有効または無効に指定します。 |
| Class Name | 使用する DHCP クラス名を入力します。12 文字以内で指定します。 |
| Option | DHCP サーバクラスを適用するオプションを指定します。 |
| Type | |

DHCP サーバクラス状態の設定

「Class State」を「Enabled」(有効)または「Disabled」(無効)に設定し、「Apply」ボタンをクリックします。

DHCP サーバクラスの追加

「Class Name」を入力後、「Add」ボタンをクリックして、入力した情報に基づいて新しいエントリを追加します。

エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。

エントリの詳細情報の追加 / 編集

指定エントリに関するより詳しい情報を設定します。

「Add/Edit」ボタンをクリックして、以下の画面を表示します。

The screenshot shows the 'DHCP Server Class Settings' dialog box. At the top right, there is a 'Safeguard' indicator. The main area contains three fields: 'Class Name' with the value 'DClass', 'Option' with a dropdown menu showing '60', and 'Type' with a dropdown menu showing 'String' and an adjacent text input field (Max: 255 characters). Below these fields are two buttons: '<<Back' and 'Add'. At the bottom, there is a section titled 'Total Entries: 1' containing a table with the following data:

| Class Name | Option | Type | Value |
|------------|--------|--------|---------------|
| DClass | 60 | String | DClass_string |

Buttons for 'Edit' and 'Delete' are located to the right of the table row.

図 13-16 DHCP Server Class Settings 画面 (追加 / 編集)

以下の項目を使用して設定、表示を行います。

| 項目 | 説明 |
|------------|--|
| Class Name | 使用する DHCP クラス名を表示します。 |
| Option | 追加するオプションインデックスを指定します。オプションは「60」または「82」から選択します。 |
| Type | 使用する DHCP クラスの文字列または HEX タイプを指定します。 <ul style="list-style-type: none"> String - 使用する文字列を入力します。255 文字以内で指定します。 Hex - 使用する文字列の 16 進値を入力します。255 文字以内で指定します。 |

「Add」ボタンをクリックして、入力した情報に基づいて新しいエントリを追加します。

指定エントリの編集

「Edit」ボタンをクリックして、指定エントリを編集します。

The screenshot shows the 'DHCP Server Class Settings' dialog box in edit mode. The fields for 'Class Name' (DClass), 'Option' (60), and 'Type' (String) are the same as in the previous screenshot. Below these fields are two buttons: '<<Back' and 'Add'. At the bottom, there is a section titled 'Total Entries: 1' containing a table with the following data:

| Class Name | Option | Type | Value |
|------------|--------|--------|---------------|
| DClass | 60 | String | DClass_string |

Buttons for 'Apply' and 'Delete' are located to the right of the table row.

図 13-17 DHCP Server Class Settings 画面 (編集)

指定エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。

DHCP Server Option Profile Settings (DHCP サーバオプションプロファイル設定)

DHCP サーバオプションのプロファイルをカスタマイズします。

Network Application > DHCP > DHCP Server > DHCP Server Option Profile Settings の順にメニューをクリックし、以下の画面を表示します。

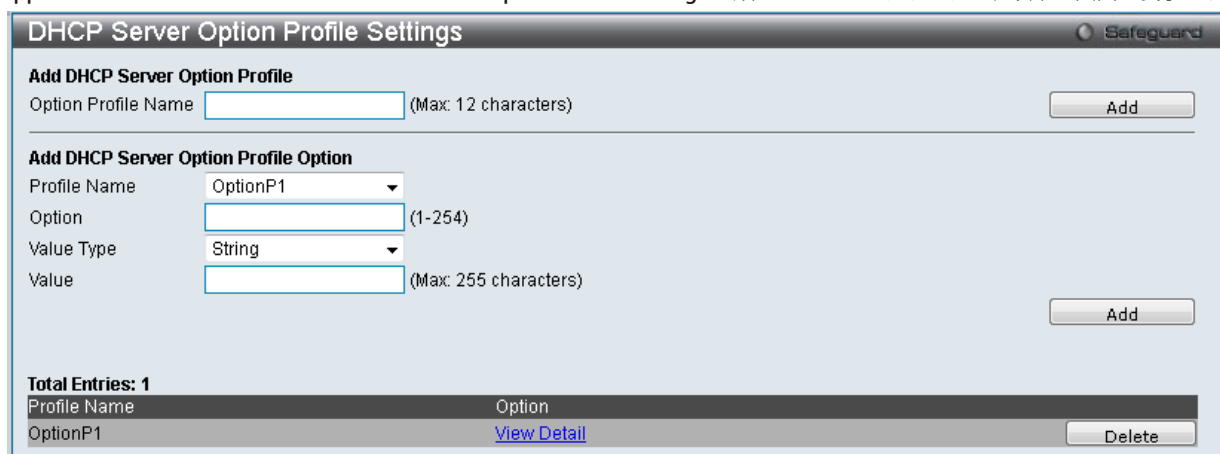


図 13-18 DHCP Server Option Profile Settings 画面

以下の項目を使用して設定、表示を行います。

| 項目 | 説明 |
|---------------------|---|
| Option Profile Name | 設定する新しい DHCP オプションプロファイル名を指定します。 |
| Profile Name | 「DHCP オプションプロファイル」作成後、追加可能なオプションプロファイルを選択します。 |
| Option | 使用するオプションの値を指定します。 |
| Value Type | 値の単位を指定します。「String」「Hex」から指定可能です。 |
| Value | オプションの値を入力します。 |

「Add」ボタンをクリックして、入力した情報に基づいて新しいエントリを追加します。

指定エントリの詳細表示

「View Detail」ボタンをクリックして、指定エントリを編集します。



図 13-19 DHCP Server Option Profile Settings 画面 (詳細表示)

指定エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。

DHCP Server Manual Binding (DHCP サーバマニュアルバインディング)

アドレスバインディングはクライアントの IP アドレスと MAC アドレスの間のマッピングです。クライアントの IP アドレスを管理者が手動で割り当てるか、または DHCP サーバがプールから自動的に割り当てることができます。プールネットワークのアドレスからクライアントに IP アドレスを割り当てると、ダイナミックバインディングエントリが作成されます。

Network Application > DHCP > DHCP Server > DHCP Server Manual Binding の順にメニューをクリックし、以下の画面を表示します。

図 13-20 DHCP Server Manual Binding 画面

以下の項目を使用して設定、表示を行います。

| 項目 | 説明 |
|------------------|--|
| Pool Name | マニュアルバインディングエントリを作成する DHCP プール名を入力します。 |
| IP Address | 特定のクライアントに割り当てられる IP アドレスを入力します。 |
| Hardware Address | デバイスの MAC アドレスを入力し、前欄で入力した IP アドレスにスタティックに連結します。 |
| Type | この手動連結するエントリが設定される接続タイプを指定します。 <ul style="list-style-type: none"> Ethernet - 手動で連結したデバイスがスイッチに直接マニュアルで制限されたデバイスが直接スイッチに接続します。 IEEE802 - 手動で連結したデバイスがスイッチのローカルネットワークより外側であることを示します。 |

「Add」 ボタンをクリックして、入力した情報に基づいて新しいエントリを追加します。

エントリの削除

「Delete All」 ボタンをクリックして、表示されたすべてのエントリを削除します。「Delete」 ボタンをクリックして、指定エントリを削除します。

DHCP Server Dynamic Binding (DHCP サーバダイナミックバインディング)

DHCP サーバダイナミックバインディングテーブルの表示と削除を行います。

Network Application > DHCP > DHCP Server > DHCP Server Dynamic Binding の順にメニューをクリックし、以下の画面を表示します。

図 13-21 DHCP Server Dynamic Binding 画面

「Pool Name」 に DHCP サーバプール名を入力します。

エントリのクリア

「Clear」 ボタンをクリックして、本欄に入力したすべてのエントリをクリアします。「Clear All」 ボタンをクリックして、テーブルに表示されたすべてのエントリを削除します。

表示されるテーブルの各項目は以下の通りです。

| パラメータ | 説明 |
|------------------|--|
| Pool Name | ダイナミックにバインドされている DHCP エントリのプール名を表示します。 |
| IP Address | 本スイッチの DHCP サーバ機能によってこのデバイスに割り当てられた IP アドレスを表示します。 |
| Hardware Address | 対応する IP アドレスにバインドされているデバイスの MAC アドレスを表示します。 |
| Type | 本エントリに定義済みの NetBIOS ネームサーバのノードタイプを表示します。 |
| Status | ダイナミックまたはマニュアルでバインドされているかというエントリのステータスを表示します。 |
| Life Time (sec) | 本 IP アドレスのリースタイムの残り時間 (秒) を表示します。 |

DHCP Conflict IP (DHCP コンフリクト IP)

DHCP サーバは、この IP をバインディングする前にその IP アドレスが他のホストとコンフリクトしているかどうかを判断するために ping パケットを使用します。コンフリクトを確認された IP アドレスはコンフリクト IP データベースに移動します。ユーザがコンフリクト IP データベースからそれをクリアしない限り、システムは、コンフリクト IP データベースの IP アドレスを割り当てません。

Network Application > DHCP > DHCP Server > DHCP Conflict IP の順にメニューをクリックし、以下の画面を表示します。

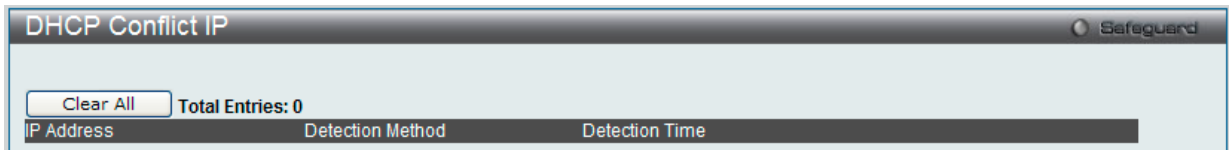


図 13-22 DHCP Conflict IP 画面

「Clear All」ボタンをクリックして、テーブルに表示されたすべてのエントリを削除します。

DHCPv6 Server (DHCPv6 サーバ設定)

DHCPv6 Server Global Settings (DHCPv6 サーバグローバル設定)

スイッチの DHCPv6 サーバ機能を有効にします。

Network Application > DHCP > DHCPv6 Server > DHCPv6 Server Global Settings の順にメニューをクリックし、以下の画面を表示します。

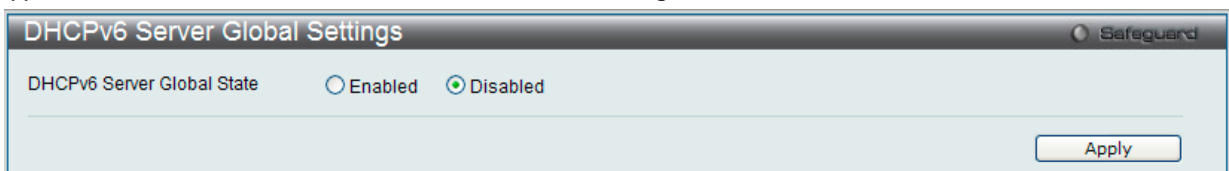


図 13-23 DHCPv6 Server Global Settings 画面

以下の項目を使用して設定、表示を行います。

| 項目 | 説明 |
|----------------------------|--|
| DHCPv6 Server Global State | ラジオボタンをクリックして DHCPv6 サーバ状態を「Enabled」(有効)/「Disabled」(無効)にします。 |

「Apply」ボタンをクリックして行った変更を適用します。

DHCPv6 Server Pool Settings (DHCPv6 サーバプール設定)

DHCPv6 プールの作成および設定を行います。

Network Application > DHCP > DHCPv6 Server > DHCPv6 Server Pool Settings の順にメニューをクリックし、以下の画面を表示します。

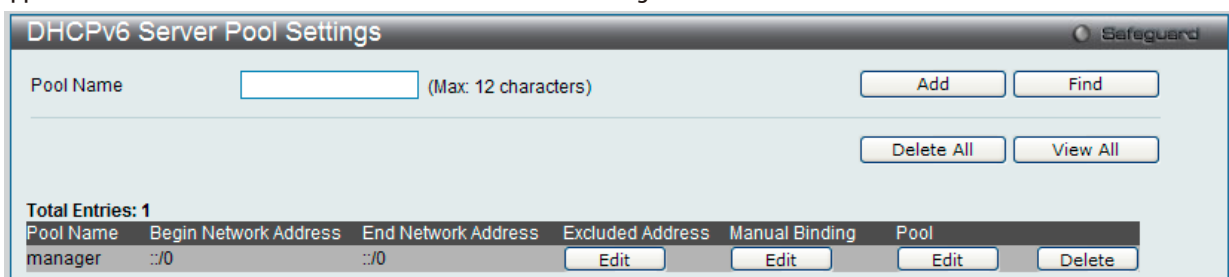


図 13-24 DHCPv6 Server Pool Settings 画面

以下の項目を使用して設定、表示を行います。

| 項目 | 説明 |
|-----------|-----------------------|
| Pool Name | DHCPv6 サーバプール名を入力します。 |

エントリの追加

「Add」ボタンをクリックして、入力した情報に基づいて新しいエントリを追加します。

エントリの参照

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

「View All」ボタンをクリックして、すべての定義済みエントリを表示します。

エントリの削除

「Delete」ボタンをクリックして、入力した情報に基づいて指定エントリを削除します。

「Delete All」ボタンをクリックして、表示されたすべてのエントリを削除します。

除外アドレスの設定

「Excluded Address」下の「Edit」ボタンをクリックすると、以下の画面が表示されます。

図 13-25 DHCPv6 Server Excluded Address Settings 画面

以下の項目を使用して設定、表示を行います。

| 項目 | 説明 |
|---------------|---|
| Begin Address | DHCPv6 プールから除く IPv6 アドレス範囲の開始の IPv6 アドレスを入力します。 |
| End Address | DHCPv6 プールから除く IPv6 アドレス範囲の終了の IPv6 アドレスを入力します。 |

「Add」ボタンをクリックして、入力した情報に基づいて新しいエントリを追加します。

「<<Back」ボタンをクリックして前のページに戻ります。

エントリの削除

「Delete」ボタンをクリックして、入力した情報に基づいて指定エントリを削除します。

「Delete All」ボタンをクリックして、表示されたすべてのエントリを削除します。

マニュアルバインディング設定

「Manual Binding」下の「Edit」ボタンをクリックすると、以下の画面が表示されます。

図 13-26 DHCPv6 Server Manual Binding Settings 画面

以下の項目を使用して設定、表示を行います。

| 項目 | 説明 |
|-----------------|--|
| IPv6 Address | デバイスにスタティックに割り当てる IPv6 アドレスを入力します。 |
| Network Address | デバイスにスタティックに割り当てる IPv6 ネットワークアドレスを入力します。 |
| Client DUID | デバイスの DUID を入力し、前のフィールドで入力した IPv6 アドレスにスタティックに連結します。 |

「Add」ボタンをクリックして、入力した情報に基づいて新しいエントリを追加します。

「<<Back」ボタンをクリックして前のページに戻ります。

エントリの削除

「Delete」ボタンをクリックして、入力した情報に基づいて指定エントリを削除します。

「Delete All」ボタンをクリックして、表示されたすべてのエントリを削除します。

DHCPv6 サーバプール設定

「Pool」下の「Edit」ボタンをクリックすると、以下の画面が表示されます。

図 13-27 DHCPv6 Server Pool Settings 画面

以下の項目を使用して設定、表示を行います。

| 項目 | 説明 |
|------------------------------------|---|
| Begin Network Address | DHCPv6 プールの開始 IPv6 ネットワークアドレスを入力します。 |
| End Network Address | DHCPv6 プールの終了 IPv6 ネットワークアドレスを入力します。 |
| Network Address | DHCPv6 プールの IPv6 ネットワークアドレスを入力します。 |
| Assigned Len | 「Assigned Length」を指定します。 |
| Interface Name | インタフェース名を指定します。 |
| Domain Name | ドメイン名は、DNS と共にホスト名を解決する場合にクライアントに使用されます。 |
| DNS Server | このプールに対する DNS サーバの IPv6 アドレスを入力します。最大 2 個までの DNS サーバアドレスを指定することができます。 |
| Preferred Lifetime (60-4294967295) | 指定プールに基づいた IPv6 アドレスが preferred-lifetime 状態を維持する時間 (秒)。 |
| Valid Lifetime (60-4294967295) | 指定プールに基づいた IPv6 アドレスが有効な状態を維持する時間 (秒)。 |

「<<Back」をボタンをクリックして前のページに戻ります。

「Apply」ボタンをクリックして行った変更を適用します。

DHCPv6 Server Dynamic Binding (DHCPv6 サーバダイナミックバインディング)

DHCPv6 ダイナミックバインディング情報を参照します。

Network Application > DHCP > DHCPv6 Server > DHCPv6 Server Dynamic Binding の順にメニューをクリックし、以下の画面を表示します。

図 13-28 DHCPv6 Server Dynamic Binding Table 画面

以下の項目を使用して設定、表示を行います。

| 項目 | 説明 |
|-----------|---|
| Pool Name | ダイナミックバインディング情報を参照する DHCPv6 プール名を入力します。 |

エントリの参照

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

「View All」ボタンをクリックして、すべての定義済みエントリを表示します。

エントリのクリア

「Clear」ボタンをクリックして、本欄に入力したすべてのエントリをクリアします。

「Clear All」ボタンをクリックして、テーブルに表示されたすべてのエントリを削除します。

DHCPv6 Server Interface Settings (DHCPv6 サーバインタフェース設定)

インタフェースごとに DHCPv6 サーバ状態を表示および設定します。

Network Application > DHCP > DHCPv6 Server > DHCPv6 Server Interface Settings の順にメニューをクリックし、以下の画面を表示します。

| Interface Name | DHCPv6 Server State | |
|----------------|---------------------|------|
| manager | Enabled | Edit |
| System | Enabled | Edit |

図 13-29 DHCPv6 Server Interface Settings 画面

以下の項目を使用して設定、表示を行います。

| 項目 | 説明 |
|----------------|--------------------|
| Interface Name | IP インタフェース名を入力します。 |

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

「View All」ボタンをクリックして、すべての定義済みエントリを表示します。

エントリの編集

1. 「Edit」ボタンをクリックすると、以下の画面が表示されます。

| Interface Name | DHCPv6 Server State | |
|----------------|---------------------|-------|
| manager | Enabled | Apply |
| System | Enabled | Edit |

図 13-30 DHCPv6 Server Interface Settings 画面 - Edit

2. エントリの編集を行い、「Apply」ボタンをクリックします。

DHCPv6 Relay (DHCPv6 リレー)

DHCPv6 Relay Global Settings (DHCPv6 リレーグローバル設定)

スイッチの DHCPv6 リレー機能を設定します。

Network Application > DHCP > DHCPv6 Relay > DHCPv6 Relay Global Settings の順にメニューをクリックし、以下の画面を表示します。

図 13-31 DHCPv6 Relay Global Settings 画面

以下の項目を使用して設定、表示を行います。

| 項目 | 説明 |
|--------------------------------|--|
| DHCPv6 Relay State | ラジオボタンをクリックして DHCPv6 リレー機能を「Enabled」(有効)/「Disabled」(無効)にします。 |
| DHCPv6 Relay Hops Count (1-32) | このメッセージにリレーすべきリレーエージェントの数を入力します。初期値は 4 です。 |

「Apply」ボタンをクリックして各セクションで行った変更を適用します。

DHCPv6 Relay Settings (DHCPv6 リレー設定)

1 つまたはすべての指定インタフェースの DHCPv6 リレー状態を設定し、スイッチの DHCPv6 リレーテーブルから (に) 宛先 IP アドレスを追加または削除します。

Network Application > DHCP > DHCPv6 Relay > DHCPv6 Relay Settings の順にメニューをクリックし、以下の画面を表示します。

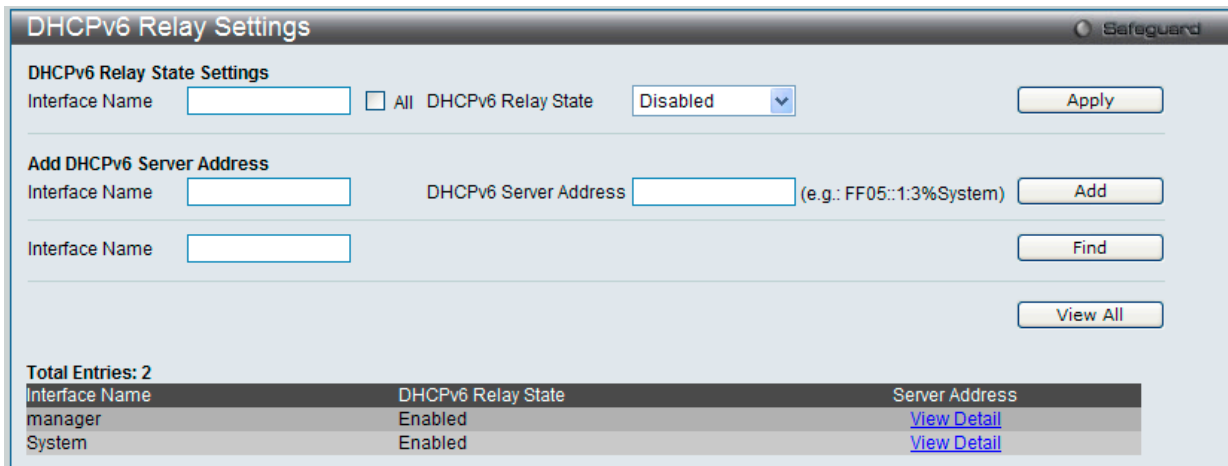


図 13-32 DHCPv6 Relay Settings 画面

以下の項目を使用して設定、表示を行います。

| 項目 | 説明 |
|-----------------------------|---|
| DHCPv6 Relay State Settings | |
| Interface Name | IPv6 インタフェース名を入力します。「All」を選択すると、すべての IPv6 インタフェースを選択します。 |
| DHCPv6 Relay State | プルダウンメニューを使用して、インタフェースの DHCPv6 リレーの状態を「Enabled」(有効)/「Disabled」(無効)にします。 |
| Add DHCPv6 Address | |
| DHCPv6 Server Address | DHCPv6 サーバの IPv6 アドレスを入力します。 |

「Apply」ボタンをクリックして行った変更を適用します。

「Add」ボタンをクリックして、入力した情報に基づいて新しいエントリを追加します。

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

「View All」ボタンをクリックして、すべての定義済みエントリを表示します。

エントリの詳細情報の表示

1. 「View Detail」ボタンをクリックすると、以下の画面が表示されます。

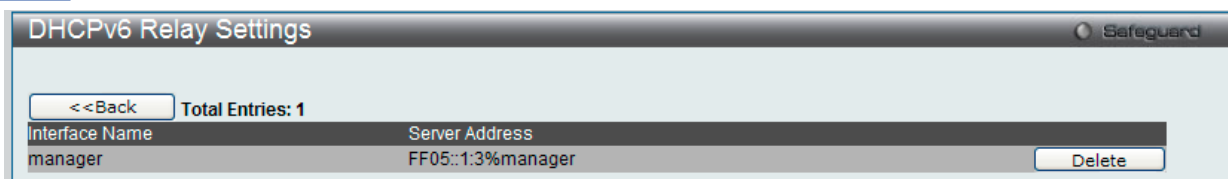


図 13-33 DHCPv6 Relay Settings 画面 - View Detail

DHCP Local Relay Settings (DHCP ローカルリレー設定)

DHCP クライアントが同じ VLAN から IP アドレスを取得する場合、DHCP ローカルリレー設定では、DHCP リクエストパケットにオプション 82 を追加できます。DHCP ローカルリレー設定をしないと、スイッチは VLAN にパケットをフラッドします。DHCP リクエストパケットにオプション 82 を追加するためには、DHCP ローカルリレー設定と Global VLAN の状態を有効にする必要があります。

Network Application > DHCP Server > DHCP Local Relay Settings の順にメニューをクリックし、以下の画面を表示します。

図 13-34 DHCP Local Relay Settings 画面

以下の項目を使用して設定、表示を行います。

| 項目 | 説明 |
|-------------------------------|---|
| DHCP Local Relay Global State | DHCP ローカルリレー設定を「Enabled」(有効)または「Disabled」(無効)にします。初期値は「Disabled」です。 |
| VLAN Name | DHCP ローカルリレー操作に適用する VLAN を識別するために使用する VLAN 名です。 |
| State | VLAN に対する DHCP ローカルリレー設定を「Enabled」(有効)または「Disabled」(無効)にします。 |

「Apply」ボタンをクリックして各セクションで行った変更を適用します。

DNS (ドメインネームシステム)

コンピュータのユーザは外部と接続するコンピュータの名前として、テキスト形式のものを使用の方が使い勝手が良いといえます。コンピュータ自身には 32 ビットの IP アドレスが必要です。このため、ネットワークデバイスのテキスト形式の名前 (ドメイン名) とそれに対応する IP アドレスのデータベースがどこかに保持される必要があります。

DNS (Domain Name System) は、そのようなドメイン名と IP アドレスの関連付けをインターネット経由で行い、イントラネットでもこれが使用されるようになってきました。異なるサブネットを通して通信する DNS サーバの間には、中継を行うために DNS リレー機能が必要になります。DNS サーバは IP アドレスにより識別します。

ドメイン名とアドレスのマッピング

ドメイン名とアドレスの関連付けはネームサーバというプログラムにより行われます。クライアントプログラムはネームリゾルバと呼ばれます。ネームリゾルバは、ドメイン名とアドレスの変換を行うためにいくつかのネームサーバと連絡を取る必要があります。

DNS サーバ群は、ドメイン名に対応した階層構造になっています。1 台のサーバは通常 1 つのネットワークにドメイン名を持ち、これが上位に位置するルート DNS サーバ (通常 ISP が管理) に接続を行います。

ドメイン名の解決

ドメイン名の解決はその都度ネームサーバに問い合わせる場合と、DNS にまとめて解決を求める場合があります。クライアントは、ドメイン名、必要な応答の種類、およびクエリを受信したサーバが名前の解決をできない場合に、DNS によってすべてのドメイン名の解決を行うか、または次の DNS サーバのアドレスのみを返せばよいのかを指定したコードを含むクエリを作成します。

DNS サーバがクエリを受信すると、その名前がサブドメイン中に存在するかどうかをチェックします。存在していればサーバは名前を解決し、クエリへの応答としてクライアントに返します。自分で解決できない場合は、クライアントが要求する方法の名前解決を実行します。1 つは再帰的解決と呼ばれる方法で、サーバは名前の解決が完了するまで、他の DNS サーバと連絡を取り合います。もう 1 つは反復的解決と呼ばれる方法で、DNS サーバが自分で解決できない場合は、クライアントが連絡すべき次の DNS サーバのアドレスのみを返します。

各 DNS クライアントは、最低 1 台の DNS サーバに連絡可能で、各 DNS サーバは最低 1 台のルートサーバに連絡する手段を持たなければなりません。

ドメインネームサービスを行うデバイスのアドレスは、DHCP または BOOTP サーバから得る場合と、初期設定時に手動で OS に設定する場合があります。

DNS Relay (DNS リレー)

DNS Relay Global Settings (DNS リレーグローバル設定)

DNS リレーのグローバル設定を行います。

Network Application > DNS > DNS Relay > DNS Relay Global Settings の順にメニューをクリックし、以下の画面を表示します。

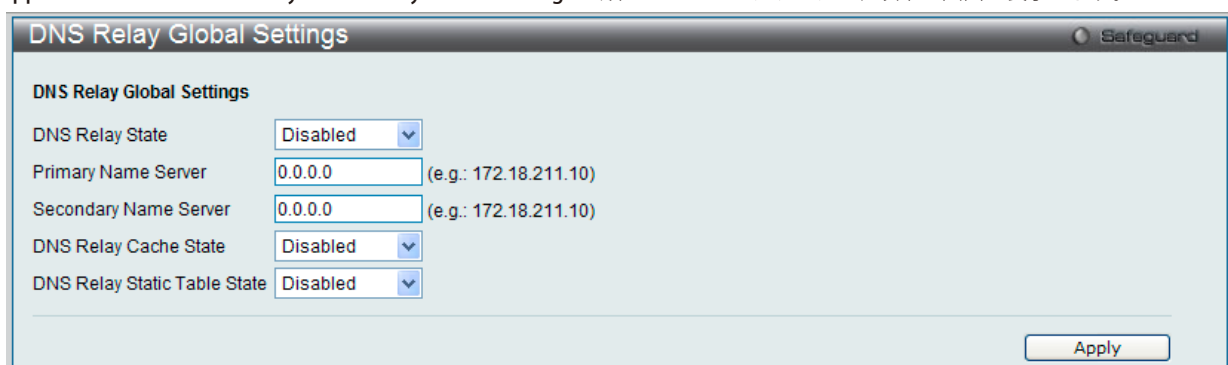


図 13-35 DNS Relay Global Settings 画面

以下の項目を使用して設定、表示を行います。

| 項目 | 説明 |
|-------------------------|--|
| DNS State | スイッチの DNS リレーサービス機能を「Enabled」(有効) / 「Disabled」(無効) にします。 |
| Primary Name Server | プライマリドメインネームサーバ (DNS) の IP アドレスを指定します。 |
| Secondary Name Server | セカンダリドメインネームサーバ (DNS) の IP アドレスを指定します。 |
| DNSR Cache Status | スイッチの DNS キャッシュを「Enabled」(有効) / 「Disabled」(無効) にします。 |
| DNSR Static Table State | スタティック DNS テーブルを「Enabled」(有効) / 「Disabled」(無効) にします。 |

「Apply」ボタンをクリックして各セクションで行った変更を適用します。

DNS Relay Static Settings (DNS リレースタティック設定)

スイッチ名前解決テーブルにスタティックなエントリの追加または削除を行います。

Network Application > DNS > DNS Relay > DNS Relay Static 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。

| Add DNS Relay Static | |
|---|--|
| Domain Name <input type="text"/> (Max: 32 characters) | IP Address <input type="text"/> (e.g.: 172.18.211.10) <input type="button" value="Add"/> |
| Total Entries: 1 | |
| Domain Name | IP Address |
| manager | 172.18.211.10 <input type="button" value="Delete"/> |

図 13-36 DNS Relay Static Settings 画面

以下の項目を使用して設定、表示を行います。

| 項目 | 説明 |
|-------------|------------------------|
| Domain Name | ドメイン名を入力します。 |
| IP Address | DNS リレー IP アドレスを指定します。 |

「Add」 ボタンをクリックして、入力した情報に基づいて新しいエントリを追加します。

エントリの削除

「Delete」 ボタンをクリックして、指定エントリを削除します。

DNS Resolver (DNS リゾルバ)

DNS Resolver Global Settings (DNS リゾルバグローバル設定)

スイッチの DNS リゾルバのグローバル状態を設定します。

Network Application > DNS Resolver > DNS Resolver Global Settings の順にメニューをクリックし、以下の画面を表示します。

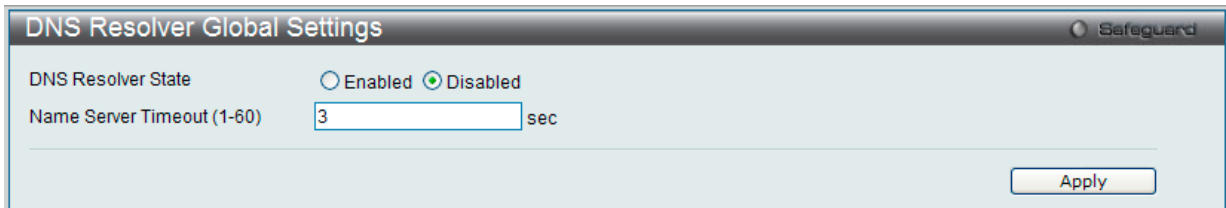


図 13-37 DNS Resolver Global Settings 画面

以下の項目を使用して設定、表示を行います。

| 項目 | 説明 |
|----------------------------|---|
| DNS Resolver State | ラジオボタンをクリックして DNS リゾルバ状態を「Enabled」(有効) / 「Disabled」(無効) にします。 |
| Name Server Timeout (1-60) | 指定のネームサーバからの応答を待つ最大時間。 |

「Apply」 ボタンをクリックして行った変更を適用します。

DNS Resolver Static Name Server Settings (DNS リゾルバスタティックネームサーバ設定)

スイッチに DNS リゾルバのネームサーバを作成します。スタティックネームサーバテーブルにプライマリネームサーバが存在している時に、新たにプライマリネームサーバを追加すると、既存のプライマリネームサーバは通常のネームサーバに変わります。追加されたプライマリネームサーバの IP アドレスが通常のネームサーバの IP アドレスと同じ場合、既存の通常ネームサーバはプライマリネームサーバとして変更され、新しいネームサーバは追加されません。プライマリのネームサーバが指定されない場合、最初に設定されたネームサーバが自動的にプライマリとして設定されます。削除したネームサーバの IP アドレスが既存のネームサーバの IP アドレスと一致した場合、そのネームサーバはプライマリかセカンダリかに関わらず削除されます。

Network Application > DNS Resolver > DNS Resolver Static Name Server Settings の順にメニューをクリックし、以下の画面を表示します。

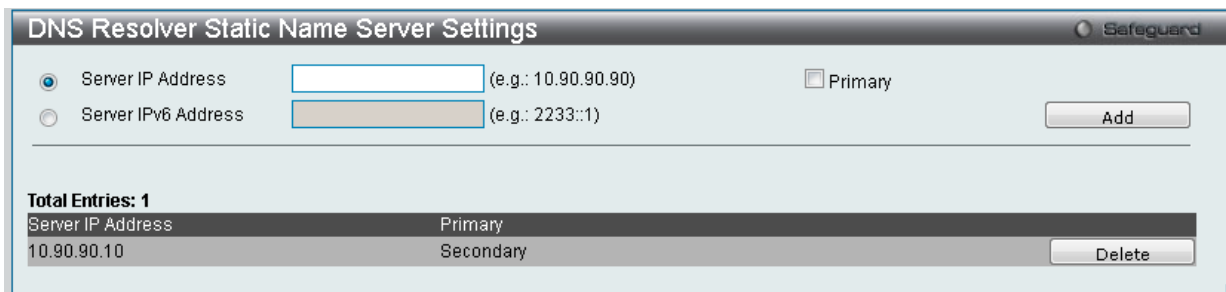


図 13-38 DNS Resolver Static Name Server Settings 画面

以下の項目を使用して設定、表示を行います。

| 項目 | 説明 |
|---------------------|--|
| Server IP Address | DNS リゾルバのネームサーバを追加します。「Primary」をチェックして、ネームサーバをプライマリネームサーバに指定します。 |
| Server IPv6 Address | DNS リゾルバのネームサーバ (IPv6) を追加します。「Primary」をチェックして、ネームサーバをプライマリネームサーバに指定します。 |

「Add」 ボタンをクリックして、入力した情報に基づいて新しいエントリを追加します。

エントリの削除

「Delete」 ボタンをクリックして、指定エントリを削除します。

DNS Resolver Dynamic Name Server Table (DNS リゾルバダイナミックネームサーバテーブル)

現在のDNS リゾルバネームサーバを表示します。

Network Application > DNS Resolver > DNS Resolver Dynamic Name Server Table の順にメニューをクリックし、以下の画面を表示します。

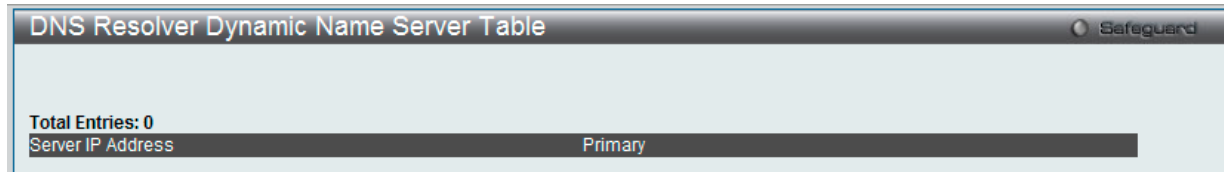


図 13-39 DNS Resolver Dynamic Name Server Table 画面

DNS Resolver Static Host Name Settings (DNS リゾルバスタティックホスト名設定)

スイッチにスタティックホスト名のエントリを作成します。

Network Application > DNS Resolver > DNS Resolver Static Host Name Settings の順にメニューをクリックし、以下の画面を表示します。

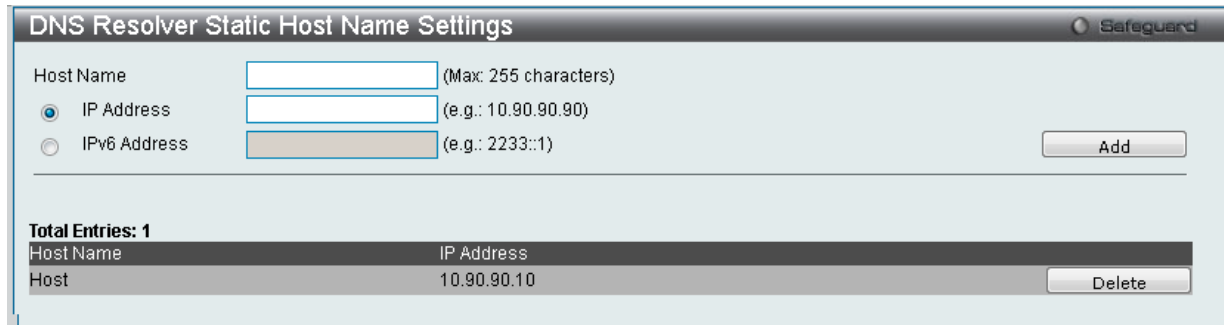


図 13-40 DNS Resolver Static Host Name Settings 画面

以下の項目を使用して設定、表示を行います。

| 項目 | 説明 |
|--------------|-----------------------|
| Host Name | ホスト名を入力します。 |
| IP Address | ホストの IP アドレスを入力します。 |
| IPv6 Address | ホストの IPv6 アドレスを入力します。 |

「Add」ボタンをクリックして、入力した情報に基づいて新しいエントリを追加します。

エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。

DNS Resolver Dynamic Host Name Table (DNS リゾルバダイナミックホスト名テーブル)

現在のホスト名のエントリを表示します。

Network Application > DNS Resolver > DNS Resolver Dynamic Host Name Table の順にメニューをクリックし、以下の画面を表示します。

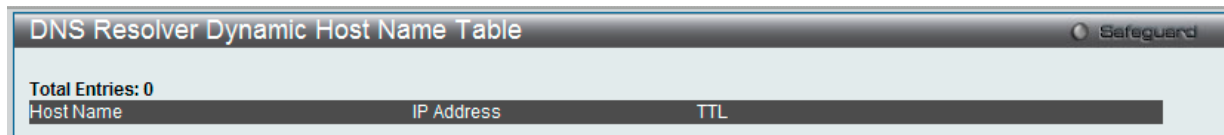


図 13-41 DNS Resolver Dynamic Host Name Table 画面

RCP Server Settings (RCP サーバ設定)

RCP サーバ情報を設定するために使用されます。サーバまたはリモートユーザ名が指定されない場合に、このグローバル RCP サーバ設定を使用できます。各システムに1つのRCPサーバだけが設定可能です。CLI コマンドでRCPサーバを指定せず、グローバルなRCPサーバが設定されていない場合、スイッチは、RCP コマンドの実行中、サーバのIPアドレスまたはリモートユーザ名を入力するように求めます。

Network Application > RCP Server Settings の順にメニューをクリックし、以下の画面を表示します。

図 13-42 RCP Server Settings 画面

以下の項目を使用して設定、表示を行います。

| 項目 | 説明 |
|------------|--|
| IP Address | グローバルな RCP サーバの IP アドレス。初期値では、未設定です。 |
| User Name | グローバルな RCP サーバにログインするためのリモートユーザ名。初期値では、グローバルなサーバのリモートユーザ名は未設定です。 |

「Apply」 ボタンをクリックして行った変更を適用します。

エントリの編集

1. 編集するエントリの「Edit」 ボタンをクリックして、以下の画面を表示します。

図 13-43 RCP Server Settings 画面 - Edit

2. 指定エントリを編集して「Apply」 ボタンをクリックします。

エントリの削除

「Delete」 ボタンをクリックして、指定エントリを削除します。

SMTP Settings (SMTP 設定)

SMTP (Simple Mail Transfer Protocol) は、以下の画面で入力するメール受信者にスイッチイベントを送信するスイッチの機能です。スイッチは SMTP のクライアントとして設定され、一方サーバはスイッチからメッセージを受信し、スイッチが設定した受信者に E-mail で適切な情報を送信します。これによって、小規模ワークグループや配線室の管理を簡素化、緊急のスイッチイベントの処理速度を向上、スイッチに起きた疑わしいイベントの記録によるセキュリティの強化など、スイッチ管理者の利便が図られます。

スイッチ用の SMTP サーバの設定と、問題がスイッチに発生した場合にスイッチのログファイルを送信する E-mail アドレスを設定します。

スイッチは、以下のイベントが 1 つ以上起きた場合に受信者に E-mail を送信します。

- スイッチでコールドスタートが起きた場合。
- リンクダウン状態でポートが接続した場合。
- リンクアップ状態でポートが接続した場合。
- SNMP 認証がスイッチによって拒否された場合。
- スイッチがスイッチ設定エントリを NVRAM に保存した場合。
- ファームウェアのダウンロードが行われている間に TFTP に異常が起きた場合。この異常には、「in-process」、「invalid-file」、「violation」、「file-not-found」、「complete」、「time-out」の各メッセージが TFTP サーバから送られた場合を含みます。
- スイッチでシステムリセットが行われた場合。

スイッチイベントに関する、SMTP サーバからの E-mail 内の情報は以下の通りです。

- 送信元デバイス名および IP アドレス。
- メッセージを送信した SMTP サーバとクライアントのアイデンティティを示すタイムスタンプ、およびスイッチからメッセージを受信した日時。リレーされているメッセージは、リレーごとにタイムスタンプがあります。
- E-mail メッセージの送信をさせた、スイッチで起きたイベント。
- ユーザがイベントに対し保存やファームウェアの更新などの処理を行うと、そのタスクを行ったユーザの IP アドレス、MAC アドレスおよびユーザ名がイベントが起きたことを知らせるシステムメッセージと共に送信されます。
- 同じイベントが 2 回以上起きる場合、2 回目のメールメッセージと続いて繰り返されるメールメッセージには、メールメッセージのタイトルにシステムエラーメッセージを記載されます。

送信過程で起こるイベントについて以下に詳細を説明します。

- 緊急メールは即座に受信者に割り当てられて最優先で送信され、通常のメールは後の順番になります。
- キューに置かれる未送信のメールメッセージの最大数は 30 を超えることはできません。送信待ちキューがフルの場合は新しいメッセージはすべて廃棄されます。
- メール受信者への最初のメッセージが受け取られない場合、そのメッセージは送信待ちキューに置かれて順番を待ち、他のメッセージの送信が行われます。
- 受信者へのメール送信指示の最大数は 3 です。メールメッセージ送信指示は指示数が最大数になるまで 5 分ごとに行われます。送信指示数が最大の時に送信に失敗した場合、そのメッセージはドロップされメール受信者には送信されません。
- スイッチがシャットダウンまたは再起動された場合、送信待ちキュー内のメッセージは消失します。

Network Application > SMTP Settings の順にメニューをクリックし、以下の画面を表示します。

図 13-44 SMTP Service Settings 画面

以下の項目を使用して設定、表示を行います。

| 項目 | 説明 |
|----------------------------|---|
| SMTP Global Settings | |
| SMTP State | 本デバイスの SMTP サービスを「Enabled」(有効)または「Disabled」(無効)にします。 |
| SMTP Server Address | 外部デバイスの SMTP サーバの IP アドレスを入力します。これはメールを送信するデバイスとなります。 |
| SMTP Server Port (1-65535) | SMTP サーバに接続するスイッチの仮想ポート番号 (1-65535) を入力します。SMTP の一般的なポート番号は 25 です。 |
| Self Mail Address | メールメッセージの送信元 E-mail アドレスを入力します。このアドレスは受信者に送られる E-mail メッセージに送信元として記載されます。このスイッチに設定できるセルフメールアドレスは 1 つだけです。英数 64 文字以内で設定します。 |
| SMTP Mail Receiver Address | |
| Add A Mail Receiver | E-mail アドレスを入力し、「Add」ボタンをクリックします。8 個までの E-mail アドレスを追加することができます。アドレスを削除する場合は、画面下部にある「Mail Receiver Address」テーブルで削除するエントリの「Delete」ボタンをクリックします。 |
| Send a Test Mail to All | |
| Subject | 設定したすべてのアドレスに送信するテストメールの題名を入力します。 |
| Content | 設定したすべてのアドレスに送信するテストメールの内容を入力します。 |

「Apply」ボタンをクリックして各セクションで行った変更を適用します。

「Add」ボタンをクリックして、入力した情報に基づいて新しいエントリを追加します。

「Delete」ボタンをクリックして、指定エントリを削除します。

SNTP (SNTP 設定)

SNTP (Simple Network Time Protocol) はインターネット経由でコンピュータのクロックに同期するプロトコルです。標準時と周波数標準サービスへのアクセス、サーバとクライアントの SNTP サブネットの体系付け、および各関係者のシステムクロックの調整を行う包括的なメカニズムを提供します。

SNTP Settings (SNTP 設定)

スイッチに時刻を設定します。

Network Application > SNTP > SNTP Settings の順にクリックし、以下の画面を表示します。

図 13-45 SNTP Settings 画面

以下の項目を使用して設定、表示を行います。

| 項目 | 説明 |
|--|--|
| Status | |
| SNTP State | SNTP を「Enabled」(有効) または「Disabled」(無効) にします。初期値は「Disabled」です。 |
| Current Time | 現在の日付と時刻を表示します。 |
| Time Source | システム時刻を設定するタイムソースを表示します。 |
| SNTP Settings | |
| IPv4 SNTP First Server | システム時刻を受け取るプライマリ SNTP サーバの IPv4 アドレスを設定します。 |
| IPv4 SNTP Second Server | システム時刻を受け取るセカンダリ SNTP サーバの IPv4 アドレスを設定します。 |
| IPv6 SNTP First Server | システム時刻を受け取るプライマリ SNTP サーバの IPv6 アドレスを設定します。 |
| IPv6 SNTP Second Server | システム時刻を受け取るセカンダリ SNTP サーバの IPv6 アドレスを設定します。 |
| SNTP Poll Interval In Seconds (30-99999) | SNTP 情報の更新リクエストの送信間隔 (秒) を設定します。 |

「Apply」 ボタンをクリックし、デバイスに SNTP 設定を適用します。

Time Zone Settings (タイムゾーン設定)

以下の画面では、SNTP 用のタイムゾーンとサマータイム (Daylight Saving Time) の設定を行います。

Network Application > SNTP > Time Zone Settings の順にメニューをクリックし、以下の設定画面を表示します。

図 13-46 TimeZone Settings 画面

以下に、画面の各項目を示します。

| 項目 | 説明 |
|--|--|
| Daylight Saving Time State | デバイスに設定するサマータイムの種類を設定します。 <ul style="list-style-type: none"> Disabled - サマータイムを無効にします。(初期値) Repeating - サマータイムを周期的に有効にします。このオプションでは開始と終了のタイミングを設定する必要があります。 Annual - サマータイムを日付指定で有効にします。このオプションでは開始と終了の日付を設定する必要があります。 |
| Daylight Saving Time Offset in Minutes | プルダウンメニューを使用して、サマータイムによる調整時間を 30、60、90、120 分から選択します。 |
| Time Zone Offset: from GMT in +/- HH:MM | プルダウンメニューを使用して、GMT (グリニッジ標準時) からのオフセット時間を選択します。 |
| DST Repeating Settings | |
| Repeating モードを使用すると、DST (サマータイム) の設定を指定した期間で自動的に調整できるようになります。本モードでは、法則に従って指定される DST (サマータイム) の開始日と終了日が必要です。例えば、サマータイムを 4 月の第 2 週の土曜日から、10 月の最終週の日曜日までと指定することができます。 | |
| From: Which Week of The Month | 月の第何週から DST が始まるかを設定します。 <ul style="list-style-type: none"> First - 月の最初の週に設定します。 Second - 月の 2 番目の週に設定します。 Third - 月の 3 番目の週に設定します。 Fourth - 月の 4 番目の週に設定します。 |
| From: Day Of Week | DST が開始する曜日を指定します。Sun、Mon、Tue、Web、Tues、Fri、Sat |
| From: Month | DST が開始する月を指定します。Jan、Feb、May、Jun、Jul、Aug、Sep、Oct、Nov、Dec |
| From: Time In HH MM | DST が開始する時間を指定します。 |

| 項目 | 説明 |
|---|--|
| To: Which Week of The Month | 月の第何週で DST が終わるかを設定します。 <ul style="list-style-type: none"> • First - 月の最初の週に設定します。 • Second - 月の 2 番目の週に設定します。 • Third - 月の 3 番目の週に設定します。 • Fourth - 月の 4 番目の週に設定します。 |
| To: Day of Week | DST が終了する曜日を指定します。 |
| To: Month | DST が終了する月を指定します。 |
| To: Time in HH MM | DST が終了する時間を指定します。 |
| DST Annual Settings | |
| Annual モードを使用すると、DST (サマータイム) 設定を指定した詳細な期日で自動的に調整できるようになります。本モードを使用すると、DST (サマータイム) の開始日と終了日を簡潔に指定することが必要です。例: DST を 4 月 3 日から開始し、10 月 14 日を終了と設定します。 | |
| From: Month | DST が開始する月を指定します。(毎年) |
| From: Day | DST が開始する日を指定します。(毎年) |
| From: Time in HH MM | DST が開始する時間を指定します。(毎年) |
| To: Month | DST が終了する月を指定します。(毎年) |
| To: Day | DST が終了する日を指定します。(毎年) |
| To: Time in HH MM | DST が終了する時間を指定します。(毎年) |

設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

UDP (UDP 設定)

UDP Helper (UDP ヘルパー)

UDP ヘルパーは、UDP 送信先ポートに応じて、特定のブロードキャストをサーバに送信します。これは、すべてのサブネットに対するブロードキャストパケットの伝播に比べてネットワークトラフィックを減少させます。

UDP Helper Settings (UDP ヘルパー設定)

UDP ヘルパーを設定します。

Network Application > UDP > UDP Helper > UDP Helper Settings の順にメニューをクリックし、以下の画面を表示します。

図 13-47 UDP Helper Settings 画面

以下の項目を使用して設定、表示を行います。

| 項目 | 説明 |
|------------------|--|
| UDP Helper State | スイッチにおける UDP ヘルパー機能を有効または無効にします。 |
| UDP Port | 本オプションは、スイッチの UDP ヘルパー機能に UDP ポートを追加するために使用されます。 <ul style="list-style-type: none"> Time - タイムサービスを指定します。UDP ポート番号は 37 です。 TACACS - TACACS (Terminal Access Controller Access Control System) サービスを指定します。UDP ポート番号は 49 です。 DNS - DNS (Domain Naming System) サービスを指定します。UDP ポート番号は 53 です。 TFTP - TFTP (Trivial File Transfer Protocol) サービスを指定します。UDP ポート番号は 69 です。 NetBIOS NS - NetBIOS ネームサーバサービスを指定します。UDP ポート番号は 137 です。 NetBIOS DS - NetBIOS データグラムサーバサービスを指定します。UDP ポート番号は 138 です。 UDP Port - リストにないサービスに使用する UDP ポートを入力します。この値は 0-65535 である必要があります。 |

「Apply」ボタンをクリックして行った変更を適用します。

エントリの追加

「Add」ボタンをクリックして、入力した情報に基づいて新しいエントリを追加します。

エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。

UDP Helper Server Settings (UDP ヘルパーサーバ設定)

UDP ヘルパーサーバを設定します。

Network Application > UDP > UDP Helper > UDP Helper Server Settings の順にメニューをクリックし、以下の画面を表示します。

図 13-48 UDP Helper Server Settings 画面

以下の項目を使用して設定、表示を行います。

| 項目 | 説明 |
|-------------------|---|
| Interface Name | 使用する IP インタフェース名を入力します。12 文字以内で指定します。 |
| Server IP Address | 入力した情報に基づいて、UDP ヘルパーサーバの IP アドレスを入力します。 |

「Add」 ボタンをクリックして、入力した情報に基づいて新しいエントリを追加します。

エントリの検出

「Find」 ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

エントリの参照

「View All」 ボタンをクリックして、すべての定義済みエントリを表示します。

「[View Detail](#)」 リンクをクリックすると、指定エントリに関する詳細情報を表示します。

「[View Detail](#)」 リンクをクリックすると、以下の画面が表示されます。

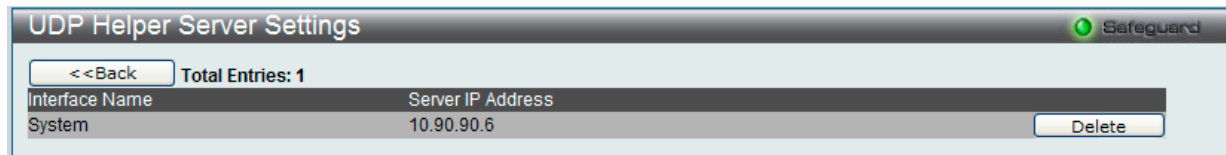


図 13-49 UDP Helper Server Settings window (詳細表示)

エントリの削除

「Delete」 ボタンをクリックして、指定エントリを削除します。

「<<Back」 ボタンをクリックして前のページに戻ります。

Flash File System Settings (フラッシュファイルシステム設定)

フラッシュファイルシステムを使用する理由

古いスイッチシステムでは、ファームウェア、コンフィグレーション、およびログ情報は固定アドレスとサイズを持つフラッシュに保存されます。これは、最大のコンフィグレーションファイルが 2M バイトだけであり、現在のコンフィグレーションが 40K バイトにすぎなくても、フラッシュストレージスペースの 2M バイトを消費することを意味します。また、コンフィグレーションファイル番号とファームウェア番号は固定されています。コンフィグレーションファイルまたはファームウェアサイズが元々設計されたサイズを超えている場合、互換性の問題が発生します。

使用するシステムにおけるフラッシュファイルシステム

フラッシュファイルシステムは、フラッシュメモリにおける柔軟なファイル操作を提供します。すべてのファームウェア、コンフィグレーション情報、および Syslog ログ情報はフラッシュ内のファイルに保存されます。これは、すべてのファイルが取得したフラッシュスペースが固定されておらず、実ファイルサイズであることを意味します。フラッシュスペースが十分であれば、より多くのコンフィグレーションファイルまたはファームウェアファイルをダウンロードできます。また、フラッシュファイル情報の表示やファイル名の変更、および削除するコマンドを使用することができます。その上、必要に応じて、起動用のランタイムイメージや動作するコンフィグレーションファイルを設定できます。

ファイルシステムに不具合がある場合、Z- モデムを使用して直接システムにバックアップファイルをダウンロードすることができます。

Network Application > Flash File System Settings の順にメニューをクリックし、以下の画面を表示します。

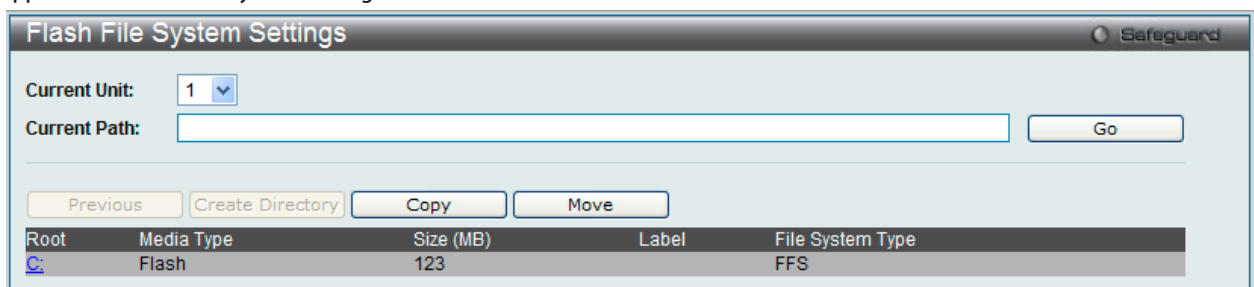


図 13-50 Flash File System Settings 画面

「Current Path」に現在のパスを入力し、「Go」ボタンをクリックすると入力したパスに遷移します。

「C:」リンクをクリックすると、「C:」ドライブに遷移します。

「C:」リンクをクリックすると、以下の画面が表示されます。

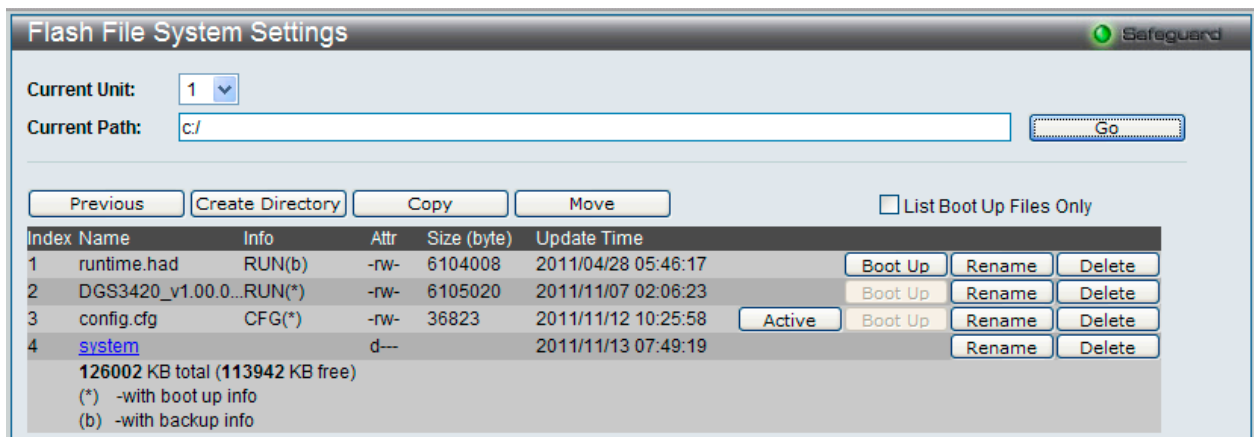


図 13-51 Flash File System Settings 画面

以下の項目を使用して設定、表示を行います。

| 項目 | 説明 |
|-------------------------|--|
| Previous | 前のページに戻ります。 |
| Create Directory | スイッチのファイルシステムに新しいディレクトリを作成します。 |
| Copy | 指定ファイルをスイッチにコピーします。 |
| Move | 指定ファイルをスイッチに移動します。 |
| List Boot Up Files Only | チェックすると起動ファイルだけを表示します。 |
| Active | アクティブなランタイムコンフィグレーションとして指定したコンフィグファイルを設定します。 |
| Boot Up | 起動用のブートアップイメージとして指定したランタイムイメージを設定します。 |
| Rename | 指定ファイルを変更します。 |
| Delete | ファイルシステムから指定ファイルを削除します。 |

ファイルのコピー

1. 「Copy」 ボタンをクリックすると、以下の画面が表示されます。

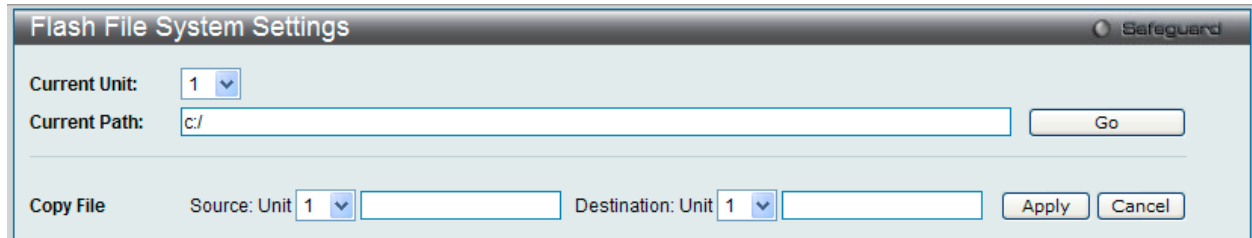


図 13-52 Flash File System Settings 画面 - Copy

2. このスイッチのファイルシステムにファイルをコピーする場合、送信元と送信先のパスを入力します。
3. 「Apply」 ボタンをクリックして、コピーを開始します。「Cancel」 ボタンをクリックすると処理は破棄されます。

ファイルの移動

「Move」 ボタンをクリックすると、以下の画面が表示されます。

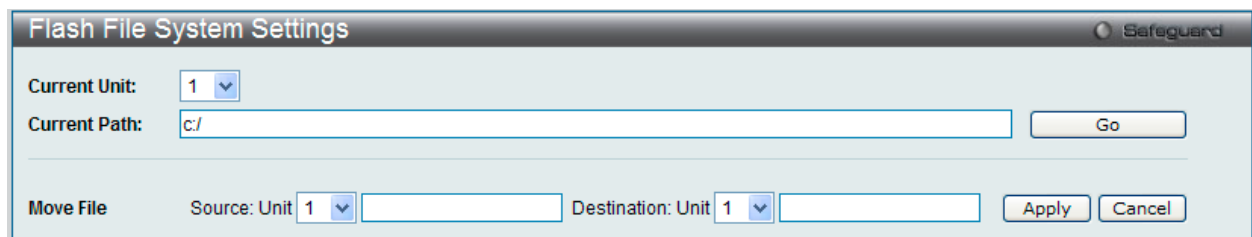


図 13-53 Flash File System Settings - Move 画面

ファイルを別の場所に移動する場合、「Source」(送信元) と「Destination」(送信先) のパスを入力する必要があります。

「Apply」 ボタンをクリックして、コピーを開始します。

「Cancel」 ボタンをクリックすると処理は破棄されます。

ファイル名の変更

1. 「Rename」 ボタンをクリックすると、以下の画面が表示されます。

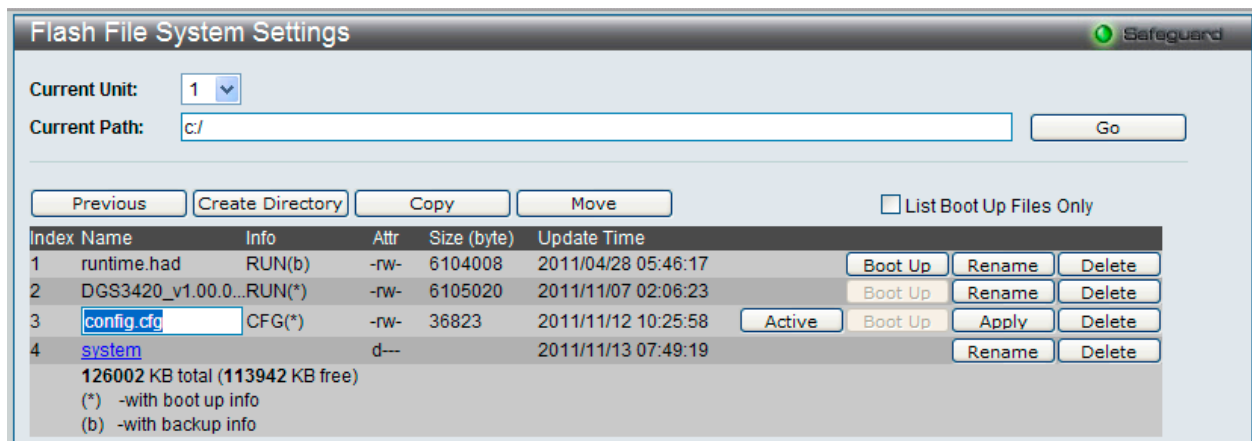


図 13-54 Flash File System Settings 画面 - Rename

2. ファイル名を変更して「Apply」 ボタンをクリックします。

第 14 章 OAM (Operations, Administration, Maintenance : 運用・管理・保守)

以下は OAM サブメニューの説明です。

必要に応じて、設定 / 変更 / 修正を行ってください。

| サブメニュー | 説明 | 参照ページ |
|--|--|---------------------|
| CFM (Connectivity Fault Management : 接続 性障害管理) | CFM 機能を設定します。以下のメニューがあります。 CFM Settings (CFM 設定)、CFM Port Settings (CFM ポート設定)、CFM MIPCCM Table (CFM MIPCCM テーブル)、CFM Loopback Settings (CFM ループバック設定)、CFM Linktrace Settings (CFM リンクトレース設定)、CFM Packet Counter (CFM パケットカウンタ)、CFM Fault Table (CFM 障害テーブル)、CFM MP Table (CFM MP テーブル) | 401 |
| Ethernet OAM (イーサネット OAM) | ポートにイーサネット OAM モード、イベント、ログを設定します。以下のメニューがあります。 Ethernet OAM Settings (イーサネット OAM 設定)、Ethernet OAM Configuration Settings (イーサネット OAM コンフィグレーション設定)、Ethernet OAM Event Log (イーサネット OAM イベントログ)、Ethernet OAM Statistics (イーサネット OAM 統計情報) | 412 |
| DULD Settings (単方向リンク検出設定) | ポートにおいて単方向リンク検出の設定および表示を行います。 | 415 |
| Cable Diagnostics (ケーブル診断機能) | ケーブル診断を行います。 | 416 |

CFM (Connectivity Fault Management : 接続性障害管理)

CFM Settings (CFM 設定)

CFM 機能を設定します。

OAM > CFM > CFM Settings の順にメニューをクリックし、以下の画面を表示します。

図 14-1 CFM Settings 画面

以下の項目を設定できます。

| 項目 | 説明 |
|---------------------|--|
| CFM Global Settings | |
| CFM State | CFM 機能を有効または無効にします。 |
| AIS Trap State | AIS トラップを有効 / 無効にします。 |
| LCK Trap State | LCK トラップを有効 / 無効にします。 |
| All MPs Reply LTRs | Link Trace Reply (LTR) メッセージに回答するために、すべての MP (メンテナンスポイント) を有効または無効にします。 |
| CFM MD Settings | |
| MD | メンテナンスドメインの名称を入力します。22 文字内で指定します。 |
| MD Index | 使用するメンテナンスドメインインデックスを入力します。 |
| Level | メンテナンスドメインのレベルを選択します。レベルは、0-7 の範囲で設定します。0 が最も低く、7 が最も高いレベルです。 |
| MIP | MIP の作成を制御します。 <ul style="list-style-type: none"> None - MIP を作成しません。(初期値) Auto - ポートがこの MD の MEP で設定されないと、MIP は常にこの MD のどのポートにも作成されます。MA の中間スイッチでは、この設定は、MIP がこのデバイスで作成されるために「Auto」である必要があります。 Explicit - 次に存在する低いレベルのポートに設定済みの MEP がなく、ポートがこの MD の MEP に設定されないと、MIP がこの MD のどのポートにも作成されません。 |
| Sender ID TLV | SenderID TLV の転送を制御します。 <ul style="list-style-type: none"> None - SenderID TLV を転送しません。(初期値) Chassis - シャーシ ID 情報を持つ SenderID TLV を転送します。 Manage - 管理アドレス情報を持つ SenderID TLV を転送します。 Chassis Manage - シャーシ ID 情報と管理アドレス情報を持つ SenderID TLV を転送します。 |

「Apply」 ボタンをクリックして各セクションで行った変更を適用します。

エントリの編集

1. 編集するエントリの「Edit」ボタンをクリックして、以下の画面を表示します。

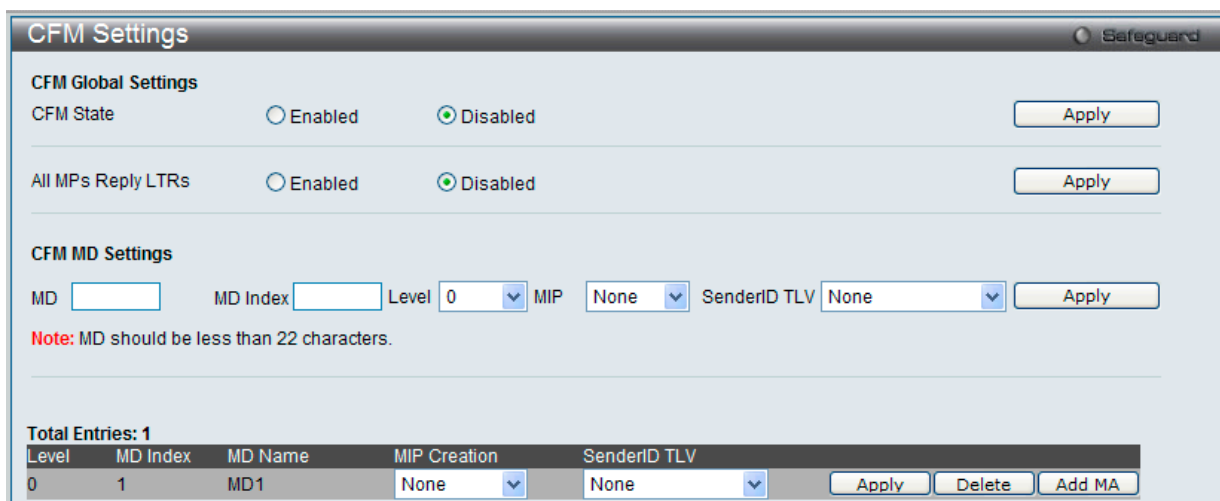


図 14-2 CFM Settings 画面 - Edit

2. 指定エントリを編集して「Apply」ボタンをクリックします。

エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。

注意 グループ名は 22 文字未満とします。

CFM メンテナンスアソシエーション (MA) 設定

メンテナンスアソシエーションを設定します。

OAM > CFM > CFM Settings 画面で「Add MA」ボタンをクリックし、以下の画面を表示します。

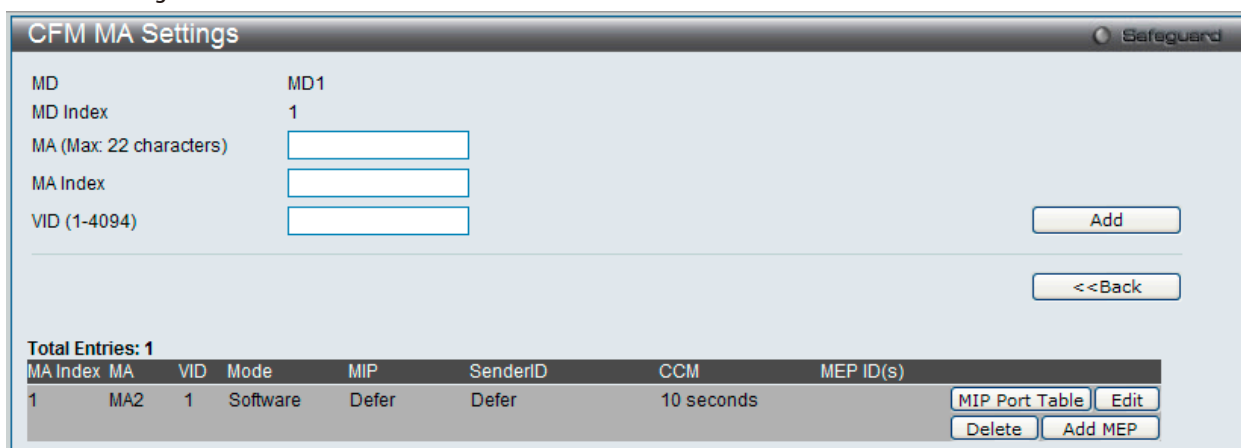


図 14-3 CFM MA Settings 画面

以下の項目が使用できます。

| 項目 | 説明 |
|--------------|--|
| MA | メンテナンスアソシエーションの名称を入力します。 |
| MA Index | メンテナンスアソシエーションのインデックスを入力します。 |
| VID (1-4094) | VLAN 識別子。異なる MA は異なる VLAN に関連付ける必要があります。 |

「<<Back」ボタンをクリックし、変更を破棄して前のページに戻ります。

「MIP Port Table」ボタンをクリックして、CFM MIP Table を参照します。

「Add MEP」ボタンをクリックして、MEP (Maintenance End Point) エントリを追加します。

エントリの削除

テーブルからエントリを削除するためには、削除対象のエントリの列の「Delete」ボタンをクリックします。

エントリの追加

項目入力後、「Add」ボタンをクリックします。

エントリの編集

1. エントリ横の「Edit」ボタンをクリックして以下の画面を表示します。

図 14-4 CFM MA Settings 画面 - Edit

以下の項目が使用できます。

| 項目 | 説明 |
|--------------|--|
| MA | メンテナンスアソシエーションの名称を入力します。 |
| VID (1-4094) | VLAN 識別子。異なる MA は異なる VLAN に関連付ける必要があります。 |
| Mode | プルダウンメニューを使用して、MA の動作モード（CFM ソフトウェアまたはハードウェアモード）を選択します。 <ul style="list-style-type: none"> Software - MA は CFM ソフトウェアモードで動作します。（初期値） Hardware - MA は CFM ハードウェアモードで動作します。 |
| MIP | MIP の作成を制御します。 <ul style="list-style-type: none"> None - MIP を作成しません。（ハードウェアモード：初期値） Defer - この MA が関連するメンテナンスドメインの設定を継承します。（ソフトウェアモード：初期値） Auto - ポートがこの MD の MEP で設定されないと、MIP は常にこの MD のどのポートにも作成されます。MA の中間スイッチでは、この設定は、MIP がこのデバイスで作成されるために「Auto」である必要があります。 Explicit - 次に存在する低いレベルのポートに設定済みの MEP がなく、ポートがこの MD の MEP に設定されないと、MIP がこの MD のどのポートにも作成されません。 <p>注意 CFM ハードウェアモードでは初期値は「None」です。</p> |
| SenderID | これは、SenderID TLV の転送を制御します。 <ul style="list-style-type: none"> None - SenderID TLV を転送しません。 Chassis - シャーシ ID 情報を持つ SenderID TLV を転送します。 Manage - 管理アドレス情報を持つ SenderID TLV を転送します。 Chassis Manage - シャーシ ID 情報と管理アドレス情報を持つ SenderID TLV を転送します。 Defer - この MA が関連するメンテナンスドメインの設定を継承します。（初期値） |
| CCM | これは CCM 送信間隔です。 <ul style="list-style-type: none"> 3.3ms - 3.3（ミリ秒）。これは CFM ハードウェアモードでのみ動作します。 10ms - 10（ミリ秒）。これは CFM ハードウェアモードでのみ動作します。 100ms - 100（ミリ秒）。推奨されません。テストの目的のために使用します。 1sec - 1（秒） 10sec - 10（秒）（初期値） 1min - 1（分） 10min - 10（分） |
| MEP ID(s) | メンテナンスアソシエーションに含まれる MEP ID を指定します。 <ul style="list-style-type: none"> Add - MEP ID を追加します。 Delete - MEP ID を削除します。 <p>初期値では、初めて作成されたメンテナンスアソシエーションには MEP ID はありません。MEP ID の範囲は、1-8191 です。</p> |

2. 項目設定後、「Apply」ボタンをクリックします。

CFM MEP 設定

MEP を追加します。

OAM > CFM > CFM Settings 画面で「Add MEP」ボタンをクリックし、以下の画面を表示します。

図 14-5 CFM MEP Settings 画面

以下の項目を設定できます。

| 項目 | 説明 |
|-----------------|---|
| MEP Name | MEP 名を入力します。デバイスに設定されたすべての MEP 内で固有です。32 文字以内で指定します。 |
| MEP ID (1-8191) | MA の MEP ID リストに設定される MEP ID を入力します。 |
| Port | プルダウンメニューを使用してポートを指定します。本ポートは MA の関連付けられている VLAN メンバである必要があります。CFM ハードウェアモードでは、本ポートは MA の関連付けられている VLAN のメンバである必要があります。 |
| MEP Direction | MEP の方向を指定します。 <ul style="list-style-type: none"> Inward - 内向き（アップ）MEP。内向きの MEP は、内側から受信する同じかそれ以下のレベルにあるすべての CFM フレームを破棄します。そして、フレームの送信元が内向きまたは外向きにかかわらず、より高いレベルにあるすべての CFM フレームを転送します。 Outward - 外向き（ダウン）MEP。外向きのポートは、ブリッジリレー機能側から受信する同じかそれ以下のレベルにあるすべての CFM フレームを破棄します。それは、そのレベルにあるすべての CFM フレームを処理して、ブリッジポートからから受信する低いレベルの CFM フレームすべてを破棄します。外向きポートは、フレームの送信先の方向にかかわらず、より高いレベルにあるすべての CFM フレームを転送します。 <p>注意 「Hardware」モードが「CFM MA Settings」画面で選択される場合、「Outward」だけが利用可能です。</p> |

項目設定後、「Add」ボタンをクリックします。

MIP ポートテーブルの参照

MIP ポートテーブルを参照します。

OAM > CFM > CFM Settings 画面で「MIP Port Table」ボタンをクリックします。

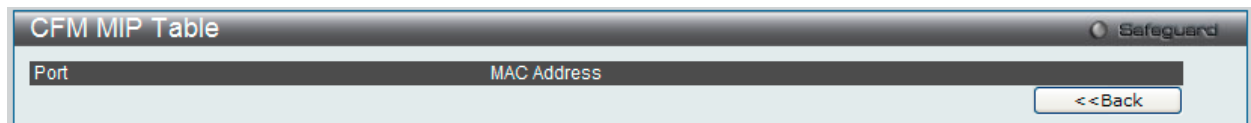


図 14-6 CFM MIP Table 画面

MEP エントリに関する詳細情報の参照

「View Detail」ボタンをクリックし、以下の画面を表示します。

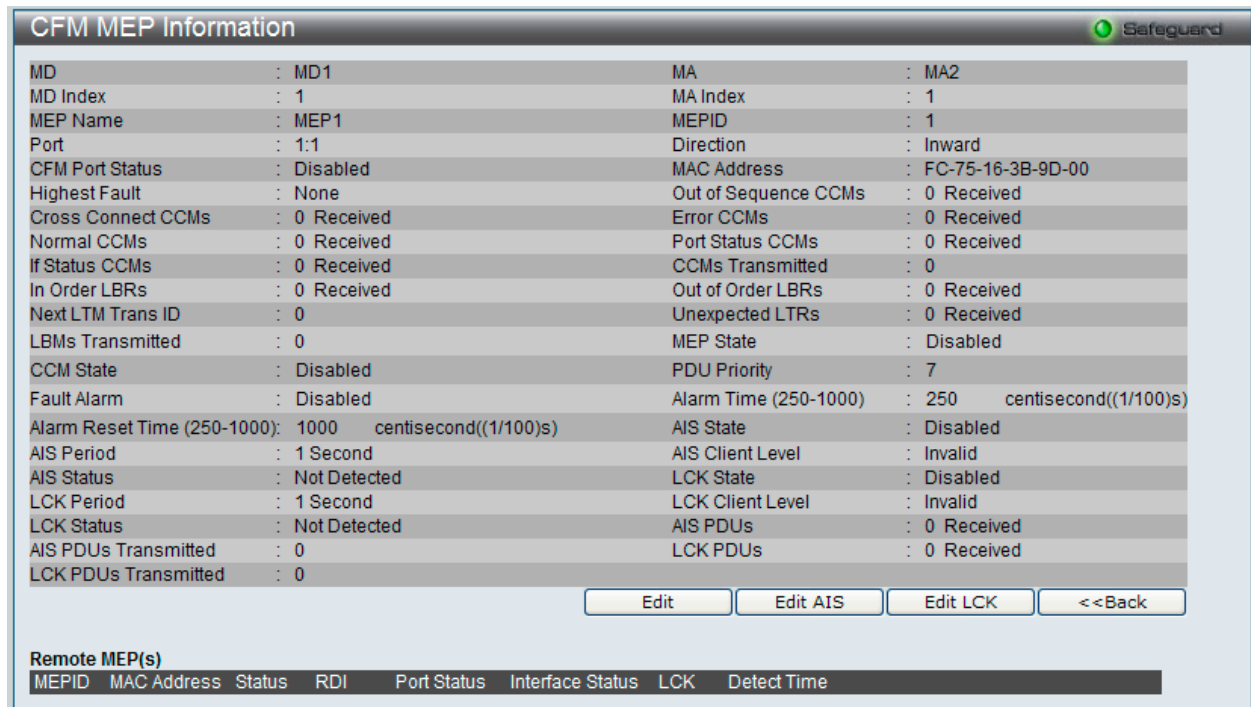


図 14-7 CFM MEP Information 画面

MEP の編集

「Edit」ボタンをクリックし、以下の画面を表示します。

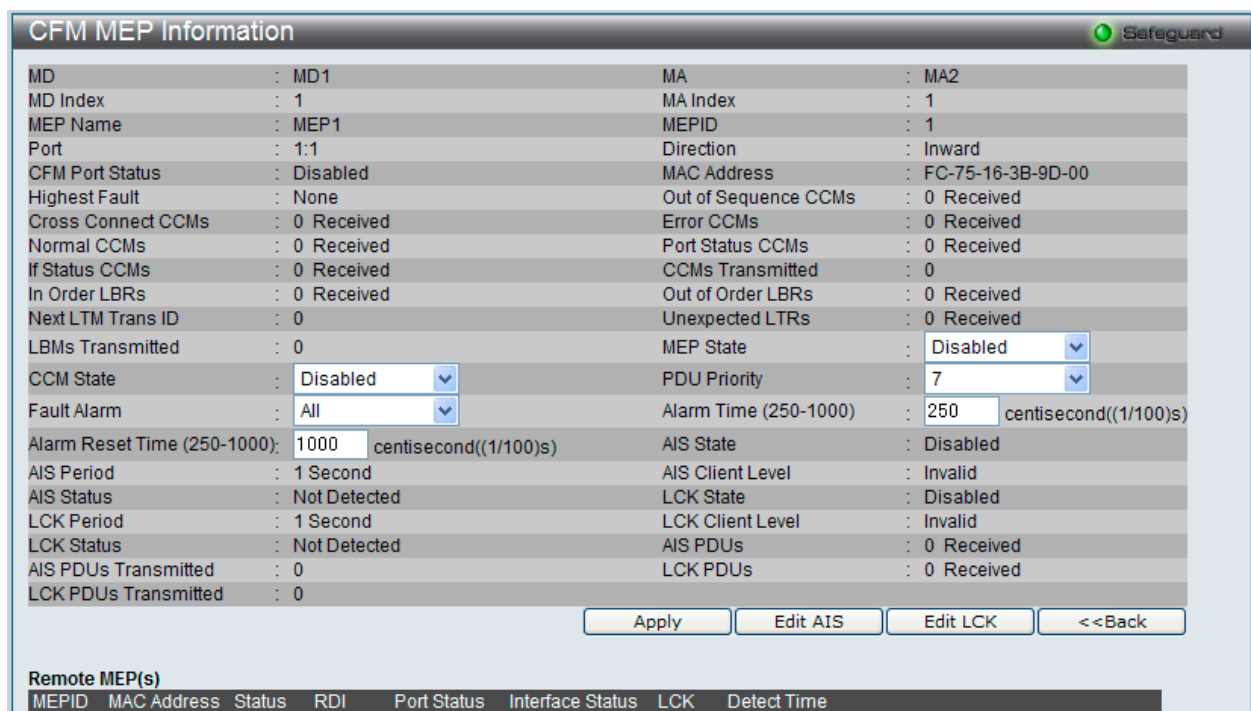


図 14-8 CFM MEP Information 画面 - Edit

以下の項目を設定または表示できます。

| 項目 | 説明 |
|-----------------------------|--|
| MEP State | MEP 管理状態を「Enabled」(有効) / 「Disabled」(無効) にします。初期値は「Disabled」です。 |
| CCM State | CCM 送信状態を「Enabled」(有効) / 「Disabled」(無効) にします。初期値は「Disabled」です。 |
| PDU Priority | 802.1p 優先度は MEP によって送信された CCM および LTM メッセージに設定されます。初期値は 7 です。 |
| Fault Alarm | これは、MEP によって送信される障害アラームの制御タイプです。 <ul style="list-style-type: none"> All - すべての障害アラームのタイプが送信されます。 Mac Status - 優先度が「Some Remote MEP MAC Status Error」(リモート MEP の MAC ステータスエラー) 以上である障害アラームだけが送信されます。 Remote CCM - 優先度が「Some Remote MEP Down」(リモート MEP のダウン) 以上である障害アラームだけが送信されます。 Error CCM - 優先度が「Error CCM Received」(エラー CCM の受信) 以上である障害アラームだけが送信されます。 Xcon CCM - 優先度が「Cross-connect CCM Received」(クロスコネクト CCM の受信) 以上である障害アラームだけが送信されます。 None - 障害アラームは送信されません。(初期値) |
| Alarm Time (250-1000) | これは、障害検出後に障害アラームが送信されるまでの経過時間です。範囲は 250-1000 (センチ秒) です。初期値は 250 (センチ秒) です。 |
| Alarm Reset Time (250-1000) | これは、障害による再度アラーム送信前の検知が始動されるまでの待機時間です。範囲は 250-1000 (センチ秒) です。初期値は 1000(センチ秒) です。 |

「Apply」 ボタンをクリックして行った変更を適用します。

「<<Back」 ボタンをクリックし、変更を破棄してと前のページに戻ります。

「Edit AIS」 ボタンをクリックして AIS を設定します。

「Edit LCK」 ボタンをクリックして LCK を設定します。

Extension AIS 設定

1. 「Edit AIS」 ボタンをクリックすると、以下の画面が表示されます。

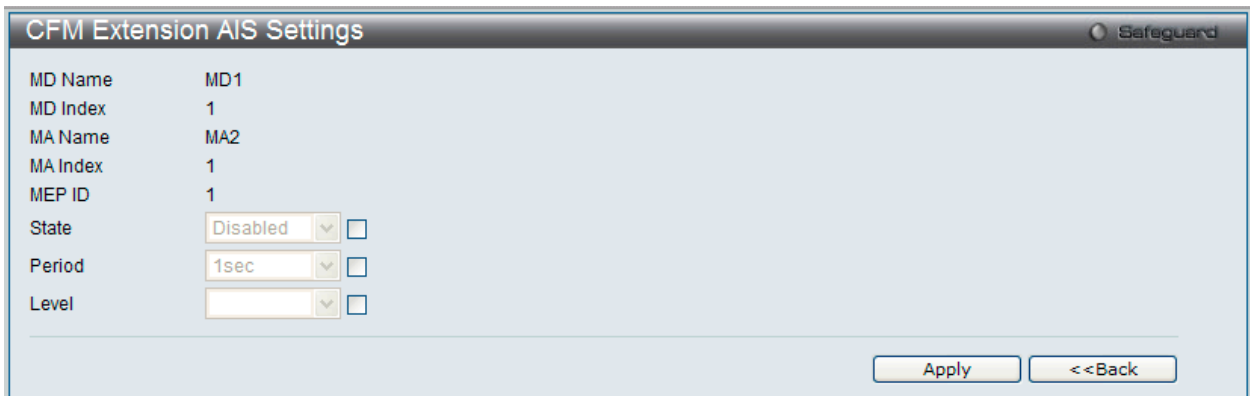


図 14-9 CFM Extension AIS (Edit) 画面

以下の項目を設定または表示できます。

| 項目 | 説明 |
|--------|--|
| State | チェックし、プルダウンメニューを使用して、AIS 機能を「Enabled」(有効) / 「Disabled」(無効) にします。 |
| Period | チェックし、プルダウンメニューを使用して、AIS PDU 送信間隔を選択します。 |
| Level | チェックし、プルダウンメニューを使用して、MEP が AIS PDU を送信するクライアントレベル ID を選択します。クライアント MD レベルの初期値は最も近いクライアントレイヤの MIP と MEP が存在する MD レベルです。オプションを 0-7 からを選択します。 |

2. エントリの編集を行い、「Apply」 ボタンをクリックします。

「<<Back」 ボタンをクリックし、変更を破棄してと前のページに戻ります。

Extension LCK 設定

1. 「Edit LCK」 ボタンをクリックすると、以下の画面が表示されます。

図 14-10 CFM Extension LCK Settings (Edit) 画面

以下の項目を設定または表示できます。

| 項目 | 説明 |
|--------|--|
| State | チェックし、プルダウンメニューを使用して、LCK 機能を「Enabled」(有効)/「Disabled」(無効)にします。 |
| Period | チェックし、プルダウンメニューを使用して、LCK PDU 送信間隔を選択します。 |
| Level | チェックし、プルダウンメニューを使用して、MEP が LCK PDU を送信するクライアントレベル ID を選択します。クライアント MD レベルの初期値は最も近いクライアントレイヤの MIP と MEP が存在する MD レベルです。オプションを 0-7 からを選択します。 |

2. エントリの編集を行い、「Apply」 ボタンをクリックします。

「<<Back」 をボタンをクリックし、変更を破棄してと前のページに戻ります。

CFM Port Settings (CFM ポート設定)

CFM ポート状態を有効または無効にします。

OAM > CFM > CFM Port Settings の順にメニューをクリックし、以下の画面を表示します。

図 14-11 CFM Port Settings 画面

設定対象となる項目は以下の通りです。

| 項目 | 説明 |
|-------------------|-------------------------------------|
| Unit | ユニットの ID を指定します。 |
| From Port/To Port | 本設定に使用されるポート範囲を選択します。 |
| State | 特定ポートの CFM 設定を有効または無効にします。初期値は無効です。 |

「Apply」 ボタンをクリックし、変更を有効にします。

CFM MIPCCM Table (CFM MIPCCM テーブル)

CFM MIPCCM 情報を表示します。

OAM > CFM > CFM MIPCCM Table の順にメニューをクリックし、以下の画面を表示します。

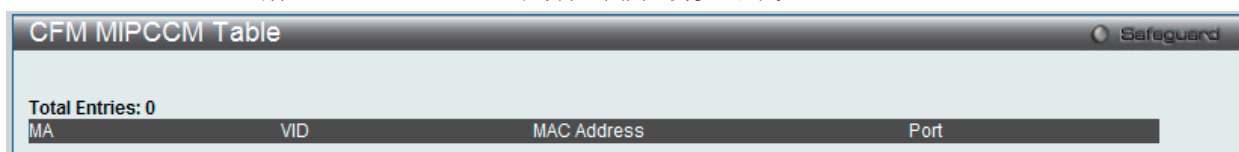


図 14-12 CFM MIPCCM Table 画面

CFM Loopback Settings (CFM ループバック設定)

CFM ループバックを設定します。

OAM > CFM > CFM Loopback Settings の順にメニューをクリックし、以下の画面を表示します。

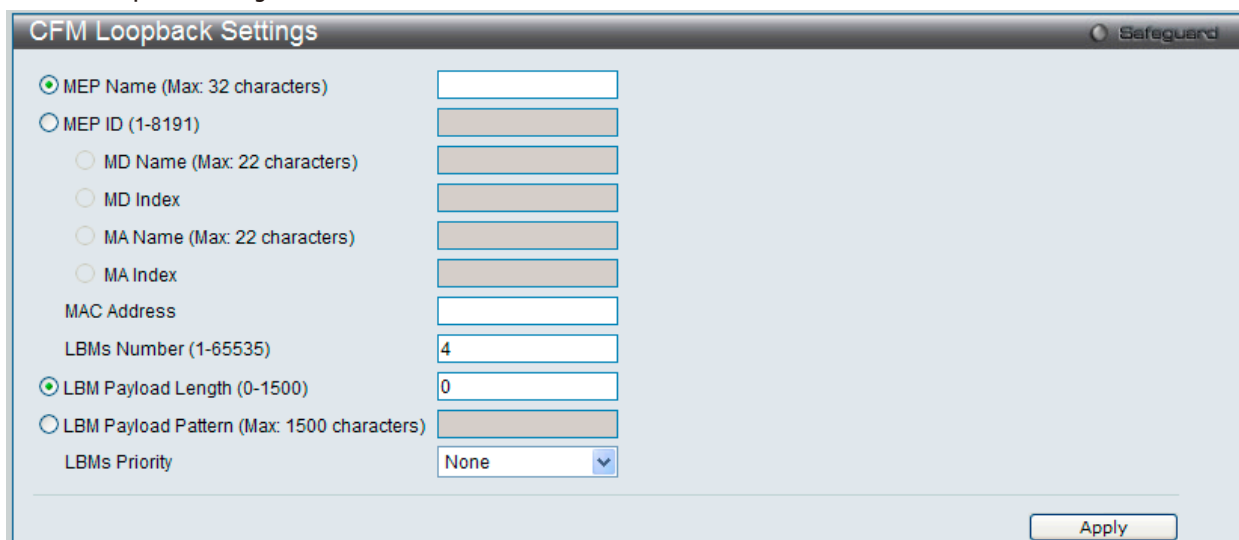


図 14-13 CFM Loopback Settings 画面

設定対象となる項目は以下の通りです。

| 項目 | 説明 |
|--|--|
| MEP Name (Max: 32 characters) | MEP 名を入力します。 |
| MEP ID (1-8191) | MEP ID を入力します。 |
| MD Name | 使用するメンテナンストメイン名を指定します。 |
| MD Index | 使用するメンテナンストメインのインデックスを指定します。 |
| MA Name | 使用するメンテナンリアソシエーション名を指定します。 |
| MA Index | 使用するメンテナンリアソシエーションのインデックスを指定します。 |
| MAC Address | 宛先 MAC アドレスを入力します。 |
| LBMs Number (1-65535) | 送信する LBM 数。初期値は 4 です。1 ~ 65525 の範囲で指定します。 |
| LBM Payload Length (0-1500) | 送信される LBM のペイロード長。初期値は 0 です。 |
| LBM Payload Pattern (Max: 1500 characters) | データ TLV が含まれるかどうかの指示に伴うデータ TLV に含める任意データの量。 |
| LBMs Priority | 送信される LBM に設定される 802.1p 優先度 (0-7)。指定しない場合、MA が送信した CCM と LTM と同じ優先度を使用します。初期値は「None」(なし) です。 |

「Apply」 ボタンをクリックし、変更を有効にします。

CFM Linktrace Settings (CFM リンクトレース設定)

CFM リンクトレースを設定します。

OAM > CFM > CFM Linktrace Settings の順にメニューをクリックし、以下の画面を表示します。

| Transaction ID | Source MEP | Destination | |
|----------------|------------|-------------------|-----------------------------|
| 0 | MEP1 | 00-11-22-33-44-55 | View Detail |

図 14-14 CFM Linktrace Settings 画面

設定対象となる項目は以下の通りです。

| 項目 | 説明 |
|-----------------|---|
| MEP Name | 使用するメンテナンスエンドポイントを指定します。 |
| MEP ID (1-8191) | 使用するエンドポイント ID を指定します。 |
| MD Name | 使用するメンテナンスドメイン名を指定します。 |
| MD Index | 使用するメンテナンスドメインのインデックスを指定します。 |
| MA Name | 使用するメンテナンスアソシエーション名を指定します。 |
| MA Index | 使用するメンテナンスアソシエーションのインデックスを指定します。 |
| MAC Address | 送信先 MAC アドレスを入力します。 |
| TTL (2-255) | リンクトレースメッセージの TTL 値。初期値は 64 です。範囲は 2-255 です。 |
| PDU Priority | 送信される LTM に設定される 802.1p 優先度 (0-7)。指定しない場合、MEP が送信した CCM と CCM と同じ優先度を使用します。 |

「Apply」ボタンをクリックし、変更を有効にします。

エントリの参照

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

検出後、「[View Detail](#)」リンクをクリックすると、CFM リンクトレースの詳細情報が表示されます。

| Hop | MEPID | MAC Address | Forwarded | Relay Action |
|------------------------------|-------|-------------|-----------|--------------|
| <<Back | | | | |

図 14-15 CFM Linktrace Settings 画面

エントリの削除

「Delete」ボタンをクリックして、入力した情報に基づいて指定エントリを削除します。

「Delete All」ボタンをクリックして、表示されたすべてのエントリを削除します。

CFM Packet Counter (CFM パケットカウンタ)

OSPF パケットカウンタ情報を表示します。CFM ハードウェアモードにおける MEP の CCM パケット統計情報はカウントしません。

OAM > CFM > CFM Packet Counter の順にメニューをクリックし、以下の画面を表示します。

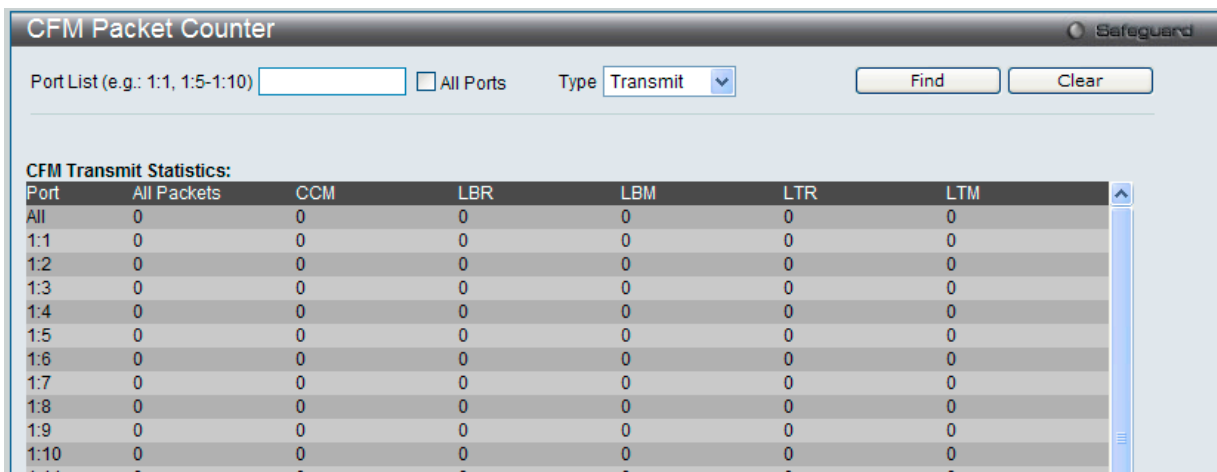


図 14-16 CFM Packet Counter 画面

画面には以下の項目があります。

| 項目 | 説明 |
|-----------|--|
| Port List | 参照するポートを選択します。「All Ports」を選択すると、すべてのポートを表示します。 |
| Type | <ul style="list-style-type: none"> Receive - 受信したすべての CFM パケットを表示します。 Transmit - 送信したすべての CFM パケットを表示します。 CCM - 送受信したすべての CFM パケットを表示します。 |

参照するポート番号を入力し、「Find」ボタンをクリックします。

「Clear」ボタンをクリックして、本欄に入力したすべてのエントリをクリアします。

CFM Fault Table (CFM 障害テーブル)

OSPF 障害情報を表示します。

OAM > CFM > CFM Fault Table の順にメニューをクリックし、以下の画面を表示します。

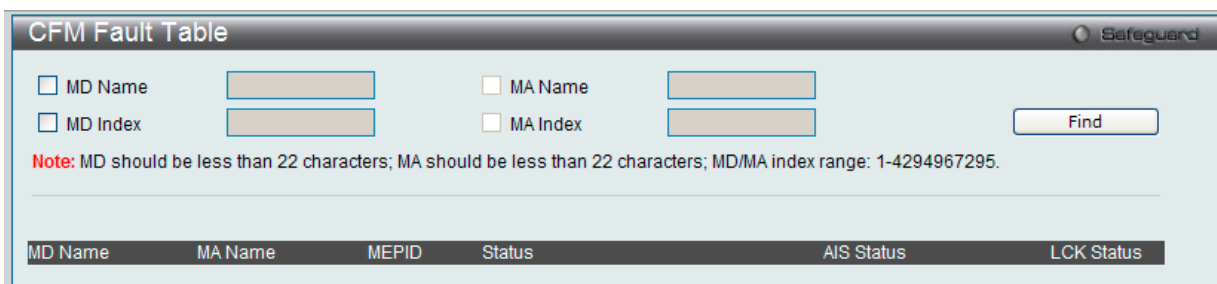


図 14-17 CFM Fault MEP 画面

画面には以下の項目があります。

| 項目 | 説明 |
|----------|----------------------------------|
| MD Name | 表示するメンテナンスドメイン名を指定します。 |
| MD Index | 表示するメンテナンスドメインのインデックスを指定します。 |
| MA Name | 表示するメンテナンスアソシエーション名を指定します。 |
| MA Index | 表示するメンテナンスアソシエーションのインデックスを指定します。 |

項目入力後、「Find」ボタンをクリックして、特定の MD および MA の接続障害を表示します。

CFM MP Table (CFM MP テーブル)

CFM MP 情報を表示します。

OAM > CFM > CFM MP Table の順にメニューをクリックし、以下の画面を表示します。

| MD Name | MA Name | MEPID | Level | Direction | VID |
|---------|---------|-------|-------|-----------|-----|
| MD1 | MA2 | 1 | 0 | Inward | 1 |

図 14-18 CFM MP Table 画面

画面には以下の項目があります。

| 項目 | 説明 |
|-------------|---|
| Port | 参照するユニット ID とポート番号を選択します。 |
| Level (0-7) | 参照するレベルを指定します。 |
| Direction | プルダウンメニューを使用して参照する方向を選択します。 <ul style="list-style-type: none"> Inward - 内向き MP を示します。 Outward - 外向き MP を示します。 |
| VID | 参照するエントリの VLAN 識別子を指定します。 |

項目入力後、「Find」ボタンをクリックして、エントリをテーブルに表示します。

Ethernet OAM (イーサネット OAM)

Ethernet OAM Settings (イーサネット OAM 設定)

ポートにイーサネット OAM モードを設定します。

OAM > Ethernet OAM > Ethernet OAM Settings の順にメニューをクリックし、以下の画面を表示します。

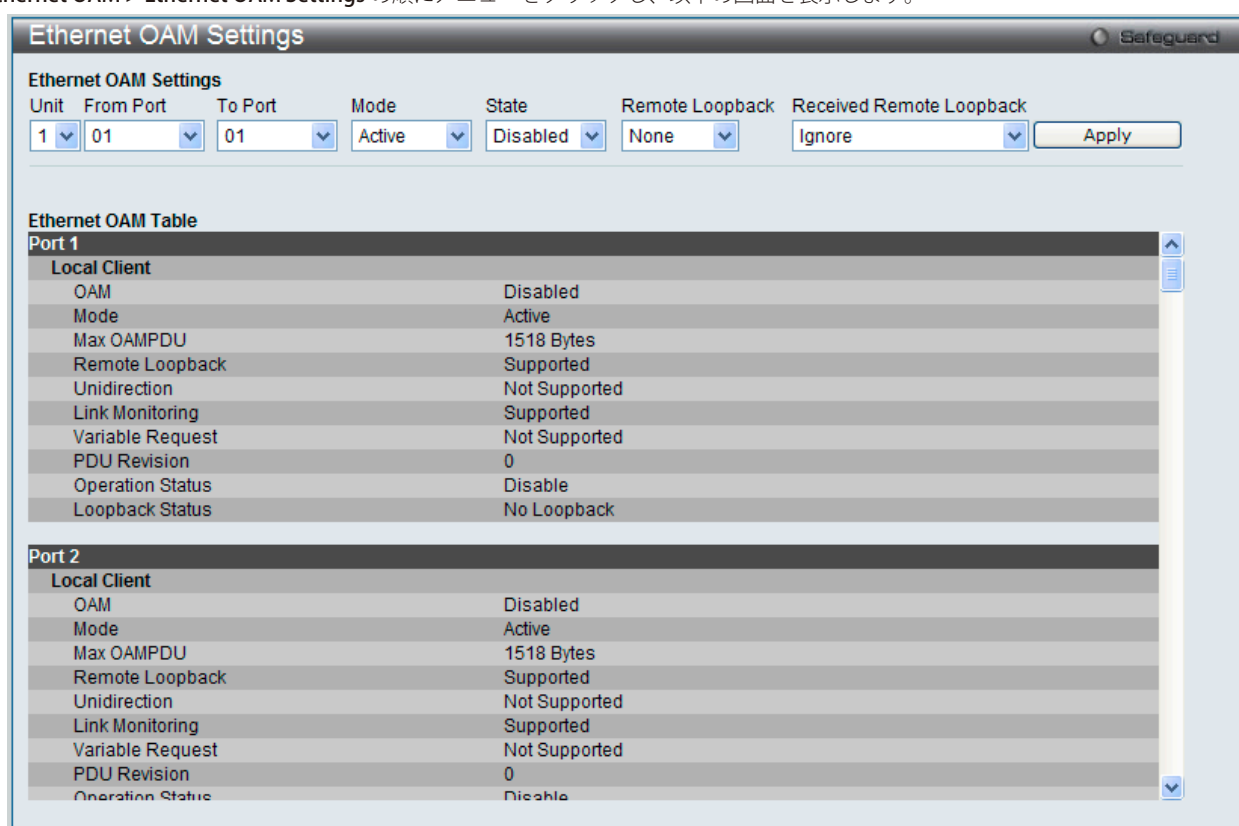


図 14-19 Ethernet OAM Settings 画面

以下の項目を設定できます。

| 項目 | 説明 |
|--------------------------|---|
| Unit | 設定するユニットを選択します。 |
| From Port / To Port | 設定するポート範囲を指定します。 |
| Mode | 動作するモード（「Active」または「Passive」）を指定します。初期モードは「Active」です。 |
| State | OAM 機能を有効または無効にします。初期値は無効です。 |
| Remote Loopback | <ul style="list-style-type: none"> • None - リモートループバックを行いません。（初期値） • Start - リモートループバックモードに変更するようにピアに要求します。 • Stop - 通常の操作モードに変更するようにピアに要求します。 |
| Received Remote Loopback | クライアントが受信したイーサネット OAM リモートループバックコマンドの処理を指定します。 <ul style="list-style-type: none"> • Process - 受信したイーサネット OAM リモートループバックコマンドを処理します。 • Ignore - 受信したイーサネット OAM リモートループバックコマンドを無視します。（初期値） |

「Apply」 ボタンをクリックし、変更を有効にします。

Ethernet OAM Configuration Settings (イーサネット OAM コンフィグレーション設定)

ポートにイーサネット OAM のイベントを設定します。

OAM > Ethernet OAM > Ethernet OAM Configuration Settings の順にメニューをクリックし、以下の画面を表示します。

図 14-20 Ethernet OAM Configuration Settings 画面

以下の項目を設定できます。

| 項目 | 説明 |
|--------------------------|--|
| Unit | 設定するユニットを選択します。 |
| From Port / To Port | 設定するポート範囲を指定します。 |
| Link Event | イーサネット OAM のクリティカルなリンクイベント機能 (「Link Monitor」または「Critical Link Event」) を設定します。イベント機能を無効にすると、ポートは対応するクリティカルなリンクイベントを送信しません。 |
| Link Monitor | ポートにイーサネット OAM リンクモニタリング (Error Symbol) を設定します。リンクモニタリング機能は、さまざまな条件のもとでリンク障害を検出して示すメカニズムを提供します。OAM はコード化されたシンボルのエラー数と共にフレームエラー数により統計情報をモニタリングします。シンボルエラー数が、期間内に定義したしきい値以上になる場合およびイベント通知状態 (Notify) が有効になる場合、リモート OAM ピアに通知するエラーシンボル期間のイベントを生成します。使用可能オプションは、Error Symbol、Error Frame、Error Frame Period、および Error Frame Second です。 |
| Critical Link Event | イーサネット OAM のクリティカルなリンクイベント機能を設定します。イベント機能が無効になると、ポートは対応するクリティカルなリンクイベントを送信しません。 <ul style="list-style-type: none"> • Critical Event - 不特定のクリティカルなイベントを参照します。 • Dying Gasp - リモートデバイスの電源障害など回復不可能なイベントの発生の検出を指定します。 |
| Threshold (0-4294967295) | イベント生成のためには、期間内に要求以上にシンボルエラー数を指定します。しきい値は 0 - 4294967295 の範囲です。初期値は 1 です。 |
| Window (1000-60000) | エラーフレームまたはシンボルのサマリイベントの期間 (ミリ秒) を入力します。 |
| Notify | イベント通知を有効または無効にします。初期値は有効です。 |

「Apply」ボタンをクリックし、設定を有効にします。

Ethernet OAM Event Log (イーサネット OAM イベントログ)

ポートのイーサネット OAM イベントログ情報を表示します。

OAM > Ethernet OAM > Ethernet OAM Event Log の順にメニューをクリックし、以下の画面を表示します。

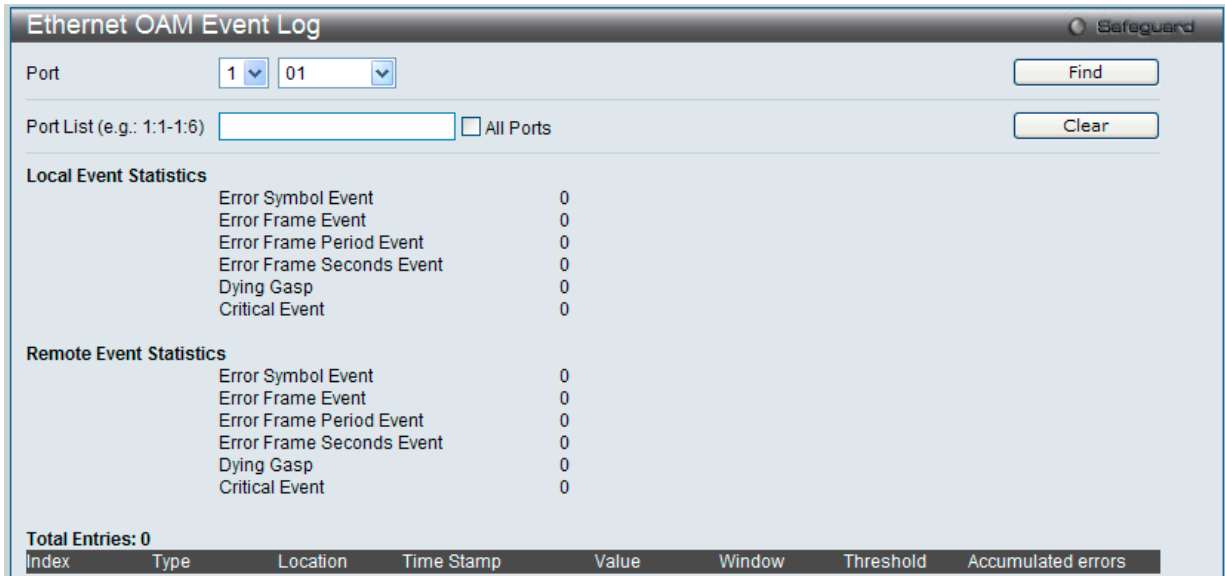


図 14-21 Ethernet OAM Event Log 画面

以下の項目を設定できます。

| 項目 | 説明 |
|-----------|---|
| Port | 参照するユニット ID とポート番号を選択します。 |
| Port List | 本設定に使用するポートリストを指定します。「All Ports」を選択すると、すべてのポートを選択します。 |

参照するポート番号またはポートリストを指定し、「Find」ボタンをクリックします。また、「All Port」を選択するとスイッチの全ポートの情報を表示します。

エントリを削除するためには、適切な情報を入力して、「Clear」ボタンをクリックします。

Ethernet OAM Statistics (イーサネット OAM 統計情報)

スイッチの各ポートに関するイーサネット OAM 統計情報を表示します。

OAM > Ethernet OAM > Ethernet OAM Statistics の順にメニューをクリックし、以下の画面を表示します。

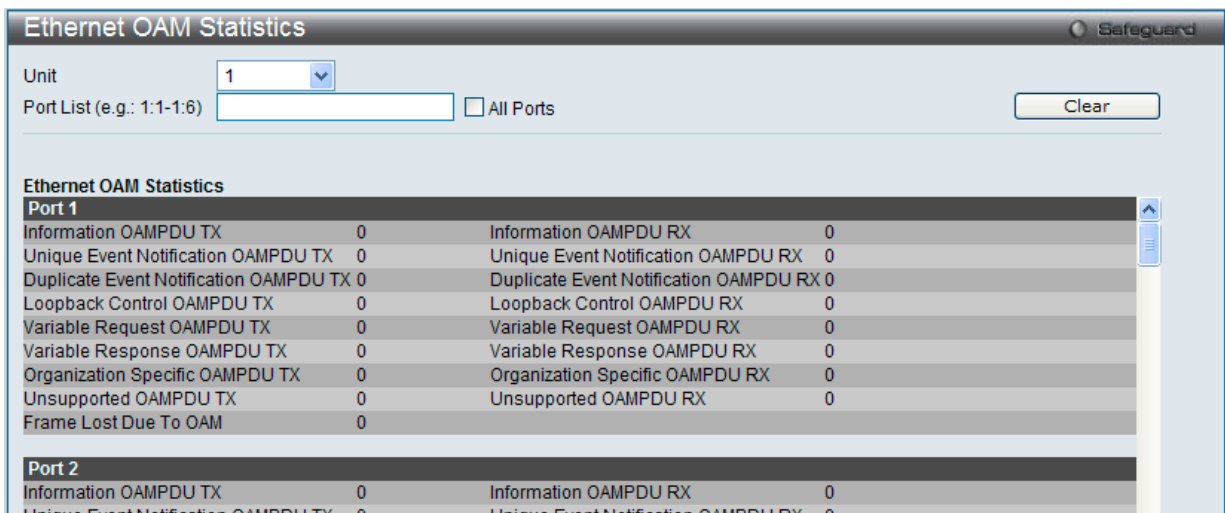


図 14-22 Ethernet OAM Statistics 画面

以下の項目を設定できます。

| 項目 | 説明 |
|-----------|---|
| Unit | 参照するユニット ID を選択します。 |
| Port List | 本設定に使用するポートリストを指定します。「All Ports」を選択すると、すべてのポートを選択します。 |

特定のポートまたはポートリストの情報をクリアするためには、ポートを入力し、「Clear」ボタンをクリックします。また、「All Port」を選択するとスイッチの全ポートの情報をクリアします。

DULD Settings (単方向リンク検出設定)

ポートにおいて単方向のリンク検出の設定および表示を行います。

OAM > DULD 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。

| Port | Admin State | Oper Status | Mode | Link Status | Discovery Time (sec) |
|------|-------------|-------------|--------|-------------|----------------------|
| 1 | Disabled | Disabled | Normal | Unknown | 5 |
| 2 | Disabled | Disabled | Normal | Unknown | 5 |
| 3 | Disabled | Disabled | Normal | Unknown | 5 |
| 4 | Disabled | Disabled | Normal | Unknown | 5 |
| 5 | Disabled | Disabled | Normal | Unknown | 5 |
| 6 | Disabled | Disabled | Normal | Unknown | 5 |
| 7 | Disabled | Disabled | Normal | Unknown | 5 |
| 8 | Disabled | Disabled | Normal | Unknown | 5 |
| 9 | Disabled | Disabled | Normal | Unknown | 5 |
| 10 | Disabled | Disabled | Normal | Unknown | 5 |
| 11 | Disabled | Disabled | Normal | Unknown | 5 |
| 12 | Disabled | Disabled | Normal | Unknown | 5 |
| 13 | Disabled | Disabled | Normal | Unknown | 5 |

図 14-23 DULD Settings 画面

以下の項目を設定できます。

| 項目 | 説明 |
|--------------------------|--|
| Unit | 設定するユニットを選択します。 |
| From Port / To Port | 設定するポート範囲を指定します。 |
| Admin State | プルダウンメニューが選択ポートの単方向リンク検出状態を「Enabled」(有効)または「Disabled」(無効)に設定します。 |
| Mode | プルダウンメニューを使用してモード (「Shutdown」および「Normal」) を選択します。 <ul style="list-style-type: none"> Shutdown - 単方向のリンクが検出されると、ポートを無効にしてイベントをログに出力します。 Normal - 単方向のリンクが検出した場合にイベントを単にログに出力します。 |
| Discovery Time (5-65535) | これらのポートの Neighbor 検出時間を入力します。検出がタイムアウトになると、単方向リンク検出が開始します。 |

「Apply」 ボタンをクリックして行った変更を適用します。

Cable Diagnostics (ケーブル診断機能)

スイッチの特定のポートに接続する UTP ケーブルの詳細について表示します。ケーブルにエラーがある場合、エラーのタイプと発生箇所を判断します。ケーブル診断機能は主に管理者とカスタマサービス担当者が UTP ケーブルを検証するために設計されています。ケーブルの品質やエラーの種類を即座に診断します。

Monitoring > Cable Diagnostics の順にメニューをクリックし、以下の画面を表示します。

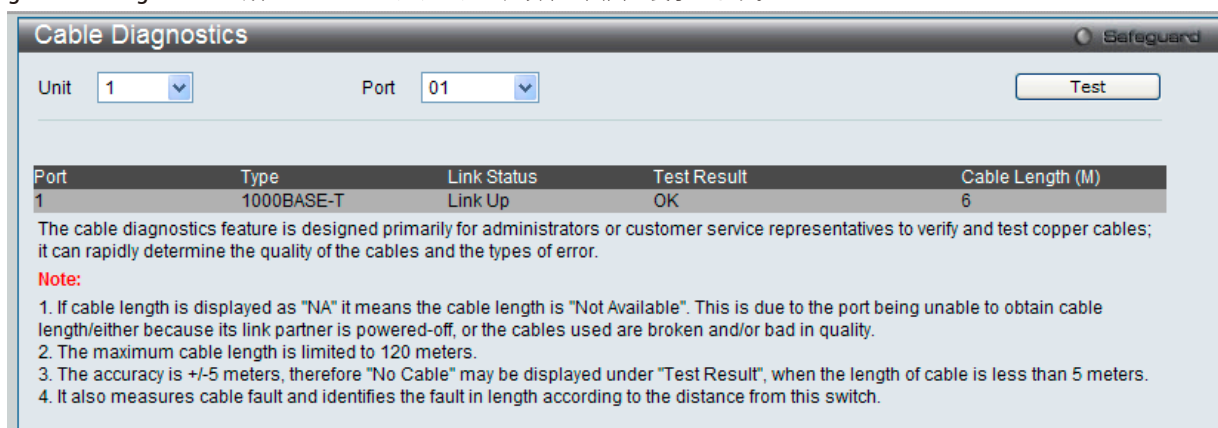


図 14-24 Cable Diagnostics 画面

特定のポートに対するケーブル診断を表示するためには、プルダウンメニューを使用してポートを選択し、「Test」ボタンをクリックします。情報が画面に表示されます。

エラーメッセージは以下の通りです。

| 項目 | 説明 |
|-----------|---|
| Open | このペアはオープン状態です。 |
| Short | このペアの2つのラインがショートしています。 |
| CrossTalk | このペアのラインは共にショートしています。 |
| Unknown | 診断はケーブルステータスを取得しません。再試行してください。 |
| NA | ケーブルが見つかりません。ケーブルが診断の仕様外であるか品質が非常に悪い可能性があります。 |

注意 ケーブル長検出は GE ポートでのみサポートされています。

注意 ポートは 1000M の速度でリンクおよび動作する必要があります。

注意 クロストークエラー検出は FE ポートではサポートされていません。

注意 有効なケーブル診断の長さは 5-120m です。

注意 ケーブル長検出の誤差は GE ポートで +/-5m です。

注意 ケーブル診断機能において、実行中に Link Down します。

注意 ケーブル診断機能において、Link 速度が 100Mbps(対向が FE のみサポートの PHY) の場合に診断結果が "Short" と表示されます。

第 15 章 Monitoring (スイッチのモニタリング)

Monitoring メニューを使用し、本スイッチのポート使用率、パケットエラーおよびパケットサイズ等の情報を提供することができます。

以下は Monitoring サブメニューの説明です。

必要に応じて、設定 / 変更 / 修正を行ってください。

| サブメニュー | 説明 | 参照ページ |
|-----------------------|--|---------------------|
| Utilization (CPU 使用率) | CPU 使用率、ポートの帯域使用率を表示します。次のメニューがあります。 CPU Utilization (CPU 使用率)、DRAM & Flash Utilization (DRAM とフラッシュ利用率)、Port Utilization (ポート使用率) | 417 |
| Statistics (統計情報) | パケット統計情報とエラー統計情報を表示します。次のメニューがあります。 Packets (パケット統計情報)、Packet Size (パケットサイズ) | 419 |
| Mirror (ポートミラーリング) | ポートミラーリングの設定を行います。次のメニューがあります。 Port Mirror Settings (ポートミラーリング設定)、RSPAN Settings (RSPAN 設定) | 430 |
| sFlow (sFlow 設定) | sFlow 機能の設定を行います。次のメニューがあります。 sFlow Global Settings (sFlow グローバル設定)、sFlow Analyzer Server Settings (sFlow アナライザ設定)、sFlow Flow Sampler Settings (sFlow サンプラ設定)、sFlow Counter Poller Settings (sFlow カウンタポーラ設定) | 433 |
| Ping (Ping 設定) | IPv4 アドレスまたは IPv6 アドレスに Ping することができます。次のメニューがあります。 Broadcast Ping Relay Settings (ブロードキャスト Ping リレー設定)、Ping Test (Ping テスト) | 436 |
| Trace Route (トレースルート) | ネットワーク上のスイッチとホスト間の経路をトレースします。 | 438 |
| Peripheral (周辺機器) | デバイス環境機能はスイッチの内部温度ステータスを表示します。次のメニューがあります。 Device Environment (デバイス環境の参照)、External Alarm Settings (外部アラームの設定) | 439 |

Utilization (使用率)

CPU Utilization (CPU 使用率)

「CPU Utilization」画面では、現在の CPU 使用率をパーセント表示し、また指定した間隔で計算した平均値も表示します。

Monitoring > Utilization > CPU Utilization メニューをクリックし、以下の画面を表示します。

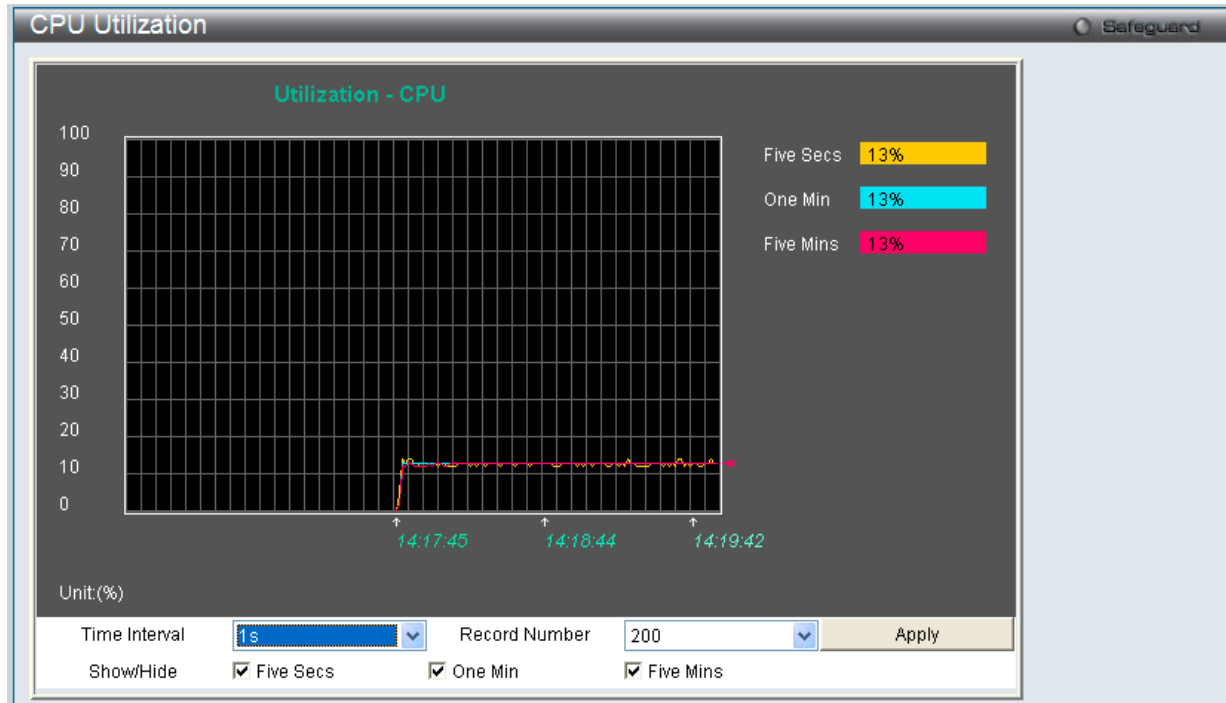


図 15-1 CPU Utilization 画面

以下の設定項目を使用して表示を変更します。

| 項目 | 説明 |
|----------------|--|
| Timer Interval | 1 秒から 60 秒で指定します。初期値は 1 秒です。 |
| Record Number | 20 から 200 でスイッチにポーリングを行う回数を指定します。初期値は 200 です。 |
| Show/Hide | チェックボックスにて CPU 使用率を計算する時間経過を Five Secs、One Min および Five Mins から選択します。各時間経過は色分けされた線で表示されます。Five Secs は黄色、One Min は青、Five Mins はピンク色で表示されます。選択すると CPU 使用率を表示します。 |

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。画面は自動的に更新されます。

DRAM & Flash Utilization (DRAM とフラッシュ利用率)

DRAM とフラッシュ利用率に関する情報を参照します。

Monitoring > Utilization > DRAM & Flash Utilization メニューをクリックし、以下の画面を表示します。

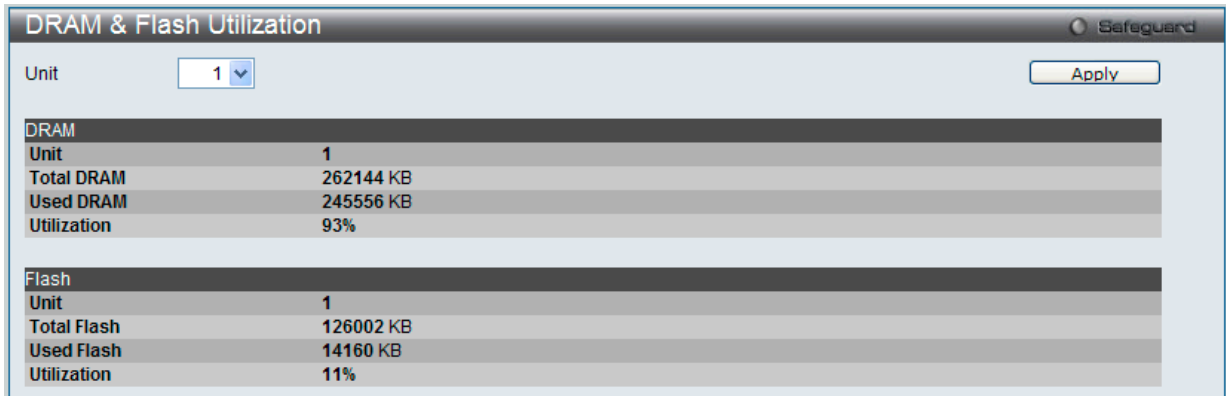


図 15-2 DRAM & Flash Utilization 画面

Port Utilization (ポート使用率)

本画面では、ポートの帯域使用率を表示します。

Monitoring > Utilization > Port Utilization の順にメニューをクリックし、以下の画面を表示します。

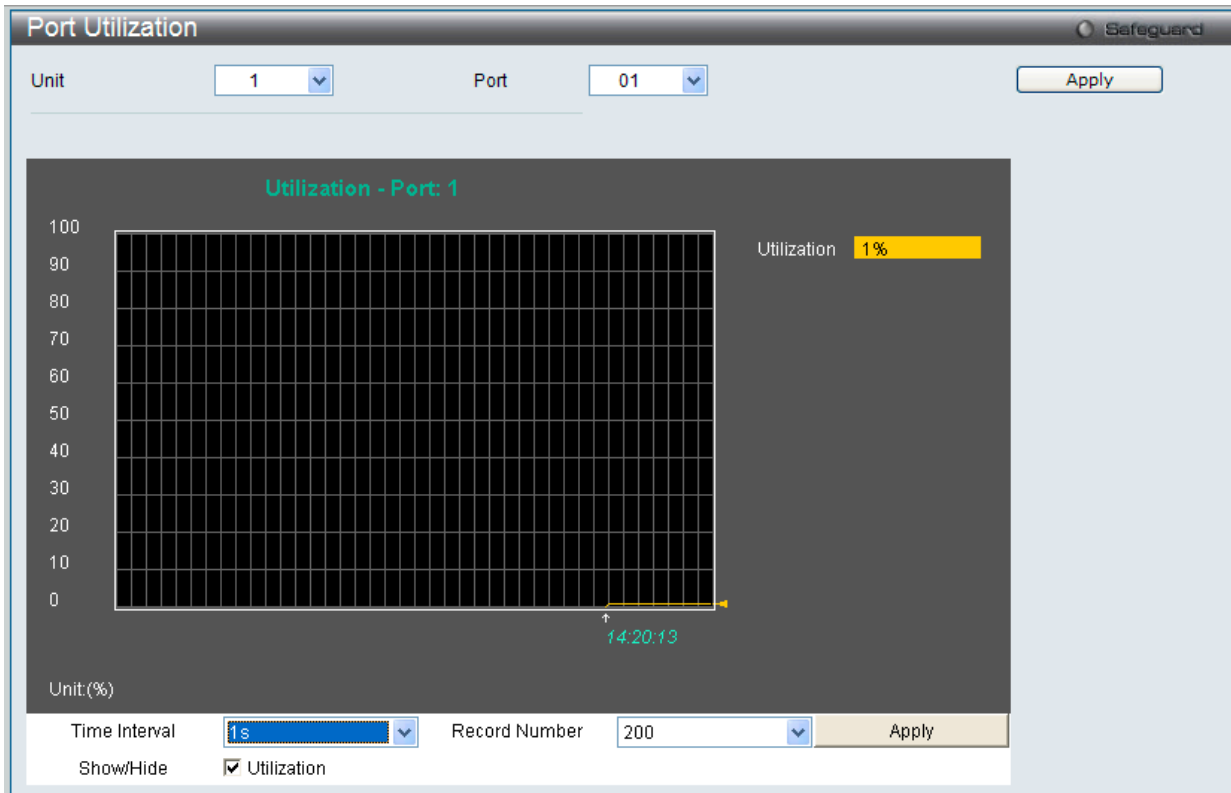


図 15-3 Port Utilization 画面

統計情報を参照するためには、プルダウンメニューでポート番号を選択します。Web ページ先頭のポートをクリックすることで、スイッチのリアルタイムグラフィックを使用することができます。

以下の設定項目が使用できます。

| 項目 | 説明 |
|---------------|---|
| Unit | 設定するユニットを選択します。 |
| Port | プルダウンメニューで統計情報を表示するポート番号を選択します。 |
| Time Interval | 1 秒から 60 秒で指定します。初期値は 1 (秒) です。 |
| Record Number | 20 から 200 でスイッチにポーリングを行う回数を指定します。初期値は 200 です。 |
| Show/ Hide | 「Utilization」にチェックすると、使用率を表示します。 |

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

Statistics (統計情報)

Port Statistics (ポート統計情報)

Packets (パケット統計情報)

Web マネージャは、パケットの統計情報を折れ線グラフまたは表の形式で表示します。6 個の画面が表示されます。

Received (RX) (受信パケット状態の参照)

スイッチが受信したパケットの情報を表示します。プルダウンメニューでポートを選択し、統計情報を参照します。Web ページ先頭のポートをクリックすることで、スイッチのリアルタイムグラフィックを使用することができます。

Monitoring > Statistics > Port Statistics > Packets > Received (RX) の順にメニューをクリックし、以下の画面を表示します。

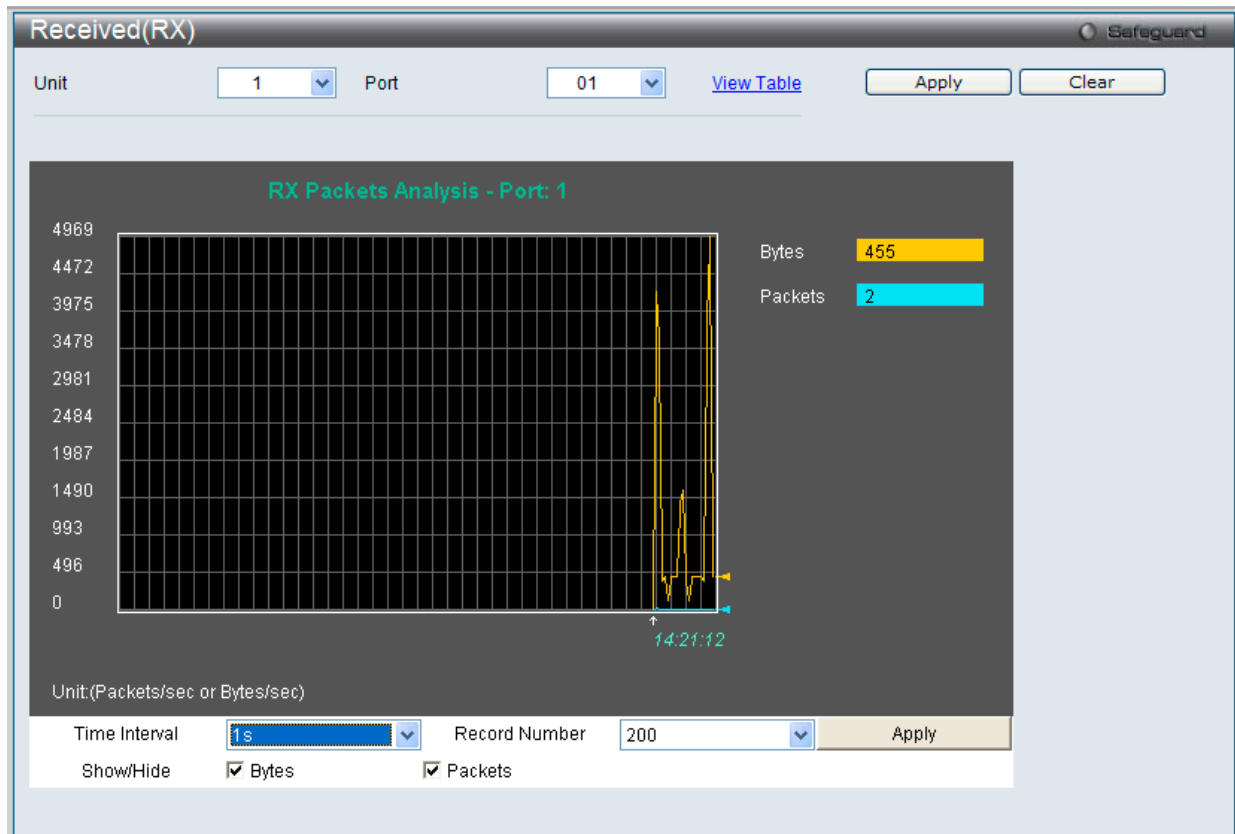


図 15-4 Received (RX) 画面 (バイトとパケットの折れ線グラフ)

「Received (RX) Table」を表示するには「View Table」リンクをクリックして、次の表を表示します。

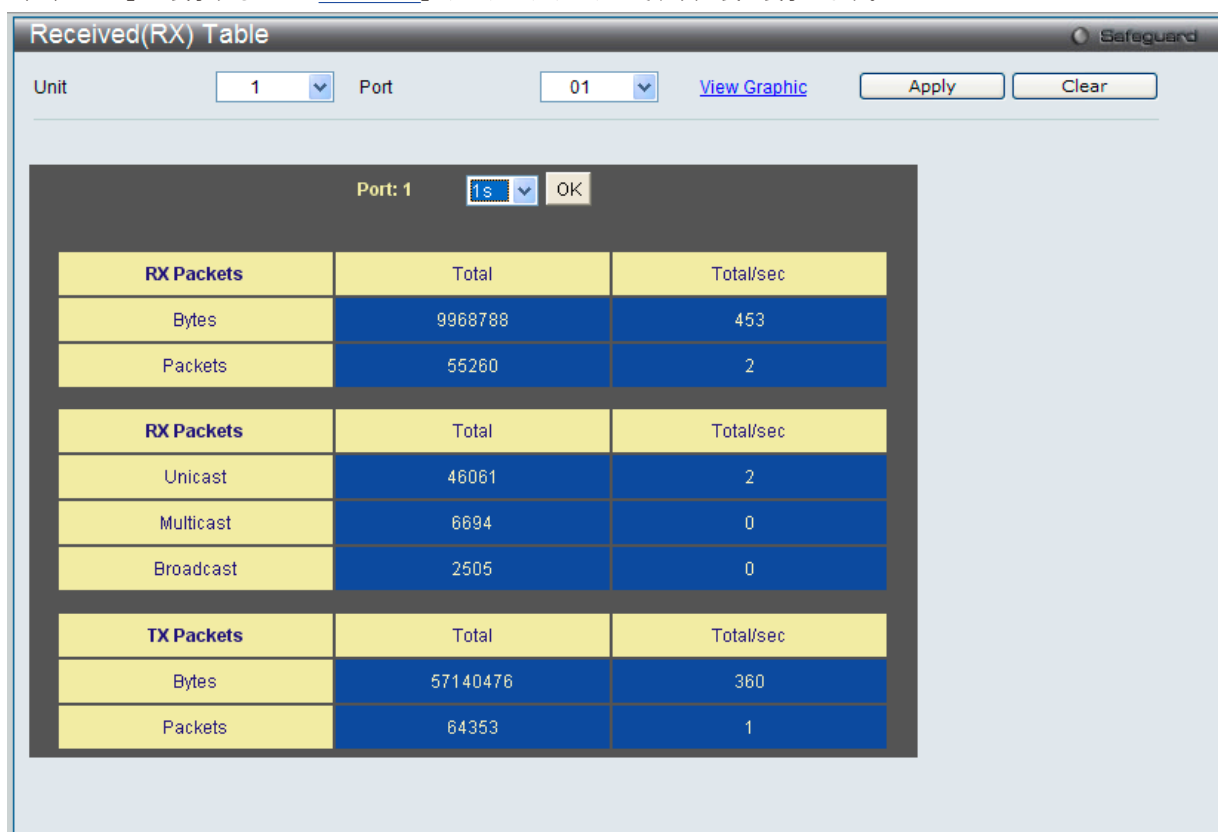


図 15-5 Received (RX) Table 画面 (バイトとパケットの表)

以下の設定項目を使用して、設定および表示を行います。

| 項目 | 説明 |
|------------------------------|---|
| Unit | 設定するユニットを選択します。 |
| Port | プルダウンメニューで統計情報を表示するポート番号を選択します。 |
| Time Interval | 1 秒から 60 秒で指定します。初期値は 1 秒です。 |
| Record Number | 20 から 200 でスイッチにポーリングを行う回数を指定します。初期値は 200 です。 |
| Bytes | ポートに受信したパケット量 (バイト) をカウントします。 |
| Packets | ポートに受信したパケット数をカウントします。 |
| Unicast | ユニキャストアドレスが受信した正常なパケットの合計数をカウントします。 |
| Multicast | マルチキャストアドレスが受信した正常なパケットの合計数をカウントします。 |
| Broadcast | ブロードキャストアドレスが受信した正常なパケットの合計数をカウントします。 |
| Show/ Hide | Bytes と Packets を表示 / 非表示にします。 |
| Clear | この画面のすべての統計情報をクリアします。 |
| View Table | 折れ線グラフ形式から表形式に表示を変更します。 |
| View Graphic | 表形式から折れ線グラフ形式に表示を変更します。 |

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

UMB_Cast (RX) (UMB Cast パケット統計情報の参照)

UMB (ユニキャスト、マルチキャスト、ブロードキャスト) に関する折れ線グラフを表示します。プルダウンメニューでポートを選択し、統計情報を参照します。Web ページ先頭のポートをクリックすることで、スイッチのリアルタイムグラフィックを使用することができます。

Monitoring > Statistics > Port Statistics > Packets > UMB_Cast (RX) の順にメニューをクリックし、以下の画面を表示します。

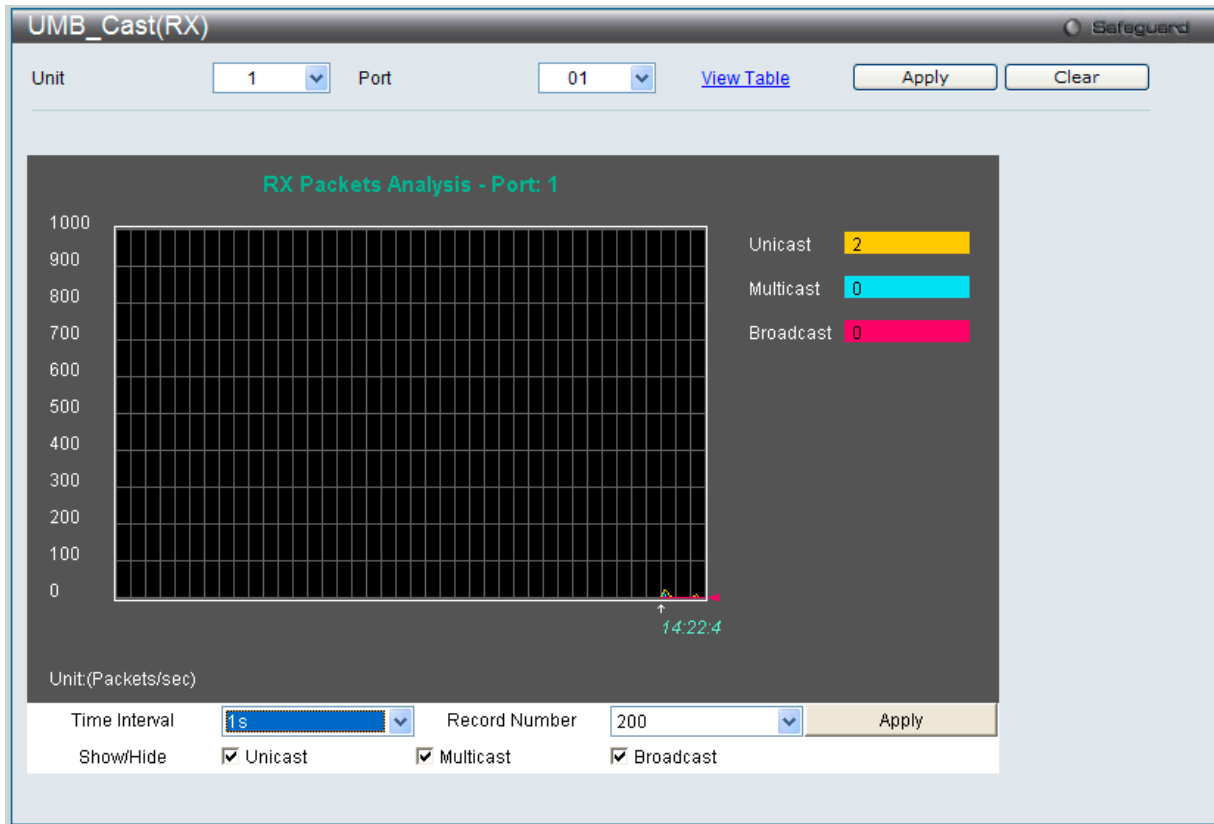


図 15-6 UMB_Cast (RX) 画面 (ユニキャスト、マルチキャスト、ブロードキャスト情報の折れ線グラフ)

「UMB_Cast (RX) Table」画面の表示を行うためには、「View Table」リンクをクリックします。

UMB_cast(RX) Table 画面のスクリーンショット。Unit: 1, Port: 01。View Graphic, Apply, Clear ボタンあり。Port: 1, 1s, OK ボタンあり。

| RX Packets | Total | Total/sec |
|------------|----------|-----------|
| Bytes | 10007929 | 125 |
| Packets | 55470 | 1 |

| RX Packets | Total | Total/sec |
|------------|-------|-----------|
| Unicast | 46258 | 1 |
| Multicast | 6707 | 0 |
| Broadcast | 2505 | 0 |

| TX Packets | Total | Total/sec |
|------------|----------|-----------|
| Bytes | 57299385 | 133 |
| Packets | 64579 | 0 |

図 15-7 UMB_Cast (RX) Table 画面 (ユニキャスト、マルチキャスト、ブロードキャスト情報の表形式表示)

Monitoring(スイッチのモニタリング)

以下の設定項目を使用して、設定および表示を行います。

| 項目 | 説明 |
|------------------------------|--|
| Unit | 設定するユニットを選択します。 |
| Port | プルダウンメニューで統計情報を表示するポート番号を選択します。 |
| Time Interval | 1秒から60秒で指定します。初期値は1秒です。 |
| Record Number | 20から200でスイッチにポーリングを行う回数を指定します。初期値は200です。 |
| Unicast | ユニキャストアドレスが受信した正常なパケットの合計数をカウントします。 |
| Multicast | マルチキャストアドレスが受信した正常なパケットの合計数をカウントします。 |
| Broadcast | ブロードキャストアドレスが受信した正常なパケットの合計数をカウントします。 |
| Show/Hide | Unicast、Multicast、Broadcast を表示 / 非表示にします。 |
| Clear | この画面のすべての統計情報をクリアします。 |
| View Table | 折れ線グラフ形式から表形式に表示を変更します。 |
| View Graphic | 表形式から折れ線グラフ形式に表示を変更します。 |

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

Transmitted (TX) (送信パケット統計情報)

スイッチから送信したパケットの情報をグラフ表示します。プルダウンメニューでポートを選択し、統計情報を参照します。Web ページ先頭のポートをクリックすることで、スイッチのリアルタイムグラフィックを使用することができます。

Monitoring > Statistics > Port Statistics > Packets > Transmitted (TX) の順にメニューをクリックし、以下の画面を表示します。

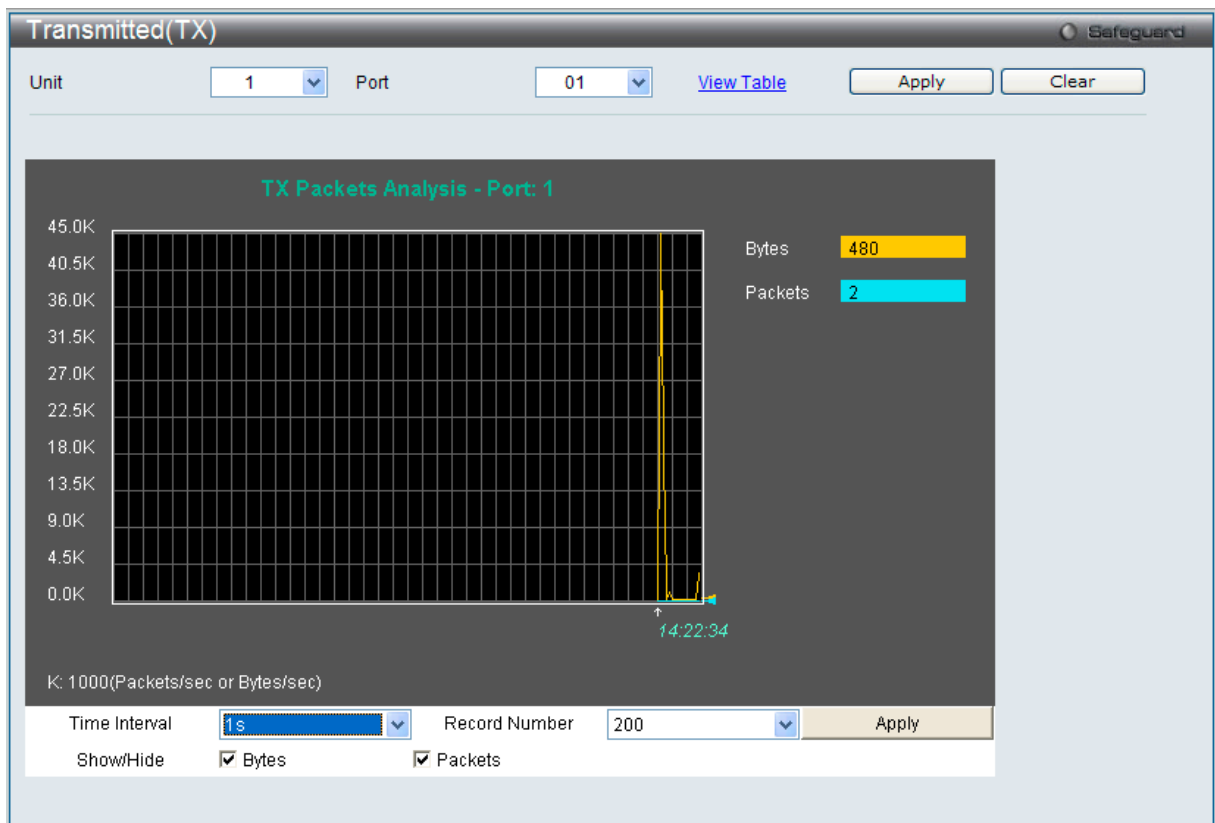


図 15-8 Transmitted (TX) 画面 (パケットサイズ、パケット数の折れ線グラフ表示)

送信パケットの情報を、表形式で表示するには、「View Table」リンクをクリックし、以下の画面を表示します。



図 15-9 Transmitted (TX) Table 画面 (パケットサイズ、パケット数の表示)

以下の設定項目を使用して、設定および表示を行います。

| 項目 | 説明 |
|------------------------------|---|
| Unit | 設定するユニットを選択します。 |
| Port | プルダウンメニューで統計情報を表示するポート番号を選択します。 |
| Time Interval | 1 秒から 60 秒で指定します。初期値は 1 秒です。 |
| Record Number | 20 から 200 でスイッチにポーリングを行う回数を指定します。初期値は 200 です。 |
| Bytes | ポートから送信に成功したパケット量 (バイト)。 |
| Packets | ポートから送信に成功したパケット数。 |
| Unicast | ユニキャストアドレスが送信した正常なパケットの合計数をカウントします。 |
| Multicast | マルチキャストアドレスが送信した正常なパケットの合計数をカウントします。 |
| Broadcast | ブロードキャストアドレスが送信した正常なパケットの合計数をカウントします。 |
| Show/Hide | Bytes と Packets を表示 / 非表示にします。 |
| Clear | この画面のすべての統計情報をクリアします。 |
| View Table | 折れ線グラフ形式から表形式に表示を変更します。 |
| View Graphic | 表形式から折れ線グラフ形式に表示を変更します。 |

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

Errors (パケットエラー)

Web マネージャは、スイッチの管理エージェントが集計したエラー統計情報を、折れ線グラフまたは表形式で表示します。以下の4つの画面で表示できます。

Received (RX) (受信エラーパケット統計情報の参照)

スイッチが受信したエラーパケットの情報を表示します。プルダウンメニューでポートを選択し、統計情報を参照します。Web ページ先頭のポートをクリックすることで、スイッチのリアルタイムグラフィックを使用することができます。

Monitoring > Statistics > Port Statistics > Errors > Received (RX) の順にメニューをクリックし、以下の画面を表示します。

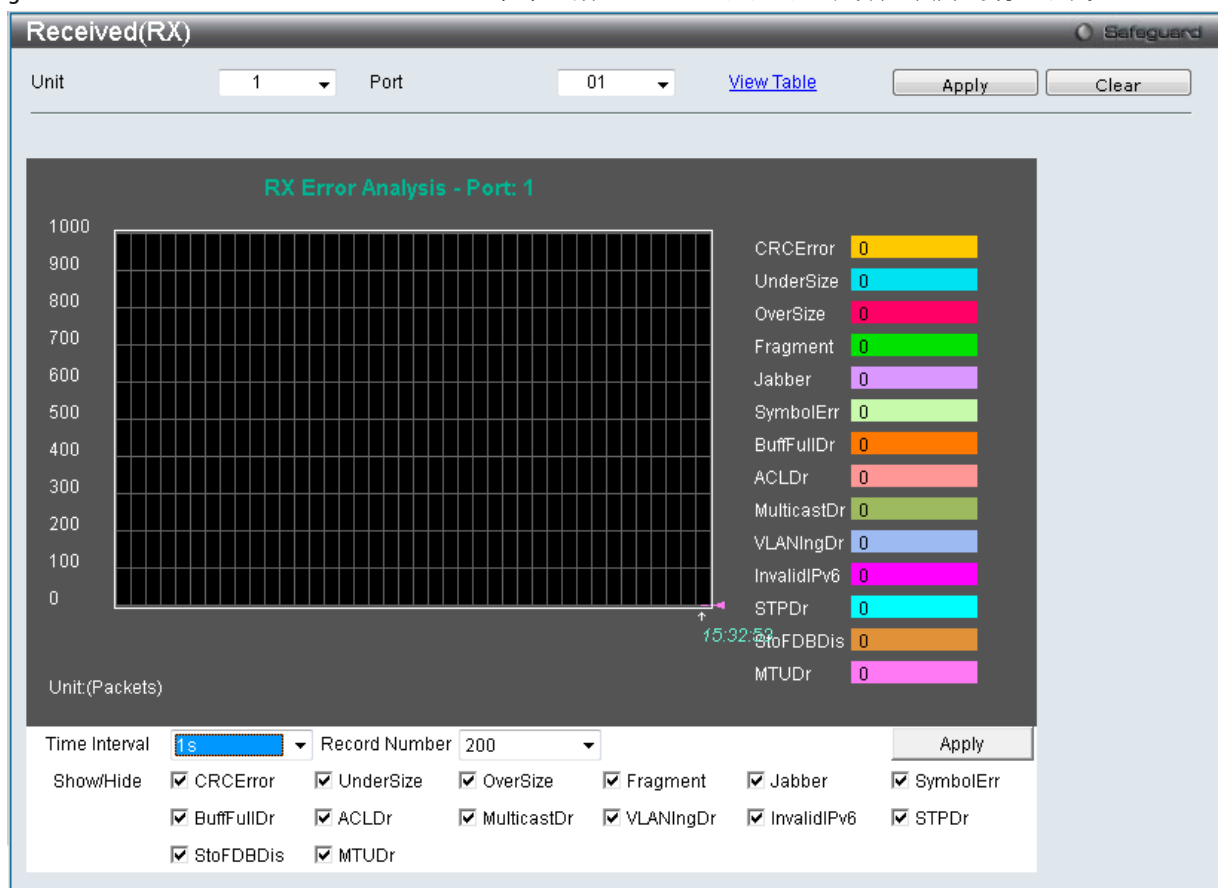


図 15-10 Received (RX) - Error 画面 (折れ線グラフ形式)

表形式の「Received (RX) Table」画面を表示するためには、「[View Table](#)」リンクをクリックします。

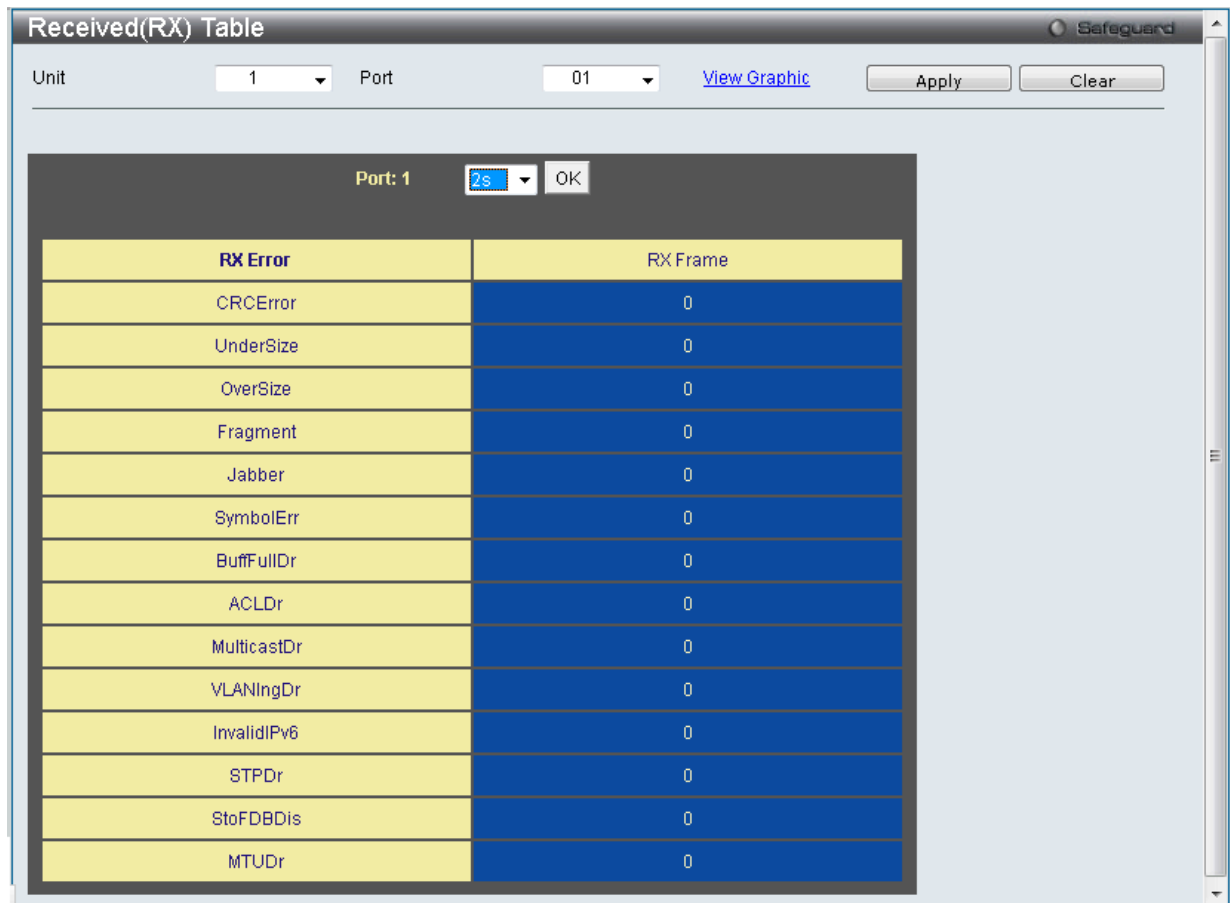


図 11-14 Received (RX) Table - Error 画面 (表形式)

以下の項目を使用して、設定および表示を行います。

| 項目 | 説明 |
|------------------------------|---|
| Unit | 設定するユニットを選択します。 |
| Port | プルダウンメニューで統計情報を表示するポート番号を選択します。 |
| Time Interval | 1 秒から 60 秒で指定します。初期値は 1 (秒) です。 |
| Record Number | 20 から 200 でスイッチにポーリングを行う回数を指定します。初期値は 200 です。 |
| CRCErr | CRC エラーがある受信パケット数。パケットの許容値のバイト (オクテット) で終了しない正常なパケットの数。 |
| UnderSize | パケットの最小許容値である 64 バイト以下で、CRC 値は正常なパケットの受信数。アンダーサイズパケットはコリジョンの発生を示しています。 |
| OverSize | エラーパケットが 1518 オクテットより長く、さらに MAX_PKT_LEN より短い正常な受信パケットをカウントします。内部的には MAX_PKT_LEN は 1536 オクテットです。 |
| Fragment | 64 バイト以下でフレーミングエラーや無効な CRC を含むパケット受信数。これらのパケットはコリジョンの発生に起因します。 |
| Jabber | エラーパケットが 1518 オクテットより長く、さらに MAX_PKT_LEN より短い不正な受信パケットをカウントします。内部的には MAX_PKT_LEN は 1536 オクテットです。 |
| SymbolErr | 物理的に配下にあるシンボル内に受信したエラーパケット数。 |
| BuffFullDr | バッファがなくなった時に廃棄された各パケットの増加数 |
| ACLDr | ACL により拒否された各パケットの増加数 |
| MulticastDr | 廃棄されたマルチキャストパケットの増加数 |
| VLANIngDr | VLANIngress チェックにより廃棄された各パケットの増加数 |
| InvalidIPv6 | 廃棄された IPv6 L3 パケットの増加数 |
| STPDr | インGRESSポートが転送状態でないときの廃棄パケット増加数 |
| StoFDBDis | 廃棄されたストームと FDB パケットの増加数 |
| MTUDr | 受信した MTU チェックエラーフレームのカウント。受信した MAXFR (最大フレーム値) を超えたフレームと有効 / 無効な FCS を含む破棄フレームの増加量。 |
| Show/Hide | CRCErr、UnderSize、OverSize、Fragment、Jabber、Drop および SymbolErr を表示するかどうかをチェックします。 |
| Clear | この画面のすべての統計情報をクリアします。 |
| View Table | 折れ線グラフ形式から表形式に表示を変更します。 |
| View Graphic | 表形式から折れ線グラフ形式に表示を変更します。 |

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

Transmitted (TX) (送信エラーパケット統計情報の参照)

スイッチでの送信エラーパケットの情報を表示します。プルダウンメニューでポートを選択し、統計情報を参照します。Web ページ先頭のポートをクリックすることで、スイッチのリアルタイムグラフィックを使用することができます。

Monitoring > Statistics > Port Statistics > Errors > Transmitted (TX) の順にメニューをクリックし、以下の画面を表示します。

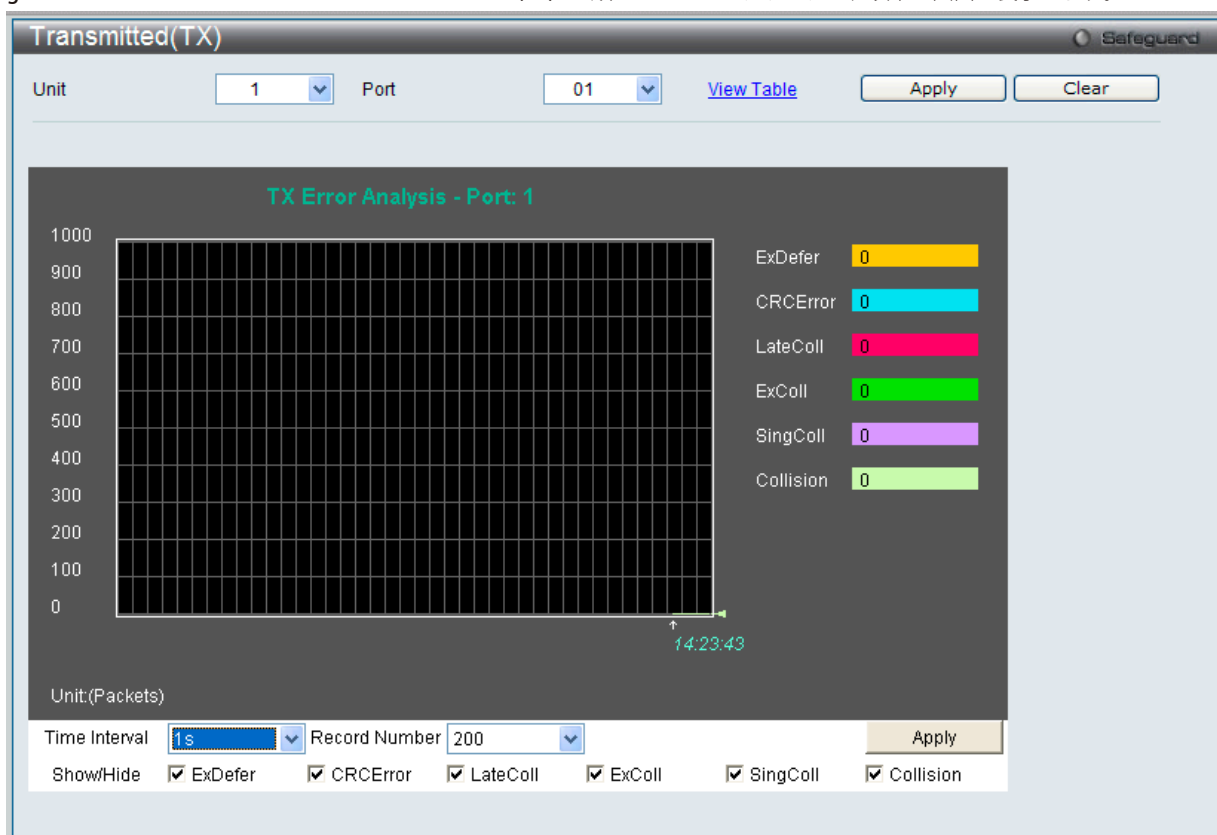


図 11-15 Transmitted (TX) -Error 画面 (折れ線グラフ形式)

表形式の「Transmitted (TX)」画面を表示するためには、「View Table」リンクをクリックします。

| TX Error | TX Frames |
|-----------|-----------|
| ExDefer | 0 |
| CRC Error | 0 |
| LateColl | 0 |
| ExColl | 0 |
| SingColl | 0 |
| Collision | 0 |

図 15-11 Transmitted (TX) Table - Error 画面 (表形式)

以下の項目を使用して、設定および表示を行います。

| 項目 | 説明 |
|------------------------------|---|
| Unit | 設定するユニットを選択します。 |
| Port | プルダウンメニューで統計情報を表示するポート番号を選択します。 |
| Time Interval | 1 秒から 60 秒で指定します。初期値は 1 秒です。 |
| Record Number | 20 から 200 でスイッチにポーリングを行う回数を指定します。初期値は 200 です。 |
| ExDefer | 特定のインタフェースに対する最初の送信が回線ビジーのために遅延したパケット数をカウントします。 |
| CRC Error | CRC エラーがある受信パケット数。パケットの許容値のバイト（オクテット）で終了しない正常なパケットの数。 |
| LateColl | パケットの送信に 512bit times より大きい往復遅延時間を検出されたコリジョンの回数をカウントします。 |
| ExColl | 過度のコリジョンのために送信エラーとなったパケット数。 |
| SingColl | シングルコリジョンフレーム数。1 個以上のコリジョンにより送信されていなかったパケットで送信に成功した数。 |
| Collision | ネットワークセグメントにおける推定総コリジョン数。 |
| Show/ Hide | CRCError、UnderSize、OverSize、Fragment、Jabber、Drop および SymbolErr を表示するかどうかをチェックします。 |
| Clear | この画面のすべての統計情報をクリアします。 |
| View Table | 折れ線グラフ形式から表形式に表示を変更します。 |
| View Graphic | 表形式から折れ線グラフ形式に表示を変更します。 |

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

Packet Size (パケットサイズ)

Web マネージャはスイッチが受信したパケットを6個のグループに整理し、サイズによってクラス分けして折れ線グラフまたはテーブルにします。2つの画面が提供されます。プルダウンメニューでポートを選択し、統計情報を参照します。Web ページ先頭のポートをクリックすることで、スイッチのリアルタイムグラフィックを使用することができます。

Monitoring > Statistics > Packet Size の順にメニューをクリックし、以下の画面を表示します。

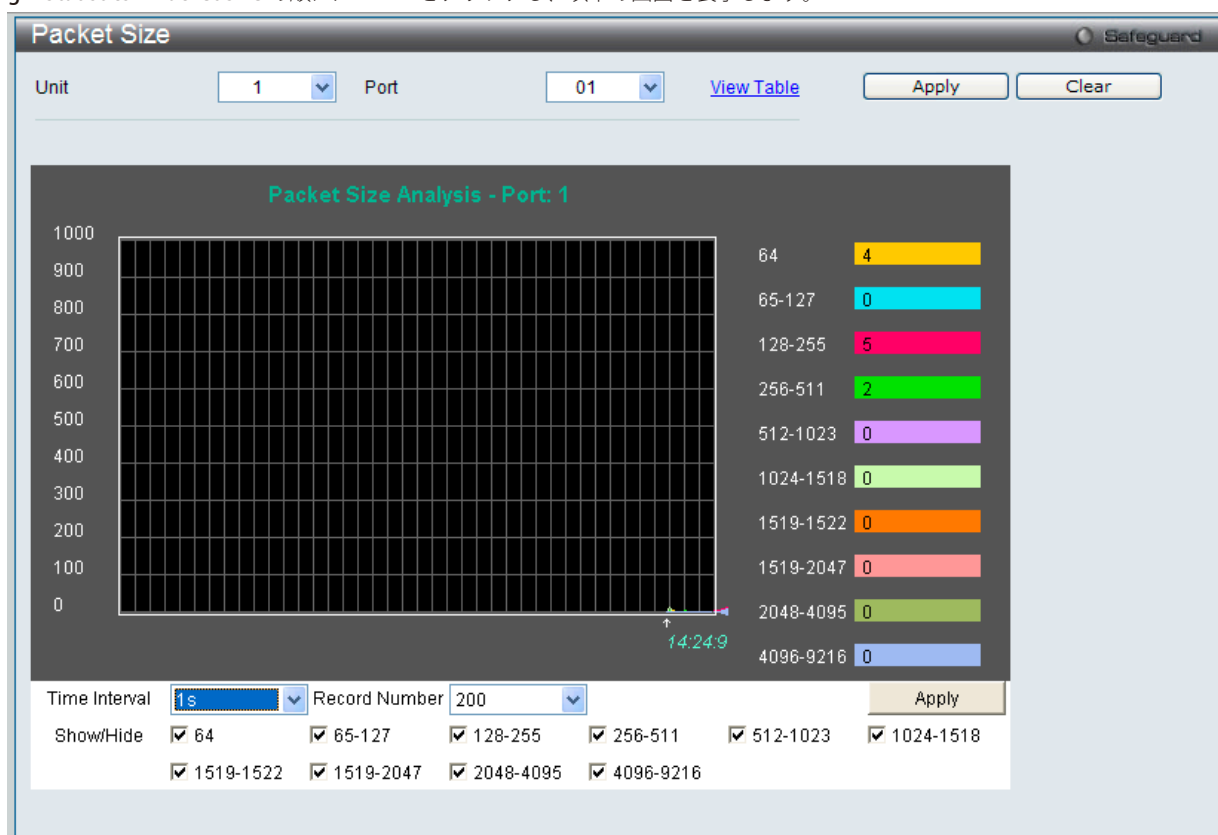


図 15-12 Packet Size 画面 (折れ線グラフ)

「Packet Size Table」を表示するためには、「View Table」リンクをクリックします。

The screenshot shows the 'Packet Size Table' interface. It features a data table with columns for Frame Size, Frame Counts, and Frames/sec. The table is filtered for Port 1 and a 1s time interval.

| Frame Size | Frame Counts | Frames/sec |
|------------|--------------|------------|
| 64 | 38005 | 4 |
| 65-127 | 3219 | 1 |
| 128-255 | 12176 | 2 |
| 256-511 | 16078 | 1 |
| 512-1023 | 25996 | 1 |
| 1024-1518 | 26233 | 0 |
| 1519-1522 | 0 | 0 |
| 1519-2047 | 0 | 0 |
| 2048-4095 | 0 | 0 |
| 4096-9216 | 0 | 0 |

図 15-13 Packet Size Table 画面 (表形式)

以下の設定項目を使用して、設定および表示を行います。

| 項目 | 説明 |
|------------------------------|--|
| Unit | 設定するユニットを選択します。 |
| Port | プルダウンメニューで統計情報を表示するポート番号を選択します。 |
| Time Interval | 1 秒から 60 秒で指定します。初期値は 1 (秒) です。 |
| Record Number | 20 から 200 でスイッチにポーリングを行う回数を指定します。初期値は 200 です。 |
| 64 | サイズが 64 オクテット (フレームビットを除き、FCS オクテットを含む) のパケット受信数 (不正なパケットを含む)。 |
| 65-127 | サイズが 65 から 127 オクテット (フレームビットを除き、FCS オクテットを含む) のパケット受信数 (不正なパケットを含む)。 |
| 128-255 | サイズが 128 から 255 オクテット (フレームビットを除き、FCS オクテットを含む) のパケット受信数 (不正なパケットを含む)。 |
| 256-511 | サイズが 256 から 511 オクテット (フレームビットを除き、FCS オクテットを含む) のパケット受信数 (不正なパケットを含む)。 |
| 512-1023 | サイズが 512 から 1023 オクテット (フレームビットを除き、FCS オクテットを含む) のパケット受信数 (不正なパケットを含む)。 |
| 1024-1518 | サイズが 1024 から 1518 オクテット (フレームビットを除き、FCS オクテットを含む) のパケット受信数 (不正なパケットを含む)。 |
| 1519-2047 | サイズが 1519 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) のパケット受信数 (不正なパケットを含む)。 |
| 2048-4095 | 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) のパケット受信数 (不正なパケットを含む)。 |
| 4096-9216 | 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) のパケット受信数 (不正なパケットを含む)。 |
| Show/Hide | 64、65-127、128-255、256-511、512-1023、1024-1518、1519-1552、1519-2047、2048-1095 および 4096-9216 の受信パケットを表示 / 非表示にします。 |
| Clear | このボタンをクリックし、この画面のすべての統計情報をクリアします。 |
| View Table | 折れ線グラフ形式から表形式に表示を変更します。 |
| View Graphic | 表形式から折れ線グラフ形式に表示を変更します。 |

設定を変更する場合は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

Mirror (ポートミラーリング)

本スイッチはポート上で送受信したフレームをコピーし、別のポートに転送します。スニファアやRMON probeのようなモニタデバイスをミラーポートに接続し、最初のポートを通過するパケット情報を参照できます。ネットワーク監視とトラブルシューティングの目的で使用します。

Port Mirror Settings (ポートミラーリング設定)

ポートミラーリング機能を設定します。

Monitoring > Mirror > Port Mirror Settings の順にメニューをクリックし、以下の画面を表示します。

図 15-14 Port Mirror Settings 画面

以下の設定項目を使用して、設定および表示を行います。

| 項目 | 説明 |
|---------------------|--|
| Mirror Global State | ラジオボタンをクリックしてポートミラーリング機能を「Enabled」(有効)/「Disabled」(無効)にします。 |
| Group ID (1-4) | ミラーグループ ID を入力します。 |

「Apply」 ボタンをクリックして各セクションで行った変更を適用します。

「Find」 ボタンをクリックして、入力した情報に基づく特定のエントリーを検出します。

「View All」 ボタンをクリックして、すべての定義済みエントリーを表示します。

「Modify」 ボタンをクリックして、指定エントリーを編集します。

「Delete」 ボタンをクリックして、指定エントリーを削除します。

エントリーの編集

「Modify」 ボタンをクリックすると、以下の画面が表示されます。

図 15-15 Port Mirror Settings 画面

本画面には次の項目があります。

| 項目 | 説明 |
|----------------|---|
| Group ID (1-4) | ミラーグループ ID を表示します。 |
| Target Port | ユニット番号とターゲットポートを設定します。 |
| Source Port | ソースデータの方向とソースポートを表示します。 <ul style="list-style-type: none"> TX - ポートが外向きトラフィックを含むかどうかを選択します。 RX - ポートが内向きトラフィックを含むかどうかを選択します。 Both - ポートが内向きおよび外向きの両方のトラフィックを含むかどうかを選択します。 None - ポートがどのトラフィックも含まないかどうかを選択します。 |
| Add / Delete | 選択したソースポートを「Add」(追加) または「Delete」(削除) します。 |
| State | ポートミラーリング機能を有効または無効にします。 |

ミラーポートの設定手順：

1. 「Mirror Global State」で「Enabled」(有効) を選択し、「Apply」ボタンをクリックします。
2. 「Group ID」を入力し、ミラーグループを選択して「Apply」ボタンをクリックします。
3. 下部のテーブルで対象のエントリの「Modify」ボタンをクリックして、ポートミラーリング設定画面を表示します。
4. ソースポートからフレームのコピーを受信する「Target Port」(ターゲット) を選択します。
5. フレームのコピーを行う対象の「Source port」(ソースポート) とコピーを行うフレームの方向 (入力:Tx、出力:Rx、両方:Both、なし:None) を選択して、「Add」(追加) または「Delete」(削除) します。
6. 設定を変更する際は、必ず「Apply」ボタンをクリックし、設定内容を適用してください。

注意 転送速度の速いポートを遅いポートにミラーリングはできません。例えば、100Mbps ポートからのトラフィックを 10Mbps ポートにミラーリングしようとする、スループットの問題が起きます。ソースポートの速度はターゲットポートと同じかそれ以下としてください。また、ターゲットポートとソースポートを同じポートにはできませんのでご注意ください。

RSPAN Settings (RSPAN 設定)

RSPAN 機能をコントロールします。RSPAN 機能の目的は、パケットをリモートスイッチにミラーリングすることです。パケットは、ミラーされるパケットを受信したスイッチから、中間スイッチを通過し、スニファアが接続するスイッチに送信します。最初のスイッチはソーススイッチと言われます。

RSPAN 機能を動作するためには、ソーススイッチに RSPAN VLAN ソース設定を行います。中間スイッチと最後のスイッチに関しては、RSPAN VLAN のリダイレクト設定を行います。

注意 RSPAN が有効な場合だけ (1 つの RSPAN VLAN がソースポートに設定されている場合)、RSPAN VLAN ミラーリングは動作します。RSPAN が有効になり、少なくとも 1 つの RSPAN VLAN がリダイレクトポートに設定されると、RSPAN リダイレクト機能は動作します。

Monitoring > Mirror > RSPAN Settings の順にメニューをクリックし、以下の画面を表示します。

図 15-16 RSPAN Settings 画面

以下の設定項目を使用して、設定および表示を行います。

| 項目 | 説明 |
|--------------|--------------------------------|
| RSPAN State | RSPAN 機能を有効または無効にします。 |
| VLAN Name | VLAN 名により RSPAN VLAN を指定します。 |
| VID (1-4094) | VLAN ID により RSPAN VLAN を指定します。 |

「RSPAN State」を「Enabled」または「Disabled」にして「Apply」ボタンをクリックして、RSPAN 機能を有効または無効にします。

エントリの追加

「VLAN Name」または「VID」を指定後、「Add」ボタンをクリックして、入力した情報に基づいて新しいエントリを追加します。

エントリの参照

「Find」ボタンをクリックして、入力した情報に基づく特定のエントリを検出します。

エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。

RSPAN 設定の編集

「Modify」ボタンをクリックして、以下の画面を表示します。

図 15-17 RSPAN Settings (Modify) 画面

以下の設定項目を使用して、設定および表示を行います。

| 項目 | 説明 |
|--------------------|--|
| VID | VLAN ID により RSPAN VLAN を表示します。 |
| VLAN Name | VLAN 名により RSPAN VLAN を表示します。 |
| Source Ports | ポートがこのオプションで指定されないと、RSPAN のソースは「mirror」コマンドによって指定されるソースまたは ACL によって指定されたフローベースのソースとなります。ソースにパラメータが指定されないと、設定されたソースパラメータは削除されます。パケットをモニタする方向 (RX、TX、Both) を選択します。「Add」または「Delete」ボタンをクリックしてソースポートを追加または削除します。 |
| Redirect Port List | RSPAN VLAN パケットに出力ポートリストを指定します。リダイレクトポートがリンクアグリゲーションポートであると、RSPAN パケットにリンクアグリゲーションの動作を行います。「Add」または「Delete」ボタンをクリックしてリダイレクトポートを追加または削除します。 |

「Apply」ボタンをクリックして行った変更を適用します。

「<<Back」ボタンをクリックし、変更を破棄して前のページに戻ります。

sFlow (sFlow 設定)

sFlow (RFC3176) はスイッチとルータを含むデータネットワークのトラフィックをモニタリングする技術です。sFlow モニタリングシステムは、(スイッチまたはルータに組み込まれている、またはスタンドアロンの検査装置にある) sFlow エージェントと中央の sFlow コレクタから成っています。sFlow モニタリングシステムで使用されるアーキテクチャとサンプリング手法は、高速でスイッチされて、ルートを決定されるネットワークに対して連続したサイト全体 (企業全体) のトラフィックモニタリングを提供するように設計されています。

sFlow Global Settings (sFlow グローバル設定)

sFlow 機能を有効または無効にします。

Monitoring > sFlow > sFlow Global Settings の順にメニューをクリックし、以下の画面を表示します。

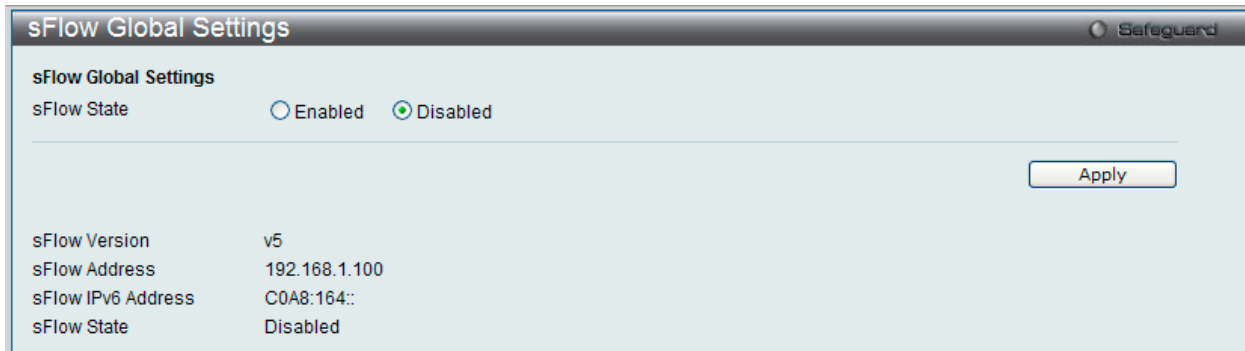


図 15-18 sFlow Global Settings 画面

以下の設定項目を使用して、設定および表示を行います。

| 項目 | 説明 |
|-------------|-----------------------|
| sFlow State | sFlow 機能を有効または無効にします。 |

「Apply」ボタンをクリックして行った変更を適用します。

sFlow Analyzer Server Settings (sFlow アナライザ設定)

スイッチは、同時に 4 個の異なるアナライザサーバをサポートすることができ、各サンブラまたはポーラはコレクタを選択してサンプルを送信します。異なるサンブラまたはポーラから異なるコレクタに異なるサンプルを送信できます。

Monitoring > sFlow > sFlow Analyzer Server Settings の順にメニューをクリックし、以下の画面を表示します。

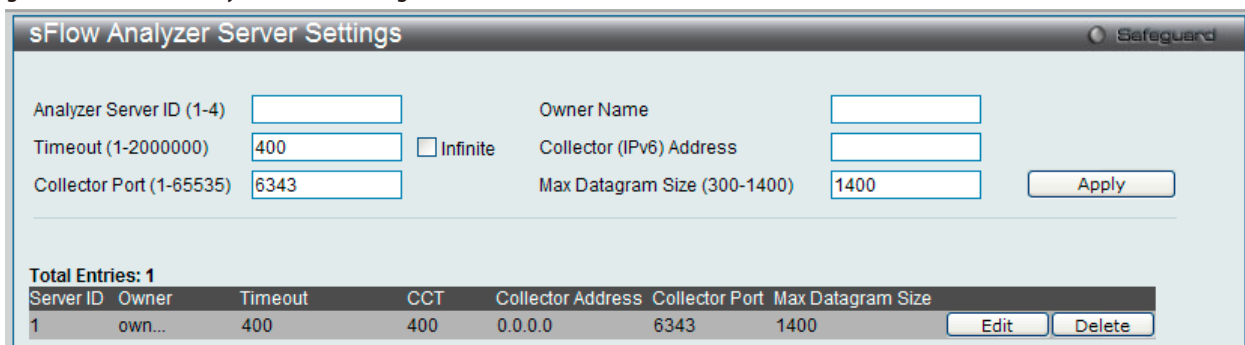


図 15-19 sFlow Analyzer Server Settings 画面

以下の設定項目を使用して、設定および表示を行います。

| 項目 | 説明 |
|------------------------------|---|
| Analyzer Server ID (1-4) | パケットが転送されるアナライザサーバの ID を指定します。 |
| Owner Name | この sFlow アナライザサーバを利用するエンティティ。オーナーが設定または変更される場合、タイムアウト値は自動で 400 になります。 |
| Timeout (1-2000000) | サーバがタイムアウトになる前の時間。アナライザサーバがタイムアウトになると、すべての sFlow サンブラとこのアナライザサーバに関連するカウンタポーラは削除されます。指定しないと、初期値は 400 です。「Infinite」をチェックすると制限はなくなります。 |
| Collector (IPv6) Address | アナライザサーバの IP アドレスを指定します。指定しないか、0 のアドレスを設定すると、エントリは非アクティブになります。 |
| Collector Port (1-65535) | sFlow データが送信される宛先 UDP ポート。指定しない場合、初期値は 6343 です。 |
| Max Datagram Size (300-1400) | 1 つのサンプルデータでバックされるデータの最大数 (バイト)。指定しない場合、初期設定は 1400 です。 |

「Apply」ボタンをクリックして行った変更を適用します。

エントリの編集

1. 編集するエントリの「Edit」ボタンをクリックして、以下の画面を表示します。

図 15-20 sFlow Analyzer Server Settings 画面 - Edit

2. 指定エントリを編集して「Apply」ボタンをクリックします。

エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。

sFlow Flow Sampler Settings (sFlow サンプラ設定)

sFlow アナライザサーバのパラメータを設定します。ポートにサンプリング機能を設定することによって、このポートが受信したサンプルパケットはカプセル化されて指定間隔でアナライザサーバに転送されます。

注意 アナライザサーバ ID の変更のために、はじめにフローサンプラを削除し、次に新しいものを作成する必要があります。

Monitoring > sFlow > sFlow Flow Sampler Settings の順にメニューをクリックし、以下の画面を表示します。

図 15-21 sFlow Flow Sampler Settings 画面

以下の設定項目を使用して、設定および表示を行います。

| 項目 | 説明 |
|---------------------|---|
| Unit | 設定するユニット番号を指定します。 |
| From Port / To Port | 設定するポートリストを指定します。 |
| Analyzer Server ID | パケットが転送されるアナライザサーバの ID を指定します。 |
| Rate | 受信パケットサンプリングのためのサンプリングレート。256 の倍数で設定されたレートが実効レートです。例えば、レートが 20 であれば、実効レートは 5120 です。あるパケットが 5120 のパケットごとに抽出されます。0 に設定されると、サンプラは無効になります。レートを指定しないと、初期値は 0 です。 |
| MAX Header Size | カプセル化してサーバに送信するサンプリングパケットの主なバイトの最大数。指定しない場合、初期設定は 128 です。 |

「Apply」ボタンをクリックして行った変更を適用します。

エントリの編集

1. 編集するエントリの「Edit」ボタンをクリックして、以下の画面を表示します。

図 15-22 sFlow Flow Sampler Settings 画面 - Edit

2. 指定エントリを編集して「Apply」ボタンをクリックします。

エントリの削除

「Delete」ボタンをクリックして、指定エントリを削除します。「Delete All」ボタンをクリックして、表示されたすべてのエントリを削除します。

sFlow Counter Poller Settings (sFlow カウンタポーラ設定)

sFlow カウンタポーラのパラメータを設定します。アナライザサーバ ID の変更のためには、はじめにカウンタポーラを削除し、次に新しいものを作成する必要があります。

Monitoring > sFlow > sFlow Counter Poller Settings の順にメニューをクリックし、以下の画面を表示します。

図 15-23 sFlow Counter Poller Settings 画面

以下の設定項目を使用して、設定および表示を行います。

| 項目 | 説明 |
|---------------------|--------------------------------|
| Unit | 設定するユニット番号を指定します。 |
| From Port / To Port | 設定するポートリストを指定します。 |
| Analyzer Server ID | パケットが転送されるアナライザサーバの ID を指定します。 |
| Interval | カウンタの連続するサンプルの間隔 (秒)。 |

「Apply」ボタンをクリックして行った変更を適用します。

エントリの編集

1. 編集するエントリの「Edit」ボタンをクリックして、以下の画面を表示します。

図 15-24 sFlow Counter Poller Settings 画面 - Edit

2. 指定エントリを編集して「Apply」ボタンをクリックします。

エントリの削除

「Delete」ボタンをクリックして、指定エント리를削除します。「Delete All」ボタンをクリックして、表示されたすべてのエント리를削除します。

Ping (Ping 設定)

Broadcast Ping Relay Settings (ブロードキャスト Ping リレー設定)

ブロードキャスト ping リレー機能 (デバイスがブロードキャスト ping リクエストに回答する) を有効または無効にします。

Monitoring > Ping > Broadcast Ping Relay Settings の順にメニューをクリックし、以下の画面を表示します。

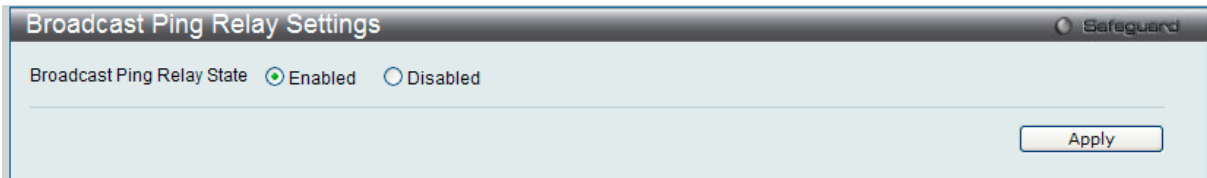


図 15-25 Broadcast Ping Relay Settings 画面

以下の項目を使用して設定、表示を行います。

| 項目 | 説明 |
|----------------------------|--|
| Broadcast Ping Relay State | ラジオボタンを使用してブロードキャスト ping リレー状態を「Enabled」(有効)/「Disabled」(無効)にします。 |

「Apply」ボタンをクリックして行った変更を適用します。

Ping Test (Ping テスト)

IPv4 アドレスまたは IPv6 アドレスに Ping することができます。

Ping とは、指定したアドレスに ICMP Echo パケットを送信する簡単なプログラムです。送信先のノードは、送信元のスイッチに回答を返すか、送信されたパケットをエコーバックします。本機能はスイッチとネットワーク上の他のノードとの接続性を確認するために使用します。

Monitoring > Ping Test の順にメニューをクリックし、以下の画面を表示します。

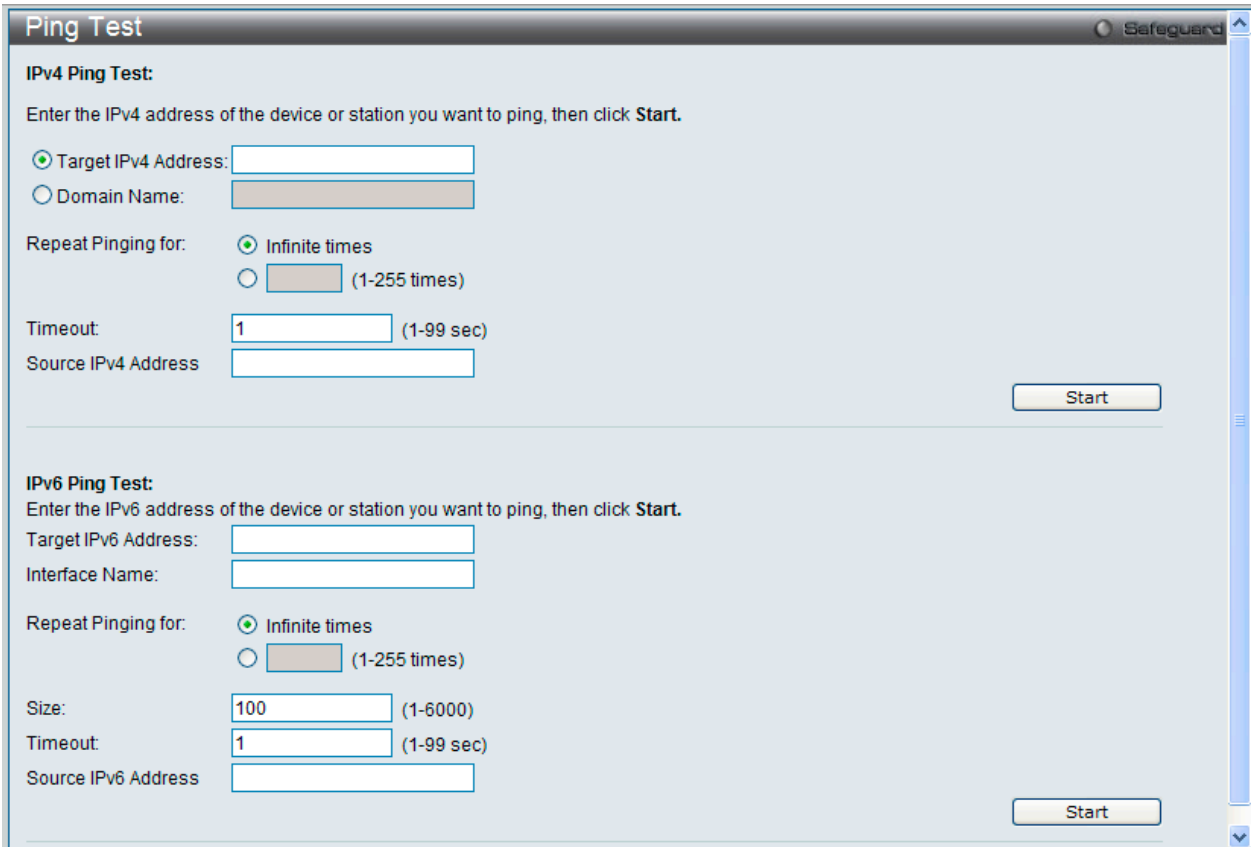


図 15-26 Ping Test 画面

「Repeat Pinging for」で「Infinite times」を選択すると、「Target IP Address」に指定した IP アドレス宛てに、ICMP Echo パケットをプログラムが停止するまで送信し続けます。または、「Repeat Pinging for」で 1-255 までの数字を指定して、送信回数を指定することもできます。

以下の項目を使用して設定、表示を行います。

| 項目 | 説明 |
|--------------------|---|
| Target IP Address | Ping する IP アドレスを入力します。 |
| Domain Name | ラジオボタンをクリックして、ホストのドメイン名を入力します。 |
| Repeat Pinging for | 送信先 IPv4 アドレスまたは IPv6 アドレスに Ping する回数 (1-255) を指定します。 「Infinite times」を選択すると、ICMP Echo パケットをプログラムが停止するまで送信し続けます。 |
| Size | IPv6 の場合、1-6000 の値を入力します。初期値は 100 です。 |
| Timeout | 送信先への Ping メッセージの応答待ち時間 1-99 (秒) で入力します。この時間内に応答パケットの検出に失敗すると、Ping パケットを破棄します。 |
| Source IP | ping パケットの送信元 IP/IPv6 アドレスを指定します。送信元 IP/IPv6 アドレスを指定すると、この IP/IPv6 アドレスは ping がリモートホストに送信するパケットの送信元アドレスとして使用されます。 |

「Start」ボタンをクリックし、Ping プログラムを開始します。

以下の結果画面が表示されます。

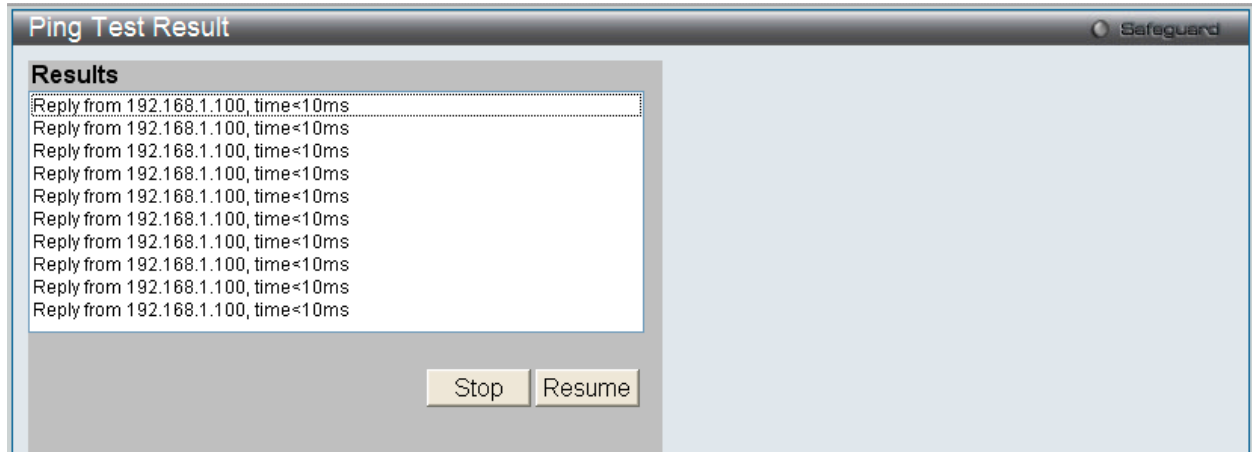


図 15-27 Ping Test (Result) 画面

「Stop」ボタンをクリックして、Ping テストを停止します。

「Resume」ボタンをクリックして、Ping テストを再開します。

Trace Route (トレースルート)

ネットワーク上のスイッチとホスト間の経路をトレースします。

Monitoring > Trace Route の順にメニューをクリックし、以下の画面を表示します。

図 15-28 Trace Route 画面

以下の項目を使用して設定、表示を行います。

| 項目 | 説明 |
|--------------------|---|
| IPv4 /IPv6 Address | 宛先ステーションの IP アドレス。 |
| Domain name | 宛先エンドステーションのドメイン名。 |
| TTL | トレースルートリクエストの有効時間。これは、トレースルートパケットが経由するルータの最大数です。トレースルートは、2つのデバイス間のネットワーク経路を検索する間に経由します。TTL の範囲は、1-60 ホップです。 |
| Port | ポート番号。値の範囲は、30000-64900 です。 |
| Timeout | リモートデバイスからの応答を待つ時間を定義します。1-65535(秒)を指定します。初期値は 5(秒)です。 |
| Probe | プローブ数。範囲は 1-9 です。指定しない場合、初期値は 1 です。 |

「Start」ボタンをクリックして、トレースルートを開始します。

以下の結果画面が表示されます。

図 15-29 Trace Route (Result) 画面

「Stop」ボタンをクリックして、トレースルートを停止します。

「Resume」ボタンをクリックして、トレースルートを再開します。

Peripheral (周辺機器)

Device Environment (デバイス環境の参照)

デバイス環境機能はスイッチの内部温度ステータスを表示します。

Monitoring > Peripheral > Device Environment の順にメニューをクリックし、以下の画面を表示します。



| Items | Data |
|--|----------------------|
| High Warning Temperature Threshold (celsius) | 79 |
| Low Warning Temperature Threshold (celsius) | 11 |
| Unit | 1 |
| Internal Power | Active |
| External Power | Fail |
| Right Fan 1 | Speed Low (3000 RPM) |
| Right Fan 2 | Speed Low (3000 RPM) |
| Right Fan 3 | Speed Low (3000 RPM) |
| Right Fan 4 | Speed Low (3000 RPM) |
| Current Temperature(celsius) | 23 |
| Fan High Temperature Threshold (celsius) | 40 |
| Fan Low Temperature Threshold (celsius) | 35 |

図 15-30 Device Environment 画面

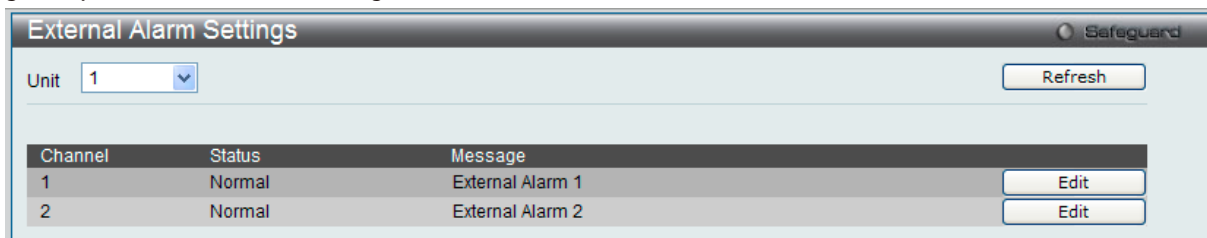
「Refresh」ボタンをクリックして、テーブルを更新して新しいエントリを表示します。

External Alarm Settings (外部アラームの設定)

チャンネルに外部アラームメッセージを設定します。

アラームのためのソースはスイッチの前面パネルに位置しています。定義済みの接続チャンネルを通じてこれらをモニタします。各チャンネルは特定のアラームイベントを表しています。また、ここでは、各チャンネルに関連付けるアラームイベントを定義できます。

Monitoring > Peripheral > External Alarm 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。



| Channel | Status | Message |
|---------|--------|------------------|
| 1 | Normal | External Alarm 1 |
| 2 | Normal | External Alarm 2 |

図 15-31 External Alarm Settings 画面

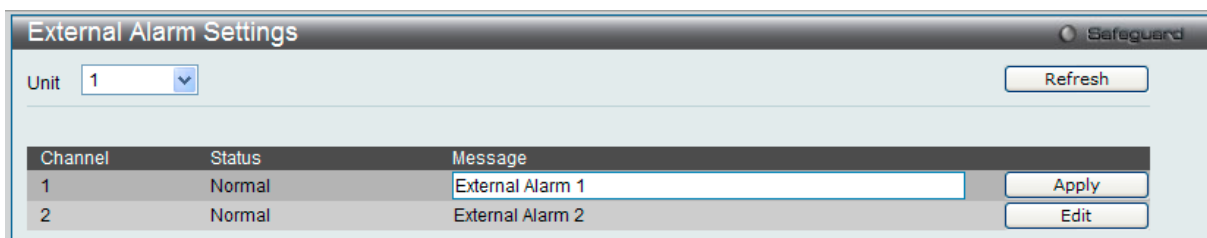
以下の項目を使用して設定、表示を行います。

| 項目 | 説明 |
|------|---------------------|
| Unit | 表示するユニット ID を指定します。 |

「Refresh」ボタンをクリックして、テーブルを更新します。

エントリの編集

「Edit」ボタンをクリックして、以下の画面を表示します。



| Channel | Status | Message |
|---------|--------|------------------|
| 1 | Normal | External Alarm 1 |
| 2 | Normal | External Alarm 2 |

図 15-32 External Alarm Settings 画面 - 編集

指定エントリの「Message」オプションを再設定し、「Apply」ボタンをクリックします。

第 16 章 Maintenance (スイッチのメンテナンス)

メンテナンス用のメニューを使用し、本スイッチのリセットおよび再起動等を行うことができます。

以下はサブメニューの説明です。

必要に応じて、設定 / 変更 / 修正を行ってください。

| サブメニュー | 説明 | 参照ページ |
|---|---------------------------|---------------------|
| Save (コンフィグレーションとログの保存) | | |
| Save Configuration / Log (コンフィグレーションとログの保存) | コンフィグレーションとログをスイッチに保存します。 | 441 |
| Tools (ツールメニュー) | | |
| Stacking Information (スタック情報) | スイッチの初期状態のスタック情報を表示します。 | 442 |
| Download Firmware (ファームウェアのダウンロード) | ファームウェアファイルをダウンロードします。 | 443 |
| Upload Firmware (ファームウェアのアップロード) | ファームウェアファイルをアップロードします。 | 445 |
| Download Configuration (コンフィグレーションのダウンロード) | コンフィグレーションファイルをダウンロードします。 | 446 |
| Upload Configuration (コンフィグレーションのアップロード) | コンフィグレーションファイルをアップロードします。 | 448 |
| Upload Log File (ログファイルのアップロード) | ログファイルをアップロードします。 | 450 |
| Reset (リセット) | 工場出荷時設定に戻し、メモリに保存します。 | 451 |
| Reboot System (システムの再起動) | スイッチの再起動を行います。 | 452 |

メンテナンスメニューは以下の通りです。

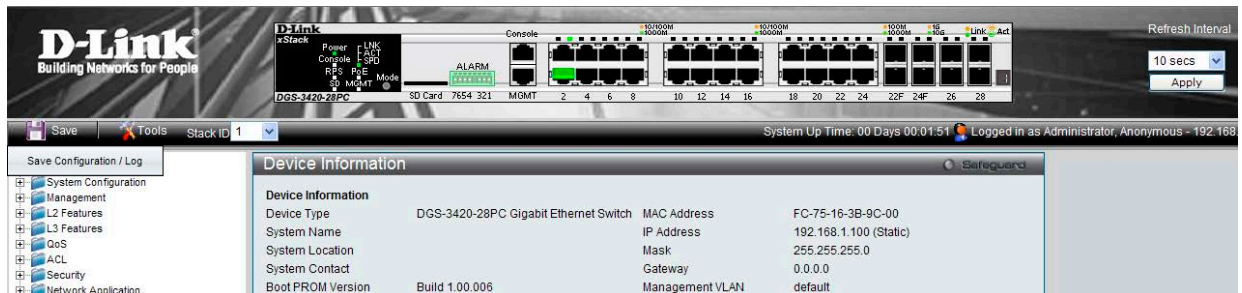


図 16-1 Save Configuration / Log 画面

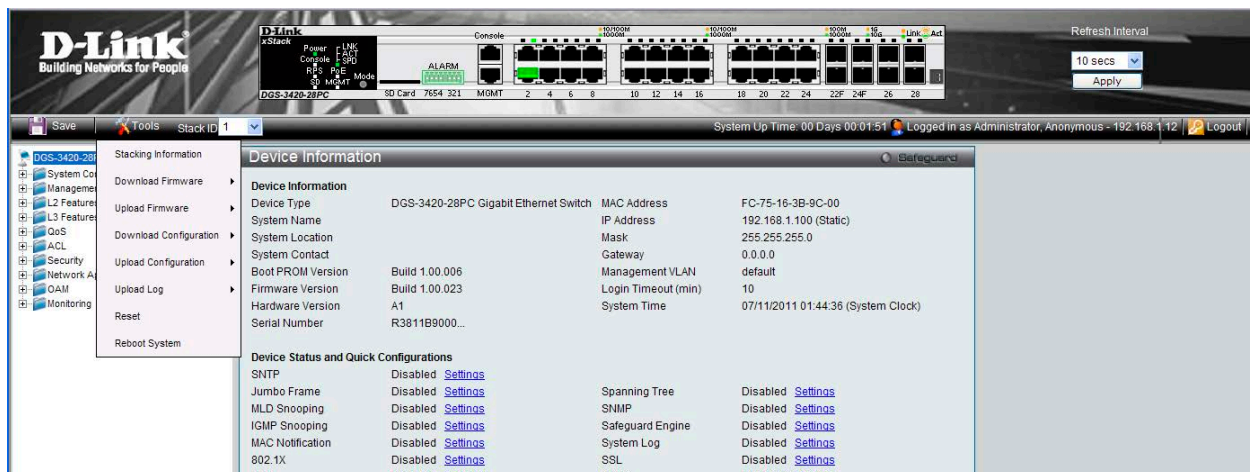


図 16-2 Tools 画面

Save Configuration / Log (コンフィグレーションとログの保存)

「Save Configuration」では現在のコンフィグレーションをスイッチに保存します。「Type」プルダウンメニューの「Configuration」を選択し、スイッチのファイルシステムにおけるパス名を「File Path」に入力して「Apply」ボタンをクリックします。



Web マネージャ先頭の **Save > Save Configuration / Log** をクリックし、以下の画面を表示します。

コンフィグレーションの保存

「Save Configuration」では現在のコンフィグレーションをスイッチに保存します。「Type」プルダウンメニューの「Configuration」を選択し、スイッチのファイルシステムにおけるパス名を「File Path」に入力して「Apply」ボタンをクリックします。

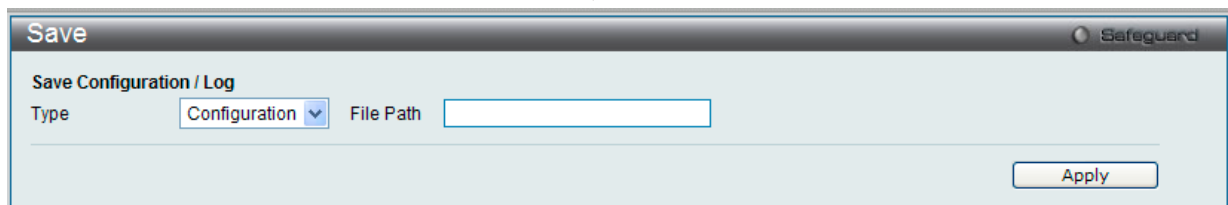


図 16-3 Save 画面 - Configuration

ログの保存

「Save Log」では現在のログをスイッチに保存します。「Type」プルダウンメニューの「Log」を選択し、「Apply」ボタンをクリックします。

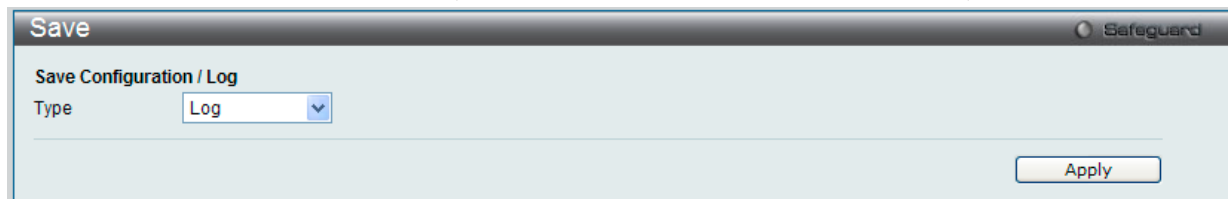


図 16-4 Save 画面 - Log

すべての保存

コンフィグレーションに行った変更を永続的に保存します。本オプションを使用すると、スイッチの再起動後も変更は維持されます。「Type」欄から「All」を選択して、「Apply」ボタンをクリックします。

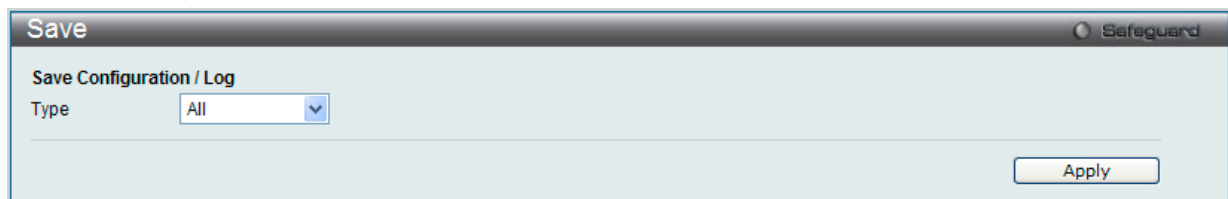
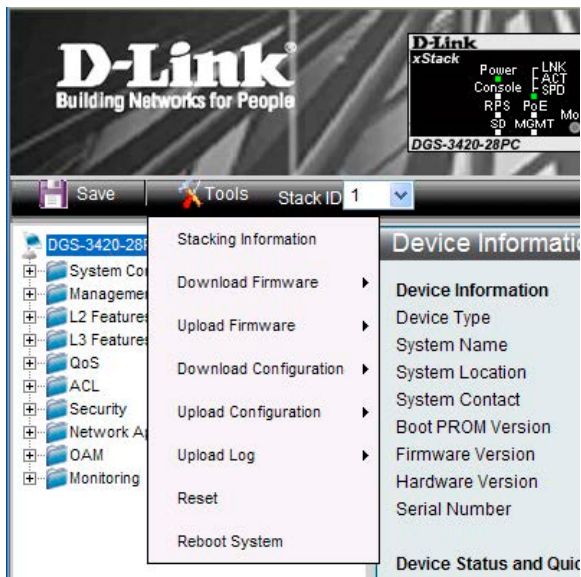


図 16-5 Save 画面 - All

Tools (ツールメニュー)

Web マネージャ先頭の **Tools** をクリックして、以下のメニューからオプションを選択します。



Stacking Information (スタック情報)

スイッチの初期状態のスタック情報 (例:スタック内の順番) を表示します。

「Tools」プルダウンメニューの隣にスイッチスタック内のスイッチ数 (最大 12 個) を表示します。アイコンは各ユニット番号と同じ順序となっており、Unit 番号 1 のスイッチはアイコングループの一番左上角のアイコンに対応しています。スタックモジュール (オプション) を経由してスイッチが相互接続する場合、スイッチスタックに関する情報は「Stack Information」に表示されます。

Tools > Stacking 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。

| Box ID | User Set | Type | Exist | Priority | MAC | Prom Version | Runtime Version | HW Version |
|--------|----------|---------------|-------|----------|-------------------|--------------|-----------------|------------|
| 1 | Auto | DGS-3420-28PC | Exist | 32 | FC-75-16-3B-9C-00 | 1.00.006 | 1.00.024 | A1 |
| 2 | - | NOT_EXIST | No | | | | | |
| 3 | - | NOT_EXIST | No | | | | | |
| 4 | - | NOT_EXIST | No | | | | | |
| 5 | - | NOT_EXIST | No | | | | | |
| 6 | - | NOT_EXIST | No | | | | | |
| 7 | - | NOT_EXIST | No | | | | | |
| 8 | - | NOT_EXIST | No | | | | | |
| 9 | - | NOT_EXIST | No | | | | | |
| 10 | - | NOT_EXIST | No | | | | | |
| 11 | - | NOT_EXIST | No | | | | | |
| 12 | - | NOT_EXIST | No | | | | | |

図 16-6 Stacking Information 画面

以下の項目があります。

| 項目 | 説明 |
|-------------------|---|
| Topology | スイッチを使用中のトポロジを表示します。 |
| My Box ID | 現在使用中のスイッチ番号 (Box ID) を表示します。 |
| Master ID | スイッチスタック内のプライマリマスタのユニット番号を表示します。 |
| Box Count | スイッチスタック内のスイッチの数を表示します。 |
| Force Master Role | Force Master Role の状態を表示します。 |
| Box ID | スイッチのスタックの順序を表示します。 |
| User Set | スイッチ番号は自動的 (Auto) またはスタティックに割り当てられます。初期値では「Auto」です。 |
| Type | スタック内で対応するスイッチのモデル名を表示します。 |
| Exist | スイッチがスタック内に存在するか、否かを示します。 |
| Priority | スイッチの優先度番号を表示します。低い値ほど高いプライオリティを示します。スタック内で最も低い優先度番号を持つボックス (スイッチ) が、プライマリマスタを示します。 |
| MAC | スイッチスタック内の対応するスイッチの MAC アドレスを表示します。 |
| Prom Version | 画面例の値と異なる場合があります。 |
| Runtime Version | スイッチで使用中のファームウェアバージョンを表示します。画面例の値と異なる場合があります。 |
| H/W Version | 画面例の値と異なる場合があります。 |

Download Firmware (ファームウェアのダウンロード)

スイッチにファームウェアをダウンロードします。

Download Firmware From TFTP (TFTP からファームウェアをダウンロード)

TFTP サーバからスイッチにファームウェアをダウンロードして、スイッチを更新することができます。

Web マネージャ先頭の **Tools > Download Firmware > From TFTP** を選択して以下の画面を表示します。

図 16-7 Download Firmware From TFTP 画面

以下の項目があります。

| 項目 | 説明 |
|-----------------------------|--|
| Download Firmware From TFTP | |
| Unit | プルダウンメニューを使用してファームウェアの受信ユニットを選択します。全ユニットのためには「All」を選択します。 |
| TFTP Server IP | 使用する TFTP サーバの IP アドレスを指定します。 <ul style="list-style-type: none"> IPv4 - ラジオボタンをクリックして、使用する TFTP サーバの IP アドレスを指定します。 IPv6 - ラジオボタンをクリックして、使用する TFTP サーバの IPv6 アドレスを指定します。 Domain Name - ラジオボタンをクリックして、ドメイン名を入力します。 |
| Source File | 送信元ファイルの位置と名前を入力します。 |
| Destination File | 送信先ファイルの位置と名前を入力します。 |
| Boot Up | ボックスをチェックして起動ファイルとして設定します。 |

Maintenance (スイッチのメンテナンス)

| 項目 | 説明 |
|-------------------------|----------------------|
| TFTP Source IP Settings | |
| Interface Name | 送信元インタフェース名を入力します。 |
| IPv4 Address | 送信元 IPv4 アドレスを入力します。 |
| IPv6 Address | 送信元 IPv6 アドレスを入力します。 |

「Download」 ボタンをクリックすると、ダウンロードが開始されます。

「Apply」 ボタンをクリックすると、変更が適用されます。

「Clear IP Address」 ボタンをクリックすると、送信元 IP インタフェースの IP アドレスが消去されます。

Download Firmware From RCP (RCP からファームウェアをダウンロード)

RCP サーバからスイッチにファームウェアをダウンロードして、スイッチを更新することができます。

Web マネージャ先頭の **Tools > Download Firmware > From RCP** を選択して以下の画面を表示します。

図 16-8 Download Firmware From RCP 画面

以下の項目があります。

| 項目 | 説明 |
|------------------|---|
| Unit | プルダウンメニューを使用してファームウェアの受信ユニットを選択します。全ユニットのためには「All」を選択します。 |
| RCP Server IP | 使用する RCP サーバの IP アドレスを指定します。 |
| Source File | 送信元ファイルの位置と名前を入力します。 |
| User Name | RCP サーバにログインするためのリモートユーザ名を入力します。 |
| Destination File | 送信先ファイルの位置と名前を入力します。 |
| Boot Up | ボックスをチェックして起動ファイルとして設定します。 |

「Download」 ボタンをクリックすると、ダウンロードが開始されます。

Download Firmware From HTTP (HTTP からファームウェアをダウンロード)

コンピュータからスイッチにファームウェアをダウンロードして、スイッチを更新することができます。

Web マネージャ先頭の **Tools > Download Firmware > From HTTP** を選択して以下の画面を表示します。

図 16-9 Download Firmware From HTTP 画面

以下の項目があります。

| 項目 | 説明 |
|------------------|---|
| Unit | プルダウンメニューを使用してファームウェアの受信ユニットを選択します。全ユニットのためには「All」を選択します。 |
| Source File | 送信元ファイルの位置と名前を入力するか、または「参照」 ボタンをクリックして、ダウンロード用のファームウェアファイルを参照します。 |
| Destination File | 送信先ファイルの位置と名前を入力します。 |
| Boot Up | ボックスをチェックして起動ファイルとして設定します。 |

「参照」 ボタンをクリックすると、ダウンロードのためのファームウェアファイルを参照することができます。

「Download」 ボタンをクリックすると、ダウンロードが開始されます。

Upload Firmware (ファームウェアのアップロード)

スイッチにファームウェアをアップロードします。

Upload Firmware To TFTP (ファームウェアを TFTP にアップロードする)

スイッチから TFTP サーバにファームウェアをアップロードすることができます。

Web マネージャ先頭の **Tools > Upload Firmware > To TFTP** を選択して以下の画面を表示します。

図 16-10 Upload Firmware To TFTP 画面

以下の項目があります。

| 項目 | 説明 |
|------------------|--|
| Unit | プルダウンメニューを使用してファームウェアのアップロード用ユニットを選択します。 |
| TFTP Server IP | 使用する TFTP サーバの IP アドレスを指定します。 <ul style="list-style-type: none"> IPv4 - ラジオボタンをクリックして、使用する TFTP サーバの IP アドレスを指定します。 IPv6 - ラジオボタンをクリックして、使用する TFTP サーバの IPv6 アドレスを指定します。 Domain Name - ラジオボタンをクリックして、ドメイン名を入力します。 |
| Destination File | 送信先ファイルの位置と名前を入力します。 |
| Source File | 送信元ファイルの位置と名前を入力します。 |

「Upload」ボタンをクリックすると、アップロードが開始されます。

Upload Firmware To RCP (ファームウェアを RCP にアップロードする)

スイッチから RCP サーバにファームウェアをアップロードすることができます。

Web マネージャ先頭の **Tools > Upload Firmware > To RCP** を選択して以下の画面を表示します。

図 16-11 Upload Firmware To RCP 画面

以下の項目があります。

| 項目 | 説明 |
|------------------|--|
| Unit | プルダウンメニューを使用してファームウェアのアップロード用ユニットを選択します。 |
| RCP Server IP | 使用する RCP サーバの IP アドレスを指定します。 |
| User Name | 使用する適切なユーザ名を指定します。 |
| Destination File | 送信先ファイルの位置と名前を入力します。 |
| Source File | 送信元ファイルの位置と名前を入力します。 |

「Upload」ボタンをクリックすると、アップロードが開始されます。

Upload Firmware To HTTP (ファームウェアを HTTP にアップロードする)

スイッチから HTTP サーバにファームウェアをアップロードすることができます。

Web マネージャ先頭の **Tools > Upload Firmware > To HTTP** を選択して以下の画面を表示します。

図 16-12 Upload Firmware To HTTP 画面

以下の項目があります。

| 項目 | 説明 |
|-------------|--|
| Unit | プルダウンメニューを使用してファームウェアのアップロード用ユニットを選択します。 |
| Source File | 送信元ファイルの位置と名前を入力します。 |

「Upload」 ボタンをクリックすると、アップロードが開始されます。

Download Configuration (コンフィグレーションのダウンロード)

スイッチにコンフィグレーションをダウンロードするために以下の画面を使用します。

Download Configuration From TFTP (TFTP サーバからコンフィグレーションファイルをダウンロードする)

TFTP サーバからスイッチにコンフィグレーションをダウンロードして、スイッチを更新することができます。

Web マネージャ先頭の **Tools > Download Configuration > From TFTP** を選択して以下の画面を表示します。

図 16-13 Download Configuration From TFTP 画面

以下の項目があります。

| 項目 | 説明 |
|------------------|--|
| Unit | プルダウンメニューを使用してコンフィグレーションの受信ユニットを選択します。全ユニットのためには「All」を選択します。 |
| TFTP Server IP | 使用する TFTP サーバの IP アドレスを指定します。 <ul style="list-style-type: none"> IPv4 - ラジオボタンをクリックして、使用する TFTP サーバの IP アドレスを指定します。 IPv6 - ラジオボタンをクリックして、使用する TFTP サーバの IPv6 アドレスを指定します。 Domain Name - ラジオボタンをクリックして、ドメイン名を入力します。 |
| Source File | 送信元ファイルの位置と名前を入力します。 |
| Destination File | 送信先ファイルの位置と名前を入力します。 |
| Increment | ボックスをチェックすると、新しいコンフィグレーションを適用する前に、既存のコンフィグレーションを保持します。ボックスからチェックを外すと、新しいコンフィグレーションを適用する前に、既存のコンフィグレーションをクリアします。 |

「Download」 ボタンをクリックすると、ダウンロードが開始されます。

Download Configuration From RCP (RCP サーバからコンフィグレーションファイルをダウンロードする)

RCP サーバからスイッチにコンフィグレーションをダウンロードして、スイッチを更新することができます。

Web マネージャ先頭の **Tools > Download Configuration > From RCP** を選択して以下の画面を表示します。

図 16-14 Download Configuration From RCP 画面

以下の項目があります。

| 項目 | 説明 |
|------------------|---|
| Unit | プルダウンメニューを使用してコンフィグレーションの受信用ユニットを選択します。全ユニットのためには「All」を選択します。 |
| RCP Server IP | 使用する RCP サーバの IP アドレスを指定します。 |
| User Name | 使用する適切なユーザ名を指定します。 |
| Source File | 送信元ファイルの位置と名前を入力します。 |
| Destination File | 送信先ファイルの位置と名前を入力します。 |

「Download」ボタンをクリックすると、ダウンロードが開始されます。

Download Configuration From HTTP (HTTP からコンフィグレーションファイルをダウンロードする)

コンピュータからスイッチにコンフィグレーションをダウンロードして、スイッチを更新することができます。

Web マネージャ先頭の **Tools > Download Configuration > From HTTP** を選択して以下の画面を表示します。

図 16-15 Download Configuration From HTTP 画面

以下の項目があります。

| 項目 | 説明 |
|------------------|---|
| Unit | プルダウンメニューを使用してコンフィグレーションの受信用ユニットを選択します。全ユニットのためには「All」を選択します。 |
| Destination File | 送信先ファイルの位置と名前を入力します。 |
| Source File | 送信元ファイルの位置と名前を入力します。 |
| Increment | ボックスをチェックすると、新しいコンフィグレーションを適用する前に、既存のコンフィグレーションを保持します。ボックスからチェックを外すと、新しいコンフィグレーションを適用する前に、既存のコンフィグレーションをクリアします。 |

「参照」ボタンをクリックすると、ダウンロードのためのコンフィグレーションファイルを参照することができます。

「Download」ボタンをクリックすると、ダウンロードが開始されます。

Upload Configuration (コンフィグレーションファイルのアップロード)

スイッチからコンフィグレーションをアップロードするために以下の画面を使用します。

Upload Configuration To TFTP (TFTP サーバにコンフィグレーションをアップロードする)

スイッチから TFTP サーバにコンフィグレーションファイルをアップロードすることができます。

Web マネージャ先頭の **Tools > Upload Configuration > To TFTP** を選択して以下の画面を表示します。

図 16-16 Upload Configuration To TFTP 画面

以下の項目があります。

| 項目 | 説明 |
|------------------|--|
| Unit | プルダウンメニューを使用してコンフィグレーションのアップロード用ユニットを選択します。 |
| TFTP Server IP | 使用する TFTP サーバの IP アドレスを指定します。 <ul style="list-style-type: none"> IPv4 - ラジオボタンをクリックして、使用する TFTP サーバの IP アドレスを指定します。 IPv6 - ラジオボタンをクリックして、使用する TFTP サーバの IPv6 アドレスを指定します。 Domain Name - ラジオボタンをクリックして、ドメイン名を入力します。 |
| Source File | 送信元ファイルの位置と名前を入力します。 |
| Destination File | 送信先ファイルの位置と名前を入力します。 |
| Filter | SNMP、VLAN または STP のようなフィルタを「Include」(含む)、「Exclude」(除外する)、または「Begin」(開始する)のように指定できます。適切な「Filter」アクションを選択し、提供されたスペースにファイル名を入力します。 |

「Upload」ボタンをクリックすると、アップロードが開始されます。

Upload Configuration To RCP (コンフィグレーションを RCP サーバにアップロードする)

スイッチから RCP サーバにコンフィグレーションファイルをアップロードすることができます。

Web マネージャ先頭の **Tools > Upload Configuration > To RCP** を選択して以下の画面を表示します。

図 16-17 Upload Configuration To RCP 画面

以下の項目があります。

| 項目 | 説明 |
|---------------|---|
| Unit | プルダウンメニューを使用してコンフィグレーションのアップロード用ユニットを選択します。 |
| RCP Server IP | 使用する RCP サーバの IP アドレスを指定します。 |

| 項目 | 説明 |
|------------------|--|
| User Name | 使用する適切なユーザ名を指定します。 |
| Destination File | 送信先ファイルの位置と名前を入力します。 |
| Source File | 送信元ファイルの位置と名前を入力します。 |
| Filter | プルダウンメニューを使用して、SNMP、VLAN または STP のようなフィルタを「Include」(含む)、「Exclude」(除外する)、または「Begin」(開始する) ように指定できます。適切な「Filter」アクションを選択し、提供されたスペースにファイル名を入力します。 |

「Upload」ボタンをクリックすると、アップロードが開始されます。

Upload Configuration To HTTP(コンフィギュレーションを HTTP にアップロードする)

スイッチからコンピュータにコンフィギュレーションファイルをアップロードすることができます。

Web マネージャ先頭の **Tools > Upload Configuration > To HTTP** を選択して以下の画面を表示します。

図 16-18 Upload Configuration To HTTP 画面

以下の項目があります。

| 項目 | 説明 |
|-------------|--|
| Unit | プルダウンメニューを使用してコンフィギュレーションのアップロード用ユニットを選択します。 |
| Source File | 送信元ファイルの位置と名前を入力します。 |
| Filter | プルダウンメニューを使用して、SNMP、VLAN または STP のようなフィルタを「Include」(含む)、「Exclude」(除外する)、または「Begin」(開始する) ように指定できます。適切な「Filter」アクションを選択し、提供されたスペースにファイル名を入力します。 |

「Upload」ボタンをクリックすると、アップロードが開始されます。

Upload Log File (ログファイルのアップロード)

スイッチのログファイルをアップロードします。

Upload Log To TFTP (TFTP サーバにログをアップロードする)

スイッチから TFTP サーバにログファイルをアップロードすることができます。

Web マネージャ先頭の **Tools > Upload Log File > To TFTP** を選択して以下の画面を表示します。

図 16-19 Upload Log To TFTP 画面

以下の項目があります。

| 項目 | 説明 |
|------------------|---|
| TFTP Server IP | 使用する TFTP サーバの IP アドレスを指定します。 <ul style="list-style-type: none"> IPv4 - ラジオボタンをクリックして、使用する TFTP サーバの IP アドレスを指定します。 IPv6 - ラジオボタンをクリックして、使用する TFTP サーバの IPv6 アドレスを指定します。 Domain Name - ラジオボタンをクリックして、ドメイン名を入力します。 |
| Destination File | 送信先ファイルの位置と名前を入力します。 |
| Log Type | 転送されるログのタイプを選択します。 <ul style="list-style-type: none"> Common Log - 一般的なログエントリをアップロードします。 Attack Log - 攻撃に関するログをアップロードします。 |

「Upload」ボタンをクリックすると、アップロードが開始されます。

Upload Log To RCP (RCP サーバにログをアップロードする)

スイッチから RCP サーバにログファイルをアップロードすることができます。

Web マネージャ先頭の **Tools > Upload Log File > To RCP** を選択して以下の画面を表示します。

図 16-20 Upload Log To RCP 画面

以下の項目があります。

| 項目 | 説明 |
|------------------|--|
| RCP Server IP | 使用する RCP サーバの IP アドレスを指定します。 |
| User Name | 使用する適切なユーザ名を指定します。 |
| Destination File | 送信先ファイルの位置と名前を入力します。 |
| Log Type | 転送されるログのタイプを選択します。 <ul style="list-style-type: none"> Common Log - 一般的なログエントリをアップロードします。 Attack Log - 攻撃に関するログをアップロードします。 |

「Upload」ボタンをクリックすると、アップロードが開始されます。

Upload Log To HTTP (HTTP にログをアップロードする)

スイッチからコンピュータにログファイルをアップロードすることができます。

Web マネージャ先頭の **Tools > Upload Log File > To HTTP** を選択して以下の画面を表示します。

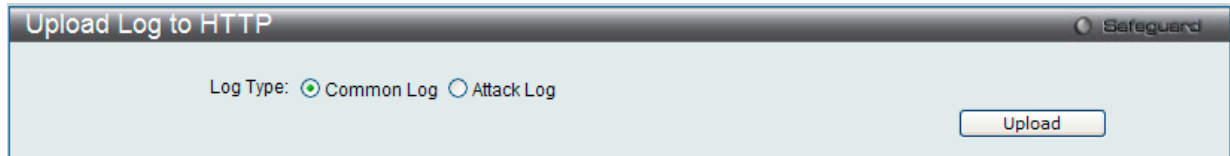


図 16-21 Upload Log To HTTP 画面

以下の項目があります。

| 項目 | 説明 |
|----------|--|
| Log Type | <p>転送されるログのタイプを選択します。</p> <ul style="list-style-type: none"> Common Log - 一般的なログエントリをアップロードします。 Attack Log - 攻撃に関するログをアップロードします。 |

「Upload」ボタンをクリックすると、アップロードが開始されます。

Reset (リセット)

スイッチのリセット機能にはいくつかのオプションが用意されています。いくつかのパラメータの設定内容を保持したままで、他のすべての設定内容を工場出荷時状態に戻すことが可能です。

注意 「Reset System」オプションだけは工場出荷時設定をスイッチの NV-RAM に書き込み、スイッチを再起動します。他のすべてのオプションは現在の設定を出荷時設定に戻しますが、この設定は保存されません。「Reset System」はスイッチのコンフィギュレーションを工場出荷状態まで戻します。

「Reset」はスイッチのユーザアカウント、ヒストリログを除いて他のすべての設定を工場出荷時の初期設定に戻します。スイッチは、本画面を使用してリセットされ、「Save Changes」が実行されないと、スイッチは再起動時に最後に保存されたコンフィギュレーションに戻ります。

Web マネージャ先頭の **Tools > Reset** を選択し、以下の画面を表示します。

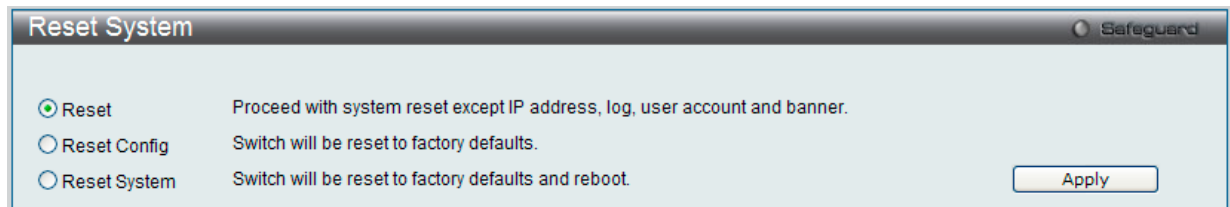


図 16-22 Reset System 画面

| 項目 | 説明 |
|--------------|---|
| Reset | IP アドレス、ユーザアカウントおよびバナーを除いてスイッチを工場出荷時の初期設定に戻します。 |
| Reset Config | スイッチを工場出荷時設定にリセットしますが、再起動は行いません。 |
| Reset System | スイッチを工場出荷時設定にリセットして、再起動を実行します。 |

「Apply」ボタンをクリックして、リセット操作を開始します。

Reboot System (システムの再起動)

以下の画面を使用してスイッチの再起動を行います。

Tools > Reboot の順にクリックし、以下の画面を表示します。

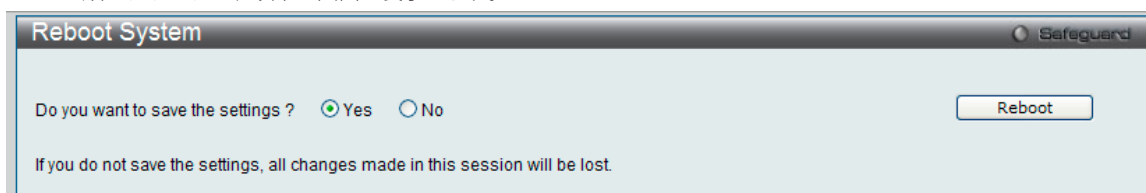


図 16-23 Reboot System 画面

| 項目 | 説明 |
|--------|---|
| Yes | スイッチは再起動する前に現在の設定を NV-RAM に保存します。 |
| No | スイッチは再起動する前に現在の設定を保存しません。すべての設定情報は破棄され、最後に保存した時の設定が使われます。 |
| Reboot | スイッチは再起動します。 |

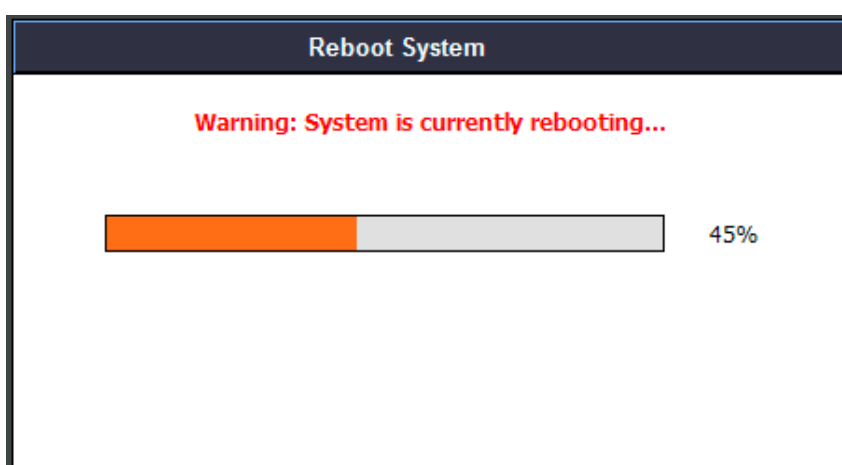


図 16-24 System Reboot 画面

付録 A ケーブルとコネクタ

イーサネットケーブル

スイッチを別のスイッチ、ブリッジまたはハブに接続する場合、ノーマルケーブルが必要です。ケーブルピンアサインに合うことを再確認してください。

以下の図と表は標準の RJ-45 プラグ / コネクタとピンアサインです。

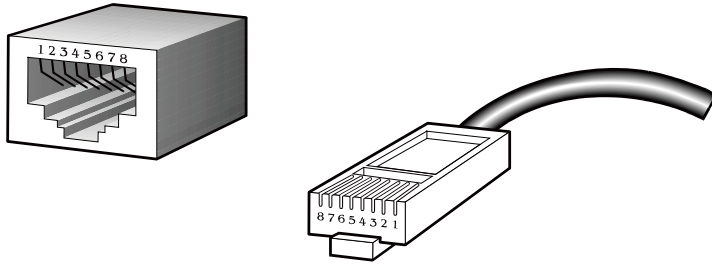


図 A-1 標準的な RJ-45 プラグとコネクタ

| RJ-45 ピンアサイン | | |
|--------------|------------|------------|
| コンタクト (ピン番号) | MDI-X 信号 | MDI-II 信号 |
| 1 | RD+ (受信) | TD+ (送信) |
| 2 | RD- (受信) | TD- (送信) |
| 3 | TD+ (送信) | RD+ (受信) |
| 4 | 1000BASE-T | 1000BASE-T |
| 5 | 1000BASE-T | 1000BASE-T |
| 6 | TD- (送信) | RD- (受信) |
| 7 | 1000BASE-T | 1000BASE-T |
| 8 | 1000BASE-T | 1000BASE-T |

コンソールケーブル

スイッチを PC に接続する場合、付属のコンソールケーブルが必要です。以下の図と表は標準のコンソール -RJ45 へのソケット / コネクタとそれらのピンアサインです。

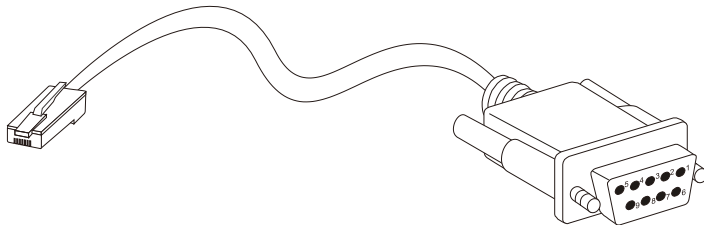


図 A-2 標準的なコンソール -RJ-45 ケーブル

| コンソール -RJ-45 ピンアサイン | | |
|---------------------|------------------------|-------|
| ピン番号 | コンソール (D-Sub9 / RS232) | RJ-45 |
| 1 | 未使用 | 未使用 |
| 2 | RXD | 未使用 |
| 3 | TXD | TXD |
| 4 | 未使用 | GND |
| 5 | GND (共有) | GND |
| 6 | 未使用 | RXD |
| 7 | 未使用 | 未使用 |
| 8 | 未使用 | 未使用 |

リダント電源 (RPS) ケーブル

スイッチをリダント電源に接続する場合、RPS ケーブルが必要です。製品がケーブルのピンアサインに一致することを確認してください。以下の図と表は標準のRPSのソケット/コネクタとそれらのピンアサインです。

注意 DGS-3420-28PC と DGS-3420-52P は RPS-500 ではなく RPS-700 を使用します。どちらもパッケージに自身のケーブルが同梱されています。

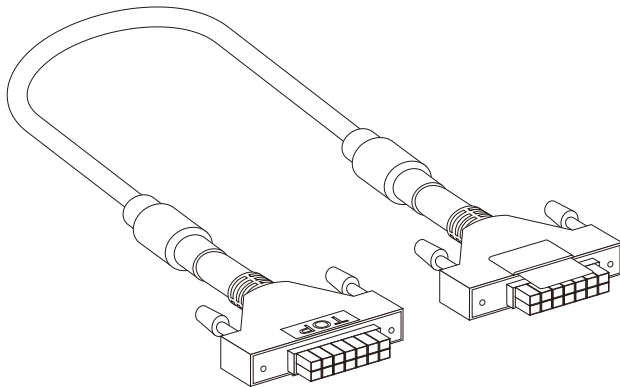


図 A-3 リダント電源ケーブル

| RPS ケーブルピンアサイン | | |
|----------------|------|---------|
| ピン番号 | デバイス | DPS-500 |
| 1 | GND | GND |
| 2 | NC | NC |
| 3 | +12V | +12V |
| 4 | +12V | +12V |
| 5 | +12V | +12V |
| 6 | +12V | +12V |
| 7 | GND | GND |
| 8 | GND | GND |
| 9 | NC | 電力良好 |
| 10 | NC | 電力供給 |
| 11 | 電力良好 | NC |
| 12 | 電力供給 | NC |
| 13 | GND | GND |
| 14 | GND | GND |

| RPS ケーブルピンアサイン | | |
|----------------|-------------|-------------|
| ピン番号 | デバイス | DPS-700 |
| 1 | -54Vrtn | -54Vrtn |
| 2 | -54V | -54V |
| 3 | +12V | +12V |
| 4 | +12V | +12V |
| 5 | +12V | +12V |
| 6 | +12V | +12V |
| 7 | NC/GND | NC/GND |
| 8 | +12vsen | +12Ven |
| 9 | LS-54v | LS-54V |
| 10 | -54V | -54V |
| 11 | -54Vrtn | -54Vrtn |
| 12 | GND | GND |
| 13 | GND/NC | GND/NC |
| 14 | RPS Present | RPS Present |
| 15 | Status_1 | RPS PG |
| 16 | Status_2 | GND |

| RPS ケーブルピンアサイン | | |
|----------------|------------|------------|
| 17 | RPS PG | Status_1 |
| 18 | GND | Status_2 |
| 19 | +12VRTNsen | +12VRTNsen |
| 20 | LS+12V | LS+12V |
| 21 | -54Vsen | -54Vsen |

付録 B ケーブル長

以下の表は各規格に対応するケーブル長（最大）です。

表 B-1 ケーブル長

| 規格 | メディアタイプ | 最大伝送距離 |
|------------|---|--------|
| SFP | 1000BASE-LX、シングルモードファイバモジュール | 10km |
| | 1000BASE-SX、マルチモードファイバモジュール | 550m |
| | 1000BASE-LH、シングルモードファイバモジュール | 40km |
| | 1000BASE-ZX、シングルモードファイバモジュール | 80km |
| 1000BASE-T | エンハンスドカテゴリ 5 UTP ケーブル カテゴリ 5 UTP ケーブル (1000Mbps) | 100m |
| 100BASE-TX | カテゴリ 5 UTP ケーブル (100Mbps) | 100m |
| 10BASE-T | カテゴリ 3 UTP ケーブル (10Mbps) | 100m |

付録C ログエントリ

スイッチのシステムログに表示される可能性のあるログエントリとそれらの意味を以下に示します。

Critical (重大)、Warning (警告)、Informational (報告)

| カテゴリ | ログの内容 | 緊急度 | イベントの説明 | 摘要 |
|--|--|--|-------------------------------|---|
| MBAC | MAC-based Access Control unauthenticated host (MAC: <macaddr>, Port <[unitID:]portNum>, VID: <vid>) unitID: ユニット ID macaddr: MAC アドレス portNum: ポート番号 vid: ホストが存在する VLAN ID | Critical | ホストは認証に失敗しました。 | |
| | Port < [unitID:]portNum> enters MAC-based Access Control stop learning state. unitID: ユニット ID portNum: ポート番号 | Warning | MAC ベースアクセス制御は学習停止状態になりました。 | ポートにおける認可ユーザ数が最大ユーザ数の制限に到達しました。 |
| | Port <[unitID:]portNum> recovers from MAC-based Access Control stop learning state. unitID: ユニット ID portNum: ポート番号 | Warning | MAC ベースアクセス制御は学習停止状態から回復しました。 | ポートにおける認可ユーザ数は経過時間に存在する最大ユーザ数を下回っています。(間隔はプロジェクトによって異なります。) |
| | MAC-based Access Control enters stop learning state. | Warning | MAC ベースアクセス制御は学習停止状態になりました。 | デバイス全体の認可ユーザ数が最大ユーザ数に到達しました。 |
| | MAC-based Access Control recovers from stop learning state. | Warning | MAC ベースアクセス制御は学習停止状態から回復しました。 | 全デバイスにおける認可ユーザ数は経過時間に存在する最大ユーザ数を下回っています。(間隔はプロジェクトによって異なります。) |
| | MBAC | MAC-based Access Control host login successful (MAC: <macaddr>, port: <[unitID:]portNum>, VID: <vid>) macaddr: MAC アドレス unitID: ユニット ID portNum: ポート番号 vid: ホストが存在する VLAN ID | Informational | MAC ベースアクセス制御ホストはログインに成功しました。 |
| MAC-based Access Control host aged out (MAC: <macaddr>, port: <[unitID:]portNum>, VID: <vid>) macaddr: MAC アドレス unitID: ユニット ID portNum: ポート番号 vid: ホストが存在する VLAN ID | | Informational | ホストはエイジングアウトします。 | |
| PTP | PTP port <[unitID:]portNum> role changed to <ptp_role>. unitID: ユニット ID portNum: ポート番号 ptp_role: ポートの PTP ロール | Informational | PTP ポートのロールが変更されました。 | |
| | The boundary clock synchronized to its master, the offset value is <+ -><Offset> second(s). Offset: スレーブとマスタのオフセット。 | Informational | PTP クロックが同期しました。 | 1 秒以上同期した場合にだけ、ログメッセージは送信されます。 |

| カテゴリ | ログの内容 | 緊急度 | イベントの説明 | 摘要 |
|---------------|--|---------------|---|---|
| DHCPv6 クライアント | DHCPv6 client on interface <ipif-name> changed state to [enabled disabled]. <ipif-name>: DHCPv6 クライアントインタフェース名 | Informational | インタフェースの DHCPv6 クライアントを有効または無効に変更しました。 | DHCPv6 クライアントインタフェースの管理状態を変更しました。 |
| | DHCPv6 client obtains an ipv6 address < ipv6address > on interface <ipif-name>. ipv6address: DHCPv6 サーバから取得した IPv6 アドレス ipif-name: DHCPv6 クライアントインタフェース名 | Informational | DHCPv6 クライアントはインタフェースに IPv6 アドレスを取得しました。 | DHCPv6 クライアントは DHCPv6 サーバから IPv6 アドレスを取得しました。 |
| | The IPv6 address < ipv6address > on interface <ipif-name> starts renewing. ipv6address: DHCPv6 サーバから取得した IPv6 アドレス ipif-name: DHCPv6 クライアントインタフェース名 | Informational | DHCPv6 サーバから取得した IPv6 アドレスの更新を開始しました。 | |
| | The IPv6 address < ipv6address > on interface <ipif-name> renews success. ipv6address: DHCPv6 サーバから取得した IPv6 アドレス ipif-name: DHCPv6 クライアントインタフェース名 | Informational | DHCPv6 サーバから取得した IPv6 アドレスの更新に成功しました。 | |
| | The IPv6 address < ipv6address > on interface <ipif-name> starts rebinding. ipv6address: DHCPv6 サーバから取得した IPv6 アドレス。 ipif-name: DHCPv6 クライアントインタフェース名。 | Informational | DHCPv6 サーバから取得した IPv6 アドレスの再割り付けを開始しました。 | |
| | The IPv6 address < ipv6address > on interface <ipif-name> rebinds success. ipv6address: DHCPv6 サーバから取得した IPv6 アドレス ipif-name: DHCPv6 クライアントインタフェース名 | Informational | DHCPv6 サーバから取得した IPv6 アドレスの再割り付けに成功しました。 | |
| | The IPv6 address < ipv6address > on interface <ipif-name> was deleted. ipv6address: DHCPv6 サーバから取得した IPv6 アドレス ipif-name: DHCPv6 クライアントインタフェース名 | Informational | DHCPv6 サーバから取得した IPv6 アドレスは削除されました。 | |
| DHCPv6 リレー | DHCPv6 relay on interface <ipif-name> changed state to [enabled disabled] ipif-name: DHCPv6 クライアントインタフェース名。 | Informational | 指定 イン タ フ ェ ー ス DHCPv6 リレーの管理モードが変更されました。 | |
| DHCPv6 サーバ | The address of the DHCPv6 Server pool <pool-name> is used up. <pool-name>: DHCPv6 サーバプール名 | Informational | DHCPv6 サーバプールのアドレスが使用されます。 | |
| DHCPv6 サーバ | The number of allocated ipv6 addresses of the DHCPv6 Server pool is equal to 4096. | Informational | 割り当てられた DHCPv6 サーバプールの IPv6 アドレス数が 4096 です。 | 割り当てられた IPv6 アドレス数が 4096 です。 |

付録C ログエントリ

| カテゴリ | ログの内容 | 緊急度 | イベントの説明 | 摘要 |
|------|--|---------------|----------------------|----|
| RCP | [RCP(1):] [Unit <unitID>] Firmware upgraded by <session> successfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) unitID: スタックシステム内のデバイス ID session: ユーザセッション username: 現在のログインユーザ ipaddr: クライアント IP アドレス macaddr: クライアント MAC アドレス | Informational | ファームの更新成功。 | |
| | [RCP(2):] [Unit <unitID>] Firmware upgrade by <session> unsuccessfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) unitID: スタックシステム内のデバイス ID session: ユーザセッション username: 現在のログインユーザ ipaddr: クライアント IP アドレス macaddr: クライアント MAC アドレス | Warning | ファームの更新失敗。 | |
| | [RCP(3):]Firmware uploaded by <session> successfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) session: ユーザセッション username: 現在のログインユーザ ipaddr: クライアント IP アドレス macaddr: クライアント MAC アドレス | Informational | ファームのアップロード成功。 | |
| | [RCP(4):]Firmware upload by <session> unsuccessfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) session: ユーザセッション username: 現在のログインユーザ ipaddr: クライアント IP アドレス macaddr: クライアント MAC アドレス | Warning | ファームウェアのアップロード失敗。 | |
| | [RCP(5):]Configuration downloaded by <session> successfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) session: ユーザセッション username: 現在のログインユーザ ipaddr: クライアント IP アドレス macaddr: クライアント MAC アドレス | Informational | コンフィグレーションのダウンロード成功。 | |
| | [RCP(6):]Configuration download by <session> unsuccessfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) session: ユーザセッション username: 現在のログインユーザ ipaddr: クライアント IP アドレス macaddr: クライアント MAC アドレス | Warning | コンフィグレーションのダウンロード失敗。 | |
| | [RCP(7):]Configuration uploaded by <session> successfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) session: ユーザセッション username: 現在のログインユーザ ipaddr: クライアント IP アドレス macaddr: クライアント MAC アドレス | Informational | コンフィグレーションのアップロード成功。 | |
| | [RCP(8):]Configuration upload by <session> unsuccessfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) session: ユーザセッション username: 現在のログインユーザ ipaddr: クライアント IP アドレス macaddr: クライアント MAC アドレス | Warning | コンフィグレーションのアップロード失敗。 | |

| カテゴリ | ログの内容 | 緊急度 | イベントの説明 | 摘要 |
|----------------|--|---------------|--------------------------|----|
| RCP | [RCP(9):]Log message uploaded by <session> successfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) session: ユーザセッション username: 現在のログインユーザ ipaddr: クライアント IP アドレス macaddr: クライアント MAC アドレス | Informational | ログメッセージのアップロード成功。 | |
| | [RCP(10):]Log message upload by <session> unsuccessfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) session: ユーザセッション username: 現在のログインユーザ ipaddr: クライアント IP アドレス macaddr: クライアント MAC アドレス | Warning | ログメッセージのアップロード失敗。 | |
| | [RCP(11):]The downloaded configurations executed by <session> successfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) session: ユーザセッション username: 現在のログインユーザ ipaddr: クライアント IP アドレス macaddr: クライアント MAC アドレス | Informational | ダウンロードしたコンフィグレーションの実行成功。 | |
| | [RCP(12):]The downloaded configurations executed by <session> unsuccessfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) session: ユーザセッション username: 現在のログインユーザ ipaddr: クライアント IP アドレス macaddr: クライアント MAC アドレス | Warning | ダウンロードしたコンフィグレーションの実行失敗。 | |
| | [RCP(13):]Attack log message uploaded by <session> successfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) session: ユーザセッション username: 現在のログインユーザ ipaddr: クライアント IP アドレス macaddr: クライアント MAC アドレス | Informational | 攻撃ログメッセージのアップロード成功。 | |
| | [RCP(14):]Attack log message upload by <session> unsuccessfully. (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) session: ユーザセッション username: 現在のログインユーザ ipaddr: クライアント IP アドレス macaddr: クライアント MAC アドレス | Warning | 攻撃ログメッセージのアップロード失敗。 | |
| TFTP クライアント | [TFTP(1):] [Unit <unitID>.] Firmware upgraded by <session> successfully (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) unitID: スタックシステム内のデバイス ID session: ユーザセッション username: 現在のログインユーザ ipaddr: クライアント IP アドレス macaddr: クライアント MAC アドレス | Informational | ファームウェアの更新成功。 | |
| | [TFTP(2):] [Unit <unitID>.] Firmware upgrade by <session> was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) unitID: スタックシステム内のデバイス ID session: ユーザセッション username: 現在のログインユーザ ipaddr: クライアント IP アドレス macaddr: クライアント MAC アドレス | Warning | ファームウェアの更新失敗。 | |

付録C ログエントリ

| カテゴリ | ログの内容 | 緊急度 | イベントの説明 | 摘要 |
|----------------|---|---------------|----------------------|----|
| TFTP クライアント | [TFTP(3):]Firmware successfully uploaded by <session> (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) session: ユーザセッション username: 現在のログインユーザ ipaddr: クライアント IP アドレス macaddr: クライアント MAC アドレス | Informational | ファームウェアのアップロード成功。 | |
| | [TFTP(4):]Firmware upload by <session> was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) session: ユーザセッション username: 現在のログインユーザ ipaddr: クライアント IP アドレス macaddr: クライアント MAC アドレス | Warning | ファームウェアのアップロード失敗。 | |
| | [TFTP(5):]Configuration successfully downloaded by <session> (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) session: ユーザセッション username: 現在のログインユーザ ipaddr: クライアント IP アドレス macaddr: クライアント MAC アドレス | Informational | コンフィグレーションのダウンロード成功。 | |
| | [TFTP(6):]Configuration download by <session> was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) session: ユーザセッション username: 現在のログインユーザ ipaddr: クライアント IP アドレス macaddr: クライアント MAC アドレス | Warning | コンフィグレーションのダウンロード失敗。 | |
| | [TFTP(7):]Configuration successfully uploaded by <session> (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) session: ユーザセッション username: 現在のログインユーザ ipaddr: クライアント IP アドレス macaddr: クライアント MAC アドレス | Informational | コンフィグレーションのアップロード成功。 | |
| | [TFTP(8):]Configuration upload by <session> was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) session: ユーザセッション username: 現在のログインユーザ ipaddr: クライアント IP アドレス macaddr: クライアント MAC アドレス | Warning | コンフィグレーションのアップロード失敗。 | |
| | [TFTP(9):]Log message successfully uploaded by <session> (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) session: ユーザセッション username: 現在のログインユーザ ipaddr: クライアント IP アドレス macaddr: クライアント MAC アドレス | Informational | ログメッセージのアップロード成功。 | |
| | [TFTP(10):]Log message upload by <session> was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) session: ユーザセッション username: 現在のログインユーザ ipaddr: クライアント IP アドレス macaddr: クライアント MAC アドレス | Warning | ログメッセージのアップロード失敗。 | |
| | [TFTP(13):]Attack log message successfully uploaded by <session> (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) session: ユーザセッション username: 現在のログインユーザ ipaddr: クライアント IP アドレス macaddr: クライアント MAC アドレス | Informational | 攻撃ログメッセージのアップロード成功。 | |

| カテゴリ | ログの内容 | 緊急度 | イベントの説明 | 摘要 |
|----------------|---|---------------|--|---------------------------------------|
| TFTP クライアント | [TFTP(14):]Attack log message upload by <session> was unsuccessful! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>) session: ユーザセッション username: 現在のログインユーザ ipaddr: クライアント IP アドレス macaddr: クライアント MAC アドレス | Warning | 攻撃ログメッセージのアップロード失敗。 | |
| DNS リゾルバ | [DNS_RESOLVER(1):]Duplicate Domain name case name: <domainname>, static IP: <ipaddr>, dynamic IP:<ipaddr> domainname: ドメイン名 ipaddr: IP アドレス | Informational | 重複するドメイン名が追加されたため、ダイナミックドメイン名が削除されました。 | |
| ARP | Conflict IP was detected with this device (IP: <ipaddr>, MAC: <macaddr>, Port <[unitID:]portNum>, Interface: <ipif_name>). ipaddr: 自分のデバイスと重複する IP アドレス macaddr: 自分のデバイスと重複する IP アドレスを持つデバイスの MAC アドレス unitID: 1. 整数値; 2. スタックシステム内のデバイス ID portNum: 1. 整数値; 2. デバイスの論理ポート番号 ipif_name: 重複する IP アドレスを持つスイッチのインタフェース名 | Warning | IP コンフリクトの検出。 | Gratuituous ARP が重複する IP アドレスを検出しました。 |
| Telnet | Successful login through Telnet (Username: <username>, IP: <ipaddr>) ipaddr: Telnet クライアントの IP アドレス username: Telnet サーバにログインしたユーザ名 | Informational | Telnet 経由のログインに成功しました。 | |
| | Login failed through Telnet (Username: <username>, IP: <ipaddr>) ipaddr: Telnet クライアントの IP アドレス username: Telnet サーバにログインしたユーザ名 | Warning | Telnet 経由のログインに失敗しました。 | |
| | Logout through Telnet (Username: <username>, IP: <ipaddr>) ipaddr: Telnet クライアントの IP アドレス username: Telnet サーバにログインしたユーザ名 | Informational | Telnet からログアウトしました。 | |
| | Telnet session timed out (Username: <username>, IP: <ipaddr>). ipaddr: Telnet クライアントの IP アドレス username: Telnet サーバにログインしたユーザ名 | Informational | Telnet セッションのタイムアウト | |
| ポート | Port <[unitID:]portNum> link up, <link state> unitID: 1. 整数値; 2. スタックシステム内のデバイス ID portNum: 1. 整数値; 2. デバイスの論理ポート番号 ipif_name: 重複する IP アドレスを持つスイッチのインタフェース名 link state: ポートのリンク状態 (例: 100Mbps FULL duplex) | Informational | ポートリンクアップ | |
| | Port <[unitID:]portNum> link down unitID: 1. 整数値; 2. スタックシステム内のデバイス ID portNum: 1. 整数値; 2. デバイスの論理ポート番号 | Informational | ポートリンクダウン | |

付録C ログエントリ

| カテゴリ | ログの内容 | 緊急度 | イベントの説明 | 摘要 |
|--------|--|---------------|---|----|
| 802.1X | 802.1X Authentication failure [for <reason>] from (Username: <username>, Port: <[unitID:]portNum>, MAC: <macaddr>) reason: 認証エラーの原因 username: 認証されるユーザ unitID: ユニット番号 portNum: スイッチのポート番号 macaddr: 認証デバイスの MAC アドレス | Warning | 802.1X 認証失敗。 | |
| | 802.1X Authentication successful from (Username: <username>, Port: <[unitID:]portNum>, MAC: <macaddr>) username: 認証されるユーザ unitID: ユニット番号 portNum: スイッチのポート番号 macaddr: 認証デバイスの MAC アドレス | Informational | 802.1X 認証成功。 | |
| RADIUS | RADIUS server <ipaddr> assigned VID :<vlanID> to port <[unitID:]portNum> (account :<username>) ipaddr: RADIUS サーバの IP アドレス vlanID: RADIUS が割り当てる VLAN ID unitID: ユニット番号 portNum: ポート番号 Username: 認証されるユーザ名 | Informational | RADIUS クライアントが RADIUS サーバによって認証された後、RADIUS サーバから VID が割り当てられました。この VID はポートに割り当てられ、このポートは VLAN タグなしメンバーになります。 | |
| | RADIUS server <ipaddr> assigned ingress bandwidth :<ingressBandwidth> to port <[unitID:]portNum> (account : <username>) ipaddr: RADIUS サーバの IP アドレス ingressBandwidth: RADIUS が割り当てる Ingress 帯域 unitID: ユニット番号 portNum: ポート番号 Username: 認証されるユーザ名 | Informational | RADIUS クライアントが RADIUS サーバによって認証された後、RADIUS サーバから Ingress 帯域が割り当てられました。この Ingress 帯域はポートに割り当てられません。 | |
| | RADIUS server <ipaddr> assigned egress bandwidth :<egressBandwidth> to port <[unitID:]portNum> (account: <username>) ipaddr: RADIUS サーバの IP アドレス egressBandwidth: RADIUS が割り当てる RADIUS の Egress 帯域 unitID: ユニット番号 portNum: ポート番号 Username: 認証されるユーザ名 | Informational | RADIUS クライアントが RADIUS サーバによって認証された後、RADIUS サーバから Egress 帯域が割り当てられました。この Egress 帯域はポートに割り当てられません。 | |
| | RADIUS server <ipaddr> assigned 802.1p default priority:<priority> to port <[unitID:]portNum> (account : <username>) ipaddr: RADIUS サーバの IP アドレス priority: RADIUS が割り当てる優先度 unitID: ユニット番号 portNum: ポート番号 Username: 認証されるユーザ名 | Informational | RADIUS クライアントが RADIUS サーバによって認証された後、RADIUS サーバから 802.1p デフォルトプライオリティが割り当てられました。802.1p デフォルトプライオリティはポートに割り当てられません。 | |
| | RADIUS server <ipaddr> assigns <username> ACL failure at port <[unitID:]portNum> (<string>) ipaddr: RADIUS サーバの IP アドレス unitID: ユニット番号 portNum: ポート番号 Username: 認証されるユーザ名 string: 失敗した RADIUS ACL コマンドの文字列 | Warning | RADIUS サーバからの ACL プロファイル/ルールの割り当てに失敗しました。 | |

| カテゴリ | ログの内容 | 緊急度 | イベントの説明 | 摘要 |
|----------|---|--------|------------------------------|----|
| LLDP-MED | <p>LLDP-MED topology change detected (on port <portNum>. chassis id: <chassisType>, <chassisID>, port id: <portType>, <portID>, device class: <deviceClass>)</p> <p>portNum: ポート番号 chassisType: シャーシ ID サブタイプ 値のリスト: 1. chassisComponent(1) 2. interfaceAlias(2) 3. portComponent(3) 4. macAddress(4) 5. networkAddress(5) 6. interfaceName(6) 7. local(7) chassisID: シャーシ ID. portType: ポート ID サブタイプ 値のリスト: 1. interfaceAlias(1) 2. portComponent(2) 3. macAddress(3) 4. networkAddress(4) 5. interfaceName(5) 6. agentCircuitId(6) 7. local(7) portID: ポート ID deviceClass: LLDP-MED デバイスタイプ</p> | Notice | LLDP-MED トポロジの変更が検出されました。 | |
| | <p>Conflict LLDP-MED device type detected (on port < portNum >, chassis id: < chassisType>, <chassisID>, port id: < portType>, <portID>, device class: <deviceClass>)</p> <p>portNum: ポート番号 chassisType: シャーシ ID サブタイプ 値のリスト: 1. chassisComponent(1) 2. interfaceAlias(2) 3. portComponent(3) 4. macAddress(4) 5. networkAddress(5) 6. interfaceName(6) 7. local(7) chassisID: シャーシ ID. portType: ポート ID サブタイプ 値のリスト: 1. interfaceAlias(1) 2. portComponent(2) 3. macAddress(3) 4. networkAddress(4) 5. interfaceName(5) 6. agentCircuitId(6) 7. local(7) portID: ポート ID deviceClass: LLDP-MED デバイスタイプ</p> | Notice | LLDP-MED デバイスタイプの重複が検出されました。 | |

付録C ログエントリ

| カテゴリ | ログの内容 | 緊急度 | イベントの説明 | 摘要 |
|----------|---|---------------|---|----|
| LLDP-MED | Incompatible LLDP-MED TLV set detected (on port < portNum >, chassis id: < chassisType>, <chassisID>, port id: < portType>, <portID>, device class: <deviceClass>) portNum: ポート番号 chassisType: シャーシ ID サブタイプ 値のリスト: 1. chassisComponent(1) 2. interfaceAlias(2) 3. portComponent(3) 4. macAddress(4) 5. networkAddress(5) 6. interfaceName(6) 7. local(7) chassisID: シャーシ ID. portType: ポート ID サブタイプ 値のリスト: 1. interfaceAlias(1) 2. portComponent(2) 3. macAddress(3) 4. networkAddress(4) 5. interfaceName(5) 6. agentCircuitId(6) 7. local(7) portID: ポート ID deviceClass: LLDP-MED デバイスタイプ | Notice | 互換性のない LLDP-MED TLV が検出されました。 | |
| 音声 VLAN | New voice device detected (Port <portNum>, MAC <macaddr>) portNum: ポート番号 macaddr: 音声デバイスの MAC アドレス | Informational | 新しい音声 VLAN がポートに検出されました。 | |
| | Port < portNum > add into Voice VLAN <vid > portNum: ポート番号 vid:VLAN ID | Informational | 自動音声 VLAN モードのポートを音声 VLAN に追加しました。 | |
| | Port < portNum > remove from Voice VLAN <vid > portNum: ポート番号 vid:VLAN ID | Informational | ポートが音声 VLAN から離脱し、同時にそのポートのエージングタイム内に音声 VLAN が見つからないとログメッセージを送信します。 | |
| DULD | [DULD(1):] port:<[unitID:] portNum> is unidirectional. unitID: ユニット番号 portNum: ポート番号 | Informational | 単方向リンクが本ポートに検出されました。 | |
| Stacking | Unit <unitID>, MAC: <macaddr> Hot insertion. unitID: ユニット番号 Macaddr: MAC アドレス | Informational | ホットインサージョン | |
| | Unit <unitID>, MAC: <macaddr> Hot removal. unitID: ユニット番号 Macaddr: MAC アドレス | Informational | ホットリムーブ | |
| | Stacking topology is <Stack_TP_TYPE>. Master(Unit <unitID>, MAC:<macaddr>). Stack_TP_TYPE: スタックトポロジのタイプは以下の通りです.: 1. Ring (リング) 2. Chain (チェーン) unitID: ユニット番号 Macaddr: MAC アドレス | Informational | スタックトポロジの変更 | |
| | Backup master changed to master. Master (Unit: <unitID>). unitID: ユニット番号 | Informational | バックアップマスタがマスタに変更になりました。 | |

| カテゴリ | ログの内容 | 緊急度 | イベントの説明 | 摘要 |
|------------|--|---------------|----------------------------------|----|
| Stacking | Slave changed to master. Master (Unit: <unitID>). unitID: ユニット番号 | Informational | スレーブがマスタに変更になりました。 | |
| | Hot insert failed, box ID conflict: Unit <unitID> conflict (MAC: <macaddr> and MAC: <macaddr>). unitID: ユニット番号 macaddr: 重複するユニットの MAC アドレス | Critical | ユニット番号が重複しています。 | |
| SNMP | SNMP request received from <ipaddr> with invalid community string. ipaddr: IP アドレス | Informational | 無効なコミュニティ名を含む SNMP request 受信 | |
| Web (SSL) | Successful login through Web (Username: <username>, IP: <ipaddr>). username: HTTP サーバにログインするユーザ名 ipaddr: HTTP クライアント IP アドレス | Informational | Web 経由のログイン成功 | |
| | Login failed through Web (Username: <username>, IP: <ipaddr>). username: HTTP サーバにログインするユーザ名 ipaddr: HTTP クライアント IP アドレス | Warning | Web 経由のログイン失敗 | |
| | Web session timed out (Username: <username>, IP: <ipaddr>). username: HTTP サーバにログインするユーザ名 ipaddr: HTTP クライアント IP アドレス | Informational | Web セッションタイムアウト | |
| | Logout through Web (Username: %S, IP: %S). username: HTTP サーバにログインするユーザ名 ipaddr: HTTP クライアント IP アドレス | Informational | Web 経由でログアウトしました。 | |
| | Successful login through Web(SSL) (Username: <username>, IP: <ipaddr>). username: SSL サーバにログインするユーザ名 ipaddr: SSL クライアント IP アドレス | Informational | Web(SSL) 経由のログイン成功。 | |
| | Login failed through Web(SSL) (Username: <username>, IP: <ipaddr>). username: SSL サーバにログインするユーザ名 ipaddr: SSL クライアント IP アドレス | Warning | Web(SSL) 経由のログイン失敗。 | |
| | Web(SSL) session timed out (Username: <username>, IP: <ipaddr>). username: SSL サーバにログインするユーザ名 ipaddr: SSL クライアント IP アドレス | Informational | Web(SSL) セッションタイムアウト。 | |
| | Logout through Web(SSL) (Username: <username>, IP: <ipaddr>). username: SSL サーバにログインするユーザ名 ipaddr: SSL クライアント IP アドレス | Informational | Web(SSL) 経由でログアウトしました。 | |
| ポートセキュリティ | Port security violation (MAC: < macaddr > on port:: < unitID: portNum >) macaddr: 違反 MAC アドレス unitID: ユニット番号 portNum: ポート番号 | Warning | ポートにおけるアドレスフル | |
| セーフガードエンジン | Unit< unitID >, Safeguard Engine enters NORMAL mode unitID: ユニット番号 | Informational | セーフガードエンジンが normal モードに入りました。 | |
| | Unit< unitID >, Safeguard Engine enters EXHAUSTED mode unitID: ユニット番号 | Warning | セーフガードエンジンが exhausted モードに入りました。 | |

付録C ログエントリ

| カテゴリ | ログの内容 | 緊急度 | イベントの説明 | 摘要 |
|------|--|---------------|---|----|
| DoS | Possible spoofing attack from IP: <ipaddr>, MAC: <macaddr>, port: <unitID:portNum> ipaddr: IP アドレス macaddr: 違反 MAC アドレス unitID: ユニット番号 portNum: ポート番号 | Critical | Spoofing 攻撃の可能性があります。 | |
| | DoS attack is blocked Log Message: <dos_name> is blocked from (IP: <ipaddr> Port: <[unit ID:]portNum>) dos_name: DoS 攻撃の種類 ipaddr: IP アドレス portNum: ポート番号 | Informational | DoS 攻撃をブロックしました。 | |
| AAA | Successful login through <Console Telnet Web(SSL) SSH>(Username: <username>, IP: <ipaddr ipv6address>). ipaddr: IP アドレス username: ユーザ名 ipv6address: IPv6 アドレス | Informational | ログイン成功。 | |
| | Login failed through <Console Telnet Web(SSL) SSH> (Username: <username>, IP: <ipaddr ipv6address>). ipaddr: IP アドレス username: ユーザ名 ipv6address: IPv6 アドレス | Warning | ログイン失敗。 | |
| | Logout through <Console Telnet Web(SSL) SSH> (Username: <username>, IP: <ipaddr ipv6address>). ipaddr: IP アドレス username: ユーザ名 ipv6address: IPv6 アドレス | Informational | ログアウトしました。 | |
| | <Console Telnet Web(SSL) SSH> session timed out (Username: <username>, IP: <ipaddr ipv6address>). ipaddr: IP アドレス username: ユーザ名 ipv6address: IPv6 アドレス | Informational | セッションタイムアウト | |
| | SSH server is enabled | Informational | SSH サーバの有効化 | |
| | SSH server is disabled | Informational | SSH サーバの無効化 | |
| | Authentication Policy is enabled (Module: AAA). | Informational | 認証ポリシーの有効化 | |
| | Authentication Policy is disabled (Module: AAA). | Informational | 認証ポリシーの無効化 | |
| | Login failed through <Console Telnet Web(SSL) SSH> from <ipaddr ipv6address> due to AAA server <ipaddr ipv6address> timeout or improper configuration (Username: <username>). ipaddr: IP アドレス username: ユーザ名 ipv6address: IPv6 アドレス | Warning | AAA サーバのタイムアウトまたは不適切な設定のため、ログインに失敗。 | |
| | Successful Enable Admin through <Console Telnet Web(SSL) SSH> from <ipaddr ipv6address> authenticated by AAA <local none server <ipaddr ipv6address>> (Username: <username>). local: AAA ローカル方式による enable admin none: AAA none 方式による enable admin server: AAA サーバ方式による enable admin ipaddr: IP アドレス ipv6address: IPv6 アドレス username: ユーザ名 | Informational | AAA ローカル、none またはサーバによる Enable Admin に成功。 | |

| カテゴリ | ログの内容 | 緊急度 | イベントの説明 | 摘要 |
|------|---|---------------|---|--|
| AAA | Enable Admin failed through <Console Telnet Web(SSL) SSH> from <ipaddr ipv6address> due to AAA server <ipaddr ipv6address> timeout or improper configuration (Username: <username>) ipaddr: IP アドレス ipv6address: IPv6 アドレス username: ユーザ名 | Warning | AAA サーバのタイムアウトまたは不適切な設定のため、サーバによる Enable Admin に失敗。 | |
| | Log Message: Enable Admin failed through <Console Telnet Web(SSL) SSH> from <ipaddr ipv6address> authenticated by AAA <local server <ipaddr ipv6address>> (Username: <username>). local: AAA ローカル方式による enable admin server: AAA サーバ方式による enable admin ipaddr: IP アドレス ipv6address: IPv6 アドレス username: ユーザ名 | Warning | AAA ローカルまたはサーバによる Enable Admin に失敗。 | |
| | Successful login through <Console Telnet Web(SSL) SSH> from < ipaddr ipv6address > authenticated by AAA <local none server <ipaddr ipv6address>> (Username: <username>). local: AAA ローカル方式を指定 none: AAA none 方式を指定 server: AAA サーバ方式を指定 ipaddr: IP アドレス ipv6address: IPv6 アドレス username: ユーザ名 | Informational | AAA ローカル、none、またはサーバによるログイン認証に成功。 | |
| | Login failed through <Console Telnet Web(SSL) SSH> from <ipaddr ipv6address> authenticated by AAA <local server <ipaddr ipv6address>> (Username: <username>). local: AAA ローカル方式を指定 server: AAA サーバ方式を指定 ipaddr: IP アドレス ipv6address: IPv6 アドレス username: ユーザ名 | Warning | AAA ローカル、またはサーバによるログイン認証に失敗。 | |
| WAC | WAC unauthenticated user (User Name: <string>, IP: <ipaddr ipv6address>, MAC: <macaddr>, Port: <[unitID:]portNum>) string: ユーザ名 ipaddr: IP アドレス ipv6address: IPv6 アドレス macaddr: MAC アドレス unitID: ユニット ID portNum : ポート番号 | Warning | クライアントホストは認証に失敗しました。 | |
| | WAC enters stop learning state. | Warning | WAC は学習停止状態になりました。 | 認可ユーザ数がデバイス全体で最大ユーザ数の制限に到達した場合にこのログが発生します。 |
| | WAC recovered from stop learning state. | Warning | WAC は学習停止状態から回復しました。 | 時間（5分）経過後認可ユーザ数が最大ユーザ数を下回るとこのログが発生します。 |

付録C ログエントリ

| カテゴリ | ログの内容 | 緊急度 | イベントの説明 | 摘要 |
|----------------|---|---------------|--------------------------------------|--|
| WAC | WAC authenticated user (Username: <string>, IP: <ipaddr ipv6address>, MAC: <macaddr>, Port: <[unitID:] portNum>) string: ユーザ名 ipaddr: IP アドレス ipv6address: IPv6 アドレス macaddr: MAC アドレス unitID: ユニット ID portNum: ポート番号 | Informational | クライアントホストは認証に成功しました。 | |
| JWAC | JWAC authenticated user (Username: <string>, IP: <ipaddr>, MAC: <macaddr>, Port: <[unitID:]portNum>) string: ユーザ名 ipaddr: IP アドレス macaddr: MAC アドレス unitID: ユニット ID portNum: ポート番号 | Informational | クライアントホストが認証に成功。 | |
| | JWAC unauthenticated user (User Name: <string>, IP: <ipaddr>, MAC: <macaddr>, Port: <[unitID:]portNum>) string: ユーザ名 ipaddr: IP アドレス macaddr: MAC アドレス unitID: ユニット ID portNum: ポート番号 | Warning | クライアントホストが認証に失敗。 | |
| | JWAC enters stop learning state. | Warning | JWAC は学習停止状態になりました。 | 認可ユーザ数がデバイス全体で最大ユーザ数の制限に到達した場合にこのログが発生します。 |
| | JWAC recovered from stop learning state. | Warning | JWAC は学習停止状態から回復しました。 | 時間経過 (5 分) 後認可ユーザ数が最大ユーザ数を下回るとこのログが発生します。 |
| ループバック検知 (LBD) | Port < [unitID:] portNum> LBD loop occurred. Port blocked. unitID: ユニット ID portNum: ポート番号 | Critical | ポートベースモードでループが発生し、ポートはブロックされました。 | |
| | Port < [unitID:] portNum> LBD port recovered. Loop detection restarted unitID: ユニット ID portNum: ポート番号 | Informational | ポートベースモードで LBD ブロック状態からポートは回復しました。 | |
| | Port < [unitID:] portNum> VID <vlanID> LBD loop occurred. Packet discard begun unitID: ユニット ID portNum: ポート番号 vlanID: VLAN ID 番号 | Critical | VLAN ベースモードでループが発生しました。 | |
| | Port < [unitID:] portNum> VID <vlanID> LBD recovered. Loop detection restarted unitID: ユニット ID portNum: ポート番号 vlanID: VLAN ID 番号 | Informational | VLAN ベースモードで LBD ブロック状態からポートは回復しました。 | |
| | Loop VLAN number overflow. | Informational | ループが発生した VLAN ID が指定番号と一致しています。 | |

| カテゴリ | ログの内容 | 緊急度 | イベントの説明 | 摘要 |
|------|---|---------|--|----|
| IMPB | Dynamic IMPB entry conflicts with static ARP(IP: <ipaddr>, MAC: <macaddr>, Port <[unitID:]portNum>) | Warning | ダイナミック IMPB エントリがスタティック ARP と重複しています。 | |
| | Dynamic IMPB entry conflicts with static FDB(IP: [<ipaddr> <ipv6addr>], MAC: <macaddr>, Port <[unitID:]portNum>) ipaddr: IP アドレス ipv6addr: IPv6 アドレス macaddr: MAC アドレス unitID: ユニット ID portNum: ポート番号 | Warning | ダイナミック IMPB エントリがスタティック FDB と重複しています。 | |
| | Dynamic IMPB entry conflicts with static IMPB(IP: [<ipaddr> <ipv6addr>], MAC: <macaddr>, Port <[unitID:]portNum>). ipaddr: IP アドレス ipv6addr: IPv6 アドレス macaddr: MAC アドレス unitID: ユニット ID portNum: ポート番号 | Warning | ダイナミック IMPB エントリがスタティック IMPB と重複しています。 | |
| | Creating IMPB entry failed due to no ACL rule being available(IP:[<ipaddr> <ipv6addr>], MAC: <macaddr>, Port <[unitID:]portNum>) ipaddr: IP アドレス ipv6addr: IPv6 アドレス macaddr: MAC アドレス unitID: ユニット ID portNum: ポート番号 | Warning | 有効な ACL ルールがないため、IMPB エントリの作成に失敗しました。 | |
| | Unauthenticated IP-MAC address and discarded by IMPB (IP: [< ipaddr > < ipv6addr >], MAC :< macaddr >, Port <[unitID:]portNum >). ipaddr: IP アドレス ipv6addr: IPv6 アドレス macaddr: MAC アドレス unitID: ユニット ID portNum: ポート番号 | Warning | IMPB はホストの不正をチェックしました。 | |
| | Dynamic IMPB entry conflicts with static ND (IP: [< ipaddr > < ipv6addr >], MAC: <macaddr>, Port <[unitID:]portNum>) ipaddr: IP アドレス ipv6addr: IPv6 アドレス macaddr: MAC アドレス unitID: ユニット ID portNum: ポート番号 | Warning | ダイナミック IMPB エントリがスタティック ND と重複しています。 | |

付録C ログエントリ

| カテゴリ | ログの内容 | 緊急度 | イベントの説明 | 摘要 |
|-----------------|--|---------------|---|----|
| トラフィックコントロール | Port <unitID: portNum> Broadcast storm is occurring. unitID: ユニット ID portNum: ポート番号 | Warning | ブロードキャストストームが発生。 | |
| | Port <unitID: portNum> broadcast storm has cleared. unitID: ユニット ID portNum: ポート番号 | Informational | ブロードキャストストームが解消。 | |
| | Port <unitID: portNum> Multicast storm is occurring. unitID: ユニット ID portNum: ポート番号 | Warning | マルチキャストストームが発生。 | |
| | Port <unitID: portNum> multicast storm has cleared. unitID: ユニット ID portNum: ポート番号 | Informational | マルチキャストストームが解消。 | |
| | Port <[unitID:]portNum> is currently shut down due to the <packet-type> storm unitID: ユニット ID portNum: ポート番号 packet-type: マルチキャストやブロードキャストを含むストームパケットの種類 | Warning | パケットストームによるポートのシャットダウン | |
| DHCP サーバスクリーニング | Detected untrusted DHCP server(IP: <ipaddr>,Port <[unitID:]portNum>) ipaddr: デバイスに検出した信頼性の低い IP アドレス unitID: ユニット ID portNum: デバイスの論理ポート番号 | Informational | 信頼性の低い DHCP サーバの IP アドレスを検出。 | |
| | Detected untrusted DHCPv6 server (IP: <ipv6addr>, Port:<[unitID:]portNum>) ipv6addr: IPv6 アドレス unitID: ユニット ID portNum: ポート番号 | Informational | 信頼性の低い DHCPv6 サーバの IP アドレスを検出。 | |
| | Detected untrusted source IP of ICMPv6 Router Advertisement message (IP: <ipv6addr>, Port:<[unitID:]portNum>) ipv6addr: IPv6 アドレス unitID: ユニット ID portNum: ポート番号 | Informational | 信頼性の低い送信元 IP アドレスを ICMPv6 ルータアドバタイズメントメッセージで検出。 | |
| ERPS | Signal failure detected on node (MAC: <macaddr>) macaddr: ノードのシステム MAC | Notice | 信号のエラーを検出しました。 | |
| | Signal failure cleared on node (MAC: <macaddr>) macaddr: ノードのシステム MAC | Notice | 信号のエラーがクリアされました。 | |
| | RPL owner conflicted on the ring (MAC: <macaddr>) macaddr: ノードのシステム MAC | Warning | RPL オーナーが重複しています。 | |

| カテゴリ | ログの内容 | 緊急度 | イベントの説明 | 摘要 |
|-----------------|---|---------------|--|----|
| MSTP デバッグ 拡張 | Topology changed [([Instance:<InstanceID>],port:<[unitID:] portNum> ,MAC: <macaddr>)] InstanceID: インスタンス ID. portNum: ポート ID macaddr: MAC アドレス | Notice | トポロジ変更 | |
| | [CIST CIST Regional MSTI Regional] New Root bridge selected([Instance: <InstanceID>]MAC: <macaddr> Priority :<value>) InstanceID: インスタンス ID. macaddr: MAC アドレス value: ルートブリッジの優先度 | Informational | スパニングツリーの新規ルートブリッジを選択 | |
| | Spanning Tree Protocol is enabled | Informational | スパニングツリープロトコル有効化 | |
| | Spanning Tree Protocol is disabled | Informational | スパニングツリープロトコル無効化 | |
| | New root port selected [([Instance:<InstanceID>], port:<[unitID:] portNum>)] InstanceID: インスタンス ID. portNum: ポート ID | Notice | 新しいルートポートが選択されました。 | |
| | Spanning Tree port status changed [([Instance:<InstanceID>], port:<[unitID:] portNum>)] <old_status> -> <new_status> InstanceID: インスタンス ID portNum: ポート ID old_status: 古いステータス new_status: 新しいステータス | Notice | スパニングツリーポートステータスが変更されました。 | |
| | Spanning Tree port status changed. [([Instance:<InstanceID>], port:<[unitID:] portNum>)] <old_role> -> <new_role> InstanceID: インスタンス ID portNum: ポート ID old_status: 古いロール new_status: 新しいロール | Informational | スパニングツリーポートロールが変更されました。 | |
| | Spanning Tree instance created. Instance:<InstanceID> InstanceID: インスタンス ID | Informational | スパニングツリーインスタンスが作成されました。 | |
| | Spanning Tree instance deleted. Instance:<InstanceID> InstanceID: インスタンス ID | Informational | スパニングツリーインスタンスが削除されました。 | |
| | Spanning Tree version changed. New version:<new_version> new_version: 新しい STP バージョン | Informational | スパニングツリーのバージョンが変更されました。 | |
| | Spanning Tree MST configuration ID name and revision level changed (name:<name> ,revision level <revision_level>). name : 新しい名称 revision_level : 新しいリビジョンレベル | Informational | スパニングツリー MST コンフィグレーション ID 名とリビジョンが変更されました。 | |
| | Spanning Tree MST configuration ID VLAN mapping table changed (instance: <InstanceID> delete vlan <startvlanid> [-<endvlanid>]). InstanceID: インスタンス ID startvlanid- endvlanid : VLAN リスト | Informational | スパニングツリー MST コンフィグレーション ID VLAN マッピングテーブルが削除されました。 | |
| | Spanning Tree MST configuration ID VLAN mapping table changed (instance: <InstanceID> add vlan <startvlanid> [-<endvlanid>]). InstanceID: インスタンス ID startvlanid- endvlanid : VLAN リスト | Informational | スパニングツリー MST コンフィグレーション ID VLAN マッピングテーブルが追加されました。 | |

| カテゴリ | ログの内容 | 緊急度 | イベントの説明 | 摘要 |
|------|--|----------|----------------------------------|----|
| CFM | <p>CFM cross-connect. VLAN:<vlanid>, Local(MD Level:<mdlevel>, Port <[unitID:]portNum>, Direction:<mepdirection>) Remote(MEPID:<mepid>, MAC:<macaddr>)</p> <p>vlanid: MEP の VLAN 識別子 mdlevel: MEP の MD レベル unitID: スタックシステムにおけるデバイス ID portNum: MEP の論理ポート番号 mepdirection: 「inward」または「outward」 mepid: MEP の MEPID。0 の値は未知の MEPID を意味します。 macaddr: MEP の MAC アドレス。すべて 0 の値は未知の MAC アドレスを意味します。</p> <p>注意 CFM ハードウェアモードでは、リモート MEP 情報 (mepid および macaddr) は不明です。</p> | Critical | クロスコネクトが検出されました。 | |
| | <p>CFM error ccm. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <[unitID:]portNum>, Direction:<mepdirection>) Remote(MEPID:<mepid>, MAC:<macaddr>)</p> <p>vlanid: MEP の VLAN 識別子 mdlevel: MEP の MD レベル unitID: スタックシステムにおけるデバイス ID portNum: MEP の論理ポート番号 mepdirection: 「inward」または「outward」 mepid: MEP の MEPID。0 の値は未知の MEPID を意味します。 macaddr: MEP の MAC アドレス。すべて 0 の値は未知の MAC アドレスを意味します。</p> <p>注意 CFM ハードウェアモードでは、リモート MEP 情報 (mepid および macaddr) は不明です。</p> | Warning | エラー CFM CCM パケットが検出されました。 | |
| | <p>CFM remote down. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <[unitID:]portNum>, Direction:<mepdirection>) Remote(MEPID:<mepid>, MAC:<macaddr>)</p> <p>vlanid: MEP の VLAN 識別子 mdlevel: MEP の MD レベル unitID: Represents the ID of the device in the stacking system. portNum: MEP の論理ポート番号 mepdirection: MEP 方向 (「inward」または「outward」) mepid: MEP の MEPID macaddr: MEP の MAC アドレス</p> | Warning | リモート MEP の CCM パケットを受信できません。 | |
| | <p>CFM remote MAC error. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <[unitID:]portNum>, Direction:<mepdirection>) Remote(MEPID:<mepid>, MAC:<macaddr>) <mepdirection></p> <p>vlanid: MEP の VLAN 識別子 mdlevel: MEP の MD レベル unitID: スタックシステムにおけるデバイス ID portNum: MEP の論理ポート番号 mepdirection: MEP の方向 (「inward」または「outward」) mepid: MEP の MEPID。0 の値は未知の MEPID を意味します。 macaddr: MEP の MAC アドレス。すべて 0 の値は未知の MAC アドレスを意味します。</p> | Warning | リモート MEP の MAC がエラー状態をレポートしています。 | |

| カテゴリ | ログの内容 | 緊急度 | イベントの説明 | 摘要 |
|--------|---|---------------|-----------------------------|----|
| CFM | CFM remote detects a defect. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <[unitID:]portNum>, Direction:<mepdirection>) Remote(MEPID:<mepid>, MAC:<macaddr>) vlanid: MEP の VLAN 識別子 mdlevel: MEP の MD レベル unitID: スタックシステムにおけるデバイス ID portNum: MEP の論理ポート番号 mepdirection: MEP の方向 (「inward」または「outward」) macaddr: MEP の MAC アドレス | Informational | リモートの MEP が CFM の欠陥を検出しました。 | |
| CFM 拡張 | [CFM_EXT(1):]AIS condition detected. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <[unitID:]portNum>, Direction:<mepdirection>, MEPID:<mepid>) vlanid: MEP の VLAN 識別子 mdlevel: MEP の MD レベル unitID: スタックシステムにおけるデバイス ID portNum: MEP の論理ポート番号 mepdirection: MEP の方向 (「inward」または「outward」) macaddr: MEP の MAC アドレス | Notice | AIS 状態が検出されました。 | |
| | [CFM_EXT(2):]AIS condition cleared. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <[unitID:]portNum>, Direction:<mepdirection>, MEPID:<mepid>) vlanid: MEP の VLAN 識別子 mdlevel: MEP の MD レベル unitID: スタックシステムにおけるデバイス ID portNum: MEP の論理ポート番号 mepdirection: MEP の方向 (「inward」または「outward」) macaddr: MEP の MAC アドレス | Notice | AIS 状態がクリアされました。 | |
| | [CFM_EXT(3):]LCK condition detected. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <[unitID:]portNum>, Direction:<mepdirection>, MEPID:<mepid>) vlanid: MEP の VLAN 識別子 mdlevel: MEP の MD レベル unitID: スタックシステムにおけるデバイス ID portNum: MEP の論理ポート番号 mepdirection: MEP の方向 (「inward」または「outward」) mepid: MEP の MEPID | Notice | LCK 状態が検出されました。 | |
| | [CFM_EXT(4):]LCK condition cleared. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <[unitID:]portNum>, Direction:<mepdirection>, MEPID:<mepid>) vlanid: MEP の VLAN 識別子 mdlevel: MEP の MD レベル unitID: スタックシステムにおけるデバイス ID portNum: MEP の論理ポート番号 mepdirection: MEP の方向 (「inward」または「outward」) mepid: MEP の MEPID | Notice | LCK 状態がクリアされました。 | |

付録C ログエントリ

| カテゴリ | ログの内容 | 緊急度 | イベントの説明 | 摘要 |
|--------------|---|---------------|------------------------|---|
| DDM | DDM Port <[unitID]:portNum> optic module [thresholdType] [exceedType] the [thresholdSubType] alarm threshold unitID: ユニット ID thresholdType: しきい値種類 exceedType: 超過種類 thresholdSubType: しきい値サブタイプ | Critical | DDM アラームしきい値の超過、または回復 | |
| | DDM Port <[unitID]:portNum> optic module [thresholdType] [exceedType] the [thresholdSubType] warning threshold unitID: ユニット ID thresholdType: しきい値種類 exceedType: 超過種類 thresholdSubType: しきい値サブタイプ | Warning | DDM 警告しきい値の超過、または回復 | |
| IP とパスワードの変更 | Unit <unitID>, Password was changed by [console] (Username: <username>[, IP: <ipaddr>]) unitID: ユニット ID username: ユーザ名 ipaddr: IP アドレス | Informational | パスワード変更のアクティビティ | "[console]" はコンソールセッション用です。 "[IP: <ipaddr>]" はコンソールセッションでは使用しません。 |
| | Unit <unitID>, Management IP address was changed by [console] (Username: <username>[, IP: <ipaddr>]) unitID: ユニット ID username: ユーザ名 ipaddr: IP アドレス | Informational | システム IP アドレス変更のアクティビティ | "[console]" はコンソールセッション用です。 "[IP: <ipaddr>]" はコンソールセッションでは使用しません。 |
| リンクアグリゲーション | Link aggregation Group <Group ID> (Interface: <ifIndex>) <linkstatus>. Group ID: グループ ID ifIndex: 変更のあったインタフェースインデックス linkstatus: リンクステータス | Informational | リンクアグリゲーショングループリンクの変更 | |

| カテゴリ | ログの内容 | 緊急度 | イベントの説明 | 摘要 |
|------|---|---------------|---|----|
| SSH | Successful login through <Console Telnet Web SSH>(Username: <username>, IP: <ipaddr ipv6address>). ipaddr: IP アドレス username: ユーザ名 ipv6address: IPv6 アドレス | Informational | ログイン成功 | |
| | Login failed through <Console Telnet Web SSH> (Username: <username>, IP: <ipaddr ipv6address>). ipaddr: IP アドレス username: ユーザ名 ipv6address: IPv6 アドレス | Warning | ログイン失敗 | |
| | Logout through <Console Telnet Web SSH> (Username: <username>, IP: <ipaddr ipv6address>). ipaddr: IP アドレス username: ユーザ名 ipv6address: IPv6 アドレス | Informational | ログアウトしました。 | |
| | <Console Telnet Web SSH> session timed out (Username: <username>, IP: <ipaddr ipv6address>). ipaddr: IP アドレス username: ユーザ名 ipv6address: IPv6 アドレス | Informational | セッションタイムアウトしました。 | |
| | SSH server is enabled | Informational | SSH サーバが有効です。 | |
| | SSH server is disabled | Informational | SSH サーバが無効です。 | |
| | Login failed through <Console Telnet Web SSH> from <ipaddr ipv6address> due to AAA server <ipaddr ipv6address> timeout or improper configuration (Username: <username>). ipaddr: IP アドレス username: ユーザ名 ipv6address: IPv6 アドレス | Warning | AAA サーバのタイムアウトまたは不適切な設定のため、ログインに失敗。 | |
| | Enable Admin failed through <Console Telnet Web SSH> from <ipaddr ipv6address> due to AAA server <ipaddr ipv6address> timeout or improper configuration (Username: <username>) ipaddr: IP アドレス ipv6address: IPv6 アドレス username: ユーザ名 | Warning | AAA サーバのタイムアウトまたは不適切な設定のため、バによる Enable Admin に失敗。 | |
| | Enable Admin failed through <Console Telnet Web SSH> from <ipaddr ipv6address> authenticated by AAA < local server <ipaddr ipv6address>> (Username: <username>). local: AAA ローカル方式による enable admin server: AAA サーバ方式による enable admin ipaddr: IP アドレス ipv6address: IPv6 アドレス username: ユーザ名 | Warning | AAA ローカルまたはサーバによる Enable Admin に失敗。 | |
| | Successful Enable Admin through <Console Telnet Web SSH> from < ipaddr ipv6address > authenticated by AAA <local none server <ipaddr ipv6address>> (Username: <username>). local: AAA ローカル方式を指定 none: AAA none 方式を指定 server: AAA サーバ方式を指定 ipaddr: IP アドレス ipv6address: IPv6 アドレス username: ユーザ名 | Informational | AAA ローカル、none、またはサーバによるログイン認証に成功。 | |

付録C ログエントリ

| カテゴリ | ログの内容 | 緊急度 | イベントの説明 | 摘要 |
|-----------|--|---------------|------------------------------|----|
| SSH | Login failed through <Console Telnet Web SSH> from <ipaddr ipv6address> authenticated by AAA <local server <ipaddr ipv6address>> (Username: <username>). local: AAA ローカル方式を指定 server: AAA サーバ方式を指定 ipaddr: IP アドレス ipv6address: IPv6 アドレス username: ユーザ名 | Warning | AAA ローカル、またはサーバによるログイン認証に失敗。 | |
| | SSH client public keys file was upgraded successfully (Username: <username>, IP: < ipaddr ipv6address >) ipaddr: IP アドレス ipv6address: IPv6 アドレス username: ユーザ名 | Informational | SSH のクライアント公開鍵がアップグレードされました。 | |
| RIPng | RIPng protocol on interface <intf-name> changed state to <enabled disabled> intf-name: インフェース名 | Informational | RIPng 状態変更 | |
| BPDU 攻撃防止 | Port<[unitID:]portNum> enter BPDU under protection state (mode: drop / block / shutdown) unitID: ユニット ID. portNum: ポート番号 mode:BPDU の状態 | Informational | BPDU 攻撃防止中 | |
| | Port <[unitID:]portNum> recover from BPDU under protection state automatically unitID: ユニット ID. portNum: ポート番号 | Informational | BPDU 攻撃からの自動復帰中 | |
| | Port<[unitID:]portNum> recover from BPDU under protection state automatically unitID: ユニット ID. portNum: ポート番号 | Informational | BPDU 攻撃からの手動復帰中 | |

付録D トラップログ

本製品では、以下のトラップログが検出されます。

| カテゴリ | トラップ名 | 説明 | 摘要 |
|----------------|---|---|----|
| MBAC | swMacBasedAccessControlLoggedSuccess /1.3.6.1.4.1.171.12.35.11.1.0.1 | MAC ベースアクセスコントロールホストがログインに成功した場合に本トラップを送信します。 関連オブジェクト： (1) swMacBasedAuthInfoMacIndex (2) swMacBasedAuthInfoPortIndex (3) swMacBasedAuthVID | |
| | swMacBasedAccessControlLoggedFail /1.3.6.1.4.1.171.12.35.11.1.0.2 | MAC ベースアクセスコントロールホストがログインに失敗した場合に本トラップを送信します。 関連オブジェクト： (1) swMacBasedAuthInfoMacIndex (2) swMacBasedAuthInfoPortIndex (3) swMacBasedAuthVID | |
| | swMacBasedAccessControlAgesOut /1.3.6.1.4.1.171.12.35.11.1.0.3 | MAC ベースアクセスコントロールホストがエージングを行った場合に本トラップを送信します。 関連オブジェクト： (1) swMacBasedAuthInfoMacIndex (2) swMacBasedAuthInfoPortIndex (3) swMacBasedAuthVID | |
| LLDP | lldpRemTablesChange/1.0.8802.1.1.2.0.0.1 | lldpRemTablesChange 通知は、lldpStatsRemTableLastChangeTime の値が変更した場合に送信されます。LLDP リモートシステムテーブルのメンテナンスポーリングを引き起こすように NMS によって利用されます。 関連オブジェクト： (1) lldpStatsRemTablesInserts (2) lldpStatsRemTablesDeletes (3) lldpStatsRemTablesDrops (4) lldpStatsRemTablesAgeouts | |
| LLDP-MED | lldpXMedTopologyChangeDetected /1.0.8802.1.1.2.1.5.4795.0.1 | 新しいリモートデバイスがローカルポートに割り当てられたこと、またはリモートデバイスが切断またはあるポートから別のポートに移動したことを示すトポロジの変化に気づいたローカルデバイスによって生成される通知。 関連オブジェクト： (1) lldpRemChassisIdSubtype (2) lldpRemChassisId (3) lldpXMedRemDeviceClass | |
| 802.3ah OAM | dot3OamThresholdEvent /1.3.6.1.2.1.158.0.1 | 本通知は、ローカルまたはリモートのしきい値クロスイベントが検出された場合に送信されます。 関連オブジェクト： (1) dot3OamEventLogTimestamp (2) dot3OamEventLogOui (3) dot3OamEventLogType (4) dot3OamEventLogLocation (5) dot3OamEventLogWindowHi (6) dot3OamEventLogWindowLo (7) dot3OamEventLogThresholdHi (8) dot3OamEventLogThresholdLo (9) dot3OamEventLogValue (10) dot3OamEventLogRunningTotal (11) dot3OamEventLogEventTotal | |
| | dot3OamNonThresholdEvent /1.3.6.1.2.1.158.0.2 | 本通知は、ローカルまたはリモートのしきい値でないクロスイベントが検出された場合に送信されます。 関連オブジェクト： (1) dot3OamEventLogTimestamp (2) dot3OamEventLogOui (3) dot3OamEventLogType (4) dot3OamEventLogLocation (5) dot3OamEventLogEventTotal | |

付録D トラップログ

| カテゴリ | トラップ名 | 説明 | 摘要 |
|-------------------|--|---|----|
| アップ/ ダウンロード | agentFirmwareUpgrade /1.3.6.1.4.1.171.12.1.7.2.0.7 | 本トラップは、SNMP 経由でファームウェアの更新処理が完了した場合に送信されます。 関連オブジェクト： (1) swMultimageVersion | |
| | agentCfgOperCompleteTrap /1.3.6.1.4.1.171.12.1.7.2.0.9 | 本トラップは、コンフィギュレーションの保存、アップロード、またはダウンロードが完了した場合に送信されます。 関連オブジェクト： (1) unitID (2) agentCfgOperate (3) agentLoginUserName | |
| Gratuitous ARP | agentGratuitousARPTrap /1.3.6.1.4.1.171.12.1.7.2.0.5 | IP アドレスの重複があると、本トラップは送信されます。 関連オブジェクト： (1) agentGratuitousARPIpAddr (2) agentGratuitousARPMacAddr (3) agentGratuitousARPPortNumber (4) agentGratuitousARPInterfaceName | |
| Stacking | swUnitInsert /1.3.6.1.4.1.171.12.11.2.2.1.0.1 | ユニットのホットインサージョン通知 関連オブジェクト： (1) swUnitMgmtId. (2) swUnitMgmtMacAddr. | |
| | swUnitRemove /1.3.6.1.4.1.171.12.11.2.2.1.0.2 | ユニットのホットリムーブ通知 関連オブジェクト： (1) swUnitMgmtId. (2) swUnitMgmtMacAddr. | |
| | swUnitFailure /1.3.6.1.4.1.171.12.11.2.2.1.0.3 | ユニットのエラー通知 関連オブジェクト： (1) swUnitMgmtId. | |
| | swUnitTPChange /1.3.6.1.4.1.171.12.11.2.2.1.0.4 | スタッキングトポロジの変更通知 関連オブジェクト： (1) swStackTopologyType (2) swUnitMgmtId (3) swUnitMgmtMacAddr | |
| | swUnitRoleChange /1.3.6.1.4.1.171.12.11.2.2.1.0.5 | スタッキングユニットのロール変更通知 change notification. 関連オブジェクト： (1) swStackRoleType (2) swUnitMgmtId | |
| ポート セキュリティ | swL2PortSecurityViolationTrap /1.3.6.1.4.1.171.11.118.X.2.100.1.2.0.2 (X: モデル番号) | ポートセキュリティトラップが有効な場合、定義済みのポートセキュリティ設定に違反する新しい MAC アドレスがあると、トラップメッセージを送信します。 関連オブジェクト： (1) swPortSecPortIndex (2) swL2PortSecurityViolationMac | |
| SafeGuard | swSafeGuardChgToExhausted /1.3.6.1.4.1.171.12.19.4.1.0.1 | システムが「normal」から「exhausted」に操作モードを変更したことを示します。 関連オブジェクト： (1) swSafeGuardCurrentStatus | |
| | swSafeGuardChgToNormal /1.3.6.1.4.1.171.12.19.4.1.0.2 | システムが「exhausted」から「normal」に操作モードを変更したことを示します。 関連オブジェクト： (1) swSafeGuardCurrentStatus | |

| カテゴリ | トラップ名 | 説明 | 摘要 |
|------------------------|--|--|----|
| LBD | swPortLoopOccurred /1.3.6.1.4.1.171.12.41.10.0.1 | ポートにループが発生すると、本トラップを送信します。 関連オブジェクト： (1) swLoopDetectPortIndex | |
| | swPortLoopRestart /1.3.6.1.4.1.171.12.41.10.0.2 | ポートにループが一定間隔後に再度発生すると、本トラップを送信します。 関連オブジェクト： (1) swLoopDetectPortIndex | |
| | swVlanLoopOccurred /1.3.6.1.4.1.171.12.41.10.0.3 | LBD VLAN ベースモードでポートにループが発生すると、本トラップを送信します。 関連オブジェクト： (1) swLoopDetectPortIndex (2) swVlanLoopDetectVID | |
| | swVlanLoopRestart /1.3.6.1.4.1.171.12.41.10.0.4 | LBD VLAN ベースモードでポートにループが一定間隔後に再度発生すると、本トラップを送信します。 関連オブジェクト： (1) swLoopDetectPortIndex (2) swVlanLoopDetectVID | |
| BPDU Attack Protection | swBpduProtectionUnderAttackingTrap /1.3.6.1.4.1.171.12.76.4.0.1 | BPDU トラップが有効な場合、指定ポートが「normal」から「attack」ステートに変更すると、トラップが送信されます。 関連オブジェクト： (1) swBpduProtectionPortIndex (2) swBpduProtectionPortMode | |
| | swBpduProtectionRecoveryTrap /1.3.6.1.4.1.171.12.76.4.0.2 | BPDU 保護トラップが有効な場合、指定ポートが「attack」から「normal」ステートに変更すると、トラップが送信されます。 関連オブジェクト： (1) swBpduProtectionPortIndex (2) swBpduProtectionPortMode | |
| IMPB | swIpMacBindingViolationTrap /1.3.6.1.4.1.171.12.23.5.0.1 | IMPB トラップが有効な場合、定義済みのポートセキュリティ設定に違反する新しい MAC があると、トラップが送信されます。 関連オブジェクト： (1) swIpMacBindingPortIndex (2) swIpMacBindingViolationIP (3) swIpMacBindingViolationMac | |
| | swIpMacBindingIPv6ViolationTrap 1.3.6.1.4.1.171.12.23.5.0.4 | IMPB トラップが有効な場合、定義済みの IPv6 IP-MAC バインディング設定に違反する新しい MAC があると、トラップが送信されます。 関連オブジェクト： (1) swIpMacBindingPortIndex (2) swIpMacBindingViolationIPv6Addr (3) swIpMacBindingViolationMac | |
| DHCP Server Screening | swFilterDetectedTrap /1.3.6.1.4.1.171.12.37.100.0.1 | 不正な DHCP サーバを検出すると、本トラップは送信されます。ログ取得を停止する未許可期間に検出された同じ不正な DHCP サーバの IP アドレスをトラップ送信先に一度だけ送信します。 関連オブジェクト： (1) swFilterDetectedIP (2) swFilterDetectedport | |
| | swFilterDHCPv6ServerDetectedTrap /1.3.6.1.4.1.171.12.37.100.0.2 | 不正な DHCPv6 サーバを検出すると、本トラップは送信されます。 関連オブジェクト： (1) swFilterDetectedIPv6 (2) swFilterDetectedport | |
| | swFilterICMPv6RaAllNodesDetectedTrap /1.3.6.1.4.1.171.12.37.100.0.3 | 不正な ICMPv6 all-nodes RA を検出すると、本トラップは送信されます。 関連オブジェクト： (1) swFilterDetectedIPv6 (2) swFilterDetectedport | |

付録D トラップログ

| カテゴリ | トラップ名 | 説明 | 摘要 |
|-----------------|---|---|----|
| Traffic Control | swPktStormOccurred /1.3.6.1.4.1.171.12.25.5.0.1 | パケットストームメカニズムがパケットストームを検出し、アクションとしてシャットダウンする場合に本トラップを送信します。 関連オブジェクト： (1) swPktStormCtrlPortIndex | |
| | swPktStormCleared /1.3.6.1.4.1.171.12.25.5.0.2 | パケットストームメカニズムがパケットストームをクリアした場合に本トラップを送信します。 関連オブジェクト： (1) swPktStormCtrlPortIndex | |
| | swPktStormDisablePort /1.3.6.1.4.1.171.12.25.5.0.3 | パケットストームメカニズムによりポートが無効になりました。 関連オブジェクト： (1) swPktStormCtrlPortIndex | |
| ERPS | swERPSSFDetectedTrap /1.3.6.1.4.1.171.12.78.4.0.1 | 信号障害の発生時にトラップは生成されます。 関連オブジェクト： (1) swERPSSNodeId | |
| | swERPSSFClearedTrap /1.3.6.1.4.1.171.12.78.4.0.2 | 信号障害が解消するとトラップは生成されます。 関連オブジェクト： (1) swERPSSNodeId | |
| | swERPSPRLOwnerConflictTrap /1.3.6.1.4.1.171.12.78.4.0.3 | コンフリクトの発生時にトラップは生成されます。 関連オブジェクト： (1) swERPSSNodeId | |
| MSTP | newRoot /1.3.6.1.2.1.17.0.1 | newRoot トラップは、送信側のエージェントがスパニングツリーの新しいルートになったことを示します。 トラップは、新しいルートとして選出された後にすぐにブリッジによって送信され、その選出に続いてすぐに Topology Change Timer のアクションの起動などを行います。 本トラップの実行はオプションです。 | |
| | topologyChange /1.3.6.1.2.1.17.0.2 | topologyChange トラップは、構成するいずれかのポートが Learning 状態から Forwarding 状態に、Forwarding 状態から Blocking 状態に、または Forwarding 状態から Blocking 状態に遷移する場合にブリッジによって送信されます。 本トラップは、newRoot トラップが同様の変更に対して送信される場合には送信されません。 本トラップの実行はオプションです | |
| CFM | dot1agCfmFaultAlarm /1.3.111.2.802.1.1.8.0.1 | MEP に持続的な欠損条件があります。通知（故障警報）は故障を検出した MEP の OID を持つ管理エンティティに送信されます。 関連オブジェクト： (1) dot1agCfmMdlIndex (2) dot1agCfmMalIndex (3) dot1agCfmMeplIdentifier | |
| CFM 拡張 | swCFMExtAISOccurred /1.3.6.1.4.1.171.12.86.100.0.1 | 通知は、ローカル MEP が AIS ステータスに入ると生成されます。 関連オブジェクト： (1) dot1agCfmMdlIndex (2) dot1agCfmMalIndex (3) dot1agCfmMeplIdentifier | |
| | swCFMExtAISCleared /1.3.6.1.4.1.171.12.86.100.0.2 | 通知は、ローカル MEP が AIS ステータスから出ると生成されます。 関連オブジェクト： (1) dot1agCfmMdlIndex (2) dot1agCfmMalIndex (3) dot1agCfmMeplIdentifier | |
| | swCFMExtLockOccurred /1.3.6.1.4.1.171.12.86.100.0.3 | 通知は、ローカル MEP が Lock ステータスに入ると生成されます。 関連オブジェクト： (1) dot1agCfmMdlIndex (2) dot1agCfmMalIndex (3) dot1agCfmMeplIdentifier | |
| | swCFMExtLockCleared /1.3.6.1.4.1.171.12.86.100.0.4 | 通知は、ローカル MEP が Lock ステータスから出ると生成されます。 関連オブジェクト： (1) dot1agCfmMdlIndex (2) dot1agCfmMalIndex (3) dot1agCfmMeplIdentifier | |

| カテゴリ | トラップ名 | 説明 | 摘要 |
|--------------|--|---|----|
| ポート トラップ | linkUp /1.3.6.1.6.3.1.1.5.4 | 通知は、ポートのリンクアップ時に生成されます。 関連オブジェクト： (1) ifIndex (2) if AdminStatus (3) ifOperStatu | |
| | linkDown /1.3.6.1.6.3.1.1.5.3 | 通知は、ポートのリンクダウン時に生成されます。 関連オブジェクト： (1) ifIndex (2) if AdminStatus (3) ifOperStatu | |
| DDM | swDdmAlarmTrap /1.3.6.1.4.1.171.12.72.4.0.1 | トラップアクションの設定に基づいて、パラメータの値がアラームしきい値を超えると本トラップは送信されます。 関連トラップ： 1. swDdmPort 2. swDdmThresholdType 3. swDdmThresholdExceedType 4. swDdmThresholdExceedOrRecover | |
| | swDdmWarningTrap /1.3.6.1.4.1.171.12.72.4.0.2 | トラップアクションの設定に基づいて、パラメータの値が警告しきい値を超えると本トラップは送信されます。 関連トラップ： 1. swDdmPort 2. swDdmThresholdType 3. swDdmThresholdExceedType 4. swDdmThresholdExceedOrRecover | |
| MAC 通知 | swL2macNotification /1.3.6.1.4.1.171.11.118.X.2.100.1.2.0.1 (X: モデル番号) | 本トラップはアドレステーブル内のの MAC アドレスの変化を示します。 関連オブジェクト： (1)swL2macNotifyInfo | |
| DoS 攻撃防 御 | swDoSAttackDetected /1.3.6.1.4.1.171.12.59.4.0.1 | 指定の DoS パケットを受信しトラップが有効な時に、本トラップは送信されます。 関連トラップ： 1. swDoSCtrlType 2. swDoSNotifyVarIpAddr 3. swDoSNotifyVarPortNumber | |
| SNMP | authenticationFailure 1.3.6.1.6.3.1.1.5.5 | authenticationFailure トラップは、SNMP エンティティが適切に認証されていないプロトコルメッセージを受信したことを示します。SNMP エンティティのすべてのインプリメンテーションがこのトラップを生成可能な場合、snmpEnableAuthenTraps オブジェクトは、このトラップが生成されるかどうかを示します。 | |

付録 E パケットコンテンツ ACL を使用した ARP スプーフィング攻撃の軽減

ARP を動作させる方法

ARP (Address Resolution Protocol) は、IP アドレスだけがわかっている場合にホストのハードウェアアドレス (MAC アドレス) を検索するための標準的な方法です。しかし、クラッカーが ARP パケット内の IP および MAC 情報を偽造して LAN への攻撃 (ARP スプーフィングとして、知られている) を行うために、このプロトコルは被害を受けやすいと言えます。ここでは ARP プロトコル、ARP スプーフィング攻撃、および D-Link スイッチが提供する ARP スプーフィング攻撃を防御する対策について紹介します。

ARP 処理中に、PC-A は、はじめに、PC-B の MAC アドレスを問い合わせる ARP リクエストを発行します。そのネットワーク構造は図 D-1 の通りです。

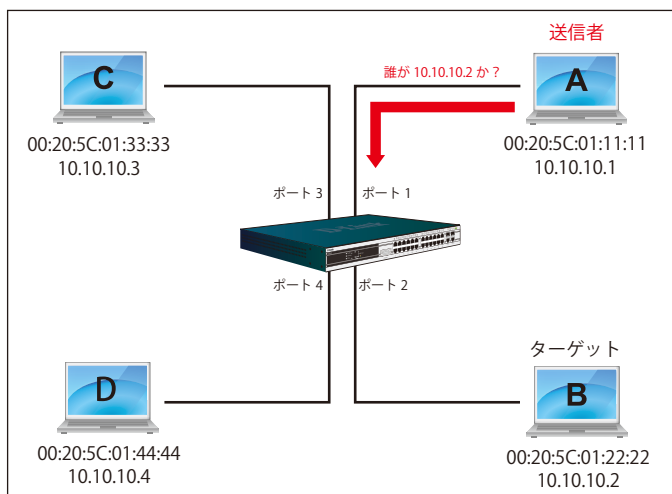


図 E-1 ARP の動作方法

その間、PC-A の MAC アドレスは「送信側 H/W アドレス」に書かれ、その IP アドレスは ARP ペイロードの「送信側プロトコルアドレス」に書かれます。PC-B の MAC アドレスが未知である場合、「ターゲット H/W アドレス」は「00-00-00-00-00-00」であり、PC-B の IP アドレスは表 D-1 に示された「ターゲットプロトコルアドレス」に書かれます。

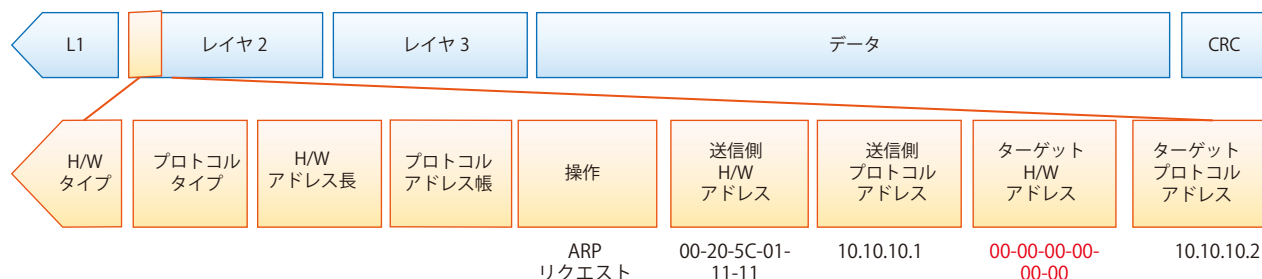


図 E-2 ARP ペイロード

ARP リクエストはイーサネットフレームにカプセル化されて送信されます。表 D-2 の通り、イーサネットフレーム内の「送信元アドレス」は、PC-A の MAC アドレスとなります。ARP リクエストは、ブロードキャスト経由で送信されるため、イーサネットのブロードキャスト (FF-FF-FF-FF-FF-FF) のフォーマットには「宛先アドレス」があります。

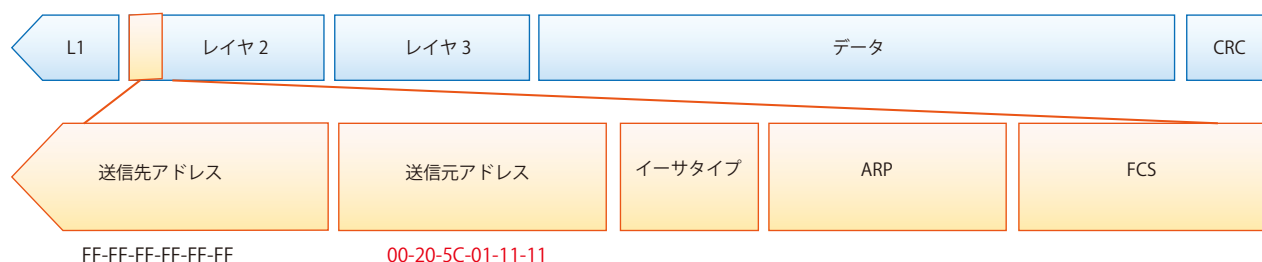


図 E-3 イーサネットフレームフォーマット

スイッチがフレームを受信すると、イーサネットフレームヘッダの「送信元アドレス」をチェックします。アドレスがフォワーディングテーブルにないと、スイッチは学習して PC-A の MAC アドレスと関連ポートをフォワーディングテーブルに追加します。

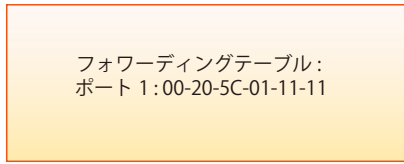


図 E-4 フォワーディングテーブル

さらに、スイッチがブロードキャストされた ARP リクエストを受信すると、送信元ポート (図 E-5 ではポート 1) を除くすべてのポートにフレームをフラッドします。

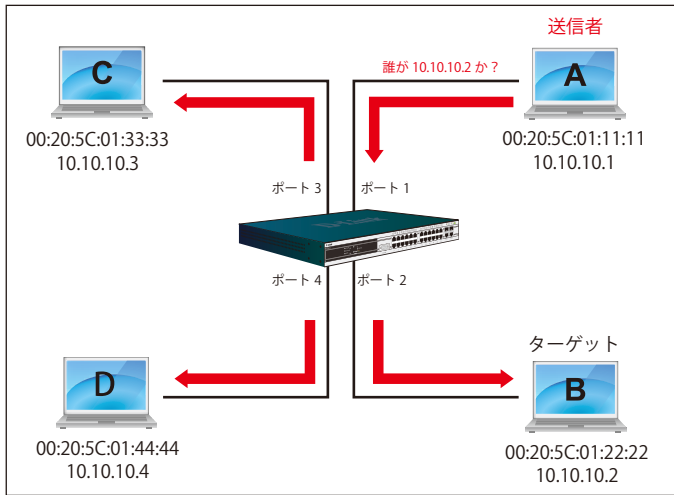


図 E-5 ポートフラッド画面

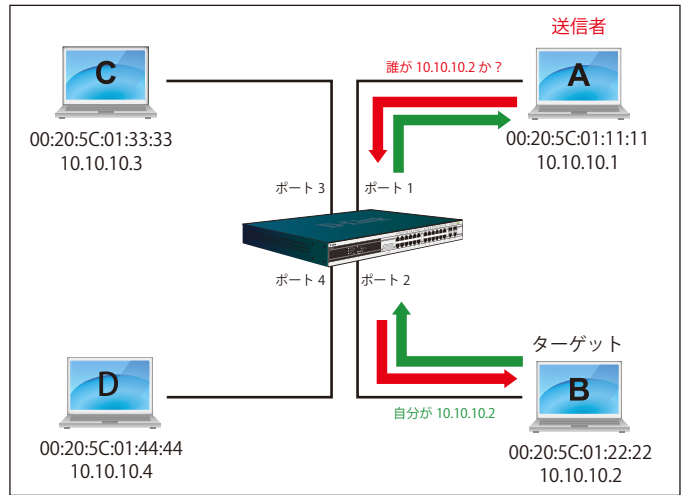


図 E-6 パケットコンテンツ ACL 画面

スイッチが ARP リクエストのフレームをネットワークにフラッドする場合、すべての PC が、フレームを受信し、検証を行います。PC-B だけが宛先 IP に一致するためにクエリに応答します (図 E-6 参照)。

PC-B が ARP リクエストに応答すると、その MAC アドレスは図 E-7 に示されている ARP ペイロード内の「ターゲット H/W アドレス」に書かれます。ARP リプライは、次に、再びイーサネットフレームにカプセル化されて、送信側に返送されます。ARP リプライはユニキャスト通信の形式です。

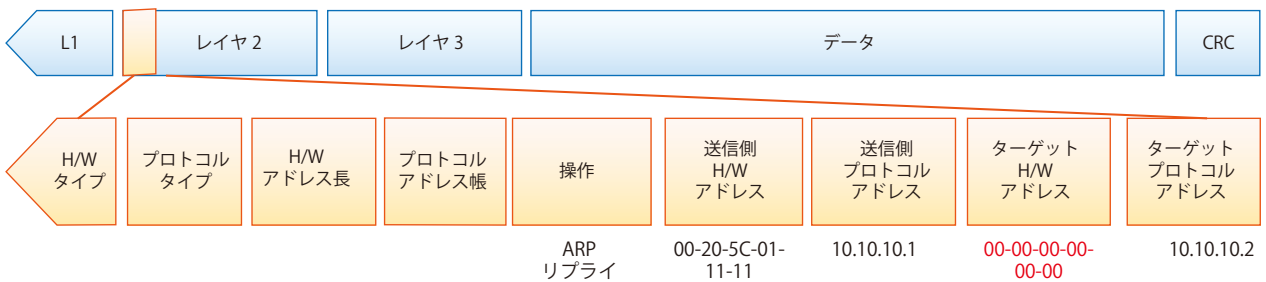


図 E-7 ARP ペイロード

PC-B がクエリに応答する場合、イーサネットフレーム内の「宛先アドレス」は、PC-A の MAC アドレスに変更されます。「送信元アドレス」は PC-B の MAC アドレスに変更されます (図 E-8 参照)。

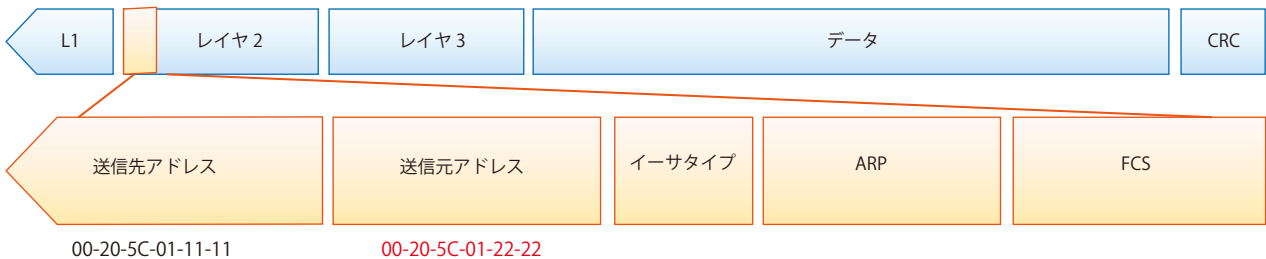


図 E-8 イーサネットフレームフォーマット

スイッチは、また、イーサネットフレームの「送信元アドレス」を調べて、フォワーディングテーブルにはアドレスがないことを見つけます。スイッチはPCのMACアドレスを学習してフォワーディングテーブルを更新します。

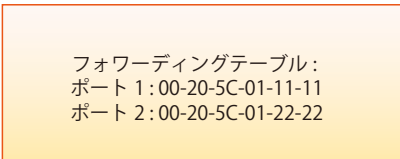


図 E-9 フォワーディングテーブル

ARP スプーフィングでネットワークを攻撃する方法

また、ARP を汚染することで知られている ARP スプーフィングは、イーサネットネットワークを攻撃する方法で、DoS (Denial of Service) として知られているように、攻撃者は LAN 上のデータフレームをかぎつけて、トラフィックを編集、またはトラフィックを停止させてしまう可能性があります。ARP スプーフィングの原則は、偽造または改ざんした ARP メッセージをイーサネットネットワークに送信することです。一般的に、目的は、デフォルトゲートウェイなどの別のノードの IP アドレスに攻撃者の MAC アドレスかでたらめの MAC アドレスを割り当ててしまうことです。その IP アドレスに向かう予定だったトラフィックが、攻撃者に指定されたノードに誤ってリダイレクトされています。

IP スプーフィング攻撃は、ホストが自身の IP アドレスを解決するため ARP リクエストを送信する場合に発生する Gratuitous ARP によって引き起こされます。図 E-10 は、LAN のハッカーによる ARP スプーフィング攻撃の開始を示しています。

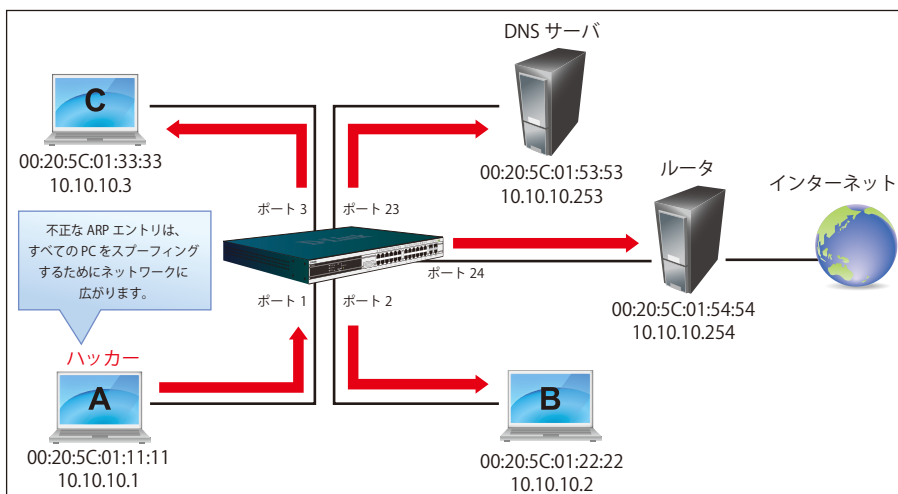


図 E-10 IP スプーフィング攻撃

Gratuitous ARP パケットでは、「送信側プロトコルアドレス」と「ターゲットプロトコルアドレス」は同じ送信元 IP アドレスとなります。「送信側 H/W アドレス」と「ターゲット H/W アドレス」は同じ送信元 MAC アドレスとなります。宛先の MAC アドレスは、イーサネットブロードキャストアドレス (FF-FF-FF-FF-FF-FF) となります。ネットワーク内のすべてのノードは、送信側の MAC アドレスおよび IP アドレスに従って、直ちに自身の ARP テーブルを更新します。Gratuitous ARP の書式は以下の表の通りです。

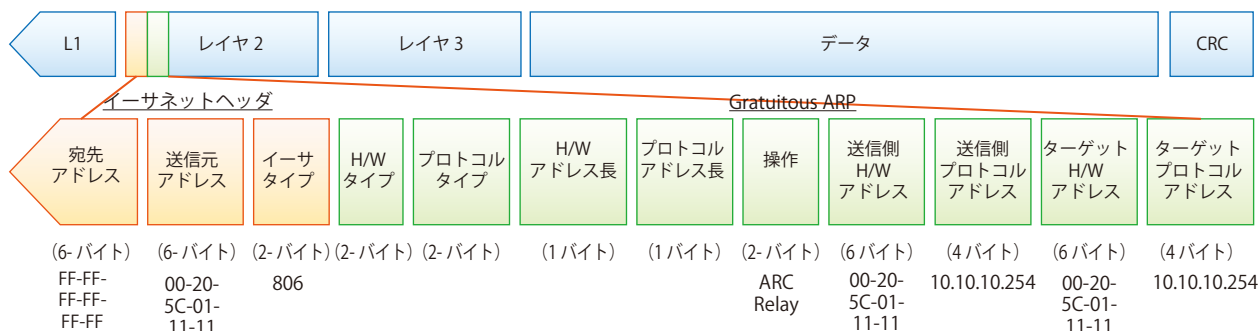


図 E-11 イーサネットフレームフォーマット

一般的な DoS 攻撃は、実在しない MAC アドレスやあらゆる指定 MAC アドレスをネットワークのデフォルトゲートウェイの IP アドレスに関連させることで行われます。悪意がある攻撃者は、一つの Gratuitous ARP をゲートウェイであると言っているネットワークに対してブロードキャストする必要があるだけであり、これによりすべてのネットワーク操作は、インターネットへの全パケットが間違ったノードに向けられるためにダウンさせられてしまいます。

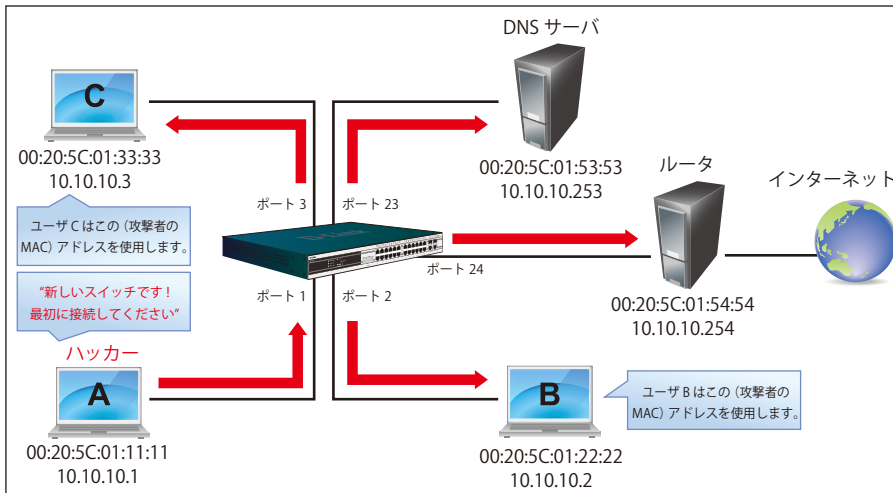


図 E-11 IP スプーフィング攻撃

同様に、攻撃者は、実際のデフォルトゲートウェイにトラフィックを転送する（パッシブスニффिंग）か、またはそれを転送する前にデータを更新する（man-in-the-middle 攻撃）を選択することが可能です。ハッカーは PC をだまし、犠牲者であるルータをだまします。図 E-11 で参照されるように、すべてのトラフィックはハッカーにスニッフingされますが、ユーザはそれを発見できません。

パケットコンテンツ ACL 経由で ARP スプーフィング攻撃を防止する

D-Link マネージドスイッチは、独自のパケットコンテンツ ACL 経由で ARP スプーフィングが引き起こした一般的な DoS を効果的に軽減することができます。基本的な ACL は、パケットタイプ、VLAN ID、送信元および送信先 MAC 情報に基づいて ARP パケットをフィルタするだけであるため、より詳細な ARP パケットの検証が必要となります。

ARP スプーフィング攻撃を防ぐために、スイッチでパケットコンテンツ ACL を使用し、偽造されたゲートウェイの MAC と IP バインディングを含む不正な ARP パケットを防御します。

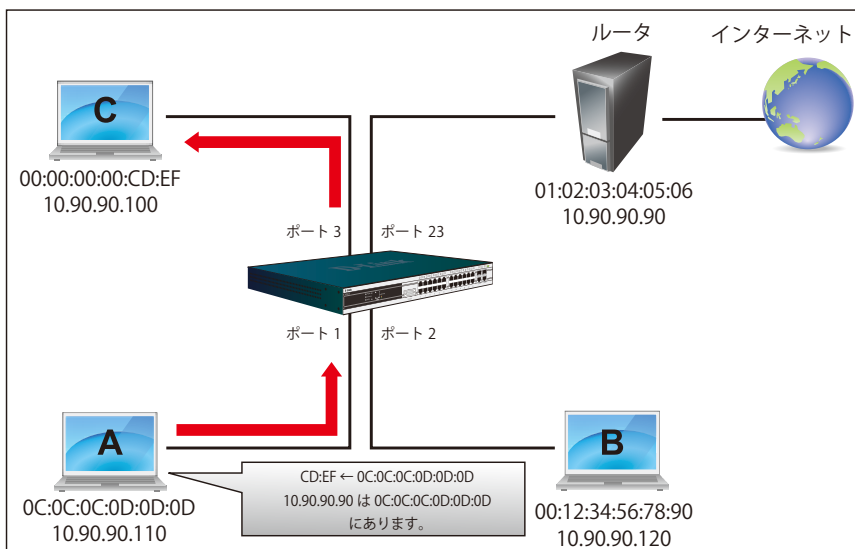


図 E-12 パケットコンテンツ ACL 経由の ARP スプーフィング防止

設定

設定のロジックは以下の通りです。

1. ARP がイーサネットにおける送信元 MAC アドレスに一致する場合にだけ、ARP プロトコルの送信者の MAC アドレスと送信者の IP アドレスはスイッチを通過することができます。(この例では、ゲートウェイの ARP です。)
2. スイッチはゲートウェイの IP アドレスから来ていると言う他のすべての ARP パケットを拒否します。

スイッチのパケットコンテンツ ACL の設計により、ユーザはどんなオフセットチャンクも検証することができます。オフセットチャンクは 16 進数形式の4バイトのブロックであり、イーサネットフレーム内の各項目に一致させるために利用されます。各プロファイルは、最大4つのオフセットチャンクを持つことができます。その上、パケットコンテンツ ACL に1個のプロファイルだけがスイッチごとサポートされます。つまり、最大 16 バイトのオフセットチャンクが各プロファイルとスイッチに適用されます。そのため、有効なオフセットチャンクの計画と設定が必要とされます。

表 E-1 で、Offset_Chunk0 が 127 バイト目から開始し、128 バイト目で終了することにご注意ください。それに、オフセットチャンクが 0 ではなく、1 から抽出されることがわかります。

表 E-1 チャンクとパケットオフセット

| Offset Chunk | Offset Chunk0 | Offset Chunk1 | Offset Chunk2 | Offset Chunk3 | Offset Chunk4 | Offset Chunk5 | Offset Chunk6 | Offset Chunk7 | Offset Chunk8 | Offset Chunk9 | Offset Chunk10 | Offset Chunk11 | Offset Chunk12 | Offset Chunk13 | Offset Chunk14 | Offset Chunk15 |
|--------------|---------------|---------------|---------------|---------------|---------------|---------------|---------------|---------------|---------------|---------------|----------------|----------------|----------------|----------------|----------------|----------------|
| バイト | 127 | 3 | 7 | 11 | 15 | 19 | 23 | 27 | 31 | 35 | 39 | 43 | 47 | 51 | 55 | 59 |
| バイト | 128 | 4 | 8 | 12 | 16 | 20 | 24 | 28 | 32 | 36 | 40 | 44 | 48 | 52 | 56 | 60 |
| バイト | 1 | 5 | 9 | 13 | 17 | 21 | 25 | 29 | 33 | 37 | 41 | 45 | 49 | 53 | 57 | 61 |
| バイト | 2 | 6 | 10 | 14 | 18 | 22 | 26 | 30 | 34 | 38 | 42 | 46 | 50 | 54 | 58 | 62 |

| Offset Chunk | Offset Chunk15 | Offset Chunk16 | Offset Chunk17 | Offset Chunk18 | Offset Chunk19 | Offset Chunk20 | Offset Chunk21 | Offset Chunk22 | Offset Chunk23 | Offset Chunk24 | Offset Chunk25 | Offset Chunk26 | Offset Chunk27 | Offset Chunk28 | Offset Chunk29 | Offset Chunk30 |
|--------------|----------------|----------------|----------------|----------------|----------------|----------------|----------------|----------------|----------------|----------------|----------------|----------------|----------------|----------------|----------------|----------------|
| バイト | 63 | 67 | 71 | 75 | 79 | 83 | 87 | 91 | 95 | 99 | 103 | 107 | 111 | 115 | 119 | 123 |
| バイト | 64 | 68 | 72 | 76 | 80 | 84 | 88 | 92 | 96 | 100 | 104 | 108 | 112 | 116 | 120 | 124 |
| バイト | 65 | 69 | 73 | 77 | 81 | 85 | 89 | 93 | 97 | 101 | 105 | 109 | 113 | 117 | 121 | 125 |
| バイト | 66 | 70 | 74 | 78 | 82 | 86 | 90 | 94 | 98 | 102 | 106 | 110 | 114 | 118 | 122 | 126 |

以下の表は、パケットオフセットの計算のためのパターンであるイーサネットフレームに含まれる完全な ARP パケットを示しています。

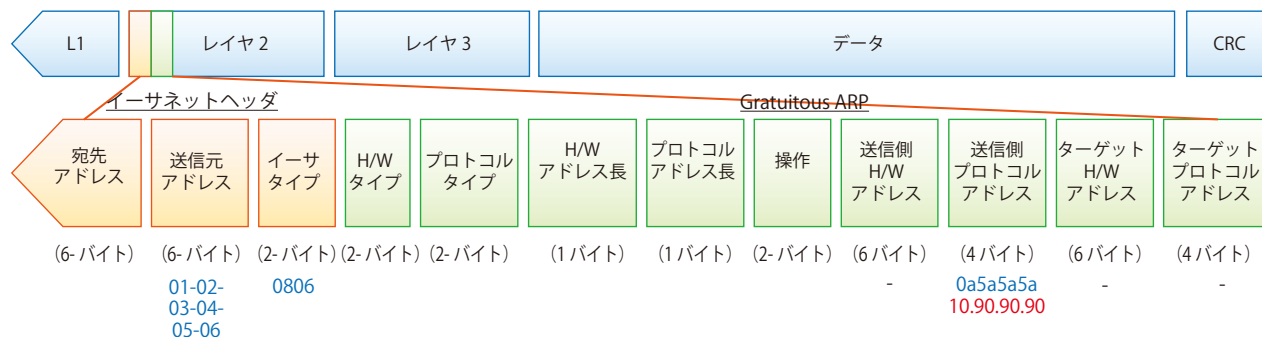


図 E-13 イーサネットフレームに含まれる完全な ARP パケット

| | コマンド | 記述 |
|------|---|--|
| 手順 1 | create access_profile profile_id 1 ethernet source_mac FF-FF-FF-FF-FF-FF ethernet_type | ・「イーサネットタイプ」と「送信元 MAC アドレス」を一致させるアクセスプロファイル 1 を作成します。 |
| 手順 2 | config access_profile profile_id 1 add access_id1 ethernet source_mac 01-02-03-04-04-06 ethernet_type 0x806 port 1-12 permit | ・アクセスプロファイル 1 を設定します。 ・ゲートウェイの ARP パケットがイーサネットフレームに正しい「送信元 MAC」を持っている場合だけスイッチを通過できます。 |
| 手順 3 | create access_profile profile_id 2 packet_content_mask offset_chunk_1 3 0x0000FFFF ↑ イーサネットタイプ (1 バイト) : ARP offset_chunk_2 7 0x0000FFFF ↑ Sdr IP (始め 2 バイト) offset_chunk_3 8 0x0000FFFF ↑ Sdr IP (最後 2 バイト) | ・アクセスプロファイル 2 を作成します。 ・2 つ目のチャンクは Chunk7 から開始します。: 「イーサネットタイプ」のマスク (表 E-1: 13/14 バイト目の青色部分) ・1 つ目のチャンクは Chunk3 から開始します。: ARP パケットの「Sender IP」(始め 2 バイト) のマスク (表 E-1: 29/30 バイト目の緑色部分) ・1 つ目のチャンクは Chunk8 から開始します。: ARP パケットの「Sender IP」(最後 2 バイト) のマスク (表 E-1: 31/32 バイト目の茶色部分) |

| | コマンド | 記述 |
|-----|---|---|
| 手順4 | <pre> config access_profile profile_id 2 add access_id 1 packet_content offset_chunk_1 0x00000806 ↑ イーサネットタイプ (1 バイト) : ARP offset_chunk_2 0x00000A5A ↑ Sdr IP (始め 2 バイト) : 10.90 offset_chunk_3 0x5A5A0000 ↑ Sdr IP (最後 2 バイト) : 90.90 port 1-12 deny </pre> | <ul style="list-style-type: none"> • アクセスプロファイル 2 を設定します。 • 「Sender IP」がゲートウェイの IP であると言う残りの ARP パケットは廃棄されます。 |
| 手順5 | <pre> save </pre> | <ul style="list-style-type: none"> • 設定を保存します。 |

付録F パスワードのリカバリ手順

ここでは、弊社スイッチのパスワードのリセットについて記述します。ネットワークにアクセスを試みるすべてのユーザに認証は必要で重要です。権限のあるユーザを受け入れるために使用する基本的な認証方法は、ローカルログイン時にユーザ名とパスワードを利用することです。時々パスワードが忘れられたり、壊れたりするため、ネットワーク管理者は、これらのパスワードをリセットする必要があります。ここでは、パスワードリカバリ機能は、そのような場合にネットワーク管理者を助けるものです。以下の手順で、容易にパスワードを回復するパスワードリカバリ機能の使用方法を説明します。

これらの手順を終了するとパスワードはリセットされます。

1. セキュリティの理由のため、パスワードリカバリ機能は物理的にデバイスにアクセスすることが必要です。そのため、デバイスのコンソールポートへの直接接続を行っている場合だけ、本機能を適用することが可能です。ユーザは端末エミュレーションソフトを使用して、スイッチのコンソールポートに端末またはPCを接続する必要があります。
2. 電源をオンにします。「UART init」が100%までロードされた後に、「Password Recovery Mode」に入るために、2秒以内に、ホットキー「^」を押します。「Password Recovery Mode」に一度入ると、スイッチのすべてのポートが無効になります。

```

Boot Procedure                                     V1.00.006
-----
Power On Self Test ..... 100%

MAC Address   : FC-75-16-3B-9C-00
H/W Version   : A1

Please Wait, Loading V1.00.024 Runtime Image ..... 100 %
UART init ..... 100 %
    
```

```

Password Recovery Mode
>
    
```

3. 「Password Recovery Mode」では、以下のコマンドのみ使用できます。

| コマンド | 説明 |
|----------------------------|---|
| reset config {force_agree} | リセットし、全設定を工場出荷時設定に戻します。オプション「force_agree」は、ユーザの同意なしで全コンフィグレーションをリセットすることを意味します。 |
| reboot {force_agree} | 「Password Recovery Mode」を終了し、スイッチを再起動します。現在の設定を保存するように確認メッセージが表示されます。オプション「force_agree」は、ユーザの同意なしで全コンフィグレーションをリセットすることを意味します。 |
| reset account | 作成済みのアカウントのすべてを削除します。 |
| reset password {< ユーザ名 >} | 指定ユーザのパスワードをリセットします。ユーザ名を指定しないと、すべてのユーザのパスワードがリセットされます。 |
| show account | 設定済みのすべてのアカウントを表示します。 |

付録 G 用語解説

| 用語 | 説明 |
|---|---|
| 1000BASE-LX | 最大伝送速度 1Gbps の Gigabit Ethernet の規格のひとつ。長い光波長で長距離伝送用に使用されます。伝送距離 (最大) はシングルモード光ファイバを使用した場合で 10km。 |
| 1000BASE-SX | 最大伝送速度 1Gbps の Gigabit Ethernet の規格のひとつ。短い光波長でマルチモード光ファイバを使用した場合伝送距離 (最大) は 550km。 |
| 100BASE-FX | 光ファイバを使用する最大伝送速度 100Mbps の Fast Ethernet の規格のひとつ。 |
| 100BASE-TX | カテゴリ 5 以上の UTP ケーブルを使用する最大伝送速度 100Mbps の Fast Ethernet の規格のひとつ。 |
| 10BASE-T | IEEE 802.3 準拠でカテゴリ 3 以上の UTP ケーブルを使用する最大伝送速度 10Mbps の Ethernet の規格のひとつ。 |
| エージング | タイムアウトし、無効のスイッチのダイナミックデータベースを自動的に消去します。 |
| ATM | 非同期転送モード。セルと呼ばれる固定長のセル(パケット)ベースで転送するプロトコル。ATM は音声、データおよびビデオ信号を含むユーザトラフィックの完全な列を転送するために開発されたものです。 |
| オートネゴシエーション | スピード、デュプレックスおよびフローコントロールを自動的に認識する機能。オートネゴシエーションをサポートする端末と接続すると、リンクは自動的に最適なリンク条件に設定されます。 |
| バックボーンポート | デバイスのアドレスを学習せず不明なアドレスを持つすべてのフレームを受信するポート。バックボーンポートは通常で使用するネットワークのバックボーンにスイッチを接続するために使用されるポートです。バックボーンポートは以前はダウンリンクポートとして知られていました。 |
| バックボーン帯域 | ネットワークセグメント間でトラフィックが転送される場合に優先パスとして使用されるネットワークの一部。1秒あたりのビット数で計算される1チャンネルが転送できる情報量。イーサネットの帯域は 10Mbps、ファーストイーサネットは 100Mbps。 |
| ボーレート | ラインのスイッチングスピード。ネットワークセグメント間のラインスピードとして知られています。 |
| BOOTP | BOOTP プロトコルはデバイスが起動するたびに IP アドレスを MAC アドレスに自動マッピングします。さらにデバイスにサブネットマスク、デフォルトゲートウェイを割り当てます。 |
| ブリッジ | たとえ高いレベルのプロトコルが関連してもローカルまたはリモートネットワークを相互接続するデバイス。ブリッジはネットワーク管理を中央に集めて 1 個の論理ネットワークを形成します。 |
| ブロードキャスト | ネットワーク上のすべての終点デバイスに送信されるメッセージ。 |
| ブロードキャストストーム | が主として可能なネットワーク帯域を奪い、ネットワークエラーを引き起こす Multiple simultaneous ブロードキャスト。 |
| コンソールポート | 端末またはモデムコネクタと接続可能なスイッチ上のポート。コンピュータ内でパラレル配列のデータをデータ転送リンクで使用されるシリアル形式に変換します。このポートはほとんどの場合ローカル管理のために使用されます。 |
| CSMA/CD | イーサネットと IEEE 802.3 標準によって使用されるチャンネルアクセス方法で検索したデータチャンネルが一定期間後クリアされた後にだけデバイスに転送します。2つのデバイスが同時に転送する場合、コリジョンが発生し、コリジョンが発生したデバイスは任意の時間再転送を遅らせます。 |
| データセンタースイッチング | スイッチがサーバファームへの高パフォーマンスアクセス、高速バックボーン接続、およびネットワーク管理とセキュリティのためのコントロールポイントを提供するコアレートネットワーク内のアグリゲーションポイント |
| イーサネット | Xerox、Intel および DEC が共同で開発した LAN 仕様。イーサネットネットワークは CSMA/CD を使用して 10Mbps で処理を行います。 |
| ファーストイーサネット | Ethernet/CD ネットワークアクセス方法をベースにした 100Mbps 技術。 |
| フローコントロール | (IEEE 802.3z) 端末に接続した転送ポートへのパケットを抑止します。受信バッファがあふれそうになった場合にパケットロスを防ぎます。 |
| フォワーディング | 中間のネットワークデバイスによりパケットを到達点に向けて送信するプロセス。 |
| フルデュプレックス | 同時にパケットの送受信を可能とし、スループットを 2 倍にするシステム。 |
| ハーフデュプレックス | パケットの送受信を行うが、同時には行えないシステム。 |
| IP アドレス | Internet Protocol アドレス。TCP/IP を使用するネットワークに付属するデバイスの固有な識別子。IPv4 アドレスは 8 ビットずつピリオドで区切られ、ネットワークセクション、サブネットセクション、ホストセクションで構成されます。 |
| IPX (Internetwork Packet Exchange) | ネットワーク通信で使用するプロトコル。 |
| LAN - ローカルエリアネットワーク | 通常フロアもしくはビルのような規模の小さいエリアで PC、プリンタ、サーバのようなコンピュータリソースを接続するネットワーク。高速で低エラー率が特長です。 |
| レイテンシ | デバイスがパケットを受信する時間とパケットが到達点ポートに転送される時間の遅延。 |
| ラインスピード | ボーレートを参照。 |
| メインポート | 通常の操作条件でデータトラフィックを送信する Resilient リンク内のポート。 |
| MDI (Medium Dependent Interface) | 1つのデバイスの送信装置が別のデバイスの受信装置に接続するイーサネットポート接続。 |
| MDI-X (Medium Dependent Interface Cross-over) | 接続送受信のラインが交差しているイーサネットポート接続。 |
| MIB (Management Information Base) | デバイスの管理特性とパラメータを保持します。MIB は SNMP で使用され、管理システムの属性を持っています。スイッチは自身の内部 MIB を持っています。 |
| マルチキャスト | シングルパケットはネットワークアドレスの特定のサブセットにコピーします。これらのアドレスはパケットの到達点アドレス内に記述されます。 |
| プロトコル | ネットワーク上のデバイス間通信のルール。ルールは形式、タイミング、配列およびエラー制御を定義しています。 |
| Resilient link | 他のポートがエラーになった場合に一方のポートがデータ転送を引き継ぐように設定された 1 対のポート。 |
| RJ-45 | 10BASE-T や 100BASE-TX などで使用される標準 8 線コネクタ |
| RMON | リモート監視。SNMP MIB II のサブセットはアドレッシングによって異なる最大 10 個のグループまでのモニタリングや管理を可能にします。 |

| 用語 | 説明 |
|---|--|
| RPS (リダンダント電源システム) | スイッチに接続されて、バックアップ電源を供給するデバイス。 |
| サーバファーム | 大量のユーザにサービスを提供する中央に位置するサーバグループ。 |
| SLIP (Serial Line Internet Protocol) | IP がシリアルライン接続を経由して動作することが可能なプロトコル。 |
| SNMP (Simple Network Management Protocol) | 当初は TCP/IP インターネットを管理するために開発されたプロトコル。SNMP は現在広範囲のコンピュータとネットワークの装置で実行され、多くのネットワークおよび端末操作の状況を管理するために使用されます。 |
| スパニングツリープロトコル (STP) | ネットワーク上のフォールトトレランスを提供するブリッジベースのシステム。STP はネットワークトラフィックに対してパラレルパスを実行し、メインのパスにエラーが発生してもメインのパスが操作できる場合はリダンダントパスを無効にすることを保証します。 |
| スタック | 1 個の論理的なデバイスの形をとするために統合されたネットワークデバイスのグループ。 |
| スタンバイポート | リンクしているメインポートにエラーが発生すると、Resilient リンク内のスタンバイポートはデータ転送を受け継ぎます。 |
| スイッチ | パケットの終点アドレスを元にパケットのフィルタ、フォワードするデバイス。スイッチは各スイッチポートで関連するアドレスを学習し、この情報を元に表を作成してスイッチの決定に使用します。 |
| TCP/IP | Telnet 端末エミュレーション、FTP ファイル転送などコンピュータ装置の広い範囲で通信サービスを提供する通信プロトコルです。 |
| telnet | 仮想端末サービスを提供する TCP/IP アプリケーションプロトコルで、ユーザが別のコンピュータシステムにログインし、ユーザが直接ホストに接続しているようにホストにアクセスすることができます。 |
| TFTP (Trivial File Transfer Protocol) | スイッチのローカルの管理能力を使用してリモートデバイスからファイルを転送する (ソフトウェアアップグレードなど) ことができます。 |
| UDP (User Datagram Protocol) | インターネットの標準プロトコルで、あるデバイスのアプリケーションプログラムがデータを別のデバイス上のアプリケーションプログラムに送信することができます。 |
| VLAN (Virtual LAN) | 物理的に接続した LAN のように通信する位置やトポロジが独立しているデバイスのグループ。 |
| VLT (Virtual LAN Trunk) | 各スイッチ上のすべての VLAN トラフィックを転送するスイッチ間のリンク。 |
| VT100 | ASCII コードを使用するターミナルタイプ。VT100 画面はテキストベースの表示をします。 |