ES0152/ES0152P

日本語版ユーザーマニュアル

本ドキュメントについて

本書は ATEN ジャパン株式会社において、ES0152/ES0152P 取り扱いの便宜を図るため、英語版ユーザーマニュアルをローカライズしたドキュメントです。

製品情報、仕様はソフトウェア・ハードウェアを含め、予告無く改変されることがあり、本日本語版ユーザーマニュアルの内容は、必ずしも最新の内容でない場合があります。また製品の不要輻射仕様、各種安全規格、含有物質についての表示も便宜的に翻訳して記載していますが、本書はその内容について保証するものではありません。

製品をお使いになるときは、英語版ユーザーマニュアルにも目を通し、その取扱方法に従い、正しく運用を行ってください。詳細な製品仕様については英語版ユーザーマニュアルの他、製品をお買い上げになった販売店または弊社テクニカルサポート窓口までお問い合わせください。

ATEN ジャパン株式会社
技術部
TEL :03-5615-5811
MAIL :support@atenjapan.jp

2019 年 9 月 12 日

ユーザーの皆様へ

本マニュアルに記載された全ての情報、ドキュメンテーション、および製品仕様は、製造元である ATEN International により、予告無く改変されることがあります。製造元 ATEN International は、製品および本ドキュメントに関して、品質・機能・商品性および特定の目的に対する適合性について、法定上の、明示的または黙示的であるかを問わず、いかなる保証もいたしません。

弊社製品は一般的なコンピューターのメインフレームおよびインターフェースの操作・運用・管理を目的として設計・製造されております。高度な動作信頼性と安全性が求められる用途、例えば軍事使用、大規模輸送システムや交通インフラの制御、原子力発電所、セキュリティシステム、放送システム、医療システム等における可用性への要求を必ずしも満たすものではございません。

キーボード、マウス、モニター、コンピューター等、弊社製品に接続されるクライアントデバイスは、それぞれベンダーの独自技術によって開発・ 製造されております。そのため、これらの異なるデバイスを接続した結果、予期できない機器同士の相性問題が発生する可能性があります。 また、機器の併用により、それぞれオリジナルで持つ機能を全て発揮できない可能性があります。異なる環境・異なる機器の組み合わせにより、機能面での使用制限が必要になる可能性があります。

本製品および付属のソフトウェア、ドキュメントの使用によって発生した装置の破損・データの損失等の損害に関して、直接的・間接的・特殊な事例・付帯的または必然的であるかを問わず、弊社の損害賠償責任は本製品の代金相当額を超えないものとします。

製品をお使いになる際には、製品仕様に沿った適切な環境、特に電源仕様についてはご注意のうえ、正しくお使いください。

ATEN ジャパン製品保証規定

弊社の規定する標準製品保証は、定められた期間内に発生した製品の不具合に対して、すべてを無条件で保証するものではありません。製品保証を受けるためには、この『製品保証規定』およびユーザーマニュアルをお読みになり、記載された使用法および使用上の各種注意をお守りください。

また製品保証期間内であっても、次に挙げる例に該当する場合は製品保証の適用外となり、有償による修理対応といたしますのでご留意ください。

◆使用上の誤りによるもの
◆ 製品ご購入後の輸送中に発生した事故等によるもの
◆ ユーザーの手による修理または故意の改造が加えられたもの
◆ 購入日の証明ができず、製品に貼付されている銘板のシリアルナンバーも確認できないもの
◆ 車両、船舶、鉄道、航空機などに搭載されたもの
◆ 火災、地震、水害、落雷、その他天変地異、公害、戦争、テロリズム等の予期しない災害によって故障、破損したもの
◆ 日本国外で使用されたもの
◆ 日本国外で購入されたもの

【製品保証手順】

弊社の製品保証規定に従いユーザーが保証を申請する場合は、大変お手数ですが、以下の手順に従って弊社宛に連絡を行ってください。

(1)不具合の確認

製品に不具合の疑いが発見された場合は、購入した販売店または弊社サポート窓口に連絡の上、製品の状態を確認してください。 この際、不具合の確認のため動作検証のご協力をお願いすることがあります。

(2)本規定に基づく製品保証のご依頼

(1)に従い確認した結果、製品に不具合が認められた場合は、本規定に基づき製品保証対応を行います。製品保証対応のご依頼をされる場合は、RMA 申請フォームの必要項目にご記入の上、『お客様の製品購入日が証明できる書類』を用意して、購入した販売店までご連絡ください。販売店が不明な場合は、弊社までお問い合わせください。

(3)製品の発送

不具合製品の発送は宅配便などの送付状の控えが残る方法で送付してください。

【製品保証期間】

製品保証期間は通常製品/液晶ディスプレイ搭載製品で異なります。詳細は下記をご覧ください。

①通常製品	製品納品日～30 日	初期不良、新品交換※1
	31 日～3 年間	無償修理
	3 年以上	有償修理※2
②型番 CL からはじまる LCD 搭載製品のみ	製品納品日～30 日	初期不良、新品交換※1
	31 日～2 年間	無償修理
	3 年目以降	有償修理※2

※1…製品購入日から30 日以内に確認された不具合は初期不良とし、新品交換を行います。初期不良の場合の送料は往復弊社にて負担いたします。

※2…有償修理の金額は別途製品を購入された販売店までお問い合わせください。

※ケーブル類、その他レールキット等のアクセサリ類は初期不良の際の新品交換のみ、承ります。

※EOL (生産終了)が確定した製品については、初期不良であっても無償修理対応とさせていただきます。また EOL 製品の修理に関して、上記無償修理期間中であっても、部材調達の都合等により修理不可になる可能性がございます。そのような場合には、機能同等品による良品交換のご対応となる可能性がございます。また、EOL 製品の型番や、修理可否、後継機種については、随時情報更新を行っておりますので、弊社 Web ページにて最新情報をご確認ください。

※製品保証期間の延長や故障時の代替品などの保証オプションについては、弊社 Web ページをご確認ください。

【補足】

・本規定は ATEN 製品に限り適用します。

・ケーブル類は初期不良対応に準じます。

・初期不良による新品交換の場合は、ATEN より発送した代替品の到着後、5 営業日以内に不具合品を弊社宛に返却してください。返却の予定期日が守られない場合は弊社から督促を行いますが、それにも係わらず不具合品が返却されない場合は、代替機相当代金を販売代理店経由でご請求いたします。

・ラベルの汚損や剥がれなどにより製品のシリアルナンバーが確認できない場合は、すべて有償修理とさせていただきます。

【免責事項】

1. 弊社製品は映像関連システムやコンピューターのメインフレームおよびインターフェースの操作・運用・管理を目的として設計・製造されております。しかし、使用環境等によってはその機能が制限されることがあります。弊社では、ご購入前に弊社製品をお試しいただける「評価機貸出サービス」を、無償でご提供しております。評価機貸出サービスに関するお問い合わせは、弊社代理店または弊社 Web サイト（https://www.aten.com/jp/ja/）内の「お問い合わせ」フォームをご利用ください。

2. キーボード、マウス、モニター、コンピューター等、弊社製品に接続されるクライアントデバイスは、それぞれベンダーの独自技術によって開発・製造されております。そのため、これらの異なるデバイスを接続した結果、予期できない機器同士の相性問題が発生する可能性があります。また、機器の併用により、それぞれオリジナルで持つ機能を全て発揮できない可能性があります。異なる環境・異なる機器の組み合わせにより、機能面での使用制限が必要になる可能性があります。

3. 他社製品のKVMスイッチ、キーボード・マウスコンバーター、キーボード・マウスエミュレーター、KVM エクステンダー等との組み合わせはサポート対象外となりますが、お客様で自己検証の上であれば、使用を制限するものではありません。

4. 製品に対しての保証は、日本国内で使用されている場合のみ対象とさせて頂きます。

5. 製品やサービスについてご不明な点がある場合は、弊社技術部門までお問い合わせください。

製品についてのお問い合わせ

製品の仕様や使い方についてのお問い合わせは、下記窓口または製品をお買い上げになった販売店までご連絡ください。

購入前のお問い合わせ	ATEN ジャパン株式会社　営業部 TEL：03-5615-5810 MAIL:sales@atenjapan.jp
購入後のお問い合わせ	ATEN ジャパン株式会社　技術部 TEL　：03-5615-5811 MAIL :support@atenjapan.jp

目次

EMC に関する情報

FCC（連邦通信委員会）電波干渉声明

本製品は、FCC（米国連邦通信委員会）規則の Part15 に準拠したデジタル装置 Class A の制限事項を満たして設計され、検査されています。この制限事項は、商業目的の使用において、有害な障害が発生しないよう、基準に沿った保護を提供する為のものです。この操作マニュアルに従わずに使用した場合、本製品から発生するラジオ周波数により、他の通信機器に影響を与える可能性があります。また、本製品を一般住宅地域で使用した場合、有害な電波障害を引き起こす可能性もあります。その際には、ユーザーご自身の負担で、その障害を取り除いてください。

本製品は、FCC（米国連邦通信委員会）規則の Part15 に準拠しています。動作は次の 2 つの条件を前提としています。(1)このデバイスが有害な干渉を引き起こさないこと、(2)このデバイスが、予想外の動作を引き起こす可能性のある干渉を含め、すべての干渉を受け入れなければならないこと。

FCC による注意：本コンプライアンスに対する責任者による明確な承認を得ていない変更または改良を行った場合は、ユーザーの本装置を操作する権利を無効とします。

注意：本製品をご家庭で使用した場合、電波干渉を引き起こす可能性があります。

推奨：FCC および CE 規格を確実に順守するために、STP ケーブルを使用するようにしてください。

RoHS

本製品は『電気・電子機器に含まれる特定有害物質の使用制限に関する欧州議会及び理事会指令』、通称 RoHS 指令に準拠しております。

安全にお使い頂くために

全般

- ◆ 本製品は、屋内での使用に限ります。
- ◆ 製品に同梱されるドキュメントは全てお読みください。またドキュメント類は全て保存してください。また、弊社 Web サイトに掲載のオンラインユーザーマニュアルもご確認ください。
- ◆ 製品に関する注意・説明に従って取り扱ってください。
- ◆ 落下による事故・製品の破損を防ぐため、設置場所は不安定な面（台車、簡易的なスタンドやテーブル等）を避けるようにしてください。
- ◆ 製品が水に濡れるおそれのあるような場所で使用しないでください。
- ◆ 製品は熱源の近く、またはその熱源の上などで使用しないでください。
- ◆ 製品のケースには必要に応じて通気口が設けられています。通気口のある製品は、安定した運用を行うため、また製品の過熱を防ぐために、開口部を塞いだり覆ったりしないでください。
- ◆ 製品をベッドやソファ、ラグなどの柔らかいものの上に置かないでください。開口部が塞がれ、適切な通気が確保できずに製品が過熱するおそれがあります。
- ◆ 製品にいかなる液体もかからないようにしてください。
- ◆ 電源プラグを電源コンセントから抜く場合は、乾いた雑巾でプラグ周りのホコリを掃除してください。液体やスプレー式のクリーナーは使用しないでください。
- ◆ 製品はラベルに記載されたタイプの電源に接続して運用してください。電源タイプについて不明な場合は、購入された販売店もしくは電気事業者にお問い合わせください。
- ◆ 電気回路が過負荷状態に陥らないようにしてください。電気機器を回路に接続する前に、電源の上限を把握しておき、これを超えないように注意してください。回路の電気仕様を常に見直して、危険な条件を生じさせていないかどうか、また、すでに危険な条件がそろっていないかどうかを確認してください。電気回路の過負荷は火災や機器破損の原因となります。
- ◆ お使いの装置への損傷を避けるためにも、すべての装置を適切に接地するようにしてください。
- ◆ 製品付属の電源ケーブルは安全のために 3 ピンタイプのプラグを使用しています。電源コンセントの形状が異なりプラグを接続できない場合には電気事業者に問い合わせて適切に処置してください。アース極を無理に使用できない状態にしないでください。使用される国/地域の電源形状に従ってください。
- ◆ 電源コンセントの形状が異なり、製品付属の電源アダプターを接続できない場合には電気事業者に問い合わせて適切に処置してください。アース極を無理に使用できない状態にしないでください。使用される国/地域の電源形状に従ってください。
- ◆ 電源コードやケーブルの上に物を置かないでください。人が通行するような場所を避けて電源

コードを設置してください。

- ◆ 電源の延長コードや電源タップを使用する場合は、合計容量とコードまたはタップの仕様が適合していることを確認してください。電源コンセントにつながれている製品全ての合計アンペア数は 15 アンペアを超えないようにしてください。
- ◆ 突然の供給電力不安定や電力過剰・電力不足からお使いのシステムを守るために、サージサプレッサー、ラインコンディショナー、または無停電電源装置(UPS)をご使用ください。
- ◆ システムケーブルや電源ケーブルは丁寧に取り扱ってください。これらのケーブル類の上には何も置かないようにしてください。
- ◆ ホットプラグ対応パワーサプライの取り付け、または取り外しする場合は、以下の注意事項に従ってください。
  - ➢ 電源ケーブルを接続する前に、パワーサプライのセットアップを行ってください。
  - ➢ パワーサプライを取り外す前に電源ケーブルを抜いてください。
  - ➢ お使いのシステムが複数のパワーサプライをお使いである場合、パワーサプライからすべての電源ケーブルを抜いてお使いのシステムから切り離してください。
- ◆ 危険な電源ポイントへの接触やショートによって、発火したり感電したりするおそれがありますので、キャビネットの空きスロット等に押し込まないようにしてください。
- ◆ 装置をご自身で修理せず、ご不明な点がございましたら技術サポートまでご相談ください。
- ◆ 下記の現象が発生した場合、コンセントからはずして技術サポートに修理を依頼してください。
  - ➢ 電源コードが破損した。
  - ➢ 装置の上に液体をこぼした。
  - ➢ 装置が雨や水にぬれた。
  - ➢ 装置を誤って落下させた、ないしはキャビネットが破損した。
  - ➢ 装置の動作に異変が見られる。(修理が必要です)
  - ➢ 製品マニュアルに従って操作しているにもかかわらず、正常に動作しない。
- ◆ 修理が必要となる故障が発生するおそれがありますので、製品マニュアルに従って操作してください。
- ◆ 「UPGRADE」と書かれた RJ-11 コネクターを公衆通信網に接続しないようにしてください。
- ◆ 本製品をスタッキングする場合、ラックにロックする場合、フレームにネジ止めする場合やその他類似の方法で設置を行う場合には、製品を確実に固定するための安全装置が追加で必要になることがあります。
- ◆ 本製品は固定させて使用するように設計されているため、通常の動作中には動かさないようにしてください。
- ◆ Cat 5e/6 ケーブルは、電気ケーブル、変圧器、照明器具といった電波障害の発生源となりうる物から、できるだけ遠ざけて配線するようにしてください。また、これらのケーブルは、電線用導管に接続したり、電灯設備の上に置いたりしないようにしてください。
- ◆ 取り付ける SFP モジュールは、次の条件を満たす必要があります。

- クラス 1 レーザー製品（IEC/EN60825-1 に準拠）
- 21 CFR1040.10 および 1040.11（2007 年 6 月 24 日付けレーザー通知 No.50 による逸脱を除く）

ラックマウント

- ラックでの作業を始める前に、スタビライザーがラックに固定され床に接していること、また、ラック全体が安定した場所に置かれていることを確認してください。作業する前に、シングルラックにフロントとサイドのスタビライザーを取り付けるか、結合された複数のラックにフロントスタビライザーを取り付けてください。
- ラックには下から上に向かって、一番重いアイテムから順番に取り付けてください。
- デバイスを拡張する前にラックが水平で安定していることを確認してください。
- ラックに供給する AC 電源の分岐回路が過剰供給にならないようご注意ください。ラック全体の電源負荷は分岐回路の 80%を越えないように設定する必要があります。
- ラックにマウントされたデバイスは、電源タップも含め、すべて正しく接地されていることを確認してください。
- ラックへの通気を十分に確保してください。
- 本製品で定められている保管温度を超えないように、ラックが設置されている場所の室温を調節してください。
- ラックに設置されているデバイスが動作している際に、デバイスを踏んだりデバイスによじ登ったりしないでください。
- **注意：**ラックにマウントされた LCD KVM ドロワーを棚や作業スペースとして使用しないでください。

同梱品

ES0152/ES0152P 製品パッケージには下記のアイテムが同梱されています。

ES0152

- ES0152 52 ポート GbE マネージドスイッチ ×1
- AC 電源ケーブル ×1
- RJ-45→DB-9 シリアルコンソールケーブル ×1
- ラックマウントキット ×1
- フットパッドセット(4pcs) ×1
- クイックスタートガイド* ×1

ES0152P

- ES0152P 52 ポート GbE マネージドスイッチ(PoE 対応) ×1
- AC 電源ケーブル ×1
- RJ-45→DB-9 シリアルコンソールケーブル ×1
- ラックマウントキット ×1
- フットパッドセット(4pcs) ×1
- クイックスタートガイド* ×1

上記のアイテムがそろっているかご確認ください。万が一、欠品または破損品があった場合はお買い上げになった販売店までご連絡ください。

本ユーザーマニュアルをよくお読みいただき、正しい使用法により、本製品および接続する機器を安全にお使いください。

*	本マニュアルの公開後に、製品仕様が追加される場合があります。最新版は弊社 Web サイトにアクセスしてご確認ください。

本マニュアルについて

このユーザーマニュアルでは、Web インターフェースを使用してスイッチを操作する方法について説明します。

概要

第 1 章　はじめに ： 52 ポート GbE マネージドスイッチについて説明します。製品の目的、機能、メリット、フロントパネルとリアパネルの各部名称、および Web インターフェースへのアクセス方法について説明します。

第 2 章　セットアップ：スイッチを設定するための手順について説明します。

第 3 章から第 17 章では、Web インターフェースのサイドメニューと、それに対応する設定/操作について説明します。

第 18 章　デバイス管理システム(DMS) ：DMS インテリジェント管理ツールと、スイッチの管理に役立つ情報について説明します。

付録　　技術的およびトラブルシューティングに関する情報が記載されています。

マニュアル表記について

[　　]	入力するキーを示します。例えば[Enter]はエンターキーを押します。複数のキーを同時に押す場合は、[Ctrl] + [Alt]のように表記してあります。
1.	番号が付けられている場合は、番号に従って操作を行ってください。
◆	◆印は情報を示しますが、作業の手順を意味するものではありません。
→	矢印は操作の手順を示します。例えばStart → Runはスタートメニューを開き、Runを選択することを意味します。
	重要な情報を示しています。

※本マニュアルに記載されている商品名・会社名等は、各社の商標ならびに登録商標です。

第 1 章
はじめに

概要

ES0152/ES0152P は、ATEN 製 IP-KVM エクステンダー（KE シリーズ）および Video over IP エクステンダー（VE89 シリーズ※1）に理想的なマネージドスイッチです。ユーザーは KE/VE89 シリーズとの併用に最適な ES0152/ES0152P を使うことで複雑なセットアップの手間を解消できるので、OT インフラを簡単に構築することができます。

ES0152/ES0152P のセットアップは簡単で時間もかかりません。接続はすべてプラグアンドプレイで行えますので、ソフトウェアのインストールやデバイスの設定は不要です。KE/VE89 シリーズのトランスミッターとレシーバーを Cat 5e/6 ケーブルで ES0152/ES0152P に接続するだけで、同一 LAN 上にあるすべての KE/VE89 シリーズのデバイスが自動的に検出されます。

ES0152/ES0152P ネットワークスイッチは、52 ポートを搭載し、L2 機能および L3 スタティックルーティングを含む高度な機能、そして、DHCP サーバー、IPv6 対応、LLDP といった高性能な設定機能を備えており、ネットワーク性能の改善に役立つ様々なソリューションを提供します。

ES0152/ES0152P は、幅広いネットワーク要件に対応できるよう、SFP+（ファイバー）と RJ-45（銅線）の両方のポートを備えています。ES0152 では、SFP+は 4 ポート（1G/10G）、また、RJ-45 は 48 ポート（10M/100M/1G）を、それぞれ搭載しています。一方、ES0152P では、SFP+は 4 ポート（1G/10G）、また、PoE 機能対応（802.3at/af をサポート）RJ-45 は 48 ポート（10M/100M/1G）を、それぞれ搭載しており、48 箇所ある RJ-45 ポートで最大 740W のパワーバジェットを提供できるため、電源アダプターの必要性を抑えて、電源設定コストを効率的に削減します。

ES0152/ES0152P はエンベデッド DMS 機能が付いているため、時間や場所を問わずデバイス管理を行うことができます。ES0152/ES0152P の直感的でユーザーフレンドリーなインターフェースを使えば、IT 管理者は自分自身が担当するネットワークや KE/VE89 デバイスを効率的にセットアップし管理することができます。ES0152/ES0152P はまた、IP ソースガードや ACL のように広範囲なセキュリティ機能を搭載しているため、ネットワークを不正なアクセスから保護することができます。

ネットワークの効率性、管理の容易性、そして信頼性を最適化する機能を多数備えた ES0152/ES0152P は、大企業や SMB はもとより、OT インフラに ATEN 製 IP-KVM エクステンダー（KE シリーズ）および Video over IP エクステンダー（VE89 シリーズ）を導入したシステムにとって最適なネットワークソリューションです。

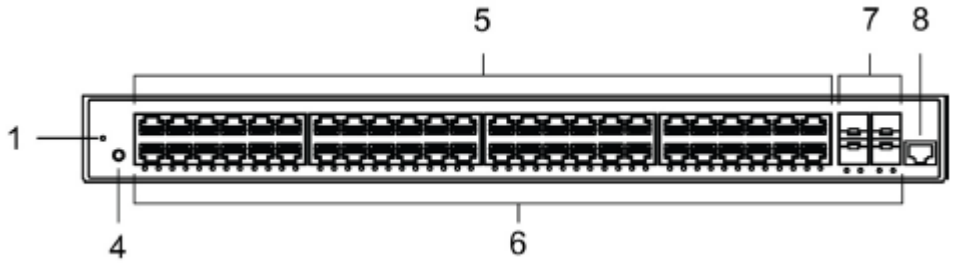
注意：	1. 対応製品は弊社 Web サイト（https://www.aten.com/jp/ja/）にてご確認ください。

特長

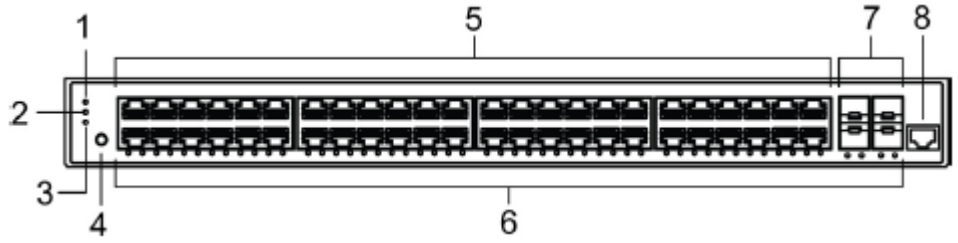
- KE/VE89 シリーズのデバイスを自動検出
- プラグアンドプレイ – 追加設定不要
- IGMP Snooping Fast Leave（IGMP スヌーピング高速脱退）対応
- フローコントロール対応
- IGMP Snooping v1/v2/v3 および IGMP v1/v2 Querier 対応
- 48 ポートのギガビットイーサネットポートおよび 4 ポートの SFP アップリンクポート※（10Gbps）を搭載
- スイッチング容量 176Gbps の高性能ギガビットイーサネット L2 アクセススイッチ – システムのレスポンスとファイル転送回数を大幅に改良
- デバイス管理システム（DMS）搭載 – 接続されている KE/VE89 デバイスすべての概要を管理用に提供
- IEEE 802.1w 高速スパニングツリープロトコル対応 – リンクエラーから速やかに回復し、ネットワークの安定性と信頼性を全体的に強化
- 広範囲な QoS - ネットワーク上で最大 4 種類のトラフィックタイプのマーキング、分類およびスケジューリングが可能
- 強化されたセキュリティ – ポートセキュリティ機能でスイッチポートを使用するデバイスの総数を制限し、MAC フラッディング攻撃を防止
- IPv4/IPv6 管理機能
- 802.3af PoE/ 802.3at PoE+ポート設定およびスケジューリング（ES0152P のみ）

製品各部名称

ES0152 フロントパネル



ES0152P フロントパネル



No.	名称	説明
1	システム LED	スイッチの電源が正しく投入されているかどうか、またはトラブルシューティングのために発動されたシステムアラームがあるかどうかを示します。 LED の動作については、p.20「システム LED」を参照してください。
2	リンク/アクティブ/スピード LED (ES0152P のみ)	この LED が点灯すると、ポートステータス LED は、各ポートのリンクの状態、ネットワークのアクティビティー、および速度を表示します。LED の動作については、p.21「ポートステータス LED」を参照してください。 ユーザーはモードボタンを押して、リンク/アクティビティー/スピードモードと PoE モードを切り替えることができます。

(表は次のページに続きます)

No.	名称	説明
3	PoE LED (ES0152P のみ)	この LED が点灯している場合、ポートステータス LED は各ポートの PoE 電源投入状態を表します。LED の動作については、p.21「ポートステータス LED」を参照してください。 ユーザーはモードボタンを押して、リンク/アクティビティー/スピードモードと PoE モードを切り替えることができます。
4	モード/リセットボタン	モード/リセットボタンを長押しすると、スイッチをリセットしたり、スイッチを工場出荷時の状態に戻したり、ポートステータス LED の表示定義を変更したりできます(ES0152P のみ)。 ◆ **デフォルトに戻す:**ボタンを 7～12 秒間、長押ししてください。そうすると、すべてのポートステータス LED が点灯している間、システム LED が点滅します。 ◆ **スイッチをリセットする:**ボタンを 2～7 秒間、長押ししてください。そうすると、システム LED が点滅を開始し、すべてのポートステータス LED が消灯します。 ◆ **(ES0152P のみ)ポートステータス LED の定義を変更する:**ボタンを 0～2 秒間、長押ししてください。ポートステータス LED が p.21「ポートステータス LED」に従って動作している間、システム LED が点灯します。
5	10/100/1000 RJ-45 ポート	
6	ポートステータス LED	接続されているポートの状態を示します。
7	10G SFP+ポート	
8	コンソールポート	CLI を操作するには、RJ-45→DB-9 シリアルコンソールケーブルを接続してください。CLI コマンドについては、「CLI ユーザーマニュアル」を参照してください。

システム LED

色	状態	説明
グリーン	ON	スイッチの電源が正しく ON になっています。
	OFF	スイッチに電源が入っていないことを示しています。
レッド	ON	スイッチで、動作温度範囲の超過などの異常状態が検出されました。

ポートステータス LED

ポートステータス LED の動作を次の表に示します。

ポート	色	状態	説明
RJ-45 ポート	グリーン	ON	ポートが有効で、接続機器へのリンクが確立されています。また、接続速度は 1000Mbps です。
	グリーン	点滅	ポートはパケットの送受信中で、接続速度は 1000Mbps です。
	オレンジ	ON	ポートが有効で、接続機器へのリンクが確立されています。また、接続速度は 10/100Mbps です。
	オレンジ	点滅	ポートはパケットの送受信中で、接続速度は 10/100Mbps です。
	-	OFF	ポートにアクティブなネットワークケーブルが接続されていないか、接続されているデバイスへのリンクが確立されていません。あるいは、スイッチのユーザーインターフェースを介してポートが無効になっている可能性があります。
SFP+ポート	ブルー	ON	ポートが有効で、接続機器へのリンクが確立されています。また、接続速度は 10Gbps です。
	ブルー	点滅	ポートはパケットの送受信中で、接続速度は 10Gbps です。
	グリーン	ON	ポートが有効で、接続機器へのリンクが確立されています。また、接続速度は 1Gbps です。
	グリーン	点滅	ポートはパケットの送受信中で、接続速度は 1Gbps です。
	-	OFF	ポートにアクティブなネットワークケーブルが接続されていないか、接続されているデバイスへのリンクが確立されていません。あるいは、スイッチのユーザーインターフェースを介してポートが無効になっている可能性があります。

■リンク/アクティブ/スピード LED 点灯時（ES0152P のみ）

ポートステータス LED の動作は、上記の表と同じです。

■PoE LED 点灯時(ES0152P のみ)

ポート	色	状態	説明
RJ-45 ポート	グリーン	ON	ポートが有効で、接続されたデバイスに電源が供給されます。
	オレンジ	ON	スイッチで過負荷状態が検出されるなどの異常状態です。
	-	OFF	ポートにアクティブなネットワークケーブルが接続されていないか、PoE PD デバイスに接続されていません。あるいは、スイッチのユーザーインターフェースを介してポートが無効になっている可能性があります。

ES0152/ES0152P リアパネル

No.	名称	説明
1	電源コネクター	付属の電源コードをこのソケットに接続し、AC 電源ソケットを使ってデバイスに電力を供給します。

Web インターフェース

スイッチの機能は、第 3 章「システム」以降の章で説明する Web インターフェースを使用して、設定や管理を行うことができます。

初期設定とログイン

スイッチに初めて電源を投入するときは、Web インターフェースを使用してスイッチの初期設定を行うことができます。

最初の設定段階から始めるには、PC とスイッチ間の通信を可能にするために、PC の IP アドレスとサブネットマスクを再設定する必要があります。

工場出荷時におけるスイッチのデフォルト設定
IP アドレス:192.168.0.1
サブネットマスク:255.255.255.0
ゲートウェイ:192.168.0.254

PC の IP アドレス(例:192.168.0.250)を変更すると、スイッチのデフォルト IP アドレス(192.168.0.1)を使用してスイッチの Web インターフェースにアクセスできます。

Windows®7/8.x/10 を実行している PC におけるスイッチの初期設定手順は、次のとおりです。

1. 「**スタート**」メニューの「**検索**」ボックスに「ネットワークと共有」と入力してください。

2. 「**ネットワークと共有センター**」を選択してください。

3. PC 画面左側の「**アダプター設定の変更**」をクリックしてください。

注意:	[Win]+[R]キーを押して入力すると、手順 1～3 を省略することができます。その場合は、「ncpa.cpl」コマンドを使用して、手順 4 に直接進んでください。

4. ローカルアダプターを右クリックし、「**プロパティ**」を選択してください。

5. 「**ローカルエリア接続のプロパティ**」ウィンドウで、「**インターネットプロトコルバージョン**

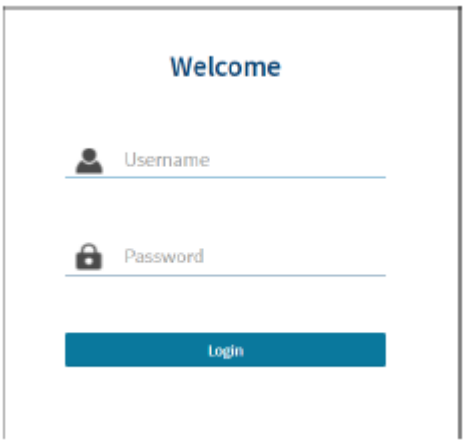
4(TCP/IPv4)」を選択したら、「**プロパティ**」ボタンをクリックしてください。

注意： PC の現在の IP 設定を後で復元できるように、すべて記録しておいてください。

6. 「**次の IP アドレスを使用する**」のラジオボタンを選択し、PC の IP アドレス（使用していない IP アドレス、192.168.0.2～192.168.0.254 の範囲内の IP アドレス、サブネットマスク（例:255.255.255.255.0）、デフォルトゲートウェイなど）を、お使いのネットワーク環境に適した値で入力してください。次に、優先および代替 DNS サーバーのアドレスを入力してください。

7. 「**OK**」をクリックして、PC の IP アドレスを変更してください。

8. PC で Web ブラウザーを開いたら、スイッチの Web インターフェースにアクセスするために、出荷時のデフォルト設定 IP アドレスを入力してください。そうすると、ログインページが表示されます。



注意： 上記のログインページが表示されない場合は、以下を試してください。

1. Web ページを更新する。
2. IP の競合問題がないかどうかを確認する。
3. ブラウザーの Cookie と一時的なインターネットファイルを消去する。
4. PC の設定を再度確認し、手順 2 を繰り返す。

9. ユーザーネームとパスワードを入力してください。デフォルトのユーザーネームは admin です。スイッチ底面のシールには、各スイッチに固有で事前にプログラムされたパスワード（下の赤枠内参照）が貼られています。次に例を示します。

10. 「Login」（ログイン）をクリックして、スイッチにログインしてください。

注意： パスワードを変更する場合は、「**Security**」（セキュリティ）→「**Management**」（管理）→「**Account**」（アカウント）を選択し、**admin**（ユーザー名）をクリックしてください。そうしたら、新しいパスワードと確認用パスワードを入力して、「**Apply**」（適用）をクリックしてください。

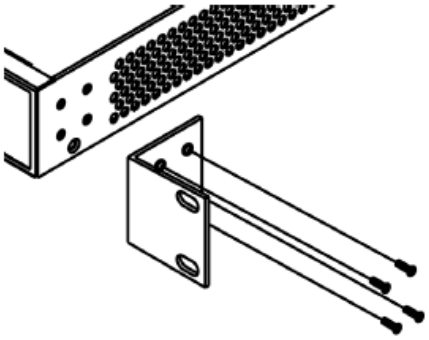
第 2 章
セットアップ

マウント方法

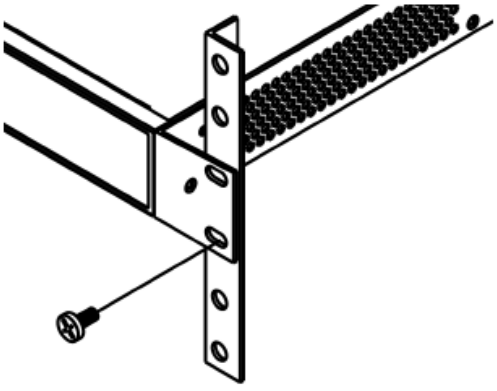
ラックへのマウント

次の手順に従って、デバイスをラックにマウントしてください。

1. シャーシの両側にマウント用ブラケットを取り付けてください。ネジを挿入したら、ドライバーで締めてブラケットを固定してください。



2. ラック内におけるスイッチのマウント位置を決めてください。ブラケットの楕円形の穴がラック支柱のマウント用ホールに合うようにしてください。

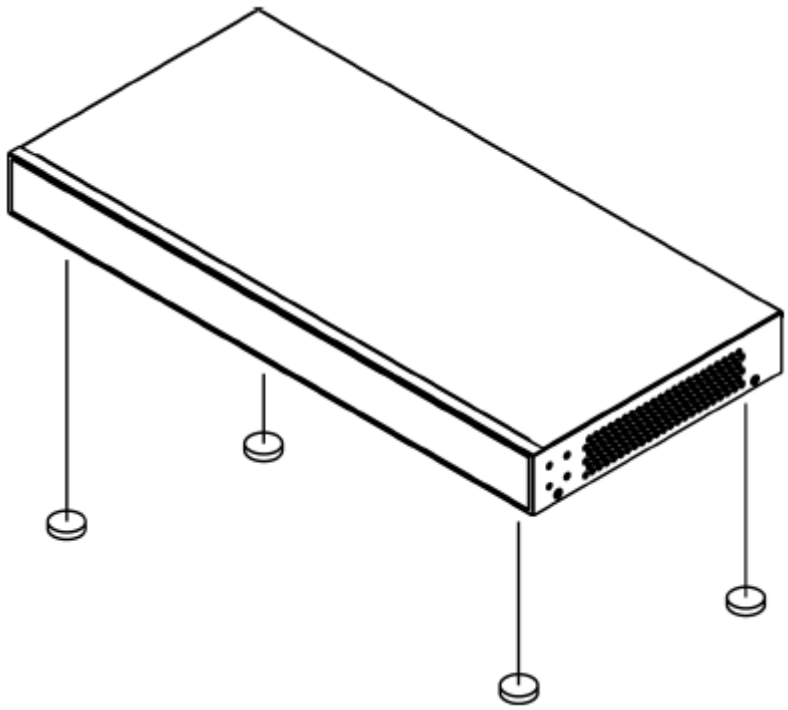


3. 支柱にブラケットを取り付けてください。ネジを挿入して締めます。

卓上設置

1. 机/作業台が、デバイスを取り付けられるだけ頑丈で、なおかつ確実に接地されていることを確認してください。

2. フットパッド(4 個)をスイッチの底面に取り付けてください。

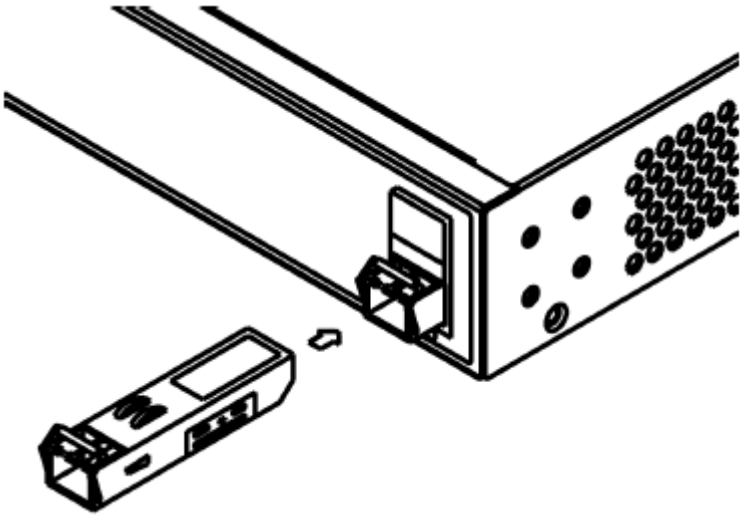


SFP+モジュールの取り付け

SFP+ポートのオプションアクセサリーとして、ミニ GBIC SFP+モジュールを取り付けることができます。SFP+ポートの接続能力は最大 10Gbps ですので、最大 10Gbps のデータ転送速度をサポートできるミニ GBIC SFP+モジュールを選択することができます。モジュールは、スイッチの電源が入っている状態でも取り付けることができます。

1. モジュールを SFP+ポートに挿入してください。

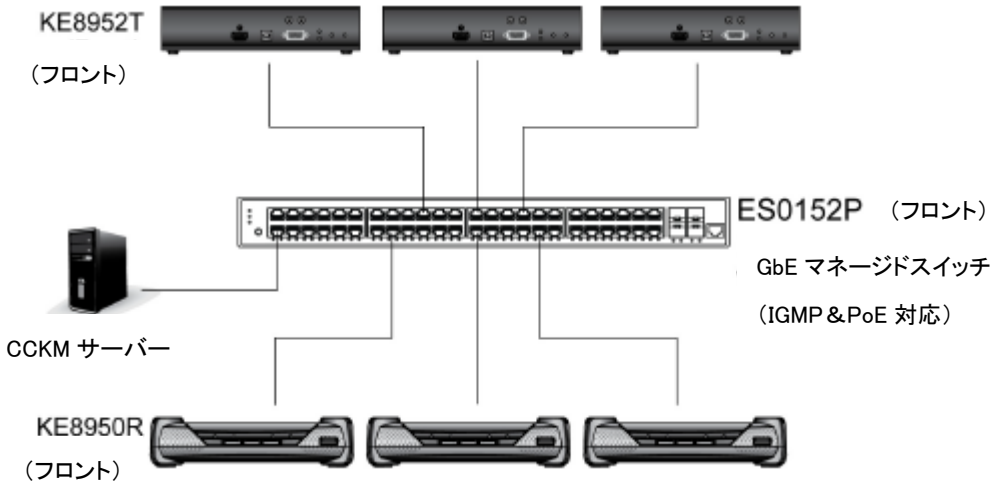
2. しっかりと押して、モジュールがコネクターに固定されていることを確認してください。



ハードウェアのセットアップ

ES0152/ES0152P の電源ソケットと AC 電源の間に電源コードを接続してください。そうしたら、スイッチの電源が入っているかどうか、システム LED で確認してください。スイッチの RJ-45 ポートと KE/VE89 シリーズエクステンダーの Ethernet RJ-45 ポートを、イーサネット LAN ケーブルで接続します。ポートステータス LED が点滅している場合は、スイッチの準備が整っています。

次に例を示します。

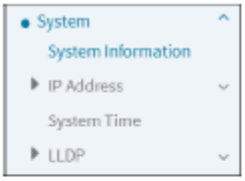


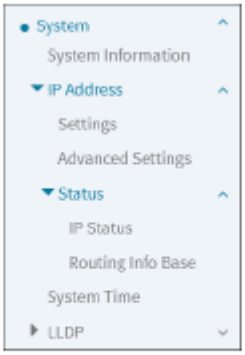
第 3 章
システム

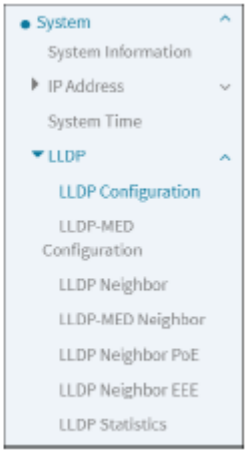
概要

この章では、基本的な設定作業全般について説明します。

メニューとサブメニューを以下に示します。

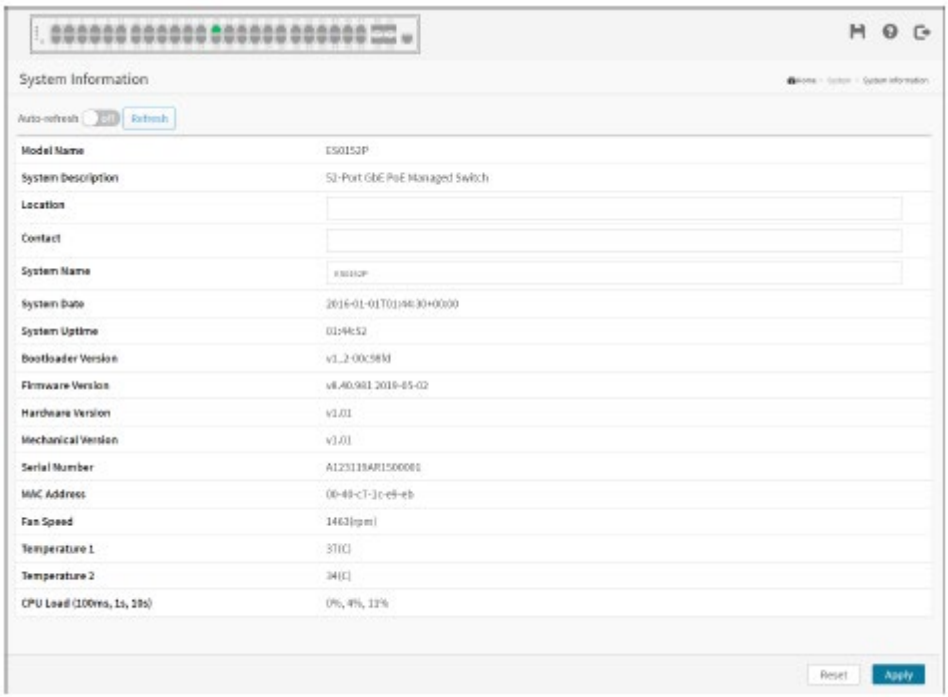






システム情報

この画面では、デバイスの場所、連絡先、およびシステム名を設定したり、システムの情報を確認したりすることができます。スイッチのシステムの連絡先情報も、ここに記載されています。



■パラメーターの説明

Model Name（モデル名）:
工場出荷時に定義されたモデル名を、識別用に表示します。

System Description（システムの説明）:
システムの説明を表示します。

Location（場所）:
Configuration（設定） ＞ System（システム） ＞ Information（情報） ＞ System Location（システムの場所）で設定されたシステムの場所です。

Contact（連絡先）:
Configuration（設定） ＞ System（システム） ＞ Information（情報） ＞ System Contact（システム連絡先）で設定されたシステムの連絡先です。

System Name（システム名）：
System（システム） ＞ System Information（システム情報） ＞ Configuration（設定） ＞ System Name（システム名）で設定されたユーザー定義のシステム名を表示します。

System Date（システム日付）：
現在の（GMT）システム時刻と日付です。システム時刻は、スイッチで実行されているタイムサーバー（存在する場合）から取得されます。

System Uptime（システム稼働時間）：
デバイスが動作している期間です。

Bootloader Version（ブートローダーバージョン）：
現在のブートローダーのバージョン番号を表示します。

Firmware Version（ファームウェアのバージョン）：
このスイッチのソフトウェアバージョンです。

Hardware Version（ハードウェアバージョン）：
デバイスのハードウェアバージョンを表示します。

Mechanical Version（メカニカルバージョン）：
デバイスの機械バージョンを表示します。

Series Number（シリーズ番号）：
このスイッチのシリアル番号です。

MAC Address（MAC アドレス）：
このスイッチの MAC アドレスです。

Fan Speed（ファン速度）：
ファン速度（rpm）に関する情報を表示します。

Temperature 1（温度 1）：
システムの温度 1 を表示します。

Temperature 2（温度 2）：

システムの温度 2 を表示します。

CPU Load (100ms, 1s, 10s)(CPU 負荷(100ms、1s、10s)):
システムの CPU 負荷(100ms、1s、10s)を表示します。

■ボタン

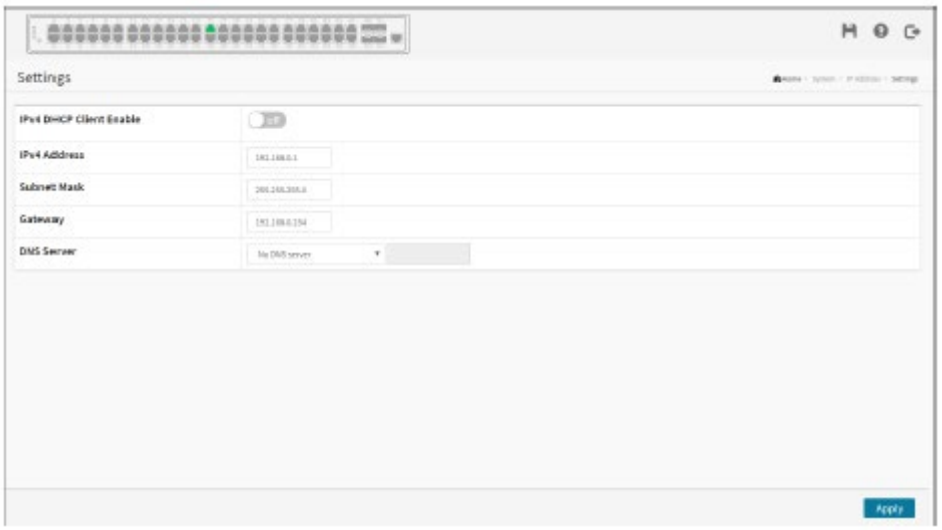
Apply(適用):
クリックすると、変更内容を保存します。

Reset(リセット):
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

IP アドレス

設定

スイッチの IPv4 アドレスは、VLAN 1 の DHCP サーバーを介して取得できます。アドレスを手動で設定するには、スイッチのデフォルト設定を、ネットワークと互換性のある値に変更する必要があります。また、スイッチと、別のネットワークセグメントに存在する管理ステーション間にデフォルトゲートウェイを確立する必要が出てくる場合もあります。



IP を設定するには:

1. 「System」(システム) ＞ 「IP Address」(IP アドレス) ＞ 「Configuration」(設定)をクリックしてください。
2. 「IPv4 DHCP Client」(IPv4 DHCP クライアント)を有効または無効にしてください。
3. 「IPv4 Address」(IPv4 アドレス)、「Subnet Mask」(サブネットマスク)、「Gateway」(ゲートウェイ)を指定してください。
4. 「DNS Server」(DNS サーバー)を選択してください。
5. 「Apply」(適用)をクリックしてください。

■パラメーターの説明

IPv4 DHCP Client Enable(IPv4DHCP クライアント有効):

DHCP クライアントを有効にする場合は、このチェックボックスを ON にしてください。このオプションを有効にすると、システムは DHCP プロトコルを使用してインターフェースの IPv4 アドレスとマ

スクを設定します。DHCP クライアントは、設定されたシステム名をホスト名として通知し、DNS ルックアップを提供します。

IPv4 Address（IPv4 アドレス）：
ドット付き 10 進表記のインターフェースの IPv4 アドレスです。
DHCP が有効である場合、この項目は使用されません。インターフェースで IPv4 操作を行わない場合は、この項目を空白のままにしておくこともできます。

Subnet Mask（サブネットマスク）：
このエントリーのユーザーIP サブネットマスクです。

Gateway（ゲートウェイ）：
IP ゲートウェイの IP アドレスです。有効な形式は、ドット付き 10 進表記または有効な IPv6 表記です。ゲートウェイとネットワークは同じタイプにする必要があります。

DNS Server（DNS サーバー）：
この設定は、スイッチが実行する DNS 名解決を制御します。
設定に使用できるサーバーは 4 台あり、サーバーのインデックスは DNS 名解決の優先度を示します（インデックスが少ないほど優先度が高くなります）。

以下のモードがサポートされています。

- No DNS Server（DNS サーバーなし）
  DNS サーバーは使用されません。
- Configured IPv4（設定された IPv4）
  DNS サーバーの有効な IPv4 ユニキャストアドレスを、ドット付き 10 進表記で明示的に指定します。
  DNS サービスを有効にするために、設定された DNS サーバーに(ping などを介して)到達できることを確認してください。
- Configured IPv6（設定された IPv6）
  DNS サーバーの有効な IPv6 ユニキャスト（リンクローカルを除く）アドレスを、明示的に指定します。
  DNS サービスを有効にするために、設定された DNS サーバーに（ping6 などを介して）到達できることを確認してください。
- From any DHCPv4 interfaces（任意の DHCPv4 インターフェースから）
  DHCPv4 リースから DHCPv4 対応インターフェースに提供された最初の DNS サーバーが使用されます。

◆ From this DHCPv4 interface（この DHCPv4 インターフェースから）
提供された DNS サーバーを優先する DHCPv4 対応インターフェースを指定します。

◆ From any DHCPv6 interfaces（任意の DHCPv6 インターフェースから）
DHCPv6 リースから DHCPv6 対応インターフェースに提供された最初の DNS サーバーが使用されます。

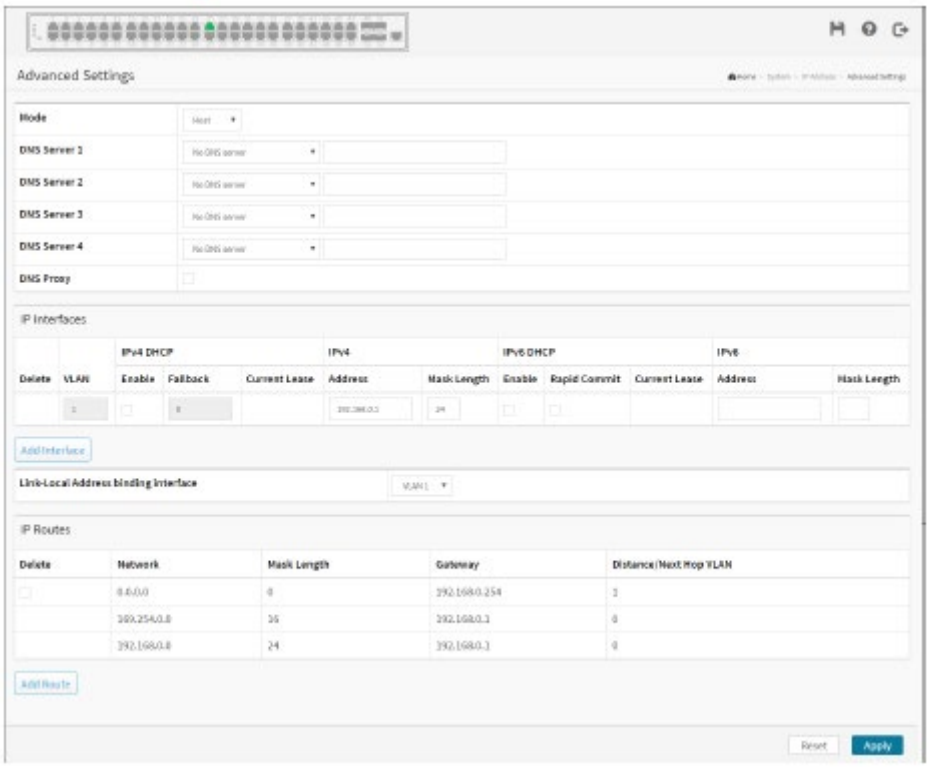
◆ From this DHCPv6 interface（この DHCPv6 インターフェースから）
提供された DNS サーバーを優先する DHCPv6 対応インターフェースを指定します。

■ボタン

Apply（適用）：
クリックすると、変更内容を保存します。

詳細設定

この画面では、スイッチが管理する IP 情報を設定します。
IP 基本設定、および IP インターフェースと IP ルートの制御を行ってください。
サポートされるインターフェースの最大数は 8 で、ルートの最大数は 8 です。



Web インターフェースで詳細設定を行うには:

1. 「System」(システム) ＞ 「IP Address」(IP アドレス) ＞ 「Advanced Settings」(詳細設定)をクリックしてください。
2. 「Add Interface」(インターフェースの追加)をクリックすると、スイッチに新しいインターフェースを作成することができます。
3. 「Add Route」(ルートの追加)をクリックすると、スイッチに新しいルートを作成することができます。
4. 「Apply」(適用)をクリックしてください。

■パラメーターの説明

Basic Setting(基本設定)

Mode(モード):

IP スタックを、ホストとルーターのどちらとして機能させるかを設定してください。ホストモードの場合、インターフェース間の IP トラフィックはルーティングされません。一方、ルーターモードの場合、トラフィックはすべてのインターフェース間でルーティングされます。

DNS Server(DNS サーバー):

この設定は、スイッチが実行する DNS 名解決を制御します。

設定に使用できるサーバーは 4 台あり、サーバーのインデックスは DNS 名解決の優先度を示します(インデックスが少ないほど優先度が高くなります)。

以下のモードがサポートされています。

- ◆ No DNS Server(DNS サーバーなし)
  DNS サーバーは使用されません。
- ◆ Configured IPv4(設定された IPv4)
  DNS サーバーの有効な IPv4 ユニキャストアドレスを、ドット付き 10 進表記で明示的に指定します。
  DNS サービスを有効にするために、設定された DNS サーバーに(ping などを介して)到達できることを確認してください。
- ◆ Configured IPv6(設定された IPv6)
  DNS サーバーの有効な IPv6 ユニキャスト(リンクローカルを除く)アドレスを、明示的に指定します。
  DNS サービスを有効にするために、設定された DNS サーバーに(ping6 などを介して)到達できることを確認してください。
- ◆ From any DHCPv4 interfaces(任意の DHCPv4 インターフェースから)

DHCPv4 リースから DHCPv4 対応インターフェースに提供された最初の DNS サーバーが使用されます。

- From this DHCPv4 interface（この DHCPv4 インターフェースから）
  提供された DNS サーバーを優先する DHCPv4 対応インターフェースを指定します。
- From any DHCPv6 interfaces（任意の DHCPv6 インターフェースから）
  DHCPv6 リースから DHCPv6 対応インターフェースに提供された最初の DNS サーバーが使用されます。
- From this DHCPv6 interface（この DHCPv6 インターフェースから）
  提供された DNS サーバーを優先する DHCPv6 対応インターフェースを指定します。

DNS Proxy（DNS プロキシ）：
DNS プロキシが有効な場合、システムは現在設定されている DNS サーバーに DNS 要求をリレーし、DNS リゾルバとしてネットワーク上のクライアントデバイスに応答します。
現時点では、IPv4DNS プロキシのみがサポートされています。

IP Interfaces（IP インターフェース）

Delete（削除）：
既存の IP インターフェースを削除するには、このオプションを選択してください。

VLAN：
IP インターフェースに関連付けられた VLAN です。この VLAN 内のポートのみが IP インターフェースにアクセスできます。この項目は、新しいインターフェースを作成する際の入力にのみ使用できます。

IPv4 DHCP Enabled（IPv4 DHCP 有効）：
DHCP クライアントを有効にする場合は、このチェックボックスを ON にしてください。このオプションを有効にすると、システムは DHCP プロトコルを使用してインターフェースの IPv4 アドレスとマスクを設定します。DHCP クライアントは、設定されたシステム名をホスト名として通知し、DNS ルックアップを提供します。

IPv4 DHCP Fallback Timeout（IPv4 DHCP フォールバックタイムアウト）：
DHCP リースの取得を試行できる秒数です。この期間が経過すると、設定された IPv4 アドレスが IPv4 インターフェースアドレスとして使用されます。値が 0 の場合、フォールバックメカニズムは無効になり、有効なリースが取得されるまで DHCP は再試行を続けます。有効な値は 0～4294967295 秒です。

IPv4 DHCP Current Lease（IPv4 DHCP 現在のリース）：
アクティブなリースを使用するDHCPインターフェースの場合、この列には、DHCPサーバーによって提供される現在のインターフェースアドレスが表示されます。

IPv4 Address（IPv4 アドレス）：
ドット付き 10 進表記のインターフェースの IPv4 アドレスです。
DHCP が有効である場合、この項目は使用されません。インターフェースで IPv4 操作を行わない場合は、この項目を空白のままにしておくこともできます。

IPv4 Mask Length（IPv4 マスク長）：
ビット数（プレフィックス長）で表した IPv4 ネットワークマスクです。有効な値は、IPv4 アドレスの 0～30 ビットです。
DHCP が有効である場合、この項目は使用されません。インターフェースで IPv4 操作を行わない場合は、この項目を空白のままにしておくこともできます。

DHCPv6 Enable（DHCPv6 有効）：
DHCPv6 クライアントを有効にする場合は、このチェックボックスを ON にしてください。このオプションを有効にすると、システムは DHCPv6 プロトコルを使用してインターフェースの IPv6 アドレスを設定します。

DHCPv6 Rapid Commit（DHCPv6 高速コミット）：
DHCPv6高速コミットオプションを有効にする場合は、このチェックボックスをONにしてください。このオプションを有効にすると、DHCPv6 クライアントは、高速コミットオプションを含む応答メッセージを受信すると、すぐに待機プロセスを終了します。
このオプションは、DHCPv6 クライアントが有効な場合にのみ管理可能です。

DHCPv6 Current Lease（DHCPv6 現在のリース）：
アクティブなリースを使用するDHCPv6インターフェースの場合、この列にはDHCPv6サーバーによって提供されるインターフェースアドレスが表示されます。

IPv6 Address（IPv6 アドレス）：
インターフェースの IPv6 アドレスです。IPv6 アドレスは、各項目（:）をコロンで区切った最大 4 桁の16進数の8項目で表される128ビットのレコードです(例 fe80:#2]c5ff:fe03:4dc7)。シンボル「::」は、連続する 0 の複数の 16 ビットグループを表す短縮形として使用できる特殊な構文ですが、一度しか使用できません。また、構文的に有効な IPv4 アドレスを表すこともできます(例 ::192.1.2.34)。

インターフェースで IPv6 操作を行わない場合は、この項目を空白のままにしておくこともできます。

IPv6 Mask Length（IPv6 マスク長）:
ビット数（プレフィックス長）で表した IPv6 ネットワークマスクです。有効な値は、IPv6 アドレスの 1～128 ビットです。
インターフェースで IPv6 操作を行わない場合は、この項目を空白のままにしておくこともできます。

IP Routes（IP ルート）

Delete（削除）:
既存の IP ルートを削除するには、このオプションを選択してください。

Network（ネットワーク）:
このルートの宛先 IP ネットワークまたはホストアドレスです。有効な形式は、ドット付き 10 進表記または有効な IPv6 表記です。デフォルトのルートでは、0.0.0.0 または IPv6 の「::」表記が使用できます。

Mask Length（マスク長）:
宛先 IP ネットワークまたはホストマスク(ビット数（プレフィックス長）)です。このルートの条件を満たすために、一致する必要があるネットワークアドレスの量を定義します。有効な値は、IPv6 ルートで、それぞれ 0～32 ビットで、合計 128 です。デフォルトのルートだけ、マスク長が 0 になります（何にでもマッチするため）。

Gateway（ゲートウェイ）:
IP ゲートウェイの IP アドレスです。有効な形式は、ドット付き 10 進表記または有効な IPv6 表記です。ゲートウェイとネットワークは同じタイプにする必要があります。

Next Hop VLAN（ネクストホップ VLAN）（IPv6 のみ）:
ゲートウェイに関連付けられた特定の IPv6 インターフェースの VLAN ID（VID）です。
指定された VID の範囲は 1～4094 で、対応する IPv6 インターフェースが有効な場合にのみ有効です。
IPv6 ゲートウェイのアドレスがリンクローカルの場合、ゲートウェイのネクストホップ VLAN を指定する必要があります。
IPv6 ゲートウェイのアドレスがリンクローカルでない場合、システムはゲートウェイのネクストホップ VLAN を無視します。

■ボタン

Add Interface（インターフェースの追加）：
クリックすると、新しい IP インターフェースを追加します。最大 8 つのインターフェースがサポートされます。

Add Route（ルートの追加）：
クリックすると、新しい IP ルートを追加します。最大 8 つのルートがサポートされます。

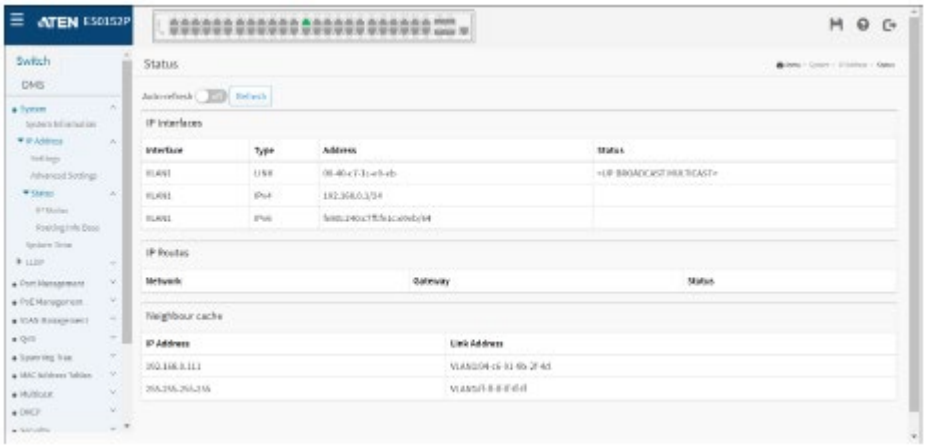
Apply（適用）：
クリックすると、変更内容を保存します。

Reset（リセット）：
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

状態

IP の状態

この画面には、IP プロトコル層の状態が表示されます。この状態は、IP インターフェース、IP ルート、およびネイバーキャッシュ（ARP キャッシュ）の状態によって定義されます。



Web インターフェースにログの設定を表示するには：

1. 「System」（システム） ＞ 「IP Address」（IP アドレス） ＞ 「Status」（状態）をクリックしてください。
2. IP 設定情報を表示してください。

■パラメーターの説明

IP Interface（IP インターフェース）

Interface（インターフェース）：
インターフェースの名前を表示します。

Type（タイプ）：
このエントリーのアドレスタイプ（LINK または IPv4）を表示します。

Address（アドレス）：
（指定されたタイプの）インターフェースの現在のアドレスを表示します。

Status（状態）：
インターフェース（および/またはアドレス）の状態フラグを表示します。

IP Route（IP ルート）

Network（ネットワーク）：
このルートの宛先 IP ネットワークまたはホストアドレスを表示します。

Gateway（ゲートウェイ）：
このルートのゲートウェイアドレスを表示します。

Status（状態）：
ルートの状態フラグを表示します。

Neighbor cache（ネイバーキャッシュ）

IP Address（IP アドレス）：
このエントリーの IP アドレスを表示します。

Link Address（リンクアドレス）：
指定された IP アドレスへのバインドが存在するリンク(MAC)アドレスを表示します。

■ボタン

Auto-refresh（自動更新）：
画面を自動的に更新する場合は、このチェックボックスを ON にしてください。自動更新は 3 秒間隔で行われます。

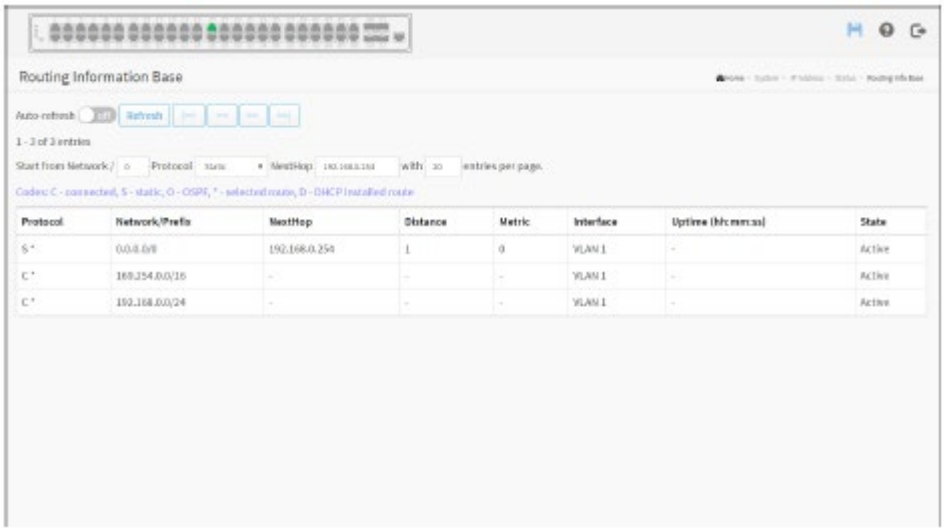
Refresh（更新）：
クリックすると、画面がすぐに更新されます。

ルーティング情報ベース

ルーティング情報ベーステーブルの操作方法

各ページには、最大 999 個のテーブルエントリーが表示されます。これは、「entries per page」（ページあたりのエントリー数）の入力フィールドで選択したものです。最初にアクセスすると、このテーブルの開始エントリーが Web ページに表示されます。

「Start from *ID*」(*ID* から開始)入力欄を使用すると、このテーブルの開始点を変更できます。「Refresh」(更新)ボタンをクリックすると、表示されているテーブルが更新されます。これは、そのテーブルまたは次のエントリーに一致するもののうち、最も近いものから始まります。さらに、これらの入力項目は、「Refresh」(更新)ボタンをクリックすると、最初に表示されたエントリーの値を想定して、同じ開始入力項目での継続的な更新を可能にします。



Web インターフェース

Web インターフェースにルーティング情報を表示するには:

1. 「System」(システム) ＞ 「IP Address」(IP アドレス) ＞ 「Status」(状態) ＞ 「Routing Info Base」(ルーティング情報ベース)をクリックしてください。
2. ルーティングベース情報を表示してください。

■パラメーターの説明

DHCP:

ルートは DHCP によって作成されます。

Connected(接続済み):

宛先ネットワークが直接接続されています。

Static(スタティック):

ルートはユーザーによって作成されます。

OSPF:

ルートは OSPF によって作成されます。

Network/Prefix（ネットワーク/プレフィックス）:
指定されたルートエントリーのネットワークとプレフィックス（例：10.0.0.0/16）です。

NextHop（ネクストホップ）:
ネクストホップの IP アドレスです。値「0.0.0.0」は、リンクが直接接続されていることを示します。

Distance（距離）:
ルートの距離です。

Metric（メトリック）:
ルートのメトリックです。

Interface（インターフェース）:
IP パケットが送信されるインターフェースです。

Uptime（稼働時間）（hh:ss:mm）:
ルートが作成されるまでの時間です。単位は秒です。

State（状態）:
宛先ネットワークに到達可能かどうかを示します。

■ボタン

Auto-refresh（自動更新）:
画面を自動的に更新する場合は、このチェックボックスを ON にしてください。自動更新は 3 秒間隔で行われます。

Refresh（更新）:
クリックすると、画面がすぐに更新されます。

|<< :

テーブルエントリーを、最初に使用可能なエントリーから更新します。テーブルの最初のエントリ

ーが表示されている場合、このボタンは無効になっています。

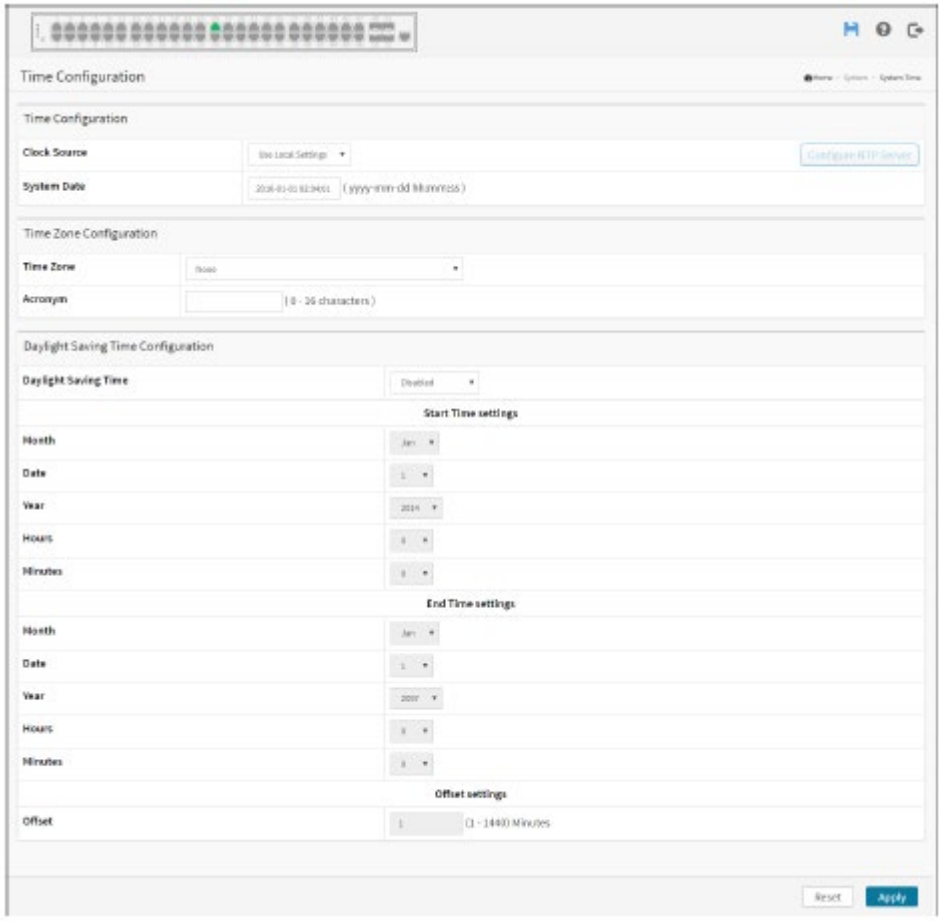
<< :
テーブルエントリーを更新し、現在表示されている最初のエントリーの前のエントリーで終了します。テーブルの最初のエントリーが表示されている場合、このボタンは無効になっています。

>> :
現在表示されている最後のエントリーの横にあるエントリーから開始して、テーブルエントリーを更新します。
テーブルの最後のエントリーが表示されている場合、このボタンは無効になっています。

>>| :
テーブルエントリーを更新し、最後に使用可能なエントリーで終了します。テーブルの最後のエントリーが表示されている場合、このボタンは無効になっています。

システム時刻

スイッチには、手動および自動で、NTP 経由でシステム時刻を設定する方法が用意されています。手動設定は簡単で、各項目の有効範囲内において、年、月、日、時、分を入力するだけです。



Web インターフェースで時刻を設定するには：

1. 「System」（システム） ＞ 「System Time」（システム時刻）をクリックしてください。
2. 時刻パラメーターを指定してください。
3. 「Apply」（適用）をクリックしてください。

■パラメーターの説明

Time Configuration（時刻設定）

Clock Source（クロックソース）：

クロックソースの設定には、2 種類のモードがあります。ローカルタイムからクロックソースを設定する場合は「Local Settings」（ローカル設定）を選択してください。NTP サーバーからクロックソースを設定する場合は、「NTP Server」（NTP サーバー）を選択してください。

System Date（システム日付）：

システムの現在の時刻を表示します。システム日付の「年」は、2000～2037 年の間で設定してください。

Time Zone Configuration（タイムゾーンの設定）

Time Zone（タイムゾーン）：

世界中の様々なタイムゾーンを一覧表示します。ドロップダウンから適切なタイムゾーンを選択し、「Apply」（適用）をクリックして設定してください。

Acronym（略語）：

ユーザーはタイムゾーンの頭文字を設定できます。これは、タイムゾーンの識別に使われるユーザー設定可能な頭文字です。（範囲：最大 16 文字）

Daylight Saving Time Configuration（サマータイムの設定）

Daylight Saving Time（サマータイム）：

定義されたサマータイム期間中に、以下の設定に従って時計を正方向または逆方向に設定するために使用します。「Disable」（無効）を選択すると、サマータイム設定を無効にします。

「Recurring」（繰り返し）を選択すると、毎年設定を繰り返すようにサマータイム期間を設定します。

「Non-Recurring」（繰り返さない）を選択すると、1 回限りでサマータイム期間を設定します（デフォルト：無効）。

Recurring Configuration（繰り返し設定）

Start time settings（開始時刻の設定）：

Week（週） – 開始週の番号を選択してください。

Day（日） – 開始日を選択してください。

Month（月） – 開始月を選択してください。

Hour（時） – 開始時間（時）を選択してください。

Minutes（分） – 開始時間（分）を選択してください。

End time settings（終了時刻の設定）:
Week（週） – 終了の週番号を選択してください。
Day（日） – 終了日を選択してください。
Month(月) – 終了月を選択してください。
Hour（時） – 終了時間（時）を選択してください。
Minutes（分） – 終了時間（分）を選択してください。

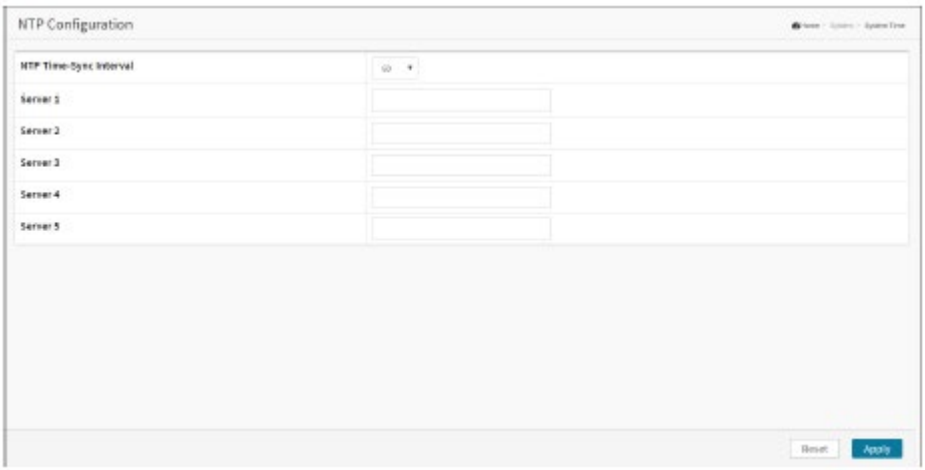
Offset settings（オフセット設定）:
Offset（オフセット） – サマータイム中に追加する時間（分）を入力してください（設定範囲：1～1440）。

注意： 「Start time settings」（開始時刻の設定）と「End time settings」（終了時刻の設定）の下には、各々のフィールド情報で設定した内容が表示されています。

■ボタン
Apply（適用）:
クリックすると、変更内容を保存します。

Reset（リセット）:
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

Configure NTP Server（NTP サーバーの設定）:



クロックソースを NTP サーバーから選択する場合は、「Configure NTP Server」（NTP サーバーの設定）をクリックしてください。NTP は「Network Time Protocol」の略ですが、これはネットワークタイムベースのグリニッジ標準時(GMT)と同期するために使用されます。NTP モードを使用して、内蔵 NTP タイムサーバーを選択するか、ユーザー定義の NTP サーバーとタイムゾーンを手動で

指定したら、「Apply」（適用）ボタンを押してください。そうすると、ボタンを押下した直後に時刻が同期されます。

時刻は自動的に同期されますが、NTP はユーザーの処理なしに定期的に時刻を更新することはありません。

タイムゾーンは、GMT のオフセット時間です。タイムゾーンを最初に選択し、次に NTP を介して時刻同期を実行する必要があります。これは、スイッチがこのタイムゾーンオフセットと更新された NTP 時刻を組み合わせてローカル時刻を取得するためです。そうしないと、正しい時刻を取得できなくなります。スイッチのタイムゾーンは、-12 から+13 まで、1 時間きざみで設定することができます。

デフォルトのタイムゾーン ： +8 時間

■パラメーターの説明

Server 1 to 5（サーバー1～5）：
このスイッチの NTP IPv4 または IPv6 アドレスを指定します。IPv6 アドレスは、各項目（:）をコロンで区切った最大 4 桁の 16 進数の 8 項目で表される 128 ビットのレコードです(例 fe80:#2]c5ff:fe03:4dc7)。シンボル「::」は、連続する 0 の複数の 16 ビットグループを表す短縮形として使用できる特殊な構文ですが、一度しか使用できません。また、構文的に有効な IPv4 アドレスを表すこともできます(例 ::192.1.2.34)。

■ボタン

これらのボタンは、SNTP 画面に表示されます。

Apply（適用）：
クリックすると、変更内容を保存します。

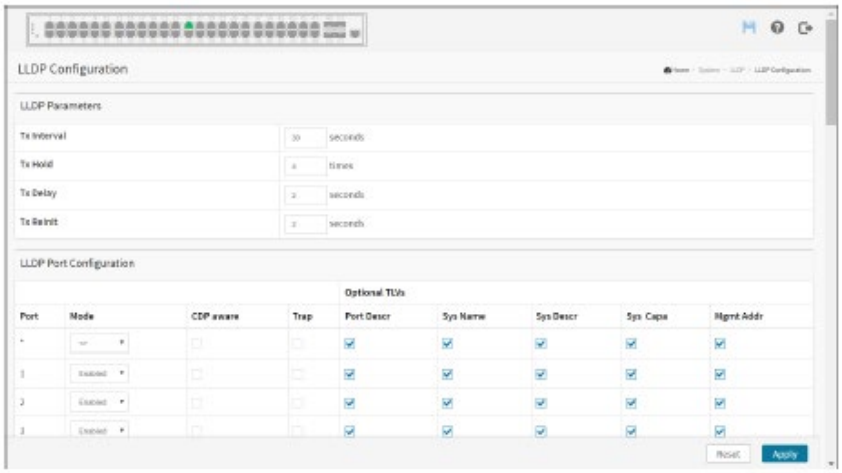
Reset（リセット）：
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

LLDP

スイッチは LLDP に対応しています。お使いのスイッチの現在の情報について、リンク層検出プロトコル(LLDP)は、スイッチが隣接するデバイスに自分自身を通知したり、隣接する LLDP デバイスについて学習したりできるよう、規格に基づいた方法を提供します。LLDP(Link Layer Discovery Protocol)は、インターネットプロトコルスイート内のベンダーに依存しないリンク層プロトコルです。このプロトコルは、IEEE802 ローカルエリアネットワーク(主に有線イーサネット)上において、ID、機能、およびネイバーを通知するためにネットワークデバイスによって使用されます。このプロトコルは、標準文書 IEEE802.1AB で規定されているステーションおよびメディアアクセス制御接続検出として、IEEE によって正式に言及されています。

LLDP の設定

LLDP と詳細パラメーターの設定は、ポートごとに行うことができます。また、設定はすぐに有効になります。この画面において、ユーザーは現在の LLDP ポートの点検や設定を行うことができます。



Web インターフェース

LLDP を設定するには:

1. 「System」(システム) ＞ 「LLDP」 ＞ 「LLDP Configuration」(LLDP の設定)をクリックしてください。
2. LLDP のタイミングに関するパラメーターを変更してください。
3. LLDP メッセージの送受信に必要なモードを設定してください。
4. 通知されたメッセージの TLV 項目に含める情報を指定してください。

5. 「Apply」(適用)をクリックしてください。

■パラメーターの説明

LLDP Parameters(LLDP パラメーター)

Tx Interval(Tx 送信間隔):
スイッチは、ネットワーク検出情報を最新にするために、ネイバーに対して LLDP フレームを定期的に送信します。各 LLDP フレームの間隔は、「Tx Interval」(Tx 送信間隔)の値によって決まります。有効な値は 5～32768 秒に制限されています。

Tx Hold(Tx 送信保留):
各 LLDP フレームには、LLDP フレーム内の情報が、どのくらいの期間、有効であると見なされるかという情報が含まれています。LLDP 情報の有効期間は、「Tx Hold」(Tx 送信保留)に「Tx Interval seconds」(Tx 送信間隔(秒))を乗算した値に設定されます。有効な値は 2～10 回に制限されています。

Tx Delay(Tx 送信遅延):
何らかの設定(IP アドレスなど)が変更された場合、新しい LLDP フレームが送信されますが、LLDP フレーム間の時間は常に少なくとも、この「Tx Delay」(Tx 送信遅延)の秒数になります。「Tx Delay」(Tx 送信遅延)は、「Tx Interval」(Tx 送信間隔)の値の 1/4 より大きくすることはできません。有効な値は 1～8192 秒に制限されています。

Tx Reinit(Tx 再初期化):
ポートが無効になっている場合、LLDP が無効になっている場合、またはスイッチが再起動された場合、LLDP シャットダウンフレームがネイバーユニットに送信され、LLDP 情報が無効になったことが通知されます。「Tx Reinit」(Tx 再初期化)は、シャットダウンフレームから新しい LLDP 初期化するまでの秒数を制御します。有効な値は 1～10 秒に制限されています。

LLDP Port Configuration(LLDP ポートの設定)

LLDP ポートの設定は、現在選択されているポートに関連します。これは、ページヘッダーにも反映されます。

Port(ポート):
論理 LLDP ポートのスイッチのポート番号です。

Mode(モード):
LLDP モードを次から選択してください。

Rx Only（Rx のみ）：スイッチは LLDP 情報を送信しませんが、ネイバーユニットからの LLDP 情報は分析されます。
Tx Only（Tx のみ）：スイッチはネイバーから受信した LLDP 情報を破棄しますが、LLDP 情報を送信します。
Disabled（無効）：スイッチは LLDP 情報を送信せず、ネイバーから受信した LLDP 情報を破棄します。
Enable（有効）：スイッチは LLDP 情報を送信し、ネイバーから受信した LLDP 情報を分析します。

CDP Aware（CDP 認識）：
CDP 認識を選択してください。

CDP 動作は、着信 CDP フレームのデコードに制限されます（スイッチは CDP フレームを送信しません）。CDP フレームは、ポート上の LLDP が有効になっている場合にのみデコードされます。デコードされるのは、LLDP ネイバーテーブルにおける対応フィールドにマップできる CDP TLV のみです。他のすべての TLV は破棄されます（認識されない CDP TLV と破棄された CDP フレームは LLDP 統計に表示されません）。CDP TLV は、次のように LLDP ネイバーのテーブルにマッピングされます。

CDP TLV の「Device ID」（デバイス ID）は、LLDP の「Chassis ID」（シャーシ ID）項目にマッピングされます。

CDP TLV の「Address」（アドレス）は、LLDP の「Management Address」（管理アドレス）項目にマッピングされます。CDP TLV の「Address」（アドレス）には複数のアドレスを含めることができますが、LLDP ネイバーのテーブルには最初のアドレスのみが表示されます。

CDP TLV の「Port ID」（ポート ID）は、LLDP の「Port ID」（ポート ID）項目にマッピングされます。

CDP TLV の「Version and Platform」（バージョンおよびプラットフォーム）は、LLDP の「System Description」（システムの説明）項目にマッピングされます。

CDP と LLDP の両方ともシステム機能をサポートしますが、CDP 機能は LLDP の一部にはない機能もカバーしています。これらの機能は、LLDP ネイバーテーブルに「others」（その他）として表示されます。

すべてのポートで CDP 認識が無効になっている場合、スイッチはネイバーデバイスから受信した CDP フレームを転送します。少なくとも 1 つのポートで CDP 認識が有効になっている場合、すべての CDP フレームがスイッチによって終了されます。

注意: CDP 情報は、ポートの CDP 認識が無効になっている場合は、すぐに削除されませんが、保留時間を超えた場合に取得されます。

Trap(トラップ):
LLDP トラップは、新たに検出されたネイバーデバイスやリンクの誤動作などのイベントを通知します。

Port Descr(ポートの説明):
Optional TLV(オプションの TLV):LLDP トラップは、新たに検出されたネイバーデバイスやリンクの誤動作などのイベントを通知します。チェックボックスを ON にすると、送信される LLDP 情報に、ポートの説明が含まれます。

Sys Name(システム名):
Optional TLV(オプションの TLV):チェックボックスを ON にすると、送信される LLDP 情報に、システム名が含まれます。

Sys Descr(システムの説明):
Optional TLV(オプションの TLV):チェックボックスを ON にすると、送信される LLDP 情報に、システムの説明が含まれます。

Sys Capa(システムの容量):
Optional TLV(オプションの TLV):チェックボックスを ON にすると、送信される LLDP 情報に、システム機能が含まれます。

Mgmt Addr(管理アドレス):
Optional TLV(オプションの TLV):チェックボックスを ON にすると、送信される LLDP 情報に、管理アドレスが含まれます。

■ボタン

Apply(適用):
クリックすると、変更内容を保存します。

Reset（リセット）：
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

LLDP-MED の設定

メディアエンドポイント探索とは、LLDP-MED と呼ばれる LLDP の拡張機能であり、以下の機能を提供します。

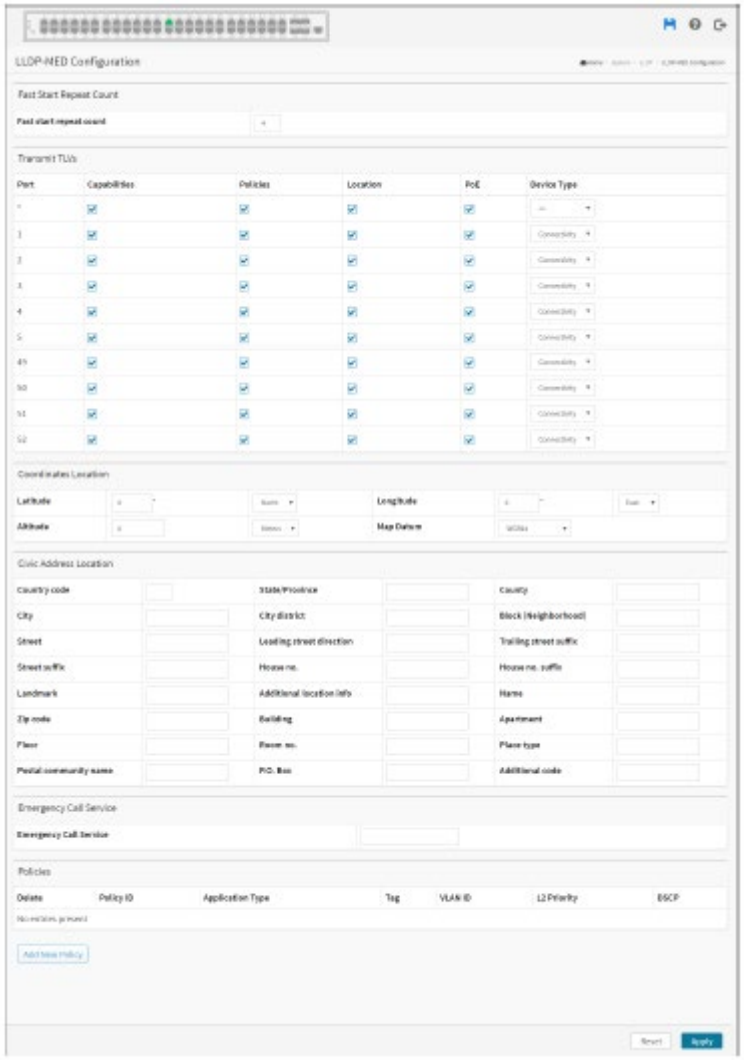
- プラグアンドプレイ・ネットワークを有効にする LAN ポリシー（VLAN、レイヤ 2 優先、Diffserv（Differentiated Services）設定など）の自動検出。

- ロケーションデータベースの作成を可能にするデバイスロケーションの検出、および VoIP（Voice over Internet Protocol）の場合は拡張 911 サービス。

- Power over Ethernet（PoE）エンドポイントの拡張および自動電源管理。

- インベントリ管理。ネットワーク管理者は、ネットワークデバイスを追跡し、その特性（製造元、ソフトウェアおよびハードウェアのバージョン、シリアル番号またはアセット番号）を確認可能。

この画面では、LLDP-MED を設定できます。この機能は、LLDP-MED をサポートする VoIP デバイスに適用されます。



Web インターフェース

LLDP-MED を設定するには:

1. 「System」(システム) ＞ 「LLDP」 ＞ 「LLDP-MED Configuration」(LLDP-MED 設定)をクリックしてください。
2. 「Fast Start Repeat Count」(ファストスタート再実行回数)のパラメーターを変更してください(デフォルトは 4)。
3. 「Transmit TLVs」(TLV の転送)パラメーターを変更してください。
4. 「Coordinates Location」(座標位置)パラメーターを変更してください。
5. 「Civic Address」(住所)パラメーターを入力してください。
6. 「Emergency Call Service」(緊急通報サービス)のパラメーターを入力してください。
7. 新規ポリシーを追加してください。
8. 「Apply」(適用)をクリックしてください。そうすると、引き続いて、「Policy Port Configuration」(ポリシーのポート設定)が表示されます。

9. 各ポートに対して、「Policy ID」(ポリシーID)を選択してください。
10. 「Apply」(適用)をクリックしてください。

■パラメーターの説明

Fast Start Repeat Count(ファストスタート再実行回数)

エンドポイントの迅速な起動、および緊急通報サービスの位置識別検出は、概して、VoIP システムの非常に重要な側面です。これに加えて、限られた LLDPU 領域を節約し、ネットワークポリシーの不適切な知識に起因するセキュリティおよびシステム整合性の問題を低減できるよう、特定のエンドポイントタイプに特に関連する情報(例:音声ネットワークポリシーのみを許可された音声対応デバイスに通知)のみを通知することを推奨します。

このことを念頭において、LLDP-MED は、これらの関連する特性を達成するために、プロトコルとプロトコル上のアプリケーション層との間の LLDP-MED ファストスタートの相互作用を定義します。初期状態では、ネットワーク接続デバイスはLLDPDU内のLLDP TLVのみを送信します。LLDP-MED 対応ネットワーク接続デバイスは、LLDP-MED エンドポイントデバイスが検出された後に初めて、関連するポート上の発信LLDPDUでLLDP-MED TLVを通知します。LLDP-MED アプリケーションは、新規 LLDP-MED ネイバーが検出されたとき、その新規ネイバーとできるだけ早く LLDPMED 情報を共有するために、LLDPDU の伝送を 1 秒以内に開始できるよう、一時的にスピードアップします。

ネイバー間の伝送中に LLDP フレームが失われる危険性があるため、ネイバーが LLDP フレームを受信する可能性を高められるよう、ファストスタート伝送を複数回繰り返すことを推奨します。ファストスタート再実行回数では、ファストスタート送信を繰り返す回数を指定することができます。新しい情報を持つLLDPフレームを受信した場合、1秒間隔で4つのLLDPフレームが送信されるため、推奨値は 4 回です。

なお、LLDP-MED および LLDP-MED ファストスタートのメカニズムは、LLDP-MED ネットワーク接続デバイスとエンドポイントデバイスの間のリンクでのみ実行することを意図しており、ネットワーク接続デバイスやその他のタイプのリンクを含む LAN インフラストラクチャー要素間のリンクには適用されません。

Transmit TLVs(送信 TLV)

Port(ポート):
設定が適用されるインターフェース名です。

Capabilities(機能):

チェックボックスを ON にすると、送信される LLDP-MED 情報にスイッチの機能が含まれるようになります。

Policies（ポリシー）:
チェックボックスを ON にすると、インターフェースに設定されたポリシーが、送信される LLDP-MED 情報に含まれるようになります。

Location（場所）:
チェックボックスを ON にすると、スイッチに対して設定された場所情報が、送信される LLDP-MED 情報に含まれるようになります。

PoE:
チェックボックスを ON にすると、送信される LLDP-MED 情報にインターフェースの設定済み PoE（Power Over Ethernet）情報が含まれるようになります。

Device Type（デバイスタイプ）:
任意の LLDP-MED 装置は、特定のタイプの LLDP-MED 装置として動作します。これは、以下に定義されるように、ネットワーク接続装置、または特定のクラスのエンドポイント装置のいずれかになります。

ネットワーク接続デバイスは、LLDP-MED エンドポイントデバイスの IEEE802 ベースの LAN インフラストラクチャーへのアクセスを提供する LLDP-MED デバイスです。

LLDP-MED ネットワーク接続デバイスは、次のいずれかのテクノロジーに基づく LAN 対応デバイスです。

1. LAN スイッチ/ルーター
2. IEEE802.1 ブリッジ
3. IEEE802.3 リピーター（歴史的経緯により追加）
4. IEEE802.11 ワイヤレスアクセスポイント
5. IEEE802 フレームを任意の方法で中継できる IEEE802.1AB および MED 拡張に対応したデバイス

エンドポイントデバイスとは、ネットワークエッジに配置され、IEEE802 LAN テクノロジーに基づいて IP 通信サービスの一部の側面を提供する LLDP-MED デバイスです。

ネットワーク接続デバイスとエンドポイントデバイスの主な違いは、エンドポイントデバイスのみ

が LLDP-MED 情報交換を開始できるという点です。

スイッチは常にネットワーク接続デバイスである必要がありますが、エンドポイントデバイスとして動作するように設定してLLDP-MED 情報交換を開始することができます(2 台のネットワーク接続デバイスが接続されている場合)。

Coordinate Location(座標位置)

Latitude(緯度):

緯度は、最大 4 桁で 0～90 度以内に標準化してください。

方向は、赤道の北または南のどちらかに指定することができます。

Longitude(経度):

経度は、最大 5 桁で 0～180 度以内で標準化してください。

本初子午線の東側と西側のどちらに向かうかを指定することができます。

Altitude(高度):

高度は、最大 4 桁で-32767～32767 以内に標準化してください。

高度は、次の 2 種類(階またはメートル)から選択できます。

Meters(メーター):指定された垂直データによって定義された高度のメーター数を表します。

Floors(階):階と階の寸法が異なる建物では、高度をより適切な形式で表します。高度=0.0 は、建物の外でも意味があり、与えられた緯度と経度での地面レベルを表します。建物内において、0.0 は正面玄関の 1 階の地表面を表します。

Map Datum(地図データ):

地図データは、以下のオプションで指定された座標に使用されます。

WGS84:(地理的 3D)世界測地系(World Geodetic System)1984、CRS コード 4327、本初子午線名:グリニッジ

NAD83/NAVD88:北米測地系(North American Datum)1983、CRS コード 4269、本初子午線名:グリニッジ。関連する垂直データは、「NorthAmerican Vertical Datum of 1988 (NAVD88)」です。この対データは、陸上で、潮汐水(データ=NAD83/MLLW を使用)に近い場所を参照する場合に使用します。

NAD83/MLLW:北米測地系(North American Datum)1983、CRS コード 4269、本初子午線名:グリニッジ。関連する垂直データは、「Mean Lower Lower Water(MLLW)」です。この対データは、水/海/海上の位置を参照する場合に使用します。

Civic Address Location（住所）
位置情報（住所 LCI）に基づいた IETF Geopriv 住所です。

Country Code（国番号）：
大文字 ASCII 文字の 2 文字 ISO3166 国コードです（例：DK、DE、または US）。

State/Province（都道府県）：
国の下位区分（州、都道府県、地域）です。

County（国）：
国、区分、郡（日本）、地区です。

City（市）：
市区町村、市（日本）です（例：コペンハーゲン）。

City district（市区町村）：
市、区、町（日本）です。

Block (neighborhood)（街区（近隣））：
近隣、街区です。

Street（番地）：
通り（例：ポペルベイ）です。

Leading street direction（町名番地に付与される方角）：
町名番地に付与される方角です（例：N）。

Trailing street suffix（後に続く町名番地のサフィックス）：
後に続く町名番地のサフィックスです（例：SW）。

Street suffix（住所のサフィックス）：
住所のサフィックスです（例：Ave、Platz）。

House no.（住居番号）：
住居番号です（例：21）。

House number suffix（住居番号のサフィックス）：
住居番号のサフィックス（例：A、1/2）。

Landmark（目印）：
目印またはバニティアドレスです（例：コロンビア大学）。

Additional location info（その他の位置情報）：
追加の場所情報です（例：South Wing）。

Name（名前）：
住居やオフィスの利用者の名前です（例：Flemming Jahn）。

Zip code（郵便番号）：
郵便番号です（例：2791）。

Building（建物）：
建物（構造）です（例：Low Library）。

Apartment（アパート）：
ユニット（アパート、スイート）です（例：Apt42）。

Floor（階数）：
階数です（例：4）。

Room no.（部屋番号）：
部屋番号です（例：450F）。

Place type（配置タイプ）：
配置タイプです（例：オフィス）。

Postal community name（郵便コミュニティ名）：
郵便コミュニティ名です（例：Leonia）。

P.O. Box（私書箱）：
私書箱の番号です（例：12345）。

Additional code（追加コード）:
追加コードです（例:1320300003）。

Emergency Call Service（緊急通報サービス）:
緊急通報サービスです（E911 など）。TIA や NENA で定義されています。

Emergency Call Service（緊急通報サービス）:
緊急通報サービスの ELIN 識別子のデータ形式は、緊急通報の設定時に使用される ELIN 識別子を従来の CAMA または ISDN トランクベースの PSAP に伝送するように定義されています。この形式は、緊急呼び出しに使用される ELIN に対応する数字の文字列で構成されます。

Policies（ポリシー）

ネットワークポリシー検出を使用すると、関連付けられたレイヤ 2 およびレイヤ 3 属性とともに、VLAN 設定での不一致の問題を効率的に検出したり診断したりすることができます。これらの属性は、そのポート上において、特定のプロトコルアプリケーションの一連に適用されます。VoIP 環境では、不適切なネットワークポリシー設定が非常に重大な問題となり、音声品質の低下やサービスの喪失が頻繁に発生します。

ポリシーは、インタラクティブな音声サービスやビデオサービスなど、特定の「リアルタイム」ネットワークポリシー要件を持つアプリケーションでのみ使用することを目的としています。

通知されるネットワークポリシー属性は次のとおりです。

1. レイヤ 2 VLAN ID（IEEE802.1Q-2003）
2. レイヤ 2 プライオリティ値（IEEE802.1D-2004）
3. レイヤ 3 Diffserv コードポイント（DSCP）値（IETF RFC2474）

このネットワークポリシーは、通知される可能性があり、特定のポートでサポートされている複数のアプリケーションタイプの設定に関連付けられています。特に対象となるアプリケーションタイプは以下のとおりです。

1. 音声
2. ゲストボイス
3. ソフトフォンボイス
4. ビデオ会議
5. ストリーミングビデオ
6. 制御/信号伝達（前述のメディアタイプに対して個別のネットワークポリシーを条件付きでサポート）

大規模なネットワークでは、組織全体で複数の VoIP ポリシーがサポートされ、アプリケーションタイプごとに異なるポリシーがサポートされる場合があります。LLDP-MED では、ポートごとに複数のポリシーを通知できます。各ポリシーは、異なるアプリケーションタイプに対応しています。同じネットワーク接続デバイス上の別ポートは、認証されたユーザーID またはポート設定に基づいて、異なる一連のポリシーを通知する場合があります。

LLDP-MED は、ネットワーク接続デバイスとエンドポイント間以外のリンク上で動作することを意図していないため、LAN の集約されたリンク内部で頻繁に実行される多数のネットワークポリシーを通知する必要がないことに注意してください。

Delete（削除）:
チェックボックスを ON にすると、ポリシーが削除されます。削除処理は、次回保存時に実行されます。

Policy ID（ポリシーID）:
ポリシーの ID です。これは自動生成された ID で、特定のポートにマッピングするポリシーを選択するときに使用されます。

Application Type（アプリケーションタイプ）:
アプリケーションタイプの使用目的は次のとおりです。

1. 音声 – 専用の IP テレフォニー端末や、インタラクティブな音声サービスをサポートするその他の類似機器で使用します。通常、これらのデバイスは、デプロイを容易にし、データアプリケーションから分離することでセキュリティを強化するために、個別の VLAN にデプロイされます。
2. 音声信号（条件付き）– 音声メディアとは異なるポリシーを音声信号に必要とするネットワークトポロジーで使用します。すべての同じネットワークポリシーが、音声アプリケーションポリシーで通知されたポリシーとして適用される場合は、このアプリケーションタイプを通知しないでください。
3. ゲストボイス – ゲストユーザーと訪問者に対して、独自の IP テレフォニー端末や、インタラクティブボイスサービスをサポートするその他の類似アプライアンスを備えた個別の「機能設定」ボイスサービスをサポートします。
4. ゲスト音声シグナリング（条件付き）– ゲスト音声信号伝達にゲスト音声信号伝達とは異なるポリシーを必要とするネットワークトポロジーで使用します。すべての同じネットワークポリシーがゲストボイスアプリケーションポリシーで通知されたポリシーと適用される場合は、この

アプリケーションタイプを通知しないでください。

5. ソフトフォン音声 – PC やノートパソコンなどの一般的なデータ中心型デバイスで、ソフトフォンアプリケーションによって使用されます。このクラスのエンドポイントは、複数の VLAN をサポートしていない場合が多く、通常、「タグなし」VLAN または単一の「タグ付き」データ固有 VLAN を使用するように設定されています。「タグなし」VLAN で使用するためにネットワークポリシーが定義されている場合（下記の「タグ付き」フラグを参照）、L2 プライオリティフィールドは無視され、DSCP 値のみに関連性があります。
6. ビデオ会議 – 専用のビデオ会議装置や、リアルタイムのインタラクティブなビデオ/オーディオサービスをサポートするその他の類似アプライアンスで使用します。
7. ストリーミングビデオ – 特定のネットワークポリシー処理を必要とするストリーミングビデオサービスをサポートする、ブロードキャストベースまたはマルチキャストベースのビデオコンテンツ配信およびその他の類似アプリケーションで使用します。TCP に依存するビデオアプリケーションでバッファリング機能を持つものは、このアプリケーションタイプの意図された用途ではありません。
8. ビデオ信号伝達（条件付き） – ビデオメディアとは別のビデオ信号方式を必要とするネットワークトポロジーで使用します。すべての同じネットワークポリシーがビデオ会議アプリケーションポリシーで通知されたポリシーと適用される場合は、このアプリケーションタイプを通知しないでください。

Tag（タグ）：

指定されたアプリケーションタイプが「タグ付き」VLAN または「タグなし」VLAN のどちらを使用しているかを示すタグです。

「タグなし」は、デバイスがタグなしフレーム形式を使用しており、IEEE802.1Q-2003 で定義されているタグヘッダーが含まれていないことを示します。この場合、VLAN ID とレイヤ 2 プライオリティフィールドの両方が無視され、DSCP 値のみが関連性を持ちます。

「タグ付き」は、デバイスが IEEE802.1Q タグ付きフレーム形式を使用していること、および VLAN ID とレイヤ 2 プライオリティ値の両方が使用されていること、および DSCP 値が使用されていることを示します。タグ付きフォーマットは、タグヘッダーとして知られる追加フィールドを含みます。タグ付きフレームフォーマットには、IEEE802.1Q-2003 によって定義された優先順位タグ付きフレームも含まれます。

VLAN ID：

IEEE802.1Q-2003 で定義されているポートの VLAN 識別子（VID）です。

L2 Priority（L2 プライオリティ）：

L2 プライオリティは、指定されたアプリケーションタイプに使用されるレイヤ 2 プライオリティです。

L2 プライオリティは、第 3 章で定義されている 8 段階のプライオリティレベル（0～7）のいずれかを指定できます。値 0 は、IEEE802.1D-2004 で定義されているデフォルトのプライオリティの使用を表します。

DSCP:
IETF RFC2474 で定義されている指定されたアプリケーションタイプの Diffserv ノード動作を提供するために使用される DSCP 値です。DSCP には、64 個のコードポイント値（0～63）のいずれかを含めることができます。値 0 は、RFC2475 で定義されているデフォルトの DSCP 値の使用を表します。

Port Policies Configuration（ポートポリシーの設定）:
すべてのポートは、認証されたユーザーID またはポート設定に基づいて、同じネットワークポリシーに対して一意のネットワークポリシーまたは異なる一連の属性を通知できます。

Port（ポート）:
設定が適用されるポート番号です。

Policy ID（ポリシーID）:
特定のポートに適用される一連のポリシーです。ポリシーの設定を選択するには、ポリシーに対応するチェックボックスを ON にします。

■ボタン

Adding New Policy（新規ポリシーの追加）:
クリックすると、新規ポリシーを追加します。新規ポリシーのアプリケーションタイプ、タグ、VLAN ID、L2 プライオリティ、および DSCP を指定します。そうしたら、「Apply」（適用）をクリックしてください。

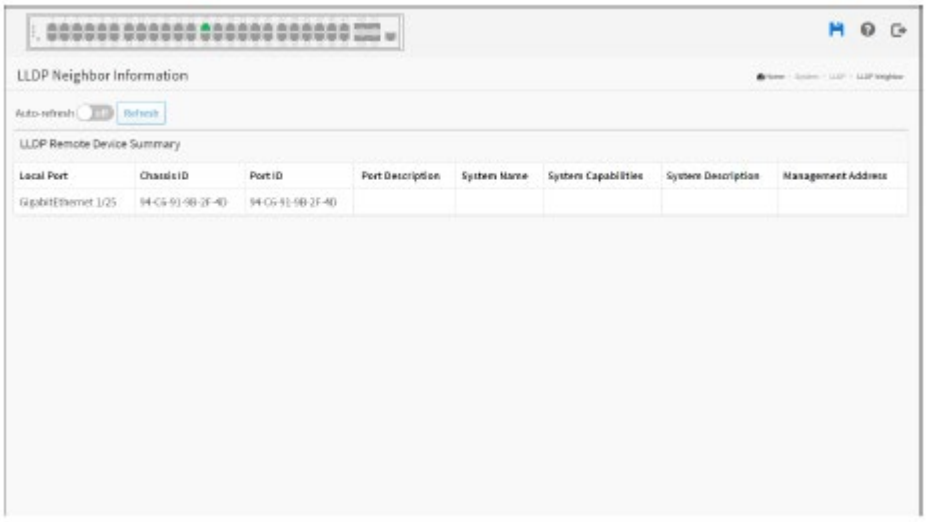
Apply（適用）:
クリックすると、変更内容を保存します。

Reset（リセット）:
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

LLDP ネイバー

このページには、すべての LLDP ネイバーの状態の概要が表示されます。表示されるテーブ

ルには、LLDP ネイバーが検出された各ポートの行が含まれます。列には、以下の情報が含まれています。



Web インターフェース

LLDP ネイバーを表示するには:

1. 「System」(システム) ＞ 「LLDP」 ＞ 「LLDP Neighbor」(LLDP ネイバー)をクリックしてください。
2. Web 画面を手動で更新する場合は、「Refresh」(更新)をクリックしてください。
3. Web 画面を自動更新する場合は、「Auto-refresh」(自動更新)をクリックしてください。

注意: ネットワークに LLDP をサポートするデバイスがない場合、テーブルには「No LLDP neighbor information found」(LLDP ネイバーの情報がありません)と表示されます。

■パラメーターの説明

Local Port(ローカルポート):

LLDP フレームを受信したポートです。

Chassis ID(シャーシ ID):

シャーシ ID は、ネイバーの LLDP フレームの識別情報です。

Port ID(ポート ID):

リモートポート ID は、ネイバーポートの識別情報です。

Port Description(ポートの説明):

ポートの説明は、ネイバーユニットによって通知されるポートの説明です。

System Name（システム名）：
システム名は、ネイバーユニットによって通知される名前です。

System Capabilities（システム機能）：
システム機能は、ネイバーユニットの機能を説明します。可能な機能は次のとおりです。

1. その他
2. リピーター
3. ブリッジ
4. 無線 LAN アクセスポイント
5. ルーター
6. 電話
7. DOCSIS ケーブルデバイス
8. ステーションのみ
9. 予約済み

機能が有効になっている場合、その機能の後に(+)が続きます。機能が無効になっている場合、その機能の後に(-)が続きます。

System Description（システムの説明）：
システムの説明を表示します。

Management Address（管理アドレス）：
管理アドレスは、ネットワーク管理による検出を支援する上位レイヤのエンティティに使用されるネイバーユニットのアドレスです。例えば、これは近隣の IP アドレスを保持する場合もあります。

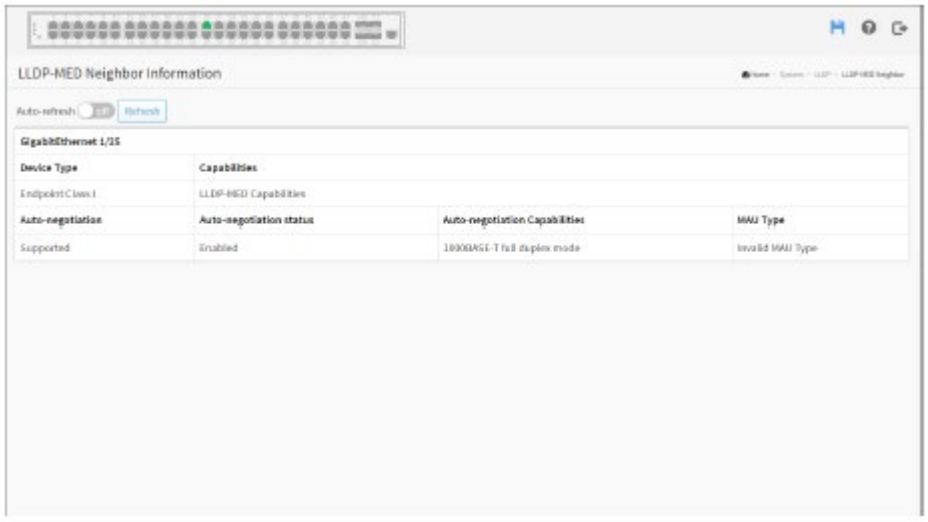
■ボタン

Auto-refresh（自動更新）：
画面を自動的に更新する場合は、このチェックボックスを ON にしてください。自動更新は 3 秒間隔で行われます。

Refresh（更新）：
クリックすると、画面がすぐに更新されます。

LLDP-MED ネイバー

この画面には、すべての LLDP-MED ネイバーの状態の概要が表示されます。表示されるテーブルには、LLDP ネイバーが検出された各ポートの行が含まれます。この機能は、LLDP-MED をサポートする VoIP デバイスに適用されます。列には、以下の情報が含まれています。



Web インターフェース

LLDP-MED ネイバーを表示するには:

1. 「System」(システム) ＞ 「LLDP」 ＞ 「LLDP Neighbor」(LLDP ネイバー)をクリックしてください。
2. Web 画面を手動で更新する場合は、「Refresh」(更新)をクリックしてください。
3. Web 画面を自動更新する場合は、「Auto-refresh」(自動更新)をクリックしてください。

■パラメーターの説明

Port (ポート) :

LLDP フレームを受信したポートです。

Device Type (デバイスタイプ) :

LLDP-MED デバイスは、2 種類のプライマリーデバイスタイプ (ネットワーク接続デバイスとエンドポイントデバイス)から構成されます。

◆ LLDP-MED Network Connectivity Device Definition (LLDP-MED ネットワーク接続デバイス定義)

LLDP-MED ネットワーク接続デバイスは、TIA-1057 で定義されているとおり、LLDP-MED

エンドポイントデバイスに対して、IEEE802 ベースの LAN インフラへのアクセスを提供します。
LLDP-MED ネットワーク接続デバイスは、次のいずれかのテクノロジーに基づく LAN 対応デバイスです。

1. LAN スイッチ/ルーター
2. IEEE802.1 ブリッジ
3. IEEE802.3 リピーター（歴史的経緯により追加）
4. IEEE802.11 ワイヤレスアクセスポイント
   TIA-1057 で定義された IEEE802.1AB および MED 拡張をサポートし、任意の方法で IEEE802 フレームを中継できるデバイス

◆ LLDP-MED Endpoint Device Definition（LLDP-MED エンドポイントデバイス定義）
LLDP-MED エンドポイントデバイスは、TIA-1057 で定義されているように、IEEE802LAN ネットワークエッジに配置され、LLDP-MED フレームワークを使用して IP 通信サービスに参加します。
LLDP-MED エンドポイントデバイスのカテゴリー内で、LLDP-MED スキームは、次の中で定義されるように、さらなるエンドポイントデバイスクラスに分割されます。
各 LLDP-MED エンドポイントデバイスのクラスは、前のエンドポイント装置クラスのために定義された性能に基づいて構築されるように定義されます。例えば、メディアエンドポイント（クラスⅡ）としての準拠していることを謳っている、すべての LLDP-MED エンドポイントデバイスは、汎用エンドポイント（クラスⅠ）に適用される TIA-1057 のすべての側面をサポートし、通信デバイス（クラスⅢ）として準拠していることを謳っている、すべての LLDP-MED エンドポイントデバイスは、メディアエンドポイント（クラスⅡ）と汎用エンドポイント（クラスⅠ）の両方に適用される TIA-1057 のすべての側面もサポートします。

◆ LLDP-MED Generic Endpoint (Class I)（LLDP-MED 汎用エンドポイント（クラスⅠ））:
LLDP-MED 汎用エンドポイント（クラスⅠ）定義は、TIA-1057 で定義されているベース LLDP 検出サービスを必要とするすべてのエンドポイント製品に適用できますが、IP メディアをサポートしないか、エンドユーザー通信アプライアンスとして機能しません。このようなデバイスには、IP 通信コントローラー、他の通信関連サーバー、または TIA-1057 で定義されている基本的なサービスを必要とするデバイスが含まれます（ただし、これらに限定されません）。
このクラスで定義されるディスカバリー・サービスには、LAN 構成、装置の場所、ネットワークポリシー、電源管理、およびインベントリ管理が含まれます。

◆ LLDP-MED Media Endpoint (Class II)（LLDP-MED メディアエンドポイント（クラスⅡ））:
LLDP-MED メディアエンドポイント（クラスⅡ）定義は、IP メディア機能を持つすべてのエン

ドポイント製品に適用できますが、特定のエンドユーザーに関連付けられているものと関連付けられていないものがあります。機能には、以前の汎用エンドポイントクラス（クラスⅠ）で定義されたすべての機能が含まれ、メディア・ストリーミングに関連する側面を含めるように拡張されています。

このクラスに準拠することが期待される製品カテゴリーには、音声/メディアゲートウェイ、会議ブリッジ、メディアサーバーなどがあります（これらに限定されません）。このクラスで定義されたディスカバリー・サービスには、メディアタイプ固有のネットワークレイヤポリシー検出が含まれます。

◆ LLDP-MED Communication Endpoint (Class III)（LLDP-MED メディアエンドポイント（クラスⅡ））:

LLDP-MED 通信エンドポイント（クラスⅢ）の定義は、IP メディアをサポートするエンドユーザー通信アプライアンスとして機能するすべてのエンドポイント製品に適用されます。機能には、以前のジェネリック・エンドポイント（クラスⅠ）クラスおよびメディア・エンドポイント（クラスⅡ）クラスで定義されたすべての機能が含まれ、エンドユーザーデバイスに関連する側面を含めるように拡張されています。このクラスに準拠することが期待される製品カテゴリーの例には、IP 電話、PC ベースのソフトフォン、またはエンドユーザーを直接サポートするその他の通信装置などのエンドユーザー通信装置が含まれます（ただし、これらに限定されません）。

このクラスで定義されるディスカバリー・サービスには、ロケーション識別子（ECS/E911 情報を含む）の提供、組み込み L2 スイッチのサポート、インベントリ管理が含まれます。

LLDP-MED Capabilities（LLDP-MED 機能）:

LLDP-MED 機能は、ネイバーユニットの LLDP-MED 機能を説明します。可能な機能は次のとおりです。

1. LLDP-MED 機能
2. ネットワークポリシー
3. 場所の識別
4. MDI を介した拡張電源 - PSE
5. MDI を介した拡張電源 - PD
6. インベントリ
7. 予約済み

Application Type（アプリケーションタイプ）:

エンドポイントまたはネットワーク接続デバイスによって通知される、このネットワークポリシーに定義されたアプリケーションの主要機能を示すアプリケーションタイプです。使用可能なアプリケー

ションの種類は次のとおりです。

1. 音声 – 専用の IP テレフォニー端末や、インタラクティブな音声サービスをサポートするその他の類似機器で使用します。通常、これらのデバイスは、デプロイを容易にし、データアプリケーションから分離することでセキュリティを強化するために、個別の VLAN にデプロイされます。
2. 音声信号 – 音声メディアとは異なるポリシーを音声信号に必要とするネットワークトポロジーで使用します。
3. ゲストボイス – ゲストユーザーと訪問者に対して、独自の IP テレフォニー端末や、インタラクティブボイスサービスをサポートするその他の類似アプライアンスを備えた個別の機能設定ボイスサービスをサポートします。
4. ゲスト音声信号 – ゲスト音声信号伝達にゲスト音声信号伝達とは異なるポリシーを必要とするネットワークトポロジーで使用します。
5. ソフトフォン音声 – PC やノートパソコンなどの一般的なデータ中心型デバイスで、ソフトフォンアプリケーションによって使用されます。
6. ビデオ会議 – 専用のビデオ会議装置や、リアルタイムのインタラクティブなビデオ/オーディオサービスをサポートするその他の類似アプライアンスで使用します。
7. ストリーミングビデオ – 特定のネットワークポリシー処理を必要とするストリーミングビデオサービスをサポートする、ブロードキャストベースまたはマルチキャストベースのビデオコンテンツ配信およびその他の類似アプリケーションで使用します。TCP に依存するビデオアプリケーションでバッファリング機能を持つものは、このアプリケーションタイプの意図された用途ではありません。
8. ビデオ信号伝達 – ビデオメディアとは別のビデオ信号方式を必要とするネットワークトポロジーで使用します。

Policy(ポリシー):

ポリシーは、ポリシーがデバイスに必要であることをエンドポイントデバイスが明示的に通知することを示します。これは、「Defined」(定義済み)または「Unknown」(不明)のいずれかになります。

Unknown(不明):指定されたアプリケーションタイプのネットワークポリシーが現在不明です。

Defined(定義済み):ネットワークポリシーが定義されています。

TAG(タグ):

タグは、指定されたアプリケーションタイプがタグ付き VLAN とタグなし VLAN のどちらを使用しているかを示します。これは、「Tagged」(タグ付き)または「Untagged」(タグなし)のいずれかになります。

Untagged（タグなし）：デバイスはタグなしフレーム形式を使用しており、IEEE802.1Q-2003で定義されているタグヘッダーは含まれていません。
Tagged（タグ付き）：デバイスは IEEE802.1Q タグ付きフレーム形式を使用しています。

VLAN ID：
IEEE802.1Q-2003 で定義されているポートの VLAN 識別子（VID）です。1～4094 の値を使用して、有効な VLAN ID を定義します。デバイスが IEEE802.1Q-2003 で定義されている優先順位のタグ付きフレームを使用している場合は、値 0（Priority Tagged）が使用されます。つまり、IEEE802.1D プライオリティレベルのみが重要で、代わりに入力ポートのデフォルト PVID が使用されます。

Priority（優先度）：
優先度は、指定されたアプリケーションタイプに使用されるレイヤ 2 プライオリティです。8 段階の優先順位レベル（0～7）のいずれかになります。

DSCP：
IETF RFC2474 で定義されている指定されたアプリケーションタイプの Diffserv ノード動作を提供するために使用される DSCP 値です。64 個のコードポイント値（0～63）のいずれかを含みます。

Auto-negotiation（オートネゴシエーション）：
オートネゴシエーションは、リンクパートナーが MAC/PHY オートネゴシエーションをサポートしているかどうかを識別します。

Auto-negotiation status（オートネゴシエーションの状態）：
オートネゴシエーションの状態は、リンクパートナーでオートネゴシエーションが現在有効になっているかどうかを識別します。オートネゴシエーションがサポートされていて、オートネゴシエーションの状態が無効になっている場合、802.3PMD 操作モードは、オートネゴシエーションではなく、動作 MAU タイプのフィールド値を決定します。

Auto-negotiation Capabilities（オートネゴシエーション機能）：
オートネゴシエーション機能には、リンクパートナーの MAC/PHY 機能が表示されます。

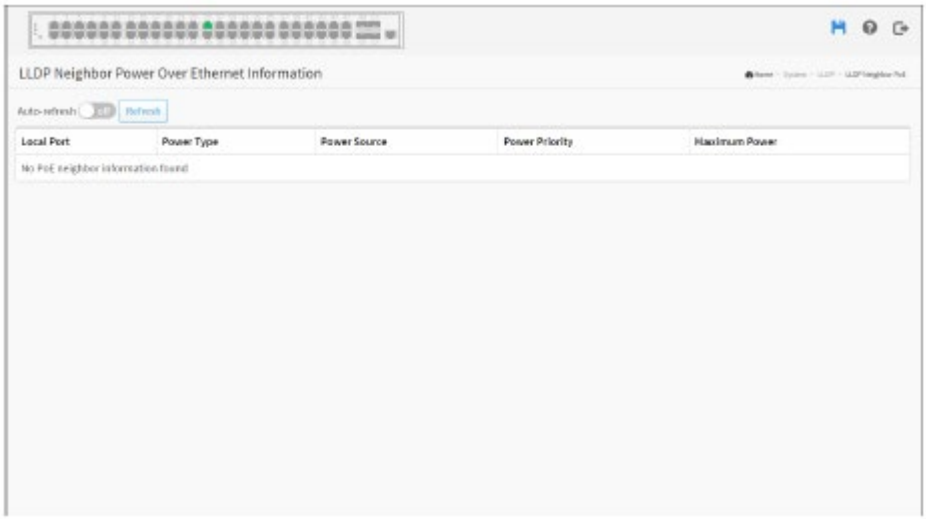
■ボタン

Auto-refresh（自動更新）:
画面を自動的に更新する場合は、このチェックボックスをONにしてください。自動更新は3秒間隔で行われます。

Refresh（更新）:
クリックすると、画面がすぐに更新されます。

LLDP ネイバーPoE

この画面には、すべての LLDP PoE ネイバーの状態の概要が表示されます。表示される表には、LLDP PoE ネイバーが検出された各インターフェースの行が含まれます。列には、以下の情報が含まれています。



Web インターフェース

LLDP ネイバーPoE を表示するには:

1. 「System」(システム) ＞ 「LLDP」 ＞ 「LLDP Neighbor PoE」(LLDP ネイバーPoE)をクリックしてください。
2. Web 画面を手動で更新する場合は、「Refresh」(更新)をクリックしてください。
3. Web 画面を自動更新する場合は、「Auto-refresh」(自動更新)をクリックしてください。

■パラメーターの説明

Local Port(ローカルポート):

LLDP フレームを受信したスイッチのインターフェースです。

Power Type(電源タイプ):

電源タイプは、デバイスが「PSE」(Power Sourcing Entity)か「PD」(Power Device)かを表します。電源タイプが不明な場合は、「Reserved」(予約済み)と表示されます。

Power Source(電源):

電源は、PSE または PD デバイスで使用されている電源を表します。

デバイスが PSE デバイスの場合は、プライマリ電源またはバックアップ電源で実行できます。PSE デバイスがプライマリ電源またはバックアップ電源のどちらを使用しているかが不明な場合は、「Unknown」（不明）と表示されます。
デバイスが PD デバイスの場合は、ローカル電源で実行するか、PSE を電源として使用できます。ローカル電源と PSE の両方を使用することもできます。
PD デバイスがどの電源を使用しているかが不明な場合は、「Unknown」（不明）と表示されます。

Power Priority（電源優先度）：
電源優先度は、PD デバイスのプライオリティ、または電源を供給している PSE タイプデバイスのインターフェースに関連付けられている電源プライオリティを表します。電源の優先度には、重要、高、低の 3 つのレベルがあります。
電力優先度が不明な場合は、「Unknown」（不明）と表示されます。

Maximum Power（最大電力値）：
最大電力値には、PSE デバイスからの PD デバイスに必要な最大電力（ワット単位）、または PSE デバイスが現在の構成に基づいて最大長ケーブルを介して供給できる最小電力を示す数値が含まれます。
最大許容値は 102.3W です。デバイスが 102.3W より大きい値を示す場合、「Reserved」（予約済み）と表示されます。

■ボタン

Auto-refresh（自動更新）：
画面を自動的に更新する場合は、このチェックボックスを ON にしてください。自動更新は 3 秒間隔で行われます。

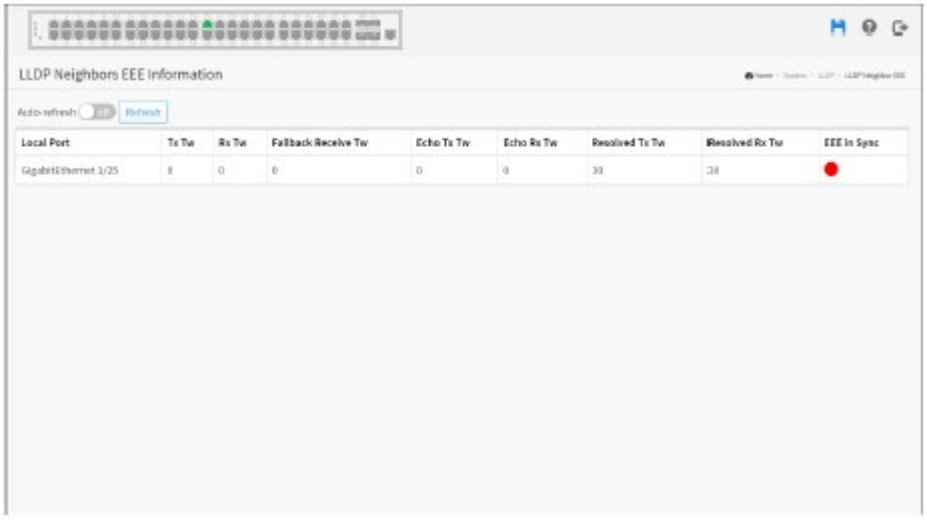
Refresh（更新）：
クリックすると、画面がすぐに更新されます。

LLDP ネイバーEEE

EEE を使用することで、トラフィック遅延を犠牲にして、電力節約を実現することができます。この遅延は、リンクを介してトラフィックを送信する前に、電力を節約し、起動する時間を必要とするために回路 EEE が OFF になることから発生します。この時間を「ウェイクアップ時間」と呼びま

す。遅延を最小限に抑えるために、デバイスは LLDP を使用して、それぞれの tx および rx のウェイクアップ時間に関する情報を交換し、必要な最小ウェイクアップ時間を合意させることができます。

このページでは、LLDP によって交換される EEE 情報の概要について説明します。



Web インターフェース

LLDP ネイバーEEE を表示するには:

1. 「System」(システム) ＞ 「LLDP」 ＞ 「LLDP Neighbor EEE」(LLDP ネイバーEEE)をクリックしてください。
2. Web 画面を手動で更新する場合は、「Refresh」(更新)をクリックしてください。
3. Web 画面を自動更新する場合は、「Auto-refresh」(自動更新)をクリックしてください。

■パラメーターの説明

Local Port(ローカルポート):

LLDP フレームが送受信されるインターフェースです。

Tx Tw(送信 Tw):

LPI のアサート停止後に、送信パスが送信データをホールドオフできるリンクパートナーの最大時間です。

Rx Tw(Rx 送信):

レシーバーが、スリープから復帰するまでの時間を許容するために、レシーバーがトランスミッターを保留にしたいリンクパートナーの時間です。

Fallback Receive Tw（フォールバック受信 Tw）：
リンクパートナーのフォールバックは Tw を受信します。
受信リンクパートナーは、Tw_sys_tx を送信者に知らせる場合があります。受信リンクパートナーは節約のために離散的なレベルを持つ可能性が高いので、これはより効率的な割り当てのために使用できる付加情報をトランスミッターに提供します。このオプションを実装していないシステムでは、既定値は Receive Tw_sys_tx と同じになります。

Echo Tx Tw（エコーTx Tw）：
リンクパートナーのエコーTx Tw 値です。それぞれのエコー値は、リモートリンクパートナーのそれぞれの値のローカルリンクパートナーリフレクション（エコー）として定義されます。ローカルリンクパートナーがリモートリンクパートナーからエコーされた値を受信すると、リモートリンクパートナーがその最新の値を受信、登録、および処理したかどうかを判断できます。例えば、ローカルリンクパートナーがローカル MIB の値と一致しないエコーパラメーターを受信した場合、ローカルリンクパートナーは、リモートリンクパートナーの要求が古い情報に基づいていると推測します。

Echo Rx Tw（エコーRx Tw）：
リンクパートナーの Echo Rx Tw 値です。

Resolved Tx Tw（解決済み Tx Tw）：
このリンクの解決された Tx Tw です。リンク先ではないことに、ご注意ください。
このリンクで使用される実際の「tx ウェイクアップ時間」（LLDP 経由で交換される EEE 情報に基づく）の解決値です。

Resolved Rx Tw（解決済み Rx Tw）：
このリンクの解決済み Rx Tw です。リンク先ではないことに、ご注意ください。
このリンクで使用される実際の「tx ウェイクアップ時間」（LLDP 経由で交換される EEE 情報に基づく）の解決値です。

EEE in Sync（同期 EEE）：
スイッチとリンクパートナーがウェイクタイムに合意したかどうかを示します。
　レッド － スイッチとリンクのパートナーがウェイクタイムに合意していません。
　グリーン － スイッチとリンクのパートナーがウェイクタイムに合意しました。

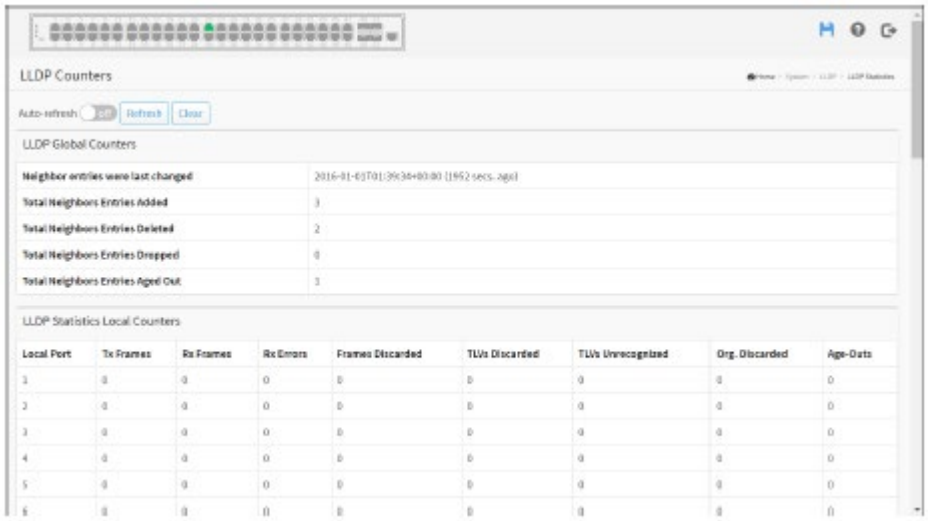
■ボタン

Auto-refresh（自動更新）:
画面を自動的に更新する場合は、このチェックボックスをONにしてください。自動更新は3秒間隔で行われます。

Refresh（更新）:
クリックすると、画面がすぐに更新されます。

LLDP 統計

2 種類のカウンターが表示されます。グローバルカウンターはスイッチ全体を参照するカウンターで、ローカルカウンターは現在選択されているスイッチのポートごとのカウンターを参照します。



Web インターフェース
LLDP 統計を表示するには:

1. 「System」（システム） ＞ 「LLDP」 ＞ 「LLDP Statistics」（LLDP 統計）をクリックしてください。
2. Web 画面を手動で更新する場合は、「Refresh」（更新）をクリックしてください。
3. Web 画面を自動更新する場合は、「Auto-refresh」（自動更新）をクリックしてください。
4. 「Clear」（消去）をクリックして、すべてのカウンターをクリアにしてください。

■パラメーターの説明

Global Counters（グローバルカウンター）

ネイバーエントリーは最後に次の場所で変更されました。
また、最後にエントリーが削除または追加された時刻も表示されます。そして、最後の変更が検出されてからの経過時間も表示されます。

Total neighbors Entries Added（追加されたネイバーの合計エントリー）:
スイッチの再起動後に追加された新しいエントリーの数が表示されます。

Total neighbors Entries Deleted（削除されたネイバーエントリーの合計）:
スイッチの再起動後に削除された新しいエントリーの数が表示されます。

Total neighbors Entries Dropped（削除されたネイバーの合計エントリー）:
エントリーテーブルが最大容量の達したことにより削除された LLDP フレームの数を示します。

Total neighbors Entries Aged Out（期限切れしたネイバーエントリーの合計）:
有効期限が切れたために削除されたエントリーの数が表示されます。

Local Counters（ローカルカウンター）
表示されるテーブルには、各ポートの行が含まれています。列には、以下の情報が含まれています。

Local Port（ローカルポート）:
LLDP フレームを受信または送信するポートです。

Tx Frames（送信フレーム）:
ポートで送信された LLDP フレームの数です。

Rx Frames（Rx フレーム）:
ポートで受信した LLDP フレームの数です。

Rx Errors（受信エラー）:
何らかのエラーを含む受信 LLDP フレームの数です。

Frames Discarded（削除されたフレーム数）:
ポートで LLDP フレームが受信され、スイッチの内部テーブルがいっぱいになると、LLDP フレームはカウントされ、破棄されます。この状況は、LLDP 規格では「多すぎるネイバー」と呼ばれています。LLDP フレームは、シャーシ ID またはリモートポート ID がテーブル内にまだ含まれていな

い場合、テーブル内に新しいエントリーを必要とします。エントリーは、特定のポートのリンクがダウンしたとき、LLDP シャットダウンフレームを受信したとき、またはエントリーが期限切れしたときにテーブルから削除されます。

TLVs Discarded（削除された TLV）:
各 LLDP フレームには、TLV(Type Length Value)と呼ばれる複数の情報を含めることができます。TLV が不正な形式の場合、カウントされ、破棄されます。

TLVs Unrecognized（認識されていない TLV）:
整形式 TLV の数ですが、型の値が不明です。

Org. Discarded（削除された組織）:
組織が受け取った TLV の数です。

Age-Outs（期限切れ）:
各 LLDP フレームには、LLDP 情報が有効な期間(エイジ・アウト・タイム)に関する情報が含まれます。エイジ・アウト・タイム内に新しい LLDP フレームが受信されない場合、LLDP 情報は削除され、エイジ・アウト・カウンターが増やされます。

■ボタン

Auto-refresh（自動更新）:
画面を自動的に更新する場合は、このチェックボックスを ON にしてください。自動更新は 3 秒間隔で行われます。

Refresh（更新）:
クリックすると、画面がすぐに更新されます。

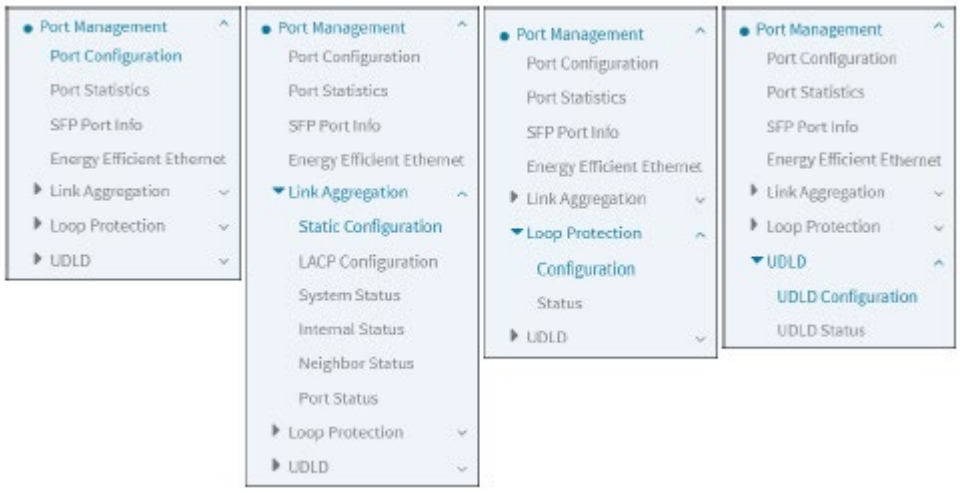
Clear（消去）:
選択したポートのカウンターを消去します。

第 4 章
ポートの管理

概要

このセクションでは、スイッチのポート詳細パラメーターを設定する方法について説明します。これ以外には、ポート設定を使用してスイッチのポートを有効または無効にできます。また、ポートの内容や機能の状態を監視します。

以下にメニューとサブメニューを示します。

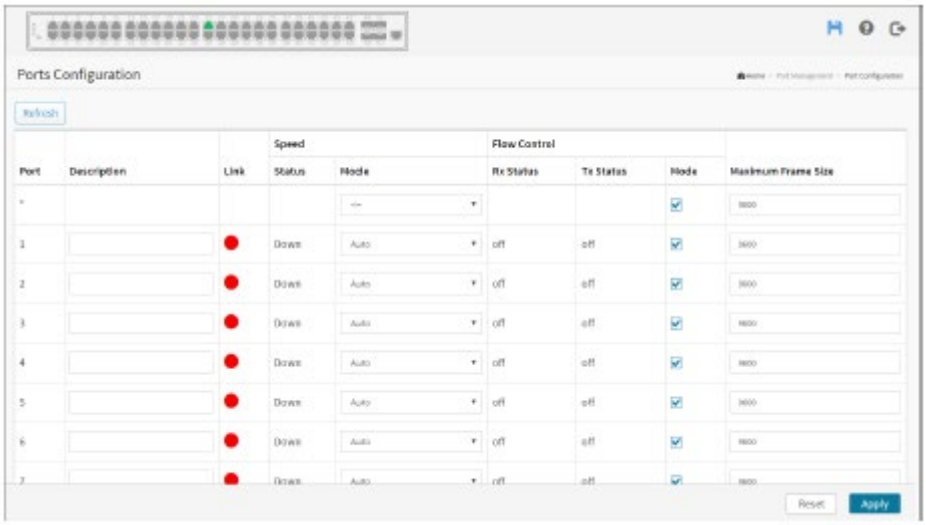


ポートの管理

このセクションでは、スイッチのポート詳細パラメーターを設定する方法について説明します。これ以外には、ポートの設定を使用してスイッチのポートを有効または無効にできます。また、ポートの内容や機能の状態を監視します。

ポートの設定

この画面には、現在のポート設定が表示されます。



ポートの統計

Web インターフェース

Web インターフェースで現在のポート設定を構成するには:

1. 「Port Management」(ポートの管理) ＞ 「Port Configuration」(ポートの設定)をクリックしてください。
2. システムのハードウェアタイプ、ソフトウェアバージョン、およびネットワークアプリケーションの完全な名前とバージョン ID を説明する英数字の文字列を、詳細ポートのエイリアスまたは説明として指定してください。
3. 「Speed Configured」(設定速度)、「Flow Control」(フローコントロール)、「Maximum Frame Size」(最大フレームサイズ)を指定してください。
4. 「Apply」(適用)をクリックしてください。

■パラメーターの説明

Port（ポート）：
これは、この行の論理ポート番号です。

Description（説明）：
このポートを識別するための説明的な名前として、最大 63 文字を入力してください。

Link（リンク）：
現在のリンク状態がグラフィカルに表示されます。グリーンはリンクがアップしていることを、また、レッドはリンクがダウンしていることを、それぞれ示します。

Current Link Speed Status（現在のリンク速度状態）：
ポートの現在のリンク速度を提供します。

Configured Link Speed（設定されたリンク速度）：
指定されたスイッチポートで使用可能なリンク速度を選択します。特定のポートでサポートされている速度のみが表示されます。可能な速度は次のとおりです。

Disabled（無効） - スイッチのポート操作を無効にします。
Auto（自動） - リンクパートナーとの自動ネゴシエーション速度を設定し、リンクパートナーと互換性のある最高速度を選択します。
10Mbps HDX - cu ポートを強制的に 10Mbps 半二重モードにします。
10Mbps FDX - cu ポートを強制的に 10Mbps 全二重モードにします。
100Mbps HDX - cu ポートを 100Mbps 半二重モードにします。
100Mbps FDX - cu ポートを 100Mbps 全二重モードにします。
1Gbps FDX - ポートを強制的に 1Gbps 全二重のフローコントロールにします。

ポートの速度に[Auto]（自動）が選択されている場合、このセクションはリンクパートナーに通知されるフローコントロール機能を示します。固定速度設定を選択した場合は、それが使用されます。「Current Rx」（現在の受信）列は、ポート上のポーズフレームが従うかどうかを示し、「Current Tx」（現在の送信）列はポート上のポーズフレームが送信されるかどうかを示します。Rx および Tx の設定は、最後の自動ネゴシエーションの結果によって決まります。
フローコントロールを使用するには、設定された列を確認してください。この設定は、「Configured Link Speed（設定されたリンク速度）」の設定に関連しています。

Maximum Frame Size（最大フレーム長）：
スイッチのポートに許可される最大フレームサイズ（FCS を含む）を入力してください。範囲は 1518～10240 バイトです。

■ボタン

Refresh（更新）：

ポートリンクの状態を手動で更新する場合は、このボタンをクリックしてください。

Apply（適用）：

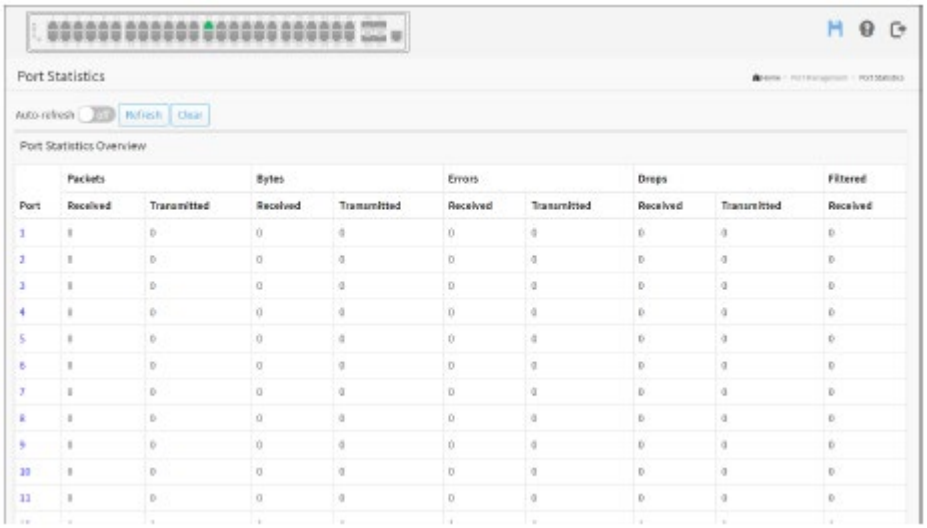
クリックすると、変更内容を保存します。

Reset（リセット）：

クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

ポートの統計

このセクションでは、ポートの統計情報について説明し、すべてのスイッチポートの全般的なトラフィック統計情報の概要を示します。



Web インターフェース

Web インターフェースでポート統計の概要を表示するには：

1. 「Port Management」（ポートの管理） ＞ 「Port Statistics」（ポートの統計）をクリックしてください。
2. 自動更新を行う場合は、「Auto-refresh」（自動更新）を呼び出す必要があります。
3. 「Refresh」（更新）をクリックすると、ポートの統計情報が更新され、「Clear」（消去）をクリックすると、すべての情報が消去されます。
4. ポート統計の詳細を表示するには、そのポートをクリックする必要があります。

■パラメーターの説明

Port（ポート）：
同じ行に含まれる設定の論理ポートです。

Packet（パケット）：
ポートあたりの受信および送信パケット数です。

Bytes（バイト）：
ポートあたりの受信バイト数と送信バイト数です。

Errors（エラー）：
エラーで受信されたフレーム数と、ポートあたりの不完全な送信数です。

Drops（ドロップ）：
入力または出力の輻輳（ふくそう）のために破棄されたフレームの数です。

Filtered（フィルター処理済）
フォワーディングプロセスによってフィルタリングされた受信フレームの数です。

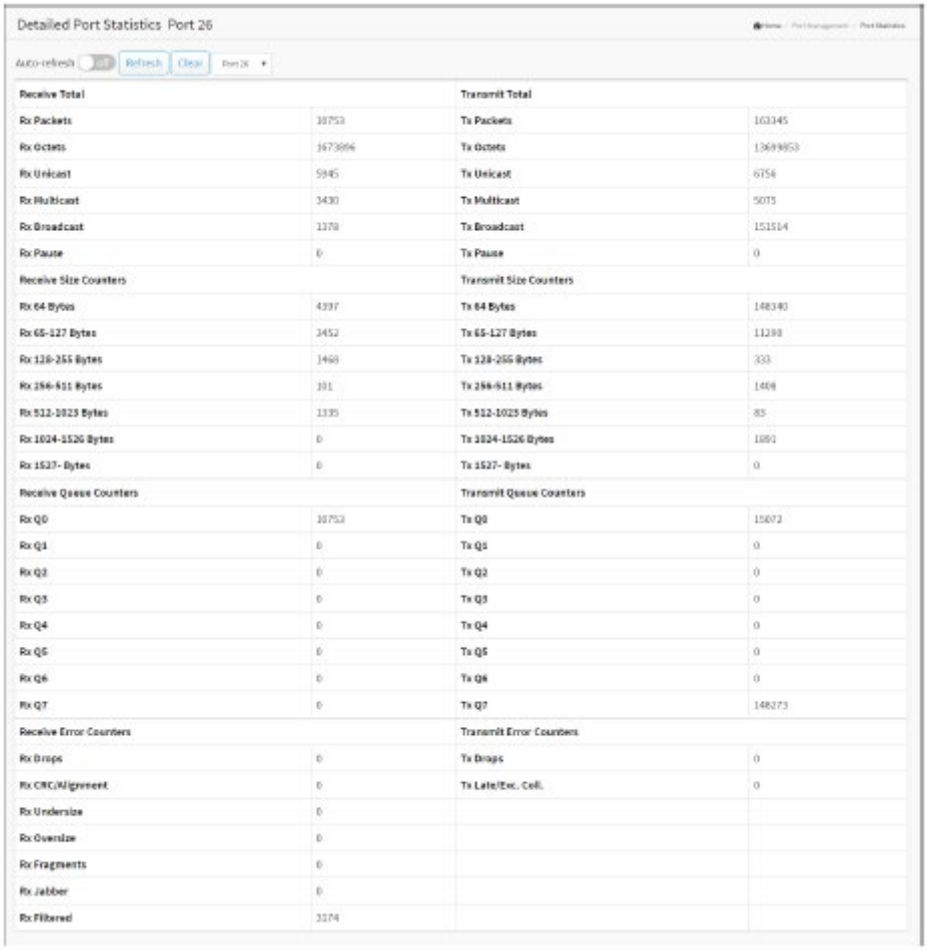
■ボタン

Auto-refresh（自動更新）：
画面を自動的に更新する場合は、このチェックボックスをONにしてください。自動更新は3秒間隔で行われます。

Refresh（更新）：
クリックしてページを更新します。

Clear（消去）：
すべてのポートのカウンターを消去します。

ポート統計の詳細を表示するには、そのポートをクリックする必要があります。表示されるカウンターは、受信と送信の合計、受信と送信のサイズカウンター、および受信と送信のエラーカウンターです。



■パラメーターの説明

左上のスクロールバー：

「Port-1」（ポート-1）、「Port-2」（ポート-2）…でポート統計を表示するポートをスクロールします。

Receive Total and Transmit Total（受信合計と送信合計）

Rx and Tx Packets（Rx および Tx パケット）：

受信および送信された（正常および不良）パケットの数です。

Rx and Tx Octets（Rx および Tx オクテット）：

受信および送信された（正常および不良）バイト数です。FCS は含まれますが、フレーミングビットは除外されます。

Rx and Tx Unicast（Rx および Tx ユニキャスト）：

受信および送信された(正常および不良の)ユニキャストパケットの数です。

Rx and Tx Multicast（Rx および Tx マルチキャスト）:
受信および送信された（正常および不良）マルチキャストパケットの数です。

Rx and Tx Broadcast（Rx および Tx ブロードキャスト）:
受信および送信された（正常および不良）ブロードキャストパケットの数です。

Rx and Tx Pause（Rx および Tx 一時停止）:
このポートで受信または送信された MAC 制御フレームのカウントで、一時停止操作を示すオペコードを持ちます。

Receive Error Counters（受信および送信サイズカウンター）
受信および送信された（正常および不良）パケットの数は、それぞれのフレームサイズに基づいてカテゴリーに分割されます。

Receive Error Counters（受信エラーカウンター）
Rx Drops（Rx ドロップ）:
受信バッファーの不足または出力輻輳（ふくそう）のためにドロップされたフレームの数です。

Rx CRC/Alignment（Rx CRC/アライメント）:
CRC またはアライメントエラーで受信されたフレームの数です。

Rx Undersize（Rx アンダーサイズ）:
有効な CRC で受信されたショート 1 フレームの数です。

Rx Oversize（Rx オーバーサイズ）:
有効な CRC で受信されたロング 2 フレームの数です。

Rx Fragments（Rx フラグメント）:
無効な CRC で受信されたショート 1 フレームの数です。

Rx Jabber（Rx ジャバー）:
無効な CRC で受信されたロング 2 フレームの数です。

Transmit Error Counters（送信エラーカウンター）

Tx Drops（送信ドロップ）：
出力バッファーの輻輳（ふくそう）によりドロップされたフレームの数です。

Tx Late/Exc. Coll.（送信遅延/過剰コリジョン）：
コリジョンが過剰または遅延したためにドロップされたフレームの数です。

Tx Oversize（送信オーバーサイズ）：
フレームのオーバーサイズのためにドロップされたフレームの数です。

■ボタン

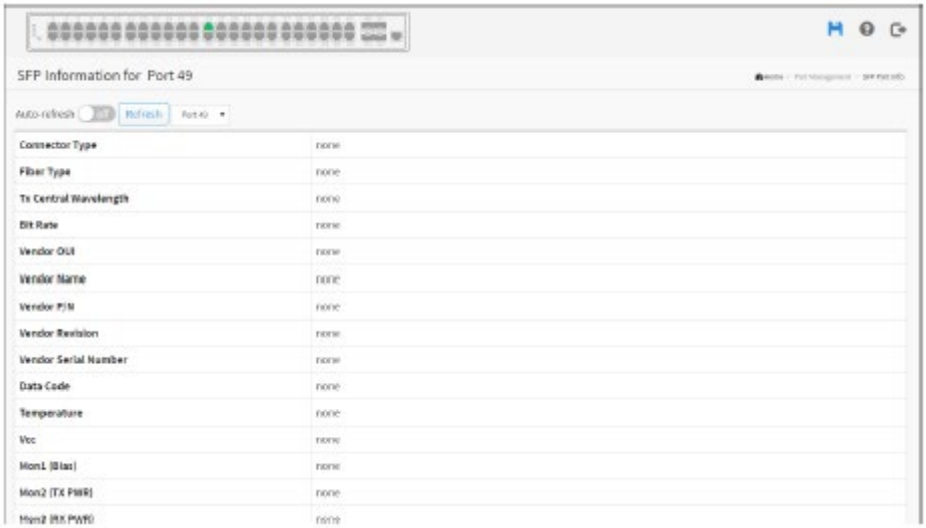
Auto-refresh（自動更新）：
画面を自動的に更新する場合は、このチェックボックスをONにしてください。自動更新は3秒間隔で行われます。

Refresh（更新）：
クリックするとページを更新します。

Clear（消去）：
選択したポートのカウンターを消去します。

SFP ポートの情報

このセクションでは、スイッチに接続する SFP モジュールの詳細情報を表示する機能について説明します。この情報には、コネクタータイプ、ファイバータイプ、波長、ビットレート、ベンダーOUI などが含まれます。



■パラメーターの説明

左上のスクロールバー：
ポートの統計情報を表示するポートをスクロールします。

Connector Type（コネクタータイプ）：
コネクタータイプ（UTP、SC、ST、LC など）を表示します。

Fiber Type（ファイバータイプ）：
ファイバーモード（マルチモード、シングルモードなど）を表示します。

Tx Central Wavelength（送信中心波長）：
中心波長（例えば、850nm、1310nm、1550nm など）を伝送する光ファイバーを表示します。

Bit Rate（ビットレート）：
トランシーバーの標準ビットレートを表示します。

Vendor OUI（ベンダーOUI）：

IEEE で割り当てられた製造元 OUI コードを表示します。

Vendor Name（ベンダー名）:
モジュールの製造元の会社名を表示します。

Vendor P/N（ベンダーP/N）:
モジュールの製造元別にネーミングされた製品名を表示します。

Vendor Rev (Revision)（ベンダーリビジョン）:
モジュールのリビジョンを表示します。

Vendor SN (Serial Number)（ベンダーSN（シリアル番号））:
製造元が割り当てたシリアル番号を表示します。

Date Code（日付コード）:
この SFP モジュールが作成された日付を表示します。

Temperature（温度）:
SFP モジュールの現在の温度を表示します。

Vcc:
SFP モジュールの動作中の DC 電圧を表示します。

Mon1(Bias) mA（Mon1（バイアス）mA）:
SFP モジュールのバイアス電流を表示します。

Mon2（TX PWR）:
SFP モジュールの送信電力を表示します。

Mon3（RX PWR）:
SFP モジュールの受信電力を表示します。

■ボタン

Auto-refresh（自動更新）:
画面を自動的に更新する場合は、このチェックボックスをONにしてください。自動更新は3秒間隔で行われます。

Refresh（更新）:
クリックするとページを更新します。

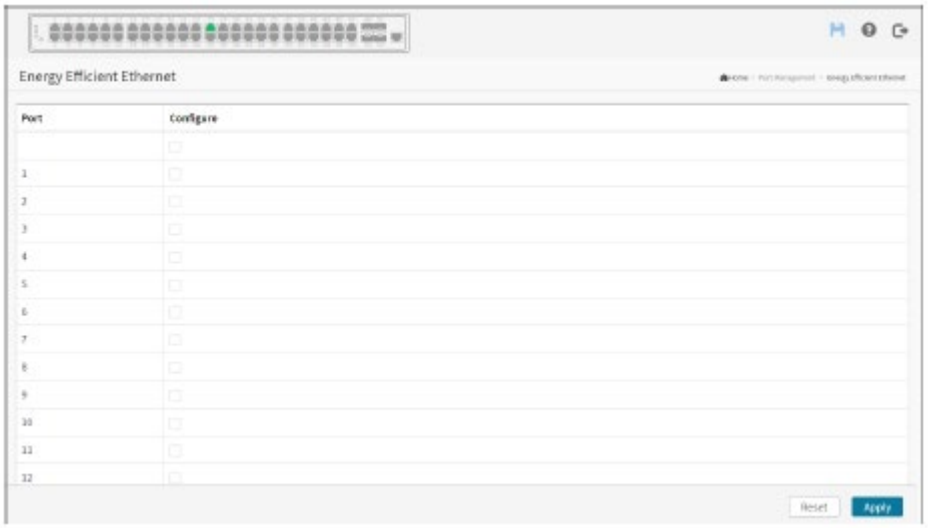
Energy Efficient Ethernet

EEE は、IEEE802.3az に定義されている「Energy Efficient Ethernet」の略です。

この画面において、ユーザーは現在の EEE ポート設定を精査したり定義したりすることができます。

EEE は、トラフィックの使用率が非常に低い（またはトラフィックがない）ときに消費電力を削減する省エネオプションです。

EEE は、トラフィックがない場合に回路の電源を切ることによって機能します。ポートが送信されるデータを受け取ると、すべての回路の電源が投入されます。回路の電源投入にかかる時間をウェイクアップ時間と呼びます。デフォルトのウェイクアップ時間は、1Gbit リンクの場合は 17us、その他のリンク速度の場合は 30us です。EEE デバイスは、トラフィックの送信時に受信側と送信側の両方のデバイスがすべての回路に電源を投入していることを確認するために、ウェイクアップ時間の値に同意する必要があります。デバイスは、LLDP プロトコルを使用して、デバイスのウェイクアップ時間に関する情報を交換できます。



Web インターフェース

Web インターフェースで Energy Efficient Ethernet を設定するには:

1. 「Port Management」(ポートの管理) ＞ 「Energy Efficient Ethernet」をクリックしてください。
2. ポートごとに「Energy Efficient Ethernet」を有効または無効にしてください。
3. 「Apply」(適用)をクリックして設定を保存してください。
4. 設定を取り消す場合は、「Reset」(リセット)ボタンをクリックする必要があります。そうすると、以前に保存した値へと戻ります。

■パラメーターの説明

Port(ポート):

論理 EEE ポートのスイッチポート番号です。

Configure(設定):

このスイッチポートで EEE を有効にするかどうかを制御します。

■ボタン

Apply(適用):

クリックすると、変更内容を保存します。

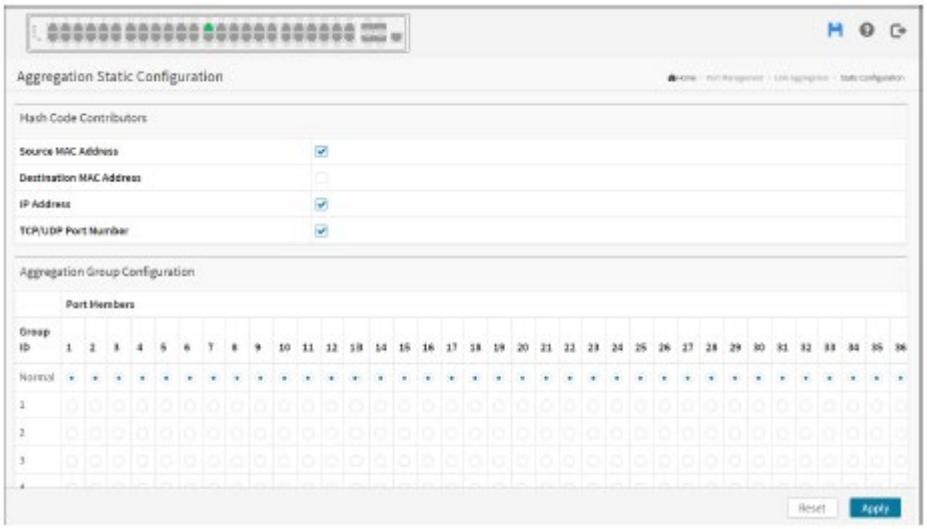
Reset(リセット):

クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

リンクアグリゲーション

スタティック設定

この画面は、アグリゲーションハッシュモードとアグリゲーショングループを設定するために使用されます。



Web インターフェース

Web インターフェースで集計ハッシュモードと集計グループを設定するには:

1. 「Port Management」(ポートの管理) ＞ 「Link Aggregation」(リンクアグリゲーション) ＞ 「Static Configuration」(スタティック設定)をクリックしてください。
2. 集計モード機能を有効または無効にしてください。
3. アグリゲーショングループ ID およびポートメンバーを呼び出してください。
4. 「Apply」(適用)をクリックして設定を保存してください。
5. 設定を取り消す場合は、「Reset」(リセット)ボタンをクリックする必要があります。そうすると、以前に保存した値へと戻ります。

■パラメーターの説明

Hash Code Contributors(ハッシュコード・コントリビューター)

Source MAC Address(送信元 MAC アドレス):

送信元MACアドレスを使って、フレームの宛先ポートを計算することができます。この項目をONにすると送信元 MAC アドレスの使用を有効にします。また、OFF にすると、このアドレスの使用を無効にします。デフォルトでは、送信元 MAC アドレスは有効になっています。

Destination MAC Address（宛先 MAC アドレス）:
宛先MACアドレスを使って、フレームの宛先ポートを計算することができます。この項目をONにすると宛先 MAC アドレスの使用を有効にします。また、OFF にすると、このアドレスの使用を無効にします。デフォルトでは、宛先 MAC アドレスは無効になっています。

IP Address（IP アドレス）:
IP アドレスを使って、フレームの宛先ポートを計算することができます。この項目を ON にすると IP アドレスの使用を有効にします。また、OFF にすると、このアドレスの使用を無効にします。デフォルトでは、IP アドレスは有効になっています。

TCP/UDP Port Number（TCP/UDP ポート番号）:
TCP/UDP ポート番号を使って、フレームの宛先ポートを計算することができます。この項目を ON にするとTCP/UDPポート番号の使用を有効にします。また、OFF にすると、このポート番号の使用を無効にします。デフォルトでは、TCP/UDP ポート番号は有効になっています。

Aggregation Group Configuration（アグリゲーショングループの設定）
Group ID（グループ ID）:
同じ行に含まれる設定のグループ ID を示します。グループ ID が「Normal」（標準）である行は、集計がないことを示します。ポートごとに有効なグループ ID は 1 つだけです。

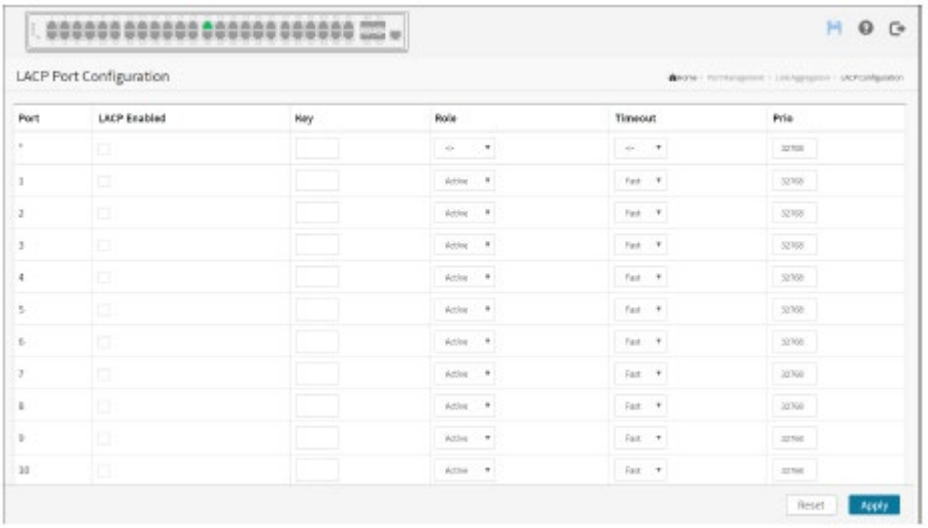
Port Members（ポートメンバー）:
各スイッチポートは、グループ ID ごとに一覧表示されます。アグリゲーションにポートを含めるにはラジオボタンを選択し、アグリゲーションからポートを削除するにはラジオボタンの選択を解除してください。デフォルトでは、どのポートもアグリゲーショングループに属していません。アグリゲーションに参加できるのは、全二重のポートのみです。また、ポートは各グループで同じ速度にする必要があります。

■ボタン
Apply（適用）:
クリックすると、変更内容を保存します。

Reset（リセット）:
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

LACP の設定

この画面では、現在の LACP ポート設定を確認し、変更することもできます。



Web インターフェース

Web インターフェースで LACP ポート設定を設定するには:

1. 「Port Management」(ポートの管理) ＞ 「Link Aggregation」(リンクアグリゲーション) ＞ 「LACP Configuration」(LACP 設定)をクリックしてください。
2. スイッチのポートで LACP を有効または無効に設定してください。
3. 「Key」(キー)パラメーターを「Auto」(自動)または「Specific」(指定)でスクロールしてください。デフォルトは「Auto」(自動)です。
4. 「Roll」(ロール)を「Active」(アクティブ)または「Passive」(パッシブ)でスクロールしてください。デフォルトは「Passive」(パッシブ)です。
5. 「Apply」(適用)をクリックして設定を保存してください。
6. 設定を取り消す場合は、「Reset」(リセット)ボタンをクリックする必要があります。そうすると、以前に保存した値へと戻ります。

■パラメーターの説明

Port(ポート):

スイッチのポート番号です。

LACP Enabled(LACP 有効):

このスイッチのポートで LACP を有効にするかどうかを制御します。2 つ以上のポートが同じパートナーに接続されている場合、LACP はアグリゲーションを形成します。

Key（キー）：
ポートで発生するキー値です（範囲 1～65535）。「Auto」（自動）設定では、物理リンク速度（10Mb=1、100Mb=2、1Gb = 3）に応じてキーが設定されます。「Specific」（指定）設定を使用すると、ユーザー定義の値を入力できます。同じキー値を持つポートは同じアグリゲーショングループに参加できますが、異なるキーを持つポートは参加できません。

Role（ロール）：
ロールには、LACP アクティビティーの状態が表示されます。アクティブは LACP パケットを毎秒送信し、パッシブはパートナーからの LACP パケットを待ちます（読み上げられた場合は読み上げられます）。

Timeout（タイムアウト）：
タイムアウトは、BPDU 伝送の間隔を制御します。「Fast」（高速）は LACP パケットを毎秒送信し、「Slow」（低速）は LACP パケットを送信する前に 30 秒間待機します。

Prio（優先度）：
ポートの優先度を制御します。LACP パートナーがこのデバイスでサポートされているよりも大きなグループを形成したい場合、このパラメーターは、どのポートをアクティブにし、どのポートをバックアップロールにするかを制御します。数値が小さいほど、優先順位が高くなります。

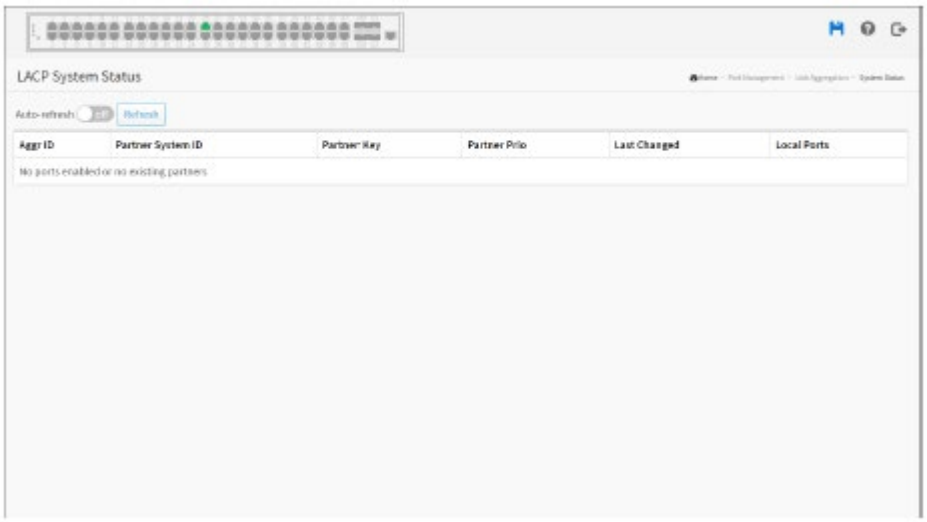
■ボタン

Apply（適用）：
クリックすると、変更内容を保存します。

Reset（リセット）：
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

システムの状態

このセクションでは、スイッチにLACP機能を設定すると、すべてのLACPインスタンスの状態の概要が表示される機能について説明します。



Web インターフェース

Web インターフェースに LACP システムの状態を表示するには:

1. 「Port Management」(ポートの管理) ＞ 「Link Aggregation」(リンクアグリゲーション) ＞ 「System Status」(システムの状態)をクリックしてください。
2. 「Auto-refresh」(自動更新)にチェックを入れてください。
3. 「Refresh」(更新)をクリックして、ポートの詳細統計情報を更新してください。

■パラメーターの説明

Aggr ID(アグリゲーション ID):

この集計インスタンスに関連付けられた集計 ID です。LLAG の場合、id は「isid:aggr-id」と表示され、GLAG の場合は「aggr-id」と表示されます。

Partner System ID(パートナーシステム ID):

アグリゲーションパートナーのシステム ID(MAC アドレス)です。

Partner Key(パートナーキー):

パートナーがこのアグリゲーション ID に割り当てたキーです。

Partner Prio(パートナー優先度):

パートナーがこのアグリゲーション ID に割り当てた優先度です。

Last changed（最終変更日）:
このアグリゲーションが変更された時間です。

Local Ports（ローカルポート）:
このスイッチのアグリゲーションの一部であるポートを示します。形式は「*スイッチ ID ： ポート*」です。

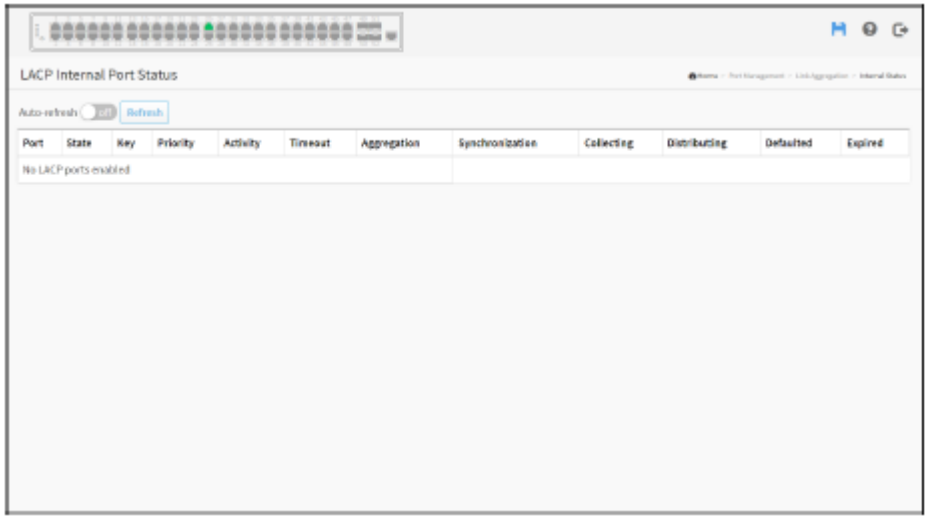
■ボタン

Auto-refresh（自動更新）:
画面を自動的に更新する場合は、このチェックボックスをONにしてください。自動更新は3秒間隔で行われます。

Refresh（更新）:
クリックするとページを更新します。

内部の状態

この画面には、すべてのポートの LACP 内部（言い換えれば、ローカルシステム）の状態の概要が表示されます。表示されるのは、LACPグループの一部のポートのみです。表示されるパラメーターの詳細については、IEEE801.AX-2014 を参照してください。



Web インターフェース

「LACP Internal System」(LACP 内部システム)の状態を Web インターフェースに表示するには:

1. 「Port Management」(ポートの管理) ＞ 「Link Aggregation」(リンクアグリゲーション) ＞ 「Internal Status」(内部の状態)をクリックしてください。
2. 「Auto-refresh」(自動更新)にチェックを入れてください。
3. 「Refresh」(更新)をクリックして、ポートの詳細統計情報を更新してください。

■パラメーターの説明

Port(ポート):

スイッチのポート番号です。

State(状態):

現在のポートの状態です:

Down(ダウン):ポートはアクティブではありません。

Active(アクティブ):ポートはアクティブです。

Standby(スタンバイ):ポートはスタンバイ状態です。

Key(キー):

このポートに割り当てられたキーです。同じキーを持つポートのみを集約できます。

Priority(優先度):

このアグリゲーショングループに割り当てられた優先度です。

Activity(アクティビティー):

グループの LACP モード(アクティブまたはパッシブ)です。

Timeout(タイムアウト):

ポートに設定されたタイムアウトモードです(高速または低速)。

Aggregation(アグリゲーション):

システムがこのリンクを「集約可能」、すなわち、アグリゲーションの潜在的な候補と見なすかどうかを示します。

Synchronization(同期):

システムがこのリンクが「IN_SYNC」であると見なしているかどうか、すなわち、正しい LAG に割り当

てられているかどうか、グループが互換性のある XBFe アグリゲーターに関連付けられているかどうか、および LAG の ID が送信されたシステム ID および操作キー情報と一致しているかどうかを示します。

Collecting（収集中）:
このリンクで受信フレームの収集が有効になっているかどうかを表示します。

Distributing（分配）:
このリンクで送信フレームの分配が有効になっているかどうかを表示します。

Defaulted（デフォルト）:
アクターの受信マシンが、デフォルトの操作パートナー情報を使用しているかどうかを表示します。

Expired（期限切れ）:
アクターの受信マシンが期限切れ状態であるかどうかを表示します。

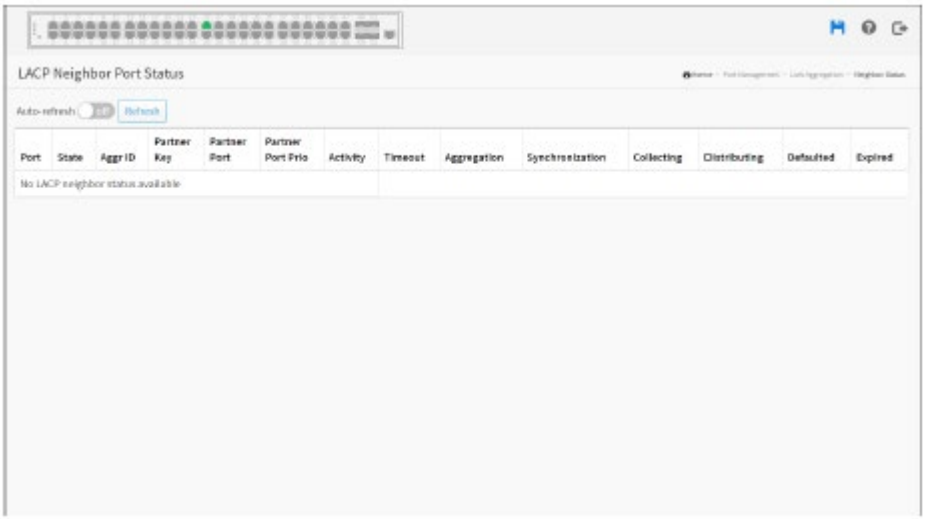
■ボタン

Auto-refresh（自動更新）:
画面を自動的に更新する場合は、このチェックボックスを ON にしてください。自動更新は 3 秒間隔で行われます。

Refresh（更新）:
クリックするとページを更新します。

ネイバーの状態

この画面には、すべてのポートの LACP ネイバーの状態の概要が表示されます。表示されるのは、LACP グループの一部のポートのみです。表示されるパラメーターの詳細については、IEEE801.AX-2014 を参照してください。



Web インターフェース

Web インターフェースで LACP ネイバーのポートの状態を表示するには:

1. 「Port Management」(ポートの管理) ＞ 「Link Aggregation」(リンクアグリゲーション) ＞ 「Neighbor Status」(ネイバーの状態)をクリックしてください。
2. 「Auto-refresh」(自動更新)にチェックを入れてください。
3. 「Refresh」(更新)をクリックして、ポートの詳細統計情報を更新してください。

■パラメーターの説明

Aggr ID(アグリゲーション ID):

ポートが割り当てられているアグリゲーショングループ ID です。

Port(ポート):

スイッチのポート番号です。

State(状態):

現在のポートの状態です:

Down(ダウン):ポートはアクティブではありません。

Active(アクティブ):ポートはアクティブです。

Standby(スタンバイ):ポートはスタンバイ状態です。

Partner Key(パートナーキー):

パートナーによって、このポートに割り当てられたキーです。

Partner Port(パートナーポート):

このリンクに関連付けられたパートナーポート番号です。

Partner Port Priority（パートナーポートの優先度）：
このパートナーポートに割り当てられた優先度です。

Activity（アクティビティー）：
グループの LACP モード（アクティブまたはパッシブ）です。

Timeout（タイムアウト）：
ポートに設定されたタイムアウトモードです（高速または低速）。

Aggregation（アグリゲーション）：
システムがこのリンクを「集約可能」、すなわち、アグリゲーションの潜在的な候補と見なすかどうかを示します。

Synchronization（同期）：
システムがこのリンクが「IN_SYNC」であると見なしているかどうか、すなわち、正しい LAG に割り当てられているかどうか、グループが互換性のある XBFe アグリゲーターに関連付けられているかどうか、および LAG の ID が送信されたシステム ID および操作キー情報と一致しているかどうかを示します。

Collecting（収集中）：
このリンクで受信フレームの収集が有効になっているかどうかを表示します。

Distributing（分配）：
このリンクで送信フレームの分配が有効になっているかどうかを表示します。

Defaulted（デフォルト）：
アクターの受信マシンが、デフォルトの操作パートナー情報を使用しているかどうかを表示します。

Expired（期限切れ）：
アクターの受信マシンが期限切れ状態であるかどうかを表示します。

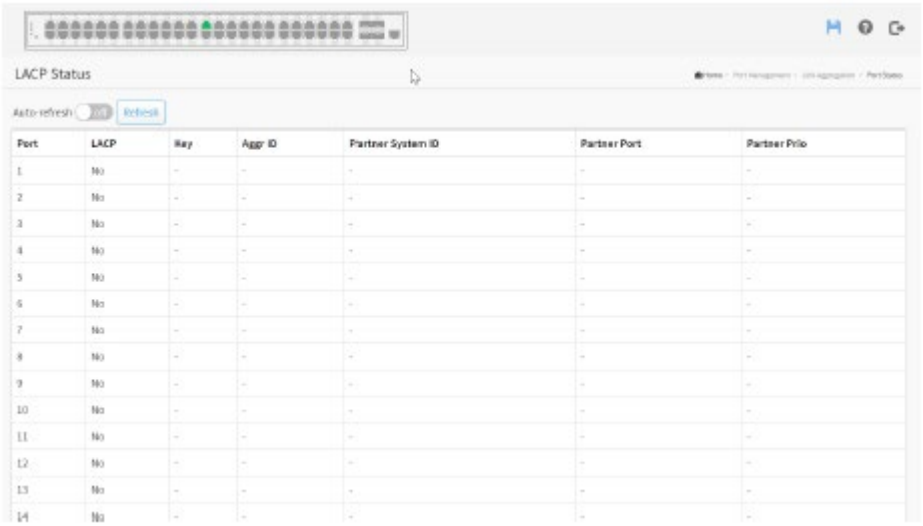
■ボタン

Auto-refresh（自動更新）:
画面を自動的に更新する場合は、このチェックボックスをONにしてください。自動更新は3秒間隔で行われます。

Refresh（更新）:
クリックするとページを更新します。

ポートの状態

このセクションでは、スイッチに LACP 機能を設定した場合に、すべての LACP インスタンスにおけるポートの状態の概要が表示される機能について説明します。



Web インターフェース
Web インターフェースで LACP ポートの状態を表示するには:

1. 「Port Management」（ポートの管理） ＞ 「Link Aggregation」（リンクアグリゲーション） ＞ 「Port Status」（ポートの状態）をクリックしてください。
2. 情報を自動更新する場合は、「Auto-refresh」（自動更新）を呼び出す必要があります。
3. 「Refresh」（更新）をクリックして、LACP ポートの状態を更新してください。

■パラメーターの説明

Port（ポート）：
スイッチのポート番号です。

LACP：
「Yes」は、LACP が有効で、ポートリンクがアップしていることを意味します。「No」は、LACP が有効になっていないか、ポートリンクがダウンしていることを示します。「Backup」（バックアップ）は、ポートがアグリゲーショングループに参加できなかったけれども、他のポートが脱退した場合に参加することを意味します。その間、LACP の状態は無効になります。

Key（キー）：
このポートに割り当てられたキーです。同じキーを持つポートのみを集約できます。

Aggr ID（アグリゲーション ID）：
このアグリゲーショングループに割り当てられたアグリゲーション ID です。ID1～2 は GLAG、ID3～14 は LLAG です。

Partner System ID（パートナーシステム ID）：
パートナーのシステム ID（MAC アドレス）です。

Partner Port（パートナーポート）：
このポートに接続されているパートナーのポート番号です。

Partner Prio（パートナーの優先度）：
パートナーのポート優先度です。

■ボタン

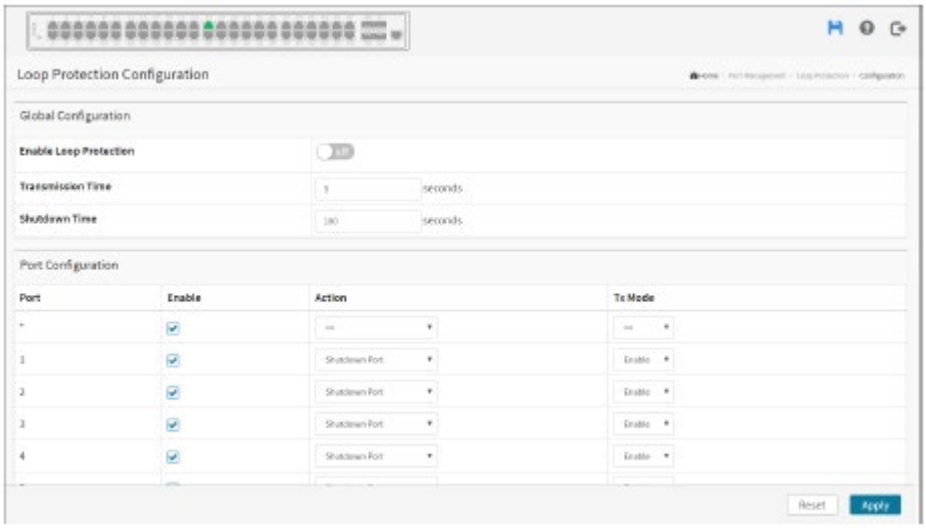
Auto-refresh（自動更新）：
画面を自動的に更新する場合は、このチェックボックスを ON にしてください。自動更新は 3 秒間隔で行われます。

Refresh（更新）：
クリックするとページを更新します。

ループ保護

設定

ループ保護は、トラフィックの存在を検出するために使用されます。スイッチがポートから自分自身と同じパケット（ループ検出フレーム）の MAC アドレスを受信すると、ループ保護が発生します。ループ保護フレームを受信すると、ポートはロックされます。ロックされたポートを再開するには、ループパスを確認し、ループパスを解除してから、ロックされたポートで再開を選択します。そうしたら、「Resume」（再開）をクリックしてロックされたポートを ON にしてください。



Web インターフェース

Web インターフェースでループ保護パラメーターを設定するには:

1. 「Port Management」（ポートの管理）＞「Loop Protection」（ループ保護）＞「Configuration」（設定）をクリックしてください。
2. ポートループ保護を有効または無効にしてください。
3. 「Apply」（適用）をクリックして設定を保存してください。
4. 設定を取り消す場合は、「Reset」（リセット）ボタンをクリックする必要があります。そうすると、以前に保存した値へと戻ります。

■パラメーターの説明

Global Configuration（グローバル設定）

Enable Loop Protection（ループ保護を有効にする）:

ループ保護を（全体的に）有効にするかどうかを制御します。

Transmission Time（送信時間）：
各ポートで送信される各ループ保護 PDU の間隔におけるインターバルです。有効な値は 1～10 秒です。

Shutdown Time（シャットダウン時間）：
ループが検出された場合（およびポートアクションによってポートがシャットダウンされた場合）に、ポートが無効の状態を維持する期間（秒）です。有効な値は 10～604800 秒（7 日）です。

Port Configuration（ポート設定）

Port（ポート）：
ポートのスイッチポート番号です。

Enable（有効にする）：
このスイッチポートでループ保護を有効にするかどうかを制御します。

Action（アクション）：
ポートでループが検出されたときに実行されるアクションを設定します。有効な値は、「Shutdown Port」（ポートのシャットダウン）、「Shutdown Port and Log」（ポートのシャットダウンとログ）または「Log Only」（ログのみ）です。

Tx Mode（送信モード）：
ポートが、ループ保護 PDU をアクティブに生成するか、またはループ PDU を単に受動的に探すかどうかを制御します。

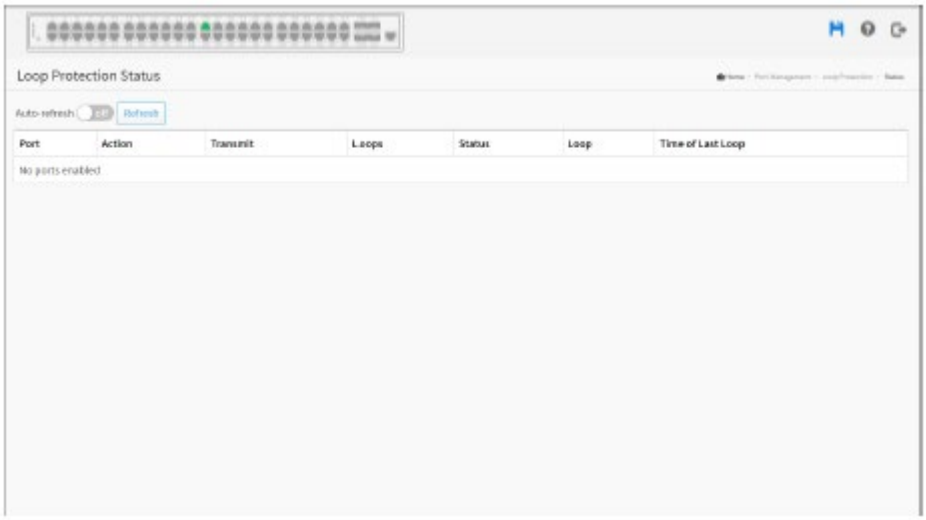
■ボタン

Apply（適用）：
クリックすると、変更内容を保存します。

Reset（リセット）：
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

状態

このセクションには、現在選択されているスイッチにおけるポートのループ保護の状態が表示されます。



Web インターフェース

Web インターフェースでループ保護の状態を表示するには:

1. 「Port Management」(ポートの管理) ＞ 「Loop Protection」(ループ保護) ＞ 「Configuration」(設定)をクリックしてください。
2. 情報を自動更新する場合は、「Auto-refresh」(自動更新)を呼び出す必要があります。
3. 「Refresh」(更新)をクリックして、ループ保護の状態を更新してください。

■パラメーターの説明

Port (ポート) :

論理ポートのスイッチポート番号です。

Action (アクション) :

現在設定されているポートアクションです。

Status (送信) :

現在設定されているポート送信モードです。

Loops (ループ) :

このポートで検出されたループの数です。

Status（状態）：
ポートにおける現在のループ保護の状態です。

Loop（ループ）：
ポートでループが現在検出されているかどうかを表します。

Time of Last Loop（最終ループ時刻）：
最後に検出されたループイベントの時間です。

■ボタン

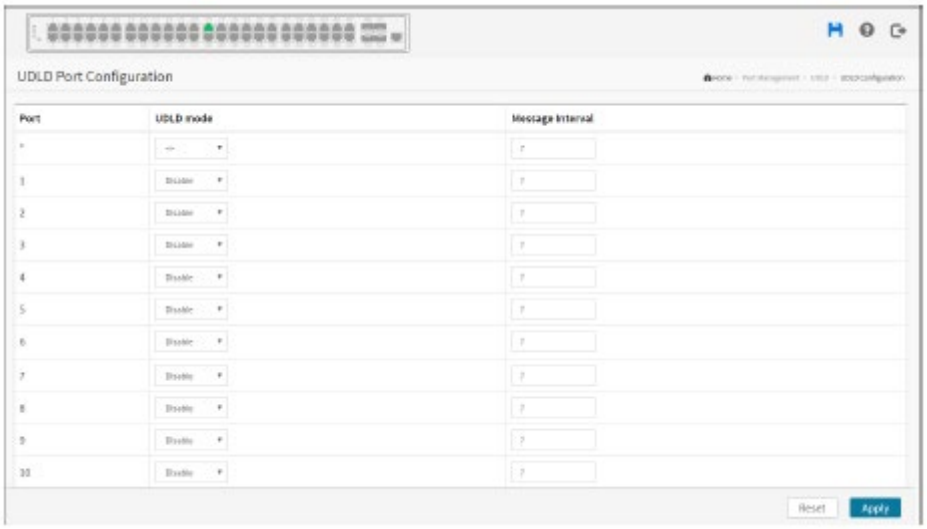
Auto-refresh（自動更新）：
画面を自動的に更新する場合は、このチェックボックスをONにしてください。自動更新は3秒間隔で行われます。

Refresh（更新）：
クリックするとページを更新します。

UDLD

UDLD の設定

この画面では、現在の UDLD 設定を確認し、変更することができます。



Web インターフェース

Web インターフェースで UDLD パラメーターを設定するには:

1. 「Port Management」(ポートの管理) ＞ 「UDLD」 ＞ 「UDLD Configuration」(UDLD の設定)をクリックしてください。
2. ポート UDLD を有効または無効にしてください。
3. メッセージ間隔を指定してください。
4. 「Apply」(適用)をクリックして設定を保存してください。
5. 設定を取り消す場合は、「Reset」(リセット)ボタンをクリックする必要があります。そうすると、以前に保存した値へと戻ります。

■パラメーターの説明

Port(ポート):

スイッチのポート番号です。

UDLD Mode(UDLD モード):

ポートの UDLD モードを設定します。有効な値は「Disable」(無効)、「Normal」(通常)、および

「Aggressive」(アグレッシブ)です。デフォルトのモードは「Disable」(無効)です。

Disable(無効):無効モードの場合、UDLD 機能はポートに存在しません。

Normal(通常):通常モードでは、ポートのリンク状態が単方向であると判断された場合、ポートの状態には影響しません。

Aggressive(アグレッシブ):アグレッシブモードでは、単方向に検出されたポートがシャットダウンされます。ポートを元に戻すには、そのポートの UDLD を無効にする必要があります。

Message Interval(メッセージ間隔):
アドバタイズメントフェーズにあり、双方向であると判断されたポートの UDLD プローブメッセージ間の期間を設定します。範囲は 7～90 秒(デフォルト値は 7 秒)です(現時点では RFC5171 に詳細情報がないため、デフォルトの時間間隔がサポートされています)。

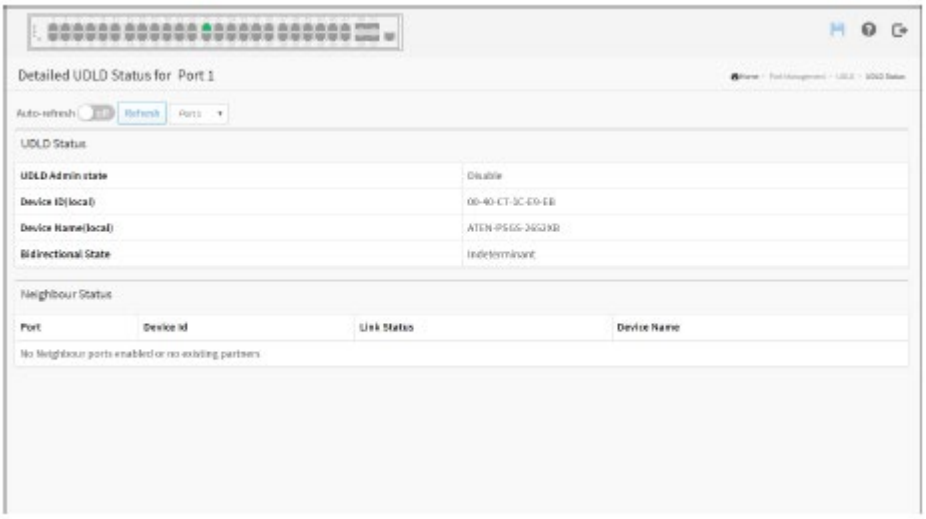
■ボタン

Apply(適用):
クリックすると、変更内容を保存します。

Reset(リセット):
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

UDLD の状態

この画面には、ポートの UDLD の状態が表示されます。



Web インターフェース

Web インターフェースでループ保護の状態を表示するには:

1. 「Port Management」(ポートの管理) ＞ 「UDLD」 ＞ 「UDLD Status」(UDLD の状態)をクリックしてください。
2. UDLD の状態を表示するポートを選択してください。
3. 情報を自動更新する場合は、「Auto-refresh」(自動更新)を呼び出す必要があります。
4. 「Refresh」(更新)をクリックして、ループ保護の状態を更新してください。

■パラメーターの説明

UDLD port status(UDLD ポートの状態)

UDLD Admin State(UDLD の管理状態):
論理ポートの現在の状態です。状態(通常、アグレッシブ)のいずれかが有効になっている場合は、有効となります。

Device ID(local)(デバイス ID(ローカル)):
デバイスの ID です。

Device Name(local)(デバイス名(ローカル)):
デバイスの名前です。

Bidirectional State(双方向状態):
ポートの現在の状態です。

Neighbor Status(ネイバーの状態)

Port(ポート):
ネイバーデバイスの現在のポートです。

Device ID(デバイス ID):
ネイバーデバイスの現在の ID です。

Link Status(リンクの状態):
ネイバーポートの現在のリンクの状態です。

Device Name(デバイス名):
ネイバーデバイスの名前です。

■ボタン

Auto-refresh（自動更新）:
画面を自動的に更新する場合は、このチェックボックスをONにしてください。自動更新は3秒間隔で行われます。

Refresh（更新）:
クリックすると、画面がすぐに更新されます。

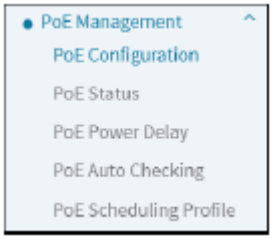
Port 1（ポート1）:
DHCP 詳細統計を表示するポートを選択してください。

第 5 章
PoE の管理（ES0152P のみ）

概要

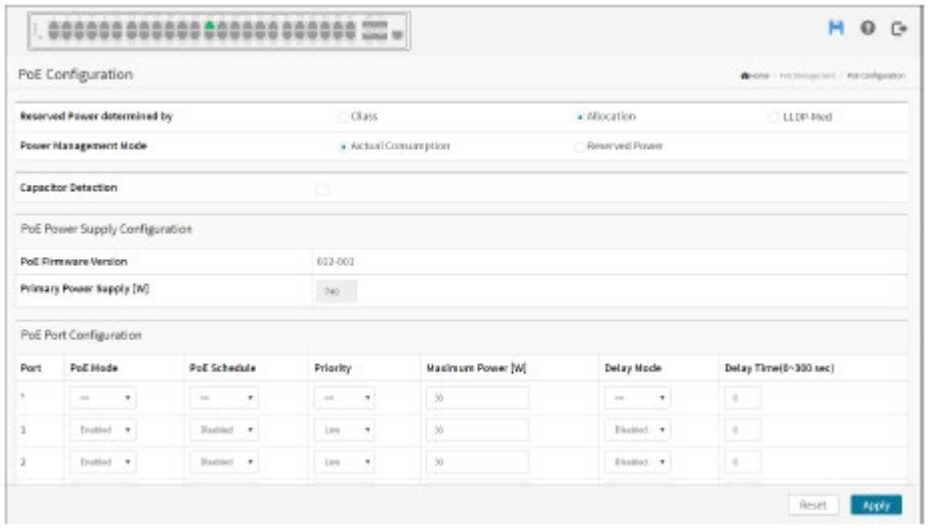
PoE は「Power over Ethernet」の略です。Power over Ethernet は、標準のイーサネットケーブルを介してリモートデバイスに電力を送信するために使用されます。例えば、IP 電話、無線 LAN アクセスポイント、およびその他の装置に電力を供給するために、装置を主電源に接続することが困難であったり、高価であったりする場合に使用することができます。

メニューは以下のとおりです。



PoE の設定

この画面では、現在の PoE ポート設定を精査および設定し、すべての PoE 供給ワットを表示できます。



Web インターフェース

Web インターフェースで Power over Ethernet を設定するには:

1. 「PoE Management」(PoE の管理) ＞ 「PoE Configuration」(PoE の設定)をクリックしてください。
2. 決定した予約電源を指定してください。
3. PoE または PoE+モード、PoE スケジュール、優先度、最大電力(W)、遅延モード、および遅延時間を指定してください。
4. 「Apply」(適用)をクリックして設定を保存してください。
5. 設定を取り消す場合は、「Reset」(リセット)ボタンをクリックする必要があります。そうすると、以前に保存した値へと戻ります。

■パラメーターの説明

Power Over Ethernet Configuration(Power Over Ethernet の設定)

予約電源は、以下によって決定されます。

ポート/PD が電源予約を行う方法を設定するのに 3 種類のモードがあります。

1. Allocated mode(割当モード):このモードにおいて、ユーザーは各ポートが予約できる電力量を割り当てます。各ポート/PD の割り当て/予約電源は、「Maximum Power」(最大電源)の項目

で指定します。

2. Class mode（クラスモード）：このモードでは、接続されたPDが属するクラスに応じて各ポートが予約する電力量を自動的に決定し、それに応じて電力を予約します。4 種類の異なるポートクラスがあり、種類は 4、7、15.4、または 30 ワット用です。このモードにおいて、「Maximum Power」（最大電源）の項目は無効になります。
3. LLDP-MED mode（LLDP-MED モード）：このモードは、各ポートが LLDP プロトコルを使用してPoE情報を交換することによって予約する電力量を決定し、それに応じて電力を予約するクラスモードに似ています。ポートに LLDP 情報がない場合、ポートはクラスモードを使用して電源を予約します。このモードにおいて、「Maximum Power」（最大電源）の項目は無効になります。

すべてのモード：ポートがポートの予約電源より多くの電源を使用する場合、ポートはシャットダウンされます。

Port Management（電源管理モード）：
ポートをシャットダウンするタイミングを設定するには、次の 2 種類のモードがあります。

1. Actual Consumption（実際の消費電力）：このモードでは、すべてのポートの実際の消費電力が、電源装置が供給できる電力量を超えた場合、または特定のポートの実際の消費電力がそのポートの予約電力を超えた場合に、ポートがシャットダウンされます。ポートは、ポート優先度に従ってシャットダウンされます。2 つのポートの優先度が同じ場合、ポート番号が最も大きいポートがシャットダウンされます。
2. Reserved Power（予約電力）：このモードでは、予約電力の合計が電力供給可能な電力量を超えると、ポートがシャットダウンされます。このモードでは、PD が電源から使用可能な電力より多くの電力を要求した場合、ポートの電源は ON になりません。

PoE Power Supply Configuration（PoE 電源の設定）

Primary Power Supply [W]（プライマリ電源[W]）：
プライマリ電源のワット数を表示します。

PoE Port Configuration（PoE ポートの設定）
Port（ポート）：
これは、この行の論理ポート番号です。

PoE Mode（PoE モード）：
PoE モードは、ポートの PoE 操作モードを表します。PoE を有効または無効にしてください。

PoE Schedule（PoE スケジュール）:
PoE スケジュールのプロファイルを無効にするか、リストから選択してください。

Priority（優先度）:
ポートの優先度を表します。「Low」（低）、「High」（高）、および「Critical」（重大）という 3 段階のレベルの電力優先度があります。
優先度は、リモートデバイスが電源装置の供給電力よりも多くの電力を必要とする場合に使用されます。この場合、優先度が最も低いポートは、ポート番号が最も大きいポートから順に OFF になります。

Maximum Power [W]（最大電力[W]）:
「Maximum Power」（最大電源）の値には、リモートデバイスに配信できる最大電力（ワット単位）を示す数値が含まれます。
最大許容値は 30W です。

Delay Mode（遅延モード）:
電源遅延機能を ON/OFF にします。
Enabled（有効）:POE 電源遅延を有効にします。
Disabled（無効）:POE 電源遅延を無効にします。

Delay Time(0～300sec)（遅延時間（0～300 秒））:
再起動の際、PoE ポートは遅延時間が終了すると PD への電力供給を開始します。デフォルト:0、範囲:0～300 秒。

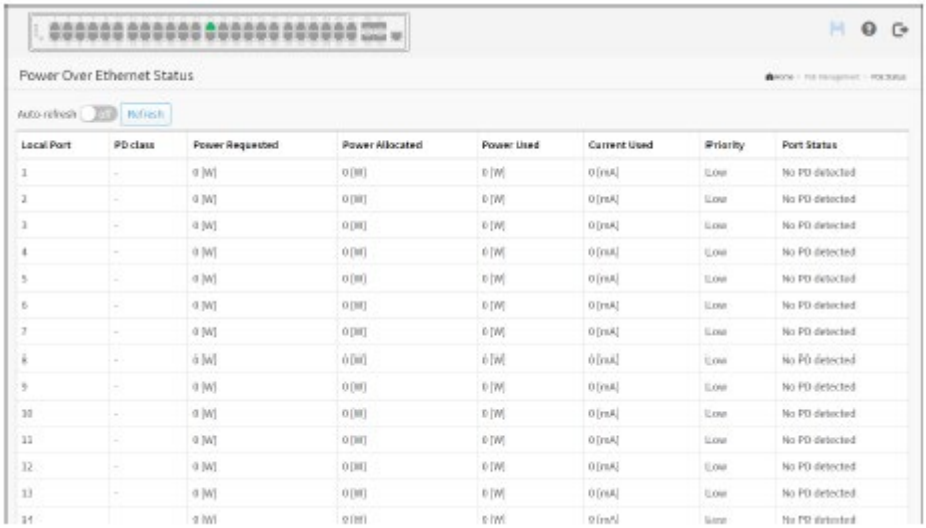
■ボタン

Apply（適用）:
クリックすると、変更内容を保存します。

Reset（リセット）:
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

PoE の状態

この画面では、すべての PoE ポートにおける現在の状態を確認できます。



■パラメーターの説明

Web インターフェース

Web インターフェースで PoE の状態を表示するには:

1. 「PoE Management」(PoE の管理) ＞ 「PoE Status」(PoE の状態)をクリックしてください。
2. 「Auto-refresh」(自動更新)をスクロールして ON/OFF にしてください。
3. 「Refresh」(更新)をクリックして、ポートの詳細統計情報を更新してください。

■パラメーターの説明

Local Ports(ローカルポート):

これは、この行の論理ポート番号です。

PD Class(PD クラス):

各 PD は、PD が使用する最大電力を定義するクラスに従って分類されます。これは、PD クラスを示します。

5 種類のクラスが定義されています。

Class 0(クラス 0):最大電力 15.4 W

Class 1(クラス 1):最大電力 4.0 W

Class 2(クラス 2):最大電力 7.0 W

Class 3（クラス 3）：最大電力 15.4W
Class 4（クラス 4）：最大電力 30.0 W

Power Requested（要求電力）：
「Power Requested」（要求電力）には、PD が予約する必要のある電力量が表示されます。

Power Allocated（割当電力）：
「Power Allocated」（割当電力）には、スイッチが PD に割り当てた電力量が表示されます。

Power Used（使用電力）：
「Power Used」（使用電力）には、PD が現在使用している電力が表示されます。

Current Used（使用電流）：
「Current Used」（使用電流）には、PD が現在使用している電流の量が表示されます。

Priority（優先度）：
「Priority」（優先度）には、ユーザーが設定したポートの優先度が表示されます。

Port Status（ポートの状態）：
「Port Status」（ポートの状態）には、ポートの状態が表示されます。状態には、次のいずれかの値を指定できます。

PoE not available（PoE 利用不可） – PoE チップが見つかりません。このポートでは PoE がサポートされていません。

PoE turned OFF – PoE disabled（PoE OFF – PoE 無効）：PoE はユーザーによって無効にされています。

PoE turned OFF – Power budget exceeded（PoE OFF – パワーバジェット超過）：PD によって要求または使用された電力の合計が、供給できる電源の最大値を超えたため、優先度が最も低いポートの電源が切断されています。

No PD detected（PD 検出なし）：ポートで PD が検出されませんでした。

PoE turned OFF – PD overload（PoE OFF – PD 過負荷）：PD は、ポートが供給可能な電力以上を要求または使用しているため、電源が切断されています。

PoE turned OFF（PoE OFF）：PD が OFF です。

Invalid PD（無効な PD）：PD が検出されましたが、正しく動作していません。

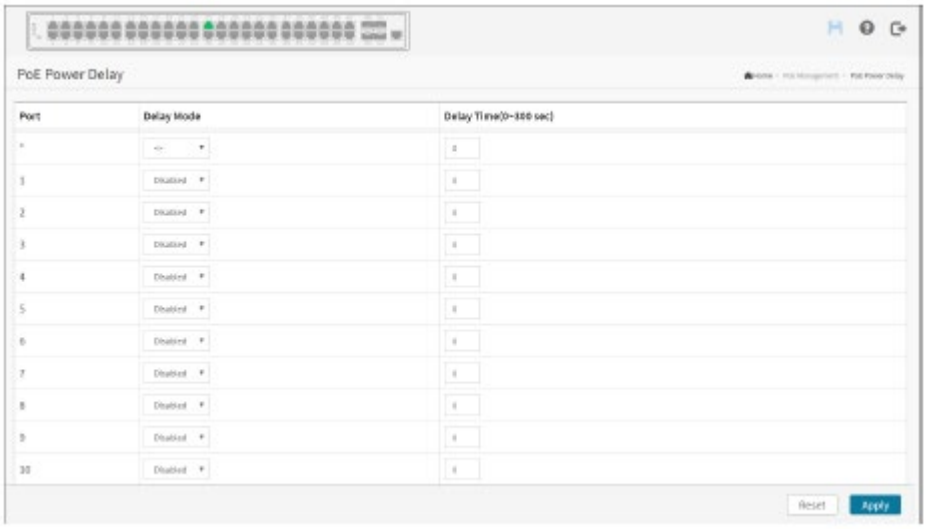
■ボタン

Auto-refresh（自動更新）：
画面を自動的に更新する場合は、このチェックボックスをONにしてください。自動更新は3秒間隔で行われます。

Refresh（更新）：
クリックするとページを更新します。

PoE 電源の遅延

この画面では、デバイスの再起動後の電源供給の遅延時間を設定できます。



Web インターフェース

Web インターフェースで Power over Ethernet の状態を表示するには:

1. 「PoE Management」(PoE の管理) ＞ 「PoE Power Delay」(PoE 電源の遅延)をクリックしてください。
2. 電源デバイスに対するポートを有効にしてください。
3. 再起動時の電源供給遅延時間を指定してください。
4. 「Apply」(適用)をクリックして変更を適用してください。

■パラメーターの説明

Port (ポート) :

これは、この行の論理ポート番号です。

Delay Mode (遅延モード) :

電源遅延機能を ON/OFF にします。

Enabled (有効) :POE 電源遅延を有効にします。

Disabled (無効) :POE 電源遅延を無効にします。

Delay Time(0～300sec) (遅延時間 (0～300 秒)) :

再起動の際、PoE ポートは遅延時間が終了すると PD への電力供給を開始します。デフォルト:0、範囲:0～300 秒。

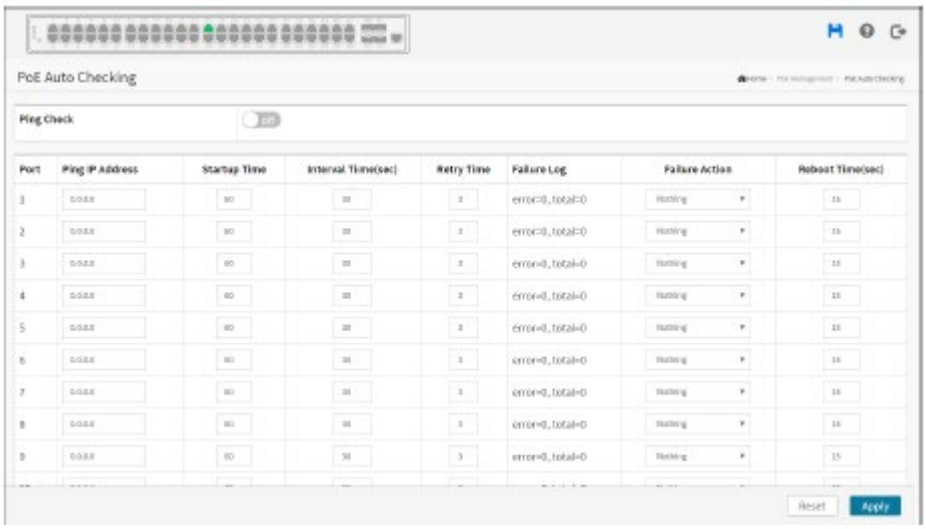
■ボタン

Apply(適用):
クリックすると、変更内容を保存します。

Reset(リセット):
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

PoE の自動チェック

この画面では、自動検出パラメーターを指定して、PoE ポートと PD 間におけるリンクの状態を確認できます。接続に失敗したことを検出すると、リモート PD を自動的に再起動します。



Web インターフェース

Web インターフェースで Power over Ethernet の自動チェック機能を設定するには:

1. 「PoE Management」(PoE の管理) ＞ 「PoE Auto Checking」(PoE の自動チェック)をクリックしてください。
2. Ping チェック機能を有効にしてください。
3. PD の IP アドレスを指定し、起動時間、インターバル時間、再試行時間、失敗アクション、および再起動時間を確認してください。
4. 「Apply」(適用)をクリックして変更を適用してください。

■パラメーターの説明

Ping Check(Ping チェック):

Ping チェック機能を有効にすると、PoE ポートと電源装置間の接続を検出できます。無効にすると、検出が OFF になります。

Port(ポート):

これは、この行の論理ポート番号です。

Ping IP Address(Ping する IP アドレス):

システムが ping を送信する PD の IP アドレスです。

Startup Time（起動時間）:
起動後、デバイスは自動チェックを有効にします。デフォルト:30、範囲:30～60 秒。

Interval Time(sec)（インターバル時間（秒））:
デバイスは、インターバル時間ごとにチェックメッセージを PD に送信します。デフォルト:30、範囲:10～120 秒。

Retry Time（再試行時間）:
PoE ポートが PD に ping できない場合は、再度検出の送信を再試行します。3 回目には、失敗アクションが実行されます。デフォルト:3、範囲:1～5。

Failure Log（エラーログ）:
エラーログのカウンターです。

Failure Action（エラーアクション）:
3 番目のエラー検出時に実行されるアクションです。
Nothing（なし）:リモート PD に Ping を実行しますが、それ以上は何も実行しません。
Reboot（再起動）:PoE ポートの電源を切り、PD を再起動します。

Reboot time (sec)（再起動時間（秒））:
PD が再起動されると、PoE ポートは指定された時間が経過した後に電源を回復します。デフォルト:15、範囲:3～120 秒。

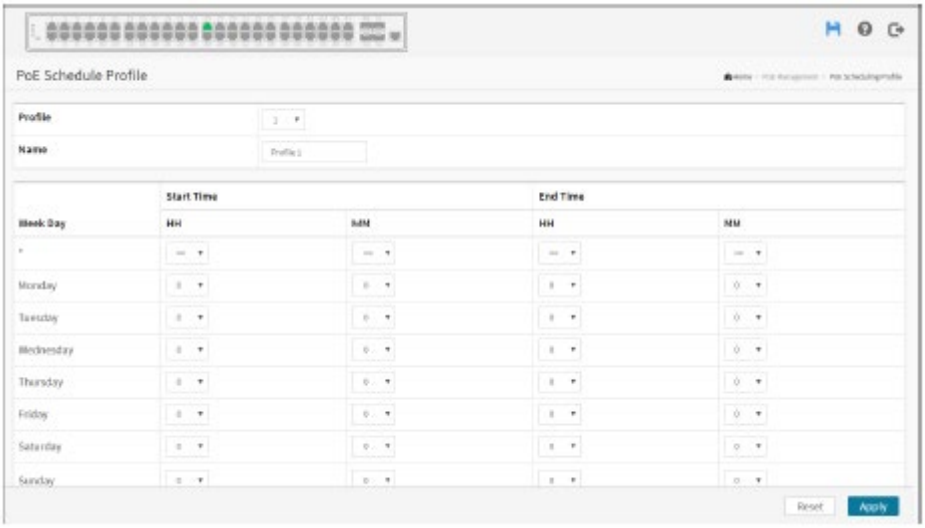
■ボタン

Apply（適用）:
クリックすると、変更内容を保存します。

Reset（リセット）:
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

PoE スケジューリングのプロファイル

この画面では、PoE スケジューリングのプロファイルを定義できます。



Web インターフェース

Web インターフェースで PoE スケジュールプロファイルを設定するには:

1. 「PoE Management」(PoE の管理) ＞ 「PoE Scheduling Profile」(PoE スケジューリングのプロファイル)をクリックしてください。
2. プロファイル番号を選択し、プロファイル名を指定してください。
3. 「Week Day」(曜日)を選択したら、「Start Time」(開始時刻)、「End Time」(終了時刻)を指定してください。
4. 「Apply」(適用)をクリックして変更を適用してください。

■パラメーターの説明

Profile(プロファイル):

プロファイルのインデックスです。設定には 16 種類のプロファイルがあります。

Name(名前):

プロファイルの名前です。デフォルト名は「Profile#」です。ユーザーは、プロファイルを識別するための名前を定義できます。

Week Day(曜日):

PoE をスケジュールする曜日です。

Start Time（開始時刻）:
PoE を開始する時刻です。時刻「00:00」は、この日の最初の秒を意味します。

End Time（終了時刻）:
PoE を停止する時間です。時刻「00:00」は、この日の最後の秒を意味します。

■ボタン

Apply（適用）:
クリックすると、変更内容を保存します。

Reset（リセット）:
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

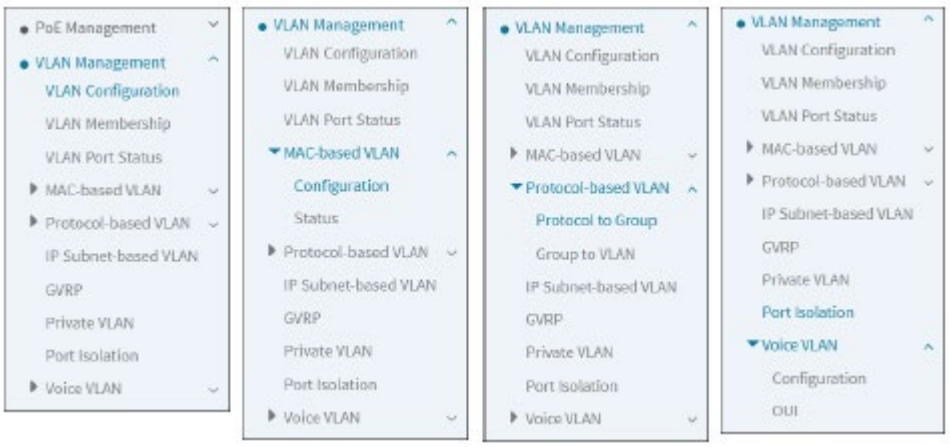
第 6 章
VLAN の管理

概要

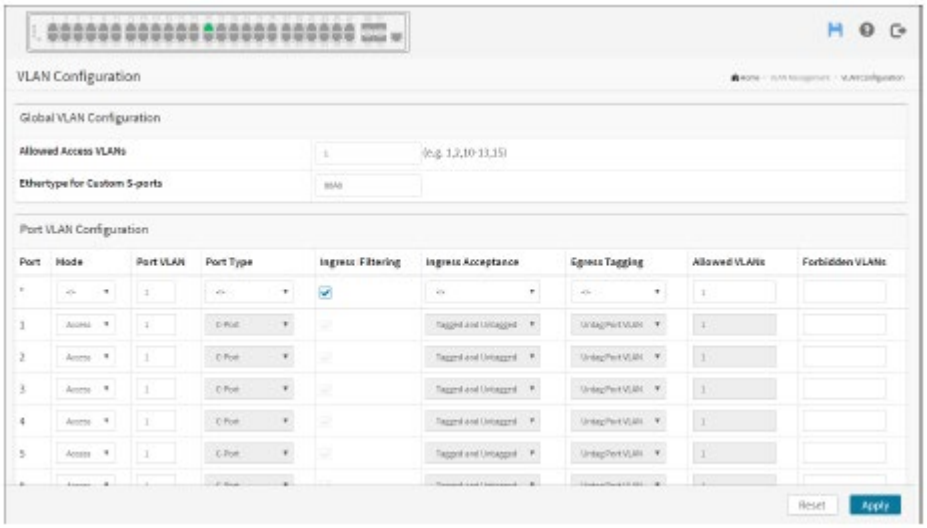
管理用に特定の VLAN を割り当てます。管理 VLAN は、VLAN 内のポートに接続されたワークステーションからスイッチへの IP 接続を確立するために使用されます。この接続は、VSM、SNMP、および TELNET セッションをサポートします。デフォルトでは、アクティブ管理 VLAN は VLAN1 ですが、「Management VLAN」（管理 VLAN）ウィンドウを使用して、任意の VLAN を管理 VLAN として指定できます。一度にアクティブにできる管理 VLAN は 1 つだけです。

新しい管理 VLAN を指定すると、古い管理 VLAN への HTTP 接続が失われます。このため、管理ステーションと新しい管理 VLAN 内のポートの間に接続するか、マルチ VLAN ルートを介して新しい管理 VLAN に接続する必要があります。

メニューとサブメニューを以下に示します。



VLAN の設定



Web インターフェース

Web インターフェースで VLAN メンバーシップの設定を行うには:

1. 「VLAN Management」(VLAN の管理) ＞ 「VLAN Configuration」(VLAN の設定)をクリックしてください。
2. 「Global VLAN Configuration」(グローバル VLAN の設定)パラメーターを変更してください。
3. 「Port LAN Configuration」(ポート VLAN の設定)パラメーターの、「Mode」(モード)、「Port VLAN」(ポート VLAN)、および「Port Type」(ポートタイプ)を設定してください。
4. 「Apply」(適用)をクリックして設定を保存してください。
5. 設定を取り消す場合は、「Reset」(リセット)ボタンをクリックする必要があります。そうすると、以前に保存した値へと戻ります。

■パラメーターの説明

Global VLAN Configuration(グローバル VLAN の設定)

Allowed Access VLANs(許可されたアクセス VLAN):

このフィールドには、スイッチで作成された VLAN が表示されます。

デフォルトでは、VLAN1 のみが存在します。リスト構文を使用して、個々の要素をカンマで区切ることで、より多くの VLAN を作成できます。範囲は、下限と上限を区切るダッシュで指定します。

次の例では、VLAN1、10、11、12、13、200、および 300 を作成します:1,10-13,200,300。区切り文字の間にはスペースを入れることができます。

Ethertype for Custom S-ports（カスタム S ポートのイーサタイプ）:
この項目は、カスタム S ポートに使用されるイーサタイプ/TPID（16 進数で指定）を指定します。この設定は、「Port Type」（ポートタイプ）が「S-Custom-Port」に設定されているすべてのポートに対して有効です。

Port VLAN Configuration（ポート VLAN の設定）

Port（ポート）:
これは、この行の論理ポート番号です。

Mode（モード）:
ポートモード（デフォルトは Access）によって、該当するポートの基本的な動作が決まります。ポートは、次の 3 つのモードのいずれかになります。特定のモードが選択されると、その行の残りのフィールドはグレー表示になったり、問題のモードに応じて変更可能になったりします。グレー表示された項目は、モードが適用されたときにポートが取得する値を示します。

Access（アクセス）:
アクセスポートは通常、末端のステーションに接続するために使用されます。音声 VLAN などの動的機能は、背後にある VLAN にポートを追加する場合があります。アクセスポートには、次の特性があります。

- デフォルトでは 1 であるポート VLAN（別名：アクセス VLAN）のメンバーです。
- タグなしフレームと C タグ付きフレームを受け入れます。
- アクセス VLAN に分類されていないすべてのフレームを破棄します。
- 出口では、すべてのフレームはタグなしで送信されます。

Trunk（トランク）:
トランクポートは、複数の VLAN で同時にトラフィックを伝送でき、通常は他のスイッチに接続するために使用されます。トランクポートには、以下の特性があります。

- デフォルトでは、トランクポートはすべての既存 VLAN のメンバーです。これは許可された VLAN の使用によって制限されるかもしれません。
- VLAN のトランクがポートで有効になっていない限り、ポートがメンバーになっていない VLAN に分類されているフレームは破棄されます。
- デフォルトでは、ポート VLAN（別名：ネイティブ VLAN）に分類されているフレームを除く、すべてのフレームは出力でタグ付けされます。ポート VLAN に分類されたフレームは出力で C タグ付けされません。
- 出力タグ付けはすべてのフレームにタグ付けするように変更できます。この場合、入力

でタグ付けされたフレームのみが受け入れられます。

- VLANトランキングが有効になる場合があります。

Hybrid（ハイブリッド）：

ハイブリッドポートは、さまざまな点でトランクポートに似ていますが、新たなポート設定機能が追加されています。トランクポートの特性に加えて、ハイブリッドポートには以下の機能があります。

- VLAN タグ非対応、C タグ対応、S タグ対応、または Scustom タグ対応に設定できます。
- イングレスフィルタリングを制御できます。
- フレームのイングレスアクセプタンスと出力タギングの設定を個別に設定できます。

Port VLAN（ポート VLAN）：

ポートの VLAN ID（別名：PVID）を指定します。許可される VLAN の範囲は 1～4095 で、デフォルトは 1 です。

入力では、ポートが VLAN 非対応として設定されているか、フレームがタグなしであるか、ポートで VLAN 認識が有効になっていますが、フレームがプライオリティタグ付き（VLAN ID=0）である場合、フレームはポート VLAN に分類されます。

出力では、出力タグ設定がタグなしポート VLAN に設定されている場合、ポート VLAN に分類されたフレームはタグ付けされません。

ポート VLAN は、アクセスモードのポートの場合は「アクセス VLAN」、トランクまたはハイブリッドモードのポートの場合は「ネイティブ VLAN」と呼ばれます。

Port Type（ポートタイプ）：

ハイブリッドモードのポートでは、ポートタイプを変更できます。つまり、フレームの VLAN タグを使用して特定の VLAN への入力でフレームを分類するかどうか、および特定の VLAN への入力でフレームを分類する場合は、どの TPID に対応するかを指定できます。同様に、出力では、タグが必要な場合、ポートタイプによってタグの TPID が決まります。

Unaware（認識しない）：

入力では、VLAN タグを運ぶかどうかにかかわらず、すべてのフレームがポート VLAN に分類され、可能なタグは出力で削除されません。

C-Port（C ポート）：

入力では、TPID=0x8100 の VLAN タグを持つフレームは、タグに組み込まれた VLAN ID に分類されます。フレームがタグなしまたは優先度タグ付きの場合、フレームはポート VLAN に分

類されます。出力側でフレームにタグを付ける必要がある場合、フレームには C タグが付けられます。

S-Port（S ポート）：
入力では、TPID=0x8100 または 0x88A8 の VLAN タグを持つフレームは、タグに組み込まれた VLAN ID に分類されます。フレームがタグなしまたはプライオリティタグ付きの場合、フレームはポート VLAN に分類されます。出力側でフレームにタグを付ける必要がある場合、フレームには S タグが付けられます。

S-Custom-Port（S カスタムポート）：
入力では、TPID=0x8100 またはカスタム S ポートに設定されたイーサタイプと等しい VLAN タグを持つフレームは、タグに組み込まれた VLAN ID に分類されます。フレームがタグなしまたは優先度タグ付きの場合、フレームはポート VLAN に分類されます。出力側でフレームにタグを付ける必要がある場合は、カスタム S タグが付けられます。

Ingress Filtering（イングレスフィルタリング）：
ハイブリッドポートでは、イングレスフィルタリングを変更できます。アクセスポートとトランクポートでは、常にイングレスフィルタリングが有効になっています。
イングレスフィルタリングが有効（チェックボックスが ON）の場合、ポートが get のメンバーでない VLAN に分類されたフレームは破棄されます。
イングレスフィルタリングが無効になっている場合、ポートがメンバーでない VLAN に分類されたフレームが受け入れられ、スイッチエンジンに転送されます。しかし、ポートは、メンバーではない VLAN に分類されたフレームを送信しません。

Ingress Acceptance（受信許可）：
ハイブリッドポートでは、入力で受け入れられるフレームのタイプを変更できます。

Tagged and untagged（タグ付きとタグなし）：
両方のタグ付きフレームとタグなしフレームが受け入れられます。

Tagged Only（タグ付きのみ）：
入力では、タグ付きフレームのみが受け入れられます。タグなしフレームは破棄されます。

Untagged Only（タグなしのみ）：
入力では、タグなしフレームのみが受け入れられます。タグ付きフレームは破棄されます。

Egress Tagging（出力方向のタグ付け）:
トランクおよびハイブリッドモードのポートは、出力側のフレームのタグ付けを制御できます。

Untag Port VLAN（ポート VLAN のタグ解除）:
ポートVLANに分類されるフレームはタグなしで送信されます。他のフレームは、関連するタグとともに送信されます。

Tag All（すべてタグ付き）:
すべてのフレームは、ポートVLANに分類されているかどうかにかかわらず、タグ付きで送信されます。

Untag All（すべてのタグを解除）:
すべてのフレームは、ポートVLANに分類されているかどうかにかかわらず、タグなしで送信されます。
このオプションは、ハイブリッドモードのポートでのみ使用できます。

Allowed VLANs（許可された VLAN）:
トランクおよびハイブリッドモードのポートは、メンバーになることを許可するVLANを制御できます。アクセスポートは、1 つの VLAN、つまりアクセス VLAN のメンバーにしかなれません。フィールドの構文は、「Existing VLANs」（既存の VLAN）フィールドで使用される構文と同じです。
デフォルトでは、ポートは可能なすべての VLAN のメンバーになる可能性があるため、1～4095 に設定されます。
この項目は空のままにしておくことができます。つまり、ポートは既存の VLAN のいずれのメンバーではないものの、VLANトランク用に設定されている場合は、すべての未知のVLANを伝送することができるということになります。

Forbidden VLANs（禁止された VLAN）:
ポートは、複数の VLAN のメンバーにならないように設定できます。これは、MVRP や GVRP などのダイナミック VLAN プロトコルが VLAN に動的にポートを追加しないようにする必要がある場合に特に役立ちます。
コツは、そのような VLAN を、問題のポートで禁止としてマークすることです。構文は、「Enabled VLANs」（有効になった VLAN）フィールドで使用される構文と同じです。
デフォルトでは、この項目は空白のままになっています。つまり、ポートはすべての VLAN のメンバーになる可能性があるということになります。

■ボタン

Apply（適用）:

クリックすると、変更内容を保存します。

Reset（リセット）：
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

VLAN のメンバーシップ

この画面では、VLAN ユーザーのメンバーシップの状態の概要を示します。

ポートは、ページヘッダーに反映されているように、現在選択されているスタックのユニットに属します。

Web インターフェース

Web インターフェースで VLAN メンバーシップを設定するには:

1. 「VLAN Management」(VLAN の管理) ＞ 「VLAN Membership」(VLAN のメンバーシップ)をクリックしてください。
2. バーをスクロールして、表示する VLAN を選択してください。
3. 「Refresh」(更新)をクリックして、状態を更新してください。

■パラメーターの説明

VLAN USER(VLAN ユーザー):

様々な内部ソフトウェアモジュールは、VLAN サービスを使用して、VLAN メンバーシップをその場で設定できます。

右側のドロップダウンリストでは、アドミニストレーター(Admin)が設定した VLAN メンバーシップを表示するか、これらの内部ソフトウェアモジュールのいずれかで設定した VLAN メンバーシップを表示するかを選択できます。

「Combined」(結合)エントリーには、アドミニストレーターと内部ソフトウェアモジュールの設定の組み合わせが表示され、基本的にハードウェアで実際に設定されている内容が反映されます。

VLAN USER（VLAN ユーザー）モジュールは、VLAN 管理機能のサービスを使用して、VLAN メンバーシップおよび PVID や UVID などの VLAN ポート設定を構成します。現在、次の VLAN ユーザータイプをサポートしています。

NAS：NAS は、ポートベースの認証を提供します。これには、サプリカント、オーセンティケーター、および認証サーバー間の通信が含まれます。

GVRP：「Generic VLAN Registration Protocol」(GVRP)を使用して、隣接する VLAN 対応デバイス間で VLAN 情報を交換できます。GVRP は「Generic Attribute Registration Protocol」(GARP)に基づいており、ブリッジネットワーク全体に VLAN 情報を伝播します。

MVR：MVR は、各 VLAN 内のサブスクライバーのマルチキャストトラフィックを複製する必要性をなくすために使用されます。すべてのチャネルのマルチキャストトラフィックは、単一（マルチキャスト）VLAN でのみ送信されます。

Voice VLAN（音声 VLAN）：音声 VLAN は、通常、IP 電話から発信される音声トラフィック用に特別に設定された VLAN です。

MSTP：「802.1s Multiple Spanning Tree Protocol」(MSTP)は、VLAN を使用してネットワーク内に複数のスパニングツリーを作成します。これにより、ループフリー環境を維持しながらネットワークリソースの使用率が大幅に向上します。

DMS：DMS VLAN メンバーシップの状態を表示します。

VCL：様々な MAC ベース VLAN ユーザーによって設定された MAC ベース VLAN エントリーを表示します。

VLAN ID：
ポートメンバーが表示される VLAN ID です。

Port Members（ポートメンバー）：
各ポートのチェックボックスの行は、VLAN ID ごとに表示されます。ポートが VLAN に含まれている場合、「 U 」と「 T 」のイメージが表示されます。タグ付きかタグなしかにかかわらず、出力フィルタリングフレームの状態を表示します。ポート VLAN に分類されるフレームは、タグ付き（ T ）またはタグなし（ U ）で送信されます。

VLAN Membership（VLAN のメンバーシップ）:
「VLAN Membership Status」（VLAN メンバーシップの状態）画面には、選択された VLAN ユーザーによって設定されたすべての VLAN の現在の VLAN ポートメンバーが表示されます（コンボボックスによって選択が許可されます）。結合されたユーザーを選択すると、すべての VLAN ユーザーについてこの情報を表示する必要があります。これはデフォルトです。VLAN メンバーシップは、VLAN ID に分類されたフレームを、それぞれの VLAN メンバーポートで転送することを可能にします。

Show entries（エントリーの表示）:
表示する項目の数を選択できます。

VLAN ユーザーを選択できます。

■ボタン

Auto-refresh（自動更新）:
画面を自動的に更新する場合は、このチェックボックスを ON にしてください。自動更新は 3 秒間隔で行われます。

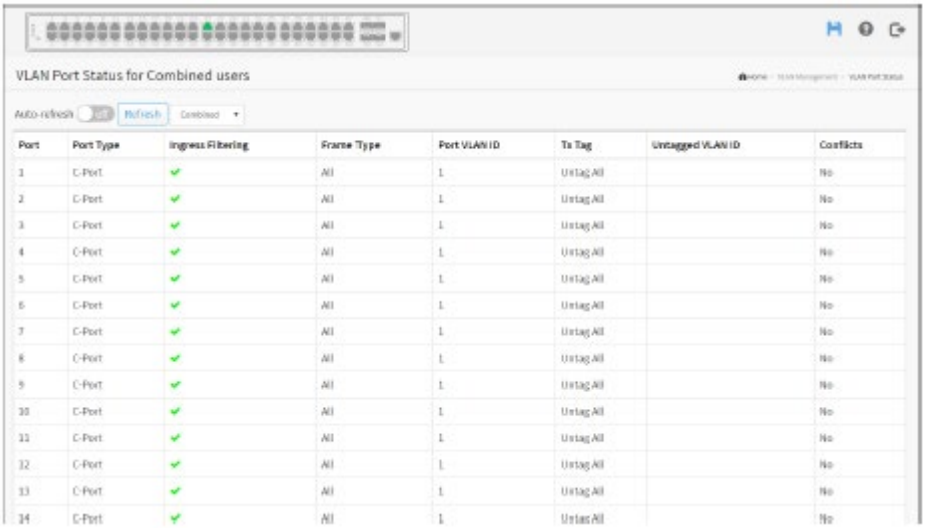
Refresh（更新）:
クリックするとページを更新します。

First Page（最初のページ）:
リストを更新し、最初のページに戻ります。

Next Page（次のページ）:
リストを更新し、次のページに進みます。

VLAN ポートの状態

ポートの状態機能は、すべての VLAN の状態に関する情報を収集し、結合、管理、NAS、GVRP、MVR、音声 VLAN、MSTP、DMS、VCL の順に報告します。



Web インターフェース

Web インターフェースで VLAN ポートの状態を表示するには:

1. 「VLAN Management」(VLAN の管理) ＞ 「VLAN Port Status」(VLAN ポートの状態)をクリックしてください。
2. 「Combined」(結合)、「Admin」、「NAS」、「GVRP」、「MVR」、「Voice VLAN」(音声 VLAN)、「MSTP」、「DMS」、「VCL」、「RMirror」(R ミラー)を指定してください。
3. ポートの状態に関する情報を表示してください。

■パラメーターの説明

VLAN USER(VLAN ユーザー):

VLAN ユーザーモジュールは、VLAN 管理機能のサービスを使用して、VLAN メンバーシップと、PVID、UVID などの VLAN ポート設定を定義します。現在、以下の VLAN ユーザータイプをサポートしています。

NAS:NAS は、ポートベースの認証を提供します。これには、サプリカント、オーセンティケーター、および認証サーバー間の通信が含まれます。

GVRP:「Generic VLAN Registration Protocol」(GVRP)を使用して、隣接する VLAN 対応デバ

イス間で VLAN 情報を交換できます。GVRP は「Generic Attribute Registration Protocol」(GARP)に基づいており、ブリッジネットワーク全体に VLAN 情報を伝播します。

MVR：MVR は、各 VLAN 内のサブスクライバーのマルチキャストトラフィックを複製する必要性をなくすために使用されます。すべてのチャネルのマルチキャストトラフィックは、単一（マルチキャスト）VLAN でのみ送信されます。

Voice VLAN（音声 VLAN）：音声 VLAN は、通常、IP 電話から発信される音声トラフィック用に特別に設定された VLAN です。

MSTP：「802.1s Multiple Spanning Tree Protocol」(MSTP)は、VLAN を使用してネットワーク内に複数のスパニングツリーを作成します。これにより、ループフリー環境を維持しながらネットワークリソースの使用率が大幅に向上します。

DMS：DMS VLAN メンバーシップの状態を表示します。

VCL：様々な MAC ベース VLAN ユーザーによって設定された MAC ベース VLAN エントリーを表示します。

Port（ポート）：
同じ行に含まれる設定の論理ポートです。

Port Type（ポートタイプ）：
ポートタイプを表示します。ポートタイプには、「Unaware」（認識しない）、「C-port」（C ポート）、「S-port」（S ポート）、「Custom S-port」（カスタム S ポート）のいずれかを指定できます。
ポートタイプが「Unaware」（認識しない）の場合、すべてのフレームは「Port VLAN ID」（ポート VLAN ID）に分類され、タグは削除されません。「C-port」（C ポート）は「Customer Port」（カスタマーポート）です。「S-port」（S ポート）は「Service Port」（サービスポート）です。「Custom S-port」（カスタム S ポート）は、カスタム TPID を持つ S ポートです。

Ingress Filtering（イングレスフィルタリング）：
ポートのイングレスフィルタリングを表示します。このパラメーターは、VLAN 入力処理に影響します。イングレスフィルタリングが有効で、イングレスポートが分類された VLAN のメンバーでない場合、フレームは破棄されます。

Frame Type（フレームタイプ）：

ポートがすべてのフレームを受け入れるか、タグ付きフレームのみを受け入れるかを示します。このパラメーターは、VLAN 入力処理に影響します。ポートがタグ付きフレームのみを受け入れる場合、そのポートで受信したタグなしフレームは破棄されます。

Port VLAN ID（ポート VLAN ID）：
特定のユーザーがポートに設定するポート VLAN ID（PVID）を表示します。選択したユーザーによって上書きされない場合、この項目は空です。

Tx Tag（送信タグ）：
タグ付きかタグなしかにかかわらず、出力フィルタリングフレームの状態を表示します。

Untagged（タグなし）
「Tx Tag」（送信タグ）が選択したユーザーによって上書きされ、タグ付き UVID、またはタグなし UVID に設定されている場合、このフィールドには、送信時にタグ付けまたはタグ解除する VLAN ID が表示されます。選択したユーザーによって上書きされない場合、この項目は空です。

Conflicts（競合）：
2 人のユーザーがポートの設定に矛盾する要件を持っている可能性があります。例えば、あるユーザーがすべてのフレームで出力にタグ付けすることを要求し、別のユーザーがすべてのフレームで出力にタグ付けしないことを要求する場合があります。
両方のユーザーが折り合わないことで、競合が発生しますが、これは優先順位付けされた方法で解決されます。優先順位が最も低いのは、管理者です。その他のソフトウェアモジュールは、ドロップダウンリスト内の位置に応じて優先順位が付けられます。リスト内の高い方が、優先順位が高くなります。
競合が存在する場合は、「Combined」（結合）ユーザーおよび問題のソフトウェアモジュールに対して「Yes」と表示されます。
「Combined」（結合）ユーザーには、実際にハードウェアで設定されている内容が反映されます。

:

VLAN ユーザーを選択できます。

■ボタン

Auto-refresh（自動更新）:
画面を自動的に更新する場合は、このチェックボックスをONにしてください。自動更新は3秒間隔で行われます。

Refresh（更新）:
クリックするとページを更新します。

MAC ベース VLAN

設定

MAC アドレスとVLAN ID のマッピングは、ここで設定できます。この画面では、MAC ベースVLAN 分類リストエントリーを追加および削除し、エントリーを別ポートに割り当てることができます。

Web インターフェース

Web インターフェースで MAC アドレスベースの VLAN 設定を定義するには:

1. 「VLAN Management」(VLAN の管理) ＞ 「MAC-based VLAN and Configuration」(MAC ベース VLAN と設定)をクリックしてください。
2. 「Add New Entry」(新規登録)をクリックしてください。

3. MAC アドレスと VLAN ID を指定してください。

4. 「Apply」（適用）をクリックしてください。

■パラメーターの説明

MAC Address（MAC アドレス）：
MAC アドレスを示します。

VLAN ID：
VLAN ID を示します。

Port Members（ポートメンバー）：
各ポートのチェックボックスの行は、MAC から VLAN ID へのマッピングエントリーごとに表示されます。マッピングにポートを含めるには、チェックボックスを ON にしてください。マッピングからポートを削除または除外するには、チェックボックスが OFF になっていることを確認してください。デフォルトでは、どのポートもメンバーになっておらず、すべてのボックスは OFF になっています。

■ボタン

Adding New Entry（新規登録）：
クリックすると、新しい MAC ベース VLAN エントリーを追加します。空の行がテーブルに追加されるため、必要に応じて MAC ベース VLAN エントリーを設定できます。MAC ベース VLAN エントリーには、任意のユニキャスト MAC アドレスを設定できます。ブロードキャストまたはマルチキャスト MAC アドレスは許可されません。VLAN ID の有効な値は 1～4095 です。

Delete（削除）：
MAC ベース VLAN エントリーを削除するには、このチェックボックスを ON にして「Apply」（適用）を押してください。エントリーは、スタック内の選択したスイッチ上で削除されます。

Apply（適用）：
クリックすると、変更内容を保存します。

Reset（リセット）：
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

■ボタン

Auto-refresh（自動更新）:
画面を自動的に更新する場合は、このチェックボックスをONにしてください。自動更新は3秒間隔で行われます。

Refresh（更新）:
クリックするとページを更新します。

First Page（最初のページ）:
リストを更新し、最初のページに戻ります。

Next Page（次のページ）:
リストを更新し、次のページに進みます。

状態

MAC ベース VLAN の状態を表示します。

Web インターフェース
Web インターフェースに MAC ベース VLAN のアドレス設定を表示するには:

1. 「VLAN Management」（VLAN の管理） ＞ 「MAC-based VLAN and Configuration」（MAC ベース VLAN と設定）をクリックしてください。
2. 情報を自動更新する場合は、「Auto-refresh」（自動更新）を呼び出す必要があります。
3. 「Refresh」（更新）をクリックして、MAC ベース VLAN メンバーシップの状態を更新してください。

■パラメーターの説明

MAC Address（MAC アドレス）:
MAC アドレスを示します。

VLAN ID:
VLAN ID を示します。

Port Members（ポートメンバー）:
MAC ベース VLAN エントリーのポートメンバーです。

■ボタン

Auto-refresh（自動更新）:
画面を自動的に更新する場合は、このチェックボックスを ON にしてください。自動更新は 3 秒間隔で行われます。

Refresh（更新）:
クリックするとページを更新します。

プロトコルベース VLAN

このセクションでは、プロトコルベースVLANについて説明します。スイッチがサポートするプロトコルには、「Ethernet LLC SNAP Protocol」が含まれます。

LLC

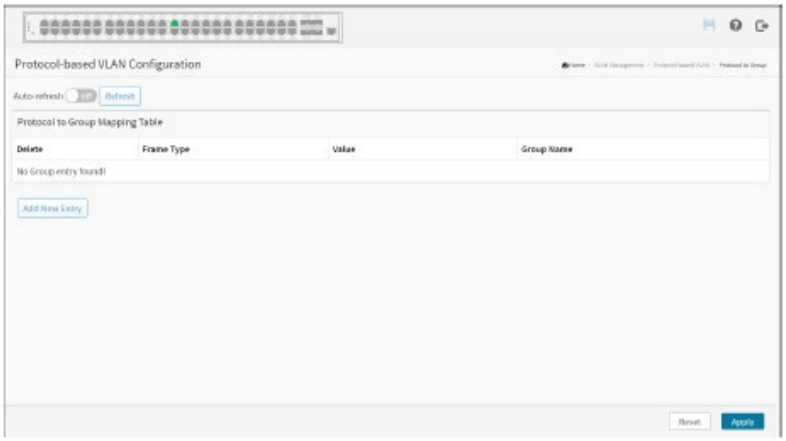
論理リンク制御（LLC）データ通信プロトコル層は、OSI 7 階層参照モデルにおけるデータリンク層（それ自体は物理層のすぐ上のレイヤ 2）の上部サブ層です。複数のネットワークプロトコル（IP、IPX、Decent、Appletalk）がマルチポイントネットワーク内で共存し、同じネットワークメディアを介して転送できるようにする多重化メカニズムを提供し、フローコントロールおよび自動リピート要求（ARQ）エラー管理メカニズムも提供できます。

SNAP

サブネットワークアクセスプロトコル（SNAP）は、IEEE802.2LLC を使用するネットワーク上で、8 ビット 802.2 サービスアクセスポイント（SAP）フィールドで区別できるよりも多くのプロトコルを多重化するためのメカニズムです。SNAP は、イーサネットタイプのフィールド値によるプロトコルの識別をサポートします。また、ベンダー独自のプロトコルにおける識別子スペースもサポートします。このプロトコルは、IEEE802.3、IEEE802.4、IEEE802.5、IEEE802.11 およびその他の IEEE802 物理ネットワーク層、および802.2LLCを使用するFDDIなどの非IEEE802物理ネットワーク層で使用されます。

グループに対するプロトコル

この画面では、エントリーをマッピングするグループ名（グループごとに固有）に新しいプロトコルを追加したり、選択したスタックスイッチのユニットスイッチに対して既にマッピングされているエントリーを表示したり削除したりすることができます。



Web インターフェース

Web インターフェースで、プロトコルベース VLAN を設定するには:

1. 「VLAN Management」(VLAN の管理) ＞ 「Protocol-based VLAN and Protocol to Group」(プロトコルベース VLAN とグループに対するプロトコル)をクリックしてください。
2. 「Add New Entry」(新規登録)をクリックしてください。

3. 「Frame Type」(フレームタイプ)、「Value」(値)、および「Group Name」(グループ名)を指定してください。
4. 「Apply」(適用)をクリックしてください。

■パラメーターの説明

Frame Type(フレームタイプ):

フレームタイプには、次のいずれかの値を指定できます。

1. イーサネット
2. LLC
3. SNAP

注意: この項目を変更する場合、以下のテキスト項目の有効な値は、選択した新しいフレームタイプによって異なります。

Value（値）:
このテキストフィールドに入力できる有効な値は、前のフレームタイプの選択メニューで選んだオプションによって異なります。
以下は、3 種類の異なるフレームタイプの基準です。

1. イーサネットの場合：フレームタイプとしてイーサネットが選択されている場合のテキストフィールドの値を「etype」と呼びます。etype の有効な値の範囲は 0x0600～0xffff です。
2. LLC の場合：この場合の有効な値は、2 つの異なるサブ値から構成されます。
   a. DSAP：1 バイト長の文字列（0x00～0xff）
   b. SSAP：1 バイト長の文字列（0x00～0xff）
3. SNAP の場合：この場合の有効な値は、2 つの異なるサブ値から構成されます。
   a. OUI：OUI(Organizationally Unique Identifier)は、「*xxx-xx*」形式の値です。文字列の各ペア（*xx*）は、0x00～0xff の 16 進値の範囲です。
   b. PID：OUI が 16 進数の 00000000 の場合、プロトコル ID は、SNAP 上で実行されているプロトコルのイーサネットタイプ（EtherType）フィールドの値になります。OUI が特定の組織の OUI である場合、プロトコル ID は、その組織によって SNAP 上で実行されているプロトコルに割り当てられた値になります。

Group Name（グループ名）:
有効なグループ名は、固有の 16 文字から構成される文字列です。

■ボタン

Delete（削除）:
グループに対してに割り当てられたエントリーを削除するには、このボックスを ON にしてください。エントリーは、次回の保存時にスイッチ上で削除されます。

Add New Entry（新規登録）:
クリックすると、マッピングテーブルに新しいエントリーを追加します。空の行がテーブルに追加されます。そうしたら、必要に応じて、「Frame Type」（フレームタイプ）、「Value」（値）、および「Group Name」（グループ名）を設定できます。
このボタンを使用すると、新しいエントリーの追加を元に戻すことができます。

Apply（適用）:
クリックすると、変更内容を保存します。

Reset（リセット）:
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

VLAN に対するグループ

このセクションでは、すでに設定されているグループ名を、選択したスタックスイッチのユニットスイッチの VLAN へとマッピングできます。

Web インターフェース

Web インターフェースで設定された VLAN マッピングテーブルにグループ名を設定するには:

1. 「VLAN Management」(VLAN の管理) ＞ 「Protocol-based VLAN and Group to VLAN」(プロトコルベース VLAN と VLAN に対するグループ)をクリックしてください。
2. 「Add New Entry」(新規登録)をクリックしてください。

3. 「Group Name」(グループ名)と「VLAN ID」を指定してください。
4. 「Apply」(適用)をクリックしてください。

■パラメーターの説明

Group Name(グループ名):

有効なグループ名は、固有の 16 文字から構成される文字列です。

VLAN ID：
グループ名がマッピングされる ID を示します。有効な VLAN ID の範囲は 1～4095 です。

Port Members（ポートメンバー）：
各ポートのチェックボックスの行は、グループ名と VLAN ID のマッピングごとに表示されます。マッピングにポートを含めるには、チェックボックスを ON にしてください。マッピングからポートを削除または除外するには、チェックボックスが OFF になっていることを確認してください。デフォルトでは、どのポートもメンバーになっておらず、すべてのボックスは OFF になっています。

■ボタン

Delete（削除）：
VLAN に対して割り当てられたグループ名のエントリーを削除するには、このチェックボックスを ON にしてください。エントリーは、次回の保存時にスイッチ上で削除されます。

Add New Entry（新規登録）：
クリックすると、マッピングテーブルに新しいエントリーを追加します。テーブルに空の行が追加されます。そうしたら、必要に応じて「Group Name」（グループ名）、VLAN ID、および「Port Members」（ポートメンバー）を設定できます。VLAN ID の有効な値は 1～4095 です。このボタンを使用すると、新しいエントリーの追加を元に戻すことができます。

Apply（適用）：
クリックすると、変更内容を保存します。

Reset（リセット）：
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

Auto-refresh（自動更新）：
画面を自動的に更新する場合は、このチェックボックスを ON にしてください。自動更新は 3 秒間隔で行われます。

Refresh（更新）：
クリックするとページを更新します。

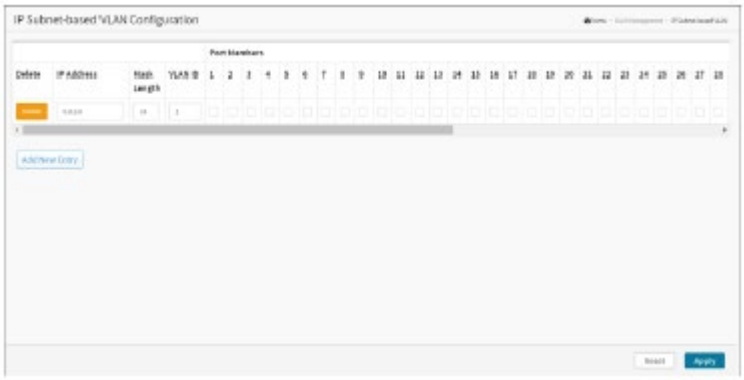
IP サブネットベース VLAN

IP サブネットベース VLAN のエントリーは、ここで設定できます。この画面では、IP サブネットベース VLAN に関するエントリーの追加、更新、削除ができます。

Web インターフェース

Web インターフェースで IP サブネットベース VLAN のメンバーシップを設定するには:

1. 「VLAN Management」(VLAN の管理) ＞ 「IP Subnet-based VLAN」(IP サブネットベース VLAN)をクリックしてください。
2. 「Add New Entry」(新規登録)をクリックしてください。



3. 「IP Address」(IP アドレス)、「Mask Length」(マスク長)、「VLAN ID」を指定してください。
4. 「Apply」(適用)をクリックしてください。

■パラメーターの説明

IP Address（IP アドレス）：
IP アドレスを表示します。

Mask Length（マスク長）：
ネットワークマスクの長さを示します。

VLAN ID：
VLAN ID を示します。既存エントリーの VLAN ID を変更できます。

Port Members（ポートメンバー）：
各ポートのチェックボックスの行は、IP サブネットと VLAN ID のマッピングエントリーごとに表示されます。マッピングにポートを含めるには、チェックボックスを ON にしてください。マッピングからポートを削除または除外するには、チェックボックスが OFF になっていることを確認してください。デフォルトでは、どのポートもメンバーになっておらず、すべてのボックスは OFF になっています。

■ボタン

Delete（削除）：
IP サブネットベース VLAN のエントリーを削除するには、このチェックボックスを ON にして「Save」（保存）を押してください。エントリーは、スタック内の選択したスイッチ上で削除されます。

Add New Entry（新規登録）：
クリックすると、新しい IP サブネットベース VLAN のエントリーを追加します。空の行がテーブルに追加され、必要に応じて IP サブネットベース VLAN のエントリーを設定できます。IP サブネットベース VLAN のエントリーには、任意の IP アドレス/マスクを設定できます。VLAN ID の有効な値は 1～4095 です。
「Save」（保存）をクリックすると、選択したスタックのスイッチユニットで IP サブネットベース VLAN のエントリーが有効になります。「Delete」（削除）ボタンを使用すると、新しい IP サブネットベース VLAN の追加を取り消すことができます。IP サブネットベース VLAN のエントリーの最大数は 128 に制限されています。

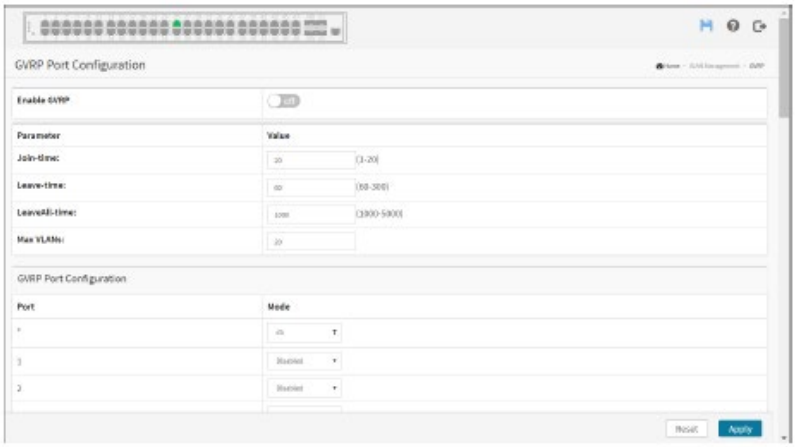
Apply（適用）：
クリックすると、変更内容を保存します。

Reset（リセット）：
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

GVRP

「Generic Attribute Registration Protocol」(GARP)は、ブリッジ LAN 内のデバイス(エンドステーションやスイッチなど)が、VLAN 識別子などの属性値を相互に登録および登録解除できる汎用フレームワークを提供します。この場合、属性はブリッジ LAN 内のデバイスに伝搬され、これらのデバイスはアクティブトポロジーのサブセットである到達可能性ツリーを形成します。GARP は、属性値の登録および登録解除のためのアーキテクチャー、操作規則、状態マシンおよび変数を定義します。

スイッチまたはエンドステーションへの GARP 参加は、GARP アプリケーションコンポーネントと、各ポートまたはスイッチに関連付けられた「GARP Information Declaration」(GID)コンポーネントから構成されます。ブリッジ内の同じアプリケーションに対する GARP 参加者間の情報の伝播は、「GARP Information Declaration」(GIP)コンポーネントによって実行されます。プロトコル交換は、関係するGARPアプリケーションに定義されたグループMACアドレスとPDUフォーマットを使用して、LLC タイプ 1 サービスによって GARP 参加者間で行われます。



Web インターフェース

Web インターフェースで GVRP を設定するには:

1. 「VLAN Management」(VLAN の管理) ＞ 「GVRP」をクリックしてください。
2. GVRP を有効または無効にしてください。
3. 「Join-time」(Join タイマー)、「Leave-time」(Leave タイマー)、「Leave-All-time」(Leave-All タイマー)、「Max VLAN」(最大 VLAN)を指定してください。
4. 「Mode」(モード)を有効または無効にしてください。
5. 「Apply」(適用)をクリックして設定を保存してください。
6. 設定を取り消す場合は、「Reset」(リセット)ボタンをクリックする必要があります。そうすると、以

前に保存した値へと戻ります。

■パラメーターの説明

Enable GVRP globally（GVRP をグローバルで有効にする）:
GVRP 機能は、「Enable GVRP」（GVRP を有効にする）チェックボックスのチェックマークを ON にすると有効になります。

GVRP protocol timers（GVRP プロトコルタイマー）:
「Join-time」（Join タイマー）は、100 秒単位（1/100 秒単位）の 1～20 の範囲の値です。デフォルトでは 20 に設定されています。
「Leave-time」（Leave タイマー）は、60～300 の範囲の値で、センチ秒単位、つまり 1/100 秒単位です。デフォルトでは 60 に設定されています。
「Leave All-time」（Leave All タイマー）は、1000～5000 秒単位の値です。つまり、1/100 秒単位です。デフォルトでは 1000 に設定されています。

Max VLANs（最大 VLAN）:
GVRP を有効にすると、GVRP でサポートされる VLAN の最大数が指定されます。デフォルトでは、この値は 20 です。この値は、GVRP が OFF になっている場合にのみ変更できます。

Port（ポート）:
「Port」（ポート）列にポートのリストが表示されます。

Mode（モード）:
この設定では、特定のポートにおける GVRP モードをローカルで有効/無効にします。

Disable（無効）:このポートで GVRP モードを無効にする場合に選択してください。

GVRP Enable（GVRP 有効）:このポートで GVRP モードを有効にする場合に選択してください。

■ボタン

Apply（適用）:
クリックすると、変更内容を保存します。

Reset（リセット）:
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

プライベート VLAN

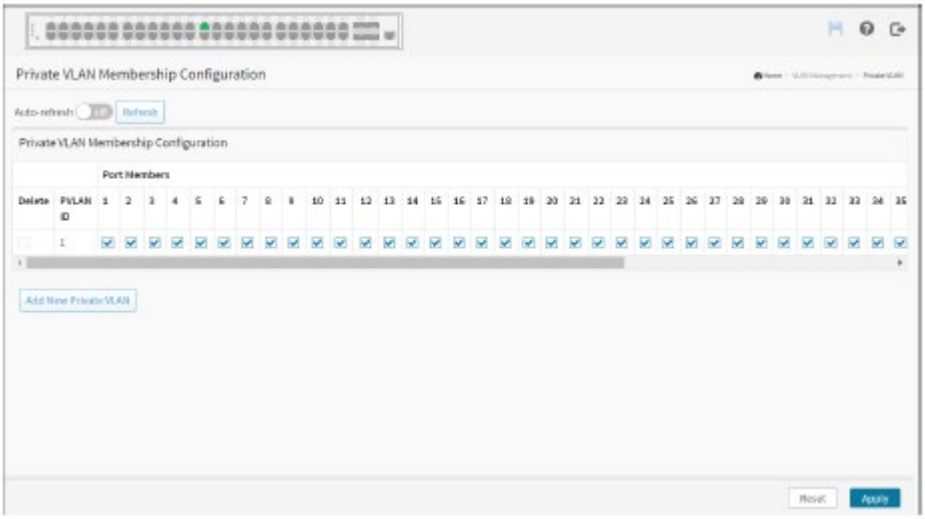
スイッチのプライベートVLANのメンバーシップ設定は、ここで監視および変更できます。プライベートVLAN、および各プライベートVLANのポートメンバーは、ここで追加または削除できます。

プライベートVLANは送信元ポートマスクに基づいており、VLANへの接続はありません。つまり、VLAN IDとプライベートVLAN IDは同じにすることができます。

パケットを転送できるようにするには、ポートがVLANとプライベートVLANの両方のメンバーである必要があります。デフォルトでは、すべてのポートはVLAN unawareであり、VLAN1およびプライベートVLAN1のメンバーです。

VLAN unawareポートは、1つのVLANのメンバーにしかなれませんが、複数のプライベートVLANのメンバーになれます。

VLANの優先順位:
音声VLAN ＞ MACベースVLAN ＞ プロトコルベースVLAN ＞ タグベースVLAN



Webインターフェース
Webインターフェースでプライベート VLANのメンバーシップを設定するには:

1. 「VLAN Management」(VLANの管理) ＞ 「Private VLAN」(プライベートVLAN)をクリックしてください。
2. スイッチのプライベートVLANメンバーシップの設定を行ってください。
3. 「Apply」(適用)をクリックしてください。

■パラメーターの説明

Delete（削除）:
プライベート VLAN のエントリーを削除するには、このチェックボックスを ON にしてください。エントリーは、次回の適用時に削除されます。

Private VLAN ID（プライベート VLAN ID）:
この特定のプライベート VLAN の ID を示します。

Port Members（ポートメンバー）:
各ポートのチェックボックスの行は、プライベート VLAN ID ごとに表示されます。プライベート VLAN にポートを含めるには、チェックボックスを ON にしてください。プライベート VLAN からポートを削除または除外するには、このボックスが OFF になっていることを確認してください。デフォルトでは、どのポートもメンバーになっておらず、すべてのボックスは OFF になっています。

Add New Private VLAN（新規プライベート VLAN の追加）:
クリックすると、新しいプライベート VLAN ID を追加します。空の行がテーブルに追加され、必要に応じてプライベート VLAN を設定できます。プライベート VLAN ID に許可される範囲は、スイッチのポート番号範囲と同じです。この範囲外の値は受け入れられず、警告メッセージが表示されます。そのような場合には、「OK」をクリックして間違ったエントリーを破棄するか、「Cancel」（キャンセル）をクリックして編集に戻り、修正を行ってください。
「Apply」（適用）をクリックすると、プライベート VLAN が有効になります。
このボタンを使用して、新しいプライベート VLAN の追加を取り消すことができます。

■ボタン

Apply（適用）:
クリックすると、変更内容を保存します。

Reset（リセット）:
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

ポートアイソレーション

ポートアイソレーションは、トラフィックフローを制限するために、同じ VLAN 上のレイヤ 2 スイッチ上のポートを隔離する機器と方法を提供します。この機器は、上記のような複数のポートを有するスイッチを備えており、各ポートは、保護ポートまたは非保護ポートとして設定されています。アドレステーブルメモリには、宛先アドレスとポート番号のペアを有するアドレステーブルが格納されます。フォワーディングマップジェネレーターは、データパケットの宛先アドレスに応答するフォワーディングマップを生成します。レイヤ 2 スイッチのポートを分離する方法は、レイヤ 2 スイッチの各ポートを保護ポートまたは非保護ポートとして設定することで構成されます。データパケット上の宛先アドレスは、上記のレイヤ 2 スイッチ上の物理アドレスと照合され、データパケット上の宛先アドレスに基づいて、データパケットのための転送マップが生成されます。次に、データパケットは、入力ポートが保護ポートか非保護ポートかに基づいて生成された転送マップに従って、複数のポートに送信されます。

この画面は、プライベート VLAN 内のポートの隔離を有効または無効にするために使用されます。VLAN のポートメンバーは、同じ VLAN およびプライベート VLAN 上の他の隔離ポートから隔離できます。

Web インターフェース

Web インターフェースでポートアイソレーションを設定するには:

1. 「VLAN Management」(VLAN の管理) ＞ 「Port Isolation」(ポートアイソレーション)をクリックしてください。
2. どのポートでポートアイソレーション機能を有効にするかを選択してください。

3. 「Apply」（適用）をクリックしてください。

■パラメーターの説明

Port Numbers（ポート番号）：
プライベート VLAN の各ポートにチェックボックスがあります。このチェックボックスを ON にすると、そのポートでポートアイソレーション機能が有効になります。このチェックボックスを OFF にすると、そのポートでポートアイソレーション機能が無効になります。デフォルトでは、ポートアイソレーション機能はすべてのポートで無効になっています。

■ボタン

Apply（適用）：
クリックすると、変更内容を保存します。

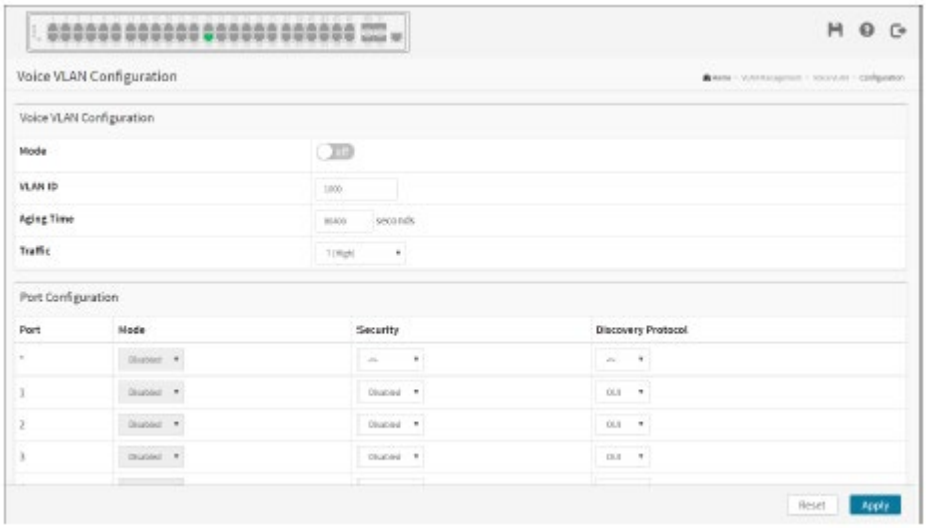
Reset（リセット）：
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

音声 VLAN

音声 VLAN は、音声トラフィック用に特別に設定された VLAN です。音声 VLAN に接続された音声デバイスを持つポートを追加することにより、音声データの QoS 関連設定を実行し、音声トラフィックの伝送優先度と音声品質を確保することができます。

設定

音声 VLAN 機能は、音声 VLAN 上で音声トラフィックの転送を有効にし、スイッチはネットワークトラフィックを分類してスケジュールできます。1 つのポートに 2 系統の VLAN（1 系統は音声用、もう 1 系統はデータ用）を設定することを推奨します。IP デバイスをスイッチに接続する前に、IP 電話で音声 VLAN ID を正しく設定する必要があります。これは、IP 電話の GUI を使用して設定してください。



Web インターフェース

Web インターフェースで音声 VLAN を設定するには：

1. 「VLAN Management」（VLAN の管理） ＞ 「Voice VLAN」（音声 VLAN） ＞ 「Configuration」（設定）をクリックしてください。
2. 「Mode」（モード）で「on」を選択してください。
3. 「VLAN ID」、「Aging Time」（エージングタイム）、および「Traffic Class」（トラフィッククラス）を指定してください。
4. 「Port Configuration」（ポート設定）でポートメンバーを選択してください。
5. 「Port Configuration」（ポート設定）で、「Mode」（モード）、「Security」（セキュリティ）、

「Discovery Protocol」（検出プロトコル）を指定してください。

6. 「Apply」（適用）をクリックして設定を保存してください。
7. 設定を取り消す場合は、「Reset」（リセット）ボタンをクリックする必要があります。そうすると、以前に保存した値へと戻ります。

■パラメーターの説明

Mode（モード）：

音声 VLAN モードの操作を示します。音声 VLAN を有効にする前に、MSTP 機能を無効にする必要があります。これによって、イングレスフィルタリングの競合を回避できます。使用可能なモードは次のとおりです。

on：音声 VLAN モードの操作を有効にします。

off：音声 VLAN モードの操作を無効にします。

VLAN ID：

音声 VLAN ID を示します。これはシステム内で一意の VLAN ID である必要があり、各ポート PVID と同じにすることはできません。値が管理 VID、MVR VID、PVID などと同じで場合、設定で競合が発生します。指定できる範囲は 1～4095 です。

Aging Time（エージングタイム）：

音声 VLAN のセキュアな学習エージングタイムを示します。指定できる範囲は 10～10000000 秒です。これは、セキュリティモードまたは自動検出モードが有効な場合に使用されます。それ以外の場合は、ハードウェアのエージングタイムに基づきます。実際のエージングタイムは、[エージングタイム]～[エージングタイム×2]の間にあります。

Traffic（トラフィック）：

音声 VLAN のトラフィッククラスを示します。音声 VLAN 上のすべてのトラフィックがこのクラスを適用します。

Port（ポート）：

音声 VLAN ポートのスイッチポート番号です。

Port Mode（ポートモード）：

音声 VLAN のポートモードを示します。使用可能なポートモードは次のとおりです。

Disabled（無効）：音声 VLAN から分離します。

Auto（自動）：自動検出モードを有効にします。特定のポートに接続されている IP 電話があるかどうかを検出し、音声 VLAN メンバーを自動的に設定します。

Forced（強制）：音声 VLAN に強制的に参加させます。この項目は、STP 機能が有効になっている場合にのみ読み込まれます。また、この項目が「Disabled」（無効）以外のモードに設定されている場合、STP ポートモードは読み取り専用になります。

Port Security（ポートセキュリティ）：
音声 VLAN ポートのセキュリティモードを示します。この機能を有効にすると、音声 VLAN 内における電話装置以外の MAC アドレスがすべて 10 秒間ブロックされます。使用可能なポートモードは次のとおりです。

Enabled（有効）：音声 VLAN のセキュリティモードの操作を有効にします。

Disabled（無効）：音声 VLAN のセキュリティモードの操作を無効にします。

Port Discovery Protocol（ポート検出プロトコル）：
音声 VLAN ポート検出プロトコルを示します。これは、自動検出モードが有効になっている場合にのみ機能します。検出プロトコルを「LLDP」または「Both」（両方）に設定する前に、LLDP 機能を有効にする必要があります。検出プロトコルを「OUI」または「LLDP」に変更すると、自動検出プロセスが再起動します。検出プロトコルは、次のとおりです。

OUI：OUI アドレスにより電話装置を検出します。

LLDP：LLDP により電話装置を検出します。

Both（両方）：OUI と LLDP の両方です。

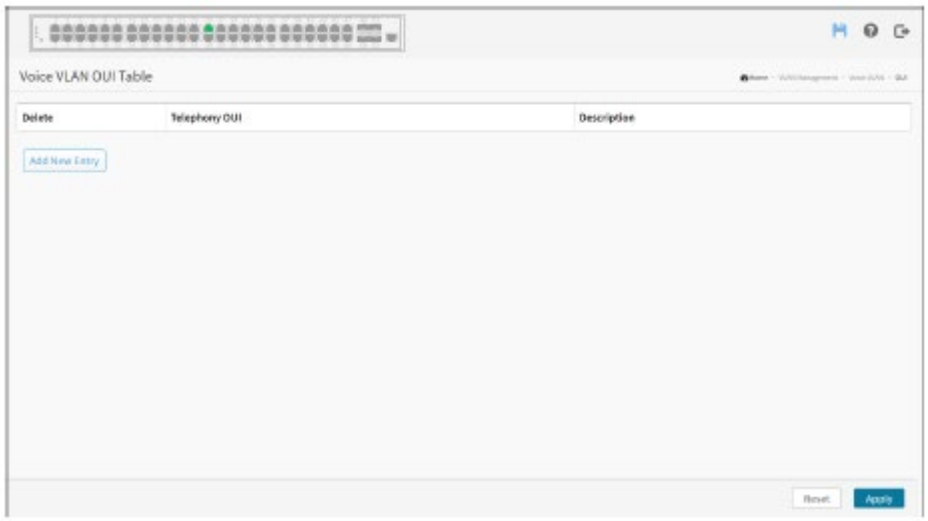
■ボタン

Apply（適用）：
クリックすると、変更内容を保存します。

Reset（リセット）：
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

OUI

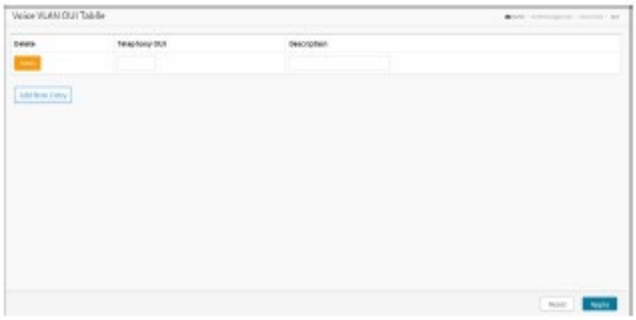
このセクションでは、音声 VLAN OUI テーブルの設定について説明します。最大エントリー数は 16 です。OUI テーブルを変更すると、OUI プロセスの自動検出が再開されます。



Web インターフェース

Web インターフェースで音声 VLAN OUI テーブルを設定するには:

1. 「VLAN Management」(VLANの管理) ＞ 「Voice VLAN」(音声VLAN) ＞ 「OUI」をクリックしてください。
2. 音声 VLAN OUI テーブルで「Add new entry」(新規登録)、「Delete」(削除)を選択してください。



3. 「Telephony OUI」(テレフォニーOUI)、「Description」(説明)を指定してください。
4. 「Apply」(適用)をクリックしてください。

■パラメーターの説明

Delete(削除):

チェックを入れると、エントリーを削除します。このエントリーは、次回保存時に削除されます。

Telephony OUI(テレフォニーOUI):

テレフォニーOUI アドレスは、IEEE によってベンダーに割り当てられるグローバルに一意の識別子です。「*xx-xx-xx*」(x は 16 進数)の形式を用いて、6 文字の長さで入力してください。

Description（説明）:
OUI アドレスの説明です。通常、これは、どのベンダーの電話装置に属するものであるかが記述されます。指定できる文字列の長さは 0～32 です。

Add New entry（新規登録）:
クリックすると、音声 VLAN OUI テーブルに新しいエントリーを追加します。空の行が、テーブル、テレフォニーOUI、説明に追加されます。

■ボタン

Apply（適用）:
クリックすると、変更内容を保存します。

Reset（リセット）:
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

第 7 章
Quality of Service (QoS)

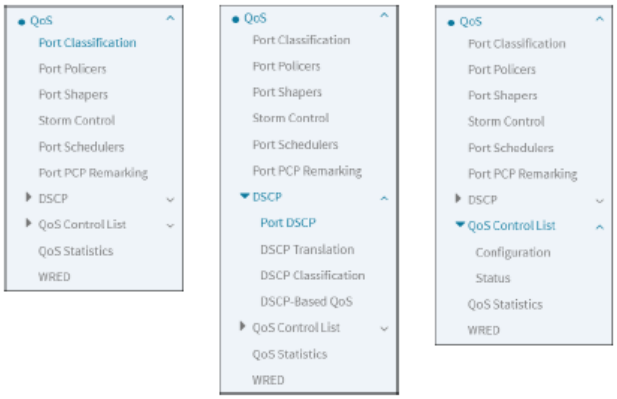
概要

スイッチは、厳密な、または重み付けされたフェアキューイングスケジューリングを使用して、ポートごとに 4 つの QoS キューをサポートします。IEEE802.1p、イーサタイプ、VID、IPv4/IPv6DSCP、および UDP/TCP ポートと範囲に基づいて、事前にプログラム可能な QoS 分類の QoS 制御リスト（QCL）をサポートします。

QoS クラスへの着信フレームの分類には高い柔軟性があります。QoS 分類は、IPv4 および IPv6 DSCP、IPv4 TCP/UDP ポート番号、タグ付きフレームのユーザープライオリティなど、レイヤ 4 までの情報を検索します。この QoS 分類メカニズムは、QoS 制御リスト（QCL）に実装されています。フレームに割り当てられた QoS クラスはデバイス全体で使用され、キューイング、スケジューリング、および輻輳制御を、その特定の QoS クラスに設定された内容に従ってフレームに保証します。

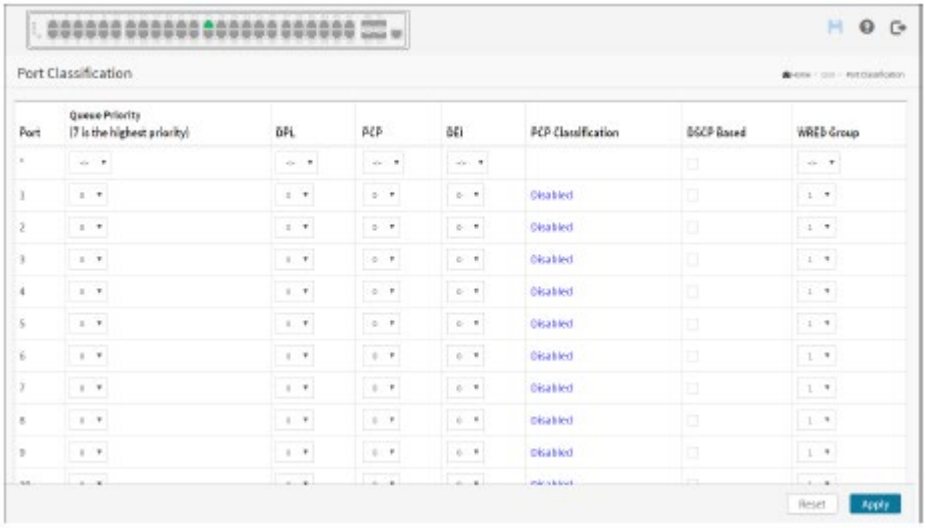
スイッチは、ジャンボフレームを含むあらゆるトラフィックシナリオで、すべての QoS クラスの優れたパフォーマンスを提供する高度なメモリ制御メカニズムをサポートします。アービトレーションで、専用メモリと厳密に最高のプライオリティを持つスーパープライオリティキューです。入力スーパープライオリティキューは、すべての QoS クラスキューが輻輳している場合でも、CPU トラフィックとして認識され、CPU への伝送のためにキューに入れられるトラフィックを許可します。

メニューとサブメニューを以下に示します。



ポートの分類

このセクションでは、すべてのスイッチポートの基本的な QoS イングレスクラスを設定することができます。



Web インターフェース

Web インターフェースで QoS 受信ポート分類パラメーターを設定するには:

1. 「Quality of Service」 ＞ 「Port Classification」(ポートの分類)をクリックしてください。
2. スクロールして、「QoS Ingress Port」(QoS イングレスポート)パラメーターを選択してください。
3. 「Apply」(適用)をクリックして設定を保存してください。
4. 設定を取り消す場合は、「Reset」(リセット)ボタンをクリックする必要があります。そうすると、以前に保存した値へと戻ります。
5. 「Port PCP Classification」(ポート PCP 分類)画面の横にある「PCP Classification」(PCP 分類)をクリックしてください。

■パラメーターの説明

Port(ポート):

以下の設定が適用されるポート番号です。

Queue Priority(キューの優先順位):

デフォルトの CoS 値を制御します。

すべてのフレームは CoS に分類されます。CoS、キュー、および優先度の間には 1 対 1 のマッピングがあります。0 の CoS が最も低い優先度になります。

ポートが VLAN 対応の場合、フレームはタグ付けされ、タグ分類が有効になっていれば、フレーム

はタグ内の PCP および DEI 値からマッピングされた CoS に分類されます。それ以外の場合、フレームはデフォルト CoS に分類されます。
分類された CoS は、QCL エントリーによって無効にすることができます。

注意: デフォルト CoS が動的に変更されている場合、実際のデフォルト CoS は、設定されているデフォルト CoS の後に括弧内に表示されます。

DPL:
デフォルトのドロップ優先度レベルを制御します。
すべてのフレームは、ドロップ優先レベルに分類されます。ポートが VLAN 対応の場合、フレームはタグ付けされ、タグ分類が有効になると、フレームはタグ内の PCP および DEI 値からマッピングされた DPL に分類されます。それ以外の場合、フレームはデフォルト DPL に分類されます。
分類された DPL は、QCL エントリーによって上書きできます。

PCP:
デフォルトの PCP 値を制御します。
すべてのフレームは PCP 値に分類されます。
ポートが VLAN 対応で、フレームにタグが付けられている場合、フレームはタグ内の PCP 値に分類されます。それ以外の場合、フレームはデフォルトの PCP 値に分類されます。

DEI:
デフォルトの DEI 値を制御します。
すべてのフレームは DEI 値に分類されます。
ポートが VLAN 対応でフレームがタグ付けされている場合、フレームはタグ内の DEI 値に分類されます。それ以外の場合、フレームはデフォルトの DEI 値に分類されます。

DSCP Based(DSCP ベース):
クリックすると、DSCP ベースの QoS 受信ポート分類を有効にします。

WRED Group(WRED グループ):
WRED グループメンバーシップを制御します。

■ボタン

Apply（適用）：

クリックすると、変更内容を保存します。

Reset（リセット）：

クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

PCP Classification（PCP 分類）：

このポートのタグ付きフレームの分類モードを表示します。

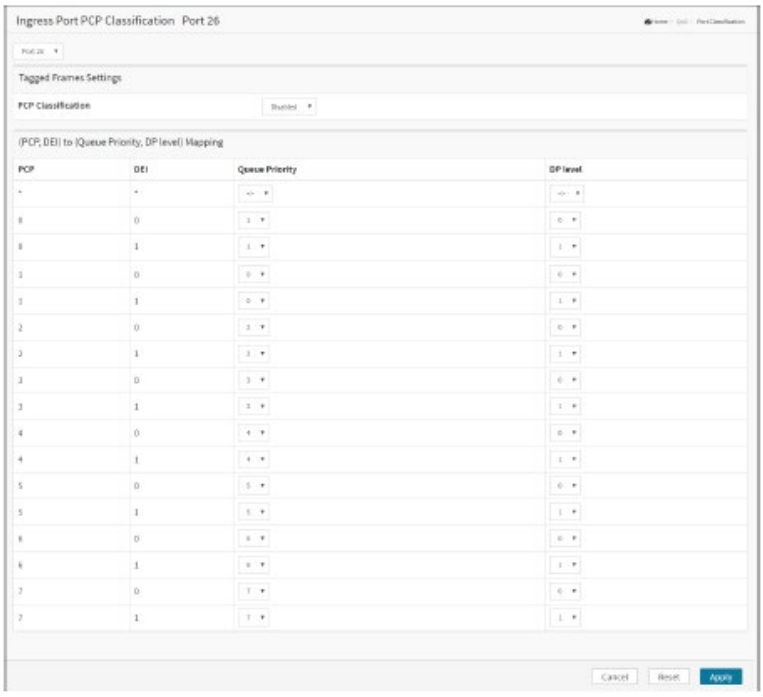
Disabled（無効）：タグ付きフレームにはデフォルトの CoS および DPL を使用します。

Enabled（有効）：タグ付きフレームには、マッピングされたバージョンの PCP および DEI を使用します。

モードまたはマッピングを設定するには、モードをクリックしてください。

注意： ポートが VLAN unaware の場合、この設定は無効になります。VLAN 非対応ポートで受信されたタグ付きフレームは、常にデフォルトの CoS および DPL に分類されます。

Port PCP Classification（ポートの PCP 分類）



■パラメーターの説明

PCP Classification（PCP 分類）：

このポートのタグ付きフレームの分類モードを制御します。

Disabled（無効）：タグ付きフレームにはデフォルトの CoS および DPL を使用します。

Enabled（有効）：タグ付きフレームには、マッピングされたバージョンの PCP および DEI を使用します。

(PCP, DEI) to (Queue Priority, DPL level) Mapping：（PCP、DEI）から（キューの優先度、DPL レベル）へのマッピング

タグ分類が有効に設定されている場合、分類された（PCP、DEI）値と（キューの優先度、DPL レベル）値のマッピングを制御します。

■ボタン

Apply（適用）：

クリックすると、変更内容を保存します。

Reset（リセット）：

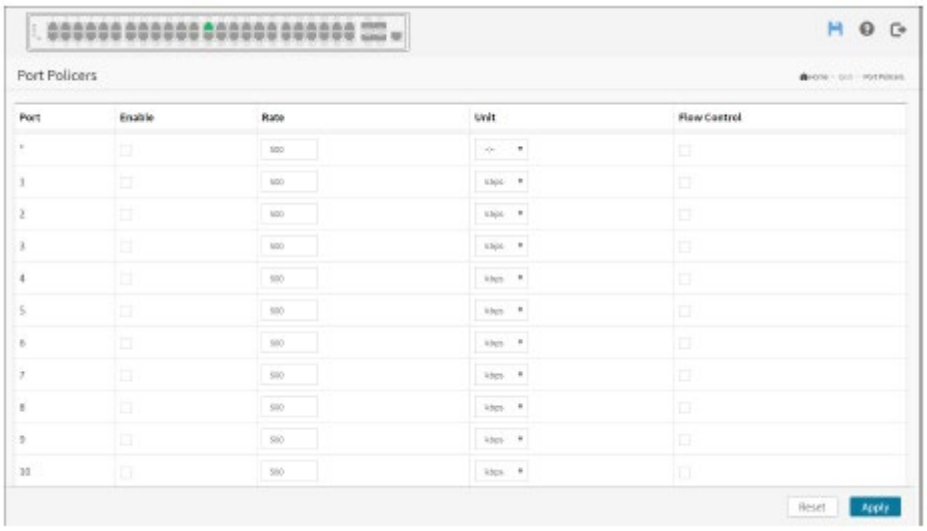
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

Cancel（キャンセル）：

クリックすると、ローカルで行った変更が取り消され、前のページに戻ります。

ポートポリサー

このセクションでは、すべてのスイッチポートの QoS イングレス・ポートポリサーの概要を示します。ポートポリシングは、トラフィックフローを制約し、特定のレートを超えるフレームをマーキングする場合に役立ちます。通常、音声とビデオは一定のトラフィックレートを維持するため、データフローと音声またはビデオフローには主にポリシングが役立ちます。



Web インターフェース

Web インターフェースで QoS ポートポリサーを設定するには:

1. 「Quality of Service」 ＞ 「Port Policer」(ポートポリサー)をクリックしてください。
2. 「QoS Ingress Port Policers」(QoS イングレス・ポートポリサー)を有効にする必要があるポートをクリックし、「Rate」(レート)の制限となる条件を設定してください。
3. スクロールして、「Rate」(レート)列と「Unit」(ユニット)列を選択してください。
4. 「Apply」(適用)をクリックして設定を保存してください。
5. 設定を取り消す場合は、「Reset」(リセット)ボタンをクリックする必要があります。そうすると、以前に保存した値へと戻ります。

■パラメーターの説明

Port(ポート):

同じ行に含まれる設定の論理ポートです。スケジューラーを設定するには、ポート番号をクリックしてください。

Enable(有効):

QoS イングレス・ポートポリサー機能を有効にする必要があるポートの場合は、この項目にチェックを入れてください。

Rate（レート）：
このポートのレート制限値を設定するための項目です。デフォルトは 1000000 です。

Unit（単位）：
ポートポリサーのレートの測定単位を kbps、Mbps、fps、または kfps で制御します。

Flow Control（フローコントロール）：
フローコントロールが有効で、ポートがフローコントロールモードの場合、フレームを破棄する代わりにポーズフレームが送信されます。

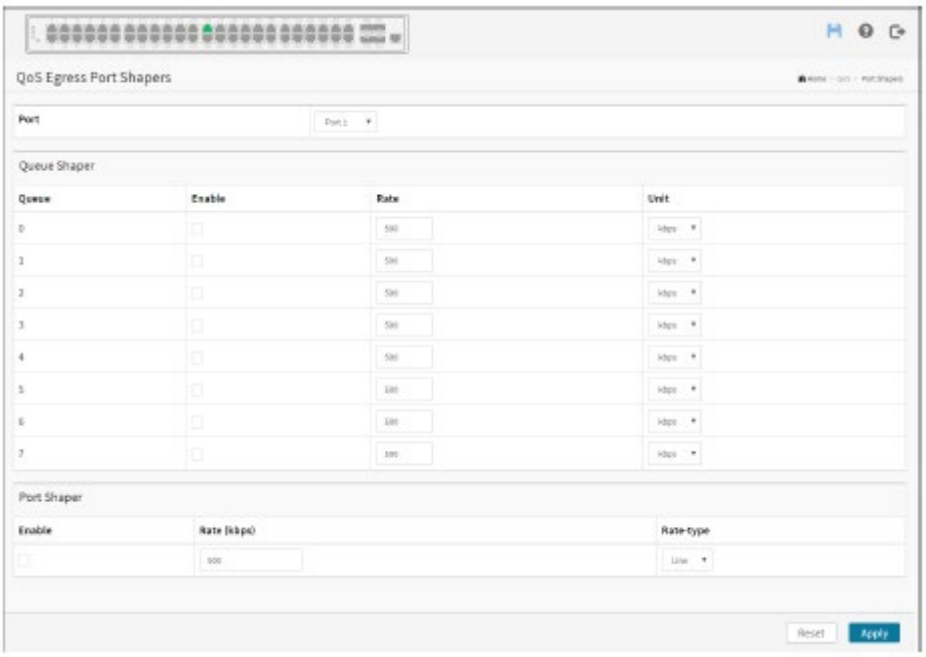
■ボタン

Apply（適用）：
クリックすると、変更内容を保存します。

Reset（リセット）：
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

ポートシェーパー

このセクションでは、すべてのスイッチポートにおける QoS 出力ポートシェーパーの概要を示します。他のユーザーは、現在選択されているスタックユニットに属するポートのすべての詳細情報を取得することができます。この情報は、ページヘッダーにも反映されています。



Web インターフェース

Web インターフェースで QoS ポートシェーパーを設定するには:

1. 「Quality of Service」 ＞ 「Port Shapers」(ポートシェーパー)をクリックしてください。
2. ポートをクリックして、「Qos Egress Port Shapers」(Qos イグレス・ポートシェーパー)を表示してください。
3. 「Port and Scheduler Mode」(ポートとスケジューラーモード)をスクロールして、「Queue Shaper」(キューシェーパー)パラメーターを指定してください。
4. 「Apply」(適用)をクリックして設定を保存してください。
5. 設定を取り消す場合は、「Reset」(リセット)ボタンをクリックする必要があります。そうすると、以前に保存した値へと戻ります。

■パラメーターの説明

Port (ポート) :

同じ行に含まれる設定の論理ポートです。

ポートシェーパーを設定するには、ポート番号をクリックしてください。

Shapers - Qn（シェーパー - Qn）：
無効と表示されるか、または実際のキューのシェーパーレート（800Mbps など）が表示されます。

Shapers - Port（シェーパー - ポート）：
無効と表示されるか、または実際のポートのシェーパーレート（800Mbps など）を表示します。

Scheduler Mode（スケジューラーモード）：
厳密にスケジュールされているキューの数と、このスイッチポートで重み付けされてスケジュールされているキューの数を制御します。

Queue Shaper Enable（キューシェーパー有効）：
このスイッチポートのキューシェーパーを有効にするかどうかを制御します。

Queue Shaper Rate（キューシェーパーレート）：
キューシェーパーのレートを制御します。単位が kbps の場合は 10013107100、Mbps の場合は 1～13107 に、それぞれ制限されます。レートは、内部的にキューシェーパーでサポートされている最も近い値に切り上げられます。

Queue Shaper Unit（キューシェーパーの単位）：
キューシェーパーレートの単位を kbps または Mbps で制御します。

Queue Shaper Rate-type（キューシェーパーのレートの種類）：
キューシェーパーのレートの種類です。指定できる値は以下のとおりです。
Line（ライン）：このシェーパーがラインレートで動作するように設定します。
Data（データ）：このシェーパーがデータレートで動作するように設定します。

Queue Scheduler Weight（キュースケジューラーの重み）：
このキューの重みを制御します。この値は 1～100 に制限されています。このパラメーターは、「Scheduler Mode」（スケジューラーモード）が「Weighted」（加重）に設定されている場合にのみ表示されます。

Queue Scheduler Percent（キュースケジューラーのパーセント）：
このキューの重みをパーセントで表示します。このパラメーターは、「Scheduler Mode」（スケジューラーモード）が「Weighted」（加重）に設定されている場合にのみ表示されます。

Port Shaper Enable（ポートシェーパー有効）:
このスイッチポートでポートシェーパーを有効にするかどうかを制御します。

Port Shaper Rate（ポートシェーパーレート）:
ポートシェーパーのレートを制御します。単位が kbps の場合は 10013107100 に、Mbps の場合は 1～13107 に、それぞれ制限されます。レートは内部的にポートシェーパーでサポートされている最も近い値に切り上げられます。

Port Shaper Unit（ポートシェーパーの単位）:
ポートシェーパーレートの単位を kbps または Mbps で制御します。

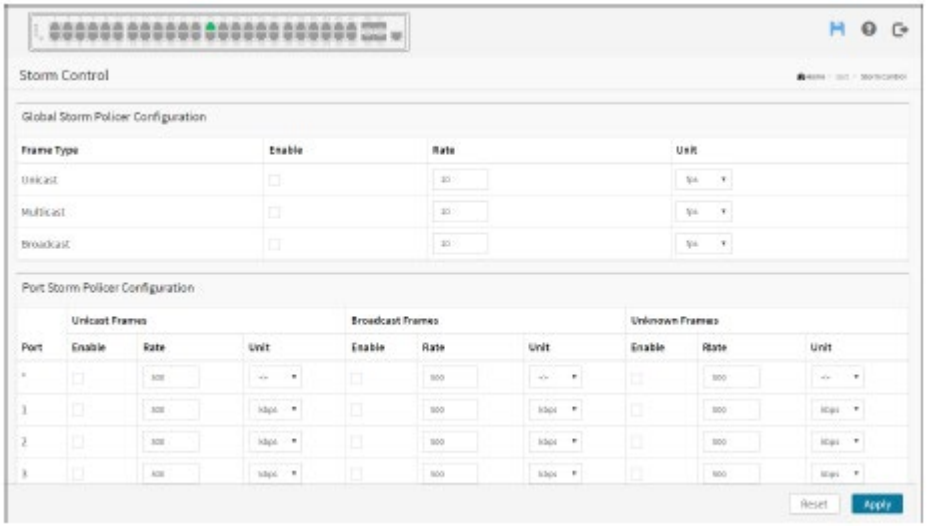
Port Shaper Rate-type（ポートシェーパーのレートの種類）:
ポートシェーパーのレートの種類です。指定できる値は以下のとおりです。
Line（ライン）:このシェーパーがラインレートで動作するように設定します。
Data（データ）:このシェーパーがデータレートで動作するように設定します。

■ボタン
Apply（適用）:
クリックすると、変更内容を保存します。

Reset（リセット）:
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

ストーム制御

このセクションでは、スイッチのストーム制御を設定できます。ストームレート制御には、宛先参照失敗ストームレート制御、マルチキャスト・ストームレート制御、およびブロードキャスト・ストームレート制御があります。これらは、フラッディングされたフレーム、つまり MAC アドレステーブルに存在しない（VLAN ID、DMAC）ペアを持つフレームにのみ影響します。設定は、スイッチ全体のユニキャスト、マルチキャスト、またはブロードキャスト・トラフィックの許可されたパケットレートを示します。



Web インターフェース

Web インターフェースで、ストーム制御を設定するパラメーターを定義するには：

1. 「Quality of Service」 ＞ 「Storm Control」（ストーム制御）をクリックしてください。
2. ストーム制御を有効にするフレームタイプを選択してください。
3. スクロールして、レートのパラメーターと単位を設定してください。
4. 有効にする必要があるポートをクリックし、レートの制限に関する条件を設定してください。
6. 「Apply」（適用）をクリックして設定を保存してください。
7. 設定を取り消す場合は、「Reset」（リセット）ボタンをクリックする必要があります。そうすると、以前に保存した値へと戻ります。

■パラメーターの説明

Global Storm Policer Configuration（グローバル・ストームポリサーの設定）

この画面では、スイッチのグローバル・ストームポリサーを設定します。

ストームポリサーには、ユニキャスト・ストームポリサー、マルチキャスト・ストームポリサー、およびブ

ロードキャスト・ストームポリサーがあります。
これらは、フラッディングされたフレーム、つまり MAC アドレステーブルに存在しない（VLAN ID、DMAC）ペアを持つフレームにのみ影響します。

Frame Type（フレームタイプ）：
以下の設定が適用されるフレームタイプです。

Enable（有効にする）：
指定したフレームタイプのグローバル・ストームポリサーを有効または無効にします。

Rate（レート）：
グローバル・ストームポリサーのレートを制御します。単位が fps または kbps の場合は 1013128147、kfps または Mbps の場合は 1～13128 に、それぞれ制限されます。レートは、グローバル・ストームポリサーでサポートされている最も近い値に内部的に切り上げられます。サポートされるレートは 10fps または 25kbps で割り切れます。
グローバル・ストームポリサーのレートの測定単位を fps、kfps、kbps、または Mbps として制御します。

Port Storm Policer Configuration Help（ポート・ストームポリサー設定のヘルプ）
すべてのスイッチポートのポート・ストームポリサーは、この画面で設定します。
既知および未知のユニキャストフレーム、既知および未知のブロードキャストフレーム、および未知の（フラッディングされた）ユニキャスト、マルチキャスト、ブロードキャストフレームのストームポリサーがあります。

Port（ポート）：
以下の設定が適用されるポート番号です。

Enable（有効にする）：
このスイッチポートのストームポリサーを有効または無効にします。

Rate（レート）：
ポート・ストームポリサーのレートを制御します。単位が fps または kbps の場合は 1013128147、kfps または Mbps の場合は 1～13128 に、それぞれ制限されます。レートは、内部的にポート・ストームポリサーでサポートされている最も近い値に切り上げられます。サポートされるレートは 10fps または 25kbps で割り切れます。

Unit（単位）:
ポート・ストームポリサーのレートの測定単位を fps、kfps、kbps、または Mbps として制御します。

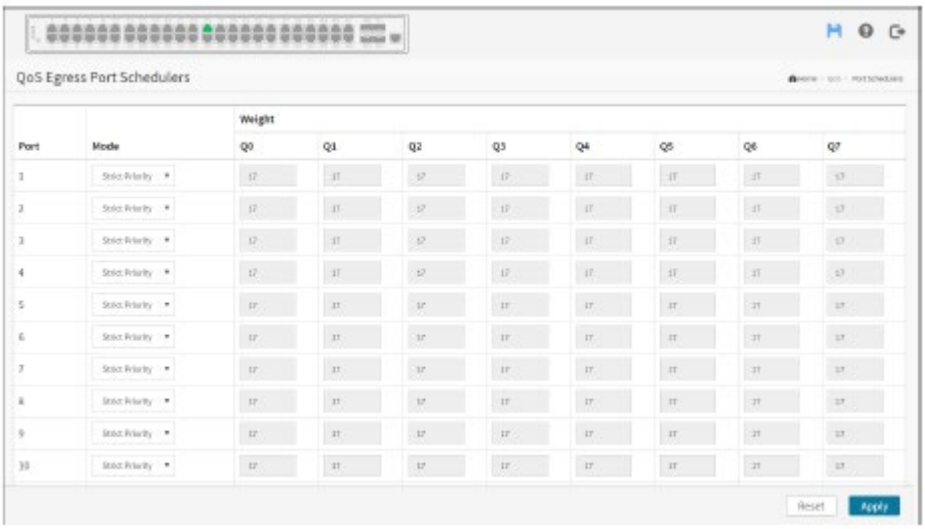
■ボタン

Apply（適用）:
クリックすると、変更内容を保存します。

Reset（リセット）:
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

ポートスケジューラー

このセクションでは、すべてのスイッチポートの QoS イグレス・ポートスケジューラーの概要を示します。ポートは現在選択されているスタックユニットに属し、ページヘッダーに反映されます。



Web インターフェース

Web インターフェースで QoS ポートスケジューラーを設定するには:

1. 「Quality of Service」 ＞ 「Port Scheduler」(ポートスケジューラー)をクリックしてください。
2. ポートをクリックし、QoS イグレス・ポートスケジューラーを表示してください。
3. ポートとスケジューラーモードをスクロールして、キューシェーパーのパラメーターを指定してください。
4. 「Apply」(適用)をクリックして設定を保存してください。
5. 設定を取り消す場合は、「Reset」(リセット)ボタンをクリックする必要があります。そうすると、以前に保存した値へと戻ります。

■パラメーターの説明

Port (ポート) :

同じ行に含まれる設定の論理ポートです。

Mode (モード) :

このポートのスケジューリングモードを表示します。

Qn:

このキューとポートの重みが表示されます。

Scheduler Mode（スケジューラーモード）：
厳密にスケジュールされているキューの数と、このスイッチポートで重み付けされてスケジュールされているキューの数を制御します。

Queue Shaper Enable（キューシェーパー有効）：
このスイッチポートのキューシェーパーを有効にするかどうかを制御します。

Queue Shaper Rate（キューシェーパーレート）：
キューシェーパーのレートを制御します。単位が kbps の場合は 10013107100、Mbps の場合は 1～13107 に、それぞれ制限されます。レートは、内部的にキューシェーパーでサポートされている最も近い値に切り上げられます。

Queue Shaper Unit（キューシェーパーの単位）：
キューシェーパーレートの単位を kbps または Mbps で制御します。

Queue Shaper Rate-type（キューシェーパーのレートの種類）：
キューシェーパーのレートの種類です。指定できる値は以下のとおりです。
Line（ライン）：このシェーパーがラインレートで動作するように設定します。
Data（データ）：このシェーパーがデータレートで動作するように設定します。

Queue Scheduler Weight（キュースケジューラーの重み）：
このキューの重みを制御します。この値は 1～100 に制限されています。このパラメーターは、「Scheduler Mode」（スケジューラーモード）が「Weighted」（加重）に設定されている場合にのみ表示されます。

Queue Scheduler Percent（キュースケジューラーのパーセント）：
このキューの重みをパーセントで表示します。このパラメーターは、「Scheduler Mode」（スケジューラーモード）が「Weighted」（加重）に設定されている場合にのみ表示されます。

Port Shaper Enable（ポートシェーパー有効）：
このスイッチポートでポートシェーパーを有効にするかどうかを制御します。

Port Shaper Rate（ポートシェーパーレート）：
ポートシェーパーのレートを制御します。単位が kbps の場合は 10013107100 に、Mbps の場合は 1

～13107 に、それぞれ制限されます。レートは内部的にポートシェーパーでサポートされている最も近い値に切り上げられます。

Port Shaper Unit（ポートシェーパーの単位）：
ポートシェーパーレートの単位を kbps または Mbps で制御します。

Port Shaper Rate-type（ポートシェーパーのレートの種類）：
ポートシェーパーのレートの種類です。指定できる値は以下のとおりです。

Line（ライン）：このシェーパーがラインレートで動作するように設定します。
Data（データ）：このシェーパーがデータレートで動作するように設定します。

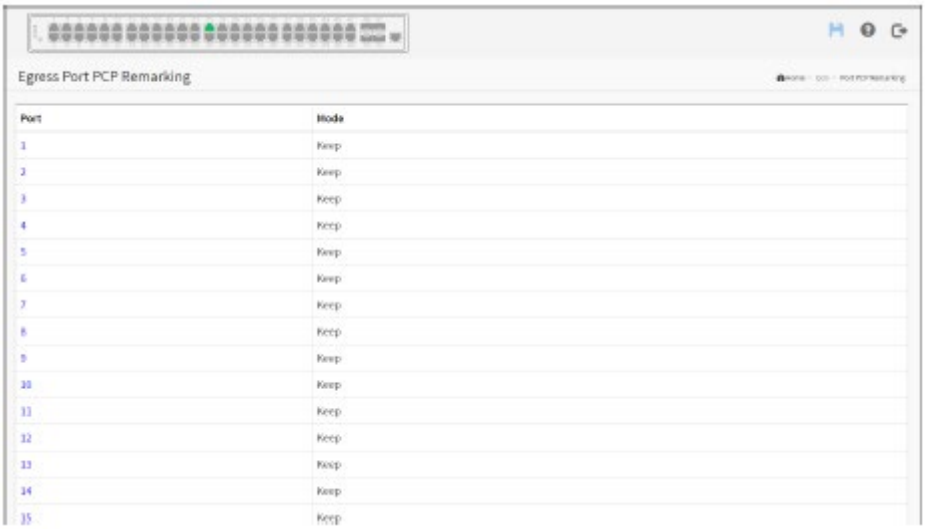
■ボタン

Apply（適用）：
クリックすると、変更内容を保存します。

Reset（リセット）：
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

ポートの PCP リマーキング

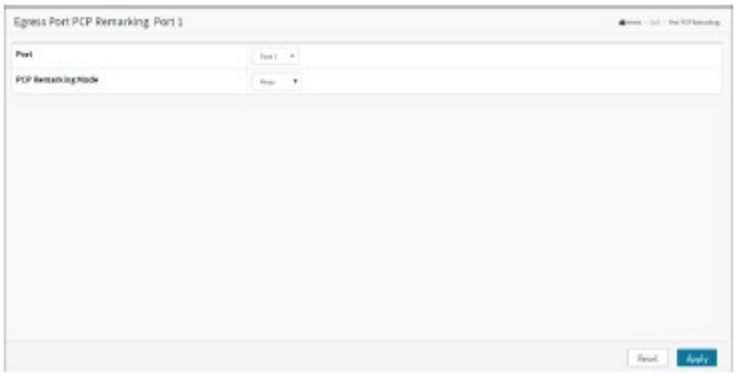
このセクションでは、すべてのスイッチポートの QoS イグレスポートの PCP リマーキングの概要を確認できます。その他のポートは、ページヘッダーに反映されるように、現在選択されているスタックユニットに属します。



Web インターフェース

Web インターフェースで QoS ポートの PCP リマーキングを設定するには:

1. 「Quality of Service」 ＞ 「Port PCP Remarking」(ポートの PCP リマーキング)をクリックしてください。
2. 「Port」(ポート)をクリックし、「QoS Port PCP Remarking」(ポート PCP リマーキング)を表示してください。



3. 「Port」(ポート)および「PCP Remarking Mode」(PCP リマーキングモード)をスクロールし、キューシェーパーのパラメーターを指定してください。

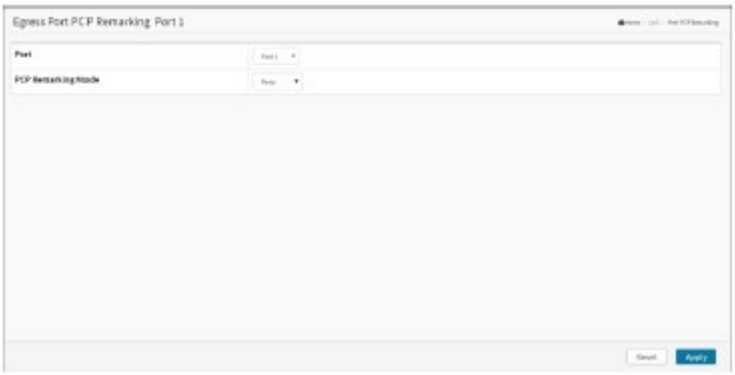
4. 「Apply」（適用）をクリックして設定を保存してください。
5. 設定を取り消す場合は、「Reset」（リセット）ボタンをクリックする必要があります。そうすると、以前に保存した値へと戻ります。

■パラメーターの説明

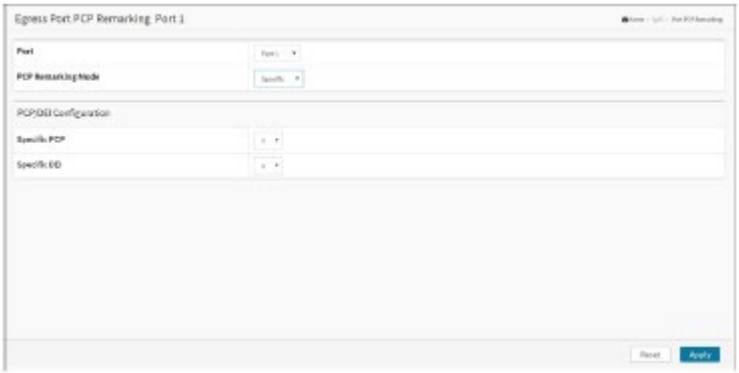
Port（ポート）：
同じ行に含まれる設定の論理ポートです。
PCP リマーキングを設定するには、ポート番号をクリックしてください。

Mode（モード）：
このポートの PCP リマーキングモードを表示します。

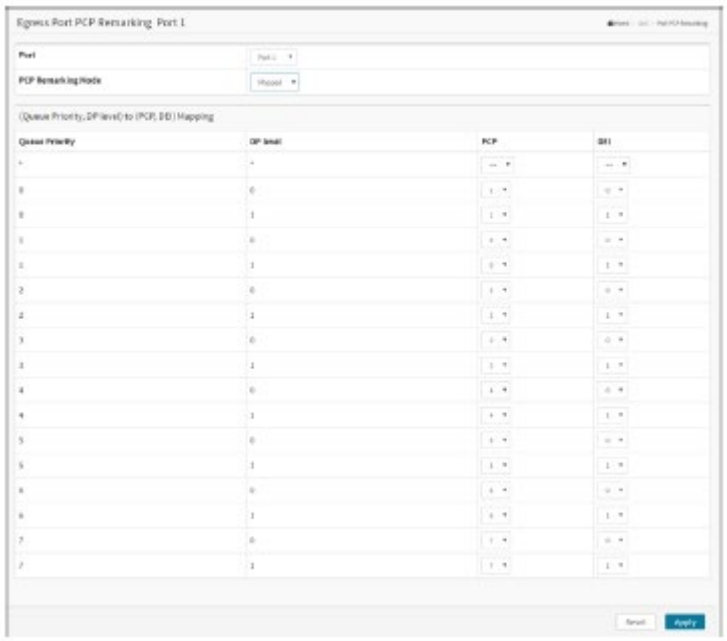
Keep（キープ）：分類された PCP/DEI 値を使用します。



Specific（特定）：デフォルトの PCP/DEI 値を使用します。



Mapped（マッピング済み）：マッピングされたバージョンの CoS および DPL を使用します。



PCP/DEI Configuration（PCP/DEI の設定）:
モードが「Default」（デフォルト）に設定されている場合に使用されるデフォルトの PCP および DEI 値を制御します。

(QoS class, DP level) to (PCP, DEI) Mapping（QoS クラス、DP レベル）から（PCP、DEI）へのマッピング:
モードが「Mapped」（マッピング済み）に設定されている場合、分類された（QoS クラス、DP レベル）値と（PCP、DEI）値のマッピングを制御します。

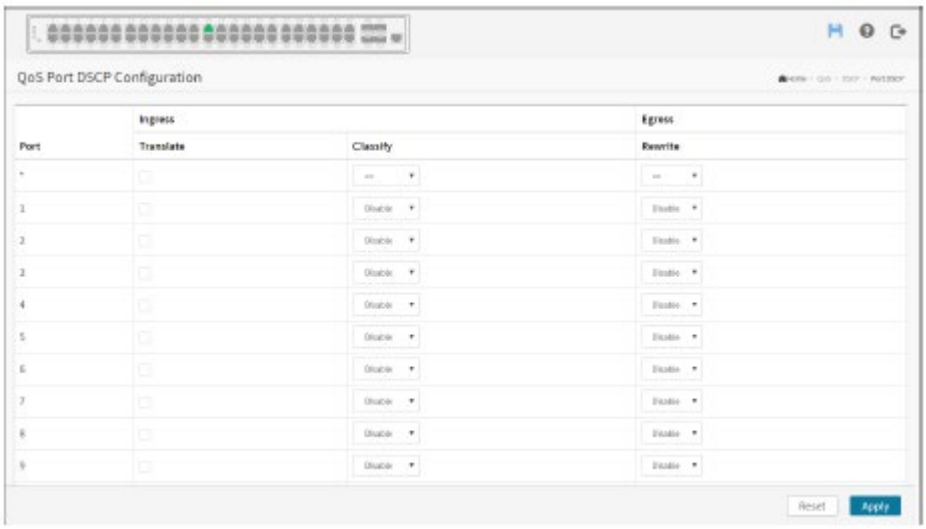
■ボタン
Apply（適用）:
クリックすると、変更内容を保存します。

Reset（リセット）:
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

DSCP

ポート DSCP

このセクションでは、すべてのスイッチポートの基本的な QoS ポート DSCP 設定を定義できる QoS ポート DSCP の設定を行うように、ユーザーに指示します。その他の設定は、ページヘッダーに反映されるように、現在選択されているスタックユニットに関連します。



Web インターフェース

Web インターフェースで QoS ポート DSCP パラメーターを設定するには:

1. 「Quality of Service」 ＞ 「DSCP」 ＞ 「Port DSCP」(ポート DSCP)をクリックしてください。
2. 「Ingress」(イングレス)の「Translate」(変換)項目へのチェックで有効/無効を選択し、「Classfy」(分類)リストから適切な項目を選択してください。
3. 「Egress」(イグレス)の「Rewrite」(書き換え)リストから適切な項目を選択してください。
4. 「Apply」(適用)をクリックして設定を保存してください。
5. 設定を取り消す場合は、「Reset」(リセット)ボタンをクリックする必要があります。そうすると、以前に保存した値へと戻ります。

■パラメーターの説明

Port(ポート):

「Port」(ポート)列には、dscp の受信および送信設定を構成できるポートのリストが表示されます。

Ingress(イングレス):

イングレス設定では、個々のポートの入力変換と分類の設定を変更できます。
イングレスには 2 種類の設定パラメーターがあります。

Translate（変換）：イングレスの変換を有効にする場合は、このチェックボックスを ON にしてください。

Classify（分類）：ポートに対する分類には 4 種類の値があります。

Disable（無効）：イングレス DSCP 分類はありません。

DSCP=0：受信（または有効な場合は変換）DSCP が 0 の場合に分類します。

Selected（選択済み）：特定の DSCP に対する DSCP 変換ウィンドウで指定されているように、分類が有効になっている選択済み DSCP のみを分類します。

All（すべて）：すべての DSCP を分類します。

Egress（イグレス）：
ポートのイグレス書き換えは次のパラメーターのいずれかになります。

Disable（無効）：イグレスの書き換えはありません。

Enable（有効）：再配置せずに書き換えを有効にします。

Remap（再マッピング）：アナライザーからの DSCP が再マッピングされ、フレームは再マッピングされた DSCP 値でリマークされます。

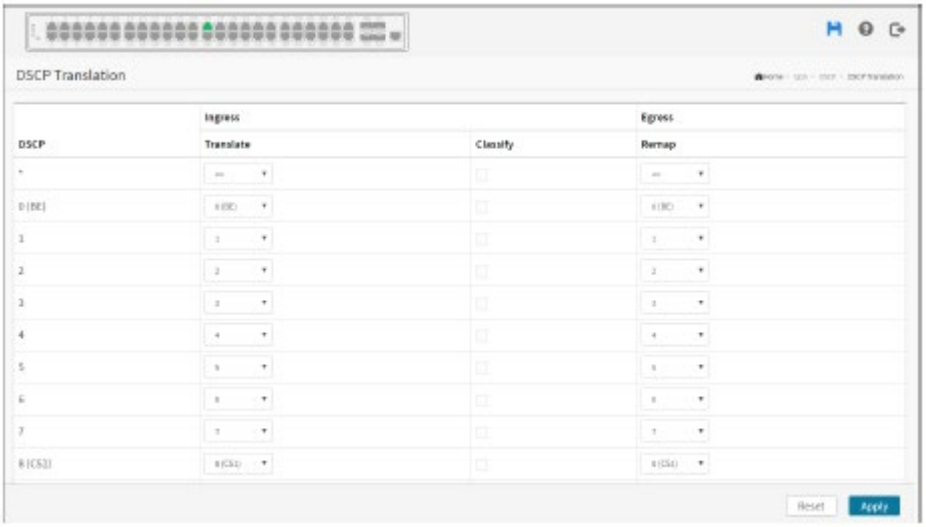
■ボタン

Apply（適用）：
クリックすると、変更内容を保存します。

Reset（リセット）：
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

DSCP の変換

このセクションでは、すべてのスイッチの基本的な QoS DSCP 変換設定を設定できるスイッチについて説明します。DSCP 変換は、イングレスまたはイグレスで実行できます。



Web インターフェース

Web インターフェースで DSCP 変換パラメーターを設定するには:

1. 「Quality of Service」 ＞ 「DSCP」 ＞ 「DSCP Translation」(DSCP の変換)をクリックしてください。
2. 「Ingress」(イングレス)の「Translate」(変換)と、「Egress」(イグレス)の「Remap」(再マッピング)を設定してください。
3. 「Classify」(分類)を有効または無効にしてください。
4. 「Apply」(適用)をクリックして設定を保存してください。
5. 設定を取り消す場合は、「Reset」(リセット)ボタンをクリックする必要があります。そうすると、以前に保存した値へと戻ります。

■パラメーターの説明

DSCP:

サポートされる DSCP 値の最大数は 64 で、有効な DSCP 値の範囲は 0～63 です。

Ingress(イングレス):

入力側 DSCP は、QoS クラスおよび DPL マップに DSCP を使用する前に、最初に新しい DSCP に変換できます。

DSCP 変換には 2 つの設定パラメーターがあります。

Translate(変換):イングレス側の DSCP は、(0～63)の任意の DSCP 値に変換できます。

Classify(分類):クリックすると、イングレス側で分類を有効にします。

Egress(イグレス):

再マッピングする DSCP 値をドロップダウンメニューから選択します。DSCP 値の範囲は 0～63 です。

■ボタン

Apply（適用）：

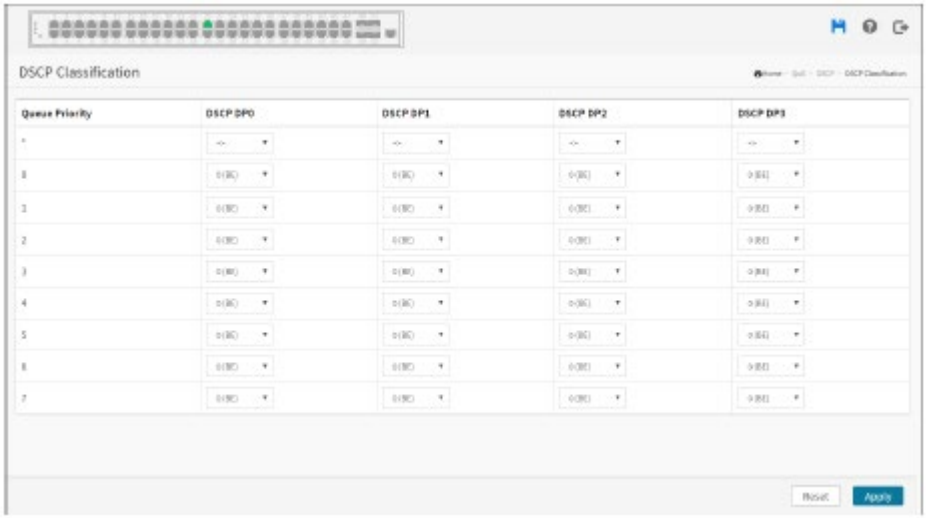
クリックすると、変更内容を保存します。

Reset（リセット）：

クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

DSCP の分類

このセクションでは、DSCP 値を QoS クラスおよび DPL 値にマッピングするように設定する方法について説明します。その他の設定は、ページヘッダーに反映されるように、現在選択されているスタックユニットに関連します。



Web インターフェース

Web インターフェースで DSCP 分類パラメーターを設定するには：

1. 「Quality of Service」 ＞ 「DSCP」 ＞ 「DSCP Classification」（DSCP の分類）をクリックしてください。
2. スクロールして、DSCP のパラメーターを設定してください。
3. 「Apply」（適用）をクリックして設定を保存してください。
4. 設定を取り消す場合は、「Reset」（リセット）ボタンをクリックする必要があります。そうすると、以前に保存した値へと戻ります。

■パラメーターの説明

Queue Priority（キューの優先順位）：
サービスの実際の分類です。

DSCP DP0：
廃棄優先度 0 に対して分類された DSCP 値（0～63）を選択してください。

DSCP DP1：
廃棄優先度 1 に対して分類された DSCP 値（0～63）を選択してください。

DSCP DP2：
廃棄優先度 2 に対して分類された DSCP 値（0～63）を選択してください。

DSCP DP3：
廃棄優先度 3 に対して分類された DSCP 値（0～63）を選択してください。

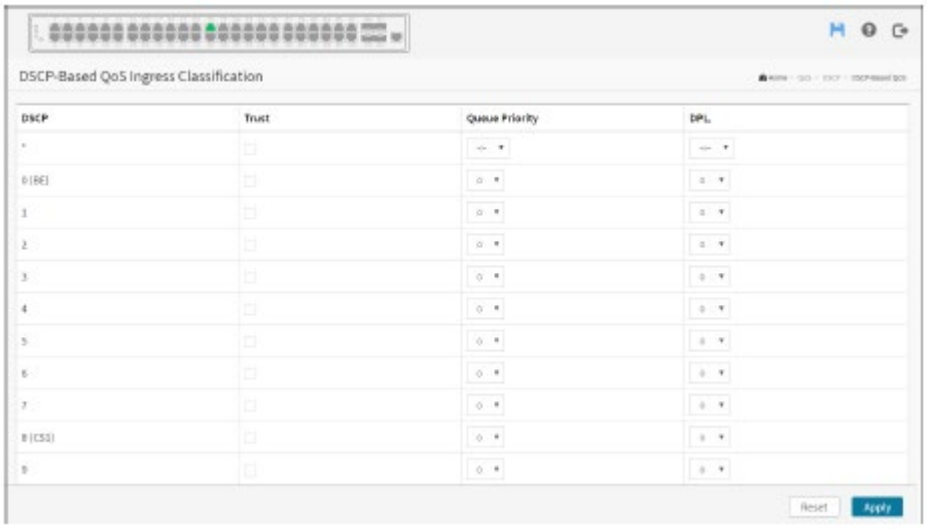
■ボタン

Apply（適用）：
クリックすると、変更内容を保存します。

Reset（リセット）：
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

DSCP ベースの QoS

このセクションでは、すべてのスイッチの基本的な QoS DSCP ベースの QoS イングレス分類設定を構成するための DSCP ベースの QoS モードの設定について説明します。



Web インターフェース

Web インターフェースで DSCP ベースの QoS イングレス分類パラメーターを設定するには:

1. 「Quality of Service」 ＞ 「DSCP」 ＞ 「DSCP-Based QoS」(DSCP ベースの QoS)をクリックしてください。
2. 「Trust」(信頼)に対する DSCP を有効または無効にしてください。
3. 「Queue Priority」(キューの優先度)および「DPL」パラメーターのドロップダウンリストをスクロールして選択してください。
4. 「Save」(保存)をクリックして設定を保存してください。設定を取り消す場合は、「Reset」(リセット)ボタンをクリックする必要があります。そうすると、以前に保存した値へと戻ります。

■パラメーターの説明

DSCP:

サポートされる DSCP 値の最大数は 64 です。

Trust(信頼):

DSCP 値が信頼されているかどうかを、クリックして確認してください。

Queue Priority(キューの優先順位):

キューの優先順位の値は 0～7 の範囲で指定できます。最大値は 7 です。

DPL:

廃棄優先度(0～3)です。

■ボタン

Apply（適用）：

クリックすると、変更内容を保存します。

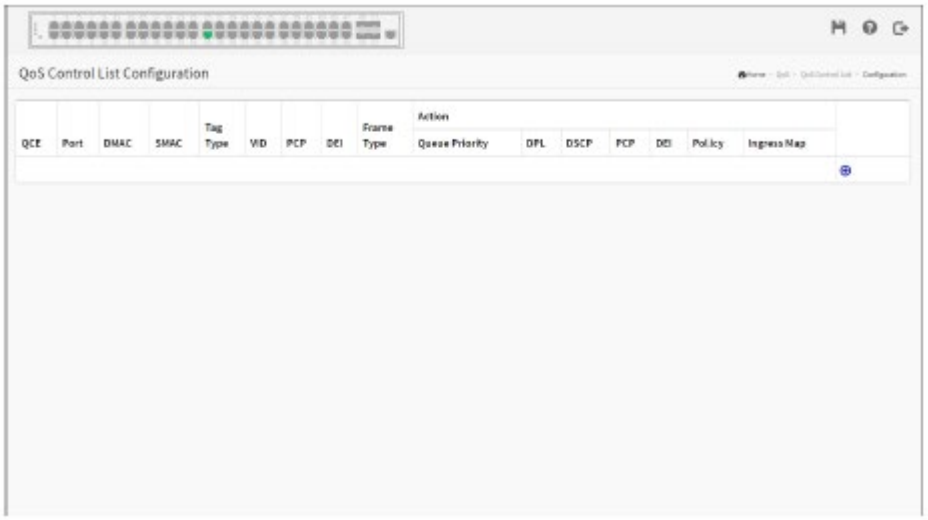
Reset（リセット）：

クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

QoS 制御リスト

設定

QCE で構成される「QoS 制御リスト」(QCL)が表示されます。各行は、定義されている QCE を示します。QCE の最大数は、各スイッチで 256 です。リストに新しい QCE を追加するには、最下位のプラス記号をクリックします。

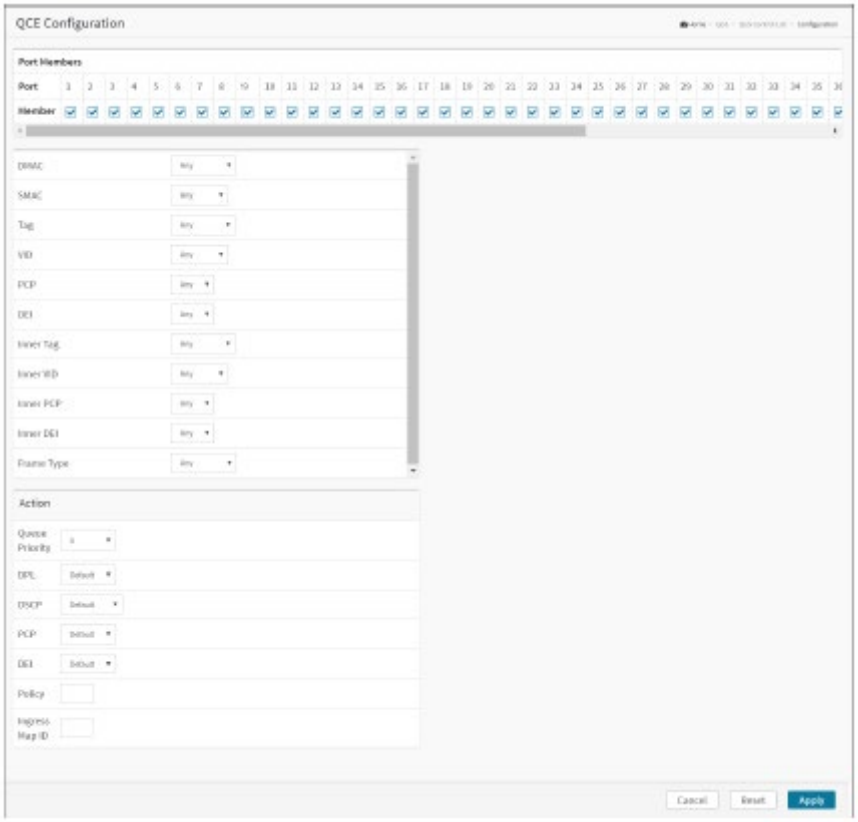


Web インターフェース

Web インターフェースで QoS 制御リストのパラメーターを設定するには:

1. 「Quality of Service」 ＞ 「QoS Contol List」(QoS 制御リスト) ＞ 「Configuration」(設定)をクリックしてください。

2. をクリックして、新しい QoS 制御リストを追加してください。



3. すべてのパラメーターをスクロールしてポートメンバーを呼び出し、QCE ルールに参加させてください。
4. 「Apply」(適用)をクリックして設定を保存してください。
5. 設定を取り消す場合は、「Reset」(リセット)ボタンをクリックする必要があります。そうすると、以前に保存した値へと戻ります。

■パラメーターの説明

QCE:

QCE のインデックスを示します。

Port(ポート):

QCE で設定されたポートのリストを示します。

DMAC:

宛先 MAC アドレスを示します。指定できる値は次のとおりです。

Any(任意):任意の DMAC に一致します。

Unicast(ユニキャスト):ユニキャスト DMAC に一致します。

Multicast(マルチキャスト):マルチキャスト DMAC に一致します。

Broadcast（ブロードキャスト）：ブロードキャスト DMAC に一致します。
<MAC>：特定の DMAC に一致します。
デフォルト値は「Any」（任意）です。

SMAC：
特定の送信元 MAC アドレスまたは「Any」（任意）に一致します。
ポートが DMAC/DIP と一致するように設定されている場合、この項目は DMAC を示します。

Tag Type（タグのタイプ）：
タグの種類を示します。可能な値は次のとおりです。
Any（任意）：タグ付きフレームとタグなしフレームに一致します。
Untagged（タグなし）：タグなしフレームに一致します。
Tagged（タグ付き）：タグ付きフレームに一致します。
C-Tagged（C タグ付き）：C タグ付きフレームに一致します。
S-Tagged（S タグ付き）：S タグ付きフレームに一致します。
デフォルト値は「Any」（任意）です。

VID：
特定の VID または VID の範囲のいずれかを示します（VLAN ID）。VID の範囲は 1～4095 または「Any」（任意）です。

PCP：
Priority Code Point（優先順位コードポイント）：PCP の有効な値は、特定（0、1、2、3、4、5、6、7）または範囲（0～1、2～3、4～5、6～7、0～3、4～7）または「Any」（任意）です。

DEI：
Drop Eligible Indicator：DEI の有効な値は 0、1、または「Any」（任意）です。

Frame Type（フレームタイプ）：
入力フレームを探すフレームのタイプを示します。可能なフレームの種類は次のとおりです。
Any（任意）：QCE はすべてのフレームタイプに一致します。
Ethernet（イーサネット）：イーサネットフレーム（イーサタイプ 0x600～0xFFFF）のみが許可されます。
LLC：（LLC）フレームのみが許可されます。
SNAP：（SNAP）フレームだけが許可されます。
IPv4：QCE は IPV4 フレームのみに一致します。

IPv6：QCE は IPV6 フレームのみに一致します。

Action（アクション）：
設定されたパラメーターがフレームの内容と一致する場合に、入力フレームに対して実行される分類アクションを示します。可能なアクションは次のとおりです。

CoS：サービスクラスを分類します。
DPL：廃棄優先度を分類します。
DSCP：DSCP 値を分類します。
PCP：PCP 値を分類します。
DEI：DEI 値を分類します。
Policy（ポリシー）：ACL ポリシー番号を分類します。

Modification Buttons（変更ボタン）：
次のボタンを使用して、テーブル内の各 QCE（QoS Control Entry）を変更できます。

 ： 現在の行の前に新しい QCE を挿入します。

 ： QCE を編集します。

 ： QCE をリストの上に移動します。

 ： QCE をリストの下に移動します。

 ： QCE を削除します。

 ： 最小のプラス記号を使用すると、QCE リストの下部に新しいエントリーが追加されます。

Port Members（ポートメンバー）：
QCL エントリーにポートを含めるには、チェックボックスを ON にしてください。デフォルトでは、すべてのポートが含まれます。

Key Parameters（主なパラメーター）：
主な設定は以下のとおりです。
DMAC Destination MAC address（DMAC 宛先 MAC アドレス）：「Unicast」（ユニキャスト）、「Multicast」（マルチキャスト）、「Broadcast」（ブロードキャスト）、「Specific」（特定）*(xx-xx-xx-xx-xx-xx)*、または「Any」（任意）の値を指定できます。

SMAC Source MAC address（SMAC 送信元 MAC アドレス）：*xx-xx-xx-xx-xx* または「Any」（任意）です。タグフィールドのタグ値には、「Untagged」（タグ無し）、「Tagged」（タグ付き）、「C-Tagged」（C タグ付き）、「S-Tagged」（S タグ付き）、または「Any」（任意）を指定できます。
VLAN ID の VID の有効な値は、1～4095 または「Any」（任意）の範囲の任意の値です。ユーザーは、特定の値または VID の範囲のいずれかを入力できます。
PCP の有効な値は、特定（0、1、2、3、4、5、6、7）または範囲（0～1、2～3、4～5、6～7、0～3、4～7）または「Any」（任意）です。
DEI の有効な値は、0、1、または「Any」（任意）です。
内部タグフィールドの内部タグ値は、「Untagged」（タグ無し）、「Tagged」（タグ付き）、「C-Tagged」（C タグ付き）、「S-Tagged」（S タグ付き）、または「Any」（任意）です。
内部 VLAN ID の内部 VID の有効な値は、1～4095 または「Any」（任意）の範囲の任意の値です。ユーザーは、特定の値または VID の範囲のいずれかを入力できます。
内部 PCP の有効な値は、特定（0、1、2、3、4、5、6、7）または範囲（0～1、2～3、4～5、6～7、0～3、4～7）、または「Any」（任意）です。
内部 DEI の有効な値は、0、1、または「Any」（任意）です。
フレームタイプには、次のいずれかの値を指定できます。
Any
EtherType
LLC
SNAP
IPv4
IPv6

注意： すべてのフレームタイプについては以下で説明します。

Any（任意）：
すべての種類のフレームを許可します。

EtherType（イーサタイプ）：
有効なイーサタイプは、0x800（IPv4）および 0x86DD（IPv6）または「Any」（任意）を除く 0x600～0xFFFF です。

LLC：
DSAP アドレスの有効な DSAP（Destination Service Access Point）は、0x00～0xFF または「Any」（任意）の範囲で指定できます。
SSAP アドレスの有効な SSAP（Source Service Access Point）は、0x00～0xFF または「Any」（任意）の範囲で指定できます。

制御有効の制御フィールドは、0x00～0xFF または「Any」（任意）の範囲で指定できます。
有効なPID（別名　イーサタイプ）は0x0000～0xFFFF または「Any」（任意）の範囲で指定できます。

SNAP：
有効なPID（別名　イーサタイプ）は0x0000～0xFFFF または「Any」（任意）の範囲で指定できます。

IPv4：
プロトコル IP のプロトコル番号：（0～255、TCP または UDP）または「Any」（任意）。
値/マスク形式または「Any」（任意）の、送信元 IP の特定送信元 IP アドレス。IP とマスクは「*x.y.z.w*」の形式です。この形式における、*x*、*y*、*z*、および *w* は、0～255 の 10 進数です。マスクを 32 ビットのバイナリ文字列に変換し、左から右に読み込む場合、最初のゼロに続くすべてのビットもゼロにする必要があります。
値/マスク形式または「Any」（任意）の、宛先 IP の特定宛先 IP アドレス。

IP Fragment IPv4 frame fragmented option（IP フラグメント IPv4 フレームフラグメント化オプション）：「Yes」、「No」、または「Any」（任意）。

DSCP Diffserv Code Point value（DSCP）：特定の値、値の範囲、または「Any」（任意）を指定できます。DSCP 値の範囲は、BE、CS1～CS7、EF、AF11～AF43 など、0～63 です。

Sport Source TCP/UDP port（スポーツソース TCP/UDP ポート）：（0～65535）または「Any」（任意）、IP プロトコル UDP/TCP に適用可能な特定またはポート範囲。

Dport Destination TCP/UDP port（Dport 宛先 TCP/UDP ポート）：（0～65535）または「Any」（任意）、IP プロトコル UDP/TCP に適用可能な特定のポート範囲またはポート範囲。

IPv6：
プロトコル IP プロトコル番号：（0～255、TCP または UDP）または「Any」（任意）。
送信元 IP 値/マスク形式または「Any」（任意）の IPv6 送信元アドレスの 32LS ビット。
値/マスク形式または「Any」（任意）の、宛先 IP の特定宛先 IP アドレス。

IP Fragment IPv4 frame fragmented option（IP フラグメント IPv4 フレームフラグメント化オプション）：「Yes」、「No」、または「Any」（任意）。

DSCP Diffserv Code Point value（DSCP）：特定の値、値の範囲、または「Any」（任意）を指定できます。DSCP 値の範囲は、BE、CS1～CS7、EF、AF11～AF43 など、0～63 です。

Sport Source TCP/UDP port（スポーツソース TCP/UDP ポート）：（0～65535）または「Any」（任意）、IP プロトコル UDP/TCP に適用可能な特定またはポート範囲。

Dport Destination TCP/UDP port（Dport 宛先 TCP/UDP ポート）：（0～65535）または「Any」（任意）、IP プロトコル UDP/TCP に適用可能な特定のポート範囲またはポート範囲。

Action Parameters（アクションパラメーター）：

CoS Class of Service（サービスの CoS クラス）：（0～7）または「Default」（デフォルト）

DPL Drop Precedence Level（DPL 廃棄優先度）：（0～3）または「Default」（デフォルト）

DSCP DSCP：（0～63、BE、CS1～CS7、EF、AF11～AF43）または「Default」（デフォルト）

PCP PCP：（0～7）または「Default」（デフォルト）

注意： PCP と DEI は個別に設定できません。

DEI DEI：（0～1）または「Default」（デフォルト）

Policy ACL Policy number（ポリシーACL ポリシー番号）：（0～127）または「Default」（デフォルト）（空のフィールド）。

「Default」（デフォルト）は、デフォルトの分類値がこの QCE によって変更されないことを意味します。

■ボタン

Apply（適用）：

クリックすると、変更内容を保存します。

Reset（リセット）：

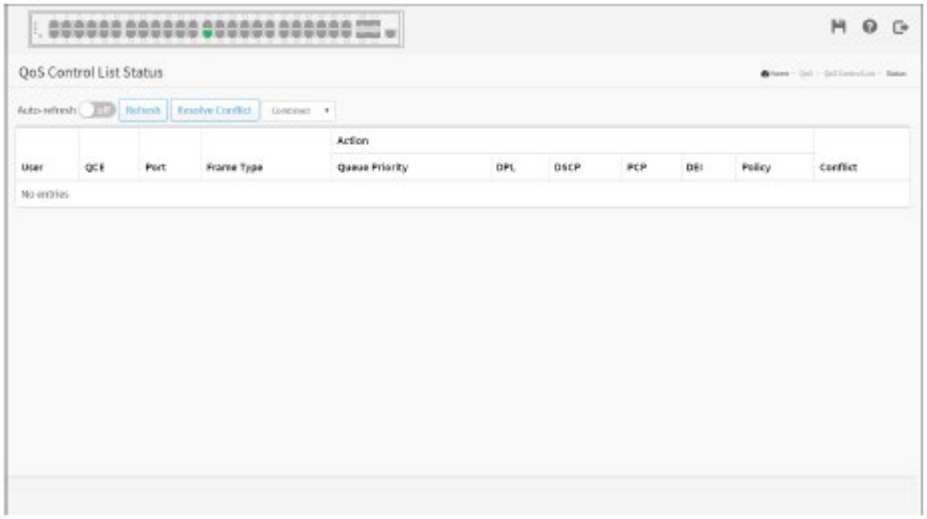
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

Cancel（キャンセル）：

設定変更を保存せずに前の画面に戻ります。

状態

このセクションでは、さまざまな QCL ユーザーによる QCL の状態の設定と表示の各方法について説明します。各行は、定義されている QCE を示します。ハードウェアの制限により、特定の QCE がハードウェアに適用されていない場合は、競合しているということになります。QCE の最大数は、各スイッチで 256 です。



Web インターフェース

Web インターフェースに QoS 制御リストの状態を表示するには:

1. 「Quality of Service」 ＞ 「QoS Contol List」(QoS 制御リスト) ＞ 「Status」(状態)をクリックしてください。
2. 情報を自動更新する場合は、「Auto-refresh」(自動更新)を呼び出す必要があります。
3. スクロールして、結合されたスタティック VLAN、ボイス VLAN、および競合を選択してください。
4. 「Refresh」(更新)をクリックして、MVR 統計情報のエントリーの最新情報を表示してください。

■パラメーターの説明

User(ユーザー):

QCL ユーザーを示します。

QCE:

QCE のインデックスを示します。

Port(ポート):

QCE で設定されたポートのリストを示します。

Frame Type（フレームタイプ）：

入力フレームを探すフレームのタイプを示します。可能なフレームの種類は次のとおりです。

Any（任意）：任意のフレームタイプに一致します。

Ethernet（イーサネット）：イーサタイプのフレームに一致します。

LLC：（LLC）フレームに一致します。

SNAP：（SNAP）フレームに一致します。

IPv4：IPv4 フレームに一致します。

IPv6：IPv6 フレームに一致します。

Action（アクション）：

設定されたパラメーターがフレームの内容と一致する場合に、入力フレームに対して実行される分類アクションを示します。可能なアクションは次のとおりです。

CoS：サービスクラスを分類します。

DPL：廃棄優先度を分類します。

DSCP：DSCP 値を分類します。

PCP：PCP 値を分類します。

DEI：DEI 値を分類します。

Policy（ポリシー）：ACL ポリシー番号を分類します。

Ingress Map（イングレス・マップ）：イングレス・マップ ID を分類します。

Conflict（競合）：

QCL エントリーの競合の状態を表示します。QCE の追加に必要なリソースが使用できない場合があります。その場合、競合の状態が「Yes」と表示され、それ以外の場合は常に「No」と表示されます。競合した場合は、「Resolve Conflict」（競合の解決）ボタンを押すと、QCL エントリーを追加するために必要な H/W リソースが解放されるため、これによって解決することができます。

■ボタン

Auto-refresh（自動更新）：

画面を自動的に更新する場合は、このチェックボックスを ON にしてください。自動更新は 3 秒間隔で行われます。

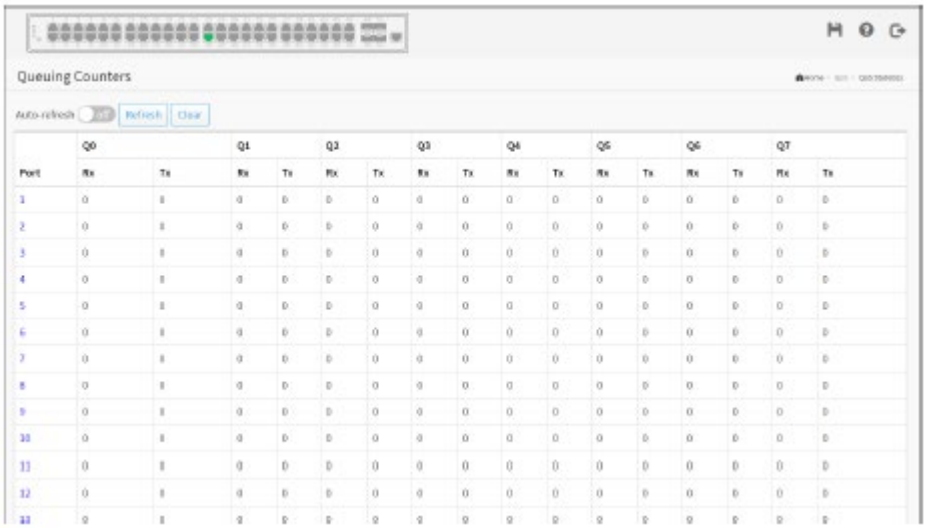
Refresh（更新）:
クリックするとページを更新します。

Combine（結合）:
このドロップダウンリストから QCL の状態を選択してください。

Resolve Conflict（競合の解決）:
QCL エントリーの競合の状態が「Yes」の場合、このボタンをクリックして、QCL エントリーの追加に必要なリソースを解放してください。

QoS の統計

この画面には、すべてのスイッチポートの各種キューに関する統計情報が表示されます。



Web インターフェース

Web インターフェースでキューイング・カウンターを表示するには:

1. 「Quality of Service」 ＞ 「QoS Statistics」(QoS の統計) をクリックしてください。
2. 情報を自動更新する場合は、「Auto-refresh」(自動更新)を呼び出す必要があります。
3. キューイング・カウンターを更新するには「Refresh」(更新)をクリックしてください。また、すべての情報を消去するには、「Clear」(消去)をクリックしてください。

■パラメーターの説明

Port (ポート) :

同じ行に含まれる設定の論理ポートです。

Qn:

Qn はキュー番号です。各ポートには 8 つの QoS キューがあります。優先順位が最も低いキューは、Q0 です。

Rx/Tx:

キューあたりの受信および送信パケット数です。

■ボタン

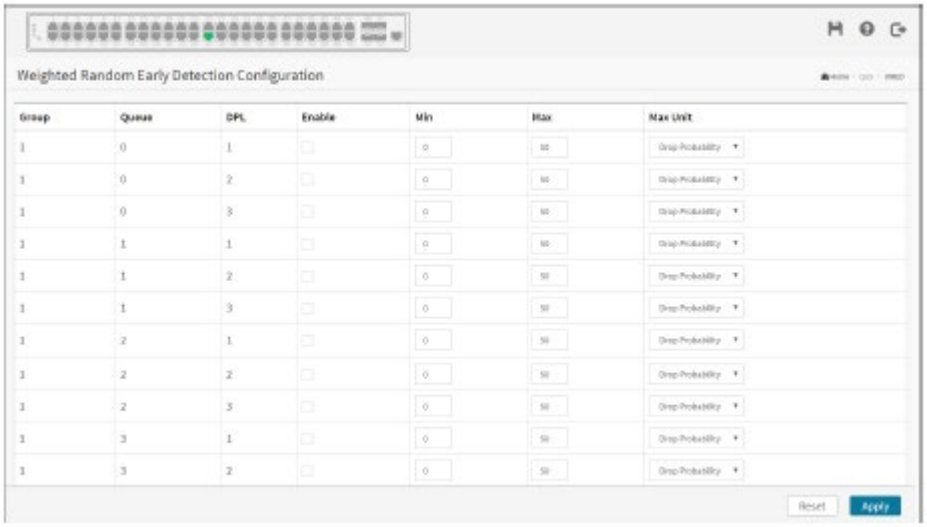
Auto-refresh（自動更新）:
画面を自動的に更新する場合は、このチェックボックスをONにしてください。自動更新は3秒間隔で行われます。

Refresh（更新）:
クリックすると、画面がすぐに更新されます。

Clear（消去）:
クリックすると、画面の内容をクリアします。

WRED

この画面では、「Random Early Detection」（ランダム初期検知、RED）の設定を定義することができます。キューの異なるRED設定を使用すると、キュー間の重み付けランダム初期検知（WRED）操作を取得することができます。設定は、スイッチのすべてのポートで共通です。



Web インターフェース

Web インターフェースで、ランダム初期検知を設定して表示するには:

1. 「Quality of Service」 ＞ 「WRED」 をクリックしてください。
2. すべてのパラメーターをスクロールし、加重ランダム初期検出設定を呼び出してください。
3. 「Apply」（適用）をクリックして設定を保存してください。
4. 設定を取り消す場合は、「Reset」（リセット）ボタンをクリックする必要があります。そうすると、以前に保存した値へと戻ります。

■パラメーターの説明

Port（ポート）:

同じ行に含まれる設定の論理ポートです。

Group（グループ）:

以下の設定が適用されるWREDグループ番号です。

Queue（キュー）:

以下の設定が適用されるキュー番号（CoS）です。

DPL：
以下の設定が適用される廃棄優先度です。

Enable（有効にする）：
このエントリーに対して RED を有効にするかどうかを制御します。

Min（最小）：
RED 充填レベルの下限しきい値を制御します。キューの充填レベルがこのしきい値を下回る場合、廃棄確率は 0 になります。この値は 0～100%に制限されています。

Max（最大）：
廃棄優先度が 0 より大きい（黄色のフレーム）ということでマークされたフレームの上部 RED 廃棄確率または充填レベルのしきい値を制御します。この値は 1～100%に制限されています。

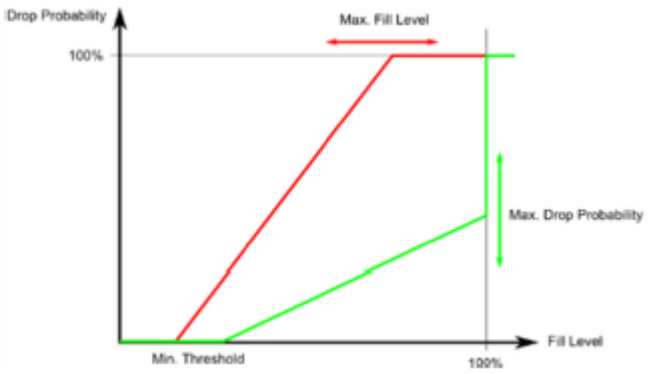
Max Unit（最大ユニット）：
最大のユニットを選択します。可能な値は次のとおりです。

Drop Probability（廃棄確率）：「Max」（最大）は、100%の充填レベルをわずかに下回るドロップ確率を制御します。

Fill Level（充填レベル）：「Max」（最大）は、廃棄確率が 100%に達する充填レベルを制御します。

RED Drop Probability Function（RED 廃棄確率関数）

次の図は、廃棄確率と、関連するパラメーターを持つ充填レベル関数を示しています。



「Min」（最小）は、「Drop Precedence Level」（廃棄確率）＞[0]（黄色のフレーム）とマークされたフレームの廃棄をキューがランダムに開始する充填レベルです。

「Max Unit」（最大ユニット）が「Drop Probability」（廃棄確率）（緑色の線）の場合、「Max」（最大）

は充填レベルが 100%をわずかに下回ったときの廃棄確率を制御します。

「Max Unit」(最大ユニット)が「Fill Level」(充填レベル)(赤い線)の場合、「Max」(最大)は廃棄確率が 100%に達する充填レベルを制御します。この設定は、廃棄優先度が 0(緑色のフレーム)でマークされたフレームのみのキューの一部を予約可能にします。予約部分は(100 - 最大)%として計算され、廃棄優先度が 0(緑色のフレーム)でマークされたフレームは破棄されません。

フレームの廃棄確率は、ゼロ(最小平均キュー充填レベル)から最大廃棄確率または充填レベルまで直線的に増加します。

■ボタン

Apply(適用):
クリックすると、変更内容を保存します。

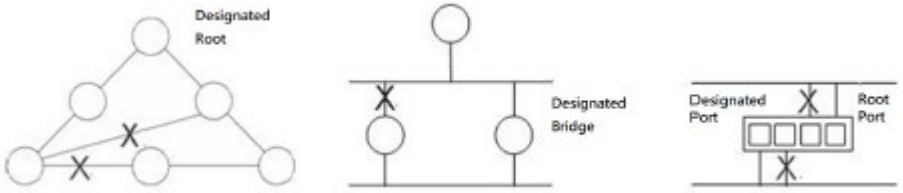
Refresh(更新):
クリックするとページを更新します。

第 8 章
スパニングツリー

概要

スパニングツリープロトコル（STP）は、ネットワーク・ループの検出と無効化、およびスイッチ、ブリッジ、またはルーター間のバックアップ・リンクの提供に使用できます。これにより、スイッチはネットワーク内の他のブリッジング・デバイス（つまり、STP 準拠のスイッチ、ブリッジ、またはルーター）と通信して、ネットワーク上の任意の 2 つのステーション間に 1 つのルートのみが存在することを確認し、プライマリーリンクがダウンしたときに自動的に引き継ぐバックアップ・リンクを提供できます。

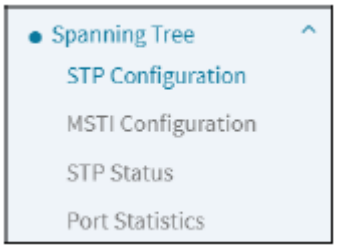
STP – STP は、分散アルゴリズムを使用して、スパニングツリー・ネットワークのルートとして機能するブリッジング・デバイス（STP 準拠のスイッチ、ブリッジ、またはルーター）を選択します。各ブリッジング・デバイス（ルートデバイスを除く）のルートポートを選択します。このルートポートは、そのデバイスからルートデバイスにパケットを転送するときに最も低いパス・コストを発生します。次に、各 LAN からルートデバイスにパケットを転送するときに最も低いパス・コストが発生する、指定されたブリッジング・デバイスを選択します。指定されたブリッジング・デバイスに接続されているすべてのポートが、指定されたポートとして割り当てられます。最低コストのスパニングツリーを決定した後、すべてのルートポートと指定ポートを有効にし、他のすべてのポートを無効にします。そのため、ネットワークパケットはルートポートと指定ポート間でのみ転送され、ネットワーク・ループが発生する可能性はありません。



安定したネットワークトポロジーが確立されると、すべてのブリッジはルートブリッジから送信された Hello BPDU（Bridge Protocol Data Units）をリッスンします。ブリッジが事前定義された間隔（最大経過時間）後に Hello BPDU を取得しない場合、ブリッジはルートブリッジへのリンクがダウンしていると見なします。その後、このブリッジは、ネットワークを再設定して、有効なネットワークトポロジーを

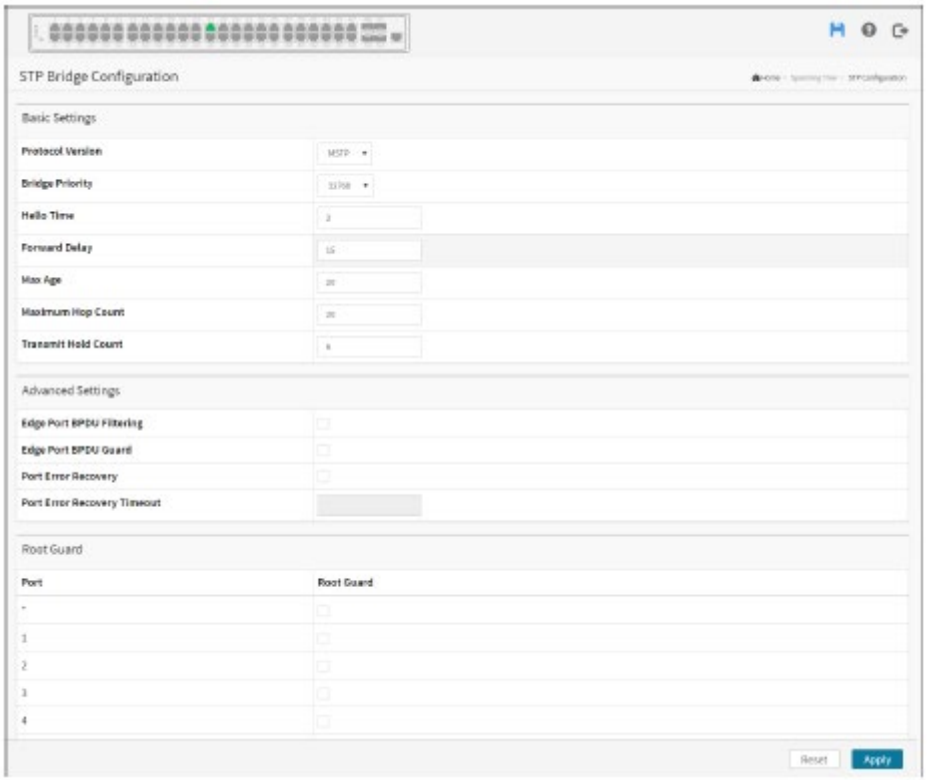
再確立するために、他のブリッジとのネゴシエーションを開始します。

メニューは以下のとおりです。



STP の設定

このセクションでは、スパニングツリープロトコルを有効にするかどうかを選択し、必要なプロトコルバージョンを選択することができます。



Web インターフェース

Web インターフェースでスパニングツリープロトコルのバージョンを設定するには:

1. 「Spanning Tree」(スパニングツリー) ＞ 「STP Configuration」(STP の設定)をクリックしてください。
2. スクロールしてパラメーターを選択したら、「Basic Settings」(基本設定)における空白のフィールドにパラメーターの使用可能な値を記録してください。
3. 起動して、パラメーターを有効または無効にし、「Advanced Settings」(詳細設定)の空白のフィールドにパラメーターの使用可能な値を記録してください。
4. 「Apply」(適用)をクリックして設定を保存してください。
5. 設定を取り消す場合は、「Reset」(リセット)ボタンをクリックする必要があります。そうすると、以前に保存した値へと戻ります。

■パラメーターの説明

Basic Settings（基本設定）

Protocol Version（プロトコルバージョン）：
MSTP/RSTP/STP プロトコルのバージョン設定です。有効な値は STP、RSTP、および MSTP です。

Bridge Priority（ブリッジ優先度）：
ブリッジの優先度を制御します。数値が小さいほど優先度が高くなります。ブリッジ優先度に MSTI インスタンス番号を加え、スイッチの 6 バイト MAC アドレスを連結すると、ブリッジ識別子が形成されます。MSTP 操作の場合、これは CIST の優先度です。それ以外の場合、これは STP/RSTP ブリッジの優先度です。

Hello Time（ハロータイム）：
STP BPDU を送信する間隔です。有効な値の範囲は 1～10 秒で、デフォルトは 2 秒です。

注意： このパラメーターをデフォルト値から変更することは推奨されません。ネットワークに悪影響を及ぼす可能性があります。

Forward Delay（転送遅延）：
STP ブリッジがルートおよび指定ポートを転送するために使用する遅延（STP 互換モードで使用）です。有効な値の範囲は 4～30 秒です。

Max Age（最大経過時間）：
ルートブリッジである場合にブリッジによって送信される情報の最大経過時間です。有効な値は 6～40 秒で、最大経過時間は、（転送遅延-1）×2 以下である必要があります。

Maximum Hop Count（最大ホップ数）：
これは、MSTI 領域の境界で生成された MSTI 情報のための残りのホップの初期値を定義します。そして、ルートブリッジが BPDU 情報を配布できるブリッジの数を定義します。有効な値の範囲は 6～40 ホップです。

Transmit Hold Count（送信ホールド数）：
ブリッジポートが 1 秒あたりに送信できる BPDU の数です。この値を超えると、次の BPDU の伝送が遅延されます。有効な値の範囲は 1～10BPDU/秒です。

Advanced Settings（詳細設定）

Edge Port BPDU Filtering（エッジポート BPDU フィルタリング）：

エッジとして明示的に設定されたポートが BPDU を送受信するかどうかを制御します。

Edge Port BPDU Guard（エッジポート BPDU ガード）：
エッジとして明示的に設定されたポートが BPDU の受信時に自身を無効にするかどうかを制御します。ポートはエラー無効状態になり、アクティブなトポロジーから削除されます。

Port Error Recovery（ポートエラー回復）：
特定の時間が経過した後に、エラー無効状態のポートを自動的に有効にするかどうかを制御します。回復が有効になっていない場合は、通常の STP 操作でポートを無効にして再度有効にする必要があります。この状態は、システムの再起動によってもクリアされます。

Port Error Recovery Timeout（ポートエラー回復タイムアウト）：
エラー無効状態のポートの前に経過する時間を有効にすることができます。有効な値は 30～86400 秒（24 時間）です。

■ボタン

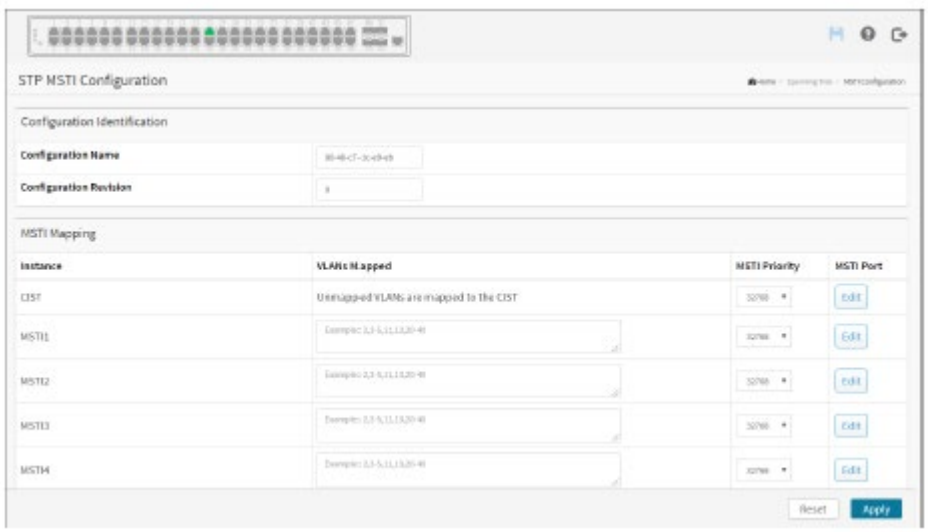
Apply（適用）：
クリックすると、変更内容を保存します。

Reset（リセット）：
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

MSTI の設定

ブリッジインスタンスであるスイッチにスパニングツリープロトコルを実装する場合、CIST は、明示的にマッピングされていない VLAN を受信するため、明示的なマッピングには使用できません。これは、MSTI にマッピングされた VLAN のリストを設定する必要があるということに起因します。VLAN は、カンマまたはスペースで区切る必要があります。VLAN は 1 つの MSTI にのみマッピングできます。未使用の MSTI は空白のままにしておく必要があります（すなわち、VLAN はマッピングされていません）。

このセクションでは、現在の STP MSTI ブリッジインスタンスの優先度設定をチェックしたり、変更したりすることができます。



Web インターフェース

Web インターフェースでスパニングツリーMSTI を設定するには：

1. 「Spanning Tree」（スパニングツリー） ＞ 「MSTI Configuration」（MSTI の設定）をクリックしてください。
2. フィールドに設定 ID パラメーターを指定してください。そうしたら、「VLAN Mapped blank」（VLAN にマッピングされた空白）の項目を指定してください。
3. 「Apply」（適用）をクリックして設定を保存してください。
4. 設定を取り消す場合は、「Reset」（リセット）ボタンをクリックする必要があります。そうすると、以前に保存した値へと戻ります。
5. 「Edit」（編集）をクリックして、STP CIST ポート設定を定義してください。

■パラメーターの説明

Configuration Identification（設定の識別）

Configuration Name（設定名）：

VLAN から MSTI へのマッピングを識別する名前です。ブリッジは、MSTI（リージョン内）のスパニングツリーを共有するために、名前とリビジョン（下記参照）、および VLAN から MSTI へのマッピング設定を共有する必要があります。名前は最大 32 文字です。

Configuration Revision（設定リビジョン）：

上記の MSTI 設定のリビジョンです。これは 0～65535 の整数である必要があります。

MSTI Mapping（MSTI マッピング）

Instance（インスタンス）：

ブリッジインスタンスです。CIST は、明示的にマッピングされていない VLAN を受信するため、明示的なマッピングには使用できません。

VLANs Mapped（マッピングされた VLAN）：

MSTI にマッピングされた VLAN のリストです。VLAN は、1 つ（*xx*、*xx* は 1～4094）の VLAN、または範囲（*xx*～*yy*）として指定できます。それぞれをカンマまたはスペースで区切る必要があります。VLAN は 1 つの MSTI にのみマッピングできます。未使用の MSTI は空白のままにしておく必要があります（つまり、VLAN がマップされていない場合）。例：2,5,20-40

MSTI Priority（MSTI 優先度）：

ブリッジの優先度を制御します。数値が小さいほど優先度が高くなります。ブリッジ優先度に MSTI インスタンス番号を加え、スイッチの 6 バイト MAC アドレスを連結すると、ブリッジ識別子が形成されます。

■ボタン

Apply（適用）：

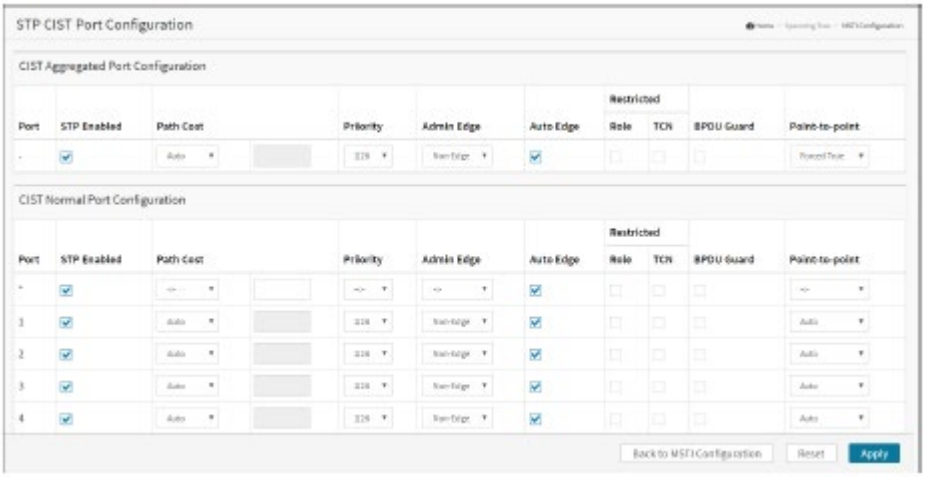
クリックすると、変更内容を保存します。

Reset（リセット）：

クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります

MSTI Port（MSTI ポート）：

クリックすると、STP CIST ポート設定を定義します。



■パラメーターの説明

Port（ポート）：

論理 STP ポートのスイッチポート番号です。

STP Enabled（STP 有効）：

このスイッチポートで STP を有効にするかどうかを制御します。この項目は、音声 VLAN 機能が有効になっている場合にのみ読み取られます。音声 VLAN ポートモードは、この項目が有効の場合にのみ読み取られます。

Path Cost（パス・コスト）：

ポートによって発生するパス・コストを制御します。「Auto」（自動）設定では、物理リンク速度に応じて、802.1D 推奨値を使用してパス・コストが設定されます。「Specific」（特定）設定を使用すると、ユーザー定義の値を入力できます。パス・コストは、ネットワークのアクティブなトポロジーを確立するときに使用されます。パス・コストの低いポートは、パス・コストの高いポートよりも優先される転送ポートとして選択されます。有効な値の範囲は 1～200000000 です。

Priority（優先度）：

ポート優先度を制御します。これは、同一のポートコストを持つポートの優先度を制御するために使用できます（上記参照）。

AdminEdge：

operEdge フラグをセットまたはクリアのどちらとして開始するかを制御します（ポートの初期化時における operEdge の初期状態）。

AutoEdge：
ブリッジポートでブリッジが自動エッジ検出を有効にするかどうかを制御します。これにより、BPDU をポートで受信するかどうかという点から operEdge を導き出すことができます。

Restricted Role（制限付きロール）：
有効にすると、最適なスパニングツリープライオリティベクターを持っていても、ポートが CIST または MSTI のルートポートとして選択されなくなります。このようなポートは、ルートポートが選択された後、代替ポートとして選択されます。設定されている場合、スパニングツリー接続が不足する可能性があります。ネットワーク管理者は、ネットワークのコアリージョンの外部にあるブリッジがスパニングツリーのアクティブトポロジーに影響を与えないように設定できます。これは、これらのブリッジが管理者の完全な制御下にない可能性があるためです。この機能は、ルートガードとも呼ばれます。

Restricted TCN（制限付き TCN）：
有効にすると、ポートは受信したトポロジー変更とトポロジー変更を他のポートに通知しません。設定されている場合、永続的に不正に学習されたステーションロケーション情報の結果として、スパニングツリーのアクティブトポロジーが変更された後、接続が一時的に失われる可能性があります。ネットワーク管理者は、ネットワークのコアリージョンの外部にブリッジが存在し、そのリージョンでアドレスがフラッシュされるのを防ぐように設定します。これは、これらのブリッジが管理者の完全な制御下にないか、接続された LAN の物理リンク状態が頻繁に通過するためです。

BPDU Guard（BPDU ガード）：
有効にすると、有効な BPDU を受信したときにポートが自身を無効にします。同様のブリッジ設定とは異なり、ポートエッジの状態はこの設定に影響しません。この設定により、ポートが error-disabled 状態になると、ブリッジポートエラーリカバリー設定も適用されます。

Point to Point（ポイント・ツー・ポイント）
ポートが共有メディアではなくポイント・ツー・ポイント LAN に接続するかどうかを制御します。これは、自動的に決定されるか、true または false のいずれかに強制的に設定されます。ポイント・ツー・ポイント LAN では、共有メディアよりも転送状態への遷移が速くなります。

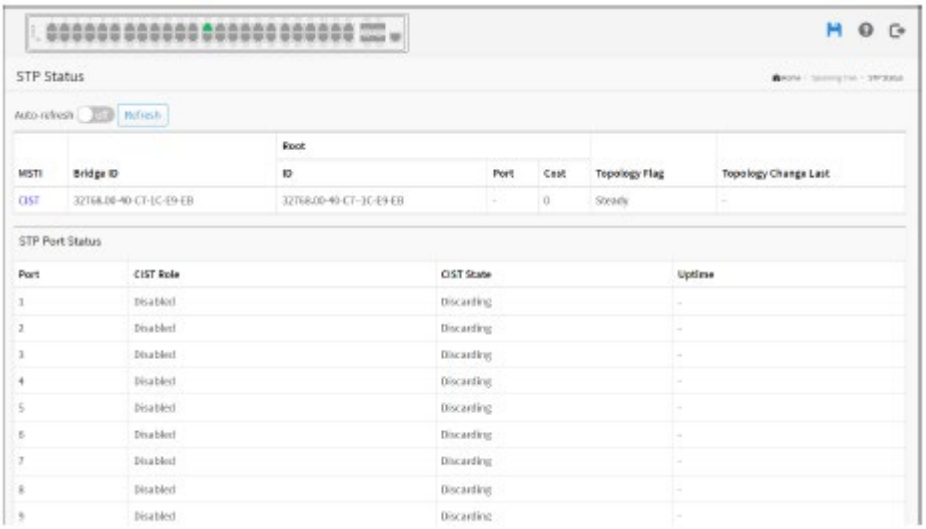
■ボタン
Apply（適用）：
クリックすると、変更内容を保存します。

Reset（リセット）：
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

STP の状態

この画面には、すべての STP ブリッジインスタンスの状態の概要が表示されます。

表示されるテーブルには、各 STP ブリッジインスタンスの行が含まれており、この列には次の情報が表示されます。



Web インターフェース

Web インターフェースで STP ブリッジの状態を表示するには:

1. 「Spanning Tree」(スパニングツリー) ＞ 「STP Status」(STP の状態)をクリックしてください。
2. 情報を自動更新する場合は、「Auto-refresh」(自動更新)を呼び出す必要があります。
3. 「Refresh」(更新)をクリックして、STP ブリッジを更新してください。
4. 「STP Detailed Bridge Status」(STP の詳細ブリッジ状態)の横にある「CIST」をクリックしてください。

■パラメーターの説明

MSTI:

ブリッジインスタンスです。これは、「STP Detailed Bridge Status」(STP の詳細ブリッジ状態)へのリンクでもあります。

Bridge ID(ブリッジ ID):

このブリッジインスタンスのブリッジ ID です。

Root ID（ルート ID）：
現在選択されているルートブリッジのブリッジ ID です。

Root Port（ルートポート）：
現在ルートポートの役割が割り当てられているスイッチポートです。

Root Cost（ルートコスト）：
ルートのパス・コストです。ルートブリッジの場合は 0 です。他のすべてのブリッジでは、ルートブリッジへの最小コスト・パス上のポート・パス・コストの合計です。

Topology Flag（トポロジーフラグ）：
このブリッジインスタンスのトポロジー変更フラグの現在の状態です。

Topology Change Last（トポロジーの最終変更時間）：
前回トポロジーの変更が発生してからの経過時間です。

STP Port Status（STP ポートの状態）
Port（ポート）：
論理 STP ポートのスイッチポート番号です。

CIST Role（CIST の役割）：
CIST ポートにおける現在の STP ポートの役割です。ポートの役割には、「Alternate Port」（代替ポート）、「Backup Port」（バックアップポート）、「Root Port」（ルートポート）、「Designated Port」（指定ポート）、「Disabled」（無効）のいずれかの値を指定できます。

CIST State（CIST の状態）：
CIST ポートにおける現在の STP ポートの状態です。ポートの状態は、「Blocking」（ブロック中）、「Learning」（学習中）、「Forwarding」（転送中）のいずれかの値になります。

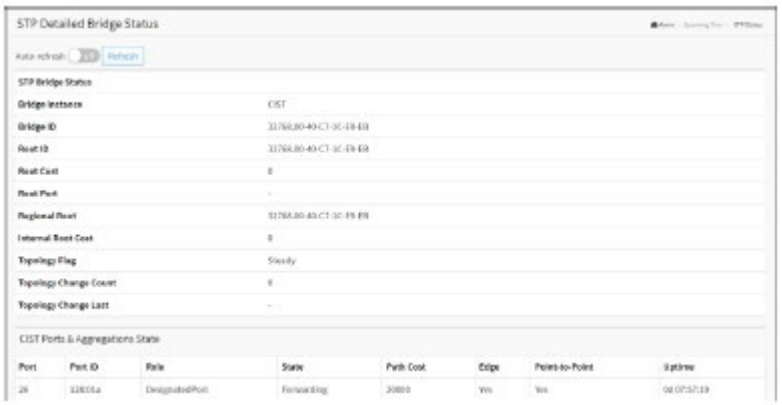
Uptime（アップタイム）：
ブリッジポートが最後に初期化されてからの時間です。

■ボタン

Auto-refresh（自動更新）:
画面を自動的に更新する場合は、このチェックボックスをONにしてください。自動更新は3秒間隔で行われます。

Refresh（更新）:
クリックすると、画面がすぐに更新されます。

CIST:
クリックすると、次の画面である「STP Detailed Bridge Status」（STPの詳細ブリッジ状態）画面に進みます。



■パラメーターの説明

STP Bridge Status（STPブリッジの状態）

Bridge Instance（ブリッジインスタンス）:
ブリッジインスタンス － CIST、MST1…

Bridge ID（ブリッジID）:
このブリッジインスタンスのブリッジIDです。

Root ID（ルートID）:
現在選択されているルートブリッジのブリッジIDです。

Root Cost（ルートコスト）:
ルートのパス・コストです。ルートブリッジの場合、これは0です。他のすべてのブリッジでは、ルートブリッジへの最小コスト・パス上のポート・パス・コストの合計です。

Root Port（ルートポート）:

現在ルートポートの役割が割り当てられているスイッチポートです。

Regional Root（リージョナル・ルート）：
現在選択されているリージョンルートのブリッジ ID です。これは、このブリッジの MSTP リージョン内にあります。

Internal Root Cost（内部ルートコスト）：
リージョナル・ルートのパス・コストです。リージョナル・ルートブリッジの場合、これは 0 です。同じ MSTP リージョン内の他のすべての CIST インスタンスの場合、内部ルートブリッジへの最小コスト・パスの内部ポート・パス・コストの合計になります（CIST インスタンスの場合のみ）。

Topology Flag（トポロジーフラグ）：
このブリッジインスタンスのトポロジー変更フラグの現在の状態です。

Topology Change Count（トポロジー変更数）：
トポロジー変更フラグが設定された回数（1 秒間隔）です。

Topology Change Last（トポロジーの最終変更時間）
トポロジーフラグが最後に設定されてからの経過時間です。

CIST Ports & Aggregations State（CIST ポート＆アグリゲーションの状態）
Port（ポート）：
論理 STP ポートのスイッチポート番号です。

Port ID（ポート ID）：
STP プロトコルで使用されるポート ID です。これは、ブリッジポートの優先度部分と論理ポートのインデックスです。

Role（役割）：
現在の STP ポートの役割です。ポートの役割には、、「Alternate Port」（代替ポート）、「Backup Port」（バックアップポート）、「Root Port」（ルートポート）、「Designated Port」（指定ポート）のいずれかの値を指定できます。

State（状態）：
現在の STP ポートの状態です。ポートの状態は、「Discarding」（破棄中）、「Learning」（学習中）、「Forwarding」（転送中）のいずれかの値になります。

Path Cost（パス・コスト）：
現在の STP ポートにおけるパス・コストです。これは、自動設定から計算された値か、明示的に設定された値のいずれかになります。

Edge（エッジ）：
現在の STP ポートにおける（動作可能な）エッジフラグです。エッジポートは、ブリッジが接続されていないスイッチポートです。フラグは自動的に計算されるか、明示的に設定されます。各エッジポートは、ループに参加する可能性がないため、直接、転送中のポート状態に遷移します。

Point-to-Point（ポイント・ツー・ポイント）：
現在の STP ポートにおけるポイント・ツー・ポイントのフラグです。ポイント・ツー・ポイントのポートは、非共有 LAN メディアに接続します。フラグは自動的に計算されるか、明示的に設定されます。ポートのポイント・ツー・ポイントのプロパティは、STP の状態に遷移する速度に影響します。

Uptime（アップタイム）：
ブリッジポートが最後に初期化されてからの時間です。

■ボタン

Auto-refresh（自動更新）：
画面を自動的に更新する場合は、このチェックボックスを ON にしてください。自動更新は 3 秒間隔で行われます。

Refresh（更新）：
クリックするとページを更新します。

ポートの統計

この画面には、スイッチのブリッジポートにおける STP ポートの統計カウンターが表示されます。

Web インターフェース

STP ポートの統計を Web インターフェースに表示するには:

1. 「Spanning Tree」(スパニングツリー) ＞ 「Port Statistics」(ポートの統計)をクリックしてください。
2. 情報を自動更新する場合は、「Auto-refresh」(自動更新)を呼び出す必要があります。
3. 「Refresh」(更新)をクリックして、STP ブリッジを更新してください。

■パラメーターの説明

Port (ポート) :

論理 STP ポートのスイッチポート番号です。

MSTP:

ポートで MSTP 設定の BPDU が受信/送信した回数です。

RSTP:

ポートで RSTP 設定の BPDU が受信/送信した回数です。

STP:

ポートでレガシーSTP 設定の BPDU の受信/送信数です。

TCN:
ポートで(レガシー)トポロジーの変更通知 BPDU の受信/送信数です。

Discarded Unknown(不明な破棄):
ポートで受信(および破棄)された不明なスパニングツリーBPDU の数です。

Discarded Illegal(不正な破棄):
ポートで不正なスパニングツリーBPDU を受信(および破棄)した回数です。

■ボタン

Auto-refresh(自動更新):
画面を自動的に更新する場合は、このチェックボックスを ON にしてください。自動更新は 3 秒間隔で行われます。

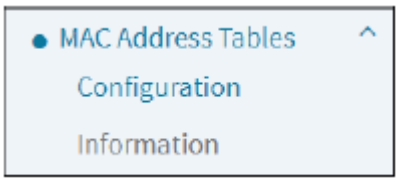
Refresh(更新):
クリックすると、画面がすぐに更新されます。

第 9 章
MAC アドレスのテーブル

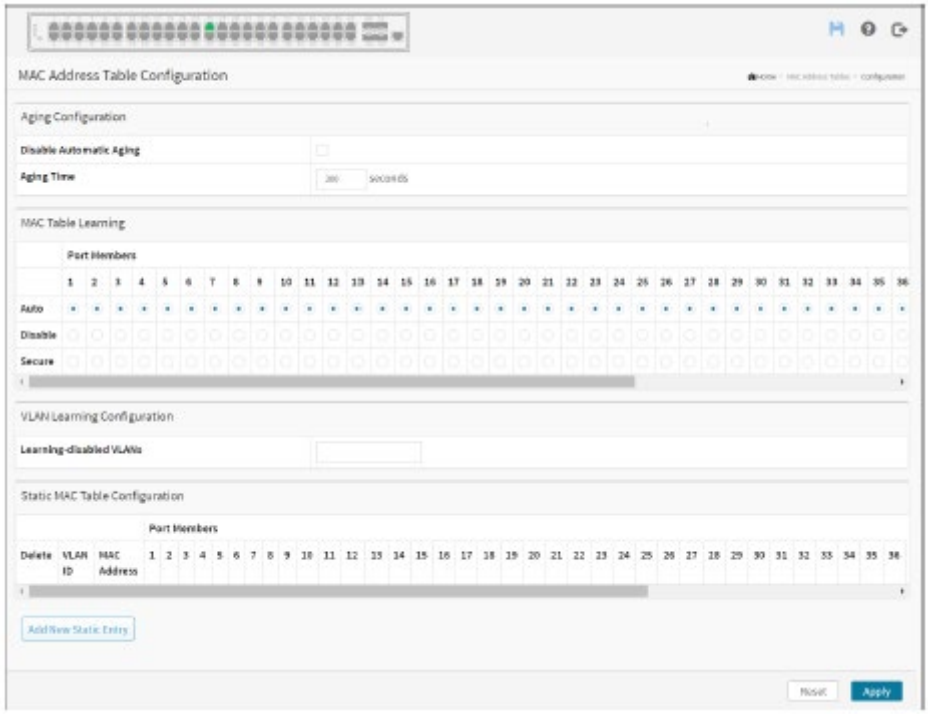
概要

フレームの切替は、フレームに含まれる DMAC アドレスに基づきます。スイッチは、(フレーム内の DMAC アドレスに基づいて)フレームがどのポートに送信されるべきかを知るために、MAC アドレスをスイッチポートにマッピングするテーブルを構築します。このテーブルには、スタティックエントリーとダイナミックエントリーの両方が含まれています。管理者が DMAC アドレスとスイッチポート間の固定マッピングを実行する場合、スタティックエントリーはネットワーク管理者によって設定されます。フレームには、フレームを送信する装置の MAC アドレスを示す MAC アドレス(SMAC アドレス)も含まれます。SMAC アドレスは、スイッチがこれらのダイナミック MAC アドレスを使用して MAC テーブルを自動的に更新するために使用されます。設定可能なエージングタイム後に対応する SMAC アドレスを持つフレームが見つからなかった場合、ダイナミックエントリーは MAC テーブルから削除されます。

メニューは以下のとおりです。



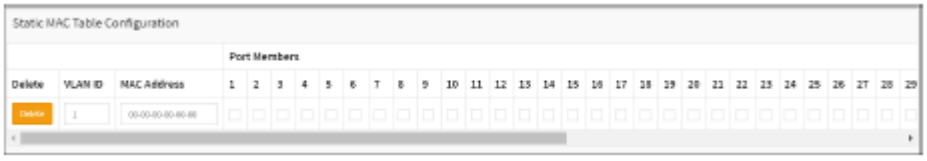
設定



Web インターフェース

Web インターフェースで MAC アドレステーブルを設定するには:

1. 「MAC Address Tables」(MAC アドレステーブル) ＞ 「Configuration」(設定)をクリックしてください。
2. 「Disable Automatic Aging」(自動エージングを無効にする)と「Aging Time」(エージングタイム)の各フィールドを指定してください。
3. 「Port Members」(ポートメンバー)の値(自動、無効、セキュア)を指定してください。
4. 「Learning-disabled VLAN」(学習無効 VLAN)を指定してください。
5. 新しいスタティックエントリーを追加し、「VLAN IP」および「MAC Address」(MAC アドレス)、「Port Members」(ポートメンバー)を指定してください。



6. 「Apply」(適用)をクリックしてください。

■パラメーターの説明

Aging Configuration（エージング設定）：

デフォルトでは、ダイナミックエントリーは 300 秒後に MAC テーブルから削除されます。この削除は、エージングとも呼ばれます。

エージング時間を設定するには、ここに秒単位の値を入力します（例：エージングタイムの秒数）。指定できる範囲は 10～1000000 秒です。

「Disable Automatic Aging」（自動エージングを無効にする）にチェックを入れると、ダイナミックエントリーの自動エージングを無効にします。

MAC Table Learning（MAC テーブルの学習）：

特定のポートの学習モードがグレー表示されている場合、別のモジュールがそのモードを制御しているため、ユーザーは変更することができません。このようなモジュールの例として、802.1X における MAC ベース認証があります。各ポートは、次の設定に基づいて学習を実行できます。

Auto（自動）：学習は、未知の SMAC を持つフレームを受信すると、すぐに自動で行われます。

Disable（無効）：学習は行われません。

Secure（セキュア）：スタティック MAC エントリーのみが学習され、他のすべてのフレームは破棄されます。

注意： セキュア学習モードに変更する前に、スイッチの管理に使用されているリンクがスタティック MAC テーブルに追加されていることを確認してください。追加されていない場合、管理リンクは失われ、別の非セキュアポートを使用するか、またはシリアルインターフェースを介してスイッチに接続することによってのみ復元できます。

VLAN Learning Configuration（VLAN 学習の設定）

Learning-disabled VLANs（学習無効 VLAN）：

このフィールドには、学習が無効な VLAN が表示されます。学習が無効な VLAN に新しい MAC が到達しても、MAC は学習されません。デフォルトでは、項目は空です。リスト構文を使用して、個々の要素をカンマで区切ることで、より多くの VLAN を作成できます。範囲は、下限と上限を区切るダッシュで指定します。以下の例は、VLAN1、10、11、12、13、200、および 300:1,10-13,200,300 を作成します。区切り文字の間にはスペースを入れることができます。

Static MAC Table Configuration（スタティック MAC テーブルの設定）

MAC テーブルのスタティックエントリーは、このテーブルに示されています。スタティック MAC テーブルには、128 のエントリーを含めることができます。最大 128 のエントリーは、スイッチごとではなく、スタック全体に適用されます。

VLAN ID：
エントリーの VLAN ID です。

MAC Address（MAC アドレス）：
エントリーの MAC アドレスです。

Port Members（ポートメンバー）：
チェックマークは、エントリーのメンバーであるポートを示します。必要に応じてチェックボックスを ON または OFF にして、エントリーを変更してください。

■ボタン

Add a New Static Entry（新規スタティックエントリーの追加）：
クリックすると、スタティック MAC テーブルに新しいエントリーを追加します。新しいエントリーの VLAN ID、MAC アドレス、およびポートメンバーを指定してください。そうしたら、「Apply」（適用）をクリックしてください。

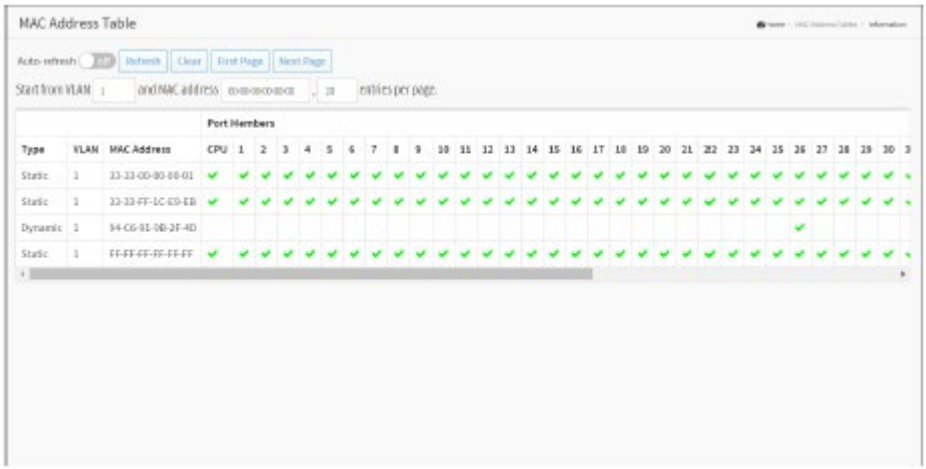
Delete（削除）：
チェックを入れると、エントリーを削除できます。このエントリーは、次回保存時に削除されます。

Apply（適用）：
クリックすると、変更内容を保存します。

Reset（リセット）：
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

情報

MAC テーブルのエントリーは、この画面に表示されます。MAC テーブルには最大 8192 個のエントリーが含まれ、最初に VLAN ID、次に MAC アドレスでソートされます。



Web インターフェース

Web インターフェースで MAC アドレステーブルを表示するには:

1. 「MAC Address Tables」(MAC アドレステーブル) ＞ 「Information」(情報)をクリックしてください。
2. 情報を自動更新する場合は、「Auto-refresh」(自動更新)を呼び出す必要があります。
3. 「Refresh」(更新)をクリックして、MAC アドレステーブルを更新してください。

■パラメーターの説明

Navigating the MAC Table(MAC テーブルのナビゲート)

各ページには、MAC テーブルから最大 999 のエントリーが表示されます。デフォルトは 10 で、「entries per page」(ページあたりのエントリー数)の入力フィールドで選択されています。最初にアクセスすると、Web ページには MAC テーブルの先頭から最初の 10 エントリーが表示されます。最初に表示されるのは、VLAN ID が最も小さく、MAC テーブルで見つかった MAC アドレスが最も小さいものです。

Type(タイプ):

エントリーがスタティックエントリーであるか、ダイナミックエントリーであるか(802.1x、DMS)を示します。

VLAN:

エントリーの VLAN ID です。

MAC Address（MAC アドレス）:
エントリーの MAC アドレスです。

Port Members（ポートメンバー）:
エントリーのメンバーであるポートです。

■ボタン

Auto-refresh（自動更新）:
画面を自動的に更新する場合は、このチェックボックスを ON にしてください。自動更新は 3 秒間隔で行われます。

Refresh（更新）:
クリックするとページを更新します。

First Page（最初のページ）:
リストを更新し、最初のページに戻ります。

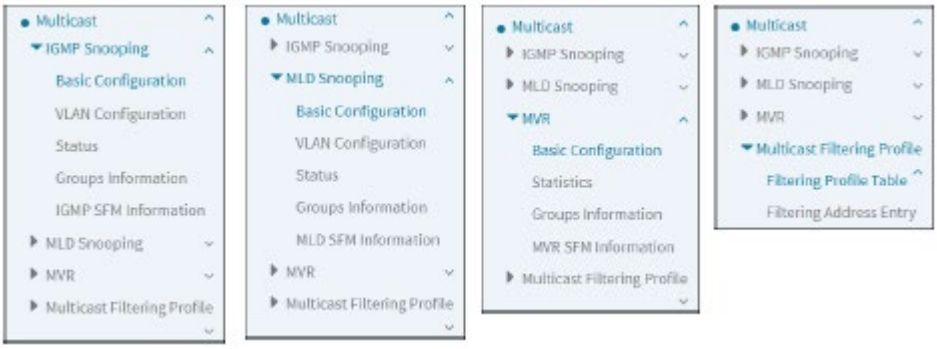
Next Page（次のページ）:
リストを更新し、次のページに進みます。

注意:	00-40-C7-73-01-29 ： スイッチの MAC アドレス（IPv4 用）
	33-33-00-00-00-01 ： 宛先 MAC（IPv6 ルーター通知用）（IPv6RA.JPG 参照）
	33-33-00-00-00-02 ： 宛先 MAC（IPv6 ルーター要請用）（IPv6RS.JPG 参照）
	33-33-FF-73-01-29 ： 宛先 MAC（IPv6 ネイバー要請用）（IPv6DAD.JPG 参照）
	33-33-FF-A8-01-01 ： スイッチの MAC アドレス（IPv6 グローバル IP 用）
	FF-FF-FF-FF-FF-FF ： ブロードキャスト用

第 10 章
マルチキャスト

概要

メニューとサブメニューを以下に示します。



IGMP スヌーピング

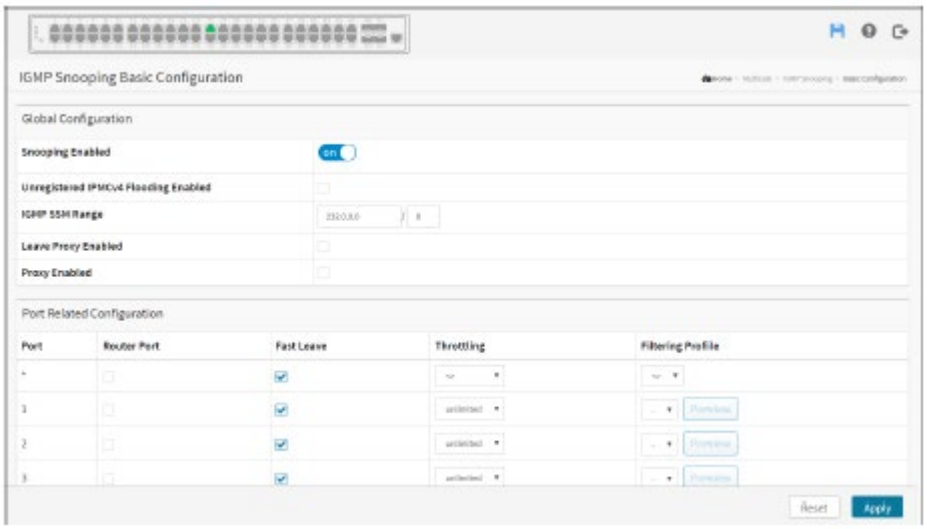
この機能は、マルチキャストグループを確立してマルチキャストパケットをメンバーポートに転送するために使用され、本質的には、IP マルチキャストパケットがネットワーク上で実行されている間、帯域幅の浪費を回避します。これは、IGMP または IGMP スヌーピングをサポートしていないスイッチは、ブロードキャストパケットからマルチキャストパケットを識別できないため、すべてをブロードキャストパケットとしてしか扱うことができないからです。IGMP スヌーピングを使用しない場合、マルチキャストパケット転送機能は単純で、ブロードキャストパケットと違いはありません。

IP マルチキャストのルーター/スイッチと IP マルチキャストホスト間で交換されるパケットのタイプであるクエリ、レポート、およびリーブ機能を備えた IGMP スヌーピングをサポートするスイッチは、メンバー（ポート）が IP マルチキャスト宛先アドレスに参加または脱退したときに、マルチキャストテーブルの情報を更新できます。この機能を使用すると、スイッチは IP マルチキャストパケットを受信すると、以前に指定された IP マルチキャストグループに参加していたメンバーにパケットを転送します。

ユーザーが事前に構築されていないマルチキャストグループにマルチキャストパケットを送信した場合、パケットは IGMP スヌーピングによって破棄されます。IGMP モードでは、スイッチは IGMP プロキシまたはスヌーピングを有効にする IGMP 機能を発行できます。スイッチは、ツリーのルートに近いルートに接続します。このインターフェースはアップストリームインターフェースです。アップストリームインターフェース上のルーターは IGMP を実行している必要があります。この画面では、現在の PoE ポート設定をチェックして設定し、すべての PoE 供給ワット数を表示することができます。

基本設定

このセクションでは、ツリーのルートに近いルーターに接続するスイッチの基本的な IGMP スヌーピングを設定する方法について説明します。このインターフェースはアップストリームインターフェースです。アップストリームインターフェース上のルーターは IGMP を実行している必要があります。



Web インターフェース

Web インターフェースで IGMP スヌーピングを設定するには:

1. 「Multicast」(マルチキャスト) ＞ 「IGMP Snooping」(IGMP スヌーピング) ＞ 「Basic Configuration」(基本設定)をクリックしてください。
2. どのグローバル設定を有効または無効にするかを選択してください。
3. ルーターポートにしたいポートを呼び出すか、高速脱退機能を有効/無効にしてください。
4. スクロールして、スロットリングとフィルタリングプロファイルを設定してください。
5. 「Apply」(適用)をクリックして設定を保存してください。
6. 設定を取り消す場合は、「Reset」(リセット)ボタンをクリックする必要があります。そうすると、以前に保存した値へと戻ります。

■パラメーターの説明

Global Configuration(グローバル設定)

Snooping Enabled(スヌーピング有効):

グローバル IGMP スヌーピングを有効にします。

Unregistered IPMCv4 Flooding enabled(未登録の IPMCv4 フラッディング有効):

未登録の IPMCv4 トラフィックフラッディングを有効にします。登録されていない IPMCv4 トラフィック

は、いわゆる不明なマルチキャストです。
選択すると、登録されていないマルチキャストストリームは通常のパケットと同様に転送されます。選択を解除すると、そのようなストリームは破棄されます。

IGMP SSM Range（IGMP SSM 範囲）：
SSM（Source-Specific Multicast）範囲では、SSM 対応ホストおよびルーターがアドレス範囲内のグループの SSM サービスモデルを実行できます。形式：（IP アドレス/サブマスク）

Leave Proxy Enabled：（プロキシを有効のままにする）：
IGMP Leave プロキシを有効にします。この機能は、ルーター側への不要な Leave メッセージの転送を回避するために使用できます。

Proxy Enabled（プロキシ有効）：
IGMP プロキシを有効にします。この機能は、ルーター側への不要な Join および Leave メッセージの転送を回避するために使用できます。

Port Related Configuration（ポート関連の設定）
Port（ポート）：
スイッチの物理ポートインデックスが表示されます。

Router Port（ルーターポート）：
ルーターポートとして機能するポートを指定してください。ルーターポートは、レイヤ 3 マルチキャストデバイスまたは IGMP クエリアに向かうイーサネットスイッチ上のポートです。
アグリゲーション・メンバーポートがルーターポートとして選択された場合、アグリゲーション全体がルーターポートとして機能します。

Fast Leave（高速脱退）：
ポートで高速脱退を有効にします。

Throttling（スロットリング）：
スイッチポートが所属できるマルチキャストグループの数を制限するには、有効にします。

Profile（プロファイル）：
このポートのプロファイルを選択してください。クリックすると、選択したプロファイルに関連付けられているルールを一覧表示する画面がプレビューされます。

■ボタン

Apply（適用）：

クリックすると、変更内容を保存します。

Reset（リセット）：

クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

VLAN の設定

ここでは、IGMP スヌーピング機能に統合された VLAN 設定プロセスについて説明します。各設定画面には、VLAN テーブルから最大 99 個のエントリーが表示されます。デフォルトは 20 で、「entries per page」（ページあたりのエントリー数）の入力フィールドで選択されています。最初にアクセスすると、Web ページには、VLAN テーブルの先頭から最初の 20 エントリーが表示されます。最初に表示されるのは、VLAN テーブルで見つかった VLAN ID が最も小さいものです。VLAN 入力フィールドを使用すると、ユーザーは VLAN テーブルで開始点を選択できます。ボタンをクリックすると、表示されているテーブルが、そのテーブルまたは次に近い VLAN テーブル一致から更新されます。

Web インターフェース

Web インターフェースで IGMP スヌーピング VLAN を設定するには：

1. 「Multicast」（マルチキャスト） ＞ 「IGMP Snooping」（IGMP スヌーピング） ＞ 「VLAN Configuration」（VLAN の設定）をクリックしてください。
2. クリックして、新しい IGMP VLAN を追加してください。
3. 「Apply」（適用）をクリックして設定を保存してください。
4. 設定を取り消す場合は、「Reset」（リセット）ボタンをクリックする必要があります。そうすると、

以前に保存した値へと戻ります。

■パラメーターの説明

Start from VLAN（VLAN から開始）：
ここをクリックすると、「VLAN」入力フィールドから、表示されているテーブルを更新します。

Delete（削除）：
チェックを入れると、エントリーを削除します。指定したエントリーは、次回の保存時に削除されます。

VLAN ID：
エントリーの VLAN ID が表示されます。

Snooping Enabled（スヌーピング有効）：
VLAN 単位の IGMP スヌーピングを有効にします。最大 32 の VLAN のみを選択できます。

IGMP Querier（IGMP クエリア）：
VLAN で IGMP クエリアの選択に参加できるようにします。IGMP 非クエリアとして機能させるには、これを無効にしてください。

Compatibility（互換性）：
ホストとルーターは、ネットワーク内のホストとルーターで動作する IGMP のバージョンに応じて適切なアクションを実行することで、互換性を維持します。許可される選択は、「IGMP-Auto」、「Forced IGMPv1」、「Forced IGMPv2」、「Forced IGMPv3」で、デフォルトの互換性値は「IGMP-Auto」です。

RV：
信頼性変数です。信頼性変数は、ネットワーク上で予想されるパケット損失の調整を可能にします。指定できる範囲は 1～255 です。デフォルトの信頼性変数の値は 2 です。

QI(sec)（QI（秒））：
クエリ送信間隔です。クエリ送信間隔は、クエリアによって送信される一般クエリ間の間隔です。指定できる範囲は 1～31744 秒です。デフォルトのクエリ間隔は 125 秒です。

QRI(0.1 sec)（QRI（0.1 秒））：
クエリ応答間隔です。定期的な一般クエリに挿入される最大レスポンスコードの計算に使用され

る最大応答時間です。指定できる範囲は 10 分の 1 秒で 0～31744 になります。デフォルトのクエリ応答間隔は 10 分の 1 秒（10 秒）で 100 になります。

LLQI (0.1 sec)（LLQI（0.1 秒））:
最後のメンバークエリ間隔です。「Last Member Query Time」（最終メンバークエリ時間）は、「Last Member Query Interval」（最終メンバークエリ間隔）に「Last Member Query Count」（最終メンバークエリカウント）を乗算した時間値です。指定できる範囲は 0～31744 です（10 分の 1 秒）。デフォルトの最終メンバークエリ間隔は 10 分の 1 秒（1 秒）です。

URI(sec)（URI（秒））:
非送信請求レポート間隔です。非送信請求レポート間隔は、グループ内のホストのメンバーシップで最初のレポートを繰り返す間隔の時間です。指定できる範囲は 0～31744 秒です。既定の非送信請求レポート間隔は 1 秒です。

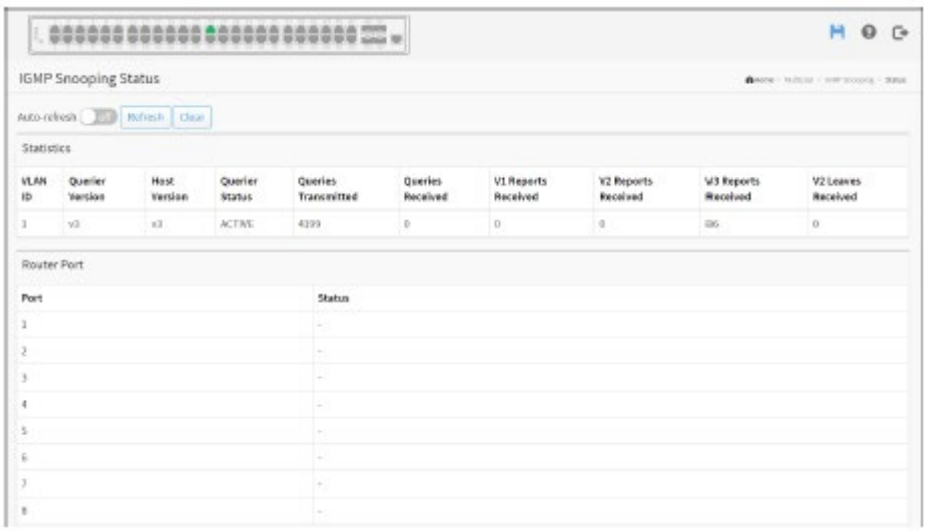
■ボタン

Apply（適用）:
クリックすると、変更内容を保存します。

Reset（リセット）:
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

状態

IGMP スヌーピング設定が完了したら、スイッチに IGMP スヌーピングの状態を表示させることができます。このセクションでは、IGMP スヌーピングの状態の詳細を表示するかどうかを切り替えることができます。



Web インターフェース

Web インターフェースで IGMP スヌーピングの状態を表示するには：

1. 「Multicast」（マルチキャスト） ＞ 「IGMP Snooping」（IGMP スヌーピング） ＞ 「Status」（状態）をクリックしてください。
2. 情報を自動更新する場合は、「Auto-refresh」（自動更新）を呼び出す必要があります。
3. 「Refresh」（更新）をクリックして、IGMP スヌーピングの状態を更新してください。

■パラメーターの説明

Statistic（統計）

VLAN ID：

エントリーの VLAN ID です。

Querier Version（クエリアバージョン）：

現在使用中のクエリアのバージョンです。

Host Version（ホストバージョン）：

現在動作しているホストのバージョンです。

Querier Status（クエリアの状態）：
クエリアの状態が「ACTIVE」（アクティブ）または「IDLE」（アイドル）であることを示します。「DISABLE」（無効）は、特定のインターフェースが管理上無効であることを示します。

Queries Transmitted（送信したクエリ）：
送信したクエリの数です。

Queries Received（受信したクエリ）：
受信したクエリの数です。

V1 Reports Received（V1 受信レポート）：
受信した V1 レポートの数です。

V2 Reports Received（V2 受信レポート）：
受信した V2 レポートの数です。

V3 Reports Received（V3 受信レポート）：
受信した V3 レポートの数です。

V2 Leaves Received（受信した V2 Leave）：
受信した V2 Leave の数です。

Router Port（ルーターポート）
ルーターポートとして機能するポートを表示します。ルーターポートは、レイヤ 3 マルチキャストデバイスまたは IGMP クエリアに向かうイーサネットスイッチ上のポートです。「Static」（スタティック）は、特定のポートがルーターポートとして設定されていることを示します。「Dynamic」（ダイナミック）は、特定のポートがルーターポートであることを学習したことを示します。どちらも、特定のポートが設定されているか、ルーターポートとして認識されていることを示します。

Port（ポート）：
スイッチのポート番号です。

Status（状態）：
特定のポートがルーターポートであるかどうかを示します。

■ボタン

Auto-refresh（自動更新）:
画面を自動的に更新する場合は、このチェックボックスをONにしてください。自動更新は3秒間隔で行われます。

Refresh（更新）:
クリックするとページを更新します。

Clear（消去）:
クリックすると、画面の内容をクリアします。

グループ情報

IGMP スヌーピング機能の設定が完了したら、スイッチに IGMP スヌーピンググループ情報を表示させることができます。IGMP グループテーブルのエントリーは、この画面に表示されます。IGMP グループテーブルは、最初に VLAN ID でソートされ、次にグループでソートされます。これにより、現在表示されているテーブルの最後のエントリーが、次のルックアップのベースとして使用されます。最後に達すると、表示されたテーブルに「これ以上エントリーはありません」というテキストが表示されます。このような場合は、ボタンを使用して、最初からやり直してください。

Web インターフェース

Web インターフェースに IGMP スヌーピングのグループ情報を表示するには:

1. 「Multicast」(マルチキャスト) ＞ 「IGMP Snooping」(IGMP スヌーピング) ＞ 「Group Information」(グループ情報)をクリックしてください。
2. 1 ページに表示するエントリーの数を指定してください。
3. 情報を自動更新する場合は、「Auto-refresh」(自動更新)を呼び出す必要があります。
4. 「Refresh」(更新)をクリックして、IGMP スヌーピンググループ情報のエントリーを更新してください。
5. 画面を変更する場合は、「First Page」(最初のページ)や「Next Page」(次のページ)をクリックしてください。

■パラメーターの説明

Navigating the IGMP Group Table (IGMP グループテーブルのナビゲート)

各ページには、IGMP グループテーブルから最大 99 のエントリーが表示されます。デフォルトは 20 で、「entries per page」(ページあたりのエントリー数)の入力フィールドで選択されています。最初にアクセスすると、IGMP グループテーブルの先頭から最初の 20 エントリーが Web ページに表示されます。

「Start from VLAN」(VLAN から開始)および「Group」(グループ)入力フィールドを使用すると、ユーザーは IGMP グループテーブルで開始点を選択できます。「Refresh」(更新)ボタンをクリックすると、表示されているテーブルが更新されます。これは、そのテーブルから、または次に一致する IGMP グループテーブルに最も近いテーブルから始まります。さらに、2 つの入力フィールドは、「Refresh」(更新)ボタンをクリックすると、最初に表示されたエントリーの値を想定し、同じ開始アドレスで継続的にリフレッシュできるようにします。

「Next Page」(次のページ)では、現在表示されているテーブルの最後のエントリーが次の参照のベースとして使用されます。最後に達すると、表示されたテーブルに「これ以上エントリーはありません」というテキストが表示されます。このような場合には、「First Page」(最初のページ)ボタンを使用して、最初からやり直してください。

Show entries (エントリーの表示) :

表示する項目の数を選択できます。

VLAN ID:

グループの VLAN ID です。

Groups (グループ) :

表示されているグループのグループアドレスです。

Port Members（ポートメンバー）：
このグループの配下にあるポートです。

■ボタン

Auto-refresh（自動更新）：
画面を自動的に更新する場合は、このチェックボックスをONにしてください。自動更新は3秒間隔で行われます。

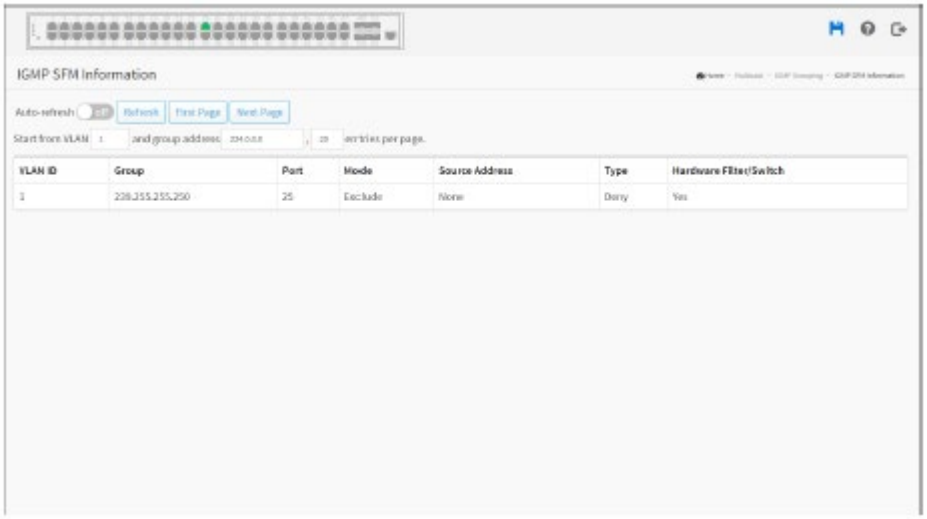
Refresh（更新）：
クリックするとページを更新します。

First Page（最初のページ）：
リストを更新し、最初のページに戻ります。

Next Page（次のページ）：
リストを更新し、次のページに進みます。

IGMP SFM 情報

IGMP SFM 情報テーブルのエントリーは、この画面に表示されます。IGMP SFM（Source-Filtered Multicast）情報テーブルには、SSM（Source-Specific Multicast）情報も含まれています。このテーブルは、最初に VLAN ID でソートされ、次にグループでソートされ、次にポートでソートされます。異なる送信元アドレスが同じグループに属している場合は、単一のエントリーとして扱われます。



Web インターフェース

Web インターフェースで IGMP SFM 情報を表示するには:

1. 「Multicast」(マルチキャスト) ＞ 「IGMP Snooping」(IGMP スヌーピング) ＞ 「IGMP SFM Information」(IGMP SFM 情報)をクリックしてください。
2. 情報を自動更新する場合は、「Auto-refresh」(自動更新)を呼び出す必要があります。
3. 「Refresh」(更新)をクリックして、IGMP SFM 情報のエントリーを更新してください。
4. 画面を変更する場合は、「First Page」(最初のページ)や「Next Page」(次のページ)をクリックしてください。

■パラメーターの説明

Navigating the IGMP SFM Information Table(IGMP SFM 情報テーブルのナビゲート)

各ページには、IGMP SFM 情報テーブルから最大 99 個のエントリーが表示されます。デフォルトは 20 で、「entries per page」(ページあたりのエントリー数)の入力フィールドで選択されています。最初にアクセスすると、IGMP SFM 情報テーブルの先頭から最初の 20 エントリーが表示されます。

「Start from VLAN」(VLAN から開始)および「Group」(グループ)入力フィールドを使用すると、IGMP SFM 情報テーブルで開始点を選択できます。「Refresh」(更新)ボタンをクリックすると、表示されているテーブルが更新されます。これは、そのテーブルから、または次に一致する IGMP SFM 情報テーブルに最も近いテーブルから始まります。さらに、(「Refresh」(更新)ボタンをクリックすると)2 つの入力フィールドは、最初に表示されたエントリーの値を想定し、同じ開始アドレスで継続的に更新することができます。

「Next Page」(次のページ)では、現在表示されているテーブルの最後のエントリーが次の参照のベースとして使用されます。最後に達すると、表示されたテーブルに「これ以上エントリーはありません」というテキストが表示されます。このような場合には、「First Page」(最初のページ)ボタ

ンを使用して、最初からやり直してください。

Show entries（エントリーの表示）：
表示する項目の数を選択できます。

VLAN ID：
グループの VLAN ID です。

Groups（グループ）：
表示されているグループのグループアドレスです。

Port（ポート）：
スイッチのポート番号です。

Mode（モード）：
（VLAN ID、ポート番号、グループアドレス）単位で維持されるフィルタリングモードを示します。「Include」（含む）または「Exclude」（除く）のいずれかになります。

Source Address（送信元アドレス）：
送信元の IP アドレスです。現在、フィルタリングする IP ソースアドレスの合計数は 128 に制限されています。

Type（タイプ）：
タイプを示します。「Allow」（許可）または「Deny」（拒否）のいずれかになります。

Hardware Filter/Switch（ハードウェア・フィルター/スイッチ）：
送信元の IPv4 アドレスから特定のグループアドレス宛てのデータプレーンをチップで処理できるかどうかを示します。

■ボタン

Auto-refresh（自動更新）：
画面を自動的に更新する場合は、このチェックボックスを ON にしてください。自動更新は 3 秒間隔で行われます。

Refresh（更新）：
クリックするとページを更新します。

First Page（最初のページ）：
リストを更新し、最初のページに戻ります。

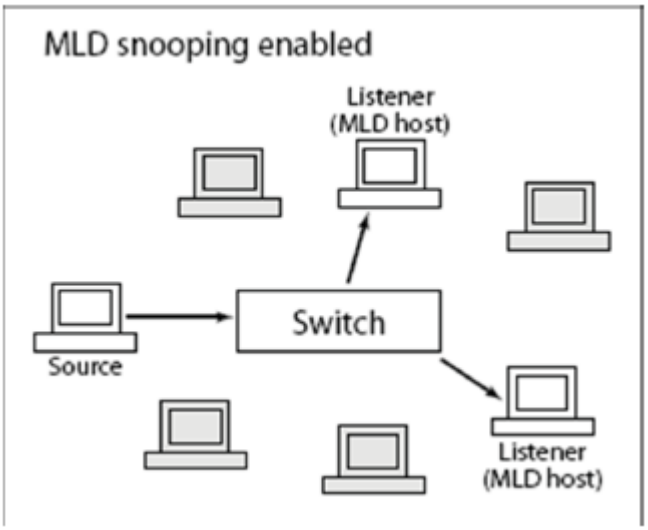
Next Page（次のページ）：
リストを更新し、次のページに進みます。

MLD スヌーピング

興味深いことに、IPv6 マルチキャストトラフィックの送信元として機能するネットワークノードは、MLD スヌーピングの間接的な参加者に過ぎず、マルチキャストトラフィックを提供するだけで、MLD はそれと対話しません。(ただし、デスクトップ会議のようなアプリケーションでは、ネットワークノードはソースホストと MLD ホストの両方として機能しますが、MLD は MLD ホストとしての役割のみでそのノードと相互作用します。)

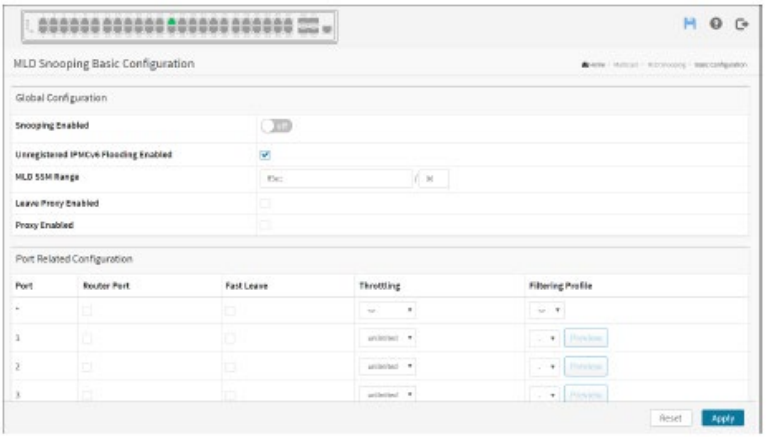
送信元ノードは、マルチキャストアドレスにパケットを送信することによってマルチキャストトラフィックを作成します。IPv6 では、最初の 8 ビットが設定されたアドレス(つまり、アドレスの最初の 2 文字として「FF」)はマルチキャストアドレスであり、そのようなアドレスをリッスンするすべてのノードがそのアドレスに送信されたトラフィックを受信します。送信元および宛先システムで実行されているアプリケーションソフトウェアは、どのマルチキャストアドレスを使用するかを決定するために連携します。(これは、MLD ではなく、アプリケーションソフトウェアの機能であることに注意してください。)

VLAN で MLD スヌーピングを有効にすると、スイッチは不要なマルチキャストトラフィックを最小限に抑えるように動作します。スイッチは、特定のマルチキャストアドレス宛てのマルチキャストトラフィックを受信すると、そのトラフィックを、そのアドレスの MLD ホストを持つ VLAN 上のポートにのみ転送します。MLD ホストを持たない VLAN 上のポートのトラフィックを破棄します。



基本設定

このセクションでは、MLD スヌーピングの基本設定とパラメーターの設定方法について説明します。



Web インターフェース

Web インターフェースで MLD スヌーピングの設定を行うには:

1. 「Multicast」(マルチキャスト) ＞ 「MLD Snooping」(MLD スヌーピング) ＞ 「Basic Configuration」(基本設定)をクリックしてください。
2. グローバル設定パラメーターを有効または無効にしてください。
3. ルーターポートと高速脱退に参加するポートを選択してください。
4. スクロールして、無制限または 1～10 のスロットリングモードを選択してください。
5. スクロールして、プロファイルを設定してください。
6. 「Apply」(適用)をクリックして設定を保存してください。
7. 設定を取り消す場合は、「Reset」(リセット)ボタンをクリックする必要があります。そうすると、以前に保存した値へと戻ります。

■パラメーターの説明

Global Configuration(グローバル設定)

Snooping Enabled(スヌーピング有効):

グローバル MLD スヌーピングを有効にします。

Unregistered IPMCv6 Flooding enabled(未登録の IPMCv6 フラッディング有効):

未登録の IPMCv6 トラフィックのフラッディングを有効にします。MLD スヌーピングが有効な場合にのみ、フラッディング制御が有効になります。

MLD スヌーピングが無効になっている場合、この設定にかかわらず、未登録の IPMCv6 トラフィックフラッディングは常にアクティブになります。

MLD SSM Range（MLD SSM 範囲）：
SSM（Source-Specific Multicast）範囲では、SSM 対応ホストおよびルーターがアドレス（IPv6 アドレスを使用）範囲内のグループに対して SSM サービスモデルを実行できます。

Leave Proxy Enabled（プロキシを有効のままにする）：
MLD Leave プロキシを有効にします。この機能は、ルーター側への不要な Leave メッセージの転送を回避するために使用できます。

Proxy Enabled（プロキシ有効）：
MLD プロキシを有効にします。この機能は、ルーター側への不要な Join および Leave メッセージの転送を回避するために使用できます。

Port Related Configuration（ポート関連の設定）
Router Port（ルーターポート）：
ルーターポートとして機能するポートを指定してください。ルーターポートは、レイヤ 3 マルチキャストデバイスまたは MLD クエリアに向かうイーサネットスイッチ上のポートです。
アグリゲーション・メンバーポートがルーターポートとして選択された場合、アグリゲーション全体がルーターポートとして機能します。

Fast Leave（高速脱退）：
ポートで高速脱退を有効にします。

Throttling（スロットリング）：
スイッチポートが所属できるマルチキャストグループの数を制限するには、有効にします。

Filtering Profile（フィルタリングプロファイル）：
マルチキャストフィルタリングプロファイルで編集する場合は、プロファイルを選択できます。

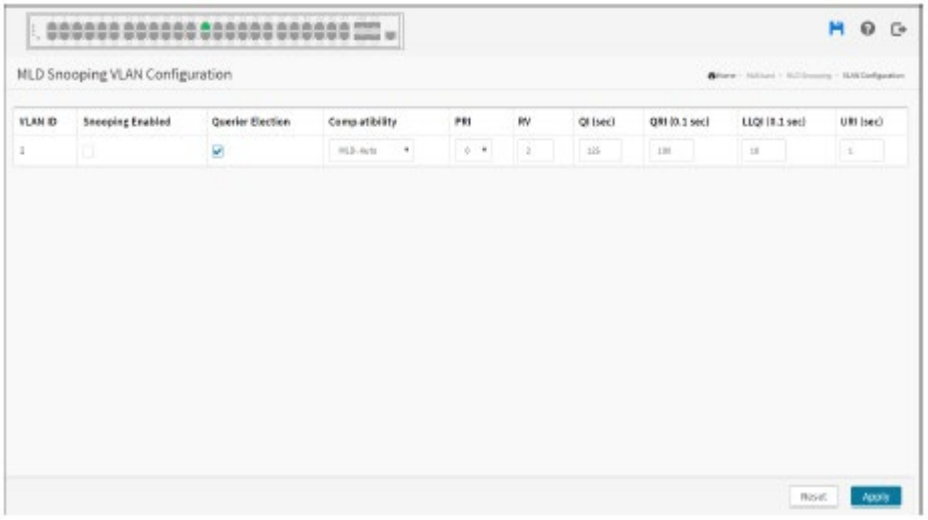
■ボタン
Apply（適用）：
クリックすると、変更内容を保存します。

Reset（リセット）：
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

VLAN の設定

VLAN で MLD スヌーピングを有効にすると、スイッチは不要なマルチキャストトラフィックを最小限に抑えるように動作します。スイッチは、特定のマルチキャストアドレス宛てのマルチキャストトラフィックを受信すると、そのトラフィックを、そのアドレスの MLD ホストを持つ VLAN 上のポートにのみ転送します。MLD ホストを持たない VLAN 上のポートのトラフィックを破棄します。

現在表示されているエントリーの最後のエントリーを、次のルックアップのベースとして使用します。最後に達すると、表示されたテーブルに「これ以上エントリーはありません」というテキストが表示されます。このような場合は、ボタンを使用して、最初からやり直してください。



Web インターフェース

Web インターフェースで MLD スヌーピング VLAN を設定するには:

1. 「Multicast」(マルチキャスト) ＞ 「MLD Snooping」(MLD スヌーピング) ＞ 「VLAN Configuration」(VLAN の設定)をクリックしてください。
2. 「Add New MLD VLAN」(新規 MLD VLAN の追加)をクリックしてください。
3. ページごとのエントリーで VLAN ID を指定してください。

■パラメーターの説明

Delete(削除):

チェックを入れると、エントリーを削除します。指定したエントリーは、次回の保存時に削除されます。

VLAN ID：
エントリーの VLAN ID が表示されます。

Snooping Enabled（スヌーピング有効）：
VLAN 単位の MLD スヌーピングを有効にします。最大 32 の VLAN のみを選択できます。

MLD Querier（MLD クエリア）：
VLAN で MLD クエリアの選択に参加できるようにします。MLD 非クエリアとして機能させるには、これを無効にしてください。

Compatibility（互換性）：
ホストとルーターは、ネットワーク内のホストとルーターで動作する IGMP のバージョンに応じて適切なアクションを実行することで、互換性を維持します。許可される選択は、「IGMP-Auto」、「Forced IGMPv1」、「Forced IGMPv2」で、デフォルトの互換性値は「IGMP-Auto」です。

RV：
信頼性変数です。信頼性変数は、ネットワーク上で予想されるパケット損失の調整を可能にします。指定できる範囲は 1～255 です。デフォルトの信頼性変数の値は 2 です。

QI(sec)（QI（秒））：
クエリ送信間隔です。クエリ送信間隔は、クエリアによって送信される一般クエリ間の間隔です。指定できる範囲は 1～31744 秒です。デフォルトのクエリ間隔は 125 秒です。

QRI(0.1 sec)（QRI（0.1 秒））：
クエリ応答間隔です。定期的な一般クエリに挿入される最大レスポンスコードの計算に使用される最大応答時間です。指定できる範囲は 0～31744 です。デフォルトのクエリ応答間隔は、10 分の 1 秒（10 秒）で 100 です。

LLQI (LMQI for IGMP)（LLQI（IGMP の LMQI））：
最後のメンバークエリ間隔です。「Last Member Query Time」（最終メンバークエリ時間）は、「Last Member Query Interval」（最終メンバークエリ間隔）に「Last Member Query Count」（最終メンバークエリカウント）を乗算した時間値です。指定できる範囲は 0～31744 です（10 分の 1 秒）。デフォルトの最終メンバークエリ間隔は 10 分の 1 秒（1 秒）です。

URI(sec)（URI（秒））：

非送信請求レポート間隔です。非送信請求レポート間隔は、グループ内のホストのメンバーシップで最初のレポートを繰り返す間隔の時間です。指定できる範囲は 0～31744 秒です。既定の非送信請求レポート間隔は 1 秒です。

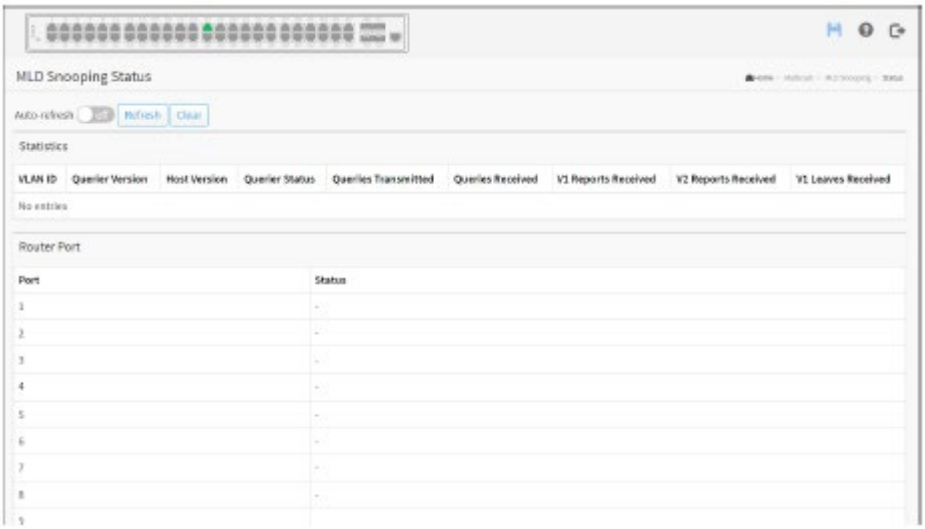
■ボタン

Apply（適用）：
クリックすると、変更内容を保存します。

Reset（リセット）：
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

状態

このセクションでは、MLD スヌーピングを完了するタイミングと、MLD スヌーピングの状態および詳細情報を表示する方法について説明します。これは、MLD スヌーピングの状態に関する詳細情報を確認するのに役立ちます。



Web インターフェース

Web インターフェースに MLD スヌーピングの状態を表示するには:

1. 「Multicast」(マルチキャスト) ＞ 「MLD Snooping」(MLD スヌーピング) ＞ 「Status」(状態) をクリックしてください。
2. 情報を自動更新する場合は、「Auto-refresh」(自動更新)を呼び出す必要があります。
3. MLD スヌーピングの状態に関する情報を更新するには、「Refresh」(更新)をクリックしてください。

■パラメーターの説明

VLAN ID:

エントリーの VLAN ID です。

Querier Version(クエリアバージョン):

現在使用中のクエリアのバージョンです。

Host Version(ホストバージョン):

現在動作しているホストのバージョンです。

Querier Status（クエリアの状態）：
クエリアの状態が「ACTIVE」（アクティブ）または「IDLE」（アイドル）であることを示します。「DISABLE」（無効）は、特定のインターフェースが管理上無効であることを示します。

Queries Transmitted（送信したクエリ）：
送信したクエリの数です。

Queries Received（受信したクエリ）：
受信したクエリの数です。

V1 Reports Received（V1 受信レポート）：
受信した V1 レポートの数です。

V2 Reports Received（V2 受信レポート）：
受信した V2 レポートの数です。

V1 Leaves Received（受信した V1 Leave）：
受信した V1 Leave の数です。

Router Port（ルーターポート）
ルーターポートとして機能するポートを表示します。ルーターポートは、レイヤ 3 マルチキャストデバイスまたは IGMP クエリアに向かうイーサネットスイッチ上のポートです。「Static」（スタティック）は、特定のポートがルーターポートとして設定されていることを示します。「Dynamic」（ダイナミック）は、特定のポートがルーターポートであることを学習したことを示します。どちらも、特定のポートが設定されているか、ルーターポートとして認識されていることを示します。

Port（ポート）：
スイッチのポート番号です。

■ボタン

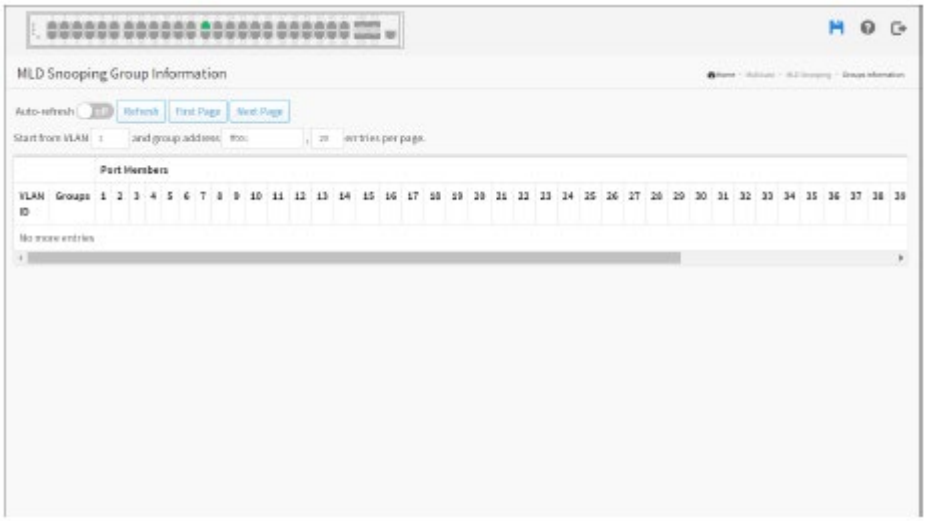
Auto-refresh（自動更新）：
画面を自動的に更新する場合は、このチェックボックスを ON にしてください。自動更新は 3 秒間隔で行われます。

Refresh（更新）:
クリックするとページを更新します。

Clear（消去）:
クリックすると、画面の内容をクリアします。

グループ情報

MLD グループテーブルのエントリーは、この画面に表示されます。MLD グループテーブルは、最初に VLAN ID でソートされ、次にグループでソートされます。



Web インターフェース
MLD スヌーピンググループの情報を Web インターフェースに表示するには:

1. 「Multicast」（マルチキャスト） ＞ 「MLD Snooping」（MLD スヌーピング） ＞ 「Group Information」（グループ情報）をクリックしてください。
2. 情報を自動更新する場合は、「Auto-refresh」（自動更新）を呼び出す必要があります。
3. 「Refresh」（更新）をクリックして、MLD スヌーピングのグループ情報のエントリーを更新してください。
4. 画面を変更する場合は、「First Page」（最初のページ）や「Next Page」（次のページ）をクリックしてください。

■パラメーターの説明

Navigating the MLD Group Table（MLD グループテーブルのナビゲート）

各ページには、MLD グループテーブルから最大 99 個のエントリーが表示されます。デフォルトは 20 で、「entries per page」（ページあたりのエントリー数）の入力フィールドで選択されています。最初にアクセスすると、MLD グループテーブルの先頭から最初の 20 エントリーが Web ページに表示されます。

「Start from VLAN」（VLAN から開始）および「Group」（グループ）入力フィールドを使用すると、MLD グループテーブルで開始点を選択できます。「Refresh」（更新）ボタンをクリックすると、表示されているテーブルが更新されます。これは、そのテーブルから、または次に一致する MLD グループテーブルに最も近いテーブルから始まります。さらに、（「Refresh」（更新）ボタンをクリックすると）2 つの入力フィールドは、最初に表示されたエントリーの値を想定し、同じ開始アドレスで継続的に更新することができます。

「Next Page」（次のページ）では、現在表示されているテーブルの最後のエントリーが次の参照のベースとして使用されます。最後に達すると、表示されたテーブルに「これ以上エントリーはありません」というテキストが表示されます。このような場合には、「First Page」（最初のページ）ボタンを使用して、最初からやり直してください。

VLAN ID：
グループの VLAN ID です。

Groups（グループ）：
表示されているグループのグループアドレスです。

Port Members（ポートメンバー）：
このグループの配下にあるポートです。

Show entries（エントリーの表示）：
表示する項目の数を選択できます。

■ボタン

Auto-refresh（自動更新）：
画面を自動的に更新する場合は、このチェックボックスを ON にしてください。自動更新は 3 秒間

隔で行われます。

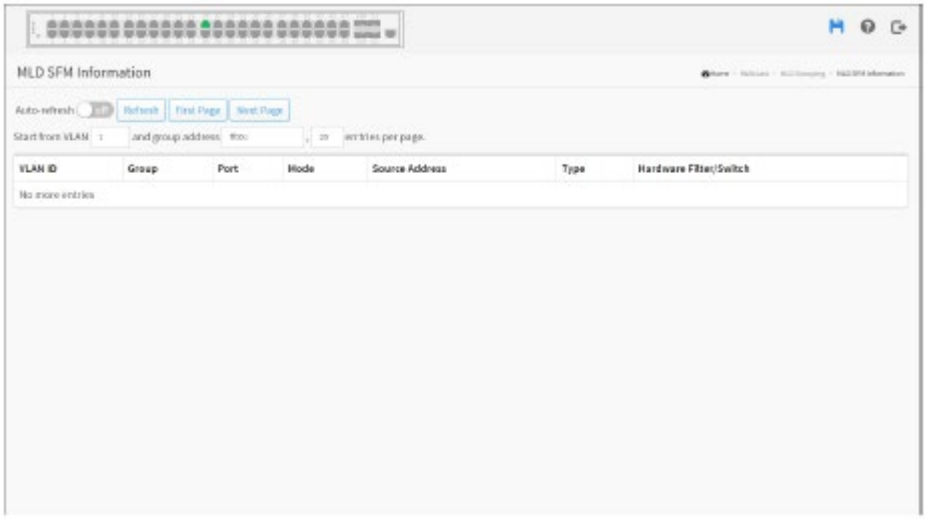
Refresh（更新）：
クリックするとページを更新します。

First Page（最初のページ）：
リストを更新し、最初のページに戻ります。

Next Page（次のページ）：
リストを更新し、次のページに進みます。

MLD SFM 情報

MLD SFM 情報テーブルのエントリーは、この画面に表示されます。MLD SFM（Source-Filtered Multicast）情報テーブルには、SSM（Source-Specific Multicast）情報も含まれています。このテーブルは、最初に VLAN ID でソートされ、次にグループでソートされ、次にポートでソートされます。異なる送信元アドレスが同じグループに属している場合は、単一のエントリーとして扱われます。



Web インターフェース

MLD SFM 情報を Web インターフェースに表示するには：

1. 「Multicast」（マルチキャスト） ＞ 「MLD Snooping」（MLD スヌーピング） ＞ 「MLD SFM Information」（MLD SFM 情報）をクリックしてください。
2. 情報を自動更新する場合は、「Auto-refresh」（自動更新）を呼び出す必要があります。
3. 「Refresh」（更新）をクリックして、MLD SFM 情報のエントリーの最新の内容を表示してください。

4. 画面を変更する場合は、「First Page」(最初のページ)や「Next Page」(次のページ)をクリックしてください。

■パラメーターの説明

Navigating the MLD SFM Information Table(MLD SFM 情報テーブルのナビゲート)

各ページには、MLD SFM 情報テーブルから最大 99 のエントリーが表示されます。デフォルトは 20 で、「entries per page」(ページあたりのエントリー数)の入力フィールドで選択されています。最初にアクセスすると、MLD SFM 情報テーブルの先頭から最初の 20 エントリーが表示されます。

「Start from VLAN」(VLAN から開始)および「Group」(グループ)入力フィールドを使用すると、MLD SFM 情報テーブルで開始点を選択できます。

「Refresh」(更新)ボタンをクリックすると、表示されているテーブルが、そのテーブルまたは次の MLD SFM情報テーブルの一致したものから更新されます。さらに、(「Refresh」(更新)ボタンをクリックすると)2 つの入力フィールドは、最初に表示されたエントリーの値を想定し、同じ開始アドレスで継続的に更新することができます。

「Next Page」(次のページ)では、現在表示されているテーブルの最後のエントリーが次の参照のベースとして使用されます。最後に達すると、表示されたテーブルに「これ以上エントリーはありません」というテキストが表示されます。このような場合には、「First Page」(最初のページ)ボタンを使用して、最初からやり直してください。

VLAN ID:
グループの VLAN ID です。

Group(グループ):
IP マルチキャストグループのアドレスです。

Port(ポート):
スイッチのポート番号です。

Mode(モード):
(VLAN ID、ポート番号、グループアドレス)単位で維持されるフィルタリングモードを示します。

Source Address(送信元アドレス):
送信元の IP アドレスです。現在、フィルタリングする IP ソースアドレスの合計数は 128 に制限されています。

Type(タイプ):

タイプを示します。「Allow」（許可）または「Deny」（拒否）のいずれかになります。

Hardware Filter/Switch（ハードウェア・フィルター/スイッチ）：
送信元の IPv6 アドレスから特定のグループアドレス宛てのデータプレーンをチップで処理できるかどうかを示します。

■ボタン

Auto-refresh（自動更新）：
画面を自動的に更新する場合は、このチェックボックスを ON にしてください。自動更新は 3 秒間隔で行われます。

Refresh（更新）：
クリックするとページを更新します。

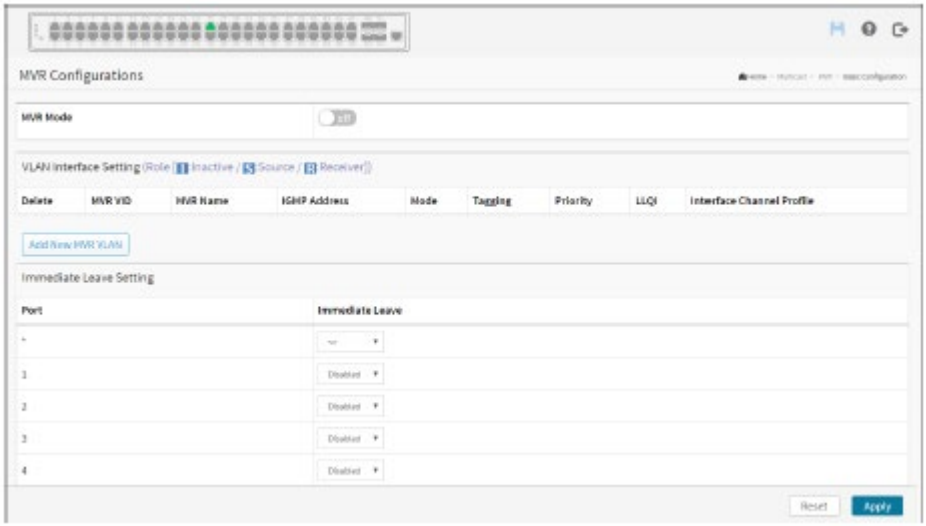
First Page（最初のページ）：
リストを更新し、最初のページに戻ります。

Next Page（次のページ）：
リストを更新し、次のページに進みます。

MVR

MVR 機能は、マルチキャスト VLAN でのマルチキャストトラフィック転送を有効にします。マルチキャスト・テレビジョン・アプリケーションにおいて、PC またはセットトップボックスを備えたテレビは、マルチキャストストリームを受信することができます。そして、複数のセットトップボックスまたは PC は、MVR レシーバーポートとして設定されたスイッチポートである 1 つのサブスクライバーポートに接続できます。加入者がチャネルを選択すると、セットトップボックスまたは PC はスイッチ A に IGMP Join メッセージを送信して、適切なマルチキャストに参加します。マルチキャスト VLAN との間でマルチキャストデータを送受信するアップリンクポートは、MVR 送信元ポートと呼ばれます。

基本設定



Web インターフェース

Web インターフェースで MVR を設定するには:

1. 「Multicast」(マルチキャスト) ＞ 「MVR」 ＞ 「Basic Configuration」(基本設定)をクリックしてください。
2. MVR モードをスクロールして有効または無効にしてください。また、スクロールしてすべてのパラメーターを設定してください。
3. 「Add New MVR VLAN」(新規 MVR VLAN の追加)をクリックしてください。
4. 「MVR VID」、「MVR Name」(MVR 名)、「IGMP Address」(IGMP アドレス)、「Mode」(モード)、「Tagging」(タギング)、「Priority」(優先度)、「LLQI」、「Interface Channel Profile」(インターフェースチャネルプロファイル)を指定してください。

5. 即時脱退を行うポートをクリックして選択してください。
6. 「Apply」(適用)をクリックして設定を保存してください。
7. 設定を取り消す場合は、「Reset」(リセット)ボタンをクリックする必要があります。そうすると、以前に保存した値へと戻ります。

■パラメーターの説明

MVR Mode(MVR モード):
グローバル MVR を有効/無効にします。未登録フラッディング制御は、IGMP/MLD スヌーピングの現在の設定に依存します。MVR グループテーブルがいっぱいになった場合は、未登録フラッディング制御を有効にすることを推奨します。

MVR VID:
マルチキャスト VLAN ID を指定します。

注意: MVR 送信元ポートを管理 VLAN ポートと重複させることは推奨しません。

MVR Name(MVR 名):
MVR 名は、特定の MVR VLAN の名前を示す任意の属性です。MVR VLAN 名の文字列の最大長は 32 です。MVR VLAN 名には、アルファベットまたは数字のみを含めることができます。MVR VLAN 名は、既存の MVR VLAN エントリーに対して編集することも、新しいエントリーに追加することもできます。

IGMP Address(IGMP アドレス):
IGMP 制御フレームの IP ヘッダーで使用される送信元アドレスとして IPv4 アドレスを定義します。
デフォルトの IGMP アドレスは設定されていません(0.0.0.0)。
IGMP アドレスが設定されていない場合、システムはこの VLAN に関連付けられた IP インターフェースの IPv4 管理アドレスを使用します。
IPv4 管理アドレスが設定されていない場合、システムは最初に使用可能な IPv4 管理アドレスを使用します。
それ以外の場合、システムは事前定義された値を使用します。デフォルトでは、この値は 192.0.2.1 になります。

Mode(モード):
MVR の動作モードを指定します。ダイナミックモードでは、MVR は送信元ポートでダイナミック MVR メンバーシップレポートを許可します。互換モードでは、MVR メンバーシップレポートは送信元ポートで禁止されます。デフォルトは「Dynamic」(ダイナミック)モードです。

Tagging（タギング）：
交差したIGMP/MLD制御フレームを「タグ無し」、または「MVR VIDタグ付き」のどちらとして送信するかを指定します。デフォルトは「tagged」（タグ付き）です。

Priority（優先度）：
交差したIGMP/MLD制御フレームを優先的に送信する方法を指定します。デフォルトの優先順位は0です。

LLQI：
マルチキャストグループメンバーシップからポートを削除する前に、レシーバーポートでIGMP/MLDレポートメンバーシップを待機する最大時間を定義します。値は1/10秒単位です。指定できる範囲は0～31744です。デフォルトのLLQIは5/10または1/2秒です。

Interface Channel Profile（インターフェース・チャネル・プロファイル）：
MVR VLANが作成されたら、プロファイルを選択して、特定のMVR VLANの対応するマルチキャストチャネル設定を展開します。フィルタリングプロファイルテーブルで確立されたファイルです。

Port Role（ポートのロール）：
指定されたMVR VLANのMVRポートを次のいずれかのロールとして設定します。

Inactive（非アクティブ）：指定されたポートはMVR操作に参加しません。

Source（送信元）：マルチキャストデータを送信元ポートとして受信および送信するアップリンクポートを設定します。サブスクライバーは送信元ポートに直接接続できません。

Receiver（レシーバー）：ポートがサブスクライバーポートであり、マルチキャストデータのみを受信する必要がある場合は、ポートをレシーバーポートとして設定します。IGMP/MLD メッセージを発行してマルチキャストグループのメンバーにならない限り、データを受信しません。

注意： MVR送信元ポートを管理VLANポートと重複させることは推奨しません。

ロールシンボルをクリックして、ポートのロールを選択し、設定を切り替えてください。I は「Inactive」（非アクティブ）、Sは「Source」（送信元）、Rは「Receiver」（レシーバー）を、それぞれ示します。デフォルトのロールは「Inactive」（非アクティブ）です。

Immediate Leave（即時脱退）：
ポートで即時脱退を有効にします。

■ボタン

Add New MVR VLAN（新規 MVR VLAN の追加）：
クリックすると、新しい MVR VLAN を追加します。「MVR VID」、「MVR Name」（MVR 名）、「IGMP Address」（IGMP アドレス）、「Mode」（モード）、「Tagging」（タギング）、「Priority」（優先度）、「LLQI」、「Interface Channel Profile」（インターフェースチャネルプロファイル）を指定してください。そうしたら、「Apply」（適用）をクリックしてください。

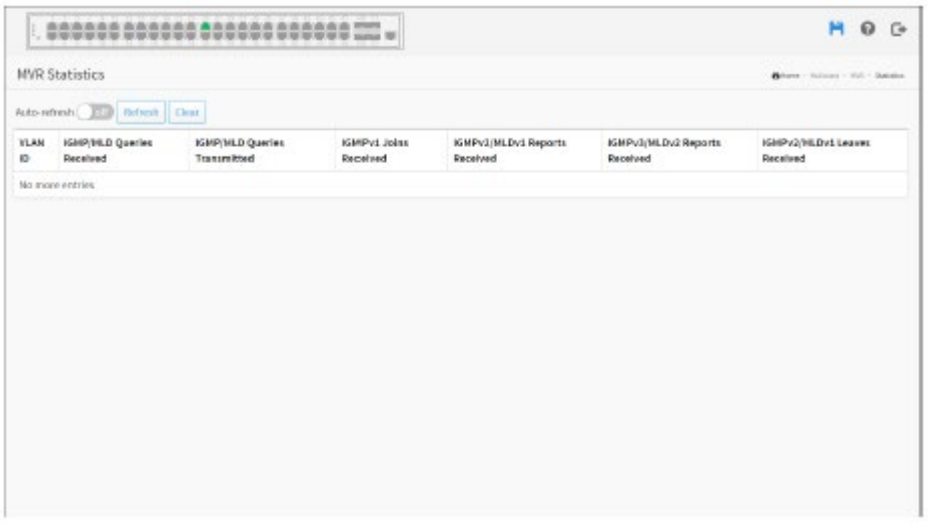
Delete（削除）：
チェックを入れると、エントリーを削除します。指定したエントリーは、次回の保存時に削除されます。

Apply（適用）：
クリックすると、変更内容を保存します。

Reset（リセット）：
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

統計

このセクションでは、スイッチに MVR を設定すると、MVR 詳細統計情報が表示されます。ここでは詳細な MVR 統計情報を提供します。



Web インターフェース
Web インターフェースで MVR 統計情報を表示するには：

1. 「Multicast」(マルチキャスト) ＞ 「MVR」 ＞ 「Statistics」(統計)をクリックしてください。
2. 情報を自動更新する場合は、「Auto-refresh」(自動更新)を呼び出す必要があります。
3. 「Refresh」(更新)をクリックして、最新の MVR 統計情報のエントリーを表示してください。

■パラメーターの説明

VLAN ID:
マルチキャストの VLAN ID です。

IGMP/MLD Queries Received(受信した IGMP/MLD クエリ):
IGMP および MLD の受信クエリの数です。

IGMP/MLD Queries Transmitted(送信した IGMP/MLD クエリ):
IGMP および MLD の送信済クエリの数です。

IGMPv1 Joins Received(受信した IGMPv1 Join):
受信した IGMPv1 Join の数です。

IGMPv2/MLDv1 Report's Received(受信した IGMPv2/MLDv1 レポート):
受信した IGMPv2Join と MLDv1 レポートの数です。

IGMPv3/MLDv2 Report's Received(受信した IGMPv3/MLDv2 レポート):
受信した IGMPv3Join と MLDv2 レポートの数です。

IGMPv2/MLDv1 Leave's Received(受信した IGMPv2/MLDv1 Leave):
受信した IGMPv2Leave と MLDv1Done の数です。

■ボタン

Auto-refresh(自動更新):
画面を自動的に更新する場合は、このチェックボックスを ON にしてください。自動更新は 3 秒間隔で行われます。

Refresh(更新):
クリックするとページを更新します。

Clear（消去）:
クリックすると、すべての統計カウンターがクリアされます。

MVR グループ情報

このセクションでは、ユーザーがスイッチの MVR グループの詳細情報を表示できるようにする方法について説明します。この画面には、MVR グループテーブルのエントリーが表示されます。MVR グループテーブルは、最初に VLAN ID でソートされ、次にグループでソートされます。

Web インターフェース
MVR グループの情報を Web インターフェースに表示するには:

1. 「Multicast」（マルチキャスト） ＞ 「MVR」 ＞ 「Groups Information」（グループ情報）をクリックしてください。
2. 情報を自動更新する場合は、「Auto-refresh」（自動更新）を呼び出す必要があります。
3. 「Refresh」（更新）をクリックして、MVR グループ情報のエントリーを更新してください。
4. 画面を変更する場合は、「First Page」（最初のページ）や「Next Page」（次のページ）をクリックしてください。

■パラメーターの説明

Navigating the MVR Channels (Groups) Information Table（MVR チャネル（グループ）情報テーブルのナビゲート）

各ページには、MVR グループテーブルから最大 99 のエントリーが表示されます。デフォルトは 20 で、「entries per page」（ページあたりのエントリー数）の入力フィールドで選択されています。最初にアクセスすると、MVR チャネル（グループ）情報テーブルの先頭から最初の 20 エントリーが表示

されます。
「Start from VLAN」(VLAN から開始)および「Group」(グループ)入力フィールドを使用すると、MVR チャネル(グループ)情報テーブルで開始点を選択できます。「Refresh」(更新)ボタンをクリックすると、表示されているテーブルが更新されます。これは、そのテーブルから、または最も近い次のMVRチャネル(グループ)情報テーブルの一致から始まります。さらに、(「Refresh」(更新)ボタンをクリックすると)2 つの入力フィールドは、最初に表示されたエントリーの値を想定し、同じ開始アドレスで継続的に更新することができます。
「Next Page」(次のページ)では、現在表示されているテーブルの最後のエントリーが次の参照のベースとして使用されます。最後に達すると、表示されたテーブルに「これ以上エントリーはありません」というテキストが表示されます。このような場合には、「First Page」(最初のページ)ボタンを使用して、最初からやり直してください。

MVR Channels (Groups) Information Table Columns(MVR チャネル(グループ)情報テーブルの列)

Show entries(エントリーの表示):
表示する項目の数を選択できます。

VLAN ID:
グループの VLAN ID です。

Groups(グループ):
表示されているグループのグループ ID です。

Port Members(ポートメンバー):
このグループの配下にあるポートです。

■ボタン

Auto-refresh(自動更新):
画面を自動的に更新する場合は、このチェックボックスをONにしてください。自動更新は3秒間隔で行われます。

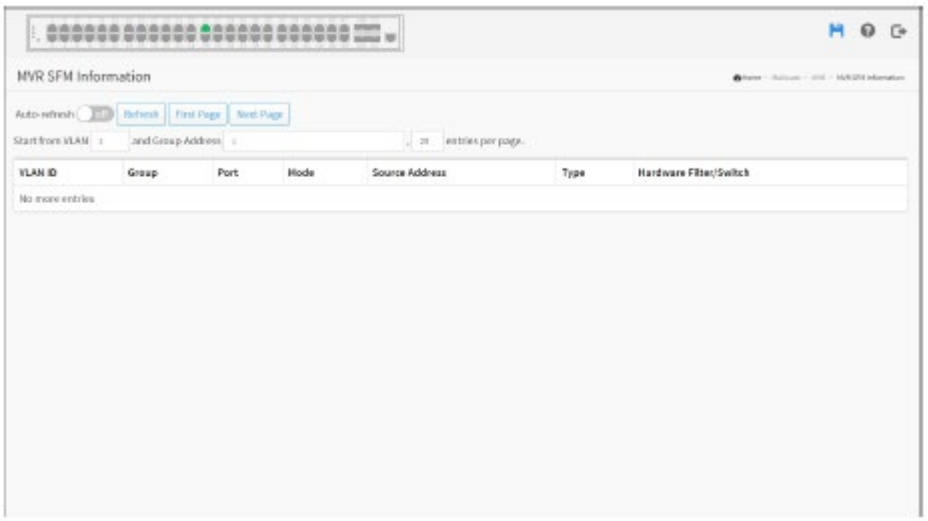
Refresh(更新):
クリックするとページを更新します。

First Page（最初のページ）:
リストを更新し、最初のページに戻ります。

Next Page（次のページ）:
リストを更新し、次のページに進みます。

MVR SFM 情報

MVR SFM（Source-Filtered Multicast）情報テーブルには、SSM（Source-Specific Multicast）情報も含まれています。このテーブルは、最初に VLAN ID でソートされ、次にグループでソートされ、次にポートでソートされます。異なる送信元アドレスが同じグループに属している場合は、単一のエントリーとして扱われます。



Web インターフェース
Web インターフェースで MVR SFM 情報を表示するには:

1. 「Multicast」（マルチキャスト） ＞ 「MVR」 ＞ 「MVR SFM Information」（MVR SFM 情報）をクリックしてください。
2. 情報を自動更新する場合は、「Auto-refresh」（自動更新）を呼び出す必要があります。
3. 「Refresh」（更新）をクリックして、MVR グループ情報のエントリーを更新します。
4. 画面を変更する場合は、「First Page」（最初のページ）や「Next Page」（次のページ）をクリックしてください。

■パラメーターの説明

Navigating the MVR SFM Information Table（MVR SFM 情報テーブルのナビゲート）

各ページには、MVR SFM 情報テーブルから最大 99 のエントリーが表示されます。デフォルトは 20 で、「entries per page」（ページあたりのエントリー数）の入力フィールドで選択されています。初めてアクセスしたときは、MVR SFM 情報テーブルの最初から最初の 20 エントリーが表示されます。「Start from VLAN」（VLAN から開始）および「Group Address」（グループアドレス）入力フィールドを使用すると、MVR SFM 情報テーブルの開始点を選択できます。「Refresh」（更新）ボタンをクリックすると、表示されているテーブルが、そのテーブルから、または次に一致する MVR SFM 情報テーブルに最も近いテーブルから更新されます。さらに、（「Refresh」（更新）ボタンをクリックすると）2 つの入力フィールドが表示されます。最初に表示されたエントリーの値を想定して、同じ開始アドレスで継続的に更新することができます。「Next Page」（次のページ）では、現在表示されているテーブルの最後のエントリーが次の参照のベースとして使用されます。最後に達すると、表示されたテーブルに「これ以上エントリーはありません」というテキストが表示されます。このような場合には、「First Page」（最初のページ）ボタンを使用して、最初からやり直してください。

MVR SFM Information Table Columns（MVR SFM 情報テーブルの列）

Show entries（エントリーの表示）：
表示する項目の数を選択できます。

VLAN ID：
グループの VLAN ID です。

Group（グループ）：
IP マルチキャストグループのアドレスです。

Port（ポート）：
スイッチのポート番号です。

Mode（モード）：
(VLAN ID、ポート番号、グループアドレス)単位で維持されるフィルタリングモードを示します。
「Include」（含む）または「Exclude」（除く）のいずれかになります。

Source Address（送信元アドレス）：

送信元の IP アドレスです。現在、フィルタリングする IP 送信元アドレスの合計数は 128 に制限されています。送信元のフィルタリングアドレスが存在しない場合、「None」(なし)というテキストが「Source Address」(送信元アドレス)フィールドに表示されます。

Type(タイプ):
タイプを示します。「Allow」(許可)または「Deny」(拒否)のいずれかになります。

Hardware Filter/Switch(ハードウェア・フィルター/スイッチ):
送信元 IPv4/IPv6 アドレスから特定のグループアドレス宛てのデータプレーンをチップで処理できるかどうかを示します。

■ボタン

Auto-refresh(自動更新):
画面を自動的に更新する場合は、このチェックボックスを ON にしてください。自動更新は 3 秒間隔で行われます。

Refresh(更新):
クリックするとページを更新します。

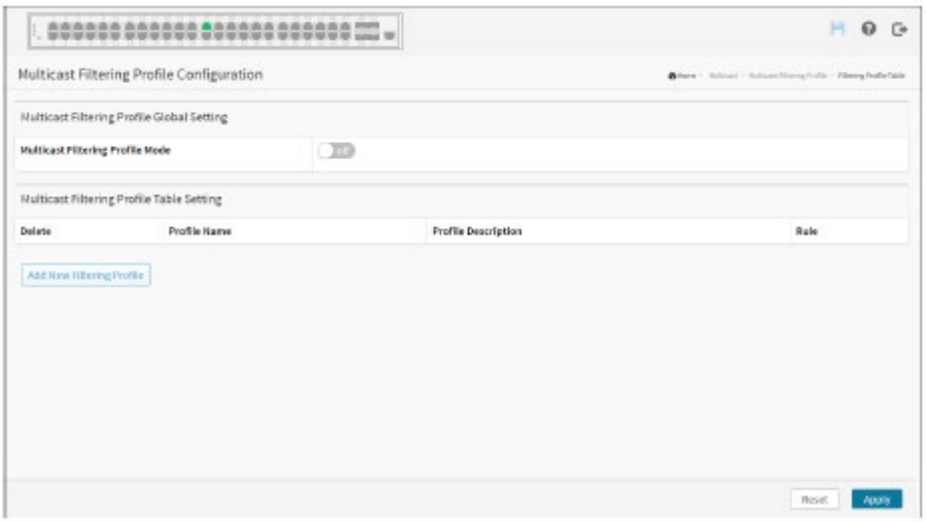
First Page(最初のページ):
リストを更新し、最初のページに戻ります。

Next Page(次のページ):
リストを更新し、次のページに進みます。

マルチキャストフィルタリングプロファイル

プロファイルテーブルのフィルタリング

IPMC プロファイルは、IP マルチキャストストリームにアクセス制御を導入するために使用されます。最大 64 個のプロファイルを作成し、それぞれに最大 128 個の対応するルールを作成できます。



Web インターフェース

Web インターフェースで IPMC プロファイル設定を定義するには:

1. 「Multicast」(マルチキャスト) ＞ 「Multicast Filtering Profile」(マルチキャスト・フィルタリング・プロファイル) ＞ 「Filtering Profile Table」(プロファイルテーブルのフィルタリング)をクリックしてください。
2. マルチキャスト・フィルタリング・プロファイルモードをスクロールして、有効または無効にしてください。
3. 「Add New Filtering Profile」(新規フィルタリングプロファイルの追加)をクリックしてください。
4. プロファイル名、プロファイルの説明、およびルールを指定してください。
5. 「Apply」(適用)をクリックして設定を保存してください。
6. 設定を取り消す場合は、「Reset」(リセット)ボタンをクリックする必要があります。そうすると、以前に保存した値へと戻ります。

■パラメーターの説明

Multicast Filtering Profile Mode（マルチキャストフィルタリングプロファイルモード）：
マルチキャストフィルタリングプロファイルを有効/無効にします。システムは、グローバルプロファイルモードが有効になっている場合にのみ、プロファイル設定に基づいてフィルタリングを開始します。

Profile Name（プロファイル名）：
プロファイルテーブルのインデックス作成に使用される名前です。各エントリーには、最大 16 文字の英字と数字で構成される一意の名前があります。

Profile Description（プロファイルの説明）：
プロファイルに関する追加の説明です。最大 64 文字の英字と数字で構成されています。
説明の一部として、空白文字やスペース文字は使用できません。説明文を区切るには、「_」または「-」を使用してください。

Rule（ルール）：
プロファイルを作成したら、「Edit」（編集）ボタンをクリックして、指定したプロファイルのルール設定画面に入ってください。「Preview」（プレビュー）ボタンをクリックすると、指定したプロファイルの概要が表示されます。次のボタンを使用して、指定したプロファイルのルールを管理またはチェックできます。

Preview（プレビュー）：指定したプロファイルに関連付けられているルールをプレビューします。

Edit（編集）：指定したプロファイルに関連付けられているルールを調整します。

Profile Name & Index（プロファイル名＆インデックス）：
関連付ける指定されたプロファイルの名前です。この項目は編集できません。

Entry Name（エントリー名）：
このルールで使用されるアドレス範囲の指定に使用される名前です。

選択したボックスでは、既存のプロファイルアドレスエントリーのみが選択されます。ルール設定テーブルがコミットされている間は、この項目をなし(-)として選択することはできません。

Address Range(アドレス範囲):
選択したプロファイルエントリーが対応するアドレス範囲です。この項目は編集できず、選択したプロファイルエントリーに従って自動的に調整されます。

Action(アクション):
グループアドレスがルールのアドレス範囲と一致する Join/Report フレームを受信したときの学習アクションを示します。

Permit(許可):グループアドレスがルールで指定された範囲に一致すると、学習されます。
Deny(拒否):グループアドレスがルールで指定された範囲に一致すると、破棄されます。

Log(ログ):
グループアドレスがルールのアドレス範囲と一致する Join/Report フレームを受信したときのロギング設定を示します。

Enable(有効):ルールで指定された範囲に一致するグループアドレスの対応する情報がログに記録されます。
Disable(無効):ルールで指定された範囲に一致するグループアドレスの対応する情報はログに記録されません。

Rule Management Buttons(ルール管理ボタン):
次のボタンを使用して、ルールとそれに対応する優先度を管理できます。

 : ルールの現在のエントリーの前に新しいルールを挿入します。

 : ルールの現在のエントリーを削除します。

 : ルールの現在のエントリーをリスト内で上に移動します。

 : ルールの現在のエントリーをリスト内で下に移動します。

■パラメーターの説明

Add New Filtering Profile(新規フィルタリングプロファイルの追加):
クリックすると、新しい IPMC プロファイルを追加します。名前を指定し、新しいエントリーを設定してください。そうしたら、「Save」(保存)をクリックしてください。

Delete（削除）：
チェックを入れると、エントリーを削除します。指定したエントリーは、次回の保存時に削除されます。

Apply（適用）：
クリックすると、変更内容を保存します。

Reset（リセット）：
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

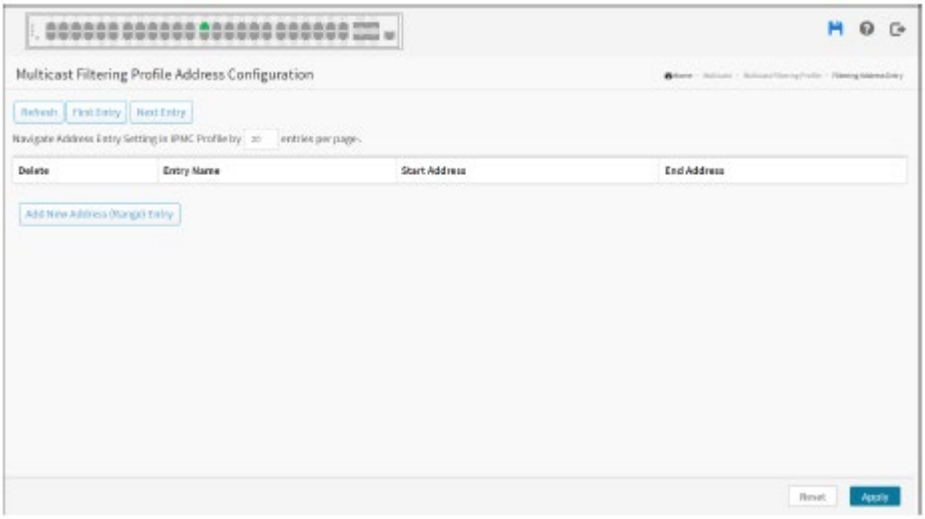
Add Last Rule（最後のルールの追加）：

クリックすると、特定のプロファイルのルールリストの端に新しいルールを追加します。アドレスエントリーを指定し、新しいエントリーを設定してください。そうしたら、「Apply」（適用）をクリックしてください。

アドレスエントリーのフィルタリング

この画面では、IPMC プロファイルで使用するアドレス範囲の設定を行います。

アドレスエントリーは、IPMC プロファイルに関連付けるアドレス範囲を指定するために使用されます。システムでは、最大 128 個のアドレスエントリーを作成できます。



Web インターフェース

Web インターフェースで IPMC プロファイルアドレスを設定するには:

1. 「Multicast」(マルチキャスト) ＞ 「Multicast Filtering Profile」(マルチキャストのフィルタリングプロファイル) ＞ 「Filtering Address Entry」(アドレスエントリーのフィルタリング)をクリックしてください。
2. 「Add New Address(Range)Entry」(新規アドレス(範囲)エントリーの追加)をクリックしてください。

3. 「Entry Name」(エントリー名)、「Start Address」(開始アドレス)、「End Address」(終了アドレス)を指定してください。
4. 「Apply」(適用)をクリックして設定を保存してください。
5. 設定を取り消す場合は、「Reset」(リセット)ボタンをクリックする必要があります。そうすると、以前に保存した値へと戻ります。

6. 「Refresh」（更新）をクリックして、アドレスエントリーを更新します。
7. エントリーを変更する場合は、「First Entry」（最初のエントリー）や「Next Entry」（次のエントリー）をクリックしてください。

■パラメーターの説明

Entry Name（エントリー名）：
アドレスエントリテーブルのインデックス作成に使用される名前です。
各エントリーには、最大 16 文字の英字と数字で構成される一意の名前があります。

Start Address（開始アドレス）：
アドレス範囲として使用される開始 IPv4/IPv6 マルチキャストグループアドレスです。

End Address（終了アドレス）：
アドレス範囲として使用される終了 IPv4/IPv6 マルチキャストグループアドレスです。

■ボタン

Add New Address (Range) Entry（新規アドレス（範囲）エントリーの追加）：
クリックすると、新しいアドレス範囲を追加します。名前を指定し、アドレスを設定してください。そうしたら、「Apply」（適用）をクリックしてください。

Delete（削除）：
チェックを入れると、エントリーを削除します。
指定したエントリーは、次回の保存時に削除されます。

Apply（適用）：
クリックすると、変更内容を保存します。

Reset（リセット）：
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

First Entry（最初のエントリー）：
IPMC プロファイルアドレス設定の最初のエントリーからテーブルを更新します。

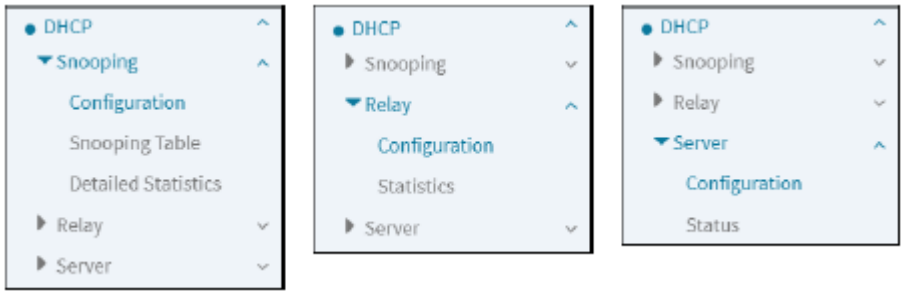
Next Entry（次のエントリー）：
現在表示されている最後のエントリーの後のエントリーから開始して、テーブルを更新します。

第 11 章
DHCP

概要

このセクションでは、スイッチの DHCP スヌーピングパラメーターの設定と表示について説明します。DHCP スヌーピングは、攻撃者が独自の DHCP サーバーをネットワークに追加できないようにすることができます。

メニューとサブメニューを以下に示します。

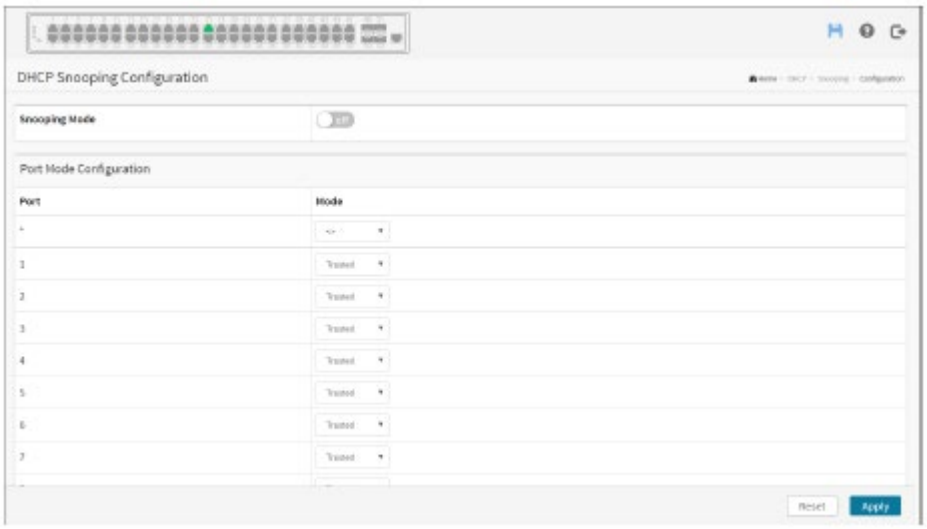


スヌーピング

設定

DHCP スヌーピングは、DHCP クライアントとサーバー間の正当な対話に偽の DHCP 応答パケットを挿入して介入しようとするときに、スイッチデバイスの信頼されていないポート上の侵入者をブロックするために使用されます。

このセクションでは、スイッチの DHCP スヌーピングパラメーターを設定する方法について説明します。DHCP スヌーピングは、攻撃者が独自の DHCP サーバーをネットワークに追加できないようにすることができます。



Web インターフェース

Web インターフェースで DHCP スヌーピングを設定するには:

1. 「DHCP」 > 「Snooping」(スヌーピング) > 「Configuration」(設定)をクリックしてください。
2. 「DHCP Snooping Configuration」(DHCP スヌーピングの設定)における「Mode」(モード)で「on」を選択してください。
3. 「Port」(ポート)の「Mode」(モード)の設定で、特定のポートに対して「Trusted」(信頼済み)を選択してください。
4. 「Apply」(適用)をクリックしてください。

■パラメーターの説明

Snooping Mode（スヌーピングモード）：

DHCP スヌーピングモードの操作を示します。使用可能なモードは次のとおりです。

on：DHCP スヌーピングモード動作を有効にします。DHCP スヌーピングモード操作が有効になっている場合、DHCP 要求メッセージは信頼できるポートに転送され、信頼できるポートからの応答パケットのみが許可されます。

off：DHCP スヌーピングモードの操作を無効にします。

Port Mode Configuration（ポートモードの設定）：

DHCP スヌーピングのポートモードを示します。使用可能なポートモードは次のとおりです。

Trusted（信頼済み）：DHCP メッセージの信頼できる送信元としてポートを設定します。信頼済みのポートは、DHCP パケットを正常に転送できます。

Untrusted（非信頼済み）：ポートを DHCP メッセージの信頼できない送信元として設定します。信頼されていないポートは、DHCP パケットを受信すると、パケットを破棄します。

■ボタン

Apply（適用）：

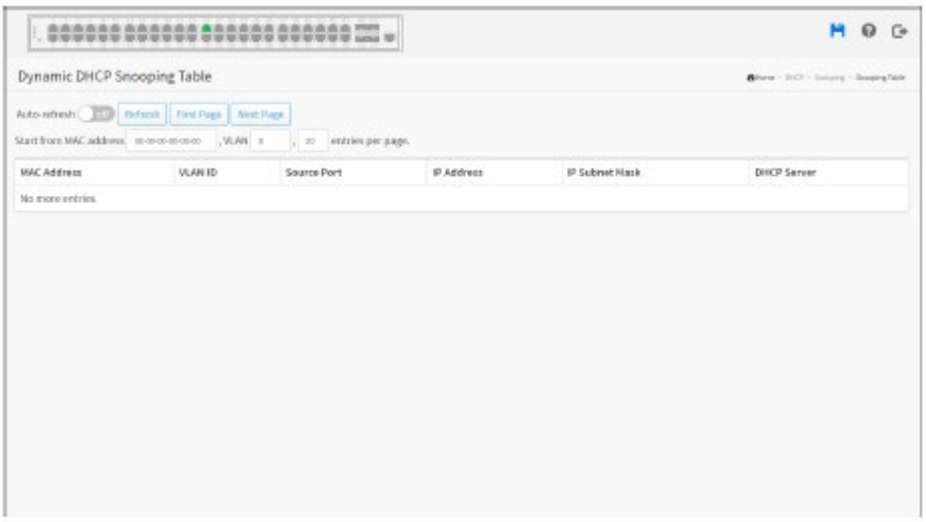
クリックすると、変更内容を保存します。

Reset（リセット）：

クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

スヌーピングテーブル

この画面には、DHCP スヌーピングモードが有効になった後に割り当てられたダイナミック IP アドレス情報が表示されます。DHCP サーバーからダイナミック IP アドレスを取得したすべての DHCP クライアントが、ローカル VLAN インターフェース IP アドレスを除き、このテーブルに一覧表示されます。この画面には、ダイナミック DHCP スヌーピングテーブルのエントリーが表示されます。



Web インターフェース

Web インターフェースで DHCP を監視するには:

1. 「DHCP」 ＞ 「Snooping」(スヌーピング) ＞ 「Snooping Table」(スヌーピングテーブル)をクリックしてください。
2. 情報を自動更新する場合は、「Auto-refresh」(自動更新)を呼び出す必要があります。
3. 「Refresh」(更新)をクリックして、スヌーピングテーブルのエントリーを更新してください。
4. 画面を変更する場合は、「First Page」(最初のページ)や「Next Page」(次のページ)をクリックしてください。

■パラメーターの説明

Show entries(エントリーの表示):

表示する項目の数を選択できます。

MAC Address(MAC アドレス):

エントリーのユーザーMAC アドレスです。

VLAN ID：
DHCP トラフィックが許可される VLAN の ID です。

Source Port（送信元ポート）：
エントリーを表示するスイッチのポート番号です。

IP Address（IP アドレス）：
エントリーのユーザーIP アドレスです。

IP Subnet Mask（IP サブネットマスク）：
エントリーのユーザーIP サブネットマスクです。

DHCP Server（DHCP サーバー）：
エントリーの DHCP サーバーアドレスです。

■ボタン

Auto-refresh（自動更新）：
画面を自動的に更新する場合は、このチェックボックスを ON にしてください。自動更新は 3 秒間隔で行われます。

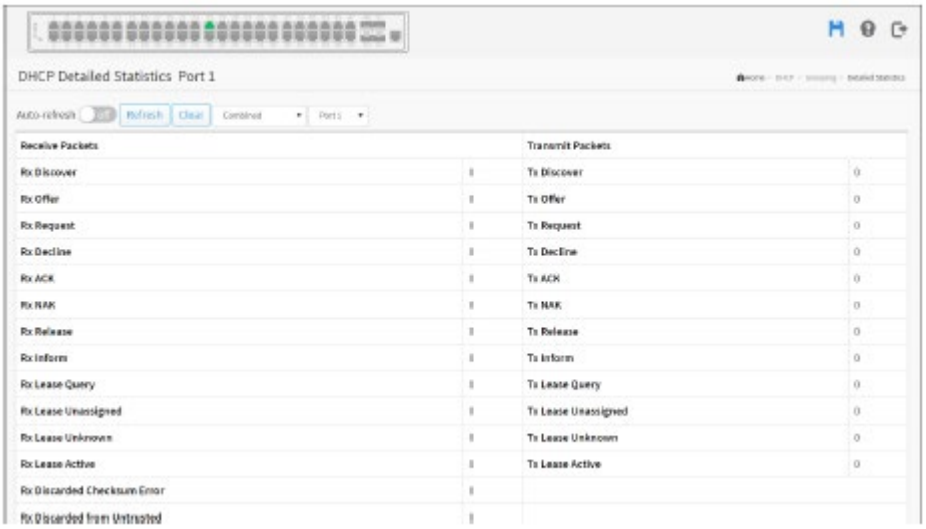
Refresh（更新）：
クリックするとページを更新します。

First Page（最初のページ）：
リストを更新し、最初のページに戻ります。

Next Page（次のページ）：
リストを更新し、次のページに進みます。

統計情報の詳細

この画面には、DHCP スヌーピングの統計情報が表示されます。着信 DHCP パケットが L3 転送メカニズムによって行われる場合、ポートごとの通常の転送 TX 統計は増加しません。また、特定のポートの統計情報は、異なる層の概要を収集するため、グローバル統計情報には有効にならない場合があります。



Web インターフェース

Web インターフェースに DHCP リレー統計を表示するには:

1. 「DHCP」 ＞ 「Snooping」(スヌーピング) ＞ 「Detailed Statistics」(詳細統計)をクリックしてください。
2. DHCP 統計の詳細を表示するポートを選択してください。
3. 情報を自動更新する場合は、「Auto-refresh」(自動更新)を呼び出す必要があります。
4. 「Refresh」(更新)をクリックして、DHCP 詳細統計のエントリーを最新表示します。

■パラメーターの説明

Server Statistics(サーバー統計)

Rx and Tx Discover(Rx および Tx ディスカバー):
受信および送信されたディスカバー(値 1 のオプション 53)のパケット数です。

Rx and Tx Offer(Rx および Tx オファー):
オファー(オプション 53、値 2)パケットの受信および送信数です。

Rx and Tx Request(Rx および Tx リクエスト):

受信および送信されたリクエスト（値 3 のオプション 53）のパケット数です。

Rx and Tx Decline（Rx および Tx 拒否）：
受信および送信された拒否パケット数（値 4 のオプション 53）です。

Rx and Tx ACK（Rx および Tx ACK）：
受信および送信された ACK（値 5 のオプション 53）のパケット数です。

Rx and Tx NAK（Rx および Tx NAK）：
受信および送信された NAK（値 6 のオプション 53）のパケット数です。

Rx and Tx Release（Rx および Tx リリース）：
受信および送信されたリリース（オプション 53、値 7）のパケット数です。

Rx and Tx Inform（Rx および Tx 通知）：
受信および送信された通知（オプション 53、値 8）のパケット数です。

Rx and Tx Lease Query（Rx および Tx Lease クエリ）：
受信および送信された Lease クエリ（値 10 のオプション 53）のパケット数です。

Rx and Tx Lease Unassigned（Rx および Tx Lease 未割り当て）：
未割り当ての Lease（値 11 のオプション 53）のパケットの受信および送信数です。

Rx and Tx Lease Unknown（Rx および Tx Lease 不明）：
受信および送信された Lease 不明（値が 12 のオプション 53）のパケット数です。

Rx and Tx Lease Active（Rx および Tx Lease アクティブ）：
受信および送信された Lease アクティブ（値 13 のオプション 53）なパケット数です。

Rx Discarded checksum error（破棄された Rx チェックサム・エラー）：
IP/UDP チェックサムがエラーである廃棄パケットの数です。

Rx Discarded from Untrusted（信頼されないポートから破棄された Rx）：
信頼されていないポートから廃棄されたパケット数です。

■ボタン

Auto-refresh（自動更新）:
画面を自動的に更新する場合は、このチェックボックスをONにしてください。自動更新は3秒間隔で行われます。

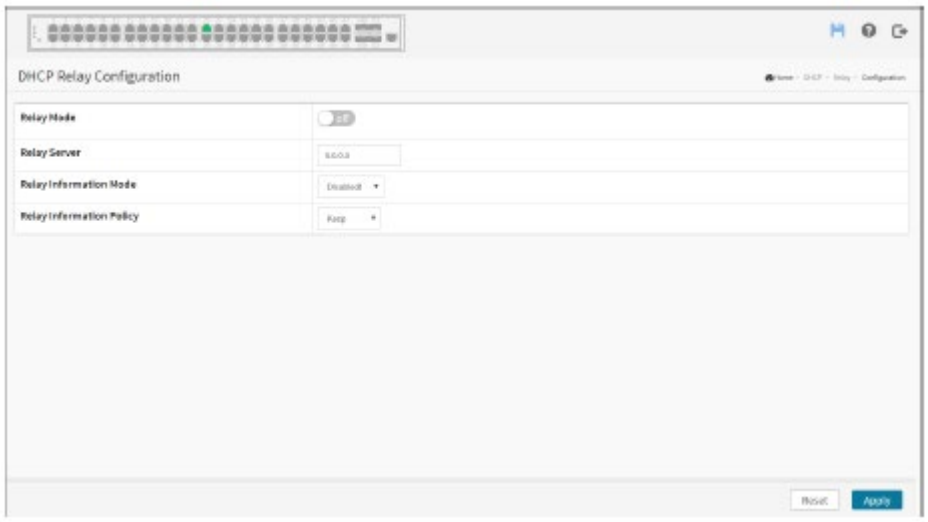
Refresh（更新）:
クリックするとページを更新します。

Port 1（ポート1）:
DHCP 詳細統計を表示するポートを選択してください。

リレー

設定

DHCP リレー・エージェントは、クライアントとサーバーが同じサブネットドメインに存在しない場合に、クライアントとサーバー間でDHCPメッセージを転送および転送するために使用されます。受信インターフェース IP アドレスは、DHCP パケットの GIADDR 項目に格納されます。DHCP サーバーは、GIADDR フィールドの値を使用して、割り当てられたサブネットを判別できます。このような状況では、VLAN インターフェースの IP アドレスと PVID（Port VLAN ID）のスイッチ設定が正しく行われていることを確認してください。



Web インターフェース

Web インターフェースで DHCP リレーを設定するには:

1. 「DHCP」 ＞ 「Relay」（リレー） ＞ 「Configuration」（設定）をクリックしてください。
2. 「Relay Mode」（リレーモード）、「Relay Server」（リレーサーバー）、「Relay Information Mode」（リレー情報モード）、「Relay Information Policy」（リレー情報ポリシー）を指定してください。
3. 「Apply」（適用）をクリックしてください。

■パラメーターの説明

Relay Mode（リレーモード）:

DHCP リレーモードの操作を示します。使用可能なモードは次のとおりです。

on：DHCP リレーモード動作を有効にします。DHCP リレーモードの操作が有効になっている場合、エージェントは、クライアントとサーバーが同じサブネットドメインに存在しないときに、ク

ライアントとサーバー間で DHCP メッセージを転送します。また、DHCP ブロードキャストメッセージは、セキュリティ上の考慮事項のためにフラッディングされません。

off:DHCP リレーモードの操作を禁止します。

Relay Server(リレーサーバー):

DHCP リレーサーバーの IP アドレスを示します。

Relay Information Mode(リレー情報モード):

DHCP リレー情報モードのオプションの操作を示します。オプション 82 の回路 ID 形式は「[*vlan_id*][*module_id*][*port_no*]」となります。最初の 4 文字は VLAN ID を表し、5 番目と 6 番目の文字はモジュール ID(スタンドアロンのデバイスでは常に 0、スタッカブルデバイスではスイッチ ID を表します)、最後の 2 文字はポート番号です。例えば、「00030108」は、VLAN ID3、スイッチ ID1、ポート番号 8 から DHCP メッセージを受信することを意味します。オプション 82 のリモート ID 値はスイッチの MAC アドレスと等しくなります。使用可能なモードは次のとおりです。

Enabled(有効):DHCP リレー情報モード動作を有効にします。DHCP リレー情報モードの動作が有効になっている場合、エージェントは DHCP サーバーに転送するときに特定の情報(オプション 82)を DHCP メッセージに挿入し、DHCP クライアントに転送するときに DHCP メッセージから削除します。これは、DHCP リレー動作モードが有効になっている場合にのみ機能します。

Disabled(無効):DHCP リレー情報モードの操作を禁止します。

Relay Information Policy(リレー情報ポリシー):

DHCP リレー情報オプションのポリシーを示します。DHCP リレー情報モードの動作が有効になっている場合、すでにリレー・エージェント情報が含まれている DHCP メッセージをエージェントが受信すると、ポリシーが適用されます。リレー情報モードが無効な場合、「Replace」(置換)ポリシーは無効です。考えられるポリシーは次のとおりです。

Replace(置換):すでにリレー情報が含まれている DHCP メッセージを受信した場合は、元のリレー情報を置き換えます。

Keep(保持):すでにリレー情報が含まれている DHCP メッセージを受信した場合は、元のリレー情報を保持します。

Drop(破棄):すでにリレー情報が含まれている DHCP メッセージを受信したら、パッケージを破棄します。

■ボタン

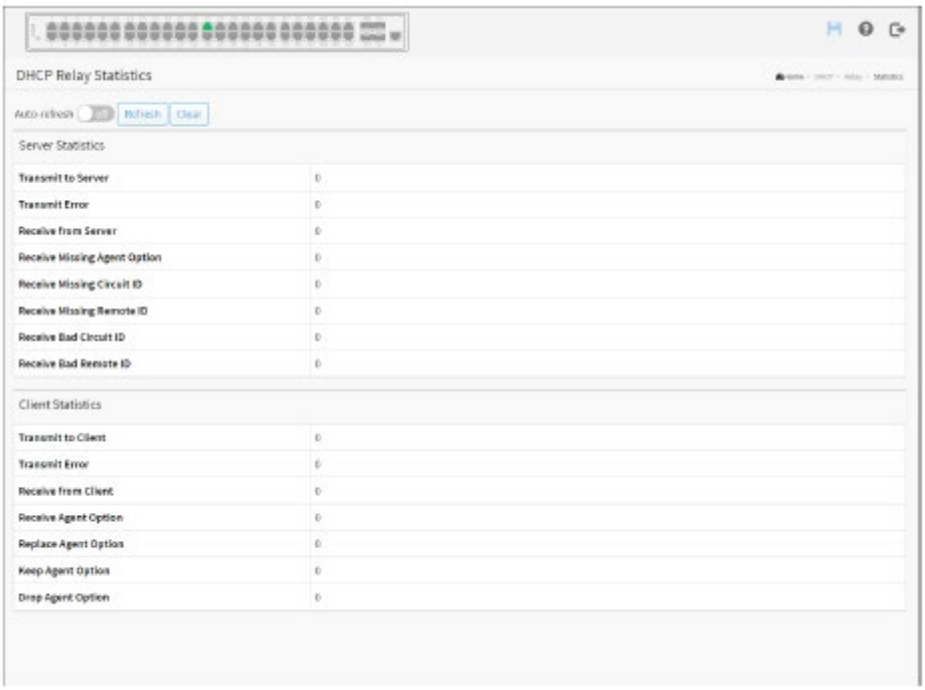
Apply(適用):

クリックすると、変更内容を保存します。

Reset（リセット）：
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

統計

この画面には、DHCP リレーの統計情報が表示されます。



Web インターフェース
Web インターフェースで DHCP リレー統計を監視するには：

1. 「DHCP」 ＞ 「Relay」（リレー） ＞ 「Statistics」（統計）をクリックしてください。
2. DHCP リレー統計情報を表示してください。
3. 情報を自動更新する場合は、「Auto-refresh」（自動更新）を呼び出す必要があります。
4. 「Refresh」（更新）をクリックして、DHCP 詳細統計のエントリーの最新を表示してください。

■パラメーターの説明

Server Statistics（サーバー統計）

Transmit to Server（サーバーへの送信）：
クライアントからサーバーに中継されるパケットの数です。

Transmit Error（送信エラー）：
クライアントへの送信中にエラーが発生したパケットの数です。

Receive from Server（サーバーからの受信）:
サーバーから受信したパケットの数です。

Receive Missing Agent Option（所在不明のエージェントオプションの受信）:
エージェント情報オプションなしで受信したパケットの数です。

Receive Missing Circuit ID（不足回路 ID の受信）:
回路 ID オプションがない状態で受信したパケットの数です。

Receive Missing Remote ID（不明リモート ID の受信）:
リモート ID オプションが見つからない状態で受信したパケットの数です。

Receive Bad Circuit ID（不良回路 ID の受信）:
回線 ID オプションが既知の回線 ID と一致しなかったパケットの数です。

Receive Bad Remote ID（不良リモート ID の受信）:
「Remote ID」（リモート ID）オプションが既知のリモート ID と一致しなかったパケットの数です。

Client Statistics（クライアント統計）
Transmit to Client（クライアントへの送信）:
サーバーからクライアントへの中継されたパケットの数です。

Transmit Error（送信エラー）:
サーバーの送信中にエラーが発生したパケットの数です。

Receive from Client（クライアントからの受信）:
サーバーから受信したパケットの数です。

Receive Agent Option（エージェント受信オプション）:
リレー・エージェント情報オプション付きの受信パケット数です。

Replace Agent Option（エージェントオプションの置換）:
リレー・エージェント情報オプションに置き換えられたパケットの数です。

Keep Agent Option（エージェントオプションの保持）:

リレー・エージェント情報が保持されたパケットの数です。

Drop Agent Option（エージェントオプションの削除）：
リレー・エージェント情報とともに受信された破棄されたパケットの数です。

■ボタン

Auto-refresh（自動更新）：
画面を自動的に更新する場合は、このチェックボックスをONにしてください。自動更新は3秒間隔で行われます。

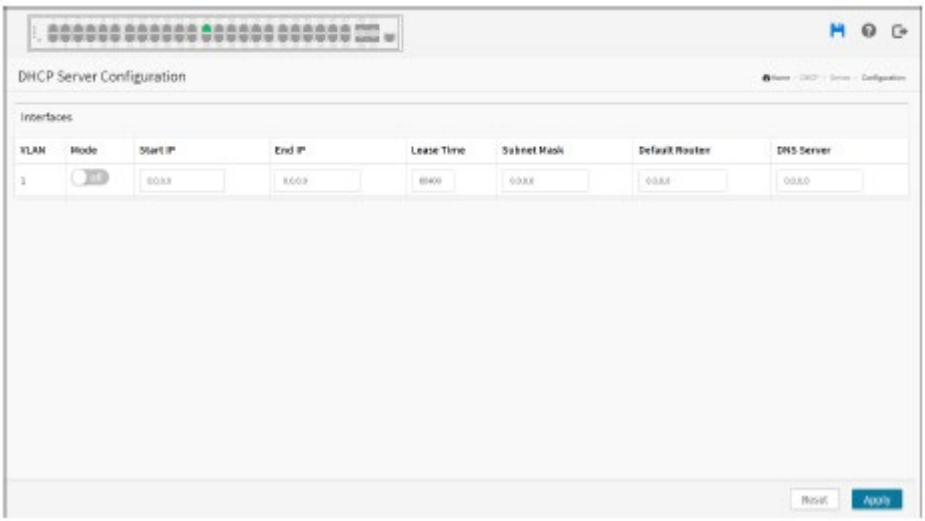
Refresh（更新）：
クリックすると、画面がすぐに更新されます。

Clear（消去）：
画面の内容をクリアします。

サーバー

設定

この画面では、システムごとおよび VLAN ごとに DHCP サーバーを有効/無効にするモードを設定します。また、開始 IP アドレスと終了 IP アドレスを設定します。DHCP サーバーは、これらの IP アドレスを DHCP クライアントに割り当てます。また、設定パラメーターを DHCP クライアントに配信します。



Web インターフェース

Web インターフェースで DHCP サーバー設定を定義するには:

1. 「DHCP」 ＞ 「Server」(サーバー) ＞ 「Configuration」(設定)をクリックしてください。
2. 「Add Interface」(インターフェースの追加)をクリックしてください。
3. 「VLAN」、「Mode」(モード)、「Start IP」(開始 IP)、「End IP」(終了 IP)、「Lease time」(Lease 時間)、「Subnet mask」(サブネットマスク)、「Default router」(デフォルトルーター)、「DNS server」(DNS サーバー)を指定してください。
4. 「Apply」(適用)をクリックしてください。

■パラメーターの説明

VLAN:

DHCP サーバーが有効または無効になっている VLAN を設定してください。許可される VLAN の範囲は 1～4095 です。

Mode（モード）:
VLAN ごとの動作モードを示します。使用可能なモードは、次のとおりです。
Enable（有効）:VLAN ごとに DHCP サーバーを有効にします。
Disable（無効）:VLAN ごとに DHCP サーバーを無効にします。

Start IP and End IP（開始 IP と終了 IP）:
IP 範囲を定義してください。「Start IP」（開始 IP）は、「End IP」（終了 IP）以下である必要があります。

Lease Time（Lease 時間）:
プールの Lease 時間を表示します。

Subnet Mask（サブネットマスク）:
DHCP アドレスのサブネットマスクを設定してください。

Default router（デフォルトルーター）:
このルートの宛先 IP ネットワークまたはホストアドレスを設定してください。

DNS Server（DNS サーバー）:
DNS サーバーを指定してください。

■ボタン
Delete（削除）:
チェックを入れると、エントリーを削除します。これは、次回保存時に削除されます。

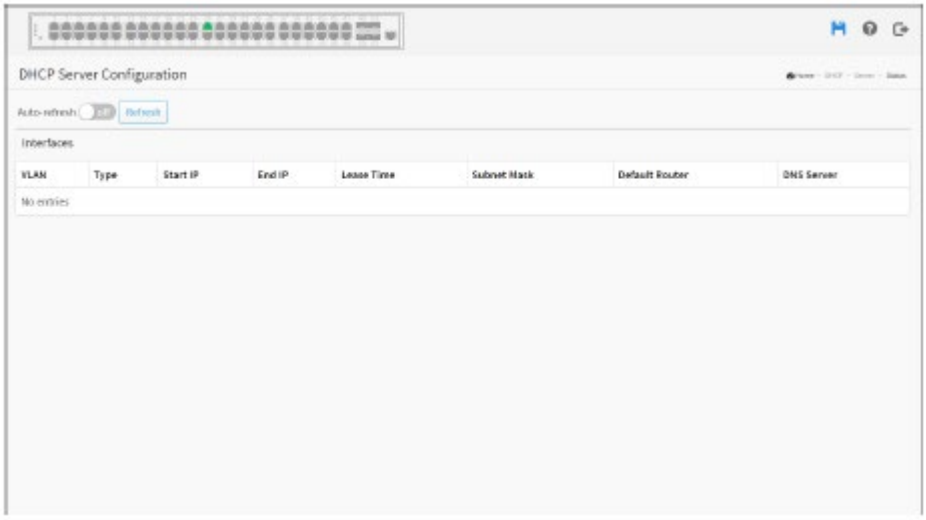
Add Interface（インターフェースの追加）:
クリックすると、新しい DHCP サーバーを追加します。

Apply（適用）:
クリックすると、変更内容を保存します。

Reset（リセット）:
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

状態

この画面には、DHCP サーバーの状態が表示されます。



Web インターフェース

Web インターフェースで DHCP サーバーの状態を表示するには:

1. 「DHCP」 ＞ 「Server」(サーバー) ＞ 「Status」(状態)をクリックしてください。
2. 情報を自動更新する場合は、「Auto-refresh」(自動更新)を呼び出す必要があります。
3. 「Refresh」(更新)をクリックして、DHCP サーバーの状態に関するエントリーを更新してください。

■パラメーターの説明

VLAN:

エントリーの VLAN ID です。

Type(タイプ):

VLAN ごとの操作タイプを示します。可能なタイプは、「Static」(スタティック)および「DMS」です。

Start IP and End IP(開始 IP と終了 IP):

「Start IP」(開始 IP)と「End IP」(終了 IP)を表示します。

Lease Time(Lease 時間):

プールの Lease 時間を表示します。

Subnet Mask(サブネットマスク):

DHCP アドレスのサブネットマスクを表示します。

Default router（デフォルトルーター）:
このルートの宛先 IP ネットワークまたはホストアドレスを表示します。

DNS Server（DNS サーバー）:
DNS サーバーを表示します。

■ボタン

Auto-refresh（自動更新）:
画面を自動的に更新する場合は、このチェックボックスを ON にしてください。自動更新は 3 秒間隔で行われます。

Refresh（更新）:
クリックすると、画面がすぐに更新されます。

第 12 章
セキュリティ

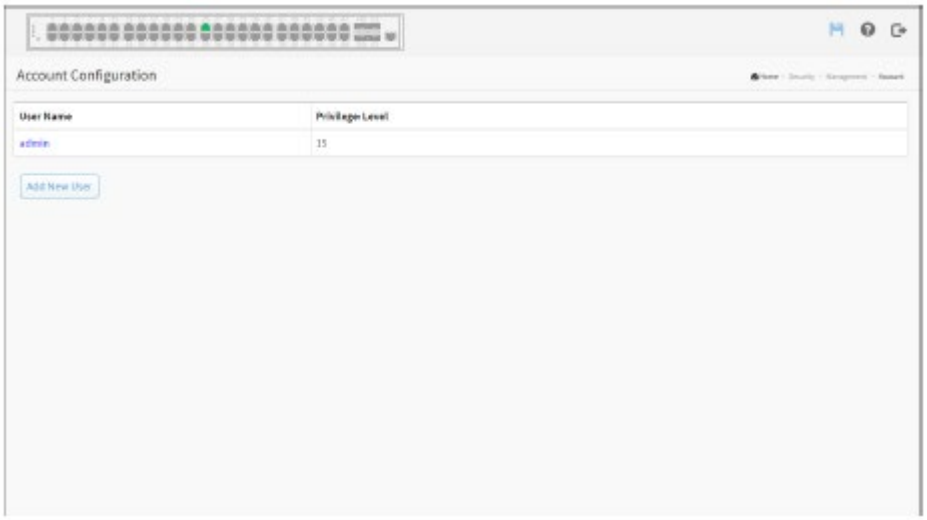
概要

このセクションでは、スイッチのポートセキュリティの設定を行います。ポートセキュリティ機能を使用して、MAC アドレスを制限および識別することで、インターフェースへの入力を制限できます。メニューとサブメニューを以下に示します。

管理

アカウント

この画面には、現在のユーザーの概要が表示されます。現在、Web サーバー上の別のユーザーとしてログインする唯一の方法は、ブラウザーを閉じてから再度開くことです。



Web インターフェース

Web インターフェースでユーザーを設定するには:

1. 「Security」(セキュリティ) ＞ 「Management」(管理) ＞ 「Account」(アカウント)をクリックしてください。
2. 「Add New User」(新規ユーザーの追加)をクリックしてください。

3. 「User Name」(ユーザーネーム)のパラメーターを指定してください。
4. 「Apply」(適用)をクリックしてください。

■パラメーターの説明

User Name（ユーザーネーム）：
ユーザーを識別する名前です。入力可能な文字数は 31 文字です。これは、「Add/Edit User」（ユーザーの追加/編集）へのリンクでもあります。

Password（パスワード）：
パスワードを入力します。フィールドには 31 文字を入力でき、許可される内容は 32～126 の ASCII 文字です。

Password (again)（パスワード（再入力））：
パスワードを再度入力します。フィールドには同じパスワードを再度入力する必要があります。

Privilege Level（権限レベル）：
ユーザーの権限レベルです。指定できる範囲は 0～15 です。権限レベルの値が 15 の場合、すべてのグループにアクセスできます。つまり、デバイスの完全な制御が付与されるということになります。ただし、他の値は、各グループ権限レベルを参照する必要があります。ユーザーの権限は、そのグループのアクセス権を持つグループの権限レベルと同じか、それよりも大きい必要があります。デフォルト設定では、ほとんどのグループ権限レベル 5 には読み取り専用アクセスがあり、権限レベル 10 には読み取り/書き込みアクセスがあります。また、システムメンテナンス（ソフトウェアのアップロード、出荷時のデフォルト設定）には、ユーザー権限レベル 15 が必要です。一般的に、権限レベル 15 は管理者アカウントに、権限レベル 10 は標準ユーザーアカウントに、権限レベル 5 はゲストアカウントに、それぞれ使用することができます。

■ボタン

Apply（適用）：
クリックすると、変更内容を保存します。

Reset（リセット）：
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

Cancel（キャンセル）：
クリックすると、ローカルで行った変更が取り消され、ユーザーへと戻ります。

Delete User（ユーザーの削除）：
現在のユーザーを削除します。このボタンは、新規設定（ユーザーの追加）で使用することができま

せん。

権限レベル

この画面では、権限レベルの概要を示します。スイッチは、ユーザーアカウント、アグリゲーション、診断、EEE、GARP、GVRP、IP、IPMC スヌーピング、LACP、LLDP、LLDP、 MED、 MAC テーブル、MRP、MVR、MVRP、メンテナンス、ミラーリング、POE ポート、プライベート VLAN、QoS、SMTP、SNMP、セキュリティ、スパニングツリー、システムトラップイベント、VCL、 VLAN、音声、VLAN、1～15 の権限レベルを提供します。

Web インターフェース

Web インターフェースで権限レベルを設定するには:

1. 「Security」(セキュリティ) ＞ 「Management」(管理) ＞ 「Privilege Levels」(権限レベル)をクリックしてください。
2. 権限パラメーターを指定してください。
3. 「Apply」(適用)をクリックしてください。

■パラメーターの説明

Group Name(グループ名):

権限グループを識別する名前です。ほとんどの場合、権限レベルグループは 1 つのモジュール(LACP、STP、QoS など)で構成されますが、その中のいくつかには複数のモジュールが含まれています。以下の説明では、これらの権限レベルグループを詳細に定義します。

System(システム):連絡先、名前、場所、タイムゾーン、サマータイム、ログ。

Privilege Levels(権限レベル):

各グループには、設定の読み取り専用、設定/実行の読み取り/書き込みといったサブグループの権限レベルがあります。ユーザー権限は、そのグループへのアクセス権を持つ許可権限レベルと同じか、それよりも大きい必要があります。

■ボタン

Apply(適用):

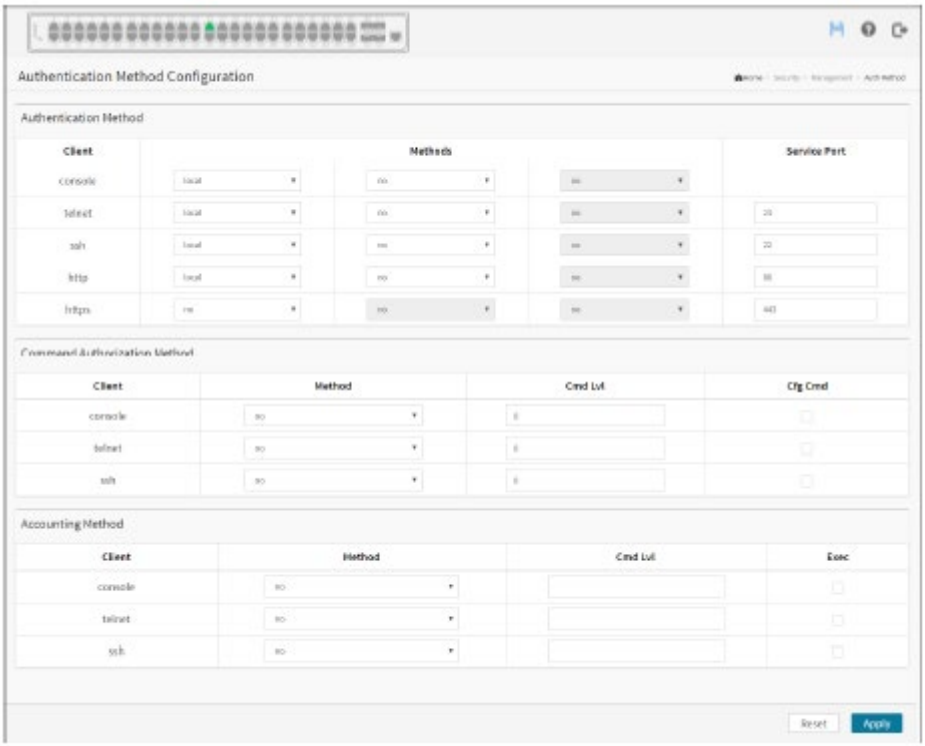
クリックすると、変更内容を保存します。

Reset(リセット):

クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

認証方法

この画面では、管理クライアントインタフェースのいずれかを介してスイッチにログインするときに、認証方法を使用してユーザーを設定する方法を示します。



Web インターフェース

Web インターフェースを使って認証方法を設定するには:

1. 「Security」(セキュリティ) ＞ 「Management」(管理) ＞ 「Auth Method」(認証方法)をクリックしてください。
2. 監視するクライアント(コンソール、telent、ssh、Web)を指定してください。
3. 方法(なし、ローカル、RADIUS、TACACS)、サービスポート、Cmd Lvl、Cfg Cmd、Fallback、Exec を指定してください。
4. 「Apply」(適用)をクリックしてください。

■パラメーターの説明

Authentication Method Configuration(認証方法の設定)

Client(クライアント):

以下の設定が適用される管理クライアントです。

Method(方法):

認証方法は、次のいずれかの値に設定できます。

none（なし）：認証が無効で、ログインできません。

local（ローカル）：スイッチのローカルユーザーデータベースを認証に使用します。

radius：認証にリモート RADIUS サーバーを使用します。

tacacs：認証にリモート TACACS サーバーを使用します。

リモートサーバーがオフラインの場合、リモートサーバーに関係する方法はタイムアウトになります。この場合、次の方法が試行されます。各方法は左から右に試行され、その方法がユーザーを承認または拒否するまで続きます。リモートサーバーがプライマリ認証に使用される場合は、セカンダリ認証を「local」（ローカル）に設定することを推奨します。これにより、設定された認証サーバーがどれも稼働していない場合に、管理クライアントがローカルユーザーデータベースを介してログインできるようになります。

Service Port（サービスポート）：

各クライアントサービスの TCP ポートです。有効なポート番号は 1～65534 です。

HTTP Redirect（HTTP リダイレクト）：

HTTP 自動リダイレクトを有効にします。

Command Authorization Method Configuration（コマンド認証方式の設定）

Client（クライアント）：

以下の設定が適用される管理クライアントです。

Method（方法）：

認証方法は、次ののいずれかの値に設定できます。

none（なし）：認証が無効で、ログインできません。

tacacs：認証にリモート TACACS+サーバーを使用します。

Cmd Lvl：

指定された権限レベルにおいて、すべてのコマンドに対して認証を実行します。認証される必要がある特定のコマンドレベルです。有効なエントリーは 0～15 です。

Cfg Cmd：

configure コマンドを有効または無効にします。

Fallback（フォールバック）：

ローカルデータベースは、いくつかの関数のフォールバック方法として機能できます。この動作は、

セキュリティ装置からの誤ったロックアウトを防止するために設計されています。

Accounting Method Configuration（アカウント認証方法の設定）

Client（クライアント）：
以下の設定が適用される管理クライアントです。

Method（方法）：
アカウント認証方法は、次のいずれかの値に設定できます。

none（なし）：アカウントが無効で、ログインできません。
tacacs：アカウント認証にリモート TACACS+サーバーを使用します。

Cmd Lvl：
指定された権限レベルにおいて、すべてのコマンドに対してアカウント認証を実行します。認証される必要がある特定のコマンドレベルです。有効なエントリーは 0～15 です。

Exec（実行）：
アカウントを実行して、ユーザーが EXEC シェルの実行を許可されているかどうかを確認します。この機能は、自動コマンド情報などのユーザープロファイル情報を戻す場合があります。

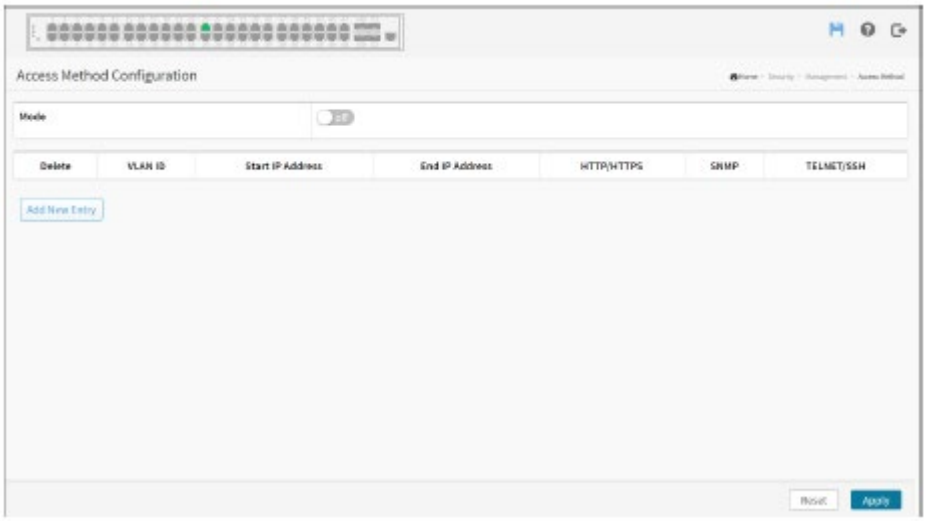
■ボタン

Apply（適用）：
クリックすると、変更内容を保存します。

Reset（リセット）：
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

アクセス方法

HTTP/HTTPS、SNMP、TELNET/SSH など、スイッチのアクセス管理テーブルを設定します。スイッチは、イーサネット LAN、またはインターネットを介して管理できます。



Web インターフェース

Web インターフェースでアクセス方法を設定するには:

1. 「Security」(セキュリティ) ＞ 「Management」(管理) ＞ 「Access Method」(アクセス方法)をクリックしてください。
2. 「Access Management Configuration」(アクセス管理設定)の「Mode」(モード)で「on」を選択してください。
3. 「Add New Entry」(新規登録)をクリックしてください。

4. 「VLAN ID」、「Start IP Address」(開始 IP アドレス)、「End IP Address」(終了 IP アドレス)を指定してください。
5. エントリーにあるアクセス管理方法(HTTP/HTTPS、SNMP、および TELNET/SSH)をチェックしてください。
6. 「Apply」(適用)をクリックしてください。

■パラメーターの説明

Mode（モード）：

アクセス管理モードの操作を示します。使用可能なモードは次のとおりです。

On：アクセス管理モードの操作を許可します。

Off：アクセス管理モードの操作を禁止します。

VLAN ID：

アクセス管理エントリーの VLAN ID を示します。

Delete（削除）：

チェックを入れると、エントリーを削除します。これは、次回保存時に削除されます。

Start IP address（開始 IP アドレス）：

アクセス管理エントリーの開始 IP ユニキャストアドレスを示します。

End IP address（終了 IP アドレス）：

アクセス管理エントリーの終了 IP ユニキャストアドレスを示します。

HTTP/HTTPS：

ホスト IP アドレスがエントリーで指定された IP アドレス範囲と一致する場合、ホストが HTTP/HTTPS インターフェースからスイッチにアクセスできることを示します。

SNMP：

ホスト IP アドレスがエントリーで指定された IP アドレス範囲と一致する場合、ホストが SNMP インターフェースからスイッチにアクセスできることを示します。

TELNET/SSH：

ホスト IP アドレスがエントリーで指定された IP アドレス範囲と一致する場合、ホストが TELNET/SSH インターフェースからスイッチにアクセスできることを示します。

■ボタン

Add New Entry（新規登録）：

クリックすると、新しいアクセス管理エントリーを追加します。

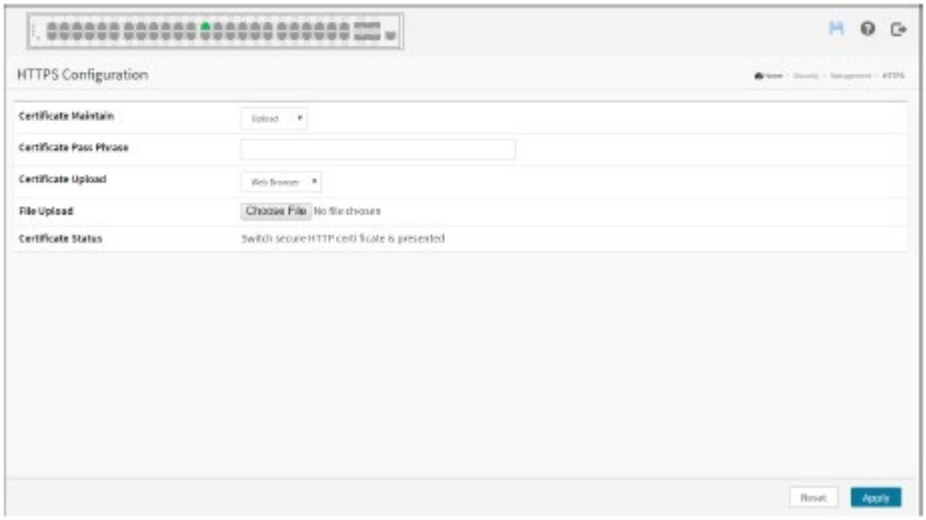
Apply（適用）：

クリックすると、変更内容を保存します。

Reset（リセット）：
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

HTTPS

この画面では、HTTPS 設定を定義し、スイッチの現在の証明書を維持することができます。



Web インターフェース
Web インターフェースでアクセス管理を設定するには：

1. 「Configuration」（設定） ＞ 「Security」（セキュリティ） ＞ 「Management」（管理） ＞ 「HTTPS」をクリックしてください。
2. 「Certificate Maintain」（証明書の維持）、「Certificate Pass Phrase」（証明書のパスフレーズ）、「Certificate Upload」（証明書のアップロード）を指定してください。
3. 「参照」をクリックして、アップロードするファイルを選択してください。
4. 「Apply」（適用）をクリックしてください。

■パラメーターの説明

Certificate Maintain（証明書のメンテナンス）：
証明書のメンテナンス操作を行います。可能な操作には、次のものがあります。

Upload（アップロード）：証明書 PEM ファイルをアップロードします。使用可能な方法は、Web ブラウザーまたは URL です。

Generate（生成）：新しい自己署名 RSA 証明書を生成します。

Certificate Pass Phrase（証明書のパスフレーズ）：

アップロードする証明書が特定のパスフレーズで保護されている場合は、このフィールドにパスフレーズを入力します。

Certificate Upload（証明書のアップロード）：
証明書 PEM ファイルをスイッチにアップロードします。ファイルには、証明書と秘密鍵を一緒に含める必要があります。認証書と秘密鍵を保存するための 2 つのファイルが別々にある場合は、Linux の cat コマンドを使用して、それらを 1 つの PEM ファイルに結合してください。
例：cat my.cert my.key > my.pem
新しいバージョンのブラウザー（例：Firefox v37 および Chrome v39）の大半では、証明書における DSA のサポートが削除されているため、RSA 証明書を推奨します。可能な方法は以下のとおりです。
Web Browser（Web ブラウザー）：Web ブラウザーから証明書をアップロードします。
URL：URL を使用して証明書をアップロードします。サポートされるプロトコルは、HTTP、HTTPS、TFTP、および FTP です。URL 形式は
<プロトコル>://[*<ユーザー名>*[:*<パスワード>*]@]*<ホスト>*[:*<ポート>*][/*<パス>*]/*<ファイル名>*です。
例：
tftp://10.10.10.10/new_image_path/new_image.dat 、
http://username:password@10.10.10.10:80/new_image_path/new_image.dat
有効なファイル名は、アルファベット（A～Z、a～z）、数字（0～9）、ドット（.）、ハイフン（-）、アンダースコア（_）から構成されたテキスト文字列です。最大長は 63 です。また、ハイフンを先頭文字にすることはできません。「.」のみを含むファイル名の内容は許可されません。

Certificate Status（証明書の状態）：
スイッチの証明書の現在の状態を表示します。使用可能な状態は次のとおりです。
Switch secure HTTP certificate is presented.（スイッチのセキュア HTTP 証明書が存在します。）
Switch secure HTTP certificate is not presented.（スイッチのセキュア HTTP 証明書は存在しません。）
Switch secure HTTP certificate is generating ....（スイッチのセキュア HTTP 証明書を生成中です。）

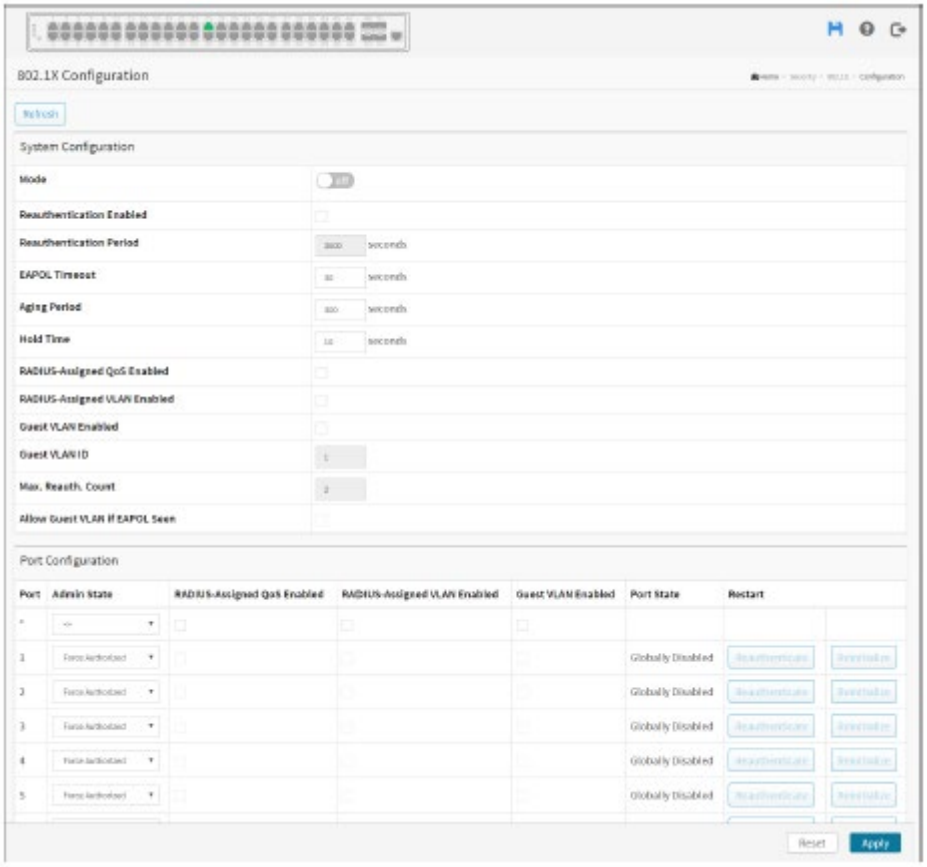
■ボタン
Apply（適用）：
クリックすると、変更内容を保存します。

Reset（リセット）：
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

802.1X

設定

このセクションでは、スイッチの 802.1X パラメーターを設定する方法について説明します。802.1X は、インターネットアクセス、会議通話、共有プリンターを使ったドキュメントの印刷、またはインターネットへの単純なログオンなど、ユーザーをさまざまなリソースへと接続するのに使用することができます。



Web インターフェース

Web インターフェースで IEEE802.1X を設定するには:

1. 「Security」(セキュリティ) ＞ 「802.1X」 ＞ 「Configuration」(設定)をクリックしてください。
2. 「IEEE 802.1X Configuration」(IEEE 802.1X の設定)における「Mode」(モード)で「on」を選択してください。
3. 「Reauthentication Enabled」(再認証の有効)にチェックを入れてください。
4. 「Reauthentication Period」(再認証期間)を設定してください(デフォルトは 3600 秒)。

5. 「EAPOL Timeout」(EAPOL タイムアウト)を設定してください(デフォルトは 30 秒)。
6. 「Aging Period」(エージング期間)を設定してください(デフォルトは 300 秒)。
7. 「Hold Time」(保留時間)を設定してください(デフォルトは 10 秒)。
8. 「RADIUS-Assigned QoS Enabled」(RADIUS が割り当てた QoS を有効にする)チェックボックスを ON にしてください。
9. 「RADIUS-Assigned VLAN Enabled]」(RADIUS が割り当てた VLAN を有効にする)を ON にしてください。
10. 「Guest VLAN Enabled」(ゲスト VLAN を有効にする)を ON にしてください。
11. 「Guest VLAN ID」(ゲスト VLAN ID)を指定してください。
12. 「Max. Reauth. Count」(最大再認証数)を指定してください。
13. 「Allow Guest VLAN if EAPOL Seen」(EAPOL が表示された場合にゲスト VLAN を許可する)チェックボックスを ON にしてください。
14. 「Admin State」(管理者の状態)を選択して、「Port State」(ポートの状態)を表示してください。
15. 「Apply」(適用)をクリックして設定を保存してください。
16. 設定を取り消す場合は、「Reset」(リセット)ボタンをクリックする必要があります。そうすると、以前に保存した値へと戻ります。

■パラメーターの説明

System Configuration(システム設定)

Mode(モード):

ON または OFF です。IEEE802.1X がスイッチでグローバルに有効または無効になっているかどうかを示します。グローバルに無効にすると、すべてのポートでフレームの転送が許可されます。

Reauthentication Enabled(再認証有効):

この項目をチェックすると、正常に認証されたサプリカント/クライアントは、「Reauthentication Period」(再認証期間)で指定された時間が経過した後に再認証されます。802.1X 対応ポートの再認証は、新しいデバイスがスイッチポートに接続されているかどうか、またはサプリカントが接続されていないかどうかを検出するために使用することができます。MAC ベースのポートでは、RADIUS サーバーの設定が変更された場合にのみ、再認証が役立ちます。スイッチとクライアント間の通信は含まれません。したがって、クライアントがまだポートに存在していることを意味するわけではありません(後述の「エージング期間」を参照)。

Reauthentication Period(再認証期間):

接続されたクライアントを再認証するまでの時間を秒単位で指定します。「Reauthentication Enabled」(再認証有効)チェックボックスが ON になっている場合にのみアクティブになります。有効な値の範囲は 1～3600 秒です。

EAPOL Timeout（EAPOL タイムアウト）：
Request Identity EAPOL フレームの再送信時間を決定します。有効な値の範囲は 1～65535 秒です。これは、MAC ベースのポートには影響しません。

Aging Period（エージング期間）：
この設定は、以下のモード、つまりポートセキュリティ機能を使用して MAC アドレスを保護するモードに適用されます。

- シングル 802.1X
- マルチ 802.1X
- MAC ベースの認証

NAS モジュールがポートセキュリティモジュールを使用して MAC アドレスを保護する場合、Port Security モジュールは、対象の MAC アドレスのアクティビティーを定期的にチェックし、一定時間内にアクティビティーが検出されない場合はリソースを解放する必要があります。このパラメーターは、正確にこの期間を制御し、10～1000000 秒の数値に設定できます。
再認証が有効で、ポートが 802.1X ベースモードの場合、ポートに接続されていないサプリカントは次回の再認証時に削除されるため、これはあまり重要ではありません。これは失敗します。しかし、再認証が有効になっていない場合、リソースを解放する唯一の方法は、エントリーを期限切れにすることです。
MAC ベース認証モードのポートについては、再認証はスイッチとクライアント間の直接通信を引き起こさないため、クライアントがまだ接続されているかどうかは検出されません。リソースを解放する唯一の方法は、エントリーを期限切れにすることです。

Hold Time（保留時間）：
この設定は、以下のモード、つまりポートセキュリティ機能を使用して MAC アドレスを保護するモードに適用されます。

- シングル 802.1X
- マルチ 802.1X
- MAC ベースの認証

クライアントがアクセスを拒否された場合（RADIUS サーバーがクライアントアクセスを拒否した場合、または RADIUS サーバー要求がタイムアウトした場合（「Configuration」（設定）→「Security」（セキュリティ）→「AAA」画面で指定されたタイムアウトに従って）、クライアントは「Unauthorized」（未認可（許可されていない））状態に保留されます。保留タイマーは、進行中の認証をカウントしません。
MAC ベースの認証モードにおいて、スイッチは、保留時間中にクライアントから送信された新しいフレームを無視します。
「Hold Time」（保留時間）には、10～1000000 秒の数値を設定できます。

RADIUS-Assigned QoS Enabled（RADIUS 割り当て QoS 有効）:
RADIUS に割り当てられた QoS は、正常に認証されたサプリカントからのトラフィックがスイッチで割り当てられるトラフィッククラスを一元的に制御する手段を提供します。この機能を利用するには、RADIUS サーバーが特別な RADIUS 属性を送信するように設定されている必要があります（詳細については、後述の「RADIUS 割り当て QoS 有効」を参照してください）。
「RADIUS-Assigned QoS Enabled」（RADIUS 割り当て QoS 有効）チェックボックスを ON にすると、RADIUS サーバーに割り当てられた QoS クラス機能をすばやくグローバルに有効/無効にできます。このチェックボックスを ON にすると、各ポートの ditto 設定によって、そのポートで RADIUS が割り当てた QoS クラスが有効になっているかどうかが決まります。このチェックボックスを OFF にすると、RADIUS サーバーが割り当てた QoS クラスがすべてのポートで無効になります。

RADIUS-Assigned VLAN Enabled（RADIUS 割り当て VLAN 有効）:
RADIUS 割り当て VLAN は、正常に認証されたサプリカントがスイッチに配置される VLAN を一元的に制御する手段を提供します。着信トラフィックは、RADIUS に割り当てられた VLAN に分類され、スイッチングされます。この機能を利用するには、RADIUS サーバーが特別な RADIUS 属性を送信するように設定されている必要があります（詳細については、後述の「RADIUS 割り当て VLAN 有効」を参照）。
「RADIUS-Assigned VLAN Enabled」（RADIUS 割り当て VLAN 有効）チェックボックスを ON にすると、RADIUS サーバーに割り当てられた VLAN 機能をすばやくグローバルに有効/無効にできます。このチェックボックスを ON にすると、個々のポートの ditto 設定によって、そのポートで RADIUS が割り当てた VLAN が有効になっているかどうかが決まります。このチェックボックスを OFF にすると、RADIUS サーバーが割り当てた VLAN がすべてのポートで無効になります。

Guest VLAN Enabled（ゲスト VLAN 有効）:
ゲスト VLAN は、ネットワーク管理者または定義されたタイムアウト後に 802.1X 非対応クライアントが配置される特別な VLAN です。通常、ネットワークアクセスは制限されます。スイッチは、次に示すように、ゲスト VLAN への出入りに関する一連のルールに従います。
「Guest VLAN Enabled」（ゲスト VLAN 有効）チェックボックスを ON にすると、ゲスト VLAN 機能をグローバルにすばやく有効/無効にできます。このチェックボックスを OFF にすると、すべてのポートでゲスト VLAN に移動する機能が無効になります。

Guest VLAN ID（ゲスト VLAN ID）:
これは、ポートがゲスト VLAN に移動された場合に、ポートのポート VLAN ID が設定される値です。これは、「Guest VLAN」（ゲスト VLAN）オプションがグローバルに有効になっている場合にのみ変更できます。
有効な値は[1;4094]の範囲です。

Max. Reauth. Count（最大再認証数）：
この設定では、ゲスト VLAN に入ることを考慮する前に、スイッチが応答なしで EAPOL Request Identity フレームを送信する回数を調整します。この値は、「Guest VLAN」（ゲスト VLAN）オプションがグローバルに有効になっている場合にのみ変更できます。
有効な値は[1;255]の範囲です。

Allow Guest VLAN if EAPOL Seen（EAPOL が表示された場合にゲスト VLAN を許可する）：
スイッチは、ポートのライフタイムの間、ポートで EAPOL フレームが受信されたかどうかを記憶します。スイッチは、ゲスト VLAN に入るかどうかを検討した後、最初にこのオプションが有効か無効かを確認します。無効（OFF、デフォルト）の場合、スイッチは、ポートのライフタイムの間、EAPOL フレームがポートで受信されなかった場合にのみゲスト VLAN に入ります。有効（チェックあり）にすると、ポートのライフタイム中に EAPOL フレームがポートで受信された場合でも、スイッチはゲスト VLAN に入ることを検討します。この値は、「Guest VLAN」（ゲスト VLAN）オプションがグローバルに有効になっている場合にのみ変更できます。

Port Configuration（ポート設定）
Port（ポート）：
以下の設定が適用されるポート番号です。

Admin State（管理状態）：
802.1X がグローバルに有効になっている場合、この選択はポートの認証モードを制御します。以下のモードを使用できます。

- Force Authorized（強制許可）：
  このモードでは、ポートリンクが起動するとスイッチは 1 つの EAPOL Success フレームを送信し、ポート上のクライアントは認証なしでネットワークアクセスを許可されます。

- Force Unauthorized（強制無許可）：
  このモードでは、ポートリンクが起動するとスイッチは 1 つの EAPOL Failure フレームを送信し、ポート上のクライアントはネットワークアクセスを拒否されます。

- Port-based 802.1X（ポートベースの 802.1X）：
  802.1X の世界において、ユーザーはサプリカント、スイッチはオーセンティケーター、RADIUS サーバーは認証サーバーと呼ばれます。オーセンティケーターは、中間者として機能し、サプリカントと認証サーバー間で要求と応答を転送します。サプリカントとスイッチ間で送信されるフレームは、EAPOL（EAP Over LAN）フレームと呼ばれる特殊な 802.1X フレームです。EAPOL フレームは EAP PDU をカプセル化します（RFC3748）。ス

イッチと RADIUS サーバー間で送信されるフレームは RADIUS パケットです。RADIUS パケットも、スイッチの IP アドレス、名前、およびスイッチ上のサプリカントのポート NO などの他の属性とともに EAP PDU をカプセル化します。EAP は、MD5-Challenge、PEAP、TLS など、さまざまな認証方法を可能にするという点で非常に柔軟性があります。重要なことは、オーセンティケーター（スイッチ）が、サプリカントと認証サーバーがどの認証方法を使用しているか、または特定の方法に必要な情報交換フレームの数を知る必要がないことです。スイッチは、フレームの EAP 部分を関連するタイプ（EAPOL または RADIUS）にカプセル化し、転送します。

認証が完了すると、RADIUS サーバーは、成功または失敗を示す特別なパケットを送信します。この決定をサプリカントに転送する以外に、スイッチはサプリカントに接続されているスイッチポートのトラフィックを開放またはブロックするためにこの決定を使用します。

注意： 2 つのバックエンドサーバーが有効で、サーバータイムアウトが X 秒（AAA 設定画面を使用）に設定されており、リストの最初のサーバーが現在停止している（ただし、停止しているとは見なされません）と仮定します。

これで、サプリカントが EAPOL Start フレームを X 秒より速い速度で再送信した場合、スイッチは、サプリカントから新しい EAPOL Start フレームを受信するたびに、実行中のバックエンド認証サーバー要求をキャンセルするため、認証されることはありません。

また、サーバーに障害が発生していないため（X 秒が経過していないため）、スイッチからの次のバックエンド認証サーバー要求時に、同じサーバーに接続されます。このシナリオは永久にループします。したがって、サーバーのタイムアウトは、サプリカントの EAPOL Start フレームの再送信レートよりも小さくする必要があります。

◆ Single 802.1X（シングル 802.1X）：

ポートベース 802.1X 認証では、サプリカントがポートで正常に認証されると、ポート全体がネットワークトラフィック用にオープンされます。これにより、（例えばハブを介して）ポートに接続されている他のクライアントは、認証に成功したクライアントをピギーバックし、実際には認証されていないにもかかわらずネットワークアクセスを取得できます。このセキュリティ違反を解消するには、Single 802.1X のバリアントを使用します。Single 802.1X は実際には IEEE 規格ではありませんが、ポートベース 802.1X と同じ特性を持つ多くの機能を備えています。Single 802.1X では、最大 1 つのサプリカントが一度にポートで認証されます。通常の EAPOL フレームは、サプリカントとスイッチ間の通信に使用されます。1 つのポートに複数のサプリカントが接続されている場合、ポートのリンクが起動したときに最初に表示されるサプリカントが最初に考慮されます。そのサプリカントが一定時間内に有効

な認証情報を提供しない場合、別のサプリカントがチャンスを取得します。サプリカントが正常に認証されると、そのサプリカントのみがアクセスを許可されます。これは、サポートされているすべてのモードの中で最もセキュアです。このモードでは、認証に成功したサプリカントの MAC アドレスを保護するために、ポートセキュリティモジュールが使用されます。

◆ Multi 802.1X（マルチ 802.1X）：

ポートベース 802.1X 認証では、サプリカントがポートで正常に認証されると、ポート全体がネットワークトラフィック用にオープンされます。これにより、（例えばハブを介して）ポートに接続されている他のクライアントは、認証に成功したクライアントをピギーバックし、実際には認証されていないにもかかわらずネットワークアクセスを取得できます。このセキュリティ違反を解消するには、Multi 802.1X のバリアントを使用します。

Multi 802.1X は実際には IEEE 規格ではありませんが、ポートベース 802.1X と同じ特性を持つ多くの機能を備えています。Multi 802.1X は、Single 802.1X と同様に、IEEE 標準ではなく、同じ特性の多くを特徴とするバリアントです。Multi 802.1X では、1 つ以上のサプリカントが同時に同じポートで認証されます。各サプリカントは、ポートセキュリティモジュールを使用して個別に認証され、MAC テーブルでセキュリティ保護されます。

Multi 802.1X では、スイッチからサプリカントに送信される EAPOL フレームの宛先 MAC アドレスとしてマルチキャスト BPDU MAC アドレスを使用することはできません。これにより、ポートに接続されているすべてのサプリカントがスイッチから送信された要求に応答することになります。代わりに、スイッチはサプリカントの MAC アドレスを使用します。これは、サプリカントによって送信された最初の EAPOL Start または EAPOL Response Identity フレームから取得されます。ただし、サプリカントがアタッチされていない場合は例外です。この場合、スイッチは BPDU マルチキャスト MAC アドレスを宛先として使用して EAPOL Request Identity フレームを送信し、ポートにある可能性のあるサプリカントをウェイクアップします。

ポートにアタッチできるサプリカントの最大数は、「Port Security Limit Control」（ポートセキュリティ制限制御）機能を使用して制限できます。

◆ MAC-based Auth.（MAC ベースの認証）：

ポートベースの 802.1X とは異なり、MAC ベースの認証は標準ではなく、業界で採用されている最良慣行の方法に過ぎません。MAC ベースの認証では、ユーザーはクライアントと呼ばれ、スイッチはクライアントの代わりにサプリカントとして機能します。クライアントによって送信された最初のフレーム（任意の種類のフレーム）はスイッチによってスヌーピングされ、次にクライアントの MAC アドレスが、RADIUS サーバーとの後続の EAP 交換でユーザー名とパスワードの両方として使用されます。6 バイトの MAC アドレスは、

「*xx-xx-xx-xx-xx-xx*」という形式の文字列に変換されます。つまり、小文字の 16 進数の間の区切り文字としてダッシュ(-)が使用されます。スイッチは MD5 チャレンジ認証方式のみをサポートしているため、RADIUS サーバーはそれに応じて設定する必要があります。

認証が完了すると、RADIUS サーバーは成功または失敗の通知を送信します。これにより、スイッチはポートセキュリティモジュールを使用して、特定のクライアントのトラフィックをオープンまたはブロックします。この場合のみ、クライアントからのフレームはスイッチで転送されます。この認証には EAPOL フレームは含まれていないため、MAC ベース認証は 802.1X 規格とは関係ありません。

ポートベース 802.1X よりも MAC ベース認証の利点は、複数のクライアントが同じポート(サードパーティ製スイッチやハブなど)に接続でき、個別の認証が必要であり、クライアントが認証に特別なサプリカントソフトウェアを必要としないことです。802.1X ベースの認証よりも MAC ベースの認証の利点は、クライアントが認証するために特別なサプリカントソフトウェアを必要としないことです。不利な点は、MAC アドレスが悪意のあるユーザーによってなりすまされる可能性があることです。MAC アドレスが有効な RADIUS ユーザーである機器は、誰でも使用できます。また、MD5 チャレンジメソッドのみがサポートされます。

ポートセキュリティ制限制御機能を使用して、ポートに接続できるクライアントの最大数を制限できます。

RADIUS-Assigned QoS Enabled(Admin State(RADIUS 割り当て QoS 有効):
特定のポートで RADIUS 割り当て QoS がグローバルに有効化され、有効化(チェック)されている場合、スイッチは、サプリカントが正常に認証されたときに RADIUS サーバーによって送信される RADIUS Access-Accept パケットで伝送される QoS クラス情報に応答します。サプリカントのポートで受信されたトラフィックが存在し、有効な場合、これは、指定された QoS クラスに分類されます。(再)認証に失敗した場合、または RADIUS アクセス許可パケットが QoS クラスを伝送しないか無効である場合、またはサプリカントがポートに存在しなくなった場合、ポートの QoS クラスは直ちに元の QoS クラスに戻されます(RADIUS 割り当てに影響を与えることなく、その間に管理者によって変更される可能性があります)。このオプションは、シングルクライアントモード、すなわち、以下のモードでのみ使用できます。

- ポートベース 802.1X
- シングル 802.1X

RADIUS attributes used in identifying a QoS Class(QoS クラスの識別に使用される RADIUS 属性):
RFC4675 で定義された User-Priority-Table 属性は、Access-Accept パケットの QoS クラスを識別するための基礎を形成します。パケット内の属性の最初の出現のみが考慮され、有効であるためには、次のルールに従う必要があります。

- 属性値の 8 オクテットはすべて同一でなければなりません。また、「0」～「7」の範囲の ASCII 文字で構成されなければならず、[0;7]の範囲の望ましい QoS クラスに変換されます。

RADIUS-Assigned VLAN Enabled（RADIUS 割り当て VLAN 有効）:
RADIUS 割り当て VLAN がグローバルに有効化され、特定のポートに対して有効化（チェック）されている場合、スイッチは、サプリカントが正常に認証されたときに RADIUS サーバーによって送信される RADIUS Access-Accept パケットで伝送される VLAN ID 情報に応答します。ポートのポート VLAN ID が存在し、有効な場合、この VLAN ID に変更され、ポートはその VLAN ID のメンバーに設定されて、ポートは強制的に VLAN unaware モードになります。割り当てられると、ポートに到着するすべてのトラフィックが分類され、RADIUS によって割り当てられた VLAN ID でスイッチングされます。
（再）認証に失敗するか、RADIUS Access-Accept パケットが VLAN ID を運ばなくなったか、無効になった場合、またはサプリカントがポートに存在しなくなった場合、ポートの VLAN ID は直ちに元の VLAN ID に戻されます（RADIUS 割り当てに影響を与えることなく、その間に管理者によって変更される可能性があります）。このオプションは、シングルクライアントモード、すなわち、以下のモードでのみ使用できます。

- ポートベース 802.1X
- シングル 802.1X

VLAN 割り当てのトラブルシューティングを行うには、「Monitor」（モニター） ＞ 「VLANs」（VLAN）＞ 「VLAN Membership and VLAN Port」（VLAN メンバーシップと VLAN ポート）画面を使用します。これらの画面には、現在のポート VLAN 設定を（一時的に）オーバーライドしたモジュールが表示されます。

RADIUS attributes used in identifying a VLAN ID（VLAN ID の識別に使用される RADIUS 属性）:
RFC2868 と RFC3580 は、Access-Accept パケットで VLAN ID を識別する際に使用される属性の基礎を形成します。次の基準が使用されます。

- Tunnel-Medium-Type、Tunnel-Type、および Tunnel-Private-GroupID 属性は、すべて Access-Accept パケットに少なくとも 1 回は存在している必要があります。
- スイッチは、同じタグ値を持ち、次の要件を満たすこれらの属性の最初のセットを探します（タグ==0 が使用されている場合、Tunnel-Private-Group-ID にタグを含める必要はありません）。
  - Tunnel-Medium-Type の値は「IEEE-802」（序数 6）に設定する必要があります。
  - Tunnel-Type の値は「VLAN」（序数 13）に設定する必要があります。
  - Tunnel-Private-Group-ID の値は、範囲「0」～「9」の ASCII 文字の文字列である必要があります。これは、VLAN ID を表す 10 進文字列として解釈されます。先頭の「0」は破棄されます。最終値は[1;4095]の範囲内でなければなりません。

Guest VLAN Enabled（ゲスト VLAN 有効）:
特定のポートでゲスト VLAN がグローバルに有効になっていて、有効になっている（チェックされている）場合、スイッチは、以下のルールに従ってポートをゲスト VLAN に移動することを検討します。このオプションは、EAPOL ベースのモードでのみ使用できます。

- ポートベース 802.1X
- シングル 802.1X
- マルチ 802.1X

VLAN 割り当てのトラブルシューティングを行うには、「Monitor」（モニター） ＞ 「VLANs」（VLAN）＞ 「VLAN Membership and VLAN Port」（VLAN メンバーシップと VLAN ポート）画面を使用します。これらの画面には、現在のポート VLAN 設定を（一時的に）オーバーライドしたモジュールが表示されます。

Guest VLAN Operation（ゲスト VLAN 操作）:
ゲスト VLAN が有効なポートのリンクが起動すると、スイッチは EAPOL Request Identity フレームの送信を開始します。そのようなフレームの送信回数が最大再認証数を超えて、その間、EAPOL フレームが受信されていない場合、スイッチはゲスト VLAN に入ると見なします。EAPOL Request Identity フレームの送信間隔は、「EAPOL Timeout」（EAPOL タイムアウト）で設定します。「Allow Guest VLAN if EAPOL Seen」（EAPOL が表示された場合にゲスト VLAN を許可する）を選択すると、ポートはゲスト VLAN に配置されます。無効にした場合、スイッチは最初にその履歴をチェックして、ポートで EAPOL フレームが受信されているかどうかを確認します（ポートリンクがダウンした場合、またはポートの管理状態が変更された場合、この履歴はクリアされます）。受信されていない場合、ポートはゲスト VLAN に配置されます。そうしないと、ゲスト VLAN には移動しませんが、EAPOL タイムアウトで指定されたレートで EAPOL 要求 ID フレームの送信を継続します。
ゲスト VLAN に入ると、ポートは認証済みと見なされ、ポートに接続されているすべてのクライアントはこの VLAN へのアクセスを許可されます。スイッチは、ゲスト VLAN に入るときに EAPOL Success フレームを送信しません。ゲスト VLAN では、スイッチは EAPOL フレームのリンクを監視し、そのようなフレームが 1 つ受信されると、すぐにゲスト VLAN からポートを取り出し、ポートモードに従ってサプリカントの認証を開始します。EAPOL フレームを受信した場合、「Allow Guest VLAN if EAPOL Seen」（EAPOL が表示された場合にゲスト VLAN を許可する）が無効になっていると、ポートはゲスト VLAN に戻ることができません。

Port State（ポートの状態）:
ポートの現在の状態です。これは、以下の値のうちの 1 つを引き受けることができます。

Globally Disabled：IEEE802.1X は、globally Disabled です。
Link Down（リンクダウン）：IEEE802.1X はグローバルに有効になっていますが、ポートにリンクがありません。

Authorized（許可）：ポートは「Force Authorized」（強制許可）モードまたはシングルサプリカントモードで、サプリカントは承認されています。

Unauthorized（無許可）：ポートが「Force Unauthorized」（強制無許可）モードまたはシングルサプリカントモードで、サプリカントが RADIUS サーバーによって正常に認証されていません。

X Auth/Y Unauth：ポートはマルチサプリカントモードです。現在、X クライアントは許可されており、Y は許可されていません。

Restart（再起動）：

各行には 2 つのボタンを使用できます。このボタンは、認証がグローバルに有効で、ポートの管理状態が EAPOL ベースまたは MAC ベースのモードの場合にのみ有効になります。

これらのボタンをクリックしても、画面の設定は変更されません。

Re-authenticate（再認証）：ポートの「Quiet Period」（抑止期間）が切れるたびに再認証をスケジュールします（EAPOL ベースの認証）。MAC ベースの認証の場合、再認証はすぐに試行されます。

このボタンは、ポートで正常に認証されたクライアントに対してのみ有効で、クライアントが一時的に不正になることはありません。

Reinitialize（再初期化）：ポート上のクライアントを強制的に再初期化するため、すぐに再認証が行われます。再認証が行われている間は、クライアントは無許可状態に移行します。

■ボタン

Apply（適用）：

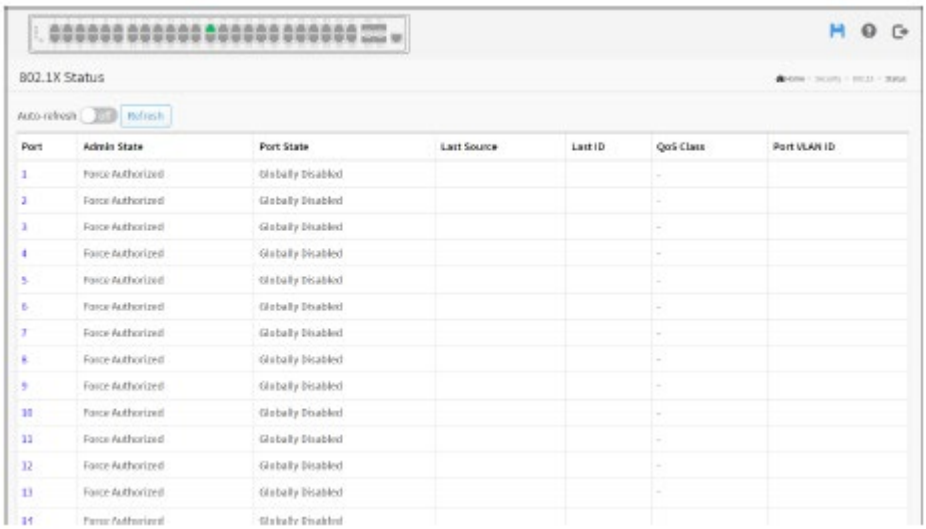
クリックすると、変更内容を保存します。

Reset（リセット）：

クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

状態

このセクションでは、スイッチの各ポートにおける 802.1X の状態に関する情報の表示方法について説明します。状態には、「Admin State」（管理状態）、「Port State」（ポート状態）、「Last Source」（最終ソース）、「Last ID」（最終 ID）、「Port VLAN ID」（ポート VLAN ID）が含まれます。



Web インターフェース

802.1X の状態を Web インターフェースに表示するには：

1. 「Security」（セキュリティ） ＞ 「IEEE 802.1X」 ＞ 「Status」（状態）をクリックしてください。
2. 「Auto-refresh」（自動更新）にチェックを入れてください。
3. ポートの詳細統計情報を更新するには、「Refresh」（更新）をクリックしてください。
4. 802.1X 統計を表示するポートを選択することができます。

■パラメーターの説明

802.1X Status（802.1X の状態）

Port（ポート）：

クリックすると、このポートの 802.1X 統計の詳細に移動します。

Admin State（管理状態）：

ポートの現在の管理状態です。可能な値の説明については、「802.1X 管理状態」を参照してください。

Port State（ポートの状態）：

ポートの現在の状態です。個々の状態の説明については、802.1X のポートの状態を参照してくだ

さい。

Last Source（最終ソース）：
EAPOL ベース認証のために最後に受信した EAPOL フレームで運ばれた送信元 MAC アドレスと、MAC ベース認証のために新しいクライアントから最後に受信したフレームです。

Last ID（最終 ID）：
最後に受信した EAPOL ベース認証用の Response Identity EAPOL フレームで運ばれたユーザー名（サプリカント ID）と、MAC ベース認証用の新しいクライアントから最後に受信したフレームのソース MAC アドレスです。

QoS Class（QoS クラス）：
RADIUS サーバーによってポートに割り当てられた QoS クラスです（有効な場合）。

Port VLAN ID（ポートの VLAN ID）：
802.1X がそのポートを入れた VLAN ID です。ポート VLAN ID が 802.1X によってオーバーライドされていない場合、この項目は空白です。
VLAN ID が RADIUS サーバーによって割り当てられている場合は、VLAN ID に「RADIUS-assigned」（RADIUS 割り当て）が付加されます。ここでは、RADIUS 割り当て VLAN について詳しく説明します。
ポートをゲスト VLAN に移動すると、VLAN ID に「Guest」（ゲスト）が付加されます。ゲスト VLAN について詳しくは、こちらを参照してください。

■ボタン

Auto-refresh（自動更新）：
画面を自動的に更新する場合は、このチェックボックスを ON にしてください。自動更新は 3 秒間隔で行われます。

Refresh（更新）：
クリックすると、画面がすぐに更新されます。

Port 1-52 Status（ポート 1～52 の状態）：
ポート番号をクリックすると、ポートの状態が個別に表示されます。

■パラメーターの説明

Port（ポート）：
ドロップダウンメニューを使用して、表示するポートを選択します。

Admin State（管理状態）：
ポートの現在の管理状態です。可能な値の説明については、「802.1X の管理状態」を参照してください。

Port State（ポートの状態）：
ポートの現在の状態です。個々の状態の説明については、802.1X ポートの状態を参照してください。

■ボタン

Auto-refresh（自動更新）：
画面を自動的に更新する場合は、このチェックボックスを ON にしてください。自動更新は 3 秒間隔で行われます。

Refresh（更新）：
クリックすると、画面がすぐに更新されます。

IP ソースガード

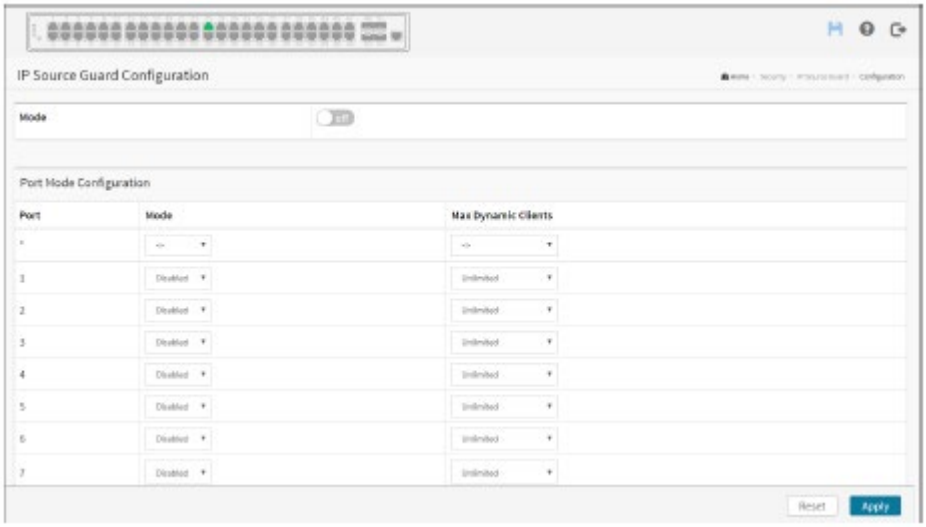
このセクションでは、スイッチの IP ソースガードの詳細パラメーターを設定する方法について説明します。IP ソースガード設定を使用すると、スイッチのポートで有効または無効にすることができます。

設定

このセクションでは、IP ソースガードの設定方法について説明します。

モード（有効および無効）

最大ダイナミッククライアント（0、1、2、無制限）



Web インターフェース

Web インターフェースで IP ソースガード設定を定義するには：

1. 「Security」（セキュリティ） ＞ 「IP Source Guard」（IP ソースガード） ＞ 「Configuration」（設定）をクリックしてください。
2. 「IP Source Guard Configuration」（IP ソースガードの設定）における「Mode」（モード）で「on」を選択してください。
3. 「Port Mode Configuration」（ポートモードの設定）で、特定のポートの「Mode」（モード）を「Enabled」（有効）にしてください。
4. 「Port Mode Configuration」（ポートモードの設定）で、特定のポートの「Maximum Dynamic Clients」（最大ダイナミッククライアント）を「0」、「1」、「Unlimited」（無制限）の中から選択してください。

5. 「Apply」（適用）をクリックしてください。

■パラメーターの説明

Mode of IP Source Guard Configuration（IP ソースガード設定のモード）：
グローバル IP ソースガードを有効または無効にします。モードが有効になると、設定されたすべての ACE が失われます。

Port Mode Configuration（ポートモードの設定）：
どのポートで IP ソースガードを有効にするかを指定します。特定のポートでグローバルモードとポートモードの両方が有効になっている場合にのみ、この特定のポートで IP ソースガードが有効になります。

Max Dynamic Clients（ダイナミッククライアントの最大数）：
特定のポートで学習できるダイナミッククライアントの最大数を指定します。この値には、0、1、2、または無制限を指定できます。ポートモードが有効で、最大ダイナミッククライアントの値が 0 の場合、特定のポートのスタティックエントリーに一致する IP パケットの転送のみを許可することを意味します。

■ボタン

Apply（適用）：
クリックすると、変更内容を保存します。

Reset（リセット）：
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

Max Dynamic Clients（ダイナミックからスタティックへの変換）：
クリックすると、すべてのダイナミックエントリーがスタティックエントリーに変換されます。

スタティックテーブル

このセクションでは、スイッチのスタティック IP ソースガードテーブルのパラメーターを設定する方法について説明します。エントリーを管理するには、「Static IP Source Guard Table」(スタティック IP ソースガードテーブル)の設定を使用します。

Web インターフェース

Web インターフェースでスタティック IP ソースガードテーブル設定を定義するには:

1. 「Security」(セキュリティ) ＞ 「IP Source Guard」(IP ソースガード) ＞ 「Static Table」(スタティックテーブル)をクリックしてください。
2. 「Add New Entry」(新規登録)をクリックしてください。

3. エントリーに「Port」(ポート)、「VLAN ID」、「IP Address」(IP アドレス)、および「MAC address」(MAC アドレス)を指定してください。
4. 「Apply」(適用)をクリックしてください。

■パラメーターの説明

Port（ポート）：
この設定の論理ポートです。

VLAN ID：
この設定の VLAN ID です。

IP Address（IP アドレス）：
許可された送信元 IP アドレスです。

MAC address（MAC アドレス）：
許可された送信元 MAC アドレスです。

Add New Entry（新規登録）：
クリックすると、スタティック IP ソースガードテーブルに新しいエントリーを追加します。新しいエントリーの「Port」（ポート）、「IP Address」（IP アドレス）、および「MAC Address」（[MAC アドレス）を指定してください。そうしたら、「Apply」（適用）をクリックしてください。

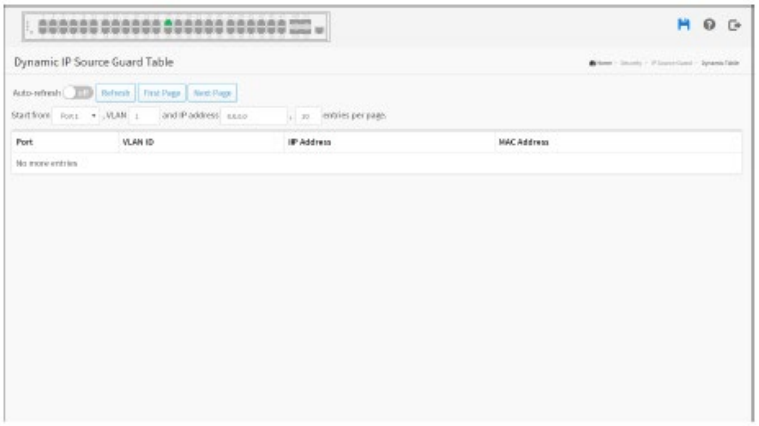
Delete（削除）：
チェックを入れると、エントリーを削除します。これは、次回保存時に削除されます。

Apply（適用）：
クリックすると、変更内容を保存します。

Reset（リセット）：
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

ダイナミックテーブル

この画面には、ダイナミック IP ソースガードテーブルのエントリーが表示されます。ダイナミック IP ソースガードテーブルは、ポート、IP アドレス、MAC アドレスの順にソートされます。



Web インターフェース

Web インターフェースでダイナミック IP アドレスソースガードテーブル設定を定義するには:

1. 「Security」(セキュリティ) ＞ 「IP Source Guard」(IP ソースガード) ＞ 「Dynamic Table」(ダイナミックテーブル)をクリックしてください。
2. 「Auto-refresh」(自動更新)にチェックを入れてください。
3. ポートの詳細統計情報を更新するには、「Refresh」(更新)をクリックしてください。
4. 画面を変更する場合は、「First Page」(最初のページ)や「Next Page」(次のページ)をクリックしてください。
5. 「Start from *port*」(*ポート*から開始)、「VLAN」、「IP Address」(IP アドレス)、「entries per page」(ページあたりのエントリー数)を指定してください。

■パラメーターの説明

Navigating the IP Source Guard Table (IP ソースガードテーブルのナビゲート)

各画面には、ダイナミック IP ソースガードテーブルから最大 99 個のエントリーが表示されます。デフォルトは 20 で、「entries per page」(ページあたりのエントリー数)入力フィールドで選択されています。最初にアクセスすると、ダイナミック IP アドレスソースガードテーブルの先頭から最初の 20 エントリーが表示されます。

「Start from」*[ポートアドレス]*(*[ポートアドレス]*から開始)、「VLAN」および「IP address」(IP アドレス)の各入力フィールドを使用すると、ダイナミック IP アドレスソースガードテーブルの開始点を選択できます。「Refresh」(更新)ボタンをクリックすると、表示されているテーブルが更新されます。これは、そのテーブルから、または次に一致するダイナミック IP アドレスソースガードテーブルに最も近いテーブルから始まります。さらに、2 つの入力フィールドは(「Refresh」(更新)ボタンをクリックすると)、最初に表示されたエントリーの値を想定し、同じ開始アドレスで継続的に更新することができます。

「Next Page」(次のページ)は、現在表示されているテーブルの最後のエントリーを次の参照のベースとして使用します。最後に達すると、表示されたテーブルに「これ以上エントリーはありません」というテキストが表示されます。このような場合は、「First Page」(最初のページ)ボタンを使用して、最初からやり直してください。

Port(ポート):
エントリーを表示するスイッチのポート番号です。

VLAN ID:
IP トラフィックが許可される VLAN ID です。

IP Address(IP アドレス):
エントリーのユーザーIP アドレスです。

MAC Address(MAC アドレス):
送信元の MAC アドレスです。

Show entries(エントリーの表示):
表示する項目の数を選択できます。

■ボタン

Auto-refresh(自動更新):
画面を自動的に更新する場合は、このチェックボックスを ON にしてください。自動更新は 3 秒間隔で行われます。

Refresh(更新):
クリックするとページを更新します。

First Page(最初のページ):
リストを更新し、最初のページに戻ります。

Next Page(次のページ):
リストを更新し、次のページに進みます。

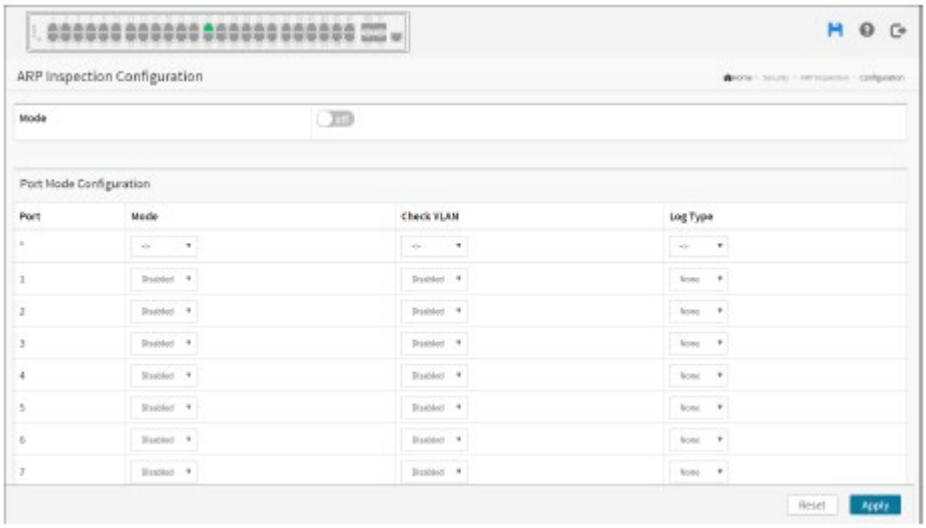
ARP インスペクション

このセクションでは、スイッチの ARP 検査パラメーターを設定する方法について説明します。ARP インスペクション設定を使用すると、ARP テーブルを管理することができます。

設定

このセクションでは、モード（on および off）を含む ARP インスペクションの設定方法について説明します。

モード（有効および無効）
ポート（有効および無効）



Web インターフェース
Web インターフェースで ARP インスペクションを設定するには：

1. 「Security」（セキュリティ） ＞ 「ARP Inspection」（ARP インスペクション） ＞ 「Configuration」（設定）をクリックしてください。
2. 「ARP Inspection Configuration」（ARP インスペクションの設定）における「Mode」（モード）で「on」を選択してください。
3. 「Port Mode Configuration」（ポートモードの設定）で、特定のポートの「Mode」（モード）を「Enabled」（有効）にしてください。
4. 「Apply」（適用）をクリックしてください。）

■パラメーターの説明

Mode of ARP Inspection Configuration（ARP インスペクション設定のモード）：
グローバル ARP インスペクションを有効にするか、グローバル ARP インスペクションを無効にします。

Port Mode Configuration（ポートモードの設定）：
どのポートで ARP インスペクションを有効にするかを指定します。特定のポートでグローバルモードとポートモードの両方が有効になっている場合にのみ、この特定のポートで ARP インスペクションが有効になります。使用可能なモードは次のとおりです。

Enabled（有効）：ARP インスペクション操作を有効にします。

Disabled（無効）：ARP インスペクション動作を無効にします。

VLAN 設定を検査する場合は、「Check VLAN」（VLAN をチェックする）の設定を有効にする必要があります。「Check VLAN」（VLAN をチェックする）のデフォルト設定は無効です。「Check VLAN」（VLAN をチェックする）の設定が無効の場合、ARP インスペクションのログタイプはポート設定を参照します。「Check VLAN」（VLAN をチェックする）の設定が有効になっている場合、ARP インスペクションのログタイプは VLAN 設定を参照します。「Check VLAN」（VLAN をチェックする）に設定できる内容は以下のとおりです。

Enabled（有効）：VLAN 動作のチェックを有効にします。

Disabled（無効）：VLAN 動作のチェックを無効にします。

特定のポートのグローバルモードとポートモードのみが有効で、「Check VLAN」（VLAN をチェックする）の設定が無効になっている場合、ARP インスペクションのログタイプはポート設定を参照します。ログタイプには、次の使用可能なタイプが 4 種類あります。

None（なし）：何も記録しません。

Deny（拒否）：拒否されたエントリーをログに記録します。

Permit（許可）：許可されたエントリーをログに記録します。

ALL（すべて）：すべてのエントリーを記録します。

Check VLAN（VLAN をチェックする）：
VLAN 設定を検査する場合は、「Check VLAN」（VLAN をチェックする）の設定を有効にする必要があります。「Check VLAN」（VLAN をチェックする）のデフォルト設定は無効です。「Check VLAN」（VLAN をチェックする）の設定が無効の場合、ARP インスペクションのログタイプはポート設定を参照します。「Check VLAN」（VLAN をチェックする）の設定が有効になっている場合、ARP インスペクションのログタイプは VLAN 設定を参照します。「Check VLAN」（VLAN をチェックする）に設定できる内容は以下のとおりです。

Enabled（有効）：VLAN 動作のチェックを有効にします。

Disabled（無効）：VLAN 動作のチェックを無効にします。

Log Type（ログタイプ）：
特定のポートのグローバルモードとポートモードのみが有効で、「Check VLAN」（VLAN をチェックする）の設定が無効になっている場合、ARP インスペクションのログタイプはポート設定を参照します。ログタイプには、次の使用可能なタイプが 4 種類あります。

None（なし）：何も記録しません。
Deny（拒否）：拒否されたエントリーをログに記録します。
Permit（許可）：許可されたエントリーをログに記録します。
ALL（すべて）：すべてのエントリーを記録します。

■ボタン

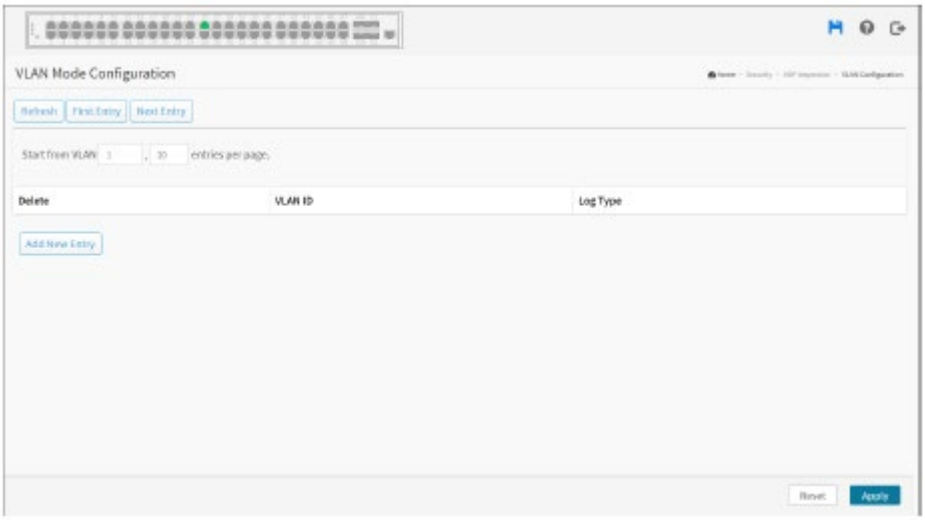
Apply（適用）：
クリックすると、変更内容を保存します。

Reset（リセット）：
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

Max Dynamic Clients（ダイナミックからスタティックへの変換）：
クリックすると、すべてのダイナミックエントリーがスタティックエントリーに変換されます。

VLAN の設定

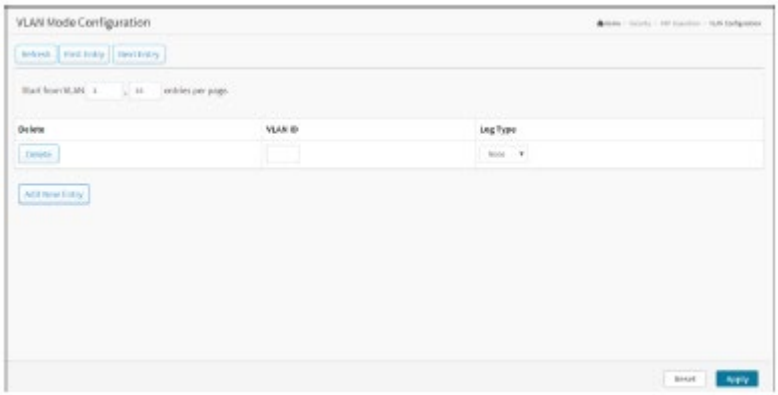
どの VLAN で ARP インスペクションを有効にするかを指定します。



Web インターフェース
Web インターフェースで VLAN モードの設定を行うには：
1. 「Security」（セキュリティ） ＞ 「ARP Inspection」（ARP インスペクション） ＞ 「VLAN

Configuration」(VLAN の設定)をクリックしてください。

2. 「Add New Entry」(新規登録)をクリックしてください。



3. 「VLAN ID」と「Log Type」(ログタイプ)を指定してください。
4. 「Apply」(適用)をクリックしてください。
5. エントリーを変更する場合は、「First Entry」(最初のエントリー)や「Next Entry」(次のエントリー)をクリックしてください。

■パラメーターの説明

Navigating the VLAN Configuration(VLAN 設定のナビゲート)

各ページには、VLAN テーブルから最大 9999 のエントリーが表示されます。デフォルトは 20 で、「entries per page」(ページあたりのエントリー数)の入力フィールドで選択されています。最初にアクセスすると、Web ページには、VLAN テーブルの先頭から最初の 20 エントリーが表示されます。最初に表示されるのは、VLAN テーブルで見つかった VLAN ID が最も小さいものです。

「VLAN」入力フィールドを使用すると、ユーザーは VLAN テーブルで開始点を選択できます。「Refresh」(更新)ボタンをクリックすると、表示されているテーブルが更新されます。これは、そのテーブルから、または、次に一致する VLAN テーブルに最も近いテーブルから始まります。「Next Entry」(次のエントリー)は、現在表示されている VLAN エントリーの次のエントリーを、次のルックアップの基準として使用します。最後に達すると、表示された表に警告メッセージが表示されます。このような場合には、「First Entry」(最初のエントリー)ボタンを使用して、最初からやり直してください。

VLAN Mode Configuration(VLAN モードの設定):

どの VLAN で ARP インスペクションを有効にするかを指定します。まず、ポートモードの設定 Web 画面でポート設定を有効にする必要があります。特定のポートでグローバルモードとポートモードの両方が有効になっている場合にのみ、この特定のポートで ARP インスペクションが有効になります。次に、VLAN モードの設定 Web 画面で検査する VLAN を指定できます。ログタイプは、VLAN 設定ごとに定義することもできます。可能なタイプは次のとおりです。

None（なし）：何も記録しません。
Deny（拒否）：拒否されたエントリーをログに記録します。
Permit（許可）：許可されたエントリーをログに記録します。
ALL（すべて）：すべてのエントリーを記録します。

■ボタン

Add New Entry（新規登録）：
ARP インスペクション VLAN テーブルに新規 VLAN を追加します。

Delete（削除）：
チェックを入れると、エントリーを削除します。これは、次回保存時に削除されます。

Apply（適用）：
クリックすると、変更内容を保存します。

Reset（リセット）：
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

First Entry（最初のエントリー）：
IPMC プロファイルアドレス設定の最初のエントリーからテーブルを更新します。

Next Entry（次のエントリー）：
現在表示されている最後のエントリーの後のエントリーから開始して、テーブルを更新します。

Refresh（更新）：
クリックすると、画面がすぐに更新されます。

スタティックテーブル

このセクションでは、スイッチのスタティック ARP インスペクションテーブルのパラメーターを設定する方法について説明します。スタティック ARP インスペクションテーブル設定を使用して、ARP エントリーを管理することができます。

Web インターフェース

Web インターフェースでスタティック ARP インスペクションテーブルを設定するには:

1. 「Security」(セキュリティ) ＞ 「ARP Inspection」(ARP インスペクション) ＞ 「Static Table」(スタティックテーブル)をクリックしてください。
2. 「Add New Entry」(新規登録)をクリックしてください。

3. エントリーに「Port」(ポート)、「VLAN ID」、「IP Address」(IP アドレス)、「MAC Address」(MAC アドレス)、および「IP Address」(IP アドレス)を指定してください。
4. 「Apply」(適用)をクリックしてください。

■パラメーターの説明

Port (ポート) :

この設定の論理ポートです。

VLAN ID:

この設定の VLAN ID です。

MAC address（MAC アドレス）:
ARP 要求パケットで許可される送信元 MAC アドレスです。

IP Address（IP アドレス）:
ARP 要求パケットで許可される送信元 IP アドレスです。

■ボタン

Add New Entry（新規登録）:
クリックすると、スタティック ARP インスペクションテーブルに新しいエントリーを追加します。

Delete（削除）:
チェックを入れると、エントリーを削除します。これは、次回保存時に削除されます。

Apply（適用）:
クリックすると、変更内容を保存します。

Reset（リセット）:
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

ダイナミックテーブル

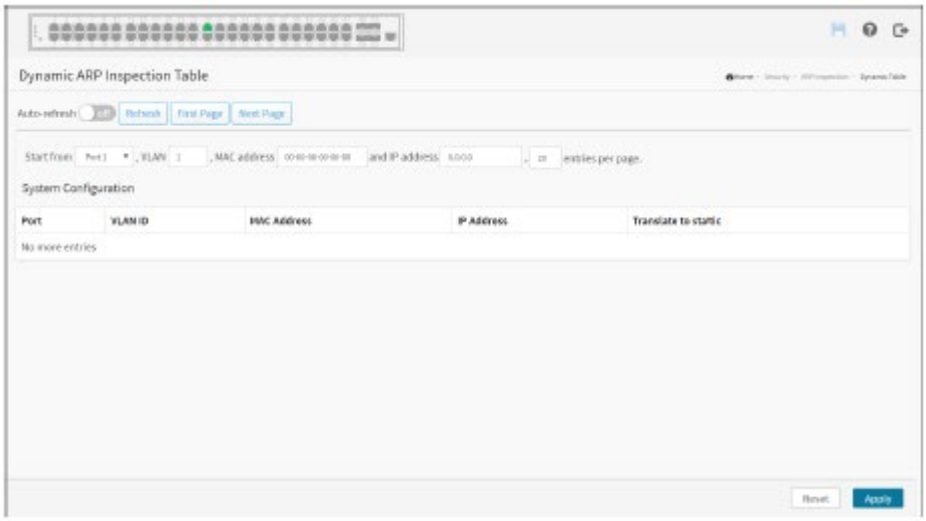
この画面には、ダイナミック ARP インスペクションテーブルのエントリーが表示されます。ダイナミック ARP インスペクションテーブルには、最大 256 個のエントリーが含まれており、ポート、VLAN ID、MAC アドレス、IP アドレスの順にソートされます。すべてのダイナミックエントリーは、DHCP スヌーピングから学習しています。

Navigating the ARP Inspection Table（ARP インスペクションテーブルのナビゲート）

各ページには、ダイナミック ARP インスペクションテーブルから最大 99 個のエントリーが表示されます。デフォルトは 20 で、「entries per page」（ページあたりのエントリー数）の入力フィールドで選択されます。最初にアクセスすると、ダイナミック ARP インスペクションテーブルの先頭から最初の 20 エントリーが Web ページに表示されます。

「Start from」*[ポートアドレス]*（*[ポートアドレス]*から開始）、「VLAN」、「MAC Address」（MAC アドレス）、および「IP address」（IP アドレス）の各入力フィールドを使用すると、ダイナミック ARP インスペクションテーブルの開始点を選択できます。「Refresh」（更新）ボタンをクリックすると、表示されているテーブルが更新されます。これは、そのテーブルから、または次に一致するダイナミック ARP インスペクションテーブルに最も近いテーブルから始まります。さらに、2 つの入力フィールドは（「Refresh」

（更新）ボタンをクリックすると)、最初に表示されたエントリーの値を想定し、同じ開始アドレスで継続的に更新することができます。「Next Page」（次のページ）は、現在表示されているテーブルの最後のエントリーを次の参照のベースとして使用します。最後に達すると、表示されたテーブルに「これ以上エントリーはありません」というテキストが表示されます。このような場合は、「First Page」（最初のページ）ボタンを使用して、最初からやり直してください。



Web インターフェース

Web インターフェースでダイナミック ARP インスペクションテーブルを設定するには:

1. 「Security」（セキュリティ） ＞ 「ARP Inspection」（ARP インスペクション） ＞ 「Dynamic Table」（ダイナミックテーブル）をクリックしてください。
2. 「Auto-refresh」（自動更新）にチェックを入れてください。
3. ポートの詳細統計情報を更新するには、「Refresh」（更新）をクリックしてください。
4. 画面を変更する場合は、「First Page」（最初のページ）や「Next Page」（次のページ）をクリックしてください。
5. 「Start from *port*」（*ポート*から開始）、「VLAN」、「MAC アドレス」（MAC アドレス）、「IP Address」（IP アドレス）、およびページごとのエントリーを指定してください。

■パラメーターの説明

ARP Inspection Table Columns（ARP インスペクションテーブルの列）

Port（ポート）:

エントリーを表示するスイッチのポート番号です。

VLAN ID:

ARP トラフィックが許可される VLAN ID です。

MAC Address（MAC アドレス）:
エントリーのユーザーMAC アドレスです。

IP Address（IP アドレス）:
エントリーのユーザーIP アドレスです。

Show entries（エントリーの表示）:
表示する項目の数を選択できます。

■ボタン

Auto-refresh（自動更新）:
画面を自動的に更新する場合は、このチェックボックスをONにしてください。自動更新は3秒間隔で行われます。

Refresh（更新）:
クリックするとページを更新します。

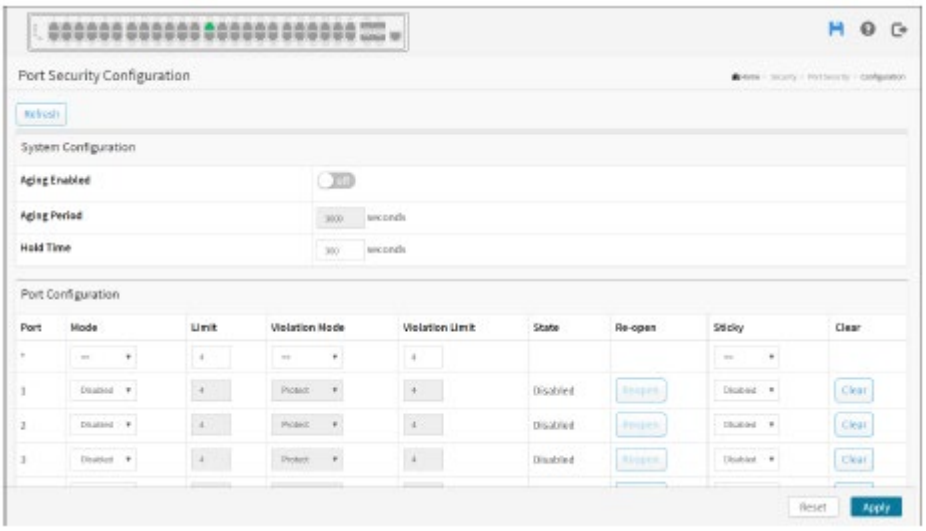
First Page（最初のページ）:
リストを更新し、最初のページに戻ります。

Next Page（次のページ）:
リストを更新し、次のページに進みます。

ポートセキュリティ

設定

このセクションでは、スイッチのポートセキュリティの設定を行います。ポートセキュリティ機能を使用すると、MAC アドレスを制限および識別することで、インターフェースへの入力を制限できます。



Web インターフェース

Web インターフェースでポートセキュリティを設定するには:

1. 「Security」(セキュリティ) ＞ 「Port Security」(ポートセキュリティ) ＞ 「Configuration」(設定)をクリックしてください。
2. エージング期間を有効にする場合は、「Aging Enabled」(エージング有効)をクリックしてください。
3. 各ポートに対して、「Mode」(モード)(有効、無効)、「Limit」(制限)、「Violation Mode」(違反モード)、「Violation Limit」(違反制限)を設定してください。
4. 「Apply」(適用)をクリックして設定を保存してください。
5. 設定を取り消す場合は、「Reset」(リセット)ボタンをクリックする必要があります。そうすると、以前に保存した値へと戻ります。

■パラメーターの説明

System Configuration(システム設定)

Aging Enabled(エージング有効):

このチェックボックスを ON にすると、エージング期間で説明されているように、セキュア MAC アドレ

スはエージングの対象になります。

Aging Period（エージング期間）：
「Aging Enabled」（エージング有効）を ON にすると、エージング期間がこの入力で制御されます。他のモジュールが MAC アドレスを保護するために基礎となる機能を使用している場合、エージング期間に対して他の要件がある可能性があります。他のモジュールが MAC アドレスを保護するために基礎となる機能を使用している場合、エージング期間に対して他の要件がある可能性があります。基礎となる機能は、エージングが有効になっているすべてのモジュールの要求されたエージング期間を短くします。
エージング期間には、10～10000000 秒の数値を設定できます（デフォルトは 3600 秒）。
エージングが必要な理由を理解するには、次のシナリオを考えてみます。エンドホストがサードパーティ製のスイッチまたはハブに接続されており、これが、ポートセキュリティが有効になっているこのスイッチのポートに接続されているとします。制限を超えない場合、エンドホストは転送を許可されます。ここで、エンドホストがログオフするか、電源が切断されるとします。エージングのためでなければ、エンドホストは引き続きこのスイッチのリソースを消費し、転送を許可されます。この状況を解消するには、エージングを有効にします。エージングを有効にした場合、エンドホストがセキュアになるとタイマーが開始されます。タイマーが切れると、スイッチはエンドホストからのフレームを探し始め、そのようなフレームが次のエージング期間内に見つからない場合、エンドホストは切断されたと見なされ、対応するリソースはスイッチ上で解放されます。

Hold Time（保留時間）：
保留時間（秒単位）は、MAC アドレスが制限に違反していることが判明した場合に、MAC テーブルに保持する MAC アドレスの長さを決定するために使用されます。有効な範囲は 10～10000000 秒で、デフォルトは 300 秒です。違反 MAC アドレスを MAC テーブルに保持する理由は、主に、同じ MAC アドレスが継続的な通知を生成しないようにするためです（違反カウントの通知が有効になっている場合）。

Port Configuration（ポート設定）
テーブルには、選択したスイッチの各ポートに 1 つの行と、次のような複数の列があります。

Port（ポート）：
以下の設定が適用されるポート番号です。

Mode（モード）：
このポートで制限コントロールを有効にするかどうかを制御します。制限コントロールを有効にするには、このモードとグローバルモードの両方を有効に設定する必要があります。他のモジュールは、

特定のポートで制限コントロールを有効にせずに、基盤となるポートセキュリティ機能を使用する可能性があることに注意してください。

Limit（制限）：
このポートで保護できる MAC アドレスの最大数です。この番号は 1024 を超えることはできません。制限を超えると、対応するアクションが実行されます。スイッチは MAC アドレスの総数で「生まれた」状態になり、ポートセキュリティが有効なポートで新しい MAC アドレスが検出されるたびに、すべてのポートがこのアドレスから取り出されます。すべてのポートが同じプールから引き出されるため、残りのポートがすでに使用可能なすべての MAC アドレスを使用している場合は、設定された最大値を付与できないことがあります。

Violation Mode（違反モード）：
制限に達すると、スイッチは次のいずれかのアクションを実行できます。

Protect（保護）：ポートで MAC アドレスの制限を超えて許可しないでください。ただし、それ以上のアクションは実行しません。

Restrict（制限）：制限に達すると、ポートの後続の MAC アドレスがカウントされ、違反としてマークされます。このような MAC アドレスは、保留時間が経過すると MAC テーブルから削除されます。最大違反制限 MAC アドレスは、いつでも違反としてマークできます。

Shutdown（シャットダウン）：制限に達すると、追加の MAC アドレスが 1 つ追加され、ポートがシャットダウンされます。これは、すべてのセキュア MAC アドレスがポートから削除され、新しいアドレスは学習されないことを意味します。ポートを再度開くには、次の 3 つの方法があります。

1) 「Configuration」（設定）＞「Ports」（ポート）画面における「Configured」（設定済み）列で、最初にポートを無効にしてから、元のモードに戻します。
2) ポートのポートセキュリティ設定を変更します。
3) スイッチを起動します。

Violation Limit（違反制限）：
このポートで違反としてマークできる MAC アドレスの最大数です。この番号は 1023 を超えることはできません。デフォルトは 4 です。違反モードが制限の場合にのみ使用されます。

State（状態）：
この列には、制限コントロールの観点から見たポートの現在の状態が表示されます。この状態は、次の 4 つの値のいずれかをとります。

Disabled（無効）：制限コントロールは、グローバルに無効になるか、ポートで無効になります。

Ready（準備完了）：制限に達していません。これは、すべてのアクションに対して表示できま

す。

Limit Reached（制限に到達）：このポートで制限に達したことを示します。この状態は、アクションが「なし」または「トラップ」に設定されている場合にのみ表示できます。

Shutdown（シャットダウン）：制限コントロールモジュールによってポートがシャットダウンされたことを示します。この状態は、アクションが「シャットダウン」または「トラップ＆シャットダウン」に設定されている場合にのみ表示できます。

■ボタン

Apply（適用）：

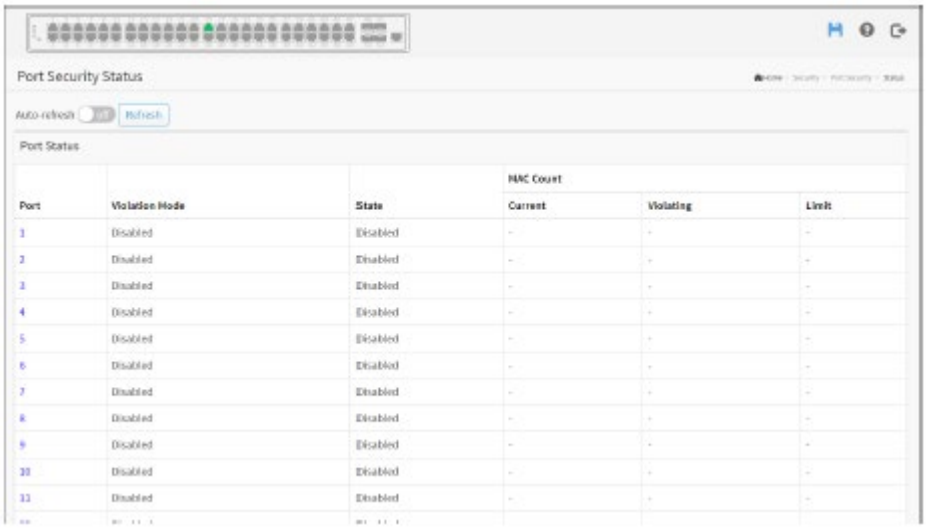
クリックすると、変更内容を保存します。

Reset（リセット）：

クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

状態

このセクションには、ポートセキュリティの状態が表示されます。ポートセキュリティは、直接設定されないモジュールです。設定は、他のモジュール（ユーザーモジュール）から間接的に行われます。ユーザーモジュールがポートのポートセキュリティを有効にすると、そのポートはソフトウェアベースの学習用に設定されます。このモードでは、未知のMACアドレスからのフレームがポートセキュリティモジュールに渡され、すべてのユーザーモジュールがこの新しいMACアドレスを転送するかブロックするかを確認します。MAC アドレスを転送状態に設定するには、有効になっているすべてのユーザーモジュールが、MACアドレスの転送を許可することに同意する必要があります。ブロックすることを選択したのが 1 つだけの場合、そのユーザーモジュールが別の方法を決定するまでブロックされます。このメニュー画面は 2 つのセクションに分かれています。1 つはユーザーモジュールの凡例で、もう 1 つは実際のポートの状態です。



Web インターフェース

Web インターフェースにポートセキュリティの状態を表示するには:

1. 「Security」(セキュリティ) ＞ 「Port Security」(ポートセキュリティ) ＞ 「Status」(状態)をクリックしてください。
2. 「Auto-refresh」(自動更新)にチェックを入れてください。
3. ポートの詳細統計情報を更新するには、「Refresh」(更新)をクリックしてください。
4. ポート番号をクリックすると、このポートの状態が表示されます。

■パラメーターの説明

Port(ポート):

状態が適用されるポート番号です。ポート番号をクリックすると、このポートの状態が表示されます。

Violation Mode(違反モード):

ポートに設定されている違反モードを表示します。次の 4 つの値のいずれかを使用できます。

Disabled(無効):ポートセキュリティは、このポートで管理上、有効になっていません。

Protect(保護):ポートセキュリティは、保護モードで管理上、有効になっています。

Restrict(制限):ポートセキュリティは、制限モードで管理上、有効になっています。

Shutdown(シャットダウン):ポートセキュリティは、シャットダウンモードで管理上、有効になっています。

State(状態):

ポートの現在の状態を表示します。次の 4 つの値のいずれかを使用できます。

Disabled(無効):現在、ポートセキュリティサービスを使用しているユーザーモジュールがありません。

Ready（準備完了）：ポートセキュリティサービスは、少なくとも 1 つのユーザーモジュールで使用中であり、未知の MAC アドレスからのフレームの到着を待機しています。

Limit Reached（制限に到達）：ポートセキュリティサービスは、少なくとも制限コントロールのユーザーモジュールによって有効化されています。このモジュールは、制限に達し、MAC アドレスを取り込む必要がないことを示しています。

Shutdown（シャットダウン）：ポートセキュリティサービスは、少なくとも制限コントロールのユーザーモジュールによって有効化されており、そのモジュールは制限を超えていることを示しています。MAC アドレスは、制限コントロールの設定 Web 画面で管理のため再アクセスされるまで、ポートで学習することはできません。

MAC Count (Current, Violating, Limit)（MAC カウント（現在、違反、制限））：
3 つの列は、現在学習されている MAC アドレスの数（転送およびブロック）、違反 MAC アドレスの数（制限モードでのみカウント）、およびポートで学習可能な MAC アドレスの最大数をそれぞれ示します。ポートでユーザーモジュールが有効になっていない場合、「Current」（現在）列にダッシュ（-）が表示されます。
ポートセキュリティが管理上有効になっていない場合、「Violating」（違反）および「Limit」（制限）の各列には、ダッシュ（-）が表示されます。

■ボタン

Auto-refresh（自動更新）：
画面を自動的に更新する場合は、このチェックボックスを ON にしてください。自動更新は 3 秒間隔で行われます。

Refresh（更新）：
クリックすると、画面がすぐに更新されます。

Port 1-52 Status（ポート 1～52 の状態）：
ポート番号をクリックすると、ポートの状態が個別に表示されます。

■パラメーターの説明

MAC Address & VLAN ID（MAC アドレスと VLAN ID）：
このポートに表示される MAC アドレスと VLAN ID です。MAC アドレスが学習されない場合は、「MAC アドレスが接続されていません」という 1 行が表示されます。

State（状態）：
対応する MAC アドレスがブロックされているか転送されているかを示します。ブロック状態では、トラフィックの送受信は許可されません。

Time of Addition（追加時刻）：
ポートでこの MAC アドレスが最初に検出された日時を示します。

Age/Hold（エージ/保留）：
少なくとも 1 つのユーザーモジュールがこの MAC アドレスをブロックすることを決定した場合、保留時間（秒単位）が経過するまでブロック状態のままになります。すべてのユーザーモジュールがこの MAC アドレスの転送を許可することを決定し、エージングが有効になっている場合、ポートセキュリティモジュールは、この MAC アドレスがトラフィックを転送しているかどうかを定期的にチェックします。経過時間（秒単位）が経過し、フレームが見つからない場合、MAC アドレスは MAC テーブルから削除されます。そうしないと、新しいエージング期間が開始されます。
エージングが無効になっている場合、またはユーザーモジュールが MAC アドレスを無期限に保持することを決定した場合、ダッシュ（-）が表示されます。

■ボタン

Auto-refresh（自動更新）：
画面を自動的に更新する場合は、このチェックボックスを ON にしてください。自動更新は 3 秒間隔で行われます。

Refresh（更新）：
クリックすると、画面がすぐに更新されます。

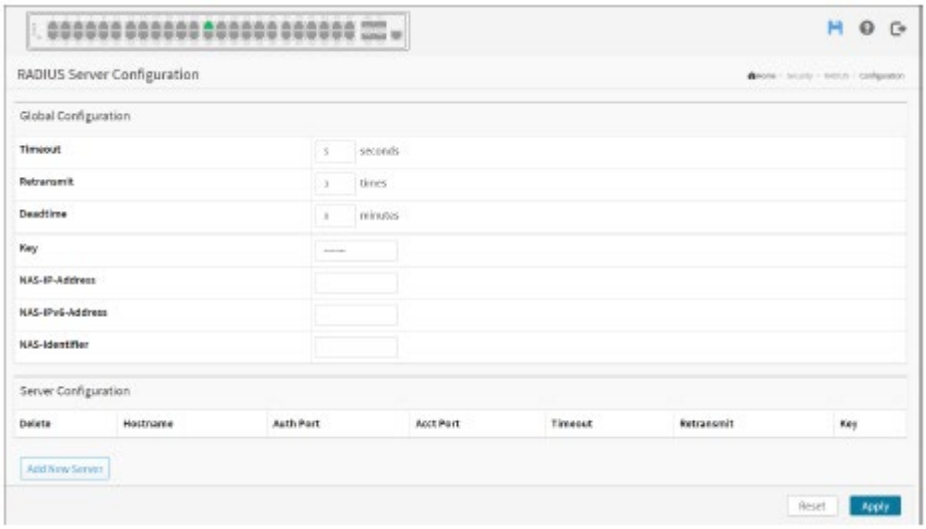
Clear（消去）：
クリックすると、MAC テーブルからこの特定の MAC アドレスを削除します。

Port 1（ポート 1）：
ポートセキュリティの状態を表示するポートを選択します。

Back（戻る）：
クリックすると、ポートセキュリティの状態に戻ります。

RADIUS

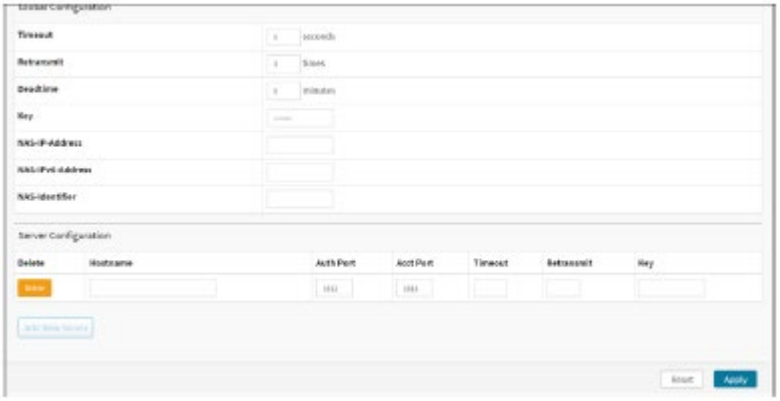
設定



Web インターフェース

Web インターフェースで RADIUS を設定するには:

1. 「Security」(セキュリティ) ＞ 「RADIUS」 ＞ 「Configuration」(設定)をクリックしてください。
2. 「Timeout」(タイムアウト)、「Retransmit」(再送信)、「Deadtime」(デッドタイム)、「Key」(キー)、「NAS-IP-Address」(NAS-IP アドレス)、「NAS IPv6-Address」(NAS-IPv6 アドレス)、「NAS-Identifier」(NAS 識別子)を設定してください。
3. 「Add New Entry」(新規登録)をクリックしてください。



4. 「Hostname」(ホスト名)、「Auth Port」(認証用ポート)、「Acct Port」(アカウンティング用ポート)、「Timeout」(タイムアウト)、「Retransmit」(再送信)、「Key」(キー)を設定してください。

5. 「Apply」(適用)をクリックして設定を保存してください。
6. 設定を取り消す場合は、「Reset」(リセット)ボタンをクリックする必要があります。そうすると、以前に保存した値へと戻ります。

■パラメーターの説明

Global Configuration(グローバル設定)

これらの設定は、すべての RADIUS サーバーで共通です。

Timeout(タイムアウト):
タイムアウトは、RADIUS サーバーからの応答を待ってから要求を再送信するまでの秒数です(範囲は 1～1000)。

Retransmit(再送信):
再送信は、1～1000 の範囲で、応答していないサーバーに RADIUS 要求が再送信される回数です。最後の再送信後にサーバーが応答しなかった場合は、デッド状態であると見なされます。

Deadtime(デッドタイム):
デッドタイムは、0～1440 分の数値に設定される番号です。これは、スイッチが以前の要求に応答番号なかったサーバーに新しい要求を送信しない時間です。これにより、スイッチは、すでにデッド状態と判定されているサーバーに継続的に接続しようとするのを停止します。デッドタイムを 0(ゼロ)より大きい値に設定すると、この機能が有効になりますが、複数のサーバーが設定されている場合に限ります。

Key(キー):
RADIUS サーバーとスイッチ間で共有される秘密鍵(最大 63 文字)です。

NAS-IP-Address(NAS-IP アドレス):
RADIUS アクセス要求パケットのアトリビュート 4 として使用される IPv4 アドレスです。この項目を空白のままにすると、発信インターフェースの IP アドレスが使用されます。

NAS-IPv6-Address(NAS-IPv6 アドレス):
RADIUS アクセス要求パケットのアトリビュート 95 として使用される IPv6 アドレスです。この項目を空白のままにすると、発信インターフェースの IP アドレスが使用されます。

NAS-Identifier(NAS 識別子):
RADIUS アクセス要求パケットのアトリビュート 32 として使用される識別子(最大 255 文字)です。こ

の項目を空白のままにすると、NAS 識別子はパケットに含まれません。

Server Configuration（サーバーの設定）

このテーブルには、RADIUS サーバーごとに 1 つの行と、次のような多数の列があります。

Hostname（ホスト名）：
RADIUS サーバーの IP アドレスまたはホスト名です。

Auth Port（認証用ポート）：
RADIUS サーバーで認証に使用する UDP ポートです。

Acct Port（アカウンティング用ポート）：
アカウンティングに RADIUS サーバーで使用する UDP ポートです。

Timeout（タイムアウト）：
このオプション設定は、グローバルタイムアウト値をオーバーライドします。空白のままにすると、グローバルタイムアウト値が使用されます。

Retransmit（再送信）：
このオプション設定は、グローバル再送信値をオーバーライドします。空白のままにすると、グローバル再送信値が使用されます。

Key（キー）：
このオプション設定は、グローバルキーをオーバーライドします。空白のままにすると、グローバルキーが使用されます。

■ボタン

Delete（削除）：
RADIUS サーバーのエントリーを削除するには、このチェックボックスを ON にしてください。エントリーは次回の保存時に削除されます。

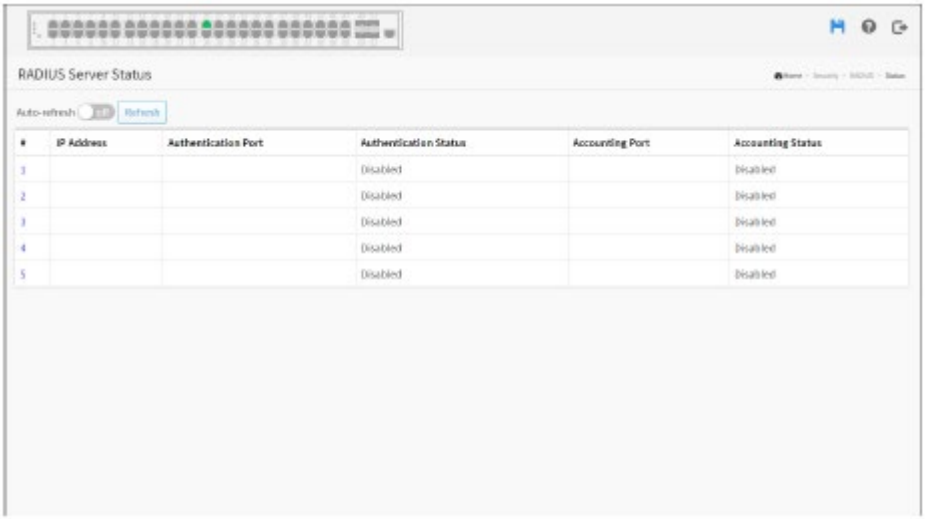
Add New Entry（新規登録）：
クリックすると、新しい RADIUS サーバーを追加します。空の行がテーブルに追加され、RADIUS サーバーを必要に応じて設定できます。最大 5 台のサーバーがサポートされます。このボタンを使用すると、新しいサーバーの追加を元に戻すことができます。

Apply（適用）：
クリックすると、変更内容を保存します。

Reset（リセット）：
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

状態

このセクションでは、RADIUS 認証およびアカウンティングサーバーの状態の概要/詳細を示し、機能が動作可能であることを確認します。



Web インターフェース
Web インターフェースに RADIUS の状態を表示するには：
1. 「Security」（セキュリティ） ＞ 「RADIUS」 ＞ 「Status」（状態）をクリックしてください。
2. 特定の RADIUS の詳細統計を表示するには、サーバーを選択してください。

■パラメーターの説明

#：
RADIUS サーバー番号です。クリックすると、このサーバーの詳細な統計情報に移動します。

IP Address（IP アドレス）：
このサーバーの IP アドレスと UDP ポート番号です（<*IP アドレス*>:<*UDP ポート*>の形式で表記）。

Authentication Port（認証用ポート）：
認証用の UDP ポート番号です。

Authentication Status（認証の状態）:
サーバーの現在の状態です。

Disabled（無効）: サーバーは無効です。

Not Ready（準備中）: サーバーは有効になっていますが、IP 通信はまだ稼働していません。

Ready（準備完了）: サーバーが有効で、IP 通信が稼働中にあり、なおかつ、RADIUS モジュールがアクセス試行を受け入れる準備ができています。

Dead (*X* seconds left)（デッド（残り X 秒））: このサーバーへのアクセスが試行されましたが、設定されたタイムアウト内に応答しませんでした。サーバーは一時的に無効にされていますが、デッドタイムが期限切れになると再び有効になります。括弧で囲まれて表示される秒数は、この現象が発生するまでの時間を表します。この状態には、複数のサーバーが有効になっている場合にのみアクセスできます。

Accounting Port（アカウンティング用ポート）:
アカウンティング用の UDP ポート番号です。

Accounting Status（アカウンティングの状態）:
サーバーの現在の状態です。このフィールドは次のいずれかの値をとります。

Disabled（無効）: サーバーは無効です。

Not Ready（準備中）: サーバーは有効になっていますが、IP 通信はまだ稼働していません。

Ready（準備完了）: サーバーが有効で、IP 通信が稼働中にあり、なおかつ、RADIUS モジュールがアクセス試行を受け入れる準備ができています。

Dead (*X* seconds left)（デッド（残り X 秒））: このサーバーへのアクセスが試行されましたが、設定されたタイムアウト内に応答しませんでした。サーバーは一時的に無効にされていますが、デッドタイムが期限切れになると再び有効になります。括弧で囲まれて表示される秒数は、この現象が発生するまでの時間を表します。この状態には、複数のサーバーが有効になっている場合にのみアクセスできます。

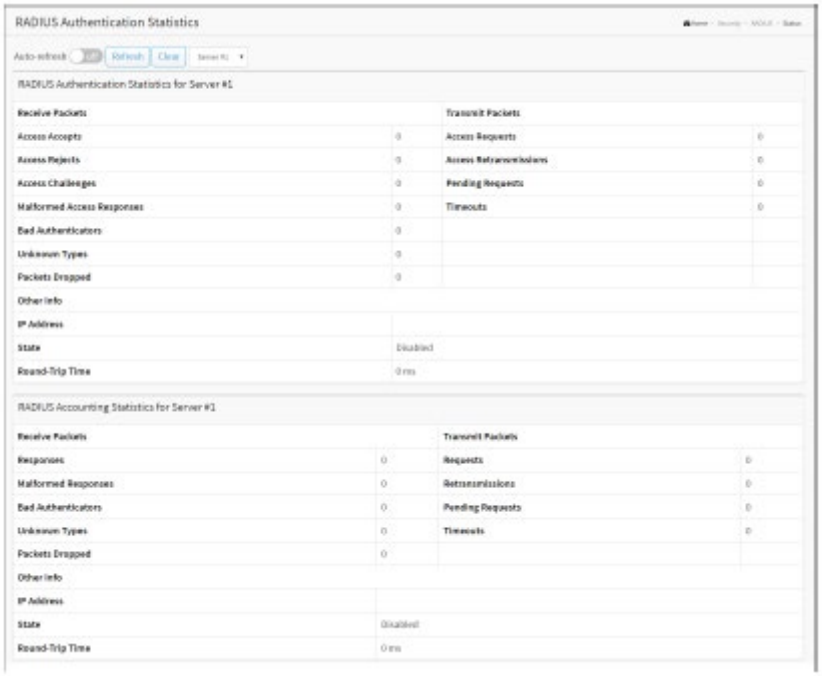
■ボタン

Auto-refresh（自動更新）:
画面を自動的に更新する場合は、このチェックボックスを ON にしてください。自動更新は 3 秒間隔で行われます。

Refresh（更新）:

クリックすると、画面がすぐに更新されます。

Port 1-52 Status（ポート 1～52 の状態）：
ポート番号をクリックすると、ポートが個別に表示されます。



■パラメーターの説明

server（サーバー）：
RADIUS を表示するサーバーを選択できます。

RADIUS Authentication Statistics for Server #1（サーバーの RADIUS 認証統計#1）
統計情報は、RFC4668-RADIUS 認証クライアント MIB で指定されたものに近いものにマップされます。
詳細を表示するバックエンドサーバーを切り替えるには、サーバーの選択ボックスを使用してください。

Access Accepts（アクセス許可）：
サーバーから受信した RADIUS Access-Accept パケット（有効または無効）の数です。

Access Rejects（アクセス拒否）：
サーバーから受信した RADIUS Access-Reject パケット（有効または無効）の数です。

Access Challenges（アクセスチャレンジ）：
サーバーから受信した RADIUSAccess Challenge パケット（有効または無効）の数です。

Malformed Access Responses（不正な形式のアクセス応答）：
サーバーから受信した不正な形式の RADIUS Access-Response パケットの数です。不正な形式のパケットには、無効な長さのパケットが含まれます。不正なオーセンティケーターまたはメッセージオーセンティケーター属性または不明なタイプは、不正な形式のアクセス応答に含まれません。

Bad Authenticators（不正なオーセンティケーター）：
サーバーから受信した無効なオーセンティケーターまたはメッセージオーセンティケーター属性を含む RADIUS Access-Response パケットの数です。

Unknown Types（不明なタイプ）：
認証ポートでサーバーから不明なタイプで受信され、破棄された RADIUS パケットの数です。

Packets Dropped（破棄されたパケット）：
認証ポートでサーバーから受信し、その他の理由で破棄された RADIUS パケットの数です。

Access Requests（アクセス要求）：
サーバーに送信された RADIUS アクセス要求パケットの数です。これには再送信は含まれません。

Access Retransmissions（アクセス再送信）：
RADIUS 認証サーバーに再送信された RADIUS アクセス要求パケットの数です。

Pending Requests（保留中のリクエスト）：
まだタイムアウトしていない、または応答を受信していない、サーバー宛ての RADIUS アクセス要求パケットの数です。この変数は、Access-Request が送られると増分し、AccessAccept、Access-Reject、Access-Challenge、Timeout、または Retransmission を受信すると減算されます。

Timeouts（タイムアウト）：
サーバーへの認証タイムアウトの数です。タイムアウト後、クライアントは同じサーバーへの再試行、別のサーバーへの送信、または放棄を行うことができます。同じ RADIUS サーバーへの再試行は、再送信およびタイムアウトとしてカウントされます。別のサーバーへの送信は、タイムアウトと同様に要求としてカウントされます。

IP Address（IP アドレス）：

問題になっている認証サーバーの IP アドレスと UDP ポートです。

Status（状態）:
サーバーの状態を表示します。以下のいずれかの値をとります。

Disabled（無効）:選択したサーバーが無効になります。

Not Ready（準備中）:サーバーは有効になっていますが、IP 通信はまだ稼働していません。

Ready（準備完了）:サーバーが有効で、IP 通信が稼働中にあり、なおかつ、RADIUS モジュールがアクセス試行を受け入れる準備ができています。

Dead（*X* seconds left）（デッド（残り X 秒））:このサーバーへのアクセスが試行されましたが、設定されたタイムアウト内に応答しませんでした。サーバーは一時的に無効にされていますが、デッドタイムが期限切れになると再び有効になります。括弧で囲まれて表示される秒数は、この現象が発生するまでの時間を表します。この状態には、複数のサーバーが有効になっている場合にのみアクセスできます。

Round-Trip Time（ラウンドトリップ時間）:
直近の AccessReply/Access-Challenge と、RADIUS 認証サーバーから一致した Access-Request との間の時間間隔（ミリ秒単位）です。この測定の粒度は 100 ミリ秒です。値 0ms は、サーバーとのラウンドトリップ通信がまだ行われていないことを示します。

RADIUS Accounting Statistics for Server #1（サーバーの RADIUS アカウンティング統計#1）
統計は、RFC4670-RADIUS Accounting Client MIB で指定されたものに近いものにマップされます。詳細を表示するバックエンドサーバーを切り替えるには、サーバーの選択ボックスを使用してください。

Responses（応答）:
サーバーから受信した RADIUS パケット（有効または無効）の数です。

Malformed Responses（不正な形式の応答）:
サーバーから受信した不正な形式の RADIUS パケットの数です。不正な形式のパケットには、無効な長さのパケットが含まれます。不正なオーセンティケーターまたは不明なタイプは、不正な形式のアクセス応答に含まれません。

Bad Authenticators（不正なオーセンティケーター）:
サーバーから受信した無効なオーセンティケーターを含む RADIUS パケットの数です。

Unknown Types（不明なタイプ）:

アカウンティングポートでサーバーから受信した不明なタイプの RADIUS パケットの数です。

Packets Dropped（破棄されたパケット）：
アカウンティングポート上のサーバーから受信し、何らかの理由で破棄された RADIUS パケットの数です。

Requests（要求）：
サーバーに送信された RADIUS パケットの数です。これには再送信は含まれません。

Retransmissions（再送信）：
RADIUS アカウンティングサーバーに再送信された RADIUS パケットの数です。

Pending Requests（保留中のリクエスト）：
まだタイムアウトしていない、または応答を受信していない、サーバー宛ての RADIUS パケットの数です。この変数は、要求が送信されると増分され、応答、タイムアウト、または再送を受信すると、減算されます。

Timeouts（タイムアウト）：
サーバーに対するアカウンティングタイムアウトの数です。タイムアウト後、クライアントは同じサーバーへの再試行、別のサーバーへの送信、または放棄を行うことができます。同じ RADIUS サーバーへの再試行は、再送信およびタイムアウトとしてカウントされます。別のサーバーへの送信は、タイムアウトと同様に要求としてカウントされます。

IP Address（IP アドレス）：
問題のアカウンティングサーバーの IP アドレスと UDP ポートです。

Status（状態）：
サーバーの状態を表示します。以下のいずれかの値をとります。

Disabled（無効）：選択したサーバーが無効になります。

Not Ready（準備中）：サーバーは有効になっていますが、IP 通信はまだ稼働していません。

Ready（準備完了）：サーバーが有効で、IP 通信が稼働中にあり、なおかつ、RADIUS モジュールがアカウンティングの試行を受け入れる準備ができています。

Dead (*X* seconds left)（デッド（残り X 秒））：このサーバーに対してアカウンティングが試行されましたが、設定されたタイムアウト内に応答しませんでした。サーバーは一時的に無効にされていますが、デッドタイムが期限切れになると再び有効になります。括弧で囲まれて表示される秒数は、この現象が発生するまでの時間を表します。この状態には、複数のサーバーが有

効になっている場合にのみアクセスできます。

Round-Trip Time（ラウンドトリップ時間）：
直近の応答と、それに一致した RADIUS アカウンティングサーバーからの要求との間の時間間隔（ミリ秒単位）です。この測定の粒度は 100 ミリ秒です。値 0ms は、サーバーとのラウンドトリップ通信がまだ行われていないことを示します。

■ボタン

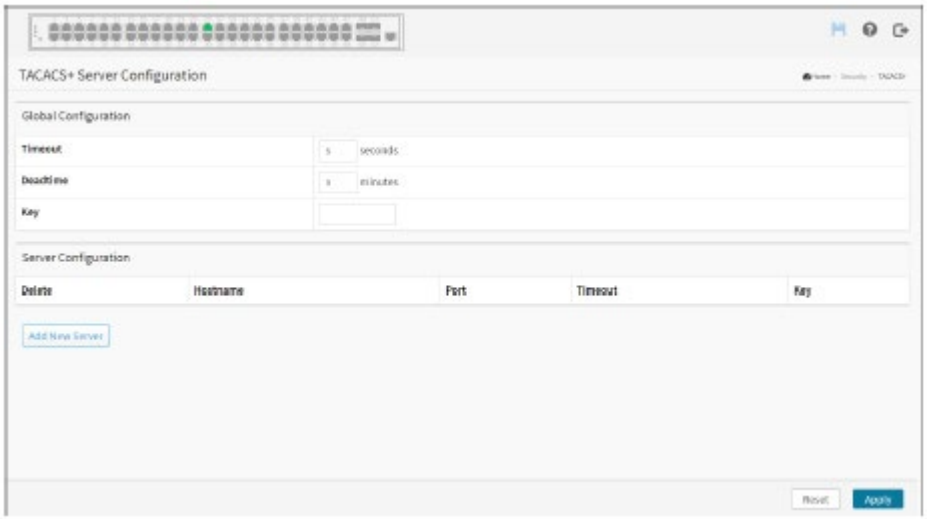
Auto-refresh（自動更新）：
画面を自動的に更新する場合は、このチェックボックスを ON にしてください。自動更新は 3 秒間隔で行われます。

Refresh（更新）：
クリックすると、画面がすぐに更新されます。

Clear（消去）：
選択したサーバーのカウンターを消去します。「Pending Requests」（保留中の要求）カウンターは、この操作によってクリアされません。

TACACS+

この画面では、最大 5 台の TACACS+サーバーを設定できます。



Web インターフェース

Web インターフェースで TACACS+サーバーを設定するには:

1. 「Security」(セキュリティ) ＞ 「TACACS+」をクリックしてください。
2. 「Add New Entry」(新規登録)をクリックしてください。

3. 「Timeout」(タイムアウト)、「Deadtime」(デッドタイム)、「Key」(キー)を指定してください。
4. サーバーの「Hostname」(ホスト名)、「Port」(ポート)、「Timeout」(タイムアウト)、「Key」(キー)を指定してください。
5. 「Apply」(適用)をクリックしてください。

■パラメーターの説明

Global Configuration(グローバル設定)

これらの設定は、すべての TACACS+サーバーで共通です。

Timeout(タイムアウト):

タイムアウトは、TACACS+サーバーからの応答がデッド状態と見なされるまで待機する秒数（1～1000）です。

Deadtime（デッドタイム）：
デッドタイムは、0～1440 分の数値に設定される番号です。これは、スイッチが以前の要求に応答番号なかったサーバーに新しい要求を送信しない時間です。これにより、スイッチは、すでにデッド状態と判定されているサーバーに継続的に接続しようとするのを停止します。デッドタイムを 0（ゼロ）より大きい値に設定すると、この機能が有効になりますが、複数のサーバーが設定されている場合に限ります。

Key（キー）：
TACACS+サーバーとスイッチ間で共有される秘密鍵（最大 63 文字）です。

Server Configuration（サーバーの設定）
このテーブルには、TACACS+サーバーごとに 1 つの行と、次のような複数の列があります。

Delete（削除）：
TACACS+サーバーのエントリーを削除するには、このチェックボックスを ON にしてください。エントリーは次回の保存時に削除されます。

Hostname（ホスト名）：
TACACS+サーバーの IP アドレスまたはホスト名です。

Port（ポート）：
認証に TACACS+サーバーで使用する TCP ポートです。

Timeout（タイムアウト）：
このオプション設定は、グローバルタイムアウト値をオーバーライドします。空白のままにすると、グローバルタイムアウト値が使用されます。

Key（キー）：
このオプション設定は、グローバルキーをオーバーライドします。空白のままにすると、グローバルキーが使用されます。

■ボタン

Delete（削除）：

このボタンを使用すると、新しいサーバーの追加を元に戻すことができます。

Add New Server（新規サーバーの追加）：
クリックすると、新しい TACACS+サーバーを追加します。空の行がテーブルに追加され、必要に応じて TACACS+サーバーを設定できます。最大 5 台のサーバーがサポートされます。

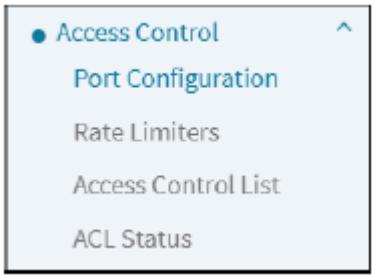
Apply（適用）：
クリックすると、変更内容を保存します。

Reset（リセット）：
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

第 13 章
アクセス制御

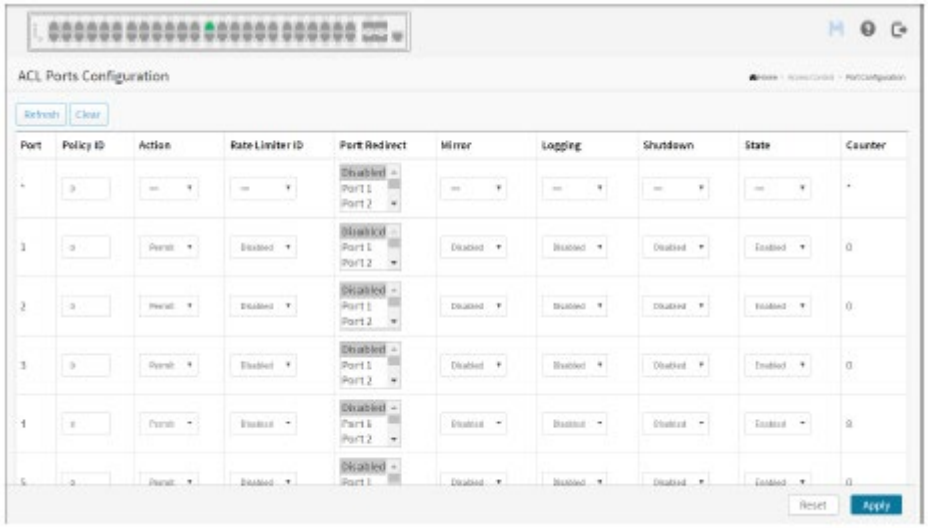
概要

メニューは以下のとおりです。



ポート設定

各スイッチにおけるポートの ACL パラメーター(ACE)を設定します。これらのパラメーターは、フレームが特定の ACE に一致しない限り、ポートで受信したフレームに影響します。



Web インターフェース

Web インターフェースでユーザーを設定するには:

1. 「Access Control」(アクセス制御) ＞ 「Port Configuration」(ポート設定)をクリックしてください。
2. 特定のパラメーター値をスクロールし、ポートの ACL 設定に対して正しい値を選択してください。
3. 「Apply」(適用)をクリックして設定を保存してください。
4. 設定を取り消す場合は、「Reset」(リセット)ボタンをクリックする必要があります。そうすると、以前に保存した値へと戻ります。
5. 設定が完了すると、ポートのカウンターが表示されます。そうしたら、「Update」(更新)をクリックしてカウンターを更新するか、「Clear」(消去)をクリックして情報をクリアしてください。

■パラメーターの説明

Port(ポート):

同じ行に含まれる設定の論理ポートです。

Policy ID(ポリシーID):

このポートに適用するポリシーを選択します。指定できる値は 1～8 です。デフォルト値は 1 です。

Action（アクション）：
転送を許可するか（「Permit」（許可））、拒否するか（「Deny」（拒否））を選択してください。デフォルト値は「Permit」（許可）です。

Rate Limiter ID（レートリミッターID）：
このポートに適用するレートリミッターを選択してください。指定できる値は「Disabled」（無効）、または値 1～16 です。

Port Redirect（ポートリダイレクト）：
リダイレクトするポートフレームを選択してください。許可される値は「Disabled」（無効）、または特定のポート番号です。アクションが許可されている場合は設定できません。デフォルト値は「Disabled」（無効）です。

Mirror（ミラー）：
このポートのミラー動作を指定してください。許可される値は次のとおりです。
Enabled（有効）：ポートで受信したフレームはミラーリングされます。
Disabled（無効）：ポートで受信したフレームはミラーリングされません。
デフォルト値は「Disabled」（無効）です。

Logging（ロギング）：
このポートのロギング動作を指定してください。許可される値は次のとおりです。
Enabled（有効）：ポートで受信したフレームはシステムログに保存されます。
Disabled（無効）：ポートで受信したフレームはログに記録されません。
デフォルト値は「Disabled」（無効）です。システムログのメモリサイズとロギングレートは制限されていることに注意してください。

Shutdown（シャットダウン）：
このポートのシャットダウン動作を指定してください。許可される値は次のとおりです。
Enabled（有効）：ポートでフレームが受信されると、ポートは無効になります。
Disabled（無効）：ポートシャットダウンは無効です。
デフォルト値は「Disabled」（無効）です。

State（状態）：
このポートの状態を指定してください。指定できる値は次のとおりです。
Enabled（有効）：ACL ユーザーモジュールの揮発性ポート設定を変更してポートを再オープ

ンします。

Disabled（無効）：ACL ユーザーモジュールの揮発性ポート設定を変更してポートを閉じます。デフォルト値は「Enabled」（有効）です。

Counter（カウンター）：
この ACE に一致するフレーム数をカウントします。

■ボタン

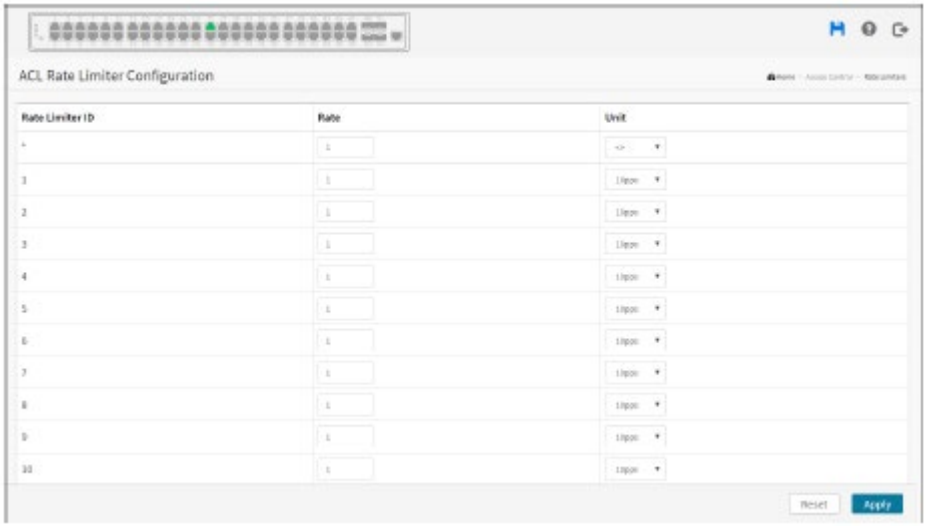
Refresh、Clear（更新、クリア）：
これらをクリックして ACL ポート設定を更新するか、手動でクリアすることができます。

Apply（適用）：
クリックすると、変更内容を保存します。

Reset（リセット）：
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

レートリミッター

このセクションでは、スイッチの ACL レートリミッターに関するパラメーターの設定方法について説明します。レートリミッターのレベルは 1～16 で、ユーザーがレートリミッターの値とユニットを pps で設定できます。



Web インターフェース

Web インターフェースで ACL レートリミッターを設定するには:

1. 「Access Control」(アクセス制御) ＞ 「Rate Limiters」(レートリミッター)をクリックしてください。
2. 「Rate」(レート)と「Unit」(単位)の各フィールドを指定してください。
3. 「Apply」(適用)をクリックして設定を保存してください。
4. 設定を取り消す場合は、「Reset」(リセット)ボタンをクリックする必要があります。そうすると、以前に保存した値へと戻ります。

■パラメーターの説明

Rate Limiter ID(レートリミッターID):

同じ行に含まれる設定のレートリミッターID で、その範囲は 1～16 です。

Rate(レート):

有効なレートは、0、10、20、30…5000000(pps)、または 0、25、50、75…10000000(kbps)です。

Unit(単位):

レート単位を指定してください。指定できる値は次のとおりです。

10pps：パケット/秒

25kbp：キロビット/秒

■ボタン

Apply（適用）：

クリックすると、変更内容を保存します。

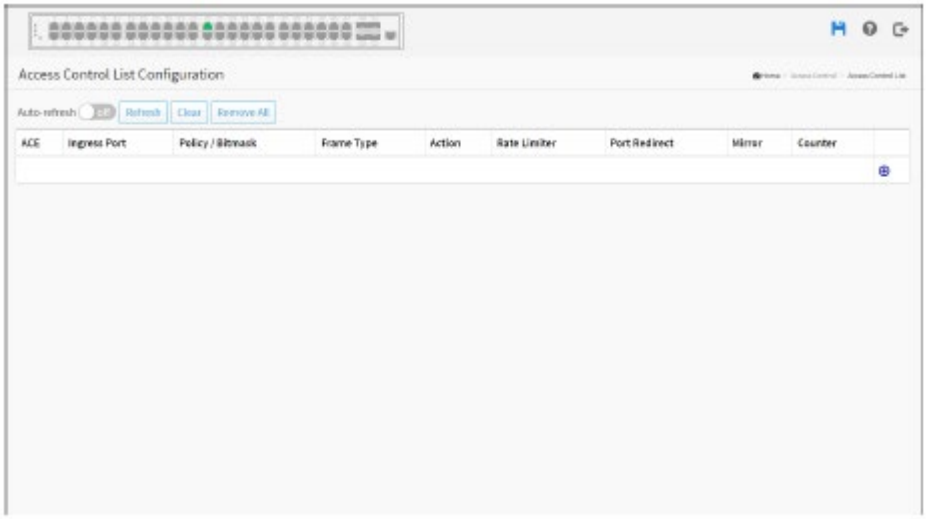
Reset（リセット）：

クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

アクセス制御リスト

この画面には、このスイッチで定義された ACE で構成されるアクセス制御リスト（ACL）が表示されます。各行は、定義されている ACE を示します。各スイッチの ACE の最大数は 512 です。

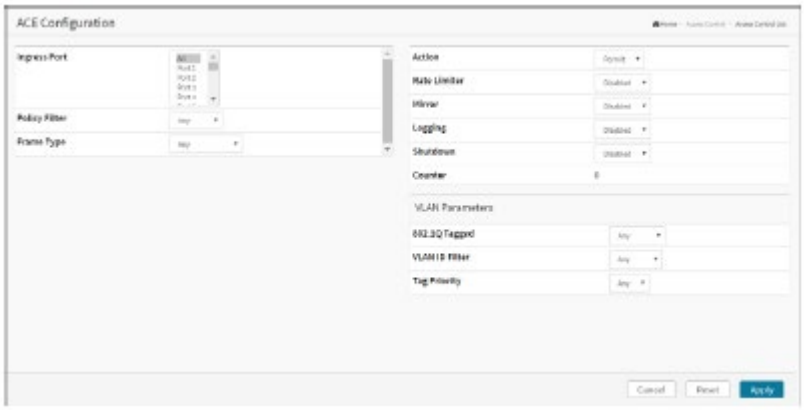
リストに新しい ACE を追加するには、最下位のプラス記号をクリックします。内部プロトコルに使用される予約済み ACE は、編集または削除できず、順序シーケンスも変更できません。また、優先順位は最も高くなります。



Web インターフェース

Web インターフェースでアクセス制御リストを設定するには：

1. 「Access Control」（アクセス制御） ＞ 「Access Control List」（アクセス制御リスト）をクリックしてください。
2. ボタンをクリックして新しい ACL を追加するか、他の ACL 変更ボタンを使用して編集アクションを指定してください（つまり、リスト内のエントリーの相対位置を編集、削除、または移動するということです）。



3. ACE のパラメーターを指定してください。
4. 「Apply」(適用)をクリックして設定を保存してください。
5. 設定を取り消す場合は、「Reset」(リセット)ボタンをクリックする必要があります。そうすると、以前に保存した値へと戻ります。
6. 「ACE Configuration」(ACE の設定)画面でエントリーを編集する場合、表示される項目は、「Frame Type」(フレームタイプ)や「IP Protocol Type」(IP プロトコルタイプ)などのさまざまな選択項目に依存することに注意してください。
7. このルールに一致する関連基準を指定し、ルールが一致したときに実行するアクション(レートリミッター、ポートコピー、ログ、シャットダウンなど)を設定してください。

■パラメーターの説明

ACE:

ACE ID を示します。

Ingress Port(イングレスポート):

ACE のイングレスポートを示します。可能な値は次のとおりです。

Any(任意):ACE は任意のイングレスポートに一致します。

Policy(ポリシー):ACE は、特定のポリシーでイングレスポートと一致します。

Port(ポート):ACE は特定のイングレスポートと一致します。

Policy / Bitmask(ポリシー/ビットマスク):

ACE のポリシー番号とビットマスクを示します。

Frame Type(フレームタイプ):

ACE のフレームタイプを示します。可能な値は次のとおりです。

Any(任意):ACE は任意のフレームタイプに一致します。

EType(E タイプ):ACE はイーサネットタイプフレームと一致します。イーサネットタイプがベー

スとなった ACE は、IP および ARP フレームと一致しません。
ARP：ACE は ARP/RARP フレームと一致します。
IPv4：ACE はすべての IPv4 フレームに一致します。
IPv4/ICMP：ACE は、ICMP プロトコルを使用して IPv4 フレームと一致します。
IPv4/UDP：ACE は UDP プロトコルを使用して IPv4 フレームと一致します。
IPv4/TCP：ACE は TCP プロトコルを使用して IPv4 フレームと一致します。
IPv4/Other（IPv4/その他）：ACE は、ICMP/UDP/TCP ではない IPv4 フレームと一致します。
IPv6：ACE はすべての IPv6 標準フレームと一致します。

Action（アクション）：
ACE の転送アクションを示します。
Permit（許可）：ACE に一致するフレームが転送され、学習される可能性があります。
Deny（拒否）：ACE に一致するフレームが破棄されます。
Filter（フィルター）：ACE に一致するフレームがフィルタリングされます。

Rate Limiter（レートリミッター）：
ACE のレートリミッター番号を示します。指定できる範囲は 1～16 です。「Disabled」（無効）と表示されている場合は、レートリミッターの操作が無効となっています。

Port Redirect（ポートリダイレクト）：
ACE のポートリダイレクト操作を示します。ACE に一致するフレームは、ポート番号にリダイレクトされます。許可される値は、「Disabled」（無効）または特定のポート番号です。「Disabled」（無効）と表示されている場合は、ポートリダイレクト操作が無効となっています。

Mirror（ミラー）：
このポートのミラー動作を指定してください。ACE に一致するフレームは、宛先ミラーポートにミラーリングされます。指定できる値は次のとおりです。
Enabled（有効）：ポートで受信したフレームはミラーリングされます。
Disabled（無効）：ポートで受信したフレームはミラーリングされません。
デフォルト値は「Disabled」（無効）です。

Counter（カウンター）：
カウンターは、ACE がフレームによってヒットした回数を示します。

変更ボタン：
次のボタンを使用すると、テーブル内の各 ACE（アクセス制御のエントリー）を変更することができま

す。

 ： 現在の行の前に新しい ACE を挿入します。

 ： ACE 行を編集します。

 ： ACE をリストの上に移動します。

 ： ACE をリストの下に移動します。

 ： ACE を削除します。

 ： 最小のプラス記号は、ACE リストの下部に新しいエントリーを追加します。

ACE Configuration（ACE の設定）

ACE は、いくつかのパラメーターで構成されます。これらのパラメーターは、選択したフレームタイプによって異なります。最初に ACE のイングレスポートを選択し、次にフレームタイプを選択してください。選択したフレームタイプに応じて、表示されるパラメーターオプションが異なります。

この ACE にヒットするフレームは、ここで定義されている設定と一致します。

Ingress Port（イングレスポート）：

この ACE が適用されるイングレスポートを選択してください。

All（すべて）：ACE はすべてのポートに適用されます。

Port *n*（ポート *n*）：ACE はこのポート番号に適用されます。*n* はスイッチポートの番号です。

Policy Filter（ポリシーフィルター）：

この ACE のポリシー番号フィルターを指定してください。

Any（任意）：ポリシーフィルターが指定されていません。（ポリシーフィルターの状態は「don't-care」となります）

Specific（特定）：この ACE で特定のポリシーをフィルタリングする場合は、この値を選択してください。ポリシー値とビットマスクを入力するための 2 つの項目が表示されます。

Policy Value（ポリシー値）：

ポリシーフィルターで「Specific」（特定）を選択すると、特定のポリシー値を入力できます。指定できる範囲は 0～255 です。

Policy Bitmask（ポリシービットマスク）：

ポリシーフィルターに「Specific」（特定）を選択すると、特定のポリシービットマスクを入力できます。指定できる範囲は 0x00～0xff です。ビットマスクの使用法に注意してください。バイナリビット値が「0」の場合、このビットが「don't-care」であることを意味します。実際に一致するパターンは、

[policy_value&policy_bitmask]です。例えば、ポリシー値が 3 で、ポリシービットマスクが 0x10（ビット 0 が「don't-care」ビット）の場合、ポリシー2 と 3 がこのルールに適用されます。

Frame Type（フレームタイプ）：
この ACE のフレームタイプを選択してください。これらのフレームタイプは相互に排他的です。

Any（任意）：任意のフレームがこの ACE に一致します。

Ethernet Type（イーサネットタイプ）：この ACE に一致できるのは Ethernet Type フレームのみです。IEEE 802.3 は、Length/Type フィールド仕様の値が 10 進数で 1536 以上（16 進数で 0600 に等しい）であることを謳っています。

ARP：この ACE に一致できるのは ARP フレームのみです。ARP フレームがイーサネットタイプの ACE と一致しないことに注意してください。

IPv4：この ACE に一致できるのは IPv4 フレームのみです。IPv4 フレームがイーサネットタイプの ACE と一致しないことに注意してください。

IPv6：この ACE に一致できるのは IPv6 フレームのみです。IPv6 フレームがイーサネットタイプの ACE と一致しないことに注意してください。

Action（アクション）：
この ACE にヒットするフレームで実行するアクションを指定してください。

Permit（許可）：この ACE にヒットしたフレームには、ACE 操作の権限が付与されます。

Deny（拒否）：この ACE にヒットしたフレームが破棄されます。

Filter（フィルター）：ACE に一致するフレームがフィルタリングされます。

Rate Limiter（レートリミッター）：
基本単位でレートリミッターを設定してください。指定できる範囲は 1～16 です。「Disabled」（無効）は、レートリミッターの操作が無効であることを示します。

Port Redirect（ポートリダイレクト）：
ACE に到達したフレームは、ここで指定したポート番号にリダイレクトされます。レートリミッターはこれらのポートに影響を与えます。許可される範囲は、スイッチのポート番号の範囲と同じです。「Disabled」（無効）は、ポートリダイレクト操作が無効であることを示し、アクションが許可されている場合はポートリダイレクトの特定のポート番号を設定できません。

Mirror（ミラー）：
このポートのミラー動作を指定してください。ACE に一致するフレームは、宛先ミラーポートにミラーリングされます。レートリミッターは、ミラーポートのフレームには影響しません。指定できる値は次のとおりです。

Enabled（有効）：ポートで受信したフレームがミラーリングされます。

Disabled（無効）：ポートで受信したフレームはミラーリングされません。

デフォルト値は「Disabled」（無効）です。

Logging（ロギング）：

ACE のロギング動作を指定してください。ロギングメッセージには 4 バイトの CRC 情報が含まれていないことに注意してください。指定できる値は次のとおりです。

Enabled（有効）：ACE に一致するフレームはシステムログに保存されます。

Disabled（無効）：ACE に一致するフレームはログに記録されません。

注意： ロギング機能は、パケット長が 1518 未満（VLAN タグなし）で、システムログのメモリサイズとロギングレートが制限されている場合にのみ機能します。

Shutdown（シャットダウン）：

ACE のポートシャットダウン動作を指定してください。許可される値は次のとおりです。

Enabled（有効）：フレームが ACE に一致する場合、イングレスポートは無効になります。

Disabled(無効)：ACE でポート停止が無効になります。

注意： シャットダウン機能は、パケット長が 1518 未満（VLAN タグなし）の場合にのみ機能します。

Counter（カウンター）：

カウンターは、ACE がフレームによってヒットした回数を示します。

MAC Parameter（MAC パラメーター）

SMAC Filter（SMAC フィルター）：

（フレームタイプがイーサネットタイプ、または ARP の場合にのみ表示）この ACE のソース MAC フィルターを指定してください。

Any（任意）：SMAC フィルターが指定されていません。（SMAC フィルターの状態は「don't-care」）

Specific（特定）：特定の送信元 MAC アドレスをこの ACE でフィルタリングする場合は、この値を選択してください。SMAC 値を入力するためのフィールドが表示されます。

SMAC Value（SMAC 値）：

SMAC フィルターに「Specific」（特定）を選択した場合は、特定の送信元 MAC アドレスを入力することができます。有効な形式は、「*xx-xx-xx-xx-xx-xx*」、「*xx.xx.xx.xx.xx*」、「*xxxxxxxxxxxx*」のいずれかです（*xx* は 16 進数）。この ACE にヒットするフレームは、この SMAC 値と一致します。

DMAC Filter（DMAC フィルター）：

この ACE の宛先 MAC フィルターを指定してください。

Any（任意）：DMAC フィルターが指定されていません。（DMAC フィルターの状態は「don't-care」です）

MC：フレームはマルチキャストにする必要があります。

BC：フレームはブロードキャストにする必要があります。

UC：フレームはユニキャストにする必要があります。

Specific（特定）：この ACE で特定の宛先 MAC アドレスをフィルタリングする場合は、この値を選択してください。DMAC 値を入力するための項目が表示されます。

DMAC Value（DMAC 値）：

DMAC フィルターに「Specific」（特定）を選択した場合、特定の宛先 MAC アドレスを入力することができます。有効な形式は、「*xx-xx-xx-xx-xx-xx*」、「*xx.xx.xx.xx.xx*」、「*xxxxxxxxxxxx*」のいずれかです（xx は 16 進数）。この ACE にヒットしたフレームは、この DMAC 値と一致します。

VLAN Parameters（VLAN パラメーター）

802.1Q Tagged（802.1Q タグ付き）：

802.1Q タグに従ってフレームがアクションにヒットできるかどうかを指定してください。指定できる値は次のとおりです。

Any（任意）：任意の値を使用できます（don't-care）。

Enabled（有効）：タグ付きフレームのみです。

Disabled（無効）：タグなしフレームのみです。

デフォルト値は「Any」（任意）です。

VLAN ID Filter（VLAN ID フィルター）：

この ACE の VLAN ID フィルターを指定してください。

Any（任意）：VLAN ID フィルターが指定されていません。（VLAN ID フィルターの状態は「don't-care」）

Specific（特定）：この ACE で特定の VLAN ID をフィルタリングする場合は、この値を選択してください。VLAN ID 番号を入力するための項目が表示されます。

VLAN ID：

VLAN ID フィルターに「Specific」（特定）を選択すると、特定の VLAN ID 番号を入力することができます。指定できる範囲は 1～4095 です。この ACE にヒットするフレームは、この VLAN ID 値と一致します。

Tag Priority（タグの優先度）:
この ACE のタグ優先度を指定してください。この ACE にヒットしたフレームは、このタグ優先度と一致します。指定できる数値の範囲は 0～7、または範囲 0～1、2～3、4～5、6～7、0～3、4～7 です。値「Any」（任意）は、タグの優先度が指定されていないことを意味します（タグの優先度は「don't-care」）。

ARP Parameters（ARP パラメーター）
ARP パラメーターは、フレームタイプに「ARP」が選択されている場合に設定できます。

ARP/RARP:
この ACE に使用可能な ARP/RARP オペコード（OP）フラグを指定してください。
Any（任意）：ARP/RARP OP フラグを指定しません。（OP は「don't-care」）
ARP：フレームの ARP オペコードが ARP に設定されている必要があります。
RARP：フレームの RARP オペコードが RARP に設定されている必要があります。
Other（その他）：フレームに不明な ARP/RARP オペコードフラグがあります。

Request/Reply（要求/応答）:
この ACE で使用可能な要求/応答オペコード（OP）フラグを指定してください。
Any（任意）：要求/応答 OP フラグが指定されていません。（OP は「don't-care」）
Request（要求）：フレームに ARP Request または RARP Request OP フラグが設定されている必要があります。
Reply（応答）：フレームに ARP Reply または RARP Reply OP フラグが必要です。

Sender IP Filter（送信者 IP フィルター）:
この ACE の送信者 IP フィルターを指定してください。
Any（任意）：送信者 IP フィルターが指定されていません。（送信者 IP フィルターは「don't-care」）
Host（ホスト）：送信者 IP フィルターは「Host」（ホスト）に設定されます。表示されている SIP アドレスのフィールドに送信者の IP アドレスを指定してください。
Network（ネットワーク）：送信者 IP フィルターがネットワークに設定されています。表示されている SIP アドレスと SIP マスクの各フィールドに、それぞれ、送信者の IP アドレスと送信者の IP マスクを指定してください。

Sender IP Address（送信者 IP アドレス）:
送信元 IP フィルターに「Host」（ホスト）または「Network」（ネットワーク）を選択した場合、特定の送信元 IP アドレスをドット区切りの 10 進表記で入力できます。

Sender IP Mask（送信者 IP マスク）：
送信元 IP フィルターで「Network」（ネットワーク）を選択した場合、特定の送信元 IP マスクをドット区切りの 10 進表記で入力できます。

Target IP Filter（ターゲット IP フィルター）：
この特定の ACE のターゲット IP フィルターを指定してください。

Any（任意）：ターゲット IP フィルターが指定されていません。（ターゲット IP フィルターは「don't-care」）

Host（ホスト）：ターゲット IP フィルターが「Host」（ホスト）に設定されています。表示されているターゲット IP アドレスのフィールドに、ターゲット IP アドレスを指定してください。

Network（ネットワーク）：ターゲット IP フィルターがネットワークに設定されています。表示されているターゲット IP アドレスとターゲット IP マスクの各フィールドに、適切な IP アドレスと IP マスクをそれぞれ指定してください。

Target IP Address（ターゲット IP アドレス）：
ターゲット IP フィルターに「Host」（ホスト）または「Network」（ネットワーク）を選択した場合、特定のターゲット IP アドレスをドット区切りの 10 進表記で入力できます。

Target IP Mask（ターゲット IP マスク）：
ターゲット IP フィルターに「Network」（ネットワーク）を選択すると、特定のターゲット IP マスクをドット区切りの 10 進表記で入力できます。

ARP Sender MAC Match（ARP 送信者の MAC 一致）：
送信元ハードウェアアドレスフィールド（SHA）の設定に従って、フレームがアクションにヒットできるかどうかを指定してください。

0：SHA が SMAC アドレスと等しくない ARP フレームです。

1：SHA が SMAC アドレスと等しい ARP フレームです。

Any（任意）：任意の値を使用できます（don't-care）。

RARP Target MAC Match（RARP ターゲットの MAC 一致）：
ターゲットハードウェアアドレスフィールド（THA）の設定に従って、フレームがアクションにヒットできるかどうかを指定してください。

0：THA がターゲット MAC アドレスと等しくない RARP フレームです。

1：THA がターゲット MAC アドレスと等しい RARP フレームです。

Any（任意）：任意の値を使用できます（don't-care）。

IP/Ethernet Length（IP/イーサネット長）：
ARP/RARP ハードウェアアドレス長（HLN）、およびプロトコルアドレス長（PLN）の設定に従って、フレームがアクションにヒットできるかどうかを指定してください。

0：HLN がイーサネット（0x06）または（PLN）と IPv4（0x04）が等しくない ARP/RARP フレームです。

1：HLN がイーサネット（0x06）に等しく、（PLN）が IPv4（0x04）に等しい ARP/RARP フレームです。

Any（任意）：任意の値を使用できます（don't-care）。

Ethernet（イーサネット）：
ARP/RARP ハードウェアアドレス空間（HRD）の設定に従って、フレームがアクションにヒットできるかどうかを指定してください。

0：HLD がイーサネット（1）と等しくない ARP/RARP フレームです。

1：HLD がイーサネット（1）に等しい ARP/RARP フレームです。

Any（任意）：任意の値を使用できます（don't-care）。

IP：
ARP/RARP プロトコルアドレス空間（PRO）の設定に従って、フレームがアクションにヒットできるかどうかを指定してください。

0：PRO が IP（0x800）と等しくない ARP/RARP フレームです。

1：PRO が IP（0x800）に等しい ARP/RARP フレームです。

Any（任意）：任意の値を使用できます（don't-care）。

IP Parameters（IP パラメーター）
IP パラメーターは、フレームタイプに「IPv4」が選択されている場合に設定できます。

IP Protocol Filter（IP プロトコルフィルター）：
この ACE の IP プロトコルフィルターを指定してください。

Any（任意）：IP プロトコルフィルターが指定されていません（don't-care）。

Specific（特定）：この ACE で特定の IP プロトコルフィルターをフィルタリングする場合は、この値を選択してください。IP プロトコルフィルターを入力するためのフィールドが表示されます。

ICMP：IPv4ICMP プロトコルフレームをフィルタリングするには、「ICMP」を選択してください。ICMP パラメーターを定義するための追加フィールドが表示されます。これらの項目については、このヘルプファイルで後述します。

UDP：IPv4UDP プロトコルフレームをフィルタリングするには、「UDP」を選択してください。UDP パラメーターを定義するための追加フィールドが表示されます。これらの項目については、このヘルプファイルで後述します。

TCP：IPv4 TCP プロトコルフレームをフィルタリングするには、「TCP」を選択してください。TCP パラメーターを定義するための追加フィールドが表示されます。これらの項目については、このヘルプファイルで後述します。

IP Protocol Value（IP プロトコル値）：

IP プロトコル値に「Specific」（特定）を選択した場合、特定の値を入力できます。指定できる範囲は 0～255 です。この ACE にヒットするフレームは、この IP プロトコル値と一致します。

IP TTL：

この ACE の Time-to-Live 設定を指定してください。

zero（ゼロ）：Time-to-Live 項目がゼロより大きい IPv4 フレームは、このエントリーに一致させられません。

non-zero（ゼロ以外）：Time-to-Live 項目がゼロより大きい IPv4 フレームは、このエントリーと一致させる必要があります。

Any（任意）任意の値を使用できます（don't-care）。

IP Fragment（IP フラグメント）：

この ACE のフラグメントオフセット設定を指定してください。これには、IPv4 フレームの「More Fragments」（MF）ビットと、「Fragment Offset」（FRAG OFFSET）フィールドの設定が含まれます。

No（いいえ）：MF ビットがセットされている IPv4 フレーム、または FRAG OFFSET 項目がゼロより大きい IPv4 フレームは、このエントリーに一致させることができません。

Yes（はい）：MF ビットが設定されている IPv4 フレーム、または FRAG OFFSET 項目がゼロより大きい IPv4 フレームは、このエントリーと一致させる必要があります。

Any（任意）：任意の値を使用できます（don't-care）。

IP Option（IP オプション）：

この ACE のオプションフラグ設定を指定してください。

No（いいえ）：オプションフラグが設定されている IPv4 フレームは、このエントリーと一致させることができません。

Yes（はい）：options フラグが設定されている IPv4 フレームは、このエントリーと一致させる必要があります。

Any（任意）：任意の値を使用できます（don't-care）。

SIP Filter（SIP フィルター）:

この ACE の送信元 IP フィルターを指定してください。

Any（任意）: 送信元 IP フィルターが指定されていません。（送信元 IP フィルターは「don't-care」）

Host（ホスト）: 送信元 IP フィルターはホストに設定されます。表示される SIP アドレスのフィールドに送信元 IP アドレスを指定してください。

Network（ネットワーク）: 送信元 IP フィルターがネットワークに設定されています。表示される SIP アドレスと SIP マスクの各フィールドに、送信元 IP アドレスと送信元 IP マスクをそれぞれ指定してください。

SIP Address（SIP アドレス）:

送信元 IP フィルターで「Host」（ホスト）または「Network」（ネットワーク）を選択した場合、特定の SIP アドレスをドット区切りの 10 進表記で入力できます。

SIP Mask（SIP マスク）:

送信元 IP フィルターで「Network」（ネットワーク）を選択した場合、特定の SIP マスクをドット区切りの 10 進表記で入力できます。

DIP Filter（DIP フィルター）:

この ACE の宛先 IP フィルターを指定してください。

Any（任意）宛先 IP フィルターが指定されていません。（宛先 IP フィルターは「don't-care」）

Host（ホスト）: 宛先 IP フィルターは「Host」（ホスト）に設定されます。表示される「DIP Address」（DIP アドレス）フィールドに宛先 IP アドレスを指定してください。

Network（ネットワーク）: 宛先 IP フィルターがネットワークに設定されています。表示される「DIP Address」（DIP アドレス）と「DIP Mask」（DIP マスク）の各フィールドに、宛先 IP アドレスと宛先 IP マスクを、それぞれ指定してください。

DIP Address（DIP アドレス）:

宛先 IP フィルターに「Host」（ホスト）または「Network」（ネットワーク）を選択した場合、特定の DIP アドレスをドット区切りの 10 進表記で入力できます。

DIP Mask（DIP マスク）:

宛先 IP フィルターに「Network」（ネットワーク）を選択すると、特定の DIP マスクをドット区切りの 10 進表記で入力できます。

IPv6 Parameters（IPv6 パラメーター）

IPv6 パラメーターは、フレームタイプに「IPv6」が選択されている場合に設定できます。
Next Header Filter（ネクストヘッダーフィルター）：
この ACE の IPv6 ネクストヘッダーフィルターを指定してください。

Any（任意）：IPv6 ネクストヘッダーフィルターが指定されていません（don't-care）。

Specific（特定）：この ACE で特定の IPv6 ネクストヘッダーフィルターをフィルタリングする場合は、この値を選択してください。IPv6 ネクストヘッダーフィルターを入力するための項目が表示されます。

ICMP：IPv6 ICMP プロトコルフレームをフィルタリングするには、「ICMP」を選択してください。ICMP パラメーターを定義するための追加フィールドが表示されます。これらの項目については、このヘルプファイルで後述します。

UDP：IPv6UDP プロトコルフレームをフィルタリングするには、「UDP」を選択します。UDP パラメーターを定義するための追加フィールドが表示されます。これらの項目については、このヘルプファイルで後述します。

TCP：IPv6 TCP プロトコルフレームをフィルタリングするには、「TCP」を選択してください。TCP パラメーターを定義するための追加フィールドが表示されます。これらの項目については、このヘルプファイルで後述します。

Next Header Value（ネクストヘッダー値）：
IPv6 ネクストヘッダー値に「Specific」（特定）を選択した場合、特定の値を入力することができます。指定できる範囲は 0～255 です。この ACE にヒットするフレームは、この IPv6 プロトコル値と一致します。

SIP Filter（SIP フィルター）：
この ACE の送信元 IPv6 フィルターを指定してください。

Any（任意）：送信元 IPv6 フィルターが指定されていません。（送信元 IPv6 フィルターは「don't-care」）

Specific（特定）：送信元 IPv6 フィルターはネットワークに設定されます。表示される SIP アドレスのフィールドに、送信元 IPv6 アドレスと送信元 IPv6 マスクを指定してください。

SIP Address（SIP アドレス）：
送信元 IPv6 フィルターに「Specific」（特定）を選択した場合、特定の SIPv6 アドレスを入力できます。この項目は、IPv6 アドレスの最後の 32 ビットのみをサポートしています。

SIP BitMask（SIP ビットマスク）：
送信元 IPv6 フィルターに「Specific」（特定）を選択すると、特定の SIPv6 マスクを入力できます。この項目は、IPv6 アドレスの最後の 32 ビットのみをサポートしています。ビットマスクの使用方法に注意

してください。バイナリビット値が「0」の場合、このビットが「don't-care」であることを意味します。実際にマッチしたパターンは[sipv6_address&sipv6_bitmask]（最後の 32 ビット）です。例えば、SIPv6 アドレスが 2001::3 で SIPv6 ビットマスクが 0xFFFFFFE（ビット 0 が「don't-care」ビット）の場合、SIPv6 アドレス 2001::2 および 2001::3 がこのルールに適用されます。

Hop Limit（ホップ制限）：
この ACE のホップ制限設定を指定してください。

zero（ゼロ）：ホップ制限フィールドがゼロより大きい IPv6 フレームは、このエントリーに一致させることができません。

non-zero（ゼロ以外）：ホップ制限フィールドがゼロより大きい IPv6 フレームは、このエントリーに一致させる必要があります。

Any（任意）：任意の値を使用できます（don't-care）。

ICMP Parameters（ICMP パラメーター）

ICMP Type Filter（ICMP タイプフィルター）：
この ACE の ICMP フィルターを指定してください。

Any（任意）：ICMP フィルターが指定されていません（ICMP フィルターの状態は「don't-care」です）。

Specific（特定）：この ACE で特定の ICMP フィルターをフィルタリングする場合は、特定の ICMP 値を入力できます。ICMP 値を入力するための項目が表示されます。

ICMP Type Value（ICMP タイプ値）：
ICMP フィルターで「Specific」（特定）を選択すると、特定の ICMP 値を入力できます。指定できる範囲は 0～255 です。この ACE にヒットするフレームは、この ICMP 値と一致します。

ICMP Code Filter（ICMP コードフィルター）：
この ACE の ICMP コードフィルターを指定してください。

Any（任意）：ICMP コードフィルターが指定されていません（ICMP コードフィルターの状態は「don't-care」です）。

Specific（特定）：この ACE で特定の ICMP コードフィルターをフィルタリングする場合は、特定の ICMP コード値を入力できます。ICMP コード値を入力するためのフィールドが表示されます。

ICMP Code Value（ICMP コード値）：

ICMPコードフィルターで「Specific」(特定)を選択すると、特定のICMPコード値を入力することができます。指定できる範囲は0～255です。このACEにヒットしたフレームは、このICMPコード値と一致します。

TCP/UDP Parameters(TCP/UDPパラメーター)

TCP/UDP Source Filter(TCP/UDP送信元フィルター):

このACEのTCP/UDP送信元フィルターを指定してください。

Any(任意):TCP/UDP送信元フィルターが指定されていません(TCP/UDP送信元フィルターの状態は「don't-care」です)。

Specific(特定):このACEで特定のTCP/UDP送信元フィルターをフィルタリングする場合は、特定のTCP/UDPソース値を入力できます。TCP/UDPソース値を入力するための項目が表示されます。

Range(範囲):特定のTCP/UDP送信元範囲フィルターをこのACEでフィルタリングする場合は、特定のTCP/UDPソース範囲値を入力することができます。TCP/UDP送信元値を入力するための項目が表示されます。

TCP/UDP Source No.(TCP/UDP送信元番号):

TCP/UDP送信元フィルターに「Specific」(特定)を選択すると、特定のTCP/UDPソース値を入力することができます。指定できる範囲は0～65535です。このACEにヒットするフレームは、このTCP/UDPソース値と一致します。

TCP/UDP Source Range(TCP/UDP送信元範囲):

TCP/UDP送信元フィルターに「Range」(範囲)を選択すると、特定のTCP/UDPソース範囲値を入力することができます。指定できる範囲は0～65535です。このACEにヒットするフレームは、このTCP/UDPソース値と一致します。

TCP/UDP Destination Filter(TCP/UDP宛先フィルター):

このACEのTCP/UDP宛先フィルターを指定してください。

Any(任意):TCP/UDP宛先フィルターが指定されていません(TCP/UDP宛先フィルターの状態は「don't-care」です)。

Specific(特定):このACEで特定のTCP/UDP宛先フィルターをフィルタリングする場合は、特定のTCP/UDP宛先値を入力することができます。TCP/UDP宛先値を入力するための項目が表示されます。

Range(範囲):このACEで特定の範囲のTCP/UDP宛先フィルターをフィルタリングする場合は、特定のTCP/UDP宛先範囲値を入力することができます。TCP/UDP宛先値を入力するための項目が表示されます。

TCP/UDP Destination Filter（TCP/UDP 宛先番号）:
TCP/UDP 宛先フィルターで「Specific」（特定）を選択すると、特定の TCP/UDP 宛先値を入力することができます。指定できる範囲は 0～65535 です。この ACE にヒットするフレームは、この TCP/UDP 宛先値と一致します。

TCP/UDP Destination Range（TCP/UDP 宛先範囲）:
TCP/UDP 宛先フィルターで「Range」（範囲）を選択した場合、特定の TCP/UDP 宛先範囲値を入力することができます。指定できる範囲は 0～65535 です。この ACE にヒットするフレームは、この TCP/UDP 宛先値と一致します。

TCP FIN:
この ACE の TCP FIN 値（No more data from sender）値を指定してください。
0：FIN 項目が設定されている TCP フレームは、このエントリーと一致させることができません。
1：FIN 項目が設定されている TCP フレームは、このエントリーと一致させる必要があります。
Any（任意）：任意の値を使用できます（don't-care）。

TCP SYN:
この ACE の TCP SYN 値（Synchronize sequence numbers）を指定してください。
0：SYN 項目が設定されている TCP フレームは、このエントリーと一致させることができません。
1：SYN 項目が設定されている TCP フレームは、このエントリーと一致させる必要があります。
Any（任意）：任意の値を使用できます（don't-care）。

TCP RST:
この ACE の TCP RST 値（Reset the connection）を指定してください。
0：RST 項目が設定されている TCP フレームは、このエントリーと一致させることができません。
1：RST 項目が設定されている TCP フレームは、このエントリーと一致させる必要があります。
Any（任意）：任意の値を使用できます（don't-care）。

TCP PSH:
この ACE の TCP PSH 値（Push Function）を指定してください。
0：PSH 項目が設定されている TCP フレームは、このエントリーと一致させることができません。
1：PSH 項目が設定されている TCP フレームは、このエントリーと一致させる必要があります。
Any（任意）：任意の値を使用できます（don't-care）。

TCP ACK:

この ACE の TCP ACK 値（Acknowledgment field significant）を指定してください。

0：ACK 項目が設定されている TCP フレームは、このエントリーに一致させることができません。

1：ACK 項目が設定されている TCP フレームは、このエントリーと一致させる必要があります。

Any（任意）：任意の値を使用できます（don't-care）。

TCP URG：

この ACE の TCP URG 値（Urgent Pointer field significant）を指定してください。

0：URG 項目が設定されている TCP フレームは、このエントリーと一致させることができません。

1：URG 項目が設定されている TCP フレームは、このエントリーと一致させる必要があります。

Any（任意）：任意の値を使用できます（don't-care）。

Ethernet Type Parameters（イーサネットタイプのパラメーター）

イーサネットタイプのパラメーターは、フレームタイプに「Ethernet Type」（イーサネットタイプ）が選択されている場合に設定できます。

EtherType Filter（イーサネットタイプフィルター）：

この ACE のイーサネットタイプフィルターを指定してください。

Any（任意）イーサネットタイプフィルターが指定されていません（イーサネットタイプフィルターの状態は「don't-care」です）。

Specific（特定）：この ACE で特定のイーサネットタイプフィルターをフィルタリングする場合は、特定のイーサネットタイプフィルター値を入力することができます。イーサネットタイプ値を入力するための項目が表示されます。

Ethernet Type Value（イーサネットタイプ値）：

イーサネットタイプフィルターで「Specific」（特定）を選択した場合、特定のイーサネットタイプ値を入力することができます。指定できる範囲は 0x600～0xFFFF ですが、0x800（IPv4）、0x806（ARP）、および 0x86DD（IPv6）は除きます。この ACE にヒットするフレームは、このイーサネットタイプ値と一致します。

■ボタン

Apply（適用）：

クリックすると、変更内容を保存します。

Reset（リセット）：

クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

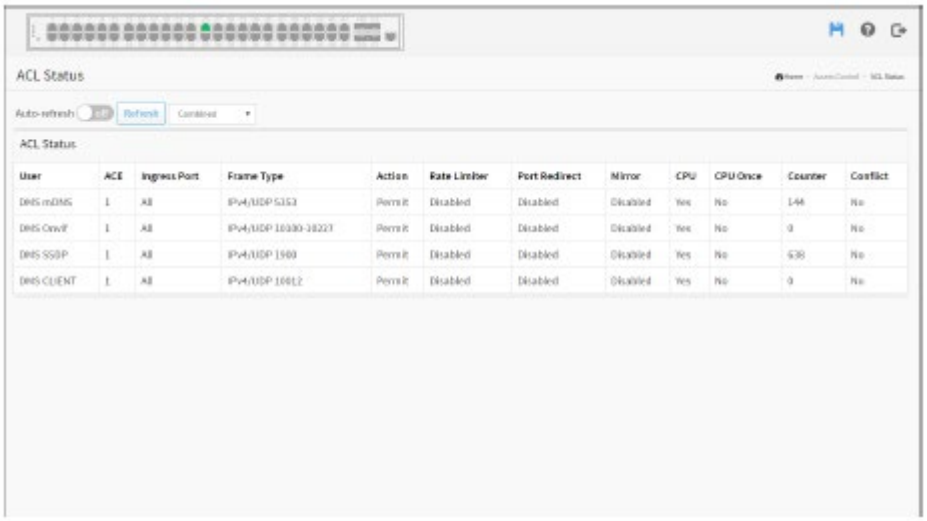
Auto-refresh（自動更新）：
自動更新をクリックすると、情報を自動的に最新の状態にします。

Refresh、clear、Remove All（更新、消去、すべて削除）：
これらをクリックして ACL 設定を更新するか、手動でクリアすることができます。その他は、テーブル上の全 ACL 設定をクリアするために、すべてを削除します。

Cancel（キャンセル）：
前のページに戻ります。

ACL の状態

このセクションでは、さまざまなACLユーザーによってACLの状態を表示する方法について説明します。各行は、定義されている ACE を示します。ハードウェアの制限のために特定の ACE がハードウェアに適用されていない場合は、競合が発生します。各スイッチの ACE の最大数は 512 です。



Web インターフェース

Web インターフェースで ACL の状態を表示するには:

1. 「Access Control」(アクセス制御) ＞ 「ACL status」(ACL の状態)をクリックしてください。
2. 情報を自動更新する場合は、「Auto-refresh」(自動更新)を呼び出す必要があります。
3. 「Refresh」(更新)をクリックして、ACL の状態を更新してください。

■パラメーターの説明

User(ユーザー):

ACL ユーザーを示します。

ACE:

ローカルスイッチの ACE ID を示します。

Frame Type(フレームタイプ):

ACE のフレームタイプを示します。可能な値は次のとおりです。

Any(任意):ACE は任意のフレームタイプに一致します。

EType（E タイプ）：ACE はイーサネットタイプフレームと一致します。イーサネットタイプベースの ACE は、IP および ARP フレームと一致しません。
ARP：ACE は ARP/RARP フレームと一致します。
IPv4：ACE はすべての IPv4 フレームと一致します。
IPv4/ICMP：ACE は、ICMP プロトコルを使用して IPv4 フレームに一致します。
IPv4/UDP：ACE は UDP プロトコルを使用して IPv4 フレームに一致します。
IPv4/TCP：ACE は TCP プロトコルを使用して IPv4 フレームに一致します。
IPv4/Other（IPv4/その他）：ACE は、ICMP/UDP/TCP 以外の IPv4 フレームに一致します。
IPv6：ACE はすべての IPv6 標準フレームに一致します。

Action（アクション）：
ACE の転送アクションを示します。
Permit（許可）：ACE に一致するフレームが転送され、学習される可能性があります。
Deny（拒否）：ACE に一致するフレームが破棄されます。
Filter（フィルター）：ACE に一致するフレームがフィルタリングされます。

Rate Limiter（レートリミッター）：
ACE のレートリミッター番号を示します。指定できる範囲は 1～16 です。「Disabled」（無効）と表示されている場合は、レートリミッターの操作が無効となっています。

CPU：
特定の ACE に一致したパケットを CPU に転送します。

Counter（カウンター）：
カウンターは、ACE がフレームによってヒットした回数を示します。

Conflict（競合）：
特定の ACE のハードウェアの状態を示します。ハードウェアの制限により、特定の ACE はハードウェアに適用されません。

■ボタン

Auto-refresh（自動更新）：
画面を自動的に更新する場合は、このチェックボックスを ON にしてください。自動更新は 3 秒間

隔で行われます。

Refresh（更新）：
クリックすると、画面がすぐに更新されます。

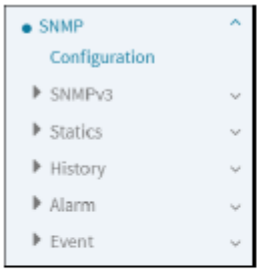
第 14 章
SNMP

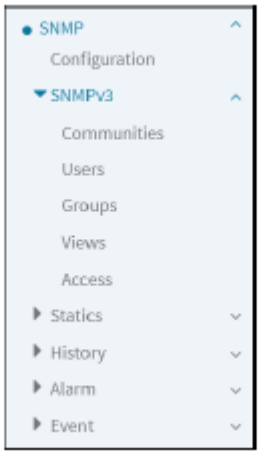
概要

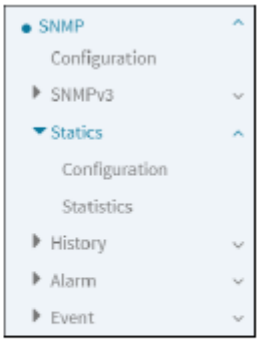
SNMP（Simple Network Management Protocol）を実行するネットワーク管理システム（NMS）は、管理情報ベース（MIB）が対象デバイスに正しくインストールされていれば、SNMP エージェントを搭載した対象デバイスを管理できます。SNMP は、SNMP マネージャーとエージェント間の情報の転送を制御するために使用されるプロトコルで、SMI 構文の形式で記述されている管理情報ベース（MIB）のオブジェクト ID（OID）を通過します。SNMP マネージャーから発行された要求に応答するために、スイッチで SNMP エージェントが実行されています。

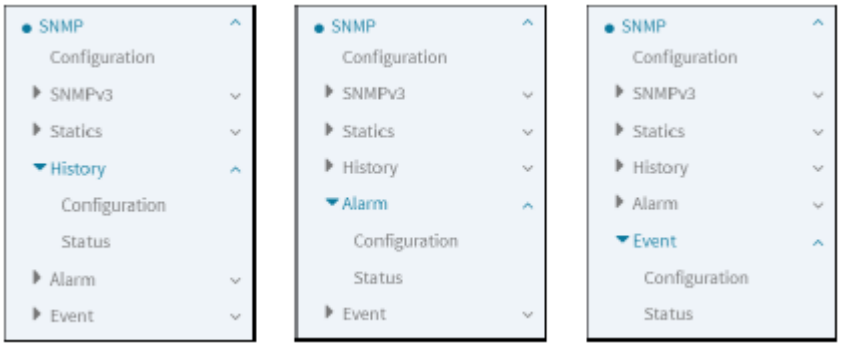
基本的には、トラップ情報を発行する以外はパッシブです。スイッチは、SNMP エージェントを ON または OFF にするスイッチをサポートします。SNMP に「Enable」（有効）を設定すると、SNMP エージェントが起動します。サポートされているすべての MIB OID（RMON MIB を含む）には、SNMP マネージャーを介してアクセスできます。SNMP が「Disable」（無効）に設定されている場合、SNMP エージェントは非アクティブ化され、関連するコミュニティ名、トラップホスト IP アドレス、トラップ、およびすべての MIB カウンターは無視されます。

メニューは以下のとおりです。



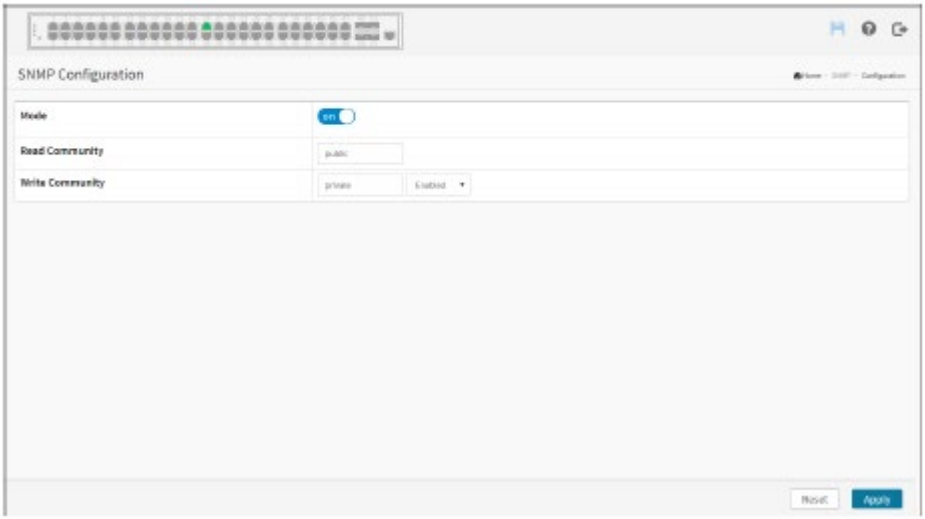





SNMP
Configuration
SNMPv3
Statics
History
Configuration
Status
Alarm
Event
SNMP
Configuration
SNMPv3
Statics
History
Alarm
Configuration
Status
Event
SNMP
Configuration
SNMPv3
Statics
History
Alarm
Event
Configuration
Status

設定

このセクションでは、スイッチで SNMP システムを設定する方法について説明します。この機能は、SNMP の設定、コミュニティ名、トラップホスト、パブリックトラップ、およびスロットルを設定するために使用します。SNMP マネージャーは、両方のコミュニティ名を識別して認証を通過させる必要があります。そうすることで、ターゲットデバイスの MIB 情報にアクセスできます。そのため、両方のパーティーが同じコミュニティ名を持つ必要があります。設定が完了したら、「Apply」（適用）をクリックして設定を有効にしてください。



Web インターフェース

Web インターフェースでユーザーを設定するには:

1. 「SNMP」 ＞ 「configuration」（設定）をクリックしてください。
2. 「Mode」（モード）を使って、SNMP 機能を有効または無効にしてください。
3. 「Read Community」（読み取りコミュニティ）と、「Write Community」（書き込みコミュニティ）を指定してください。
4. 「Apply」（適用）をクリックしてください。

■パラメーターの説明

Mode（モード）:

SNMP モードの操作を示します。有効なモードは次のとおりです。

on：SNMP モードの操作を有効にします。

off：SNMP モードの操作を無効にします。

Read Community（読み取りコミュニティ）：
SNMP エージェントへのアクセスを許可するコミュニティ読み取りアクセス文字列を示します。指定できる文字列の長さは 1～31 で、使用できる内容は ASCII 文字（33～126）です。
この項目は、SNMP バージョンが SNMPv1 または SNMPv2c の場合にのみ適用されます。SNMP バージョンが SNMPv3 の場合、コミュニティ文字列は SNMPv3 コミュニティテーブルに関連付けられます。SNMPv1 または SNMPv2c コミュニティ文字列よりも柔軟にセキュリティ名を設定できます。コミュニティ文字列に加えて、特定の範囲の送信元アドレスを使用して送信元サブネットを制限することができます。

Write Community（書き込みコミュニティ）：
SNMP エージェントへのアクセスを許可するコミュニティ書き込みアクセス文字列を示します。指定できる文字列の長さは 1～31 で、使用できる内容は ASCII 文字（33～126）です。
この項目は、SNMP バージョンが SNMPv1 または SNMPv2c の場合にのみ適用されます。SNMP バージョンが SNMPv3 の場合、コミュニティ文字列は SNMPv3 コミュニティテーブルに関連付けられます。SNMPv1 または SNMPv2c コミュニティ文字列よりも柔軟にセキュリティ名を設定できます。コミュニティ文字列に加えて、特定の範囲の送信元アドレスを使用して送信元サブネットを制限することができます。

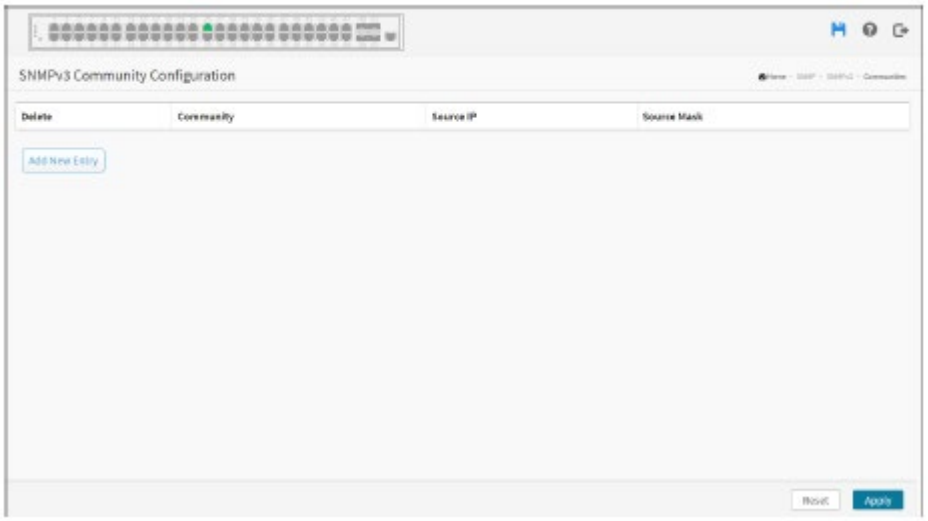
■ボタン
Apply（適用）：
クリックすると、変更内容を保存します。

Reset（リセット）：
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

SNMPv3

コミュニティ

この画面では、SNMPv3 コミュニティテーブルを設定します。エントリーのインデックスキーは「Community」です。



Web インターフェース

Web インターフェースで SNMP コミュニティを設定するには:

1. 「SNMP」 > 「SNMPv3」 > 「Communities」(コミュニティ)をクリックしてください。
2. 「Add New Entry」(新規登録)をクリックしてください。

3. SNMP コミュニティのパラメーターを指定してください。
4. 「Apply」(適用)をクリックしてください。
5. 設定を取り消す場合は、「Reset」(リセット)ボタンをクリックしてください。

■パラメーターの説明

Community（コミュニティ）：
コミュニティを SNMP グループ設定にマッピングするためのセキュリティ名を示します。許可される文字列の長さは 1～32 で、許可される内容は ASCII 文字（33～126）です。

Source IP（送信元 IP）：
SNMP アクセスの送信元アドレスを示します。送信元マスクと組み合わせると、特定の範囲の送信元アドレスを使用して送信元サブネットを制限することができます。

Source IP Prefix（送信元 IP プレフィックス）：
SNMP アクセスの送信元アドレスのプレフィックスを示します。

■ボタン

Add New Entry（新規登録）：
クリックすると、新しいエントリーが追加されます。名前を指定し、新しいエントリーを設定してください。そうしたら、「Apply」（適用）をクリックしてください。

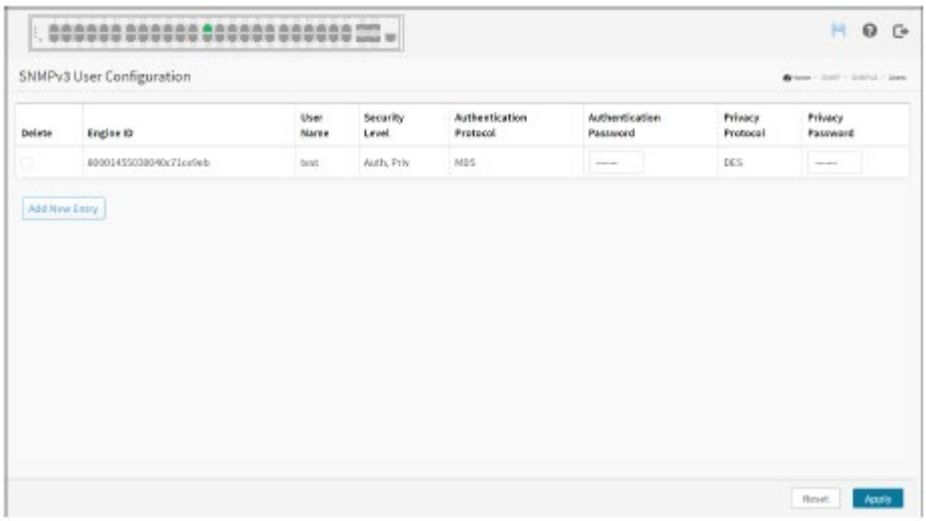
Delete（削除）：
チェックを入れると、エントリーを削除します。これは、次回保存時に削除されます。

Apply（適用）：
クリックすると、変更内容を保存します。

Reset（リセット）：
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

ユーザー

この機能は、SNMPv3 ユーザーを設定するために使用されます。エントリーのインデックスキーはユーザーネームです。新しいユーザーネームアカウントを作成するには、「Add new user」（新規ユーザーの追加）ボタンをチェックし、ユーザー情報を入力してから「Apply」（適用）をチェックしてください。最大グループ番号は 6 です。



Web インターフェース

Web インターフェースで SNMP ユーザーを設定するには:

1. 「SNMP」 ＞ 「SNMPv3」 ＞ 「Users」(ユーザー)をクリックしてください。
2. 「Add New Entry」(新規登録)をクリックしてください。

3. SNMPv3 ユーザーのパラメーターを指定してください。
4. 「Apply」(適用)をクリックしてください。

■パラメーターの説明

Engine ID(エンジン ID):

このエントリーが属するエンジン ID を識別するオクテット文字列です。文字列には、10～64 の桁数の偶数(16 進形式)を含める必要がありますが、すべてをゼロにしたり、すべてを F にしたりすることはできません。SNMPv3 アーキテクチャーでは、メッセージセキュリティに USM(User-based Security Model)を使用し、アクセス制御に VACM(View-based Access Control Model)を使用します。USM エントリーの場合、usmUserEngineID と usmUserName はエントリーのキーです。単純なエージェントでは、usmUserEngineID は常にそのエージェント自身の snmpEngineID 値です。この値には、このユーザーが通信できるリモート SNMP エンジンの snmpEngineID の値を指定することもでき

ます。つまり、ユーザーエンジン ID がシステムエンジン ID と等しい場合はローカルユーザー、等しくない場合はリモートユーザーです。

User Name（ユーザー名）：
このエントリーが属するユーザー名を識別する文字列です。指定できる文字列の長さは 1～31 で、使用できる内容は ASCII 文字（33～126）です。

Security Level（セキュリティレベル）：
このエントリーが属するセキュリティモデルを示します。可能なセキュリティモデルは次のとおりです。

NoAuth, NoPriv：認証なし、プライバシーなし。
Auth, NoPriv：認証あり、プライバシーなし。
Auth, Priv：認証あり、プライバシーあり。

エントリーがすでに存在する場合、セキュリティレベルの値は変更できません。つまり、最初に値が正しく設定されていることを確認する必要があります。

Authentication Protocol（認証プロトコル）：
このエントリーが属する認証プロトコルを示します。使用可能な認証プロトコルは次のとおりです。

MD5：このユーザーが MD5 認証プロトコルを使用することを示すフラグです（オプション）。
SHA：このユーザーが SHA 認証プロトコルを使用することを示すフラグです（オプション）。

エントリーがすでに存在する場合、セキュリティレベルの値は変更できません。つまり、最初に値が正しく設定されていることを確認する必要があります。

Authentication Password（認証パスワード）：
認証パスワードのフレーズを識別する文字列です。MD5 認証プロトコルの場合、許可される文字列の長さは 8～39 です。SHA 認証プロトコルの場合、許可される文字列の長さは 8～39 です。許可される内容は、33～126 の ASCII 文字です。

Privacy Protocol（プライバシープロトコル）：
このエントリーが属するプライバシープロトコルを示します。考えられるプライバシープロトコルは次のとおりです。

DES：このユーザーが DES 認証プロトコルを使用することを示すフラグです（オプション）。
AES：このユーザーが AES 認証プロトコルを使用することを示すフラグです（オプション）。

Privacy Password（プライバシーパスワード）：
プライバシーパスワードのフレーズを識別する文字列です。使用できる文字列の長さは 8～31 で、

使用できるコンテンツは ASCII 文字（33～126）です。

■ボタン

Add New Entry（新規登録）:

クリックすると、新しいエントリーが追加されます。名前を指定し、新しいエントリーを設定してください。そうしたら、「Apply」（適用）をクリックしてください。

Delete（削除）:

チェックを入れると、エントリーを削除します。これは、次回保存時に削除されます。

Apply（適用）:

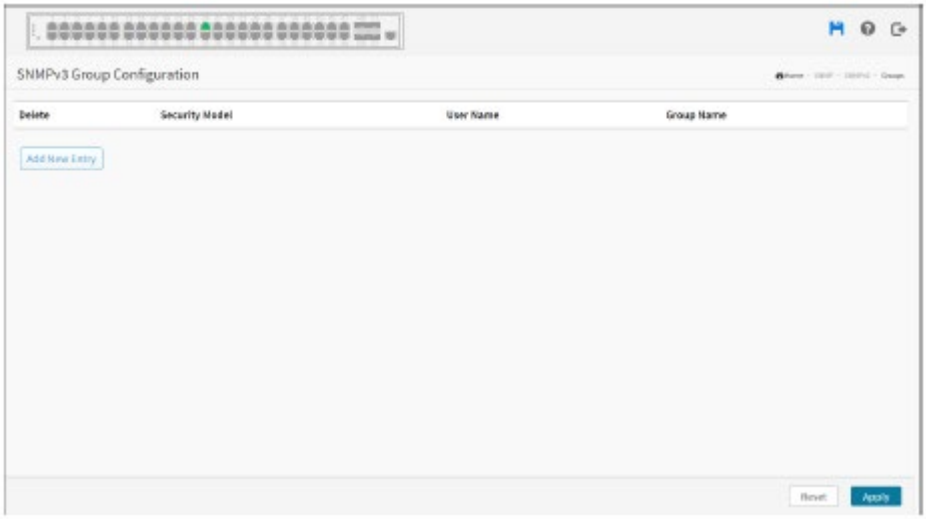
クリックすると、変更内容を保存します。

Reset（リセット）:

クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

グループ

この機能は、SNMPv3 グループを設定するために使用されます。エントリーのインデックスキーはセキュリティモデルとセキュリティ名 です。新しいグループアカウントを作成するには、「Add new group」（新規グループの追加）ボタンをチェックし、グループ情報を入力してから「Apply」（適用）をチェックしてください。最大グループ番号は 12 です。

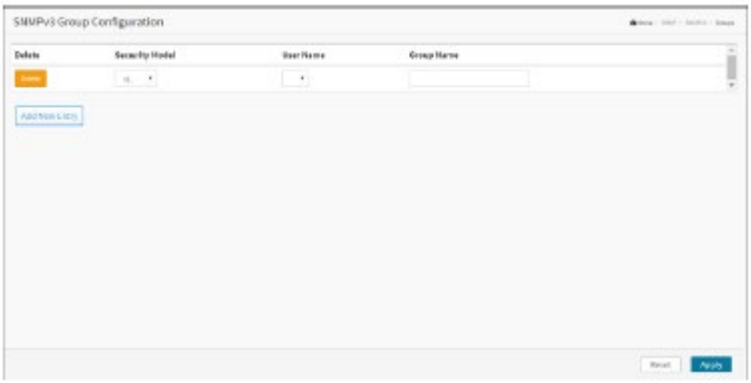


Web インターフェース

Web インターフェースで SNMP グループを設定するには:

1. 「SNMP」 ＞ 「SNMPv3」 ＞ 「Groups」（グループ）をクリックしてください。

2. 「Add New Entry」(新規登録)をクリックしてください。



3. SNMP グループのパラメーターを指定してください。
4. 「Apply」(適用)をクリックしてください。

■パラメーターの説明

Security Model(セキュリティモデル):
このエントリーが属するセキュリティモデルを示します。可能なセキュリティモデルは次のとおりです。

v1:SNMPv1 用に予約されています。
v2c:SNMPv2c 用に予約されています。
usm:USM(User-based Security Model)です。

Security Name(セキュリティ名):
この項目が属するセキュリティ名を識別する文字列です。指定できる文字列の長さは 1～31 で、使用できる内容は ASCII 文字(33～126)です。

Group Name(グループ名):
このエントリーが属するグループ名を識別する文字列です。許可される文字列の長さは 1～32 で、許可される内容は ASCII 文字(33～126)です。

■ボタン

Add New Entry(新規登録):
クリックすると、新しいエントリーが追加されます。名前を指定し、新しいエントリーを設定してください。そうしたら、「Apply」(適用)をクリックしてください。

Delete(削除):
チェックを入れると、エントリーを削除します。これは、次回保存時に削除されます。

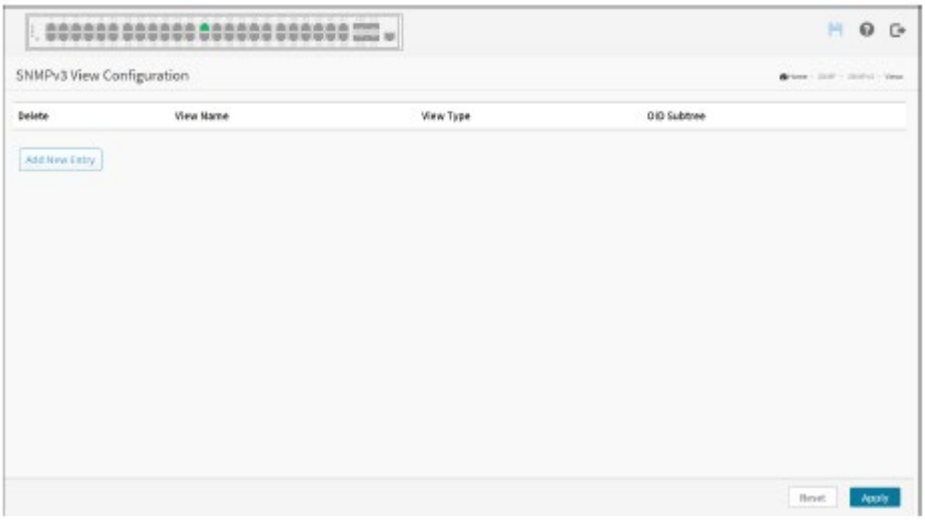
Apply（適用）：
クリックすると、変更内容を保存します。

Reset（リセット）：
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

ビュー

この機能は、SNMPv3ビューの設定に使用されます。エントリーのインデックスキーは、OIDサブツリーとビュー名です。新しいビューアカウントを作成するには、「Add new view」（新規ビューの追加）ボタンをチェックし、ビュー情報を入力して「Apply」（適用）をクリックしてください。最大グループ番号は12です。

この画面でSNMPv3ビューテーブルを設定してください。エントリーのインデックスキーは、ビュー名およびOIDサブツリーです。



Webインターフェース
Webインターフェースで SNMPビューを設定するには：
1. 「SNMP」 ＞ 「SNMPv3」 ＞ 「Views」（ビュー）をクリックしてください。
2. 「Add New Entry」（新規登録）をクリックしてください。

3. SNMP ビューのパラメーターを指定してください。
4. 「Apply」(適用)をクリックしてください。
5. 設定を取り消す場合は、「Reset」(リセット)ボタンをクリックしてください。

■パラメーターの説明

View Name(ビュー名):
このエントリーが属するビュー名を識別する文字列です。指定できる文字列の長さは 1～31 で、使用できる内容は ASCII 文字(33～126)です。

View Type(ビュータイプ):
このエントリーが属するビュータイプを示します。使用可能なビュータイプは次のとおりです。

Included(含まれる):このビューサブツリーが含まれることを示すオプションのフラグです。

Excluded(除外):このビューサブツリーを除外することを示すフラグです(オプション)。

一般的に、ビュー入力のビュータイプが「Excluded」(除外)である場合は、ビュータイプが「Included」(含まれる)のビューエントリーが別に存在し、なおかつ、その OID サブツリーは「Excluded」(除外)ビューエントリーの限度を超えているはずです。

OID Subtree(OID サブツリー):
名前付きビューに追加するサブツリーのルートを定義する OID です。許可される OID の長さは 1～128 です。許可される文字列の内容は、数字またはアスタリスク(*)です。

■ボタン

Add New Entry(新規登録):
クリックすると、新しいエントリーが追加されます。名前を指定し、新しいエントリーを設定してください。そうしたら、「Apply」(適用)をクリックしてください。

Delete(削除):

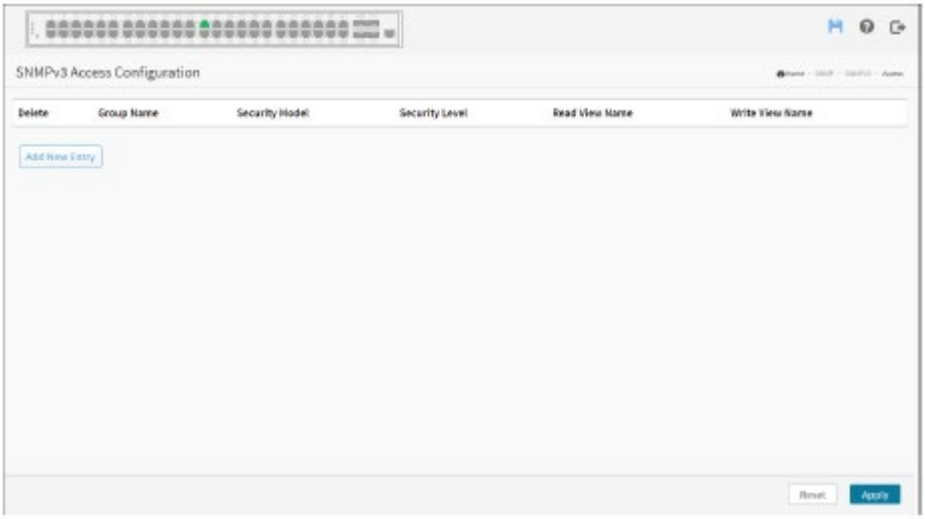
チェックを入れると、エントリーを削除します。これは、次回保存時に削除されます。

Apply（適用）：
クリックすると、変更内容を保存します。

Reset（リセット）：
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

アクセス

この機能は、SNMPv3 アクセスを設定するために使用されます。エントリーのインデックスキーは、グループ名、セキュリティモデル、セキュリティレベルです。新しいアクセスアカウントを作成するには、「Add new access」（新規アクセスの追加）ボタンをチェックし、アクセス情報を入力して「Apply」（適用）をチェックしてください。最大グループ番号は 12 です。



Web インターフェース

Web インターフェースで SNMP アクセスの設定を表示するには：

1. 「SNMP」 ＞ 「SNMPv3」 ＞ 「Accesses」（アクセス）をクリックしてください。
2. 「Add New Entry」（新規登録）をクリックしてください。

3. SNMP アクセスのパラメーターを指定してください。
4. 「Apply」(適用)をクリックしてください。
5. 設定を取り消す場合は、「Reset」(リセット)ボタンをクリックしてください。

■パラメーターの説明

Group Name(グループ名):
このエントリーが属するグループ名を識別する文字列です。指定できる文字列の長さは 1～31 で、使用できる内容は ASCII 文字(33～126)です。

Security Model(セキュリティモデル):
このエントリーが属するセキュリティモデルを示します。可能なセキュリティモデルは次のとおりです。

Any(任意):任意のセキュリティモデルを使用できます(v1v2c usm)。
v1:SNMPv1 用に予約されています。
v2c:SNMPv2c 用に予約されています。
usm:USM(User-based Security Model)です。

Security Level(セキュリティレベル):
このエントリーが属するセキュリティモデルを示します。可能なセキュリティモデルは次のとおりです。

NoAuth, NoPriv:認証なし、プライバシーなし。
Auth, NoPriv:認証あり、プライバシーなし。
Auth, Priv:認証あり、プライバシーあり。

Read View Name(読み取りビュー名):
この要求が現在の値を要求する可能性がある MIB オブジェクトを定義する MIB ビューの名前です。指定できる文字列の長さは 1～31 で、使用できる内容は ASCII 文字(33～126)です。

Write View Name（書き込みビュー名）：
この要求が新しい値を設定する可能性があるMIBオブジェクトを定義するMIBビューの名前です。
指定できる文字列の長さは 1～31 で、使用できる内容は ASCII 文字（33～126）です。

■ボタン

Add New Entry（新規登録）：
クリックすると、新しいエントリーが追加されます。名前を指定し、新しいエントリーを設定してください。そうしたら、「Apply」（適用）をクリックしてください。

Delete（削除）：
チェックを入れると、エントリーを削除します。これは、次回保存時に削除されます。

Apply（適用）：
クリックすると、変更内容を保存します。

Reset（リセット）：
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

スタティック

設定

この画面では統計テーブルを設定します。エントリーのインデックスキーは ID です。

Web インターフェース

Web インターフェースで統計を設定するには:

1. 「SNMP」 ＞ 「Statics」(スタティック) ＞ 「Configuration」(設定)をクリックしてください。
2. 「Add New Entry」(新規登録)をクリックしてください。

3. ID パラメーターを指定してください。
4. 「Apply」(適用)をクリックしてください。

■パラメーターの説明

これらのパラメーターは、「RMON Statistics Configuration」(RMON 統計設定)画面に表示されま

す。

ID：
エントリーのインデックスを示します。指定できる範囲は 1～65535 です。

Data Source（データソース）：
監視するポート ID を示します。スタッキングスイッチでは、値に 1000 ×（スイッチ ID-1）を加算する必要があります。例えば、ポートがスイッチ 3 のポート 5 の場合、値は 2005 です。

■ボタン

Delete（削除）：
チェックを入れると、エントリーを削除します。これは、次回保存時に削除されます。

Add New Entry（新規登録）：
クリックすると、新しいエントリーが追加されます。

Apply（適用）：
クリックすると、変更内容を保存します。

Reset（リセット）：
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

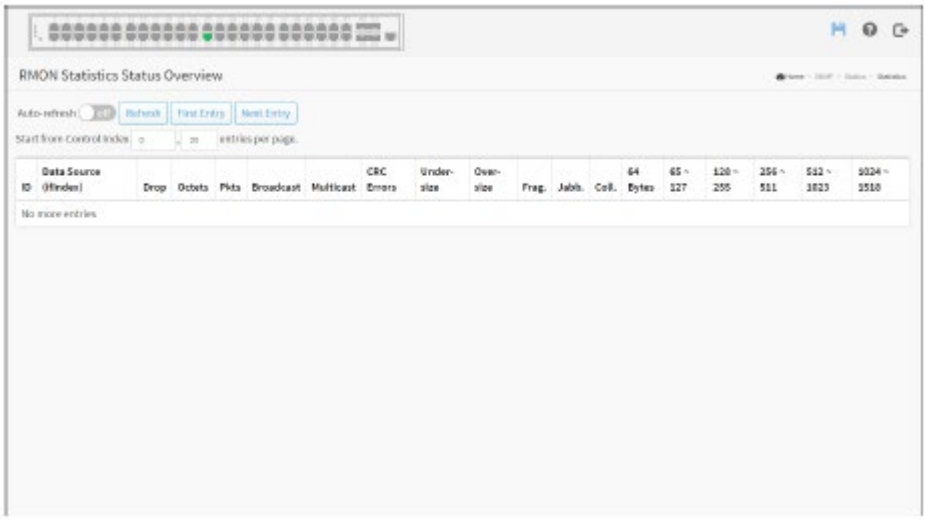
統計

この画面では、RMON 統計エントリーの概要を説明します。各ページには、統計テーブルから最大 99 個のエントリーが表示されます。デフォルトは 20 で、「entries per page」（ページあたりのエントリー数）の入力フィールドで選択されています。最初にアクセスしたとき、Web ページには統計テーブルの先頭から最初の 20 件のエントリーが表示されます。最初に表示されるのは、統計テーブルで見つかった ID が最も小さいものです。

「Start from Control Index」（制御インデックスから開始）を使用すると、統計テーブルで開始点を選択できます。「Refresh」（更新）ボタンをクリックすると、表示されているテーブルが、そのテーブルまたは次に近い統計テーブルの一致から更新されます。

「Next Entry」（次のエントリー）は、現在表示されているエントリーの最後のエントリーを、次のルックアップの基準として使用します。最後に達すると、表示されたテーブルに「これ以上エントリーはあり

ません」というテキストが表示されます。このような場合は、「First Entry」（最初のエントリー）ボタンを使用して、最初からやり直してください。



Web インターフェース

Web インターフェースに RMON 統計の状態を表示するには：

1. 「SNMP」 ＞ 「Statics」（スタティック） ＞ 「Statistics」（統計）をクリックしてください。
2. 確認するポートを指定してください。
3. 「Auto-refresh」（自動更新）にチェックを入れてください。
4. ポートの詳細統計情報を更新するには、「Refresh」（更新）をクリックしてください。

■パラメーターの説明

ID：

統計エントリーのインデックスを示します。

Data Source（データソース）（インデックスの場合）：

監視するポート ID です。

Drop（破棄）：

リソース不足のためにプローブによってパケットが破棄されたイベントの合計数です。

Octets（オクテット）：

ネットワーク上で受信したデータの総オクテット数です（不良パケットのデータを含む）。

Pkts：

受信したパケットの総数です（不良パケット、ブロードキャストパケット、マルチキャストパケットを含む）。

Broadcast（ブロードキャスト）：
ブロードキャストアドレス宛に受信した正しいパケットの合計数です。

Multicast（マルチキャスト）：
マルチキャストアドレス宛に受信した正しいパケットの合計数です。

CRC Errors（CRC エラー）：
64 オクテットから 1518 オクテットまでの長さ（フレーミングビットは除き、FCS オクテットは含む）を持ちますが、整数オクテット（FCS エラー）を持つ不良フレームチェックシーケンス（FCS）またはオクテット数が整数でない不良 FCS（アライメントエラー）を持つ受信パケットの総数です。

Under-size（アンダーサイズ）：
64 オクテット未満で受信したパケットの合計数です。

Over-size（オーバーサイズ）：
1518 オクテットより長い受信パケットの合計数です。

Frag.：
無効な CRC で受信された 64 オクテット未満のサイズのフレームの数です。

Jabb.：
無効な CRC で受信した 64 オクテットより大きいサイズのフレームの数です。

Coll.：
このイーサネットセグメントのコリジョンを最適に見積もった合計数です。

64 Bytes（64 バイト）：
64 オクテット長の受信パケット（不良パケットを含む）の合計数です。

65-127：
長さが 65～127 オクテットの間で受信されたパケット（不良パケットを含む）の合計数です。

128-255：

長さが 128～255 オクテットの間で受信されたパケット(不良パケットを含む)の合計数です。

256-511：
長さが 256～511 オクテットの間で受信されたパケット（不良パケットを含む）の合計数です。

512-1023：
長さが 512～1023 オクテットの間で受信されたパケット（不良パケットを含む）の合計数です。

1024-1588：
長さが 1024～1588 オクテットの間で受信されたパケット（不良パケットを含む）の合計数です。

Search（検索）：
表示する情報を検索できます。

Show entries（エントリーの表示）：
表示する項目の数を選択できます。

■ボタン

Auto-refresh（自動更新）：
画面を自動的に更新する場合は、このチェックボックスをONにしてください。自動更新は3秒間隔で行われます。

Refresh（更新）：
クリックするとページを更新します。

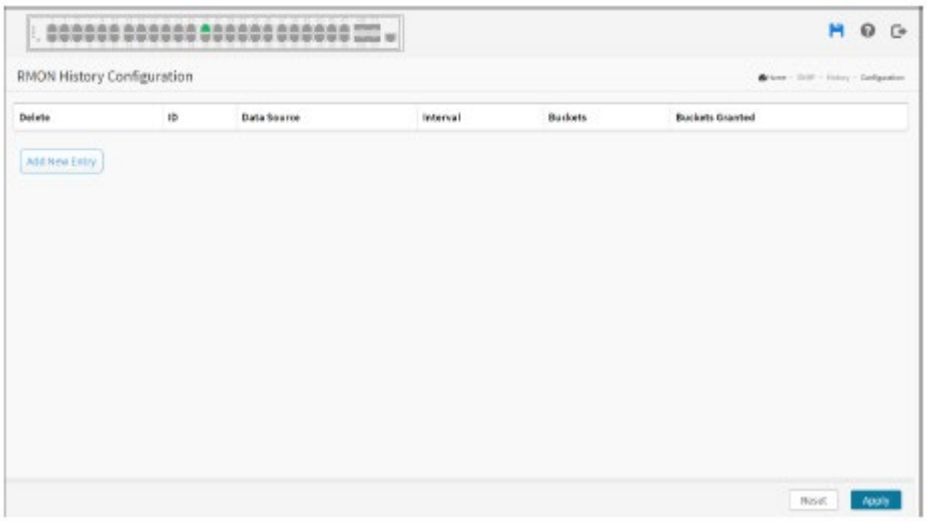
First Entry（最初のエントリー）：
最初のエントリーからテーブルを更新します。

Next Entry（次のエントリー）：
現在表示されている最後のエントリーの後のエントリーで始まるテーブルを更新します。

履歴

設定

この画面では、RMON 履歴テーブルを設定します。エントリーのインデックスキーは ID です。



Web インターフェース

Web インターフェースで RMON 履歴の設定を行うには:

1. 「SNMP」 > 「History」(履歴) > 「Configuration」(設定)をクリックしてください。
2. 「Add New Entry」(新規登録)をクリックしてください。

3. ID パラメーターを指定してください。
4. 「Apply」(適用)をクリックしてください。

■パラメーターの説明

これらのパラメーターは、RMON 履歴設定画面に表示されます。

ID：
エントリーのインデックスを示します。指定できる範囲は 1～65535 です。

Data Source（データソース）：
監視するポート ID を示します。スタッキングスイッチでは、値に 1000 ×（スイッチ ID-1）を加算する必要があります。例えば、ポートがスイッチ 3 のポート 5 の場合、値は 2005 です。

Interval（間隔）：
履歴統計データをサンプリングする間隔を秒単位で示します。指定できる範囲は 1～3600 で、デフォルト値は 1800 秒です。

Buckets（バケット）：
RMON に格納されたこの履歴制御エントリーに関連する最大データエントリーを示します。指定できる範囲は 1～3600 で、デフォルト値は 50 です。

Buckets Granted（付与されたバケット）：
データの数は RMON に保存されます。

■ボタン

Delete（削除）：
チェックを入れると、エントリーを削除します。これは、次回保存時に削除されます。

Add New Entry（新規登録）：
クリックすると、新しいエントリーが追加されます。

Apply（適用）：
クリックすると、変更内容を保存します。

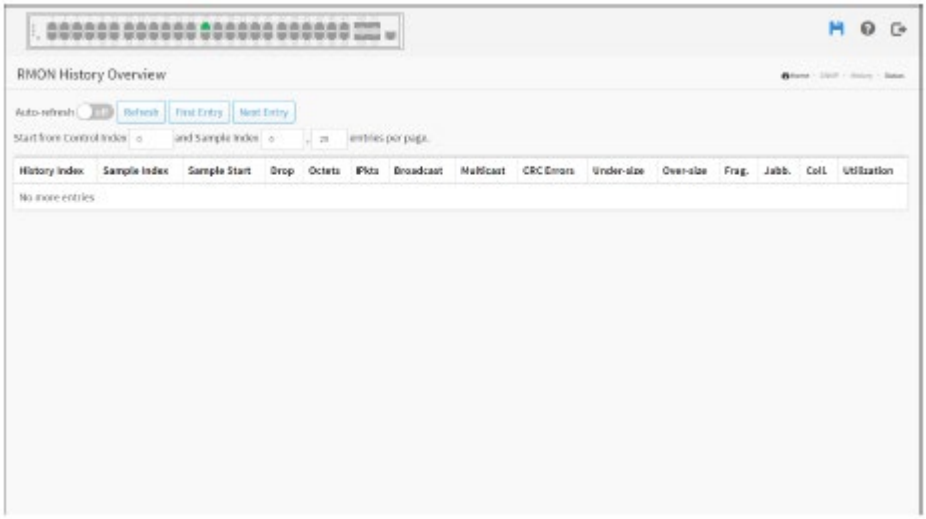
Reset（リセット）：
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

状態

この画面では RMON 履歴項目の概要を提供します。各ページには、履歴テーブルから最大 99 個のエントリーが表示されます。デフォルトは 20 で、「entries per page」(ページあたりのエントリー数)の入力フィールドで選択されています。最初にアクセスすると、Web ページには履歴テーブルの先頭から最初の 20 件のエントリーが表示されます。最初に表示されるのは、履歴テーブルにある履歴インデックスとサンプルインデックスが最も小さいものです。

「Start from History Index and Sample Index」(履歴インデックスとサンプルインデックスから開始)を使用すると、履歴テーブルで開始点を選択できます。「Refresh」(更新)ボタンをクリックすると、表示されているテーブルが、そのテーブルまたは次に近い履歴テーブルの一致から更新されます。

「Next Entry」(次のエントリー)は、現在表示されているエントリーの最後のエントリーを、次のルックアップの基準として使用します。最後に達すると、表示されたテーブルに「これ以上エントリーはありません」というテキストが表示されます。このような場合は、「First Entry」(最初のエントリー)ボタンを使用して、最初からやり直してください。



Web インターフェース

Web インターフェースに RMON 履歴の状態を表示するには:

1. 「SNMP」 > 「History」(履歴) > 「Status」(状態)をクリックしてください。
2. 「Auto-refresh」(自動更新)にチェックを入れてください。
3. ポートの詳細統計情報を更新するには、「Refresh」(更新)をクリックしてください。
4. エントリーを変更する場合は、「First Entry」(最初のエントリー)や「Next Entry」(次のエントリー)をクリックしてください。

■パラメーターの説明

History Index（履歴インデックス）：
履歴管理項目のインデックスを示します。

Sample Index（サンプルインデックス）：
制御エントリーに関連付けられたデータエントリーのインデックスを示します。

Sample Start（サンプル開始）：
このサンプルが測定されたインターバルの開始時における sysUpTime の値です。

Drop（破棄）：
リソース不足のためにプローブによってパケットが破棄されたイベントの合計数です。

Octets（オクテット）：
ネットワーク上で受信したデータの総オクテット数です（不良パケットのデータを含む）。

Pkts：
受信したパケットの総数です（不良パケット、ブロードキャストパケット、マルチキャストパケットを含む）。

Broadcast（ブロードキャスト）：
ブロードキャストアドレス宛に受信した正しいパケットの合計数です。

Multicast（マルチキャスト）：
マルチキャストアドレス宛に受信した正しいパケットの合計数です。

CRC Errors（CRC エラー）：
64 オクテットから 1518 オクテットまでの長さ（フレーミングビットは除き、FCS オクテットは含む）を持ちますが、整数オクテット（FCS エラー）を持つ不良フレームチェックシーケンス（FCS）またはオクテット数が整数でない不良 FCS（アライメントエラー）を持つ受信パケットの総数です。

Under-size（アンダーサイズ）：
64 オクテット未満で受信したパケットの合計数です。

Over-size（オーバーサイズ）：

1518 オクテットより長い受信パケットの合計数です。

Frag.:
無効な CRC で受信された 64 オクテット未満のサイズのフレームの数です。

Jabb.:
無効な CRC で受信した 64 オクテットより大きいサイズのフレームの数です。

Coll.:
このイーサネットセグメントのコリジョンを最適に見積もった合計数です。

Utilization(使用率):
このサンプリング間隔中において、このインターフェース上の物理レイヤの平均ネットワーク使用率の最良の推定値です(100 分の 1)。

Show entries(エントリーの表示):
表示する項目の数を選択できます。

■ボタン

Auto-refresh(自動更新):
画面を自動的に更新する場合は、このチェックボックスを ON にしてください。自動更新は 3 秒間隔で行われます。

Refresh(更新):
クリックすると、画面がすぐに更新されます。

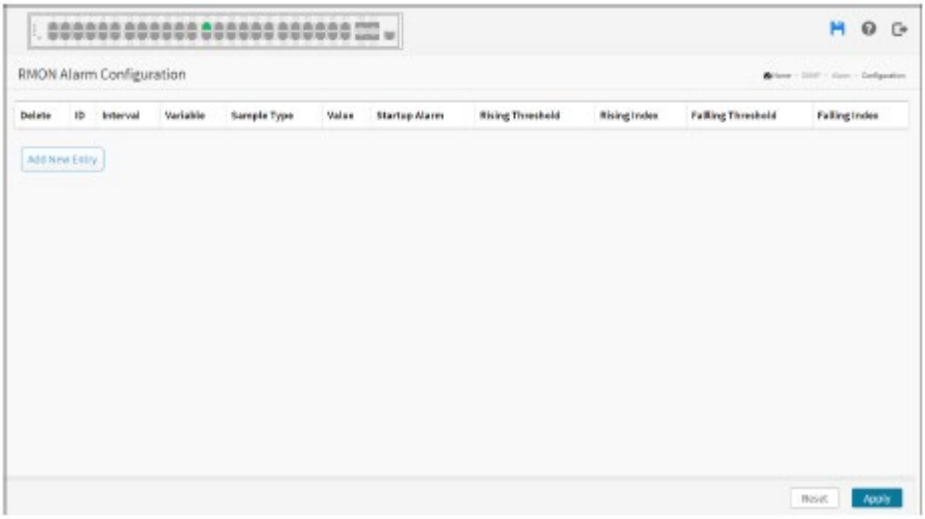
First Entry(最初のエントリー):
IPMC プロファイルアドレス設定の最初のエントリーからテーブルを更新します。

Next Entry(次のエントリー):
現在表示されている最後のエントリーの後のエントリーから開始して、テーブルを更新します。

アラーム

設定

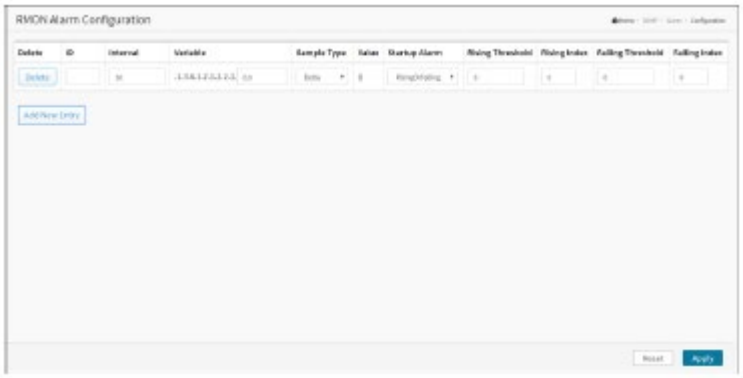
この画面では RMON アラームテーブルを設定します。エントリーのインデックスキーは ID です。



Web インターフェース

Web インターフェースで RMON アラームを設定するには:

1. 「SNMP」 ＞ 「Alarm」(アラーム) ＞ 「Configuration」(設定)をクリックしてください。
2. 「Add New Entry」(新規登録)をクリックしてください。



3. ID パラメーターを指定してください。
4. 「Apply」(適用)をクリックしてください。

■パラメーターの説明

これらのパラメーターは、RMON アラーム設定画面に表示されます。

ID：
エントリーのインデックスを示します。指定できる範囲は 1～65535 です。

Interval（間隔）：
サンプリングおよび上昇/下限しきい値の比較の間隔を秒単位で示します。指定できる範囲は 1～2^31-1 です。

Variables（変数）：
サンプリングされる特定の変数を示します。可能な変数は以下のとおりです。

InOctets：フレーミング文字を含むインターフェースで受信したバイトの総数です。

InUcastPkts：上位層プロトコルに配送されたユニキャストパケットの数です。

InNUcastPkts：上位層プロトコルに配信されたブロードキャストおよびマルチキャストパケットの数です。

InDiscards：パケットが正常であっても破棄されるインバウンドパケットの数です。

InErrors：上位層のプロトコルへの送信を妨げるエラーが含まれていた着信パケットの数です。

InUnknownProtos：未知またはサポートされていないプロトコルのために破棄されたインバウンドパケットの数です。

OutOctets：フレーミング文字を含む、インターフェースから送信されたオクテットの数です。

OutUcastPkts：送信を要求するユニキャストパケットの数です。

OutNUcastPkts：送信を要求するブロードキャストおよびマルチキャストパケットの数です。

OutDiscards：パケットが正常な場合に破棄されるアウトバウンドパケットの数です。

OutErrors：エラーのために送信できなかった送信パケットの数です。

OutQLen：送信パケットキューの長さです（パケット単位）。

Sample Type（サンプルタイプ）：
選択した変数をサンプリングし、しきい値と比較する値を計算する方法です。可能なサンプルタイプは次のとおりです。

Absolute：サンプルを直接取得します。

Delta：サンプル間の差を計算します（デフォルト）。

Value（値）：
最後のサンプリング期間中の統計の値です。

Startup Alarm（起動アラーム）：
選択した変数をサンプリングし、しきい値と比較する値を計算する方法です。可能なサンプルタイ

プは次のとおりです。

Rising Trigger alarm：最初の値が上昇しきい値より大きい場合にアラームをトリガーします。

FallingTrigger alarm：最初の値が下限しきい値より小さい場合にアラームをトリガーします。

RisingOrFallingTrigger alarm：最初の値が上昇しきい値より大きいか、下降しきい値より小さい場合にアラームをトリガーします（デフォルト）。

Rising Threshold（上昇しきい値）：
上昇しきい値です（-2147483648-2147483647）。

Rising Index（上昇インデックス）：
上昇イベントインデックスです（1-65535）。

Falling Threshold（下限しきい値）：
下限しきい値です（-2147483648-2147483647）。

Falling Index（下限インデックス）：
下限イベントインデックスです（1-65535）。

■ボタン

Delete（削除）：
チェックを入れると、エントリーを削除します。これは、次回保存時に削除されます。

Add New Entry（新規登録）：
クリックすると、新しいエントリーを追加します。

Apply（適用）：
クリックすると、変更内容を保存します。

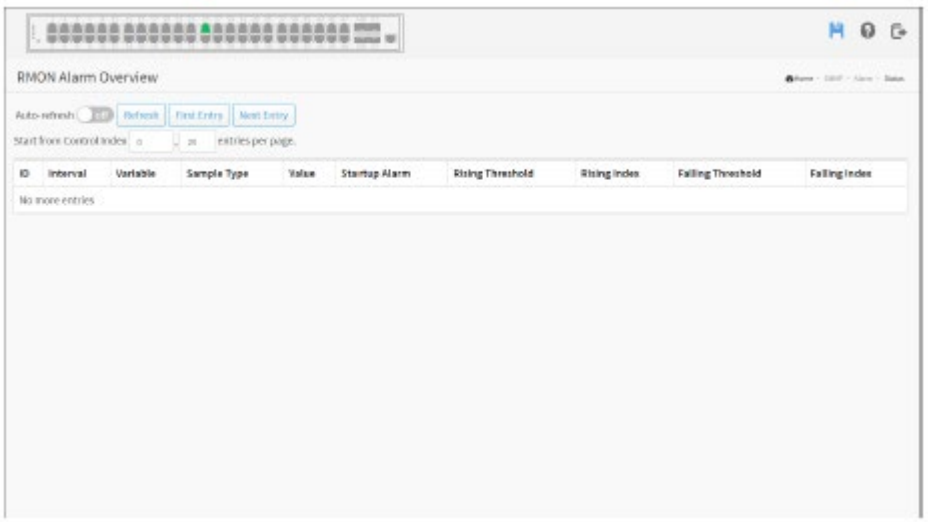
Reset（リセット）：
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

状態

この画面では、RMON アラームエントリーの概要を説明します。各ページには、アラームテーブルから最大 99 のエントリーが表示されます。デフォルトは 20 で、「entries per page」（ページあたりのエントリー数）の入力フィールドで選択されています。最初に表示された Web ページには、アラームテーブルの最初から 20 件のエントリーが表示されます。最初に表示されるのは、アラームテーブルで見つかった ID が最も小さいものです。

「Start from Control Index」（制御インデックスから開始）では、アラームテーブルの開始点を選択できます。「Refresh」（更新）ボタンをクリックすると、そのテーブルまたは次に近いアラームテーブルの一致から表示されているテーブルが更新されます。

「Next Entry」（次のエントリー）は、現在表示されているエントリーの最後のエントリーを、次のルックアップの基準として使用します。最後に達すると、表示されたテーブルに「これ以上エントリーはありません」というテキストが表示されます。このような場合には、「First Entry」（最初のエントリー）ボタンを使用して、最初からやり直してください。



Web インターフェース

Web インターフェースに RMON アラームの状態を表示するには：

1. 「SNMP」 ＞ 「Alarm」（アラーム） ＞ 「Status」（状態）をクリックしてください。
2. 「Auto-refresh」（自動更新）にチェックを入れてください。
3. ポートの詳細統計情報を更新するには、「Refresh」（更新）をクリックしてください。
4. エントリーを変更する場合は、「First Entry」（最初のエントリー）や「Next Entry」（次のエントリー）をクリックしてください。

■パラメーターの説明

ID：
アラーム制御エントリーのインデックスを示します。

Interval（間隔）：
サンプリングおよび上昇/下限しきい値の比較の間隔を秒単位で示します。サンプリングする特定の変数を「Sample Type」（サンプルタイプ）で指定します。選択した変数をサンプリングし、しきい値と比較する値を計算する方法です。

Value（値）：
最後のサンプリング期間中の統計の値です。

Startup Alarm（起動アラーム）：
このエントリーが最初に有効に設定されたときに送信される可能性があるアラームです。

Rising Threshold（上昇しきい値）：
上昇しきい値です。

Rising Index（上昇インデックス）：
上昇イベントインデックスです。

Falling Threshold（下限しきい値）：
下限しきい値です。

Falling Index（下限インデックス）：
下限イベントインデックスです。

Show entries（エントリーの表示）：
表示する項目の数を選択できます。

■ボタン

Auto-refresh（自動更新）：
画面を自動的に更新する場合は、このチェックボックスをONにしてください。自動更新は3秒間

隔で行われます。

Refresh（更新）：
クリックすると、画面がすぐに更新されます。

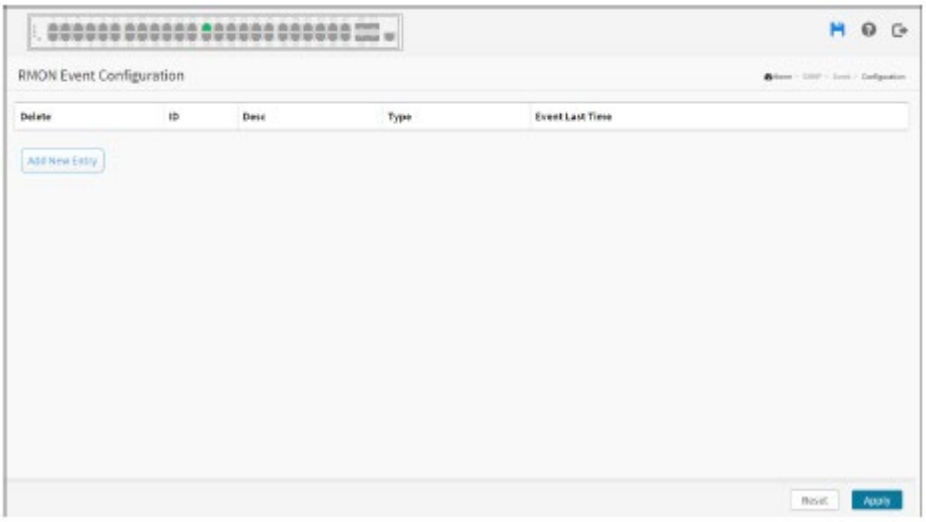
First Entry（最初のエントリー）：
IPMC プロファイルアドレス設定の最初のエントリーからテーブルを更新します。

Next Entry（次のエントリー）：
現在表示されている最後のエントリーの後のエントリーから開始して、テーブルを更新します。

イベント

設定

この画面では、RMON イベントテーブルを設定します。エントリーのインデックスキーは ID です。



Web インターフェース

Web インターフェースで RMON イベントを設定するには:

1. 「SNMP」 ＞ 「Event」(イベント) ＞ 「Configuration」(設定)をクリックしてください。
2. 「Add New Entry」(新規登録)をクリックしてください。

3. ID パラメーターを指定してください。
4. 「Apply」(適用)をクリックしてください。

■パラメーターの説明

これらのパラメーターは、RMON 履歴設定画面に表示されます。

ID：
エントリーのインデックスを示します。指定できる範囲は 1～65535 です。

Desc（説明）：
このイベントを示します。文字列の長さは 0～127 で、デフォルトは NULL の文字列です。

Type（タイプ）：
イベントの通知を示します。可能なタイプは以下のとおりです。

None（なし）：SNMP ログは作成されず、SNMP トラップも送信されません。
Log（ログ）：イベントがトリガーされたときに SNMP ログエントリーを作成します。
Snmp trap（SNMP トラップ）：イベント発生時に SNMP トラップを送信します。
Log and trap（ログとトラップ）：SNMP ログエントリーを作成し、イベントがトリガーされたときに SNMP トラップを送信します。

Event Last Time（最終イベント時刻）：
このイベントのエントリーが最後にイベントを生成した時点の sysUpTime の値を示します。

■ボタン

Delete（削除）：
チェックを入れると、エントリーを削除します。これは、次回保存時に削除されます。

Add New Entry（新規登録）：
クリックすると、新しいエントリーが追加されます。

Apply（適用）：
クリックすると、変更内容を保存します。

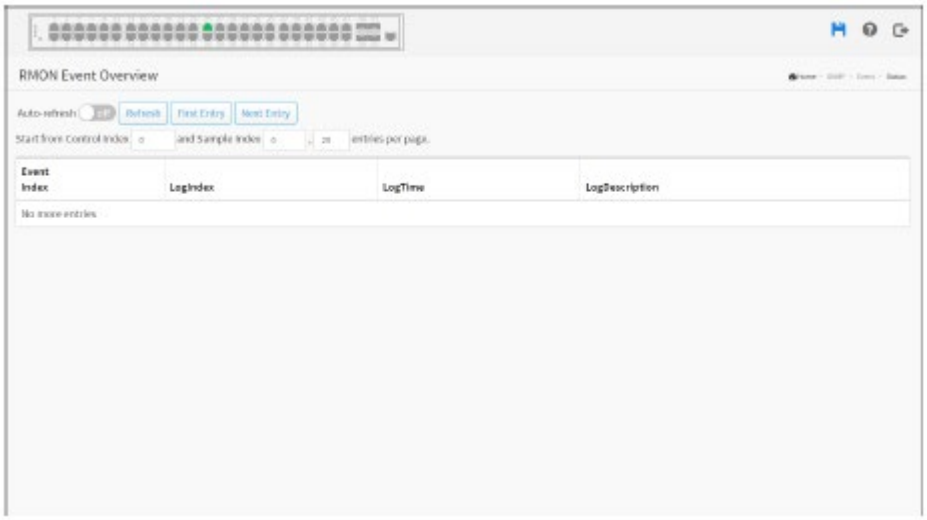
Reset（リセット）：
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

状態

この画面では、RMON イベントテーブルにおけるエントリーの概要を提供します。各ページには、イベントテーブルから最大 99 のエントリーが表示されます。デフォルトは 20 で、「entries per page」（ページあたりのエントリー数）の入力フィールドで選択されています。最初にアクセスすると、Web ページにはイベントテーブルの先頭から最初の 20 個のエントリーが表示されます。最初に表示されるのは、イベントテーブルで見つかったイベントインデックスとログインデックスが最も小さいものです。

「Start from Event Index and Log Index」（イベントインデックスとログインデックスから開始）では、イベントテーブルの開始点を選択できます。「Refresh」（更新）ボタンをクリックすると、表示されているテーブルが、そのテーブルまたは次に近いイベントテーブルの一致から更新されます。

「Next Entry」（次のエントリー）は、現在表示されているエントリーの最後のエントリーを、次のルックアップの基準として使用します。最後に達すると、表示されたテーブルに「これ以上エントリーはありません」というテキストが表示されます。このような場合は、「First Entry」（最初のエントリー）ボタンを使用して、最初からやり直してください。



Web インターフェース

Web インターフェースに RMON イベントの状態を表示するには:

1. 「SNMP」 ＞ 「Event」（イベント） ＞ 「Status」（状態）をクリックしてください。
2. 「Auto-refresh」（自動更新）にチェックを入れてください。
3. ポートの詳細統計情報を更新するには、「Refresh」（更新）をクリックしてください。
4. エントリーを変更する場合は、「First Entry」（最初のエントリー）や「Next Entry」（次のエントリ

ー）をクリックしてください。

■パラメーターの説明

Event Index（イベントインデックス）：
イベントエントリーのインデックスを示します。

Log Index（ログインデックス）：
ログエントリーのインデックスを示します。

Log Time（ログ時刻）：
イベントログ時刻を示します。

Log Description（ログの説明）：
イベントの説明を示します。

Show entries（エントリーの表示）：
表示する項目の数を選択できます。

■ボタン

Auto-refresh（自動更新）：
画面を自動的に更新する場合は、このチェックボックスをONにしてください。自動更新は3秒間隔で行われます。

Refresh（更新）：
クリックすると、画面がすぐに更新されます。

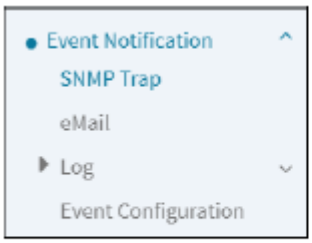
First Entry（最初のエントリー）：
IPMC プロファイルアドレス設定の最初のエントリーからテーブルを更新します。

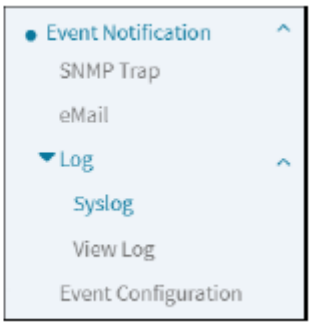
Next Entry（次のエントリー）：
現在表示されている最後のエントリーの後のエントリーから開始して、テーブルを更新します。

第 15 章
イベント通知

概要

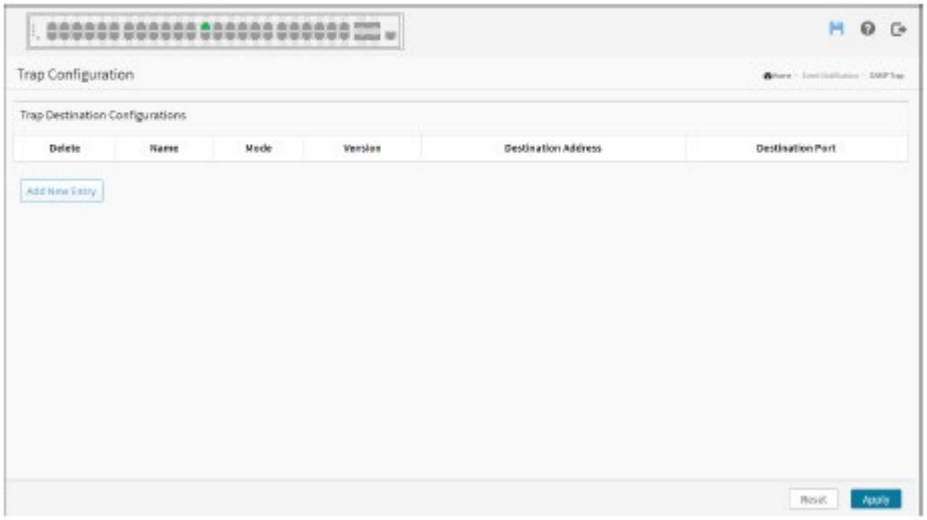
メニューとサブメニューを以下に示します。





SNMP トラップ

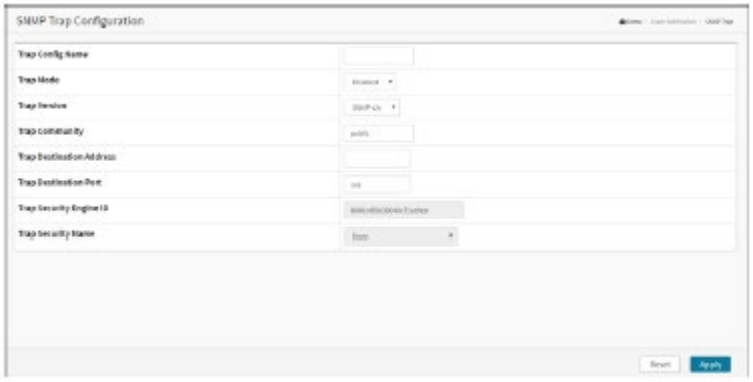
この画面では、トラップを設定します。



Web インターフェース

Web インターフェースで SNMP トラップを設定するには:

1. 「Event Notification」(イベント通知) ＞ 「SNMP Trap」(SNMP トラップ)をクリックしてください。
2. 「Add New Entry」(新規登録)をクリックして、スイッチに新しい SNMP トラップを作成してください。



3. SNMP トラップのパラメーターを指定してください。
4. 「Apply」(適用)をクリックしてください。

■パラメーターの説明

Trap Destination Configurations（トラップ宛先設定）

Name（名前）：

トラップ設定の名前を示します。トラップ宛先の名前を示します。

Enable（有効にする）：

トラップ宛先モードの操作を示します。有効なモードは次のとおりです。

Enabled（有効）：SNMP トラップモードの操作を有効にします。

Disabled（無効）：SNMP トラップモードの操作を無効にします。

Version（バージョン）：

SNMP トラップがサポートされているバージョンを示します。可能なバージョンは次のとおりです。

SNMPv1：SNMP トラップがサポートされているバージョン 1 を設定します。

SNMPv2c：SNMP トラップ対応バージョン 2c を設定します。

SNMPv3：SNMP トラップ対応バージョン 3 を設定します。

Destination Address（宛先アドレス）：

ドット付き 10 進表記（*x.y.z.w*）で有効な IP アドレスを使用できます。

また、有効なホスト名も許可します。有効なホスト名は、アルファベット（A～Z、a～z）、数字（0～9）、ドット（.）、ダッシュ（-）から構成された文字列です。スペースは使用できません。最初の文字はアルファベットでなければなりません。また、最初と最後の文字にドットやダッシュを使用することはできません。

これは、SNMP トラップの宛先 IPv6 アドレスを示します。IPv6 アドレスは、各項目（:）をコロンで区切った最大 4 桁の 16 進数の 8 項目で表される 128 ビットのレコードです。例） fe80:#2]c5ff:fe03:4dc7 シンボル「::」は、連続するゼロの複数の 16 ビットグループを表す短縮形として使用できる特別な構文ですが、一度しか使用できません。また、合法的に有効な IPv4 アドレスを表すこともできます。例）::192.1.2.34

Destination port（宛先ポート）：

SNMP トラップの宛先ポートを示します。SNMP エージェントはこのポートを介して SNMP メッセージを送信します。ポート範囲は 1～65535 です。

SNMP Trap Configuration（SNMP トラップの設定）

Trap Config Name（トラップ設定名）：

設定するトラップの名前を示します。許可される文字列の長さは 1～32 で、許可される内容は

ASCII 文字（33～126）です。

Trap Mode（トラップモード）：
SNMP モードの操作を示します。有効なモードは次のとおりです。
on：SNMP モードの操作を有効にします。
off：SNMP モードの操作を無効にします。

Trap Version（トラップバージョン）：
SNMP がサポートされているバージョンを示します。可能なバージョンは次のとおりです。
SNMP v1：SNMP サポートバージョン 1 を設定します。
SNMP v2c:SNMP サポートバージョン 2c を設定します。
SNMP v3：SNMP サポートバージョン 3 を設定します。

Trap Community（トラップコミュニティ）：
SNMP トラップパケット送信時のコミュニティアクセス文字列を示します。許可される文字列の長さは 0～63 で、許可される内容は ASCII 文字（33～126）です。

Trap Destination Address（トラップ送信先アドレス）：
SNMPトラップの宛先アドレスを示します。ドット付き 10 進表記（*x.y.z.w*）で有効な IP アドレスを使用できます。
また、有効なホスト名も許可します。有効なホスト名は、アルファベット（A～Z、a～z）、数字（0～9）、ドット（.）、ダッシュ（-）から構成された文字列です。スペースは使用できません。最初の文字はアルファベットでなければなりません。また、最初と最後の文字にドットやダッシュを使用することはできません。
これは、SNMP トラップの宛先 IPv6 アドレスを示します。IPv6 アドレスは、各項目（:）をコロンで区切った最大 4 桁の 16 進数の 8 項目で表される 128 ビットのレコードです。例） fe80:#2]c5ff:fe03:4dc7
シンボル「::」は、連続するゼロの複数の 16 ビットグループを表す短縮形として使用できる特別な構文ですが、一度しか使用できません。また、合法的に有効な IPv4 アドレスを表すこともできます。
例）::192.1.2.34

Trap Destination port（トラップ宛先ポート）：
SNMP トラップの宛先ポートを示します。SNMP エージェントはこのポートを介して SNMP メッセージを送信します。ポート範囲は 1～65535 です。

Trap Security Engine ID（トラップセキュリティエンジン ID）：
SNMP トラップセキュリティエンジン ID を示します。SNMPv3 は、認証とプライバシーのために USM

を使用してトラップとインフォームを送信します。これらのトラップとインフォームには、一意のエンジン ID が必要です。「Trap Probe Security Engine ID」（トラッププローブセキュリティエンジン ID）を有効にすると、ID は自動的に精査されます。それ以外の場合は、このフィールドで指定された ID が使用されます。文字列には、10～64 の桁数の偶数（16 進形式）を含める必要がありますが、すべてを 0（ゼロ）にしたり、すべてを F にしたりすることはできません。

Trap Security Name（トラップセキュリティ名）：
SNMPv3 は、認証とプライバシーのために USM を使用してトラップとインフォームを行います。トラップとインフォームが有効になっている場合は、一意のセキュリティ名が必要です。

■ボタン

Add New Entry（新規登録）：
クリックすると、新しいエントリーが追加されます。

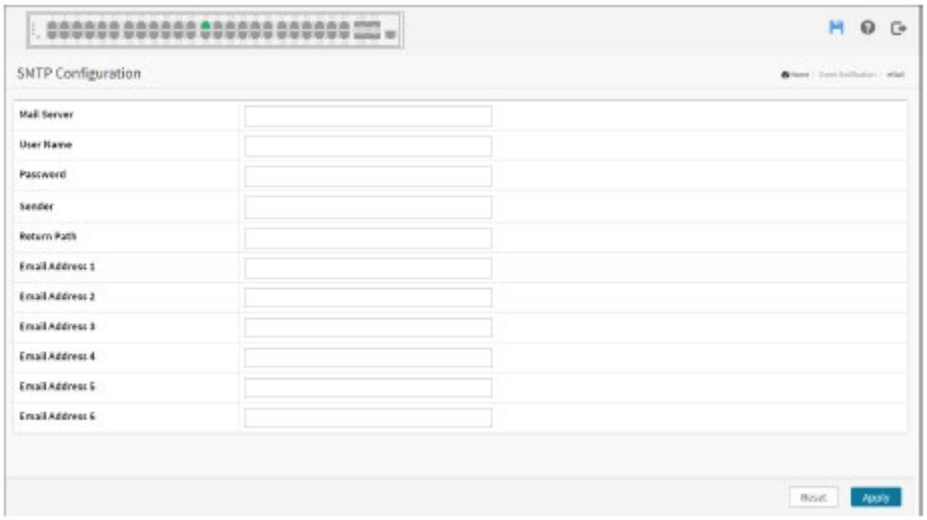
Apply（適用）：
クリックすると、変更内容を保存します。

Reset（リセット）：
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

E メール

この画面では、SMTP（Simple Mail Transfer Protocol）を設定します。SMTP（Simple Mail Transfer Protocol）は、インターネットのメッセージ交換規格です。

サーバーが、アラームイベントが発生したというメッセージをスイッチから受信するリモートデバイスである間、このスイッチは SMTP のクライアントとして設定されます。



Web インターフェース

Web インターフェースで SMTP を設定するには：

1. 「Event Notification」（イベント通知） ＞ 「eMail」（E メール）をクリックしてください。
2. SMTP 設定パラメーターを指定してください。
3. 「Apply」（適用）をクリックしてください。

■パラメーターの説明

Mail Server（メールサーバー）：

メールサーバーの IP アドレスまたはホスト名です。IP アドレスは、ドット付き 10 進表記で表されます。これは、メールを送信するデバイスになります。

User Name（ユーザー名）：

メールサーバーのユーザー名を指定してください。

Password（パスワード）：

メールサーバー上のユーザーのパスワードを指定してください。

Sender（送信者）：
警告メールの送信者名を指定してください。

Return Path（リターンパス）：
警告メールの送信者メールアドレスを指定してください。これは、E メールメッセージの送信元アドレスになります。

Email Address #（メールアドレス#）：
受信者の E メールアドレスを指定してください。

■ボタン

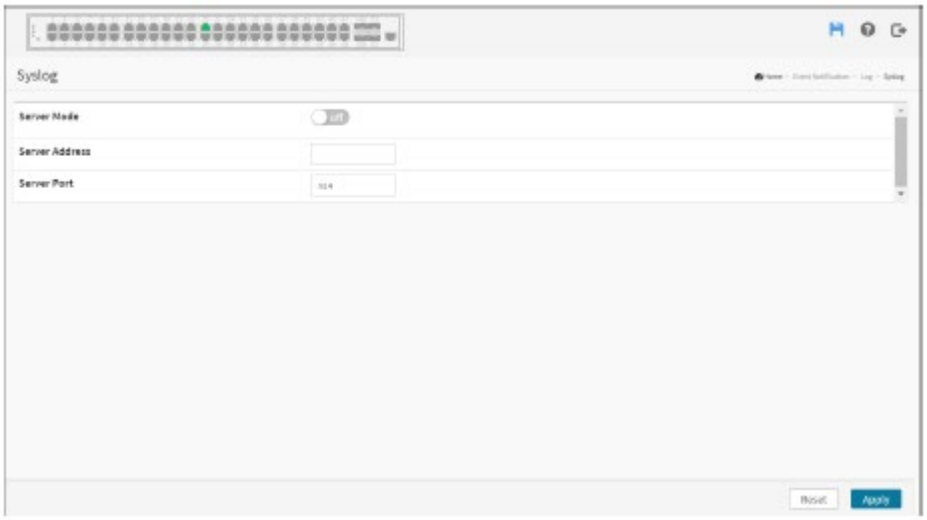
Apply（適用）：
クリックすると、変更内容を保存します。

Reset（リセット）：
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

ログ

Syslog

Syslog 設定は、プログラムメッセージを記録するための規格です。メッセージを格納するシステムから、メッセージを生成するソフトウェアと、メッセージをレポートおよび分析するソフトウェアを分離することができます。これは、一般化された情報、分析、デバッグメッセージにも使用することができます。また、これは、複数のプラットフォームにまたがる幅広い種類のデバイスおよびレシーバーによってサポートされています。



Web インターフェース

Web インターフェースで Syslog を設定するには:

1. 「Event Notification」(イベント通知) ＞ 「Log」(ログ) ＞ 「Syslog」をクリックしてください。
2. サーバーモードを有効にしてください。
3. Syslog のパラメーターとして、サーバーアドレスとサーバーポートを指定してください。
4. 「Apply」(適用)をクリックしてください。

■パラメーターの説明

Server Mode(サーバーモード):

サーバーモードの操作を示します。モード操作が有効になっている場合、Syslog メッセージは Syslog サーバーに送信されます。Syslog プロトコルは UDP 通信に基づいており、UDP ポート 514 で受信されます。UDP はコネクションレスプロトコルであり、確認応答を提供しないため、Syslog サーバーは確認応答を送信者に返しません。Syslog サーバーが存在しない場合でも、Syslog パケット

は常に送信されます。使用可能なモードは、次のとおりです。

Enabled（有効）：サーバーモードの操作を有効にします。

Disabled（無効）：サーバーモードの操作を無効にします。

Server Address（サーバーアドレス）：

Syslog サーバーの IPv4 ホストアドレスを示します。スイッチが DNS 機能を提供する場合は、ドメイン名にすることもできます。

Server Port（サーバーポート）：

Syslog サーバーのサービスポートを示します。

■ボタン

Apply（適用）：

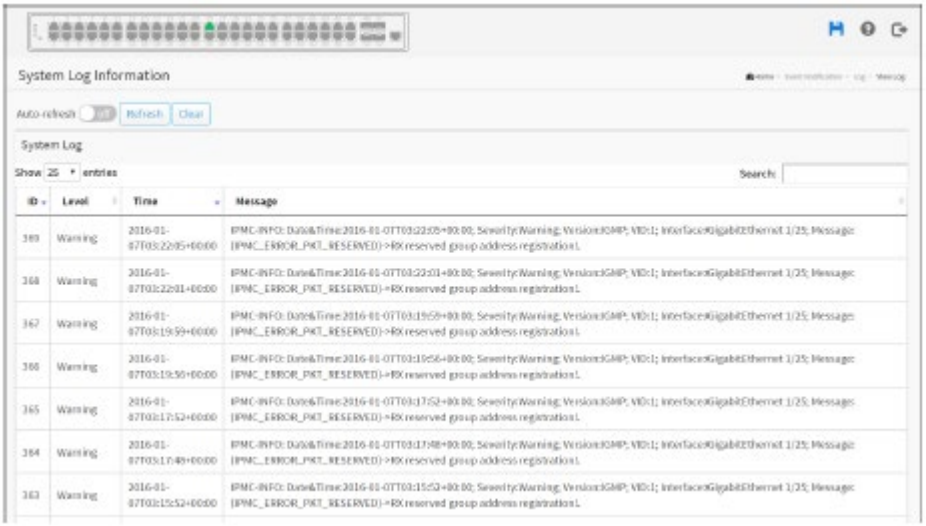
クリックすると、変更内容を保存します。

Reset（リセット）：

クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

ログの参照

このセクションでは、スイッチのシステムログ情報を表示する方法について説明します。



Web インターフェース

Web インターフェースでログ情報を表示するには:

1. 「Event Notification」(イベント通知) ＞ 「Log」(ログ) ＞ 「View Log」(ログの参照)をクリックしてください。
2. ログ情報を表示してください。

■パラメーターの説明

ID:

システムログエントリーの ID(1 以上)です。

Level(レベル):

システムログエントリーのレベルです。以下のレベルタイプがサポートされています。

Debug(デバッグ):デバッグレベルのメッセージです。

Info(情報):情報メッセージです。

Notice(通知):正常ですが、重大な状態です。

Warning(注意):注意が必要な状態です。

Error(エラー):エラーの状態です。

Crit(重大):障害状態です。

Alert(警告):アクションをすぐに実行する必要があります。

Emerg(緊急):システムが使用できません。

Time（時間）：
ログレコードがデバイス時間別に表示されます。システムログエントリーの時刻です。

Message（メッセージ）：
ログ詳細メッセージが表示されます。システムログエントリーのメッセージです。

Search（検索）：
表示する情報を検索できます。

Show entries（エントリーの表示）：
表示する項目の数を選択できます。

■ボタン

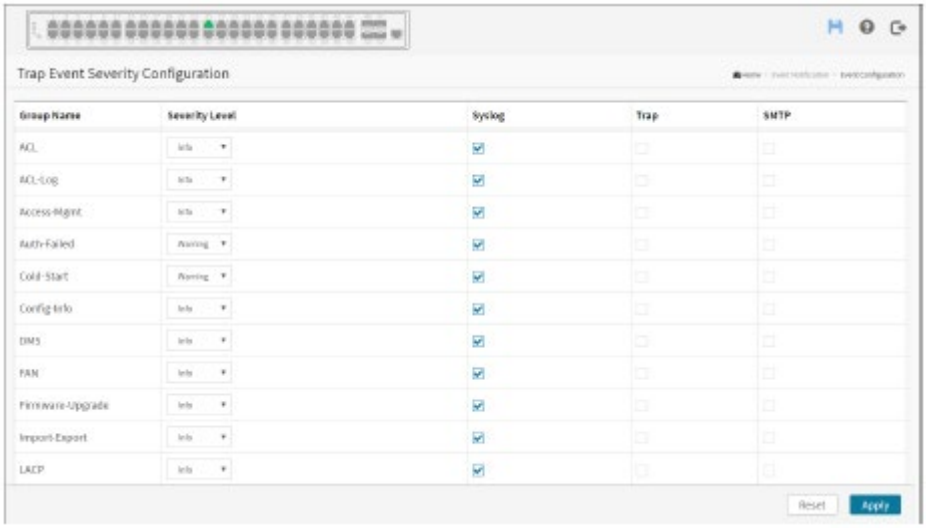
Auto-refresh（自動更新）：
画面を自動的に更新する場合は、このチェックボックスをONにしてください。自動更新は3秒間隔で行われます。

Refresh（更新）：
クリックするとページを更新します。

Clear（消去）：
クリックすると、画面の内容をクリアします。

イベント設定

この画面には、現在のトラップイベントの重大度の設定が表示されます。トラップイベントの重大度もここで設定できます。



Web インターフェース

Web インターフェースでトラップイベントの重大度の設定を表示するには:

1. 「Event Notification」(イベント通知) ＞ 「Event Configuration」(イベント通知)をクリックしてください。
2. スクロールして、グループ名と重大度のレベルを選択してください。
3. 「Enable」(有効にする)をクリックして、別のトラップイベントを選択してください。
4. 「Apply」(適用)をクリックして設定を保存してください。
5. 設定を取り消す場合は、「Reset」(リセット)ボタンをクリックする必要があります。そうすると、以前に保存した値へと戻ります。

■パラメーターの説明

Group Name(グループ名):

重大度グループを識別する名前です。

Severity Level(重大度レベル):

すべてのグループには重大度レベルがあります。以下のレベルタイプがサポートされています。

<0>Emergency(<0>緊急):システムが使用できません。

<1>Alert(<1>警告):すぐに対処する必要があります。

<2>Critical(<2>重大):重大な状態です。
<3>Error(<3>エラー):エラーの状態です。
<4>Warning(<4>注意):注意が必要な状態です。
<5>Notice(<5>通知):正常ですが、重大な状態です。
<6>Imformation(<6>情報):情報メッセージです。
<7>Debug(<7>デバッグ):デバッグレベルのメッセージです。

Syslog:
Enable(有効):Syslog でこのグループ名を選択します。

Trap(トラップ):
Enable(有効):このグループ名をトラップで選択します。

Switch2go:
Enable(有効):プッシュ通知でこのグループ名を選択します。

■ボタン

Apply(適用):
クリックすると、変更内容を保存します。

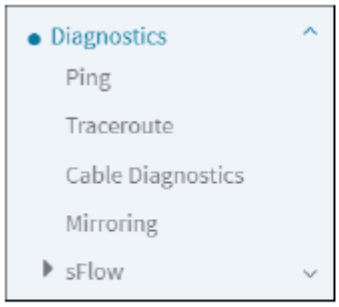
Reset(リセット):
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

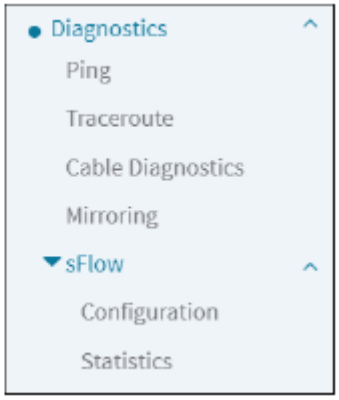
第 16 章
診断

概要

この章では、基本的なシステム診断について説明します。これには、Ping、トレースルート、ケーブル診断、およびポートミラーリングが含まれます。

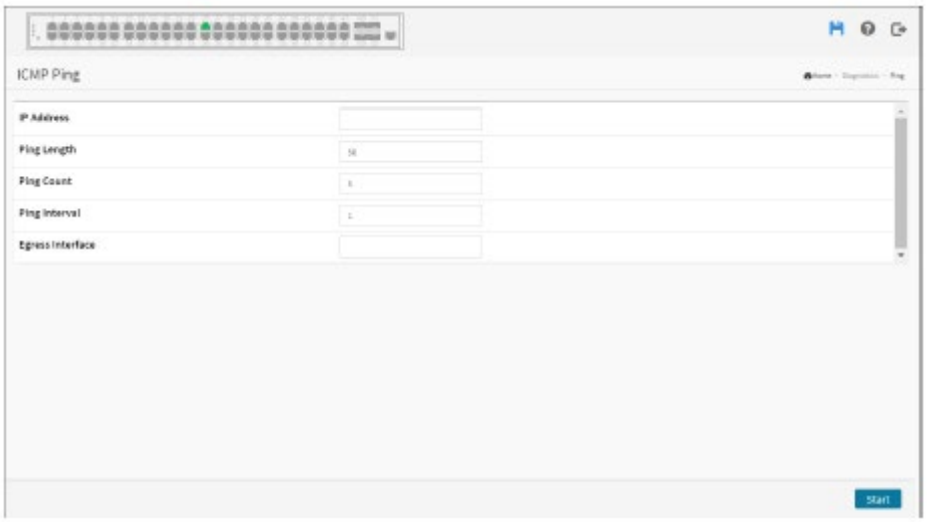
メニューとサブメニューを以下に示します。





Ping

このセクションでは、ICMP エコーのパケットを発行して、IPv4/6 接続の問題をトラブルシューティングできます。



Web インターフェース

Web インターフェースで Ping を設定するには:

1. 「Diagnostics」(診断) ＞ 「Ping」をクリックしてください。
2. IP アドレス、Ping 長、Ping 数、Ping 間隔、および出力インターフェースを指定してください。
3. 「Start」(開始)をクリックしてください。

■パラメーターの説明

IP Address (IP アドレス) :

Ping のターゲット IP アドレスを指定します。

Ping Length (Ping 長) :

ICMP パケットのペイロードサイズです。値の範囲は 2～1452 バイトです。

Ping Count (Ping 数) :

ICMP パケットの数です。値の範囲は 1～60 回です。

Ping Interval (Ping 間隔) :

ICMP パケットの間隔です。値の範囲は 0～30 秒です。

Egress Interface （イグレスインターフェース）（IPv6 のみ）:
ICMP パケットが送信される特定のイグレス IPv6 インターフェースの VLAN ID（VID）です。
指定された VID の範囲は 1～4094 で、対応する IPv6 インターフェースが有効な場合にのみ有効です。
イグレスインターフェースが指定されていない場合、PING6 は宛先に最適なインターフェースを見つけます。
ループバックアドレスには、イグレスインターフェースを指定しないでください。
リンクローカルまたはマルチキャストアドレスには、イグレスインターフェースを指定してください。

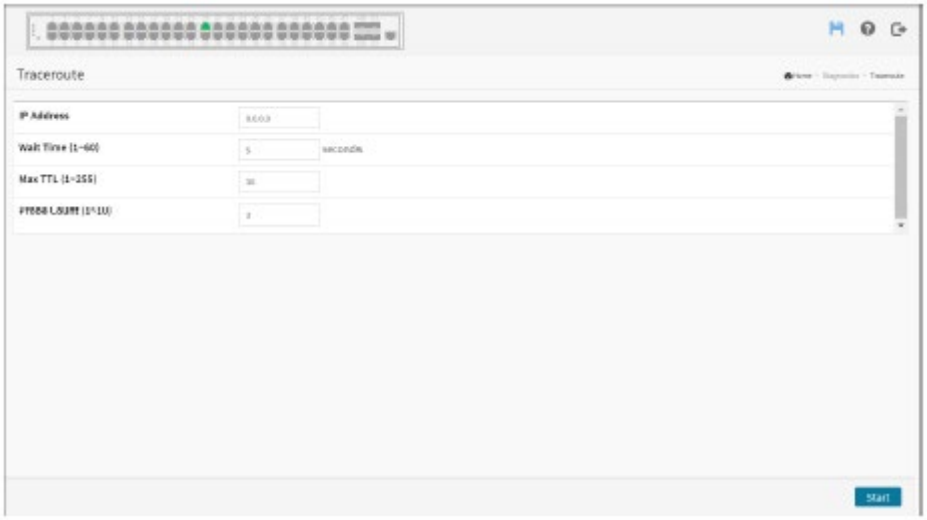
■ボタン

Start（開始）:
「Start」（開始）ボタンをクリックすると、ターゲット IP アドレスへの ping を開始します。

New Ping（新規 Ping）:
「ICMP Ping」画面に戻ります。

トレースルート

この画面では、ICMP、TCP、または UDP パケットを発行して、ネットワーク接続の問題を診断できます。



Web インターフェース

Web インターフェースでトレースルートを起動するには:

1. 「Diagnostics」(診断) ＞ 「Traceroute」(トレースルート)をクリックしてください。
2. IP アドレス、待機時間、最大 TTL、およびプローブ数を指定してください。
3. 「Start」(開始)をクリックしてください。

■パラメーターの説明

IP Address(IP アドレス):

宛先 IP アドレスです。

Wait Time(待機時間):

プローブへの応答を待機する時間(秒)を設定します(デフォルトは 5.0 秒)。値の範囲は 1～60 です。

Max TTL（最大 TTL）:
トレースルートがプローブするホップの最大数（最大有効期間の値）を指定します。値の範囲は 1～255 です。デフォルトでは 30 に設定されています。

Probe Count（プローブ数）:
ホップあたりのプローブパケット数を設定します。値の範囲は 1～10 です。デフォルトでは 3 に設定されています。

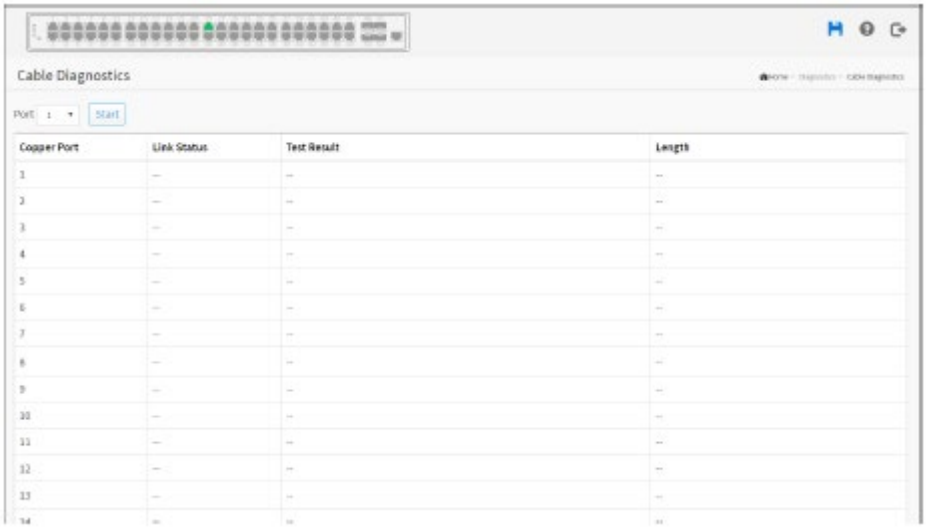
■ボタン

Start（開始）:
「Start」（開始）ボタンをクリックすると、ターゲット IP アドレスのトレースルートを開始します。

New Traceroute（新規トレースルート）:
トレースルート画面に戻ります。

ケーブル診断

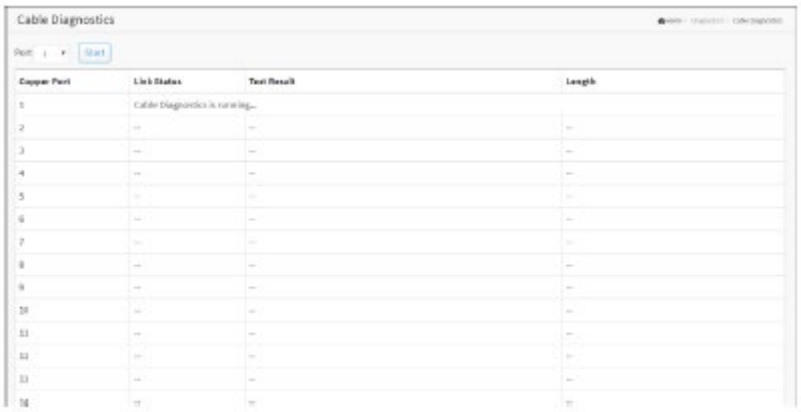
このセクションでは、銅線用ポートのケーブル診断を実行する方法を示します。



Web インターフェース

Web インターフェースでケーブル診断を設定するには:

1. 「Diagnostics」(診断) ＞ 「Cable Diagnostics」(ケーブル診断)をクリックしてください。
2. 確認するポートを指定してください。
3. 「Start」(開始)をクリックしてください。



■パラメーターの説明

Port (ポート) :

ケーブル診断を要求しているポートです。

Copper Port（銅線用ポート）:
銅線用ポートの番号です。

Link Status（リンクの状態）:
ケーブルの状態です。

10M：ケーブルはリンクアップしており、正常です。速度は 10Mbps です。

100M：ケーブルはリンクアップしており、正常です。速度は 100Mbps です。

1G：ケーブルはリンクアップしており、正常です。速度は 1Gbps です。

Link Down（リンクダウン）：リンクダウンしているか、ケーブルが正しくありません。

Test Result（テスト結果）:
ケーブルのテスト結果です。

OK：ペアが正常に終了しました。

Abnormal（異常）：ペアが不正に終了したか、リンクダウンしています。

Length（長さ）:
ケーブルペアの長さ（メートル）です。解像度は 3 メートルです。リンクの状態が以下のように表示されている場合は、長さの定義が異なります。

1G：長さは 4 ペアの最小値です。

10M/100M：長さは 2 ペアの最小値です。

Link Down（リンクダウン）：長さは、4 ペアの非ゼロの最小値です。

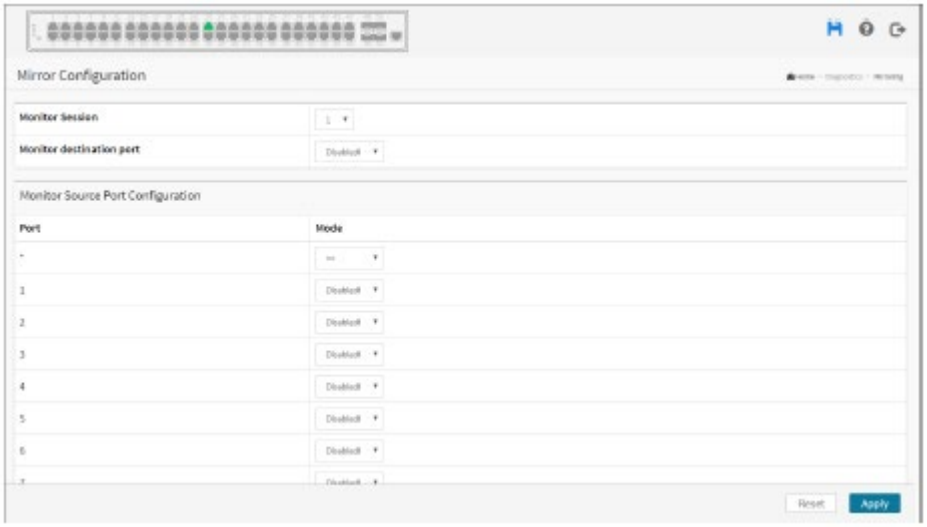
■ボタン

Start（開始）:
選択したポートのケーブル診断を開始します。

ミラーリング

リアルタイム分析を行うために、任意の送信元ポートからターゲットポートへのトラフィックをミラーリングすることができます。その後、ロジックアナライザーまたは RMON プローブをターゲットポートに接続し、送信元ポートを通過するトラフィックを、通信の妨げにならない方法で調べることができます。

ミラーリングの設定は、ネットワークのトラフィックを監視します。例えば、ポート A がモニタリングを行うポートで、ポート B がモニタリングされるポートであると仮定すると、ポート B によって受信されたトラフィックはモニタリングのためにポート A にコピーされます。



Web インターフェース

Web インターフェースでポートのミラーリング機能を設定するには:

1. 「Diagnostics」(診断) ＞ 「Mirroring」(ミラーリング)をクリックしてください。
2. モニター対象となるポート(ミラーポート)を選択してください。
3. モニタリングされるポートそれぞれに対して、モード(無効、有効、送信のみ、および受信のみ)を選択してください。
4. 「Apply」(適用)ボタンをクリックして、設定を保存してください。
5. 設定を取り消す場合は、「Reset」(リセット)ボタンをクリックして、以前に保存した値に戻す必要があります。

■パラメーターの説明

Monitor Destination Port(モニター先のポート):

ミラーリングされたトラフィックを出力するポートです。これはミラーポートとも呼ばれます。送信元（rx）または宛先（tx）ミラーリングが有効になっているポートからのフレームは、このポートでミラーリングされます。

Mirror Source Port Configuration（ミラー送信元ポートの設定）
Rx および Tx の有効化には、次のテーブルを使用します。

Port（ポート）：
同じ行に含まれる設定の論理ポートです。

Mode（モード）：
ミラーモードを選択します。

Rx only（受信のみ）：このポートで受信したフレームは、ミラーポートでミラーリングされます。送信されたフレームはミラーリングされません。
Tx only（送信のみ）：このポートで送信されたフレームは、ミラーポートでミラーリングされます。受信したフレームはミラーリングされません。
Disabled（無効）：送信されたフレームも受信されたフレームもミラーリングされません。
Enabled（有効）：受信フレームと送信フレームはミラーポートでミラーリングされます。

■ボタン

Apply（適用）：
クリックすると、変更内容を保存します。

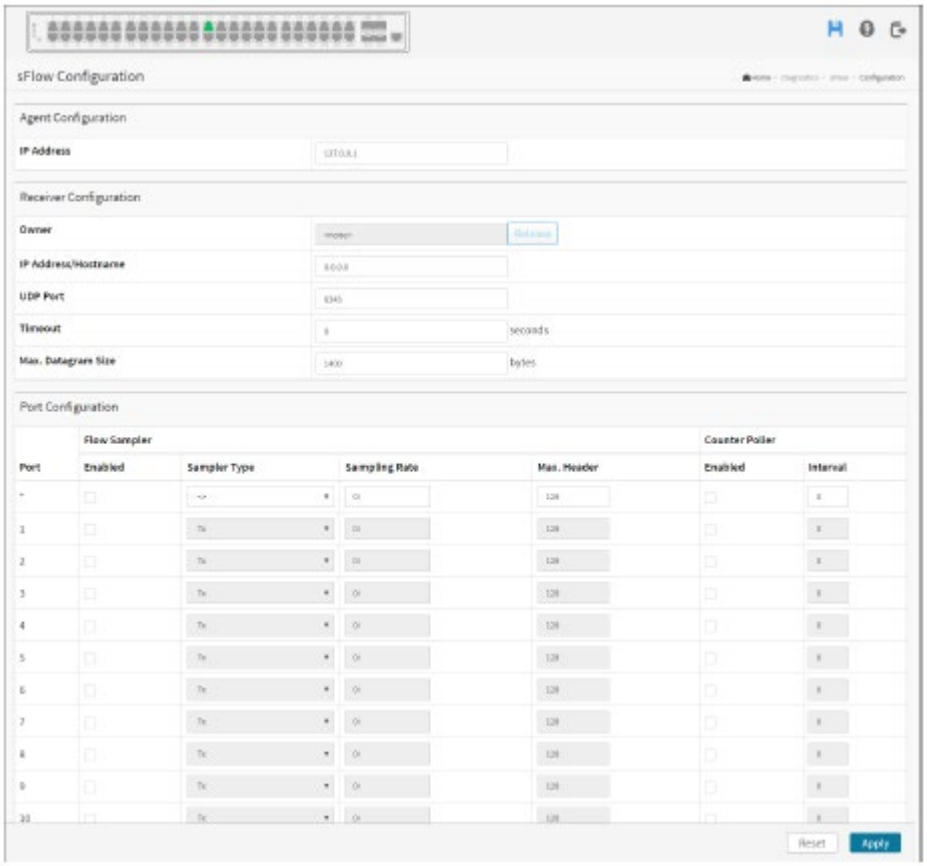
Reset（リセット）：
クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

sFlow

設定

スイッチの sFlow コレクターの設定は、ここで監視および変更することができます。設定は、sFlow レシーバーの設定（別名 sFlow コレクター）、そして、ポートごとのフローサンプラーとカウンタサンプラーの設定といった、2 つの部分に分かれています。

sFlow 設定は不揮発性メモリには保持されません。つまり、リブートまたはマスター変更により sFlow サンプリングが無効になります。



Web インターフェース

Web インターフェースで sFlow を設定するには：

1. 「Diagnostics」（診断） ＞ 「sFlow」 ＞ 「Configuration」（設定）をクリックしてください。
2. sFlow のパラメーターを設定してください。
3. 「Apply」（適用）をクリックして設定を保存してください。

4. 設定を取り消す場合は、「Reset」(リセット)ボタンをクリックする必要があります。そうすると、以前に保存した値へと戻ります。

■パラメーターの説明

Agent Configuration(エージェントの設定)

IP Address(IP アドレス):

sFlow データグラムのエージェント IP アドレスとして使用される IP アドレスです。これは、長期間に渡って、このエージェントを識別するユニークキーとして機能します。

IPv4 アドレスと IPv6 アドレスの両方がサポートされています。

Receiver Configuration(レシーバーの設定)

Owner(所有者):

基本的に、sFlow は、Web または CLI インターフェースを使用したローカル管理、または SNMP を介したローカル管理の 2 つの方法で設定することができます。この参照のみの項目には、現在の sFlow 設定の所有者が表示され、値は次のように想定されます。

- sFlow が現在未設定/未請求の場合、所有者は<none>を含みます。
- sFlow が現在 Web または CLI を介して設定されている場合、所有者には<Configured through local management>(ローカル管理を介した設定)が含まれます。
- sFlow が現在 SNMP を通して設定されている場合、所有者は sFlow レシーバーを識別する文字列を含みます。

sFlow が SNMP を介して設定されている場合、不注意による再設定を回避するために、「Release」(解放)ボタンを除くすべてのコントロールが無効になります。

「Release」(解放)ボタンを使用すると、現在の所有者を解放し、sFlow サンプリングを無効にすることができます。sFlow が現在請求されていない場合、このボタンは無効になります。SNMP を介して設定されている場合は、解放を確認する必要があります(この場合、確認要求が表示されます)。

IP Address/Hostname(IP アドレス/ホスト名):

sFlow レシーバーの IP アドレスまたはホスト名です。IPv4 アドレスと IPv6 アドレスの両方がサポートされています。

UDP Port(UDP ポート):

sFlow レシーバーが sFlow データグラムをリッスンする UDP ポートです。0(ゼロ)に設定すると、デフォルトのポート(6343)が使用されます。

Timeout(タイムアウト):

サンプリングが停止し、現在の sFlow 所有者が解放されるまでの残り秒数です。アクティブな状態

で、「Refresh」（更新）ボタンをクリックすると、現在の残り時間を更新できます。ローカルで管理されている場合、タイムアウトは他の設定に影響を与えることなくその場で変更できます。

Max. Datagram Size（最大データグラムサイズ）：
1 つのサンプルデータグラムで送ることができる最大データバイト数です。これは、sFlow データグラムの断片化を避ける値に設定する必要があります。有効な範囲は 200～1468 バイトで、デフォルトは 1400 バイトです。

Port Configuration（ポート設定）
Port（ポート）：
以下の設定が適用されるポート番号です。

Flow Sampler Enabled（フローサンプラー有効）：
このポートでフローサンプリングを有効/無効にします。

Flow Sampler Sampling Rate（フローサンプラーのサンプリングレート）：
パケットサンプリングの統計サンプリングレートです。N に設定すると、ポートで送受信されたパケットの平均 1/N でサンプリングされます。
ただし、すべてのサンプリングレートが達成できるわけではありません。サポートされていないサンプリングレートが要求された場合、スイッチはそれを最も近い達成可能なものに自動的に調整します。これは、このフィールドに戻されます。

Flow Sampler Max. Header（フローサンプラーの最大ヘッダー）：
サンプリングされたパケットから sFlow データグラムにコピーされる最大バイト数です。有効な範囲は 14～200 バイトで、デフォルトは 128 バイトです。
最大データグラムサイズが最大ヘッダーサイズを考慮しない場合、サンプルは破棄される可能性があります。

Counter Poller Enabled（カウンターポーラー有効）：
このポートにおけるカウンターポーリングを有効/無効にします。

Counter Poller Interval（カウンターポーラーの間隔）：
カウンターポーリングが有効になっている場合、カウンターポーラーサンプル間の間隔（秒単位）を指定します。

■ボタン

Apply（適用）：

クリックすると、変更内容を保存します。

Reset（リセット）：

クリックすると、ローカルで行った変更が取り消され、以前に保存した値に戻ります。

Release（解放）：

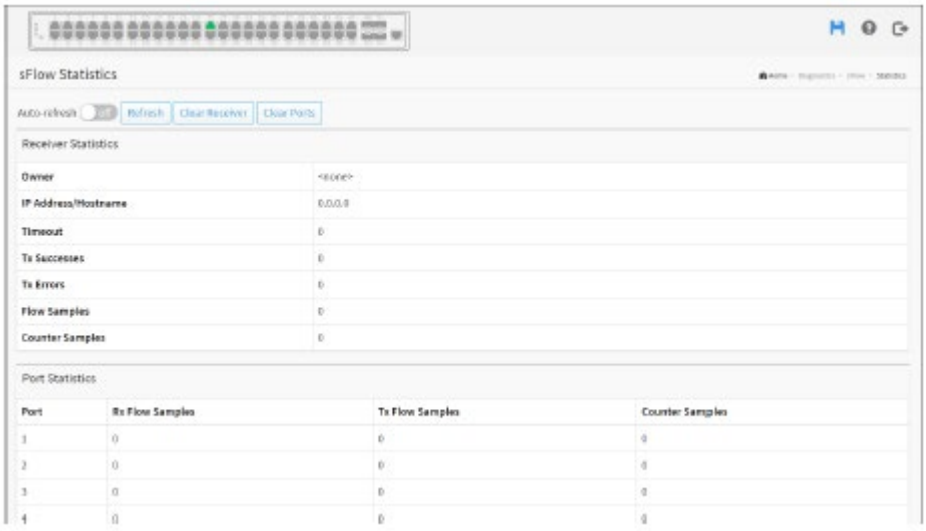
「Owner」（所有者）の説明を参照してください。

Refresh（更新）：

クリックするとページを更新します。保存されていない変更は失われることに注意してください。

統計

このセクションでは、レシーバーおよびポートごとの sFlow 統計情報を表示します。



Web インターフェース

Web インターフェースでポートの sFlow 統計を表示するには：

1. 「Diagnostics」（診断） ＞ 「sFlow」 ＞ 「statistics」（統計）をクリックしてください。
2. sFlow 情報を表示してください。

■パラメーターの説明

Receiver Statistics（レシーバーの統計）

Owner（所有者）：

このフィールドには、sFlow 設定の現在の所有者が表示されます。次の 3 つの値のいずれかを想定しています。

- sFlow が現在未設定/未請求の場合、所有者は<none>を含みます。
- sFlow が現在 Web または CLI を介して設定されている場合、所有者には<Configured through local management>(ローカル管理を介した設定)が含まれます。
- sFlow が現在 SNMP を通して設定されている場合、所有者は sFlow レシーバーの IP アドレス/ホスト名を識別する文字列を含みます。

IP Address/Hostname(IP アドレス/ホスト名):
sFlow レシーバーの IP アドレスまたはホスト名です。

Timeout(タイムアウト):
サンプリングが停止し、現在の sFlow 所有者が解放されるまでの残り秒数です。

Tx Successes(送信成功):
sFlow レシーバーに正常に送信された UDP データグラムの数です。

Tx Errors(送信エラー):
伝送に失敗した UDP データグラムの数です。エラーの最も一般的な原因は、sFlow のレシーバーIP/ホスト名の設定が無効であることです。診断するには、受信者の IP アドレス/ホスト名を Ping Web 画面(診断→Ping/Ping6)に貼り付けます。

Flow Samples(フローサンプル):
sFlow レシーバーに送信されたフローサンプルの合計数です。

Counter Samples(カウンターサンプル):
sFlow レシーバーに送信されたカウンターサンプルの合計数です。

Port Statistics(ポート統計)

Port(ポート):
以下の統計が適用されるポート番号です。

Rx and Tx Flow Samples(Rx および Tx フローのサンプル):
このポートから sFlow レシーバーに送信されたフローサンプルの数です。ここで、フローサンプルは Rx および Tx フローサンプルに分割されます。Rx フローサンプルには、ポートでの受信(入力)時にサンプリングされたパケットの数が含まれ、Tx フローサンプルには、ポートでの伝送(出力)

時にサンプリングされたパケットの数が含まれます。

Counter Samples（カウンターサンプル）：
このポートから送信された sFlow レシーバーに送信されたカウンターサンプルの合計数です。

■ボタン

Auto-refresh（自動更新）：
画面を自動的に更新する場合は、このチェックボックスを ON にしてください。自動更新は 3 秒間隔で行われます。

Refresh（更新）：
クリックすると、画面がすぐに更新されます。

Clear Receiver（レシーバーのクリア）：
sFlow 受信カウンターを消去します。

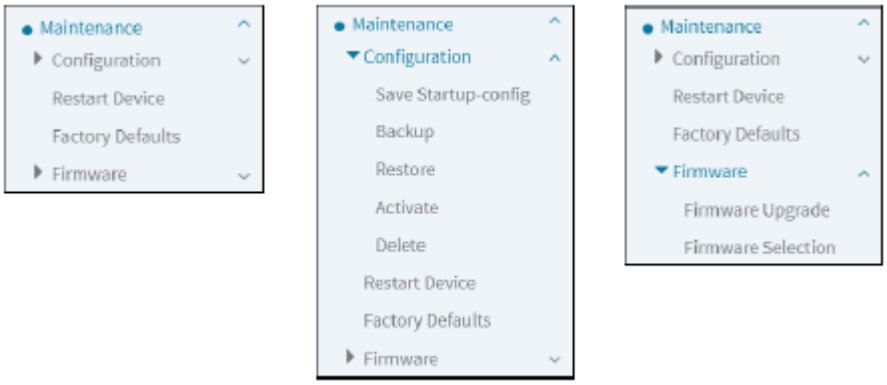
Clear Port（ポートのクリア）：
ポートごとのカウンターを消去します。

第 17 章
メンテナンス

概要

この章では、メンテナンス設定タスク全般について説明します。これらのタスクには、保存/バックアップ/リストア/有効化/削除、デバイスの再起動、工場出荷時におけるデフォルト値、ファームウェアのアップグレードなどが含まれます。

メニューとサブメニューを以下に示します。



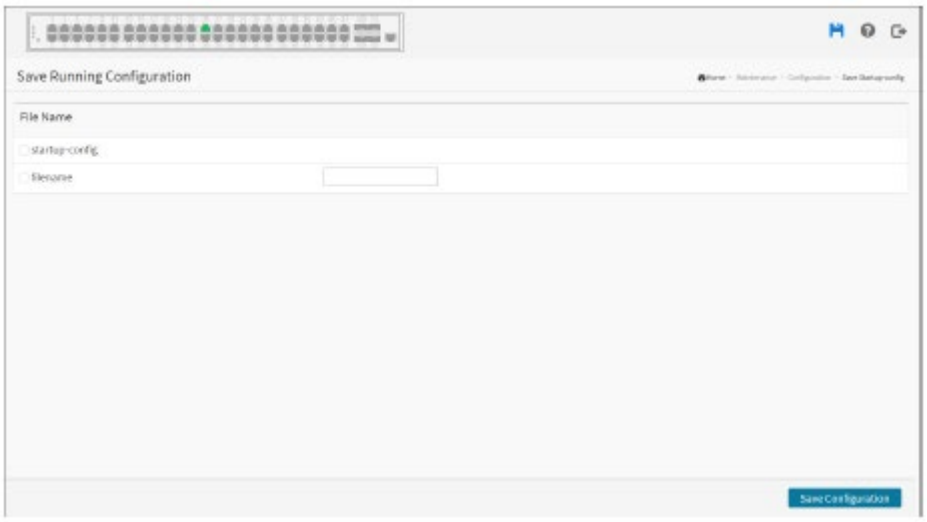
設定

スイッチの設定は、テキスト形式で複数のファイルに保存されます。ファイルは、バーチャル（RAMベース）またはスイッチのフラッシュに保存されます。

システムファイルは 3 つあります。
running-config：スイッチで現在アクティブな設定を表す仮想ファイルです。このファイルは揮発性です。
startup-config：スイッチの起動設定で、起動時に読み取られます。
default-config：ベンダー固有の設定を持つ読み取り専用ファイルです。このファイルは、システムがデフォルト設定に復元されたときに読み込まれます。

startup-config の保存

これは、running-config を startup-config にコピーします。これにより、次回のリブート時に現在のアクティブな設定が確実に使用されるようになります。



Web インターフェース

Web インターフェースで running-config を保存するには：

1. 「Maintenance」（メンテナンス） ＞ 「Configuration」（設定） ＞ 「Save startup-config」（startup-config の保存）をクリックしてください。
2. 「Save Configuration」（設定の保存）をクリックしてください。

■ボタン

Save Configuration（設定の保存）：

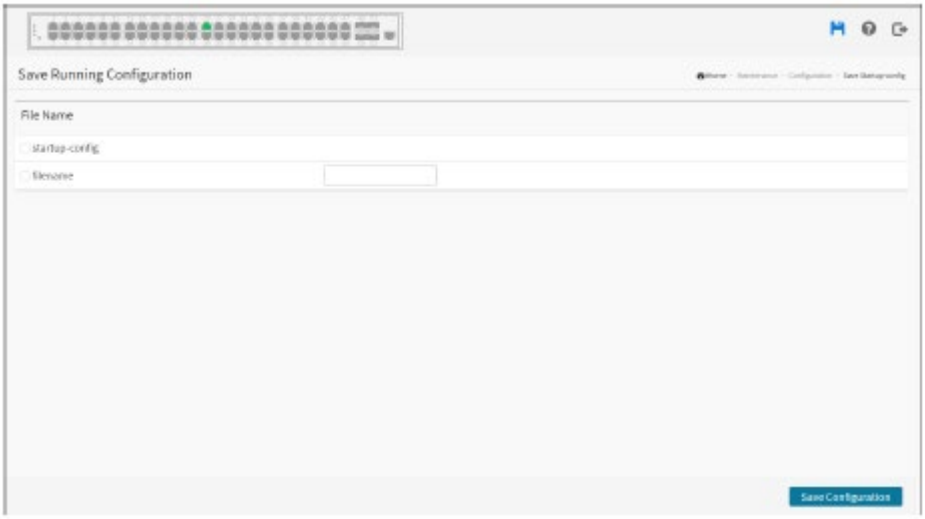
クリックして設定を保存すると、実行設定がフラッシュメモリに書き込まれ、システム起動時にこの startup-config ファイルが読み込まれます。

バックアップ

このセクションでは、メンテナンスの必要性に応じて、スイッチの設定をエクスポートする方法について説明します。現在の設定ファイルはテキスト形式でエクスポートされます。

スイッチの設定ファイルは、Web ブラウザーを実行しているステーションにバックアップしたり保存したりすることができます。

スイッチ上の任意のファイルはWebブラウザーに転送することができます。running-configを選択すると、バックアップ前にファイルを準備する必要があるため、完了するまでに少し時間がかかることがあります。



Web インターフェース

Web インターフェースで設定をバックアップするには：

1. 「Maintenance」（メンテナンス） ＞ 「Configuration」（設定） ＞ 「Backup」（バックアップ）をクリックしてください。
2. 「Backup」(バックアップ)ボタンをクリックしてください。

■パラメーターの説明

running-config：

スイッチで現在アクティブな設定を表す仮想ファイルです。このファイルは揮発性です。

startup-config：
スイッチの起動設定で、ブート時に読み込まれます。

default-config：
ベンダー固有の設定が保存されている読み取り専用ファイルです。このファイルは、システムがデフォルト設定に復元されたときに読み込まれます。

■ボタン

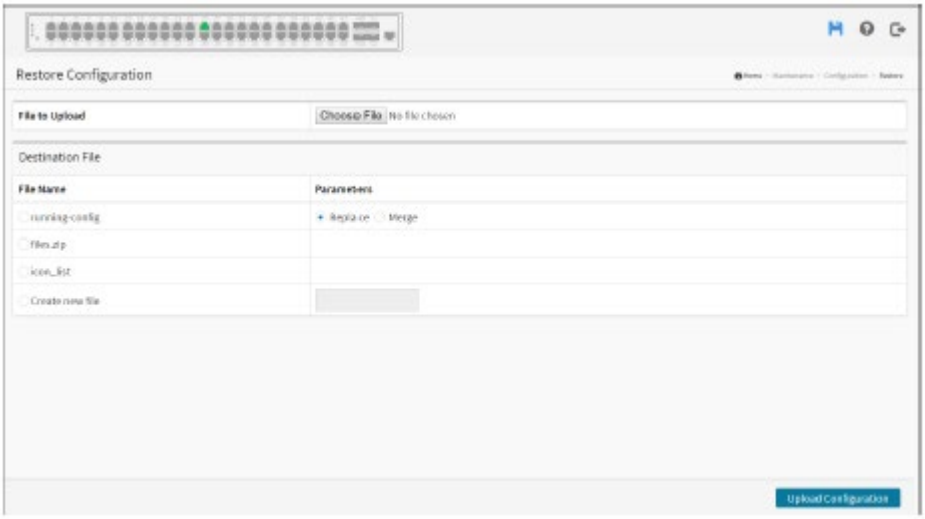
Download Configuration（設定のダウンロード）：
ボタンをクリックすると、スイッチは設定ファイルのワークステーションへの転送を開始します。

リストア

Web ブラウザーからスイッチ上のすべてのファイルにファイルをインポートできます。ただし、default-config は読み取り専用です。

復元するソースファイルを選択したら、復元先のファイルを選択してください。

保存先が running-config の場合、ファイルはスイッチ設定に適用されます。これは、次の 2 つの方法で行うことができます。
置換モード：現在の設定は、元のファイルで指定された設定に完全に置き換えられます。
マージモード：元のファイルの設定が running-config にマージされます。



Web インターフェース
Web インターフェースで設定を復元するには：

1. 「Maintenance」(メンテナンス) ＞ 「Configuration」(設定) ＞ 「Restore」(リストア)をクリックしてください。
2. 「Restore」(リストア)ボタンをクリックしてください。
3. 「ファイルの選択」をクリックし、ファイルを選択してください。
4. 「Upload Configuration」(設定のアップロード)をクリックしてください。

■パラメーターの説明

running-config:

スイッチで現在アクティブな設定を表す仮想ファイルです。このファイルは揮発性です。

置換モード:現在の設定は、アップロードされたファイルの設定に完全に置き換えられます。

マージモード:アップロードされたファイルは running-config にマージされます。

startup-config:

スイッチの起動設定で、ブート時に読み込まれます。

Create new file(新規ファイルの作成):

新しいファイルを作成します。

■ボタン

Browse(参照):

このボタンをクリックすると、設定テキストファイルとファイル名を検索します。

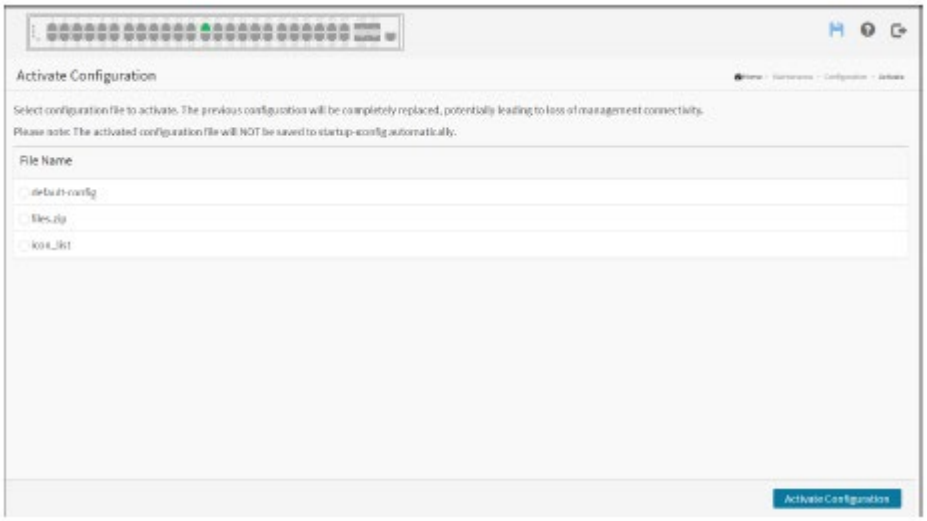
Upload Configuration(設定のアップロード):

ボタンをクリックすると、コピー元のファイルがコピー先のファイルに転送されます。

有効化

現在アクティブな設定を表す running-config を除き、スイッチに存在する設定ファイルのいずれかをアクティブにすることができます。

アクティブにするファイルを選択し、クリックしてください。これにより、既存の設定を選択したファイルの設定に完全に置き換える処理が開始されます。



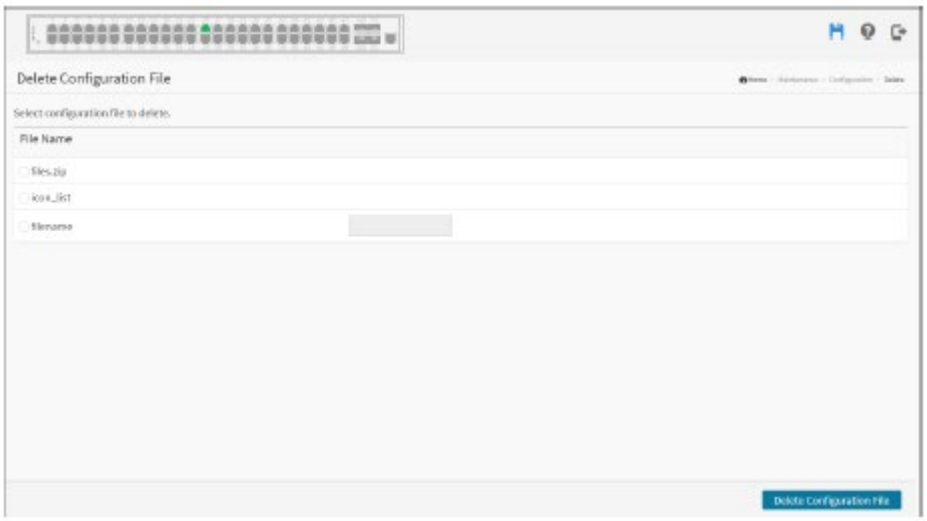
Web インターフェース

Web インターフェースで設定を有効化するには:

1. 「Maintenance」(メンテナンス) ＞ 「Configuration」(設定) ＞ 「Activate」(有効化)をクリックしてください。
2. アクティブにする設定を選択してください。
3. 「Activate Configuration」(設定の有効化)をクリックしてください。

削除

フラッシュに保存されている書き込み可能なファイル(startup-config を含む)を削除することができます。これが実行され、スイッチが事前に保存されることなくリブートされた場合、スイッチは事実上、デフォルト設定にリセットされます。



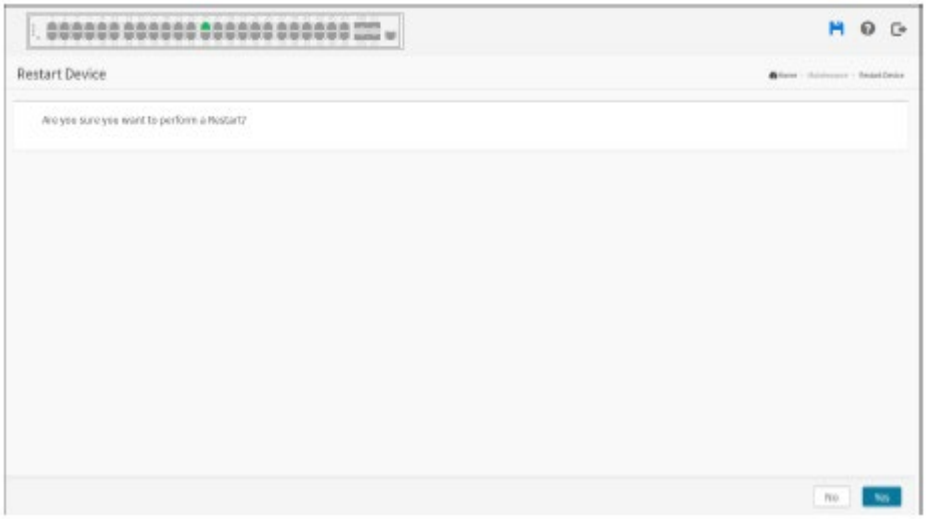
Web インターフェース

Web インターフェースで設定を削除するには:

1. 「Maintenance」(メンテナンス) ＞ 「Configuration」(設定) ＞ 「Delete」(削除)をクリックしてください。
2. 削除したい設定を選択してください。
3. 「Delete Configuration File」(設定ファイルの削除)をクリックしてください。

デバイスの再起動

このセクションでは、メンテナンスが必要な場合にデバイスを再起動する方法について説明します。スイッチに保存した設定ファイルまたはスクリプトは、後で使用できるようにしておく必要があります。



Web インターフェース

Web インターフェースでデバイスを再起動するには:

1. 「Maintenance」(メンテナンス) ＞ 「Restart Device」(デバイスの再起動)をクリックしてください。
2. 「Yes」(はい)をクリックしてください。

出荷時のデフォルト設定

このセクションでは、スイッチの設定を工場出荷時のデフォルトに復元する方法について説明します。

Web インターフェース

Web インターフェースで出荷時のデフォルト設定を復元するには:

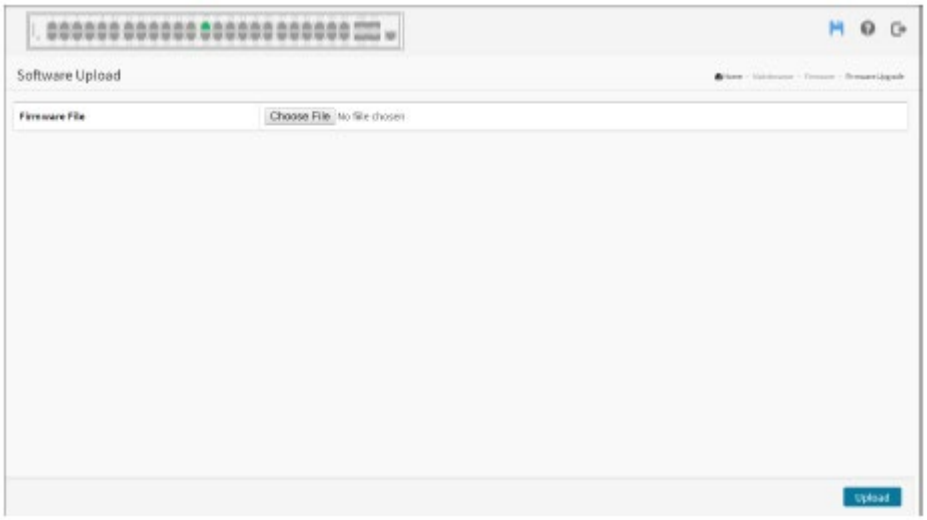
1. 「Maintenance」(メンテナンス) ＞ 「Factory Defaults」(出荷時のデフォルト設定)をクリックしてください。
2. 「Keep IP setup」(IP 設定を保持する)オプションを ON にして、IP 設定を保持するかどうかを選択することができます。
3. 「Yes」(はい)をクリックしてください。

ファームウェア

ここでは、ファームウェアのアップグレード（または更新）方法について説明します。

ファームウェアのアップグレード

この画面では、スイッチを制御するファームウェアのアップデートを簡単に行うことができます。



Web インターフェース

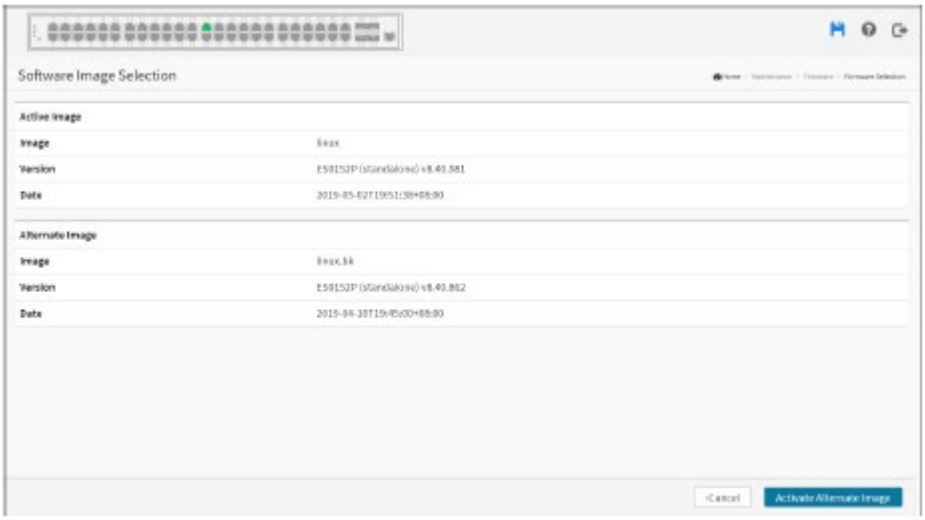
Web インターフェースでデバイスのファームウェアを更新するには：

1. 「Maintenance」（メンテナンス） ＞ 「Firmware」（ファームウェア） ＞ 「Firmware Upgrade」（ファームウェアのアップグレード）をクリックしてください。
2. 「ファイルの選択」をクリックし、ファイルを選択してください。
3. 「Upload」（アップロード）をクリックしてください。

ファームウェアの選択

この画面には、デバイス内のアクティブおよび代替（バックアップ）ファームウェアイメージに関する情報が表示され、代替イメージをアクティブにすることができます。

Web ページには、アクティブファームウェアイメージと代替ファームウェアイメージに関する情報を含む 2 つの表が表示されます。



Web インターフェース

Web インターフェースでファームウェア情報を表示したり、起動中のファームウェアをスワップしたりするには:

1. 「Maintenance」(メンテナンス) ＞ 「Firmware」(ファームウェア) ＞ 「Firmware Selection」(ファームウェアの選択)をクリックしてください。
2. 「Activate Alternate Image」(代替イメージの有効化)をクリックしてください。

Image Information(イメージの情報)

Image(イメージ):

イメージが最後に更新された時に設定されたファームウェアイメージのファイル名です。

Version(バージョン):

ファームウェアイメージのバージョンです。

Date(日付):

ファームウェアが作成された日付です。

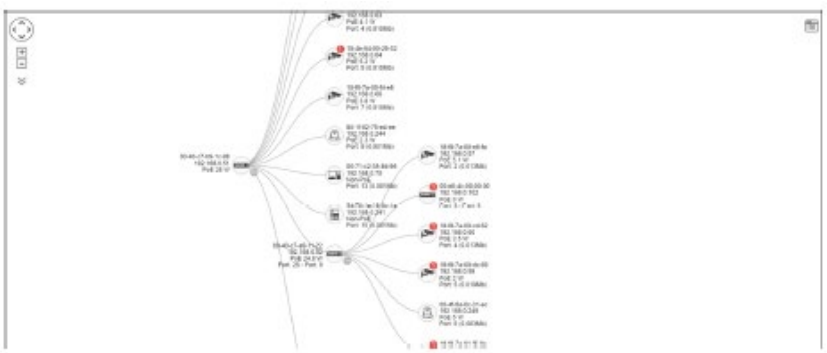
第 18 章
デバイス管理システム（DMS）

概要

1. DMS は、スイッチに組み込まれたインテリジェントな管理ツールで、IT/TS がサポートを行うコスト/時間/労力を削減するのに直感的に役立ちます。
2. スイッチに接続されているすべてのデバイスは、LLDP、UPnP、ONVIF、Bonjour などの標準ネットワークプロトコルを使用して、DMS によって自動的に検出および表示することができます。
3. ユーザーは、直感的な Web GUI を使用して、以下の機能を操作することができます。
   - ◆ IP カメラ、NVR、または、あらゆる PoE デバイスのリモート電源 OFF
   - ◆ リモートからケーブルの破損箇所の確認
   - ◆ IP カメラ/NVR における異常トラフィックの問題の検出
   - ◆ リンクアップ、PoE 電源、トラフィックなど、デバイスの状態を直感的に監視
   - ◆ ソリューションの品質/信頼性を向上させるために、VLAN/QoS を直感的に設定
4. DMS は、4 つのサブネット内で最大 256 台のデバイスをサポートします。

本製品に組み込まれたデバイス管理システムは、業務システム用に IP Phone、IP カメラ、または Wifi-AP を非常に簡単に使用/管理/セットアップできるように設計されています。

ユーザーは、トポロジー/フロア/マップビューを介してセットアップ場所に IP デバイスを展開できます。また、診断およびトラフィックモニターを介して、リンクの状態をチェックし、スループットを監視することもできます。

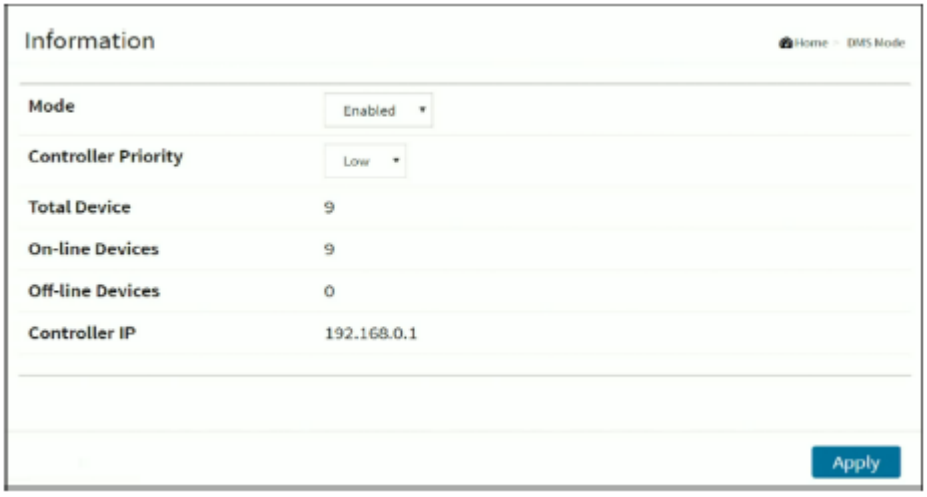


メインメニューは以下のとおりです。

管理

管理メニューを以下に示します。

DMS モード



- DMS Mode（DMS モード）：DMS 機能の有効/無効を設定します。または、「High Priority」（優先度 高）を選択すると、デバイスがマスタースイッチになります。
- Total Device（デバイス合計）：検出され、トポロジービューに表示される IP デバイスの数が表示されます。
- On-Line Devices（オンラインデバイス）：トポロジービューで、オンラインになっている IP デバイスの数が表示されます。
- Off-Line Devices（オフラインデバイス）：トポロジービューでオフラインになっている IP デバイスの数が表示されます。
- Controller IP（コントローラーIP）：マスターIP が表示されます。

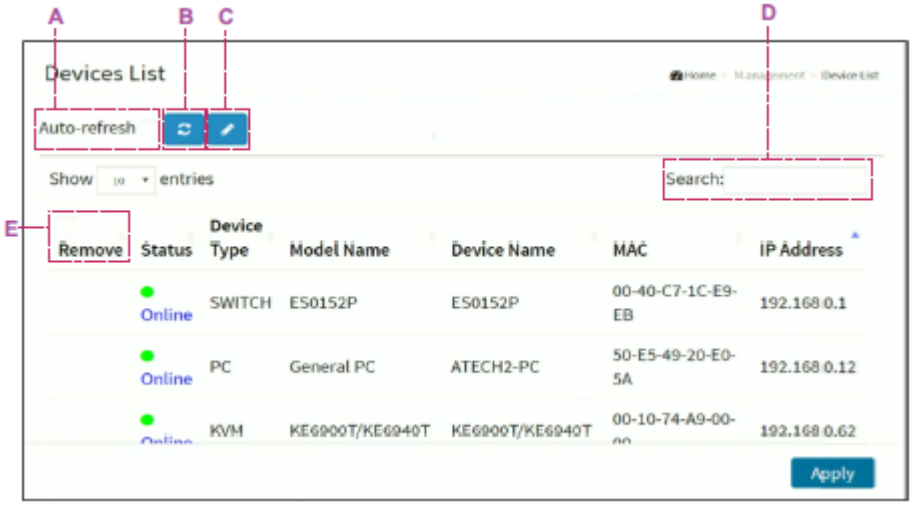
API キーのマッピング

Google Maps Platform の発表によると、2018 年 6 月 11 日以降、Google コア製品にアクセスするには、有効な API キーと Google Cloud Platform 請求アカウントが必要になります。課金を有効にすると、Google マップ、ルート、およびプレース製品に使用する無料の月額使用料 200 ドルにアクセスできるようになります。

マップビューでマップ機能を使用するには、API キーを取得し、このページのキーフィールドに入力して「Apply」（適用）をクリックする必要があります。

デバイスリスト

DMS によって検出されたすべてのデバイスとその情報が表示されます。



a) 

情報を自動更新する場合は、「Auto-refresh」(自動更新)を呼び出す必要があります。

b)  このアイコンをクリックすると、すべてのデバイスの状態が更新されます。

c) 

このアイコンをクリックすると、デバイス名と http ポートを編集します。「Edit」(編集)アイコンを押すと、各 IP デバイスのデバイス名と HTTP ポートを編集できます。この機能は、「Dashboard of Topology」(トポロジーのダッシュボード)ビューでも設定することができます。

不明なデバイス、および PC タイプのデバイスには HTTP 接続機能がないため、UI では設定用の HTTP ポート編集機能は提供されません。

d)

キーワードを使って全文検索でデバイスを検索します。

e) 

オフラインデバイスのみが、DMS デバイスリストから削除する機能を提供します。

注意： デバイス名は、「Apply」（適用）ボタンをクリックするまで保存されません。新しいデバイス名を適用する前に、「Refresh」（更新）、「Auto-refresh」（自動更新）、または「Edit」（編集）ボタンをクリックしないでください。

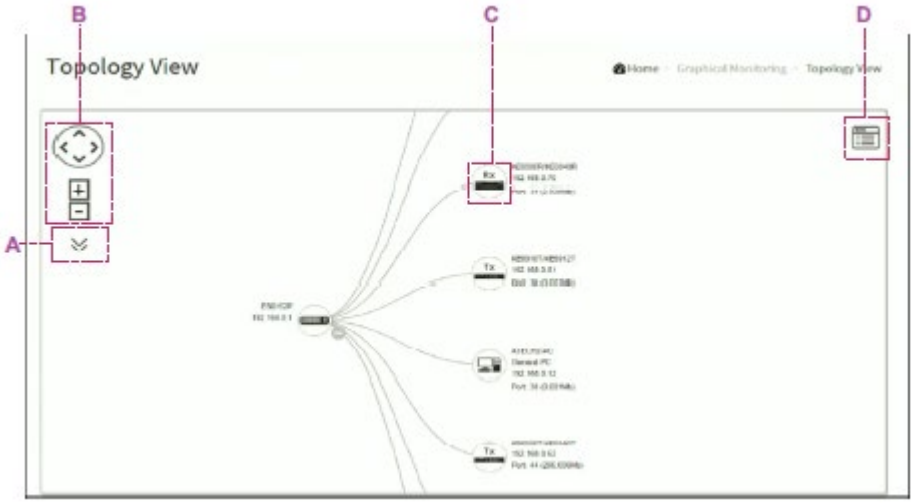
グラフィックを使ったモニタリング

グラフィカルなモニタリングメニューを以下に示します。

トポロジービュー

DMS は、すべての IP デバイスを自動的に検出し、グラフィッカルなネットワークトポロジービューでデバイスを表示できます。ユーザーは、ケーブル接続状態のリモート診断、クリティカルイベントの自動アラーム通知、生存していない場合の PoE デバイスの遠隔リブートといったタスクを、トポロジービューによって管理および監視することができます。したがって、ユーザーは、タブレットやスマートフォンによっていつでもどこでも異常問題を解決するために DMS プラットフォームを適用することができ、ネットワークはスムーズに動作します。

「Graphical Monitoring Topology View」(グラフィカル監視トポロジービュー)をクリックすると、ネットワークトポロジーを視覚的に表示できます。



■パラメーターの説明

a) 情報リストのあるアイコン：各機器のトポロジービューに表示する情報の種類を選択できます。選択できるのは 3 件までです。

b)  プラスマークとマイナスマーク付きのアイコン：トポロジービューをズームインおよびズームアウトします。ユーザーはマウスで上下にスクロールすることでも、同様の操作を行うことができます。

c) デバイスのアイコン

◆ 

黒い印のあるアイコン：デバイスリンクが起動しています。ユーザーは機能を選択し、問題をチェックすることができます。

◆  赤色のマークが付いたアイコン：デバイスリンクがダウンしています。ユーザーはリンクの状態を診断することができます。

◆ 

数字の付いたアイコン：IP デバイスで何らかのイベント（デバイスオフライン、IP 重複など）が発生したことを意味します。ユーザーはデバイスアイコンをクリックして、通知でイベントを確認できます。

◆ 

クエスチョンマークのあるアイコン：IP デバイスが DMS によって検出されましたが、デバイスタイプが認識できず、不明なデバイスタイプとして分類されることを意味します。

◆ デバイスアイコンを左クリックしてデバイスコンソールを表示し、さらに操作を行うには、次の手順を実行します。

1. Dashboard Console（ダッシュボードコンソール）：デバイス情報とデバイスの関連アクションが表示されます。
   - ◆ デバイスタイプによってサポートされる機能は異なります。
     - ➢ IP デバイスが DMS スイッチとして認識されると、「アップグレード」、「PoE 設定」、「スイッチの検索」の各機能がサポートされます。
     - ➢ IP デバイスが PoE デバイスとして認識されると、「アップグレード」および「スイッチの検索」の各機能に加えて「PoE リブート」機能がサポートされます。
     - ➢ IP デバイスが ONVIF プロトコル経由で IP カメラとして認識される場合。
   - ◆ Device Type（デバイスタイプ）：自動的に表示されます。不明なタイプが検出された場合でも、ユーザーは定義済みのリストからタイプを選択することができます。
   - ◆ Device Name（デバイス名）：「1F_Lobby_Cam1」など、管理を容易にするために、自分のデバイス名またはエイリアスを作成します。
   - ◆ DMS では、機種名、MAC アドレス、IPv4 アドレス、サブネットマスク、ゲートウェイ、PoE 供給、PoE 使用が自動的に表示されます。
   - ◆ Http Port（HTTP ポート）：セキュリティを向上させるために、デバイスに http ポートの番号を再割り当てします。
   - ◆ DHCP Client（DHCP クライアント）：DHCP クライアントを有効または無効にします。この機能を有効にすると、システムは DHCP プロトコルを使用してインターフェースの IPv4 アドレスとマスクを設定します。DHCP クライアントは、設定されたシステム名をホスト名としてアナウンスし、DNS ルックアップを提供します。
   - ◆ 

Login（ログイン）：「Login Action」（ログインアクション）アイコンを選択すると、HTTP 経由でデバイスにログインして、詳細な設定や状態の監視を行うことができま

す。

- 

Upgrade（アップグレード）：クリックすると、ソフトウェアバージョンがアップグレードされます。

- 

Find Switch（スイッチの検索）：この機能を有効にすると、スイッチの LED がすべて明るくなり、15 秒間点滅します。

- 

PoE Config（PoE の設定）：PoE 機能を設定し、PoE 自動チェック機能を有効/無効にし、ポートごとに PoE モードを有効/無効にします。

- 

Diagnostics（診断）：「Diagnostic Action」（診断アクション）アイコンをクリックして、ケーブル診断を実行し、破損したケーブルがどこにあるかを調べ、デバイスの接続が正常に行われているかどうかを ping で確認します。

ケーブルの状態：

- グリーンのアイコン：ケーブルが正しく接続されています。
- レッドのアイコン：ケーブルが正しく接続されていません。ユーザーは、距離情報（*XX* メートル）を確認して、破損したケーブルの位置を特定することができます。

接続：

- グリーンのアイコン：デバイスは正しく ping されています。
- レッドのアイコン：デバイスが正しく送受信されていません。これは、正常に ping

されない可能性があることを意味します。

- 

PoE Reboot（PoE の再起動）：デバイスを通常の動作に復元するためにデバイスをリモートで再起動するには、「Reboot Action」（再起動アクション）アイコンをクリックします。
- 

ブランクノードの付いたアイコン：DMS スイッチが同じポートから複数の IP デバイスを検出した場合、スイッチはこの IP デバイスのレイアウトを解決できず、代わりに空のノードを表示してこの状況を表示します。ユーザーは「親ノード」機能を使用して、ダッシュボードのレイアウトを調整することができます。

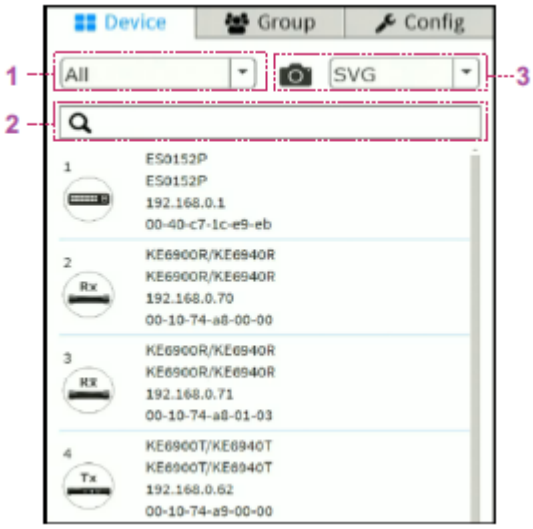
2. Notification Console（通知コンソール）：イベントによってトリガーされたアラームとログを表示します。

3. Monitor Console（モニターコンソール）：デバイスのヘルスチェックを目的としたトラフィックが表示されます。
   - DMS スイッチを除く各 IP デバイスについて、ユーザーは IP デバイスのスループットのしきい値を設定し、スループットが設定より低いか、または高い場合に通知を受け取ることができます。
   - 両方の値が「0」の場合は、機能が無効であることを意味します。
   - ポーリング間隔は 1 秒で、画面を閉じると、ポーリング間隔は約 5 秒に変わります。

d)  右上には「Setting」(設定)アイコンがあります。ユーザーがアイコンをクリックすると、トポロジーのデバイス、グループ、設定、エクスポートのトポロジービュー、および高度な検索機能がポップアップ表示されます。

◆ Device Search Console(デバイス検索コンソール)

すべてのデバイスと情報がリストに表示されます。



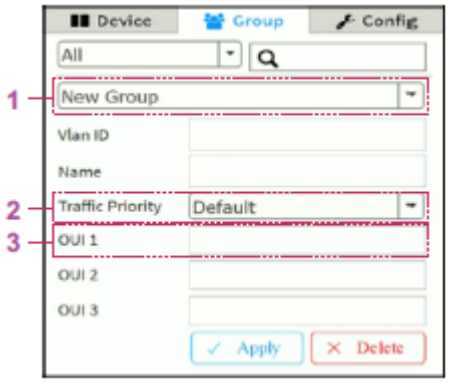
No.	機能
1	デバイスタイプによるデバイスのフィルタリングを行います。
2	キーワード全文検索でデバイスを検索します。
3	ビュー全体を SVG、PNG、または PDF 形式で保存します。

◆ グループ設定コンソール

➢ ユーザーは、OUI またはデバイスアイコンをクリックして各 IP デバイスの VLAN グループを設定し、各 VLAN グループのトラフィックプライオリティ(0～7)を設定できま

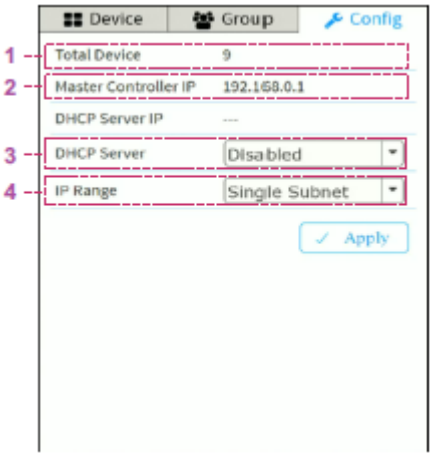
す。

- MAC ベース VLAN を使用してグループを分離します。
- 1 つの IP デバイスが参加できるのは、1 つの VLAN グループだけです。



No.	機能
1	フィルタリング、検索、デバイスアイコンのクリック、またはQUIの指定が行われたグループデバイスです。
2	VLAN のトラフィックプライオリティを設定します。
3	VLAN ID または名前をグループに割り当てます。

◆ システム設定コンソール

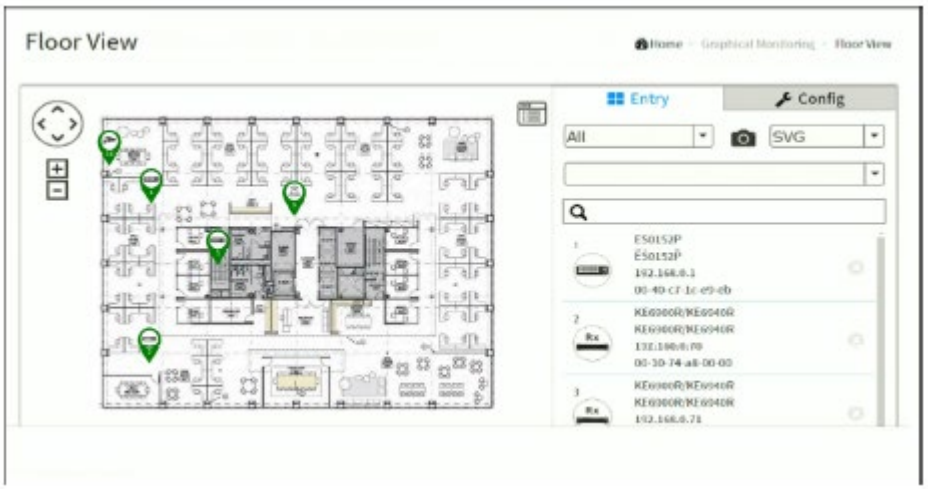


No.	機能
1	検出されて、トポロジービューに表示される IP デバイスの数を示します。
2	マスターIP です。
3	DHCP サーバーを有効/無効にすることができます。
4	- Single Subnet（単一サブネット）DMS はマススイッチの IP

	アドレスに基づきます。この場合、サブネットは「255.255.255.0」を意味します。 － Multiple Subnet（複数サブネット）：手動で入力するための 4 つの範囲を指定します（この場合、IP デバイスが認識されないように、スイッチのサブネットマスクも「255.255.0.0」に調整することを推奨します）。

フロアビュー

ユーザーは、カスタムアップロードされたフロアイメージに IP デバイスの設置場所を簡単に計画することができます。



- フロアマップへのデバイスのアンカー
- デバイスの位置を速やかに検索
- 各スイッチにには 10 個のマップを保存可能
- IP 監視/VoIP/Wi-Fi アプリケーション
- その他の機能はトポロジービューと同じ
- デバイスアイコンを配置および削除するには：
  - デバイスを選択し、デバイス一覧からそのアイコンをクリックします。
  - デバイスアイコンは、フロアイメージのデフォルトの場所に表示されます。
  - アイコンをフロアビュー上の正しい場所にドラッグアンドドロップして、左マウスをクリックしたままにします。イスアイコンは、フロアイメージのデフォルトの場所に表示されます。
  - デバイスアイコンの右側にあるクロス記号をクリックして、すべてのフロアビューのイメージからデバイスを削除します。
- フロアイメージが 2 つ以上ある場合は、検索項目の上の項目から選択できます。

マップビュー

デバイスが異なる建物に設置されていても、デバイスの場所を見つけるのに役立ちます。ユーザーは、Google マップによってナビゲートされたマップビューにデバイスアイコンを配置できます。

ここでは、次のことができます。

- Google マップに対するデバイスのアンカー
- 「マップ」から速やかにデバイスを検索
- 会社/住所のオンライン検索
- 屋外の IP カメラ/Wi-Fi アプリケーション
- その他の機能はトポロジービューと同じ

メンテナンス

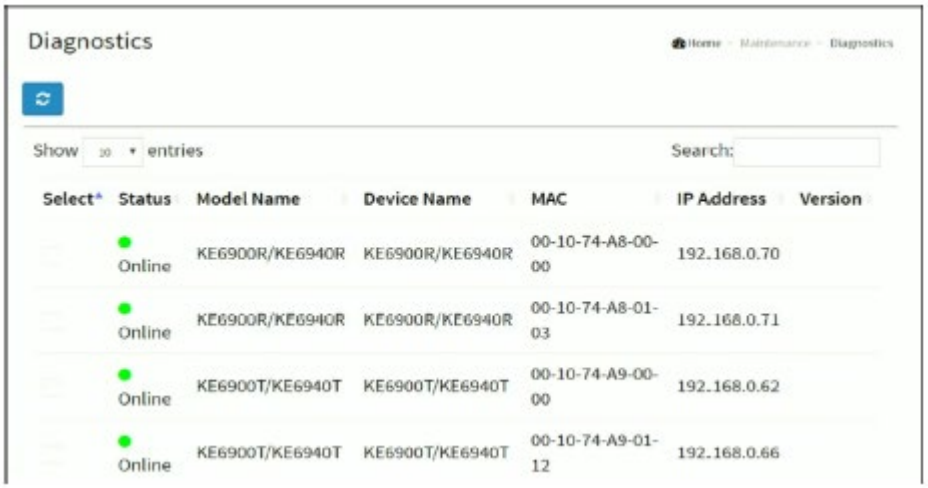
フロアイメージ

ユーザーは、この画面で、フロアイメージを追加したり削除したりすることができます。

- 各 DMS スイッチには、アップロード用に 10 個のファイル領域があります。
- JPG および PNG 形式のみをサポートします。
- ファイルサイズは 512KB に制限されています。
- 同じネットワーク内のすべての DMS スイッチのフロアイメージを共有できます。
  - 次に例を示します。
    スイッチ 1 が 10 枚のフロアイメージをアップロードし、スイッチ 2 が 5 枚の画像をアップロードした場合、同じネットワーク内のすべての DMS スイッチで合計 15 枚のフロア画像を共有し、選択することができます。
- ファイル名には、どの DMS スイッチにフロアイメージが保存されているかをユーザーに知らせる IP アドレスが付加されます。

診断

この画面では、すべての IP デバイスが表に表示され、ユーザーはネットワーク内の IP デバイスの接続状態を診断することができます。



◆ ユーザーは、診断手順を自動的に開始するデバイスを選択します。

◆ Another Try 「Another Try」(再試行する)を押すと、IP デバイス一覧画面に戻ります。

◆ 診断機能は、トポロジービューのダッシュボードにもあります。

付録

トラブルシューティング

問題	考えられる原因	推奨される解決方法
システム LED が OFF になっている。	スイッチに電源が入っていないことを示しています。	1. 正しい電源コードがスイッチとコンセントにしっかりと接続されているか確認してください。 2. スイッチの電源を再投入するには、電源コードを取り外し、スイッチに再度差し込みます。 3. それでもLEDが消灯する場合は、電源コードを別のコンセントに差し込んで、正しいAC電源が供給されていることを確認してください。
システムLEDがレッドである。	スイッチが異常状態を検出しました。	WEB UIからスイッチ内のシステムログをチェックし、異常状態（動作温度範囲超過など）を把握した上で、対応する措置を取ってください。
リンク/アクティブ/スピードモードのポート状態 LED が OFF になっている。	ポートが接続されていないか、接続が機能していません。	1. ケーブルコネクターのプラグ部分がスイッチと接続機器の両方のポートにしっかりと差し込まれ、ロックされていることを確認してください。 2. 接続したデバイスが正常に動作していることを確認してください。 3. それでも症状が解決しない場合は、別のケーブルまたは別のポートを試して、ケーブルまたは特定のポートに関連しているかどうかを確認してください。 4. Web ユーザーインターフェースを使用して、設定でポートが無効になっているかどうかを確認してください。
PoE モードでポート状態LEDがOFFになっている。	ポートに電源が供給されていません。	1. ケーブルコネクターのプラグ部分がスイッチと接続機器の両方のポートにしっかりと差し込まれ、ロックされていることを確認してください。 2. 正しいイーサネットケーブルが使用されていることを確認してください。

（表は次のページに続きます）

問題	考えられる原因	推奨される解決方法
PoE モードでポート状態 LED が OFF になっている。(続き)		3. それでも症状が解決しない場合は、別のケーブルまたは別のポートを試して、ケーブルまたは特定のポートに関連しているかどうかを確認してください。 4. Web ユーザーインターフェースを使用して、設定でポートが無効になっているかどうかを確認してください。

製品仕様

機能	ES0152	ES0152P
コネクター		
RJ-45 10/100/1000 ポート	48	
SFP アップリンクポート	4	
コンソールポート	RJ-45 メス×1	
性能		
スイッチング容量	176 Gbps	
転送レート	130.95 Mpps	
ジャンボフレーム	10240 バイト	
最大入力定格電力	AC100～240V、50～60Hz	
消費電力	AC110V:45.98W 、 AC220V:46.55W	AC110V:885.36W 、 AC220V:858.09W(PoE on)
PoE		
規格準拠	-	802.3af PoE / 802.3at PoE+
PoE/PoE+対応ポート数	-	48
ポートあたりの 最大 PoE パワーバジェット	-	PoE : 15.4W / PoE+: 30.0W
総 PoE パワーバジェット	-	740W
動作環境		
動作温度	0～50℃	
保管温度	-20～60℃	
湿度	10～90% RH、結露なきこと	
ケース		
ラックスペース	19″	
ケース材料	メタル	
重量	4.20 kg	5.60 kg
サイズ(W×D×H)	442×300×44 mm	442×375×44 mm

(表は次のページに続きます)

機能	ES0152	ES0152P
同梱品	AC 電源ケーブル×1 フットパッド（4pcs）×1 ラックマウントキット×1 クイックスタートガイド×1	