AXprimoM210

Web 管理ガイド

第 3 版

AXprimo-S002-20

■対象製品

このマニュアルは AXprimoM210 を対象に記載しています。

■輸出時の注意

本製品を輸出される場合には，外国為替及び外国貿易法の規制ならびに米国の輸出管理規則など外国の輸出関連法規をご確認のうえ，必要な手続きをお取りください。なお，不明な場合は，弊社担当営業にお問い合わせください。

■商標一覧

Cisco は，米国 Cisco Systems, Inc. の米国および他の国々における登録商標です。
Ethernet は，富士ゼロックス株式会社の登録商標です。
Firefox は，米国およびその他の国における The Mozilla Foundation の登録商標です。
Google Chrome は，米国およびその他の国における Google LLC の登録商標または商標です。
Internet Explorer は，米国 Microsoft Corporation の米国およびその他の国における登録商用または商標です。
Linux は，米国およびその他の国における The Linux Foundation の登録商標です。
sFlow は，米国およびその他の国における米国 InMon Corp.の登録商標です。
UNIX は，The Open Group の米国ならびに他の国における登録商標です。
Windows は，米国 Microsoft Corporation の米国およびその他の国における登録商用または商標です。
イーサネットは，富士ゼロックス株式会社の登録商標です。
そのほかの記載の会社名，製品名は，それぞれの会社の商標もしくは登録商標です。

■マニュアルはよく読み，保管してください。

製品を使用する前に，安全上の説明をよく読み，十分理解してください。
このマニュアルは，いつでも参照できるよう，手近な所に保管してください。

■ご注意

このマニュアルの内容については，改良のため，予告なく変更する場合があります。

■発行

２０１９年　９月　（第３版）　ＡＸｐｒｉｍｏ－Ｓ００２－２０

■著作権

変更内容

【第 2 版】

表　変更内容

章・節・項・タイトル	追加・変更内容
このマニュアルの読み方	IPv6 ACLs (中継パケットフィルタのみ)をサポートしました。

なお，単なる誤字・脱字などはお断りなく訂正しました。

【第 3 版】

表　変更内容

章・節・項・タイトル	追加・変更内容
このマニュアルの読み方	ゼロタッチプロビジョニングをサポートしました。
4.4.12 / 8.3.3 / 8.3.7 / 8.4.1 / 8.4.6	各コマンドの応答待ち時間の最大設定範囲を 60sec に変更

なお，単なる誤字・脱字などはお断りなく訂正しました。

はじめに

■対象製品

このマニュアルは AXprimoM210 を対象に記載しております。

■対象読者

本装置を利用したネットワークシステムを構築し，運用するシステム管理者の方を対象としています。
また，次に示す知識を理解していることを前提としています。
・ネットワークシステム管理の基礎的な知識

■このマニュアルの URL

このマニュアルの内容は下記 URL に掲載しております。
http://www.alaxala.com/

■ドキュメント体系

AXprimoM210 のマニュアルを以下に示します。
・AXprimoM210 ハードウェア取扱説明書（AXprimo-H001）
・AXprimoM210 CLI レファレンスガイド（AXprimo-S001）
・AXprimoM210 Web 管理ガイド（AXprimo-S002）

このマニュアルの読み方

■将来サポート機能

このマニュアルの内容には将来サポート予定の機能に関する記述も掲載しております。将来サポート予定の機能を以下に示します。

・IPv6 機能全般（以下の代表的な機能以外に、各コマンドのパラメータも含む、但しパケットフィルタ除く）

MLD snooping	22.3 章、22.4 章
IPv6 DHCP Client	25.1 章
IPv6 インタフェース	26.2 章
・IGMP snooping proxy 機能	22.1 章
・リモート認証(Tacacs+)	8.4 章
・設定時間範囲指定(Time-range)機能	4.9 章
・レート制御機能	8.1 章
・VLAN 状態変更	.1.2 章
・MIB 書込みアクセス	12.4 章

■機能間の共存について

複数の機能を併用する際、共存不可または制限事項がある機能があります。機能間の共存についての制限事項を次の表に示します。

使用したい機能	制限のある機能	制限の内容
リンクアグリゲーション	ACL	共存不可
	QoS	共存不可
	優先制御	共存不可
	IPv4 ソースガード	共存不可
ARP 検査	ACL	共存不可
MAC アドレス学習無効化	ポートセキュリティ	共存不可

■注意事項

本装置の運用は、コンソールもしくはリモート端末からのログインが可能ですが、複数ユーザによる運用はしないようお願いいたします。

本装置で以下に示すコンフィグレーション編集を行った場合、必ず save およびバックアップを行ってください。また運用開始前に装置再起動が必要になります。

・IGMP snooping 機能
・スパニングツリー機能
・ループ検知機能
・QoS 機能
・IP インタフェース機能

Web インタフェースの画面表示が正しく表示できなくなった場合は、他のページへ一度変更した後、再度表示させてください。

複数のエントリを同時設定した際に、エラーポップアップが表示された場合、指定したエントリ全てに対して設定が完了していない可能性があります。

一度設定状態を確認し、再度実行してください。なお、VLAN リストを使用する場合、RSPAN VLAN は対象外としてください。

目次

1 概要

このスイッチは、レイヤ 2 スイッチング機能を提供します。本マニュアルには、このマニュアルに記載されている機能を設定できる管理エージェントが含まれています。デフォルト設定でも、ほとんどの機能は使用できます。ただし、特定のネットワーク環境でスイッチのパフォーマンスを最大にするために設定する必要のあるオプションも多くあります。

1.1 主な特徴

表 1-1 主な特徴

特徴	説明
構成のバックアップと復元	管理ステーションまたは FTP / TFTP サーバの使用
認証	コンソール、Telnet、Web ユーザ名/パスワード、RADIUS、TACACS + ポート - IEEE 802.1X、MAC アドレスフィルタリング SNMP v1 / 2c - コミュニティ文字列 SNMP バージョン 3 - MD5 または SHA パスワード Telnet - SSH Web - HTTPS
一般的なセキュリティ対策	AAA ARP 検査 DHCP スヌーピング（オプション 82 リレー情報付き） DoS プロテクション IP ソースガード ポートセキュリティ
アクセス制御リスト	システムあたり最大 256 の ACL、最大 512 のルールをサポート
DHCP/DHCPv6	クライアント
ポート構成	速度、デュプレックスモード、およびフロー制御
ポートトランキング	最大 8 つのトランク（スタティックまたはダイナミックトランキング（LACP））をサポート
ポートミラーリング	3 つのセッション、分析ポートへの 1 つまたは複数のソースポート
輻輳制御	レート制限 ブロードキャスト、マルチキャスト、未知のユニキャストストームのためのスロットル
アドレステーブル	アドレス表 8K のフォワーディングテーブルの MAC アドレス（ L2 ユニキャスト、L2 マルチキャスト、IPv4 マルチキャスト、IPv6 マルチキャスト、 1K スタティック MAC アドレス。 511 L2 IPv4 マルチキャストグループ（MAC アドレステーブルと共有）
IP バージョン 4 および 6	IPv4 と IPv6 のアドレス指定と管理をサポート
IEEE 802.1D ブリッジ	動的なデータの切り替えと学習のサポート
ストアアンドフォワードスイッチング	不良フレームを排除しながらワイヤスピードの切り替えを保証するためのサポート
スパニングツリーアルゴリズム	標準 STP、RSTP（Rapid Spanning Tree Protocol）、および MSTP（Multiple Spanning Trees）をサポートしています。
VLAN	最大 4094 の IEEE 802.1Q、ポートベース、プロトコルベース、および QinQ トンネルを使用
トラフィックの優先順位付け	デフォルトのポートプライオリティ、トラフィッククラスマップ、キュースケジューリング、IP Precedence、Differentiated Services Code Point (DSCP)
Qualify of Service	差別化サービス（DiffServ）をサポート
リンク層発見プロトコル	近接デバイスに関する基本情報を検出するために使用されます。

特徴	説明
ARP	静的および動的アドレス設定、プロキシ ARP
IP ルーティング	スタティックルート
マルチキャストフィルタリング	IGMP スヌーピングとレイヤ 2 クエリーをサポート

1.2 ソフトウェア機能の説明

このスイッチは、幅広い高度なパフォーマンス向上機能を提供します。フロー制御により、ポートの飽和に起因するボトルネックによるパケットの損失がなくなります。ストーム抑制は、ブロードキャスト、マルチキャスト、および未知のユニキャストトラフィックストームがネットワークを巻き込むのを防ぎます。タグなし（ポートベース）、タグ付き、およびプロトコルベースの VLAN のサポートにより、トラフィックのセキュリティとネットワーク帯域幅の効率的な使用が実現します。CoS プライオリティキューイングにより、ネットワーク上でリアルタイムマルチメディアデータを移動するための最小限の遅延が保証されます。マルチキャストフィルタリングは、リアルタイムネットワークアプリケーションのサポートを提供します。

いくつかの管理機能について以下に簡単に説明します。

(1) コンフィグレーションのバックアップとリストア

現在の設定を管理ステーションのファイル（Web インタフェースを使用）または FTP / TFTP サーバ（Web またはコンソールインタフェースを使用）に保存し、後でこのファイルをダウンロードしてスイッチコンフィグレーションを復元することができます。

(2) 認証

このスイッチは、コンソールポート、Telnet、または Web ブラウザ経由の管理アクセスを認証します。ユーザ名とパスワードは、ローカルに設定することも、リモート認証サーバ（RADIUS や TACACS +など）を使って検証することもできます。

その他の認証オプションには、Web 経由のセキュアな管理アクセス用の HTTPS、Telnet 同等の接続によるセキュアな管理アクセス用の SSH、SNMP バージョン 3、SNMP / Telnet / Web 管理アクセス用の IP アドレスフィルタリングなどがあります。安全でないポートからの悪意のある攻撃を防ぐために、DHCP スヌーピングが提供されています。

(3) アクセス制御リスト

ACL は、アドレス、プロトコル、TCP / UDP ポート番号、TCP 制御コードに基づく IP フレーム、MAC アドレスまたはイーサネットタイプに基づく任意のフレームのパケットフィルタリングを提供します。ACL は、不要なネットワークトラフィックをブロックすることにより、パフォーマンスを改善するために、または特定のネットワークリソースやプロトコルへのアクセスを制限することで、セキュリティ制御を実装するために使用することができます。

(4) ポートのコンフィグレーション

特定のポートで使用される速度、デュプレックスモード、およびフロー制御を手動で設定するか、または自動ネゴシエーションを使用して接続デバイスで使用される接続設定を検出できます。スイッチは、IEEE 802.3x 規格（現在は IEEE 802.3-2002 に組み込まれています）に基づいたフロー制御をサポートしています。

(5) レート制限

この機能は、インタフェース上で送受信されるトラフィックの最大レートを制御します。レート制限は、ネットワークのエッジのインタフェースに設定され、ネットワークとの間のトラフィックを制限します。許容されるトラフィック量を超えるパケットは廃棄されます。

(6) ポートミラーリング

スイッチは、任意のポートからモニタポートへのトラフィックを邪魔にならないようにミラーリングできます。

(7) リンク集約

ポートを集約接続に結合することができます。トランクは、リンク集約制御プロトコル（LACP-IEEE 802.3-2005）を使用して、手動で設定するか、動的に設定することができます。ポート集約接続によるスループットの向上が可能であり、またトランク内のあるポートで障害が発生した場合にトランク内の他のポートで通信を継続することもできます。このスイッチは、最大 8 のトランクをサポートします。

(8) ストームコントロール

ブロードキャスト、マルチキャスト、および未知のユニキャストストーム抑制により、トラフィックがネットワークの通信負荷を圧迫しないようにできます。ポートでイネーブルにすると、ポートを通過するトラフィックのレベルが制限されます。トラフィックがあらかじめ定義された閾値を上回った場合、トラフィックは閾値が閾値を下回るまで抑制されます。

(9) 静的 MAC アドレス。

静的アドレスは、このスイッチの特定のインタフェースに割当てることができます。静的アドレスは割当てられたインタフェースにバインディングし、削除されません。静的アドレスが他のインタフェース上に見られる場合、アドレスは無視されアドレステーブルには書き込まれません。静的アドレスは、既知のホストへのアクセスを特定のポートに制限することによって、ネットワークセキュリティを提供するために使用できます。

(10) IP アドレスフィルタリング

安全でないポートへのアクセスは、静的 IP アドレスと DHCP スヌーピングテーブルに格納されているアドレスに基づいて入力トラフィックをフィルタリングする DHCP スヌーピングを使用して制御できます。トラフィックは、DHCP スヌーピングテーブルに格納された静的エントリまたはエントリに基づいて、特定の送信元 IP アドレスまたは送信元 IP / MAC アドレスペアに制限することもできます。

(11) IEEE 802.1D ブリッジ

スイッチは、IEEE 802.1D トランスペアレントブリッジングをサポートします。アドレステーブルは、アドレスを学習することで、データ交換を容易にし、この情報に基づいてフィルタリングやトラフィックを転送します。アドレステーブルは 8K までのアドレスをサポートします。

(12) ストアアンドフォワードスイッチング

スイッチは各フレームをメモリにコピーしてから別のポートに転送します。これにより、すべてのフレームが標準のイーサネットサイズであり、かつフレームの CRC チェックにより、不正なフレームがネットワークに侵入し、帯域幅が無駄にならないようになっています。

輻輳したポートでフレームを廃棄しないように、スイッチはフレームバッファリングをおこなえます。このバッファにより、輻輳したネットワーク上で送信待ちのパケットをキューに入れることができます。

(13) スパニングツリーアルゴリズム

スイッチは、次のスパニングツリープロトコルをサポートしています。

- スパニングツリープロトコル（STP、IEEE 802.1D） - このプロトコルはループ検出を提供します。セグメント間に複数の物理パスがある場合、このプロトコルは単一のパスを選択し、他のすべてのネットワークを無効にして、ネットワーク上の 2 つのステーション間に 1 つのルートしか存在しないようにします。これにより、ネットワークループを防止します。ただし、何らかの理由で選択したパスに異常が発生すると、接続を維持するために別のパスがアクティブになります。
- 高速スパニングツリープロトコル（RSTP、IEEE 802.1w） - このプロトコルは、ネットワークトポロジの変更の収束時間を、従来の IEEE 802.1D STP 標準の 30 秒以上と比較して、約 3〜5 秒に短縮します。STP を完全に置き換えることを意図していますが、接続されたデバイスから STP プロトコルメッ

セージを検出した場合、ポートを STP 準拠のモードに自動的に再構成することにより、古い標準を実行するスイッチと相互運用できます。

- マルチプルスパニングツリープロトコル（MSTP、IEEE 802.1s） - このプロトコルは RSTP の拡張版です。これは、異なる VLAN に対して独立したスパニングツリーを提供できます。ネットワーク管理を簡素化し、1 つ 1 つのグループを小さくすることにより、RSTP よりも高速なトポロジ変更時の収束が可能です。

(14) VLAN

スイッチは、最大 4094 の VLAN をサポートします。スイッチは、IEEE 802.1Q 標準に基づくタグ付き VLAN をサポートします。VLAN グループのメンバーは、ポートを手動で特定の VLAN セットに割当てることができます。これにより、スイッチは、ユーザが割当てられた VLAN グループへのトラフィックを制限できます。ネットワークを VLAN にセグメント化することにより、次のことが可能になります。

- フラットなネットワークでパフォーマンスを著しく低下させるブロードキャストストームを排除します。
- 手動でネットワーク接続を変更するのではなく、任意のポートの VLAN メンバーシップをリモートで設定することにより、ノードの変更/移動のためのネットワーク管理を簡素化できます。
- プロトコル VLAN を使用して、プロトコルタイプに基づいて特定のインタフェースへのトラフィックを制限します。

(15) IEEE 802.1Q トンネリング（QinQ）

この機能は、ネットワークを介して複数の顧客にトラフィックを伝送するサービスプロバイダ向けに設計されています。IEEE802.1Q（QinQ）トンネリングは、異なる顧客が同じ内部 VLAN ID を使用する場合でも、顧客固有の VLAN およびレイヤ 2 プロトコル構成を維持することを可能とします。これは、サービスプロバイダのネットワークに入るときに顧客を識別するためのカスタマーのフレームに Service Provider VLAN（SPVLAN）タグを挿入し、フレームがネットワークを離れるときにタグを取り除くことによって実現されます。

(16) トラフィックの優先制御

このスイッチは、優先度の高い 8 つのプライオリティキュー、Weighted Round Robin (WRR) スケジューリング、または厳密および重み付けキューイングの組み合わせを使用して、必要なサービスレベルに基づいて各パケットに優先順位を付けます。IEEE 802.1p および 802.1Q タグを使用して、エンドステーションアプリケーションからの入力に基づいて着信トラフィックに優先順位を付けます。これらの機能を使用して、遅延に敏感なデータとベストエフォート型データの独立した優先順位を設定できます。

このスイッチは、アプリケーションの要件を満たすレイヤ 3/4 トラフィックに優先順位を付けるいくつかの一般的な方法もサポートしています。トラフィックは、IP ヘッダ内の ToS フィールドにある DSCP 値、または IP Precedence を使用して IP フレームのタイプに優先順位を付けることができます。これらのサービスが有効になると、優先順位はスイッチによってサービスクラス値にマッピングされ、トラフィックは対応する出力キューに送信されます。

(17) QoS

Differentiated Services（DiffServ）は、ホップ単位で特定のトラフィックタイプの要件を満たすためにネットワークリソースに優先順位を付けるために使用されるポリシーベースの管理メカニズムを提供します。各パケットは、アクセスリスト、IP Precedence または DSCP 値、または VLAN リストに基づいて、ネットワークへの入力時に分類されます。アクセスリストを使用すると、各パケットに含まれるレイヤ 2、レイヤ 3、またはレイヤ 4 の情報に基づいてトラフィックを選択できます。ネットワークポリシーに基づいて、異なる種類のトラフィックを別の異なる種類の転送用にマークすることができます。

(18) アドレス解決プロトコル

スイッチは、ARP と Proxy ARP を使用して、IP アドレスと MAC（ハードウェア）アドレスを変換します。このスイッチは、特定の IP アドレスに対応する MAC アドレスを検索する従来の ARP をサポートしています。

(19) マルチキャストフィルタリング

特定のマルチキャストトラフィックを独自の VLAN に割当てることで、通常のネットワークトラフィックを妨げず、指定された VLAN に必要な優先順位を設定してリアルタイム配信を保証することができます。スイッチは、マルチキャストグループの登録を管理するために、IGMP スヌーピングと IPv4 のクエリー、MLD スヌーピングと IPv6 のクエリーを使用できます。

(20) LLDP

LLDP は、ローカルブロードキャストドメイン内の隣接デバイスに関する基本情報を検出するために使用されます。LLDP は、送信デバイスに関する情報を広告し、検出された隣接ネットワークノードから収集された情報を収集するレイヤ 2 プロトコルです。

広告された情報は、IEEE 802.1ab 規格に準拠した TLV(Type Length Value)形式で表示され、デバイスの識別、機能、および設定などの詳細を含めることができます。Media Endpoint Discovery（LLDP-MED）は、Voice over IP 電話やネットワークスイッチなどのエンドポイントデバイスを管理するための LLDP の拡張版です。LLDP-MED TLV は、ネットワークポリシー、電力、およびデバイスの場所の詳細などの情報を広告します。LLDP および LLDP-MED 情報は、トラブルシューティングを簡素化し、ネットワーク管理を強化し、正確なネットワークトポロジを維持するために、SNMP アプリケーションで使用できます。

1.3 デフォルト設定

スイッチの工場出荷時のデフォルトは、設定ファイル “ztp_startup.cfg”に提供されています。スイッチを工場出荷時の状態に戻すには、このファイルをスタートアップコンフィグレーションファイルとして設定する必要があります。

次の表は、基本的なシステムデフォルトの一部を示しています。

表 1-2 システムデフォルト

機能	パラメータ	デフォルト
Console Port Connection	Baud Rate	115200 bps
	Data bits	8
	Stop bits	1
	Parity	none
	Local Console Timeout	600 seconds
Authentication and Security Measures	Privileged Exec Level	Username “admin” Password “admin”
	Normal Exec Level	Username “guest” Password “guest”
	Enable Privileged Exec from Normal Exec Level	Password “super”
	RADIUS Authentication	Disabled
	TACACS+ Authentication	Disabled
	HTTPS	Enabled
	SSH	Disabled
	Port Security	Disabled
	IP Filtering	Disabled
	DHCP Snooping	Disabled
	IP Source Guard	Disabled (all ports)
Web Management	HTTP Server	Enabled
	HTTP Port Number	80
	HTTP Secure Server	Enabled
	HTTP Secure Server Port	443
SNMP	SNMP Agent	Enabled
	Community Strings	None
	Traps	Authentication traps: enabled Link-up-down events: enabled
	SNMP V3	View: defaultview Group: public (read only); private (read/write)
Port Configuration	Admin Status	Enabled
	Auto-negotiation	Enabled
	Flow Control	Disabled
Port Trunking	Static Trunks	None
	LACP (all ports)	Disabled

機能	パラメータ	デフォルト
Congestion Control	Rate Limiting	Disabled
	Storm Control	Broadcast: Enabled (64 kbits/sec) Multicast: Disabled Unknown Unicast: Disabled
Address Table	Aging Time	300 seconds
Spanning Tree Algorithm	Status	Disabled
	Edge Ports	Auto
LLDP	Status	Enabled
Virtual LANs	Default VLAN	1
	PVID	1
	Acceptable Frame Type	All
	Ingress Filtering	Enabled
	Switchport Mode (Egress Mode)	Hybrid
	QinQ Tunneling	Disabled
Traffic Prioritization	Ingress Port Priority	0
	Queue Mode	WRR
	Queue Weight	Queue: 0 1 2 3 4 5 6 7 Weight: 1 2 4 6 8 10 12 14
	Class of Service	Enabled
	IP Precedence Priority	Disabled
	IP DSCP Priority	Disabled
	IPv6 DSCP Priority	Disabled
	IP Port Priority	Disabled
IP Settings	Management.VLAN	VLAN 1
	IP Address	dhcp
	Subnet Mask	dhcp
	Default Gateway	Not configured
	DHCP	Client: Enabled
		Dynamic Provision: Enabled
	DNS	Proxy service: Disabled
	BOOTP	Disabled
	ARP	Enabled Cache Timeout: 20 minutes
Multicast Filtering	IGMP Snooping (Layer 2)	Snooping: Disabled Querier: Disabled
	MLD Snooping (Layer 2 IPv6)	Snooping: Disabled Querier: Disabled
	IGMP Proxy Reporting	Disabled
System Log	Status	Enabled
	Messages Logged to RAM	Levels 0-7 (all)
	Messages Logged to Flash	Levels 0-3

機能	パラメータ	デフォルト
SMTP Email Alerts	Event Handler	Enabled (but no server defined)
SNTP	Clock Synchronization	Disabled

Note：

スイッチのシステムデフォルトは、設定ファイル "Factory_Default_Config.cfg"に提供されています。スイッチのデフォルトをリセットするには、このファイルをスタートアップコンフィグレーションファイルとして設定する必要があります。

次の表に表 1-2 との差分を示しています。

表 1-3 システムデフォルト

機能	パラメータ	デフォルト
SNMP	Community Strings	“public” (read only) “private” (read/write)
IP Settings	IP Address	192.168.2.10
	Subnet Mask	255.255.255.0
	DHCP	Dynamic Provision: Disabled

2 Web インタフェースの使用

このスイッチには、HTTP Web エージェントが組み込まれています。Web ブラウザを使用して、ネットワークアクティビティを監視するようにスイッチを設定し、統計を表示できます。Web エージェントは、標準の Web ブラウザ（Internet Explorer はバージョン 11 以上、Mozilla Firefox または Google Chrome は、最新バージョンもしくは最新より 1 つ古いバージョン）を使用してネットワーク上の任意のコンピュータからアクセスできます。

Note: コマンドラインインタフェース（CLI）を使用して、コンソールポートまたは Telnet 経由のシリアル接続を介してスイッチを管理することもできます。CLI の使用方法の詳細については、CLI リファレンスガイド参照してください。

2.1 Web インタフェースへの接続

Web ブラウザからスイッチにアクセスする前に、以下について必ず実行してください:

1. スイッチをシステムデフォルト設定で起動させるとデフォルト IP アドレスとサブネットマスクは 192.168.2.10 と 255.255.255.0 で、デフォルトゲートウェイはありません。これがスイッチに接続されているサブネットと互換性がない場合は、有効な IP アドレス、サブネットマスク、およびデフォルトゲートウェイを設定してください。
2. Web エージェントへのアクセスは、CLI と同じユーザ名とパスワードで制御されます。(「11.2 ユーザアカウントの設定」を参照してください。) CLI でユーザ名とパスワードをデフォルト以外に設定済みの場合は、そのユーザ名とパスワードを使用できます。
3. ユーザ名とパスワードを入力すると、システム構成プログラムにアクセスできます。

Note: 正しいパスワードを 3 回入力することができます。 3 回失敗すると、現在の接続を終了します。

Note: 装置起動後リセットボタンを 5 秒以上押すことで、スイッチをシステムデフォルト設定で起動させることができます。

Note: ゲストとして Web インタフェースにログインすると (Normal Exec レベル)、コンフィグレーションを表示したりゲストパスワードを変更することができます。「admin」(Privileged Exec レベル) でログインすると、任意のページの設定を変更できます。

Note: 管理ステーションとこのスイッチの間のパスがスパニングツリーアルゴリズムを使用するデバイスを通過しない場合は、管理ステーションに接続されているスイッチポートを高速転送に設定して (つまり、管理エッジポートを有効にする)、Web インタフェースから発行された管理コマンドに対するスイッチの応答時間を向上させることができます。「7.5 STA のインタフェース設定」を参照してください。

Note: 600 秒間入力が検知されなかった場合、ユーザは HTTP サーバまたは HTTPS サーバから自動的にログオフされます。

Note: IPv6 リンクローカルアドレスを使用する HTTPS では、Web インタフェースへの接続はサポートされていません。

2.2 Web ブラウザインタフェースの操作

Web ブラウザインタフェースにアクセスするには、まずユーザ名とパスワードを入力する必要があります。管理者は、すべての構成パラメータと統計情報に対する読み取り/書き込みアクセス権を持っています。管理者のデフォルトのユーザ名とパスワードは「admin」です。管理者は、Web インタフェースのパラメータを設定するための完全なアクセス権を持っています。ゲストアクセスのデフォルトのユーザ名とパスワードは "guest"です。ゲストはほとんどの設定パラメータに対してのみ読み取りアクセス権を持ちます。詳細は「11.2　ユーザアカウントの設定」を参照してください。

2.2.1 ダッシュボード

Web ブラウザがスイッチの Web エージェントに接続すると、ダッシュボードが次のように表示されます。ダッシュボードには、画面の左側にメインメニューが表示され、右側にシステム情報、CPU やメモリ使用率、直近のイベント情報、インタフェース情報が表示されます。メインメニューは、他のメニューに移動したり、設定パラメータと統計情報を表示するために使用されます。

図 2-1 ダッシュボード

2.2.2 コンフィグレーション操作オプション

設定可能なパラメータには、ダイアログボックスまたはドロップダウンリストがあります。ページの設定が変更されたら、[Apply]ボタンをクリックして新しい設定を確定してください。次の表に、Web ページの設定ボタンの概要を示します。

表 2-1 Web ページ構成ボタン

ボタン	対処方法
Apply	指定された値をシステムに設定します。
Revert	指定された値を取り消し、「Apply」を押す前の値に復元します。
	現在の設定を保存します。
	選択したページのヘルプを表示します。
	現在のページを更新します。
	サイトマップを表示します。
	管理インタフェースからログアウトします。
	ベンダーにメールを送信します。
	ベンダーの Web サイトへのリンクです。

2.2.3 パネル表示

Web エージェントは、スイッチのポートのイメージを表示します。モードは、アクティブ（すなわち、アップまたはダウン）、デュプレックス（半二重または全二重）、またはフロー制御（フロー制御ありまたはなし）を含む、ポートに関する異なる情報を表示するように設定することができます。

図 2-2 フロントパネルインジケータ

Note: 本マニュアルでは、AXprimoM210-08T/08P ギガビットイーサネットスイッチについて説明します。ポートタイプの違いと PoE のサポート以外に、大きな違いはありません。

2.2.4 メインメニュー

Web エージェントを使用すると、システムパラメータを定義し、スイッチとそのポートすべてを管理および制御したり、ネットワーク状態を監視したりすることができます。以下の表は、Web エージェントから利用可能な選択肢を簡単に説明しています。

表 2-2 メインメニューの切換え

メニュー	説明
Dashboard	システム情報、CPU やメモリ使用率、温度、およびインタフェース情報を表示します。
System	
General	連絡先情報を含む基本的なシステムの説明を提供します。
Switch	ポート数、ハードウェアバージョン、電源ステータス、ソフトウェアバージョン番号を表示します。
Capability	ジャンボフレームのサポートを有効にします。 ブリッジ拡張パラメータを示します。

メニュー	説明
File	
Copy	ファイルの転送とコピーを許可します。
Automatic Operation Code Upgrade	新しいバージョンがある場合、オペレーションコードを自動的にアップグレードします。
Set Startup	スタートアップファイルを設定します。
Show	フラッシュメモリに保存されているファイルを表示します。ファイルの削除を許可します。
Time	
Configure General	
Manual	現在の時刻を手動で設定します。
SNTP	SNTP ポーリング間隔を設定します。
NTP	NTP 認証パラメータを設定します。
Configure Time Server	SNTP サーバのリストを設定します。
Configure SNTP Server	SNTP タイムサーバの IP アドレスを設定します。
Add NTP Server	NTP タイムサーバと認証キーのインデックスを追加します。
Show NTP Server	設定済みの NTP タイムサーバのリストを表示します。
Add NTP Authentication Key	キーインデックスと対応する MD5 キーを追加します。
Show NTP Authentication Key	設定された認証キーのリストを表示します。
Configure Time Zone	システムクロックのローカルタイムゾーンを設定します。
Configure Summer Time	サマータイムを設定します。
Console	コンソールポート接続パラメータを設定します。
Telnet	Telnet 接続パラメータを設定します。
CPU Utilization	CPU 使用率に関する情報を表示します。
CPU Guard	CPU ガードの閾値を設定します。
Memory Status	メモリ使用率に関する情報を表示します。
Reset	スイッチを直ちに再起動する、もしくは指定した時間、定期的な時間などに再起動するための設定をします。
Interface	
Port	
General	
Configure by Port List	ポートリストによる各ポートのスピード、ディプレックスなど接続設定をします。
Configure by Port Range	ポート範囲指定による複数ポートのスピード、ディプレックスなど接続設定をします。
Show Information	ポートの接続状態を表示します。
Statistics	インタフェース、Ether-like、および RMON ポートの統計情報を表示します。
Chart	インタフェース、Ether-like、および RMON ポートの統計情報を表示します。
History	指定されたインタフェースの統計履歴を表示します。
Transceiver	トランシーバーの詳細情報を表示します。またトランシーバの警告メッセージの閾値を設定します。
Cable Test	選択されたポートのケーブル診断を実行して、ケーブル障害（短絡、開放など）を診断し、ケーブル長を報告します。

メニュー	説明
Trunk	
Static	
Configure Trunk	
Add	トランクを作成するとともに、そのポートがトランクのメンバに入ります。
Show	設定済みのトランク ID を表示します。
Add Member	静的トランクへポートを追加（トランク作成時に加入したポートを除き）します。
Show Member	選択したトランクのポートメンバーを表示します。
Configure General	
Configure	静的トランク接続設定をします。
Show Information	静的トランク接続設定を表示します。
Dynamic	
Configure Aggregator	特定の LACP グループの管理キーとタイムアウトを設定します。
Configure Aggregation Port	
Configure	
General	ポートを動的にトランクへ加入できるようにします。
Actor	ローカル側のリンク集約グループメンバーのパラメータを設定します。
Partner	リモート側のリンク集約グループメンバーのパラメータを設定します。
Show Information	
Counters	LACP プロトコルメッセージの統計情報を表示します。
Internal	リンク集約のローカル側のコンフィグレーションと動作状態を表示します。
Neighbors	リンク集約のリモート側のコンフィグレーションと動作状態を表示します。
Configure Trunk	
Configure	動的トランクの接続設定をします。
Show	動的トランクのポートの接続設定と状態を表示します。
Show Member	トランク内のアクティブなメンバーを表示します。
Statistics	インタフェース、Ether-like、および RMON ポートの統計情報を表示します。
Chart	インタフェース、Ether-like、および RMON ポートの統計情報を表示します。
Load Balance	トランク内で受信したトラフィックのロードバランス方式を設定します。
History	指定されたインタフェースの統計履歴を表示します。
Green Ethernet	他のデバイスへの接続に使用されるケーブルの長さに基づいてポートに供給される電力を調整します
Mirror	
Add	ミラーリングのソースポートとターゲットポートを設定します。

メニュー	説明
Show	設定されたミラーセッションを表示します。
RSPAN	ローカルスイッチの宛先ポートでの分析のために、リモートスイッチからのトラフィックをミラーリングします。
sFlow	受信ポートとインスタンスのフローサンプリングを設定します。
Configure Receiver	スイッチに sFlow レシーバを作成します。
Configure Details	指定された時間間隔に基づいて定期的にポーリングする sFlow ポーリングデータソース、または処理されたパケット数に基づいてサンプルを定期的に取得する sFlow データソースインスタンスを有効にします。
Traffic Segmentation	
Configure Global	トラフィックセグメンテーションをグローバルに可能にします。
Configure Session	セグメント化されたポートグループのアップリンクおよびダウンリンクポートを設定します。
VLAN	
Static	
Add	VLAN グループを作成します。
Show	設定済みの VLAN グループを表示します。
Modify	グループ名と管理ステータスを設定します。
Edit Member by VLAN	VLAN ごとの VLAN 属性を指定します。
Edit Member by Interface	インタフェースごとの VLAN 属性を指定します。
Edit Member by Interface Range	インタフェース範囲指定での VLAN 属性を指定します。
Tunnel	IEEE 802.1Q（QinQ）トンネリングを設定します。
Configure Global	スイッチのトンネルモードを設定します。
Configure Interface	参加しているインタフェースのトンネルモードを設定します。
Protocol	
Configure Protocol	
Add	サポートされているプロトコルを指定してプロトコルグループを作成します。
Show	設定済みのプロトコルグループを表示します。
Configure Interface	
Add	プロトコルグループを VLAN にマッピングします。
Show	各 VLAN にマッピングされたプロトコルグループを表示します。
MAC-Based	
Add	指定された送信元 MAC アドレスを持つトラフィックを VLAN にマッピングします。
Show	ソース MAC アドレスから VLAN へのマッピングを示します。
MAC Address	
Dynamic	
Configure Aging	動的に学習された MAC アドレスエントリのタイムアウトを設定します。

メニュー	説明
Show Dynamic MAC	動的 MAC アドレスエントリのアドレステーブルを表示します。
Clear Dynamic MAC	学習した動的 MAC アドレスエントリを転送データベースから削除し、静的エントリまたはシステム構成エントリの送受信カウントをクリアします。
Learning Status	選択したインタフェースで MAC アドレスを有効にします。
Static	選択したインタフェースで MAC アドレス学習を有効にします。
MAC Notification	
Configure Global	動的 MAC アドレスの追加または削除時のトラップを発行します。
Spanning Tree	
Loopback Detection	ループバック検出パラメータを設定します。
STA	スパニングツリーアルゴリズムの設定をします。
Configure Global	
Configure	STP、RSTP、および MSTP のグローバルブリッジの設定をします。
Show Information	ブリッジに使用される STA 値を表示します。
Configure Interface	
Configure	STA のインタフェース設定をします。
Show Information	STA のインタフェース設定を表示します。
MSTP	マルチプルスパニングツリーを設定します。
Configure Global	
Add	MST インスタンスの初期 VLAN とプライオリティを設定します。
Modify	MST インスタンスのプライオリティを変更します。
Show	MST インスタンスのグローバル設定をします。
Add Member	MST インスタンスに VLAN メンバーを追加します。
Show Member	MST インスタンスの VLAN メンバーを追加または削除します。
Show Information	ブリッジに使用される MSTP 値を表示します。
Configure Interface	
Configure	MST インスタンスのインタフェース設定をします。
Show Information	MST インスタンスのインタフェース設定を表示します。
Traffic	
Rate Limit	ポートの入力レート制限と出力レート制限を設定します。
Storm Control	各インタフェースのブロードキャストストームの閾値を設定します。
Priority	
Default Priority	各ポートまたはトランクのデフォルト優先順位を設定します。
Queue	スイッチのキューモード、および重み付けの設定をします。
Trust Mode	DSCP または CoS プライオリティ処理を選択します。
CoS to Queue	受信パケットの CoS / CFI 値を優先処理のためのホップ単位

メニュー	説明
	の動作にマッピングします。
DSCP to Queue	受信パケットの DSCP 値を優先処理のためのホップ単位の動作にマッピングします。
DiffServ	
Configure Class	
Add	トラフィックタイプのクラスマップを作成します。
Show	設定されたクラスマップを表示します。
Modify	クラスマップの名前を変更します。
Add Rule	入力トラフィックを分類するために使用される基準を設定します。
Show Rule	クラスマップのトラフィック分類ルールを表示します。
Configure Policy	
Add	複数のインタフェースに適用するポリシーマップを作成します。
Show	設定済みのポリシーマップを表示します。
Modify	ポリシーマップの名前を変更します。
Add Rule	受信トラフィックを監視するために使用される境界パラメータと、適合トラフィックおよび不適合トラフィックに対して実行するアクションを設定します。
Show Rule	ポリシーマップに帯域幅ポリシングを適用するために使用されるルールを表示します。
Configure Interface	入力ポートにポリシーマップを適用します。
Security	
AAA	認証、認可、およびアカウンティングの設定をします。
System Authentication	認証シーケンスを指定します。 - ローカル、RADIUS、および TACACS +
Server	
Configure Server	RADIUS および TACACS サーバのメッセージ交換を設定します。
Configure Group	
Add	認証サーバのグループを指定し、優先順位を設定します。
Show	認証サーバグループと優先順位を表示します。
Accounting	セキュリティ目的で要求されたサービスのアカウンティングを可能にします。
Configure Global	ローカルアカウンティングサービスがアカウンティングサーバに情報を更新する間隔を指定します。
Configure Method	
Add	さまざまなサービスタイプのアカウンティングを設定します。
Show	さまざまなサービスタイプに使用されるアカウンティング設定を表示します。
Show Information	
Summary	設定されたアカウンティング方式と、特定のインタフェースに適用された方式を表示します。
Statistics	ユーザセッション用に記録された基本アカウンティング情報

メニュー	説明
	を表示します。
Authorization	要求されたサービスの許可を有効にします。
Configure Method	
Add	さまざまなサービスタイプの認可を設定します。
Show	さまざまなサービスタイプに使用される認証設定を表示します。
Configure Service	コンソールポートおよび Telnet に適用された認証方法を設定します。
Show Information	設定された認証方法と特定のインタフェースに適用されたメソッドを表示します。
HTTPS	セキュアな HTTP です。
Configure Global	HTTP を有効にし、使用する UDP ポートを指定します。
Copy Certificate	デフォルトのセキュアサイト証明書を置き換えます。
SSH	セキュアシェルです。
Configure Global	SSH サーバを設定します。
Configure Host Key	
Generate	ホスト鍵ペア（公開鍵と秘密鍵）を生成します。
Show	RSA および DSA ホスト鍵を表示します。ホスト鍵を削除します。
Configure User Key	
Copy	TFTP サーバからユーザ公開鍵をインポートします。
Show	RSA と DSA のユーザ鍵を表示します。 ユーザ鍵を削除します。
ACL	アクセス制御リストです。
Configure ACL	
Show TCAM	TCAM の使用状況を示します。
Add	IP または MAC アドレスのフィルタリングに基づいて ACL を追加します。
Show	設定された ACL の名前とタイプを表示します。
Add Rule	IP または MAC アドレスおよびその他のパケット属性に基づいてパケットフィルタリングを設定します。
Show Rule	ACL に指定されたルールを表示します。
Configure Interface	ACL をポートへ適用、および ACL が有効な時間範囲を設定します。
Configure	ACL をポートへ適用、および ACL が有効な時間範囲を設定します。
Show Hardware Counters	ACL ハードウェアカウンタの統計情報を表示します。
IP Filter	
Add	Web、SNMP、および Telnet 経由で管理アクセスを許可されたクライアントの IP アドレスを設定します。
Show	管理アクセスを許可するアドレスを表示します。
Port Security	ステータス、セキュリティ違反の対応、最大許容 MAC アドレスなど、ポート単位のセキュリティを設定します。
DoS Protection	Denial-of-Service 攻撃から保護します。

メニュー	説明
DHCP Snooping	
Configure Global	DHCP スヌーピングをグローバルに有効にし、MAC アドレス検証、情報オプションを有効にします。 情報ポリシーを設定します。
Configure VLAN	VLAN 上で DHCP スヌーピングを有効にします。
Configure Interface	インタフェースの信頼モードを設定します。
Show Information	DHCP スヌーピングバインディング情報を表示します。
IP Source Guard	IP ソースガードテーブルの静的エントリ、または DHCP スヌーピングテーブルの動的エントリに基づいて IP トラフィックをフィルタリングします。
General	IP ソースガードを有効にし、ポートごとにフィルタタイプを選択します。
Static Binding	
Configure ACL Table	
Add	ソースガード ACL バインディングテーブルに静的アドレスを追加します。静的アドレスをソースガードバインディングテーブルに追加します。
Show	ソースガード ACL バインディングテーブルの静的アドレスを表示します。
Configure MAC Table	
Add	ソースガード MAC アドレスバインディングテーブルに静的アドレスを追加します。
Show	ソースガード MAC アドレスバインディングテーブルの静的アドレスを表示します。
Dynamic Binding	選択したインタフェースのソースガードバインディングテーブルを表示します。
ARP Inspection	
Configure General	グローバルに検査を有効にし、追加のアドレスコンポーネントの検証を設定し、パケット検査のログレートを設定します。
Configure VLAN	指定された VLAN 上で ARP 検査を有効にします。
Configure Interface	ポートの信頼モードを設定し、パケット検査のレート制限を設定します。
Show Information	
Show Statistics	検査プロセスに関する統計を表示します。
Show Log	検査ログリストを表示します。
Administration	
Log	
System	
Configure Global	ローカルメモリにエラーメッセージを格納します。
Show System Logs	ログに記録されたエラーメッセージを表示します。
Remote	リモートログプロセスへのメッセージのログを構成します。
SMTP	サーバに SMTP クライアントメッセージを送信します。
LLDP	
Configure Global	グローバル LLDP の送信間隔を設定します。

メニュー	説明
Configure Interface	
Configure General	メッセージ送信モードを設定します。 SNMP 通知を有効にします。 LLDP 属性を広告する内容を設定します。
Add CA-Type	インタフェースに接続されたデバイスの物理的な位置を指定します。
Show Local Device Information	
General	ローカルデバイスに関する一般的な情報を表示します。
Port/Trunk	各インタフェースに関する情報を表示します。
Show Remote Device Information	
Port/Trunk	このスイッチのポートに接続されているリモートデバイスに関する情報を表示します。
Port/Trunk Details	このスイッチに接続されているリモートデバイスに関する詳細情報を表示します。
Show Device Statistics	
General	接続されているすべてのリモートデバイスの統計を表示します。
Port/Trunk	選択したポートまたはトランク上のリモートデバイスの統計情報を表示します。
PoE※	Power over Ethernet
PSE	ポートの電力パラメータを設定します。
SNMP	Simple Network Management Protocol
Configure Global	SNMP エージェントのステータスを有効にし、関連するトラップ機能を設定します。
Configure Engine	
Set Engine ID	このスイッチに SNMP v3 エンジン ID を設定します。
Add Remote Engine	リモートデバイスの SNMP v3 エンジン ID を設定します。
Show Remote Engine	リモートデバイスのコンフィグレーションされたエンジン ID を表示します。
Configure View	
Add View	OID MIB の SNMP v3 ビューを追加します。
Show View	SNMPv3 ビューの設定を表示します。
Add OID Subtree	選択したビューのサブツリーの一部を指定します。
Show OID Subtree	各ビューに割当てられたサブツリーを表示します。
Configure Group	
Add	割当てられたユーザのアクセスポリシーを含むグループを追加します。
Show	設定されたグループとアクセスポリシーを表示します。
Configure User	
Add Community	コミュニティ文字列とアクセスモードを設定します。
Show Community	コミュニティ文字列とアクセスモードを表示します。
Add SNMPv3 Local User	このスイッチで SNMPv3 ユーザを設定します。
Show SNMPv3 Local User	このスイッチで設定された SNMPv3 ユーザを表示します。
Change SNMPv3 Local User Group	新しいユーザにローカルユーザを割当てます。
Add SNMPv3 Remote User	リモートデバイスから SNMPv3 ユーザを設定します。

メニュー	説明
Show SNMPv3 Remote User	リモートデバイスから設定された SNMPv3 ユーザを表示します。
Configure Trap	
Add	このスイッチで発生するキーイベントに関するメッセージを受信するようにトラップマネージャを設定します。
Show	設定されたトラップマネージャを表示します。
Configure Notify Filter	
Add	SNMP 通知ログを作成します。
Show	SNMP 通知ログを表示します。
Show Statistics	SNMP 通信の統計情報を表示します。
RMON	遠隔モニタリング
Configure Global	
Add	
Alarm	監視対象変数の閾値範囲を設定します。
Event	アラームの応答イベントを作成します。
Show	
Alarm	設定されたすべてのアラームを表示します。
Event	設定されたすべてのイベントを表示します。
Configure Interface	
Add	
History	物理インタフェースの統計を定期的にサンプリングします。
Statistics	物理インタフェース上の統計情報の収集を有効にします。
Show	
History	履歴グループの各エントリのサンプリングパラメータを表示します。
Statistics	統計グループの各エントリのサンプリングパラメータを表示します。
Show Details	
History	履歴グループの各エントリのサンプルデータを表示します。
Statistics	履歴グループの各エントリのサンプルデータを表示します。
Time Range	ACL を適用する時間を設定します。
Add	時間範囲の名前を指定します。
Show	設定された時間範囲の名前を表示します。
Add Rule	
Absolute	正確な時間または時間範囲を設定します。
Periodic	繰り返し時間を設定します。
Show Rule	ルールで指定された時間を表示します。
LDB	ループバック検出
Configure Global	ループバック検出をグローバルに有効にし、制御フレームを送信する間隔を指定し、インタフェースをシャットダウン状態から解放するまで待機する間隔を指定し、ループバックを検出するための応答を指定し、送信するトラップを指定します。

メニュー	説明
Configure Interface	インタフェースごとにループバック検出を有効にします。
Tools	
Ping	ICMP エコー要求パケットをネットワーク上の別のノードに送信します。
Trace Route	パケットが指定されたルートまでを示します。
ARP	アドレス解決プロトコルキャッシュのエントリを表示します。
IP	
General	
Routing Interface	
Add Address	VLAN の IP インタフェースを設定します。
Show Address	VLAN に割当てられた IP インタフェースを表示します。
Routing	
Static Routes	
Add	静的ルーティングエントリを構成します。
Show	静的ルーティングエントリを表示します。
Routing Table	ローカル、静的、および動的ルートを含む、すべてのルーティングエントリを表示します。
IPv6 Configuration	
Configure Global	既知のネクストホップが無いトラフィックに、IPv6 のデフォルトゲートウェイを設定します。
Configure Interface	自動設定またはリンクローカルアドレスを使用して IPv6 インタフェースのアドレスを設定し、関連するプロトコル設定を設定します。
Add IPv6 Address	グローバルユニキャスト、EUI-64、またはリンクローカル IPv6 アドレスをインタフェースに追加します。
Show IPv6 Address	インタフェースに割当てられた IPv6 アドレスを表示します。
Show IPv6 Neighbor Cache	IPv6 近隣探索キャッシュ内の情報を表示します。
Show Statistics	
IPv6	IPv6 トラフィックに関する統計情報を表示します。
ICMPv6	ICMPv6 メッセージに関する統計情報を表示します。
UDP	UDP メッセージに関する統計情報を表示します。
Show MTU	ICMP パケットを返送した宛先の最大伝送ユニット（MTU）キャッシュを示します。このスイッチに受け入れ可能な MTU とともにあまりにも大きなメッセージが表示されます。
IP Service	
DNS	Domain Name Service
General	
Configure Global	DNS ルックアップを有効にします。 不完全なホスト名に追加されたデフォルトドメイン名を定義します。
Add Domain Name	不完全なホスト名に追加できるドメイン名のリストを定義します。
Show Domain Names	設定されたドメイン名のリストを表示します。

メニュー	説明
Add Name Server	動的ルックアップのネームサーバの IP アドレスを指定します。
Show Name Servers	ネームサーバのアドレス一覧を表示します。
Static Host Table	
Add	ドメイン名の静的エントリをアドレスマッピングに設定します。
Show	静的マッピングエントリのリストを表示します。
Modify	選択したホスト名にマップされた静的アドレスを変更します。
Cache	指定されたネームサーバが検出したキャッシュエントリを表示します。
Multicast DNS	専用サーバを必要とせずに、ローカルネットワーク上でマルチキャスト DNS ルックアップを設定します。
DHCP	Dynamic Host Configuration Protocol
Client	インタフェースの DHCP クライント識別子を指定します。
Relay	DHCP リレーサーバを指定します。
Relay Option 82	DHCP オプション 82 情報を含む、接続されたホストデバイスの DHCP リレーサービスを設定します。
Dynamic Provision	DHCP による動的なプロビジョニングを可能にします。
Multicast	
IGMP Snooping	
General	マルチキャストフィルタリングを有効にします。 マルチキャストスヌーピングのパラメータを設定する
Multicast Router	
Add Static Multicast Router	隣接するマルチキャストルータに接続されているポートを割当てます。
Show Static Multicast Router	隣接するマルチキャストルータに接続されているように静的に設定されたポートを表示します。
Show Current Multicast Router	近接またはマルチキャストルータに接続されているポートを、静的または動的構成で表示します。
IGMP Member	
Add Static Member	選択した VLAN にマルチキャストアドレスを静的に割当てます
Show Static Member	選択した VLAN 上に静的に設定されたマルチキャストアドレスを表示します。
Interface	
Configure VLAN	VLAN インタフェースごとに IGMP スヌーピングを設定します。
Show VLAN Information	VLAN インタフェースごとの IGMP スヌーピング設定を表示します。
Configure Port	IGMP クエリーパケットまたはすべてのマルチキャストデータパケットをドロップするようにインタフェースを設定します。
Configure Trunk	IGMP クエリーパケットまたはすべてのマルチキャストデータパケットをドロップするようにインタフェースを設定します。

メニュー	説明
Forwarding Entry	IGMP スヌーピングによって学習された現在のマルチキャストグループを表示します。
Filter	
Configure General	スイッチの IGMP フィルタリングを有効にします。
Configure Profile	
Add	IGMP フィルタプロファイルを追加します。 アクセスモードを設定します。
Show	設定済みの IGMP フィルタプロファイルを表示します。
Add Multicast Group Range	選択したプロファイルにマルチキャストグループを割当てます。
Show Multicast Group Range	プロファイルに割当てられたマルチキャストグループを表示します。
Configure Interface	ポートインタフェースに IGMP フィルタプロファイルを割当て、調整処理を設定します。
Statistics	
Show Query Statistics	クエリ関連のメッセージの統計情報を表示します。
Show VLAN Statistics	プロトコルメッセージの統計情報、アクティブなグループの数を表示します。
Show Port Statistics	プロトコルメッセージの統計情報、アクティブなグループの数を表示します。
Show Trunk Statistics	プロトコルメッセージの統計情報、アクティブなグループの数を表示します。
MLD Snooping	
General	マルチキャストフィルタリングを有効にします。 IPv6 マルチキャストスヌーピングのパラメータを設定します。
Interface	VLAN の即時脱退ステータスを設定します。
Multicast Router	
Add Static Multicast Router	隣接するマルチキャストルータに接続されているポートを割当てます。
Show Static Multicast Router	隣接するマルチキャストルータに接続されているように静的に設定されたポートを表示します。
Show Current Multicast Router	近接またはマルチキャストルータに接続されているポートを、静的または動的構成で表示します。
MLD Member	
Add Static Member	選択した VLAN にマルチキャストアドレスを静的に割当てます。
Show Static Member	選択した VLAN 上に静的に設定されたマルチキャストアドレスを表示します。
Show Current Member	選択された VLAN に関連付けられたマルチキャストアドレスを静的または動的構成で表示します。
Filter	
Configure General	スイッチの MLD フィルタリングを有効にします。
Configure Profile	
Add	MLD フィルタプロファイルを追加します。 アクセスモードを設定します。

メニュー	説明
Show	設定された MLD フィルタプロファイルを表示します。
Add Multicast Group Range	選択したプロファイルにマルチキャストグループを割当てます。
Show Multicast Group Range	プロファイルに割当てられたマルチキャストグループを表示します。
Query Drop	MLD クエリパケットをドロップするようにインタフェースを設定します。
Group Information	既知のマルチキャストグループ、メンバーポート、各グループが学習された手段、および対応するソースリストを表示します。
Statistics	
Input	MLD 受信トラフィックの統計情報を表示します。
Output	MLD 送信トラフィックの統計情報を表示します。
Query	クエリ関連のメッセージの統計情報を表示します。
Summary	クエリアおよびレポート/離脱メッセージの要約統計情報を表示します。
Clear	指定された VLAN /ポートのすべての MLD 統計情報または統計情報をクリアします。

注※ AXprimoM210-08P

3 基本的な管理作業

この章では、次のトピックについて説明します。

- Displaying System Information - 基本的なシステム情報を表示します。
- Displaying Hardware/Software Versions - ハードウェアのバージョン、電源の状態、およびソフトウェアのバージョンを表示します。
- Configuring Support for Jumbo Frames - ジャンボフレームのサポートを有効にします。
- Displaying Bridge Extension Capabilities - ブリッジ拡張パラメータを表示します。
- Managing System Files - オペレーティングソフトウェアまたは構成ファイルをアップグレードし、システム起動ファイルを設定する方法について説明します。
- Setting the System Clock - 手動で、または指定された NTP または SNTP サーバを介して現在の時刻を設定します。
- Configuring the Console Port - コンソールポート接続のパラメータを設定します。
- Configuring Telnet Settings - Telnet 接続のパラメータを設定します。
- Displaying CPU Utilization - CPU 使用率に関する情報を表示します。
- Configuring CPU Guard - CPU ガードに関する閾値を設定します。
- Displaying Memory Utilization - メモリ使用率パラメータを表示します。
- Resetting the System - スイッチを直ちに再起動する、または指定された時間に再起動するための設定をします。

3.1 システム情報の表示

[System]> [General]ページを使用して、デバイス名、場所、連絡先情報などの情報を表示してシステムを識別します。

パラメータ

次のパラメータが表示されます。

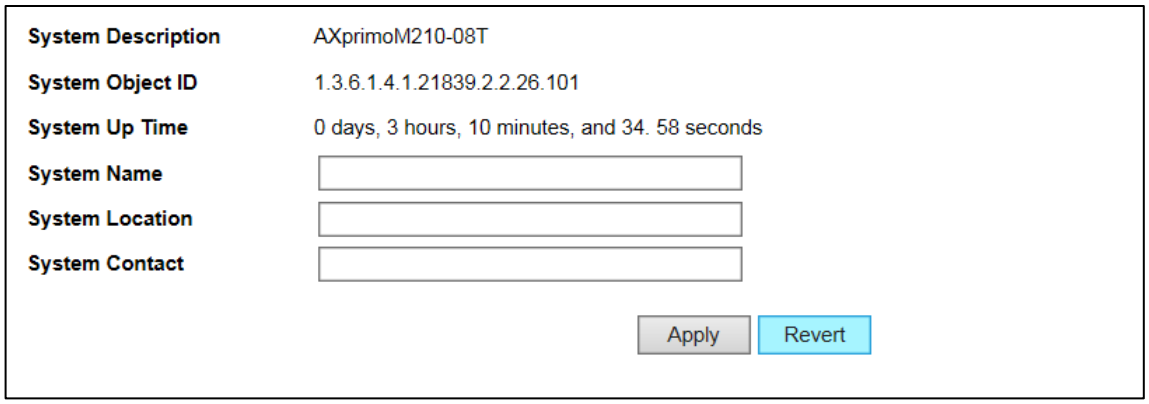
- System Description - デバイスタイプの簡単な説明です。
- System Object ID - スイッチのネットワーク管理サブシステムの MIB II オブジェクト ID の簡単な説明です。
- System Up Time - 管理エージェントが起動していた時間です。
- System Name - スイッチシステムに割当てられた名前です。
- System Location - システムの場所を指定します。
- System Contact - システムを担当する管理者です。

Web インタフェース

一般的なシステム情報を設定するには：

1. [System]、[General]をクリックします。
2. システム管理者のシステム名、場所、連絡先情報を指定します。
3. [Apply]をクリックします。

図 3-1　システム情報



3.2 ハードウェア/ソフトウェアバージョンの表示

[System]> [Switch]ページを使用して、メインボードおよび管理ソフトウェアのハードウェア/ソフトウェアバージョン番号と、システムの電源ステータスを表示します。

パラメータ

次のパラメータが表示されます。

メインボード情報

- Serial Number - スイッチのシリアル番号です。
- Number of Ports - 組み込みポートの数です。
- Hardware Version - メインボードのハードウェアバージョンです。
- Main Power Status - 内部電源装置の状態を表示します。

管理ソフトウェア情報

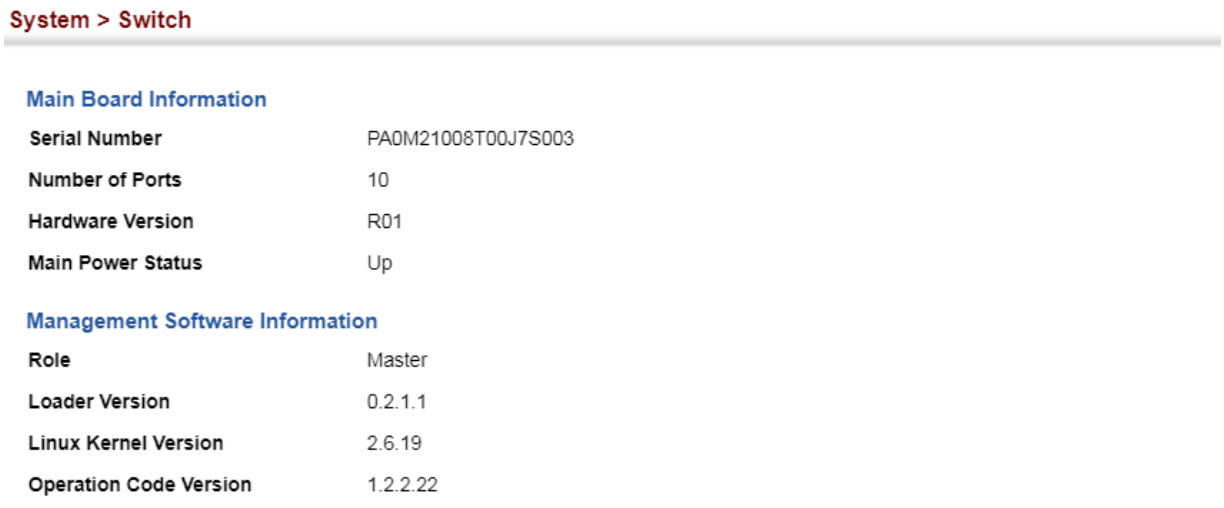
- Role - このスイッチがマスタまたはスレーブとして動作していることを示します。
- Loader Version - ローダーコードのバージョン番号です。
- Linux Kernel Version - Linux カーネルのバージョン番号です。
- Operation Code Version - ランタイムコードのバージョン番号です。

Web インタフェース

ハードウェアおよびソフトウェアのバージョン情報を表示します。

1. [System]、[Switch]の順にクリックします。

図 3-2　一般的なスイッチ情報



3.3 ジャンボフレームの設定

[System]> [Capability]ページを使用して、レイヤ 2 ジャンボフレームのサポートを設定します。スイッチは、ギガビットイーサネットおよび 10 ギガビットイーサネットポートまたはトランクの最大 10240 バイトのジャンボフレームをサポートすることにより、大規模なシーケンシャルデータ転送に対してより効率的なスループットを提供します。ジャンボフレームを使用すると、1.5 KB までしか実行されない標準イーサネットフレームと比較すると、プロトコルカプセル化フィールドを処理するために必要なパケットごとのオーバーヘッドが大幅に削減されます。

使用上のガイドライン

ジャンボフレームを使用するには、送信元と宛先の両方のエンドノード(コンピュータやサーバなど)がこの機能をサポートしている必要があります。また、接続が全二重で動作している場合、2 つのエンドノード間のネットワーク内のすべてのスイッチは、拡張フレームサイズを受け入れる必要があります。また、半二重接続の場合、衝突ドメイン内のすべてのデバイスが、ジャンボフレームをサポートしていなければなりません。

パラメータ

次のパラメータが表示されます。

◆ Jumbo Frame - ジャンボフレームのサポートを設定します。(デフォルト: Disabled)

Web インタフェース

ジャンボフレームのサポートを設定するには：

1. [System]、[Capability]の順にクリックします。
2. ジャンボフレームのサポートを有効または無効にします。
3. [Apply]をクリックします。

図 3-3　ジャンボフレームのサポートの設定

3.4 ブリッジ拡張機能の表示

[System]> [Capability]ページを使用して、Bridge MIB に基づく設定を表示します。ブリッジ MIB には、マルチキャストフィルタリング、トラフィッククラス、および VLAN をサポートする管理対象デバイスの拡張機能が含まれています。これらの拡張にアクセスして、キー変数のデフォルト設定を表示することができます。

パラメータ

次のパラメータが表示されます。

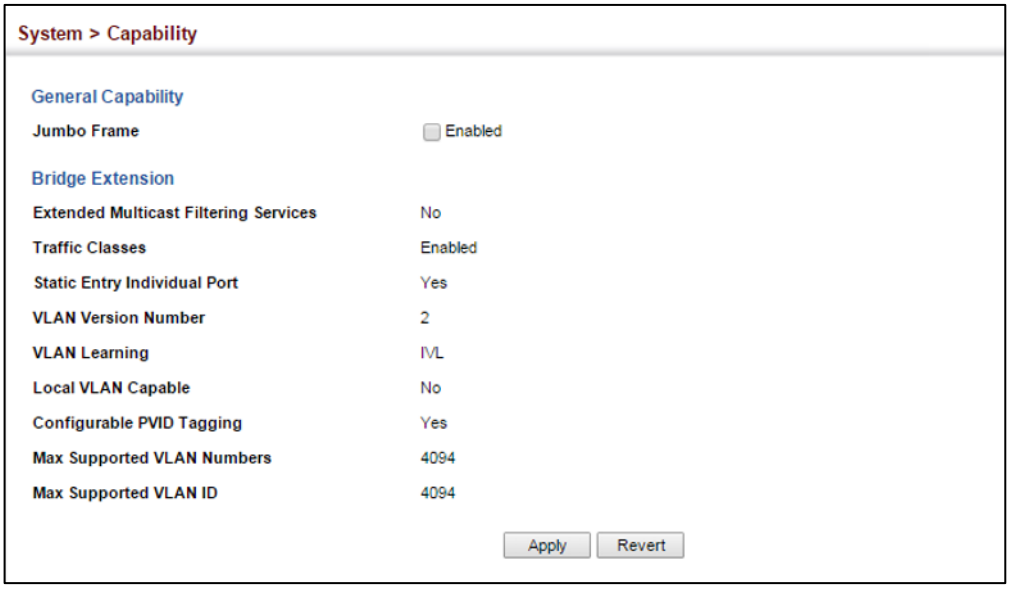
- Extended Multicast Filtering Services - このスイッチは、GMRP（GARP Multicast Registration Protocol）に基づく個々のマルチキャストアドレスのフィルタリングをサポートしていません。
- Traffic Classes - このスイッチは、ユーザの優先順位を複数のトラフィッククラスにマッピングします。（「9　CoS」を参照してください。）
- Static Entry Individual Port - このスイッチは、ユニキャストおよびマルチキャストアドレスの静的フィルタリングを可能にします。（「6.5　静的アドレスの設定」を参照してください。）
- VLAN Version Number - IEEE 802.1Q に基づいて、「1」は単一のスパニングツリー（SST）操作のみをサポートするブリッジを示し、「2」はマルチプルスパニングツリー（MST）操作をサポートするブリッジを示します。
- VLAN Learning - このスイッチでは、独立した VLAN 学習（IVL）が使用され、各ポートで独自のフィルタリングデータベースが維持されます。
- Local VLAN Capable - このスイッチは、802.1Q で定義された VLAN の範囲外の複数のローカルブリッジをサポートしていません。
- Configurable PVID Tagging - このスイッチを使用すると、各ポートでデフォルトのポート VLAN ID（フレームタグで使用される PVID）および出力ステータス（VLAN タグ付きまたはタグなし）を上書きできます。（「5　VLAN 設定」を参照してください。）
- Max Supported VLAN Numbers - このスイッチでサポートされている VLAN の最大数です。
- Max Supported VLAN ID - このスイッチでサポートされる設定可能な最大 VLAN 識別子です。

Web インタフェース

ブリッジ拡張情報を表示するには：

1. [System]、[Capability]の順にクリックします。

図 3-4　ブリッジ拡張設定の表示



3.5 システムファイルの管理

ここでは、スイッチのオペレーティングソフトウェアまたはコンフィグレーションファイルをアップグレードし、システムのスタートアップファイルを設定する方法について説明します。

警告: システムファイル管理を正確に実施するために、システムファイルの管理について変更等の操作を行う場合は、本スイッチへのセッションが 1 つであることを確認の上、実施してください。

3.5.1 FTP/ TFTP または HTTP によるファイルコピー

[System]>[File（Copy）]ページを使用して、FTP、TFTP または HTTP を使用してソフトファームウェアまたはコンフィグレーションをアップロード/ダウンロードします。ファイルを FTP /TFTP サーバまたは管理ステーションにバックアップすることによって、そのファイルを後でスイッチにダウンロードして復元操作を行うことができます。必要に応じて、ファイル転送の方法と、ファイルの種類とファイル名を指定します。

現在のバージョンを上書きせずに、新しいソフトウェアまたはコンフィグレーションを使用するようにスイッチを設定することもできます。現在のバージョンとは異なる名前を使用してファイルをダウンロードし、新しいファイルをスタートアップファイルとして設定します。

コマンドの使用方法

- FTP サーバにログインすると、インタフェースはリモートサーバに設定されたユーザ名とパスワードの入力を要求します。“anonymous”がデフォルトのユーザ名として設定されていることに、注意してください。
- フラッシュメモリへのコピー操作中は、リセットコマンドは受け付けられません。

パラメータ

次のパラメータが表示されます。

- Copy Type – ソフトウェアのコピー操作には、次のオプションがあります。
  - Running-Config - ランニングコンフィグレーションをスタートアップコンフィグレーションファイルにコピーします。
  - FTP Upload - ファイルを FTP サーバからスイッチにコピーします。
  - FTP Download - ファイルをスイッチから FTP サーバにコピーします。
  - HTTP Upload - ファイルを管理ステーションからスイッチにコピーします。
  - HTTP Download - ファイルをスイッチから管理ステーションにコピーします。
  - TFTP Upload - ファイルを TFTP サーバからスイッチにコピーします。
  - TFTP Download - ファイルをスイッチから TFTP サーバにコピーします。
- FTP/ TFTP Server IP Address - FTP / TFTP サーバの IP アドレスです。
- User Name - FTP サーバクセスのユーザ名です。
- Password - FTP サーバクセスのパスワードです。
- File Type – ソフトウェアをコピーするためのオペレーションコードを指定してください。
- File Name - ファイル名にはスラッシュ（¥または/）を使用しないでください。ファイル名の先頭文字

はピリオド（.）であってはならず、ファイル名の最大長はスイッチ上のファイルでは 32 文字 (有効な文字: A-Z, a-z, 0-9, “.”, “-”, “_”)

Note: システムソフトウェアの 2 つまでのコピー（すなわちランタイムソフトウェア）をスイッチのファイルディレクトリに格納することができます。

Note: ユーザ定義の構成ファイルの最大数は、使用可能なフラッシュメモリ空間によってのみ制限されます。

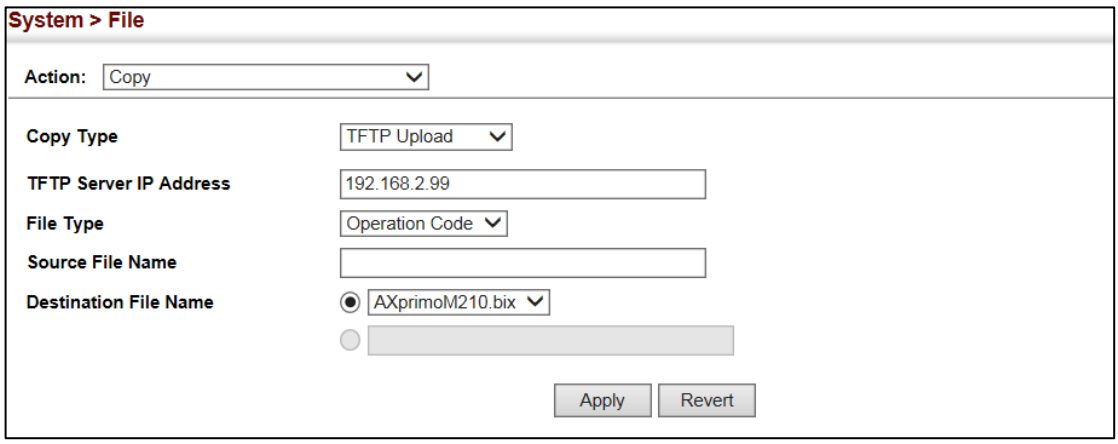
Note: ファイル “Factory_Default_Config.cfg” は、ファイルサーバまたは管理ステーションにコピーできますが、スイッチの宛先ファイル名としては使用できません。

Web インタフェース

ソフトウェアファイルをコピーするには：

1. [System]、[File]の順にクリックします。
2. [Action]リストから[Copy]を選択します。
3. ファイル転送方法として FTP アップロード、HTTP アップロード、または TFTP アップロードを選択します。
4. FTP、または TFTP Upload が使用されている場合は、ファイルサーバの IP アドレスを入力します。
5. FTP Upload が使用されている場合は、FTP サーバにアカウントのユーザ名とパスワードを入力します。
6. ファイルタイプを Operation Code に設定します。
7. ダウンロードするファイル名を入力します。
8. スイッチ上のファイルを選択して上書きするか、新しいファイル名を指定します。
9. 次に、[Apply]をクリックします。

図 3-5　ソフトウェアのコピー



現在起動しているファイルを置き換えて新しいファイルの使用を開始する場合は、[System]>[Reset]メニューからシステムを再起動してください。

3.5.2 ローカルファイルへのランニングコンフィグレーションの保存

[System]> [File（Copy）]ページを使用して、現在の設定をスイッチのローカルファイルに保存します。コ

ンフィグレーションは、スイッチが再起動されたときに後で使用するためにシステムによって自動的に保存されません。これらの設定は、現在のスタートアップファイル、または後でスタートアップファイルとして設定できる別のファイルに保存する必要があります。

パラメータ

次のパラメータが表示されます。

- Copy Type - コピー操作には次のオプションがあります。
  - Running-Config - 現在の設定をスイッチ上のローカルファイルにコピーします。
- Destination File Name - 現在指定されているスタートアップファイルまたは新しいファイルにコピーします。ファイル名にスラッシュ（¥または/）を使用しないでください。ファイル名の先頭文字はピリオド（.）でなく、ファイル名の最大長は 32 文字です。(有効な文字: A-Z, a-z, 0-9, “.”, “-”, “_”)

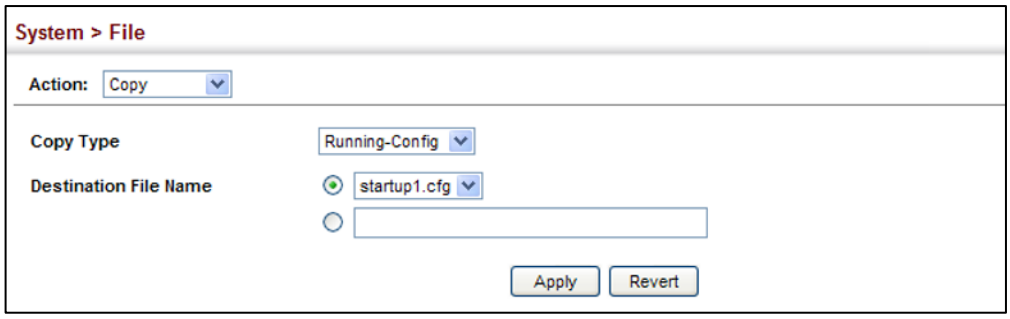
Note: ユーザ定義の構成ファイルの最大数は、使用可能なフラッシュメモリ空間によってのみ制限されます。

Web インタフェース

ランニングコンフィグレーションファイルを保存するには：

1. [System]、[File]の順にクリックします。
2. [Action]リストから[Copy]を選択します。
3. Copy Type リストから Running-Config を選択します。
4. スイッチ上の現在のスタートアップファイルを選択して上書きするか、新しいファイル名を指定します。
5. 次に、[Apply]をクリックします。

図 3-6　ランニングコンフィグレーションの保存



現在起動しているファイルを置き換えて新しいファイルの使用を開始する場合は、[System]>[Reset]メニューからシステムを再起動してください。

3.5.3 スタートアップコンフィグレーションの設定

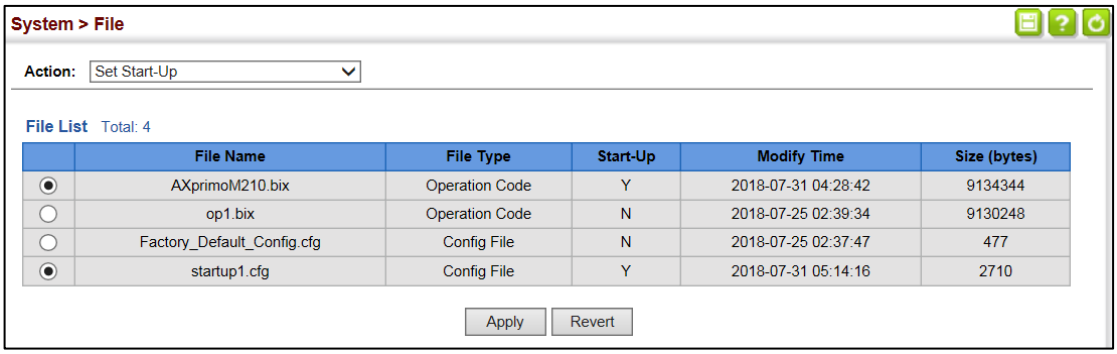
[System] >[File（Set Start-Up）]ページを使用して、システムの初期化に使用するソフトウェアまたはコンフィグレーションファイルを指定します。

Web インタフェース

システムの初期化に使用するファイルを設定するには：

1. [System]、[File]の順にクリックします。
2. [Action]リストから[Set Start-Up]を選択します。
3. 起動時に使用されるオペレーションコードまたは構成ファイルをマークします。
4. 次に、[Apply]をクリックします。

図 3-7　起動ファイルの設定



新しいソフトウェアまたはコンフィグレーションの使用を開始するには、[System]>[Reset]メニューからシステムを再起動します。

3.5.4 システムファイルの表示

[System] >[File（show）]ページを使用して、システムディレクトリにファイルを表示するか、ファイルを削除します。

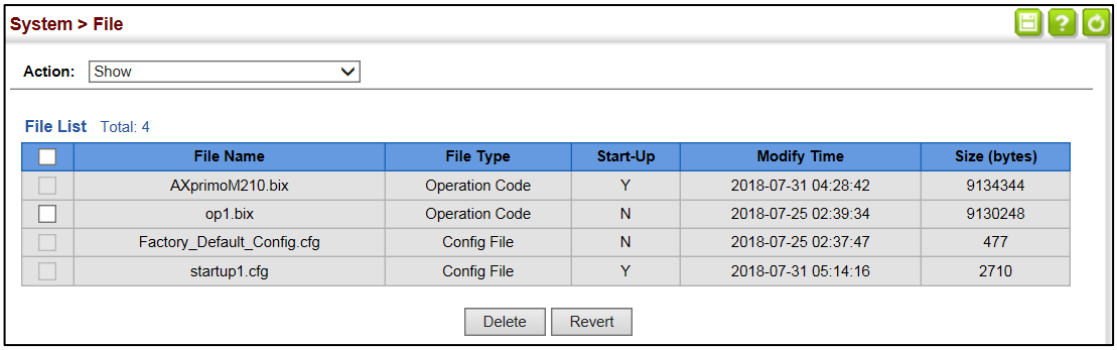
Note: 始動用に指定されたファイル、および Factory_Default_Config.cfg ファイルは削除できません。

Web インタフェース

システムファイルを表示するには：

1. [System]、[File]の順にクリックします。
2. [Action]リストから[Show]を選択します。
3. ファイルを削除するには、ファイルリストでそのファイルをマークし、[Delete]をクリックします。

図 3-8　システムファイルの表示



3.5.5 オペレーションコードの自動アップグレード

[System]>[File（Automatic Operation Code Upgrade）]ページを使用して、現在インストールされているファ

イルよりも新しいファイルがファイルサーバ上で検出されたときに自動アップグレードすることを指定します。

ファイルがサーバから転送され、ファイルシステムに正常に書き込まれると、自動的にスタートアップファイルとして設定されます。新しいオペレーションコードファイルの使用を開始するには、[System]>[Reset]メニューからシステムを再起動する必要があります。

使用上のガイドライン

- この機能が有効化されると、スイッチは起動シーケンス中に定義された URL を一度検索します。

  新しいソフトウェアの使用を開始するには、[System]>[Reset]メニューからシステムを再起動します。
- FTP (ポート 21)と TFTP (ポート 69)の両方がサポートされます。TCP/UDP ポートバインディングは変更できないため、非標準ポートで待ち受けているサーバはサポートしていません。
- 自動アップグレードを実施する時、IP インタフェースは装置に 1 つのみとしてください。
- アップグレードファイルの場所の URL のホスト部分は、有効な IPv4 IP アドレスである必要があります。DNS ホスト名は認識されません。有効な IP アドレスは、ピリオドで区切られた 0 から 255 の 4 つの数字で構成されます。
- ディレクトリへのパスも、定義する必要があります。ファイルが FTP / TFTP サービスのルートディレクトリに保存されている場合は、「/」を使用して指定します（例：ftp://192.168.0.1/）。
- ファイル名は、アップグレードファイルの場所の URL に含めないでください。リモートサーバに保存されているコードのファイル名は、AXprimoM210.bix （大文字と小文字を正確にここに示すとおりに使用する）でなければなりません。このマニュアルに記載されている他のスイッチのファイル名は、Web インタフェースに表示されているとおりに正確に入力してください。
- FTP は、有効化された PASV モードで接続されます。FTP トラフィックがブロックされていない場合でも、PASV モードがいくつかのファイアウォールを通過する必要があります。PASV モードを無効にすることはできません。
- スイッチベースの検索機能は、大文字または小文字のファイル名を受け入れるという点で大文字と小文字を区別しません（つまり、AXprimoM210.BIX が要求されても、スイッチはサーバから AXprimoM210.bix を受け入れます）。しかし、Unix や Unix に似たシステム(FreeBSD、NetBSD、OpenBSD や、ほとんどの Linux ディストリビューションなど）のような多くのオペレーティングシステムのファイルシステムでは、大文字と小文字が区別されます。つまり、同じディレクトリにある 2 つのファイル、axprimom210.bix および AXprimoM210.BIX は一意のファイルとみなされます。したがって、アップグレードファイルが AXprimoM210.bix（または AxprimoM210.bix）として大文字小文字を区別するサーバに格納されている場合、サーバはアップグレードされません（axprimom210.bix を要求しています）。 要求されたファイル名と格納されているファイル名が等しいと認識します。大文字と小文字を区別する Unix ライクなオペレーティングシステムのリストにある注目すべき例外は Mac OS X で、デフォルトでは大文字と小文字を区別しません。ファイルシステムの動作が不明な場合は、ご使用のサーバのオペレーティングシステムマニュアルを確認してください。
- スイッチ自体は、大文字のファイル名と小文字のファイル名を区別せず、サーバに保存されているファイルが現在のランタイムイメージより新しいかどうかを確認するだけです。
- 2 つのオペレーションコードイメージファイルが既にスイッチのファイルシステムに保存されている場合には、非起動イメージはアップグレードイメージが転送される前に削除されます。
- 自動アップグレード処理が、スイッチの正常な動作(データの切り替えなど)を妨げることなく動作します。
- 自動検索および転送処理中に、管理者は他のオペレーションコードイメージ、設定ファイル、パブリックキー、または HTTPS 証明書の転送またはアップグレードすることができません(例; 同時に他のファイル管理操作は不可能です)。

◆ アップグレード用オペレーションコードイメージは、ファイルシステムへの書き込みに成功した後に、起動イメージとして設定されます。

◆ スイッチは SNMP トラップを送信し、すべてのアップグレードの成功と失敗時にログエントリを作成します。

パラメータ

次のパラメータが表示されます。

◆ Automatic Opcode Upgrade - スイッチがスイッチの起動プロセス中にアップグレードされたオペレーションコードファイルを検索できるようにします。(デフォルト: Disabled)

◆ Automatic Upgrade Location URL - スイッチがオペレーションコードのアップグレードファイルを検索する場所を定義します。この URL の最後の文字は、スラッシュ（ "/"）でなければなりません。AXprimoM210.bix ファイル名は、スイッチによって自動的に付加されるため、含めないでください。(オプション: ftp, tftp)
それぞれ、以下例のように定義してください:
tftp://*host*[/*filedir*]/

- tftp://- サーバ接続の TFTP プロトコルを定義します。
- *host* - TFTP サーバの IP アドレスを定義します。有効な IP アドレスは、ピリオドで区切られた 0 から 255 の 4 つの数字で構成されます。DNS ホスト名は認識されません。
- *filedir* - アップグレードファイルが見つかる TFTP サーバのルートからの相対的なディレクトリを定義します。ネストされたディレクトリ構造が受け入れられます。ディレクトリ名は、ホストとネストされたディレクトリ構造で親ディレクトリから分離し、先頭にスラッシュ「/」を付ける必要があります。
- / - スラッシュは URL の最後の文字でなければなりません。

ftp://[*username*[:*password*@]]*host*[/*filedir*]/

- ftp://- サーバ接続の FTP プロトコルを定義します。
- *username* - FTP 接続のユーザ名を定義します。ユーザ名が省略されている場合には、接続のために” anonymous”が仮定のユーザ名となります。
- *password* - FTP 接続のためにパスワードを定義します。ユーザ名と URL のホスト部分からのパスワードと差をつけるために、コロン (:) をパスワードの前に付け、“at”シンボル (@)をパスワードの後に付ける必要があります。パスワードが省略されている場合には、“” (空文字列)が接続の仮想パスワードになります。
- *host* - FTP サーバの IP アドレスを定義します。有効な IP アドレスは、ピリオドで区切られた 0 から 255 の 4 つの数字で構成されます。DNS ホスト名は認識されません。
- *filedir* - アップグレードファイルが見つかる FTP サーバのルートからの相対的なディレクトリを定義します。ネストされたディレクトリ構造が受け入れられます。ディレクトリ名は、ホストとネストされたディレクトリ構造で親ディレクトリから分離し、先頭にスラッシュ「/」を付ける必要があります。
- / - スラッシュは URL の最後の文字でなければなりません。

例
次の例では、IP アドレス 192.168.0.1 の TFTP サーバの URL 構文を、さまざまな場所に格納されたオペレーションコードイメージとともに示しています。

- tftp://192.168.0.1/
  イメージファイルは TFTP ルートディレクトリにあります。

- tftp://192.168.0.1/switch-opcode/
  イメージファイルは TFTP ルートを基準にした "switch-opcode"ディレクトリにあります。
- tftp://192.168.0.1/switches/opcode/
  イメージファイルは、 "switches"の親ディレクトリの TFTP ルートを基準にした "opcode"ディレクトリにあります。

次の例は、IP アドレス 192.168.0.1 の FTP サーバの URL 構文を示し、さまざまなユーザ名、パスワード、およびファイルの場所のオプションが示されています。

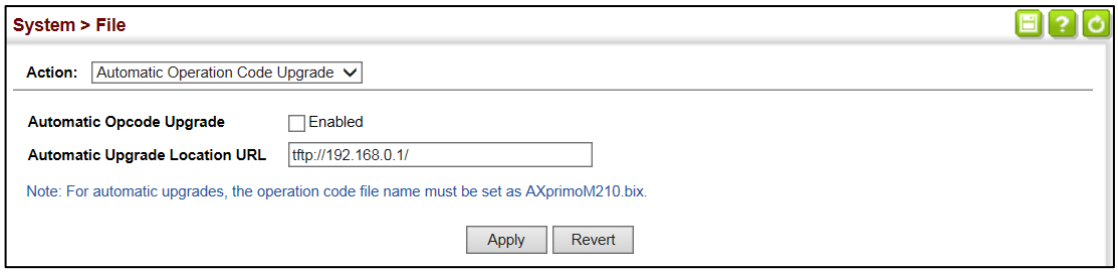
- ftp://192.168.0.1/
  ユーザ名とパスワードは空です。したがって、「anonymous」がユーザ名になり、パスワードは空白になります。イメージファイルは FTP ルートディレクトリにあります。
- ftp://switches:upgrade@192.168.0.1/
  ユーザ名は“switches”、パスワードは“upgrade”です。イメージファイルは FTP ルートにあります。
- ftp://switches:upgrade@192.168.0.1/switches/opcode/
  ユーザ名は“switches”、パスワードは“upgrade”です。イメージファイルは、 “switches”親ディレクトリの FTP ルートに関連する “opcode”ディレクトリにあります。

Web インタフェース

自動アップグレードを設定するには：

1. [System]、[File]の順にクリックします。
2. Action リストから[Automatic Operation Code Upgrade]を選択します。
3. オペレーションコードの自動アップグレードを有効にするには、チェックボックスをオンにします。
4. FTP または TFTP サーバの URL、およびオペレーションコードを含むパスとディレクトリを入力します。
5. [Apply]をクリックします。

図 3-9　自動アップグレードの設定



指定した場所で新しいイメージが検出されると、ブートアップ中に以下のメッセージタイプが表示されます。

```
.
.
.
Automatic Upgrade is looking for a new image
New image detected: current version 1.2.1.3; new version 1.2.1.6
Image upgrade in progress
Downloading new image
```

```
Flash programming started
Flash programming completed
.
.
.
```

3.6 システムクロックの設定

シンプルネットワークタイムプロトコル（SNTP）は、スイッチがタイムサーバ（SNTP または NTP）からの定期的なアップデートに基づいて内部クロックを設定できるようにします。スイッチの正確な時刻を維持することで、システムログにイベントエントリの意味のある日時を記録することができます。また手動でクロックを設定することもできます。クロックが手動で設定されていない場合や、SNTP または NTP を介して設定されていない場合には、スイッチは最後の起動時に設定された、工場出荷時のデフォルト設定からの時刻だけを記録します。

警告: スイッチイベントを正確に記録するために、SNTP または NTP を使うことを強く推奨します。システムクロックの手動での設定の場合、システムイベントのタイムスタンプが正確でない場合があります。

SNTP クライアントが有効な場合、スイッチは設定されたタイムサーバに時刻更新の要求を定期的に送信します。最大 3 つのタイムサーバ IP アドレスを設定することができます。スイッチは、設定された順序で各サーバのポーリングを試みようとします。

3.6.1 時刻の手動設定

SNTP または NTP を使用せずに手動でスイッチのシステム時間を設定するには、[System]> [Time（Configure General - Manual）]ページを使用します。

パラメータ

次のパラメータが表示されます。

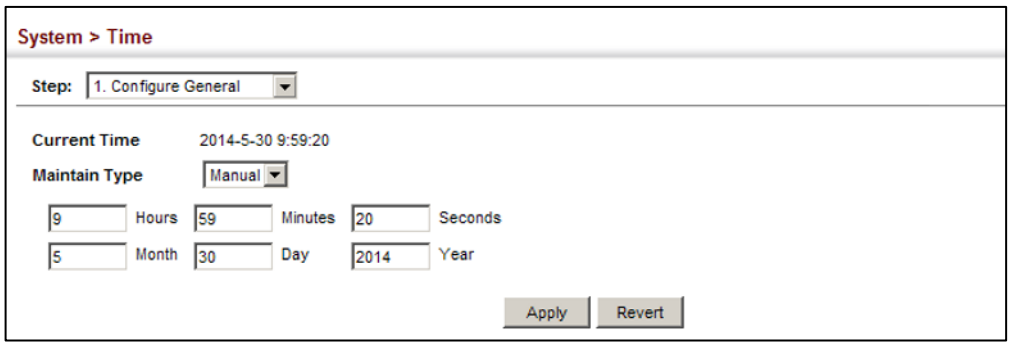
- Current Time - スイッチに設定されている現在の時刻を表示します。
- Hours - 時間を設定します。(範囲: 0 から 23)
- Minutes - 分の値を設定します。(範囲: 0 から 59)
- Seconds - 秒の値を設定します。(範囲: 0 から 59)
- Month - 月を設定します。(範囲: 1 から 12)
- Day - 日を設定します。(範囲: 1 から 31)
- Year - 年を設定します。(範囲: 1970 から 2037)

Web インタフェース

手動でシステムクロックを設定するには :

1. [System]、[Time]の順にクリックします。
2. [Step]リストから[Configure General]を選択します。
3. [Maintain Type]リストから[Manual]を選択します。
4. 該当するフィールドに時間と日付を入力します。
5. [Apply]をクリックします。

図 3-10　システムクロックの手動設定



3.6.2 SNTP ポーリング間隔の設定

[System]> [Time（Configure General - SNTP）]ページを使用して、スイッチが指定されたタイムサーバに照会するポーリング間隔を設定します。

パラメータ

次のパラメータが表示されます。

- Current Time - スイッチに設定されている現在の時刻を表示します。
- SNTP Polling Interval - タイムサーバからの時刻更新の要求送信間隔を設定します。(範囲: 16 から 16384 秒; デフォルト: 16 秒)

Web インタフェース

SNTP のポーリング間隔を設定するには：

1. [System]、[Time]の順にクリックします。
2. [Step]リストから[Configure General]を選択します。
3. [Maintain Type]リストから[SNTP]を選択します。
4. 必要に応じてポーリング間隔を変更します。
5. [Apply]をクリックします。

図 3-11　SNTP のポーリング間隔の設定

3.6.3 NTP の設定

[System]> [Time（Configure General - NTP）]ページを使用して、NTP 認証を設定し、スイッチが指定されたタイムサーバに照会するポーリング間隔を表示します。

パラメータ

次のパラメータが表示されます。

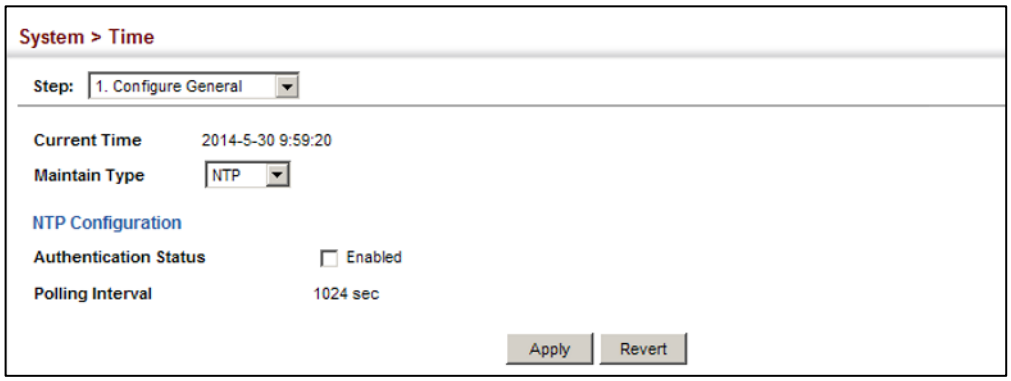
- Current Time - スイッチに設定されている現在の時刻を表示します。
- Authentication Status - スイッチと NTP サーバ間の時間要求と更新の認証を有効にします。(デフォルト: Disabled)
  NTP 認証を有効にすると、認証された NTP サーバからの信頼できる更新が確実に受信されます。認証キーとそれに関連するキー番号は一元的に管理し、NTP サーバとクライアントに手動で配布する必要があります。キー番号とキー値は、サーバとクライアントの両方で一致する必要があります。
- Polling Interval - NTP サーバからの時刻更新要求の送信間隔を示します。（一定：1024 秒)

Web インタフェース

クロックメンテナンスタイプを NTP に設定するには：

1. [System]、[Time]の順にクリックします。
2. [Step]リストから[Configure General]を選択します。
3. [Maintain Type]リストから[NTP]を選択します。
4. 必要に応じて認証を有効にします。
5. [Apply]をクリックします。

図 3-12　NTP の設定



3.6.4 タイムサーバの設定

[System]> [Time（Configure Time Server）]ページを使用して、NTP / SNTP タイムサーバの IP アドレスを指定するか、NTP タイムサーバの認証キーを設定します。

(1)　SNTP タイムサーバの指定

[System]> [Time（Configure Time Server - Configure SNTP Server）]ページを使用して、最大 3 つの SNTP タイムサーバの IP アドレスを指定します。

パラメータ

次のパラメータが表示されます。

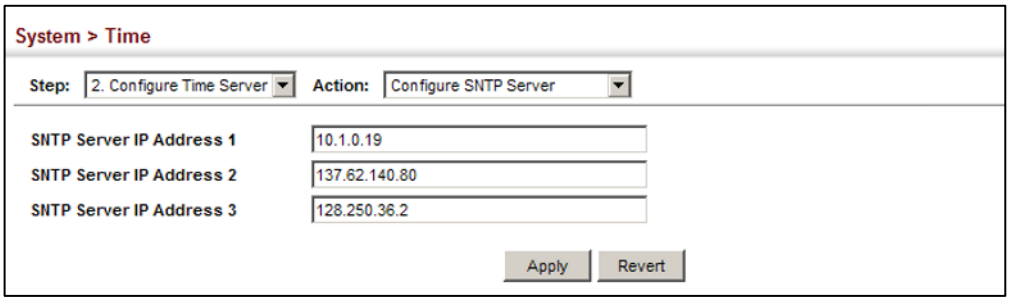
- SNTP Server IP Address - 最大 3 つのタイムサーバの IPv4 アドレスを設定します。スイッチは、最初のサーバから時刻を更新しようとします。これが失敗すると、シーケンス内の次のサーバからのアップデートが試行されます。

Web インタフェース

SNTP タイムサーバを設定するには：

1. [System]、[Time]の順にクリックします。
2. [Step]リストから[Configure Time Server]を選択します。
3. [Action]リストから[Configure SNTP Server]を選択します。
4. 最大 3 つのタイムサーバの IP アドレスを入力します。
5. [Apply]をクリックします。

図 3-13　SNTP タイムサーバの指定



(2)　NTP タイムサーバの指定

[System]> [Time（Configure Time Server - Add NTP Server）]ページを使用して、最大 50 の NTP タイムサーバの IP アドレスを追加します。

パラメータ

次のパラメータが表示されます。

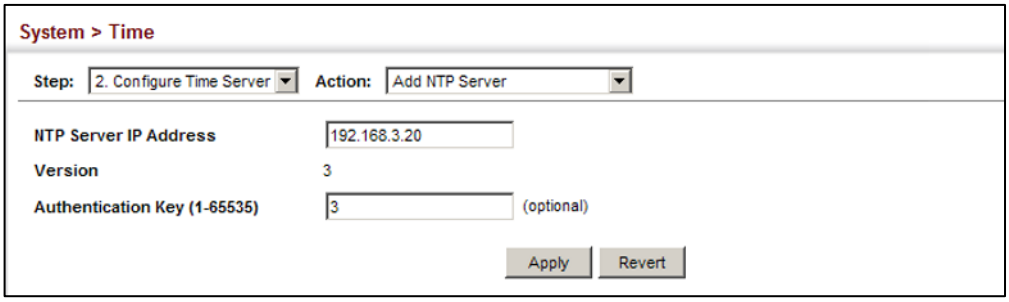
- NTP Server IP Address - 最大 3 つのタイムサーバの IPv4 アドレスを設定します。スイッチは、[System]>[Time（Configure General ）]ページでクロックメンテナンスタイプが NTP に設定されている場合、指定されたタイムサーバにアップデートをポーリングします。これは、1024 秒の固定間隔で時刻同期要求を発行します。スイッチは設定されているすべてのタイムサーバをポーリングし、受信したレスポンスをフィルタリングして比較して、スイッチの最も信頼性の高い正確な時刻アップデートを決定します。
- Version - サーバでサポートされている NTP のバージョンを指定します。(Version 3 固定)
- Authentication Key - 設定されたサーバとの認証に使用する NTP 認証キーリストのキーの番号を指定します。NTP 認証はオプションです。[System]> [Time（Configure General）]ページで有効になっている場合は、[System]> [Time（Add NTP Authentication Key）]ページで少なくとも 1 つの鍵を設定する必要があります。(範囲: 1 から 65533)

Web インタフェース

サーバリストに NTP タイムサーバを追加するには、次の手順を実行します。

1. [System]、[Time]の順にクリックします。
2. [Step]リストから[Configure Time Server]を選択します。
3. [Action]リストから[Add NTP Server]を選択します。
4. NTP タイムサーバの IP アドレスを入力し、認証が必要な場合は認証鍵のインデックスを指定します。
5. [Apply]をクリックします。

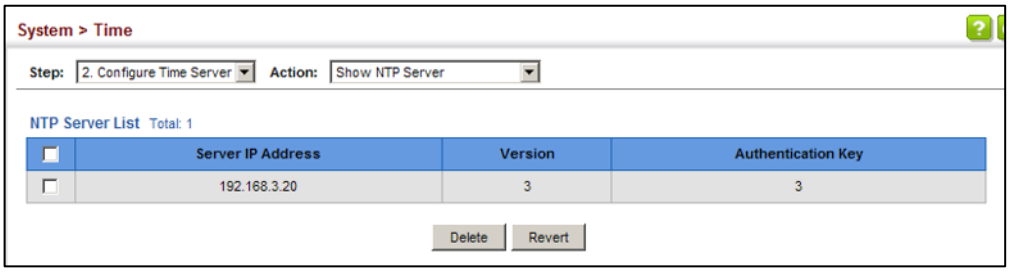
図 3-14　NTP サーバを追加



設定済みの NTP タイムサーバのリストを表示するには、次の手順を実行します。

1. [System]、[Time]の順にクリックします。
2. [Step]リストから[Configure Time Server]を選択します。
3. [Action]リストから[Show NTP Server]を選択します。

図 3-15　NTP タイムサーバリストの表示



3.6.5 NTP 認証鍵の指定

[System]> [Time（Configure Time Server - Add NTP Authentication Key）]ページを使用して、認証キーリストにエントリを追加します。

パラメータ

次のパラメータが表示されます。

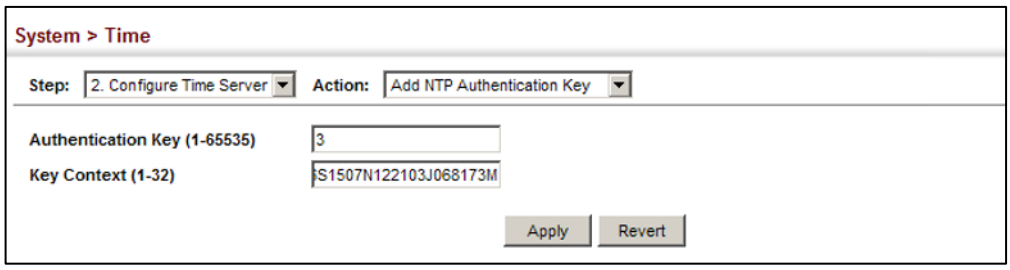
- Authentication Key - 設定されたサーバとの認証に使用する NTP 認証キーリストのキーの番号を指定します。.NTP 認証はオプションです。[System]> [Time（Configure General）]ページで有効にすると、このページに少なくとも 1 つのキーも設定する必要があります。スイッチでは最高 255 文字まで設定することができます。(範囲: 1 から 65535)
- Key Context - Md5 認証鍵文字列です。キー文字列は、最大 32 文字の大文字と小文字を区別できる印字可能な ASCII 文字(スペースなし)です。
  NTP 認証の鍵番号と値は、サーバとクライアントの両方で一致する必要があります。

Web インタフェース

NTP 認証鍵リストにエントリを追加するには：

1. [System]、[Time]の順にクリックします。
2. [Step]リストから[Configure Time Server]を選択します。
3. [Action]リストから[Add NTP Authentication Key]を選択します。
4. インデックス番号と MD5 認証キー文字列を入力します。
5. [Apply]をクリックします。

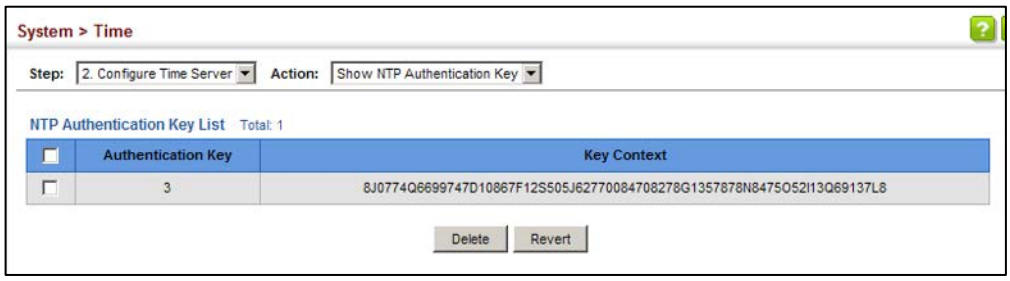
図 3-16　NTP 認証キーの追加



設定済みの NTP 認証キーのリストを表示するには：

1. [System]、[Time]の順にクリックします。
2. [Step]リストから[Configure Time Server]を選択します。
3. [Action]リストから[Show NTP Authentication Key]を選択します。

図 3-17　NTP 認証キーリストの表示



3.6.6 タイムゾーンの設定

[System]> [Time（Configure Time Zone）]ページを使用して、時間帯を設定します。SNTP は、イングランドのグリニッジを通過する地球の本来の子午線（経度 0 度）の時間に基づいて協定世界時（UTC、以前はグリニッジ標準時、または GMT）を使用しています。現地時間に対応する時間を表示するには、時間帯が UTC の東(前)または西(後)にある時間と分の数を指定する必要があります。80 の定義済みタイムゾーン定義のいずれかを選択するか、ローカルタイムゾーンのパラメータを手動で設定できます。

パラメータ

次のパラメータが表示されます。

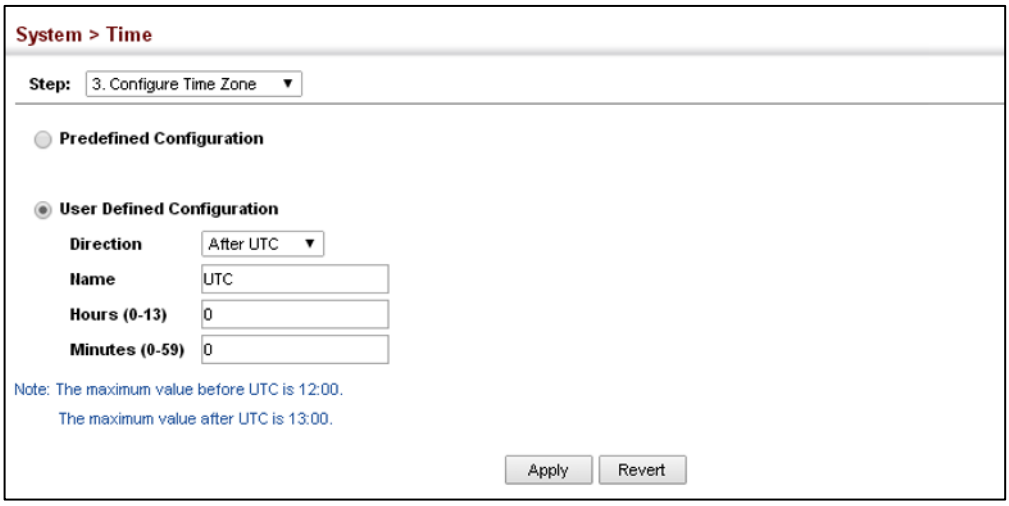
- Predefined Configuration - ドロップダウンボックスを使用すると、事前定義された 80 のタイムゾーン設定にアクセスできます。それぞれの選択肢は、UTC からオフセットされていることを示し、タイムゾーンでカバーされる少なくとも 1 つの主要都市または場所をリストします。
- User-defined Configuration - ユーザがローカルタイムゾーンのすべてのパラメータを定義できるようにします。
  - Direction - タイムゾーンを UTC の前（東方）または後（西側）に設定します。
  - Name - タイムゾーンに名前を割当てます。(範囲: 1 から 30 文字)
  - Hours (0-13) - UTC の前後の時間です。UTC 前の最大値は 12 です。UTC 後の最大値は 13 です。
  - Minutes (0-59) - UTC の前後の分です。

Web インタフェース

現地時間帯を設定するには：

1. [System]、[Time]の順にクリックします。
2. [Step]リストから[Configure Time Zone]を選択します。
3. タイムゾーンのオフセットを UTC との相対的な時間と分で設定します。
4. [Apply]をクリックします。

図 3-18　タイムゾーンの設定



3.6.7 サマータイムの設定

サマータイムページを使用して、夏季にシステムクロックを前方に設定します（サマータイムとも呼ばれます)。

国や地域によっては、時計は夏の季節に調整され、午後には昼間が長く午前中は短くなります。これは、サマータイムまたは夏時間(DST)として知られています。通常、クロックは春の開始時に 1 時間前に調整され、その後秋には後ろに調整されます。

パラメータ

次のパラメータが Web インタフェースに表示されます。

一般的な設定

- Summer Time in Effect - システム時刻が調整されたかどうかを示します。
- Status - サマータイムが指定された期間中有効になるように設定されているかどうかを示します。
- Name - サマータイムが有効な時間帯の名前です。通常は略語です。(範囲: 1 から 30 文字)
- Mode - 次のいずれかの設定モードを選択します。(Mode オプションは、Summer Time Status オプションがスイッチでイネーブルに設定されている場合にのみ管理できます)。

Predefined Mode - 世界のいくつかの主要地域で事前定義された設定を使用して、夏時間のステータスとスイッチを設定します。サマータイムが有効になっている現地時間に対応する時間を指定するには、お住まいの地域に適した事前定義されたサマータイムゾーンを選択します。

表 3-1　事前定義された夏時間パラメータ

地域	開始時刻、曜日、週、および月	終了時刻、曜日、週、および月	Rel.オフセット
オーストラリア	10 月第 1 日曜日 02:00:00	4 月第 1 日曜日 01:59:59	60 分
ヨーロッパ	3 月最終日曜日 01:00:00	10 月最終土曜日 23:59:59	60 分
ニュージーランド	9 月最終日曜日 02:00:00	4 月第 1 日曜日 01:59:59	60 分

地域	開始時刻、曜日、週、および月	終了時刻、曜日、週、および月	Rel.オフセット
アメリカ	3 月第 2 日曜日 02:00:00	11 月第 1 日曜日 00:59:59	60 分

Date Mode - スイッチのサマータイムの開始、終了、およびオフセット時間を一度に設定します。このモードでは、現在設定されているタイムゾーンを基準にサマータイムゾーンを設定します。サマータイムが有効になっている現地時間に対応する時間を指定するには、サマータイムゾーンが通常のタイムゾーンから逸脱した分の数を指定する必要があります。

- Offset - サマータイムは通常のタイムゾーンから分単位でオフセットされます。(範囲: 1 から 120 分)
- From - サマータイムオフセットの開始時刻です。
- To - サマータイムオフセットの終了時刻です。

Recurring Mode - 定期的にスイッチのサマータイムの開始、終了、およびオフセット時間を設定します。このモードでは、現在設定されているタイムゾーンを基準にサマータイムゾーンを設定します。サマータイムが有効になっている現地時間に対応する時間を指定するには、サマータイムゾーンが通常のタイムゾーンから逸脱した分の数を指定する必要があります。

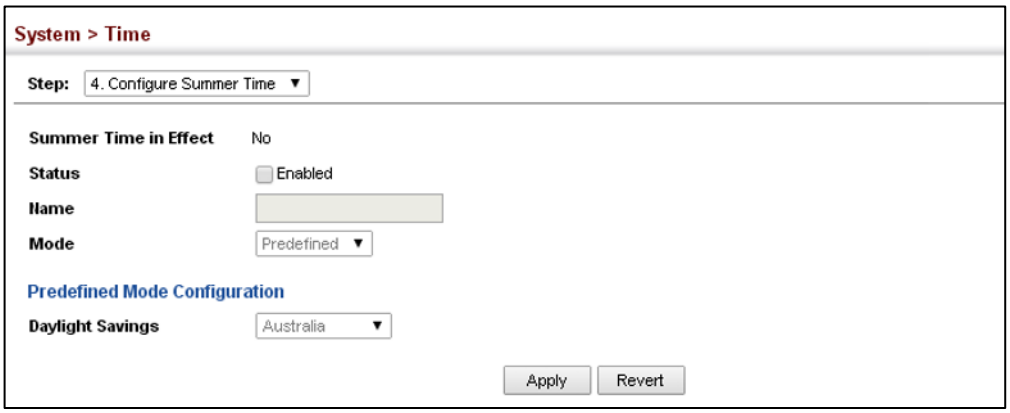
- Offset - サマータイムは通常のタイムゾーンから分単位でオフセットされます。(範囲: 1 から 120 分)
- From - サマータイムオフセットの開始時刻です。
- To - サマータイムオフセットの終了時刻です。

Web インタフェース

サマータイムの設定を指定するには：

1. SNTP、Summer Time をクリックします。
2. 設定モードの 1 つを選択し、関連するアトリビュートを設定し、サマータイムステータスを有効にします。
3. [Apply]をクリックします。

図 3-19　サマータイムの設定



3.7 コンソールポートの設定

[System]> [Console]メニューを使用して、スイッチのコンソールポートの接続パラメータを設定します。VT100 互換デバイスをスイッチのシリアルコンソールポートに接続することで、スイッチにアクセスできます。コンソールポートによる管理アクセスは、パスワード（CLI を使用してのみ設定可能）、タイムアウト、基本的な通信設定など、さまざまなパラメータによって制御されます。これらのパラメータは、Web インタフェースまたは CLI インタフェースを使用して設定できます。

パラメータ

次のパラメータが表示されます。

- Login Timeout - システムがユーザに CLI へのログインを待つ間隔を設定します。タイムアウト間隔内にログイン試行が検出されない場合、セッションは終了します。(範囲: 10 から 300 秒、デフォルト: 300 秒)
- Exec Timeout - ユーザの入力が検出されるまで、システムが待機する間隔を設定します。タイムアウト時間内にユーザの入力が検出されない場合、セッションは終了します。(範囲: 60 から 65535 秒、デフォルト: 600 秒)
- Password Threshold - 失敗したログオン試行回数を制限するパスワード侵入閾値を設定します。ログオン試行の閾値に達すると、次のログオン試行を許可する前に、システムインタフェースが指定された時間（Silent Time パラメータで設定された時間）は管理コンソールにアクセスできません（サイレントになります）。(範囲: 1 から 120、デフォルト: 3 回の試行)
- Silent Time - 失敗したログオン試行の回数を超えた後で、管理コンソールにアクセスできない時間を設定します。(範囲: 1 から 65535 秒、デフォルト: Disabled)
- Data Bits - コンソールポートによって解釈され生成される文字あたりのデータビット数を設定します。パリティが生成されている場合は、1 文字につき 7 データビットを指定します。パリティを必要としない場合は、1 文字につき 8 データビットを指定します。(デフォルト: 8 bits)
- Stop Bits - バイトごとに送信されるストップビットの数を設定します。(範囲: 1 から 2、デフォルト: 1 ストップビット)
- Parity - パリティビットの生成を定義します。いくつかの端末によって提供される通信プロトコルは、特定のパリティビット設定を必要とする可能性があります。Even、Odd、None の何れかを指定します。(デフォルト: None)
- Speed - 送信（端末）および受信（端末から）の端末回線のボーレートを設定します。シリアルポートに接続されているデバイスのボーレートと一致するように速度を設定します。(範囲: 9600、19200、38400、57600、または 115200 baud; デフォルト：115200 baud)

Note: コンソール接続のパスワードは、CLI を使用してのみ設定できます（CLI レファレンスガイドの“password”コマンドを参照してください）。

Note: パスワードチェックは、コンソール接続へのログインに対して有効または無効にすることができます（CLI レファレンスガイドの“login”コマンドを参照）。

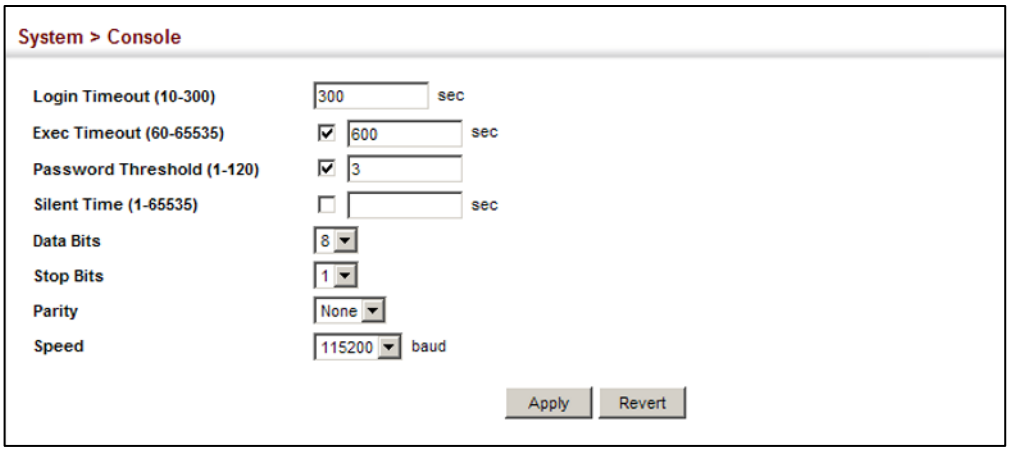
Web インタフェース

コンソールポートのパラメータを設定するには、次の手順を実行します。

1. [System]、[Console]の順にクリックします。

2. 必要に応じて接続パラメータを指定します。
3. [Apply]をクリックします。

図 3-20　コンソールポートの設定



3.8 Telnet の設定

[System]> [Telnet]メニューを使用して、Telnet 接続を介して CLI にアクセスするためのパラメータを設定します。Telnet（すなわち、仮想端末）を使用してネットワーク上でスイッチにアクセスすることができます。Telnet による管理アクセスは、TCP ポート番号、タイムアウト、およびパスワードを含む、有効/無効およびその他のパラメータを設定できます。パスワードは CLI によってのみ設定可能です。これらのパラメータは、Web インタフェースまたは CLI インタフェースを使用して設定できます。

パラメータ

次のパラメータが表示されます。

- Telnet Status - スイッチへの Telnet アクセスを有効または無効にします。(デフォルト: Enabled)
- TCP Port - スイッチ上の Telnet の TCP ポート番号を設定します。(範囲: 1 から 65535、デフォルト: 23)
- Max Sessions - このシステムに同時に接続できる Telnet セッションの最大数を設定します。(範囲: 0 から 8、デフォルト: 8)
  Telnet と Secure Shell に対して最大 2 つのセッションを同時に開くことができます(例; Telnet と SSH の両方が最大 2 セッションを共有します)。
- Login Timeout - システムがユーザに CLI へのログインを待つ間隔を設定します。タイムアウト間隔内にログイン試行が検出されない場合、セッションは終了します。(範囲: 10 から 300 秒、デフォルト: 300 秒)
- Exec Timeout - ユーザの入力が検出されるまで、システムが待機する間隔を設定します。タイムアウト時間内にユーザの入力が検出されない場合、セッションは終了されます。(範囲: 60 から 65535 秒、デフォルト: 600 秒)
- Password Threshold - 失敗したログオン試行回数を制限するパスワード侵入閾値を設定します。ログオン試行の閾値に達すると、次のログオン試行を許可する前に、システムインタフェースが指定された時間（Silent Time パラメータで設定された時間）管理コンソールにアクセスできません（サイレントになります）。(範囲: 1 から 120、デフォルト: 3 回の試行)
- Silent Time - 失敗したログオン試行の回数を超えた後で、管理インタフェースにアクセスできない時間を設定します。(範囲: 1 から 65535 秒、デフォルト: Disabled)

Note: Telnet 接続のパスワードは、CLI を使用してのみ設定できます（CLI レファレンスガイドの“password”コマンドを参照してください）。

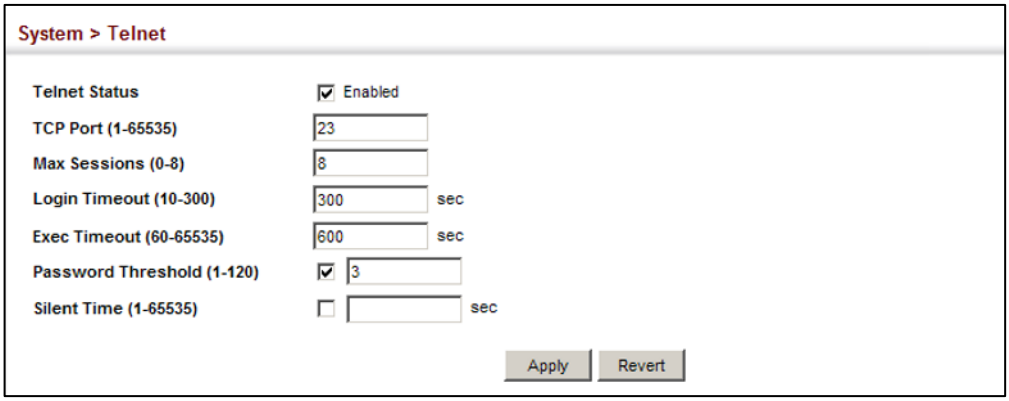
Note: パスワードチェックは、コンソール接続へのログインに対してイネーブルまたはディセーブルにすることができます（CLI レファレンスガイドの“login”コマンドを参照）。

Web インタフェース

コンソールポートのパラメータを設定するには、次の手順を実行します。

1. [System]、[Telnet]の順にクリックします。
2. 必要に応じて接続パラメータを指定します。
3. [Apply]をクリックします。

図 3-21　Telnet 接続の設定



3.9 CPU 使用率の表示

[System]> [CPU Utilization]ページを使用して、CPU 使用率に関する情報を表示します。

パラメータ

次のパラメータが表示されます。

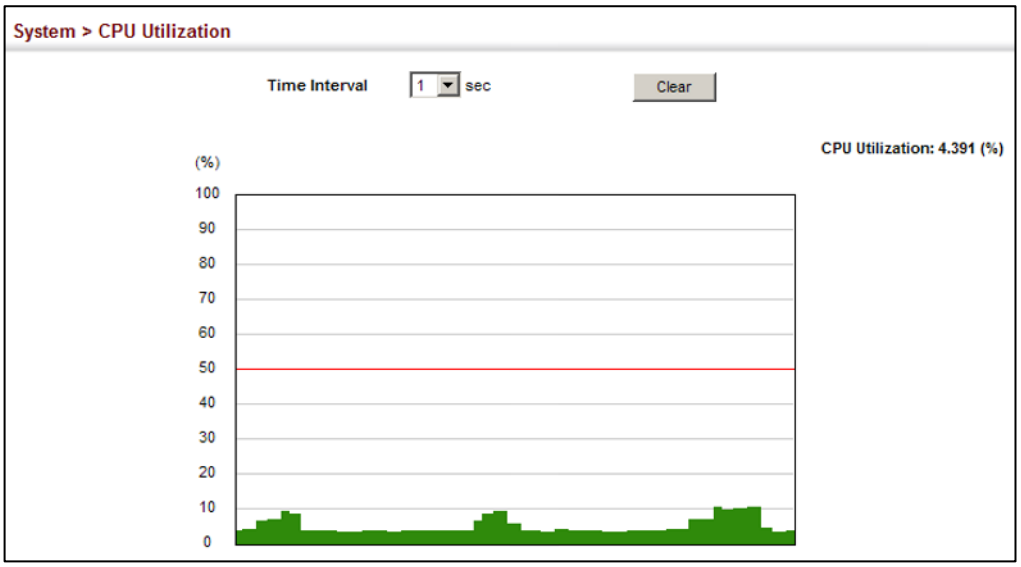
- Time Interval - 表示された稼働率を更新する間隔です。(オプション: 1 秒、5 秒、10 秒、30 秒、60 秒、デフォルト: 1 秒)
- CPU Utilization - 指定した間隔での CPU 使用率です。

Web インタフェース

CPU 使用率を表示するには :

1. [System]、[CPU Utilization]の順にクリックします。
2. 必要に応じて更新間隔を変更します。新しい設定が選択されるとすぐに間隔が変更されることに注意してください。

図 3-22　CPU 使用率の表示



3.10 CPU ガードの設定

[System]> [CPU Guard]ページを使用して、使用された CPU 時間のパーセンテージで CPU 使用率の上限と下限のウォーターマークを設定し、1 秒あたりに処理されるパケット数で CPU の上限と下限の閾値を設定します。

パラメータ

次のパラメータが表示されます。

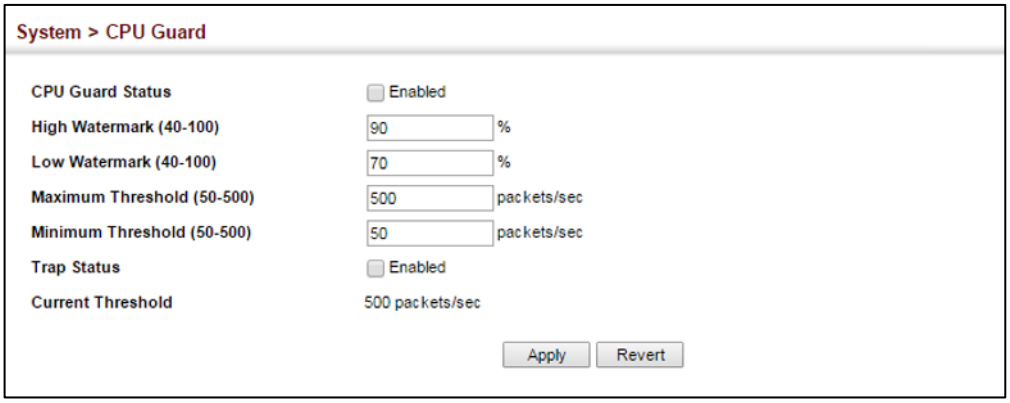
- CPU Guard Status - CPU ガードを有効にします。(デフォルト: Disabled)
- High Watermark - CPU 使用時間の割合が高ウォーターマークよりも高い場合、スイッチは使用時間が低水準を下回るまで（バッファ内のパケットに追いつくために）CPU にパケットフローを停止します。(範囲: 40 から 100 %、デフォルト: 90 %)
- Low Watermark - 最高水準点を超えた後にパケットフローが停止した場合、Osage が低水準水準点の下に落ちた後、正常なフローが復元されます。(範囲: 40 から 100 %、デフォルト: 70 %)
- Maximum Threshold - CPU によって処理されているパケット数が最大閾値を超えている場合、スイッチは処理中のパケット数が最小閾値を下回るまで、CPU へのパケットフローを停止します（バッファ内のパケットに追いつくことができます） 。(範囲: 50 から 300 pps、デフォルト: 300 pps)
- Minimum Threshold - パケットフローが最大閾値を超えて停止した場合、使用率が最小閾値を下回った後に通常フローが復元されます。(範囲: 50 から 300 pps、デフォルト: 50 pps)
- Trap Status - 有効にした場合の利用率が高ウォーターマークを超えるか、最大閾値を超えた場合、警告メッセージが生成されます。(デフォルト: Disabled)
  一度高水準値を超えて警告メッセージが生成されたあと、同一の警告メッセージを再度生成するには、アラームが停止する前に使用率は低水準値を下回る必要があります。そして、他のアラームの引き金となる前に高水準値を再度超えなければなりません。
  一度最大閾値を超えて警告メッセージが生成されたあと、同一の警告メッセージを再度生成するには、アラームが停止する前に使用率は最低閾値を下回る必要があります。そして、他のアラームの引き金となる前に最大閾値を再度超えなければなりません。
- Current Threshold - 設定された閾値をパケット/秒で表示します。

Web インタフェース

CPU Guard を設定するには：

1. [System]、[CPU Guard]をクリックします。
2. CPU ガードのステータスを設定し、ウォーターマークまたは閾値パラメータを設定し、必要に応じてトラップを有効にします。
3. [Apply]をクリックします。

図 3-23　CPU ガードの設定



3.11 メモリ使用率の表示

[System]> [Memory Status]ページを使用して、メモリ使用率パラメータを表示します。

パラメータ

次のパラメータが表示されます。

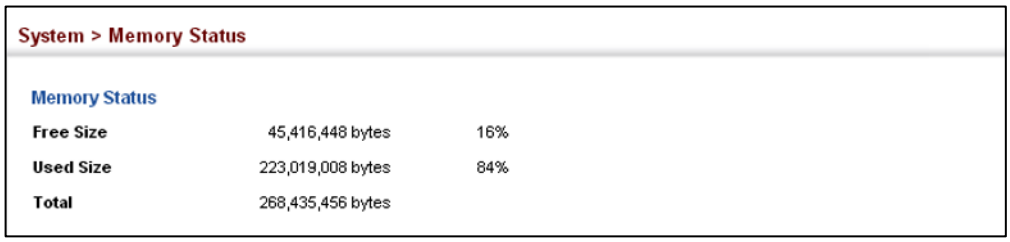
- Free Size - 現在使用可能なメモリの量です。
- Used Size - アクティブなプロセスに割当てられるメモリの量です。
- Total - システムメモリの合計量です。

Web インタフェース

メモリ使用率を表示するには：

1. [System]、[Memory Status]をクリックします。.

図 3-24　メモリ使用率の表示



3.12 システムのリセット

[System]> [Reset]メニューを使用して、スイッチを直ちに、指定した時間に、指定した遅延の後に、または定期的に再起動します。

コマンドの使用方法

- このコマンドは、システム全体をリセットします。
- システムを再起動すると、常にパワーオンセルフテストが実行されます。不揮発性メモリに格納されているすべての構成情報も保持されます。(「3.5.2　ローカルファイルへのランニングコンフィグレーションの保存」を参照してください。)

パラメータ

次のパラメータが表示されます。

システムリロード情報

- Reload Settings - 次の例に示すように、次にスケジュールされたリロードと選択したリロードモードに関する情報を表示します。
  “The switch will be rebooted at March 9 12:00:00 20XX. Remaining Time: 0 days, 2 hours, 46 minutes, 5 seconds.
  Reloading switch regularly time: 12:00 everyday.”
- Refresh - リロード情報を更新します。現在の設定を表示するには、コンソールまたはシステム時間による変更をリフレッシュする必要があります。
- Cancel - このフィールドに表示されている現在の設定を取り消します。

システムリロード構成

- Reset Mode - スイッチを直ちにまたは指定された時刻に再起動します。
  - Immediately - すぐにシステムを再起動します。
  - In - スイッチをリロードする間隔を指定します。(指定された時間は 24 日以内でなければなりません)
    - hours - スイッチがリセットされるまでの時間（分)。(範囲: 0 から 576)
    - minutes - スイッチがリセットされるまでの時間(分)。(範囲: 0 から 59)
  - At - スイッチをリロードする時刻を指定します。
    - DD - リロードする日です。(範囲: 01 から 31)
    - MM - リロードする月です。(範囲: 01 から 12)
    - YYYY - リロードする年です。(範囲: 1970 から 2037)
    - HH - リロードする時間です。(範囲: 00 から 23)
    - MM - リロードする分です。(範囲: 00 から 59)
  - Regularly - スイッチをリロードする定期的な間隔を指定します。
    Time
    - HH - リロードする時間です。(範囲: 00 から 23)
    - MM - リロードする分です。(範囲: 00 から 59)

    Period
    - Daily - 毎日です。

- Weekly - リロードする曜日です。
  (範囲: Sunday ...Saturday)
- Monthly - リロードする日です。(範囲: 1 から 31)

Web インタフェース

スイッチを再起動するには：

1. [System]、[Reset]の順にクリックします。
2. 必要なリセットモードを選択します。
3. 直ちにリセットする以外のオプションについては、必要なパラメータを入力してください。
4. [Apply]をクリックします。
5. プロンプトが表示されたら、スイッチをリセットすることを確認します。

図 3-25　スイッチの再起動 (Immediately)

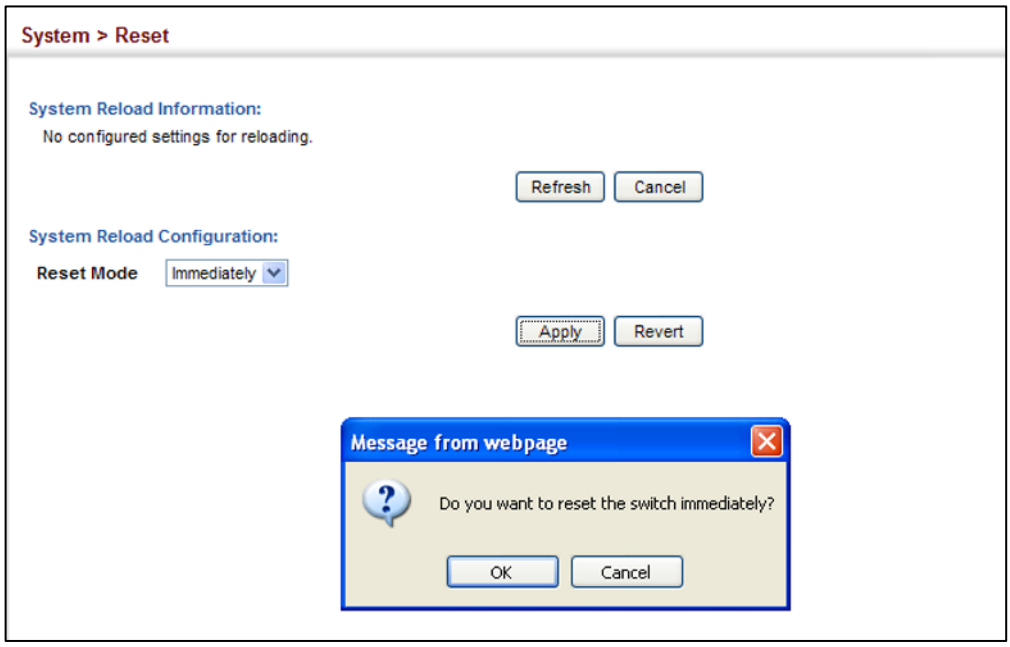


図 3-26　スイッチの再起動 (In)

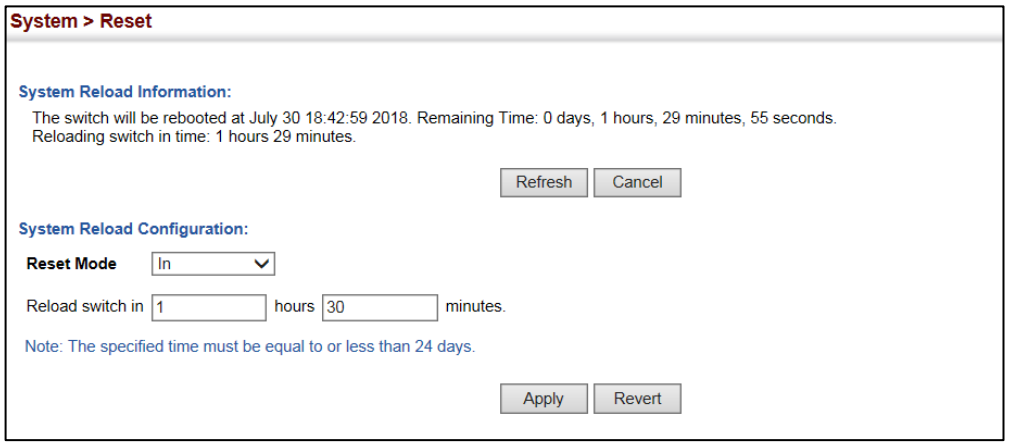


図 3-27　スイッチの再起動 (At)

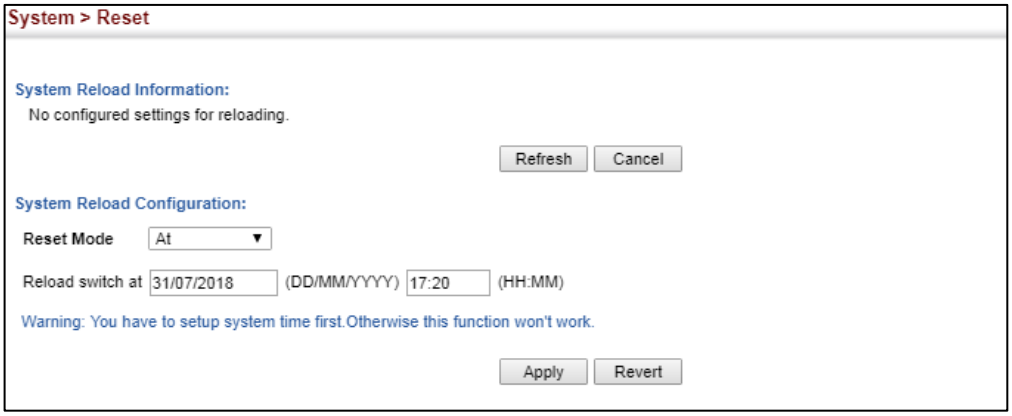
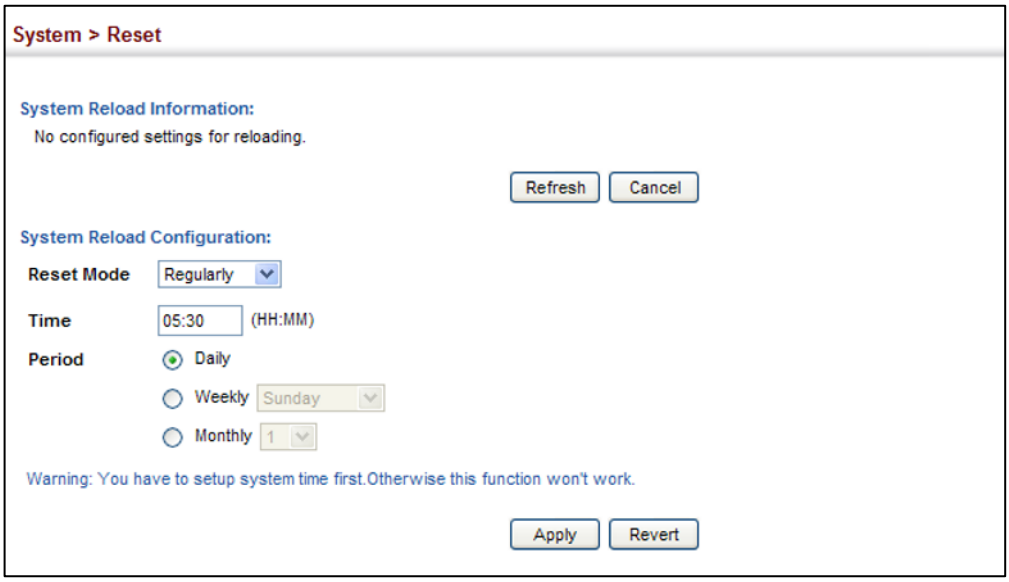


図 3-28　スイッチの再起動 (Regularly)



4 インタフェース設定

本章では、次のトピックについて説明します。

- Port Configuration - オートネゴシエーション、速度、duplex モード、およびフロー制御の手動設定などの接続を設定します。
- Displaying Statistics - インタフェース、Etherlike、および RMON のポート統計を表形式またはチャート形式で表示します。
- Displaying Statistical History - 指定したインタフェースの統計履歴を表示します。
- Displaying Transceiver Data - DDM をサポートする光トランシーバの識別情報と操作パラメータを表示します。
- Configuring Transceiver Thresholds - DDM をサポートする光トランシーバのアラームおよび警告メッセージの閾値を設定します。
- Cable Test - 指定されたポートでケーブル診断を実行します。
- Trunk Configuration - スタティックまたはダイナミックなトランクを設定します。
- Saving Power - 他のデバイスに接続するために使用されるケーブルの長さにもとづいてポートに供給される電力を調整します。
- Local Port Mirroring - ローカルスイッチ上のミラーリングのためのソースポートとターゲットポートを設定します。
- Remote Port Mirroring - ローカルスイッチ上の宛先ポートでの分析のために、リモートスイッチからのトラフィックのミラーリングを設定します。
- Flow Sampling - トラフィックフローの定期サンプリングを設定します。
- Traffic Segmentation - セグメント化されたポートグループへのアップリンクおよびダウンリンクを設定します。

4.1 ポート設定

本章では、ポート接続の設定、あるポートから別のポートへのトラフィックのミラーリング、およびケーブル診断の実行方法について説明します。

4.1.1 ポートリストによる設定

インタフェースの有効/無効、オートネゴシエーションおよびアドバタイズするインタフェース機能の設定、または速度、duplex モード、およびフロー制御の手動修正を行うには、[Interface]> [Port]> [General（Configure by Port List）]ページを使用します。

コマンドの使用方法

- Gigabit RJ-45 インタフェースで速度 / Duplex モードまたはフロー制御オプションを使用するように設定または強制するには、オートネゴシエーションを無効にする必要があります。
- オートネゴシエーションを使用する場合、アドバタイズされた機能にもとづいてリンクパートナー間で最適な設定がネゴシエートされます。オートネゴシエーションで速度、duplex モード、またはフロー制御を設定するには、インタフェースの機能リストで必要な動作モードを指定する必要があります。
- 速度/duplex モードは、ギガビットトランシーバの 1000full に固定されています。オートネゴシエーションが有効な場合、アドバタイズできる属性はスピードとフロー制御と対称ポーズフレームが含まれます。
- 1000BASE-T 規格は強制モードをサポートしていません。1000BASE-T ポートまたはトランクを介した接続を確立するには、オートネゴシエーションを常に使用する必要があります。使用しない場合、他のタイプのスイッチに接続する場合、リンクプロセスの成功を保証することはできません。

パラメータ

次のパラメータが表示されます。

- Port - ポート識別です。(範囲: 1 から 10)
- Type - ポートの種類を示します。(1000BASE-T, 1000BASE SFP)
- Name - インタフェースにラベルを付けることができます。(範囲: 1 から 32 文字)
- Admin - インタフェースを手動で無効にすることができます。異常な動作（過度の衝突など）が起きた場合にインタフェースを無効にしてから、問題が解決した後で再度有効にすることができます。セキュリティ上の理由から、インタフェースを無効にすることもできます。(デフォルト: Enabled)
- Media Type - SFP ポートのトランシーバモードを強制的に設定できます。次のモードがサポートされています。(デフォルト: 無し)
  - SFP-Forced 1000SFP - 常に 1000BASE SFP モードを使用します。
- Autonegotiation (Port Capabilities) -オートネゴシエーションを有効または無効にできます。オートネゴシエーションが有効になっている場合は、アドバタイズする機能を指定する必要があります。オートネゴシエーションが無効になっている場合は、速度、モード、およびフロー制御の設定を強制できます。次の機能がサポートされています。
  - 10h - 10 Mbps の半二重動作をサポートします。
  - 10f - 10 Mbps の全二重動作をサポートします。
  - 100h - 100 Mbps の半二重動作をサポートします。
  - 100f - 100 Mbps の全二重動作をサポートします。

- 1000f - 1000 Mbps の全二重動作をサポートします。
- Sym - 対照的に送受信ポーズフレームを交換します。
- FC - フロー制御は、バッファが満杯になったときにスイッチに直接接続されたエンドステーションまたはセグメントからのトラフィックを制御することによって、フレーム損失をなくすことができます。有効にすると、半二重動作にはバックプレッシャーが使用され、全二重動作には IEEE 802.3-2005（正式には IEEE 802.3x）が使用されます。
  デフォルト: オートネゴシエーションが有効になっています。
  以下をアドバタイズする機能があります。
  1000BASE-T - 10half, 10full, 100half, 100full, 1000full
  1000BASE-SX/LX/LH/BX (SFP) - 1000full

◆ Speed/Duplex - ポート速度と duplex モードを手動で設定できます。（オートネゴシエーションが無効の場合）

◆ Flow Control - フロー制御を自動または手動で選択できます。(デフォルト: Disabled)

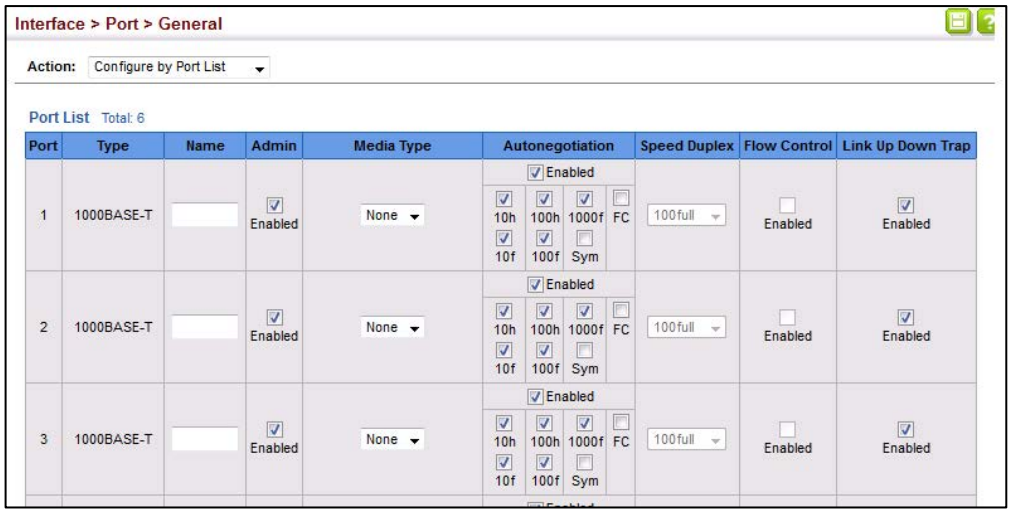
◆ Link Up Down Trap - ポートリンクが Up または Down したときに通知メッセージを発行します。(デフォルト: Enabled)

Web インタフェース

ポート接続パラメータを設定するには：

1. [Interface]、[Port]、[General]をクリックします。
2. [Action]リストから[Configure by Port List]を選択します。
3. 必要なインタフェース設定を変更します。
4. [Apply]をクリックします。

図 4-1　ポートリストによる接続の設定



4.1.2 ポート範囲による設定

インタフェースの有効/無効、オートネゴシエーションおよびアドバタイズするインタフェース機能の設定、または速度、duplex モード、およびフロー制御の手動修正を行うには、[Interface]> [Port]> [General（Configure by Port Range）]ページを使用します。

パラメータ

trap コマンド以外のコマンドの使用方法とパラメータの説明の詳細については、「4.1.1　ポートリストによ

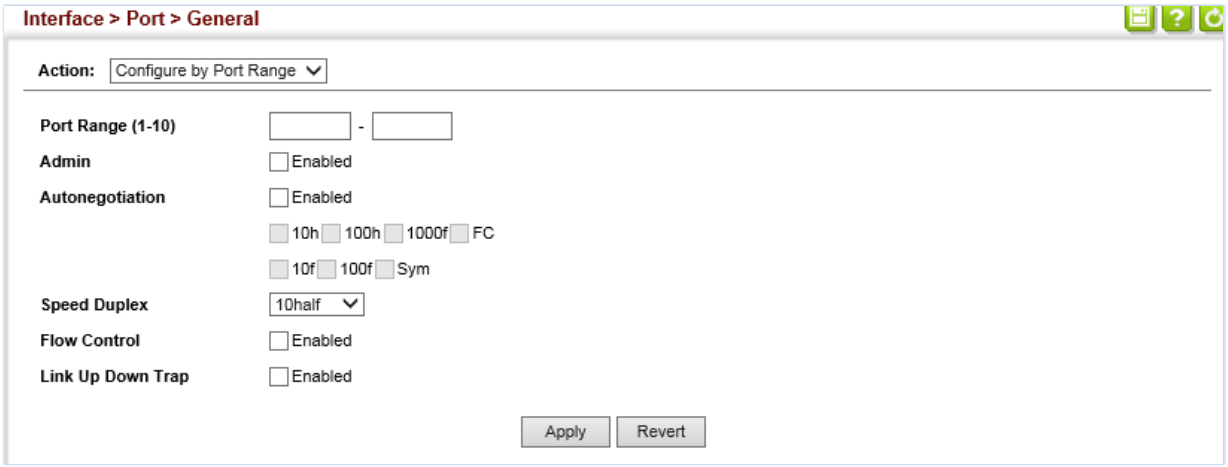
る設定」を参照してください。

Web インタフェース

ポート接続パラメータを設定するには：

1. [Interface]、[Port]、[General]をクリックします。
2. [Action]リストから[Configure by Port Range]を選択します。
3. 設定変更が適用されるポートの範囲を入力します。
4. 必要なインタフェース設定を変更します。
5. [Apply]をクリックします。

図 4-2　ポート範囲による接続設定



4.1.3 接続ステータスの表示

[Interface]> [Port]> [General（Show Information）]ページを使用して、リンクステート、速度/duplex モード、フロー制御、オートネゴシエーションなどの現在の接続ステータスを表示します。

パラメータ

次のパラメータが表示されます。

- Port - ポート番号です。
- Type - ポートの種類を示します。(1000BASE-T, 1000BASE SFP)
- Name - インタフェースラベルです。
- Admin - ポートが有効か無効かを示します。
- Oper Status - リンクが Up または Down のいずれであるかを示します。
- Shutdown Reason - 該当する場合、このインタフェースがシャットダウンされた理由を示します。インタフェースをシャットダウンする理由のいくつかには、管理上無効になっているか、または自動トラフィック制御によって設定されたトラフィック境界の制限を超えていることが含まれます。
- Media Type - SFP ポートのトランシーバモードを示します。
- Autonegotiation - オートネゴシエーションが有効か無効かを示します。
- Oper Speed Duplex - 現在の速度と duplex モードを表示します。
- Oper Flow Control - 使用されるフロー制御タイプを示します。
- Link Up Down Trap - ポートリンクが Up または Down したときに通知メッセージが送信されるかどう

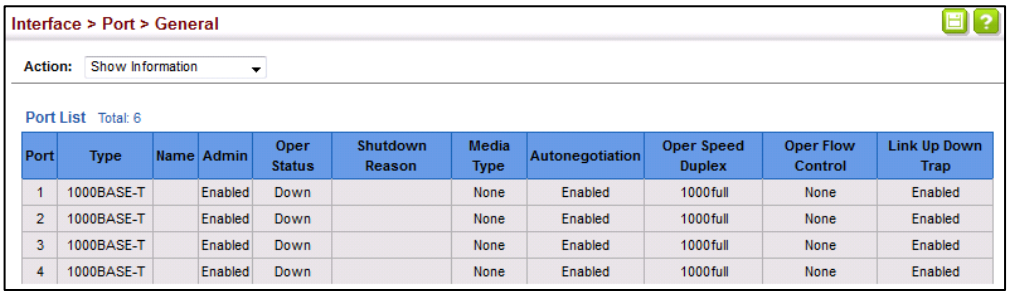
かを示します。(デフォルト: Enabled)

Web インタフェース

ポート接続パラメータを表示するには：

1. [Interface]、[Port]、[General]をクリックします。
2. [Action]リストから[Show Information]を選択します。

図 4-3 ポート情報の表示



4.1.4 ポートまたはトランク統計情報の表示

[Interface]> [Port] / [Trunk]> [Statistics]または[Chart]ページを使用して、インタフェースグループおよびEthernet MIB からのネットワークトラフィックに関する標準統計情報、および RMON MIB に基づくトラフィックの詳細なブレークダウンを表示します。インタフェースとイーサライク統計は、各ポートを通過するトラフィックのエラーを表示します。この情報を使用して、スイッチの潜在的な問題（ポートの障害または異常に重い負荷など）を特定できます。RMON 統計は、各ポートを通過するさまざまなフレームタイプとサイズの合計数を含む広範な統計情報へのアクセスを提供します。表示されるすべての値は、最後にシステムを再起動してから累積され、1 秒あたりのカウント数として表示されます。統計はデフォルトで 60 秒ごとに更新されます。

Note: RMON グループ 2,3、および 9 は、SNMP 管理ソフトウェアを使用してのみアクセスできます。

パラメータ

以下のパラメータが表示されます:

表 4-1 ポート統計

パラメータ	説明
Interface Statistics	
Received Octets	フレーミング文字を含むインタフェースで受信されたオクテットの総数です。
Transmitted Octets	フレーミング文字を含むインタフェースから送信されたオクテットの総数です。
Received Errors	上位層のプロトコルに配信できないようなエラーを含む受信パケットの数です。
Received Unicast Packets	上位層プロトコルに配信されるサブネットワークユニキャストパケットの数です。
Transmitted Unicast Packets	上位プロトコルが要求したパケットのうち、破棄されたパケットや送信されなかったものを含め、サブネットワークユニキャストアドレス

パラメータ	説明
	に送信されたパケットの総数です。
Transmitted Discarded Packets	エラーが検出されていなくても破棄された送信パケットの数です。パケットバッファが解放されるとパケット破棄が発生する可能性があります。
Received Multicast Packets	上位（サブ）レイヤに配信された、このサブレイヤのマルチキャストアドレス宛てのパケット数です。
Transmitted Multicast Packets	上位プロトコルが送信を要求した、このサブレイヤのマルチキャストアドレス宛のパケットの総数です（破棄されたパケットまたは送信されなかったパケットを含む）。
Received Broadcast Packets	上位（サブ）レイヤに配信された、このサブレイヤのブロードキャストアドレス宛てのパケット数です。
Transmitted Broadcast Packets	上位プロトコルが送信を要求した、このサブレイヤのブロードキャストアドレス宛のパケットの総数です（破棄されたパケットまたは送信されなかったパケットを含む）。
Etherlike Statistics	
Single Collision Frames	1 回のコリジョンによって送信が阻害された時に、正常に送信されたフレーム数です。
Multiple Collision Frames	2 回以上のコリジョンによって送信が阻害された時に、正常に送信されたフレーム数です。
Late Collisions	パケットの送信の 512 ビット時間後にコリジョンが検出された回数です。
Excessive Collisions	過度のコリジョンのために特定のインタフェースで送信が失敗したフレームの数です。このカウンタは、インタフェースが全二重モードで動作している場合は増加しません。
Deferred Transmissions	メディアがビジーとなった時に、特定のインタフェース上の最初の送信試行で遅延したフレーム数です。
Frames Too Long	特定のインタフェースで受信されたフレームの最大許容フレームサイズを超えるフレーム数です。
FCS Errors	長さがオクテットの整数であるが、FCS チェックに合格しない特定のインタフェースで受信されたフレームの数です。このカウントには、frame-too-long または frame-too-short エラーで受信したフレームは含まれません。
Internal MAC Transmit Errors	内部 MAC サブレイヤ送信エラーのために、特定のインタフェースでの送信が失敗したフレームの数です。
Pause Frames Input	ポートで受信したポーズフレームの数です。ポーズフレームは、処理できる以上のフレームを受信したときにフレームの送信者に対して送られます。
Pause Frames Output	ポートで送信したポーズフレームの数です。ポーズフレームは、処理できる以上のフレームを受信したときにフレームの送信者に対して送られます。
Symbol Errors	シンボルエラーの起きた回数です。シンボルエラーは接続しているケーブルから電気的に受信したビットをインタフェースのハードウェアがデコードできないという内容のエラーです。シンボルエラーが多発する場合はハードウェアに問題がある可能性があります。
RMON Statistics	
Drop Events	リソース不足のためにパケットがドロップされたイベントの総数。
Jabbers	長さが 1518 オクテットよりも長く（フレーミングビットは除くが FCS オクテットを含む）、FCS またはアラインメントエラーのいずれかを持つ受信フレームの総数です。

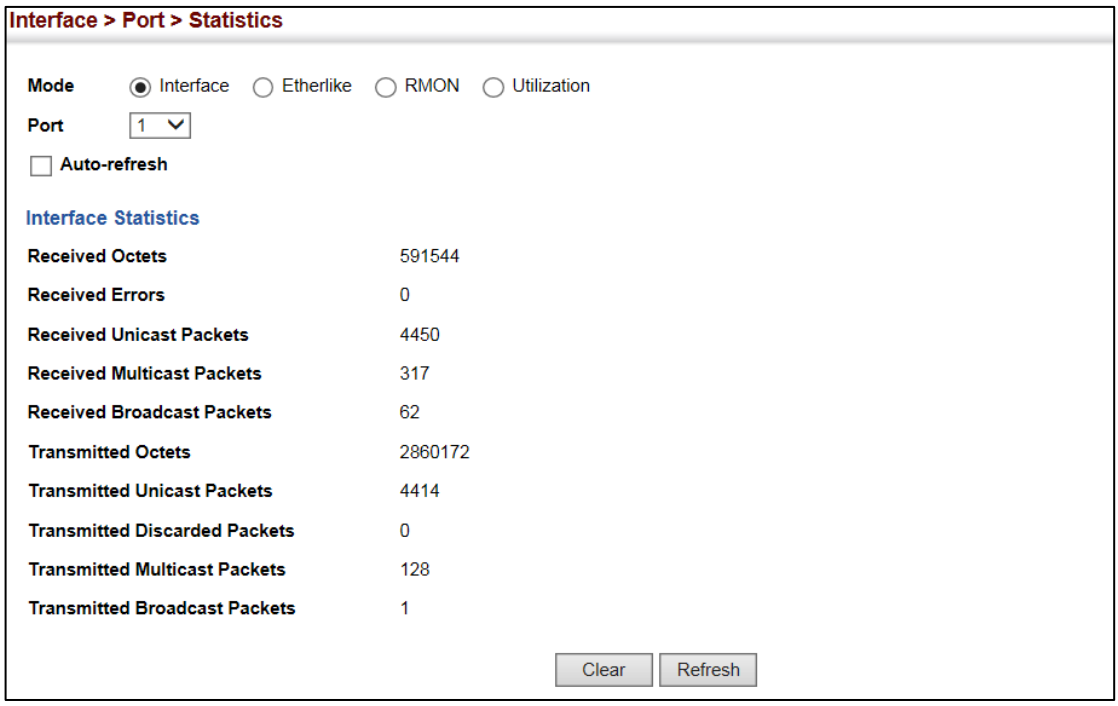
パラメータ	説明
Fragments	長さが 64 オクテット未満（フレーミングビットは除くが、FCS オクテットを含む）であり、FCS またはアライメントエラーのいずれかを持つ、受信フレームの総数です。
Collisions	このイーサネットセグメント上のコリジョン発生回数です。
Received Octets	ネットワーク上で受信したデータの総オクテット数です。この統計値は、イーサネット使用率の妥当な指標として使用できます。
Received Packets	受信したパケットの総数です（不良、ブロードキャスト、マルチキャスト）。
Broadcast Packets	ブロードキャストアドレスに送信された正常パケットの総数です。これにはマルチキャストパケットは含まれないことに注意してください。
Multicast Packets	このマルチキャストアドレスに送信された正常パケットの総数です。
Undersize Packets	フレームフォーマットは正常だが、64 オクテット未満の長さ（フレーミングビットは除くが、FCS オクテットを含む）の受信パケットの総数です。
Oversize Packets	フレームフォーマットは正常だが、1518 オクテットより長い（フレーミングビットは除くが、FCS オクテットを含む）受信パケットの総数です。
64Bytes Packets	長さが 64 オクテット（フレーミングビットを除くが、FCS オクテットを含む）だった送受信パケットの総数です（不良パケットを含む）。
65-127Byte Packets 128-255Byte Packets 256-511Byte Packets 512-1023Byte Packets 1024-1518Byte Packets	オクテット数が指定された範囲内にある（フレーミングビットを除くが、FCS オクテットを含む）送受信パケットの総数です（不良パケットを含む）。
CRC Align Errors	CRC エラーの起きた回数です。ハードウェアに問題がある可能性があります。
Utilization Statistics	
Input Octets in kbits per second	このインタフェースで 1 秒あたりに受信したオクテットの数（kbits / 秒）です。
Input Packets per second	このインタフェースで 1 秒あたりに受信したパケットの数です。
Input Utilization	このインタフェースの受信使用率です。
Output Octets in kbits per second	このインタフェースで 1 秒あたりに送信したオクテットの数（kbits / 秒）です。
Output Packets per second	このインタフェースで 1 秒あたりに送信したパケットの数です。
Output Utilization	このインタフェースの送信使用率です。

Web インタフェース

ポート統計のリストを表示するには:

1. [Interface]、[Port]、[Statistics]をクリックします。
2. 表示する統計モード（Interface、Etherlike、RMON、Utilization）を選択します。
3. ドロップダウンリストからポートを選択します。
4. [Refresh]をクリックして画面を更新し、[Clear]をクリックカウンタを 0 にリセットします。

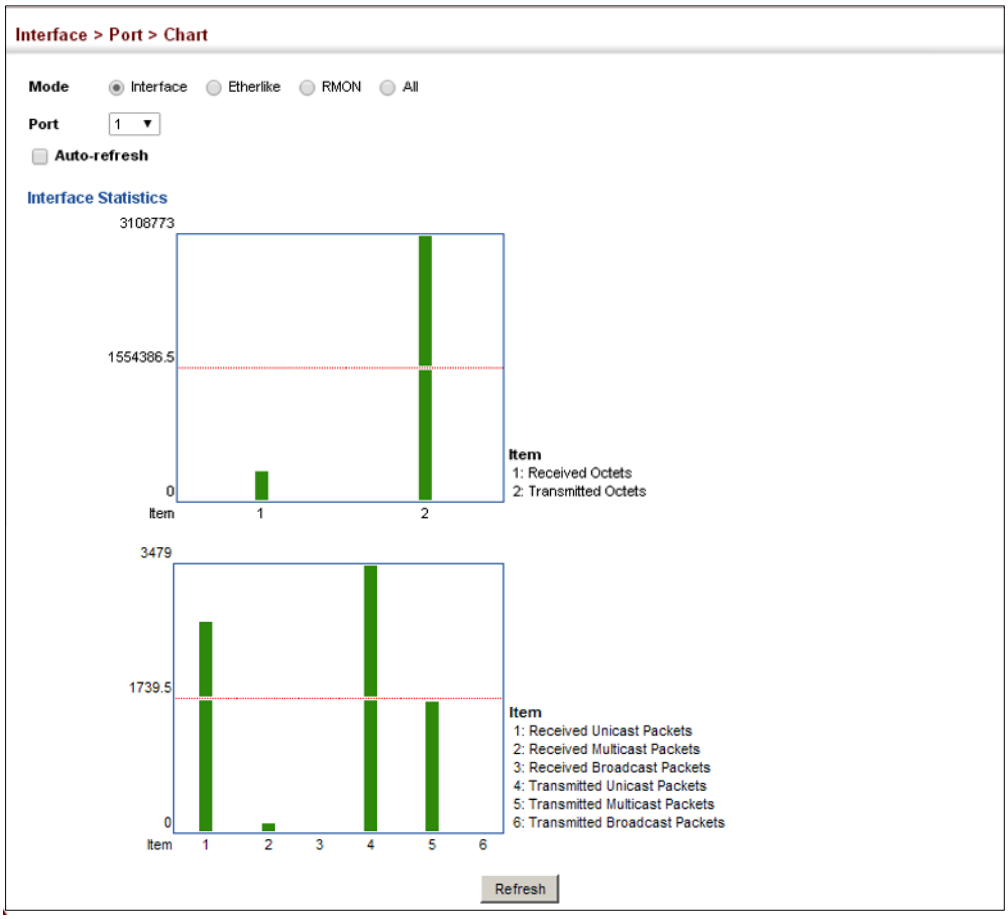
図 4-4　ポート統計情報の表示 (表)



ポート統計のチャートを表示するには：

1. [Interface]、[Port]、[Chart]をクリックします。
2. 表示する統計モード（Interface、Etherlike、RMON または All）を選択します。
3. [Interface]、[Etherlike]、[RMON]統計モードが選択されている場合は、ドロップダウンリストからポートを選択します。[All（ports）]統計モードが選択されている場合は、表示する統計タイプを選択します。

図 4-5　ポート統計情報の表示 (チャート)



4.1.5 統計履歴の表示

[Interface]> [Port]> [History]または[Interface]> [Trunk]> [History]ページを使用して、指定されたインタフェースの統計履歴を表示します。

コマンドの使用方法

- これらのページに表示される統計の説明については、「4.1.4　ポートまたはトランク統計情報の表示」を参照してください。
- 統計履歴のサンプリングは次の手順で設定します。

パラメータ

次のパラメータが表示されます。

Add

- Port - ポート番号です。(範囲: 1 から 10)
- History Name - サンプル間隔の名前です。(範囲: 1 から 32 文字)
- Interval - 統計をサンプリングする間隔です。(範囲: 1 から 86400 分)
- Requested Buckets - 取得するサンプルの数です。(範囲: 1 から 96)

Show

- Port - ポート番号です。(範囲: 1 から 10)
- History Name - サンプル間隔の名前です。(デフォルトの設定：15min, 1day)

- Interval - 統計をサンプリングする間隔です。
- Requested Buckets - 取得するサンプルの数です。

Show Details

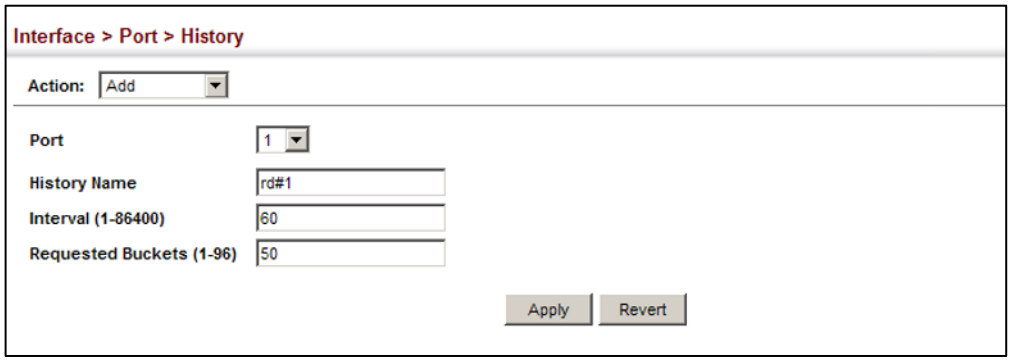
- モード
  - Status - サンプルパラメータを表示します。
  - Current Entry - 指定されたポートと名前付きサンプルの現在の統計情報を表示します。
  - Input Previous Entries - 受信トラフィックの統計履歴を表示します。
  - Output Previous Entries - 送信トラフィックの統計履歴を表示します。
- Port - ポート番号です。(範囲: 1 から 10)
- Name - サンプル間隔の名前です。

Web 設定

統計の定期的なサンプルを設定するには：

1. [Interface]、[Port]、[History]、または[Interface]、[Trunk]、[History]をクリックします。
2. [Action]メニューから[Add]を選択します。
3. [Port]または[Trunk]リストからインタフェースを選択します。
4. [History Name]、[Interval]、および[Requested Buckets]を入力します。
5. [Apply]をクリックします。

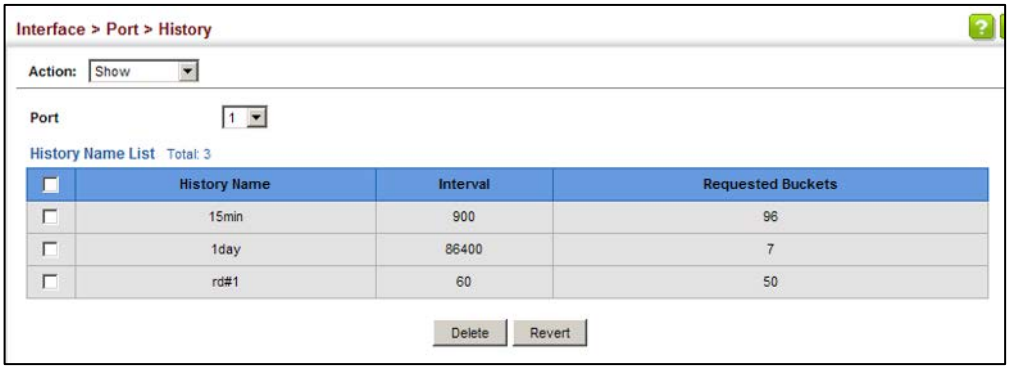
図 4-6　履歴サンプルの設定



履歴サンプルの設定済みのエントリを表示するには：

1. [Interface]、[Port]、[History]、または[Interface]、[Trunk]、[History]をクリックします。
2. [Action]メニューから[Show]を選択します。
3. [Port]または[Trunk]リストからインタフェースを選択します。

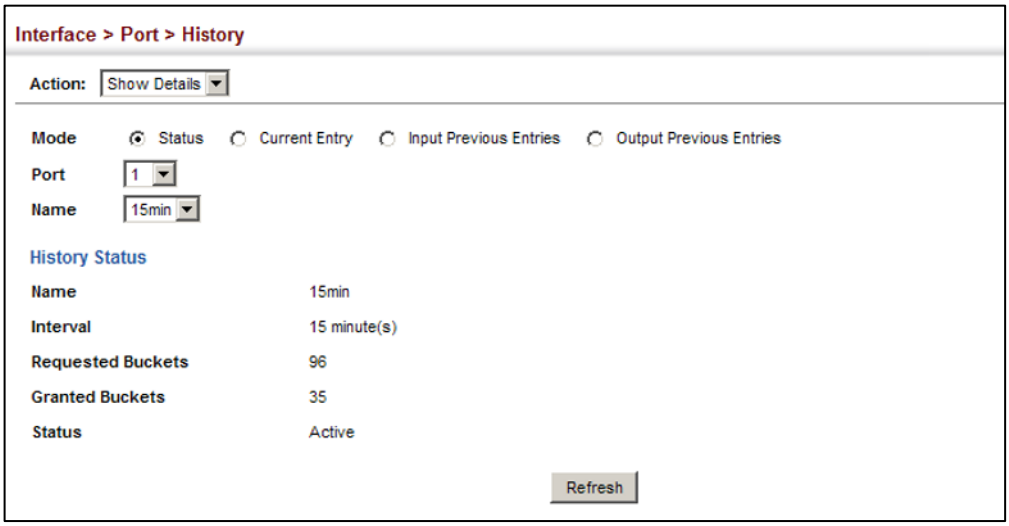
図 4-7　履歴サンプリングのエントリを表示



サンプリング項目の設定済みのパラメータを表示するには：

1. [Interface]、[Port]、[History]、または[Interface]、[Trunk]、[History]をクリックします。
2. [Action]メニューから[Show Details]を選択します。
3. [Mode]オプションから[Status]を選択します。
4. [Port]または[Trunk]リストからインタフェースを選択します。
5. [Name]リストからサンプリング項目を選択します。

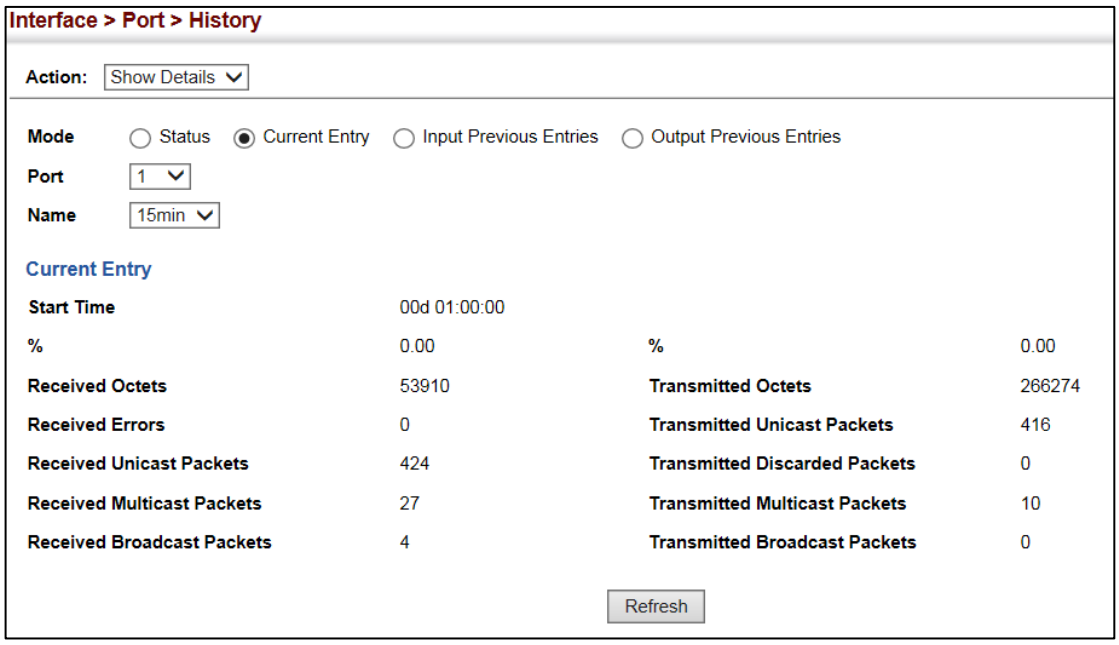
図 4-8　統計履歴サンプルのステータスの表示



サンプルエントリの現在の間隔に関する統計情報を表示するには：

1. [Interface]、[Port]、[History]、または[Interface]、[Trunk]、[History]をクリックします。
2. [Action]メニューから[Show Details]を選択します。
3. [Mode]オプションから[Current Entry]を選択します。
4. [Port]または[Trunk]リストからインタフェースを選択します。
5. [Name]リストからサンプリング項目を選択します。

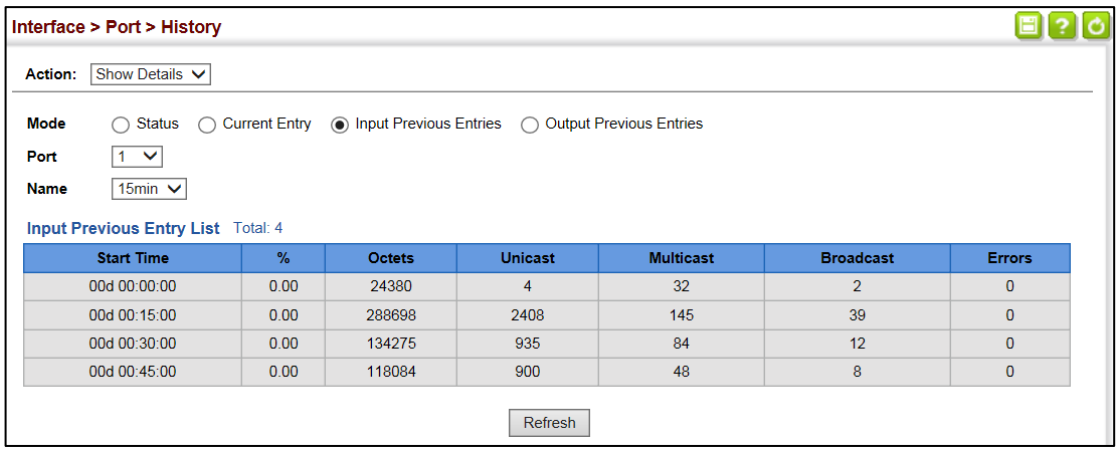
図 4-9　履歴サンプルの現在の統計情報を表示



サンプルエントリの受信トラフィックまたは送信トラフィックの統計情報を表示するには、次の手順を実行します。

1. [Interface]、[Port]、[History]、または[Interface]、[Trunk]、[History]をクリックします。
2. [Action]メニューから[Show Details]を選択します。
3. [Mode]のオプションから[Input Previous Entries]または[Output Previous Entries]を選択します。
4. [Port]または[Trunk]リストからインタフェースを選択します。
5. [Name]リストからサンプリング項目を選択します。

図 4-10　履歴サンプルの入力統計情報の表示



4.1.6 トランシーバデータの表示

[Interface]> [Port]> [Transceiver]ページを使用して、識別情報を表示し、デジタル診断モニタリング（DDM）をサポートする光トランシーバで動作可能にします。

パラメータ

次のパラメータが表示されます。

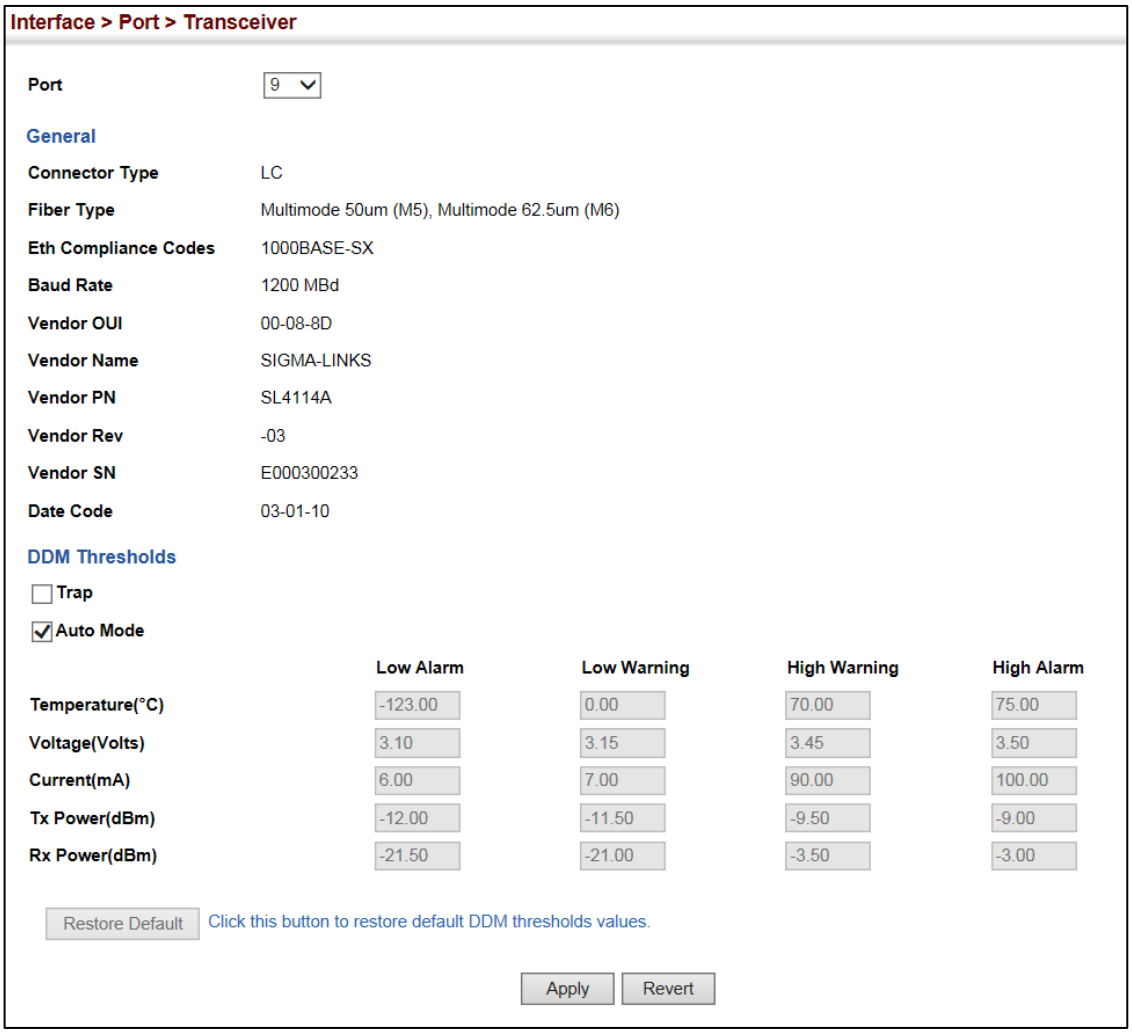
- Port - ポート番号です。(範囲: 9-10)
- General - コネクター・タイプおよびベンダ関連のパラメータに関する情報です。
- DDM Information - 温度、電源電圧、レーザバイアス電流、レーザパワー、および受光パワーに関する情報です。
  スイッチは、光トランシーバの診断モニタリングインタフェースの SFF-8472 仕様をサポートする SFP モジュールの診断情報を表示できます。この情報により、管理者は光デバイスの問題を遠隔から診断することができます。デジタル診断モニタリング（DDM）と呼ばれるこの機能は、トランシーバのパラメータに関する情報を提供します。

Web インタフェース

光トランシーバの識別情報と機能パラメータを表示するには：

1. [Interface]、[Port]、[Transceiver]をクリックします。
2. スクロールダウンリストからポートを選択します。

図 4-11　トランシーバデータの表示



4.1.7 トランシーバ閾値の設定

[Interface]> [Port]> [Transceiver]ページを使用して、デジタル診断モニタリング（DDM）をサポートする光トランシーバのアラームおよび警告メッセージの閾値を設定します。また、このページにはサポートされているトランシーバタイプの識別情報、および DDM をサポートするトランシーバの動作パラメータも表

示されます。

パラメータ

次のパラメータが表示されます。

- Port - ポート番号です。(範囲: 9-10)
- General - コネクター・タイプおよびベンダ関連のパラメータに関する情報です。
- DDM Information - 温度、電源電圧、レーザバイアス電流、レーザパワー、および受光パワーに関する情報です。
  スイッチは、光トランシーバの診断モニタリングインタフェースの SFF-8472 仕様をサポートする SFP モジュールの診断情報を表示できます。この情報により、管理者は光デバイスの問題を遠隔から診断することができます。デジタル診断モニタリング（DDM）と呼ばれるこの機能は、トランシーバのパラメータに関する情報を提供します。
- Trap - トランシーバの動作値のいずれかが指定された閾値を超えた場合にトラップを送信します。(デフォルト: Disabled)
- Auto Mode - トランシーバから得られたデフォルトの閾値設定を使用して、アラームまたはトラップメッセージの送信時期を決定します。(デフォルト: Enabled)
- DDM Thresholds - アラームおよび警告の閾値に関する情報です。測定されたパラメータが指定された閾値を超えた場合に、トラップを送信するようにスイッチを設定できます。
  次のアラームおよび警告パラメータがサポートされています。
  - High Alarm - 高閾値を超えたときにアラームメッセージを送信します。
  - High Warning - 高閾値を超えたときに警告メッセージを送信します。
  - Low Warning - 低閾値を超えたときに警告メッセージを送信します。
  - Low Alarm - 低閾値を超えたときにアラームメッセージを送信します。

  設定可能な範囲は次のとおりです。
  - Temperature: -128.00 から 128.00 ℃
  - Voltage: 0.00 から 6.55V
  - Current: 0.00 から 131.00 mA
  - Power: -40.00 から 8.20 dBm
    Rx および Tx パワーの閾値は、1 ミリワット（mW）を基準としたパワーのデシベル（dB）で計算されます。

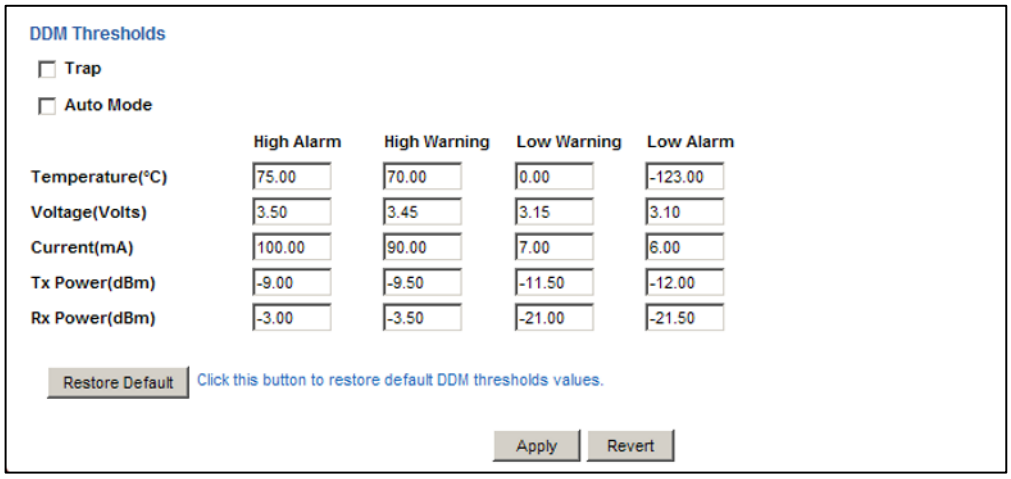
  アラームメッセージと警告メッセージの閾値は、以下のように設定できます。
  - 現在の値が高閾値以上で、前回のサンプル値が高閾値よりも小さい場合に、高閾値のアラームまたは警告メッセージが送信されます。高閾値イベントが生成された後は、値が高閾値を下回り、低閾値に達するまで、別のイベントは生成されません。
  - 現在の値が低閾値以下で、前回のサンプル値が低閾値よりも大きい場合は、低閾値のアラームまたは警告メッセージが送信されます。低閾値イベントが生成された後は、値が低閾値を上回り、高閾値に達するまで、別のイベントは生成されません。
  - 電力レベルが閾値のちょうど上下で変動することで連続的にイベントメッセージを送信してしまうヒステリシス効果を回避するために、上記のように動作します。
  - このコマンドで設定されたトラップメッセージは、[Administration]> [SNMP（トラップの設定）] ページを使用して SNMP トラップマネージャとして設定された管理ステーションに送信されます。

Web インタフェース

光トランシーバの閾値を設定するには：

1. [Interface]、[Port]、[Transceiver]をクリックします。
2. スクロールダウンリストからポートを選択します。
3. デフォルトまたは手動の設定にもとづいてトラップを送信するようにスイッチを設定します。
4. 手動構成が使用されている場合は、アラームおよび警告の閾値を設定します。
5. [Apply]をクリックします。

図 4-12　トランシーバの閾値の設定



4.1.8 ケーブル診断の実行

[Interface]> [Port]> [Cable Test]ページを使用して、ポートに接続されたケーブルをテストします。ケーブルテストは、ケーブルの不具合（ショート、オープンなど）をチェックします。障害が発見された場合、スイッチは障害までの長さを報告します。それ以外の場合は、ケーブル長を報告します。これは、ケーブル、コネクタ、および終端の品質を判断するために使用できます。オープン、ショート、ケーブルインピーダンスのミスマッチなどの問題は、このテストで診断できます。

コマンドの使用方法

- ケーブル診断は、ポートリンクアップ速度が 1 Gbps の場合、Digital Signal Processing（DSP）テスト方式を使用して実行されます。DSP はケーブルにパルス信号を送信し、そのパルスの反射を調べることによってケーブルを分析します。ポートのリンクアップ速度が 1 Gbps でない場合、Time Domain Reflectometry（TDR）を使用して実行されます。TDR は、ケーブルを介して信号を送信し、反射された信号を読み取ることによって、ケーブルの障害を検出します。TDR は、リンクが有効かどうかを判断します。
- ケーブル診断は、ツイストペアメディアでのみ実行できます。
- このケーブルテストは、長さ 7 から 100 メートルのギガビットイーサネットケーブルでのみ正確です。
- テストには約 5 秒かかります。テスト実行後 5 秒経過したら、refresh を押下すると、テストの結果が表示されます。テスト結果には、一般的なケーブルの障害、障害の状態、障害までのおよその距離が含まれます。
- 診断によって列挙される可能性のある状態には、以下のものが含まれます。TDR テストでは、[Test failed]または[OK]のみが表示されます。

- Test failed: 障害を検出したペアです。
- OK: 正しく終了したペアです。
- Open: オープンペア、リンク先がありません。
- Short: ショートペアです。
- Impedance mismatch: 終端インピーダンスが基準範囲内にありません。
- No cable: ケーブルの接続が確認できません。
- Not tested: 実行していません。
- Not Supported: このメッセージは、1000 Mbps 未満の速度でリンクされたギガビットイーサネットポート、または 10G イーサネットポートに対して表示されます。
- Unknown - 不明なエラーです。

パラメータ

次のパラメータが表示されます。

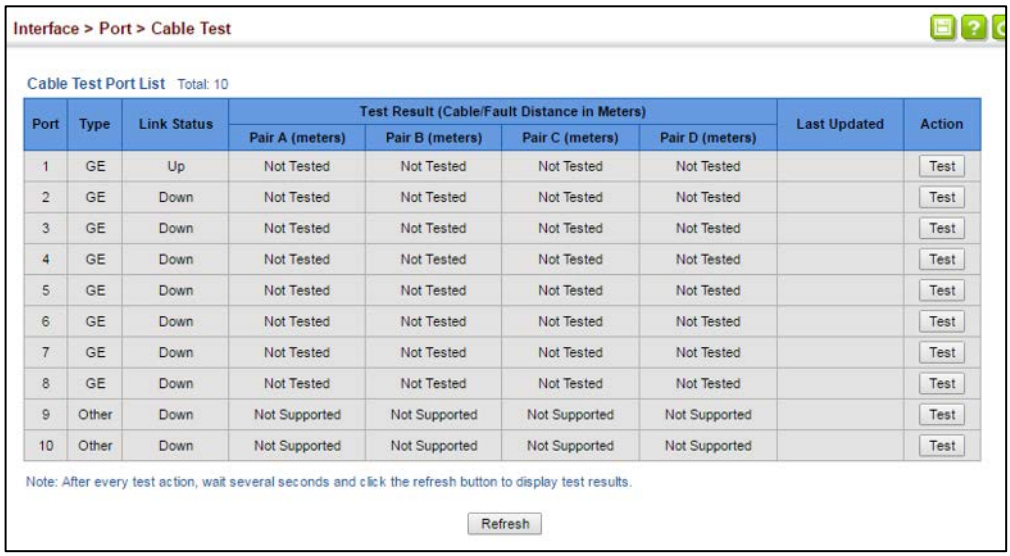
- Port - ポート番号です。
- Type - メディアタイプを表示します。(GE - Gigabit Ethernet, Other - SFP)
- Link Status - ポートリンクがアップまたはダウンしているかどうかを示します。
- Test Result - 結果には、一般的なケーブルの障害、障害の状態と近似距離、または障害がない場合のおおよそのケーブル長が含まれます。
  リンクダウンポートの場合、報告された障害までの距離は±2 メートル以内で正確です。リンクアップポートの場合、精度は±10 メートルです。
- Last Updated - このポートが最後にテストされた時刻を示します。
- Test - ケーブル診断を開始します。

Web インタフェース

ポートに接続されたケーブルを診断するには：

1. [Interface]、[Port]、[Cable Test]をクリックします。
2. 任意のポートの診断をクリックして、ケーブル診断を開始します。

図 4-13　ケーブル診断の実行



4.2 トランク構成

本章では、静的および動的トランクを設定する方法について説明します。

1 つの仮想集約リンクとして機能するデバイス間に複数のリンクを作成できます。ポートトランクは劇的なボトルネックが存在するネットワークセグメントの帯域幅の増加だけでなく、2 つのデバイス間のフォールトトレラントなリンクを提供しています。スイッチ上で一度に最大 8 のトランクを作成できます。

スイッチは、静的トランキングと動的リンク集約制御プロトコル（LACP）の両方をサポートします。リンクの両端で静的トランクを手動で設定する必要があります。一方、LACP 設定ポートは、別のデバイス上の LACP 設定ポートとのトランクリンクを自動的にネゴシエートできます。静的トランクの一部として設定されていない限り、スイッチ上の任意の数のポートを LACP として設定できます。別のデバイス上のポートも LACP として設定されている場合、スイッチと他のデバイスは、それらの間のトランクリンクをネゴシエートします。

コマンドの使用方法

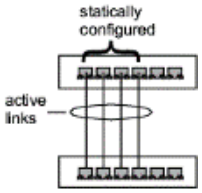
トランク内の各ポートで負荷を分散するほか、トランク内のポートに障害が発生した場合に負荷を引き継ぐことによって、他のポートは冗長性を提供します。ただし、デバイス間の物理的な接続を行う前に、Web インタフェースまたは CLI を使用して、両端のデバイス上のトランクを指定してください。トランクを使用する場合は、次の点に注意してください。

- ループを作成しないように、スイッチ間で対応するネットワークケーブルを接続する前にトランクの設定を完了してください。
- 1 つのスイッチに最大 8 つのトランクを作成でき、1 つのトランクに最大 8 つのポートを作成できます。
- 接続の両端のポートは、トランクポートとして設定する必要があります。
- トランクの両端のポートは、通信モード（速度、デュプレックスモードとフロー制御）、VLAN 割当て、CoS 設定など、同じ方法で設定する必要があります。
- フロントパネルのギガビットポートは、異なるメディアタイプのポートを含めて、一緒にトランクすることができます。
- STP、VLAN、および IGMP の設定は、トランク全体に対してのみ行うことができます。
- 動的トランクの設定を変更する場合、トランク内ポートを shutdown する、またはケーブルを開放してリンクダウンした状態で行ってください。
- 動的トランクにポートを集約する場合、トランクと集約するポートには必ず同じ Admin-Key を設定してください。
- 動的トランクからポートを削除する場合、lacp を無効にしてからポートの Admin-Key を削除してください。

4.2.1 静的トランクの設定

[Interface]> [Trunk]> [Static]ページを使用して、トランクを作成し、メンバーポートを割当て、接続パラメータを設定します。

図 4-14　静的トランクの設定



コマンドの使用方法

- 静的トランクを設定する場合、ベンダの実装に応じて、異なるタイプのスイッチをリンクできない場合があります。
- ネットワークにループが発生しないようにするには、ポートを接続する前に設定インタフェースで静的トランクを追加し、設定インタフェースで静的トランクを削除する前にポートを切断してください。

パラメータ

次のパラメータが表示されます。

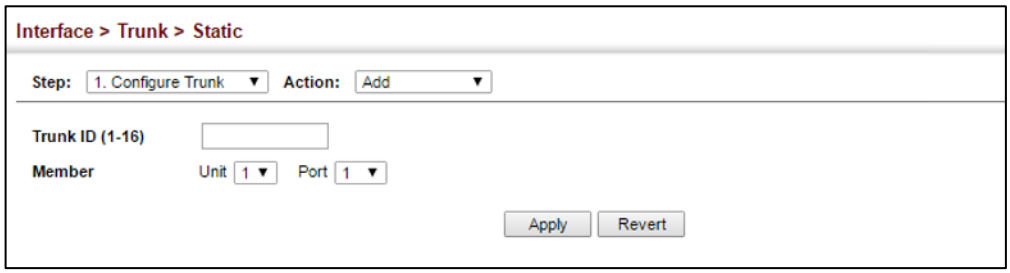
- Trunk ID - トランク識別子です。(範囲: 1-8)
- Member - 最初のトランクメンバーです。[Add Member]ページを使用して、追加のメンバーを構成します。
  - Unit - ユニット識別子です。(範囲: 1)
  - Port - ポート番号です。(範囲: 1 から 10)

Web インタフェース

静的トランクを作成するには：

1. [Interface]、[Trunk]、[Static]をクリックします。
2. [Step]リストから[Configure Trunk]を選択します。
3. [Action]リストから[Add]を選択します。
4. トランク識別子を入力します。
5. 最初のトランクメンバーのユニットとポートを設定します。
6. [Apply]をクリックします。

図 4-15　静的トランクの設定

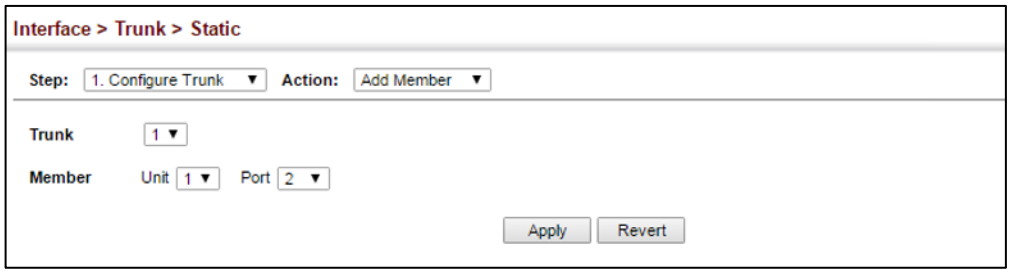


静的トランクにメンバーポートを追加するには：

1. [Interface]、[Trunk]、[Static]をクリックします。
2. [Step]リストから[Configure Trunk]を選択します。

3. [Action]リストから[Add Member]を選択します。
4. トランク識別子を選択します。
5. 追加のトランクメンバーのために装置とポートを設定します。
6. [Apply]をクリックします。

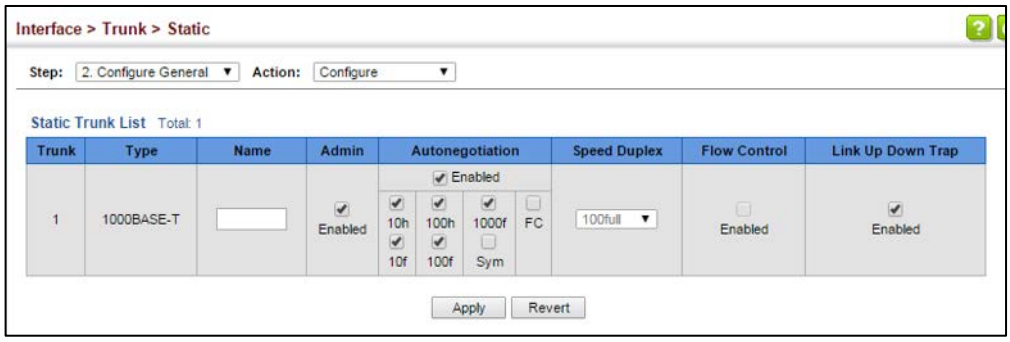
図 4-16　静的トランクメンバーの追加



静的トランクの接続パラメータを設定するには：

1. [Interface]、[Trunk]、[Static]をクリックします。
2. [Step]リストから[Configure General]を選択します。
3. [Action]リストから[Configure]を選択します。
4. 必要なインタフェース設定を変更します。（パラメータの説明については、「4.1.1　ポートリストによる設定」を参照してください。）
5. [Apply]をクリックします。

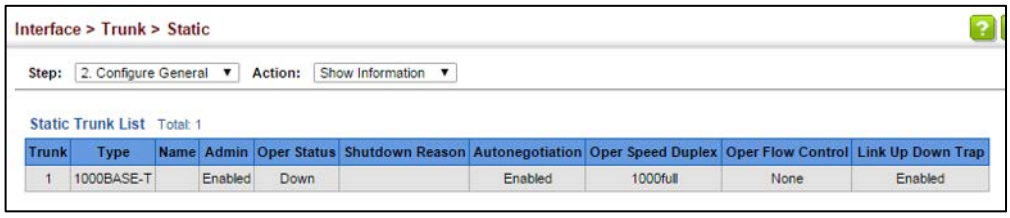
図 4-17　静的トランクの接続パラメータの設定



トランク接続パラメータを表示するには、

1. [Interface]、[Trunk]、[Static]をクリックします。
2. [Step]リストから[Configure General]を選択します。
3. [Action]リストから情報を表示を選択します。

図 4-18　静的トランクの情報の表示



4.2.2 動的トランクの設定

[Interface]> [Trunk]> [Dynamic]ページを使用して、集約グループの管理キーを設定し、ポート上で LACP を有効にし、ローカルポートおよびパートナーポートのプロトコルパラメータを設定するか、イーサネット接続パラメータを設定します。

コマンドの使用方法

- ネットワークにループが発生しないようにするには、ポートを接続する前に LACP を有効にし、LACP を無効にする前にポートを切断してください。
- ターゲットスイッチが接続ポートで LACP も有効にしている場合、トランクは自動的にアクティブになります。
- LACP を使用して別のスイッチで形成されたトランクには、次に使用可能なトランク ID が自動的に割当てられます。
- LACP トランクの両端のすべてのポートは、全二重および自動ネゴシエーション用に設定する必要があります。
- ポートは、(1) LACP ポートシステムの優先順位が一致する場合、(2) LACP ポートの管理キーが一致する場合、(3) LAG 管理キーが一致する場合（LACP キーが一致する場合)、同じ Link Aggregation Group（LAG）にのみ参加できます。ただし、LAG 管理キーが設定されている場合は、ポート管理キーを同じ値に設定して、ポートがそのグループに参加できるようにする必要があります。

パラメータ

次のパラメータが表示されます。

Configure Aggregator

- Admin Key - LACP 管理キーは、スイッチのローカル LACP 設定中に特定のリンクアグリゲーショングループ（LAG）を識別するために使用されます。(範囲: 0 から 65535)
  ポートグループの管理キーが設定されていない場合、このキーはポート管理キーと同じ値に設定されます（集約ポートの設定 - Actor/Partner） グループに参加したインタフェースで使用されます。LAG が使用されなくなると、ポートチャネルの管理キーは 0 にリセットされます。
  ポートチャネル管理キーがデフォルト以外の値に設定されている場合、操作キーはパートナーから受信した LACP PDU にもとづいており、チャネル管理キーはデフォルト値にリセットされます。トランク識別子もこのプロセスによって変更されます。
- Timeout Mode - 次の LACP データユニット（LACPDU）の受信タイムアウト時間：
  - Long Timeout - 90 秒のタイムアウト時間を指定します。（これがデフォルトの設定です。）
  - Short Timeout - 3 秒のタイムアウト時間を指定します。

  タイムアウト時間は、送信される LACPDU の Actor State フィールドの LACP タイムアウトビットに設定されます。パートナースイッチは、アクタースイッチから Short Timeout が設定された LACPDU を受信すると、LACPDU の送信間隔を 1 秒に調整します。アクタースイッチから Long Timeout が設定された LACPDU を受信すると、LACPDU の送信間隔が 30 秒に調整されます。
  設定されたタイムアウト時間が経過する前にパートナースイッチから LACPDU を受信しない場合、アクタースイッチは当該ポートを LACP グループから削除します。
  動的ポートチャネルのメンバポートがポートチャネルを離れると、デフォルトのタイムアウト時間がそのポートに復元されます。
- System Priority - リンク集約グループ（LAG）メンバシップを決定し、LAG ネゴシエーション中にこのデバイスを他のスイッチに識別するために、LACP システムプライオリティが使用されます。

- System MAC Address - 各トランクに割当てられたデバイスの MAC アドレスです。

集約ポートの設定 - 一般

- Port - ポート番号です。(範囲: 1 から 10)
- LACP Status - ポート上で LACP を有効または無効にします。

集約ポートの設定 - Actor/Partner

- Port - ポート番号です。(範囲: 1 から 10)
- Admin Key - LACP 管理キーは、同じ LAG に属するポートに対して同じ値に設定する必要があります。(範囲: 0 から 65535; デフォルト - Actor: 1, Partner: 0)
  リンクのリモート側が確立されると、その側で LACP 運用設定がすでに使用されています。パートナーの LACP を設定するのは、運用状態ではなく管理状態のみに適用されます。

Note: パートナー管理キーを設定しても、リモートまたはローカルのスイッチ操作には影響しません。ローカルスイッチは、ユーザ参照用のパートナー管理キーを記録するだけです。

  デフォルトでは、actor の操作キーはポートのリンク速度（1000f - 4、100f - 3、10f - 2）によって決定され、管理キーにコピーされます。

- System Priority - リンク集約グループ（LAG）メンバシップを決定し、LAG ネゴシエーション中にこのデバイスを他のスイッチに識別するために、LACP システムプライオリティが使用されます。(範囲: 0 から 65535、デフォルト: 32768)
  システムプライオリティはスイッチの MAC アドレスと組み合わされて LAG 識別子を形成します。この識別子は、他のシステムとの LACP ネゴシエーション中に特定の LAG を示すために使用されます。

Note: ポートの LACP を設定するのは、運用状態ではなく管理状態にのみ適用され、次にそのポートで集約リンクが確立されたときにのみ有効です。

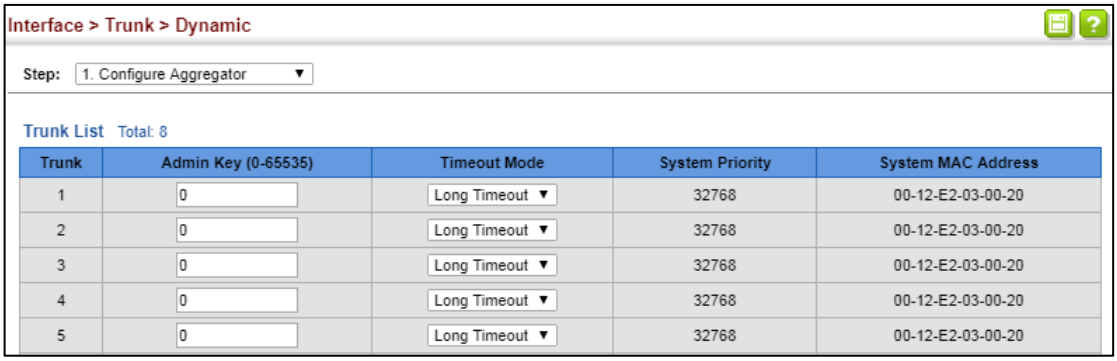
Note: ポートパートナーを設定すると、集約リンクのリモート側が設定されます。 すなわち、接続されたデバイス上のポートです。コマンド属性は、ポートアクターに使用されたものと同じ意味を持ちます。

Web インタフェース

動的トランクの管理キーを設定するには、次の手順を実行します。

1. [Interface]、[Trunk]、[Dynamic]をクリックします。
2. [Step]リストから[Configure Aggregator]を選択します。
3. 必要な LACP グループの管理キーとタイムアウトモードを設定します。
4. [Apply]をクリックします。

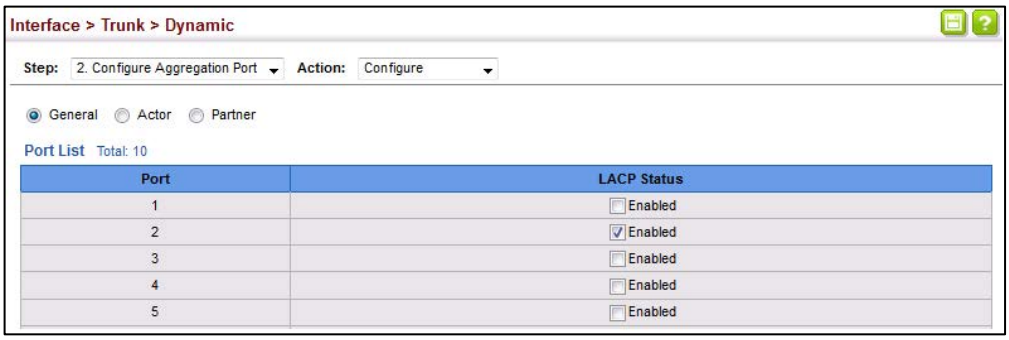
図 4-19　LACP アグリゲータ管理キーの設定



ポートに LACP を有効にするには：

1. [Interface]、[Trunk]、[Dynamic]をクリックします。
2. [Step]リストから[Configure Aggregation Port]を選択します。
3. [Action]リストから[Configure]を選択します。
4. [General]をクリックします。
5. 必要なポートで LACP を有効にします。
6. [Apply]をクリックします。

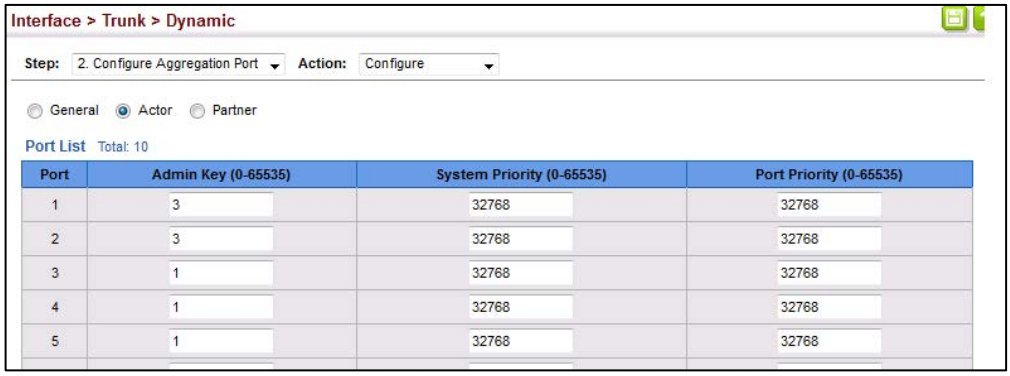
図 4-20　ポートでの LACP の有効化



グループメンバーの LACP パラメータを設定するには：

1. [Interface]、[Trunk]、[Dynamic]をクリックします。
2. [Step]リストから[Configure Aggregation Port]を選択します。
3. [Action]リストから[Configure]を選択します。
4. [Actor]または[Partner]をクリックします。
5. 必要な設定を行います。
6. [Apply]をクリックします。

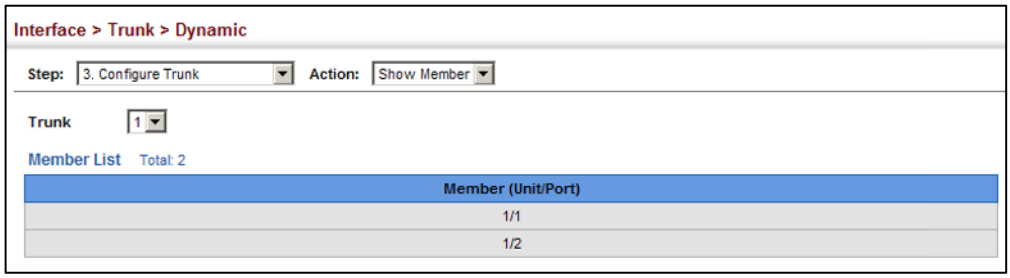
図 4-21　ポートでの LACP パラメータの設定



動的トランクのアクティブなメンバーを表示するには：

1. [Interface]、[Trunk]、[Dynamic]をクリックします。
2. [Step]リストから[Configure Trunk]を選択します。
3. [Action]リストから[Show Member]を選択します。
4. トランクを選択します。

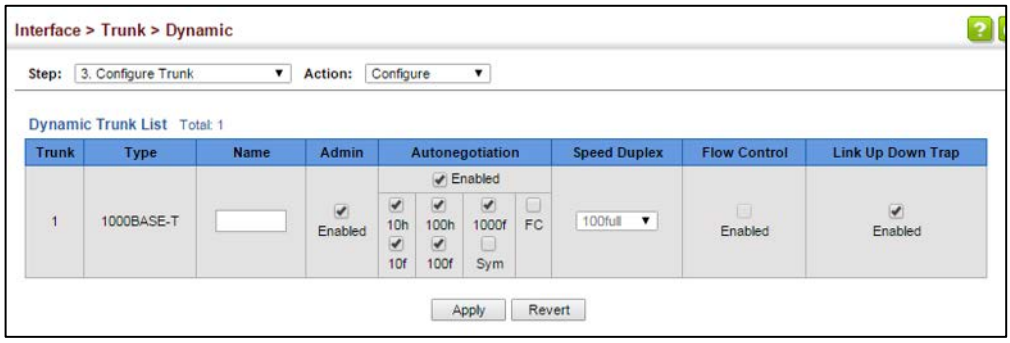
図 4-22　動的トランクのメンバーを表示



動的トランクの接続パラメータを設定するには：

1. [Interface]、[Trunk]、[Dynamic]をクリックします。
2. [Step]リストから[Configure Trunk]を選択します。
3. [Action]リストから[Configure]を選択します。
4. 必要なインタフェース設定を変更します。（インタフェース設定の説明については、「4.1.1　ポートリストによる設定」を参照してください）。
5. [Apply]をクリックします。

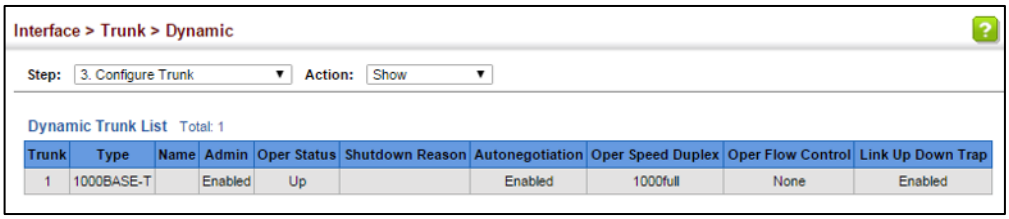
図 4-23　動的トランクの接続設定の設定



動的トランクの接続パラメータを表示するには：

1. [Interface]、[Trunk]、[Dynamic]をクリックします。
2. [Step]リストから[Configure Trunk]を選択します。
3. [Action]リストから[Show]を選択します。

図 4-24　動的トランクの接続パラメータの表示



4.2.3 LACP ポートカウンタの表示

LACP プロトコルメッセージの統計情報を表示するには、[Interface]> [Trunk]> [Dynamic（Configure Aggregation Port – Show Information - Counters]）ページを使用します。

パラメータ

次のパラメータが表示されます。

表 4-2　LACP ポートカウンタ

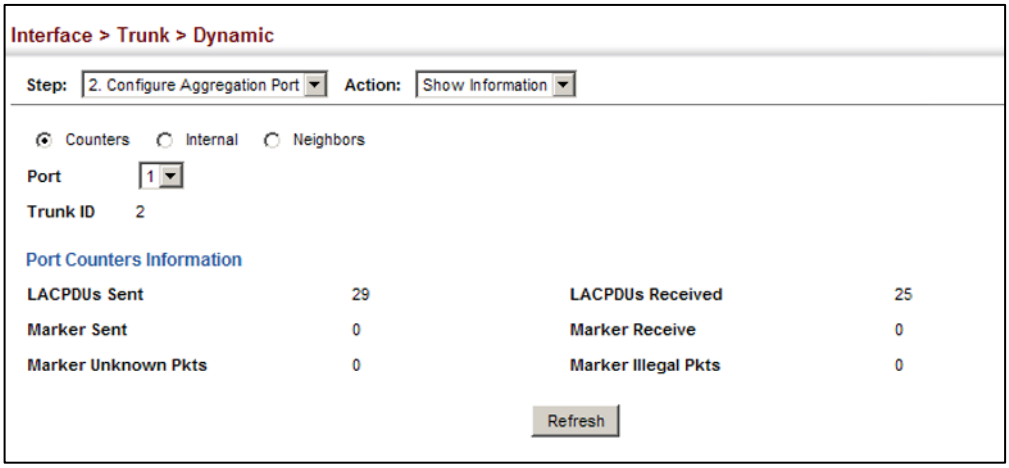
パラメータ	説明
LACPDUs Sent	このチャネルグループから送信された有効な LACPDU の数です。
LACPDUs Received	このチャネルグループで受信された有効な LACPDU の数です。
Marker Sent	このチャネルグループから送信された有効なマーカーPDU の数です。
Marker Received	このチャネルグループによって受信された有効なマーカーPDU の数です。
Marker Unknown Pkts	以下のどちらかに当てはまる受信フレームの数です。 （1）Slow プロトコルのイーサネットタイプの値を持つが、未知の PDU を含んでいる。 （2）Slow プロトコルグループの MAC アドレスに宛てられているが、Slow プロトコルのイーサネットタイプの値でないフレーム。
Marker Illegal Pkts	Slow プロトコルのイーサネットタイプ値を運んでいるが不正に形成された PDU またはプロトコルサブタイプに不正な値を含むフレームの数です。

Web インタフェース

LACP ポートカウンタの表示

1. [Interface]、[Trunk]、[Dynamic]をクリックします。
2. [Step]リストから[Configure Aggregation Port]を選択します。
3. [Action]リストから情報を表示を選択します。
4. [Counters]をクリックします。
5. [Port]リストからグループメンバーを選択します。

図 4-25　LACP ポートカウンタの表示



4.2.4 ローカル側の LACP 設定とステータスの表示

[Interface]> [Trunk]> [Dynamic（Configure Aggregation Port – Show Information - Internal）]ページを使用して、リンク集約のローカル側の設定値および動作状態を表示します。

パラメータ

次のパラメータが表示されます。

表 4-3　LACP 内部設定情報

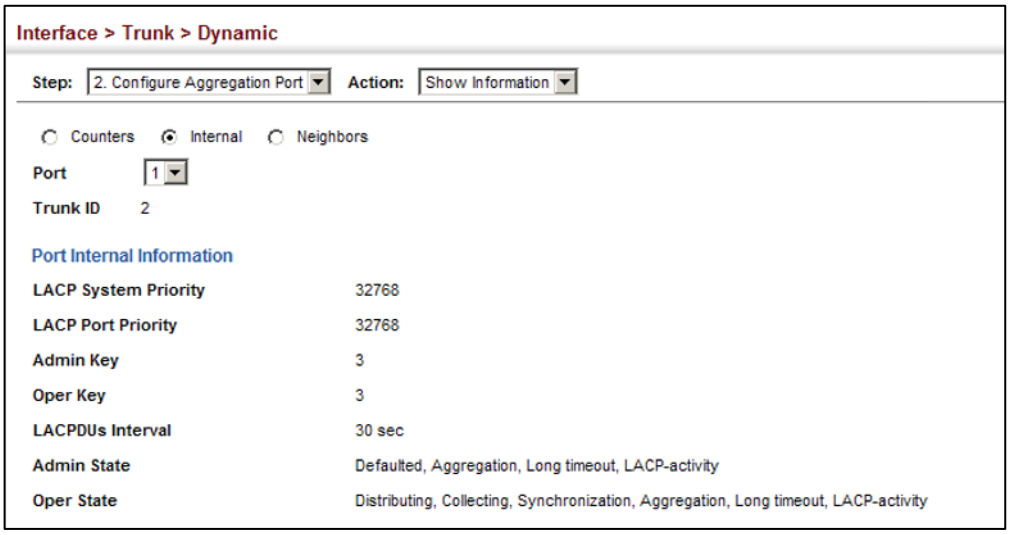
パラメータ	説明
LACP System Priority	このポートチャネルに割当てられた LACP システムプライオリティです。
LACP Port Priority	チャネルグループ内のこのインタフェースに割当てられた LACP ポートプライオリティです。
Admin Key	集約ポートキーの現在の管理上の値です。
Oper Key	集約ポートキーの現在の操作上の値です。
LACPDUs Interval	受信した LACPDU 情報を無効にするまでの秒数です。
Admin State, Oper State	actor の状態パラメータの管理値または操作上の値です。 ・Expired - actor の受信機が期限切れの状態です。 ・Defaulted - actor の受信機は、既定の運用パートナー情報を使用しており、パートナーに対して管理的に構成されています。 ・Distributing - false の場合、このリンク上の発信フレームの配信は無効になります。 すなわち配信は現在無効であり、受信したプロトコル情報の管理上の変更または変更がない場合には有効になることは期待されません。 ・Collecting - このリンク上の受信フレームの収集が有効になっています。 すなわち収集が現在有効であり、受信したプロトコル情報の管理上の変更または変更がない場合には無効になることは期待されません。 ・Synchronization - システムは、このリンクを IN_SYNC と見なします。 すなわち、それが正しいリンク集約グループに割当てられており、そのグループが互換性のあるアグリゲータに関連付けられており、リンク集約グループのアイデンティティが、送信されたシステム ID および操作上の鍵情報と一致しています。 ・Aggregation - システムは、このリンクを集約可能と見なします。 すなわち、集約候補となる可能性があります。 ・Long timeout - LACPDU の周期的な伝送は、遅い伝送速度を使用します。 ・LACP-Activity - このリンクに関する活動制御値です。(0: Passive; 1: Active)

Web インタフェース

ローカル側の LACP 設定とステータスを表示するには：

1. [Interface]、[Trunk]、[Dynamic]をクリックします。
2. [Step]リストから[Configure Aggregation Port]を選択します。
3. [Action]リストから情報を表示を選択します。
4. [Internal]をクリックします。
5. [Port]リストからグループメンバーを選択します。

図 4-26　LACP ポート内部情報の表示



4.2.5 リモート側の LACP 設定とステータスの表示

[Interface]> [Trunk]> [Dynamic（Configure Aggregation Port – Show Information - Neighbors）]ページを使用して、リンク集約のローカル側の設定値および動作状態を表示します。

パラメータ

次のパラメータが表示されます。

表 4-4　LACP リモートデバイス設定情報

パラメータ	説明
Partner Admin System ID	ユーザが割当てた LAG パートナーのシステム ID。
Partner Oper System ID	LACP プロトコルによって割当てられた LAG パートナーのシステム ID。
Partner Admin Port Number	プロトコルパートナーのポート番号の現在の管理上の値。
Partner Oper Port Number	ポートのプロトコルパートナーによってこの集約ポートに割当てられた操作ポート番号。
Port Admin Priority	プロトコルパートナーのポート優先順位の現在の管理上の値。
Port Oper Priority	パートナーによってこの集約ポートに割当てられたプライオリティ値。
Admin Key	プロトコルパートナーキーの現在の管理上の値。
Oper Key	プロトコルパートナーキーの現在の操作上の値。
Admin State	パートナーの状態パラメータの管理値。（上記の表を参照してください）。
Oper State	パートナーの状態パラメータの操作上の値（上記の表を参照してくださ

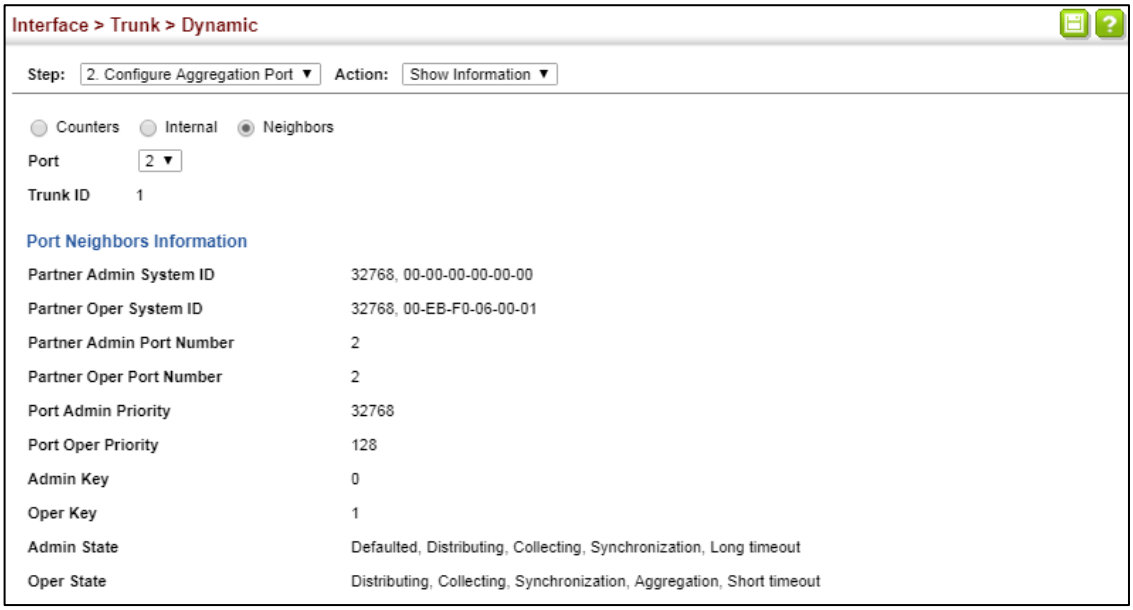
パラメータ	説明
	い）。

Web インタフェース

リモート側の LACP 設定とステータスを表示するには：

1. [Interface]、[Trunk]、[Dynamic]をクリックします。
2. [Step]リストから[Configure Aggregation Port]を選択します。
3. [Action]リストから情報を表示を選択します。
4. [Neighbors]をクリックします。
5. [Port]リストからグループメンバーを選択します。

図 4-27　LACP ポートリモート情報の表示



4.2.6 ロードバランシングの設定

[Interface]> [Trunk]> [Load Balance]ページを使用して、集約リンク内のポート間で使用される負荷分散方法を設定します。

コマンドの使用方法

- 本コマンドは、スイッチ上のすべての静的トランクと動的トランクに適用されます。
- スイッチのトラフィック負荷がトランク内のすべてのリンクに均等に分散されるようにするには、負荷バランス計算で使用される送信元アドレスと宛先アドレスを選択して、トランク接続に最適な結果を提供します。
  - Destination IP Address: 同じ宛先 IP アドレスを持つすべてのトラフィックは、トランク内の同じリンクに出力されます。このモードは、スイッチを通過するトラフィックが多くの異なるホストに向けられているスイッチ間トランクリンクに最適です。宛先 IP アドレスがすべてのトラフィックで同じであるスイッチツーサーバトランクリンクには、このモードを使用しないでください。
  - Destination MAC Address: 同じ宛先 MAC アドレスを持つすべてのトラフィックは、トランク内の同じリンクに出力されます。このモードは、スイッチを通過するトラフィックが多くの異なるホストを宛先とするスイッチ間トランクリンクに最適です。宛先 MAC アドレスがすべてのトラ

フィックで同じであるスイッチ間トランクリンクには、このモードを使用しないでください。

- Source and Destination IP Address: 同じ送信元および宛先 IP アドレスを持つすべてのトラフィックは、トランク内の同じリンクに出力されます。このモードは、スイッチを経由するトラフィックがさまざまなホストから受信され、多数の異なるホスト宛てのスイッチ間ルータトランクリンクに最適です。
- Source and Destination MAC Address: 同じ送信元および宛先 MAC アドレスを持つすべてのトラフィックは、トランク内の同じリンクに出力されます。このモードは、スイッチを経由するトラフィックが多くの異なるホストから受信され、多くの異なるホスト宛てのスイッチ間トランクリンクに最適です。
- Source IP Address: 同じ送信元 IP アドレスを持つすべてのトラフィックは、トランク内の同じリンクに出力されます。このモードは、スイッチ間トラフィックが多くの異なるホストから受信されるスイッチ間ルータまたはスイッチ間トランクリンクに最適です。
- Source MAC Address: 同じ送信元 MAC アドレスを持つすべてのトラフィックは、トランク内の同じリンクに出力されます。このモードは、スイッチを経由するトラフィックが多くの異なるホストから受信されるスイッチ間トランクリンクに最適です。

パラメータ

これらのパラメータは、ロードバランスモードで表示されます。

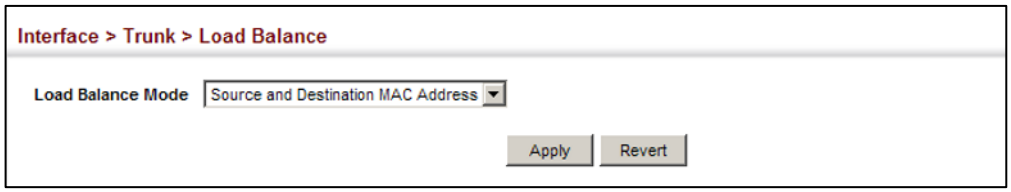
- Destination IP Address - 宛先 IP アドレスにもとづくロードバランシングです。
- Destination MAC Address - 宛先 MAC アドレスに基づくロードバランシングです。
- Source and Destination IP Address - 送信元および宛先 IP アドレスに基づくロードバランシングです。
- Source and Destination MAC Address -送信元 MAC アドレスと宛先 MAC アドレスに基づくロードバランシングです。
- Source IP Address - 送信元 IP アドレスに基づくロードバランシングです。
- Source MAC Address - 送信元 MAC アドレスに基づくロードバランシングです。

Web インタフェース

集約リンクのポートが使用する負荷分散方式を表示します：

1. [Interface]、[Trunk]、[Load Balance]をクリックします。
2. [Load Balance Mode]リストから必要な方法を選択します。
3. [Apply]をクリックします。

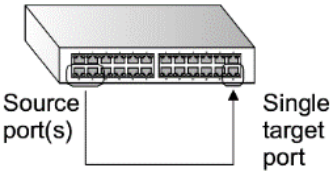
図 4-28　ロードバランシングの設定



4.3 ローカルポートミラーリングの設定

[Interface]> [Mirror]ページを使用して、リアルタイム分析のために、任意のソースポート（送信元ポート）からターゲットポート（宛先ポート）へトラフィックをミラーリングできます。

図 4-29 ローカルポートミラーリングの設定



コマンドの使用方法

- トラフィックは、1 つまたは複数の送信元ポートから同じスイッチ上の宛先ポート（本章で説明するローカルポートミラーリング）に、またはリモートスイッチ上の 1 つ以上の送信元ポートからこのスイッチ上の宛先ポートにミラーリングできます。
- 宛先ポートの速度が送信元ポートの速度と同じかそれを超える必要があります。さもないと、トラフィックがモニタポートで廃棄される可能性があります。
- 宛先ポートは、トランクまたはトランクメンバーポートにすることはできません。
- スパニングツリーBPDU パケットはターゲットポートにミラーリングされません。

パラメータ

次のパラメータが表示されます。

- Source Port - トラフィックが監視される送信元ポートです。
- Target Port - 送信元ポートのトラフィックを反映する宛先ポートです。
- Type - 送信元ポートの Rx（受信）、Tx（送信）、または Both のミラーリングするトラフィックを選択できます。(デフォルト: Both)

Web インタフェース

ローカルミラーセッションを設定するには：

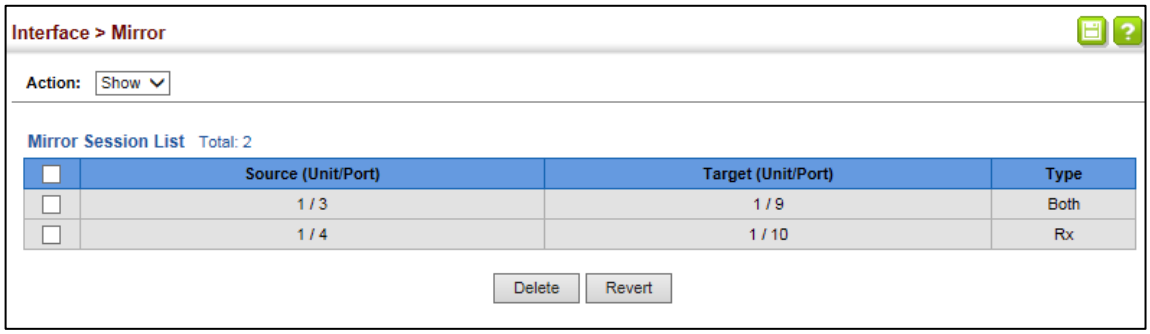
1. [Interface]、[Mirror]をクリックします。
2. [Action]リストから[Add]を選択します。
3. 送信元ポートを指定します。
4. 宛先ポートを指定します。
5. ミラーリングするトラフィックタイプを指定します。
6. [Apply]をクリックします。

図 4-30　ローカルポートミラーリングの設定

設定済みのミラーセッションを表示するには：

1. [Interface]、[Mirror]をクリックします。
2. [Action]リストから[Show]を選択します。

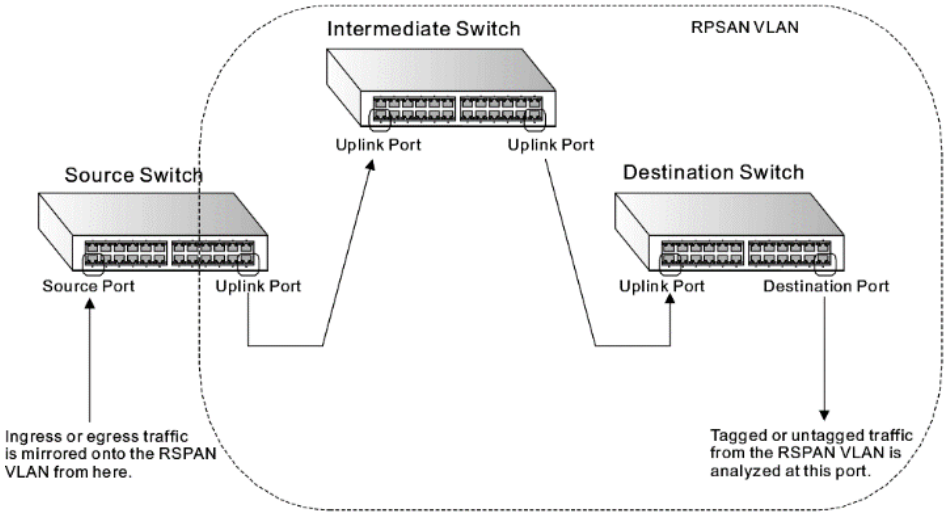
図 4-31　ローカルポートミラーセッションの表示



4.4 リモートポートミラーリングの設定

[Interface]> [RSPAN]ページを使用して、ローカルスイッチ上の宛先ポートで分析するためにリモートスイッチからのトラフィックをミラーリングします。リモートスイッチドポートアナライザ（RSPAN）とも呼ばれるこの機能は、各セッションの指定された送信元ポートで生成されたトラフィックを、参加しているすべてのスイッチの RSPAN セッション専用のユーザ指定 VLAN で伝送します。1 つ以上の送信元からの監視トラフィックは、IEEE 802.1Q トランクポートまたはハイブリッドポートを介して RSPAN VLAN にコピーされ、RSPAN VLAN を監視する RSPAN 宛先ポートに送信されます（下図参照）。

図 4-32　リモートポートミラーリングの設定



コマンドの使用方法

◆ トラフィックは、1 つ以上の送信元ポートから同じスイッチ上の宛先ポートにミラーリングされます。またはリモートスイッチ上の 1 つ以上の送信元ポートからこのスイッチの宛先ポート（本章で説明するリモートポートミラーリング）に接続できます。

◆ 設定ガイドライン

RSPAN セッションを設定するには、次の手順を実行します。

1. RSPAN で使用するために VLAN を予約する VLAN 静的リストを使用してください（VLAN グループの設定の章を参照）。(デフォルト VLAN1 は禁止されています。)
2. ミラーセッション、スイッチの役割（Source）、RSPAN VLAN、およびアップリンクポートを指定して、RSPAN 設定ページでソーススイッチを設定します※。送信元ポートと、監視するトラフィックタイプ（Rx、Tx または Both）を指定します。
3. RSPAN 設定ページのすべての中間スイッチを設定し、ミラーセッション、スイッチの役割（中間）、RSPAN VLAN、およびアップリンクポートを入力します。
4. ミラーセッションを指定して RSPAN 設定ページの宛先スイッチを設定し、スイッチの役割（Destination）、宛先ポート※、このポートを出るトラフィックにタグ付けまたはタグなし、および RSPAN VLAN を指定します。次に、ミラーリングされたトラフィックが受信されている各アップリンクポートを指定します。

注※ 802.1Q トランクポートまたはハイブリッド（すなわち一般的な）ポートだけが、RSPAN アップリンクポートまたは宛先ポートとして設定できます。アクセスポートは許可されません。

◆ RSPAN の制限

スイッチで RSPAN を使用するために、下記の制限が適用されます。

- RSPAN Ports - RSPAN 送信元、宛先またはアップリンクとして設定できる唯一のポートであり、静的および動的トランクは許容されません。ポートは、RSPAN インタフェースの 1 つのタイプ（送信元、宛先、またはアップリンク）としてのみ設定できます。また、送信元ポートと宛先ポートを同じスイッチ上で設定することはできないことに留意してください。
- Local/Remote Mirror - [Interface]> [Mirror]ページで作成されたローカルミラーセッションの宛先は、RSPAN トラフィックの宛先として使用できません。
- Spanning Tree - スパニングツリーが無効の場合、BPDU は RSPAN VLAN にフラッディングしません。
- RSPAN がスイッチで有効な場合、MAC アドレス学習は RSPAN アップリンクポートではサポートされません。そのため、RSPAN 設定後にスパニングツリーが有効になった場合でも、RSPAN アップリンクポートにおいて MAC アドレス学習は再開しません。
- Port Security - ポートセキュリティが任意のポートで有効になっている場合、そのポートは RSPAN 送信元ポートまたは宛先ポートとして設定できますが、RSPAN アップリンクポートとして設定することはできません。また、ポートが RSPAN アップリンクポートとして設定されている場合、そのポートでポートセキュリティを有効にすることはできません。

パラメータ

次のパラメータが表示されます。

- Session - この RSPAN セッションを識別する番号です。(範囲: 1 から 3)
  1 つのアクティブセッションのみが許可されます。
- Operation Status - RSPAN が現在機能しているかどうかを示します。
- Switch Role - このスイッチがトラフィックをミラーリングする際に果たす役割を指定します。
  - None - このスイッチは RSPAN に参加しません。
  - Source - このデバイスをリモートミラーリングされたトラフィックの送信元スイッチとして指定します。
  - Intermediate - このデバイスを中間スイッチとして指定し、ミラーリングされたトラフィックを 1 つ以上のソースから 1 つ以上の宛先に透過的に渡します。
  - Destination - このデバイスを、このセッションのミラーリングされたトラフィックを受信する宛先ポートで設定された宛先スイッチとして指定します。
- Remote VLAN - 送信元ポートからミラーリングされたトラフィックがフラッディングされる VLAN。このフィールドで指定された VLAN は、まず[VLAN]> [Static]ページを使用して RSPAN アプリケーション用に予約する必要があります.
- Uplink Port - ミラーリングされたトラフィックが RSPAN VLAN に渡される、または RSPAN VLAN から受信される、RSPAN に関与するすべてのスイッチ上のポート。
  送信元スイッチに設定できるアップリンクポートは 1 つだけですが、中間または宛先スイッチに設定されるアップリンクポート※の数に制限はありません。
  宛先ポートとアップリンクポートだけが、スイッチによって RSPAN VLAN のメンバーとして割当てられます。[VLAN]> [Static]ページを使用して、ポートを RSPAN VLAN に手動で割当てることはできません。また、[VLAN]> [Static（Show）]ページには RSPAN VLAN のメンバーは表示されませんが、設定された RSPAN VLAN ID のみが表示されます。
- Type - リモートでミラーリングされるトラフィックタイプを指定します。(オプション: Rx, Tx, Both)
- Destination Port - 送信元ポート※からミラーリングされたトラフィックを監視する宛先ポートを指定します。セッションごとに同じスイッチに設定できる宛先ポートは 1 つだけですが、同じセッションで複数のスイッチに宛先ポートを設定することができます。また、宛先ポートはスイッチドトラフィックを送受信でき、割当てられたレイヤ 2 プロトコルに参加できます。

◆ Tag - 宛先デバイスからモニタデバイスへのトラフィックが RSPAN VLAN タグを伝送するかどうかを指定します。

注※ 802.1Q トランクポートまたはハイブリッド（すなわち一般的な）ポートだけが、RSPAN アップリンクポートまたは宛先ポートとして設定できます。アクセスポートは許可されません。

Web インタフェース

リモートミラーセッションを設定するには：

1. [Interface]、[RSPAN]をクリックします。
2. Switch Role を None、Source、Intermediate、または Destination に設定します。
3. RSPAN VLAN に参加する各スイッチに必要な設定を行います。
4. [Apply]をクリックします。

図 4-33　リモートポートミラーリングの設定（Source)

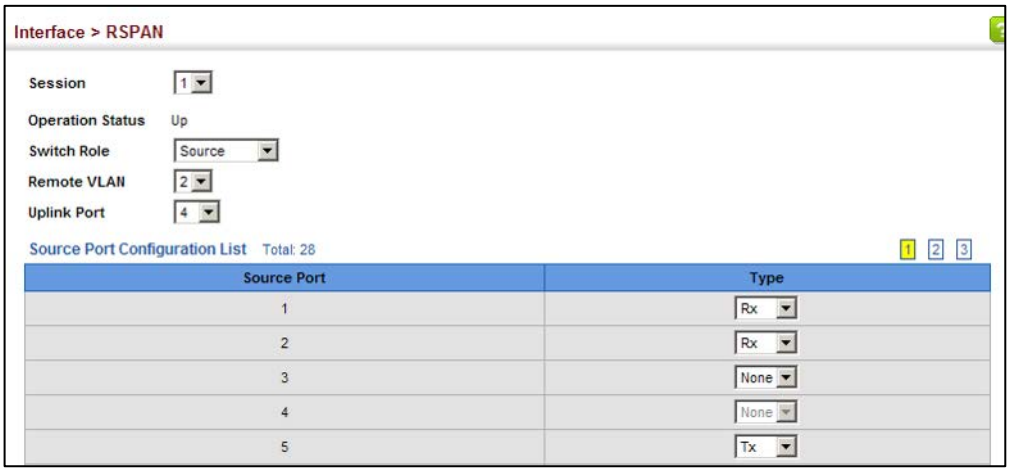


図 4-34　リモートポートミラーリングの設定（Intermediate)

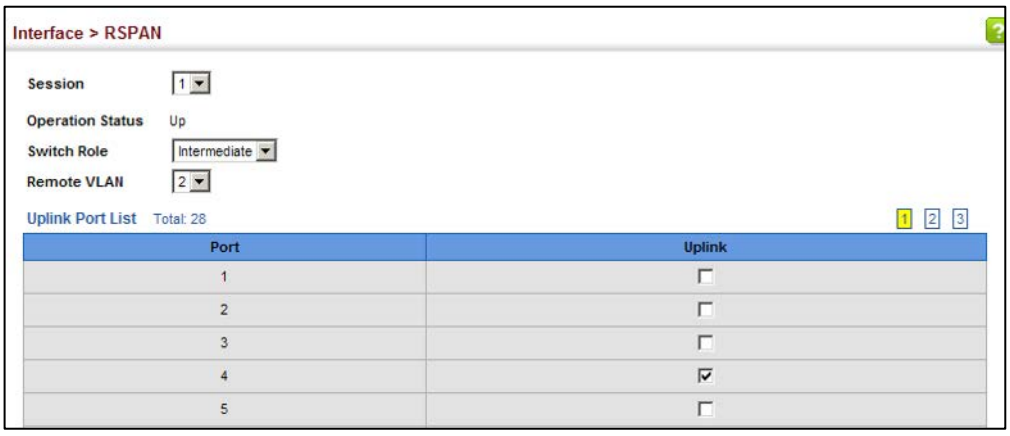
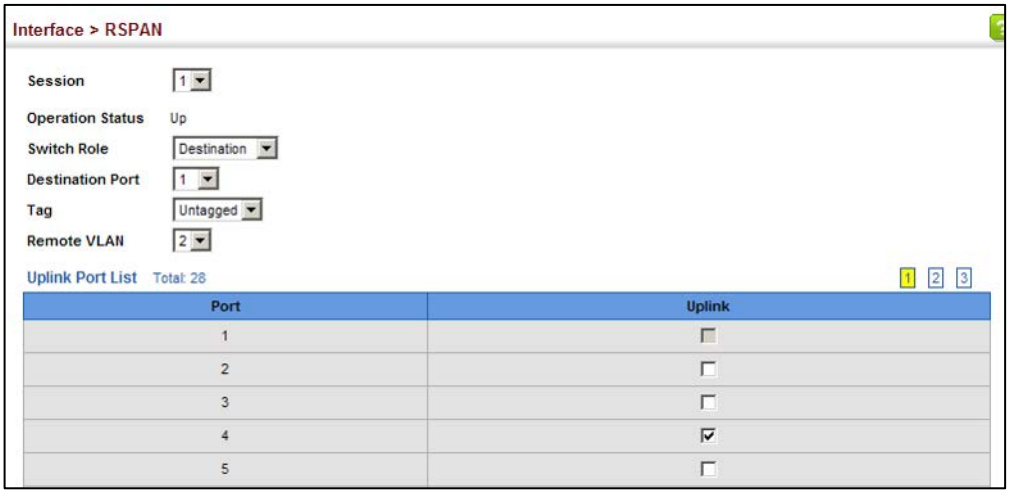


図 4-35　リモートポートミラーリングの設定 (Destination)



4.5 sFlow

このスイッチに埋め込まれたフローサンプリング（sFlow）機能は、リモート sFlow Collector とともにネットワーク管理者に、ネットワーク上に存在するトラフィックの種類とレベルの正確で詳細なリアルタイムの概要を提供します。sFlow Agent は、スイッチを通過するすべてのデータから n 個のパケットのうち 1 つをサンプリングし、サンプルを sFlow データグラムとして再カプセル化して、sFlow コレクタに送信します。このサンプリングは、すべてのトラフィックが表示される内部ハードウェアレベルで行われますが、従来のプローブでは、監視されたインタフェースでサンプリングされたトラフィックの一部分しか表示されません。さらに、ローカル解析が行われないため、sFlow エージェントが課すプロセッサとメモリの負荷は最小限に抑えられます。このサンプリングは、すべてのトラフィックが見られる内部ハードウェアレベルで行われますが、従来のプローブでは、監視されたインタフェースでサンプリングされたトラフィックの一部しか表示されません。

Note: 本章では、[コレクタ]、[レシーバ]、および[所有者]という用語はすべて、スイッチの sFlow エージェントによって生成された sFlow データグラムを受信できるリモートサーバを指します。

コレクタは、ネットワーク上のさまざまな sFlow エージェント（他のスイッチまたはルータ）からのストリームを受信すると、タイムリーなネットワーク全体の利用状況とトラフィックフローの図が作成されます。sFlow ストリームの分析は、以下の方法で活用できる傾向と情報を明らかにすることができます。

- ネットワークの問題の検出、診断、および修正
- リアルタイムの輻輳管理
- アプリケーションのミックス（P2P、Web、DNS など）と変更の理解
- 不正なネットワークアクティビティの特定と追跡
- アカウント使用方法
- 傾向分析とキャパシティプランニング

4.5.1 sFlow レシーバの設定

[Interface]> [sFlow（Configure Receiver – Add）]ページを使用して、スイッチ上に sFlow レシーバを作成します。

パラメータ

次のパラメータが表示されます。

- Receiver Owner Name - レシーバの名前。(範囲: 1 から 30 文字、デフォルト: None)
- Receiver Timeout - すべての sFlow ポートパラメータをリセットする前に、sFlow プロセスがサンプルをコレクタに継続的に送信する時間です。(範囲: 30 から 10000000 秒）
  このコマンドの影響を受ける sFlow パラメータには、サンプリング間隔、レシーバの名前、アドレスと UDP ポート、タイムアウト、最大ヘッダーサイズ、および最大データグラムサイズが含まれます。
- Receiver Destination - sFlow Collector の IP アドレスです。
  - ipv4-address - sFlow コレクタの IPv4 アドレスです。有効な IPv4 アドレスは、ピリオドで区切られた 0 から 255 の 4 つの 10 進数で構成されます。
  - ipv6-address - sFlow コレクタの IPv6 アドレスです。ネットワークプレフィックスとホストアドレスビットを含むフル IPv6 アドレスです。IPv6 アドレスは、8 つのコロンで区切られた 16 ビットの 16 進数で構成されています。1 つの二重コロンを使用して、未定義フィールドを埋めるために

必要なゼロの適切な数を示すことができます。

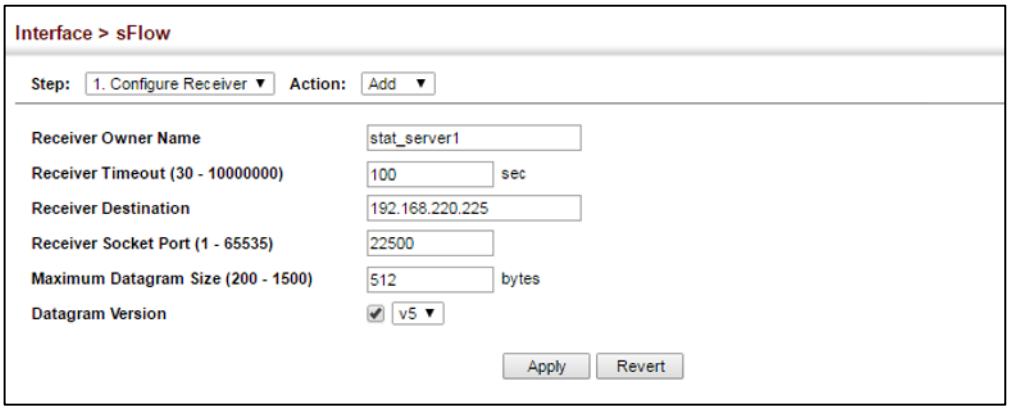
- Receiver Socket Port - sFlow Collector が sFlow ストリームを聴取する UDP ポートです。(範囲: 1 から 65535)
- Maximum Datagram Size - sFlow データグラムペイロードの最大サイズです。(範囲: 200 から 1500 バイト)
- Datagram Version - v4 または v5 の sFlow データグラムをレシーバに送信します。

Web インタフェース

sFlow レシーバを設定するには：

1. [Interface]、[sFlow]をクリックします。
2. [Step]リストから[Configure Receiver]を選択します。
3. [Action]リストから[Add]を選択します。
4. sFlow レシーバとモニタされたトラフィックのパラメータを入力します。
5. [Apply]をクリックします。

図 4-36　sFlow レシーバの設定

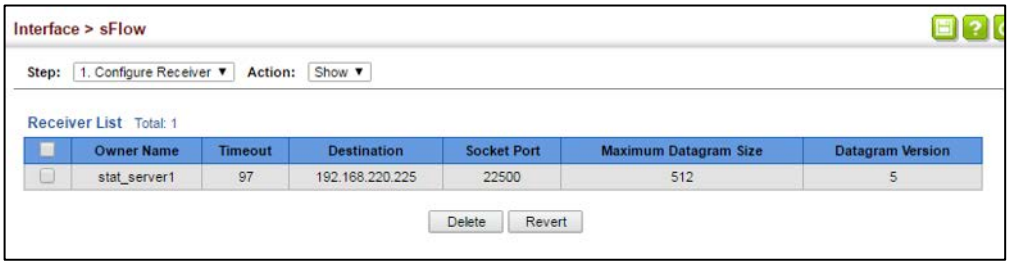


Web インタフェース

設定済みのレシーバを表示するには：

1. [Interface]、[sFlow]をクリックします。
2. [Step]リストから[Configure Receiver]を選択します。
3. [Action]リストから[Show]を選択します。

図 4-37　sFlow レシーバの表示



4.5.2 sFlow ポーリングインスタンスの設定

[Interface]> [sFlow（Configure Details – Add）]ページを使用して、指定された時間間隔にもとづいて定期的

にポーリングする sFlow ポーリングデータソース、または処理されたパケット数にもとづいてサンプルを定期的に取得する sFlow データソースインスタンスを有効にします。

パラメータ

これらのパラメータは、Web インタフェースに表示されます。

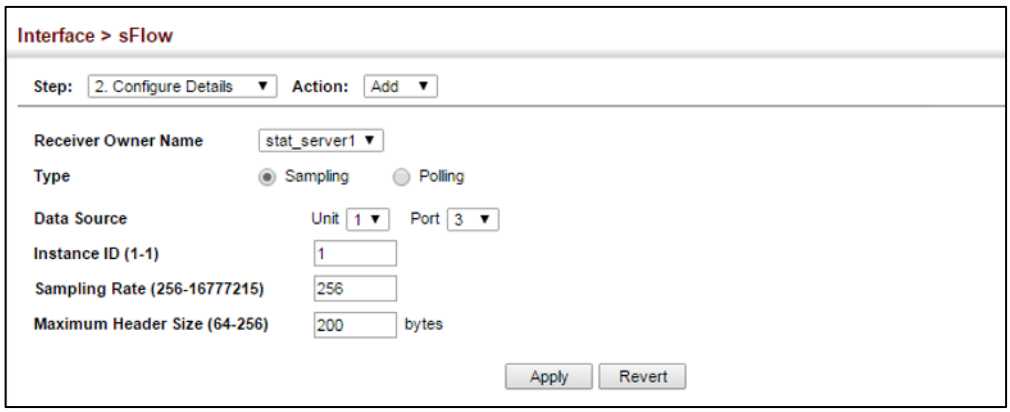
- Receiver Owner Name - レシーバの名前です。(範囲: 1 から 30 文字、デフォルト: None)
- Type - ポーリングタイプを、指定された時間間隔にもとづいて定期的にポーリングする指定インタフェースの sFlow ポーリングデータソース、または処理されたパケット数にもとづいて定期的にサンプルを取得する特定のインタフェースの sFlow データソースインスタンスとして指定します。
- Data Source - サンプルが採取され、コレクタに送られるソースです。
- Instance ID - サンプリングソースを識別するために使用されるインスタンス ID です。(範囲: 1)
- Sampling Rate - 1 つのサンプルが取り出されるパケットの数です。(範囲: 2-65535 パケット、デフォルト：Disabled)
- Maximum Header Size - sFlow データグラムヘッダの最大サイズです。
  (範囲: 64 から 256 バイト)

Web インタフェース

sFlow サンプリングまたはポーリングインスタンスを設定するには：

1. [Interface]、[sFlow]をクリックします。
2. [Step]リストから[Configure Details]を選択します。
3. [Action]リストから[Add]を選択します。
4. サンプリングレートと最大ヘッダーサイズを含む sFlow インスタンスのパラメータを入力します。
5. [Apply]をクリックします。

図 4-38　sFlow インスタンスの設定



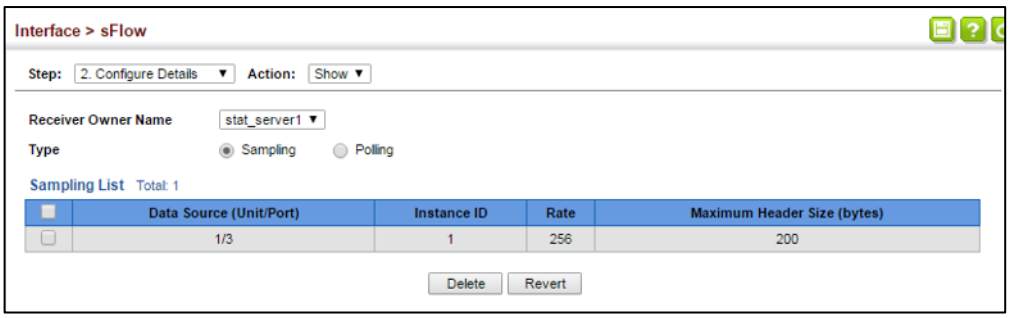
Web インタフェース

設定されたインスタンスを表示するには：

1. [Interface]、[sFlow]をクリックします。
2. [Step]リストから[Configure Details]を選択します。
3. [Action]リストから[Show]を選択します。
4. スクロールダウンリストから所有者名を選択します。

5.　sFlow type をサンプリングまたはポーリングとして選択します。

図 4-39　sFlow インスタンスの表示



4.6 トラフィックセグメンテーション

異なるクライアントからのトラフィックをローカルネットワークのダウンリンクポートとアップリンクポートを介してサービスプロバイダーに渡すために、より厳しいセキュリティが必要な場合には、ポートベースのトラフィックセグメンテーションを使用して、個々のクライアントのトラフィックを分離することができます。

ダウンリンクポートは、各クライアント毎に使用するポートを分けることでトラフィックを分離します。一方、アップリンクポートもクライアント毎に使用するポートを分けてトラフィックを分離しますが、他のクライアントが使用するアップリンクポートを介してトラフィックを転送することもできます。

4.6.1 トラフィックセグメンテーションの有効化

[Interface]> [Traffic Segmentation（Configure Global）]ページを使用してトラフィックセグメント化を有効にします。

パラメータ

次のパラメータが表示されます。

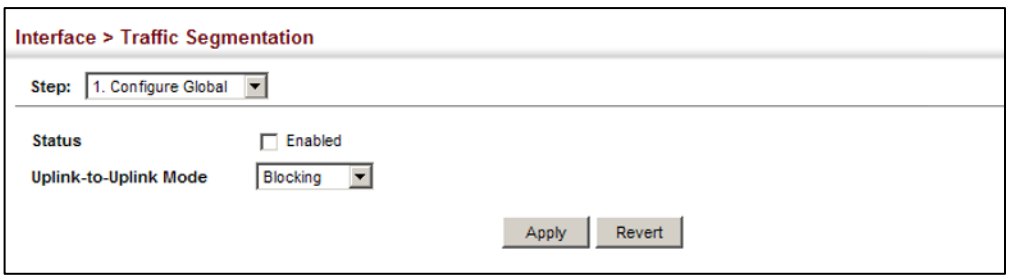
- Status - ポートベースのトラフィックセグメンテーションを有効にします。(デフォルト: Disabled)
- Uplink-to-Uplink Mode - 異なるクライアントセッションに割当てられたアップリンクポート間でトラフィックを転送できるかどうかを指定します。
  - Blocking - 異なるセッションに割当てられたアップリンクポート間のトラフィックをブロックします。
  - Forwarding - 異なるセッションに割当てられたアップリンクポート間でトラフィックを転送します。

Web インタフェース

トラフィックのセグメント化を有効にするには：

1. [Interface]、[Traffic Segmentation]をクリックします。
2. [Step]リストから[Configure Global]を選択します。
3. [Status]チェックボックスをオンにして、必要なアップリンク/アップリンクモードを設定します。
4. [Apply]をクリックします。

図 4-40　トラフィックセグメンテーションの有効化



4.6.2 アップリンクおよびダウンリンクポートの設定

[Interface]> [Traffic Segmentation（Configure Session）]ページを使用して、セグメント化されたグループで使用するダウンリンクおよびアップリンクポートを割当てます。ダウンリンクポートとして指定されたポートは、アップリンクポート以外のスイッチ上の他のポートと通信できません。アップリンクポートは、ス

イッチ上の他のポートおよび指定されたダウンリンクポートと通信できます。

コマンドの使用方法

◆ トラフィックのセグメント化が有効な場合の、異なるクライアントセッションに割当てられたアップリンクおよびダウンリンクポートの転送状態について、以下に示します:

表 4-5 トラフィックセグメントの転送

宛先 送信元	セッション#1 ダウンリンク	セッション#1 アップリンク	セッション#2 ダウンリンク	セッション#2 アップリンク	通常ポート
セッション#1 ダウンリンクポート	Blocking	Forwarding	Blocking	Blocking	Blocking
セッション#1 アップリンクポート	Forwarding	Forwarding	Blocking	Blocking/Forwarding※	Forwarding
セッション#2 ダウンリンクポート	Blocking	Blocking	Blocking	Forwarding	Blocking
セッション#2 アップリンクポート	Blocking	Blocking/Forwarding※	Forwarding	Forwarding	Forwarding
Normal Ports	Forwarding	Forwarding	Forwarding	Forwarding	Forwarding

注※ アップリンクからアップリンクへのポートのフォワーディングステートは、一般構成ページで設定します。

◆ トラフィックのセグメント化が無効な場合、すべてのポートは VLAN およびスパニングツリープロトコルのような、その他の機能によって指定された設定にもとづいて、通常転送モードで作動します。

◆ アップリンクとダウンリンクリストの両方では、ポートを設定することはできません。

◆ ポートは、1 つのトラフィックセグメンテーションセッションにのみ割当てることができます。

◆ ダウンリンクポーとは、同じセッションの中でのみ、アップリンクポートと通信できます。故に、セッションに対してアップリンクポートが設定されていない場合には、割当てられたダウンリンクポートは他のポートと通信することができません。

◆ セッションに対してダウンリンクポートが設定されていない場合、割当てられたアップリンクポートは通常ポートとして動作します。

パラメータ

次のパラメータが表示されます。

◆ Session ID - トラフィックセグメンテーションセッションです。(範囲: 1 から 4)

◆ Direction - 方向をアップリンクまたはダウンリンクに設定して、セグメント化されたグループにインタフェースを追加します。(デフォルト: Uplink)

◆ Interface - ポートまたはトランクのリストを表示します。

◆ Port - ポート番号です。(範囲: 1 から 10)

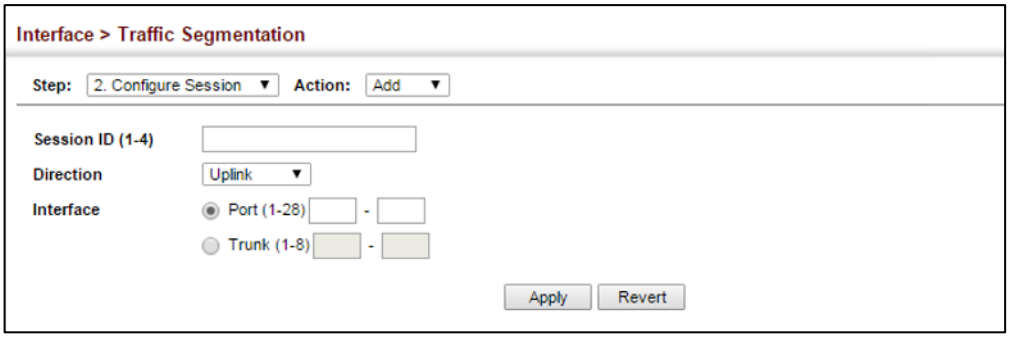
◆ Trunk - トランク識別子です。(範囲: 1-8)

Web インタフェース

トラフィックセグメンテーショングループのメンバーを設定するには、次の手順を実行します。

1. [Interface]、[Traffic Segmentation]をクリックします。
2. [Step]リストから[Configure Session]を選択します。
3. [Action]リストから[Add]を選択します。
4. セッション ID を入力し、方向をアップリンクまたはダウンリンクに設定し、追加するインタフェースを選択します。
5. [Apply]をクリックします。

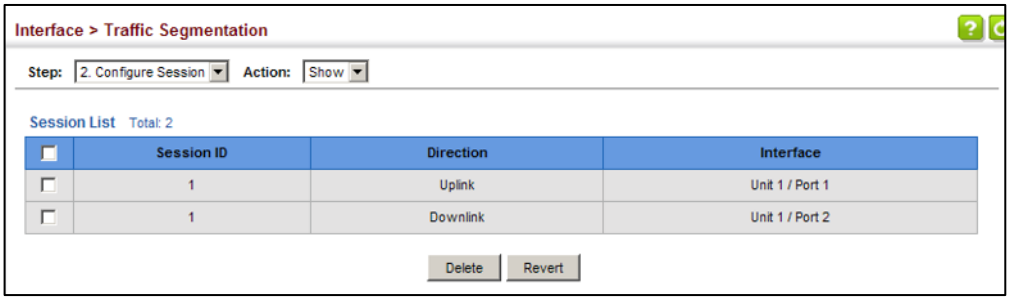
図 4-41　トラフィックセグメンテーションのメンバーの設定



トラフィックセグメンテーショングループのメンバーを表示するには：

1. [Interface]、[Traffic Segmentation]をクリックします。
2. [Step]リストから[Configure Session]を選択します。
3. [Action]リストから[Show]を選択します。

図 4-42　トラフィックセグメンテーションメンバーの表示



5 VLAN 設定

本章では、次のトピックについて説明します。

- IEEE 802.1Q VLANs - 静的 VLAN を設定します。
- IEEE 802.1Q Tunneling - QinQ トンネリングを設定して、異なる顧客が同じ内部 VLAN ID を使用している場合でも、サービスプロバイダネットワーク全体でカスタマー固有の VLAN およびレイヤ 2 プロトコル設定を維持します。
- Protocol VLANs - 指定されたプロトコルにもとづいて VLAN グループを設定します。
- MAC-based VLANs - 送信元 MAC アドレスが IP MAC アドレス/ VLAN マッピングテーブルにある場合、タグなし入力フレームを指定された VLAN にマッピングします。

5.1 IEEE 802.1Q VLANs

大規模なネットワークでは、各サブネットのブロードキャストトラフィックを別々のドメインに分離するためにルーターが使用されます。このスイッチは、VLAN を使用してネットワークノードのグループを別々のブロードキャストドメインに編成することによって、レイヤ 2 で同様のサービスを提供します。VLAN はブロードキャストトラフィックを発信グループに限定し、大規模なネットワークでのブロードキャストストームを排除できます。これにより、より安全でクリーンなネットワーク環境も提供されます。

IEEE 802.1Q VLAN は、ネットワーク内のどこにでも配置でき、同じ物理セグメントに属するかのように通信できるポートのグループです。

VLAN を使用すると、物理接続を変更することなくデバイスを新しい VLAN に移行できるため、ネットワーク管理が簡単になります。VLAN は、部門別グループ（マーケティングや研究開発など）、使用グループ（電子メールなど）、またはマルチキャストグループ（ビデオ会議などのマルチメディアアプリケーションに使用）を反映するように簡単に編成できます。

VLAN は、ブロードキャストトラフィックを削減してネットワーク効率を向上させ、IP アドレスまたは IP サブネットを更新せずにネットワークを変更できるようにします。トラフィックは設定されたレイヤ 3 リンクを通過して別の VLAN に到達する必要があるため、VLAN は本質的に高いレベルのネットワークセキュリティを提供します。

このスイッチは、次の VLAN 機能をサポートしています。

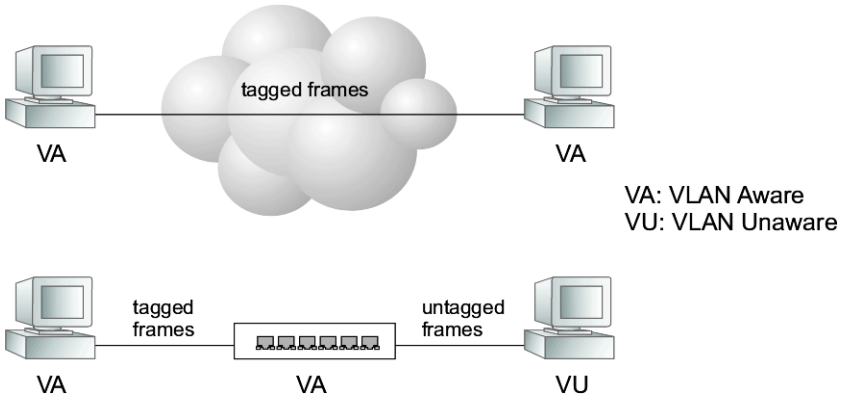
- IEEE 802.1Q 標準に基づく最大 4094 の VLAN
- 明示的なタグ付けを使用して複数のスイッチにまたがる分散型 VLAN 学習
- ポートオーバーラップ、ポートを複数の VLAN に参加させることができます
- エンドステーションは複数の VLAN に属することができます
- VLAN 対応デバイスと VLAN 未対応デバイス間のトラフィックの受け渡し
- 優先度タグ付け

VLAN へのポートの割当て

各ポートが参加する VLAN グループを割当てる必要があります。デフォルトでは、すべてのポートはタグなしポートとして VLAN 1 に割当てられます。1 つまたは複数の VLAN のトラフィックを伝送し、中間ネットワークデバイスまたは接続の反対側のホストが VLAN をサポートする場合は、ポートをタグ付きポートとして追加します。ただし、中間ネットワークデバイスも接続の反対側のホストも VLAN をサポートしていない場合には、このポートをタグなしポートとして VLAN に追加する必要があります。

Note: VLAN タグ付きフレームは、VLAN 対応または VLAN 未対応のネットワーク相互接続デバイスを通過できますが、VLAN タグは、VLAN タグ付けをサポートしていないエンドノードホストに渡す前に切り離す必要があります。

図 5-1 VLAN 準拠および VLAN 非対応デバイス



VLAN Classification - スイッチがフレームを受け取った際に、2 つの方法のうちにいずれかでフレームを分別します。フレームがタグなしの場合、スイッチはフレームを関連する VLAN に割当てます（受信ポートのデフォルト VLAN ID にもとづいて）。しかし、フレームにタグが設定されている場合、スイッチはタグ付き VLAN ID を使用して、フレームのポートブロードキャストドメインを識別します。

Port Overlapping - ポートオーバーラップを使用すると、ファイルサーバやプリンタなどの異なる VLAN グループ間で共通に共有されるネットワークリソースにアクセスできます。重複していないが通信する必要のある VLAN を実装する場合は、このスイッチの有効なルーティングによって VLAN を接続できます。

Untagged VLANs - タグなし VLAN は、通常、ブロードキャストトラフィックを削減し、セキュリティを強化するために使用されます。VLAN に割当てられたネットワークユーザのグループは、スイッチ上で設定された他の VLAN とは別のブロードキャストドメインを形成します。パケットは同じ VLAN に指定されたポート間でのみ転送されます。タグなし VLAN は、ユーザグループまたはサブネットを手動で隔離するために使用できます。

タグ付き/タグなしフレームの転送

1 つのスイッチに直接接続されたデバイス用の小さなポートベースの VLAN を作成する場合は、同じタグなし VLAN にポートを割当てることができます。ただし、複数のスイッチを横断する VLAN グループに参加するには、そのグループの VLAN を作成し、すべてのポートでタグ付けを有効にする必要があります。

ポートは、複数のタグ付き VLAN またはタグなし VLAN に割当てることができます。したがって、スイッチ上の各ポートはタグ付きフレームまたはタグなしフレームを渡すことができます。このスイッチから VLAN 対応デバイスを含むパスにフレームを転送する場合、スイッチには VLAN タグが含まれている必要があります。VLAN 対応デバイス（宛先ホストを含む）を含まないパスに沿ってこのスイッチからフレームを転送する場合、フレームを転送する前にスイッチは最初に VLAN タグを除去する必要があります。スイッチがタグ付きフレームを受信すると、スイッチはフレームタグで示された VLAN にこのフレームを渡します。ただし、このスイッチが VLAN 非対応デバイスからタグなしフレームを受信すると、最初にフレームを転送する場所を決定し、次に入力ポートのデフォルト VID を反映する VLAN タグを挿入します。

5.1.1 VLAN グループの設定

[VLAN]> [Static（Add）]ページを使用して、VLAN グループの作成または削除、管理ステータスの設定、またはリモート VLAN タイプの指定を行います（「4.5 リモートポートミラーリングの設定」を参照してください）。このスイッチで使用されている VLAN グループに関する情報を外部ネットワークデバイスに伝播するには、これらのグループごとに VLAN ID を指定する必要があります。

パラメータ

次のパラメータが表示されます。

Add

- VLAN ID - VLAN の ID または VLAN の範囲です（1 から 4094）。
  VLAN 1 がデフォルトのタグなし VLAN です。
- Status - 指定された VLAN を有効または無効にします。
- Remote VLAN - RSPAN にこの VLAN を予約します。

Modify

- VLAN ID - 設定済み VLAN の ID です（1 から 4094）。
- VLAN Name - VLAN の名前です（1 から 32 文字）。
- Status - 指定された VLAN を有効または無効にします。
- L3 Interface - レイヤ 3 設定をサポートするようにインタフェースを設定し、このインタフェースタイプに関する追加情報を維持するために必要なメモリスペースを予約します。このパラメータは、VLAN に IP アドレスを割当てる前に有効にする必要があります（「15.1　スイッチの IP アドレスを設定（IP Version 4）」を参照してください）。VLAN4094 の L3 Interface を有効にした場合、VLAN4094 の L3 Interface で ND DAD Attempts が無効に自動設定されることがありますが、動作や通信に影響はありません。

Show

- VLAN ID - 設定済み VLAN の ID です。
- VLAN Name - VLAN の名前です。
- Status - 設定済みの VLAN の動作ステータスです。
- Remote VLAN - この VLAN で RSPAN が有効になっているかどうかを示します。
- L3 Interface - インタフェースがレイヤ 3 設定をサポートしているかどうかを示します。

Web インタフェース

VLAN グループを作成するには：

1. [VLAN]、[Static]をクリックします。
2. [Action]リストから[Add]を選択します。
3. VLAN ID または ID の範囲を入力します。
4. ステータスを確認して、VLAN を動作可能に設定します。
5. リモートポートミラーリングに VLAN を使用するかどうかを指定します。
6. [Apply]をクリックします。

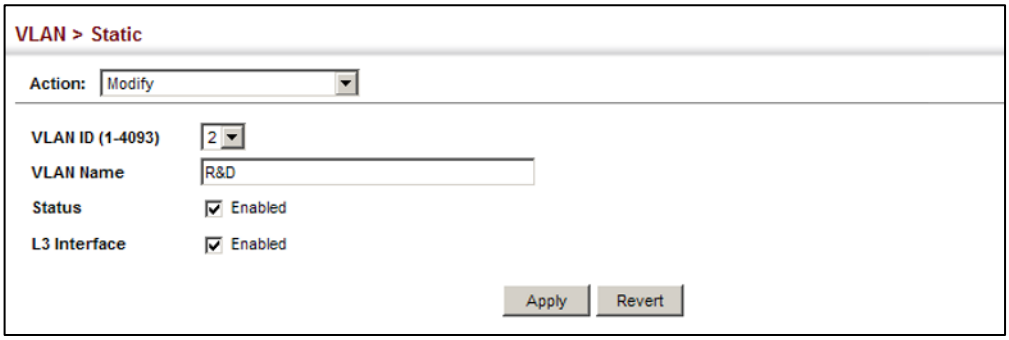
図 5-2　静的 VLAN の作成

VLAN グループの設定を変更するには：

1. [VLAN]、[Static]をクリックします。
2. [Action]リストから[Modify]を選択します。

3. 設定済みの VLAN の識別子を選択します。
4. 必要に応じて、VLAN 名または動作ステータスを変更します。
5. L3 インタフェースフィールドを有効にして、VLAN をレイヤ 3 インタフェースとして使用するように指定します。
6. [Apply]をクリックします。

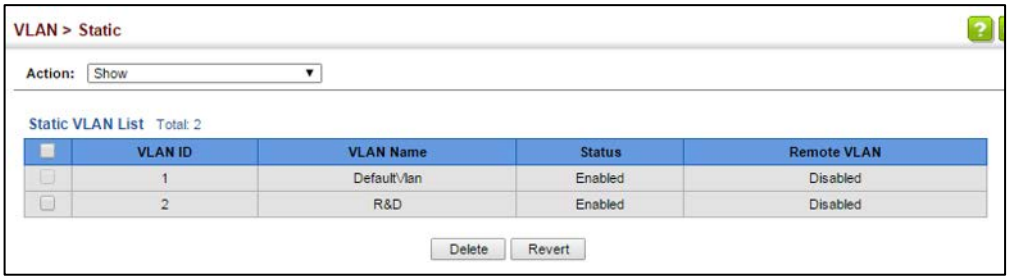
図 5-3 静的 VLAN の設定の変更



VLAN グループの設定を表示するには、次の手順を実行します。

1. [VLAN]、[Static]をクリックします。
2. [Action]リストから[Show]を選択します。

図 5-4 静的 VLAN の表示



5.1.2 VLAN に静的メンバーを追加

選択した VLAN インデックス、インタフェース、またはインタフェースの範囲のポートメンバーを設定するには、[VLAN]>[Static（Edit Member by VLAN、Edit Member by Interface、または Edit Member by Interface Range）]を使用します。操作モード（ハイブリッドまたは 1Q トランク）、デフォルト VLAN 識別子（PVID）、受け入れられたフレームタイプ、入力フィルタリングなど、特定のインタフェースの VLAN 動作を設定するには、ポートメンバーを編集するためのメニューを使用します。ポートが 802.1Q VLAN 準拠のデバイスに接続されているかタグなしのポートが VLAN 対応デバイスに接続されていない場合は、タグ付きとして割当てます。

パラメータ

次のパラメータが表示されます。

Edit Member by VLAN

- VLAN - 設定済み VLAN の ID です（1 から 4094）。
- Interface - ポートまたはトランクのリストを表示します。
- Port - ポート番号です。(範囲: 1 から 10)
- Trunk - トランク識別子です。(範囲: 1-8)

- Mode - インタフェースの VLAN メンバーシップモードを示します。(デフォルト: Hybrid)
  - Access - ポートがタグなしインタフェースとして動作するように設定します。ポートはタグ無しフレームを単一 VLAN でのみ送受信します。
  - Hybrid - ハイブリッド VLAN インタフェースを指定します。ポートはタグ付きまたはタグ無しフレームを送信します。
  - 1Q Trunk - ポートを VLAN トランクのエンドポイントとして指定します。トランクは 2 つのスイッチ間の直接リンクなので、ポートは送信元 VLAN を識別するタグ付きフレームを送信します。ポートのデフォルト VLAN に属する(例; PVID に関連付けられた)フレームも、タグ付きフレームとして送信されることに留意してください。
- PVID - インタフェース上で受信したタグなしフレームに割当てられた VLAN ID です。(デフォルト: 1)
  アクセスモードを使用してインタフェースが新しい VLAN に割当てられると、その VLAN の PVID が自動的にその VLAN の識別子に設定されます。ハイブリッドモードを使用する場合、インタフェースの PVID はタグ無しメンバーである任意の VLAN に設定できます。
- Acceptable Frame Type - タグ付きフレームまたはタグなしフレーム、またはタグ付きフレームのみを含むすべてのフレームタイプを受け入れるようにインタフェースを設定します。全フレームタイプを受け入れるよう設定した際、受け入れたすべてのタグ無しフレームは、デフォルト VLAN に割当てられます。(オプション: All, Tagged; Default: All)
- Membership Type - ポートまたはトランクに適切なラジオボタンをマーキングして、各インタフェースの VLAN メンバーシップを選択します。
  - Tagged: インタフェースは VLAN のメンバーです。ポートによって送信されたすべてのパケットにタグが付けられます。つまり、タグを運ぶため、VLAN または CoS 情報が伝送されます。
  - Untagged: インタフェースは VLAN のメンバーです。ポートによって送信されるすべてのパケットはタグなし、つまりタグを持たないため、VLAN または CoS 情報は伝送されません。少なくとも 1 つのグループにタグなしポートとしてインタフェースを割当てる必要があることに注意してください。
  - Forbidden: インタフェースを VLAN のメンバーとして含めることはできません。
  - None: インタフェースは VLAN のメンバーではありません。この VLAN に関連付けられたパケットは、インタフェースによって送信されません。

Note: VLAN 1 は、ハイブリッドモードを使用するスイッチ上のすべてのポートを含むデフォルトのタグなし VLAN です。

Edit Member by Interface

各パラメータの説明は、Edit Member by VLAN を参照してください。

Edit Member by Interface Range

以下に示す項目を除き、各パラメータの説明は、Edit Member by VLAN を参照してください。

- Port Range - ポートのリストを表示します。(範囲: 1 から 10)
- Trunk Range - ポートのリストを表示します。(範囲: 1-8)

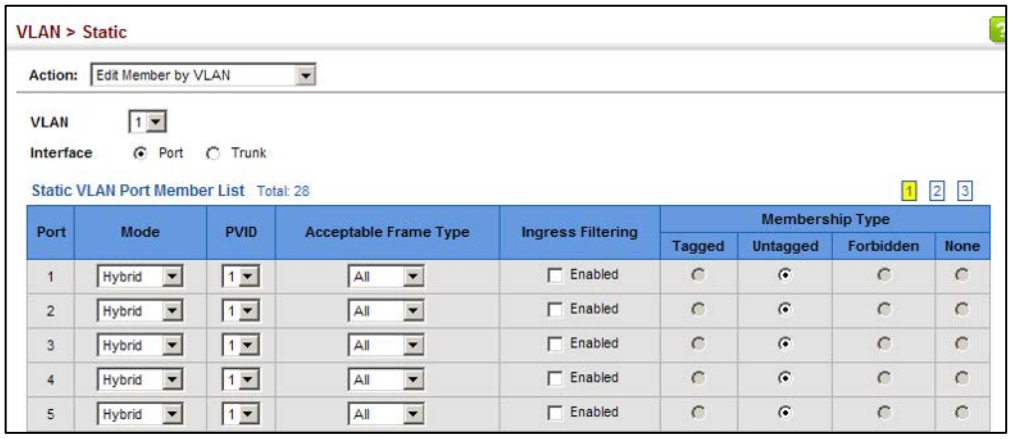
Note: 指定範囲内の各インタフェースの PVID、許容フレームタイプ、および入力フィルタリングパラメータは、[Edit Member by VLAN]または[Edit Member by Interface]ページで設定する必要があります。

Web インタフェース

VLAN インデックスで静的メンバーを設定するには、次の手順を実行します。

1. [VLAN]、[Static]をクリックします。
2. [Action]リストから[Edit Member by VLAN]を選択します。
3. スクロールダウンリストから VLAN を選択します。
4. インタフェースタイプをポートまたはトランクとして表示するように設定します。
5. 必要に応じて、任意のインタフェースの設定を変更します。
6. [Apply]をクリックします。

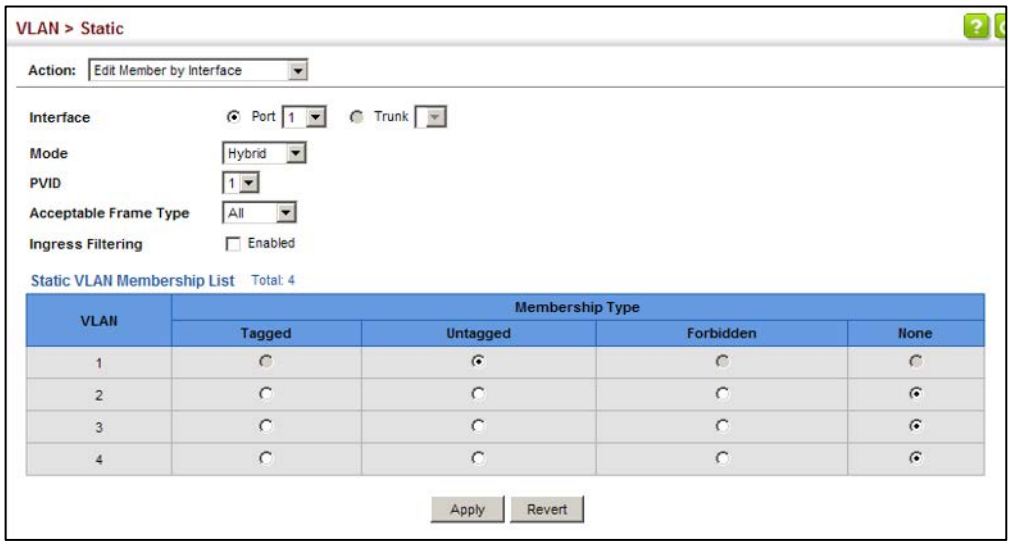
図 5-5 VLAN インデックスによる静的メンバーの設定



インタフェースで静的メンバーを設定するには：

1. [VLAN]、[Static]をクリックします。
2. [Action]リストから[Edit Member by Interface]を選択します。
3. ポートまたはトランクの設定を選択します。
4. 必要に応じて、任意のインタフェースの設定を変更します。
5. [Apply]をクリックします。

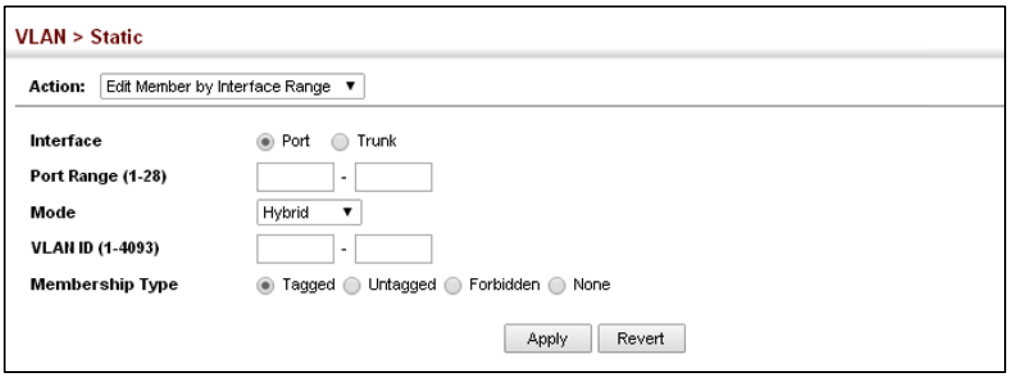
図 5-6 インタフェースによる静的 VLAN メンバーの設定



インタフェース範囲で静的メンバーを設定するには：

1. [VLAN]、[Static]をクリックします。
2. [Action]リストから[Edit Member by Interface Range]を選択します。
3. インタフェースタイプをポートまたはトランクとして表示するように設定します。
4. インタフェースの範囲を入力します。
5. 必要に応じて VLAN パラメータを変更します。指定した範囲内の各インタフェースの PVID、許容フレームタイプ、および入力フィルタリングパラメータは、[Edit Member by VLAN]または[Edit Member by Interface]ページで設定する必要があります。
6. [Apply]をクリックします。

図 5-7 インタフェース範囲による静的 VLAN メンバーの設定



5.2 IEEE 802.1Q トンネリング

IEEE 802.1Q トンネリング（QinQ）は、ネットワーク上の複数の顧客に対してトラフィックを伝送するサービスプロバイダ向けに設計されています。QinQ トンネリングは、異なる顧客が同じ内部 VLAN ID を使用する場合でも、顧客固有の VLAN およびレイヤ 2 プロトコル構成を維持するために使用されます。これは、サービスプロバイダのネットワークに入るときにカスタマーのフレームに Service Provider VLAN（SPVLAN）タグを挿入し、フレームがネットワークを離れるときにタグを取り除くことによって実現されます。

サービスプロバイダの顧客は、内部 VLAN ID とサポートされている VLAN の数について特定の要件を持つ場合があります。同じサービスプロバイダネットワーク内の異なる顧客が必要とする VLAN 範囲は容易に重複し、インフラストラクチャを通過するトラフィックは混在する可能性があります。各顧客に一意の VLAN ID を割当てることで、顧客の構成が制限され、VLAN マッピングテーブルの処理が集中し、最大 VLAN 制限 4094 を簡単に超える可能性があります。

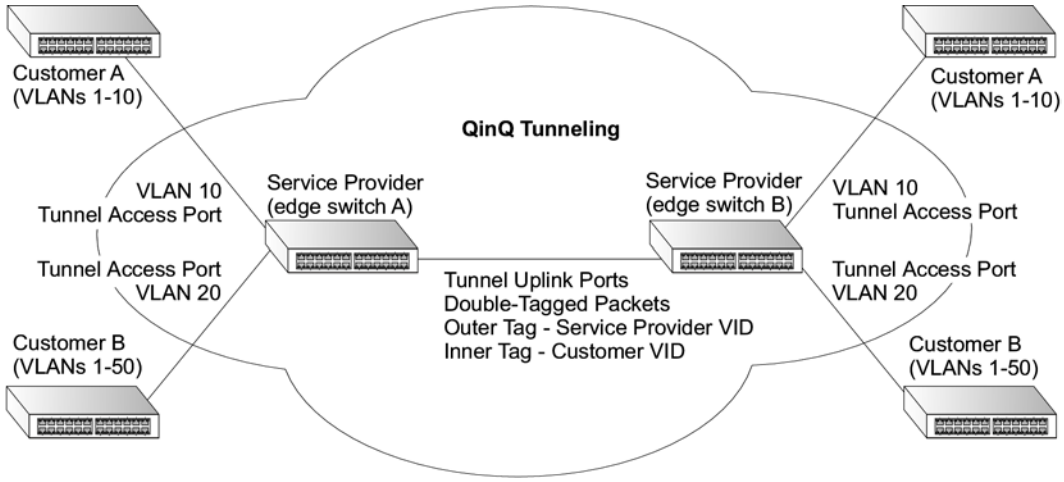
QinQ トンネリングは、複数の VLAN を持つ顧客に対して単一のサービスプロバイダ VLAN（SPVLAN）を使用します。同じ顧客固有の VLAN ID を使用している場合でも、カスタマーVLAN ID は保持され、異なる顧客からのトラフィックはサービスプロバイダのネットワーク内で分離されます。QinQ トンネリングは、VLAN-in-VLAN 階層を使用し、顧客の元のタグ付きパケットを保存し、各フレームに SPVLAN タグを追加することによって VLAN スペースを拡張します(ダブルタギングとも呼ばれます)。

QinQ トンネリングをサポートするように設定されたポートは、トンネルポートモードに設定する必要があります。特定の顧客のサービスプロバイダ VLAN（SPVLAN）ID は、カスタマートラフィックがサービスプロバイダのネットワークに入るエッジスイッチの QinQ トンネルアクセスポートに割当てる必要があります。各顧客は個別の SPVLAN を必要としますが、この VLAN はすべての顧客の内部 VLAN をサポートします。エッジスイッチからサービスプロバイダのメトロネットワークにトラフィックを渡す QinQ トンネルアップリンクポートもこの SPVLAN に追加する必要があります。アップリンクポートを複数の SPVLAN に追加して、異なる顧客のインバウンドトラフィックをサービスプロバイダのネットワークに伝送することができます。

ダブルタグパケットがサービスプロバイダのネットワーク内の中間またはコアスイッチの別のトランクポートに入ると、パケット処理のために外部タグが取り除かれます。パケットが同じコアスイッチ上の別のトランクポートを終了すると、同じ SPVLAN タグがパケットに再度追加されます。

パケットがサービスプロバイダの出口スイッチのトランクポートに入ると、パケット処理のために外部タグが再び取り除かれます。ただし、SPVLAN タグは、エッジスイッチ上のトンネルアクセスポートから顧客のネットワークに送信されるときには追加されません。パケットは、通常の IEEE 802.1Q タグ付きフレームとして送信され、顧客のネットワークで使用されていた元の VLAN 番号が保持されます。

図 5-8 QinQ の運用コンセプト



トンネルアクセスポートに受信するパケットのレイヤ 2 フロー

QinQ トンネルポートは、タグ付きパケットまたはタグなしパケットのいずれかを受信することがあります。受信パケットのタグ数にかかわらず、タグ付きパケットとして扱われます。

受信プロセスは、送信元と宛先の検索を行います。両方の検索が成功した場合、受信プロセスはパケットをメモリに書き込みます。その後、送信プロセスはパケットを送信します。QinQ トンネルポートに入るパケットは、次のように処理されます。

1. SPVLAN タグは、SPVLAN インタフェース上のすべての送信パケットに追加されます（すでにタグがいくつあるにかかわらず）。スイッチは、デフォルト VLAN ID およびタグプロトコル識別子（TPID、つまりタグの ether-type）にもとづいて、外部タグ（SPVLAN）を構築してパケットに挿入します。.内部タグの優先順位は、タグ付きパケットまたは優先タグ付きパケットであれば外側タグにコピーされます。
2. 送信元と宛先の検索が成功した後、送信プロセスはパケットを 2 つのタグを使用してスイッチングプロセスに送信します。受信パケットがタグなしの場合、外側のタグは SPVLAN タグで、内側のタグはダミーのタグ（8100 0000）です。受信パケットがタグ付けされている場合、外側のタグは SPVLAN タグで、内側のタグは CVLAN タグです。
3. スイッチングプロセスによるパケット分類後、パケットは 1 つのタグ（外側のタグ）または 2 つのタグ（外側のタグと内側のタグの両方）でメモリに書き込まれます。
4. スイッチはパケットを適切な出力ポートに送信します。
5. 出力ポートが SPVLAN のタグなしメンバーの場合、外側のタグは削除されます。タグ付きメンバの場合、送信パケットには 2 つのタグがあります。

トンネルアップリンクポートに受信するパケットのレイヤ 2 フロー

アップリンクポートは、次のいずれかのパケットを受信します。

- Untagged
- One tag (CVLAN or SPVLAN)
- Double tag (CVLAN + SPVLAN)

受信プロセスは、送信元と宛先の検索を行います。両方の検索が成功した場合、受信プロセスはパケットをメモリに書き込みます。その後、送信プロセスはパケットを送信します。QinQ アップリンクポートに入るパケットは、次のように処理されます。

1. 受信パケットがタグなしの場合、PVID VLAN ネイティブタグが追加されます。

2. 受信パケット（単一または二重タグ付き）の ether-type がアップリンクポートの TPID と等しくない場合、VLAN タグはカスタマーVLAN（CVLAN）タグであると判断されます。アップリンクポートの PVID VLAN ネイティブタグがパケットに追加されます。この外部タグは、サービスプロバイダのネットワーク内でパケットを学習およびスイッチングするために使用されます。TPID はポートごとに設定する必要があり、検証を無効にすることはできません。
3. 受信パケット（シングルタグまたはダブルタグ）の ether-type がアップリンクポートの TPID と等しい場合、新しい VLAN タグは追加されません。アップリンクポートが受信パケットの外部 VLAN のメンバーでない場合、パケットは廃棄されます。VLAN が VLAN テーブルにリストされていない場合、パケットは廃棄されます。
4. 送信元と宛先の検索が正常に終了すると、パケットにはダブルタグが付けられます。スイッチは、0x8100 の TPID を使用して、受信パケットが二重タグ付けされていることを示します。受信ダブルタグパケットの外側タグがポート TPID と等しく、内側タグが 0x8100 の場合、ダブルタグ付きパケットとして扱われます。単一タグ付きパケットの TPID が 0x8100 でポート TPID が 0x8100 でない場合は、新しい VLAN タグが追加され、二重タグ付きパケットとしても扱われます。
5. 宛先アドレス検索に失敗した場合、パケットは外部タグの VLAN のすべてのメンバーポートに送信されます。
6. パケット分類の後、パケットはシングルタグまたはダブルタグのパケットとして処理するためにメモリに書き込まれます。
7. スイッチはパケットを適切な出力ポートに送信します。
8. 出力ポートが SPVLAN のタグなしメンバーの場合、外側のタグは削除されます。タグ付きメンバーの場合には、出力パケットには 2 つのタグが付きます。

QinQ 設定上の制限

- アップリンクポートのネイティブ VLAN を SPVLAN として使用しないでください。SPVLAN がアップリンクポートのネイティブ VLAN である場合、アップリンクポートは SPVLAN のタグなしメンバーでなければなりません。パケットが送信されると、外側の SPVLAN タグが削除されます。別の理由は、非顧客パケットが SPVLAN に転送される原因になります。
- 静的トランクポートグループは、QinQ 設定がトランクポートグループ内で一致する限り、QinQ トンネルポートと互換性があります。
- ネイティブ VLAN（VLAN 1）は通常、送信フレームに追加されません。カスタマートラフィックの SPVLAN タグとして VLAN 1 を使用しないでください。使用しないことにより誤った設定のリスクを軽減します。代わりに、サービスプロバイダネットワーク内のデータ VLAN ではなく、管理 VLAN として VLAN 1 を使用してください。
- レイヤ 2 スイッチングとレイヤ 3 スイッチングの間には、いくつかの固有の非互換性があります。
  - トンネルポートは IP アクセスコントロールリストをサポートしていません。
  - レイヤ 3 情報を含むレイヤ 3 QoS（Quality of Service）およびその他の QoS 機能は、トンネルポートではサポートされていません。
  - スパニングツリーブリッジプロトコルデータユニット（BPDU）フィルタリングは、トンネルポートで自動的に無効になります。

QinQ の一般的な設定ガイドライン

1. トンネルステータスを有効にし、トンネルアクセスポートの Tag Protocol Identifier（TPID）値を（Ethernet Type フィールドに）設定します。この手順は、接続されたクライアントが 802.1Q タグ付きフレームを識別するために非標準の 2 バイトの ethertype を使用している場合に必要です。デフォルトの ethertype 値は 0x8100 です。

2. SPVLAN とも呼ばれるサービスプロバイダ VLAN を作成します。
3. QinQ トンネルアクセスポートをアクセスモードに設定します。
4. タグなしメンバーとして SPVLAN に参加するように QinQ トンネルアクセスポートを設定します。
5. SPVLAN ID を QinQ トンネルアクセスポートのネイティブ VID として設定します。
6. QinQ トンネルアップリンクポートをアップリンクモードに設定する。
7. QinQ トンネルアップリンクポートを設定して、SPVLAN をタグ付きメンバーとして参加させます。

5.2.1 スイッチでの QinQ トンネリングの有効化

[VLAN]> [Tunnel（Configure Global）]ページを使用して、スイッチが IEEE 802.1Q（QinQ）トンネリングモードで動作するように設定します。このモードは、サービスプロバイダのメトロポリタンエリアネットワーク上でレイヤ 2 トラフィックを渡すために使用されます。また、接続されたクライアントが 802.1Q タグ付きフレームを識別するために非標準の 2 バイトの ethertype を使用している場合、トンネルポートの Tag Protocol Identifier（TPID）値をグローバルに設定することもできます。

パラメータ

次のパラメータが表示されます。

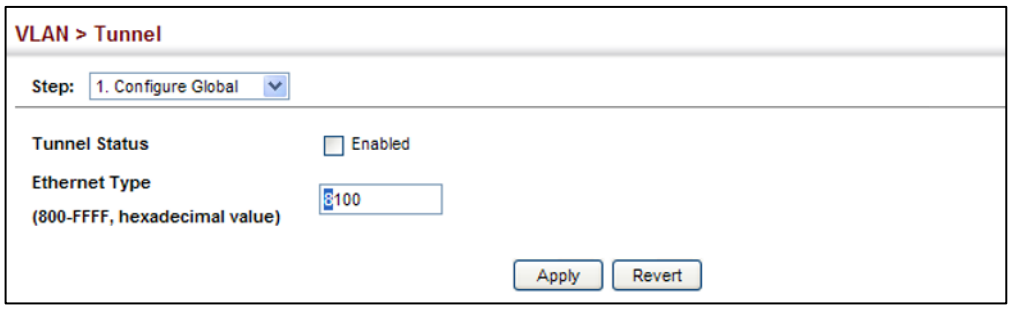
- Tunnel Status - スイッチを QinQ モードに設定します。(デフォルト: Disabled)
- Ethernet Type - タグプロトコル識別子（TPID）は、トンネルポート上の受信パケットの Ethernet Type(ethertype)を指定します。(範囲：16 進数 0800 から FFFF; デフォルト: 8100)
  このフィールドを使用して、802.1Q トンネル TPID のカスタム 802.1Q ethertype 値を設定します。この機能により、スイッチは 802.1Q タグ付きフレームを識別するために標準の 0x8100 ethertype を使用しないサードパーティのスイッチと相互運用できます。たとえば、0x1234 がトランクポート上のカスタム 802.1Q ethertype として設定されている場合、その ethertype を含む受信フレームは、ethertype フィールドに続くタグに含まれる VLAN に割当てられます。標準の 802.1Q トランクと同様です。標準の 802.1Q トランクと同様です。 他の ethertype を含むポートに到着したフレームは、タグなしフレームとみなされ、そのポートのネイティブ VLAN に割当てられます。
  指定された ethertype は、アップリンクモードで設定されたポートにのみ適用されます。ポートが通常モードの場合、TPID は常に 8100 です。ポートがアクセスモードの場合、受信パケットはタグなしパケットとして処理されます。
  すべての副作用を排除できない限り、TPID によく知られた ethertype を使用しないでください。たとえば、TPID を 16 進数の 0800（IPv4 に使用）に設定すると、Web インタフェースを介した管理アクセスが妨げられます。

Web インタフェース

スイッチ上での QinQ トンネリングを有効にするには：

1. [VLAN]、[Tunnel]をクリックします。
2. [Step]リストから[Configure Global]を選択します。
3. トンネルステータスを有効にし、トンネルポートに接続されているクライアントが非標準の Ethertype を使用して 802.1Q タグ付きフレームを識別している場合は、TPID を指定します。
4. [Apply]をクリックします。

図 5-9 QinQ トンネリングの有効化



5.2.2 QinQ トンネルへのインタフェースの追加

スイッチに QinQ トンネルを設定するには、前項のガイドラインに従ってください。次に、[VLAN]> [Tunnel（Configure Interface）]ページを使用して、参加しているインタフェースのトンネルモードを設定します。

コマンドの使用方法

- [Configure Global]ページを使用して、トンネルアクセスポートまたはトンネルアップリンクポートを設定する前にスイッチを QinQ モードに設定します。また、接続されたクライアントが非標準の 2 バイトの ethertype を使用して 802.1Q タグ付きフレームを識別している場合は、トンネルアクセスポートのタグプロトコル識別子（TPID）値を設定します。
- 次に、[Configure Interface]ページを使用して、エッジスイッチのアクセスインタフェースをアクセスモードに設定し、サービスプロバイダネットワークに接続されているスイッチのアップリンクインタフェースをアップリンクモードに設定します。

パラメータ

次のパラメータが表示されます。

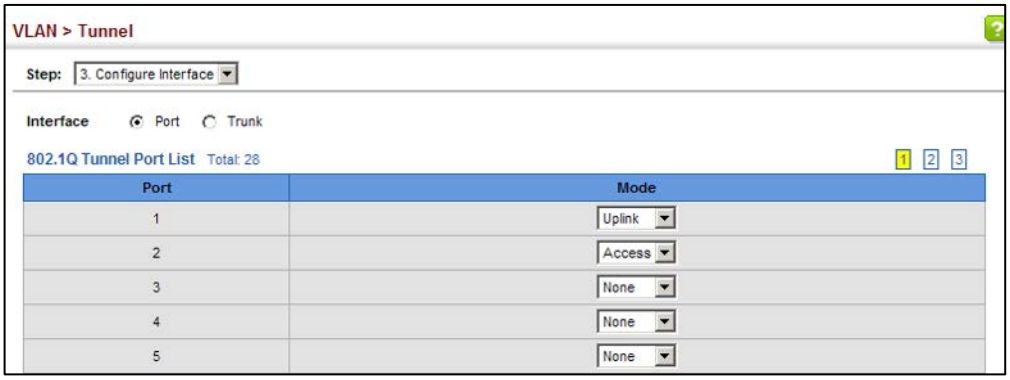
- Interface - ポートまたはトランクのリストを表示します。
- Port - ポート番号です。(範囲: 1 から 10)
- Trunk - トランク識別子です。(範囲: 1-8)
- Mode - ポートの VLAN メンバーシップモードを設定します。
  - None - ポートは通常の VLAN モードで動作します。(これがデフォルトです。)
  - Access - クライアントアクセスポートの QinQ トンネリングを設定して、サービスプロバイダネットワークを通過するトラフィックのカスタマーVLAN ID を分離して保存します。
  - Uplink - サービスプロバイダネットワーク内の別のデバイスへのアップリンクポートの QinQ トンネリングを設定します。

Web インタフェース

QinQ トンネルにインタフェースを追加するには：

1. [VLAN]、[Tunnel]をクリックします。
2. [Step]リストから[Configure Interface]を選択します。
3. 任意のトンネルアクセスポートのモードを Access に設定し、トンネルアップリンクポートを Uplink に設定します。
4. [Apply]をクリックします。

図 5-10　QinQ トンネルへのインタフェースの追加



5.3 プロトコル VLAN

複数のプロトコルをサポートするために必要なネットワークデバイスは、共通の VLAN に簡単にグループ化することはできません。これは、特定のプロトコルに参加するすべてのデバイスを包含するために、非標準デバイスが異なる VLAN 間でトラフィックを通過することを必要とする場合があります。この種の設定では、セキュリティと簡単なアクセシビリティを含め、VLAN の基本的な利点がユーザに奪われます。

これらの問題を回避するには、物理ネットワークを必要なプロトコルごとに論理 VLAN グループに分割するプロトコルベースの VLAN でこのスイッチを構成します。フレームがポートで受信されると、その VLAN メンバーシップは、受信パケットによって使用されているプロトコルタイプにもとづいて決定されます。

コマンドの使用方法

- プロトコルベースの VLAN を設定する手順は、次のとおりです。:
  1. まず、使用するプロトコルの VLAN グループを設定します。必須ではありませんが、ネットワーク上で動作する主要なプロトコルごとに別々の VLAN を設定することをお勧めします。この時点でポートメンバーを追加しないでください。
  2. [Configure Protocol（Add）]ページを使用して、VLAN に割当てるプロトコルごとにプロトコルグループを作成します。
  3. 次に、[Configure Protocol（Add）]ページを使用して、各インタフェースのプロトコルを適切な VLAN にマッピングします。
- MAC ベース VLAN、またはプロトコルベース VLAN が同時にサポートされている場合、このシーケンスで優先順位が適用され、ポートベースの VLAN が最後に適用されます。

5.3.1 プロトコル VLAN グループの設定

[VLAN]> [Protocol（Configure Protocol - Add）]ページを使用してプロトコルグループを作成します。

パラメータ

次のパラメータが表示されます。

- Frame Type - このプロトコルで使用されるフレームタイプとして、Ethernet、RFC 1042、または LLC Other のいずれかを選択します。
- Protocol Type - 一致させるプロトコルタイプを指定します。使用可能なオプションは、IP、ARP、RARP、PPPOE-DIS、PPPOE-SES、および IPv6 です。フレームタイプとして LLC Other を選択した場合、使用可能なプロトコルタイプは IPX Raw のみです。
- Protocol Group ID - プロトコル VLAN グループに割当てられたプロトコルグループ ID です。(範囲: 1 から 2147483647)

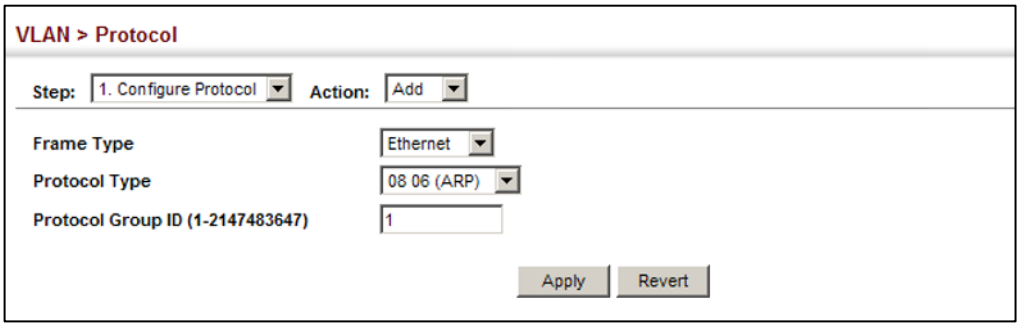
Note: IP プロトコルイーサネットフレームに一致するトラフィックは、スイッチの管理 IP で設定された VLAN（VLAN 1）にマッピングされます。IP プロトコルイーサネットトラフィックを別の VLAN にマッピングすることはできません。そうしないと、スイッチへの管理ネットワーク接続が失われます。この方法で紛失した場合、コンソールから違反しているプロトコル VLAN ルールを削除することで、ネットワークアクセスを回復できます。あるいは、スイッチの電源を切ることもできますが、保存されていない設定変更はすべて失われます。

Web インタフェース

プロトコルグループを設定するには：

1. [VLAN]、[Protocol]をクリックします。
2. [Step]リストから[Configure Protocol]を選択します。
3. [Action]リストから[Add]を選択します。
4. [Frame Type]リストからエントリを選択します。
5. [Protocol Type]リストからエントリを選択します。
6. プロトコルグループの識別子を入力します。
7. [Apply]をクリックします。

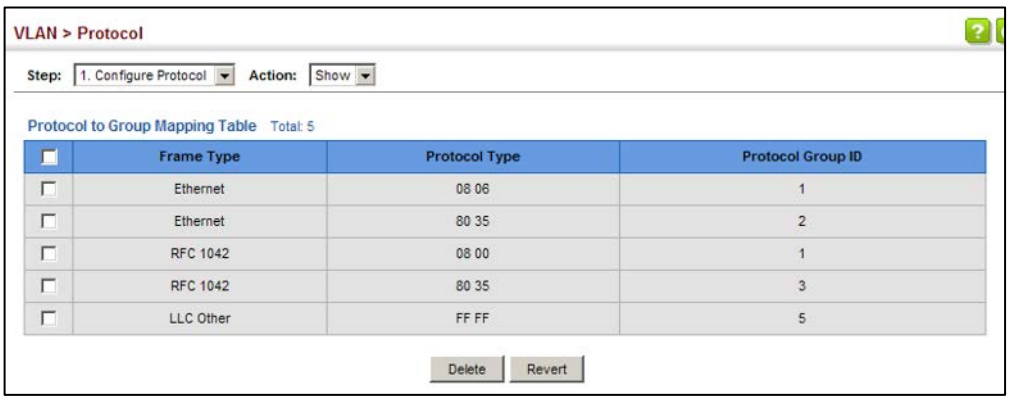
図 5-11 プロトコル VLAN の設定



プロトコルグループを設定するには：

1. [VLAN]、[Protocol]をクリックします。
2. [Step]リストから[Configure Protocol]を選択します。
3. [Action]リストから[Show]を選択します。

図 5-12 プロトコル VLAN の表示



5.3.2 インタフェースへのプロトコルグループのマッピング

[VLAN]> [Protocol（Configure Protocol - Add）]ページを使用して、グループに参加する各インタフェースの VLAN にプロトコルグループをマッピングします。

コマンドの使用方法

◆ プロトコルベースの VLAN を作成する場合、この設定画面を使用してインタフェースを割当てるだけです。VLAN 静的テーブルなどの他の VLAN メニューのいずれかを使用してインタフェースを割当て

る場合、これらのインタフェースは、関連する VLAN に任意のプロトコルタイプのトラフィックを許可します。

- フレームがプロトコル VLAN に割当てられたポートに入ると、次のように処理されます。
  - フレームにタグが付いている場合は、タグ付きフレームに適用されている標準規則に従って処理されます。
  - フレームがタグなしでプロトコルタイプが一致する場合、フレームは適切な VLAN に転送されます。
  - フレームがタグなしでプロトコルタイプが一致しない場合、フレームはこのインタフェースのデフォルト VLAN に転送されます。

パラメータ

次のパラメータが表示されます。

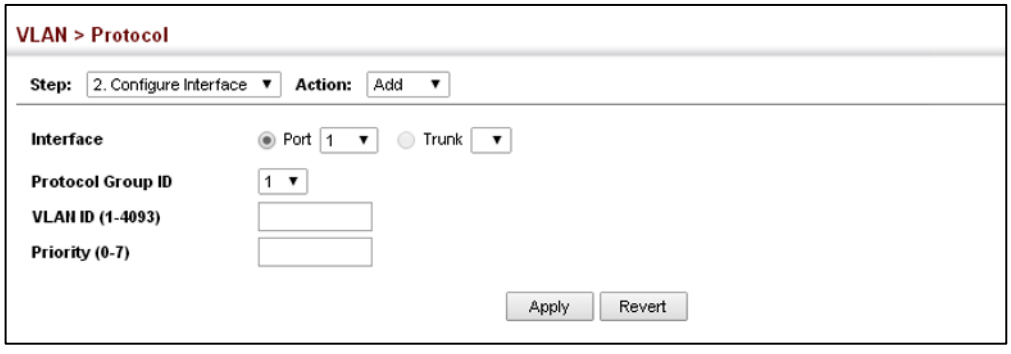
- Interface - ポートまたはトランクのリストを表示します。
- Port - ポート番号です。(範囲: 1 から 10)
- Trunk - トランク識別子です。(範囲: 1-8)
- Protocol Group ID - プロトコル VLAN グループに割当てられたプロトコルグループ ID です。(範囲: 1 から 2147483647)
- VLAN ID - 一致するプロトコルトラフィックが転送される VLAN です。(範囲: 1 から 4094)
- Priority - タグなし入力トラフィックに割当てられた優先順位です。
  (範囲: 0 から 7、7 が最も高い優先順位です)

Web インタフェース

ポートまたはトランクの VLAN にプロトコルグループをマッピングするには：

1. [VLAN]、[Protocol]をクリックします。
2. [Step]リストから[Configure Interface]を選択します。
3. [Action]リストから[Add]を選択します。
4. [Port]または[Trunk]を選択します。
5. プロトコルグループの識別子を入力します。
6. プロトコルトラフィックが転送される対応する VLAN を入力します。
7. タグなし入力フレームに割当てる優先度を設定します。.
8. [Apply]をクリックします。

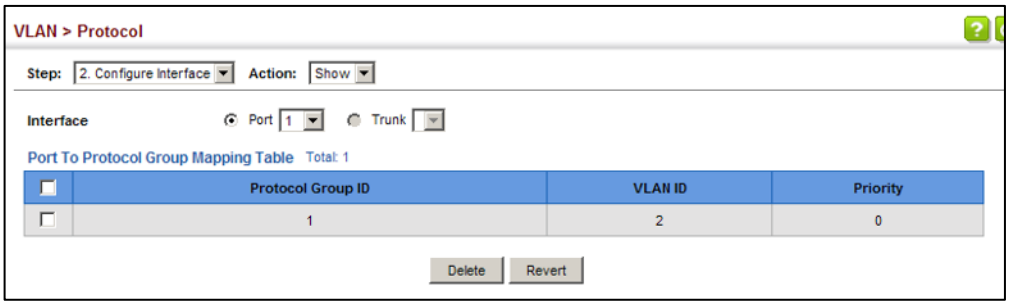
図 5-13 プロトコル VLAN へのインタフェースの割当て



ポートまたはトランクにマッピングされたプロトコルグループを表示するには、次の手順を実行します。

1. [VLAN]、[Protocol]をクリックします。
2. [Step]リストから[Configure Interface]を選択します。
3. [Action]リストから[Show]を選択します。
4. [Port]または[Trunk]を選択します。

図 5-14 プロトコルグループマッピングへのインタフェースの表示



5.4 MAC ベースの VLAN の設定

[VLAN]> [MAC-Based]ページを使用して、MAC アドレスにもとづいて VLAN を設定します。MAC ベース VLAN 機能は、送信元 MAC アドレスに従って、入力タグなしフレームに VLAN ID を割当てます。

MAC ベース VLAN 分類が有効の場合、ポートで受信されたタグなしフレームは、フレームの送信元 MAC アドレスにマップされた VLAN に割当てられます。MAC アドレスが一致しない場合、タグなしフレームは受信ポートのネイティブ VLAN ID（PVID）に割当てられます。

コマンドの使用方法

- MAC から VLAN へのマッピングは、スイッチ上のすべてのポートに適用されます。
- 送信元 MAC アドレスは、1 つの VLAN ID にのみマッピングできます。
- 設定された MAC アドレスはブロードキャストまたはマルチキャストアドレスにすることはできません。
- MAC ベース VLAN、またはプロトコルベース VLAN が同時にサポートされている場合、このシーケンスで優先順位が適用され、ポートベースの VLAN が最後に適用されます。

パラメータ

次のパラメータが表示されます。

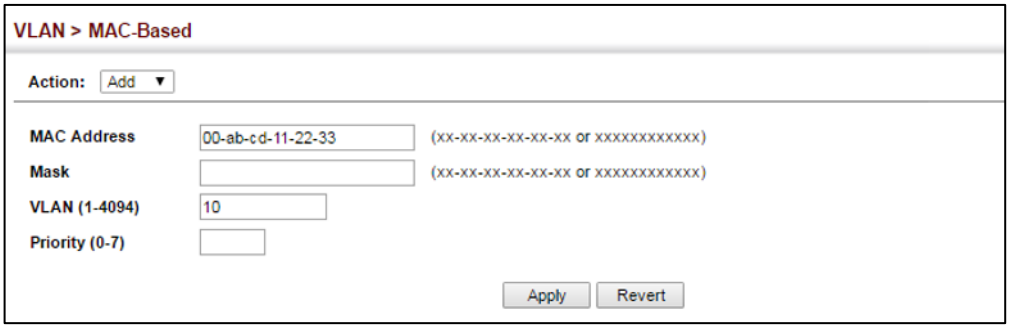
- MAC Address - 特定の VLAN にマッピングされる送信元 MAC アドレスです。MAC アドレスは、xx-xx-xx-xx-xx-xx の形式で指定する必要があります。
- Mask - MAC アドレスの範囲を指定します。(範囲: 00-00-00-00-00-00 から ff-ff-ff-ff-ff-ff)
  最初の非ゼロ文字の前にある文字と一致するバイナリ相当マスクは、すべて 1 でなければなりません（たとえば、111、つまり 101 または 001 にすることはできません）。
  MAC アドレスのマスク：00-12-E2-8F-2C-A7 バイナリに変換：
  MAC: 00000000-00010010-11100010-10001111-00101100-10100111
  になり得る：11111111-1111xxxx-xxxxxxxx-xxxxxxxx-xxxxxxxx-xxxxxxxx
  したがって、この例の 16 進数のマスクは次のようになります。
  ff-fx-xx-xx-xx-xx
- VLAN - 指定された送信元 MAC アドレスに一致する入力トラフィックが転送される VLAN です。(範囲: 1 から 4094)
- Priority - タグなし入力トラフィックに割当てられた優先順位です。(範囲: 0-7、ここで 7 は最高の優先順位です。 デフォルト: 0)

Web インタフェース

VLAN への MAC アドレスをマップするには：

1. [VLAN]、[MAC-Based]をクリックします。
2. [Action]リストから[Add]を選択します。
3. MAC Address フィールドにアドレスを入力し、必要に応じてアドレスの範囲を示すマスクを入力します。
4. VLAN フィールドに識別子を入力します。指定された VLAN は、すでに設定されている必要はありません。
5. 優先度フィールドにタグなしフレームに割当てる値を入力します。
6. [Apply]をクリックします。

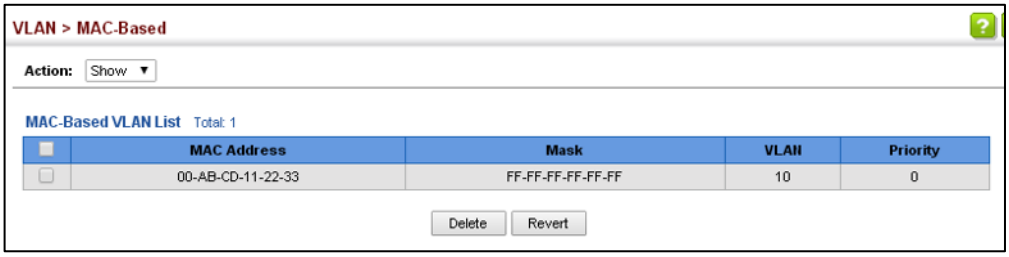
図 5-15 MAC ベース VLAN の設定



VLAN にマッピングされた MAC アドレスを表示するには：

1. [VLAN]、[MAC-Based]をクリックします。
2. [Action]リストから[Show]を選択します。

図 5-16 MAC ベースの VLAN の表示



6 MAC アドレステーブルの設定

スイッチは、既知のすべてのデバイスのアドレスを格納します。この情報は、受信ポートと送信ポート間でトラフィックを直接渡すために使用されます。トラフィックを監視することによって学習されたすべてのアドレスは、動的アドレステーブルに格納されます。また、特定のポートにバインドされた静的アドレスを手動で設定することもできます。

本章では、次のトピックについて説明します。

- Dynamic Address Cache - アドレステーブルに動的エントリを表示します。
- Address Aging Time - 動的に学習されたエントリのタイムアウトを設定します。
- MAC Address Learning - インタフェースのアドレス学習を有効または無効にします。
- Static MAC Addresses - アドレステーブルに静的エントリを設定します。
- MAC Notification Traps - 動的 MAC アドレスの追加または削除時にトラップを発行します。

6.1 動的アドレステーブルの表示

スイッチに入るトラフィックの送信元アドレスを監視して学習した MAC アドレスを表示するには、[MAC Address]> [Dynamic（Show Dynamic MAC）]ページを使用します。受信トラフィックの宛先アドレスがデータベースで見つかると、そのアドレス宛てのパケットは、関連付けられたポートに直接転送されます。それ以外の場合、トラフィックはすべてのポートにフラッディングされます。

パラメータ

次のパラメータが表示されます。

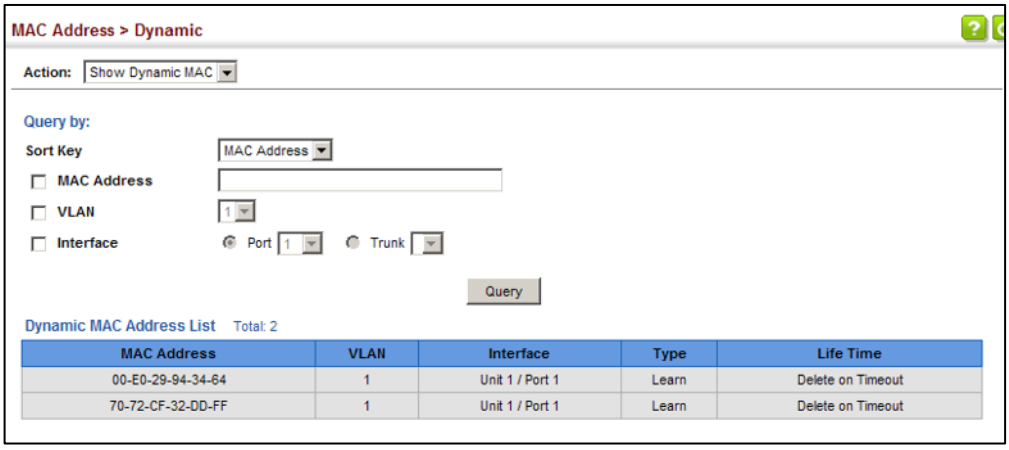
- Sort Key - MAC アドレス、VLAN、またはインタフェース（ポートまたはトランク）にもとづいて表示される情報を並べ替えることができます。
- MAC Address - このインタフェースに関連付けられた物理アドレスです。
- VLAN - 設定済み VLAN の ID です（1 から 4094）。
- Interface - ポートまたはトランクを示します。
- Type - この表のエントリが学習されていることを示します。
  (値: Learn または Security、（ポートセキュリティを示します））
- Life Time - 指定したアドレスを保持する時間を表示します。

Web インタフェース

動的アドレステーブルを表示するには：

1. [MAC Address]、[Dynamic]をクリックします。
2. [Action]リストから[Show Dynamic MAC]を選択します。
3. ソートキー（MAC アドレス、VLAN、またはインタフェース）を選択します。
4. 検索パラメータ（MAC アドレス、VLAN、またはインタフェース）を入力します。
5. [Query]をクリックします。

図 6-1　動的 MAC アドレステーブルの表示



6.2 動的アドレステーブルのクリア

[MAC Address]> [Dynamic（Clear Dynamic MAC）]ページを使用して、学習したエントリを転送データベースから削除します。

パラメータ

次のパラメータが表示されます。

- Clear by - すべてのエントリをクリアすることができます。 あるいは、特定の MAC アドレスのエントリ、VLAN 内のすべてのエントリ、またはポートまたはトランクに関連付けられているすべてのエントリを消去することもできます。

Web インタフェース

動的アドレステーブルのエントリをクリアするには：

1. [MAC Address]、[Dynamic]をクリックします。
2. [Action]リストから[Clear Dynamic MAC]を選択します。
3. エントリをクリアする方法（すべて、MAC アドレス、VLAN、またはインタフェース）を選択します。
4. MAC アドレス、VLAN、またはインタフェースによるエントリのクリアに必要な追加フィールドに情報を入力します。
5. [Clear]をクリックします。

図 6-2　動的 MAC アドレステーブルのエントリのクリア

6.3 エージングタイムの変更

動的アドレステーブルのエントリのエージングタイムを設定するには、[MAC Address]> [Dynamic（Configure Aging）]ページを使用します。エージングタイムは、動的に学習された転送情報のエージングに使用されます。

パラメータ

次のパラメータが表示されます。

- Aging Status - この機能を有効または無効にします。
- Aging Time - 学習されたエントリが破棄されるまでの時間です。(範囲: 6 から 7200 秒、デフォルト: 300 秒)

Web インタフェース

動的アドレステーブルのエントリのエージングタイムを設定するには：

1. [MAC Address]、[Dynamic]をクリックします。
2. [Action]リストから[Configure Aging]を選択します。
3. 必要に応じてエージングステータスを変更します。
4. 新しいエージングタイムを指定します。
5. [Apply]をクリックします。

図 6-3　アドレスエージングタイムの設定

6.4 MAC アドレス学習の設定

[MAC Address]> [Learning Status]ページを使用して、インタフェース上で MAC アドレス学習を有効または無効にします。

コマンドの使用方法

- MAC アドレス学習が無効の場合、スイッチは指定されたインタフェース上で新しい MAC アドレスの学習を直ちに停止します。静的アドレステーブルに格納されている送信元アドレスを持つ受信トラフィックは、そのインタフェースを介してネットワークにアクセスするために承認されたものとして受け入れられます。
- MAC アドレス学習が無効になったときにアドレステーブルに格納された動的アドレスがシステムから消去され、MAC アドレス学習が再度有効になるまで動的アドレスが学習されません。MAC アドレス学習が無効にされた後でインタフェースを使用しようとする静的アドレステーブルに格納されていないデバイスは、スイッチにアクセスできなくなります。
- また、次のいずれかの条件が当てはまる場合、MAC アドレス学習を無効にすることはできません。
  - 同じインタフェース上でセキュリティステータス（「11.7　ポートセキュリティの設定」を参照してください）が有効になっている場合。.

パラメータ

次のパラメータが表示されます。

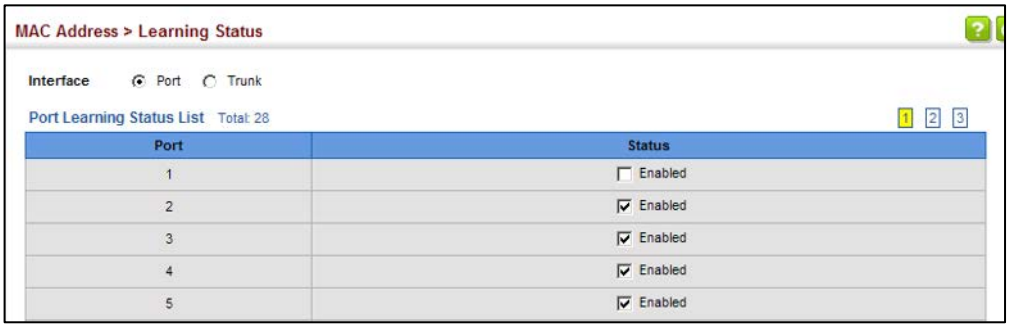
- Interface - ポートまたはトランクのリストを表示します。
- Port - ポート識別子です。(範囲: 1 から 10)
- Trunk - トランク識別子です。(範囲: 1-8)
- Status - MAC アドレス学習のステータスです。(デフォルト: Enabled)

Web インタフェース

MAC アドレス学習を有効または無効にするには :

1. [MAC Address]、[Learning Status]をクリックします。
2. インタフェースの学習ステータスを設定します。
3. [Apply]をクリックします。

図 6-4　MAC アドレス学習の設定



6.5 静的アドレスの設定

静的 MAC アドレスを設定するには、[MAC Address]> [Static]ページを使用します。静的アドレスは、このスイッチの特定のインタフェースに割当てることができます。静的アドレスは割当てられたインタフェースにバインディングし、削除されません。静的アドレスが他のインタフェース上に見られる場合、アドレスは無視されアドレステーブルには書き込まれません。

コマンドの使用方法

ホストデバイスの静的アドレスは、特定 VLAN 内の指定ポートへ割当てることができます。このコマンドを使用して、静的アドレスを MAC Address Table に追加します。静的アドレスには、以下の特徴があります:

- 静的アドレスは割当てられたインタフェースにバインディングし、削除されません。静的アドレスが他のインタフェース上に見られる場合、アドレスは無視されアドレステーブルには書き込まれません。
- 付与されたインタフェースリンクがダウンしている場合、静的アドレスはアドレステーブルから削除されません。
- 静的アドレスは、アドレスがテーブルから削除されるまで、別のポートで学習することはできません。
- 静的 MAC エントリの最大数は 1024 です。

  最大数はポートセキュリティ機能で学習したセキュア MAC アドレス数との合算になります。

パラメータ

次のパラメータが表示されます。

Add Static Address

- VLAN - 設定済み VLAN の ID です。(範囲: 1 から 4094)
- Interface - 静的アドレスが割当てられるデバイスのポートまたはトランクです。
- MAC Address - このインタフェースにマップされたデバイスの物理アドレスです。xx-xx-xx-xx-xx-xx または xxxxxxxxxxxx の形式でアドレスを入力します。
- Static Status - 指定されたアドレスを保持する時間を設定します。
  - Delete-on-reset - スイッチがリセットされるまで割当てが続きます。
  - Permanent - 割当ては永続的です。(これがデフォルトです。)

Show Static Address

この Web ページには、次の追加フィールドが表示されます。

Type - アドレス設定方法を表示します。(値: CPU、Config)

Life Time - このエントリが適用される期間です。(値: Delete On Reset, Permanent)

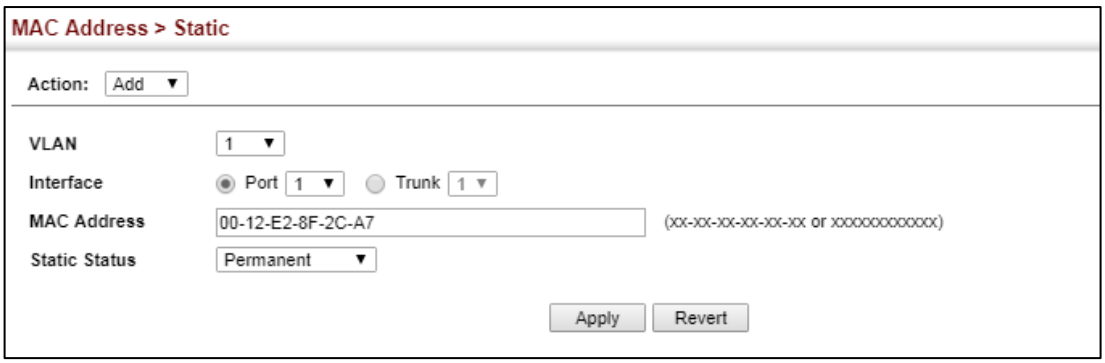
Web インタフェース

静的 MAC アドレスを設定するには :

1. [MAC Address]、[Static]をクリックします。
2. [Action]リストから[Add]を選択します。
3. VLAN、アドレスが割当てられるポートまたはトランク、MAC アドレス、およびこのエントリを保持する時間を指定します。

4.　[Apply]をクリックします。

図 6-5　静的 MAC アドレスの設定

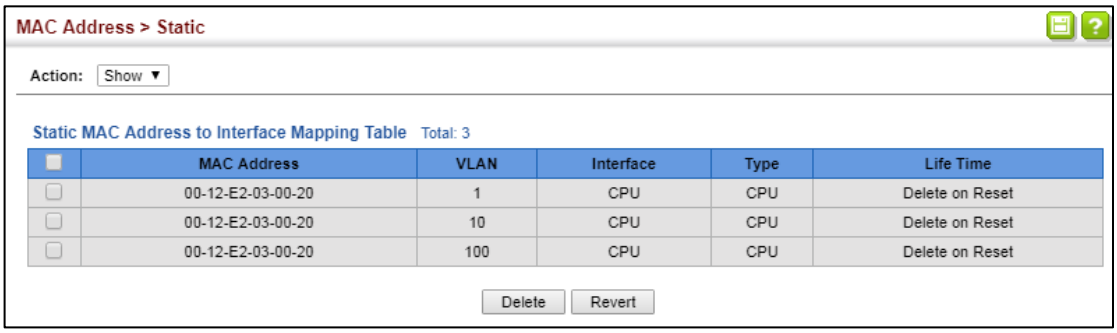


MAC アドレステーブルに静的アドレスを表示するには：

1.　[MAC Address]、[Static]をクリックします。

2.　[Action]リストから[Show]を選択します。

図 6-6　静的 MAC アドレスの表示



6.6 MAC アドレストラップの発行

[MAC Address]> [MAC Notification]ページを使用して、動的 MAC アドレスの追加または削除時に SNMP トラップ（SNMP 通知）を送信します。

パラメータ

次のパラメータが表示されます。

一般設定

- MAC Notification Traps - 動的 MAC アドレスが追加または削除されたときにトラップを発行します。(デフォルト: Disabled)
- MAC Notification Trap Interval - 連続する 2 つのトラップを発行する間隔を指定します。(範囲: 1 から 3600 秒; デフォルト: 1 秒)

Configure Interface

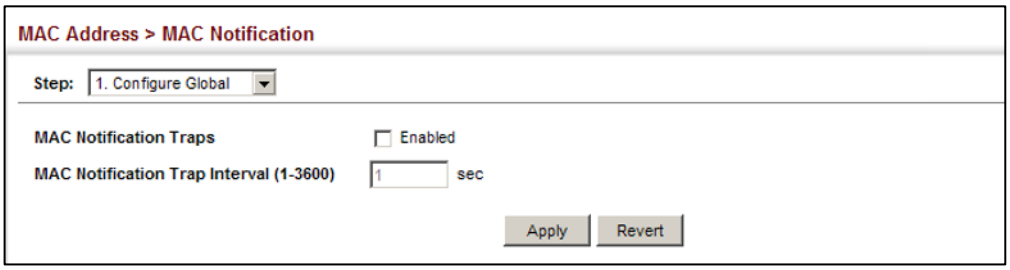
- Port - ポート識別子です。(範囲: 1 から 10)
- MAC Notification Trap - 現在のインタフェース上で MAC アドレストラップを有効にします。(デフォルト: Disabled)
  この属性を有効にするには、MAC アドレストラップをグローバルレベルで有効にする必要があります。

Web インタフェース

グローバルレベルで MAC アドレストラップを有効にするには：

1. [MAC Address]、[MAC Notification]をクリックします。
2. [Step]リストから[Configure Global]を選択します。
3. MAC 通知トラップと送信間隔を設定します。
4. [Apply]をクリックします。

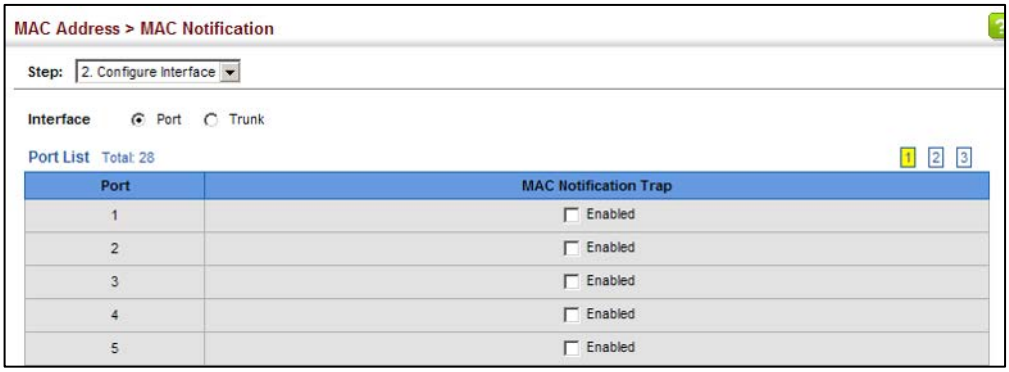
図 6-7　MAC アドレストラップの発行(Configure Global)



インタフェースレベルで MAC アドレストラップを有効にするには、次の手順を実行します。

1. [MAC Address]、[MAC Notification]をクリックします。
2. [Step]リストから[Configure Interface]を選択します。
3. 必要なポートの MAC 通知トラップを有効にします。
4. [Apply]をクリックします。

図 6-8　MAC アドレストラップの発行(Configure Interface)



7 スパニングツリープロトコル

この章では、次の基本的なトピックについて説明します。

- Loopback Detection - ループバック BPDU に対する検出と応答を設定します。
- Global Settings for STA - STP、RSTP、および MSTP のグローバルブリッジを設定します。
- Interface Settings for STA - 優先度、パスコスト、リンクタイプ、エッジポートとしての指定など、STA のインタフェースを設定します。
- Global Settings for MSTP - MST インスタンスに割当てられた VLAN および関連する優先順位を設定します。
- Interface Settings for MSTP - 優先度とパスコストを含む MSTP のインタフェースを設定します。

7.1 概要

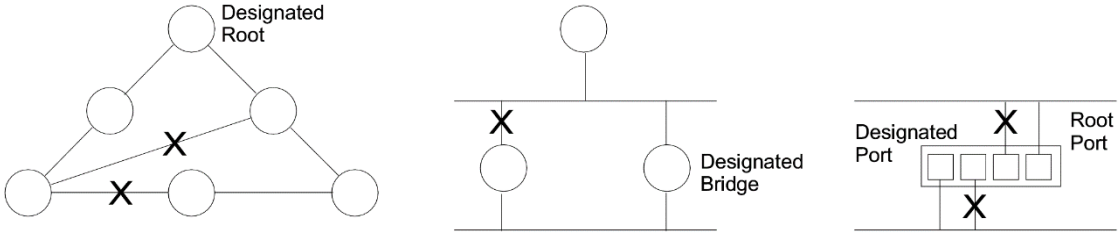
スパニングツリーアルゴリズム(STA)は、ネットワークループの検出と無効化、スイッチ、ブリッジ、ルータ間のバックアップリンクを提供することができます。これにより、スイッチはネットワーク内の他のブリッジングデバイス(STA 準拠のスイッチ、ブリッジ、またはルータ)と連携して、ネットワーク上の 2 つのステーション間で通信経路の冗長化を可能とし、プライマリリンクがダウンするとバックアップリンクに通信経路を切り替えることができます。

このスイッチでサポートされているスパニングツリーアルゴリズムには、次のバージョンがあります。

- STP - スパニングツリープロトコル（IEEE 802.1D）
- RSTP - 高速スパニングツリープロトコル(IEEE 802.1w)
- MSTP - マルチプルスパニングツリープロトコル(IEEE 802.1s)

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）を選択します。次に各ブリッジングデバイス（ルートブリッジデバイスを除く）上のルートポートを選択します。ルートポートは、そのデバイスからルートブリッジデバイスにパケットをフォワーディングするときに最も低いパスコストを発生させます。次に、各 LAN から指定されたブリッジングデバイスを選択します。このブリッジングデバイスは、その LAN からルートブリッジデバイスにパケットをフォワーディングするときに最も低いパスコストを発生させます。指定されたブリッジングデバイスに接続されたすべてのポートは、指定ポートとして割当てられます。ルートポートと指定ポートを決定した後、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。したがって、ネットワークパケットはルートポートと指定されたポート間でのみフォワーディングされるため、ネットワークループが発生する可能性はありません。

図 7-1　STP ルートポートと指定ポート

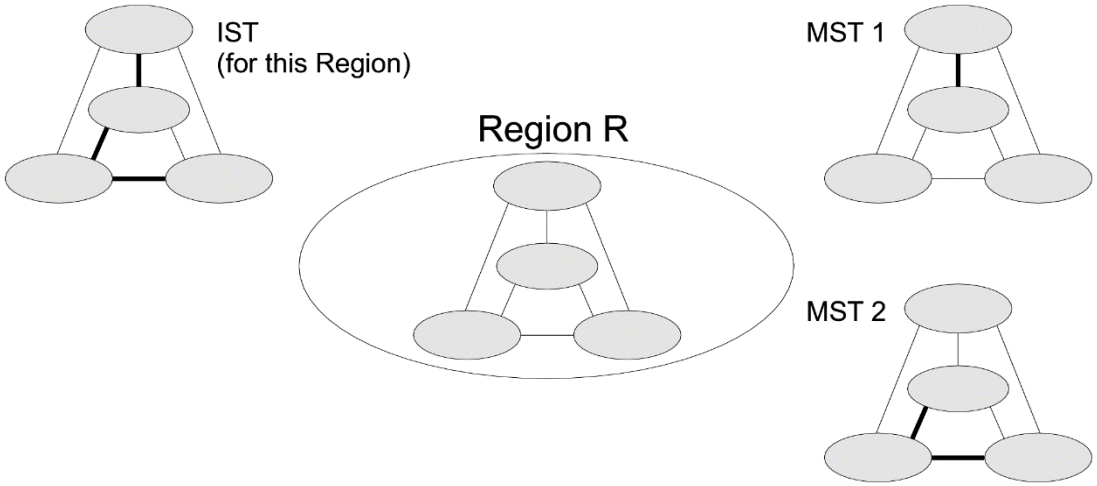


安定したネットワークトポロジが確立されると、すべてのブリッジはルートブリッジから送信された Hello BPDU（ブリッジプロトコルデータユニット）を待ち受けます。ブリッジがあらかじめ定義された間隔（Maximum Age）の後で Hello BPDU を取得しない場合、ブリッジはルートブリッジへのリンクがダウンしているとみなします。このブリッジは、他のブリッジとのネゴシエーションを開始し、ネットワークを再構成して有効なネットワークトポロジを再確立します。

RSTP - RSTP は、より低速のレガシーSTP の一般的な代替品として設計されています。RSTP は MSTP にも組み込まれています。アクティブポートがラーニングを開始する前に状態変化の数を減らすことによって、RSTP ははるかに速い再構成（すなわち、STP の場合 30 秒以上に比べて約 1〜3 秒）を達成し、ノードまたはポートに障害が発生したときに使用できる代替ルートを事前定義し、再構成が発生したときにツリー構造の変化に鈍感なポート用のフォワーディングデータベースを保持します。

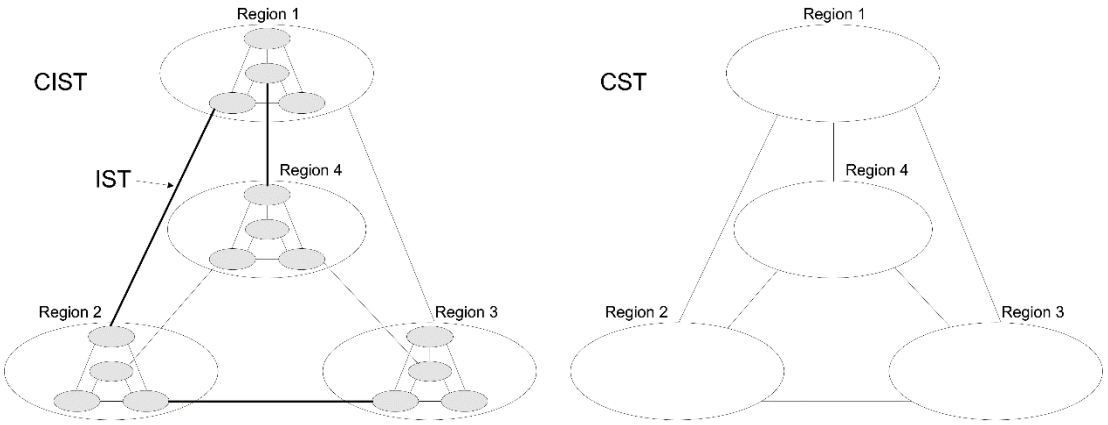
MSTP - マルチプルスパニングツリーを使用すると、複数のフォワーディングパスが提供され、負荷分散が可能になります。1 つ以上の VLAN をマルチプルスパニングツリーインスタンス（MSTI）にグループ化できます。MSTP は、各インスタンスに対して個別のマルチプルスパニングツリー（MST）を構築して、割当てられた各 VLAN グループ間の接続を維持します。次に、MSTP は、すべての一般的に設定された MSTP ブリッジを含むリージョンの内部スパニングツリー（IST）を構築します。

図 7-2 MSTP リージョン、内部スパニングツリー、マルチプルスパニングツリー



MST リージョンは、同じ MST コンフィグレーション識別子を持つ相互接続されたブリッジのグループで構成されています。(リージョン名、リビジョンレベル、構成ダイジェストを含まれます)。MST リージョンには、複数の MSTP インスタンスが含まれる場合があります。内部スパニングツリー（IST）は、MST 領域内のすべての MSTP スイッチを接続するために使用されます。共通スパニングツリー（CST）は、隣接するすべての MST リージョンを相互接続し、グローバルネットワーク内の STP または RSTP ノードと通信するための仮想ブリッジノードとして機能します。

図 7-3 スパニングツリー - 共通および内部スパニングツリー（CIST）と共通スパニングツリー（CST）



MSTP は、すべてのブリッジと LAN セグメントを 1 つの共通および内部スパニングツリー（CIST）で接続します。CIST は、STP、RSTP、MSTP プロトコルをサポートするスイッチ間で実行中のスパニングツリーアルゴリズムの結果として形成されます。

MSTI に含める VLAN を指定すると、プロトコルは自動的に各 VLAN 間の接続を維持する MSTI ツリーを構築します。各インスタンスは CST 内の RSTP ノードとして扱われるため、MSTP はグローバルネットワークとの接続を維持します。

7.2 ループ検出の設定

[Spanning Tree]> [Loopback Detection]ページを使用して、インタフェースにループバック検出を設定します。ループバック検出が有効になり、ポートまたはトランクが自身の BPDU を受信すると、検出エージェントはループバック BPDU を廃棄し、SNMP トラップを送信し、インタフェースを Discarding 状態にします。このループバック状態は、手動解除できます。

Note: ループバック検出が有効にされておらず、インタフェースが自身の BPDU を受信すると、インタフェースは IEEE 標準 802.1w-2001 9.3.4（Note 1）に従ってループバック BPDU を廃棄します。

Note: スイッチ上でスパニングツリーが無効の場合、ループバック検出はアクティブになりません。

Note: 手動解除モードに設定されている場合、リンクダウン/アップイベントはポートを破棄状態から解放しません。

Note: ループバック検出を使用する場合、手動解除モードのみサポートします。必ず手動解除モードに変更して使用してください。

パラメータ

次のパラメータが表示されます。

- Interface - ポートまたはトランクのリストを表示します。
- Status - このインタフェースでループバック検出を有効にします。(デフォルト: Disabled)
- Trap - このインタフェースのループバックイベントに対する SNMP トラップ通知を有効にします。(デフォルト: Disabled)
- Release Mode - Discarding 状態を解除するリリースモードについて、手動（Manual）を設定します。(デフォルト: Auto) ループバック検出を使用する場合は必ず手動設定を行ってください。
- Release - インタフェースを Discarding 状態から手動で解放できるようにします。これは、インタフェースが手動リリースモードに設定されている場合にのみ使用できます。
- Action - ループバック検出の応答を設定して、インタフェースをシャットダウンします。(デフォルト: Shutdown)
- Shutdown Interval - インタフェースをシャットダウンする時間です。(範囲: 60 から 86400 秒、デフォルト: 60 秒)
  ループバック検出によってインタフェースがシャットダウンされ、リリースモードが“Auto,”に設定されている場合、シャットダウン間隔が経過すると、選択されたインタフェースが自動的に有効になります。
  検出されたループバックによってインタフェースがシャットダウンされ、リリースモードが“Manual,”に設定されている場合、インタフェースはリリースボタンを使用して再び有効にできます。

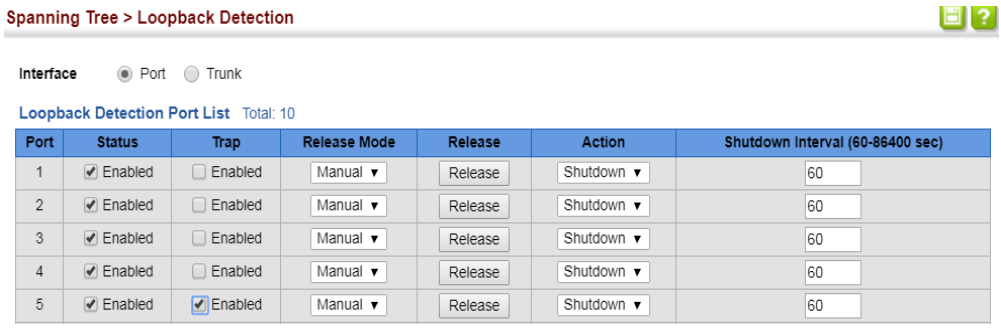
Web インタフェース

ループバック検出を設定するには：

1. [Spanning Tree]、[Loopback Detection]をクリックします。
2. [Port]または[Trunk]をクリックして、必要なインタフェースタイプを表示します。
3. 必要なループバック検出属性を変更します。

4.　[Apply]をクリックします。

図 7-4　ポートループバック検出の設定



7.3 STA のグローバル設定

[Spanning Tree]> [STA (Configure Global - Show Information)]ページを使用して、スイッチ全体に適用されるスパニングツリーのグローバルを設定します。

コマンドの使用方法

- スパニングツリープロトコル※
- このオプションは、STP 強制互換モードに設定された RSTP を使用します。内部ステートマシンには RSTP を使用しますが、802.1D BPDU だけを送信します。高速スパニングツリープロトコル※
  RSTP では、受信プロトコルメッセージを監視することにより、STP または RSTP ノードのいずれかへの接続をサポートします。そして以下に示すように、RSTP ノードが送信するプロトコルメッセージタイプを動的に調整します。:
  - STP モード - ポートが 802.1D BPDU（つまり STP BPDU）を受信し、ポートの移行遅延タイマ（migration delay timer）満了後も 802.1D BPDU を受信した場合、スイッチは 802.1D ブリッジに接続されているものとみなし、802.1D BPDU のみの使用を開始します。
  - RSTP モード -ポート上で RSTP BPDU を受信した場合、あるいは RSTP で 802.1D BPDU を使用しているときに RSTP BPDU を受信し、移行遅延タイマ（migration delay timer）満了後、RSTP BPDU を受信した場合、スイッチは RSTP BPDU を送信する RSTP モードで動作します。

  注※ STP および RSTP BPDU はタグなしフレームとして送信され、任意の VLAN 境界を通過します。
- マルチプルスパニングツリープロトコル
  MSTP は、インスタンスごとに一意のスパニングツリーを生成します。これにより、ネットワーク全体で複数の経路が提供されるため、単一インスタンス内のブリッジノードに障害が発生した場合の大規模な中断を防ぎ、障害の発生したインスタンスに対して新しいトポロジのコンバージェンスを高速化できます。
  - マルチプルスパニングツリーでは、各スイッチがブリッジ関連の設定を合わせることにより、特定のスパニングツリーインスタンス上で動作するできるようになります。
  - スパニングツリーインスタンスは、対応する VLAN インスタンス割当てを持つブリッジ上でのみ存在することができます。
  - スパニングツリーモードを切り替える場合は注意してください。モードを変更すると、以前のモードのすべてのスパニングツリーインスタンスが停止し、新しいモードでシステムが再起動され、一時的にユーザトラフィックが中断されます。

パラメータ

次のパラメータが表示されます。

グローバル設定の基本設定

- Spanning Tree Status - このスイッチで STA を有効または無効にします。(デフォルト: Disabled)
- Spanning Tree Type - このスイッチで使用されるスパニングツリーのタイプを指定します。
  - STP: スパニングツリープロトコル（IEEE 802.1D)。 すなわち、このオプションが選択されると、スイッチは STP 強制互換モードに設定された RSTP を使用する。
  - RSTP: 高速スパニングツリー（IEEE 802.1w）; RSTP がデフォルトです。
  - MSTP: マルチプルスパニングツリー（IEEE 802.1s）
- Priority - ブリッジプライオリティは、ルートブリッジデバイス、ルートポート、および指定ポートの選択に使用されます。最高のプライオリティを持つデバイスが STA ルートブリッジデバイスになります。ただし、すべてのデバイスの優先度が同じ場合、MAC アドレスが最も小さいデバイスがルートブ

リッジデバイスになります。（数値が小さいほど優先度が高いことに注意してください）。

- デフォルト: 32768
- 範囲: 0 から 61440、4096 ステップ
- オプション: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440

◆ BPDU Flooding - スパニングツリーがスイッチ上でグローバルに無効になっているか、特定のポートで無効になっている場合、BPDU をスイッチ上の他のすべてのポートまたは同じ VLAN 内の他のすべてのポートにフラッディングさせるようにシステムを設定します。

- To VLAN: 受信ポートのネイティブ VLAN 内の他のすべてのポートに（つまり、ポートの PVID によって決定されるように）BPDU をフラッディングします。これがデフォルトです。
- To All: BPDU をスイッチ上の他のすべてのポートにフラッディングします。

ポートで BPDU フラッディングが無効になっている場合、設定は無効です。

高度な設定

次の属性は RSTP にもとづいていますが、スイッチが STP を実装するために RSTP の下位互換性のあるサブセットを使用し、標準に従って RSTP に基づく MSTP にも適用されるため、STP にも適用されます。

◆ Path Cost Method - パスコストは、デバイス間の最適なパスを決定するために使用されます。パスコスト法は、各インタフェースに割当てることができる値の範囲を決定するために使用されます。

- Long: 1 から 200,000,000 の範囲の 32 ビットベースの値を指定します。(これがデフォルトです。)
- Short: 1 から 65535 の 16 ビット値を指定します。

◆ Transmission Limit - BPDU の最大伝送速度は、連続するプロトコルメッセージの送信間隔の最小値を設定することによって指定されます。(範囲: 1 から 10、デフォルト: 3)

スイッチがルートになるとき

◆ Hello Time - ルートブリッジデバイスが設定メッセージを送信する間隔です（秒単位）。

- デフォルト: 2
- 最小：1
- 最大：9 または[（Maximum Age / 2）-1]の低いほう

◆ Maximum Age - ルートブリッジデバイスから設定メッセージを受信しなかったとき、デバイスがスパニングツリーの再構成を再構成を試みるまでの最大エージングタイム（秒単位）。すべてのデバイスポート(指定されたポートを除く)は、定期的に設定メッセージを受信する必要があります。タイムアウトを検出した場合、STA 情報を最後に使用したポート(最後の設定メッセージで提供)は、接続された LAN の指定ポートになります。ルートポートの場合は、ネットワークに接続されているデバイスポートの中から新しいルートポートが選択されます。（このセクションの「ポート」とは、ポートとトランクの両方を含む「インタフェース」を意味します）。

- デフォルト: 20
- 最小：6、または[2 x (Hello Time + 1)]の高い方です。
- 最大：40、または[2 x (Forward Delay - 1)]の低い方です。

◆ Forward Delay - 状態を変更する前にこのデバイスが待機する最大時間（秒）です（Discarding → Learning → Forwarding）。この遅延は、すべてのデバイスがフレームフォワーディングを開始する前にトポロジの変更に関する情報を受信する必要があるためにあります。

- デフォルト: 15
- 最小：4 または[（Max. Message Age/ 2）+ 1]の高い方です。
- 最大：30

ほとんどの場合、RSTP は転送遅延（Forward Delay）時間に依存しません。タイマー設定に依存するこ

となく、ポートが Forwarding 状態に移行できることを確認できます。高速なコンバージェンスを実現するために、RSTP はエッジポートの使用、およびポイントツーポイントリンクタイプの自動検出に依存しています。どちらの場合も、ポートは Forwarding 状態に直接移行できます。

MSTP のコンフィグレーション

- Max Instance Numbers - このスイッチを割当てることができる MSTP インスタンスの最大数です。
- Region Revision - この MSTI のリビジョンです。(範囲: 0 から 65535、デフォルト: 0)
- Region Name - この MSTI の名前です。(最長: 32 文字; デフォルト: スイッチの MAC アドレス)
- Max Hop Count - BPDU が破棄される前の MST 領域で許可されているホップの最大数です。(範囲: 1-40、デフォルト：20)

NOTE:Region Revision と Region Name はどちらも MST リージョンを一意に識別するために必要です。

Web インタフェース

グローバル STA を設定するには：

1. [Spanning Tree]、[STA]をクリックします。
2. [Step]リストから[Configure Global]を選択します。
3. [Action]リストから[Configure]を選択します。
4. 必要な属性を変更します。スパニングツリータイプ（STP、RSTP、MSTP）に表示されるパラメータは、前のセクションで説明したように異なります。
5. [Apply]をクリックします。

図 7-5　STA のグローバル設定(STP)

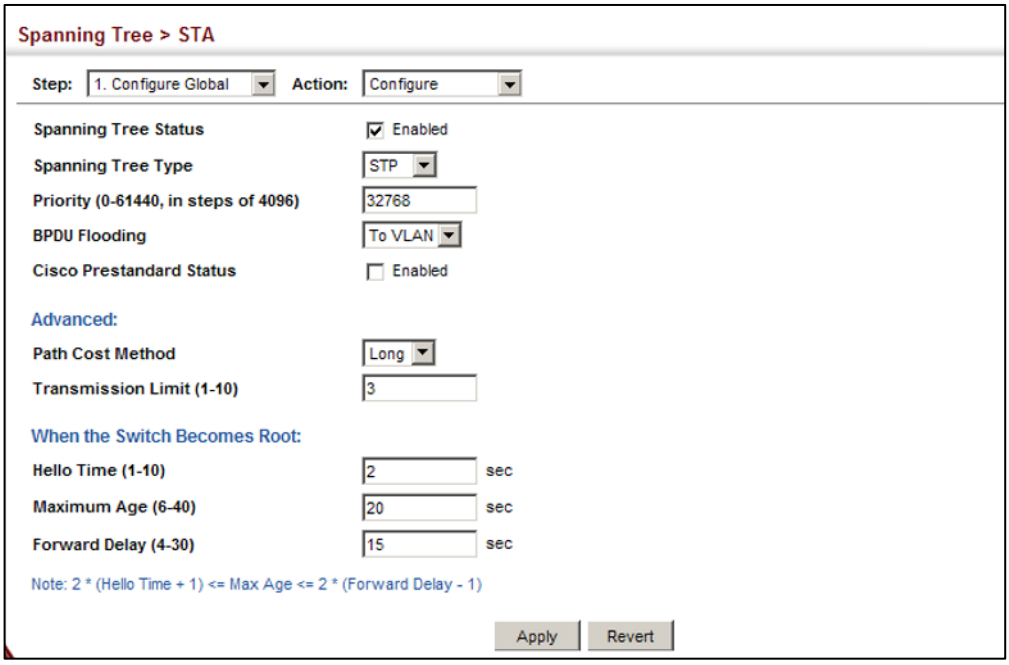


図 7-6　STA のグローバル設定(RSTP)

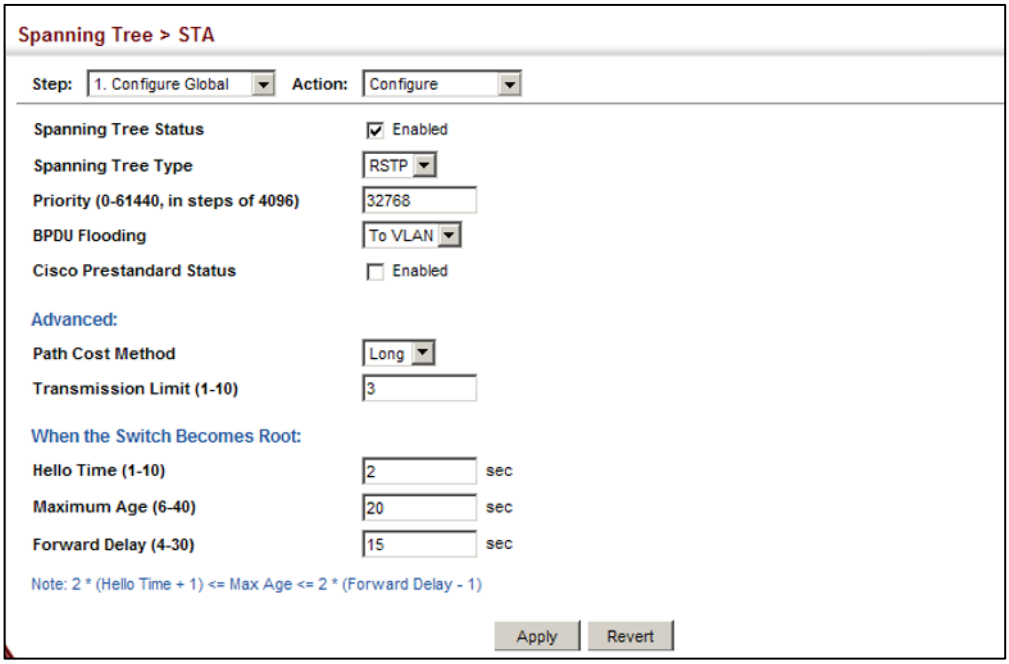
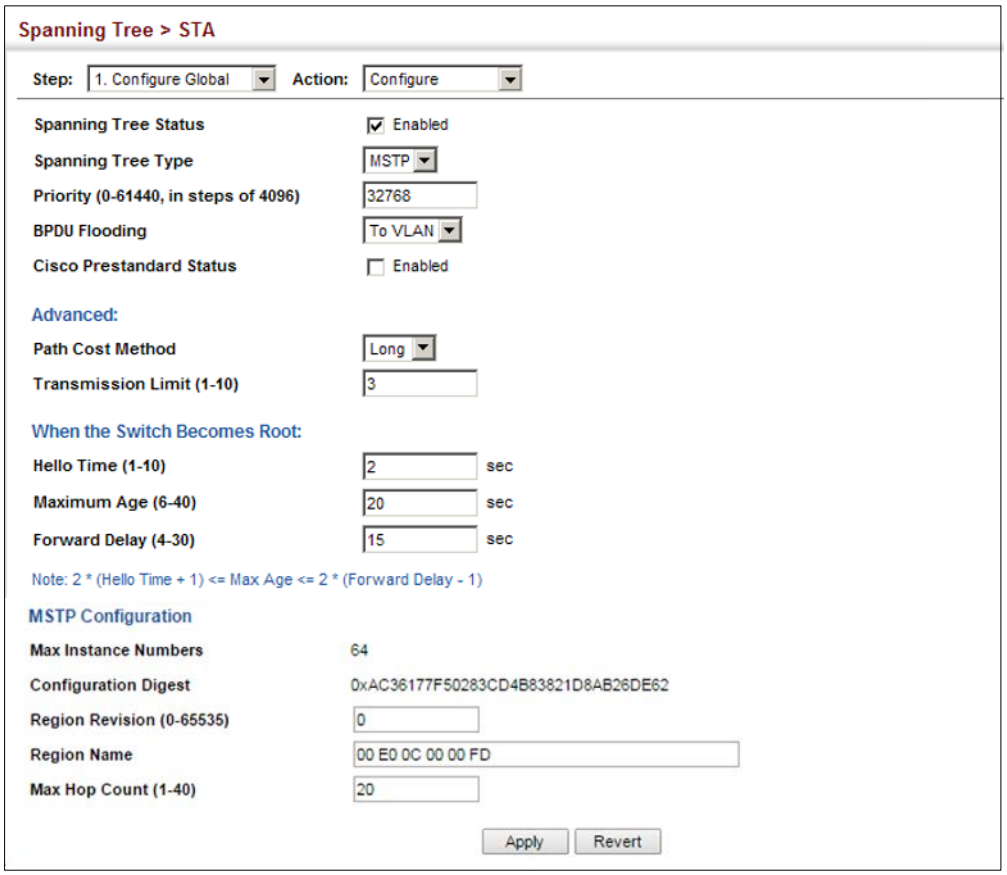


図 7-7　STA のグローバル設定(MSTP)



7.4 STA のグローバル設定の表示

[Spanning Tree]> [STA (Configure Global - Show Information)]ページを使用して、スイッチ全体に適用される現在のブリッジ STA 情報の要約を表示します。

パラメータ

表示されるパラメータは、次の項目を除いて、前のセクションで説明されています。

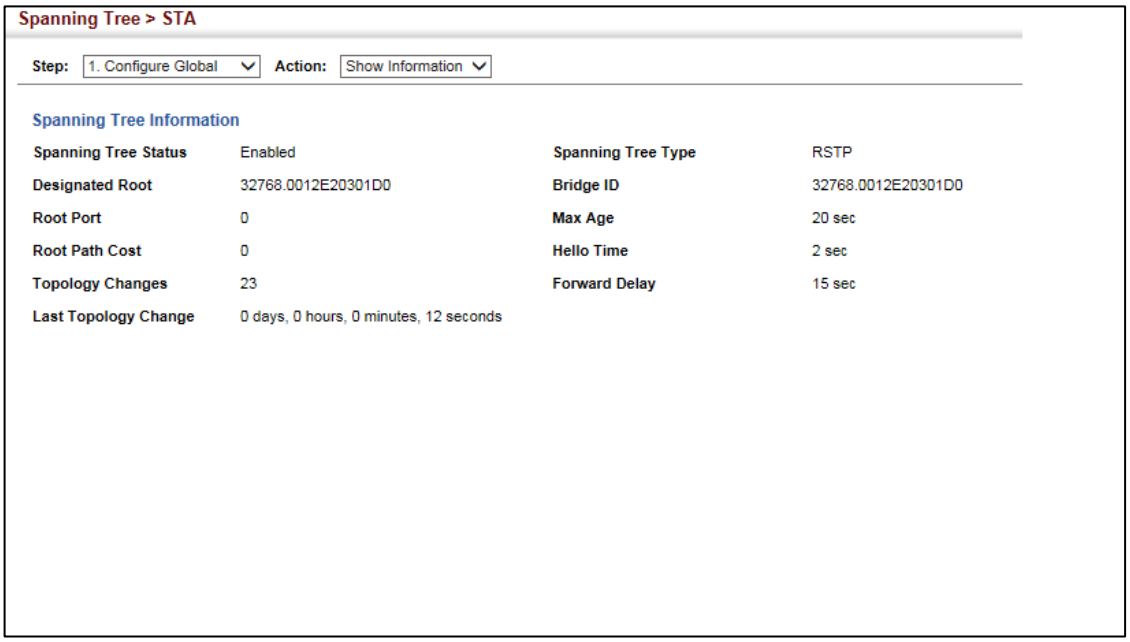
- Bridge ID - このブリッジの一意の識別子。ブリッジプライオリティ、スパニングツリータイプが MSTP に設定されている場合の共通スパニングツリーの MST インスタンス ID は 0、MST 領域の名称は MAC アドレスです（スイッチの MAC アドレス）。
- Designated Root - スパニングツリー内のデバイスの優先順位と MAC アドレスにより決定されるルートブリッジデバイスです。
- Root Port - ルートに最も近いスイッチ上のポートがルートポートとなります。スイッチは、このポートを介してルートブリッジデバイスと通信します。ルートポートがないスイッチは、スパニングツリーネットワークのルートブリッジデバイスです。
- Root Path Cost - このスイッチのルートポートからルートブリッジデバイスまでのパスコストです。
- Topology Changes - スパニングツリーが再構成された回数です。
- Last Topology Change - スパニングツリーが最後に再構成されてからの経過時間です。

Web インタフェース

全体 STA 設定を表示するには：

1. [Spanning Tree]、[STA]をクリックします。
2. [Step]リストから[Configure Global]を選択します。
3. [Action]リストから情報を表示を選択します。

図 7-8　STA のグローバル設定の表示



7.5 STA のインタフェース設定

[Spanning Tree]> [STA (Configure Interface - Configure)]ページを使用して、ポートプライオリティ、パスコスト、リンクタイプ、エッジポートなど、特定のインタフェースの RSTP および MSTP アトリビュートを設定します。ポイントツーポイント接続または共有メディア接続を示すリンクタイプ、および接続されたデバイスが高速の回線速度のエッジポートなど、様々なポートから優先するパスを示すために、同じメディアタイプのポートに異なる優先順位またはパスコストを使用することができます。(このセクションの「ポート」とは、ポートとトランクの両方を含む「インタフェース」を意味します)。

パラメータ

次のパラメータが表示されます。

- Interface - ポートまたはトランクのリストを表示します。
- Spanning Tree - このインタフェースで STA を有効または無効にします。(デフォルト: Enabled)
- BPDU Flooding - グローバルスパニングツリーが無効の場合、または特定のポートでスパニングツリーが無効の場合、BPDU の他のポートへのフラッディングを有効または無効にします。フラッディングが有効の場合、BPDU は、スイッチ上の他のすべてのポート、または受信ポートのネイティブ VLAN 内の他のすべてのポートにフラッディングされます。(デフォルト: Enabled)
- Priority - スパニングツリープロトコルでこのポートに使用されるプライオリティを定義します。スイッチ上のすべてのポートのパスコストが同じである場合、最も優先度の高いポート（最低値）がスパニングツリーのアクティブリンクとなります。スパニングツリープロトコルがネットワークループを検出している場合、優先度の高いポートはブロックされにくくなります。複数のポートに最高の優先度が割当てられている場合は、最も小さいポート番号のポートが有効になります。
  - デフォルト: 128
  - 範囲: 0 から 240、ステップは 16
- Admin Path Cost - このパラメータは、デバイス間の最適なパスを決定するために STA によって使用されます。したがって、より低い値は、より高速のメディアに接続されたポートに割当てられ、より高い値は、より低速のメディアに割当てられます。パスコストはポートの優先度よりも優先されます。(範囲: 自動構成の場合は 0、short パスコスト方式の場合は 1 から 65535※、long パスコストの場合は 1 から 200,000,000)
  デフォルトでは、各ポートで使用される速度とデュプレックスモードが自動的に検出され、以下に示す値に従ってパスコストが設定されます。パスコスト「0」は、自動構成モードを示すために使用されます。短パスコスト方式が選択され、IEEE8021w 標準で推奨されるデフォルトパスコストが 65,535 を超える場合、デフォルトは 65,535 に設定されます。
  注※ パスコスト方式の設定については、「7.3 STA のグローバル設定」を参照してください。STA インタフェース設定ページに表示される範囲には、パスコストの最大値が表示されます。 ただし、スイッチは指定されたパスコスト方式（long または short）にもとづいてパスコストの規則を適用することに注意してください。

表 7-1 推奨される STA パスのコスト範囲

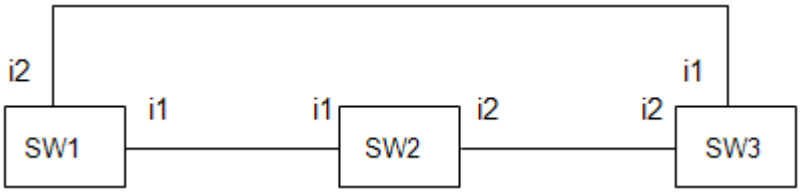
ポートタイプ	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	50-600	200,000-20,000,000
Fast Ethernet	10-60	20,000-2,000,000
Gigabit Ethernet	3-10	2,000-200,000
10G Ethernet	1-5	200-20,000

表 7-2　デフォルトの STA パスコスト

ポートタイプ	short パスコスト (IEEE 802.1D-1998)	long パスコスト (IEEE 802.1D-2004)
Ethernet	65,535	1,000,000
Fast Ethernet	65,535	100,000
Gigabit Ethernet	10,000	10,000
10G Ethernet	1,000	1,000

管理パスコストを使用して、スイッチ上のルートポートを直接決定することはできません。他のデバイスへの接続は IEEE 802.1Q-2005 を使用して、次の例のようにルートポートを決定します。

図 7-9　ルートポートの決定



SW3 の i1 で受信された BPDU メッセージの場合、パスコストは 0 です。
SW3 の i2 が受信する BPDU メッセージの場合、パスコストは SW2 の i1 のコストです。
ルートポートの役割を果たすために使用された SW3 上の i1 のルートパスコストは、SW3 上の 0＋i1 のパスコストです。
0 は i1 がルートブリッジに直接接続されているためです。
SW2 の i1 のパスコストが設定/変更されない場合、パスコストは 10000 です。
次に、ルートポートの役割を競合するために使用された SW3 上の i2 のルートパスコストは、10000 + SW3 上の i2 のパスコストです。
SW3 上の i1 のパスコストは、設定/変更されていない場合も 10000 です。
SW3 上の i2 のパスコストが 0 に設定/変更されても、これらのポートは同じルートパスコストを持ちますが、SW3 上のパスコストを変更するだけで i2 がルートポートになることは不可能です。
なお RSTP モードの場合は、SW2 上の i1 のパスコストを調整するだけでルートポートを決定できます。ただし、MSTP モードでは、外部パスコストが同じ領域に追加されず（i1 のリージョナルルートが SW1 であるが、i2 は SW2 であるため）、パスコストを変更するだけではこれを達成できません。

- Admin Link Type - このインタフェースに接続されているリンクの種類です。
  - Point-to-Point - 他の 1 つのブリッジへの接続です。
  - Shared - 2 つ以上のブリッジへの接続です。
  - Auto - スイッチは、インタフェースがポイントツーポイントリンクまたは共有メディアに接続されているかどうかを自動的に判断します。.（これがデフォルトの設定です。）
- Root Guard - STA では、ブリッジ識別子（または同じ識別子と低い値の MAC アドレス）を持つブリッジをいつでもルートブリッジとして引き継ぐことができます。ルートガードを使用して、最適な位置にルートブリッジが形成されないようにすることができます。低速ブリッジに接続されている指定ポートではルートガードを有効にする必要があります。ルートポートとして引き継ぎ、新しいスパニングツリートポロジを形成することにより、低速リンクに過負荷をかける可能性があります。ルートブリッジが許可されているネットワークの一部の周りに境界線を形成するために使用することもできます。(デフォルト: Disabled)
- Admin Edge Port - エッジポートを指定すると、再構成の際に、アドレステーブルを再構築するために必要となるフレームのフラッディング量を削減できます。ただし、エッジポートは、エンドノードデバイスに接続されたポートに対してのみ有効にする必要があります。(デフォルト: Auto)

- Auto - RSTP または MSTP BPDU を受信せずにエッジ遅延時間が経過すると、ポートは自動的にエッジポートとして設定されます。ポートのリンクタイプがポイントツーポイント（IEEE 802.3D-2004 17.20.4 で定義されているように 3 秒）の場合、エッジ遅延時間（802.1D-2004 17.20.4）はプロトコル移行時間に等しいことに注意してください。 それ以外の場合は、スパニングツリーの設定メッセージの最大経過時間と同じです。

インタフェースは、次の条件ではエッジポートとして機能できません。

- スパニングツリーモードが STP に設定されている場合、エッジポートモードを auto 設定にしてもエッジポート状態に移行できません。
- ループバック検出が有効になっており、ループバック BPDU が検出された場合、ループバック状態が解除されるまで、インタフェースはエッジポートとして機能できません。
- インタフェースが Forwarding 状態にあり、その役割が変更された場合、エッジ遅延時間が経過してもインタフェースはエッジポートとして機能し続けることができません。
- エッジ遅延時間が経過後もポートが BPDU を受信しない場合、ポートの役割は指定ポートに変更され、ただちに Forwarding 状態に移行します。

エッジポートが自動設定されている場合、動作状態は 802.1D-2004 に記載されているブリッジ検出ステートマシンによって自動的に決定されます。エッジポートの状態は、環境の変化（BPDU の受信状況など）にもとづいて動的に変化します。

- BPDU Guard - この機能は、エッジポートが BPDU を受信するのを防ぎます。BPDU が受信されたときにエッジポートをシャットダウンすることによってループを防止します。有効な構成では、設定されたエッジポートは BPDU を受信すべきではありません。エッジポートで BPDU を受信するときは、不正なデバイスの接続や、無効な設定が存在する可能性があります。BPDU ガード機能でシャットダウンしたポートは、管理者が手動でポートを有効にする必要があるため、無効な設定に対する安全な応答を提供します。(デフォルト: Disabled)
  BPDU ガードは、エッジポートアトリビュートが無効になっていない場合（つまり、エッジポートが有効または自動に設定されている場合）にのみインタフェース上で設定できます。
- BPDU Guard Auto Recovery - 指定した間隔の後にインタフェースを自動的に再び有効にします。(デフォルト: Disabled)
- BPDU Guard Auto Recovery Interval - インタフェースを再度有効にするまで待機する時間です。(範囲: 30 から 86400 秒、デフォルト: 300 秒)
- BPDU Filter - BPDU フィルタリングにより、エンドノードに接続されている構成済みのエッジポートで BPDU を送信しないようにできます。デフォルトでは、ポート上で管理エッジが有効になっているかどうかにかかわらず、STA は BPDU をすべてのポートに送信します。BPDU フィルタリングは、ポート単位で構成されています。(デフォルト: Disabled)
  BPDU フィルタは、エッジポート属性が無効でない場合（つまり、エッジポートが有効または自動に設定されている場合）にのみインタフェース上で設定できます。
- Migration - スイッチが設定またはトポロジ変更通知 BPDU を含む STP BPDU を検出すると、いつでも、選択されたインタフェースが強制 STP 互換モードに自動的に設定されます。ただし、[Protocol Migration]ボタンを使用して、適切な BPDU 形式（RSTP または STP 互換）を手動で再確認し、選択したインタフェースで送信することもできます。(デフォルト: Disabled)
- TC Propagate Stop - トポロジ変更通知（TCN）の伝播を停止します。(デフォルト: Disabled)

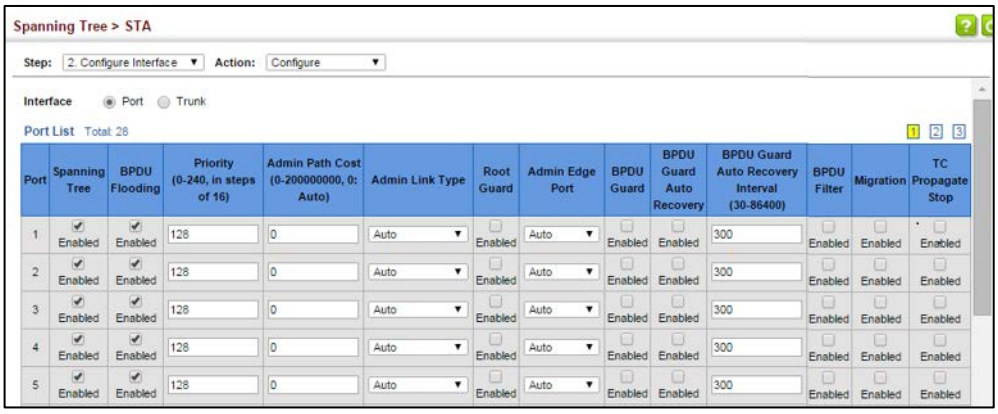
Web インタフェース

STA のインタフェースを設定するには:

1. [Spanning Tree]、[STA]をクリックします。
2. [Step]リストから[Configure Interface]を選択します。

3. [Action]リストから[Configure]を選択します。
4. 必要な属性を変更します。
5. [Apply]をクリックします。

図 7-10 STA のインタフェース設定



7.6 STA のインタフェース設定の表示

[Spanning Tree]> [STA (Configure Interface - Show Information)]ページを使用して、スパニングツリー内のポートまたはトランクの現在のステータスを表示します。

パラメータ

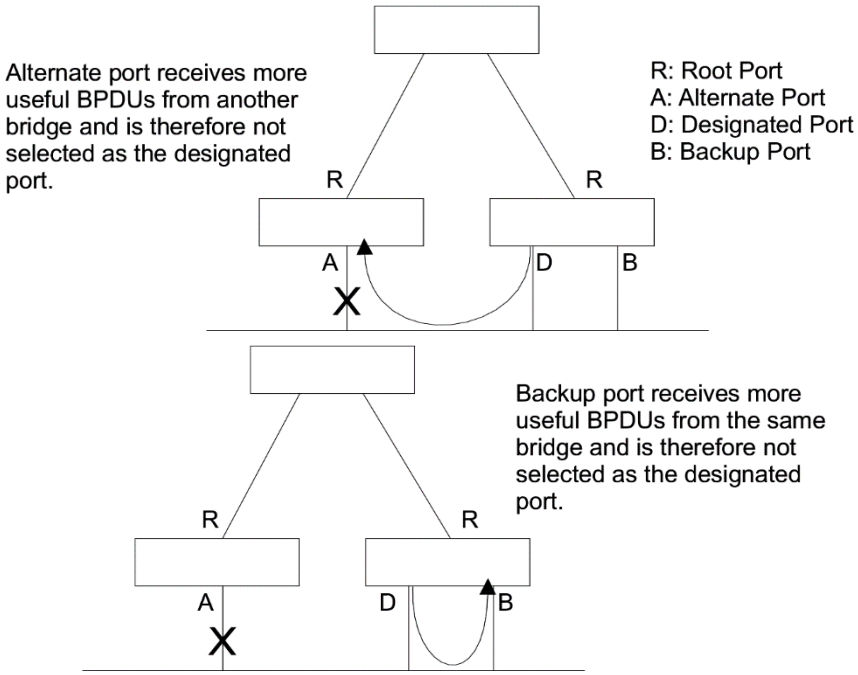
次のパラメータが表示されます。

- Spanning Tree - このインタフェースで STA が有効になっているかどうかを示します。
- BPDU Flooding - スイッチ上でスパニングツリーがグローバルに無効になっている場合、または特定のポートで無効になっている場合に BPDU が他のポートにフラッディングされるかどうかを示します。
- STA Status - スパニングツリー内のこのポートの現在の状態を表示します。
  - Discarding - ポートは STA 構成メッセージを受信しますが、パケットはフォワーディングしません。
  - Learning - ポートは、Forward Delay タイマで設定された間隔で設定メッセージを送信します。ポートアドレステーブルがクリアされ、ポートはアドレスのラーニングを開始します。
  - Forwarding - ポートはパケットをフォワーディングし、アドレスのラーニングを続けます。

  ポートステータスを定義するルールは次のとおりです。
  - 他の STA 準拠ブリッジングデバイスのないネットワークセグメント上のポートは常にフォワーディングされます。
  - スイッチの 2 つのポートが同じセグメントに接続され、このセグメントに他の STA デバイスが接続されていない場合、ID の小さいポートはパケットをフォワーディングし、もう一方のポートは廃棄します。
  - スイッチが起動されると、すべてのポートは Discarding 状態となり、そのうちいくつかは状態を Learning 状態に変更してから Forwarding 状態になります。
- Forward Transitions - このポートが Learning 状態から Forwarding 状態に移行した回数です。
- Designated Cost - 現在のスパニングツリー設定で、このポートからルートにパケットを転送するコストです。低速のメディアほど、コストが高くなります。
- Designated Bridge - このポートがスパニングツリーのルートに到達するために通信する必要があるデバイスのブリッジプライオリティと MAC アドレスです。
- Designated Port - 指定されたブリッジングデバイスのポート優先度とポート番号です。このスイッチはスパニングツリーのルートと通信する必要があります。
- Oper Path Cost - このポートを含む、スパニングツリールートに向かうパスのパスコストへのこのポートの寄与です。
- Oper Link Type - このインタフェースに接続された LAN セグメントの動作可能なポイントツーポイントステータス。STP インタフェース設定の Admin Link Type の説明の通り、このパラメータは、手動設定するか、自動検出によって決定されます。
- Oper Edge Port - このパラメータは、STP インタフェースの Admin Edge Port の設定（Enable または Disable）で初期化されますが、別のブリッジがこのポートに接続されていることを示す BPDU が受信された場合は false に変わります。
- Port Role - 役割は、ポートがアクティブなトポロジの一部であるかどうか、すなわち、非ルートブリッジをルートブリッジに接続する最良のポート（すなわちルートポート）であるか、ブリッジを介してルートブリッジに LAN を接続する（すなわち 指定ポート）、または他のブリッジ、ブリッジポート、または LAN に障害が発生した場合や削除された場合に、接続を提供する代替ポートまたはバック

アップポートです。 ポートがスパニングツリー内で役割を持たない場合、役割は無効（すなわち、無効なポート）に設定されます。

図 7-11 STA ポートの役割



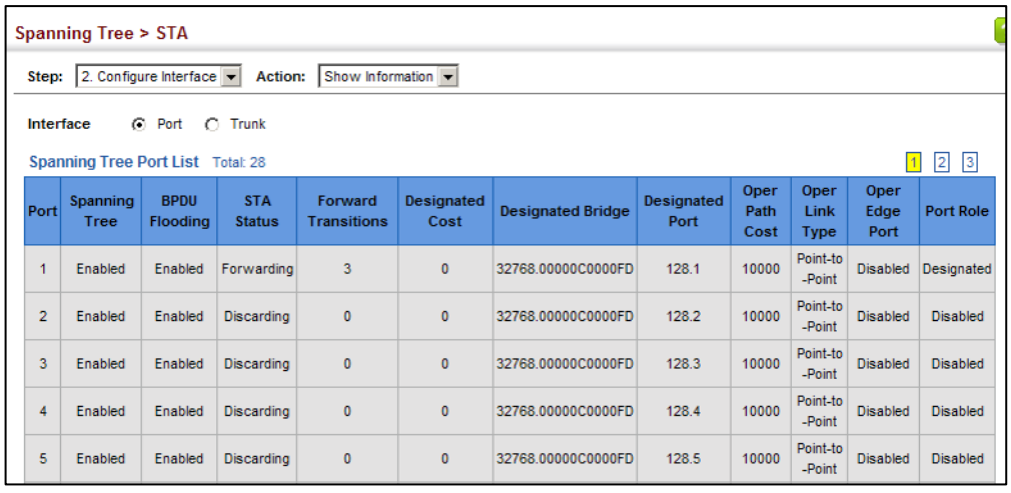
ポートの役割を決定するために使用される基準は、ルートブリッジ ID、ルートパスコスト、指定ブリッジ、指定ポート、ポートプライオリティ、およびポート番号にもとづいております。

Web インタフェース

STA のインタフェース設定を表示するには:

1. [Spanning Tree]、[STA]をクリックします。
2. [Step]リストから[Configure Interface]を選択します。
3. [Action]リストから情報の表示を選択します。

図 7-12 STA のインタフェース設定の表示



Port	Spanning Tree	BPDU Flooding	STA Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port	Oper Path Cost	Oper Link Type	Oper Edge Port	Port Role
1	Enabled	Enabled	Forwarding	3	0	32768.00000C0000FD	128.1	10000	Point-to-Point	Disabled	Designated
2	Enabled	Enabled	Discarding	0	0	32768.00000C0000FD	128.2	10000	Point-to-Point	Disabled	Disabled
3	Enabled	Enabled	Discarding	0	0	32768.00000C0000FD	128.3	10000	Point-to-Point	Disabled	Disabled
4	Enabled	Enabled	Discarding	0	0	32768.00000C0000FD	128.4	10000	Point-to-Point	Disabled	Disabled
5	Enabled	Enabled	Discarding	0	0	32768.00000C0000FD	128.5	10000	Point-to-Point	Disabled	Disabled

7.7 MSTP の設定

[Spanning Tree]> [MSTP (Configure Global)]ページを使用して、MSTP インスタンスを作成するか、MSTP インスタンスに VLAN グループを追加します。

コマンドの使用方法

MSTP は、インスタンスごとに一意のスパニングツリーを生成します。これにより、ネットワーク全体で複数の経路が提供されるため、単一インスタンス内のブリッジノードに障害が発生した場合の大規模な中断を防ぎ、障害の発生したインスタンスに対して新しいトポロジのコンバージェンスを高速化できます。

デフォルトでは、すべての VLAN は、MST 領域内のすべてのブリッジと LAN を接続する内部スパニングツリー（MST インスタンス 0）に割当てられます。このスイッチは、最大 16 のインスタンスをサポートします。ネットワークの同じ一般的な領域をカバーする VLAN をグループ化するようにしてください。ただし、同じ MSTI 領域内のすべてのブリッジを同じインスタンスセットで構成し、同じインスタンス(各ブリッジ上)を同じ VLAN セットで構成する必要があることに留意してください。また、RSTP は各 MSTI 領域を単一のノードとして取り扱い、すべての領域を共通スパニングツリーに接続します。

MSTP を使用するには :

1. スパニングツリータイプを MSTP に設定します。
2. [Spanning Tree]> [MSTP (Configure Global - Add)]ページで、選択した MST インスタンスのスパニングツリー優先順位を入力します。
3. [Spanning Tree]> [MSTP(Configure Global - Add Member)]ページでこの MSTI を共有する VLAN を追加します。

Note: すべての VLAN は自動的に IST（インスタンス 0）に追加されます。

MSTI がネットワーク経由で接続を維持するようにするには、同じ MSTI 設定で関連するブリッジセットを構成する必要があります。

パラメータ

次のパラメータが表示されます。

- MST ID - 設定するインスタンス識別子です。(範囲: 0 から 4094)
- VLAN ID - この MST インスタンスに割当てる VLAN です。(範囲: 1 から 4094)
- Priority - スパニングツリーインスタンスの優先順位です。(範囲: 0 から 61440(4096 ステップ単位)、オプション: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440; デフォルト: 32768)

Web インタフェース

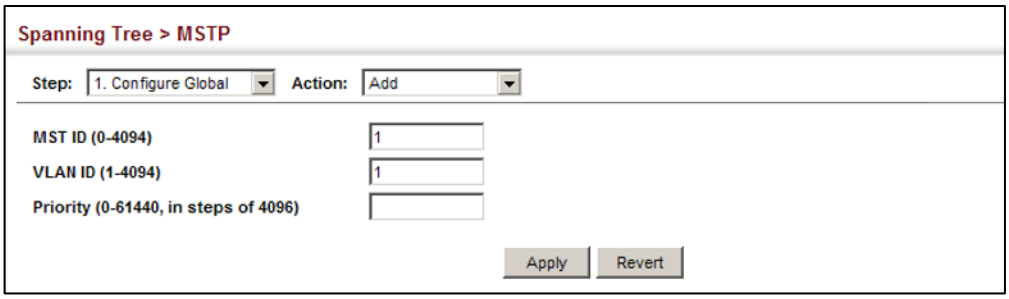
MSTP のインスタンスを作成するには:

1. [Spanning Tree]、[MSTP]をクリックします。
2. [Step]リストから[Configure Global]を選択します。
3. [Action]リストから[Add]を選択します。
4. MST インスタンス識別子と初期 VLAN メンバーを指定します。[Spanning Tree]> [MSTP(Configure Global - Add Member)]ページを使用して、追加のメンバーを追加できます。優先度が指定されていない

場合、デフォルト値 32768 が使用されます。

5. [Apply]をクリックします。

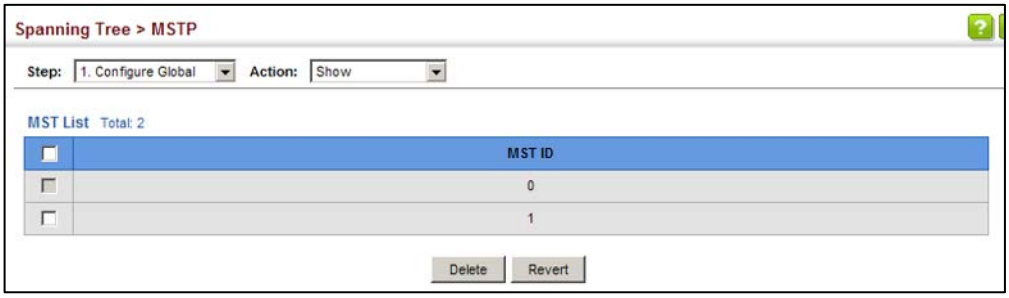
図 7-13　MST インスタンスの作成



MSTP インスタンスを表示するには：

1. [Spanning Tree]、[MSTP]をクリックします。
2. [Step]リストから[Configure Global]を選択します。
3. [Action]リストから[Show]を選択します。

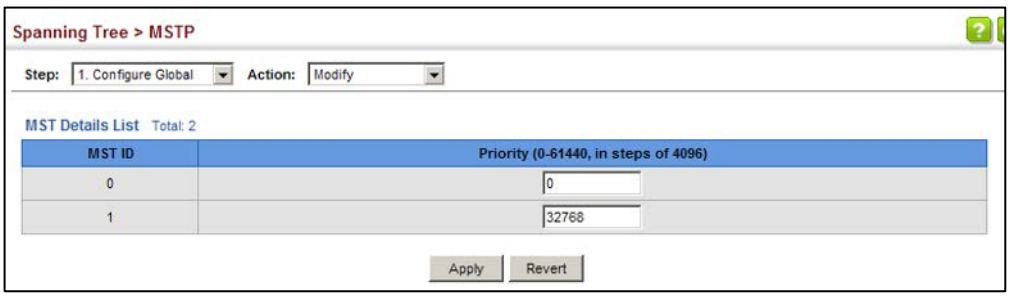
図 7-14　MST インスタンスの表示



MST インスタンスの優先度を変更するには：

1. [Spanning Tree]、[MSTP]をクリックします。
2. [Step]リストから[Configure Global]を選択します。
3. [Action]リストから[Modify]を選択します。
4. MSTP インスタンスの優先順位を変更します。
5. [Apply]をクリックします。

図 7-15　MST インスタンスの優先順位の変更

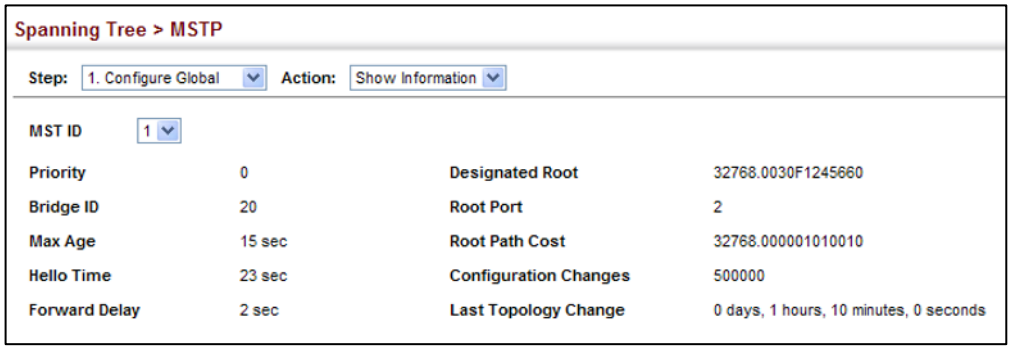


MSTP のグローバル設定を表示するには：

1. [Spanning Tree]、[MSTP]をクリックします。
2. [Step]リストから[Configure Global]を選択します。
3. [Action]リストから情報を表示を選択します。

4. MST ID を選択します。このページに表示されるアトリビュートについては、「7.4　STA のグローバル設定の表示」を参照してください。

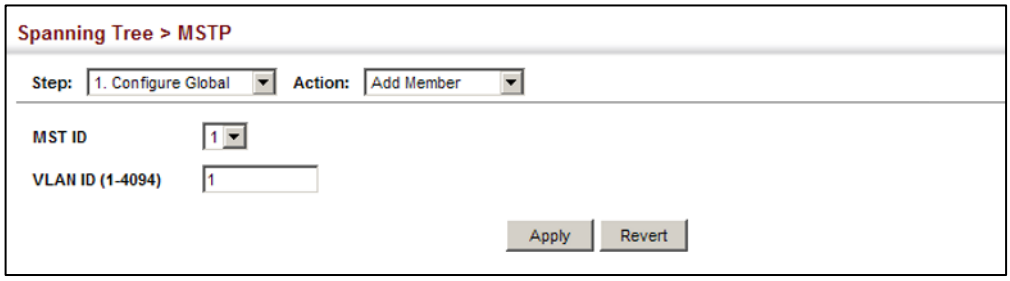
図 7-16　MST インスタンスのグローバル設定の表示



追加の VLAN グループを MSTP インスタンスに追加します。

1. [Spanning Tree]、[MSTP]をクリックします。
2. [Step]リストから[Configure Global]を選択します。
3. [Action]リストから[Add Member]を選択します。
4. MST ID リストから MST インスタンスを選択します。
5. VLAN ID フィールドにインスタンスに追加する VLAN グループを入力します。指定されたメンバーは、設定された VLAN である必要はありません。
6. [Apply]をクリックします。

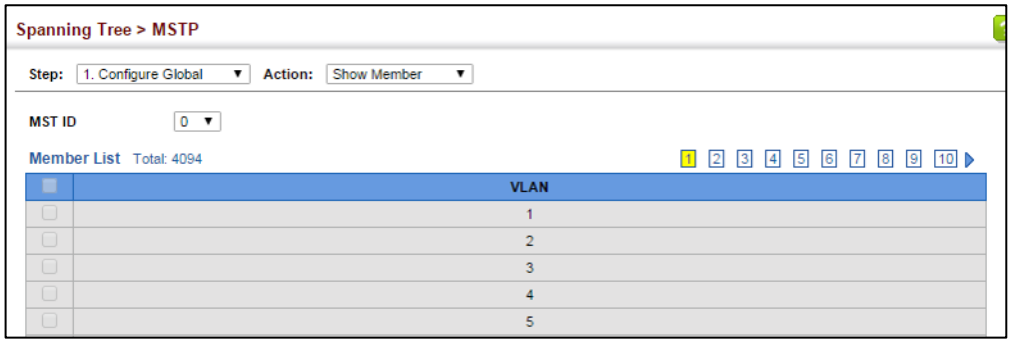
図 7-17　MST インスタンスへの VLAN の追加



MSTP インスタンスの VLAN メンバーを表示するには、次の手順を実行します。

1. [Spanning Tree]、[MSTP]をクリックします。
2. [Step]リストから[Configure Global]を選択します。
3. [Action]リストから[Show Member]を選択します。

図 7-18　MST インスタンスのメンバーの表示



7.8 MSTP のインタフェース設定

[Spanning Tree]> [MSTP (Configure Interface - Configure)]ページを使用して、MST インスタンスの STA インタフェースを設定します。

パラメータ

次のパラメータが表示されます。

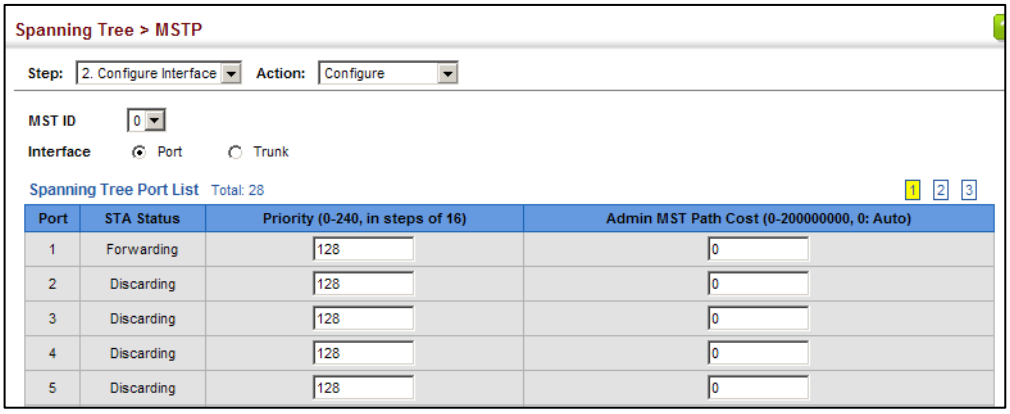
- MST ID - 設定するインスタンス識別子です。(デフォルト: 0)
- Interface - ポートまたはトランクのリストを表示します。
- STA Status - スパニングツリー内のこのインタフェースの現在の状態を表示します。（追加の情報については「7.6　STA のインタフェース設定の表示」を参照してください。）
  - Discarding - ポートは STA 構成メッセージを受信しますが、パケットはフォワーディングしません。
  - Learning - ポートは、Forward Delay タイマで設定された間隔で設定メッセージを送信します。ポートアドレステーブルがクリアされ、ポートはアドレスのラーニングを開始します。
  - Forwarding - ポートはパケットをフォワーディングし、アドレスのラーニングを続けます。
- Priority - スパニングツリープロトコルでこのポートに使用されるプライオリティを定義します。スイッチ上のすべてのポートのパスコストが同じである場合、最も優先度の高いポート（最低値）がスパニングツリーのアクティブリンクとして設定されます。スパニングツリープロトコルがネットワークループを検出している場合、優先度の高いポートはブロックされにくくなります。複数のポートに最高の優先度が割当てられている場合は、最も小さいポート番号のポートが有効になります。(デフォルト: 128; 範囲：0 から 240、ステップは 16)
- Admin MST Path Cost - このパラメータは、MSTP によってデバイス間の最適なパスを決定するために使用されます。したがって、より低い値は、より高速のメディアに接続されたポートに割当てられ、より高い値は、より低速のメディアに割当てられます。（パスコストはポートの優先度よりも優先されます）。STP のグローバル設定の Path Cost Method が short に設定されている場合、最大パスコストは 65,535 です。
  デフォルトでは、各ポートで使用される速度とデュプレックスモードが自動的に検出され、以下に示す値に従ってパスコストが設定されます。パスコスト「0」は、自動構成モードを示すために使用されます。short パスコスト方式が選択され、IEEE8021w 標準で推奨されるデフォルトパスコストが 65,535 を超える場合、デフォルトは 65,535 に設定されます。
  推奨範囲は、「表 7-1　推奨される STA パスのコスト範囲」を参照してください。
  デフォルトパスコストは、「表 7-2　デフォルトの STA パスコスト」を参照してください。

Web インタフェース

ポートまたはトランクの MSTP パラメータを設定するには：

1. [Spanning Tree]、[MSTP]をクリックします。
2. [Step]リストから[Configure Interface]を選択します。
3. [Action]リストから[Configure]を選択します。
4. インタフェースの優先度とパスコストを入力します
5. [Apply]をクリックします。

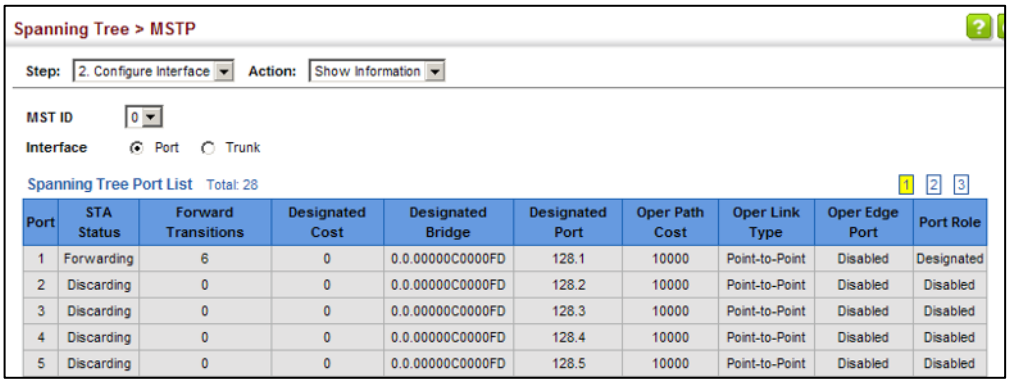
図 7-19　MSTP インタフェース設定



ポートまたはトランクの MSTP パラメータを表示するには：

1. [Spanning Tree]、[MSTP]をクリックします。
2. [Step]リストから[Configure Interface]を選択します。
3. [Action]リストから情報を表示を選択します。

図 7-20　MSTP インタフェース設定の表示



8 輻輳制御

スイッチでは、すべてのポートに対して、トラフィックの転送レートを設定することができます。また、ブロードキャストトラフィックまたはマルチキャストトラフィックの最大閾値を設定することによって、トラフィックストームを制御することもできます。また、ブロードキャストおよびマルチキャストストームの境界閾値を設定して、自動的にレート制限をおこなうか、ポートをシャットダウンすることもできます。

輻輳制御には以下のオプションがあります。

- Rate Limiting - ポートの入出力レート制限を設定します。
- Storm Control - 各インタフェースのトラフィックストーム閾値を設定します。

8.1 レート制限

[Traffic]> [Rate Limit]ページを使用して、入力ポートまたは出力ポートにレート制限を適用します。この機能により、ネットワーク管理者は、インタフェース上で送受信されるトラフィックの最大レートを制御できます。

レート制限は各ポートまたはトランクに適用することができます。この機能をインタフェースに設定することにより、トラフィックレートはハードウェアによって監視され、レート制限を超えたトラフィックは廃棄されます。

パラメータ

次のパラメータが表示されます。

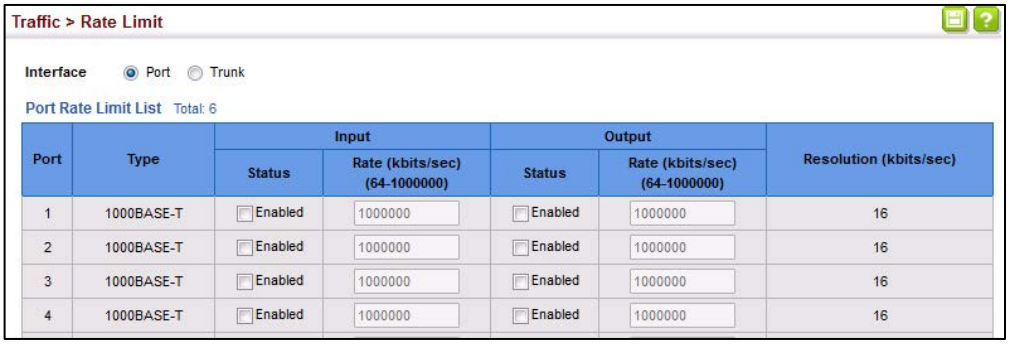
- Interface - スイッチのポートまたはトランクを表示します。
- Type - ポートの種類を示します。(1000BASE-T, 1000BASE SFP)
- Status - レート制限を有効または無効にします。(デフォルト: Disabled)
- Rate - レート制限レベルを設定します。
  (範囲: 64 から 1,000,000 kbits / sec for Gigabit Ethernet ports)
- Resolution - レートを設定できる粒度は 16 kbits / sec です。

Web インタフェース

レート制限を設定するには：

1. [Traffic]、[Rate Limit]をクリックします。
2. インタフェースタイプを[Port]または[Trunk]に設定します。
3. 必要なインタフェースのレート制限ステータスを有効にします。
4. 必要なインタフェースのレート制限を設定します。
5. [Apply]をクリックします。

図 8-1 レート制限の設定



8.2 ストームコントロール

[Traffic]> [Storm Control]ページを使用して、ブロードキャスト、マルチキャスト、および未知のユニキャストトラフィックに対して、ストームコントロールの閾値を設定します。ネットワーク構成間違いや、ネットワーク上のデバイス、もしくはユーザが使用するアプリケーションプログラムが誤動作した場合、トラフィックストームが発生する場合があります。ネットワークに意図しないトラフィックが多すぎると、ユーザトラフィックのパフォーマンスが著しく低下するか、あるいは停止する可能性があります。

ブロードキャスト、マルチキャストまたは未知のユニキャストトラフィックに閾値を設定することにより、ネットワークをトラフィックストームから防御することができます。指定した閾値を超えるパケットについては破棄されます。

コマンドの使用方法

- ブロードキャストストームコントロールは、デフォルトで無効になっています。
- トラフィックがブロードキャストおよびマルチキャストまたは未知のユニキャストトラフィックに指定された閾値を超えた場合、閾値を超えるパケットは、レートが閾値を下回って低下するまで廃棄されます。
- レート制限とストームコントロールを同じインタフェースで使用すると、期待と異なる動作となる場合があります。したがって、これらの機能を同じインタフェース上で使用しないでください。

パラメータ

次のパラメータが表示されます。

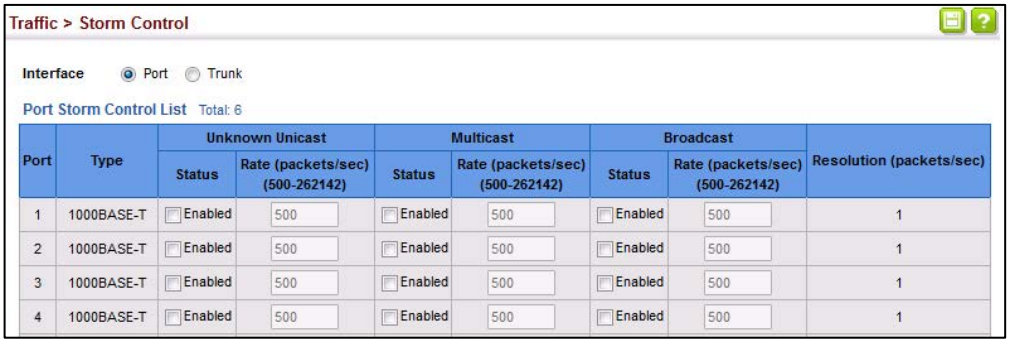
- Interface - ポートまたはトランクのリストを表示します。
- Type - ポートの種類を示します。(1000BASE-T, 1000BASE SFP).
- Unknown Unicast - 未知のユニキャストトラフィックのストーム制御を指定します。
- Multicast - マルチキャストトラフィックのストームコントロールを指定します。
- Broadcast - ブロードキャストトラフィックのストームコントロールを指定します。
- Status - ストームコントロールを有効または無効にします。(デフォルト: Disable）
- Rate - 1 秒あたりのパケット単位の閾値レベルです。
  (範囲: 500 から 262142pps; デフォルト： 500 pps）
- Resolution - レートを設定できる粒度を示します。

Web インタフェース

ブロードキャストストームコントロールを設定するには :

1. [Traffic]、[Storm Control]をクリックします。
2. インタフェースタイプを[Port]または[Trunk]に設定します。
3. ステータスフィールドを設定して、ストームコントロールを有効または無効にします。
4. スイッチがパケットの廃棄を開始するために必要な閾値を設定します。
5. [Apply]をクリックします。

図 8-2 ストームコントロールの設定



9 CoS

サービスクラス（CoS）では、輻輳のためにトラフィックがスイッチ内でバッファされるときに、優先順位の高いデータパケットを指定できます。このスイッチは、ポートごとに 8 つのプライオリティキューを持つ CoS をサポートしています。ポートの高優先度キューのデータパケットは、低優先度キューのデータパケットの前に送信されます。各インタフェースのデフォルトプライオリティを設定し、スイッチのプライオリティキューにフレーム優先度タグのマッピングを設定できます。

この章では、次の基本的なトピックについて説明します。

- Layer 2 Queue Settings - デフォルトプライオリティ、キューモード、キュー重み、および CoS タグに基づくキューへのパケットマッピングを含む各キューを設定します。
- Layer 3/4 Priority Settings - 受信パケットの処理方法（DSCP または CoS）を選択し、内部処理のためのホップ単位の動作および廃棄優先順位を設定します。

9.1 レイヤ 2 キューの設定

このセクションでは、タグなしフレームのデフォルトの優先度を設定し、キューモードを設定し、各キューに割当てられた重みを設定し、CoS タグをキューにマップする方法について説明します。

9.1.1 インタフェースのデフォルト優先順位の設定

[Traffic]> [Priority]> [Default Priority]ページを使用して、スイッチ上の各インタフェースのデフォルトポートプライオリティを指定します。スイッチに入るすべてのタグなしパケットは、指定されたデフォルトのポートプライオリティでタグ付けされ、出力ポートで適切なプライオリティキューにソートされます。

コマンドの使用方法

- このスイッチは、各ポートに 8 つのプライオリティキューを提供します。重み付けラウンドロビンを使用して HOL ブロッキングを防止しますが、完全優先で各キューを処理するように構成することも、完全優先キューイングと重み付けキューイングを組み合わせて使用することもできます。
- デフォルトの優先度は、すべてのフレームタイプを受け入れる（つまり、タグなしフレームとタグ付きフレームの両方を受信する）ポートセットで受信したタグなしフレームに適用されます。この優先順位は、IEEE 802.1Q VLAN タグ付きフレームには適用されません。受信フレームが IEEE 802.1Q VLAN タグ付きフレームである場合、IEEE 802.1p ユーザ優先度ビットが使用されます。
- 送信ポートが関連 VLAN のタグなしメンバーである場合、これらのフレームは送信前にすべての VLAN タグが削除されます。

パラメータ

次のパラメータが表示されます。

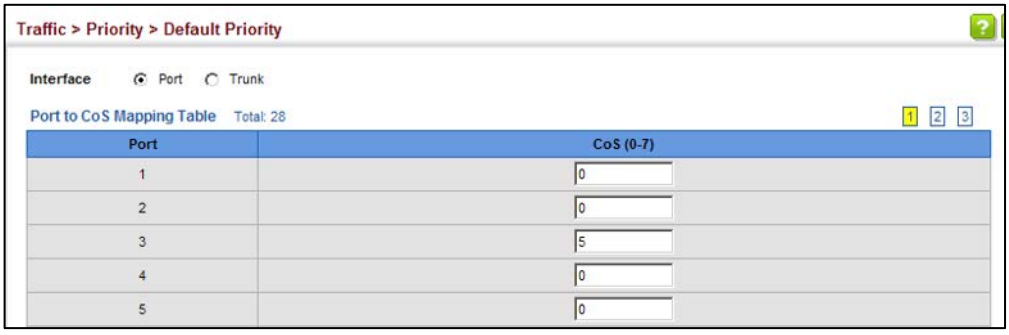
- Interface - ポートまたはトランクのリストを表示します。
- CoS - 指定されたインタフェースで受信されたタグなしフレームに割当てられる優先順位です。(範囲: 0 から 7、デフォルト: 0)

Web インタフェース

キューモードを設定するには：

1. [Traffic]、[Priority]、[Default Priority]をクリックします。
2. 表示するインタフェースタイプ（ポートまたはトランク）を選択します。
3. インタフェースのデフォルトの優先度を変更します。
4. [Apply]をクリックします。

図 9-1　デフォルトのポートプライオリティの設定



9.1.2 キューモードの選択

[Traffic]> [Priority]> [Queue]ページを使用して、任意のインタフェース上の送信キューのキューモードを設定します。スイッチは、より高い優先度のキュー内のすべてのトラフィックを処理してより低い優先度のキューを処理する必要がある完全優先ルールにもとづいてキューを処理するように設定できます。または、各キューのスケジューリング重みを指定する重み付けラウンドロビン（WRR）キューイングも設定できます。また、完全優先キューイングと重み付けキューイングの組み合わせを使用するように設定することもできます。

コマンドの使用方法

- 完全優先制御では、優先順位の低いキューが処理される前に、優先順位の高いキューのすべてのトラフィックを処理する必要があります。
- WRR キューイングは、各キューの相対的な重みを指定します。WRR は各キューにあらかじめ定義された相対的な重みを使用し、スイッチが各キューを処理してから次のキューに移動するまでのサービス時間のパーセンテージを決定します。これにより、完全優先のキューイングで発生する可能性のある HOL ブロッキングが防止されます。
- Strict and WRR モードが選択されている場合、高優先度キューには完全優先サービスが使用され、残りのキューには重み付けサービスが使用されます。完全優先制御を使用するように割当てられたキューは、Strict Mode フィールドパラメータを使用して指定する必要があります。
- 重み付けされた各キューに（したがって、対応するトラフィック優先度に）重みを割当てることができます。この重みは、各キューがサービスのためにポーリングされる頻度を設定するため、特定の優先度値が割当てられたソフトウェアアプリケーションの応答時間に影響します。
  サービス時間は、WRR のスケジューリング重み、または完全優先キューイングと重み付けキューイングの組み合わせを使用するキューイングモードの 1 つを定義することにより、送信ポートで共有されます。
- トランクポートとなるインタフェースでは、デフォルトの重み付けでの WRR モードのみ使用できます。

パラメータ

次のパラメータが表示されます。

- キューモード
  - Strict - 送信キューを順番に処理し、優先度の低いキューを処理する前に、優先度が高いキューのすべてのトラフィックを送信します。これにより、最も優先順位の高いパケットが、他のすべてのトラフィックよりも常に先にサービスされます。
  - WRR - 重み付きラウンドロビンは、スケジューリング重みを使用し、各キューをラウンドロビン方式で処理することによって、送信ポートで帯域幅を共有します。（これがデフォルトの設定です。）
  - Strict and WRR - 優先順位の高いキューに完全優先を使用し、残りのキューに WRR を使用します。
- Queue ID - 優先度キューの ID です。(範囲: 0 から 7)
- Strict Mode - 「Strict and WRR」モードが選択されている場合、完全優先サービスが高優先順位のキューに使用され、残りのキューに重み付けされたサービスが使用されます。このパラメータを使用して、Strict and WRR モードを使用するときに完全優先を使用するように割当てられたキューを指定します。(デフォルト: Disabled)
- Weight - WRR スケジューラによって使用される各キューの重みを設定します。(範囲: 1-127、デフォル

ト：重み 1,2,4,6,8,10,12、および 14 はそれぞれキュー0-7 に割当てられます）

Web インタフェース

キューモードを設定するには：

1. [Traffic]、[Priority]、[Queue]をクリックします。
2. キューモードを設定します。
3. 重み付きキューモードが選択されている場合は、必要に応じてキューの重みを変更できます。
4. 完全優先キューイングと重み付けキューイングの組み合わせを使用するキューモードが選択されている場合、最初に処理されるキューは、表の Strict Mode パラメータを有効にすることによって指定する必要があります。
5. [Apply]をクリックします。

図 9-2 キューモードの設定(Strict)

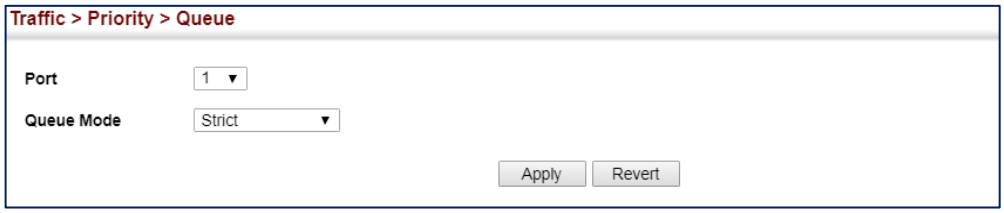


図 9-3 キューモードの設定(WRR)

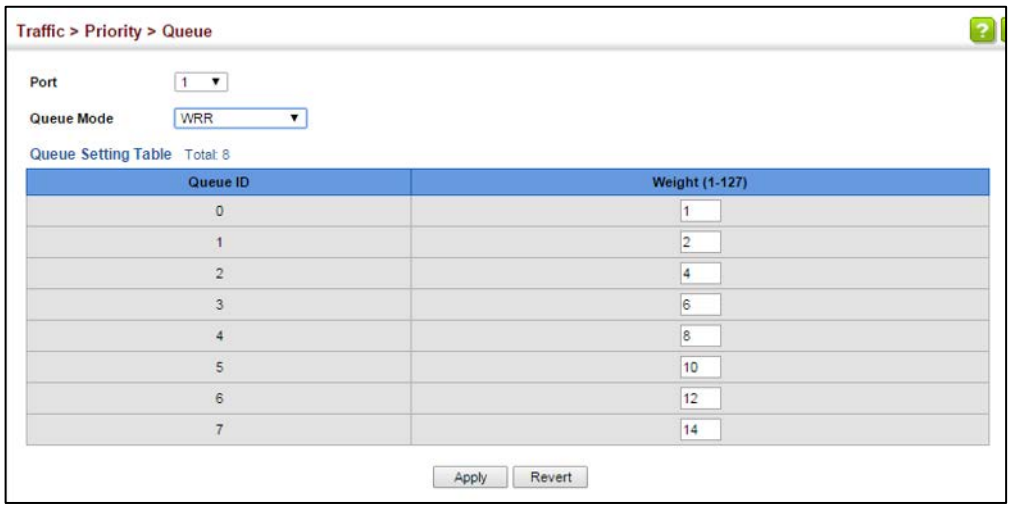
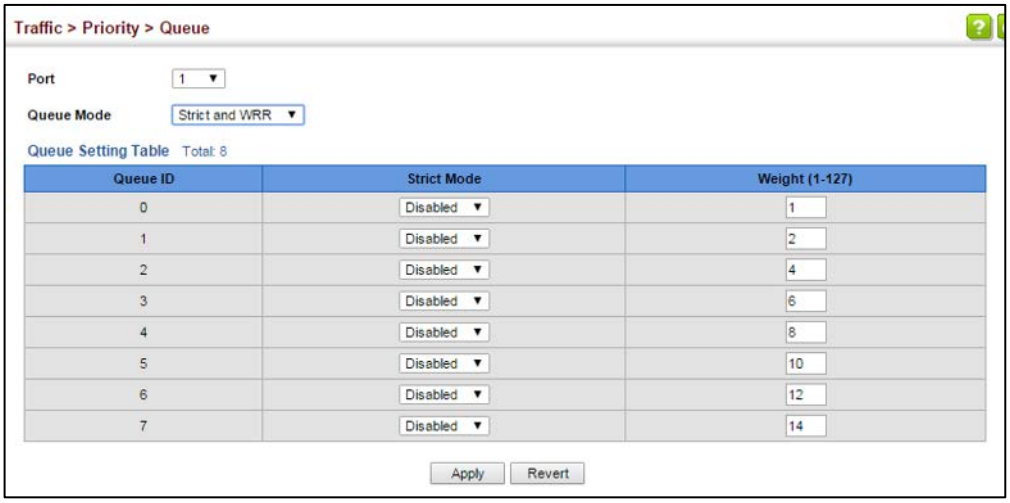


図 9-4 キューモードの設定(Strict and WRR)



9.2 レイヤ 3/4 プライオリティ設定

CoS 値へのレイヤ 3/4 プライオリティのマッピング

スイッチは、アプリケーションの要件を満たすために、レイヤ 3/4 トラフィックに優先順位を付けるいくつかの一般的な方法をサポートしています。トラフィックの優先順位は、Type of Service（ToS）オクテットの優先度ビット、または TCP / UDP ポートの番号を使用して、フレームの IP ヘッダーで指定できます。優先度ビットが使用される場合、ToS オクテットは、IP Precedence のための 3 ビットまたは Differentiated Services Code Point（DSCP）サービスのための 6 ビットを含むことができます。これらのサービスが有効になると、優先順位はスイッチによってサービスクラス値にマッピングされ、トラフィックは対応する送信キューに送信されます。

トラフィックに異なる優先度情報が含まれている可能性があるため、このスイッチは次のように優先度値を送信キューにマッピングします。優先度マッピングの優先度は DSCP Priority、次に Default Port Priority です。

Note: 受信トラフィックから内部 DSCP 値へのプライオリティ値のマッピングに使用されるデフォルト設定は、送信トラフィックに使用されるハードウェアキューを決定するものであり、プライオリティ値を置き換えるわけではありません。これらのデフォルト設定は、大部分のネットワークアプリケーションで優先制御サービスを最適化するように設計されています。特定のアプリケーションでキューイングの問題が発生しない限り、デフォルト設定を変更する必要はありません。

9.2.1 優先制御を DSCP または CoS に設定

このスイッチでは、DSCP または CoS の優先制御方法を選択できます。[Traffic]> [Priority]> [Trust Mode] ページを使用して、必要な処理方法を選択します。

コマンドの使用方法

- QoS マッピングモードが DSCP に設定され、受信パケットタイプが IPv4 または IPv6 の場合、優先制御は受信パケットの DSCP 値にもとづいて行われます。
- QoS マッピングモードが DSCP に設定され、タグがつけられた非 IP パケットを受信した場合、パケットの CoS および CFI（正規フォーマットインジケータ）値が優先制御に使用されます。タグなしパケットの場合、優先制御にはデフォルトのポート優先順位が使用されます。
- QoS マッピングモードが CoS に設定され、受信パケットタイプが IPv4 の場合、優先制御は受信パケットの CoS 値と CFI 値にもとづいて行われます。
  タグなしパケットの場合、優先制御にはデフォルトのポート優先順位が使用されます。

パラメータ

次のパラメータが表示されます。

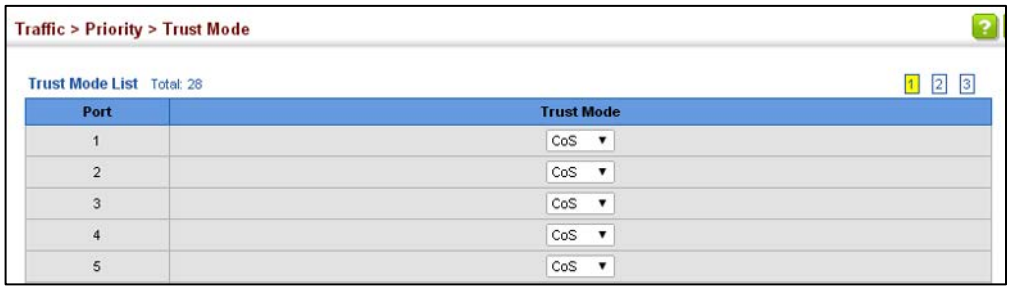
- Port - ポート識別です。(範囲: 1 から 10)
- Trust Mode
  - CoS - CoS 値を使用してレイヤ 3/4 の優先度をマッピングします。（これがデフォルトの設定です。）
  - DSCP - DSCP 値を使用してレイヤ 3/4 の優先度をマッピングします。

Web インタフェース

信頼モードを設定するには：

1. [Traffic]、[Priority]、[Trust Mode]をクリックします。
2. 任意のポートの信頼モードを設定します。
3. [Apply]をクリックします。

図 9-5 信頼モードの設定



9.2.2 ホップごとの動作への CoS 優先度マッピング

[Traffic]> [Priority]> [CoS to Queue]ページを使用して、受信パケットの CoS / CFI 値を優先制御のためのホップ単位の動作にマッピングします。

コマンドの使用方法

◆ CoS / CFI と Queue / CFI 値のデフォルトマッピングを以下に示します。

表 9-1 キュー/ CFI への CoS / CFI 値のデフォルトマッピング

CFI CoS	0	1
0	2	2
1	0	0
2	1	1
3	3	3
4	4	4
5	5	5
6	6	6
7	7	7

◆ CoS / CFI ペア値のホップ単位の動作を入力します。

◆ パケットが 802.1Q ヘッダーと共に受信するが IP パケットでない場合、
処理の優先順位を生成するために CoS / CFI-to-Queue マッピングテーブルが使用されます。元のパケットの優先度タグは、本コマンドで変更されないことに注意してください。

◆ 設定はすべてのインタフェースに適用されます。

パラメータ

次のパラメータが表示されます。

◆ Port - ポートを指定します。

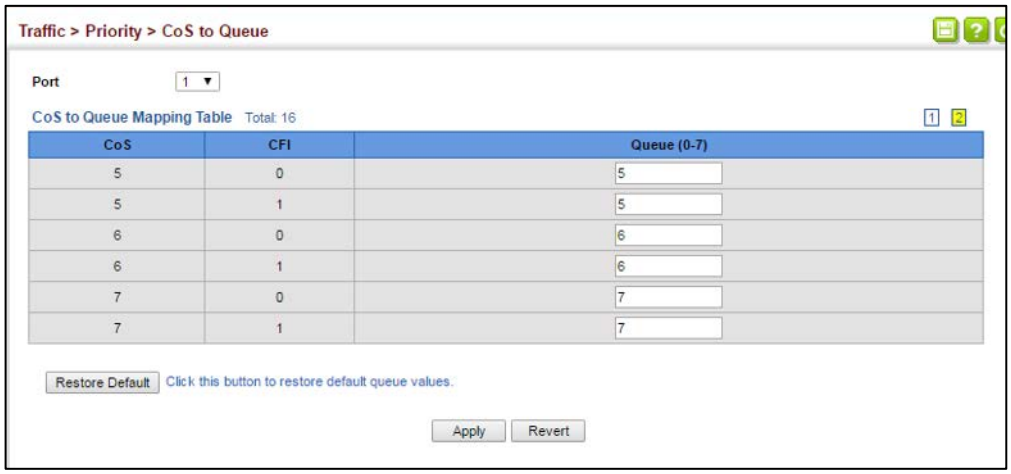
- CoS - 受信パケットの CoS 値です。(範囲: 0 から 7)
- CFI - 正規フォーマットインジケータです。このパラメータを "0"に設定すると、フレームで搬送される MAC アドレス情報が正規フォーマットになっていることを示します。(範囲: 0 から 1)
- Queue - ホップごとの動作、またはこのルータホップに使用されるプライオリティです。(範囲: 0 から 7)

Web インタフェース

CoS / CFI 値をキューの優先順位にマッピングするには：

1. [Traffic]、[Priority]、[CoS to Queue]をクリックします。
2. CoS / CFI の組み合わせのいずれかのキューを設定します。
3. [Apply]をクリックします。

図 9-6 CoS からキューへのマッピングの設定



9.2.3 ホップごとの動作への DSCP 優先度マッピング

[Traffic]> [Priority]> [DSCP to Queue]ページを使用して、受信パケットの DSCP 値を優先制御のためのホップ単位の動作にマッピングします。

DSCP は 6 ビット幅であり、64 までの異なる転送動作のコーディングが可能です。DSCP は ToS ビットを置き換えますが、3 つの優先度ビットとの下位互換性を維持するため、非 DSCP 対応の ToS 対応デバイスは DSCP マッピングと競合しません。ネットワークポリシーにもとづいて、異なる種類のトラフィックを異なる種類の転送用にマークすることができます。

コマンドの使用方法

- DSCP 値 0 から 63 の任意のホップ単位の動作を入力します。
- このマップは、プライオリティマッピングモードが DSCP に設定され、受信パケットタイプが IPv4 または IPv6 の場合にのみ使用されます。信頼モードが DSCP に設定されていない限り、DSCP とキューのマップを設定しようとする試みはスイッチによって受け入れられません。
- 2 つの QoS ドメインは異なる DSCP 定義を持つことができるため、DSCP-to-Queue マップを使用して、別のドメインの定義に一致する 1 組の DSCP 値を変更できます。ミューテーションマップは、QoS 管理ドメインの境界にある受信ポートで適用する必要があります。
- 設定はすべてのインタフェースに適用されます。

パラメータ

次のパラメータが表示されます。

- Port - ポートを指定します。
- DSCP - 受信パケットの DSCP 値(範囲: 0 から 63)
- Queue - ホップごとの動作、またはこのルータホップに使用されるプライオリティです。(範囲: 0 から 7)

表 9-2 キュー/ CFI への DSCP 値のデフォルトマッピング

ingress-dscp1 ingress-dscp10	0	1	2	3	4	5	6	7	8	9
0	2	2	2	2	2	2	2	2	0	0
1	0	0	0	0	0	0	1	1	1	1
2	1	1	1	1	3	3	3	3	3	3
3	3	3	4	4	4	4	4	4	4	4
4	5	5	5	5	5	5	5	5	6	6
5	6	6	6	6	6	6	7	7	7	7
6	7	7	7	7						

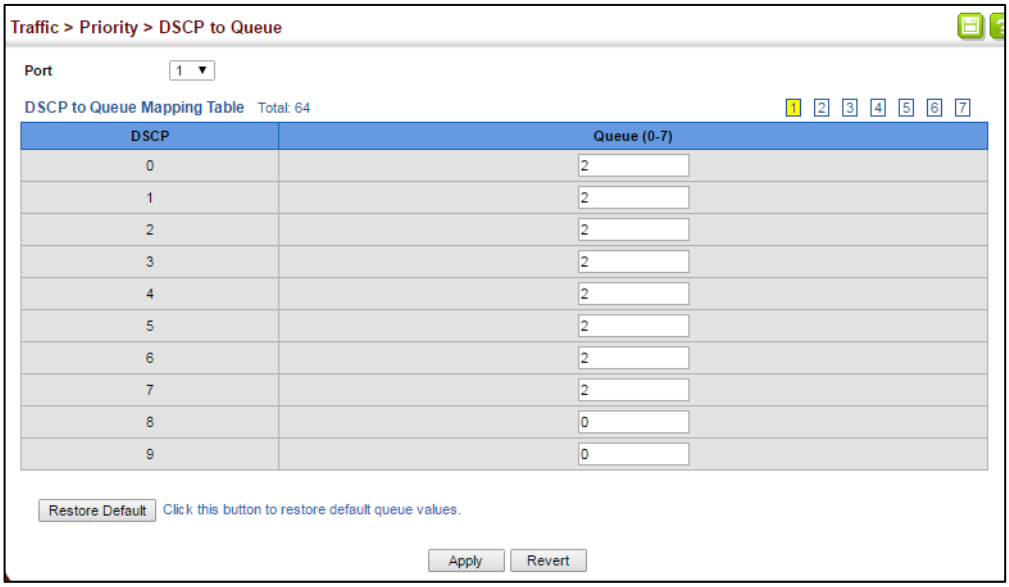
受信 DSCP は、ingress-dscp10（左桁の最上位桁）と ingress-dscp1（最下桁の最上位桁（つまり、ingress-dscp = ingress-dscp10 * 10 + ingress-dscp1）で構成されます。 対応するキュー/ cfi がテーブル内の交差するセルに表示されます。

Web インタフェース

DSCP 値を内部優先制御キューにマッピングするには:

1. [Traffic]、[Priority]、[DSCP to Queue]をクリックします。
2. 設定するポートを選択します。
3. 任意の DSCP 値のキューを設定します。
4. [Apply]をクリックします。

図 9-7 DSCP とキューマッピングの設定



10 QoS

本章では、QoS ポリシーを適用するために必要な次のタスクについて説明します。

- Class Map - 特定のトラフィッククラスを識別するマップを作成します。
- Policy Map - 受信トラフィックの監視に使用される境界パラメータと、適合トラフィックのために実行するアクションを設定します。
- Binding to a Port - 受信ポートにポリシーマップを適用します。

10.1 概要

このセクションで説明するコマンドは、Quality of Service（QoS）分類基準とサービスポリシーを設定するために使用されます。Differentiated Services（DiffServ）は、ホップごとに特定のトラフィックタイプの要件を満たすためにネットワークリソースを優先順位付けするために使用されたポリシーベースの管理メカニズムを提供します。各パケットは、アクセスリスト、IP Precedence、DSCP 値、VLAN リスト、または CoS 値にもとづいてネットワークから受信する際に分類されます。アクセスリストを使用すると、各パケットに含まれるレイヤ 2、レイヤ 3、またはレイヤ 4 の情報にもとづいてトラフィックを選択できます。設定されたネットワークポリシーにもとづいて、異なる種類のトラフィックを異なる種類の転送にマーキングすることができます。

インターネットにアクセスするすべてのスイッチまたはルータは、クラス情報に依存して、同じクラスのパケットに同じ転送処理を提供します。クラス情報は、エンドホスト、パス上のスイッチまたはルータによって割当てられます。優先度は、一般ポリシーまたはパケットの詳細な検査にもとづいて割当てることができます。ただし、パケットの詳細な検査はネットワークのエッジの近くで行う必要があり、コアスイッチとルータに過負荷がかからないようにする必要があります。

パスに沿ったスイッチおよびルータは、クラス情報を使用して、異なるトラフィッククラスに割当てられたリソースに優先順位を付けることができます。個々のデバイスが DiffServ アーキテクチャでトラフィックを処理する方法は、ホップごとの動作と呼ばれます。一貫したエンドツーエンドの QoS ソリューションを構築するには、パスに沿ったすべてのデバイスを一貫した方法で設定する必要があります。

Note: クラスマップごとに最大 16 のルールを設定できます。また、ポリシーマップに複数のクラスを含めることもできます。

Note: ポリシーマップを作成する前に、クラスマップを作成する必要があります。クラスマップを作成していない場合、ポリシーで選択できません。

コマンドの使用方法

特定のカテゴリまたは受信トラフィックのサービスポリシーを作成するには、次の手順を実行します。

1. [Configure Class（Add）]ページを使用して、特定のカテゴリのトラフィッククラス名を指定します。
2. [Configure Class（Add Rule）]ページを使用して、アクセスリスト、DSCP または IP Precedence 値、VLAN、または CoS 値にもとづいてトラフィックタイプを指定する各クラスのルールを編集します。
3. [Configure Policy（Add）]ページを使用して、受信トラフィックを処理する特定の方法のポリシー名を指定します。
4. [Configure Policy（Add Rule）]ページを使用して、1 つ以上のクラスをポリシーマップに追加します。一致するトラフィッククラスに割当てる QoS 値（CoS または IP DSCP）を Apply することによって、各クラスにポリシールールを割当てます。次に、適合するトラフィックに対して実行するアクションを指定します。
5. [Configure Interface]ページを使用して、特定のインタフェースにポリシーマップを割当てます。

Note: ポリシーマップには、最大 16 のクラスを含めることができます。

10.2 クラスマップの設定

クラスマップは、パケットを指定されたクラスに照合するために使用されます。[Traffic]> [DiffServ（Configure Class）]ページを使用して、クラスマップを設定します。

コマンドの使用方法

- クラスマップは、パケット分類、サービスタグ付け、および帯域幅ポリシングを定義する特定のインタフェースのサービスポリシーを作成するためのポリシーマップとともに使用されます。1 つ以上のクラスマップをポリシーマップに割当てることができます。
- 最大 32 のクラスマップを設定できます。

パラメータ

次のパラメータが表示されます。

Add

- Class Name - クラスマップの名前です。(範囲: 1 から 32 文字)
- Type - クラスマップごとに 1 つの match コマンドだけが許可されるので、match-any フィールドは単独の match コマンドで指定された基準を参照します。
- Description - クラスマップの簡単な説明です。(範囲: 1 から 64 文字)

Add Rule

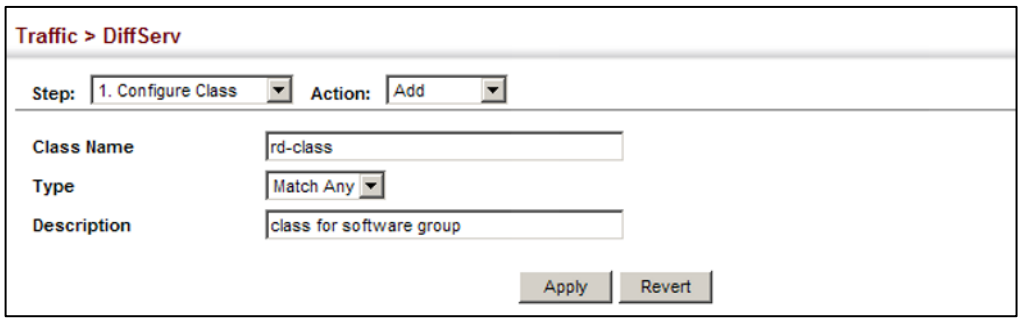
- Class Name - クラスマップの名前です。
- Type - クラスマップごとに 1 つの match コマンドだけが許可されるので、match-any フィールドは単独の match コマンドで指定された基準を参照します。
- ACL - アクセス制御リストの名前です。標準または拡張 IPv4 / IPv6 ACL および MAC ACL から任意のタイプの ACL を指定できます。
- IP DSCP - DSCP 値です。(範囲: 0 から 63)
- IP Precedence - IP precedence 値です。(範囲: 0 から 7)
- IPv6 DSCP - IPv6 パケットに含まれる DSCP 値です。(範囲: 0 から 63)
- VLAN ID - VLAN です。（範囲:1 から 4094）
- CoS - CoS 値です。(範囲: 0 から 7)

Web インタフェース

クラスマップを設定するには：

1. [Traffic]、[DiffServ]をクリックします。
2. 「Step」リストから「Configure Class」を選択します。
3. [Action]リストから[Add]を選択します。
4. クラス名を入力します。
5. 説明を入力します。
6. [Apply]をクリックします。

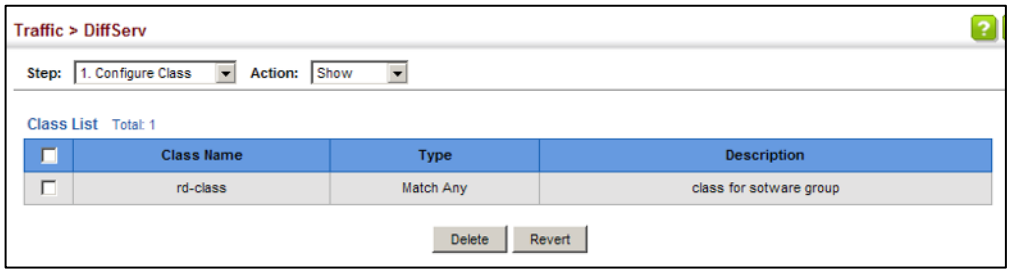
図 10-1 クラスマップの設定



設定済みのクラスマップを表示するには：

1. [Traffic]、[DiffServ]をクリックします。
2. 「Step」リストから「Configure Class」を選択します。
3. [Action]リストから[Show]を選択します。

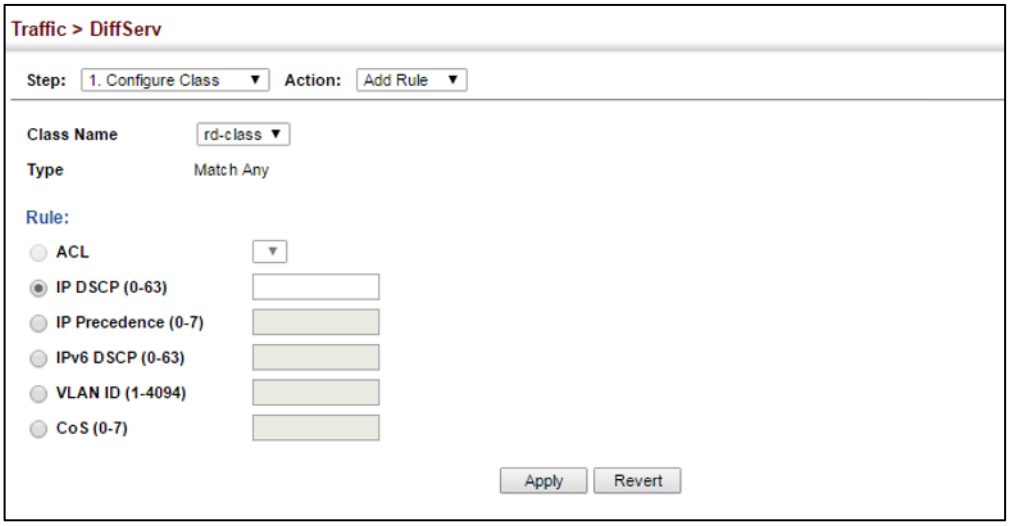
図 10-2 クラスマップの表示



クラスマップのルールを編集するには：

1. [Traffic]、[DiffServ]をクリックします。
2. 「Step」リストから「Configure Class」を選択します。
3. [Action]リストから[Add Rule]を選択します。
4. クラスマップの名前を選択します。
5. アクセスリスト、DSCP または IP Precedence 値、VLAN、または CoS 値にもとづいて、このクラスのトラフィックタイプを指定します。受信トラフィックをクラスマップに割当てる際、合致させるルールを最大 16 項目設定できます。
6. [Apply]をクリックします。

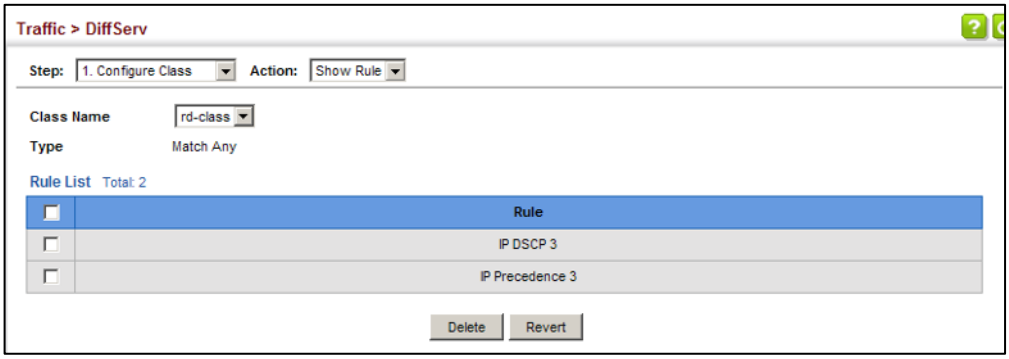
図 10-3 クラスマップへのルールの追加



クラスマップのルールを表示するには：

1. [Traffic]、[DiffServ]をクリックします。
2. 「Step」リストから「Configure Class」を選択します。
3. [Action]リストから「Show Rule」を選択します。

図 10-4 クラスマップのルールを表示



クラスマップのルールを削除するには：

1. 削除したい[Rule]を選択します。Rule List 単位での削除はできません。
2. [Delete]をクリックします。

10.3 QoS ポリシーの作成

[Traffic]> [DiffServ（Configure Policy）]ページを使用して、複数のインタフェースに割り当てられるポリシーマップを作成します。ポリシーマップは、1 つまたは複数のクラスマップステートメントをグループ化するために使用されます。ポリシーマップは、サービスポリシーによって 1 つまたは複数のインタフェースに割り当てられます。

QoS ポリシーを設定するには、いくつかの手順が必要です。まず、アクセスリスト、DSCP または IP Precedence 値、特定の VLAN のメンバー、または CoS 値に従って受信パケットを照合する方法を示すクラスマップを設定する必要があります。ポリシーマップは、受信トラフィックを監視するために使用される境界パラメータと、適合トラフィックに対して行うアクションを最初に設定する必要があります。ポリシーマップは、以前に定義されたクラスマップにもとづいて 1 つまたは複数のクラスを含むことができる。

パラメータ

次のパラメータが表示されます。

Add

- Policy Name - ポリシーマップの名前です。(範囲: 1 から 32 文字)
- Description - ポリシーマップの簡単な説明です。(範囲: 1 から 64 文字)

Add Rule

- Policy Name - ポリシーマップの名前です。
- Class Name - ポリシーが動作するトラフィック分類を定義するクラスマップの名前です。ポリシーマップには、最大 32 のクラスマップを含めることができます。
- Action - この属性は、一致するパケットのハードウェア内の内部 QoS 値を設定するために使用されます。
  - Set CoS - 一致するパケット（クラスマップのルール設定で指定）に内部 CoS 値を設定することにより、受信トラフィックに提供されるサービスを設定します。(範囲: 0 から 7)
    （「表 9-1　キュー/ CFI への CoS / CFI 値のデフォルトマッピング」を参照してください。)
  - Set IP DSCP - 一致するパケット（クラスマップのルール設定で指定）の内部 DSCP 値を設定することにより、受信トラフィックに提供されるサービスを設定します。(範囲: 0 から 63)
    （「表 9-2　キュー/ CFI への DSCP 値のデフォルトマッピング」を参照してください。)
- Meter - これをチェックして最大帯域を定義します。
- Meter Mode (レート制限) - 受信ポートに帯域制限を適用します。この機能により、ネットワーク管理者は、インタフェース上で受信されるトラフィックの最大帯域を制御できます。帯域制限は、ネットワークのエッジのインタフェースに設定され、ネットワークとの間のトラフィックを制限します。許容されるトラフィック量を超えるパケットは廃棄されます。
- Rate - 帯域制限レベルを設定します。(範囲: 64～1,000,000 kbits /秒）

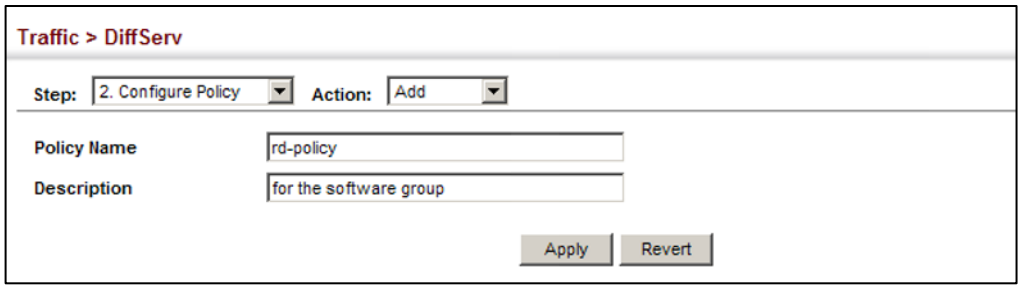
Web インタフェース

ポリシーマップを設定するには

1. [Traffic]、[DiffServ]をクリックします。
2. [Step]リストから[Configure Policy]を選択します。
3. [Action]リストから[Add]を選択します。
4. ポリシー名を入力します。

5. 説明を入力します。
6. [Apply]をクリックします。

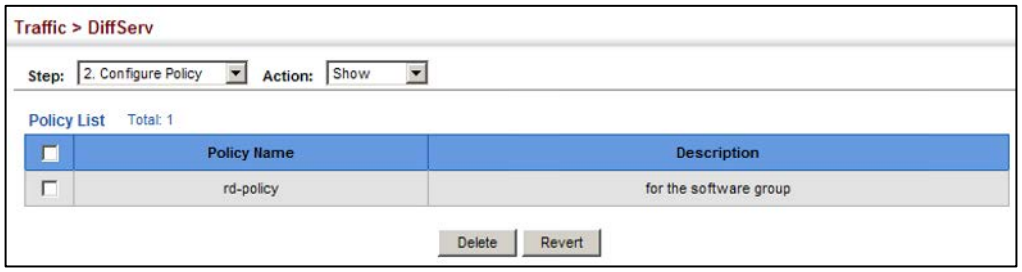
図 10-5 ポリシーマップの設定



設定済みのポリシーマップを表示するには、

1. [Traffic]、[DiffServ]をクリックします。
2. [Step]リストから[Configure Policy]を選択します。
3. [Action]リストから[Show]を選択します。

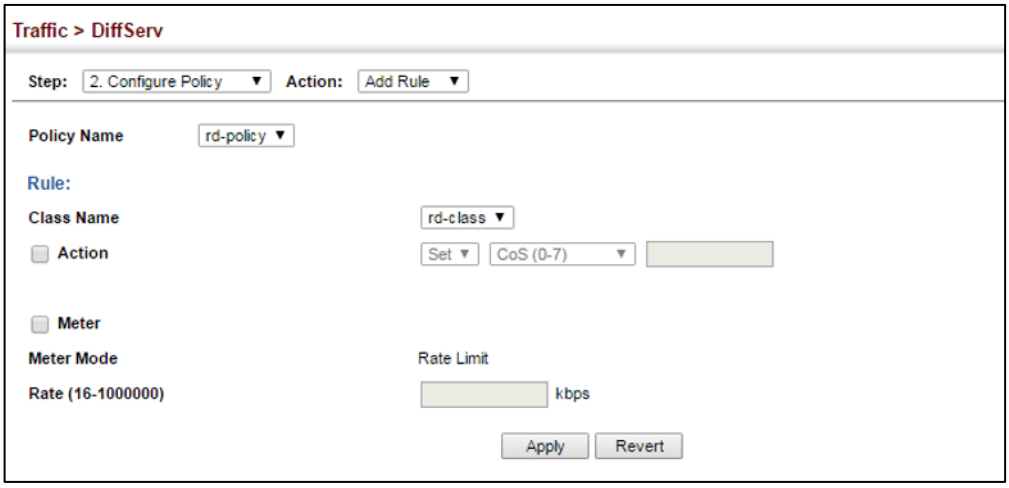
図 10-6 ポリシーマップの表示



ポリシーマップのルールを編集するには：

1. [Traffic]、[DiffServ]をクリックします。
2. [Step]リストから[Configure Policy]を選択します。
3. [Action]リストから[Add Rule]を選択します。
4. ポリシーマップの名前を選択します。
5. 一致するトラフィッククラスに割当てる QoS を指定するために、一致するパケットの CoS またはホップごとの動作を設定します。必要に応じてレート制限を入力します。
6. [Apply]をクリックします。

図 10-7 ポリシーマップへのルールの追加



ポリシーマップのルールを表示するには：

1. [Traffic]、[DiffServ]をクリックします。
2. [Step]リストから[Configure Policy]を選択します。
3. [Action]リストから「Show Rule」を選択します。

図 10-8 ポリシーマップのルールの表示

10.4 ポートへのポリシーマップの割り当て

[Traffic]> [DiffServ（Configure Interface）]ページを使用して、ポリシーマップをポートに割り当てます。

コマンドの使用方法

まず、クラスマップを定義し、ポリシーマップを定義してから、サービスポリシーを必要なインタフェースに割り当てます。

パラメータ

次のパラメータが表示されます。

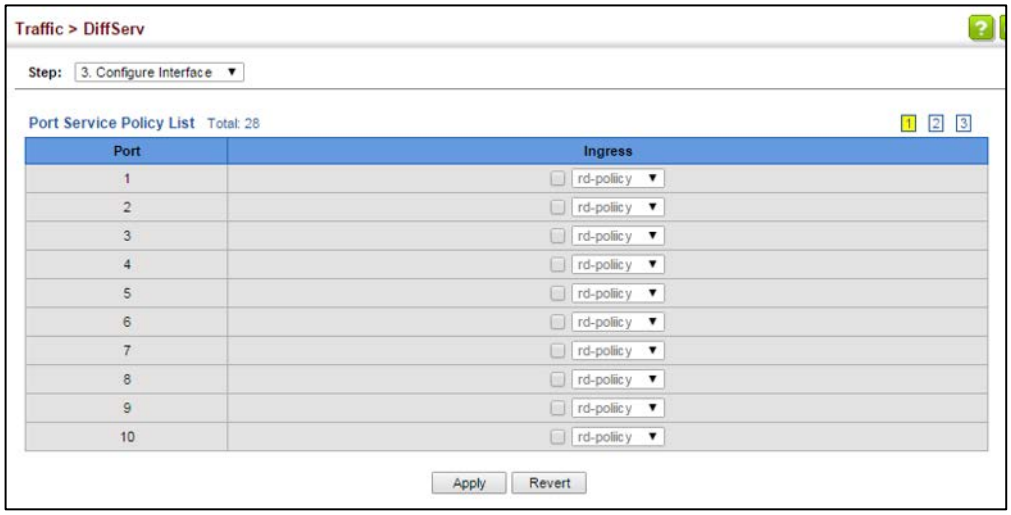
- Port - ポートを指定します。
- Ingress - 選択したルールを受信トラフィックに適用します。

Web インタフェース

ポリシーマップをポートに割り当てるには、次の手順を実行します。

1. [Traffic]、[DiffServ]をクリックします。
2. [Step]リストから[Configure Interface]を選択します。
3. [Ingress]フィールドの下にあるチェックボックスをオンにして、ポートのポリシーマップを有効にします。
4. スクロールダウンボックスからポリシーマップを選択します。
5. [Apply]をクリックします。

図 10-9 ポートへのポリシーマップの付加



11 セキュリティの設定

ローカルまたはリモート認証方式を使用して管理アクセス用にシステムにログインするユーザを認証するように、このスイッチを設定できます。このスイッチは、次のオプションを使用して安全なネットワーク管理アクセスを提供します。

- AAA - ローカルまたはリモート認証を使用してアクセス権を設定し、認証サーバを指定し、リモート認証とアカウンティングを設定します。
- User Accounts - 指定されたユーザのスイッチでアクセス権を手動で設定します。
- Network Access - MAC 認証、侵入応答、動的 VLAN 割当て、および動的 QoS 割当てを設定します。
- HTTPS - 安全な Web 接続を提供します。
- SSH - 安全なシェル（セキュアな Telnet アクセス用）を提供します。
- ACL - アクセスコントロールリストは、アドレス、プロトコル、レイヤ 4 プロトコルポート番号または TCP 制御コードにもとづいて、IP フレームのパケットフィルタリングを提供します。
- IP Filter - Web、SNMP、または Telnet インタフェースへの管理アクセスをフィルタリングします。
- Port Security - 個々のポートのセキュアアドレスを設定します。
- DoS Protection - サービス拒否攻撃から保護します。
- DHCP Snooping - DHCP スヌーピングによって送信元アドレスを識別できない、安全でないポート上の IP トラフィックをフィルタリングします。
- IPv4 Source Guard - DHCPv4 スヌーピングまたは静的ソースバインディングを介して送信元アドレスを識別できない、安全でないポートで IPv4 トラフィックをフィルタリングします。
- ARP Inspection - アドレス解決プロトコルパケットの MAC アドレスバインディングを検証するセキュリティ機能。無効な MAC から IP アドレスへのバインディングによる ARP トラフィックに対する保護を提供します。これは特定の「man-in-the-middle」攻撃の基礎を形成します。

Note: これからのフィルタリングコマンドの実行の優先順位は、ポートセキュリティ、ポート認証、ネットワークアクセス、アクセス制御リスト、DHCP 送信元ガード、DHCP スヌーピングです。

11.1 AAA (Authentication, Authorization and Accounting)

認証、承認、およびアカウンティング（AAA）機能は、スイッチのアクセス制御を設定するための主要なフレームワークを提供します。3 つのセキュリティ機能は、以下のように要約できます。

- Authentication — ネットワークへのアクセスを要求するユーザを識別します。
- Authorization — ユーザが特定のサービスにアクセスできるかどうかを決定します。
- Accounting — ユーザがネットワーク上でアクセスしたサービスのレポート、監査、請求を提供します。

AAA 機能では、ネットワーク内に設定された RADIUS サーバまたは TACACS +サーバを使用する必要があります。セキュリティサーバは、指定されたサービスへのユーザアクセスを制御する方法として適用されます。いずれかの時点で認証または非認証が戻された場合、プロセスは停止します。

スイッチは、次の AAA 機能をサポートしています。

- コンソールおよび Telnet を使用して、スイッチ上の管理インタフェースにアクセスするユーザのアカウンティング。
- ユーザが特定の CLI Privileged レベルで入力するコマンドのアカウンティング。
- コンソールおよび Telnet を使用して、スイッチ上の管理インタフェースにアクセスするユーザの承認。

スイッチ上で AAA を設定するには、次の一般的な手順に従う必要があります。

1. RADIUS および TACACS +サーバへのアクセスパラメータを設定します。
2. サービスのアカウンティングおよび承認をサポートする RADIUS および TACACS +サーバグループを定義します。
3. アカウンティングまたは承認を適用し、使用する RADIUS または TACACS +サーバグループを指定する各サービスのメソッド名を定義します。
4. ポートまたはラインインタフェースにメソッド名を適用します。

Note: このガイドでは、RADIUS サーバと TACACS +サーバが AAA をサポートするように設定されていることを前提としています。RADIUS および TACACS +サーバソフトウェアの設定は、このガイドの範囲外です。RADIUS または TACACS +サーバソフトウェアに付属のマニュアルを参照してください。

Note: 定義されたグループの最初のサーバに要求が送信され、応答がない場合は 2 番目のサーバが試行されるような複数のサーバによる優先度付けされたサーバグループの設定は、将来サポート予定です。

11.1.1 ローカル/リモートログオン認証の設定

[Security]> [AAA]> [System Authentication]ページを使用して、ローカル認証またはリモート認証を指定します。ローカル認証は、スイッチ上において手動で設定されたユーザ名とパスワードにもとづいて管理アクセスを制限します。リモート認証では、RADIUS または TACACS +プロトコルに基づくリモートアクセス認証サーバを使用して、管理アクセスを確認します。

コマンドの使用方法

- デフォルトでは、スイッチに格納された認証データベースに対して常に管理アクセスがチェックされます。リモート認証サーバを使用する場合は、認証シーケンスを指定する必要があります。次に、[Security]> [AAA]> [Server]ページを使用して、リモート認証プロトコルに対応するパラメータを指定

します。ローカルおよびリモートのログオン認証は、コンソールポート、Web ブラウザ、または Telnet 経由の管理アクセスを制御します。

◆ 任意のユーザが認証シーケンスを示すために、最大 3 つの認証方法を指定できます。たとえば、(1) RADIUS、(2) TACACS、および (3) Local を選択すると、RADIUS サーバのユーザ名とパスワードが最初に確認されます。RADIUS サーバが使用できない場合、TACACS +サーバを使用して認証が試行され、最後にローカルユーザ名とパスワードが確認されます。

パラメータ

次のパラメータが表示されます。

◆ Authentication Sequence - 必要な認証または認証シーケンスを選択します。

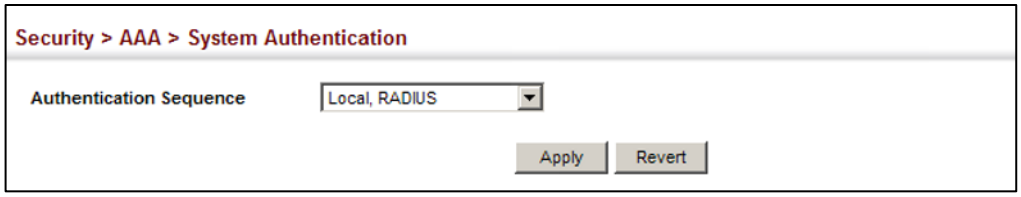
- Local - ユーザ認証は、スイッチに格納された認証データベースのみを使用して実行されます。
- RADIUS - ユーザ認証は、RADIUS サーバのみを使用して実行されます。
- TACACS - ユーザ認証は、TACACS +サーバのみを使用して実行されます。
- [authentication sequence] - ユーザ認証は、示された順序で最大 3 つの認証方法によって実行されます。

Web インタフェース

管理アクセスを制御する方法を設定するには：

1. [Security]、[AAA]、[System Authentication]の順にクリックします。
2. 認証シーケンス（1 から 3 つのメソッド）を指定します。
3. [Apply]をクリックします。

図 11-1　認証シーケンスの設定

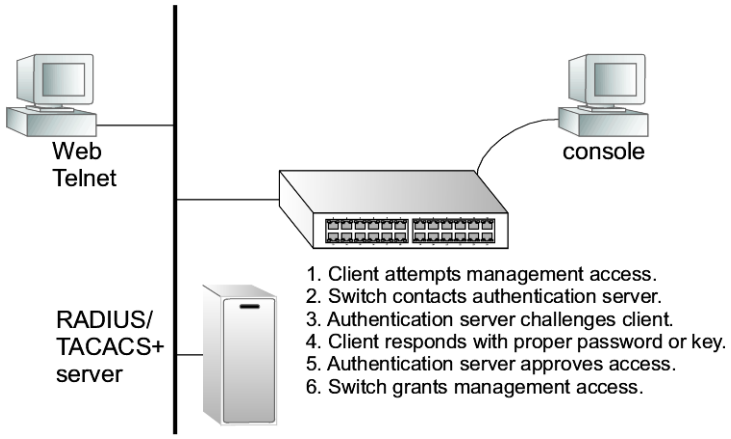


11.1.2 リモートログオン認証サーバの設定

[Security]> [AAA]> [Server]ページを使用して、RADIUS または TACACS +リモートアクセス認証サーバのメッセージ交換パラメータを設定します。

リモート認証ダイヤルインユーザサービス（RADIUS）とターミナルアクセスコントローラアクセス制御システムプラス（TACACS +）は、ネットワーク上の RADIUS 対応または TACACS 対応デバイスへのアクセスを制御するために中央サーバ上で実行されるソフトウェアを使用するログオン認証プロトコルです。認証サーバには、スイッチへの管理アクセスが必要な各ユーザの関連する特権レベルを持つ複数のユーザ名とパスワードのペアのデータベースが含まれています。

図 11-2　認証サーバの操作



RADIUS は UDP を使用し、TACACS +は TCP を使用します。UDP はベストエフォート型の配信のみを提供し、TCP はより信頼性の高いコネクション型のトランスポートを提供します。また、RADIUS はクライアントからサーバへのアクセス要求パケットのパスワードだけを暗号化し、TACACS +はパケットの本体全体を暗号化します。

コマンドの使用方法

- リモート認証サーバを使用する場合は、リモート認証プロトコルのメッセージ交換パラメータを指定する必要があります。ローカルとリモートの両方のログオン認証は、コンソールポート、Web ブラウザ、または Telnet 経由で管理アクセスを制御します。
- RADIUS および TACACS +ログオン認証では、各ユーザ名/パスワードのペアに対して特定の特権レベルを割当てます。ユーザ名、パスワード、および特権レベルは、認証サーバで設定する必要があります。認証プロセスに使用される暗号化方法も、認証サーバとログオンクライアントの間で構成またはネゴシエートする必要があります。このスイッチは、MD5（Message-Digest 5）、TLS（Transport Layer Security）、または TTLS（Tunneled Transport Layer Security）を使用して暗号化されたサーバとクライアント間の認証メッセージを渡すことができます。

パラメータ

次のパラメータが表示されます。

Configure Server

- RADIUS
  - Global - グローバルに適用可能な RADIUS 設定を提供します。
  - Server Index - 構成可能な 5 つの RADIUS サーバの 1 つを指定します。スイッチは、リストされた一連のサーバを使用して認証を試みます。このプロセスは、サーバがユーザへのアクセスを認証または拒否すると終了します。
  - Server IP Address - 認証サーバのアドレスです。
    （この項目を表示するには、Server Index 項目を選択する必要があります。）
  - Accounting Server UDP Port - アカウンティングメッセージに使用される認証サーバ上のネットワーク（UDP）ポートです。(範囲: 1 から 65535、デフォルト: 1813)
  - Authentication Server UDP Port - 認証メッセージに使用される認証サーバ上のネットワーク（UDP）ポートです。(範囲: 1 から 65535、デフォルト: 1812)
  - Authentication Timeout - スイッチが要求を再送信するまで RADIUS サーバからの応答を待機する秒数です。(範囲: 1 から 65535、デフォルト: 5)

- Authentication Retries - スイッチが認証サーバ経由でログオンアクセスを認証しようとする回数です。(範囲: 1 から 30、デフォルト: 2)
- Set Key - このボックスにマークを付けて、暗号化鍵を設定または変更します。
- Authentication Key - クライアントのログオンアクセスを認証するために使用される暗号化鍵です。空白を含む文字列を二重引用符で囲んでください。(最長: 48 文字)
- Confirm Authentication Key - エラーが発生していないことを確認するために、前のフィールドに入力した文字列を再入力します。これらの 2 つのフィールドが一致しない場合、スイッチは暗号化鍵を変更しません。

◆ TACACS+

- Global - グローバルに適用可能な TACACS +設定を提供します。
- Server Index - 構成するサーバのインデックス番号を指定します。スイッチは現在、1 つの TACACS +サーバしかサポートしていません。
- Server IP Address - TACACS +サーバのアドレスです。
（この項目を表示するには、Server Index 項目を選択する必要があります。）
- Authentication Server TCP Port - 認証メッセージに使用される TACACS +サーバのネットワーク（TCP）ポートです。(範囲: 1 から 65535、デフォルト: 49)
- Authentication Timeout - スイッチが要求を再送信するまでに TACACS +サーバからの応答を待つ秒数です。
(範囲: 1 から 540、デフォルト: 5)
- Authentication Retries - スイッチが認証サーバ経由でログオンアクセスを認証しようとする回数です。(範囲: 1 から 30、デフォルト: 2)
- Set Key - このボックスにマークを付けて、暗号化鍵を設定または変更します。
- Authentication Key - クライアントのログオンアクセスを認証するために使用される暗号化鍵です。空白を含む文字列を二重引用符で囲んでください。(最長: 48 文字)
- Confirm Authentication Key - エラーが発生していないことを確認するために、前のフィールドに入力した文字列を再入力します。これらの 2 つのフィールドが一致しない場合、スイッチは暗号化鍵を変更しません。

Configure Group

◆ Server Type - RADIUS または TACACS +サーバを選択します。

◆ Group Name - RADIUS または TACACS +サーバグループの名前を定義します。(範囲: 1 から 64 文字)

◆ Sequence at Priority - グループに使用するサーバとシーケンスを指定します。(範囲: RADIUS の場合は 1 から 5。 TACACS の場合は 1）
サーバの優先順位を指定するときは、サーバインデックスが既に定義されている必要があります。

Web インタフェース

RADIUS 認証または TACACS +認証のパラメータを設定するには、次の手順を実行します。

1. [Security]、[AAA]、[Server]をクリックします。
2. [Step]リストから[Configure Server]を選択します。
3. RADIUS または TACACS +サーバタイプを選択します。
4. グローバルを選択して、指定したすべてのサーバにグローバルに適用するパラメータを指定するか、特定のサーバインデックスを選択して、特定のサーバに適用されるパラメータを指定します。
5. 認証鍵を設定または変更するには、[Set Key]ボックスにマークを付け、鍵を入力して確認します
6. [Apply]をクリックします。

図 11-3　リモート認証サーバの構成(RADIUS)

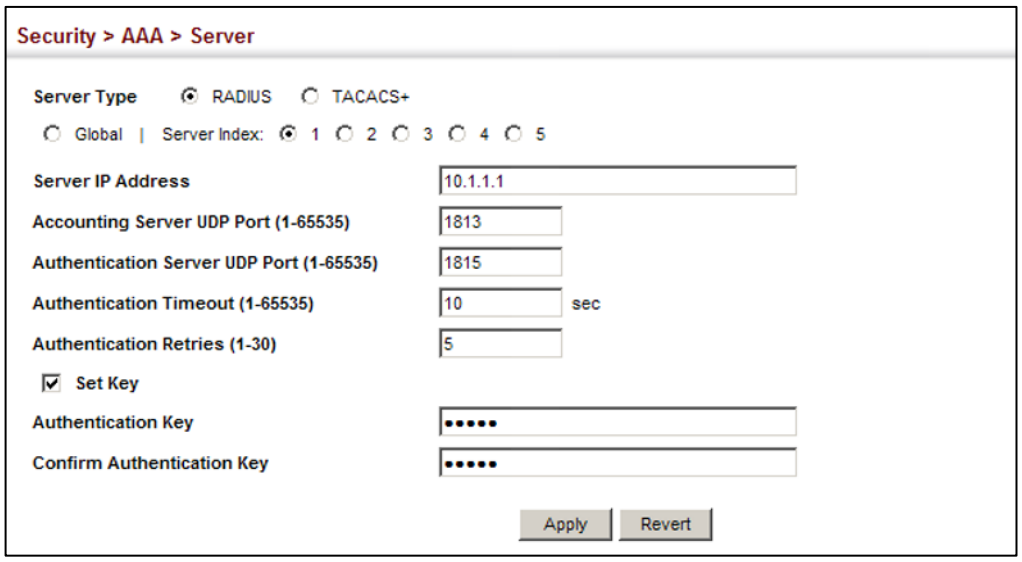
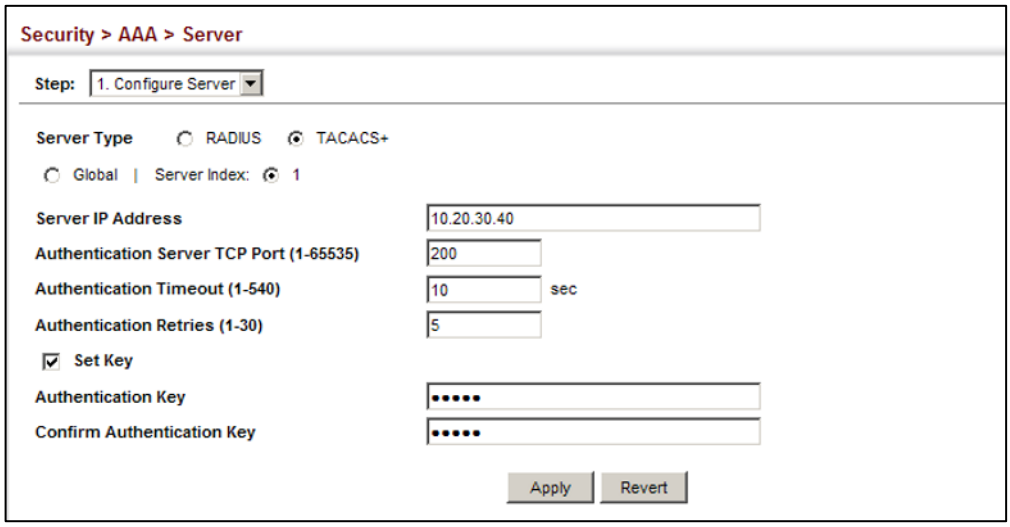


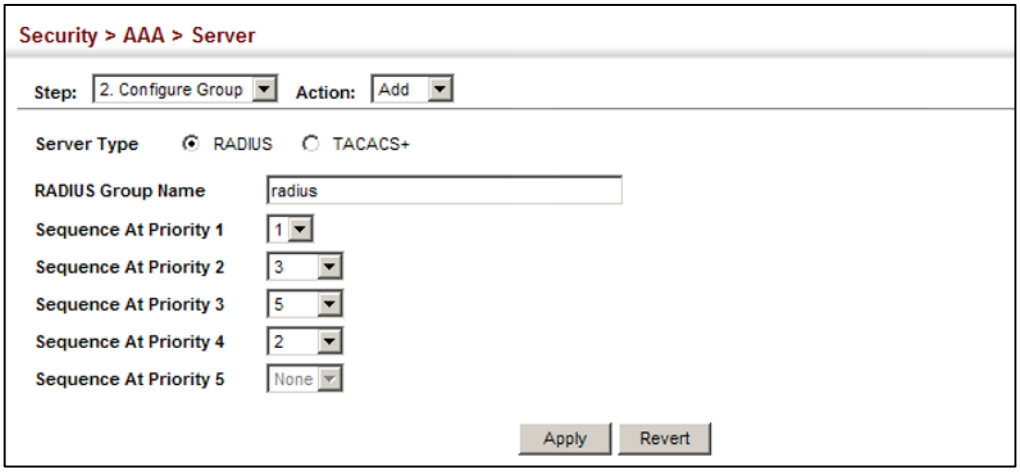
図 11-4　リモート認証サーバの構成(TACACS+)



アカウンティングと認証に使用する RADIUS または TACACS +サーバグループを設定するには：

1. [Security]、[AAA]、[Server]をクリックします。
2. [Step]リストから[Configure Group]を選択します。
3. [Action]リストから[Add]を選択します。
4. RADIUS または TACACS +サーバタイプを選択します。
5. グループ名を入力し、優先度ごとに使用するサーバのインデックスを入力します。
6. [Apply]をクリックします。

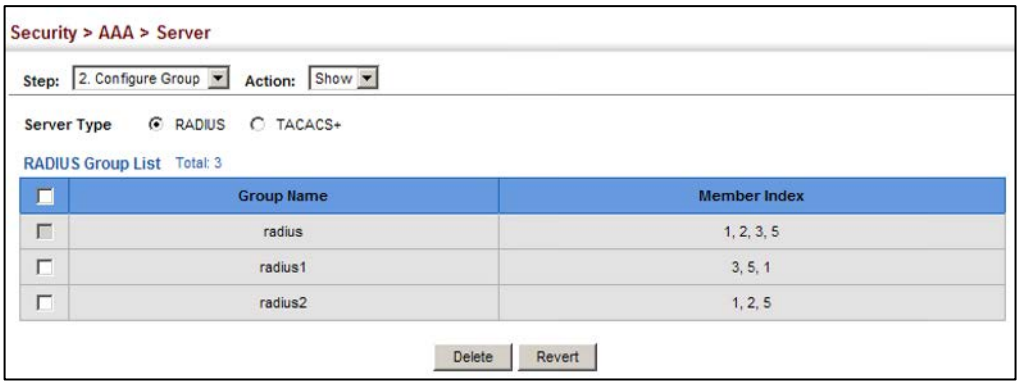
図 11-5　AAA サーバグループの設定



アカウンティングおよび認証に使用される RADIUS または TACACS +サーバグループを表示するには、次の手順を実行します。

1. [Security]、[AAA]、[Server]をクリックします。
2. [Step]リストから[Configure Group]を選択します。
3. [Action]リストから[Show]を選択します。

図 11-6　AAA サーバグループの表示



11.1.3 AAA アカウンティングの設定

[Security]> [AAA]> [Accounting]ページを使用して、アカウンティングまたはセキュリティのために要求されたサービスのアカウンティングを有効にし、設定されたアカウンティング方法、特定のインタフェースに適用される方式、およびユーザセッションに記録される基本アカウンティング情報を表示します。

コマンドの使用方法

アカウンティングが有効になる前に、RADIUS または TACACS +サーバを介した AAA 認証を有効にする必要があります。

パラメータ

次のパラメータが表示されます。

一般設定

◆ Periodic Update - ローカルアカウンティングサービスが、システム上の全ユーザ情報をアカウンティン

グサーバに更新する間隔を指定します。(範囲: 1 から 2147483647 分、デフォルト: 1 分)

Configure Method

- Accounting Type - サービスを次のように指定します。
  - Exec - ローカルコンソール、Telnet、または SSH 接続の管理アカウンティングです。
- Method Name - サービス要求のアカウンティング方法を指定します。.他のメソッドが定義されていない場合、要求されたサービスに対して「default」メソッドが使用されます。(範囲: 1 から 64 文字)
  メソッド名は、指定された RADIUS サーバまたは TACACS +サーバで設定されたアカウンティング方法を記述するためにのみ使用されることに注意してください。使用する方法についての情報はサーバに送信されません。
- Accounting Notice - ログインからログオフまでのユーザアクティビティを記録します。
- Server Group Name - アカウンティングサーバグループを指定します。(範囲: 1 から 64 文字)
  グループ名「radius」および「tacacs +」は、設定されたすべての RADIUS および TACACS +ホストを指定します。他のグループ名は、[Security]> [AAA]> [Server（Configure Group）]ページで設定されたサーバグループを参照します。

Configure Service

- Accounting Type - 前の章で説明したように、サービスを Exec として指定します。
- Exec
  - Console Method Name - コンソール接続に適用するユーザ定義のメソッド名を指定します。
  - VTY Method Name - Telnet 接続と SSH 接続に適用するユーザ定義のメソッド名を指定します。

Show Information - Summary

- Accounting Type - アカウンティングサービスを表示します。
- Method Name - ユーザ定義またはデフォルトのアカウンティング方法を表示します。
- Server Group Name - アカウンティングサーバグループを表示します。
- Interface - これらのルールが適用されるポート、コンソール、または Telnet インタフェースを表示します。（アカウンティング方法および関連するサーバグループがインタフェースに割当てられていない場合は、このフィールドは空白になります）。

Show Information - Statistics

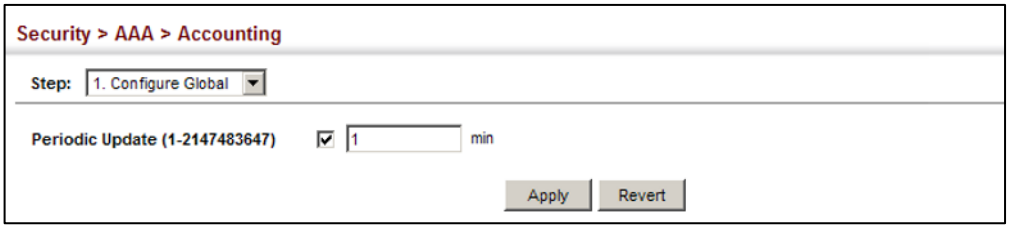
- User Name - 登録されたユーザ名を表示します。
- Accounting Type - アカウンティングサービスを表示します。
- Interface -ユーザがスイッチに接続しているポート番号を表示します。
- Time Elapsed - このエントリがアクティブであった時間を表示します。

Web インタフェース

AAA アカウンティングのグローバル設定を設定するには、

1. [Security]、[AAA]、[Accounting]をクリックします。
2. [Step]リストから[Configure Global]を選択します。
3. 必要な更新間隔を入力します。
4. [Apply]をクリックします。

図 11-7　AAA アカウンティングのグローバル設定の設定



様々なサービスの種類と割当てられたサーバグループに適用されるアカウンティング処理方法を設定するには：

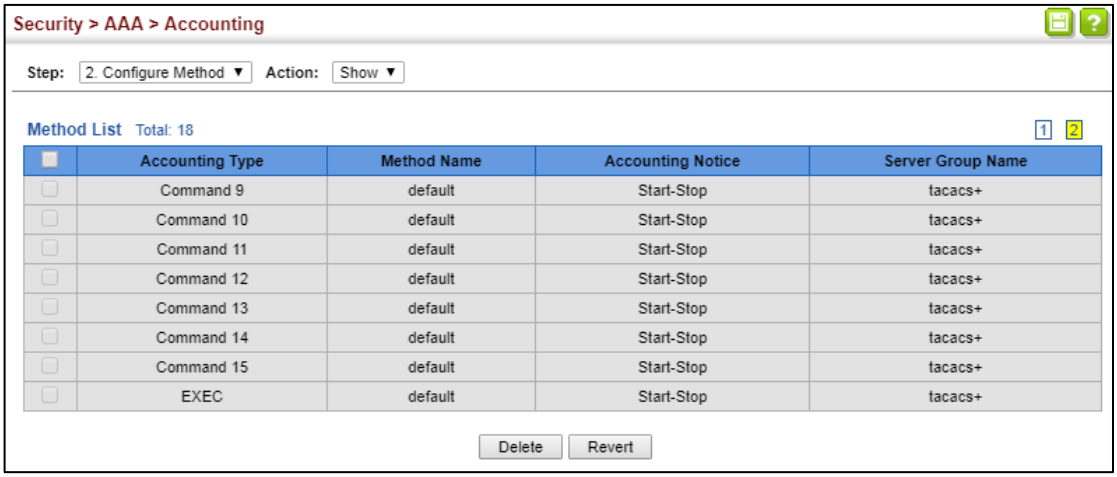
1. [Security]、[AAA]、[Accounting]をクリックします。
2. 「ステップ」リストから「メソッドの構成」を選択します。
3. [Action]リストから[Add]を選択します。
4. アカウンティングタイプ（Exec）を選択します。
5. アカウンティング方法の名前とサーバグループ名を指定します。
6. [Apply]をクリックします。

図 11-8　AAA アカウンティング方法の設定

様々なサービスの種類と割当てられたサーバグループに適用されるアカウンティング処理方法を表示するには：

1. [Security]、[AAA]、[Accounting]をクリックします。
2. [Step]リストから[Configure Method]を選択します。
3. [Action]リストから[Show]を選択します。

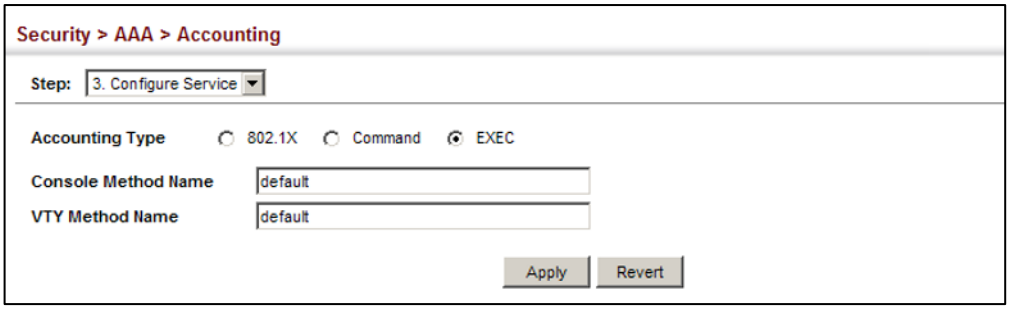
図 11-9　AAA カウンティング方式の表示



特定のインタフェース、特定の特権レベルで入力されたコンソールコマンド、およびローカルコンソール、Telnet、または SSH 接続に適用されるアカウンティング方法を設定するには、

1. [Security]、[AAA]、[Accounting]をクリックします。
2. [Step]リストから[Configure Service]を選択します。
3. アカウンティングタイプ（Exec）を選択します。
4. 必要なアカウンティング方法を入力します。
5. [Apply]をクリックします。

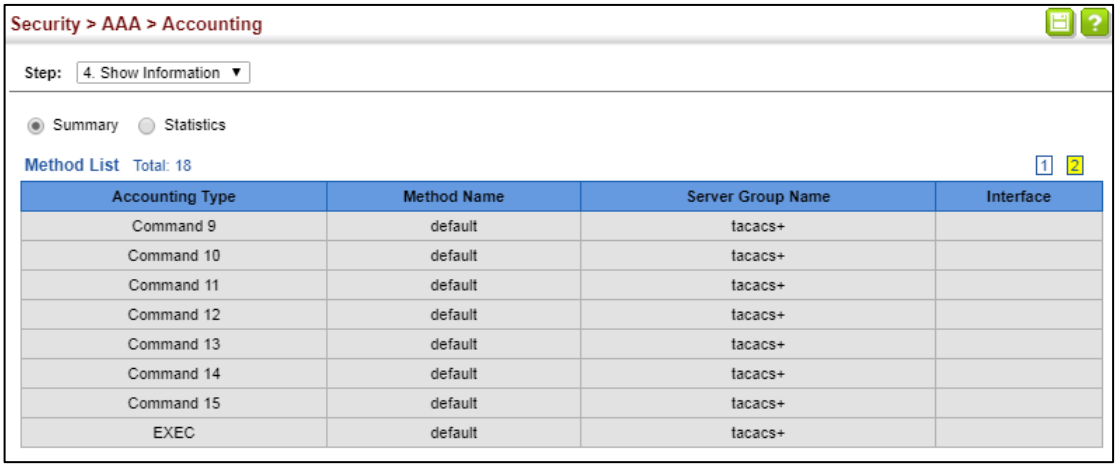
図 11-10　EXEC サービスの AAA アカウンティングサービスの設定



指定されたサービスタイプに対して、設定されたアカウンティング方法と割当てられたサーバグループの概要を表示するには、次の手順を実行します。

1. [Security]、[AAA]、[Accounting]をクリックします。
2. [Step]リストから[Show Information]を選択します。
3. [Summary]をクリックします。

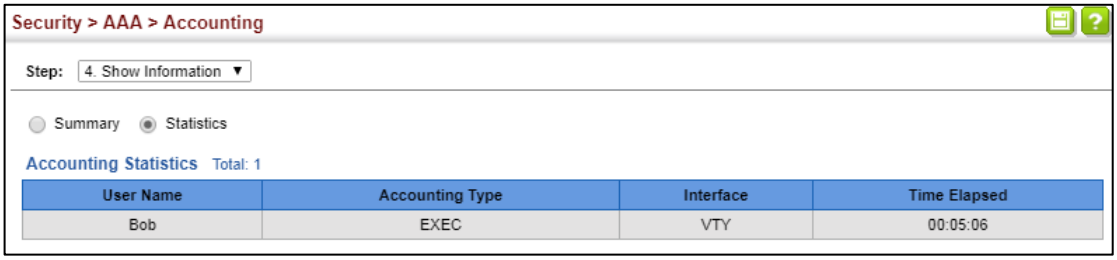
図 11-11　適用された AAA アカウンティング方法の要約の表示



ユーザセッション用に記録された基本アカウンティング情報と統計情報を表示するには：

1. [Security]、[AAA]、[Accounting]をクリックします。
2. [Step]リストから[Show Information]を選択します。
3. [Statistics]をクリックします。

図 11-12　AAA アカウンティングセッションの統計情報の表示



11.1.4 AAA 承認の設定

[Security]> [AAA]> [Authorization]ページを使用して、要求されたサービスの承認を有効にし、設定された承認方式および特定のインタフェースに適用された方式を表示します。

コマンドの使用方法

- この機能は、ユーザが Exec シェルを実行できるかどうかを判断するための承認を実行します。
- 承認が有効になる前に、RADIUS または TACACS +サーバを介した AAA 承認を有効にする必要があります。

パラメータ

次のパラメータが表示されます。

Configure Method

- Authorization Type - サービスを次のように指定します。
  - authorizationExec - ローカルコンソール、Telnet、または SSH 接続の管理権限です。
- Method Name - サービス要求の承認方法を指定します。他のメソッドが定義されていない場合、要求されたサービスに対して“default”方法が使用されます。(範囲: 1 から 64 文字)
- Server Group Name - 承認サーバグループを指定します。

(範囲: 1 から 64 文字)
グループ名 "tacacs +"は、設定されたすべての TACACS +ホストを指定します。他のグループ名は、TACACS + Group Settings ページで設定されたサーバグループを参照します。承認は、TACACS +サーバでのみサポートされています。

Configure Service

- Authorization Type - サービスを Exec として指定し、ローカルコンソール、Telnet、または SSH 接続の管理権限を示します。
- Console Method Name - コンソール接続に適用するユーザ定義のメソッド名を指定します。
- VTY Method Name - Telnet 接続と SSH 接続に適用するユーザ定義のメソッド名を指定します。

Show Information

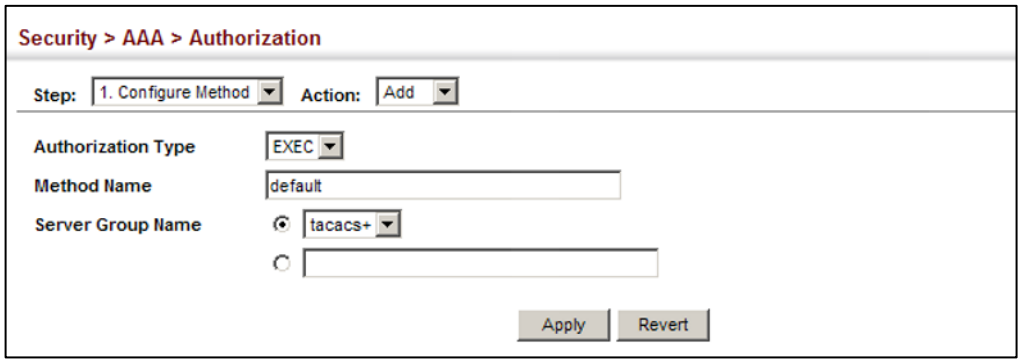
- Authorization Type - 承認サービスを表示します。
- Method Name - ユーザ定義またはデフォルトのアカウンティング方法を表示します。
- Server Group Name - 承認サーバグループを表示します。
- Interface - これらのルールが適用されるコンソールまたは Telnet インタフェースを表示します。(承認方法と関連するサーバグループがインタフェースに割当てられていない場合、このフィールドは空白になります)。

Web インタフェース

Exec のサービスの種類と割当てられたサーバグループに適用される承認方式を設定するには：

1. [Security]、[AAA]、[Authorization]をクリックします。
2. [Step]リストから[Configure Method]を選択します。
3. 承認方法の名前とサーバグループ名を指定します。
4. [Apply]をクリックします。

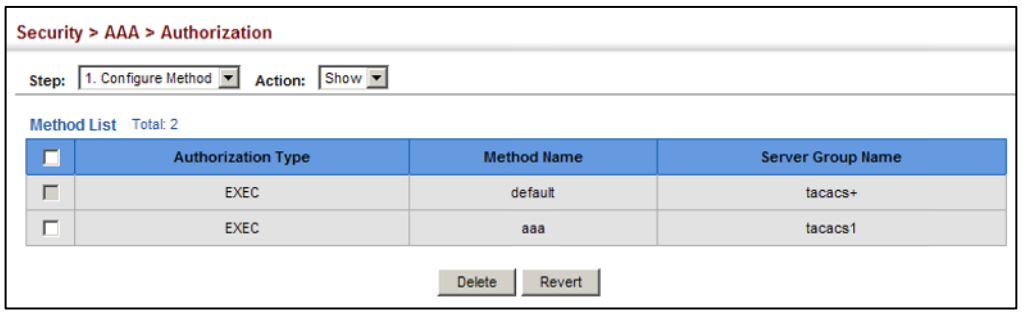
図 11-13　AAA 認証方式の設定



EXEC サービスの種類と割当てられたサーバグループに適用される承認方法を表示するには：

1. [Security]、[AAA]、[Authorization]をクリックします。
2. [Step]リストから[Configure Method]を選択します。
3. [Action]リストから[Show]を選択します。

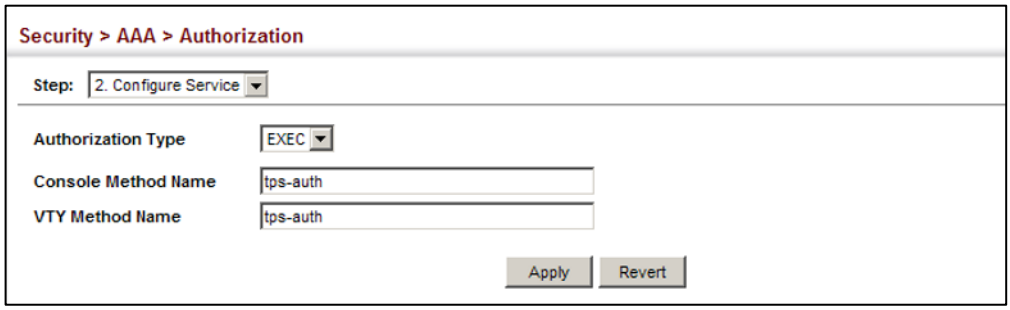
図 11-14　AAA 承認方式の表示



ローカルコンソール、Telnet、または SSH 接続に適用される承認方法を設定するには：

1. [Security]、[AAA]、[Authorization]をクリックします。
2. [Step]リストから[Configure Service]を選択します。
3. 必要な権限方法を入力します。
4. [Apply]をクリックします。

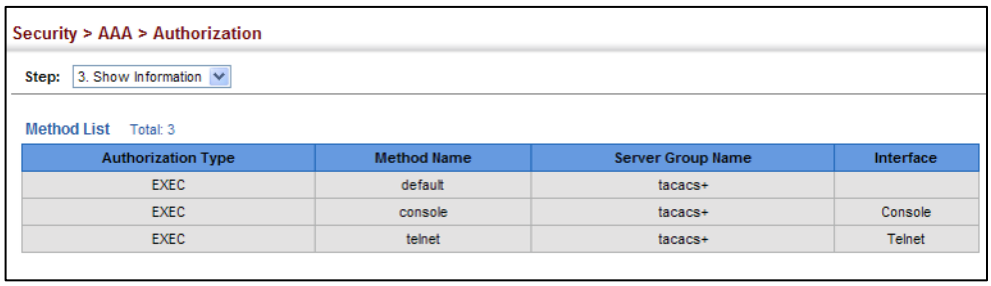
図 11-15　EXEC サービスの AAA 承認方式の設定



設定済みの承認方法と、Exec サービスタイプに割当てられたサーバグループを表示するには、次のように入力します。

1. [Security]、[AAA]、[Authorization]をクリックします。
2. [Step]リストから[Show Information]を選択します。

図 11-16　適用された AAA 承認方式の表示



11.2 ユーザアカウントの設定

[Security]> [User Accounts]ページを使用して、手動で設定されたユーザ名とパスワードにもとづいてスイッチへの管理アクセスを制御します。

コマンドの使用方法

- デフォルトのゲスト名は“guest”で、パスワードは“guest”です。デフォルトの管理者名は“admin”で、パスワードは“admin”です。
- ゲストはほとんどの設定パラメータに対してのみ読み取りアクセス権を持ちます。ただし、管理者はスイッチを管理するすべてのパラメータに対して書き込みアクセス権を持っています。したがって、できるだけ早く新しい管理者パスワードを割当て、安全な場所に保管してください。

パラメータ

次のパラメータが表示されます。

- User Name - ユーザの名前です。
  (最長: 32 文字。 最大ユーザ数：16)
- Access Level - コマンドのアクセス権を指定します。(範囲: 0 から 15)
  レベル 0、8 および 15 は、ユーザ(ゲスト)、マネージャ(ネットワークメンテナンス)、および管理者(上位アクセス)に割当てられます。その他のレベルは、設定された特殊アクセスプロファイルに使用することができます。
  レベル 0 から 7 は、限られた数のコマンドに対して同じデフォルトアクセスを提供し、スイッチの現在のステータスと、いくつかのデータベースクリアおよびリセット機能を表示します。これらのコマンドは、CLI の Normal Exec コマンドモードで使用可能なコマンドと同等です。
  レベル 8 から 14 は、レベル 0 から 7（CLI Normal Exec コマンドモードに相当）に提供されているものよりも多くの追加コマンドを含む、同じデフォルトアクセス特権を提供します。そして、レベル 15（CLI Privileged Exec モードに相当）に提供された構成コマンドのサブセットが含まれています。
  レベル 15 は、すべてのコマンドへのフルアクセスを提供します。
  コマンドに関連付けられた特権レベルは、CLI レファレンスガイドで説明されている“privilege”コマンドを使用して変更できます。
  すべての特権レベルは、より低い特権レベルに割当てられたすべてのコマンドにアクセスできます。たとえば、特権レベル 8 は、CLI レファレンスガイドで説明されている“privilege”コマンドを使用して、デフォルト設定および特権レベル 7 から 0 に割当てられたすべてのコマンドにアクセスできます。
- Password Type - 次のオプションを指定します。
  - No Password - このユーザがログインするためのパスワードは必要ありません。
  - Plain Password - プレーンテキストの暗号化されていないパスワードです。
  - Encrypted Password - 暗号化されたパスワードです。
    暗号化されたパスワードは、システムの起動中に設定ファイルを読み込むとき、または TFTP または FTP サーバから設定ファイルをダウンロードするときに、従来のパスワード設定（プレーンテキストまたは暗号化）との互換性のために必要です。暗号化されたパスワードを手動で設定する必要はありません。
- Password - ユーザのパスワードを指定します。(範囲: 0 から 16 文字、大文字と小文字を区別されます)
- Confirm Password - エラーが発生していないことを確認するために、前のフィールドに入力した文字列を再入力します。これらの 2 つのフィールドが一致しない場合、スイッチはパスワードを変更しませ

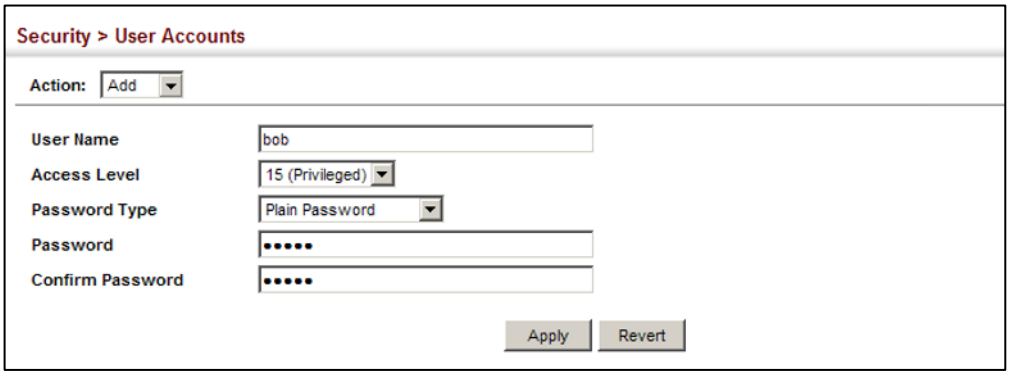
ん。

Web インタフェース

ユーザアカウントを構成するには：

1. [Security]、 [User Accounts]をクリックします。
2. [Action]リストから[Add]を選択します。
3. ユーザ名を指定し、ユーザのアクセスレベルを選択し、必要に応じてパスワードを入力して確認します。
4. [Apply]をクリックします。

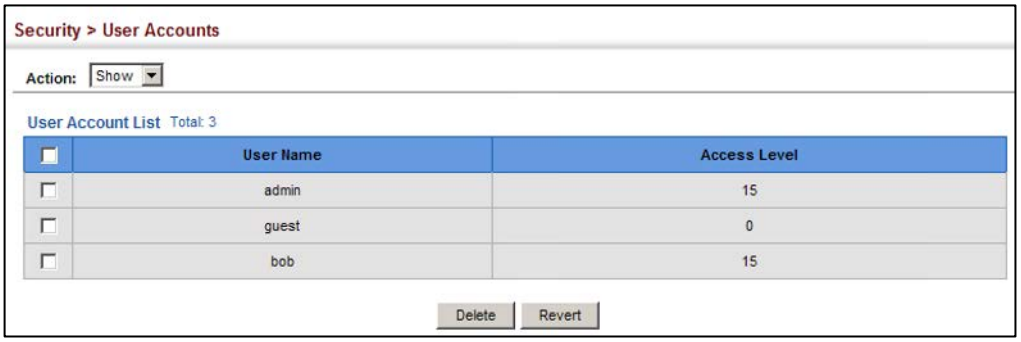
図 11-17　ユーザアカウントの構成



ユーザアカウントを表示するには：

1. [Security]、 [User Accounts]をクリックします。
2. [Action]リストから[Show]を選択します。

図 11-18　ユーザアカウントの表示



11.3 HTTPS の設定

スイッチを設定して、Secure Socket Layer（SSL）上で Secure Hypertext Transfer Protocol（HTTPS）を有効にし、スイッチの Web インタフェースに安全なアクセス（暗号化された接続）を提供できます。

11.3.1 HTTPS のグローバル設定

HTTPS を有効または無効にし、このサービスに使用する TCP ポートを指定するには、[Security]> [HTTPS（Configure Global）]ページを使用します。

コマンドの使用方法

- HTTP と HTTPS の両方のサービスをスイッチ上で個別に有効にすることができます。ただし、両方のサービスを同じ TCP ポートを使用するように設定することはできません。（HTTP は CLI レファレンスガイドで説明されている“ip http server”コマンドを使用して CLI を使用してのみ設定できます）。
- HTTPS を有効にする場合は、ブラウザで指定した URL で指定する必要があります:
  https://*device*[:*port_number*]
- HTTPS を開始すると、下記の方法で接続が確立されます:
  - サーバデジタル証明を使用して、クライアントがサーバを認証します。
  - クライアントとサーバは、接続に使用する一連のセキュリティプロトコルをネゴシエートします。
  - クライアントとサーバは、暗号化および非暗号化データのために、セッション鍵を生成します。
- クライアントとサーバは、安全な暗号化接続を確立します。
  I Internet Explorer はバージョン 11 以上、Mozilla Firefox または Google Chrome は、最新バージョンもしくは最新より 1 つ古いバージョンのステータスバーに、南京錠のアイコンが表示されなければなりません。
- 以下の Web ブラウザおよびオペレーティングシステムで、HTTPS をサポートしています:

表 11-1　HTTPS システムサポート

Web ブラウザ	オペレーティングシステム
Internet Explorer 11 またはそれ以降	Windows 7, 8, 10
Mozilla Firefox 最新または最新の 1 つ前のバージョン	Windows 7, 8, 10, Linux
Google Chrome 最新または最新の 1 つ前のバージョン	Windows 7, 8, 10

- セキュアサイト証明書を指定するには、「11.3.2　デフォルトのセキュアサイト証明書の置換」を参照してください。

Note: IPv6 リンクローカルアドレスを使用する HTTPS では、Web インタフェースへの接続はサポートされていません。

パラメータ

次のパラメータが表示されます。

- HTTPS Status - スイッチの HTTPS サーバ機能を有効/無効にできます。(デフォルト: Enabled)

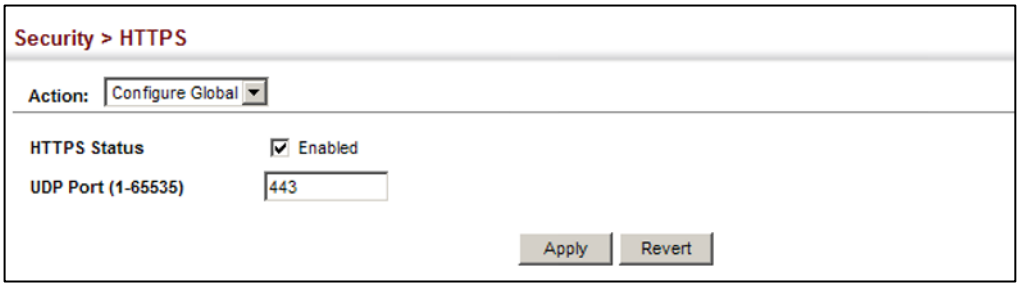
◆ HTTPS Port - スイッチの Web インタフェースへの HTTPS 接続に使用される TCP ポート番号を指定します。(範囲: 1 から 65535、デフォルト: ポート 443)

Web インタフェース

HTTPS を設定するには：

1. [Security]、[HTTPS]をクリックします。
2. [Action]リストから[Configure Global]を選択します。
3. HTTPS を有効にし、必要に応じてポート番号を指定します。
4. [Apply]をクリックします。

図 11-19　HTTPS の設定



11.3.2 デフォルトのセキュアサイト証明書の置換

[Security]> [HTTPS（Copy Certificate）]ページを使用して、デフォルトのセキュアサイト証明書を置換ます。

HTTPS（セキュアアクセス用）を使用して Web インタフェースにログオンすると、スイッチ用の Secure Sockets Layer（SSL）証明書が表示されます。デフォルトでは、Web ブラウザが表示する証明書には、サイトが安全なサイトとして認識されないという警告が関連付けられます。これは、証明書が認証済みの認証局によって署名されていないためです。スイッチへの接続が安全であることを確認するメッセージでこの警告を置換る場合は、認定された認証局から固有の証明書と秘密鍵とパスワードを取得する必要があります。

警告: 最大限のセキュリティを確保するため、できるだけ早く固有の Secure Sockets Layer 証明書を取得することをお勧めします。これは、スイッチのデフォルト証明書が購入したハードウェアに固有のものではないためです。

これらを取得後、TFTP サーバを通してスイッチに転送し、デフォルトの証明書と置換します。

Note: スイッチをリセットして、新しい証明書をアクティブにする必要があります。スイッチをリセットするには「3.12　システムのリセット」を参照してください。またはコマンドプロンプトで”reload”と入力してください。コマンドプロンプト:Console#reload

---

パラメータ

次のパラメータが表示されます。

◆ TFTP Server IP Address -証明書ファイルを含む TFTP サーバの IP アドレスです。

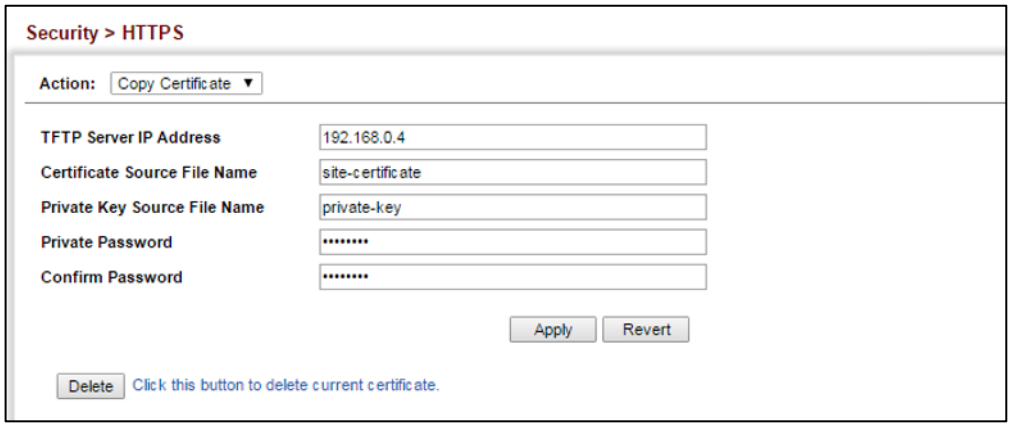
- Certificate Source File Name - TFTP サーバに保存されている証明書ファイルの名前です。
- Private Key Source File Name - TFTP サーバに格納されている秘密鍵ファイルの名前です。
- Private Password - 秘密鍵ファイルに格納されているパスワードです。このパスワードは、証明書を使用するための認証を確認するために使用され、証明書をスイッチにダウンロードするときに確認されます。
- Confirm Password - エラーが発生していないことを確認するために、前のフィールドに入力した文字列を再入力します。これらの 2 つのフィールドが一致しない場合、スイッチは証明書をダウンロードしません。
- Delete - HTTPS セキュアサイト証明書を削除します。デフォルトの証明書をロードするには、スイッチを再起動する必要があります。

Web インタフェース

デフォルトのセキュアサイト証明書を置換するには：

1. [Security]、[HTTPS]をクリックします。
2. [Action]リストから[Copy Certificate]を選択します。
3. TFTP サーバ、証明書とプライベート鍵ファイル名、プライベートパスワードを入力します。
4. [Apply]をクリックします。

図 11-20　セキュアサイト証明書のダウンロード



11.4 SSH の設定

BSD には、もともと Unix システム用に設計されたリモートアクセスツールが含まれています。rlogin (リモートログイン)、rsh (リモートシェル)、rcp （リモートコピー）などのコマンドを含むこれらのツールは、敵対的な攻撃から保護されていません。

Secure Shell（SSH）には、過去の BSD のリモートアクセスツールを安全に置換するためのサーバ/クライアントアプリケーションが含まれています。SSH は Telnet の安全な交換としてこのスイッチにリモート管理アクセスを提供することもできます。クライアントが SSH プロトコル経由でスイッチに接続すると、スイッチはクライアントがアクセス認証のためにローカルユーザ名とパスワードとともに使用する公開鍵を生成します。SSH はまた、スイッチと SSH 対応の管理端末クライアント間を通過するすべてのデータ転送を暗号化し、ネットワーク上を移動するデータが変更されないようにします。

Note: 管理端末に SSH クライアントをインストールして、スイッチにアクセスして SSH プロトコル経由で管理する必要があります。

Note: このスイッチは SSH バージョン 1.5 および 2.0 クライアントの両方をサポートします。

コマンドの使用方法

このスイッチの SSH サーバは、パスワードと公開鍵の両方の認証をサポートしています。SSH クライアントによってパスワード認証が指定されている場合は、システム認証ページで指定されているように、ローカルまたは RADIUS または TACACS +リモート認証サーバを使用してパスワードを認証できます。クライアントによって公開鍵認証が指定されている場合は、次の章で説明するように、クライアントとスイッチの両方で認証鍵を設定する必要があります。公開鍵認証とパスワード認証のどちらを使用するかにかかわらず、スイッチ（SSH ホスト鍵設定）で認証鍵を生成し、SSH サーバ（認証設定）を有効にする必要があります。

SSH サーバを使用するには、次のステップを完了させてください:

1. Generate a Host Key Pair - [SSH（Configure Host Key）]ページで、ホストの公開鍵と秘密鍵のペアを作成します。
2. Provide Host Public Key to Clients - 多くの SSH クライアントプログラムは、スイッチの初期接続設定中にホスト公開鍵を自動的にインポートします。それ以外の場合は、管理端末に既知のホストファイルを手動で作成し、そのホストに公開鍵を配置する必要があります。既知のホストファイル内の公開鍵の入力は、以下の例のようになります:
   10.1.0.54 1024 35 15684995401867669259333946775054617325313674890836547254
   15020245593199868544358361651999923329781766065830956 10825913212890233
   76546801726272571413428762941301196195566782
   59566410486957427888146206519417467729848654686157177393901647793559423035774130980227370877945452408397175264635805817671670957480477611 7
3. Import Client's Public Key to the Switch - スイッチへのすべての SSH クライアントが許可した管理アクセスのための公開鍵を含むファイルをコピーするには、「11.4.3　ユーザ公開鍵のインポート」を参照してください。これらのクライアントは[User Accounts]ページを使用してスイッチ上でローカルに設定する必要があります。（クライアントの設定については、「11.2　ユーザアカウントの設定」を参照してください。）次に、クライアントはこれらの鍵を使用して認証されます。現在のソフトウェアは、RSA バージョン 1 の鍵の次の例に示すように、標準 UNIX 形式に基づいた公開鍵ファイルのみを受け入れます。
   1024 35

134108168560989392104094492015542534763164192187295892114317388005553616163105177594083868631109291232226828519254374603100937187721199696317813662774141689851320491172048303392543241016379975923714490119380060902539484084827178194372288402533115952134861022902978982721353267131629432532818915045306393916643 steve@192.168.1.19

4. Set the Optional Parameters - [SSH（Configure Global）]ページで、認証タイムアウト、再試行回数、およびサーバ鍵サイズなど、オプションのパラメータを構成します。
5. Enable SSH Service - [SSH（Configure Global）]ページで、スイッチ上の SSH サーバを有効にします。
6. Authentication - 以下のいずれかの認証方式が採用されています：
   パスワード認証 (SSH v1.5 または V2 クライアント)
   a. クライアントがサーバにパスワードを送信します。
   b. スイッチが、クライアントパスワードをメモリに格納されている他のクライアントパスワードと比較します。
   c. 合致した場合、接続が許可されます。

Note: パスワード認証のみで SSH を使用するには、初期接続中または既知のホストファイルに手動で入力した場合でも、ホスト公開鍵をクライアントに与えなければなりません。ただし、クライアントの鍵を設定する必要はありません。

Public Key Authentication - SSH クライアントがスイッチに接続しようとすると、SSH サーバはホスト鍵ペアを使用してセッション鍵と暗号化方式をネゴシエートします。スイッチに格納されている公開鍵に対応する秘密鍵を持つクライアントだけがアクセスできます。このプロセス中に以下の交換が行われます:

SSH v1.5 クライアントの認証

a. クライアントがスイッチに公開鍵を送信します。
b. スイッチが、クライアント公開鍵をメモリに格納されている他のクライアント公開鍵と比較します。
c. 一致した場合には、スイッチは秘密鍵を使用してランダムな 256 ビット文字列をチャレンジとして生成し、この文字列をユーザの公開鍵で暗号化してクライアントに送信します。
d. クライアントは秘密鍵を使用してチャレンジ文字列を復号化し、MD5 チェックサムを計算し、チェックサムをスイッチに返します。
e. スイッチは、クライアントから送信されたチェックサムと、送信した元の文字列の計算結果を比較します。2 つのチェックサムが一致する場合、これはクライアントの秘密鍵が許可された公開鍵に対応し、クライアントが認証されていることを意味します。

SSH v2 クライアントの認証

a. クライアントはまずスイッチに照会して、優先アルゴリズムを使用する DSA 公開鍵認証が受け入れ可能かどうかについて判断します。
b. 指定されたアルゴリズムがスイッチによってサポートされている場合、認証プロセスを進めるようにクライアントに通知します。そうでなければ、要求を拒否します。
c. クライアントが、秘密鍵を使用して生成された署名をスイッチに送信します。
d. サーバはこのメッセージを受信すると、指定された鍵が認証に適しているかどうかをチェックし、そうであれば、署名が正しいかどうかをチェックします。両方のチェックが成功すると、クライアントは認証されます。

Note: SSH サーバは、最大 8 つのクライアントセッションをサポートします。クライアントセッションの最大数には、現在の Telnet セッションと SSH セッションの両方が含まれます。

Note: SSH サーバには、スイッチ上の設定済みの IPv4 または IPv6 インタフェースアドレスを使用してアクセスすることができます。

11.4.1 SSH サーバの設定

[Security]> [SSH（Configure Global）]ページを使用して SSH サーバを有効にし、認証の基本を設定します。

Note: SSH サーバを確立する前に、DSA ホスト鍵および RSA ホスト鍵の両方を生成する必要があります。「11.4.2　ホスト鍵ペアの生成」を参照してください。

パラメータ

次のパラメータが表示されます。

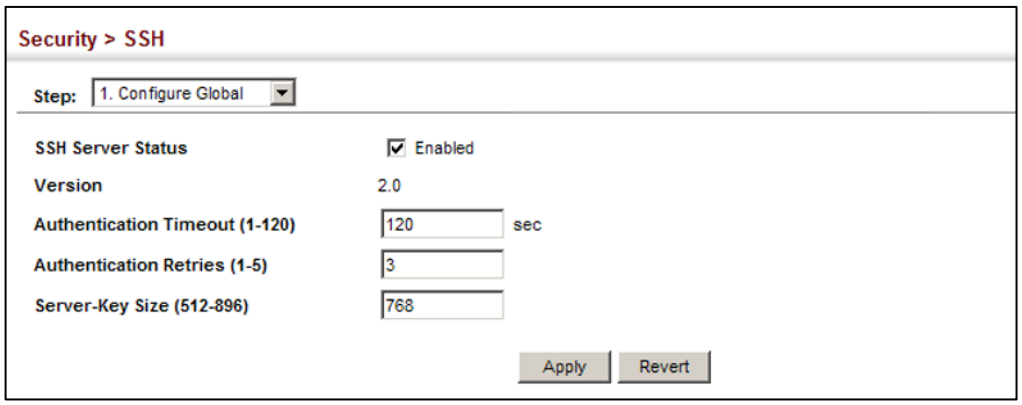
- SSH Server Status - スイッチ上の SSH サーバを有効/無効にすることができます。(デフォルト: Disabled)
- Version - セキュアシェルのバージョン番号。バージョン 2.0 が表示されますが、スイッチは SSH バージョン 1.5 または 2.0 クライアント経由の管理アクセスをサポートします。
- Authentication Timeout - 認証試行中に SSH サーバがクライアントからの応答を待つ時間間隔を秒単位で指定します。(範囲: 1 から 120 秒; デフォルト：120 秒)
- Authentication Retries - 認証に失敗してクライアントが認証プロセスを再開するまでにクライアントが許可される認証試行回数を指定します。(範囲: 1 から 5 回; デフォルト：3)
- Server-Key Size - SSH サーバの鍵サイズを指定します。(範囲: 512 から 896 ビット; デフォルト：768）
  - サーバ鍵は、スイッチの外部では決して共有されない秘密鍵です。
  - ホスト鍵は SSH クライアントと共有され、1024 ビット固定です。

Web インタフェース

SSH サーバを設定するには：

1. [Security]、[SSH]をクリックします。
2. [Step]リストから[Configure Global]を選択します。
3. SSH サーバを有効にします。
4. 必要に応じて認証パラメータを調整します。
5. [Apply]をクリックします。

図 11-21　SSH サーバの設定



11.4.2 ホスト鍵ペアの生成

[Security]> [SSH（Configure Host Key - Generate）]ページを使用して、SSH クライアントとスイッチ間の安全な通信を提供するためのホスト公開鍵と秘密鍵のペアを生成します。この鍵ペアを生成した後、SSH クライアントにホスト公開鍵を提供し、クライアントの公開鍵をスイッチにインポートする必要があります。「11.4.3　ユーザ公開鍵のインポート」を参照してください。

Note: SSH サーバを有効にするには、スイッチ上でホスト鍵ペアを設定する必要があります。

パラメータ

次のパラメータが表示されます。

◆ Host-Key Type - ホスト鍵ペア（つまり、公開鍵と秘密鍵）を生成するために使用される鍵タイプ。(範囲: RSA (Version 1), DSA (Version 2), Both; デフォルト: Both)
SSH サーバは、クライアントが最初にスイッチとの接続を確立した後、クライアントと交渉してデータ暗号化用の DES（56 ビット）または 3DES（168 ビット）のいずれかを選択するときに、鍵交換に RSA または DSA を使用します。

Note: スイッチは SSHv1.5 クライアントでは RSA バージョン 1 のみ、SSHv2 クライアントでは DSA バージョン 2 のみを使用します。

◆ Save - ホスト鍵を RAM（すなわち、揮発性メモリ）からフラッシュメモリに保存する。それ以外の場合、ホスト鍵ペアはデフォルトで RAM に格納されます。このアイテムは[Show]ページから選択する必要があります。(デフォルト: Disabled)

Web インタフェース

SSH ホスト鍵ペアを生成するには：

1. [Security]、[SSH]をクリックします。
2. [Step]リストから[Configure Host Key]を選択します。
3. [Action]リストから[Generate]を選択します。
4. ドロップダウンボックスからホスト鍵タイプを選択します。

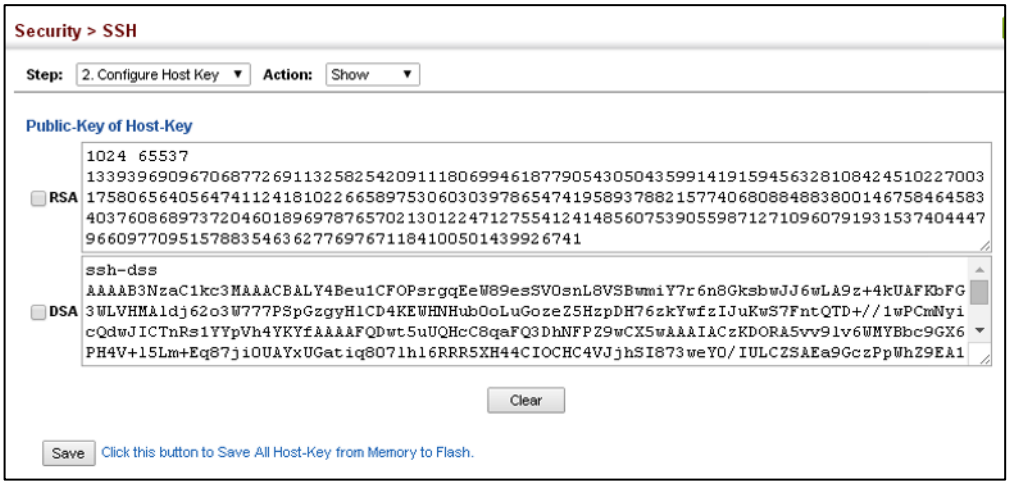
5. [Apply]をクリックします。

図 11-22　SSH ホスト鍵ペアの生成

SSH ホスト鍵ペアを表示またはクリアするには：

1. [Security]、[SSH]をクリックします。
2. [Step]リストから[Configure Host Key]を選択します。
3. [Action]リストから[Show]を選択します。
4. [Save]をクリックしてホスト鍵をメモリからフラッシュに保存するオプションを選択するか、クリアするホスト鍵タイプを選択して[Clear]をクリックします。

図 11-23　SSH ホスト鍵ペアの表示



11.4.3 ユーザ公開鍵のインポート

[Security]> [SSH（Configure User Key - Copy）]ページを使用してユーザの公開鍵をスイッチにアップロードします。この公開鍵は、ユーザが公開鍵認証メカニズムを使用してログインできるように、スイッチに格納する必要があります。ユーザの公開鍵がスイッチに存在しない場合、SSH は対話型パスワード認証メカニズムに戻り、認証を完了します。

パラメータ

次のパラメータが表示されます。

- User Name - このドロップダウンボックスでは、管理する公開鍵のユーザを選択します。最初にユーザアカウントページでユーザを作成する必要があります。
- User Key Type - アップロードする公開鍵のタイプです。
  - RSA: スイッチは RSA バージョン 1 の暗号化された公開鍵を受け入れます。
  - DSA: スイッチは DSA バージョン 2 の暗号化された公開鍵を受け入れます。

SSH サーバは、クライアントが最初にスイッチとの接続を確立した後、クライアントと交渉してデータ暗号化用の DES（56 ビット）または 3DES（168 ビット）のいずれかを選択するときに、鍵交換に

RSA または DSA を使用します。
スイッチは SSHv1.5 クライアントでは RSA バージョン 1 のみ、SSHv2 クライアントでは DSA バージョン 2 のみを使用します。

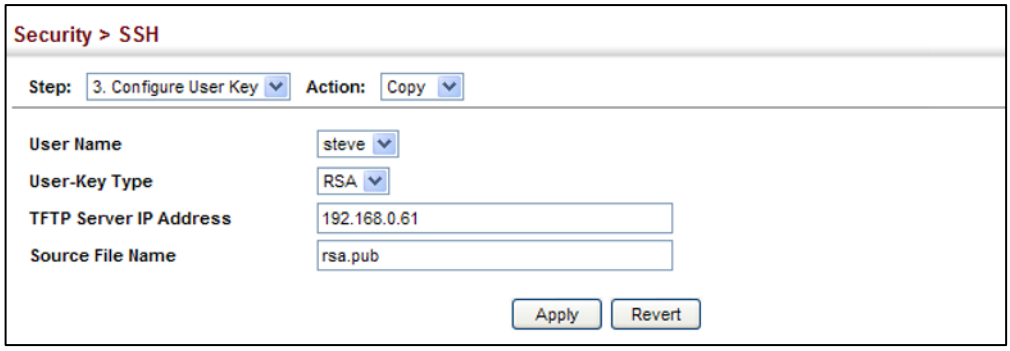
- TFTP Server IP Address - インポートする公開鍵ファイルを含む TFTP サーバの IP アドレスです。
- Source File Name - アップロードする公開鍵ファイルです。

Web インタフェース

SSH ユーザの公開鍵をコピーするには：

1. [Security]、[SSH]をクリックします。
2. [Step]リストから[Configure User Key]を選択します。
3. [Action]リストから[Copy]を選択します。
4. それぞれのドロップダウンボックスからユーザ名と公開鍵タイプを選択し、TFTP サーバの IP アドレスと公開鍵ソースファイル名を入力します。
5. [Apply]をクリックします。

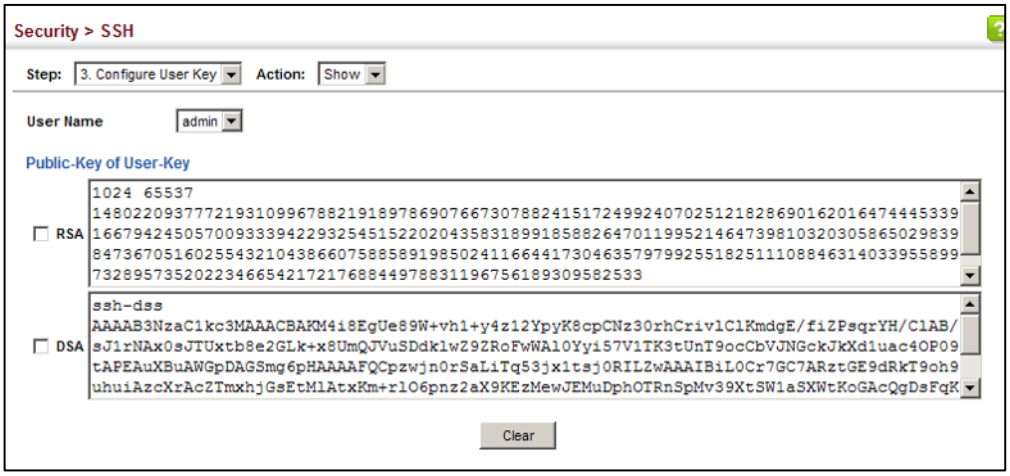
図 11-24　SSH ユーザの公開鍵のコピー



SSH ユーザの公開鍵を表示または消去するには：

1. [Security]、[SSH]をクリックします。
2. [Step]リストから[Configure User Key]を選択します。
3. [Action]リストから[Show]を選択します。
4. ユーザ名リストからユーザを選択します。
5. クリアするホスト鍵タイプを選択します。
6. [Clear]をクリックします。

図 11-25　SSH ユーザの公開鍵を表示



11.5 アクセス制御リスト

アクセス制御リスト（ACL）は、IPv4 フレーム（アドレス、プロトコル、レイヤ 4 プロトコルポート番号または TCP 制御フラグに基づく）、IPv6 フレーム（アドレス、DSCP トラフィッククラスに基づく）、または任意のフレーム（MAC アドレスまたはイーサネットタイプ）です。受信パケットをフィルタリングするには、最初にアクセスリストを作成し、必要なルールを追加して、そのリストを特定のポートにバインドします。

アクセス制御リストの設定 -

ACL は、IP アドレス、MAC アドレス、またはその他の特定の基準に適用される permit 条件または deny 条件の順次リストです。このスイッチは、受信パケットを 1 つずつ ACL の条件と照合してテストします。パケットは permit ルールと一致するとすぐに受け入れられ、deny ルールと一致するとすぐに破棄されます。ルールが一致しない場合、パケットは受け入れられます。

コマンドの使用方法

ACL には次の制限が適用されます。

- ACL は受信パケットまたは受信フレームにしか適用できません。
- ACL の最大数は 256 です。
- 1 システムあたりに設定できるルールの最大数は 512 ルール、バインドできるルールの最大数は 256 です。
- ACL は 128 までのルールを持つことができます。
- ポートにバインドできるルールの最大数は、次のように制限されます。
  - 128 MAC ACL
  - 128 IPv4 ACL（標準および拡張 IPv4 ACL を含む）
  - 60 IPv6 ACL（標準および拡張 IPv6 ACL を含む）

  上記のルール（アクセス制御エントリまたは ACE）の最大数は、最悪の場合のシナリオです。実際には、スイッチは TCAM（ACE の格納に使用されるハードウェアテーブル）内の ACE を圧縮しますが、実際に可能な ACE の最大数は、あまりにも多くの要素に依存するため、正確には定められません。これは、この目的のために実行時に予約されたハードウェアリソースの量に依存します。
  自動 ACE 圧縮は、ハードウェアリソースをより効率的に利用するために、ACL のすべての ACE を圧縮するために使用されるソフトウェア機能です。圧縮を行わないと、1 つの ACE が TCAM の固定数のエントリを占有します。したがって、1 つの ACL に 25 の ACE が含まれている場合、ACL には TCAM に（25 * n）エントリが必要です（n は 1 つの ACE に必要な TCAM エントリの固定数です）。ACE を TCAM に書き込む前に圧縮を使用すると、ソフトウェアは ACE を圧縮して、必要な TCAM エントリの数を減らします。例えば、1 つの ACL は、192.168.1.0 から 255 のような連続した IP アドレス範囲を分類する 128 の ACE を含むことができます。圧縮が無効の場合、ACL は（128 * n）エントリの TCAM を占有し、ほぼすべてのハードウェアリソースを使用します。圧縮を使用すると、128 個の ACE が 1 つの ACE に圧縮され、TCAM に「n」エントリだけが必要な 192.168.1.0/24 という IP アドレスが分類されます。上記の例は、圧縮の理想的なケースです。最悪の場合は、ACE が圧縮できない場合です。この場合、使用された TCAM エントリの数は圧縮なしと同じになります。ACE の処理にはさらに時間が必要です。
- SNMP を使用した ACL 情報の取得は 63 個まで可能です。

- リストの最後まで一致が見つからない場合、トラフィックは受け入れられます。必要なチェックの回数を減らすために、頻繁にヒットするエントリはリストの一番上に置くのが理想的です。スイッチは最初の一致後にテストを停止するため、条件の順序が重要です。一致する条件がない場合、パケット

は受け入れられます。

アクティブな ACL のチェック順序は次のとおりです。

1. 受信ポートの IP ACL および MAC ACL のユーザ定義ルールは、MAC ACL、IP ACL の順にチェックされます。
2. ACL 内のルールは、上から下に設定された順序でチェックされます。
3. IP ACL を検査した結果が permit であるが、同じパケット上の MAC ACL の結果が deny である場合、パケットは廃棄されます（パケットを廃棄する決定はセキュリティ上の理由により優先順位が高くなります） 。IP ACL が deny で、MAC ACL が permit である場合もまた、パケットは廃棄されます。

11.5.1 TCAM の使用状況の表示

[Security]> [ACL（Configure ACL - Show TCAM）]ページを使用して、使用中のエントリ数、空きエントリ数、使用中の TCAM 全体の割合など、TCAM（Ternary Content Addressable Memory）の使用率パラメータを表示します。

コマンドの使用方法

アクセス制御リスト（ACL）、IP ソースガードフィルタルール、QoS（Quality of Service）プロセス、QinQ、MAC ベース VLAN、VLAN 変換、トラップなどのルールベースの検索に依存するさまざまなシステム機能によって、ポリシーコントロールエントリ（PCE）が使用されます。

たとえば、ACL をポートにバインドする場合、ACL の各ルールは 2 つの PCE を使用します。 また、ポートに IP ソースガードフィルタルールを設定すると、システムは 2 つの PCE も使用します。

パラメータ

次のパラメータが表示されます。

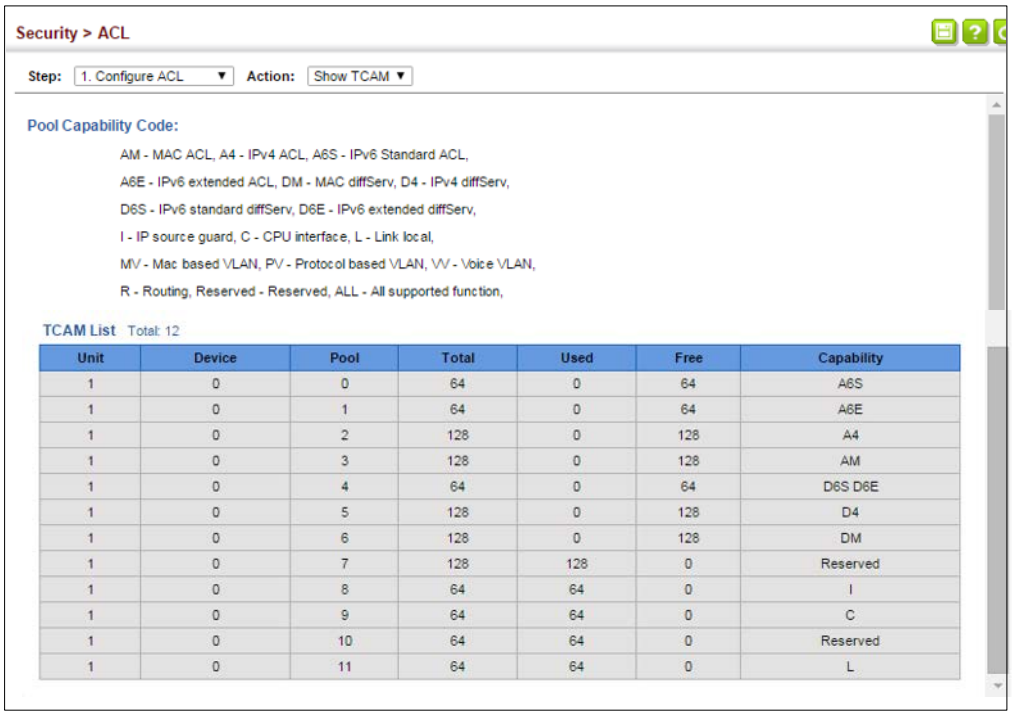
- Pool Capability Code - TCAM リストに示されているプロセスの略語です。
- Unit - ユニットの識別子です。
- Device - 示されたプールに使用されるメモリチップです。
- Pool - ルールスライス（またはグループと呼ぶ）です。各スライスには、指定された機能に使用される固定数の規則があります。
- Total - 各プールに割当てられたポリシーコントロールエントリの最大数です。
- Used - オペレーティングシステムによって使用されるポリシーコントロールエントリの数です。
- Free - 使用可能なポリシーコントロールエントリの数です。
- Capability - 各プールに割当てられたプロセスです。

Web インタフェース

TCAM の使用状況を表示するには：

1. [Security]、[ACL]をクリックします。
2. [Step]リストから[Configure ACL]を選択します。
3. [Action]リストから[Show TCAM]を選択します。

図 11-26　TCAM の使用状況の表示



Unit	Device	Pool	Total	Used	Free	Capability
1	0	0	64	0	64	A6S
1	0	1	64	0	64	A6E
1	0	2	128	0	128	A4
1	0	3	128	0	128	AM
1	0	4	64	0	64	D6S D6E
1	0	5	128	0	128	D4
1	0	6	128	0	128	DM
1	0	7	128	128	0	Reserved
1	0	8	64	64	0	I
1	0	9	64	64	0	C
1	0	10	64	64	0	Reserved
1	0	11	64	64	0	L

11.5.2 ACL の名前とタイプの設定

[Security]> [ACL（Configure ACL - Add）]ページを使用して ACL を作成します。

パラメータ

次のパラメータが表示されます。

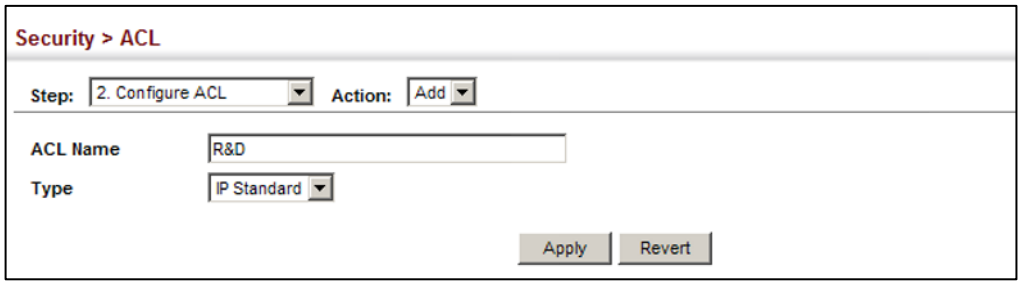
- ACL Name - ACL の名前です。(最長: 32 文字、ARP ACL は 16 文字)
- Type - 次のフィルタモードがサポートされています。
  - IP Standard: IPv4 ACL モードは、送信元 IPv4 アドレスにもとづいてパケットをフィルタリングします。
  - IP Extended: IPv4 ACL モードは、送信元または宛先の IPv4 アドレス、およびプロトコルタイプとプロトコルポート番号にもとづいてパケットをフィルタリングします。「TCP」プロトコルが指定されている場合は、TCP 制御フラグにもとづいてパケットをフィルタリングすることもできます。
  - IPv6 Standard: IPv6 ACL モードは、送信元 IPv6 アドレスにもとづいてパケットをフィルタリングします。
  - IPv6 Extended: IPv6 ACL モードは、送信元 IP アドレスまたは宛先 IP アドレス、および DSCP にもとづいてパケットをフィルタリングします。
  - MAC - MAC ACL モードは、送信元または宛先 MAC アドレスとイーサネットフレームタイプ（RFC 1060）にもとづいてパケットをフィルタリングします。
  - ARP - ARP ACL は、ARP 検査に使用される静的 IP-MAC アドレスバインディングを指定します。

Web インタフェース

ACL の名前とタイプを設定するには：

1. [Security]、[ACL]をクリックします。
2. [Step]リストから[Configure ACL]を選択します。
3. [Action]リストから[Add]を選択します。
4. ACL 名フィールドに入力し、ACL タイプを選択します。
5. [Apply]をクリックします。

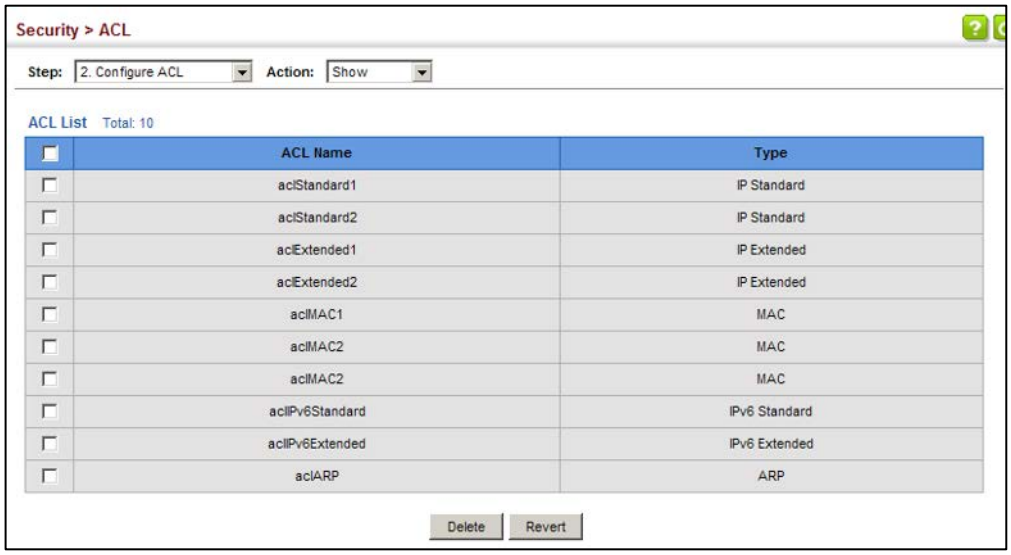
図 11-27　ACL の作成



ACL のリストを表示するには：

1. [Security]、[ACL]をクリックします。
2. [Step]リストから[Configure ACL]を選択します。
3. [Action]リストから[Show]を選択します。

図 11-28　ACL のリストを表示する



11.5.3 標準 IPv4 ACL の設定

[Security]> [ACL（Configure ACL - Add Rule - IP Standard）]ページを使用して、標準 IPv4 ACL を設定します。

パラメータ

次のパラメータが表示されます。

- Type - Name リストに表示する ACL のタイプを選択します。
- Name - 選択したタイプに一致する ACL の名前を表示します。
- Action - ACL には、permit ルールまたは deny ルールの任意の組み合わせを含めることができます。

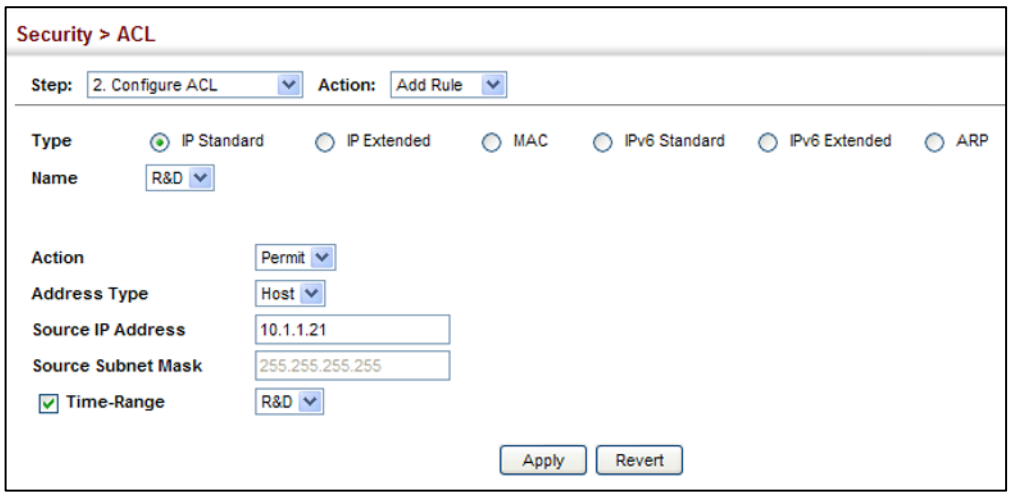
- Address Type - 送信元 IP アドレスを指定します。すべての可能なアドレスを含めるには "Any"、アドレスフィールドに特定のホストアドレスを指定するには "Host"、アドレスおよびサブネットマスクフィールドでアドレスの範囲を指定するには "IP"を使用します。(オプション: Any、Host、IP、デフォルト Any)
- Source IP Address - 送信元 IP アドレスです。
- Source Subnet Mask - それぞれがピリオドで区切られた 0 から 255 の 4 つの整数を含むサブネットマスクです。マスクは、「有効」を示すために 1 ビットを使用し、「無視」を示すために 0 ビットを使用します。マスクは、指定された送信元 IP アドレスとビット単位で AND され、この ACL が割当てられているポートに入る各 IP パケットのアドレスと比較されます。
- Time Range - 時間範囲の名前です。

Web インタフェース

標準 IPv4 ACL にルールを追加するには：

1. [Security]、[ACL]をクリックします。
2. [Step]リストから[Configure ACL]を選択します。
3. [Action]リストから[Add Rule]を選択します。
4. [Type]リストから[IP Standard]を選択します。
5. [Name]リストから ACL の名前を選択します。
6. 操作（permit または deny）を指定します。
7. アドレスタイプ（Any、Host、または IP）を選択します。
8. [Host]を選択した場合は、特定のアドレスを入力します。[IP]を選択した場合は、サブネットアドレスとアドレス範囲のマスクを入力します。
9. [Apply]をクリックします。

図 11-29　標準 IPv4 ACL の設定



11.5.4 拡張 IPv4 ACL の設定

[Security]> [ACL（Configure ACL - Add Rule - IP Extended）]ページを使用して、拡張 IPv4 ACL を設定します。

パラメータ

次のパラメータが表示されます。

- Type - Name リストに表示する ACL のタイプを選択します。
- Name - 選択したタイプに一致する ACL の名前を表示します。
- Action - ACL には、permit ルールまたは deny ルールの任意の組み合わせを含めることができます。
- Source/Destination Address Type - 送信元または宛先 IP アドレスタイプを指定します。すべての可能なアドレスを含めるには "Any"、アドレスフィールドに特定のホストアドレスを指定するには "Host"、アドレスおよびサブネットマスクフィールドでアドレスの範囲を指定するには "IP"を使用します。(オプション: Any、Host、IP、デフォルト Any)
- Source/Destination IP Address - 送信元または宛先 IP アドレスです。
- Source/Destination Subnet Mask - 送信元または宛先アドレスのサブネットマスクです。
- Source/Destination Port - 指定されたプロトコルタイプの送信元/宛先ポート番号です。(範囲: 0 から 65535)
- Source/Destination Port Bit Mask - 有効なポートビットを表す 10 進数です。(範囲: 0 から 65535)
- Protocol - プロトコルタイプを TCP、UDP またはその他と一致するように指定します。他のプロトコルは特定のプロトコル番号（0 から 255）を示します。(オプション: TCP、UDP、Others、デフォルト：Others)
  次の項目は TCP の場合に設定できます。
  - Control Code - TCP ヘッダーの 14 バイト目のフラグビットを指定する 10 進数（ビットストリングを表す）です。(範囲: 0 から 63)
  - Control Code Bit Mask - 有効なフラグビットを表す 10 進数です。(範囲: 0 から 63)

  制御ビットマスクは、制御フラグに適用される 10 進数（等価 2 進ビットマスクの場合）です。等価バイナリビット "1"はビットが有効であることを意味し、 "0"はビットを無視することを意味する 10 進数を入力します。以下のビットを指定することができます:。
  - 1 (fin) - Finish
  - 2 (syn) - Synchronize
  - 4 (rst) - Reset
  - 8 (psh) - Push
  - 16 (ack) - Acknowledgement
  - 32 (urg) - Urgent pointer

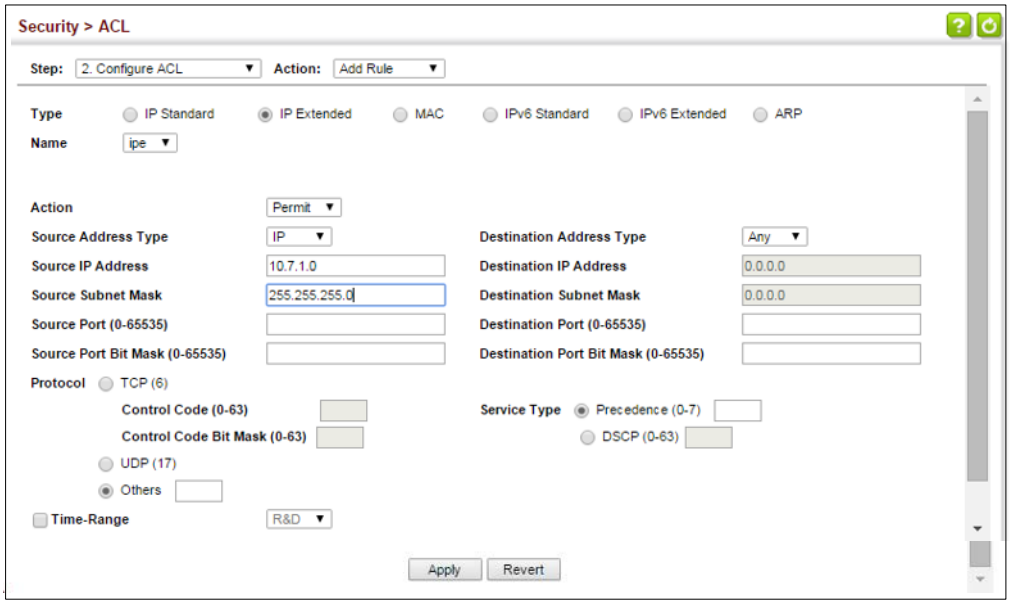
  たとえば、次のフラグを設定してパケットを捕捉するには、フラグ値とマスクを使用します:
  - SYN フラグ有効、制御フラグ 2 を使用、制御ビットマスク 2
  - SYN と ACK の両方が有効、制御フラグ 18、制御ビットマスク 18
  - SYN 有効かつ ACK 無効、制御フラグ 2 を使用、制御ビットマスク 18
- Service Type - パケット優先度の設定は、次の基準にもとづいています。
  - Precedence - IP precedence レベルです。(範囲: 0 から 7)
  - DSCP - DSCP 優先レベルです。(範囲: 0 から 63)
- Time Range - 時間範囲の名前です。

Web インタフェース

拡張 IPv4 ACL にルールを追加するには：

1. [Security]、[ACL]をクリックします。
2. [Step]リストから[Configure ACL]を選択します。
3. [Action]リストから[Add Rule]を選択します。
4. [Type]リストから[IP Extended]を選択します。
5. [Name]リストから ACL の名前を選択します。
6. 操作（permit または deny）を指定します。
7. アドレスタイプ（Any、Host、または IP）を選択します。
8. [Host]を選択した場合は、特定のアドレスを入力します。[IP]を選択した場合は、サブネットアドレスとアドレス範囲のマスクを入力します。
9. サービスタイプ、プロトコルタイプ、または制御フラグなど、その他の必要な条件を設定します。
10. [Apply]をクリックします。

図 11-30　拡張 IPv4 ACL の設定



11.5.5 標準 IPv6 ACL の設定

[Security]> [ACL（Configure ACL - Add Rule - IPv6 Standard）]ページを使用して、標準 IPv6 ACL を設定します。

パラメータ

次のパラメータが表示されます。

- Type - Name リストに表示する ACL のタイプを選択します。
- Name - 選択したタイプに一致する ACL の名前を表示します。
- Action - ACL には、permit ルールまたは deny ルールの任意の組み合わせを含めることができます。
- Source Address Type - 送信元 IP アドレスを指定します。すべての可能なアドレスを含めるには "Any"、アドレスフィールドに特定のホストアドレスを指定するには "Host"、アドレスの範囲を指定するには "IPv6-Prefix"を使用します。(オプション: Any, Host, IPv6-Prefix; デフォルト: Any)
- Source IPv6 Address - IPv6 送信元アドレスまたはネットワーククラスです。アドレスは、RFC 2373「IPv6 Addressing Architecture」フォーマットに従って、コロンで区切られた 8 つの 16 ビット 16 進数

を使用する必要があります。未定義のフィールドを埋めるために必要な 0 の適切な数を示すために、アドレスに 1 つの二重コロンを使用することができます。

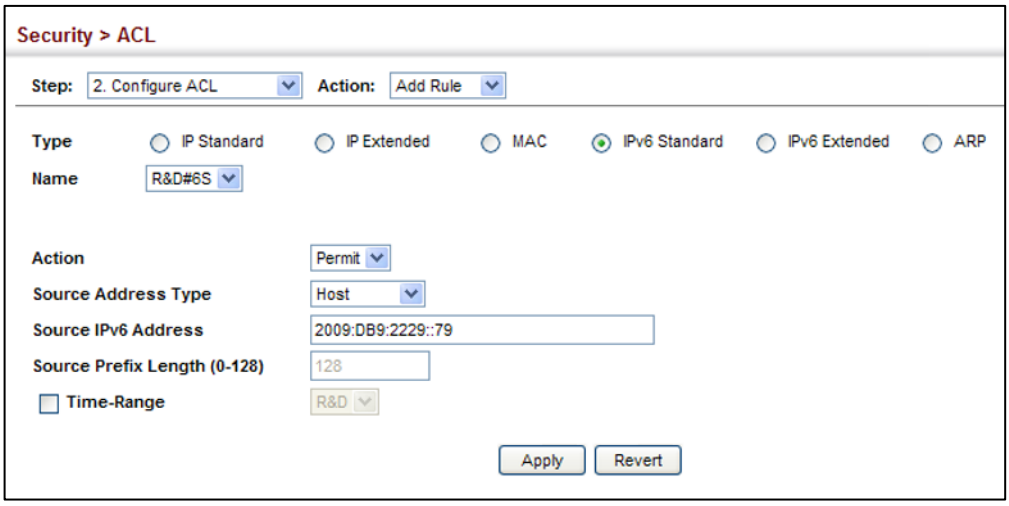
- Source Prefix-Length - アドレスの連続ビット数（左から）がプレフィックス（すなわち、アドレスのネットワーク部分）を含むことを示す 10 進数です。(範囲: 0 から 128 ビット）
- Time Range - 時間範囲の名前です。

Web インタフェース

標準 IPv6 ACL にルールを追加するには：

1. [Security]、[ACL]をクリックします。
2. [Step]リストから[Configure ACL]を選択します。
3. [Action]リストから[Add Rule]を選択します。
4. [Type]リストから[IPv6 Standard]を選択します。
5. [Name]リストから ACL の名前を選択します。
6. 操作（permit または deny）を指定します。
7. 送信元アドレスタイプ（Any、Host、または IPv6-prefix）を選択します。
8. [Host]を選択した場合は、特定のアドレスを入力します。「IPv6-prefix」を選択した場合は、サブネットアドレスとプレフィックスの長さを入力します。
9. [Apply]をクリックします。

図 11-31　標準 IPv6 ACL の設定



11.5.6 拡張 IPv6 ACL の設定

[Security]> [ACL（Configure ACL - Add Rule - IPv6 Extended）]ページを使用して、拡張 IPv6 ACL を設定します。

パラメータ

次のパラメータが表示されます。

- Type - Name リストに表示する ACL のタイプを選択します。
- Name - 選択したタイプに一致する ACL の名前を表示します。
- Action - ACL には、permit ルールまたは deny ルールの任意の組み合わせを含めることができます。

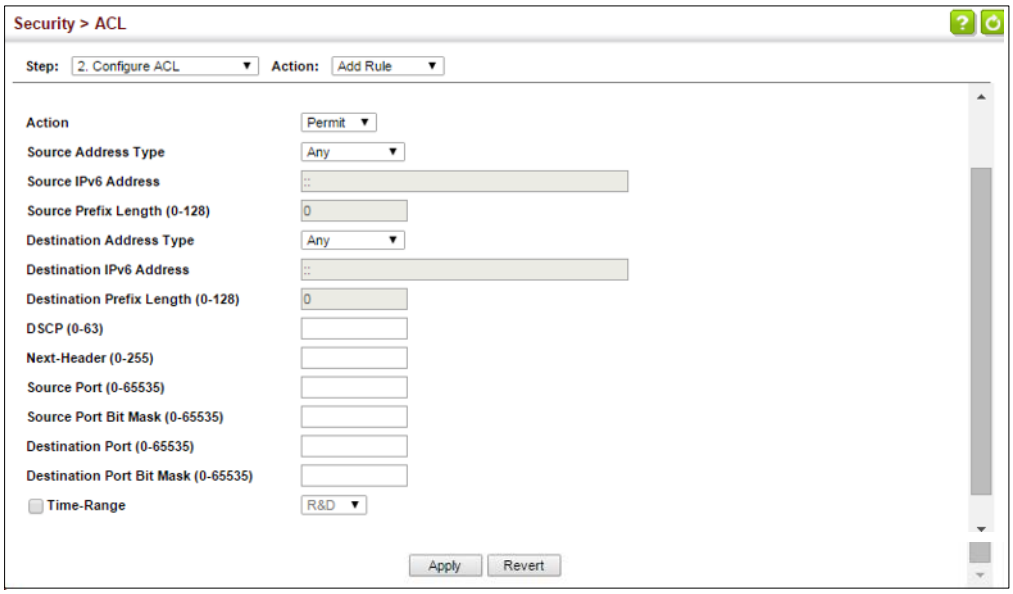
- Source Address Type - 送信元 IP アドレスの種類を指定します。すべての可能なアドレスを含めるには "Any"、アドレスフィールドに特定のホストアドレスを指定するには "Host"、アドレスの範囲を指定するには "IPv6-Prefix"を使用します。(オプション: Any, Host, IPv6-Prefix; デフォルト: Any)
- Destination Address Type - 宛先 IP アドレスタイプを指定します。すべての可能なアドレスを含めるには "Any"、アドレスフィールドに特定のホストアドレスを指定するには "Host"、アドレスの範囲を指定するには "IPv6-Prefix"を使用します。(オプション: Any, Host, IPv6-Prefix; デフォルト: Any)
- Source/Destination IPv6 Address - IPv6 アドレスまたはネットワーククラスです。アドレスは、RFC 2373「IPv6 Addressing Architecture」フォーマットに従って、コロンで区切られた 8 つの 16 ビット 16 進数を使用する必要があります。未定義のフィールドを埋めるために必要な 0 の適切な数を示すために、アドレスに 1 つの二重コロンを使用することができます。
- Source/Destination Prefix-Length - アドレスの連続したビット数（左から）がプレフィックスを構成することを示す 10 進数です。 すなわち、アドレスのネットワーク部分です。(範囲: 送信元プレフィックスの 0 から 128 ビット。 宛先プレフィックスの場合は 0 から 128 ビット）
- DSCP - DSCP トラフィッククラス。(範囲: 0 から 63)
- Next Header - IPv6 ヘッダ直後に続くヘッダの種類を識別します。(範囲: 0 から 255)
- Source Port - プロトコル※送信元ポート番号です。(範囲: 0 から 65535)
- Source Port Bit Mask - 有効なポートビットを表す 10 進数です。(範囲: 0 から 65535)
- Destination Port - プロトコル※宛先ポート番号です。(範囲: 0 から 65535)
- Destination Port Bit Mask - 有効なポートビットを表す 10 進数です。(範囲: 0 から 65535)
- Time Range - 時間範囲の名前です。
  注※ TCP、UDP、またはその他のプロトコルタイプが含まれます。

Web インタフェース

拡張 IPv6 ACL にルールを追加するには：

1. [Security]、[ACL]をクリックします。
2. [Step]リストから[Configure ACL]を選択します。
3. [Action]リストから[Add Rule]を選択します。
4. [Type]リストから[IPv6 Extended]を選択します。
5. [Name]リストから ACL の名前を選択します。
6. 操作（permit または deny）を指定します。
7. アドレスタイプ（Any、Host、または IPv6-prefix）を選択します。
8. [Host]を選択した場合は、特定のアドレスを入力します。「IPv6-prefix」を選択した場合は、サブネットアドレスとプレフィックス長を入力します。
9. DSCP などのその他の必要条件を設定します。
10. [Apply]をクリックします。

図 11-32　拡張 IPv6 ACL の設定



11.5.7 MAC ACL の設定

[Security]> [ACL（Configure ACL - Add Rule - MAC）]ページを使用して、ハードウェアアドレス、パケットフォーマット、およびイーサネットタイプにもとづいて MAC ACL を設定します。

パラメータ

次のパラメータが表示されます。

- Type - Name リストに表示する ACL のタイプを選択します。
- Name - 選択したタイプに一致する ACL の名前を表示します。
- Action - ACL には、permit ルールまたは deny ルールの任意の組み合わせを含めることができます。
- Source/Destination Address Type - すべての可能なアドレスを含めるには“Any”、特定の MAC アドレスを示すには“Host”、アドレスおよびビットマスクフィールドを使用してアドレス範囲を指定するには“MAC”を使用します。(オプション: Any、Host、MAC、デフォルト Any)
- Source/Destination MAC Address - 送信元または宛先 MAC アドレス。
- Source/Destination Bit Mask - 送信元 MAC アドレスまたは宛先 MAC アドレスの 16 進マスク。
- Packet Format - この属性には、次のパケットタイプが含まれます。
  - Any - 任意のイーサネットパケットタイプです。
  - Untagged-eth2 - タグなしイーサネット II パケットです。
  - Untagged-802.3 - タグなしイーサネット 802.3 パケットです。
  - Tagged-eth2 - タグ付きイーサネット II パケットです。
  - Tagged-802.3 - タグ付きイーサネット 802.3 パケットです。
- VID - VLAN ID です。(範囲: 1 から 4094)
- VID Bit Mask - VLAN ビットマスクです。(範囲: 0 から 4095)
- Ethernet Type - このオプションは、イーサネット II でフォーマットされたパケットをフィルタリングする場合にのみ使用できます。(範囲: 0 から ffff 16 進数。)
  イーサネットプロトコルタイプの詳細なリストは、RFC 1060 にあります。より一般的なタイプには、

0800（IP）、0806（ARP）、8137（IPX）などがあります。

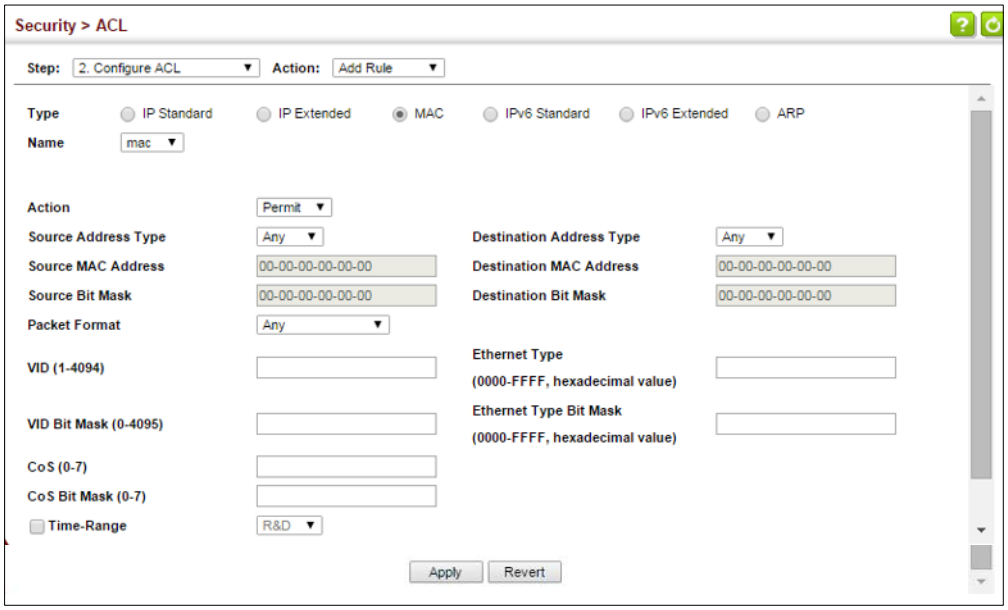
- Ethernet Type Bit Mask - プロトコルビットマスクです。(範囲: 0 から ffff 16 進数)
- CoS - CoS 値です。(範囲: 0 から 7、7 が最も高い優先順位です）
- CoS Bit Mask - CoS ビットマスクです。(範囲: 0 から 7)
- Time Range - 時間範囲の名前です。

Web インタフェース

MAC ACL にルールを追加するには：

1. [Security]、[ACL]をクリックします。
2. [Step]リストから[Configure ACL]を選択します。
3. [Action]リストから[Add Rule]を選択します。
4. [Type]リストから[MAC]を選択します。
5. [Name]リストから ACL の名前を選択します。
6. 操作（permit または deny）を指定します。
7. アドレスタイプ（Any、Host、または MAC）を選択します。
8. [Host]を選択した場合は、特定のアドレス（例：11-22-33-44-55-66）を入力します。[MAC]を選択した場合は、アドレス範囲のベースアドレスと 16 進数のビットマスクを入力します。
9. VID、イーサネットタイプ、パケットフォーマットなど、その他の必要な基準を設定します。
10. [Apply]をクリックします。

図 11-33　MAC ACL の設定



11.5.8 ARP ACL の設定

ARP メッセージアドレスにもとづいて ACL を設定するには、[Security]> [ACL（Configure ACL - Add Rule - ARP）]ページを使用します。ARP 検査では、これらの ACL を使用して疑わしいトラフィックをフィルタリングできます(「11.11　ARP 検査」を参照してください)。

パラメータ

次のパラメータが表示されます。

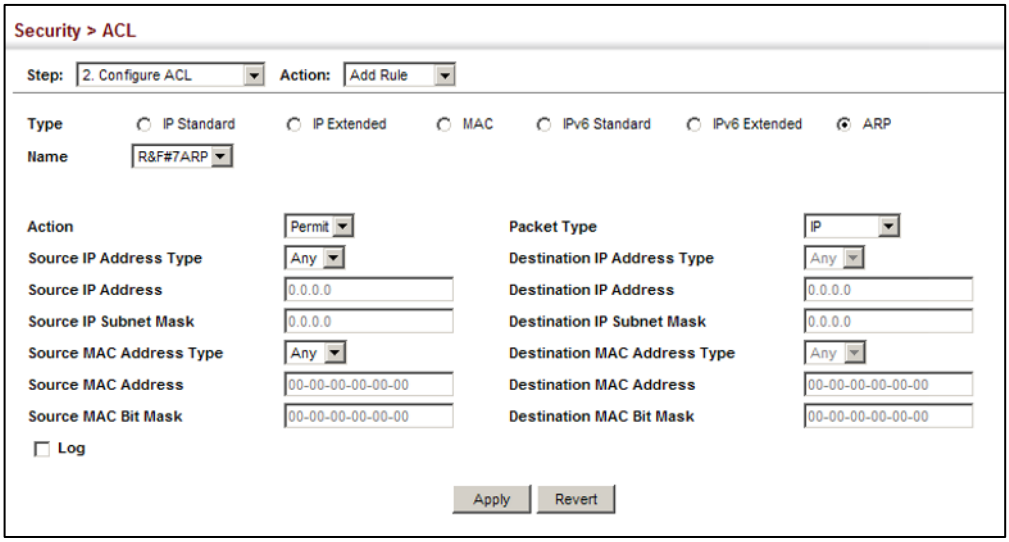
- Type - Name リストに表示する ACL のタイプを選択します。
- Name - 選択したタイプに一致する ACL の名前を表示します。
- Action - ACL には、permit ルールまたは deny ルールの任意の組み合わせを含めることができます。
- Packet Type - ARP 要求、ARP 応答、またはいずれかのタイプを示します。(範囲: IP, Request, Response; デフォルト: IP)
- Source/Destination IP Address Type - 送信元または宛先 IPv4 アドレスを指定します。すべての可能なアドレスを含めるには "Any"、アドレスフィールドに特定のホストアドレスを指定するには "Host"、アドレスフィールドと Mask フィールドでアドレス範囲を指定するには "IP"を使用します。(オプション: Any、Host、IP、デフォルト Any)
- Source/Destination IP Address - 送信元または宛先 IP アドレスです。
- Source/Destination IP Subnet Mask - 送信元または宛先アドレスのサブネットマスクです。(サブネットマスクの説明を参照してください。)
- Source/Destination MAC Address Type - すべての可能なアドレスを含めるには“Any”、特定の MAC アドレスを示すには“Host”、アドレスおよびマスクフィールドを使用してアドレス範囲を指定するには“MAC”を使用します。(オプション: Any、Host、MAC、デフォルト Any)
- Source/Destination MAC Address - 送信元または宛先 MAC アドレスです。
- Source/Destination MAC Bit Mask - 送信元 MAC アドレスまたは宛先 MAC アドレスの 16 進マスクです。
- Log - パケットがアクセス制御エントリと一致すると、パケットを記録します。

Web インタフェース

ARP ACL にルールを追加するには：

1. [Security]、[ACL]をクリックします。
2. [Step]リストから[Configure ACL]を選択します。
3. [Action]リストから[Add Rule]を選択します。
4. [Type]リストから[ARP]を選択します。
5. [Name]リストから ACL の名前を選択します。
6. 操作（permit または deny）を指定します。
7. パケットタイプ（Request、Response、All）を選択します。
8. アドレスタイプを選択(Any、Host、または IP)します。
9. [Host]を選択した場合は、特定のアドレス（例：11-22-33-44-55-66）を入力します。[IP]を選択した場合は、アドレス範囲のベースアドレスと 16 進数のビットマスクを入力します。
10. 必要に応じてログを有効にします。
11. [Apply]をクリックします。

図 11-34　ARP ACL の設定



11.5.9 ポートをアクセス制御リストにバインド

ACL を設定後、[Security]> [ACL（Configure Interface - Configure）]ページを使用して、トラフィックをフィルタリングする必要のあるポートを適切な ACL にバインドします。

Note: アクセスリストは物理ポートにのみバインドできます。ポートチャネルにアクセスリストをバインドする場合は、一度トランクポートの設定を削除し、アクセスリストを物理ポートへバインドした後、再度トランクポートの設定を行ってください。

パラメータ

次のパラメータが表示されます。

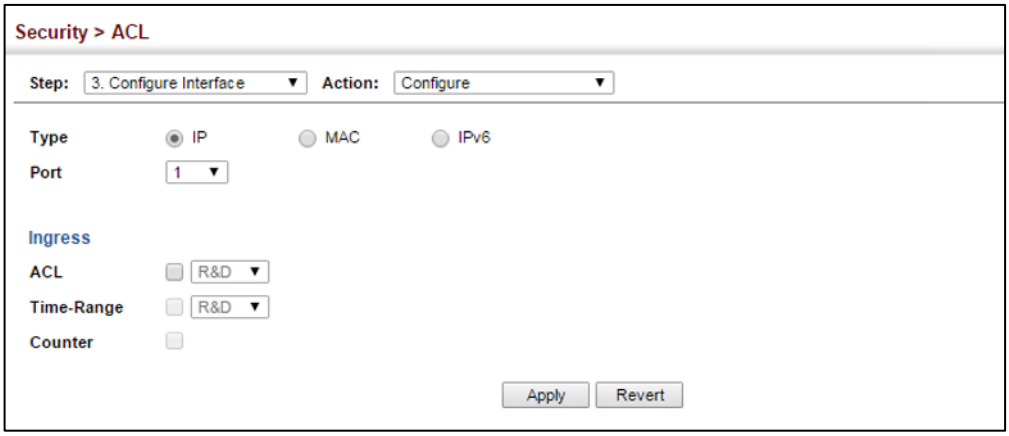
- Type - ポートにバインドする ACL のタイプを選択します。
- Port - ポート識別です。
- ACL -受信パケットに使用される ACL です。
- Time Range - 時間範囲の名前です。
- Counter - ACL 統計情報のカウンタを有効にします。

Web インタフェース

ACL をポートにバインドするには：

1. [Security]、[ACL]をクリックします。
2. [Step]リストから[Configure Interface]を選択します。
3. [Action]リストから[Configure]を選択します。
4. [Type]オプションから[IP]、[MAC]または[IPv6]を選択します。
5. ポートを選択します。
6. ACL リストから ACL の名前を選択します。
7. [Apply]をクリックします。

図 11-35　ポートへの ACL のバインド



11.5.10 ACL ハードウェアカウンタの表示

ACL ハードウェアカウンタの統計情報を表示するには、[Security]> [ACL]> [Configure Interface（Show Hardware Counters）]ページを使用します。

基準の選択

表示させたいデータの基準を設定します。

- Port - ポート識別です。(範囲: 1 から 10)
- Type - ACL のタイプを選択します。
- Direction - 受信トラフィックの統計情報を表示します。

Note: ACL を送信トラフィックに適用することはできません。

- Query - 選択した条件の統計を表示します。

標準 IPv4 ACL のパラメータ

次のパラメータが表示されます。

- ACL Name - ポートにバインドされている ACL です。
- Action - 指定されたパケットを permit または deny するかどうかを表示します。
- Source IP Address - ACL が有効な送信元 IP アドレスまたは IP アドレスの範囲です。
- Hit - この ACL と一致するパケット数を表示します。
- Clear Counter - 指定した ACL のヒットカウンタをクリアします。

拡張 IPv4 ACL のパラメータ

次のパラメータが表示されます。

- ACL Name - ポートにバインドされている ACL です。
- Action - 指定されたパケットを permit または deny するかどうかを表示します。
- Source IP Address - ACL が有効な送信元 IP アドレスまたは IP アドレスの範囲です。
- Destination IP Address - ACL が有効な宛先 IP アドレスまたは IP アドレスの範囲です。
- Source Port - プロトコルタイプの送信元ポート番号です。
- Destination Port - プロトコルタイプの宛先ポート番号です。

- Control Code - TCP 制御フラグです。(TCP ヘッダの 14 バイト目のフラグビット)
- Precedence - IP Precedence レベルです。
- DSCP - DSCP 優先レベルです。
- Time-Range - 時間範囲の名前です。
- Hit - この ACL と一致するパケット数を表示します。
- Clear Counter - 指定した ACL のヒットカウンタをクリアします。

MAC ACL のパラメータ

次のパラメータが表示されます。

- ACL Name - ポートにバインドされている ACL です。
- Action - 指定されたパケットを permit または deny するかどうかを表示します。
- Source MAC Address - ACL が有効な送信元 MAC アドレスです。
- Destination MAC Address - ACL が有効な宛先 MAC アドレスです。
- Packet Format - ACL が有効なパケットタイプです。
- VID - VLAN ID です。
- Ethernet Type - RFC1060 に準ずるイーサネットプロトコルタイプです。
- Hit - この ACL と一致するパケット数を表示します。
- Clear Counter - 指定した ACL のヒットカウンタをクリアします。

標準 IPv6 ACL のパラメータ

次のパラメータが表示されます。

- ACL Name - ポートにバインドされている ACL です。
- Action - 指定されたパケットを permit または deny するかどうかを表示します。
- Source IPv6 Address - ACL が有効な送信元 IPv6 アドレスまたは IPv6 アドレスの範囲を表示します。
- Hit - この ACL と一致するパケット数を表示します。
- Clear Counter - 指定した ACL のヒットカウンタをクリアします。

拡張 IPv6 ACL のパラメータ

次のパラメータが表示されます。

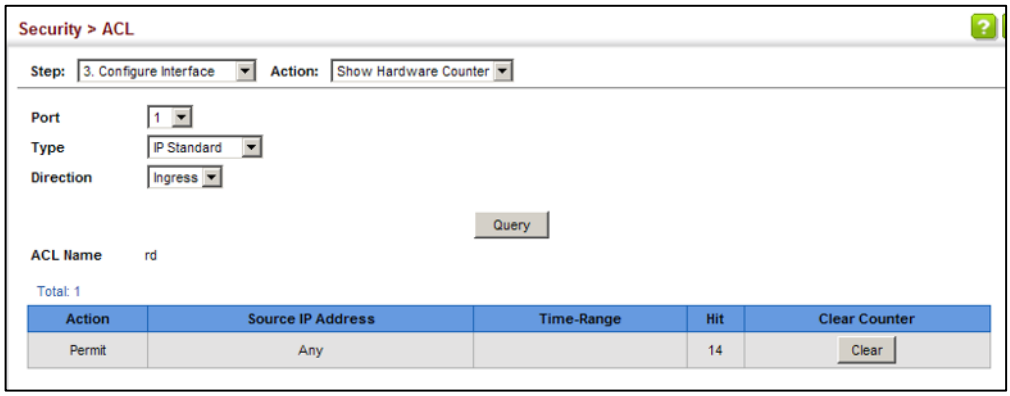
- ACL Name - ポートにバインドされている ACL です。
- Action - 指定されたパケットを permit または deny するかどうかを表示します。
- Source IPv6 Address - ACL が有効な送信元 IPv6 アドレスまたは IPv6 アドレスの範囲を表示します。
- Destination IPv6 Address - ACL が有効な宛先 IPv6 アドレスまたは IPv6 アドレスの範囲を表示します。
- DSCP - DSCP 優先レベルです。
- Next-Header - すぐ後に続く IPv6 ヘッダのタイプを表します。
- Time-Range - 時間範囲の名前です。
- Hit - この ACL と一致するパケット数を表示します。
- Clear Counter - 指定した ACL のヒットカウンタをクリアします。

Web インタフェース

ACL ハードウェアカウンタの統計情報を表示するには

1. [Security]、[ACL]をクリックします。
2. [Step]リストから[Configure Interface]を選択します。
3. [Action]リストから[Show Hardware Counter]を選択します。
4. ポートを選択します。
5. 受信トラフィックを選択します。

図 11-36　ACL 統計の表示



11.6 管理アクセス用の IP アドレスのフィルタリング

[Security]> [IP Filter]ページを使用して、Web インタフェース、SNMP、または Telnet 経由でスイッチへの管理アクセスが許可されている最大 15 の IP アドレスまたは IP アドレスグループのリストを作成します。

コマンドの使用方法

- 管理インタフェースは、デフォルトですべての IP アドレスに対して開いています。フィルタリストにエントリを追加すると、そのインタフェースへのアクセスは指定されたアドレスに制限されます。
- 無効なアドレスからスイッチの管理インタフェースにアクセスしようとすると、スイッチは接続を拒否し、システムログにイベントメッセージを入力し、トラップメッセージをトラップマネージャに送信します。
- IP アドレスは、それぞれ SNMP、Web、および Telnet アクセス用に構成できます。これらの各グループには個々のアドレスまたはアドレス範囲のいずれかで、最大 5 つの異なるアドレスセットを含めることができます。
- 同じグループ（SNMP、Web、または Telnet）のアドレスを入力する場合、スイッチは重複するアドレス範囲を受け入れません。異なるグループのアドレスを入力する場合、スイッチは重複したアドレス範囲を受け付けます。
- 指定した範囲から個々のアドレスを削除することはできません。範囲全体を削除し、アドレスを再入力する必要があります。
- 開始アドレスを指定するだけでアドレス範囲を削除することも、開始アドレスと終了アドレスの両方を指定することもできます。

パラメータ

次のパラメータが表示されます。

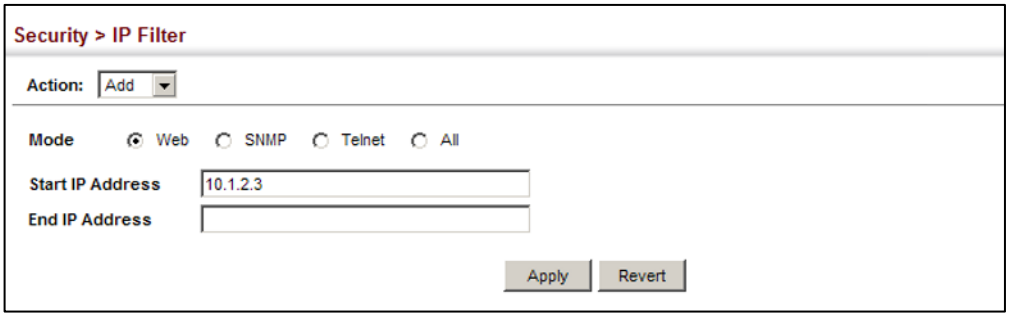
- モード
  - Web - Web グループの IP アドレスを設定します。
  - SNMP - SNMP グループの IP アドレスを設定します。
  - Telnet - Telnet グループの IP アドレスを設定します。
  - All - すべてのグループの IP アドレスを設定します。
- Start IP Address - 単一の IP アドレス、または範囲の開始アドレスです。
- End IP Address - 範囲の終了アドレスです。

Web インタフェース

管理アクセス用に認証された IP アドレスのリストを作成するには：

1. [Security]、[IP Filter]をクリックします。
2. [Action]リストから[Add]を選択します。
3. フィルタリングする管理インタフェース（Web、SNMP、Telnet、All）を選択します。
4. インタフェースへの管理アクセスを許可する IP アドレスまたはアドレスの範囲を入力します。
5. [Apply]をクリックします。

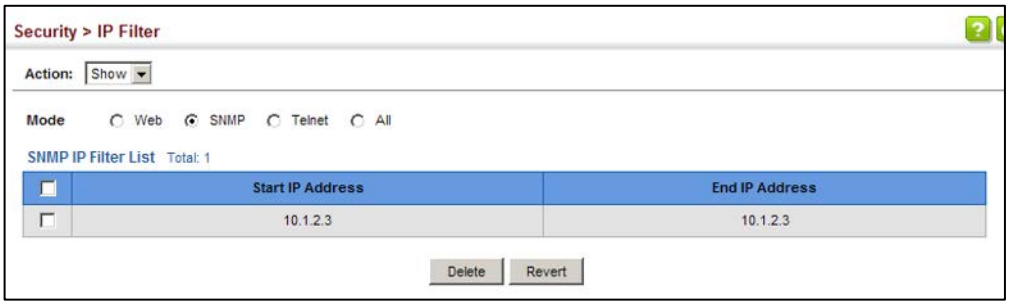
図 11-37　管理アクセス用の IP アドレスフィルタの作成



管理アクセス用に認証された IP アドレスのリストを表示するには：

1. [Security]、[IP Filter]をクリックします。
2. [Action]リストから[Show]を選択します。

図 11-38　管理アクセス用に認証された IP アドレスの表示



11.7 ポートセキュリティの設定

[Security]> [Port Security]ページを使用して、スイッチポートで学習され、アドレステーブルに保存され、ネットワークにアクセスする権限を持つデバイス MAC アドレスの最大数を設定します。

ポートセキュリティがポートで有効になっている場合、スイッチは設定された最大数に達したときに、指定されたポート上で新しい MAC アドレスの学習を停止します。アドレステーブルにすでに格納されている送信元アドレスを持つ受信トラフィックだけが、そのポートを介してネットワークにアクセスする権限を与えられます。許可されていない MAC アドレスを持つデバイスがスイッチポートを使用しようとすると、侵入が検出され、スイッチは自動的にポートを無効にしてトラップメッセージを送信することができます。

コマンドの使用方法

- セキュアポートで許可される MAC アドレスのデフォルト最大数はゼロです（つまり、無効です)。ポートセキュリティを使用するには、ポートに許可されている最大アドレス数を設定する必要があります。
- ポートで学習できるアドレスエントリの最大数を設定し、許可されている動的アドレスの最大数を指定します。スイッチは、ポートで受信したフレームの許可されたアドレスペアの最大数<送信元 MAC アドレス、VLAN>を学習します。ポートが MAC アドレスの最大数に達すると、ポートは新しいアドレスの学習を停止します。すでにアドレステーブルにある MAC アドレスは保持され、期限切れになりません。
  静的アドレステーブルを使用して、追加のセキュアアドレスを手動でポートに追加することができます。
- ポートのセキュリティ状態が有効から無効に変更されると、動的に学習されたすべてのエントリがアドレステーブルからクリアされます。
- ポートセキュリティが有効で、最大許容アドレス数がゼロ以外の値に設定されている場合、ポートの使用を試みているアドレステーブルにないすべてのデバイスが、スイッチからのアクセスを防御します。
- セキュリティ違反のためにポートが無効になっている（シャットダウンされている）場合は、[Interface]> [Port]> [General]ページにおいて、手動で再度有効にする必要があります。
- セキュアポートには以下の制限があります:
  - 静的または動的トランクのメンバーとして使用することはできません。
  - ポートセキュリティを設定したインタフェースをネットワーク相互接続装置に接続すべきではありません。
  - RSPAN とポートセキュリティは、相互に排他的な機能です。ポートセキュリティがポート上で有効な場合、ポートは RSPAN アップリンクポートとして設定することはできません。また、ポートが RSPAN アップリンクポートとして設定されている場合、送信元ポートまたは宛先ポート、ポートセキュリティはポート上で有効にできません。
  - MAC アドレス学習を無効化している状態では、ポートセキュリティは有効に出来ません。

パラメータ

次のパラメータが表示されます。

- Port - ポート識別子です。
- Security Status - ポートのポートセキュリティを有効または無効にします。(デフォルト: Disabled)
- Port Status - 操作ステータスです。

- Secure/Down - ポートセキュリティが無効です。
- Secure/Up - ポートセキュリティが有効です。
- Shutdown - ポートセキュリティ違反の応答のため、ポートはシャットダウンしています。

◆ Action - ポートセキュリティ違反が検出されたときに実行される操作を示します。
- None: 何もする必要はありません。(これがデフォルトです。)
- Trap: SNMP トラップメッセージを送信します。
- Shutdown: ポートを無効にします。
- Trap and Shutdown: SNMP トラップメッセージを送信し、ポートを無効にします。

◆ Max MAC Count - ポートで学習できる MAC アドレスの最大数です。(範囲: 0 から 1024。0 は無効の意味です)
最大アドレスカウントは、ポートセキュリティが有効または無効の場合に有効です。

◆ Current MAC Count - このインタフェースに現在関連付けられている MAC アドレスの数。

◆ MAC Filter ID - MAC アドレスフィルタの識別子です。

◆ Last Intrusion MAC - 最後に許可されていない MAC アドレスが検出されました。

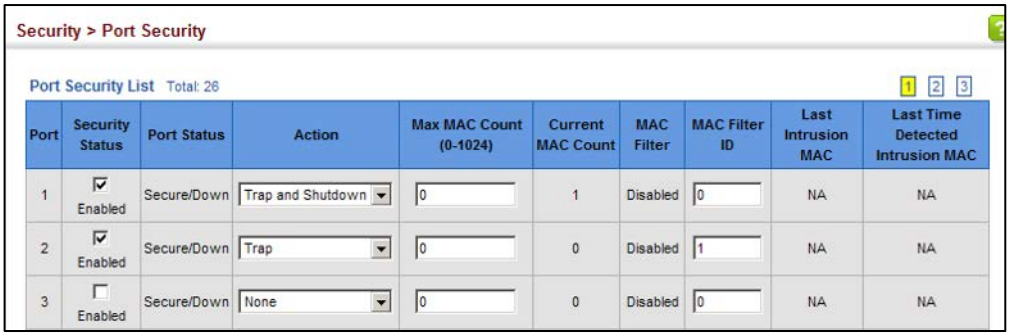
◆ Last Time Detected Intrusion MAC - 不正な MAC アドレスが最後に検出された時刻です。

Web インタフェース

ポートセキュリティを設定するには：

1. [Security]、[Port Security]をクリックします。
2. Security Status 列のチェックボックスをオンにすると、セキュリティを有効にし、無効なアドレスがポートで検出されたときに実行する操作を設定し、ポートで許可されている MAC アドレスの最大数を設定します。
3. [Apply]をクリックします。

図 11-39　ポートセキュリティの設定



11.8 DoS 攻撃プロテクション

DoS（Denial of Service）攻撃から保護するには、[Security]> [DoS Protection]ページを使用します。DoS 攻撃は、コンピュータまたはネットワークリソースによって提供されるサービスをブロックする攻撃です。この種の攻撃は、インターネットサイトやサービスが効率的に機能しないようにさせます。一般的に、DoS 攻撃は、ターゲットを強制的にリセットしたり、リソースの大部分を消費して意図したサービスを提供できないようにしたり、意図したユーザとターゲットとの間の通信メディアを妨害して、 適切に通信できないようにします。この章では、DoS 攻撃から保護する方法について説明します。

パラメータ

次のパラメータが表示されます。

- Echo/Chargen Attack - 送信されたものと同じものを送り返す Echo サービスと、連続したデータストリームを生成する chargen（キャラクタジェネレータ）サービスを使った攻撃です。一緒に使用すると、無限ループが発生し DoS が発生します。(デフォルト: Disabled)
- Echo/Chargen Attack Rate - 最大許容レートです。(範囲: 64 から 2000 kbits /秒; デフォルト：1000 kbits /秒)
- Smurf Attack - 攻撃者がブロードキャスト宛先 IP アドレス（255.255.255.255）への偽装された ICMP エコー要求トラフィックを大量に生成する攻撃です。それらのすべては、攻撃対象の送信元アドレスに偽装したパケットを使用しています。攻撃対象は、返ってくる大量の ICMP エコー応答パケットを処理するために多くの割り込みが必要なため、クラッシュしてしまいます。(デフォルト: Disabled)
- TCP Flooding Attack - 攻撃者が TCP SYN 要求（送信元 IP が偽装されているかどうかにかかわらず）をターゲットに送信し、ACK パケットを返さないようにする攻撃です。これらのハーフオープン接続は、ターゲット上のリソースをバインドし新しい接続を行うことができず、これにより DoS が発生します。(デフォルト: Disabled)
- TCP Flooding Attack Rate - 最大許容レートです。(範囲: 64 から 2000 kbits /秒; デフォルト：1000 kbits /秒)
- TCP Null Scan - 受信 TCP ポートを識別するために、TCP NULL スキャンメッセージが使用されます。このスキャンでは、シーケンス番号が 0 でフラグがない構成の TCP パケットが使用されます。ターゲットの TCP ポートが閉じている場合、ターゲットは TCP RST(リセット)パケットで応答します。ターゲット TCP ポートが開いている場合には、単純に TCP NULL スキャンを破棄します。(デフォルト: Disabled)
- TCP-SYN/FIN Scan - 受信 TCP ポートを識別するために TCP SYN / FIN スキャンメッセージが使用されます。スキャンでは、SYN(同期)フラグと FIN(終了)フラグを含む構成の TCP パケットを使用します。ターゲットの TCP ポートが閉じている場合、ターゲットは TCP RST(リセット)パケットで応答します。ターゲット TCP ポートが開いている場合には、単純に TCP SYN FIN スキャンを破棄します。(デフォルト: Disabled)
- TCP Xmas Scan - 受信 TCP ポートを識別するために、いわゆる TCP XMAS スキャンメッセージが使用されます。このスキャンは、シーケンス番号 0 と URG、PSH、および FIN フラグを含む構成の TCP パケットを使用します。ターゲットの TCP ポートが閉じている場合、ターゲットは TCP RST パケットで応答します。ターゲット TCP ポートが開いている場合には、TCP XMAS スキャンを破棄します。(デフォルト: Disabled)
- UDP Flooding Attack - 攻撃者がリモートホスト上のランダムなポートに大量の UDP パケット（送信元 IP が偽装されているかどうかにかかわらず）を送信する攻撃です。ターゲットは、アプリケーションがそのポートで待機中であると判断し、ICMP Destination Unreachable パケットで応答します。多くの ICMP パケットを強制的に送信することになり、最終的に他のクライアントに到達できなくなります。

(デフォルト: Disabled)

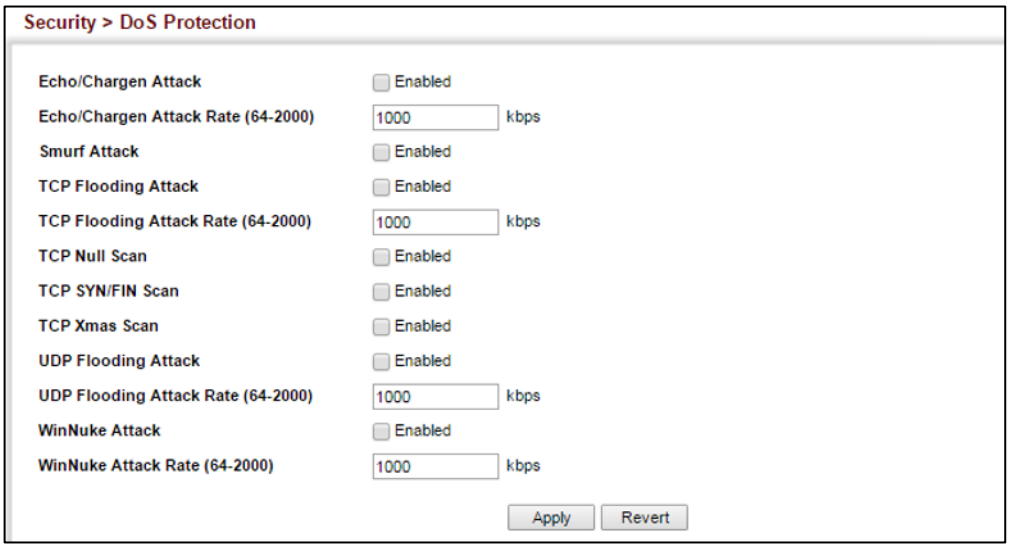
- UDP Flooding Attack Rate - 最大許容レートです。(範囲: 64 から 2000 kbits /秒; デフォルト：1000 kbits /秒)
- WinNuke Attack - Microsoft Windows 3.1x / 95 / NT オペレーティングシステムに影響を与えた攻撃です。この種の攻撃では、TCP URG フラグを含む OOB(OOB out-of-band)パケットの文字列をターゲットコンピュータの TCP ポート 139(NetBIOS)に送信することで、ロックして「ブルースクリーン 」の表示を引き起こします。これにより、コンピュータのハードディスクに何らの損害やデータの変更が生じることはありませんが、保存されていないデータは失われます。Microsoft は WinNuke 攻撃を防ぐためのパッチを作成しましたが、OOB パケットは依然として利用可能なすべての CPU 時間を消費するタイトなループを引き起こします。(デフォルト: Disabled)
- WinNuke Attack Rate - 最大許容レートです。(範囲: 64 から 2000 kbits /秒; デフォルト：1000 kbits /秒)

Web インタフェース

DoS 攻撃から保護するには：

1. [Security]、[DoS Protection]の順にクリックします。
2. 特定の DoS 攻撃に対する保護を有効にし、必要に応じて最大許容レートを設定します。
3. [Apply]をクリックします。

図 11-40　DoS 攻撃からの保護



11.9 DHCP スヌーピング

DHCP スヌーピングで登録された動的バインディング（または IP ソースガードで設定された静的バインディングを使用）を使用して、安全ではないポートの DHCP クライアントに割当てられたアドレスを慎重に制御できます。DHCP スヌーピングにより、スイッチは不正な DHCP サーバまたはポート関連の情報を DHCP サーバに送信する他のデバイスからネットワークを保護できます。この情報は物理ポートに戻って IP アドレスを追跡する際に有益です。

コマンドの使用方法

DHCP スヌーピングプロセス

- 悪意のある DHCP メッセージが外部の送信元から受信されると、ネットワークトラフィックが中断される可能性があります。DHCP スヌーピングは、ネットワークまたはファイヤアウォールの外側から非セキュアインタフェースで受信した DHCP メッセージをフィルタリングするために使用されます。DHCP スヌーピングをグローバルに有効にして VLAN インタフェースで有効にすると、DHCP スヌーピングテーブルにリストされていないデバイスから信頼されていないインタフェースで受信された DHCP メッセージが廃棄されます。
- テーブルエントリは、信頼されたインタフェースに対してのみ学習されます。クライアントが DHCP サーバから IP アドレスを受信または解放すると、エントリが DHCP スヌーピングテーブルに動的に追加または削除されます。各エントリには、MAC アドレス、IP アドレス、リース時間、VLAN 識別子、およびポート識別子が含まれています。
- スイッチが処理できる DHCP メッセージ数のレート制限は 100 パケット/秒です。この制限を超える DHCP パケットはすべて破棄されます。
- DHCP スヌーピングが有効の場合、信頼されないインタフェースに入る DHCP メッセージは、DHCP スヌーピングを介して学習された動的エントリにもとづいてフィルタリングされます。
- フィルタリングルールは以下のように導入します:
  - グローバル DHCP スヌーピングが無効の場合、すべての DHCP パケットが転送されます。
  - グローバル DHCP スヌーピングがグローバルに有効で、DHCP パケットが受信される VLAN 上でも有効な場合は、すべての DHCP パケットは信頼できるポートに転送されます。受信したパケットが DHCP ACK メッセージの場合には、動的 DHCP スヌーピングエントリもバインディングテーブルに追加されます。
  - DHCP スヌーピングがグローバルに有効化され、また DHCP パケットが受信される VLAN でも有効化されるが、ポートが信頼できない場合には、以下のように処理します:
    - DHCP パケットが DHCP サーバからのリプライパケット(OFFER、ACK または NAK メッセージを含む)の場合、パケットは破棄されます。
    - DHCP パケットが、DECLINE または RELEASE メッセージのようなクライアントからの場合、対応エントリがバインディングテーブルで見つかった時、スイッチはパケットのみを転送します。
    - DISCOVER、REQUEST、INFORM、DECLINE または RELEASE メッセージなどの DHCP パケットがクライアントからのものである場合、MAC アドレス検証が無効になっているとパケットは転送されます。ただし、MAC アドレス検証が有効な場合、DHCP パケットに格納されているクライアントのハードウェアアドレスがイーサネットヘッダーの送信元 MAC アドレスと同じである場合にのみ、パケットは転送されます
    - DHCP パケットが認識可能なタイプでない場合、これは破棄されます。
  - クライアントからの DHCP パケットが上記のフィルタリング基準を満たす場合、その VLAN は同

じ VLAN 内の信頼できるポートにのみ転送されます。

- 信頼されたポートでサーバからの DHCP パケットが受信された場合、そのパケットは同じ VLAN 内の信頼できるポートと信頼されていないポートの両方に転送されます。
- DHCP スヌーピングがグローバルに無効になっていると、すべての動的バインディングがバインディングテーブルから削除されます。
- スイッチ自体が DHCP クライアントである場合の追加の考慮事項―スイッチがクライアント要求を DHCP サーバに送信するためのポートは、信頼できるものとして設定する必要があります。DHCP サーバから ACK メッセージを受信すると、スイッチはバインディングテーブルに動的エントリを追加しません。また、スイッチが DHCP クライアントパケットを送信すると、フィルタリングは行われません。ただし、スイッチが DHCP サーバからメッセージを受信すると、信頼できないポートから受信したパケットはすべて廃棄されます。

DHCP スヌーピングオプション 82

- DHCP は、DHCP クライアントまたはリレーエージェント自体に関する情報を DHCP サーバに送信するためのリレーメカニズムを提供します。DHCP オプション 82 とも呼ばれ、互換性のある DHCP サーバは、IP アドレスを割当てる際に情報を使用したり、クライアントに対して他のサービスやポリシーを設定したりすることができます。また、IP スプーフィング、クライアント識別子スプーフィング、MAC アドレススプーフィング、アドレス枯渇など、DHCP サービス上の接続されたクライアントからの悪意のあるネットワーク攻撃を防ぐための効果的なツールです。
- オプション 82 の情報を要求パケットに挿入するには、DHCP スヌーピングを有効にする必要があります。
- DHCP スヌーピング情報オプション 82 が有効になると、要求側のクライアント(または自身を記述するために情報フィールドを使用した中間のリレーエージェント）が、スイッチによって転送された DHCP 要求パケットと送信された応答パケット DHCP サーバから戻ってきます。この情報は、要求デバイスの MAC アドレスまたは IP アドレス（このコンテキストではスイッチ）を指定することができます。
  デフォルトでは、スイッチはオプション 82 の circuit-id フィールドに、スイッチが DHCP クライアント要求を受信したローカルインタフェース（ポートと VLAN ID を含む）を示す情報も入力します。これにより、DHCP クライアントとサーバ間の交換メッセージを、VLAN 全体にフラッディングすることなく、サーバとクライアント間で転送することができます。
- スイッチ上で DHCP スヌーピング情報オプション 82 が有効になっている場合、DHCP スヌーピングフィルタリングルールに応じて、任意の VLAN で受信した DHCP 要求パケットに情報を挿入できます。リレーされたパケットに挿入される情報には、circuit-id と remote-id、およびゲートウェイのインターネットアドレスが含まれます。
- スイッチがクライアントから受信した DHCP パケットに、DHCP オプション 82 情報が既に含まれている場合の、スイッチでのこれらのパケットの操作ポリシーが設定できます。
  DHCP パケットをドロップするか、既存の情報を保持するか、スイッチのリレー情報で置換します。

11.9.1 DHCP スヌーピンググローバル設定

[Security]> [DHCP Snooping（Configure Global）]ページを使用して、スイッチ上で DHCP スヌーピングをグローバルに有効にするか、MAC アドレス検証を設定します。

パラメータ

次のパラメータが表示されます。

一般

- DHCP Snooping Status - DHCP スヌーピングをグローバルに有効にします。(デフォルト: Disabled)

- DHCP Snooping MAC-Address Verification - MAC アドレスの確認を有効または無効にします。パケットのイーサネットヘッダー内の送信元 MAC アドレスが、DHCP パケット内のクライアントのハードウェアアドレスと同じでない場合、パケットは廃棄されます。(デフォルト: Enabled)

情報

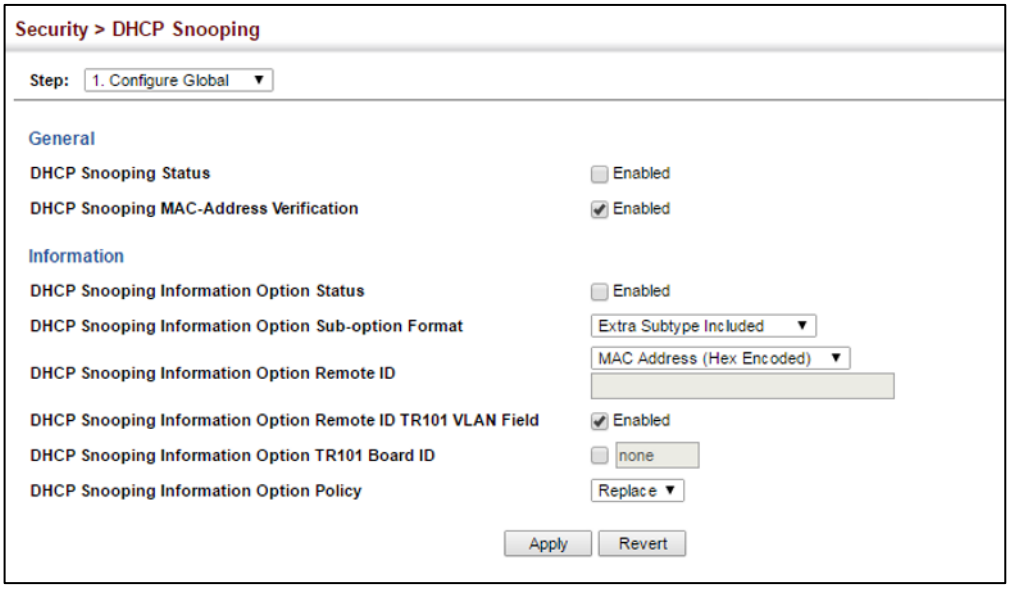
- DHCP Snooping Information Option Status - DHCP オプション 82 情報リレーを有効または無効にします。(デフォルト: Disabled)
- DHCP Snooping Information Option Sub-option Format - オプション 82 情報のサーキット ID（CID）およびリモート ID（RID）のサブタイプおよびサブ長フィールドの使用を有効または無効にします。(デフォルト: Extra Subtype Included)
- DHCP Snooping Information Option Remote ID - 要求デバイス（つまり、このコンテキストのスイッチ）の MAC アドレス、IP アドレス、または任意の識別子、または TR01 を指定します。
  - MAC Address - DHCP スヌーピングエージェントのリモート ID サブオプション（つまり、スイッチの CPU の MAC アドレス）に MAC アドレスを挿入します。この属性は、16 進数または ASCII でエンコードできます。
  - IP Address - DHCP スヌーピングエージェントのリモート ID サブオプション（つまり、管理インタフェースの IP アドレス）に IP アドレスを挿入します。この属性は、16 進数または ASCII でエンコードできます。
  - string - リモート識別子フィールドに挿入された任意の文字列です。(範囲: 1 から 32 文字)
  - TR101-TR101 構文に従いノード識別子を挿入します。
- DHCP Snooping Information Option Remote ID TR101 VLAN Field - タグなしパケット用の TR101 フィールドに“:VLAN”を追加します。
  TR101 オプション 82 のフォーマットは: “<IP> eth <SID>/<PORT>[:<VLAN>]”.SID(スイッチ ID)は常に 0 であることに留意してください。デフォルトでは、PVID はタグ無しパケットの TR101 フィールドの末尾に追加されます。タグ付きパケットの場合、VLAN ID は常に追加されます。
- DHCP Snooping Information Option TR101 Board ID - TR-101 の構文をもとにオプション 82 情報の中で使用されるボード識別子を設定します。(範囲: 0-9; Default: undefined)
- DHCP Snooping Information Option Policy - すでにオプション 82 情報を含む DHCP クライアント要求パケットを処理する方法を指定します。
  - Drop - クライアントの要求パケットをリレーするのではなく、ドロップします。
  - Keep - クライアント要求内のオプション 82 情報を保持し、パケットをトラステッドポートに転送します。
  - Replace - クライアントの要求内のオプション 82 の information circuit-id および remote-id フィールドを、リレーエージェント自体に関する情報で置換、リレーエージェントのアドレスを挿入し（DHCP スヌーピングが有効な場合）、パケットをトラステッドポートに転送します。(This is the default policy.)

Web インタフェース

DHCP スヌーピングのグローバルを設定するには：

1. [Security]、[DHCP Snooping]の順にクリックします。
2. [Step]リストから[Configure Global]を選択します。
3. 一般的な DHCP スヌーピングプロセスおよび DHCP スヌーピング情報オプションに必要なオプションを選択します。
4. [Apply]をクリックします。

図 11-41　DHCP スヌーピングのグローバル設定



11.9.2 DHCP スヌーピング VLAN の設定

特定の VLAN で DHCP スヌーピングを有効または無効にするには、[Security]> [DHCP Snooping（Configure VLAN）]ページを使用します。

コマンドの使用方法

- DHCP スヌーピングがスイッチ上でグローバルに有効にされ、指定された VLAN で有効にされると、VLAN 内の信頼できないポートで DHCP パケットフィルタリングが実行されます。
- DHCP スヌーピングがグローバルに無効になっている場合でも、特定の VLAN に対して DHCP スヌーピングを設定することはできますが、DHCP スヌーピングをグローバルに再度有効にするまでは変更は反映されません。
- DHCP スヌーピングがグローバルに有効にされ、VLAN 上で DHCP スヌーピングが無効になると、この VLAN に対して学習されたすべての動的バインディングがバインディングテーブルから削除されます。

パラメータ

次のパラメータが表示されます。

- VLAN - 設定済み VLAN の ID です。(範囲: 1 から 4094)
- DHCP Snooping Status - 選択した VLAN の DHCP スヌーピングを有効または無効にします。DHCP スヌーピングがスイッチ上でグローバルに有効にされ、指定された VLAN で有効にされると、VLAN 内の信頼できないポートで DHCP パケットフィルタリングが実行されます。(デフォルト: Disabled)

Web インタフェース

DHCP スヌーピングのグローバルを設定するには：

1. [Security]、[DHCP Snooping]の順にクリックします。
2. [Step]リストから[Configure VLAN]を選択します。
3. 既存の VLAN で DHCP スヌーピングを有効にする。

4. [Apply]をクリックします。

図 11-42　VLAN での DHCP スヌーピングの設定

11.9.3 DHCP スヌーピング用のポートの設定

[Security]> [DHCP Snooping（Configure Interface）]ページを使用して、スイッチポートを信頼済みまたは信頼できないものとして設定します。

コマンドの使用方法

- 信頼できるインタフェースは、ネットワーク内からのメッセージのみを受信するように設定されたインタフェースです。信頼できないインタフェースとは、ネットワークの外側、またはファイアウォールからのメッセージを受信するように設定されたインタフェースです。
- DHCP スヌーピングがグローバルおよび VLAN の両方で有効にされている場合、DHCP パケットフィルタリングは VLAN 内の信頼できないポートで実行されます。
- 信頼できないポートが信頼できるポートに変更される場合、ポートに関連するすべての動的 DHCP スヌーピングバインディングは削除されます。
- ローカルネットワークまたはファイアウォール内の DHCP サーバに接続されているすべてのポートを信頼できる状態に設定します。ローカルネットワークまたはファイアウォール外の他のすべてのポートを信頼できない状態に設定します。
- TR101 オプション 82 のフォーマットは: “<IP> eth <SID>/<PORT>[:<VLAN>]”.SID(スイッチ ID)は常に 0 であることに留意してください。デフォルトでは、PVID はタグ無しパケットの TR101 フィールドの末尾に追加されます。タグ付きパケットの場合、VLAN ID は常に追加されます。

パラメータ

次のパラメータが表示されます。

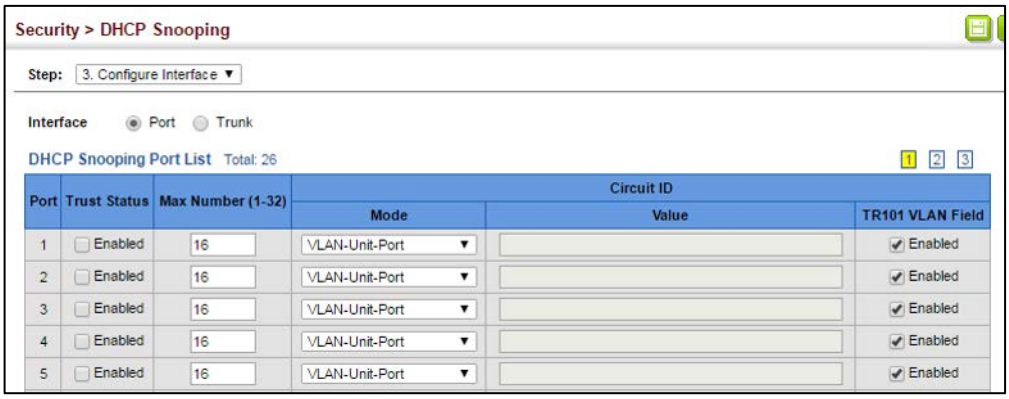
- Trust Status - ポートを信頼できるポートとして使用可能または使用不可にします。(デフォルト: Disabled)
- Max Number - インタフェースごとにサポートできる DHCP クライアントの最大数です。(範囲: 1-32、デフォルト：16)
- Circuit ID - DHCP オプション 82 のサーキット ID サブオプション情報を指定します。
  - Mode - デフォルト文字列 "VLAN-Unit-Port"、または任意の文字列、または TR101 を指定します。(デフォルト: VLAN-Unit-Port)
  - Value - サーキット識別子フィールドに挿入された任意の文字列です。(範囲: 1 から 32 文字)
  - TR101 VLAN Field - タグなしパケット用の TR101 フィールドに “:VLAN”を追加します。

Web インタフェース

DHCP スヌーピングのグローバルを設定するには：

1. [Security]、[DHCP Snooping]の順にクリックします。
2. [Step]リストから[Configure Interface]を選択します。
3. ローカルネットワークまたはファイアウォール内の任意のポートを信頼できるものに設定します。
4. サーキット ID 情報の送信に使用するモードと、必要に応じて任意の文字列を指定します。
5. [Apply]をクリックします。

図 11-43　DHCP スヌーピングのポートモードの設定



11.9.4 DHCP スヌーピングバインディング情報の表示

[Security]> [DHCP Snooping（Show Information）]ページを使用して、バインディングテーブルのエントリを表示します。

パラメータ

次のパラメータが表示されます。

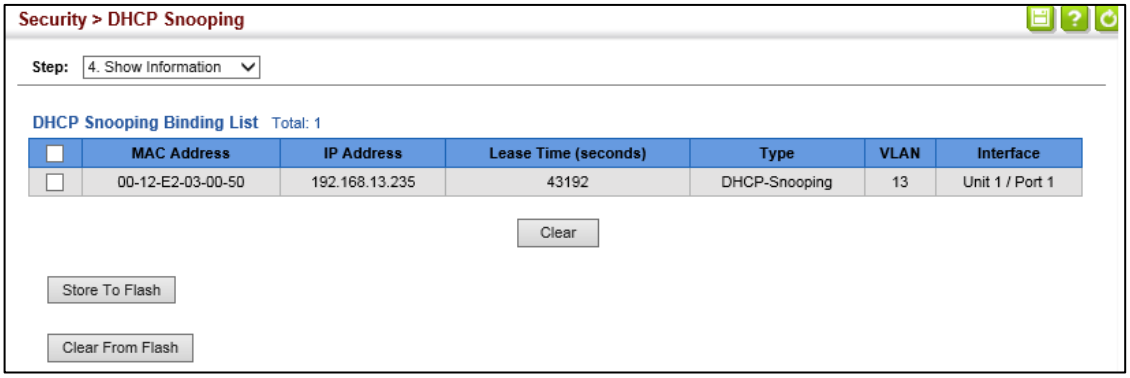
- MAC Address - エントリに関連付けられた物理アドレスです。
- IP Address - クライアントに対応する IP アドレスです。
- Lease Time - この IP アドレスがクライアントにリースされる時間です。
- Type - エントリの種類は次のとおりです。
  - DHCP-Snooping - 動的にスヌーピングされています。
- VLAN - このエントリがバインドされている VLAN です。
- Interface - このエントリがバインドされているポートまたはトランクです。
- Store - 動的に学習されたすべてのスヌーピングエントリをフラッシュメモリに書き込みます。この機能を使用して、現在学習している動的 DHCP スヌーピングエントリをフラッシュメモリに保存できます。スイッチがリセットされると、これらのエントリはスヌーピングテーブルに復元されます。ただし、フラッシュメモリから復元された動的エントリのリース期間は有効ではなくなります。
- Clear - 動的に学習されたすべてのスヌーピングエントリをフラッシュメモリから削除します。

Web インタフェース

DHCP スヌーピングのバインディングテーブルを表示するには：

1. [Security]、[DHCP Snooping]の順にクリックします。
2. [Step]リストから[Show Information]を選択します。
3. 必要に応じて Store または Clear 機能を使用します。

図 11-44　DHCP スヌーピングのバインディングテーブルの表示



11.10 IPv4 ソースガード

IPv4 ソースガードは、IP ソースガードテーブルの手動で設定されたエントリ、または有効になっている場合の DHCP スヌーピングテーブルの動的エントリにもとづいて、ネットワークインタフェース上の IP トラフィックをフィルタリングするセキュリティ機能です。IP ソースガードは、ホストがネイバーの IPv4 アドレスを使用してネットワークにアクセスしようとするときに発生するトラフィック攻撃を防止するために使用できます。ここでは、IPv4 ソースガードの設定方法について説明します。

11.10.1 IPv4 ソースガード用のポートの設定

[Security]> [IP Source Guard]> [General]ページを使用して、送信元 IP アドレス、または送信元 IP アドレスと MAC アドレスのペアにもとづいてフィルタリングタイプを設定します。また、ACL バインディングテーブルまたは MAC アドレスバインディングテーブル内のルックアップ、およびルックアップテーブルの許可されたバインディングエントリの最大数も指定します。

IP ソースガードは、ネットワークまたはファイアウォールの外側からメッセージを受信する安全でないポートでトラフィックをフィルタリングするために使用されるため、ネイバーの IP アドレスを使用しようとしているホストによるトラフィック攻撃の対象となります。

コマンドの使用方法

フィルタタイプ

- ソースガードモードを SIP（Source IP）または SIP-MAC（Source IP and MAC）に設定すると、選択したポートでこの機能が有効になります。SIP オプションを使用して、バインディングテーブルのすべてのエントリに対して VLAN ID、送信元 IP アドレス、ポート番号を確認します。SIP-MAC オプションを使用して、これらの同じパラメータに加えて送信元 MAC アドレスを確認します。一致するエントリが見つからない場合、パケットは廃棄されます。

Note: マルチキャストアドレスは IP ソースガードで使用できません。

- 有効にすると、トラフィックは DHCP スヌーピングまたはソースガードバインディングテーブルで設定された静的アドレスを介して学習された動的エントリにもとづいてフィルタリングされます。
- IP ソースガードが有効の場合、着信パケットの IP アドレス（SIP オプション）またはその IP アドレスと対応する MAC アドレス（SIP-MAC オプション）の両方がバインディングテーブルに対してチェックされます。一致するエントリが見つからない場合には、パケットは破棄されます。
- 同じ MAC アドレスと異なる VLAN ID を持つエントリを、バインディングテーブルに追加することはできません。
- フィルタリングルールは以下のように導入します:
  - DHCP スヌーピングが無効になっている場合、IP ソースガードは VLAN ID、送信元 IP アドレス、ポート番号、および送信元 MAC アドレス（SIP-MAC オプションの場合）をチェックします。一致するエントリがバインディングテーブルに見つかり、エントリタイプが静的 IP ソースガードバインディングの場合には、パケットは転送されます。
  - DHCP スヌーピングが有効の場合、IP ソースガードは VLAN ID、送信元 IP アドレス、ポート番号、および送信元 MAC アドレス（SIP-MAC オプションの場合）をチェックします。一致するエントリがバインディングテーブルに見つかり、エントリタイプが静的 IP ソースガードバインディングまたは動的 DHCP スヌーピングバインディングの場合には、パケットは転送されます。
  - IP ソースバインディングがまだ設定されていないインタフェース（IP ソースガードバインディン

グテーブルの静的設定でも DHCP スヌーピングからも動的に学習されていないインタフェース）で IP ソースガードが有効になっている場合、DHCP スヌーピングで許可された DHCP パケットを除き、スイッチはそのポート上のすべての IP トラフィックをドロップします。

パラメータ

次のパラメータが表示されます。

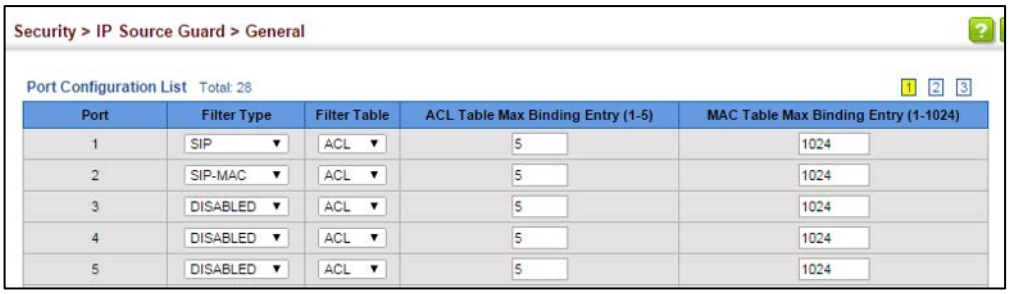
- Filter Type - インバウンドトラフィックに基づく送信元 IP アドレス、または送信元 IP アドレスと対応する MAC アドレスをフィルタリングするようにスイッチを設定します。(デフォルト: None)
  - Disabled - ポート上の IP ソースガードフィルタリングを無効にします。
  - SIP - バインディングテーブルに格納されている IP アドレスにもとづいてトラフィックフィルタリングを有効にします。
  - SIP-MAC - バインディングテーブルに格納されている IP アドレスと対応する MAC アドレスにもとづいてトラフィックフィルタリングを有効にします。
- Filter Table - ソースガード学習モデルを設定して、ACL バインディングテーブルまたは MAC アドレスバインディングテーブルのアドレスを検索します。(デフォルト: ACL binding table)
- Max Binding Entry - インタフェースにバインドできるエントリの最大数です。(ACL Table: 1 から 5, デフォルト: 5; MAC Table: 1 から 32, デフォルト: 16)
  このパラメータは、DHCP スヌーピングによって検出された動的エントリと IP ソースガードによって設定された静的エントリの両方を含む、バインディングテーブルのインタフェースにマップできるアドレスエントリの最大数を設定します。

Web インタフェース

ポートの IP ソースガードフィルタを設定するには、次の手順を実行します。

1. [Security]、[IP Source Guard]、[General]をクリックします。
2. 必要なフィルタリングタイプを設定し、ACL または MAC アドレスバインディングを使用するようにテーブルタイプを設定し、各ポートの最大バインディングエントリを設定します。
3. [Apply]をクリックします。

図 11-45　IPv4 ソースガードのフィルタタイプの設定



11.10.2 IPv4 ソースガードの静的バインディングの設定

静的アドレスをポートにバインドするには、[Security]> [IP Source Guard]> [Static Binding（Configure ACL Table と Configure MAC Table）]ページを使用します。テーブルエントリには、MAC アドレス、IP アドレス、VLAN 識別子、およびポート識別子が含まれます。すべての静的

エントリは、無期限のリース時間で構成されます。このリース時間は、表にゼロの値で示されます。

コマンドの使用方法

- MAC アドレス、IP アドレス、VLAN 識別子、ポート識別子を含むテーブルエントリです。
- ソースガードバインディングテーブルに入力された静的アドレスは、無期限のリース時間で自動的に設定されます。
- ソースガードが有効の場合、トラフィックは DHCP スヌーピングによって学習された動的エントリ、またはソースガードバインディングテーブルで設定された静的アドレスにもとづいてフィルタリングされます。
- 同じ MAC アドレスと異なる VLAN ID を持つエントリを、バインディングテーブルに追加することはできません。
- 静的バインディングは、以下のように処理されます:
  - 下記の条件のうちの一つが正しい場合、有効な静的 IP ソースガードエントリは、ACL モードの中のバインディングテーブルに追加されます:
    - 同じ VLAN ID および MAC アドレスを持つエントリがない場合は、新しいエントリがタイプ「静的 IP ソースガードバインディング」を使用してバインディングテーブルに追加されます。
    - 同じ VLAN ID および MAC アドレスでエントリがあり、エントリタイプが静的 IP ソースガードバインディングの場合には、新規のエントリが古いエントリと置換されます。
    - 同じ VLAN ID および MAC アドレスでエントリがあり、エントリタイプが動的 DHCP スヌーピングバインディングの場合には、新規のエントリが古いエントリと置換られ、エントリタイプが静的 IP ソースガードバインディングに変更されます。
  - 下記の条件のうちの一つが正しい場合、有効な静的 IP ソースガードエントリは、MAC モードのバインディングテーブルに追加されます:
    - 同じ IP アドレスおよび MAC アドレスでバインディングエントリが無い場合、静的 IP ソースガードバインディングエントリを使用して、新しいエントリがバインディングテーブルに追加されます。
    - 同じ IP アドレスおよび MAC アドレスでエントリがある場合、新規のエントリが古いエントリと置換されます。
  - 静的バインディングには、ユニキャストアドレスのみが受け入れられます。

パラメータ

次のパラメータが表示されます。

Add - ACL テーブルの設定

- Port - 静的エントリがバインドされているポートです。
- VLAN - 設定済み VLAN の ID です（範囲：1 から 4094)
- MAC Address - 有効なユニキャスト MAC アドレスです。
- IP Address - クラス A、B、または C を含む有効なユニキャスト IP アドレスです。

Add - MAC テーブルの設定

- MAC Address - 有効なユニキャスト MAC アドレスです。
- VLAN - 設定済み VLAN または VLAN の範囲の ID です。(範囲: 1 から 4094)
- IP Address - クラス A、B、または C を含む有効なユニキャスト IP アドレスです。
- Port - 静的エントリがバインドされているポートです。物理ポート番号またはポート番号のリストを指定します。非連続ポート番号をコンマで区切り、スペースは入れないでください; ハイフンを使用

してポート番号の範囲を指定することもできます。(範囲: 1 から 10)

Show

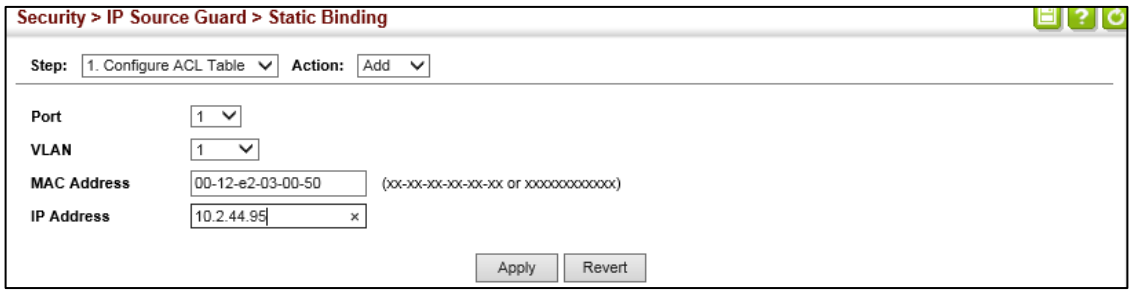
- MAC Address - エントリに関連付けられた物理アドレスです。
- IP Address - クライアントに対応する IP アドレスです。
- VLAN - このエントリがバインドされている VLAN です。
- Interface - このエントリがバインドされているポートです。

Web インタフェース

IP ソースガードの静的バインディングを設定するには：

1. [Security]、[IP Source Guard]、[Static Binding]の順にクリックします。
2. [Step]リストから[Configure ACL Table]または[Configure MAC Table]を選択します。
3. [Action]リストから[Add]を選択します。
4. 各ポートに必要なバインディングを入力します。
5. [Apply]をクリックします。

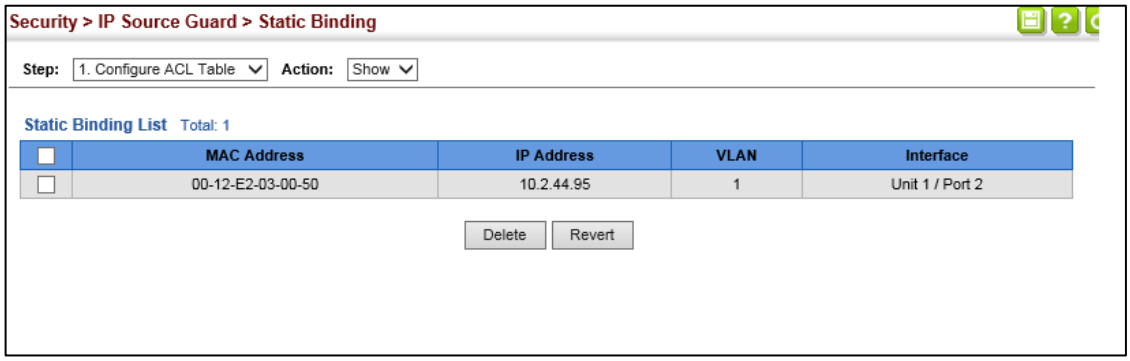
図 11-46　IPv4 ソースガードの静的バインディングの設定



IP ソースガードの静的バインディングを表示するには：

1. [Security]、[IP Source Guard]、[Static Binding]の順にクリックします。
2. [Step]リストから[Configure ACL Table]または[Configure MAC Table]を選択します。
3. [Action]リストから[Show]を選択します。

図 11-47　IPv4 ソースガードの静的バインディングの表示



11.10.3 動的 IPv4 ソースガードバインディングの情報の表示

[Security]> [IP Source Guard]> [Dynamic Binding]ページを使用して、選択したインタフェースのソースガードバインディングテーブルを表示します。

パラメータ

次のパラメータが表示されます。

Query by

- Port - このスイッチのポートです。.
- VLAN - 設定済み VLAN の ID です（範囲：1 から 4094)
- MAC Address - 有効なユニキャスト MAC アドレスです。
- IP Address - クラス A、B、または C を含む有効なユニキャスト IP アドレスです。

Dynamic Binding List

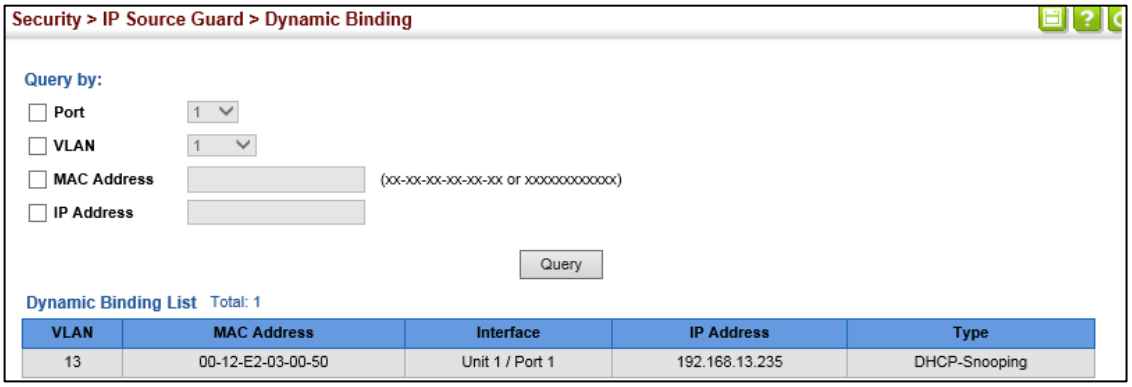
- VLAN - このエントリがバインドされている VLAN です。
- MAC Address - エントリに関連付けられた物理アドレスです。
- Interface - このエントリがバインドされているポートです。
- IP Address - クライアントに対応する IP アドレスです。
- Type - エントリタイプには、DHCP スヌーピングまたは BOOTP スヌーピングが含まれます。

Web インタフェース

IP ソースガードのバインディングテーブルを表示するには：

1. [Security]、[IP Source Guard]、[Dynamic Binding]の順にクリックします。
2. 検索条件にマークを付け、必要な値を入力します。
3. [Query]をクリックします。

図 11-48　IPv4 ソースガードバインディングテーブルの表示



11.11 ARP 検査

ARP 検査は、アドレス解決プロトコルパケットの MAC アドレスバインディングを検証するセキュリティ機能です。特定の“man-in-the-middle”攻撃の基盤となる、無効な MAC-to-IP アドレスバインディングによる ARP トラフィックに対する保護を提供します。これは、すべての ARP 要求と応答を傍受し、ローカル ARP キャッシュが更新されるか、またはパケットが適切な宛先に転送される前に、これらのパケットのそれぞれを検証することによって達成されます。無効な ARP パケットは廃棄されます。

ARP 検査は、信頼できるデータベース（DHCP スヌーピングバインディングデータベース）に格納されている有効な IP-MAC アドレスバインディングにもとづいて ARP パケットの妥当性を判断します。このデータベースは、スイッチ上および必要な VLAN 上でグローバルに有効にされている場合、DHCP スヌーピングによって構築されます。ARP 検査では、静的に設定されたアドレスを持つホストのユーザ設定 ARP アクセス制御リスト（ACL）に対して ARP パケットを検証することもできます。

コマンドの使用方法

ARP 検査の有効化と無効化

- ARP 検査は、グローバルおよび VLAN 単位で制御されます。
- デフォルトでは、ARP 検査はグローバルおよびすべての VLAN で無効になっています。
  - ARP 検査がグローバルに有効にされている場合、有効になっている VLAN 上でのみアクティブになります。
  - ARP 検査がグローバルに有効の場合、検査対応 VLAN 上のすべての ARP 要求パケットとリプライパケットが CPU にリダイレクトされ、ARP 検査エンジンによって処理されます。
  - ARP 検査がグローバルに無効にされている場合、検査が有効にされている VLAN を含むすべての VLAN で非アクティブになります。
  - ARP 検査が無効の場合、すべての ARP 要求および応答パケットは ARP 検査エンジンをバイパスし、そのスイッチング動作は他のすべてのパケットの動作と一致します。
  - グローバル ARP 検査を無効にしてから再度有効にしても、VLAN の ARP 検査設定には影響しません。
  - ARP 検査をグローバルに無効にした場合、個々の VLAN に対して ARP 検査を設定することは可能です。これらの設定変更は、ARP 検査がグローバルに再度有効になった後にのみアクティブになります。

11.11.1 ARP 検査のグローバル設定

[Security]> [ARP Inspection（Configure General）]ページを使用して、スイッチの ARP 検査をグローバルに有効にし、各パケットのアドレス情報を検証し、ロギングを設定します。

コマンドの使用方法

ARP Inspection Validatio

- デフォルトでは、ARP Inspection Validatio は無効になっています。
- 次の検証の少なくとも 1 つを指定すると、ARP Inspection Validatio がグローバルに有効になります。以下のチェックの任意の組み合わせを同時にアクティブにすることができます。
  - Destination MAC - イーサネットヘッダーの宛先 MAC アドレスを ARP 本体のターゲット MAC アドレスと照合します。このチェックは、ARP 応答に対して実行されます。有効にした場合、MAC アドレスの異なるパケットは無効と分類され廃棄されます。

- IP - ARP 本体の無効で予期しない IP アドレスを確認します。これらのアドレスには、0.0.0.0,255.255.255.255、およびすべての IP マルチキャストアドレスが含まれます。送信者 IP アドレスはすべての ARP 要求と応答でチェックされ、ターゲット IP アドレスは ARP 応答でのみチェックされます。
- Source MAC - イーサネットヘッダーの送信元 MAC アドレスを ARP 本体の送信側 MAC アドレスと照合します。このチェックは、ARP 要求と応答の両方で実行されます。有効にした場合、MAC アドレスの異なるパケットは無効と分類され廃棄されます。

ARP 検査ロギング

- デフォルトでは、ARP 検査のロギングはアクティブであり、無効にすることはできません。
- 管理者はログファシリティのレートを設定できます。
- スイッチがパケットをドロップすると、ログバッファにエントリが格納され、レート制御された基準でシステムメッセージが生成されます。システムメッセージが生成された後、エントリはログバッファからクリアされます。
- 各ログエントリには、受信 VLAN、ポート番号、送信元および宛先 IP アドレス、送信元および宛先 MAC アドレスなどのフロー情報が含まれています。
- 複数の同一の無効な ARP パケットが同じ VLAN 上で連続して受信された場合、ロギングファシリティはログバッファに一つのエントリとそれに対応するシステムメッセージのみを生成します。
- ログバッファがいっぱいになると、最も古いエントリが最新のエントリに置換られます。

パラメータ

次のパラメータが表示されます。

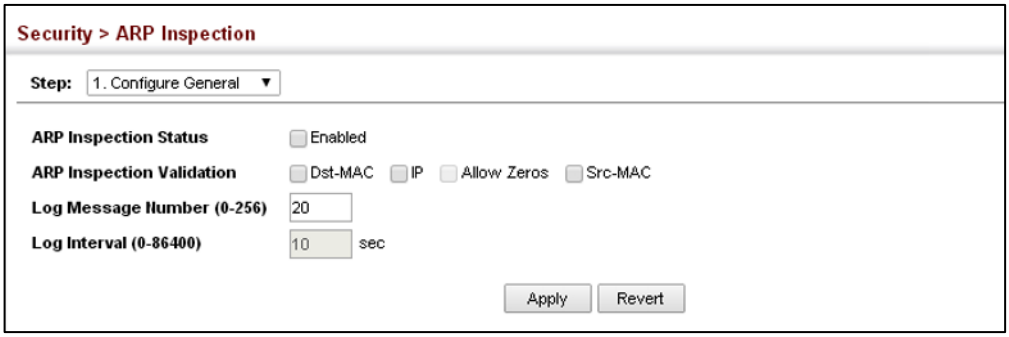
- ARP Inspection Status - ARP 検査をグローバルに有効にします。(デフォルト: Disabled)
- ARP Inspection Validation - 次のいずれかのオプションが有効な場合、拡張 ARP 検査の検証を有効にします。(デフォルト: Disabled)
  - Dst-MAC - イーサネットヘッダーの宛先 MAC アドレスを、ARP 応答の本体のターゲット MAC アドレスと照合して検証します。
  - IP - ARP 本体の無効で予期しない IP アドレスを確認します。送信者 IP アドレスはすべての ARP 要求と応答でチェックされ、ターゲット IP アドレスは ARP 応答でのみチェックされます。
  - Allow Zeros - 送信者の IP アドレスを 0.0.0.0 にすることができます。
  - Src-MAC - イーサネットヘッダーの送信元 MAC アドレスを ARP 本体の送信側 MAC アドレスと照合して検証します。このチェックは、ARP 要求と応答の両方で実行されます。
- Log Message Number - ログメッセージに保存されるエントリの最大数。(範囲: 0-256、デフォルト：20)
- Log Interval - ログメッセージが送信される間隔です。(範囲: 0 から 86400 秒、デフォルト: 10 秒)

Web インタフェース

ARP 検査のグローバルを設定するには：

1. [Security]、[ARP Inspection]をクリックします。
2. [Step]リストから[Configure General]を選択します。
3. ARP 検査をグローバルに有効にし、任意のアドレス検証オプションを有効にし、必要に応じて任意のログパラメータを調整します。
4. [Apply]をクリックします。

図 11-49　ARP 検査のグローバル設定



11.11.2 ARP 検査の VLAN 設定

[Security]> [ARP Inspection（Configure VLAN）]ページを使用して、任意の VLAN の ARP 検査を有効にし、使用する ARP ACL を指定します。

コマンドの使用方法

ARP 検査 VLAN フィルタ（ACL）

- デフォルトでは、ARP 検査 ACL は設定されておらず、機能は無効になっています。
- ARP 検査 ACL は、ARP ACL 設定ページ内で設定されます。
- ARP 検査 ACL は、設定された任意の VLAN に適用できます。
- ARP 検査では、DHCP スヌーピングバインディングデータベースを有効な IP-MAC アドレスバインディングのリストに使用します。ARP ACL が DHCP スヌーピングバインディングデータベースのエントリよりも優先されます。スイッチは、まず ARP パケットと指定された ARP ACL を比較します。
- Static が指定されている場合、ARP パケットは選択された ACL に対してのみ検証されます。一致するルールに従ってパケットがフィルタリングされ、ルールに一致しないパケットは廃棄され、DHCP スヌーピングバインディングデータベースチェックはバイパスされます。
- Static が指定されていない場合、ARP パケットは最初に選択された ACL に対して検証されます。 パケットに一致する ACL ルールがない場合、DHCP スヌーピングバインディングデータベースはその妥当性を判断します。

パラメータ

次のパラメータが表示されます。

- VLAN - VLAN 識別子です。(範囲: 1 から 4094)
- DAI Status - 選択した VLAN の Dynamic ARP Inspection を有効にします。(デフォルト: Disabled)
- ACL Name - 設定済みの任意の ARP ACL を選択できます。(デフォルト: None)
- Static - ARP ACL が選択され、静的モードも選択されている場合、スイッチは ARP 検査を実行し、DHCP スヌーピングバインディングデータベースに対して検証をバイパスします。ARP ACL が選択されていても静的モードが選択されていない場合、スイッチはまず ARP 検査を実行してから、DHCP スヌーピングバインディングデータベースに対して検証を実行します。(デフォルト:　Disabled)

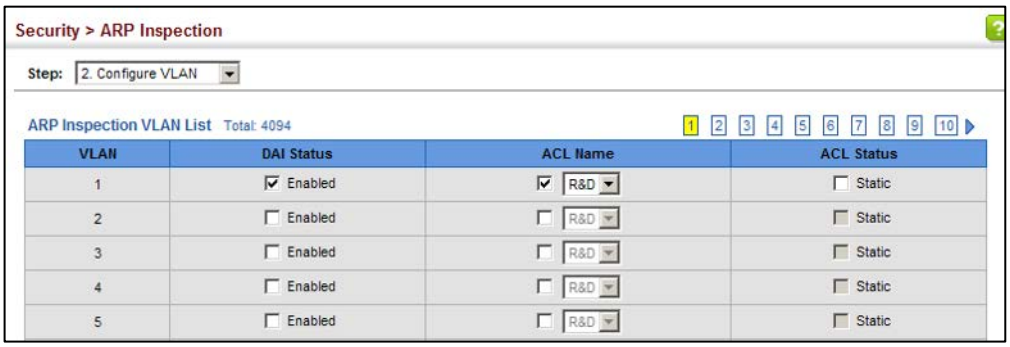
Web インタフェース

ARP 検査のための VLAN を設定するには：

1. [Security]、[ARP Inspection]をクリックします。

2. [Step]リストから[Configure VLAN]を選択します。
3. 必要な VLAN の ARP 検査を有効にし、設定されたアドレスを確認する ARP ACL フィルタを選択し、必要に応じて DHCP スヌーピングバインディングデータベースのチェックをバイパスする Static オプションを選択します。
4. [Apply]をクリックします。

図 11-50　ARP 検査の VLAN 設定



11.11.3 ARP 検査のインタフェース設定

ARP 検査が必要なポートを指定し、パケット検査レートを調整するには、[Security]> [ARP Inspection（Configure Iinterface）]ページを使用します。

パラメータ

次のパラメータが表示されます。

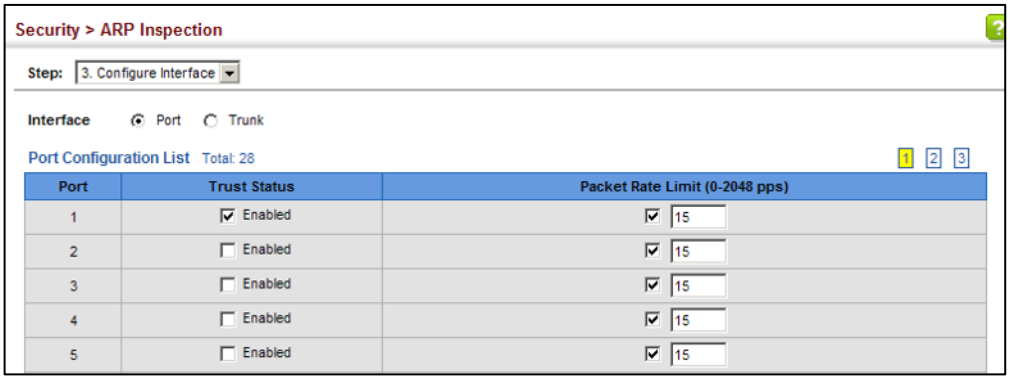
- Interface - ポートまたはトランクの識別子です。
- Trust Status - ポートを信頼できるものまたは信頼できないものとして設定します。(デフォルト: Untrusted)
  デフォルトでは、すべての信頼できないポートは ARP パケットレート制限の対象となり、すべての信頼ポートは ARP パケットレート制限から除外されます。
  信頼できるインタフェースに到着したパケットは、すべての ARP 検査および ARP 検査検証チェックをバイパスし、常に転送されますが、信頼できないインタフェースに到着したパケットは、すべての ARP 検査検査の対象となります。
- Packet Rate Limit - 信頼できるポートまたは信頼できないポートで CPU が処理できる ARP パケットの最大数を 1 秒あたりに設定します。
  (範囲: 0-2048、デフォルト：15)
  レート制限を "0"に設定すると、CPU が処理できる ARP パケットの数に制限がないことを意味します。
  スイッチは、設定された ARP パケット/秒のレート制限を超えるポートで受信されたすべての ARP パケットをドロップします。

Web インタフェース

ARP 検査のためのインタフェースを設定するには：

1. [Security]、[ARP Inspection]をクリックします。
2. [Step]リストから[Configure Interface]を選択します。
3. ARP 検査が必要な信頼できないポートを指定し、パケット検査率を調整します。
4. [Apply]をクリックします。

図 11-51　ARP 検査のインタフェース設定



11.11.4 ARP 検査統計情報の表示

[Security]> [ARP Inspection（Show Information - Show Statistics）]ページを使用して、さまざまな理由で処理された ARP パケット数、またはドロップされた ARP パケット数に関する統計情報を表示します。

パラメータ

次のパラメータが表示されます。

表 11-2　ARP 検査統計

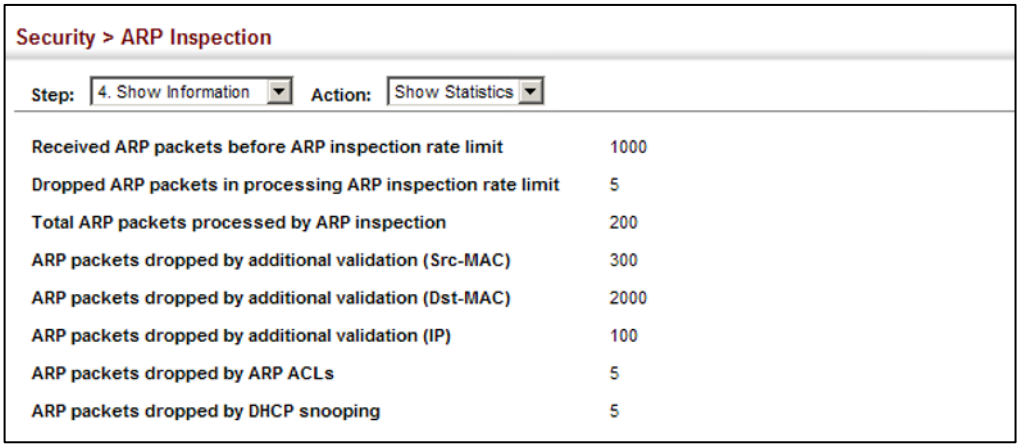
パラメータ	説明
Received ARP packets before ARP inspection rate limit	ARP 検査のレート制限を超えないで受信された ARP パケットの数です。
Dropped ARP packets in the process of ARP inspection rate limit	ARP レート制限を超える（およびドロップした）ARP パケット数です。
ARP packets dropped by additional validation (IP)	IP アドレステストに失敗した ARP パケットの数です。
ARP packets dropped by additional validation (Dst-MAC)	宛先 MAC アドレステストに失敗したパケットの数です。
Total ARP packets processed by ARP inspection	ARP 検査エンジンによって処理されたすべての ARP パケットの数です。
ARP packets dropped by additional validation (Src-MAC)	送信元 MAC アドレステストに失敗したパケットの数です。
ARP packets dropped by ARP ACLs	ARP ACL ルールに対する検証に失敗した ARP パケットの数です。
ARP packets dropped by DHCP snooping	DHCP スヌーピングバインディングデータベースに対する検証に失敗したパケットの数です。

Web インタフェース

ARP 検査の統計情報を表示するには：

1. [Security]、[ARP Inspection]をクリックします。
2. [Step]リストから[Show Information]を選択します。
3. [Action]リストから[Show Statistics]を選択します。

図 11-52　ARP 検査の統計情報の表示



11.11.5 ARP 検査ログの表示

関連する VLAN、ポート、およびアドレスコンポーネントを含め、ログに保存されているエントリに関する情報を表示するには、[Security]> [ARP Inspection（Show Information - Show Log）]ページを使用します。

パラメータ

次のパラメータが表示されます。

表 11-3　ARP 検査ログ

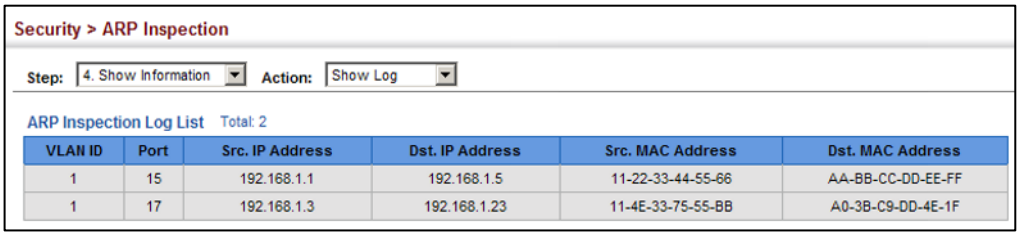
パラメータ	説明
VLAN ID	このパケットが見られた VLAN です。
Port	このパケットが見られたポートです。
Src.IP Address	パケット内の送信元 IP アドレスです。
Dst.IP Address	パケット内の宛先 IP アドレスです。
Src.MAC Address	パケット内の送信元 MAC アドレスです。
Dst.MAC Address	パケット内の宛先 MAC アドレスです。

Web インタフェース

ARP 検査ログを表示するには、次の手順を実行します。

1. [Security]、[ARP Inspection]をクリックします。
2. [Step]リストから[Show Information]を選択します。
3. [Action]リストから[Show Log]を選択します。

図 11-53　ARP 検査ログの表示



12 基本的な管理プロトコル

この章では、以下を含む基本的な管理作業について説明します。

- Event Logging - イベントメッセージをシステムメモリまたはフラッシュメモリにロギングするための条件を設定し、トラップメッセージをリモートログサーバに送信する条件を設定し、SMTP（Simple Mail Transfer Protocol）を使用してリモートホストにトラップレポートを設定します。
- Link Layer Discovery Protocol (LLDP) - ローカルスイッチに関する基本情報の通知、またはローカルブロードキャストドメイン上の隣接デバイスに関する情報の検出を設定します。
- Power over Ethernet※ - 各ポートの優先度と電力バジェットを設定します。
  注※ AXprimoM210-08P
- Simple Network Management Protocol (SNMP) - SNMPv1、SNMPv2c、または SNMPv3 を使用してスイッチ管理を設定します。
- Remote Monitoring (RMON) - SNMP で取得できる詳細な統計またはイベント収集内容を設定します。
- Time Range - 適用される ACL や PoE など、さまざまな機能が適用される時間範囲を設定します。
- Loopback Detection (LBD) - ハードウェアの問題またはプロトコル設定の障害によって引き起こされる一般的なループバック状態を検出します。

12.1 イベントロギングの設定

スイッチを使用すると、スイッチメモリに記録されたイベントのタイプ、リモートシステムログ（syslog）サーバへのロギング、最近のイベントメッセージのリストを含むエラーメッセージのロギングを制御できます。

12.1.1 システムログの設定

[Administration]> [Log]> [System (Configure Global)]ページを使用して、イベントロギングを有効または無効にし、RAM またはフラッシュメモリに記録されるレベルを指定します。

フラッシュメモリに記録される重大なエラーメッセージは、ネットワークの問題のトラブルシューティングを支援するためにスイッチに永続的に格納されます。最大 4096 のログエントリをフラッシュメモリに格納できます。使用可能なログメモリ（256 キロバイト）を超過すると、最も古いエントリが最初に上書きされます。

システムログページでは、フラッシュメモリまたは RAM メモリに記録されたシステムメッセージを設定および制限できます。デフォルトでは、イベントレベル 0～3 はフラッシュに記録され、レベル 0 から 7 は RAM に記録されます。

パラメータ

次のパラメータが表示されます。

- System Log Status - デバッグまたはエラーメッセージのロギングプロセスへのロギングを有効または無効にします。(デフォルト: Enabled)
- Flash Level - スイッチのフラッシュメモリに保存されるログメッセージを、指定されたレベルまでのすべてのレベルで制限します。たとえば、レベル 3 を指定すると、レベル 0 からレベル 3 までのすべてのメッセージがフラッシュされます。(範囲: 0 から 7、デフォルト: 3)

表 12-1 ロギングレベル

レベル	重大度の名称	説明
7	Debug	デバッグメッセージです。
6	Informational	情報メッセージのみです。
5	Notice	コールドスタートなどの正常だが、重要な状態です。
4	Warning	警告状態(例; 不良戻り、予期しない返品など)
3	Error	エラー状態(例; 無効な入力、デフォルトの使用)
2	Critical	重大な状態(例; メモリ割当て、またはフリーメモリエラー - リソースの枯渇)
1	Alert	直ちに対処が必要です。
0	Emergency	システムが使用不可です。

注 現在のファームウェアリリースには、レベル 2、5、および 6 のエラーメッセージしかありません。

- RAM Level - スイッチの一時 RAM メモリに保存されたログメッセージを、指定されたレベルまでのすべてのレベルで制限します。たとえば、レベル 7 を指定すると、レベル 0 からレベル 7 までのすべてのメッセージが RAM に記録されます。(範囲: 0 から 7、デフォルト: 7)

Note: Flash レベルは RAM レベル以下でなければなりません。

Note: すべてのログメッセージは、ウォームリスタート後(例; コマンドインタフェースで電源がリセットされた後)に RAM およびフラッシュに保持されます。

Note: すべてのログメッセージは、コールドリスタート後(例; 電源を切ってから電源を入れた後)、フラッシュメモリに保持され、RAM から消去されます。

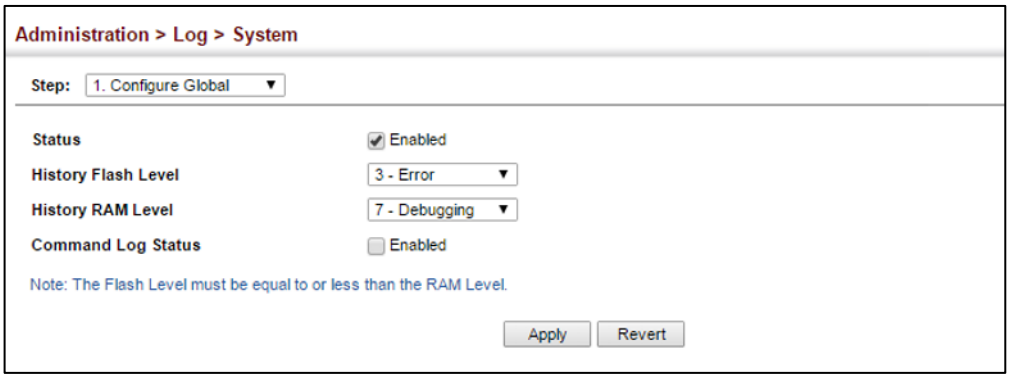
◆ Command Log Status - CLI から実行されたコマンドを記録します。実行時間と、ユーザ名、ユーザインタフェース（コンソールポート、Telnet または SSH）、ユーザ IP アドレスなどの CLI ユーザに関する情報が記録されます。このレコードタイプの重大度は 6 です（ログメッセージを適切なサービスに送信するために syslog サーバが使用する機能を示す番号）。

Web インタフェース

システムメモリへのエラーメッセージのロギングを設定するには：

1. [Administration]、[Log]、[System]をクリックします。
2. [Step]リストから[Configure Global]を選択します。
3. Status を有効または無効にし、フラッシュメモリおよび RAM に記録するイベントメッセージのレベルを設定します。
4. [Apply]をクリックします。

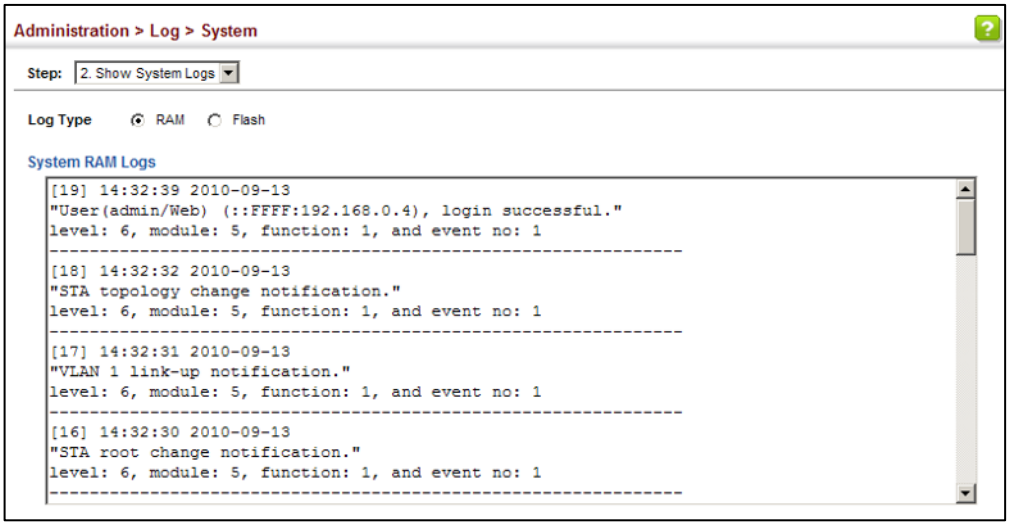
図 12-1　システムメモリログの設定



システムまたはフラッシュメモリに記録されたエラーメッセージを表示:

1. [Administration]、[Log]、[System]をクリックします。
2. [Step]リストから[Show System Logs]を選択します。
3. システムメモリに保存されたログメッセージを表示するには RAM をクリックし、フラッシュメモリに保存されたメッセージを表示するには Flash をクリックします。
   このページでは、記録されたシステムおよびイベントメッセージをスクロールできます。スイッチは、一時的ランダムアクセスメモリ（RAM、すなわち電源リセット時にフラッシュされるメモリ）および永続フラッシュメモリ内の最大 4096 エントリに、2048 までのログエントリを格納することができる。

図 12-2　システムメモリに記録されたエラーメッセージの表示



12.1.2 リモートログの設定

[Administration]> [Log]> [Remote]ページを使用して、ログメッセージを Syslog サーバまたは他の管理端末に送信します。また、送信されるイベントメッセージを指定されたレベル以下のメッセージのみに制限することもできます。

パラメータ

次のパラメータが表示されます。

- Remote Log Status - リモートロギングプロセスへのデバッグメッセージまたはエラーメッセージのロギングを有効または無効にします。(デフォルト: Disabled)
- Logging Facility - syslog メッセージのリモートロギングのファシリティタイプを設定します。16 から 23 の値で指定される 8 種類のファシリティタイプがあります。ファシリティタイプは、ログメッセージを適切なサービスにディスパッチするために syslog サーバによって使用されます。
  この属性は、syslog メッセージで送信されるファシリティタイプタグを指定します（RFC 3164 を参照してください）。このタイプは、スイッチから報告されたメッセージの類には影響を与えません。しかしながら、メッセージをソートしたり、対応するデータベースにメッセージを保管するために使用される可能性があります。(範囲: 16 から 23、デフォルト: 23)
- Logging Trap Level - 指定されたレベルまでのすべてのレベルのリモート syslog サーバに送信されるログメッセージを制限します。たとえば、レベル 3 を指定すると、レベル 0 からレベル 3 までのすべてのメッセージがリモートサーバに送信されます。(範囲: 0 から 7、デフォルト: 7)
- Server IP Address - syslog メッセージを送信するリモートサーバの IPv4 または IPv6 アドレスを指定します。
- Port - リモートサーバが使用する UDP ポート番号を指定します。
  (範囲: 1 から 65535、デフォルト: 514)

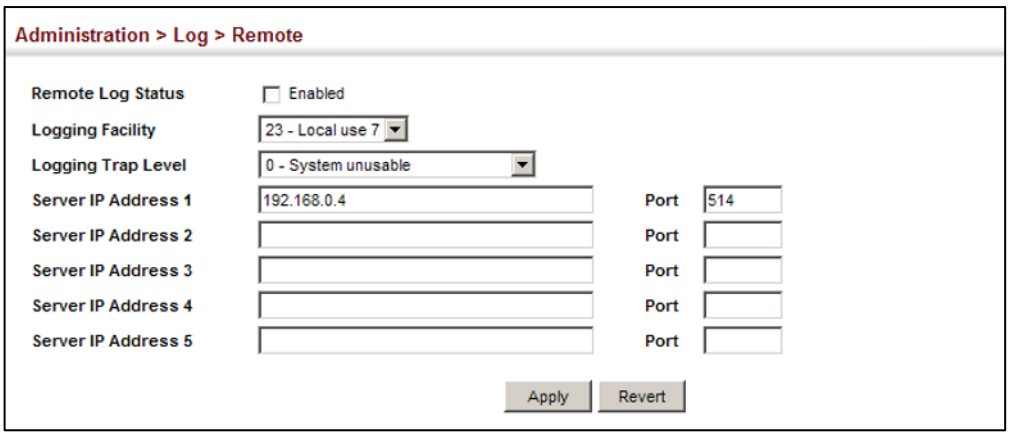
Web インタフェース

リモートサーバへのエラーメッセージの記録を設定するには：

1. [Administration]、[Log]、[Remote]をクリックします。
2. リモートロギングを有効にするには、syslog メッセージに使用するファシリティタイプを指定します。 リモートサーバの IP アドレスを入力します。

3. [Apply]をクリックします。

図 12-3　エラーメッセージのリモートロギングの設定



12.1.3 SMTP アラート送信

[Administration]> [Log]> [SMTP]ページを使用して、指定されたレベルのイベントを記録することによってトリガされたときに SMTP（Simple Mail Transfer Protocol）電子メールメッセージを送信することによってシステム管理者に問題を警告します。メッセージは、ネットワーク上の指定された SMTP サーバに送信され、POP または IMAP クライアントを使用して取得できます。

パラメータ

次のパラメータが表示されます。

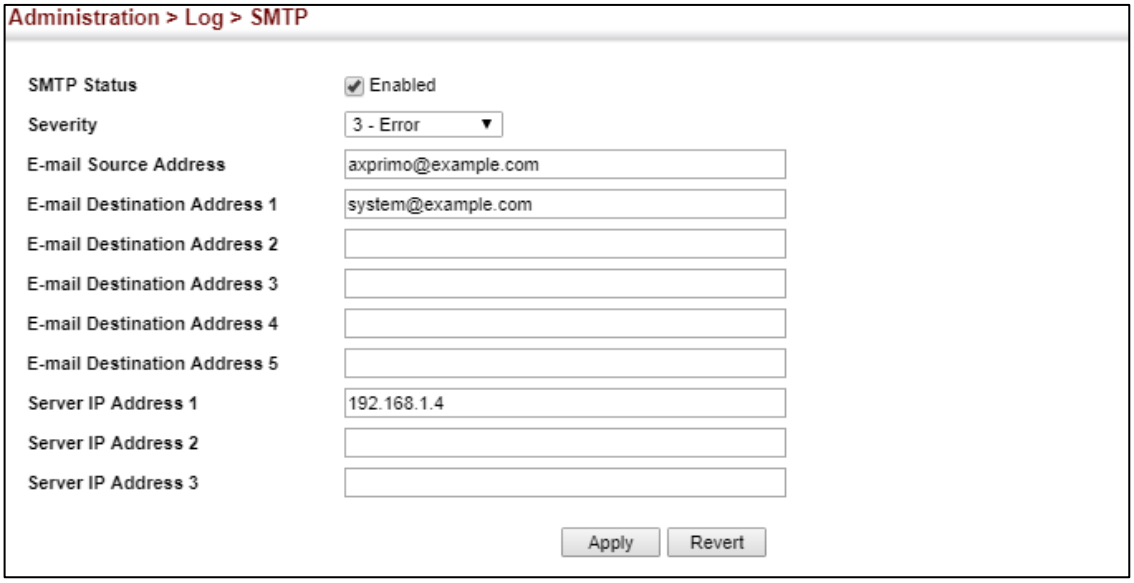
- SMTP Status - SMTP 機能を有効または無効にします。(デフォルト: Enabled)
- Severity - 警告メッセージをトリガするために使用される syslog の重大度閾値レベル(ロギングレベルの表を参照してください)を設定します。このレベル以上のすべてのイベントは、設定された電子メール受信者に送信されます。たとえば、レベル 7 を使用すると、レベル 7 からレベル 0 までのすべてのイベントが報告されます。(デフォルト: Level 7)
- Email Source Address - 警告メッセージの“From”フィールドに使用する電子メールアドレスを設定します。スイッチを識別するシンボリック電子メールアドレス、またはスイッチを担当する管理者のアドレスを使用できます。
  (範囲: 1 から 41 文字)
- Email Destination Address - 警告メッセージの電子メール受信者を指定します。最大 5 人の受信者を指定できます。
- Server IP Address - 最大 3 つの受信者 SMTP サーバの一覧を指定します。IPv4 または IPv6 アドレスを指定することができます。スイッチは、最初のサーバが応答しない場合、リストされたサーバに順番に接続を試みます。

Web インタフェース

SMTP アラートメッセージを設定するには：

1. [Administration]、[Log]、[SMTP]をクリックします。
2. SMTP を有効にし、送信元電子メールアドレスを指定し、最小重大度を選択します。送信元と送信先の電子メールアドレス、および 1 つ以上の SMTP サーバを指定します。
3. [Apply]をクリックします。

図 12-4　SMTP アラートメッセージの設定



12.2 LLDP

LLDP(Link Layer Discovery Protocol)は、ローカルブロードキャストドメイン上の隣接デバイスに関する基本情報を検出するために使用されます。LLDP は、定期的なブロードキャストを使用して送信デバイスに関する情報を広告するレイヤ 2 プロトコルです。広告された情報は、IEEE 802.1AB 規格に準拠した Type Length Value（TLV）形式で表され、デバイスの識別、機能、設定などの詳細を含めることができます。LLDP では、検出された隣接ネットワークノードについて収集された情報を保存および維持する方法も定義します。

Link Layer Discovery Protocol - Media Endpoint Discovery（LLDP-MED）は、Voice over IP 電話やネットワークスイッチなどのエンドポイントデバイスを管理するための LLDP の拡張版です。LLDP-MED TLV は、ネットワークポリシー、電力、およびデバイスの場所の詳細などの情報を通知します。LLDP および LLDP-MED 情報は、トラブルシューティングを簡素化し、ネットワーク管理を強化し、正確なネットワークトポロジを維持するために、SNMP アプリケーションで使用できます。

12.2.1 LLDP タイミング属性の設定

[Administration]> [LLDP (Configure Global)]ページを使用して、スイッチ上で LLDP をグローバルに有効にする、メッセージエージアウト時間を設定する、LLDP MIB の変更に関する一般的な通知やレポートをブロードキャストする頻度を設定するなどの一般機能の属性を設定します。

パラメータ

次のパラメータが表示されます。

- LLDP - スイッチ上で LLDP をグローバルに有効にします。(デフォルト: Enabled)
- Transmission Interval -LLDP 広告の定期的な送信間隔を設定します。(範囲: 5 から 32768 秒; デフォルト：30 秒)
- Hold Time Multiplier - 下の数式に示すように、LLDP 広告で送信される生存時間（TTL）値を設定します。(範囲: 2 から 10; デフォルト：4)
  TTL は、受信側の LLDP エージェントに対して、送信側の LLDP エージェントが適時に更新を送信しない場合に、受信側の LLDP エージェントが送信側の LLDP エージェントに関するすべての情報をどのくらい保持するかの保持時間を示します。
  秒単位の TTL は、次のルールにもとづいています。
  最小値（(Transmission Interval * Hold Time Multiplier)、または 65535）
  したがって、デフォルトの TTL は 30 * 4 = 120 秒です。
- Delay Interval - ローカル LLDP MIB 変数の変更によって開始された通知の連続送信間に遅延を設定します。(範囲: 1 から 8192 秒、デフォルト: 2 秒)
  送信遅延は、ローカル LLDP MIB オブジェクトの短期間の急激な変化中に一連の連続する LLDP 送信を防止し、単一の変更ではなく複数の変更が各送信で報告される確率を高めるために使用されます。
  この属性は、以下の条件を遵守しなければなりません。
  （4 * Delay Interval） ≦ Transmission Interval
- Reinitialization Delay - LLDP ポートが無効またはリンクがダウンしたあとで、再初期化を試行する前に遅延を設定します。(範囲: 1 から 10 秒、デフォルト: 2 秒)
  ポートで LLDP が再初期化される際、このポートに関連するリモートシステム LLDP MIB の中の情報は削除されます。
- Notification Interval - LLDP MIB の変更に関する SNMP 通知を送信する間隔を設定します。(範囲: 5 から 3600 秒; デフォルト: 5 秒)
  このパラメータは、ネットワーク監視または管理のために LLDP MIB に格納されたデータを使用する

SNMP アプリケーションにのみ適用されます。
SNMP 通知間で発生する LLDP 隣接の変更に関する情報は送信されません。通知時に存在した状態変更のみが送信に含まれます。したがって SNMP エージェントは、lldpStatsRemTableLastChangeTime の値を定期的にチェックして、伝送損失などのために lldpRemTablesChange 通知イベントが検知されなかったことを検出する必要があります。

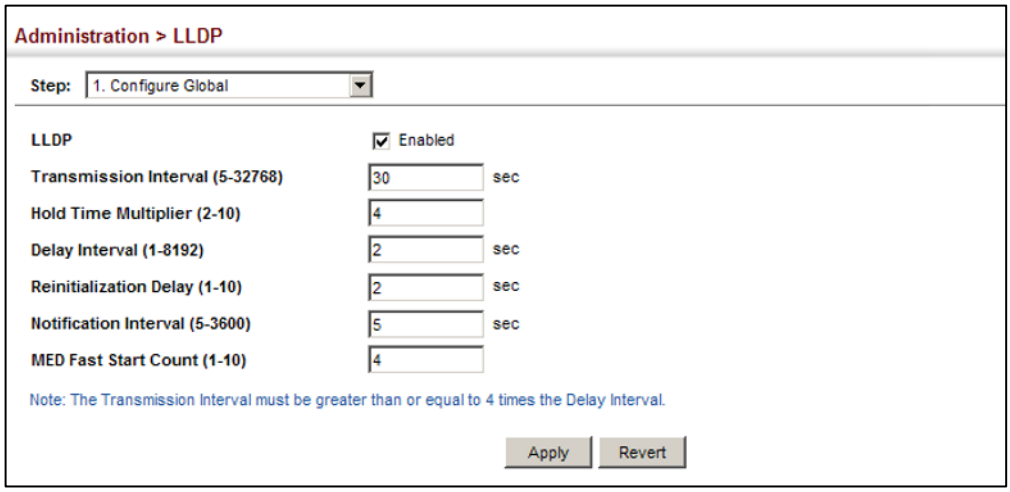
- MED Fast Start Count - LLDP-MED Fast Start メカニズムのアクティブ化プロセス中に送信する LLDP MED ファーストスタート LLDPDU の量を設定します。(範囲: 1 から 10 パケット、デフォルト：4 パケット)
  MED ファーストスタートカウントパラメータは、LLDP-MED ファストスタートメカニズムがポートでアクティブになっていることを確認するタイマーの一部です。LLDP-MED ファーストスタートは、LLDP のタイムリーな起動にとって非常に重要であり、緊急コールサービスの迅速な可用性に不可欠です。

Web インタフェース

LLDP タイミング属性を設定するには：

1. [Administration]、[LLDP]をクリックします。
2. [Step]リストから[Configure Global]を選択します。
3. LLDP を有効にし、必要に応じてタイミングパラメータのいずれかを変更します。
4. [Apply]をクリックします。

図 12-5　LLDP タイミング属性の設定



12.2.2 LLDP インタフェース属性の設定

[Administration]> [LLDP (Configure Interface - Configure General)]ページを使用して、メッセージの送信、受信、または送受信の有無、SNMP 通知の送信の有無、および通知される情報の種類など、個々のインタフェースのメッセージ属性を指定します。

パラメータ

次のパラメータが表示されます。

- Admin Status - LLDP プロトコルデータユニットの LLDP メッセージ送受信モードを有効にします。(オプション: Tx only, Rx only, TxRx, Disabled; デフォルト TxRx)
- SNMP Notification - LLDP および LLDP-MED の変更に関する SNMP トラップ通知の送信を有効にします。(デフォルト: Enabled)

このオプションは、Notification Interval で指定された間隔で、指定されたターゲット端末に SNMP トラップ通知を送信します。トラップ通知には、LLDP MIB（IEEE 802.1AB）、LLDP-MED MIB（ANSI / TIA-1057）、またはベンダ固有の LLDP-EXT-DOT1 および LLDP-EXT-DOT3 MIB の状態変化に関する情報が含まれます。
SNMP トラップ宛先の定義については、「12.4.9　トラップマネージャーの設定」を参照してください。
SNMP 通知間で発生する LLDP 隣接追加の変更に関する情報は送信されません。トラップ通知の時点で存在する状態変化のみが送信に含まれます。したがって SNMP エージェントは、lldpStatsRemTableLastChangeTime の値を定期的にチェックして、伝送損失などのために lldpRemTablesChange 通知イベントが検知されなかったことを検出する必要があります。

- MED Notification - LLDP-MED の変更に関する SNMP トラップ通知の送信を有効にします。(デフォルト: Disabled)
- Basic Optional TLVs - 通知されたメッセージの TLV フィールドに含まれる基本情報を設定します。
  - Management Address - 管理アドレス・プロトコル・パケットは、スイッチの IPv4 アドレスを含んでいます。管理アドレスを設定していない場合には、アドレスは CPU、またはこの通知を送信するポートの MAC アドレスが入ります。(デフォルト: Enabled)
  - Port Description - ポートの説明は RFC 2863 の ifDescr オブジェクトで取得できる情報が入ります。このオブジェクトには、製造元、製品名、およびインタフェースハードウェア/ソフトウェアのバージョンに関する情報が含まれています。(デフォルト: Enabled)
  - System Capabilities - システム機能は、システムの主要な機能と、これらの主要な機能が有効かどうかを識別します。この TLV によって通達される情報は、IEEE 802.1AB に記載されています。(デフォルト: Enabled)
  - System Description - システムの説明は、RFC 3418 の sysDescr オブジェクトで取得できる情報が入ります。このオブジェクトには、システムのハードウェアタイプ、ソフトウェアオペレーティングシステム、およびネットワーキングソフトウェアのフルネームとバージョン ID が含まれています。(デフォルト: Enabled)
  - System Name - システム名は、システムの管理上割当てられた名前を含む RFC 3418 の sysName オブジェクトで取得できる情報が入ります。システム名を設定するには、「3.1　システム情報の表示」を参照してください。(デフォルト: Enabled)
- 802.1 Organizationally Specific TLVs - 通知されたメッセージの TLV フィールドに含まれる IEEE 802.1 情報を設定します。
  - Protocol Identity -このインタフェースを通じてアクセス可能なプロトコルです。(デフォルト: Enabled)
  - VLAN ID - ポートのデフォルト VLAN 識別子（PVID）は、タグなしフレームまたは優先タグ付きフレームが関連付けられている VLAN を示します（「5.1　IEEE 802.1Q VLANs」を参照してください）。(デフォルト: Enabled)
  - VLAN Name - このインタフェースが割当てられているすべての VLAN の名前です。(デフォルト: Enabled)
  - Port and Protocol VLAN ID - このインタフェース上で設定されたポートベースのプロトコル VLAN です（「5.3　プロトコル VLAN」を参照してください）。(デフォルト: Enabled)
- 802.3 Organizationally Specific TLVs - 通知されたメッセージの TLV フィールドに含まれる IEEE 802.3 情報を設定します。
  - Link Aggregation - リンク集約機能、リンクの集約ステータス、およびこのインタフェースが現在リンク集約メンバーである場合の IEEE 802.3 集約ポート ID です。(デフォルト: Enabled)
  - Max Frame Size - 最大フレームサイズです。このスイッチの最大フレームサイズの設定について

は、「3.3　ジャンボフレームの設定」を参照してください。(デフォルト: Enabled)

- MAC/PHY Configuration/Status - 自動ネゴシエーションのサポート/機能、および動作可能な Multistation Access Unit（MAU;マルチ端末アクセスユニット）タイプに関する情報を含む MAC / PHY の設定とステータスです。(デフォルト: Enabled)
- PoE※ -Power-over-Ethernet 機能、PoE がサポートされているかどうか、現在有効されているかどうかなど、電力が供給されるポートピン、電力を供給するように選択されたポートピン、および電力クラスが含まれます。(デフォルト: Enabled)
  注※ AXprimoM210-08P

◆ MED TLVs - 通知されたメッセージの MED TLV フィールドに含まれる一般情報を設定します。

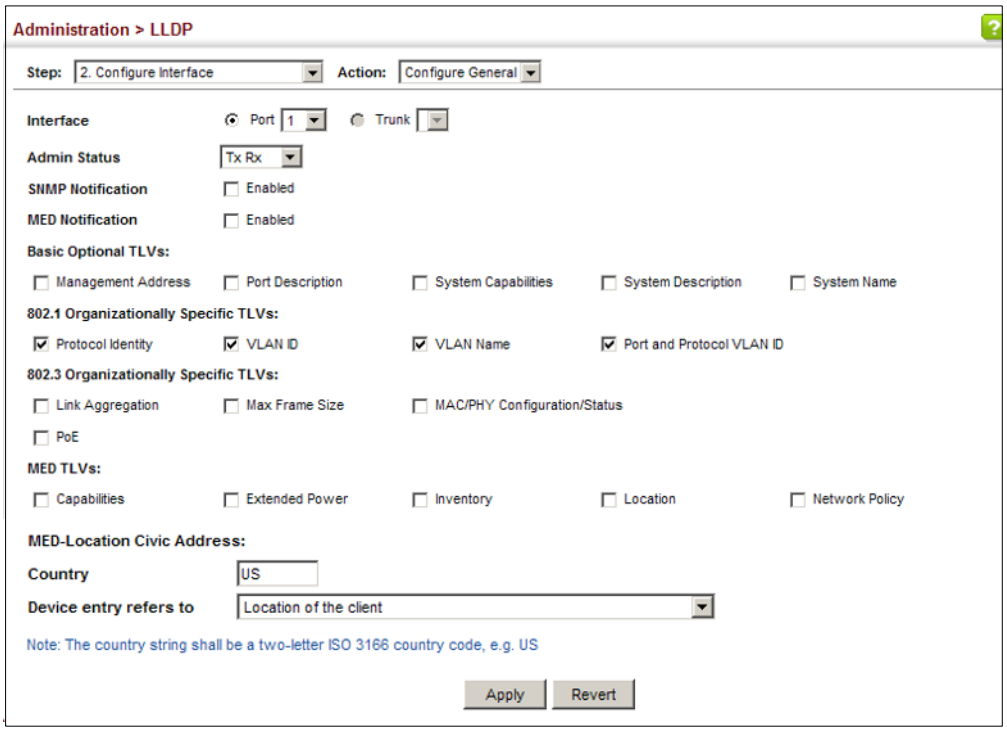
- Capabilities - このオプションは、LLDP-MED TLV 機能を通知し、メディアエンドポイントおよび接続デバイスがスイッチ上でサポートされている LLDP-MED 関連 TLV を効率的に検出できるようにします。(デフォルト: Enabled)
- Extended Power - このオプションは、スイッチからの電力の可用性や、スイッチがプライマリまたはバックアップ電源から動作しているかどうかなど、スイッチの電源状態など、拡張された Power-over-Ethernet 機能の詳細を通知します。（エンドポイントデバイスは、この情報を使用して省電力モードに入ることを決定することができる）。(デフォルト: Enabled)
- Inventory - このオプションは、製造元、モデル、ソフトウェアのバージョン、その他の関連情報など、在庫管理に役立つデバイスの詳細を通知します。(デフォルト: Enabled)
- Location - このオプションは、ロケーション識別の詳細を通知します。(デフォルト: Enabled)
- Network Policy - このオプションは、ポート上の VLAN 構成の不一致の検出と診断を支援するネットワークポリシー構成情報を通知します。不適切なネットワークポリシー設定は、しばしば音声品質の低下または完全なサービスの中断を招きます。(デフォルト: Enabled)

Web インタフェース

LLDP インタフェースの属性を設定するには：

1. [Administration]、[LLDP]をクリックします。
2. [Step]リストから[Configure Interface]を選択します。
3. [Action]リストから[Configure General]を選択します。
4. [Port]または[Trunk]リストからインタフェースを選択します。
5. LLDP 送受信モードを設定し、SNMP トラップメッセージを送信するかどうかを指定し、LLDP メッセージで通知する情報を選択します。
6. [Apply]をクリックします。

図 12-6　LLDP インタフェース属性の設定



12.2.3 LLDP ローカルデバイス情報の表示

[Administration]> [LLDP (Show Local Device Information)]ページを使用して、MAC アドレス、シャーシ ID、管理 IP アドレス、およびポート情報など、スイッチに関する情報を表示します。

パラメータ

次のパラメータが表示されます。

一般設定

◆ Chassis Type - 送信側 LLDP エージェントに関連付けられた IEEE 802 LAN エンティティを含むシャーシを識別します。シャーシが識別され、シャーシ ID フィールドによって参照されるコンポーネントのタイプを示すためにシャーシ ID サブタイプが使用されるいくつかの方法があります。

表 12-2　シャーシ ID サブタイプ

ID ベース	参照
Chassis component	EntPhysClass の値が 'chassis（3）'（IETF RFC 2737）の場合の EntPhysicalAlias
Interface alias	IfAlias（IETF RFC 2863）
Port component	entPhysicalClass の値が 'port（10）'または 'backplane（4）'の場合の EntPhysicalAlias（IETF RFC 2737）
MAC address	MAC アドレス（IEEE 標準 802-2001）
Network address	ネットワークアドレス
Interface name	ifName（IETF RFC 2863）
Locally assigned	ローカルに割当て

◆ Chassis ID - このシステム内の特定のシャーシの特定の識別子を示すオクテット文字列です。

◆ System Name - システムの管理上割当てられた名前を示す文字列です（「3.1　システム情報の表示」を参照してください）。

- System Description - ネットワークエンティティのテキスト記述です。このフィールドは、show system コマンドでも表示されます。
- System Capabilities Supported - システムの主要な機能を定義する機能です。

表 12-3　システム機能

ID ベース	参照
Other	–
Repeater	IETF RFC 2108
bridge	IETF RFC 2674
WLAN Access Point	IEEE 802.11 MIB
Router	IETF RFC 1812
Telephone	IETF RFC 2011
DOCSIS cable device	IETF RFC 2669 and IETF RFC 2670
End Station Only	IETF RFC 2011

- System Capabilities Enabled - 現在有効になっているシステムの主な機能です。上記の表を参照してください。
- Management Address - ローカルシステムに関連付けられた管理アドレスです。管理アドレスを設定していない場合には、アドレスは CPU、またはこの通知を送信するポートの MAC アドレスが入ります。

インタフェース設定

次の属性は、ポートとトランクの両方のインタフェースタイプに適用されます。トランクがリストされている場合、説明はトランクの最初のポートに適用されます。

- Port/Trunk Description - ポートまたはトランクの説明を示す文字列です。RFC 2863 が実装されている場合は、このフィールドに ifDescr オブジェクトで取得できる情報を使用する必要があります。
- Port/Trunk ID - この LLDPDU が送信されたポートまたはトランクの特定の識別子を含む文字列です。

インタフェースの詳細

次の属性は、ポートとトランクの両方のインタフェースタイプに適用されます。トランクがリストされている場合、説明はトランクの最初のポートに適用されます。

- Local Port/Trunk - このスイッチのローカルインタフェース
- Port/Trunk ID Type - ポートを特定する方法はいくつかあります。Port ID TLV でポートがどのように参照されているかを示すために、Port ID サブタイプが使用されます。

表 12-4　Port ID サブタイプ

ID ベース	参照
Interface alias	IfAlias（IETF RFC 2863）
Chassis component	EntPhysClass の値が 'chassis（3）'（IETF RFC 2737）の場合の EntPhysicalAlias
Port component	entPhysicalClass の値が 'port（10）'または 'backplane（4）'の場合の EntPhysicalAlias（IETF RFC 2737）
MAC address	MAC アドレス（IEEE 標準 802-2001）
Network address	ネットワークアドレス
Interface name	ifName（IETF RFC 2863）
Agent circuit ID	エージェント回線 ID（IETF RFC 3046）
Locally assigned	ローカルに割当て

- Port/Trunk ID - このスイッチで使用されるインタフェースのサブタイプにもとづいて、ローカルイン

タフェースの特定の識別子を含む文字列です。

- Port/Trunk Description - ポートまたはトランクの説明を示す文字列です。RFC 2863 が実装されている場合は、このフィールドに ifDescr オブジェクトを使用する必要があります。
- MED Capability - インタフェースの主要な機能を定義する、サポートされている一連の機能です
  - LLDP-MED Capabilities
  - Network Policy
  - Location Identification
  - Extended Power via MDI - PSE
  - Extended Power via MDI - PD
  - Inventory

Web インタフェース

ローカルデバイスの LLDP 情報を表示するには：

1. [Administration]、[LLDP]をクリックします。
2. [Step]リストから[Show Local Device Information]を選択します。
3. [General]、[Port]、[Port Details]、[Trunk]、または[Trunk Details]を選択します。

図 12-7　LLDP のローカルデバイス情報の表示 (一般)

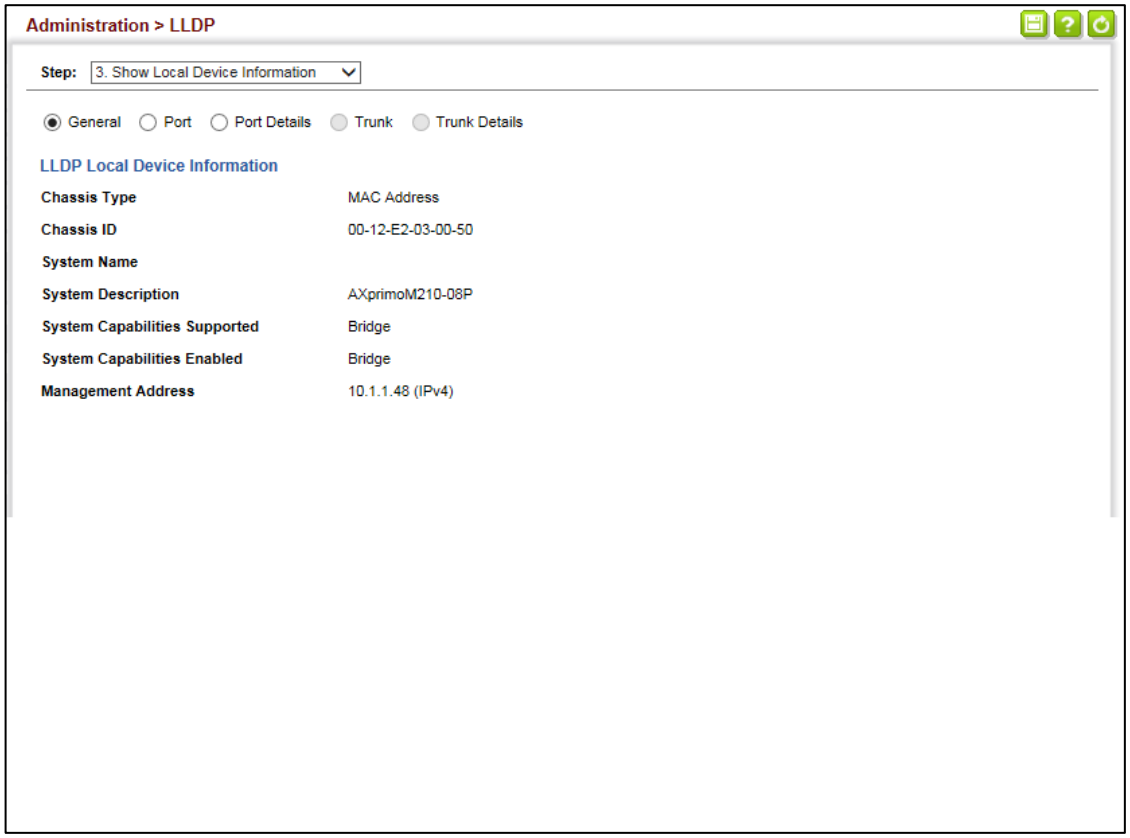


図 12-8　LLDP のローカルデバイス情報の表示 (ポート:)

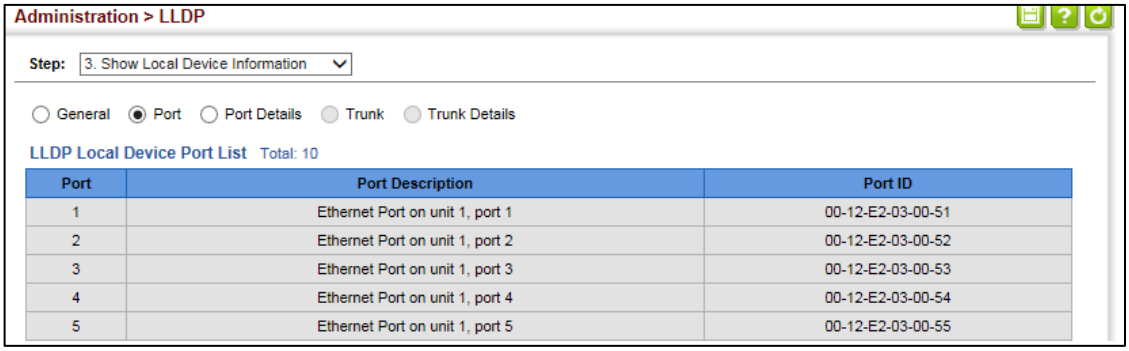
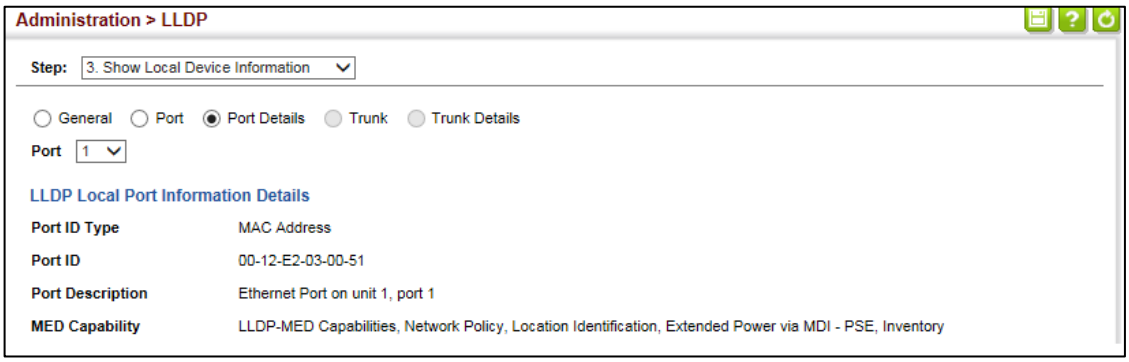


図 12-9　LLDP のローカルデバイス情報の表示 (ポートの詳細)



12.2.4 LLDP リモートデバイス情報の表示

[Administration]> [LLDP (Show Remote Device Information)]ページを使用して、スイッチのポートに直接接続されている LLDP、またはローカルスイッチ上の特定のポートに接続されている LLDP 対応デバイスに関する詳細情報を表示できます。

パラメータ

次のパラメータが表示されます。

ポート

- Local Port - リモート LLDP 対応デバイスが接続されているローカルポートです。
- Chassis ID - このシステム内の特定のシャーシの特定の識別子を示すオクテット文字列です。
- Port ID - この LLDPDU が送信されたポートの特定の識別子を含む文字列です。
- System Name - システムに管理上割当てられた名前を示す文字列です。

ポートの詳細

- Port - ローカルスイッチ上のポート識別子です。
- Remote Index - このポートに接続されているリモートデバイスのインデックスです。
- Chassis Type - 送信側 LLDP エージェントに関連付けられた IEEE 802 LAN エンティティを含むシャーシを識別します。シャーシが識別され、シャーシ ID フィールドによって参照されるコンポーネントのタイプを示すためにシャーシ ID サブタイプが使用されるいくつかの方法があります。(「表 12-3 シャーシ ID サブタイプ」を参照してください)
- Chassis ID - このシステム内の特定のシャーシの特定の識別子を示すオクテット文字列です。
- Port ID Type - [Port ID]フィールドにリストされている識別子のベースを示します。「表 12-5　Port ID

サブタイプ」を参照してください。

- Port ID - この LLDPDU が送信されたポートの特定の識別子を含む文字列です。
- Port Description - ポートの説明を示す文字列です。RFC 2863 が実装されている場合は、このフィールドに ifDescr オブジェクトを使用する必要があります。
- System Name - システムに割当てられた名前を示す文字列です。
- System Description - ネットワークエンティティのテキスト記述です。
- System Capabilities Supported - システムの主要な機能を定義する機能です。(「表 12-4　システム機能」を参照してください。)
- System Capabilities Enabled - 現在有効になっているシステムの主な機能です。
- Management Address List - このデバイスの管理アドレスです。
  管理アドレスが設定されていない場合には、アドレスは CPU、またはこの通知を送信するポートの MAC アドレスが入ります。

ポートの詳細 - 802.1 拡張情報

- Remote Port VID - ポートのデフォルト VLAN 識別子（PVID）は、タグなしフレームまたは優先タグ付きフレームが関連付けられている VLAN を示します。
- Remote Port-Protocol VLAN List - このインタフェースで設定されたポートベースのプロトコル VLAN、指定されたポートがポートベースのプロトコル VLAN（リモートシステムに関連付けられている）をサポートしているかどうか、およびポートベースのプロトコル VLAN がリモートシステムに関連付けられている特定のポートで有効になっているかどうかを確認します。
- Remote VLAN Name List - ポートに関連付けられた VLAN 名です。
- Remote Protocol Identity List - ポートを通じてアクセス可能な特定のプロトコルに関する情報です。このオブジェクトは、このエージェントが特定のプロトコル ID を識別するために使用する任意のローカル整数値、およびリモートシステムのポートに関連付けられたプロトコルを識別するために使用されるオクテット文字列を表します。

ポートの詳細 - 802.3 拡張ポート情報

- Remote Port Auto-Neg Supported - 指定されたポート（リモートシステムに関連付けられている）が自動ネゴシエーションをサポートしているかどうかを示します。
- Remote Port Auto-Neg Adv-Capability - リモートシステムのポートに関連付けられている ifMauAutoNegCapAdvertisedBits オブジェクト（IETF RFC 3636 で定義）の値（ビットマップ）です。

表 12-5　リモートポート自動ネゴシエーションで通知された機能

ビット	機能
0	その他または不明
1	10BASE-T 半二重モード
2	10BASE-T 全二重モード
3	100BASE-T4
4	100BASE-TX 半二重モード
5	100BASE-TX 全二重モード
6	100BASE-T2 半二重モード
7	100BASE-T2 全二重モード
8	全二重リンクの PAUSE
9	全二重リンクの非対称 PAUSE
10	全二重リンクの対称 PAUSE

ビット	機能
11	全二重リンクの非対称および対称 PAUSE
12	1000BASE-X、-LX、-SX、-CX 半二重モード
13	1000BASE-X、-LX、-SX、-CX 全二重モード
14	1000BASE-T 半二重モード
15	1000BASE-T 全二重モード

- Remote Port Auto-Neg Status - ポート自動ネゴシエーションがリモートシステムに関連付けられたポートで有効になっているかどうかを示します。
- Remote Port MAU Type - 送信デバイスの動作可能な MAU タイプを示す整数値です。このオブジェクトには、IETF RFC 3636 にリストされている対応する dot3MauType のリスト位置から派生した整数値が含まれ、それぞれの dot3MauType OID の最後の数値と等しくなります。

ポートの詳細 - 802.3 拡張電源情報

- Remote Power Class - リモートシステム（PSE - Power Sourcing Equipment または PD Powered Device）に関連付けられたポートのポートクラスです。
- Remote Power MDI Status - リモートシステムに関連付けられた特定のポートで MDI 電源が有効になっているかどうかを示します。
- Remote Power Pairs - “Signal”は信号ペアのみが使用中であることを意味し、“Spare”はスペアペアのみが使用中であることを意味する。
- Remote Power MDI Supported - リモートシステムに関連付けられた特定のポートで MDI 電源がサポートされているかどうかを示します。
- Remote Power Pair Controllable - リモートシステムに関連付けられている特定のポートで電源を供給するためにペア選択を制御できるかどうかを示します。
- Remote Power Classification - この分類は、消費電力に従って、PoE ネットワーク上の異なる端末にタグを付けるために使用されます。IP 電話、WLAN アクセスポイントなどのデバイスは、電力要件に従って分類されます。

ポートの詳細 - 802.3 内線トランク情報

- Remote Link Aggregation Capable - リモートポートがリンク集約状態にないか、リンク集約をサポートしていないかどうかを示します。
- Remote Link Aggregation Status - リンクの現在の集約状態です。
- Remote Link Port ID - このオブジェクトには、リモートシステムに関連付けられたポートコンポーネントの ifIndex の ifNumber から派生した IEEE 802.3 集約ポート識別子 aAggPortID（IEEE 802.3-2002,30.7.2.1.1）が含まれています。リモートポートがリンク集約状態にない場合、またはリンク集約をサポートしていない場合、この値はゼロにする必要があります。

ポートの詳細 - 802.3 拡張フレーム情報

- Remote Max Frame Size - リモートシステムに関連付けられたポートコンポーネントのオクテット単位でサポートされている最大フレームサイズを示す整数値です。

Web インタフェース

リモートポートの LLDP 情報を表示するには、次の手順を実行します。

1. [Administration]、[LLDP]をクリックします。
2. [Step]リストから[Show Remote Device Information]を選択します。
3. [Port]、[Port Details]、[Trunk]、または[Trunk Details]を選択します。

4. 次のページが開いたら、このスイッチのポートとこのポートに接続されているリモートデバイスのインデックスを選択します。
5. [Query]をクリックします。

図 12-10　LLDP のリモートデバイス情報の表示 (ポート)

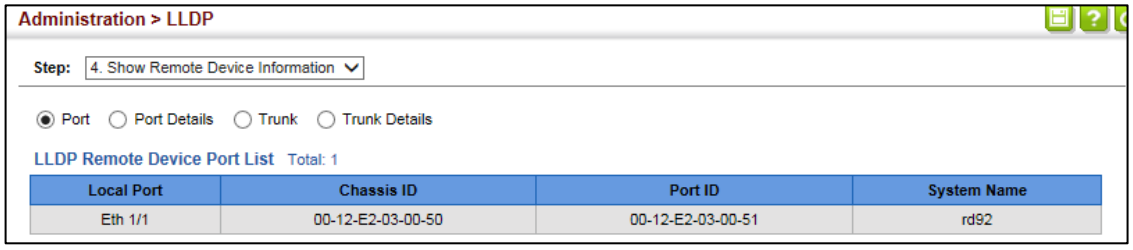
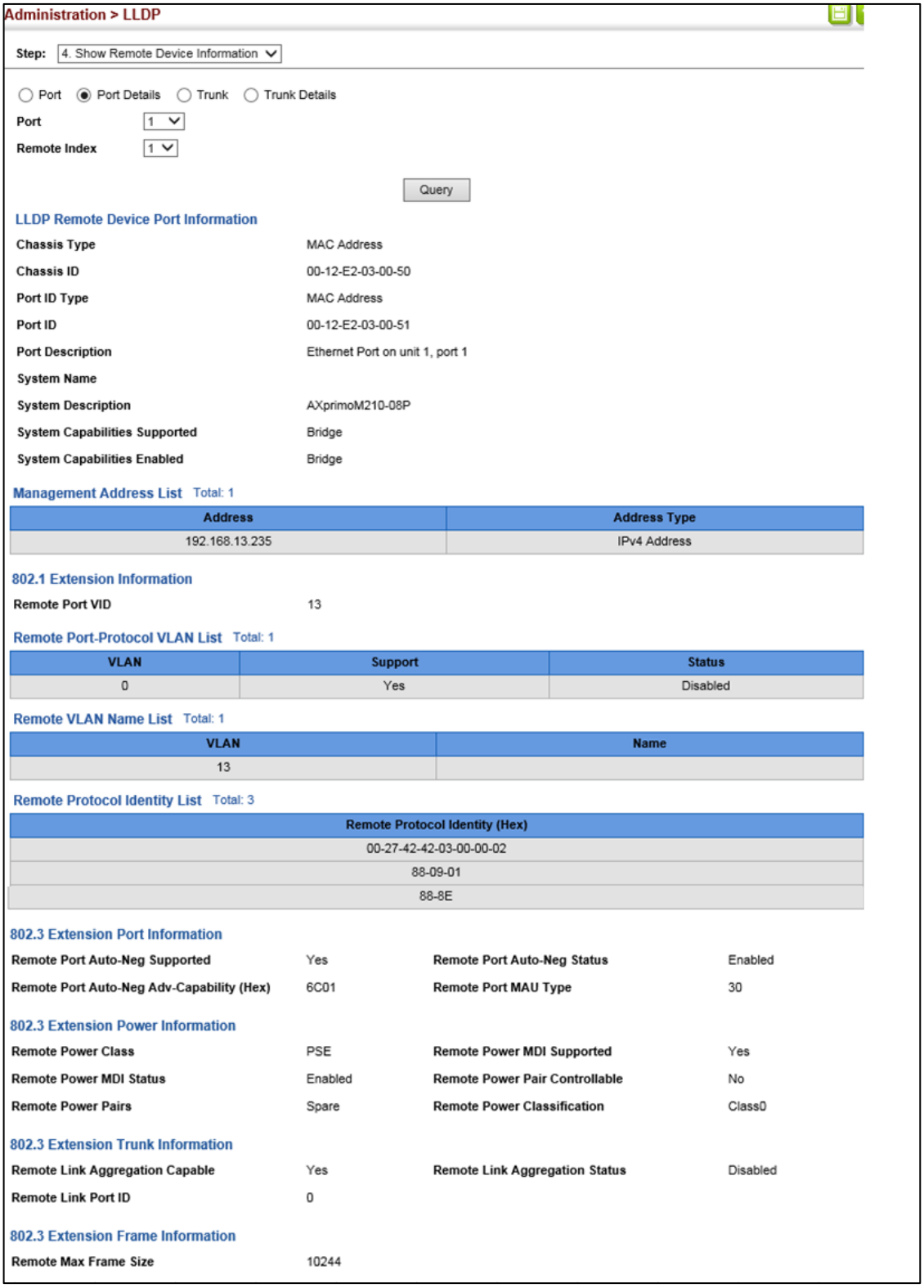


図 12-11　LLDP のリモートデバイス情報の表示 (ポート詳細)



12.2.5 デバイス統計情報の表示

[Administration]> [LLDP (Show Device Statistics)]ページを使用して、スイッチに接続された LLDP 対応デバイスの統計情報、およびすべてのローカルインタフェースで送受信された LLDP プロトコルメッセージの統計情報を表示します。

パラメータ

次のパラメータが表示されます。

リモートデバイスの一般的な統計

- Neighbor Entries List Last Updated - LLDP ネイバーエントリリストが最後に更新された時刻です。
- New Neighbor Entries Count - リモート TTL がまだ期限切れになっていない LLDP ネイバーの数です。
- Neighbor Entries Deleted Count - 何らかの理由で LLDP リモートシステム MIB から削除された LLDP ネイバーの数です。
- Neighbor Entries Dropped Count - 不十分なリソースのために、このスイッチのリモートデータベースが LLDPDU を削除した回数です。
- Neighbor Entries Age-out Count - リモート TTL タイマーが期限切れになっているため、ネイバーの情報が LLDP リモートシステム MIB から削除された回数です。

ポート/トランク

- Frames Discarded - 一般的な検証ルールおよび特定の TLV に対して定義された特定の使用ルールに準拠していないために破棄されたフレームの数です。
- Frames Invalid - 1 つまたは複数の検出可能なエラーで受信されたすべての LLDPDU の数回数です。
- Frames Received -受信した LLDP PDU の数回数です。
- Frames Sent - 送信された LLDP PDU の数回数です。
- TLVs Unrecognized - 受信側 LLDP ローカルエージェントによって認識されないすべての TLV の数回数です。
- TLVs Discarded - 不十分なメモリ容量、シーケンス属性の欠落、またはその他の理由により、受信されて破棄されたすべての LLDPDU の数回数です。
- Neighbor Ageouts - リモート TTL タイマーが期限切れになっているため、ネイバーの情報が LLDP リモートシステム MIB から削除された回数回数です。

Web インタフェース

スイッチに接続された LLDP 対応デバイスの統計情報を表示するには、次の手順を実行します。

1. [Administration]、[LLDP]をクリックします。
2. [Step]リストから[Show Device Statistics]を選択します。
3. [General]、[Port]、または[Trunk]を選択します。

図 12-12　LLDP デバイス統計情報の表示 （一般）

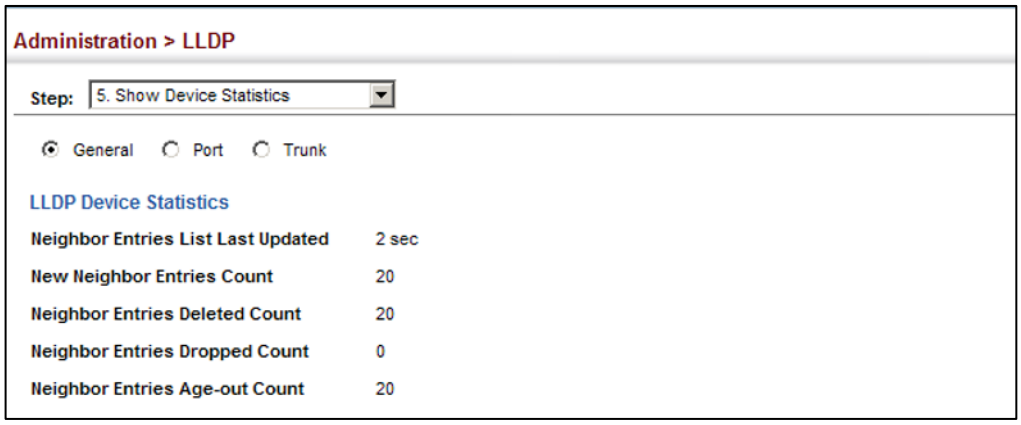
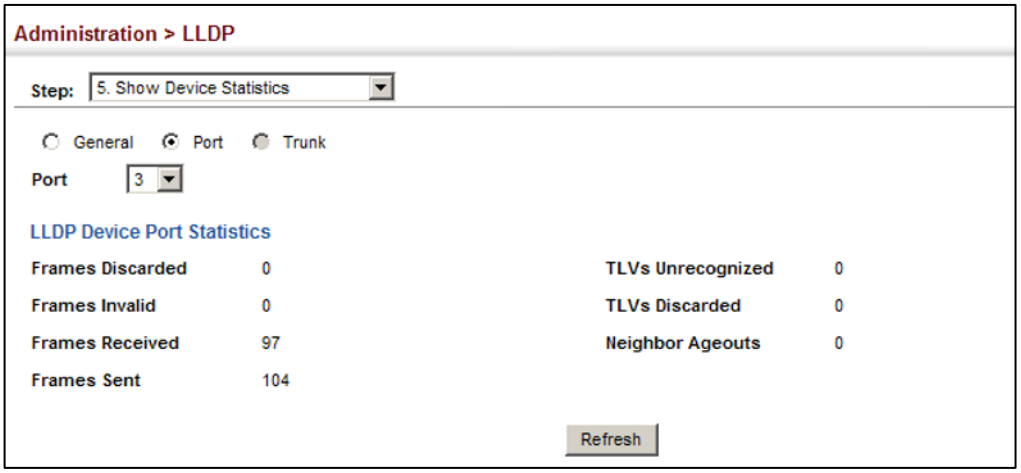


図 12-13　LLDP デバイス統計情報の表示 (ポート)



12.3 PoE

AXprimoM210-08P スイッチは、接続された広範囲の受電装置に DC 電源を供給することができるため、追加の電源を必要とせず、各受電装置に接続されるケーブルの量を削減できます。電源を供給するよう設定されると、自動検出プロセスは、接続された受電装置からの PoE シグネチャによって認証されたスイッチによって初期化されます。検出と認証により、IEEE 802.3af より前の非対応受電装置の損傷を防止します。

スイッチの電源管理により、個々のポートの電力をスイッチの給電能力内で制御することができます。接続された受電装置のポート電力供給は自動的にオン/オフされ、ポートごとの電源供給の優先順位は、スイッチがその給電能力を決して超えないように設定できます。受電装置がスイッチポートに接続されている場合、電源が供給される前にスイッチによってその電源要件が検出されます。受電装置が必要とする電力がポートまたはスイッチ全体の給電能力を超える場合には、電力は供給されません。

ポートは、3 つの電力優先レベル（critical、high、または low）のいずれかに設定できます。スイッチの給電能力内で電力供給を制御するため、重要度が高い優先度に設定されたポートは、低優先度に設定されたポートより優先して電力を有効にします。たとえば、ポートに接続されたデバイスがクリティカルプライオリティに設定されている場合、必要に応じてスイッチは必要な電力を供給します。

12.3.1 スイッチ全体の PoE 情報の設定

[Administration]> [PoE]> [PSE（グローバル設定）]ページを使用して、スイッチの最大 PoE 情報（すべてのギガビットイーサネットポートで使用可能な電力）を設定します。スイッチに接続された受電装置からの電力需要が給電能力を超える場合、スイッチはポート電力優先順位設定を使用して供給電力を制限します。

パラメータ

次のパラメータが表示されます。

- PoE Maximum Available Power - スイッチの PoE 最大使用可能電力量（つまり、すべてのスイッチポートで使用可能な電力）です。スイッチに接続されている受電装置がスイッチの PoE 最大使用可能電力量より多くの電力を必要とする場合は、ポートの電力の優先順位設定を使用して、供給される電力を制御します。
- PoE Maximum Allocation Power - スイッチの PoE 最大割当能力を設定します。
  (AXprimoM210-08P: 50000 から 125000 ミリワット; デフォルト：125000 ミリワット)
- System Operation Status - スイッチポートに提供される PoE 電力サービスのステータスです。
- PoE Power Consumption - スイッチに接続された PoE 受電装置が消費する電力量です。
- Software Version - スイッチ内の PoE コントローラサブシステムで動作するソフトウェアのバージョンです。
- Compatible Mode - スイッチが IEEE 802.3af PoE 標準より前に設計された受電装置に電力を検出して供給できるようにします。(デフォルト: Disabled)
  スイッチは、ギガビットイーサネット UTP ポートを介して定期的にテスト電圧を送信することによって、接続された PoE 受電装置を自動的に検出します。IEEE 802.3af または 802.3at 互換受電装置がこれらのポートのいずれかに差し込まれると、受電装置は試験電圧をスイッチに反映しスイッチの電源をオンにすることができます。互換モードが有効の場合、このスイッチは IEEE 802.3af または 802.3at 準拠の受電装置と、テスト電圧をスイッチに反映した最新の 802.3af 準拠の受電装置を検出できます。テスト電圧を反映しない他のレガシー受電装置を検出することはできません。
  このスイッチでサポートされているレガシー受電装置については、RJ-45 ポートに接続されたデータペアを介して電力を受け入れることができなければなりません。
- Maximum Allocation Mode - PD（受電装置）クラスまたはユーザ構成にもとづいて最大電力割当てモー

ドを設定します。(デフォルト: Class)

- Class - 電力配分は、受電装置の Class 分類にもとづいています。
  IEEE 標準では各電力クラスの最大出力電力を定義していません。 割り当てる電力クラスと最大出力電力を次の表に示します。

表 12-6　電力クラスと最大出力電力

電力クラス	最大出力電力(ワット)
Class 0	15.4
Class 1	4.0
Class 2	7.0
Class 3	15.4
Class 4	30.0

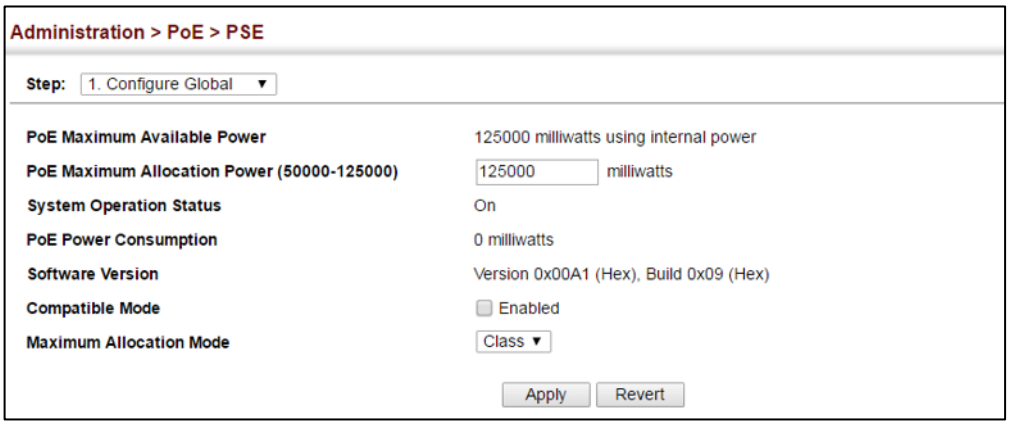
- User - 電力割当ては、このページの[PoE Maximum Allocation Power]設定で定義されているユーザ設定、または[Administration]> [PoE]> [PSE（インタフェースの設定）]ページで定義されているユーザ設定にもとづいています。

Web インタフェース

スイッチの供給可能な最大電力量を設定するには、次の手順を実行します。

1. 管理、PoE、PSE をクリックします。
2. [Step]リストから[Configure Global]を選択します。
3. スイッチが提供する最大 PoE 電力量を設定し、互換モードを有効にし、必要に応じて最大割当てモードを設定します。
4. [Apply]をクリックします。

図 12-14　スイッチの PoE バジェットの設定



12.3.2 ポート PoE 情報の設定

[Administration]> [PoE]> [PSE]ページを使用して、ポートに供給される最大電力を設定します。

コマンドの使用方法

◆ このスイッチは、IEEE 802.3af PoE と IEEE 802.3at-2009 PoE Plus 標準の両方をサポートします。これらの規格に準拠した受電装置（PD）に正しい電力が供給されるように、スイッチからの最初の検出受電装置は、802.3af PD が正常に応答する 802.3af にもとづいています。その後、802.3at PD をクラス 4 受電装置として応答させ、クラス 4 電流を引き出す第 2 の PoE Plus パルスを送信します。その後、ス

イッチはデューティサイクル、ピーク電力、平均電力などの情報を PD と交換します。

◆ 接続受電装置に同時に最大電力を供給することができるポート数について、以下の表に示されています。

表 12-7　同時給電を提供するポートの最大数

Switch	30W (802.3at)	15.4W (802.3af)	7.5W (802.3af)
AXprimoM210-08P	4	8	8

◆ 受電装置がスイッチポートに接続されており、スイッチがポートまたはスイッチ全体に割当てられた最大電力を超えることが検出された場合、デバイスに電力は供給されません（ポート電源はオフのままです)。

◆ すべてのスイッチポートに接続されている受電装置からの電力要求がスイッチに割当てられた最大電力を超える場合は、ポート電力優先順位設定を使用して電力を制御します。下記に例を示します。

- 受電装置が低優先度ポートに接続され、スイッチがその最大電力供給量を超えると、このポートの電力供給はオンになりません。
- 受電装置がクリティカルポートまたはハイプライオリティポートに接続され、ブートアップ中にスイッチがその電力供給量を超えると、受電装置が接続されているポートのうち、スイッチが 1 つ以上の優先度が低く、且つポート番号が大きいポートへの電力供給が停止します。
- スイッチのブートアップ後に受電装置がポートに接続され、電力量を超過する原因となる場合には、優先度の低いポート且つポート番号の大きいポートへの電力供給が停止されます。
- どのポートにプライオリティが設定されておらず、すべてのポートに電力を供給するのに十分な電力がない場合、ポートプライオリティはデフォルトでポート 1＞ポート 2＞ポート 3 ...となります。ポート 8 は、利用可能な電力がその順序で供給されます。
- いずれのポートにもプライオリティが設定されておらず、PoE 消費量がスイッチの最大電力を超えている場合、ポート 8(老番)から逆の順序で電源がシャットダウンされます。

パラメータ

次のパラメータが表示されます。

◆ Port - スイッチ上のポート番号です。

◆ Admin Status - ポート上で PoE 電力供給を有効にします。要求される電力がスイッチまたはポートの電力供給量を超えていない場合、受電装置がポートで検出されたときに自動的に電力が供給されます。(デフォルト: Enabled)

◆ Mode - PoE 電源がポートに供給されているかどうかを示します。過負荷のために電源がオフになっても、管理ステータスは引き続き有効になります。

◆ Time Range Name - 時間帯指定の名前です。時間帯指定が設定されている場合は、指定された期間に電力供給がインタフェースに提供されます。

◆ Time Range Status - インタフェースに時間帯指定が適用されているかどうか、および現在アクティブか非アクティブかを示します。

◆ Class - PoE> PSE（Configure Global）ページの Maximum Allocation Mode 設定で定義されている最大電力割当てクラスを表示します。　クラス情報は、Mode = on のときのみ表示されます。

◆ Priority - ポートの電力供給の優先度を設定します。(オプション: Low, High or Critical; デフォルト: Low)

◆ Power Allocation - ポートの電力供給量を設定します。(範囲: 3000 から 33600 ミリワット; デフォルト：33600 ミリワット）

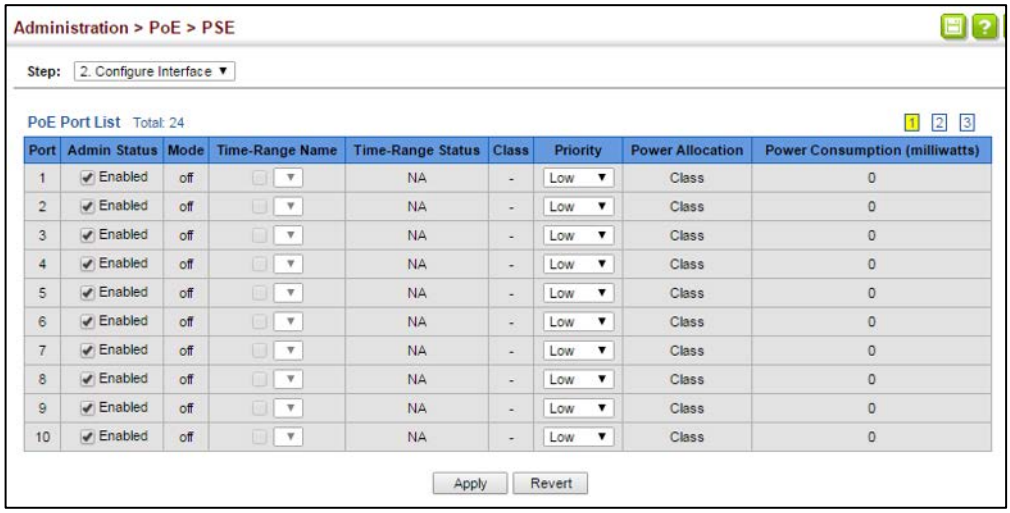
◆ Power Consumption - ポートの現在の消費電力です。

Web インタフェース

ポートの PoE 電力バジェットを設定するには、次の手順を実行します。

1. [Administration]、[PoE]、[PSE]をクリックします。
2. [Step]リストから[Configure Interface]を選択します。
3. 選択したポートで PoE 電力供給を有効にします。優先度と電力予算を設定します。PoE をインタフェースに提供する時間帯指定を指定します。
4. [Apply]をクリックします。

図 12-15　ポートの PoE 情報の設定



12.4 SNMP

SNMP（Simple Network Management Protocol）は、ネットワーク上のデバイスを管理するために特別に設計された通信プロトコルです。SNMP で一般的に管理される機器には、スイッチ、ルータ、およびホストコンピュータが含まれます。SNMP は、通常、ネットワーク環境で適切な操作を行うためにこれらのデバイスを設定したり、パフォーマンスを評価したり、潜在的な問題を検出するためにこれらのデバイスを監視するために使用されます。

SNMP をサポートする管理対象デバイスには、デバイス上でローカルに実行されるソフトウェアが含まれ、エージェントと呼ばれます。定義された変数セット（管理対象オブジェクト）は、SNMP エージェントによって管理され、デバイスの管理に使用されます。これらのオブジェクトは、エージェントによって制御される情報の標準提示を提供する管理情報ベース（MIB）で定義されます。SNMP は、MIB 仕様のフォーマットと、ネットワーク上でこの情報にアクセスするために使用されるプロトコルの両方を定義します。

スイッチには、SNMP バージョン 1,2c、および 3 をサポートするスイッチが含まれています。このエージェントは、スイッチハードウェアのステータスとポートを通過するトラフィックを継続的に監視します。ネットワーク管理端末は、ネットワーク管理ソフトウェアを使用してこの情報にアクセスできます。SNMP v1 および v2c を使用するクライアントからのスイッチへのアクセスは、コミュニティストリングによって制御されます。スイッチと通信するには、まず管理端末が認証のために有効なコミュニティストリングを送信する必要があります。

SNMPv3 を使用してクライアントからスイッチにアクセスすると、メッセージの整合性、認証、および暗号化を保護する追加のセキュリティ機能が提供されます。 MIB ツリーの特定の領域へのユーザアクセスを制御することができます。

SNMPv3 のセキュリティ構造はセキュリティモデルで構成され、各モデルには独自のセキュリティレベルがあります。SNMPv1、SNMPv2c、SNMPv3 の 3 つのセキュリティモデルが定義されています。ユーザは、セキュリティモデルと指定されたセキュリティレベルによって定義される[グループ]に割当てられます。また、各グループには、読み取りと書き込みのための MIB オブジェクトのセットに対するセキュリティアクセス権が定義されています。これは[ビュー]と呼ばれます。スイッチには、セキュリティモデル v1 および v2c に定義されたデフォルトビュー（すべての MIB オブジェクト）とデフォルトグループがあります。次の表は、使用可能なセキュリティモデルとレベル、およびシステムのデフォルト設定を示しています。

表 12-8　SNMPv3 セキュリティモデルとレベル

モデル	レベル	グループ	Read View	Write View	Notify View	セキュリティ
v1	noAuthNoPriv	public (read only)	defaultview	none	none	コミュニティ文字列のみ
v1	noAuthNoPriv	private (read/write)	defaultview	defaultview	none	コミュニティ文字列のみ
v1	noAuthNoPriv	user defined	user defined	user defined	user defined	コミュニティ文字列のみ
v2c	noAuthNoPriv	public (read only)	defaultview	none	none	コミュニティ文字列のみ
v2c	noAuthNoPriv	private (read/write)	defaultview	defaultview	none	コミュニティ文字列のみ
v2c	noAuthNoPriv	user defined	user defined	user defined	user defined	コミュニティ文字列のみ
v3	noAuthNoPriv	user defined	user defined	user defined	user defined	ユーザ名との一致のみ

モデル	レベル	グループ	Read View	Write View	Notify View	セキュリティ
v3	AuthNoPriv	user defined	user defined	user defined	user defined	MD5 または SHA アルゴリズムによるユーザ認証を提供します。
v3	AuthPriv	user defined	user defined	user defined	user defined	DES 56 ビット暗号化を使用した MD5 または SHA アルゴリズムによるユーザ認証とデータプライバシーを提供します。

Note: 定義済みのデフォルトのグループとビューは、システムから削除できます。その際に、アクセスが必要な SNMP クライアントのためにカスタマイズしたグループとビューを定義することができます。

コマンドの使用方法

SNMPv1 / 2c 管理アクセスの設定

スイッチへの SNMPv1 または v2c 管理アクセスを設定するには、次の手順を実行します。

1. [Administration]> [SNMP（Configure Global）]ページを使用して、スイッチ上で SNMP を有効にし、トラップメッセージを有効にします。
2. [Administration]> [SNMP（Configure Community - Add）]ページを使用して、管理アクセス用に認可されたコミュニティストリングを設定します。
3. [Administration]> [SNMP（Configure Trap）]ページを使用してトラップマネージャーを指定し、このスイッチによってキーイベントが管理端末に報告されるようにします。

SNMPv3 管理アクセスの設定

1. [Administration]> [SNMP（Configure Global）]ページを使用して、スイッチ上で SNMP を有効にし、トラップメッセージを有効にします。
2. [Administration]> [SNMP（Configure Trap）]ページを使用してトラップマネージャーを指定し、このスイッチによってキーイベントが管理端末に報告されるようにします。
3. [Administration]> [SNMP（Configure Engine）]ページを使用して、ローカルエンジン ID を変更します。デフォルトのエンジン ID を変更する場合は、他のパラメータを設定する前に変更する必要があります。
4. [Administration]> [SNMP（Configure View）]ページを使用して、スイッチ MIB ツリーの読み取りおよび書き込みアクセスビューを指定します。
5. [Administration]> [SNMP（Configure User）]ページを使用して、必要なセキュリティモデル（SNMP v1、v2c または v3）およびセキュリティレベル（認証とプライバシー）で SNMP ユーザグループを構成します。
6. [Administration]> [SNMP（Configure Group）]ページを使用して、特定の認証パスワードとプライバシーパスワードと共に、SNMP ユーザをグループに割当てます。

12.4.1 SNMP のグローバル設定

[Administration]> [SNMP（Configure Global）]ページを使用して、すべての管理クライアント（バージョン

1、2c、3）に対して SNMPv3 サービスを有効にし、トラップメッセージを有効にします。

パラメータ

次のパラメータが表示されます。

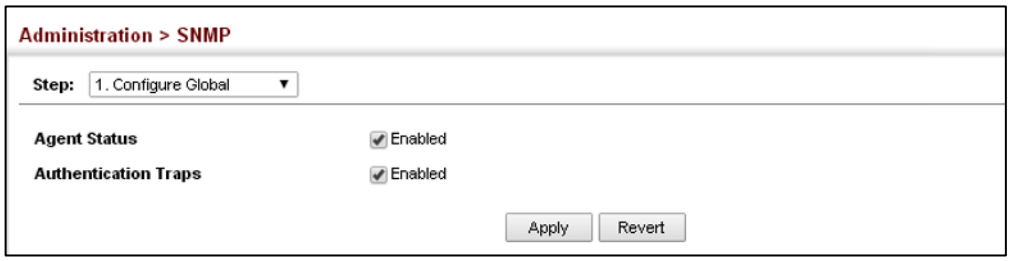
- Agent Status - スイッチ上で SNMP を有効にします。(デフォルト: Enabled)
- Authentication Traps※ - SNMP アクセス認証プロセス中に無効なコミュニティストリングが送信されるたびに、指定された IP トラップマネージャーに通知メッセージを発行します。(デフォルト: Enabled)
  注※ これらは従来の通知であるため、SNMPv3 ホストで使用する場合は、通知ビューの対応するエントリとともに有効にする必要があります。

Web インタフェース

SNMP のグローバルを設定するには：

1. [Administration]、[SNMP]をクリックします。
2. [Step]リストから[Configure Global]を選択します。
3. SNMP と必要なトラップタイプを有効にします。
4. [Apply]をクリックします。

図 12-16　SNMP のグローバル設定



12.4.2 ローカルエンジン ID の設定

[Administration]> [SNMP（Configure Engine - Set Engine ID）]ページを使用して、ローカルエンジン ID を変更します。SNMPv3 エンジンは、スイッチに常駐する独立した SNMP エージェントです。このエンジンは、メッセージの再送、遅延、およびリダイレクトから保護します。エンジン ID は、ユーザパスワードと組み合わせて使用され、SNMPv3 パケットの認証と暗号化のためのセキュリティキーを生成します。

コマンドの使用方法

スイッチに固有のローカルエンジン ID が自動的に生成されます。これはデフォルトのエンジン ID と呼ばれます。ローカルエンジン ID が削除または変更された場合、すべての SNMP ユーザがクリアされます。既存のすべてのユーザを再構成する必要があります。

パラメータ

次のパラメータが表示されます。

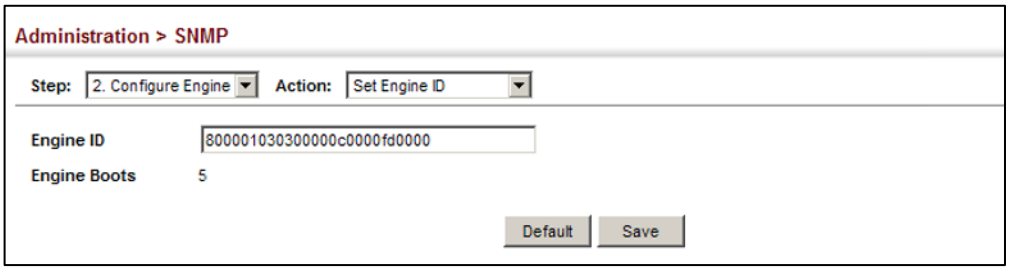
- Engine ID - 新しいエンジン ID は、9 から 64 桁の 16 進数（16 進数で 5 から 32 オクテット）を入力することで指定できます。奇数個の文字が指定された場合は、末尾の 0 が最後のオクテットを埋める値に追加されます。たとえば、値[123456789]は[1234567890]に相当します。
- Engine Boots - SNMP エンジン ID が最後に設定されてからエンジンが（再）初期化された回数です。

Web インタフェース

ローカル SNMP エンジン ID を設定するには：

1. [Administration]、[SNMP]をクリックします。
2. [Step]リストから[Configure Engine]を選択します。
3. [Action]リストから Set Engine ID を選択します。
4. 少なくとも 9 桁の 16 進数の ID を入力します。
5. [Save]をクリックします。

図 12-17　SNMP のローカルエンジン ID の設定



12.4.3 リモートエンジン ID の設定

[Administration]> [SNMP（Configure Engine - Add Remote Engine）]ページを使用して、リモート管理端末のエンジン ID を設定します。リモートデバイス上の SNMPv3 ユーザからの管理アクセスを許可するには、まず、ユーザが常駐するリモートデバイス上の SNMP エージェントのエンジン識別子を指定する必要があります。リモートエンジン ID は、スイッチとリモートホスト上のユーザ間で渡されるパケットの認証と暗号化のためのセキュリティダイジェストを計算するために使用されます。

コマンドの使用方法

SNMP パスワードは、権限のあるエージェントのエンジン ID を使用してローカライズされています。informs の場合、権限のある SNMP エージェントはリモートエージェントです。したがって、プロキシ要求または通知を送信する前に、リモートエージェントの SNMP エンジン ID を設定する必要があります。

パラメータ

次のパラメータが表示されます。

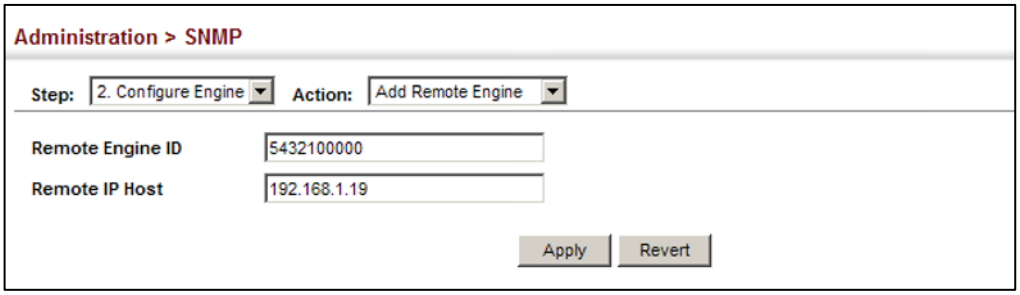
- Remote Engine ID - エンジン ID は、9 から 64 桁の 16 進数（16 進数で 5 から 32 オクテット）を入力することによって指定できます。奇数個の文字が指定された場合は、末尾の 0 が最後のオクテットを埋める値に追加されます。たとえば、値[123456789]は[1234567890]に相当します。
- Remote IP Host - 指定されたエンジン ID を使用しているリモート管理端末の IPv4 アドレスです。

Web インタフェース

リモート SNMP エンジン ID を設定するには：

1. [Administration]、[SNMP]をクリックします。
2. [Step]リストから[Configure Engine]を選択します。
3. [Action]リストから[Add Remote Engine]を選択します。
4. 少なくとも 9 桁の 16 進数の ID とリモートホストの IP アドレスを入力します。
5. [Apply]をクリックします。

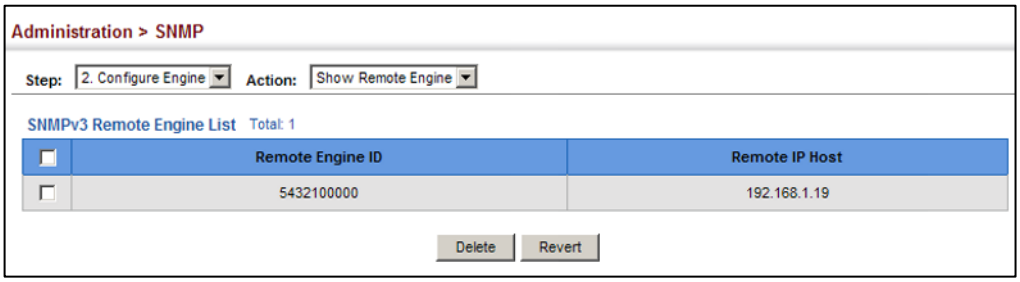
図 12-18　SNMP 用のリモートエンジン ID の設定



リモート SNMP エンジン ID を表示するには：

1. [Administration]、[SNMP]をクリックします。
2. [Step]リストから[Configure Engine]を選択します。
3. [Action]リストから[Show Remote Engine]を選択します。

図 12-19　SNMP のリモートエンジン ID の表示



12.4.4 SNMPv3 ビューの設定

[Administration]> [SNMP（Configure View）]ページを使用して、MIB ツリーの特定の部分へのユーザアクセスを制限するために使用される SNMPv3 ビューを設定します。定義済みビュー "defaultview"には、MIB ツリー全体へのアクセスが含まれます。

パラメータ

次のパラメータが表示されます。

ビューを追加

- View Name - SNMP ビューの名前です。(範囲: 1 から 32 文字)
- OID Subtree - MIB ツリー内のブランチの初期オブジェクト識別子を指定します。OID 文字列の特定部分をマスクするためにワイルドカードを使用することができます。[Add OID Subtree]ページを使用して、追加のオブジェクト識別子を構成します。(範囲: 1 から 64 文字)
- Type - MIB ツリー内のブランチのオブジェクト識別子が SNMP ビューに含まれているか、または SNMP ビューから除外されているかどうかを示します。

OID サブツリーを追加

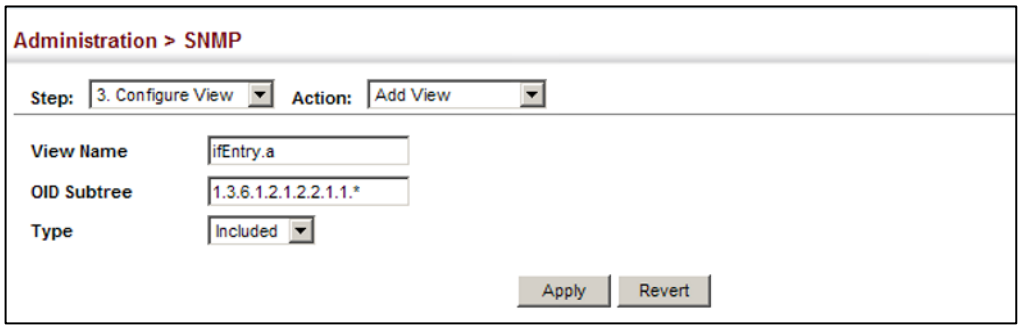
- View Name - [Add View]ページで設定された SNMP ビューを一覧表示します。(範囲: 1 から 32 文字)。
- OID Subtree - MIB ツリー内のブランチの追加のオブジェクト識別子を、選択したビューに追加します。OID 文字列の特定部分をマスクするためにワイルドカードを使用することができます。(範囲: 1 から 64 文字)
- Type - MIB ツリー内のブランチのオブジェクト識別子が SNMP ビューに含まれているか、または SNMP ビューから除外されているかどうかを示します。

Web インタフェース

スイッチの MIB データベースの SNMP ビューを設定するには、次の手順を実行します。

1. [Administration]、[SNMP]をクリックします。
2. [Step]リストから[Configure View]を選択します。
3. [Action]リストから[Add View]を選択します。
4. ビューの名前を入力し、スイッチの MIB データベースの最初の OID サブツリーをビューに含めるか除外するかを指定します。[Add OID Subtree]ページを使用して、オブジェクト識別子ブランチをビューに追加します。
5. [Apply]をクリックします。

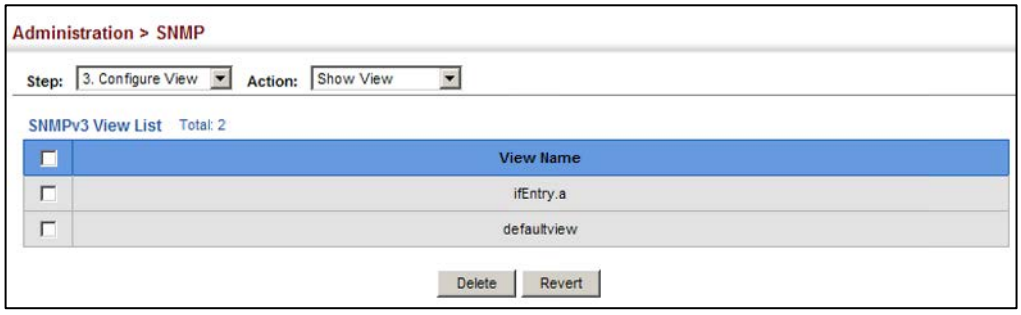
図 12-20　SNMP ビューの作成



スイッチの MIB データベースの SNMP ビューを表示するには、次の手順を実行します。

1. [Administration]、[SNMP]をクリックします。
2. [Step]リストから[Configure View]を選択します。
3. 操作リストから[Show View]を選択します。

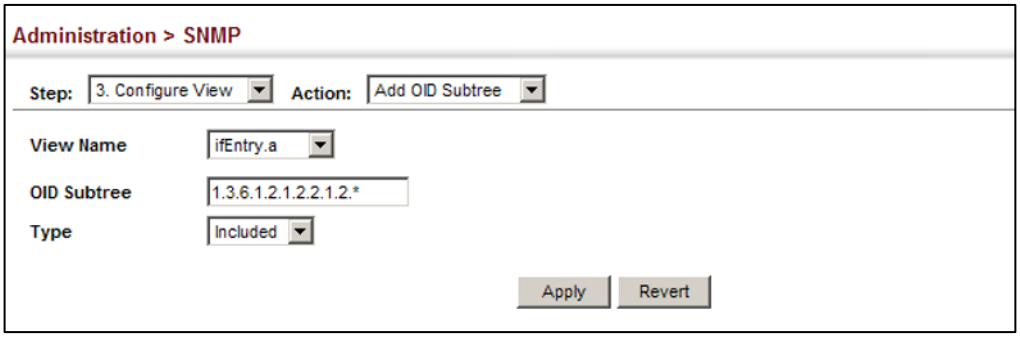
図 12-21　SNMP ビューの表示



スイッチの MIB データベースの既存の SNMP ビューにオブジェクト識別子を追加するには、次の手順を実行します。

1. [Administration]、[SNMP]をクリックします。
2. [Step]リストから[Configure View]を選択します。
3. [Action]リストから[Add OID Subtree]を選択します。
4. 既存のビューのリストからビュー名を選択し、スイッチの MIB データベース内の追加の OID サブツリーをビューに含めるか除外するかを指定します。
5. [Apply]をクリックします。

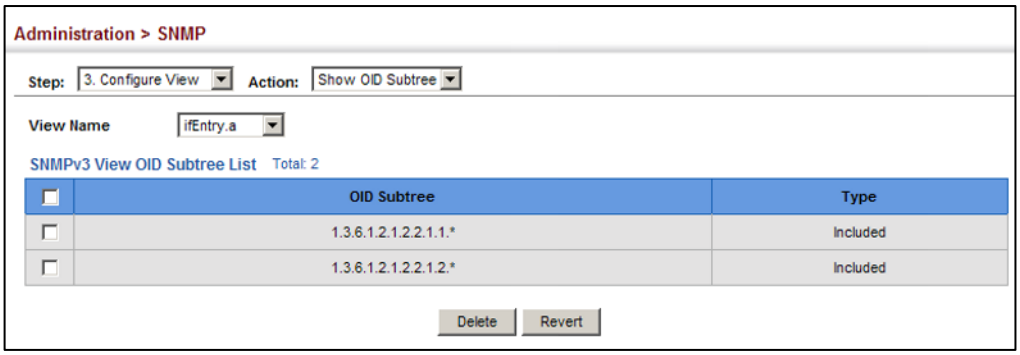
図 12-22　SNMP ビューへの OID サブツリーの追加



スイッチの MIB データベースの SNMP ビュー用に設定された OID ブランチを表示するには、次の手順を実行します。

1. [Administration]、[SNMP]をクリックします。
2. [Step]リストから[Configure View]を選択します。
3. [Action]リストから[Show OID Subtree]を選択します。
4. 既存のビューのリストからビュー名を選択します。

図 12-23　SNMP ビュー用に構成された OID サブツリーの表示



12.4.5 SNMPv3 グループの設定

[Administration]> [SNMP（Configure Group）]ページを使用して、割当てられたユーザのアクセスポリシーを設定するために使用できる SNMPv3 グループを追加し、特定の読み取り、書き込み、および通知ビューに制限します。あらかじめ定義されたデフォルトグループを使用するか、または新しいグループを作成して、一連の SNMP ユーザを SNMP ビューにマッピングできます。

パラメータ

次のパラメータが表示されます。

- Group Name - ユーザが割当てられている SNMP グループの名前です。(範囲: 1 から 32 文字)
- Model - ユーザセキュリティモデルです。 SNMP v1、v2c、または v3。
- Level - 次のセキュリティレベルは、SNMP セキュリティモデルに割当てられたグループに対してのみ使用されます。
  - noAuthNoPriv - SNMP 通信では、認証や暗号化は使用されません。これがデフォルトのセキュリティレベルです。
  - AuthNoPriv - SNMP 通信は認証を使用しますが、データは暗号化されません。
  - AuthPriv - SNMP 通信は、認証と暗号化の両方を使用します。

- Read View - 読み取りアクセス用に構成されたビューです。(範囲: 1 から 32 文字)
- Write View - 書き込みアクセス用に構成されたビューです。(範囲: 1 から 32 文字)
- Notify View - 通知用に構成されたビューです。(範囲: 1 から 32 文字)

表 12-9 サポートされている通知メッセージ

モデル	レベル	グループ
RFC 1493 トラップ		
newRoot	1.3.6.1.2.1.17.0.1	newRoot トラップは、送信エージェントがスパニングツリーの新しいルートになったことを示します。 トラップは、その選出の直後に、新しいルートとして、例えばその選出の直後にトポロジ変更タイマーが満了したときに、ブリッジによって直ちに送信されます。
topologyChange	1.3.6.1.2.1.17.0.2	topologyChange トラップは、設定されたポートのいずれかがラーニングステートからフォワーディングステートに移行するとき、または転送ステートから廃棄ステートに移行するときにブリッジによって送信されます。 同じ移行に対して newRoot トラップが送信された場合、topologyChange トラップは送信されません
SNMPv2 トラップ		
coldStart	1.3.6.1.6.3.1.1.5.1	coldStart トラップは、エージェントロールで動作している SNMPv2 エンティティが自身を再初期化していて、その構成が変更されている可能性があることを示します。
warmStart	1.3.6.1.6.3.1.1.5.2	warmStart トラップは、エージェントロールで動作している SNMPv2 エンティティが、コンフィグレーションが変更されないように自身を再初期化していることを示します。
linkDown※	1.3.6.1.6.3.1.1.5.3	linkDown トラップは、エージェントロールで動作している SNMP エンティティが、その通信リンクの 1 つに対する ifOperStatus オブジェクトが down 状態への遷移を検出したことを示します（notPresent 状態からではありません）。この他の状態は、ifOperStatus のインクルードされた値によって示されます。
linkUp※	1.3.6.1.6.3.1.1.5.4	linkUp トラップは、エージェン

モデル	レベル	グループ
		トロールで動作している SNMP エンティティが、その通信リンクの 1 つに対する ifOperStatus オブジェクトが down 状態から、他の状態に遷移したことを検出したことを示します（notPresent 状態には移行しません）。この他の状態は、ifOperStatus のインクルードされた値によって示されます。
authenticationFailure※	1.3.6.1.6.3.1.1.5.5	authenticationFailure トラップは、エージェントロールで動作している SNMPv2 エンティティが正しく認証されていないプロトコルメッセージを受信したことを示します。SNMPv2 のすべての実装でこのトラップを生成できる必要がありますが、snmpEnableAuthenTraps オブジェクトはこのトラップが生成されるかどうかを示します。
RMON イベント（V2）		
risingAlarm	1.3.6.1.2.1.16.0.1	アラームエントリが上昇閾値を超えたときに生成され、SNMP トラップを送信するように設定されたイベントを生成する SNMP トラップです。
fallingAlarm	1.3.6.1.2.1.16.0.2	アラームエントリが下限閾値を超えたときに生成され、SNMP トラップを送信するように設定されたイベントを生成する SNMP トラップです。
Private Traps		
swPowerStatusChangeTrap	1.3.6.1.4.1.21839.10.1.43.2.1.0.1	このトラップは、電源状態が変更されたときに送信されます。
swPortSecurityTrap	1.3.6.1.4.1.21839.10.1.44.2.1.0.36	このトラップは、ポートが侵入されたときに送信されます。このトラップは、portSecActionTrap が有効な場合にのみ送信されます。
swIpFilterRejectTrap	1.3.6.1.4.1.21839.10.1.43.2.1.0.40	このトラップは、不適切な IP アドレスが IP フィルタによって拒否された場合に送信されます。
pethPsePortOnOffNotification	1.3.6.1.4.1.21839.10.1.43.2.1.0.43	この通知は、PSE ポートが PD に電力を供給しているかどうかを示します。この通知は、検索モードを除くすべてのステータス変更時に送信する必要があります。
pethMainPowerUsageOnNotification	1.3.6.1.4.1.21839.10.1.43.2.1.0.45	この通知は、PSE 閾値の使用状況表示がオンであることを示します。 電力使用量が閾値を超え

モデル	レベル	グループ
		ています。
pethMainPowerUsageOffNotification	1.3.6.1.4.1.21839.10.1.43.2.1.0.46	この通知は、PSE 閾値の使用状況がオフであることを示します。 使用電力が閾値を下回っています。
swAtcBcastStormAlarmFireTrap	1.3.6.1.4.1.21839.10.1.43.2.1.0.70	ブロードキャストトラフィックがストームとして検出されると、このトラップは起動されます。
swAtcBcastStormAlarmClearTrap	1.3.6.1.4.1.21839.10.1.43.2.1.0.71	ブロードキャストストームが通常のトラフィックとして検出されると、このトラップは起動されます。
swAtcBcastStormTcApplyTrap	1.3.6.1.4.1.21839.10.1.43.2.1.0.72	ATC が起動されると、このトラップは起動されます。
swAtcBcastStormTcReleaseTrap	1.3.6.1.4.1.21839.10.1.43.2.1.0.73	ATC が解放されると、このトラップ起動されます。
swAtcMcastStormAlarmFireTrap	1.3.6.1.4.1.21839.10.1.43.2.1.0.74	ストームとしてマルチキャストトラフィックが検出されると、このトラップは起動されます。
swAtcMcastStormAlarmClearTrap	1.3.6.1.4.1.21839.10.1.43.2.1.0.75	マルチキャストストームが通常のトラフィックとして検出されると、このトラップは起動されます。
swAtcMcastStormTcApplyTrap	1.3.6.1.4.1.21839.10.1.43.2.1.0.76	ATC が起動されると、このトラップは起動されます。
swAtcMcastStormTcReleaseTrap	1.3.6.1.4.1.21839.10.1.43.2.1.0.77	ATC が解放されると、このトラップ起動されます。
stpBpduGuardPortShutdownTrap	1.3.6.1.4.1.21839.10.1.43.2.1.0.91	このトラップは、BPDU ガードのためにインタフェースがシャットダウンされたときに送信されます。
swLoopbackDetectionTrap	1.3.6.1.4.1.21839.10.1.43.2.1.0.95	このトラップは、ループバック BPDU が検出されたときに送信されます。
autoUpgradeTrap	1.3.6.1.4.1.21839.10.1.43.2.1.0.104	このトラップは、自動アップグレードが実行されたときに送信されます。
swCpuUtiRisingNotification	1.3.6.1.4.1.21839.10.120.2.1.0.107	この通知は、CPU 使用率が cpuUtiFallingThreshold から cpuUtiRisingThreshold に上昇したことを示します。
swCpuUtiFallingNotification	1.3.6.1.4.1.21839.10.1.43.2.1.0.108	この通知は、CPU 使用率が cpuUtiRisingThreshold から cpuUtiFallingThreshold に低下したことを示します。
swMemoryUtiRisingThreshold Notification	1.3.6.1.4.1.21839.10.1.43.2.1.0.109	この通知は、メモリ使用率が memoryUtiFallingThreshold から memoryUtiRisingThreshold に上昇したことを示します。

モデル	レベル	グループ
swMemoryUtiFallingThreshold Notification	1.3.6.1.4.1.21839.10.1.43.2.1.0.110	この通知は、メモリ使用率が memoryUtiRisingThreshold から memoryUtiFallingThreshold に低下したことを示します。
dhcpRougeServerAttackTrap	1.3.6.1.4.1.21839.10.1.43.2.1.0.114	このトラップは、不正なサーバから DHCP パケットを受信したときに送信されます。
macNotificationTrap	1.3.6.1.4.1.21839.10.1.43.2.1.0.138	このトラップは、スイッチ上で動的 MAC アドレスが変更された場合に送信されます。
lbdDetectionTrap	1.3.6.1.4.1.21839.10.1.43.2.1.0.141	このトラップは、LBD によってループバック状態が検出されたときに送信されます。
lbdRecoveryTrap	1.3.6.1.4.1.21839.10.1.43.2.1.0.142	このトラップは、LBD によって回復が行われたときに送信されます。
sfpThresholdAlarmWarnTrap	1.3.6.1.4.1.21839.10.1.43.2.1.0.189	このトラップは、sfp の A / D 量がアラーム/警告閾値内にないときに送信されます。
userAuthenticationFailureTrap	1.3.6.1.4.1.21839.10.1.43.2.1.0.199	このトラップは、認証に失敗した場合にトリガされます。
userAuthenticationSuccessTrap	1.3.6.1.4.1.21839.10.1.43.2.1.0.200	認証が成功すると、このトラップがトリガされます。
loginTrap	1.3.6.1.4.1.21839.10.1.43.2.1.0.201	このトラップは、ユーザがログインするときに送信されます。
logoutTrap	1.3.6.1.4.1.21839.10.1.43.2.1.0.202	このトラップは、ユーザがログアウトしたときに送信されます。
fileCopyTrap	1.3.6.1.4.1.21839.10.1.43.2.1.0.208	このトラップは、ファイルコピーの実行時に送信されます。 コピー操作がシステムによってトリガされた場合、ログインユーザ情報（trapVarLoginUserName / trapVarSessionType / trapVarLoginInetAddressTypes / trapVarLoginInetAddres）は NULL 値になります。
userauthCreateUserTrap	1.3.6.1.4.1.21839.10.1.43.2.1.0.209	このトラップは、ユーザアカウントが作成されたときに送信されます。
userauthDeleteUserTrap	1.3.6.1.4.1.21839.10.1.43.2.1.0.210	このトラップは、ユーザアカウントが削除されたときに送信されます。
userauthModifyUserPrivilegeTrap	1.3.6.1.4.1.21839.10.1.43.2.1.0.211	このトラップは、ユーザ特権が変更されたときに送信されます。
cpuGuardControlTrap	1.3.6.1.4.1.21839.10.1.43.2.1.0.213	このトラップは、CPU 使用率が最初に高水準を超えるか CPU 使用率が低水準点を下回って高水準点を上回った場合に送信され

モデル	レベル	グループ
		ます。
cpuGuardReleaseTrap	1.3.6.1.4.1.21839.10.1.43.2.1.0.214	このトラップは、CPU 使用率が高水準点を上回って低水準点を下回ると送信されます。

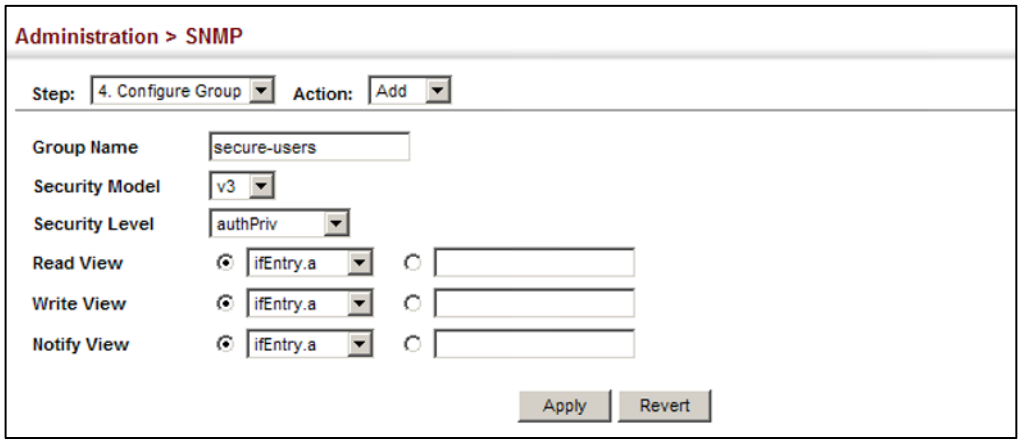
注※ これらは従来の通知であるため、[SNMP]メニューの設定で対応するトラップと併用して有効にする必要があります。

Web インタフェース

SNMP グループを設定するには：

1. [Administration]、[SNMP]をクリックします。
2. [Step]リストから[Configure Group]を選択します。
3. [Action]リストから[Add]を選択します。
4. グループ名を入力し、セキュリティモデルとレベルを割当て、読み取り、書き込み、および通知のビューを選択します。
5. [Apply]をクリックします。

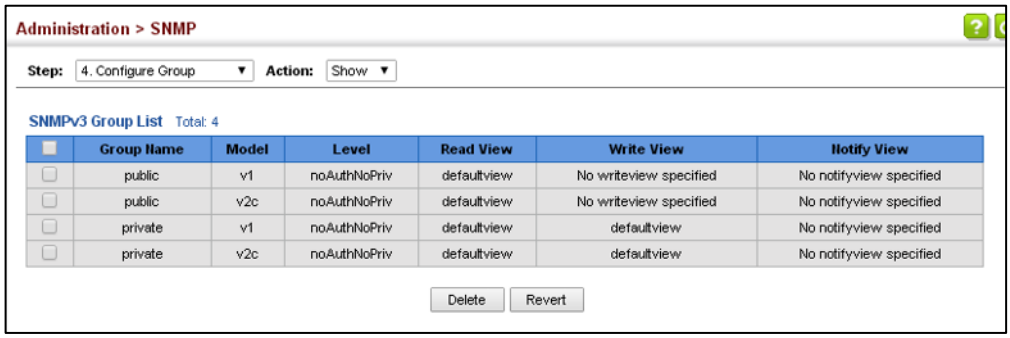
図 12-24　SNMP グループの作成



SNMP グループを表示するには:

1. [Administration]、[SNMP]をクリックします。
2. [Step]リストから[Configure Group]を選択します。
3. [Action]リストから[Show]を選択します。

図 12-25　SNMP グループの表示



12.4.6 コミュニティアクセス文字列の設定

[Administration]> [SNMP（Configure Community - Add）]ページを使用して、SNMP v1 および v2c を使用するクライアントによる管理アクセスを許可された最大 5 つのコミュニティストリングを設定します。セキュリティ上の理由から、デフォルトの文字列を削除することを検討する必要があります。

パラメータ

次のパラメータが表示されます。

- Community String - パスワードのように動作し、SNMP プロトコルへのアクセスを許可するコミュニティストリングです。
  範囲: 1 から 16 文字、大文字と小文字を区別
  デフォルトの文字列：なし
- Access Mode - コミュニティ文字列のアクセス権を指定します。
  - Read-Only - 認可された管理端末は、MIB オブジェクトのみを取り出すことができます。
  - Read/Write - 認可された管理端末は、MIB オブジェクトの検索と変更の両方を行うことができます。

Web インタフェース

コミュニティアクセス文字列を設定するには：

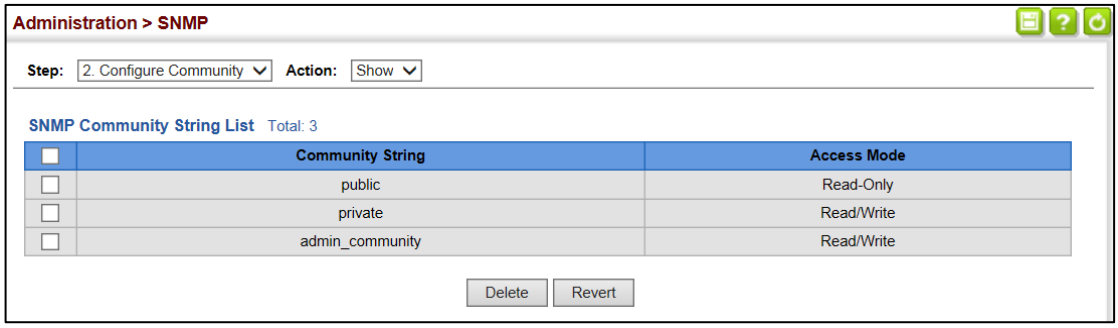
1. [Administration]、[SNMP]をクリックします。
2. [Step]リストから[Configure Community]を選択します。
3. [Action]リストから[Add]を選択します。
4. 必要に応じて新しいコミュニティ文字列を追加し、アクセスモードリストから対応するアクセス権を選択します。
5. [Apply]をクリックします。

図 12-26　コミュニティアクセス文字列の設定

コミュニティアクセス文字列を表示するには：

1. [Administration]、[SNMP]をクリックします。
2. [Step]リストから[Configure Community]を選択します。
3. [Action]リストから[Show]を選択します。

図 12-27　コミュニティアクセス文字列を表示する



12.4.7 ローカル SNMPv3 ユーザの設定

[Administration]> [SNMP（Configure User - Add SNMPv3 Local User）]ページを使用して、SNMPv3 クライアントの管理アクセスを許可するか、ローカルスイッチから送信された SNMPv3 トラップメッセージの送信元を識別します。各 SNMPv3 ユーザは一意の名前で定義されます。ユーザは特定のセキュリティレベルで構成され、グループに割当てられている必要があります。SNMPv3 グループは、特定の読み取り、書き込み、および通知ビューにユーザを制限します。

パラメータ

次のパラメータが表示されます。

- User Name - SNMP エージェントに接続するユーザの名前です。
  (範囲: 1 から 32 文字)
- Group Name - ユーザが割当てられている SNMP グループの名前です。(範囲: 1 から 32 文字)
- Security Model - ユーザセキュリティモデルです。 SNMP v1、v2c、または v3。
- Security Level - 次のセキュリティレベルは、SNMP セキュリティモデルに割当てられたグループに対してのみ使用されます。
  - noAuthNoPriv - SNMP 通信では、認証や暗号化は使用されません。これがデフォルトのセキュリティレベルです。
  - AuthNoPriv - SNMP 通信は認証を使用しますが、データは暗号化されません。
  - AuthPriv - SNMP 通信は、認証と暗号化の両方を使用します。
- Authentication Protocol - ユーザ認証に使用される方法です。
  (オプション: MD5, SHA; デフォルト: MD5)
- Authentication Password - 最低 8 つのプレーンテキスト文字が必要です。(範囲: 8 から 32 文字)
- Privacy Protocol - 暗号化アルゴリズムはデータプライバシーのために使用されます。 現在、56 ビットの DES のみが利用可能です。
- Privacy Password - 最低 8 つのプレーンテキスト文字が必要です。

Web インタフェース

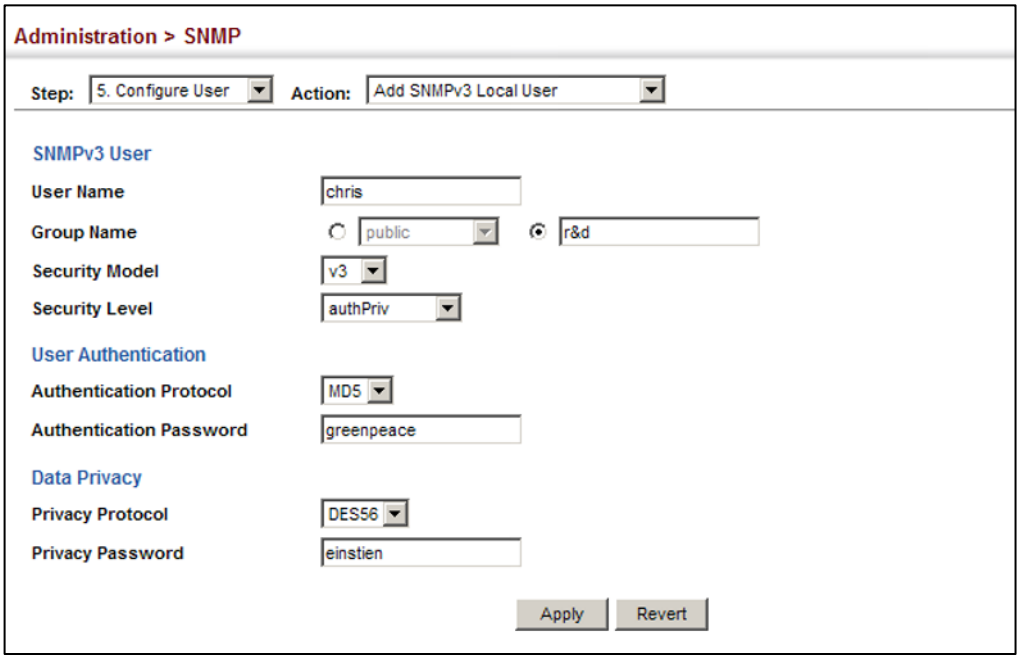
ローカルの SNMPv3 ユーザを設定するには：

1. [Administration]、[SNMP]をクリックします。
2. [Step]リストから[Configure User]を選択します。
3. [Action]リストから[Add SNMPv3 Local User]を選択します。
4. 名前を入力してグループに割当てます。セキュリティモデルが SNMPv3 に設定され、セキュリティレ

ベルが authNoPriv または authPriv の場合、認証プロトコルとパスワードを指定する必要があります。セキュリティレベルが authPriv の場合、プライバシーパスワードも指定する必要があります。

5. [Apply]をクリックします。

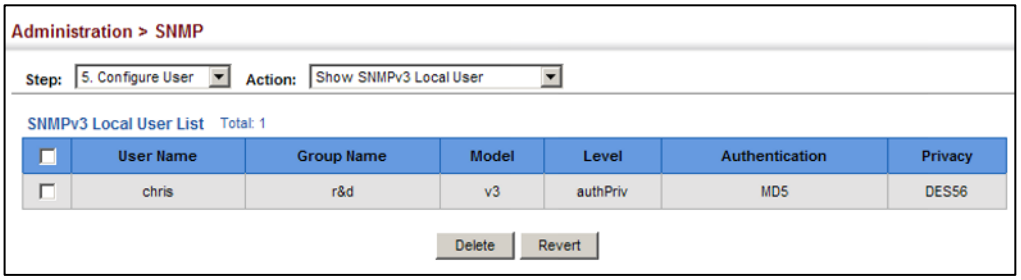
図 12-28　ローカル SNMPv3 ユーザの設定



ローカル SNMPv3 ユーザを表示するには：

1. [Administration]、[SNMP]をクリックします。
2. [Step]リストから[Configure User]を選択します。
3. [Action]リストから[Show SNMPv3 Local User]を選択します。

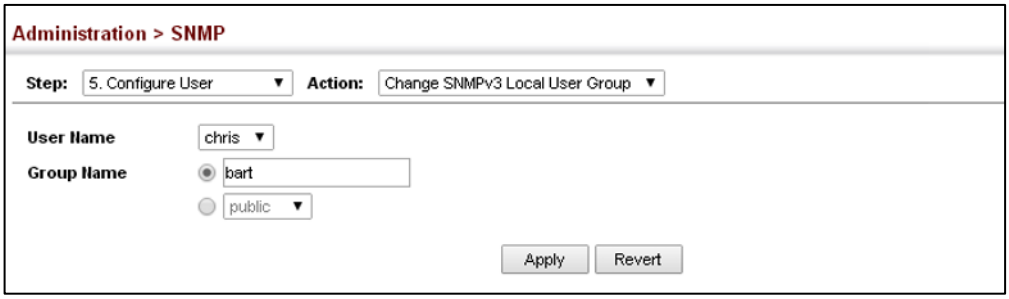
図 12-29　ローカル SNMPv3 ユーザの表示



ローカルの SNMPv3 ローカルユーザグループを変更するには：

1. [Administration]、[SNMP]をクリックします。
2. [Action]リストから[Change SNMPv3 Local User Group]を選択します。
3. ユーザ名を選択します。
4. 新しいグループ名を入力してください。
5. [Apply]をクリックします。

図 12-30　ローカル SNMPv3 ユーザグループの変更



12.4.8 リモート SNMPv3 ユーザの設定

[Administration]> [SNMP（Configure User - Add SNMPv3 Remote User）]ページを使用して、ローカルスイッチから送信された SNMPv3 通知メッセージの送信元を識別します。各 SNMPv3 ユーザは一意の名前で定義されます。ユーザは特定のセキュリティレベルで構成され、グループに割当てられている必要があります。SNMPv3 グループは、特定の読み取り、書き込み、および通知ビューにユーザを制限します。

コマンドの使用方法

- リモートデバイス上の SNMPv3 ユーザへの管理アクセスを許可するには、まず、ユーザが常駐するリモートデバイス上の SNMP エージェントのエンジン識別子を指定する必要があります。リモートエンジン ID は、スイッチとリモートユーザの間で渡されるパケットの認証と暗号化のためのセキュリティダイジェストを計算するために使用されます。

パラメータ

次のパラメータが表示されます。

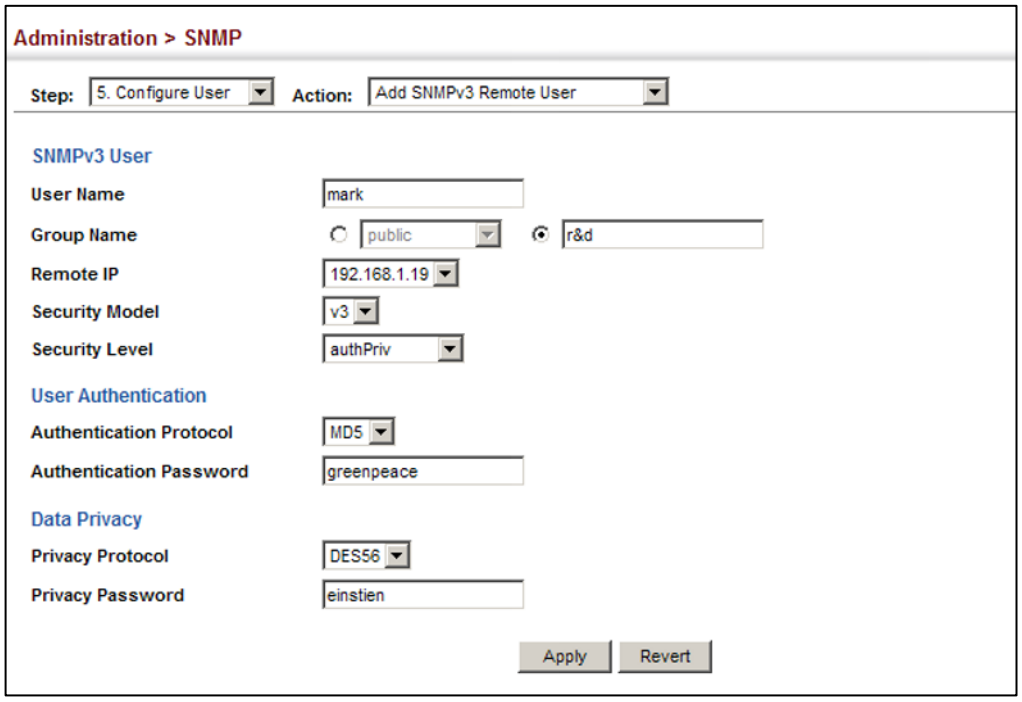
- User Name - SNMP エージェントに接続するユーザの名前です。
  (範囲: 1 から 32 文字)
- Group Name - ユーザが割当てられている SNMP グループの名前です。(範囲: 1 から 32 文字)
- Remote IP - ユーザが常駐しているリモートデバイスの IPv4 アドレスです。
- Security Model - ユーザセキュリティモデルです。 SNMP v1、v2c、または v3。（デフォルト：v3）
- Security Level - 次のセキュリティレベルは、SNMP セキュリティモデルに割当てられたグループに対してのみ使用されます。
  - noAuthNoPriv - SNMP 通信では、認証や暗号化は使用されません。これがデフォルトのセキュリティレベルです。
  - AuthNoPriv - SNMP 通信は認証を使用しますが、データは暗号化されません。
  - AuthPriv - SNMP 通信は、認証と暗号化の両方を使用します。
- Authentication Protocol - ユーザ認証に使用される方法です。(オプション: MD5, SHA; デフォルト: MD5)
- Authentication Password - 最低 8 つのプレーンテキスト文字が必要です。
- Privacy Protocol - 暗号化アルゴリズムはデータプライバシーのために使用されます。 現在、56 ビットの DES のみが利用可能です。
- Privacy Password - 最低 8 つのプレーンテキスト文字が必要です。

Web インタフェース

リモート SNMPv3 ユーザを設定するには：

1. [Administration]、[SNMP]をクリックします。
2. [Step]リストから[Configure User]を選択します。
3. [Action]リストから[Add SNMPv3 Remote User]を選択します。
4. 名前を入力してグループに割当てます。ローカルスイッチから送信された SNMPv3 通知メッセージの送信元を識別する IP アドレスを入力します。セキュリティモデルが SNMPv3 に設定され、セキュリティレベルが authNoPriv または authPriv の場合、認証プロトコルとパスワードを指定する必要があります。セキュリティレベルが authPriv の場合、プライバシーパスワードも指定する必要があります。
5. [Apply]をクリックします。

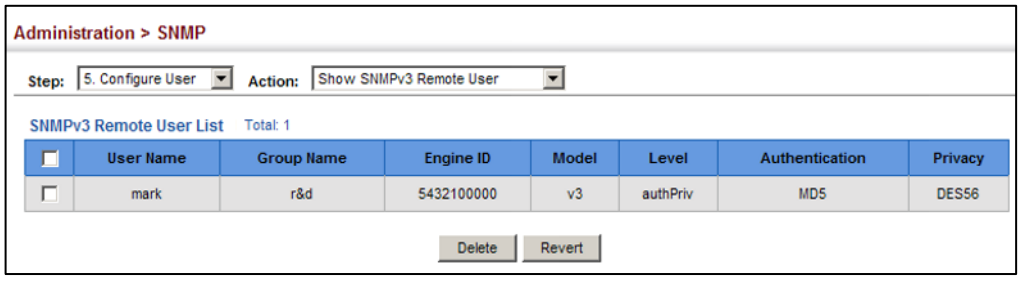
図 12-31　リモート SNMPv3 ユーザの設定



リモート SNMPv3 ユーザを表示するには：

1. [Administration]、[SNMP]をクリックします。
2. [Step]リストから[Configure User]を選択します。
3. [Action]リストから[Show SNMPv3 Remote User]を選択します。

図 12-32　リモート SNMPv3 ユーザの表示



12.4.9 トラップマネージャーの設定

[Administration]> [SNMP（Configure Trap）]ページを使用して、送信するホストデバイスと送信するトラップの種類を指定します。ステータス変更を示すトラップが、スイッチによって指定されたトラップマネージャーに発行されます。トラップマネージャーを指定して、このスイッチによってキーイベントが（ネットワーク管理ソフトウェアを使用して）管理端末に報告されるようにする必要があります。スイッチから認証失敗メッセージやその他のトラップメッセージを受信する管理端末を最大 5 つ指定できます。

コマンドの使用方法

- 通知はデフォルトでトラップメッセージとしてスイッチによって発行されます。トラップメッセージの受信者は、スイッチに応答を送信しません。したがって、トラップは通知メッセージのように信頼性が高くなく、受信確認の要求を含みます。インフォームを使用して、重要な情報がホストによって確実に受信されるようにすることができます。ただし、情報が応答を受信するまでメモリに保持されなければならないため、情報はより多くのシステムリソースを消費することに注意してください。インフォームはネットワークトラフィックにも追加されます。トラップや通知として通知を発行するかどうかを決定するときは、これらの影響を考慮する必要があります。
  SNMPv2c ホストにインフォームを送信するには、下記の手順を完了させてください:
  1. SNMP エージェントを有効にします。
  2. 必要な通知メッセージでビューを作成します。
  3. 必要な通知ビューを含めるようにグループを設定します（[Configure Trap] - [Add]ページで指定されたコミュニティ文字列と一致します）。
  4. 次のページの説明に従って、トラップ通知を有効にします。

  SNMPv3 ホストにインフォームを送信するには、下記の手順を完了させてください:
  1. SNMP エージェントを有効にします。
  2. メッセージ交換処理で使用するリモート SNMPv3 ユーザを作成します。トラップ設定ページで指定したユーザが存在しない場合、指定されたリモートユーザの名前と読み取り、書き込み、および通知ビューのデフォルト設定を使用して、SNMPv3 グループが自動的に作成されます。
  3. 必要な通知メッセージでビューを作成します。
  4. 必要な通知ビューを含むグループを作成します。
  5. 次のページの説明に従って、トラップ通知を有効にします。

パラメータ

次のパラメータが表示されます。

SNMP バージョン 1

- IP Address - 通知メッセージを受信するための新しい管理端末の IPv4 または IPv6 アドレスです（つまり、対象の受信者）。
- Version - SNMP v1、v2c、または v3 トラップとして通知を送信するかどうかを指定します。（デフォルト：v1）
- Community String - 新しいトラップマネージャエントリの有効なコミュニティ文字列を指定します。(範囲: 1 から 32 文字、大文字と小文字を区別されます)
  この文字列は[Configure Trap] - [Add]ページで設定できますが、[Configure User] - [Add Community]ページで定義することをお勧めします。
- UDP Port - トラップマネージャーが使用する UDP ポート番号を指定します。(デフォルト: 162)

SNMP バージョン 2c

- IP Address - 通知メッセージを受信するための新しい管理端末の IPv4 または IPv6 アドレスです（つまり、対象の受信者）。
- Version - SNMP v1、v2c、または v3 トラップとして通知を送信するかどうかを指定します。
- 通知タイプ
  - Traps - 通知はトラップメッセージとして送信されます。
  - Inform - 通知は通知メッセージとして送信されます。オプションはバージョン 2c と 3 ホストにのみ使用することができます。(デフォルト: トラップを使用)
    - Timeout - 通知メッセージを再送信するまでの確認応答を待機する秒数です。(範囲: 0 から 2147483647 センチ秒; デフォルト: 1500 センチ秒)
    - Retry times - 受信者が受信確認を確認しなかった場合に通知メッセージを再送信する最大回数です。
      (範囲: 0 から 255; デフォルト：3)
- Community String - 新しいトラップマネージャエントリの有効なコミュニティ文字列を指定します。(範囲: 1 から 32 文字、大文字と小文字を区別されます)
  この文字列は[Configure Trap] - [Add]ページで設定できますが、[Configure User] - [Add Community]ページで定義することをお勧めします。
- UDP Port - トラップマネージャーが使用する UDP ポート番号を指定します。(デフォルト: 162)

SNMP バージョン 3

- IP Address - 通知メッセージを受信するための新しい管理端末の IPv4 または IPv6 アドレスです（つまり、対象の受信者）。
- Version - SNMP v1、v2c、または v3 トラップとして通知を送信するかどうかを指定します。
- 通知タイプ
  - Traps - 通知はトラップメッセージとして送信されます。
  - Inform - 通知はインフォームメッセージとして送信されます。オプションはバージョン 2c と 3 ホストにのみ使用することができます。(デフォルト: トラップを使用)
    - Timeout - 通知メッセージを再送信するまでの確認応答を待機する秒数です。(範囲: 0 から 2147483647 センチ秒; デフォルト: 1500 センチ秒)
    - Retry times - 受信者が受信確認を確認しなかった場合に通知メッセージを再送信する最大回数です。
      (範囲: 0 から 255; デフォルト：3)
- Local User Name - ローカルスイッチから送信された SNMPv3 トラップメッセージの送信元を識別するために使用されるローカルユーザの名前です。(範囲: 1 から 32 文字)
  指定したユーザのアカウントが作成されていない場合、自動的にアカウントが作成されます。
- Remote User Name - ローカルスイッチから送信された SNMPv3 通知メッセージの送信元を識別するために使用されるリモートユーザの名前です。(範囲: 1 から 32 文字)
  指定したユーザのアカウントが作成されていない場合、自動的にアカウントが作成されます。
- UDP Port - トラップマネージャーが使用する UDP ポート番号を指定します。(デフォルト: 162)
- Security Level - トラップバージョン 3 が選択されている場合は、次のいずれかのセキュリティレベルを指定する必要があります。(Default: noAuthNoPriv)
  - noAuthNoPriv - SNMP 通信では、認証や暗号化は使用されません。
  - AuthNoPriv - SNMP 通信は認証を使用しますが、データは暗号化されません。
  - AuthPriv - SNMP 通信は、認証と暗号化の両方を使用します。

Web インタフェース

トラップマネージャーを設定するには：

1. [Administration]、[SNMP]をクリックします。
2. [Step]リストから[Configure Trap]を選択します。
3. [Action]リストから[Add]を選択します。
4. 選択した SNMP バージョンにもとづいて必要なパラメータを入力します。
5. [Apply]をクリックします。

図 12-33　トラップマネージャーの設定 (SNMPv1)

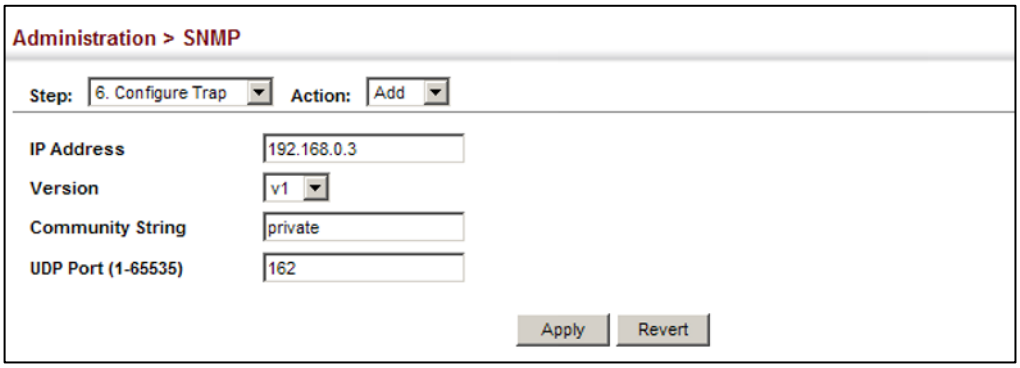


図 12-34　トラップマネージャーの設定 (SNMPv2c)

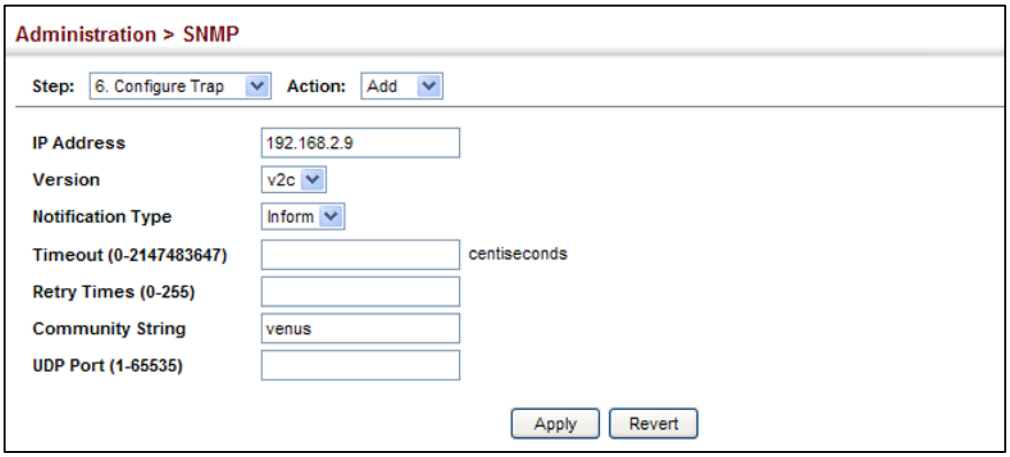
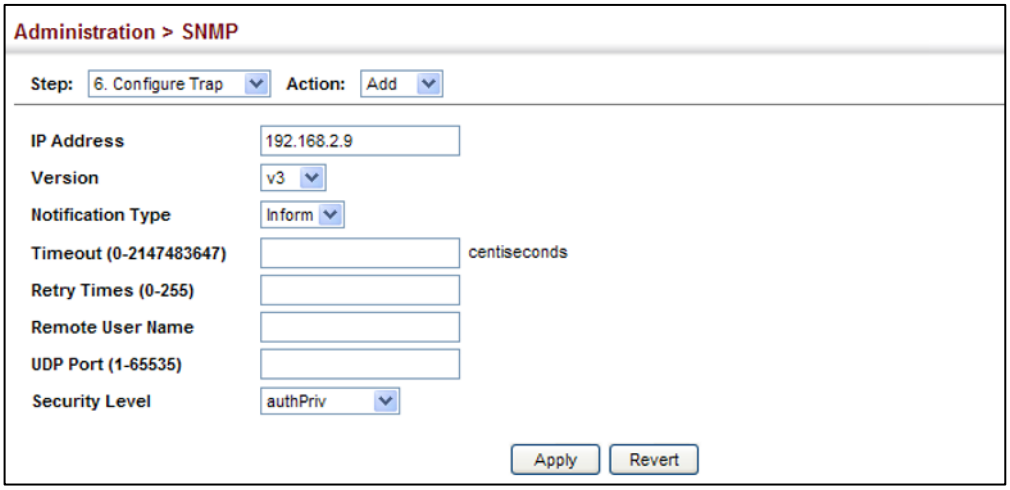


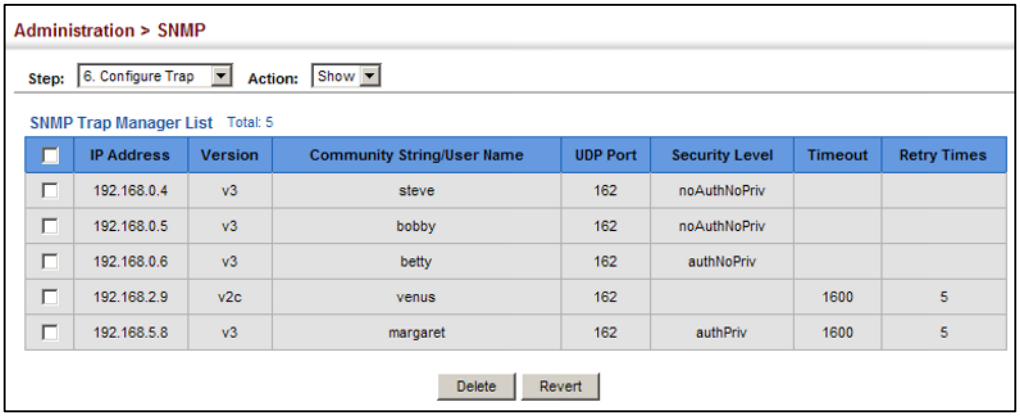
図 12-35　トラップマネージャーの設定 (SNMPv3)



設定済みのトラップマネージャーを表示するには：

1. [Administration]、[SNMP]をクリックします。
2. [Step]リストから[Configure Trap]を選択します。
3. [Action]リストから[Show]を選択します。

図 12-36　トラップマネージャーの表示



12.4.10 SNMP 通知ログの作成

SNMP 通知ログを作成するには、[Administration]> [SNMP（通知フィルタの設定 - 追加）]ページを使用します。

コマンドの使用方法

- SNMP をサポートするシステムでは、再送信の制限を超えている可能性のあるトラップや情報があるかどうかにかかわらず、通知情報を紛失通知に対する記録として記録するメカニズムが必要になることがあります。通知ログ MIB(NLM、RFC 3014)は、他の MIB からの情報が記録されるインフラを提供します。
- NLM によって提供されるサービスが提供されると、個々の MIB は通知メッセージが失われる可能性を考慮して、イベントに関連する過渡情報を記録する責任を負うことが少なくなり、アプリケーションはログをポーリングして、 重要な通知が抜けていないかについて確認します。
- 通知ロギングが設定されていない場合、スイッチの再起動時に、一部の SNMP トラップ（ウォームスタートなど）をログに記録できません。

- この問題を回避するには、この章で説明するように通知ロギングを設定し、このコマンドを[System]>[File（コピー実行中の設定）]ページを使用してスタートアップコンフィグレーションファイルに保存します。(「3.5.2　ローカルファイルへのランニングコンフィグレーションの保存」を参照してください。）スイッチリブート時に、SNMP トラップ(ウォームスタート等)に記録できるようになります。
- RFC 3014 で使用されたデフォルト設定をベースに、通知ログには最大 256 エントリを含むことができます。そして、エントリエージングタイムは 1440 分です。通知ログに記録された情報とエントリエージングタイムは、ネットワーク管理端末からの SNMP を使用してのみ、設定することができます。
- [Administration]＞[SNMP（Configure Trap - Add）]ページを使用してトラップホストを作成すると、デフォルトの通知フィルタが作成されます。

パラメータ

次のパラメータが表示されます。

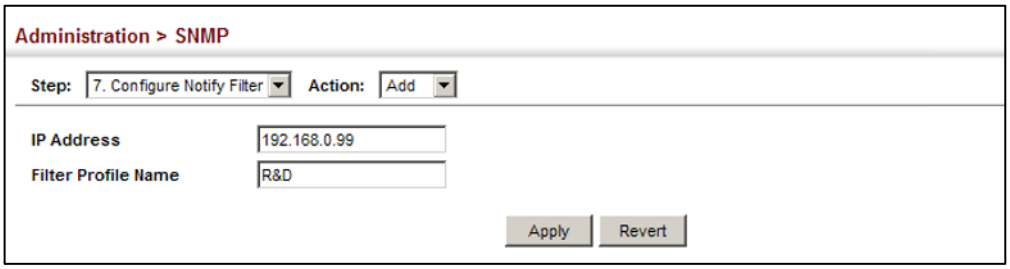
- IP Address - リモートデバイスの IPv4 または IPv6 アドレスです。指定されたターゲットホストは、[Administration]> [SNMP（Configure Trap - Add）]ページを使用して設定済みでなければなりません。通知ログはローカルで保存します。リモートデバイスには送信されません。このリモートホストパラメータは、SNMP 通知 MIB の必須フィールドを完了させる場合のみ必要となります。
- Filter Profile Name - 通知ログプロファイル名です。(範囲: 1 から 32 文字)

Web インタフェース

通知ログプロファイル名です。

1. [Administration]、[SNMP]をクリックします。
2. [Step]リストから[Configure Notify Filter]を選択します。
3. [Action]リストから[Add]を選択します。
4. 設定されたトラップマネージャーの IP アドレスとフィルタプロファイル名を入力します。
5. [Apply]をクリックします。

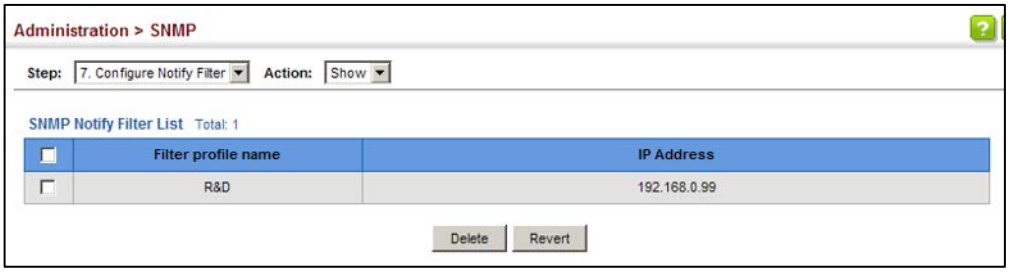
図 12-37　SNMP 通知ログの作成



設定済みの SNMP 通知ログを表示するには：

1. [Administration]、[SNMP]をクリックします。
2. [Step]リストから[Configure Notify Filter]を選択します。
3. [Action]リストから[Show]を選択します。

図 12-38　SNMP 通知ログの表示



12.4.11 SNMP 統計情報の表示

[Administration]> [SNMP（Show Statistics）]ページを使用して、SNMP 入力および出力プロトコルデータユニットのカウンタを表示します。

パラメータ

次のカウンタが表示されます。

- SNMP packets input - トランスポートサービスから SNMP エンティティに配信されたメッセージの合計数です。
- Bad SNMP version errors - SNMP エンティティに配信され、サポートされていない SNMP バージョン用の SNMP メッセージの総数です。
- Unknown community name - エンティティに知られていない SNMP コミュニティ名を使用した SNMP エンティティに配信された SNMP メッセージの総数です。
- Illegal operation for community name supplied - メッセージで指定された SNMP コミュニティによって許可されていない SNMP 操作を表す SNMP エンティティに配信された SNMP メッセージの総数です。
- Encoding errors - 受信した SNMP メッセージをデコードする際に SNMP エンティティが検出した ASN.1 または BER エラーの合計数です。
- Number of requested variables - 有効な SNMP Get-Request および Get-Next PDU を受信した結果、SNMP プロトコルエンティティによって正常に取得された MIB オブジェクトの総数です。
- Number of altered variables - 有効な SNMP Set-Request PDU を受信した結果、SNMP プロトコルエンティティによって正常に変更された MIB オブジェクトの総数です。
- Get-request PDUs - SNMP プロトコルエンティティによって受け入れられて処理された、または生成された SNMP Get-Request PDU の総数です。
- Get-next PDUs - SNMP プロトコルエンティティによって受け入れられて処理または生成された SNMP Get-Next PDU の総数です。
- Set-request PDUs - SNMP プロトコルエンティティによって受け入れられて処理された、または生成された SNMP Set-Request PDU の総数です。
- SNMP packets output - SNMP プロトコルエンティティからトランスポートサービスに渡された SNMP メッセージの総数です。
- Too big errors - SNMP プロトコルエンティティによって生成され、エラーステータスフィールドの値が“tooBig.”である SNMP PDU の総数です。
- No such name errors - SNMP プロトコルエンティティに配信された、または SNMP プロトコルエンティティによって生成され、エラーステータスフィールドの値が“noSuchName”である SNMP PDU の総数です。
- Bad values errors - SNMP プロトコルエンティティに配信された、または SNMP プロトコルエンティ

ティによって生成された、エラーステータスフィールドの値が“badValue”である SNMP PDU の総数です。

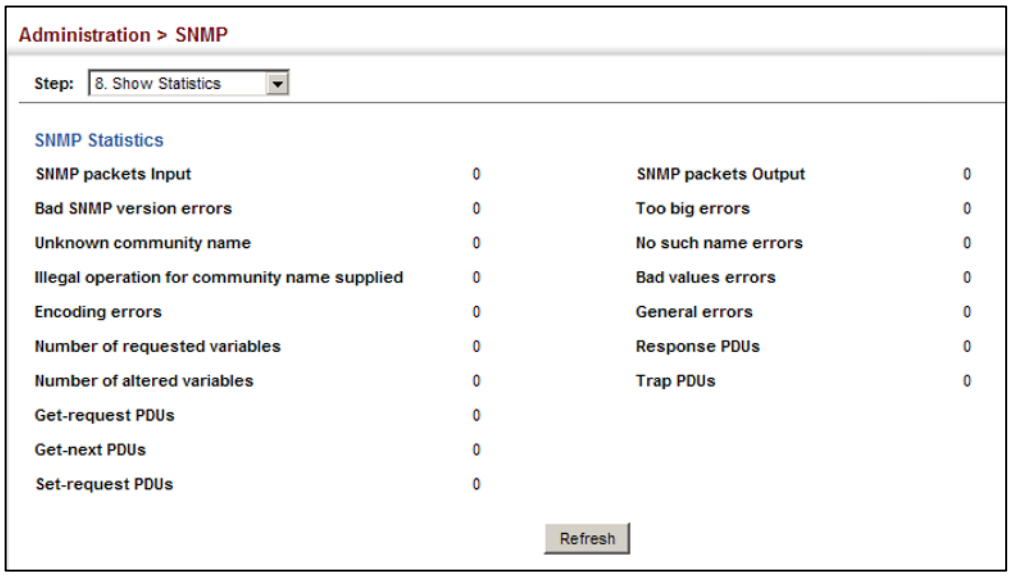
- General errors - SNMP プロトコルエンティティに配信された、または SNMP プロトコルエンティティによって生成され、エラーステータスフィールドの値が“genErr”である SNMP PDU の総数です。
- Response PDUs - SNMP プロトコルエンティティによって受け入れられ、処理された、または SNMP プロトコルエンティティによって生成された SNMP Get-Response PDU の総数です。
- Trap PDUs - SNMP プロトコルエンティティによって受け入れられ、処理された、または SNMP プロトコルエンティティによって生成された SNMP トラップ PDU の総数です。

Web インタフェース

SNMP 統計を表示するには：

1. [Administration]、[SNMP]をクリックします。
2. [Step]リストから[Show Statistics]を選択します。

図 12-39　SNMP 統計情報の表示



12.5 RMON

リモート監視により、リモートデバイスは情報の収集や独立した基準で特定のイベントに応答することができます。このスイッチは RMON 対応デバイスであり、幅広いタスクを独立して実行できるため、ネットワーク管理トラフィックを大幅に削減することができます。診断を継続して実行し、ネットワークパフォーマンスに関する情報を記録できます。イベントがトリガされると、自動的にネットワーク管理者に障害を通知し、イベントに関する履歴情報を提供することができます。管理エージェントに接続できない場合は指定されたタスクの実行を継続し、次に連絡を受けたときに管理端末にデータを戻します。

スイッチは、Statistics、History、Event、Alarm の各グループで構成されるミニ RMON をサポートしています。RMON が有効になると、システムは物理インタフェースに関する情報を徐々に構築し、この情報を関連する RMON データベースグループに格納します。管理エージェントは、SNMP プロトコルを使用してスイッチと定期的に通信します。ただし、スイッチが重大なイベントに遭遇した場合、スイッチは管理エージェントに自動的にトラップメッセージを送信できます。トラップメッセージが設定されていれば、イベントに応答することができます。

12.5.1 RMON アラームの設定

[Administration]> [RMON（Configure Global - Add - Alarm）]ページを使用して、応答イベントを生成する特定の基準を定義します。アラームは、任意の指定された時間間隔でデータをテストするように設定でき、絶対値または変更値（統計カウンタが特定の値に達するか、一定の間隔で一定量だけ変化する統計値など）を監視できます。アラームは、上昇または下降閾値に応答するように設定できます。ただし、アラームがトリガされた後は、統計値が反対の境界閾値を超えてからトリガ閾値を超えて戻されるまで、再度トリガされません。

コマンドの使用方法

- インデックスにアラームがすでに定義されている場合は、変更を行う前にそのエントリを削除する必要があります。

パラメータ

次のパラメータが表示されます。

- Index - このエントリのインデックスです。(範囲: 1 から 65535)
- Variable - サンプリングされる MIB 変数のオブジェクト識別子です。etherStatsEntry.n.n の変数のみがサンプリングされます。
  etherStatsEntry.n は MIB 変数を一意に定義し、etherStatsEntry.n.n は MIB 変数と etherStatsIndex を定義します。たとえば、1.3.6.1.2.1.16.1.1.1.6.1 は etherStatsBroadcastPkts と etherStatsIndex の 1 を示します。
- Interval - ポーリング間隔です。(範囲: 1 から 65535 秒)
- Sample Type - 指定された変数の絶対または相対変化をテストします。
  - Absolute - この変数は、サンプリング期間の終わりに閾値と直接比較されます。
  - Delta - 最後のサンプルが現在の値から減算され、その差が閾値と比較されます。
- Rising Threshold - 現在の値が上昇閾値以上で、最後のサンプル値がこの閾値よりも小さい場合は、アラームが生成されます。上昇イベントが生成された後、サンプリングされた値が上昇閾値を下回って下降閾値に達し、再び上昇閾値に戻るまで、別のイベントは生成されません。(範囲: 0 から 2147483647)
- Rising Event Index - アラームが、監視された変数が上昇閾値を超えているか交差している場合に使用するイベントのインデックスです。イベント制御テーブルに対応するエントリが無い場合には、イベ

ントは生成されません。(範囲: 0 から 65535)

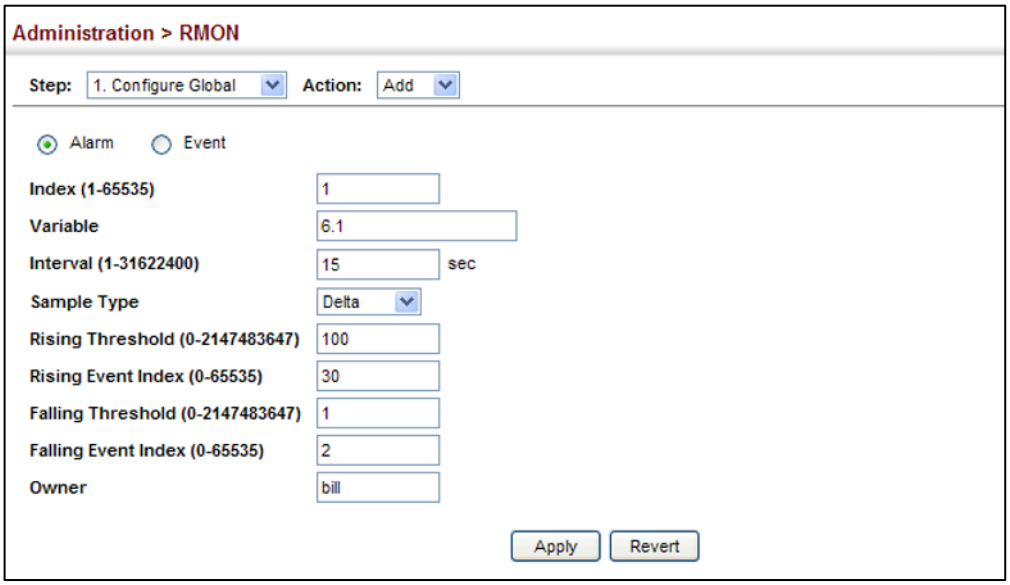
- Falling Threshold - 現在の値が下降閾値以下で、最後のサンプル値がこの閾値より大きい場合、アラームが生成されます。下降イベントが生成された後、サンプリングされた値が下降閾値を上回って上昇閾値に達し、再び下限閾値に戻るまで、別のイベントは生成されません。(範囲: 0 から 2147483647)
- Falling Event Index - 監視されている変数が下限閾値を下回ったり下がったりすることによってアラームがトリガされた場合に使用するイベントのインデックスです。イベント制御テーブルに対応するエントリが無い場合には、イベントは生成されません。(範囲: 0 から 65535)
- Owner - このエントリを作成した人の名前です。(範囲: 1 から 32 文字)

Web インタフェース

RMON アラームを設定するには：

1. [Administration]、[RMON]をクリックします。
2. [Step]リストから[Configure Global]を選択します。
3. [Action]リストから[Add]を選択します。
4. [Alarm]をクリックします。
5. インデックス番号、ポーリングする MIB オブジェクト（etherStatsEntry.n.n）、ポーリング間隔、サンプルタイプ、閾値、トリガするイベントを入力します。
6. [Apply]をクリックします。

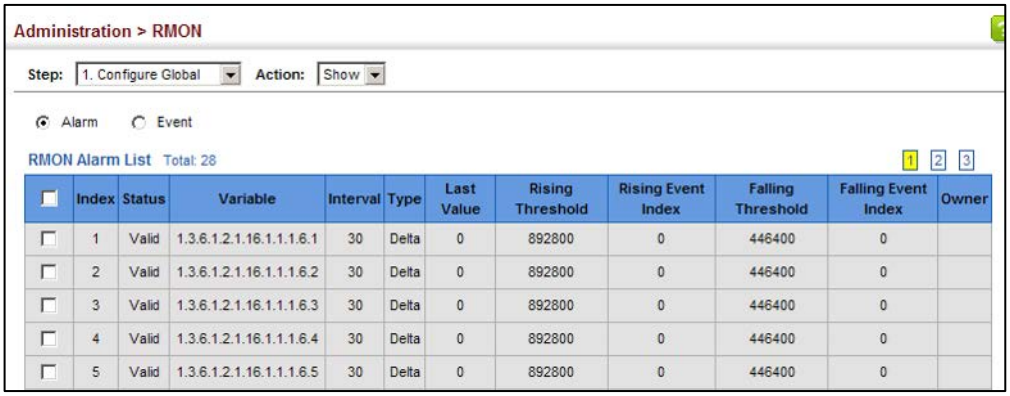
図 12-40　RMON アラームの設定



設定済みの RMON アラームを表示:

1. [Administration]、[RMON]をクリックします。
2. [Step]リストから[Configure Global]を選択します。
3. [Action]リストから[Show]を選択します。
4. [Alarm]をクリックします。

図 12-41　設定済みの RMON アラームの表示



Index	Status	Variable	Interval	Type	Last Value	Rising Threshold	Rising Event Index	Falling Threshold	Falling Event Index	Owner
1	Valid	1.3.6.1.2.1.16.1.1.1.6.1	30	Delta	0	892800	0	446400	0	
2	Valid	1.3.6.1.2.1.16.1.1.1.6.2	30	Delta	0	892800	0	446400	0	
3	Valid	1.3.6.1.2.1.16.1.1.1.6.3	30	Delta	0	892800	0	446400	0	
4	Valid	1.3.6.1.2.1.16.1.1.1.6.4	30	Delta	0	892800	0	446400	0	
5	Valid	1.3.6.1.2.1.16.1.1.1.6.5	30	Delta	0	892800	0	446400	0	

12.5.2 RMON イベントの設定

[Administration]> [RMON（Configure Global - Add - Event）]ページを使用して、アラームがトリガされたときに実行する操作を設定します。応答には、アラームの記録やトラップマネージャーへのメッセージの送信が含まれます。アラームとそれに対応するイベントは、重要なネットワークの問題に即座に対応する方法を提供します。

コマンドの使用方法

- インデックスにアラームがすでに定義されている場合は、変更を行う前にそのエントリを削除する必要があります。
- 1 つのデフォルトイベントは、次のように構成されます。
  event Index = 1
  Description: RMON_TRAP_LOG
  Event type: log & trap
  Event community name is public
  Owner is RMON_SNMP

パラメータ

次のパラメータが表示されます。

- Index - このエントリのインデックスです。(範囲: 1 から 65535)
- Type - 開始するイベントのタイプを指定します。
  - None - イベントは生成されません。
  - Log - イベントがトリガされたときに RMON ログエントリを生成します。イベントログの現在の設定内容にもとづいて処理されます（「12.1.1　システムログの設定」を参照してください）。
  - Trap - 設定されたすべてのトラップマネージャーにトラップメッセージを送信します。
  - Log and Trap - イベントを記録し、トラップメッセージを送信します。
- Description - このイベントを説明するコメントです。(範囲: 1 から 127 文字)
- Owner - このエントリを作成した人の名前です。(範囲: 1 から 32 文字)

Web インタフェース

RMON イベントを設定するには：

1. [Administration]、[RMON]をクリックします。

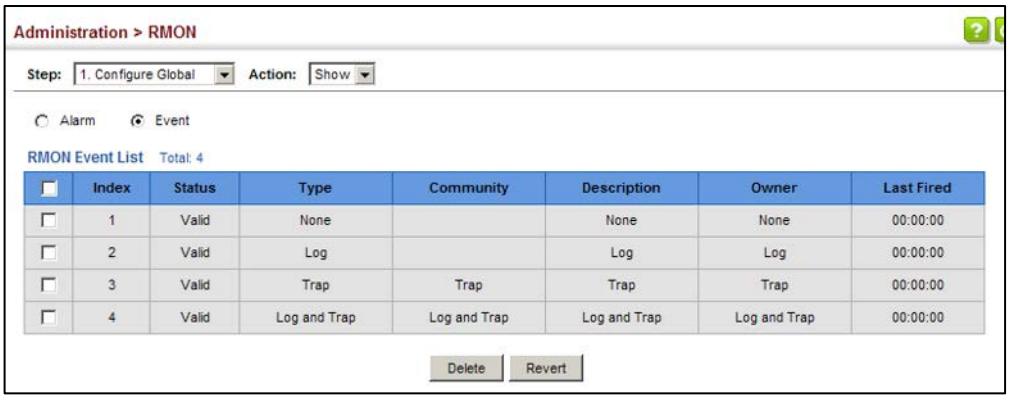
2. [Step]リストから[Configure Global]を選択します。
3. [Action]リストから[Add]を選択します。
4. [Event]をクリックします。
5. インデックス番号、開始するイベントのタイプ、トラップメッセージで送信するコミュニティストリング、このイベントを作成した人物の名前、およびイベントの簡単な説明を入力します。
6. [Apply]をクリックします。

図 12-42　RMON イベントの設定

設定済みの RMON イベントを表示する:

1. [Administration]、[RMON]をクリックします。
2. [Step]リストから[Configure Global]を選択します。
3. [Action]リストから[Show]を選択します。
4. [Event]をクリックします。

図 12-43　設定済みの RMON イベントの表示



12.5.3 RMON 履歴サンプルの設定

[Administration]> [RMON（Configure Interface - Add - History）]ページを使用して、物理インタフェースの統計情報を収集して、ネットワーク使用率、パケットタイプ、およびエラーをモニタします。断続的な問題を追跡するために、過去の活動記録を使用することができます。この記録は、通常のベースライン活動を確立するために使用することができ、高いトラフィックレベル、ブロードキャストストーム、またはその他の異常なイベントに関連する問題を明らかにする可能性があります。また、ネットワークの成長を予測し、ネットワークが過負荷になる前に拡張計画を立てるために使用することもできます。

コマンドの使用方法

◆　各インデックス番号は、スイッチ上のポートに相当します。

- 履歴収集がすでにインタフェースで有効になっている場合は、変更を行う前にエントリを削除する必要があります。
- 各サンプルに対して収集した情報には、以下が含まれます:
  入力オクテット、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、アンダーサイズパケット、オーバーサイズパケット、フラグメント、ジャバー、CRC アラインメントエラー、衝突、ドロップイベント、およびネットワーク使用率。
  [Show Details]ページに表示される統計の説明は、「4.1.4　ポートまたはトランク統計情報の表示」を参照してください。
- スイッチは各ポートに 2 つのインデックスエントリを予約します。追加ページを使用してデフォルトのインデックスエントリが別のポートに再割当てされた場合、このインデックスは通常割当てられているポートの[Show]または[Show Details]ページに表示されません。たとえば、コントロールエントリ 15 がポート 5 に割当てられている場合、このインデックスエントリはポート 8 の[Show]または[Show Details]ページから削除されます。

パラメータ

次のパラメータが表示されます。

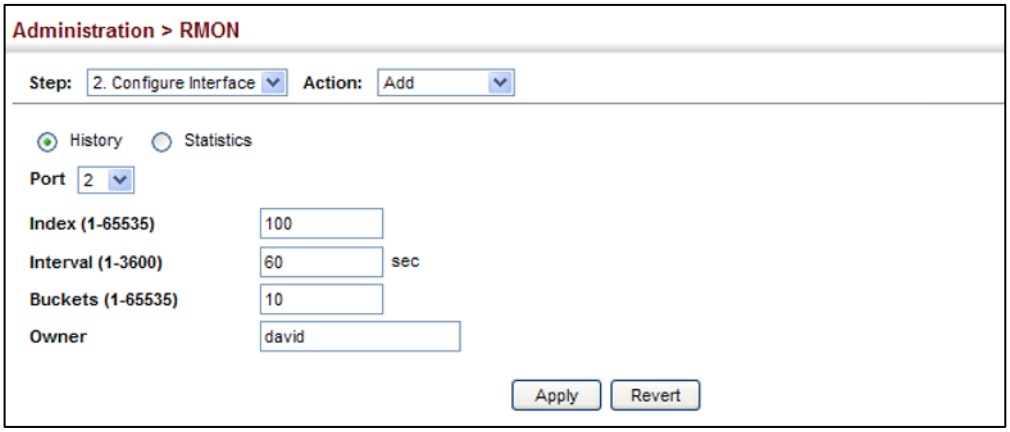
- Port - スイッチ上のポート番号です。
- Index - このエントリのインデックスです。(範囲: 1 から 65535)
- Interval - ポーリング間隔です。(範囲: 1 から 3600 秒; デフォルト: 1800 秒)
- Buckets - このエントリに要求されたバケットの数です。(範囲: 1 から 65536、デフォルト: 8)
  付与されたバケットの数は、表示ページに表示されます。
- Owner - このエントリを作成した人の名前です。(範囲: 1 から 32 文字)

Web インタフェース

ポート上の統計情報を定期的にサンプリングするには :

1. [Administration]、[RMON]をクリックします。
2. [Step]リストから[Configure Interface]を選択します。
3. [Action]リストから[Add]を選択します。
4. [History]をクリックします。
5. リストからデータ送信元としてポートを選択します。
6. インデックス番号、サンプリング間隔、使用するバケットの数、およびこのエントリの所有者の名前を入力します。
7. [Apply]をクリックします。

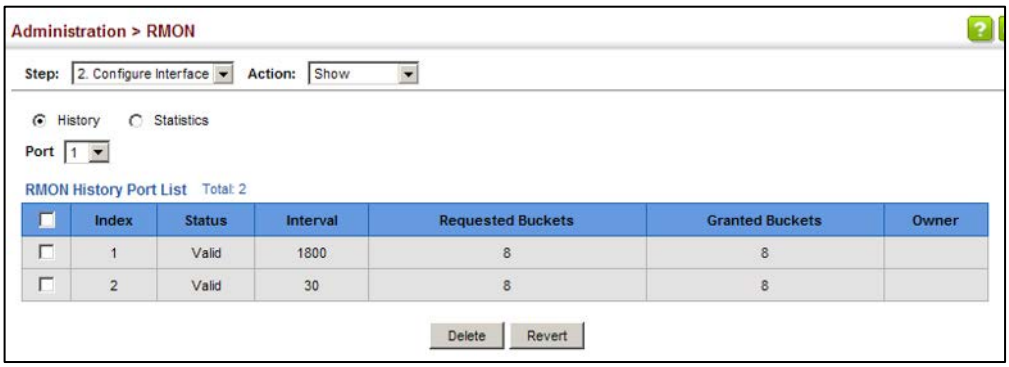
図 12-44　RMON 履歴サンプルの設定



設定済みの RMON 履歴サンプルを表示する:

1. [Administration]、[RMON]をクリックします。
2. [Step]リストから[Configure Interface]を選択します。
3. [Action]リストから[Show]を選択します。
4. リストからポートを選択します。
5. [History]をクリックします。

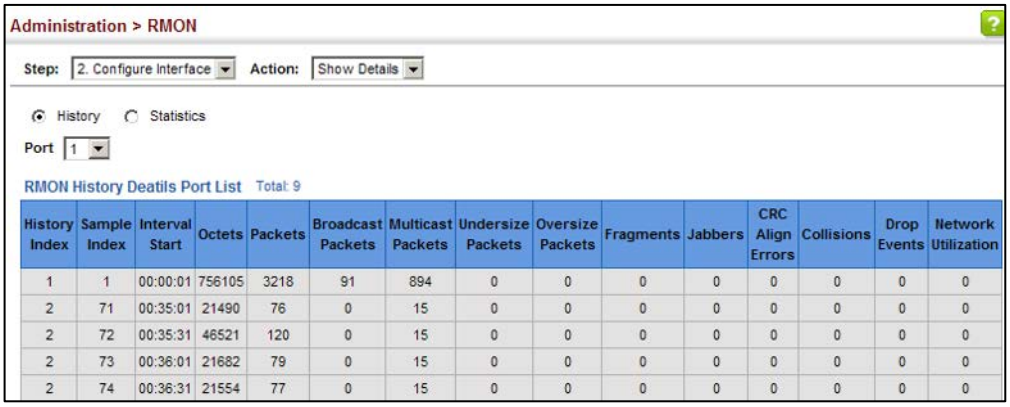
図 12-45　設定済みの RMON 履歴サンプルの表示



収集された RMON 履歴サンプルを表示するには、

1. [Administration]、[RMON]をクリックします。
2. [Step]リストから[Configure Interface]を選択します。
3. [Action]リストから[Show Details]を選択します。
4. リストからポートを選択します。
5. [History]をクリックします。

図 12-46　収集された RMON 履歴サンプルの表示



History Index	Sample Index	Interval Start	Octets	Packets	Broadcast Packets	Multicast Packets	Undersize Packets	Oversize Packets	Fragments	Jabbers	CRC Align Errors	Collisions	Drop Events	Network Utilization
1	1	00:00:01	756105	3218	91	894	0	0	0	0	0	0	0	0
2	71	00:35:01	21490	76	0	15	0	0	0	0	0	0	0	0
2	72	00:35:31	46521	120	0	15	0	0	0	0	0	0	0	0
2	73	00:36:01	21682	79	0	15	0	0	0	0	0	0	0	0
2	74	00:36:31	21554	77	0	15	0	0	0	0	0	0	0	0

12.5.4 RMON 統計サンプルの設定

[Administration]> [RMON（Configure Interface – Add - Statistics）]ページを使用してポートの統計情報を収集し、一般的なエラーおよび全体的なトラフィックレートをネットワークで監視することができます。

コマンドの使用方法

- 統計収集がすでにインタフェース上で使用可能になっている場合は、変更を行う前にその項目を削除する必要があります。
- 各サンプルに対して収集した情報には、以下が含まれます:
  オーバーサイズパケット、CRC アライメントエラー、ジャバー、フラグメント、コリジョン、ドロップイベント、および様々なサイズのフレーム。

パラメータ

次のパラメータが表示されます。

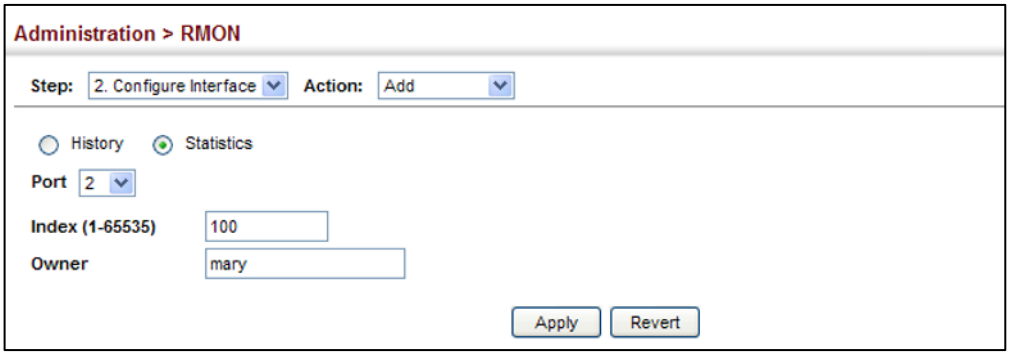
- Port - スイッチ上のポート番号です。
- Index - このエントリのインデックスです。(範囲: 1 から 65535)
- Owner - このエントリを作成した人の名前です。(範囲: 1 から 32 文字)

Web インタフェース

ポートの統計情報を定期的にサンプリングできるようにするには：

1. [Administration]、[RMON]をクリックします。
2. [Step]リストから[Configure Interface]を選択します。
3. [Action]リストから[Add]を選択します。
4. [Statistics]をクリックします。
5. リストからデータ送信元としてポートを選択します。
6. インデックス番号と、このエントリの所有者の名前を入力します
7. [Apply]をクリックします。

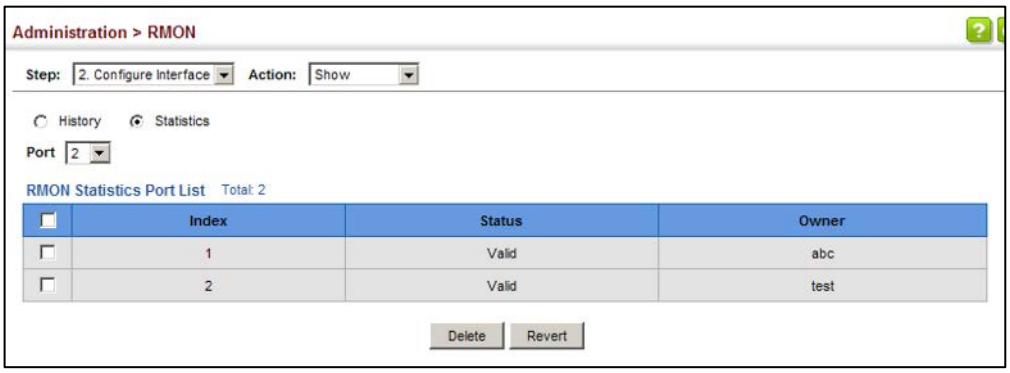
図 12-47　RMON 統計サンプルの設定



設定済みの RMON 統計サンプルを表示するには:

1. [Administration]、[RMON]をクリックします。
2. [Step]リストから[Configure Interface]を選択します。
3. [Action]リストから[Show]を選択します。
4. リストからポートを選択します。
5. [Statistics]をクリックします。

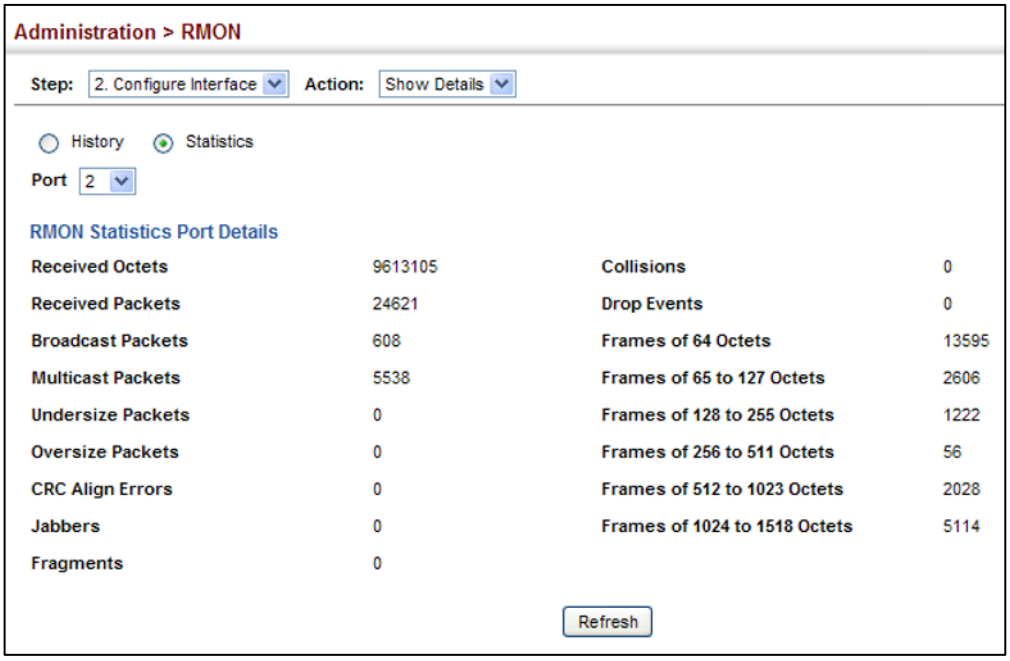
図 12-48　設定済みの RMON 統計サンプルの表示



収集された RMON 統計サンプルを表示するには：

1. [Administration]、[RMON]をクリックします。
2. [Step]リストから[Configure Interface]を選択します。
3. [Action]リストから[Show Details]を選択します。
4. リストからポートを選択します。
5. [Statistics]をクリックします。

図 12-49　収集された RMON 統計サンプルの表示



12.6 時間範囲の設定

[Administration]> [Time Range]ページを使用して、適用された ACL や PoE など、さまざまな機能が適用される時間範囲を設定します。

コマンドの使用方法

- 同じ時間範囲に絶対時間ルールと複数の定期ルールの両方が設定されている場合には(例; 名前付きエントリ)、現在の時間が絶対時間範囲と定期的時間範囲の中にある場合のみ、このエントリが有効となります。
- 時間範囲には、最大 8 つのルールを設定することができます。

パラメータ

次のパラメータが表示されます。

追加

- Time-Range Name - 時間範囲の名前です。(範囲: 1 から 32 文字)

ルールを追加

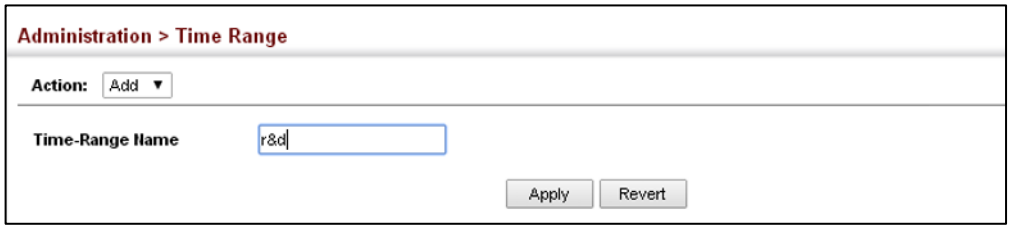
- Time-Range - 時間範囲の名前です。
- モード
  - Absolute - 特定の時刻または時間範囲を指定します。
    - Start/End - 開始または終了する時間、分、月、日、年を指定します。
  - Periodic - 定期的な間隔を指定します。
    - Start/To - 開始または終了する曜日、時間、および分の曜日を指定します。

Web インタフェース

時間範囲を設定するには：

1. [Administration]、[Time Range]をクリックします。
2. [Action]リストから[Add]を選択します。
3. 時間範囲の名前を入力します。
4. [Apply]をクリックします。

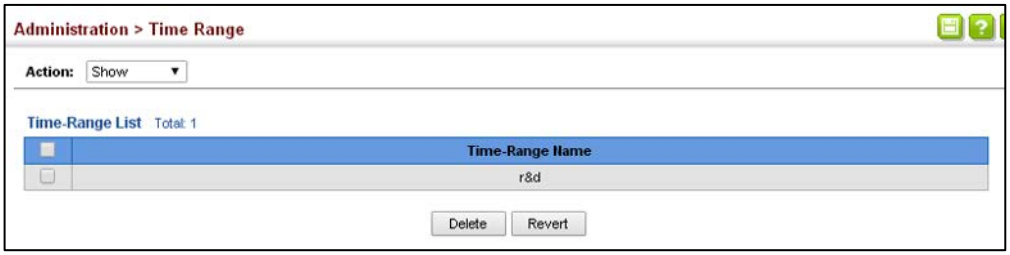
図 12-50　時間範囲の名前の設定



時間範囲の一覧を表示するには：

1. [Administration]、[Time Range]をクリックします。
2. [Action]リストから[Show]を選択します。

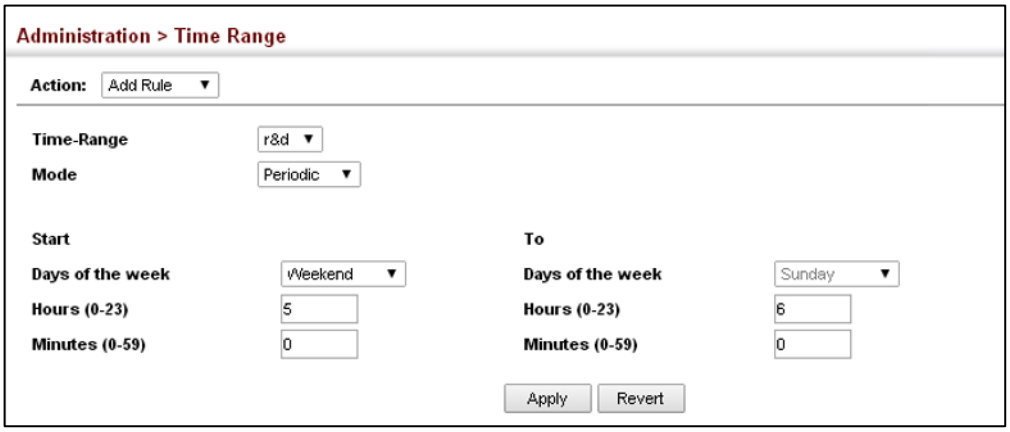
図 12-51　時間範囲のリストを表示



時間範囲のルールを設定するには：

1. [Administration]、[Time Range]をクリックします。
2. [Action]リストから[Add Rule]を選択します。
3. ドロップダウンリストから時間範囲の名前を選択します。
4. [Absolute]または[Periodic]のモードオプションを選択します。
5. 選択したモードに必要なパラメータを入力します。
6. [Apply]をクリックします。

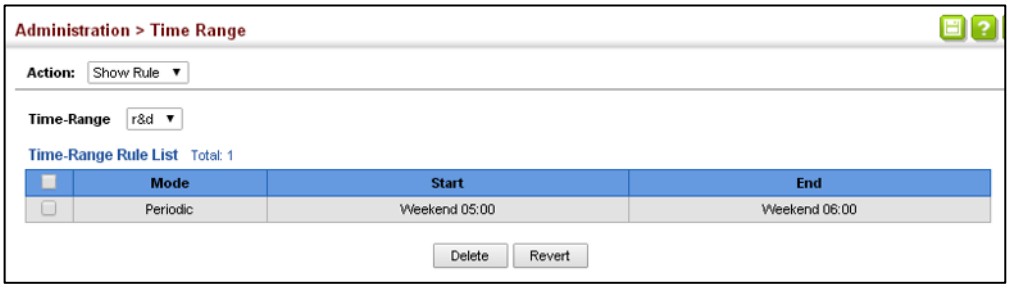
図 12-52　時間範囲にルールを追加



時間範囲に対して設定されたルールを表示するには：

1. [Administration]、[Time Range]をクリックします。
2. [Action]リストから[Show Rule]を選択します。

図 12-53　時間範囲に対して設定されたルールの表示



12.7 ループ検知の設定

スイッチは、ハードウェア問題や工場出荷時のプロトコル設定が原因の一般的なループバック状態を検出するよう、設定することができます。ループバック検出（LBD）が有効の場合、参加するポートで制御フレームが送信され、スイッチはインバウンドトラフィックを監視して、フレームがループバックされているかどうかを確認します。

使用上のガイドライン

- 制御フレームの送信間隔をデフォルト設定に調整し、特定の環境のパフォーマンスを向上させることができます。ループバックされているパケットの種類を判断する場合、シャットダウンモードも変更する必要があります。
- 本章で説明するコマンドによって提供される一般的なループバック検出と、スパニングツリープロトコルによって提供されるループバック検出の両方を同時に有効にすることはできません。スパニングツリープロトコルでループバック検出が有効になっている場合には、同じインタフェース上で一般ループバック検出を有効にすることはできません。
- インタフェースまたはインタフェースがループバックイベントによりシャットダウン状態から解放された場合にループバックイベントが検出されると、トラップメッセージが送信され、システムログにイベントが記録されます。
- ループバック検出を有効にするには、ループバック検出をグローバルでもインタフェース上でも有効にする必要があります。
- インタフェースでループバックイベントが検出された後、自動的にインタフェースをシャットダウン状態から解放する設定が有効である場合、その監視タイマは装置起動もしくは Recover Time 設定を契機に装置共通で実行されます。そのため、ループバックイベント検出後の 1 回目の解放までの時間は設定値より短くなります。

12.7.1 ループ検知のグローバル設定

[Administration]> [LBD（Configure Global）]ページを使用して、ループバック検出をグローバルに有効にし、制御フレームを送信する間隔、インタフェースをシャットダウン状態から解除するまでの待機間隔、検出されたループバックに対する反応、および送信するトラップを設定します。

パラメータ

次のパラメータが表示されます。

- Global Status - スイッチ上でループバック検出をグローバルに有効にします。(デフォルト: Enabled)
- Transmit Interval - ループバック検出制御フレームを送信する間隔を指定します。(範囲: 1 から 32767 秒; デフォルト：10 秒)
- Recover Time - スイッチがシャットダウン状態からインタフェースを自動的に解放するまで待機する間隔を指定します。(範囲: 60 から 1,000,000 秒、または 0(自動回復無効)、デフォルト: 60 秒)
  ループバック検出モードが変更（有効または無効）されると、ループバック検出プロセスによってシャットダウン状態にされたポートは、残りの回復時間に関係なく、すぐに開放されます。
  復旧時間が有効になっていない場合（チェックボックスがオフの場合）、シャットダウン状態にあるすべてのポートは、Release ボタンを使用してシャットダウン状態を解除できます。特定のポートを復元するには、[Configure Interface]ページで[Admin State]を再度有効にします。
  回復時間は、ループが検出された後に回復がトリガされる最大時間です。回復と検出の間の実際の間隔は、回復時間以下になります。
- Action - ループバック状態が検出されたときにスイッチが行う保護動作を指定します。(オプション:

None, Shutdown; デフォルト：Shutdown)

- None - 措置はとられていません。
- Shutdown -ループバック検出への反応がポートをシャットダウンするように設定され、ポートはそれ自身で送信された制御フレームを受信すると、ポートがループ状態にあり、フレームペイロード内の VLAN も、間違った VLAN タグでループ状態になっていることを意味します。したがって、ループしたポートはシャットダウンされます。

ループバック検出への反応動作が変更されると、ループバック検出処理によってシャットダウン状態に置かれたポートは、残存の回復時間にかかわらず直ちに動作状態に復元されます。

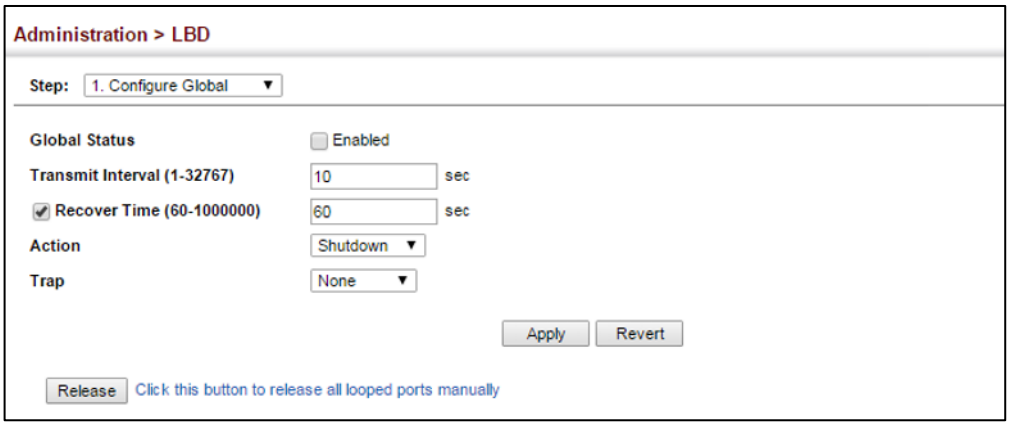
- Trap - ループバック状態が検出されたとき、またはスイッチがループバック状態から回復したときにトラップを送信します。(オプション: Both, Detect, None, Recover; デフォルト：None)
  - Both - ループバック状態が検出されたとき、またはスイッチがループバック状態から回復したときに SNMP トラップメッセージを送信します。
  - Detect - ループバック状態が検出されたときに SNMP トラップメッセージを送信します。
  - None - ループバック検出または回復時の SNMP トラップメッセージを送信しません。
  - Recover - スイッチがループバック状態から回復したときに SNMP トラップメッセージを送信します。
- Release - ループバック検出機能によって現在シャットダウンされているすべてのインタフェースを解放します。

Web インタフェース

LBD のグローバルを設定するには：

1. [Administration]、[LBD]、[Configure Global]の順にクリックします。
2. 必要な構成変更を行います。
3. [Apply]をクリックします。

図 12-54　LBD のグローバル設定



12.7.2 ループ検知のインタフェース設定

[Administration]> [LBD（Configure Interface）]ページを使用して、インタフェースでループバック検出を有効にし、ループバック動作ステート、およびループバックされた VLAN を表示します。

パラメータ

次のパラメータが表示されます。

- Port (範囲: 1 から 10)
- Trunk (範囲: 1-8)

◆ Admin State

◆ Operation State

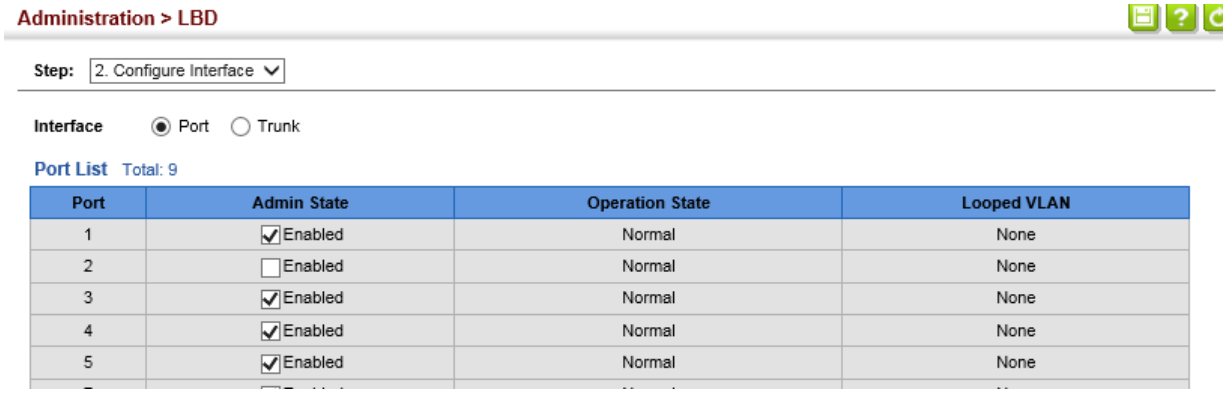
◆ Looped VLAN

Web インタフェース

LBD のインタフェースを設定するには：

1. [Administration]、[LBD]、[Configure Interface]の順にクリックします。
2. チェックボックスを変更し、ループバック検出を有効、または無効に設定します。
3. [Apply]をクリックします。

図 12-55　LBD のインタフェース設定



13 マルチキャストフィルタリング

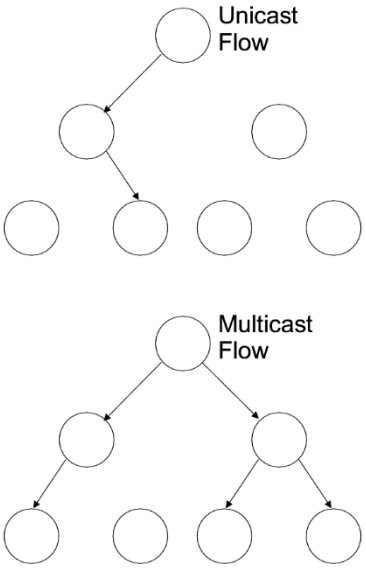
この章では、次のマルチキャストサービスを設定する方法について説明します。

- IGMP Snooping - IGMP snooping のパラメータを設定します。
- Filtering and Throttling - IGMP snooping においてインタフェースにフィルタを指定して加入するマルチキャストグループを制御したり、インタフェースで加入できるマルチキャストグループの最大数を制限します。
- MLD Snooping - MLD snooping のパラメータを設定します。
- MLD Filtering and Throttling - MLD snooping においてインタフェースにフィルタを指定して加入するマルチキャストグループを制御したり、インタフェースで加入できるマルチキャストグループの最大数を制限します。
- Filtering MLD Query Packets on an Interface - MLD Query メッセージを廃棄するようにインタフェースを設定します。

13.1 概要

マルチキャストは、ビデオ会議やストリーミングオーディオなどのリアルタイムアプリケーションをサポートするために使用されます。マルチキャスト送信者は、各受信者と別個の中継経路を確立する必要はありません。マルチキャスト送信者は、ネットワークにマルチキャストパケットを配信するだけで、ネットワーク内のマルチキャストスイッチ/ルータが、加入要求を送信するすべての受信者に中継します。このアプローチでは、マルチキャストサーバが必要とする中継制御処理の負荷が軽減されますが、マルチキャストパケットがマルチキャストグループに加入している受信者にのみ中継されるように、通過するすべてのマルチキャストスイッチ/ルータで配信されたマルチキャストパケットを注意深く制御する必要があります。

図 13-1 マルチキャストフィルタリングの概念



このスイッチは、インターネットグループ管理プロトコル（IGMP）を使用してマルチキャストパケットをフィルタリングする IGMP snooping をサポートしています。IGMP snooping では、受信者と IGMP 対応デバイス（一般的にはマルチキャストルータ）間で交換している加入/離脱要求を監視または解析することで、マルチキャストグループに加入するポートを検出し、それに従ってフィルタを設定します。

VLAN にマルチキャストルータが接続されていない場合、スイッチでマルチキャストパケットおよび IGMP Query メッセージが受信されない可能性があります。この場合、IGMP snooping では IGMP クエリア機能を使用して、特定のマルチキャストパケットを受信するかどうかを受信者に問い合わせることができます。これにより、IGMP クエリアは、マルチキャストグループに加入するポートを検出し、それらのポートにのみマルチキャストパケットを中継します。その後、隣接するマルチキャストスイッチ/ルータに加入要求を中継し、マルチキャストパケットを継続して受信できるようにします。

これにより、マルチキャストフィルタリングは、当該マルチキャストパケットを受信者およびマルチキャストルータ/スイッチだけに中継することで、VLAN 内にマルチキャストパケットがフラッディングされることを抑制し、通信帯域を節約することでネットワークパフォーマンスの最適化を行います。

Note: IGMP snooping と MLD snooping を同時に使用する場合、最大エントリ数は IGMP snooping と MLD snooping の合計で 511 エントリになります。

Note: IGMPv3 snooping と MLDv2 snooping では ASM(any-source multicast)だけをサポートします(SSM (source-specific multicast)は未サポート)。そのため、送信元アドレスを指定した IGMPv3 Report メッ

セージおよび MLDv2 Report メッセージを受信した場合、当該 Report メッセージではエントリを生成しません。

13.2 IGMP snooping

ネットワーク内の他のスイッチでマルチキャストルーティングがサポートされていない場合は、IGMP snooping および IGMP クエリアを使用して、マルチキャスト受信者とマルチキャストルータ/スイッチ間を通過する IGMP Report メッセージを監視し、マルチキャストパケットを中継する必要のあるポートを Dynamic に設定できます。これにより、当該マルチキャストグループに加入要求を行っていない受信者への中継が抑止されるため、VLAN 内の帯域幅を節約することができます。マルチキャストルーティングをサポートしていないスイッチ、または VLAN 内の他のスイッチでマルチキャストルーティングがすでに有効になっている場合、IGMP snooping はマルチキャストフィルタリングをサポートするために必要な唯一のサービスです。

IGMPv3 snooping を使用する際、IGMP バージョン 1, 2 または 3 受信者から要求されるすべてのサービスが、IGMPv3 Report メッセージとして上流のルータに転送されます。IGMPv3 snooping によって提供される主な拡張点は、IGMPv3 受信者がマルチキャスト送信元を特定して加入または離脱を行えることです。IGMPv1 / v2 受信者の場合、マルチキャスト送信元のアドレスは常に Null です（すべての送信元が受け入れ可能であることを示します）。IGMPv3 受信者の場合は、加入要求に特定のマルチキャスト送信元のアドレスを設定することができます。スイッチは、受信者からの特定の送信元を指定しない加入要求を受信した場合(IGMPv1 および v2 の加入要求。スイッチ上で静的に送信元が設定されていないときに限る)、マルチキャストグループ情報だけを管理し、特定の送信元を指定する加入要求を受信した場合、マルチキャストグループと送信元情報を管理します。

IGMPv3 受信者のみが特定のマルチキャスト送信元からのマルチキャストパケットを要求できます。受信者が特定の送信元を指定してマルチキャストパケットを要求すると、これらの送信元はすべて Include リストに設定され、当該送信元からのマルチキャストパケットを受信者に中継します。また、指定された送信元以外の送信元からのマルチキャストパケットを要求することもできます。この場合、送信元は Exclude リストに設定され、設定された送信元以外のすべてのマルチキャストパケットを受信者に中継します。

Note: スイッチが IGMPv3 snooping を使用するように設定されている場合、各 VLAN で検出された IGMP Query メッセージのバージョンに応じて、IGMP バージョンがバージョン 2 またはバージョン 1 にダウングレードされる可能性があります。

Note: IGMP snooping は、スイッチ上でマルチキャストルータポートが有効にされていないと機能しません。これは 2 つの方法のいずれかで達成できます。Static マルチキャストルータポートは手動で設定できます。この方法を使用すると、マルチキャストルータポートはタイムアウトすることはなく、明示的に削除されるまで機能し続けます。もう 1 つの方法は、ポート上でマルチキャストルーティングプロトコルパケットまたは IGMP Query メッセージが検出されたときに、スイッチがマルチキャストルータポートを Dynamic に作成します。

Note: IGMP snooping は最大 511 マルチキャストエントリを維持できます。最大数に達すると、新しいエントリは学習されません。なお、マルチキャストエントリ数は、IGMP snooping と MLD snooping との合算値で制御します。この場合、当該マルチキャストパケットは Unregistered-flooding が無効（デフォルト動作）で、VLAN にマルチキャストルータポートが設定されていない場合は廃棄され、Unregistered-flooding が有効の場合はフラッディングされます。

Static IGMP Router Interface - IGMP snooping が IGMP クエリア（マルチキャストルータ/スイッチ）を検出できない場合は、既知の IGMP クエリアが接続されているインタフェース(マルチキャストルータポート)を Static に指定できます。このインタフェースには、すべてのマルチキャストパケットを中継します。

Static IGMP Host Interface - マルチキャストアプリケーションをスイッチの特定のインタフェースに手動で割当てることができます。

IGMP Snooping with Proxy Reporting - スイッチは、Last Leave と Query Suppression をサポートします（DSL Forum TR-101、2006 年 4 月で定義されています)。

- プロキシ機能が無効の場合、スイッチが受信したすべての IGMP Report メッセージは、ネイティブでアップストリームマルチキャストルータに転送されます。
- Last Leave: 受信者からの IGMP Leave メッセージを要約します。IGMP Leave メッセージは、最後の受信者がマルチキャストグループを離れるときにのみアップストリームで中継されます。
- Query Suppression: IGMP Query メッセージをインターセプトして処理し、IGMP Specific Query メッセージがクライアントポートに送信されないようにします。

TR-101 からの唯一の逸脱は、R-250 で定義されているように、スイッチによって開始された IGMP トラフィックのマーキングが優先ビットでサポートされていないことです。

13.2.1 IGMP snooping の設定

[Multicast]> [IGMP Snooping]> [General]ページを使用して、マルチキャストトラフィックをインテリジェントに転送するようにスイッチを設定します。IGMP Query メッセージおよび IGMP Report メッセージにもとづいて、スイッチはマルチキャストトラフィックを要求するポートにのみマルチキャストトラフィックを転送します。これにより、スイッチがトラフィックをすべてのポートにブロードキャストすることがなくなり、ネットワークのパフォーマンスが低下することを防止します。

コマンドの使用方法

- IGMP Snooping - このスイッチは、IP マルチキャストルータ/スイッチと IP マルチキャストホストグループ間で転送された IGMP Query および Report メッセージを解析して、グループ情報を取り出し、それに応じてマルチキャストフィルタを設定します。

Note: 未学習のマルチキャストトラフィックがマルチキャストルータポートを設定した VLAN に受信すると、トラフィックはそのマルチキャストルータポートに転送されます。ただし、VLAN にマルチキャストルータポートが存在しない場合、Unregistered-flooding が無効の場合（デフォルト動作）は、トラフィックがドロップされます（Unregistered-flooding が有効の場合は VLAN 全体にフラッディングされます） 。

- IGMP Querier - ルータまたはマルチキャスト対応スイッチは、マルチキャストトラフィックを受信するかどうかを定期的に受信者に問い合わせることができます。IP マルチキャストを実行する LAN 上に複数のルータ/スイッチが存在する場合、これらのデバイスの 1 つが「クエリア」に選出され、グループメンバーに問い合わせる役割を引き受けます。

Note: マルチキャストルータは、DVMRP または PIM などのマルチキャストルーティングプロトコルとともに、IGMP snooping および IGMP Query、Report メッセージの情報を使用して、インターネット上の IP マルチキャストをサポートします。

パラメータ

次のパラメータが表示されます。

- IGMP Snooping Status - 有効にすると、グローバルに IGMP snooping を有効にします。(デフォルト: Disabled)

IGMP snooping がグローバルに有効の場合、IGMP snooping の VLAN 単位のインタフェース設定が優先されます。
IGMP snooping をグローバルに無効にすると、VLAN インタフェースごとに IGMP snooping を設定できますが、IGMP snooping がグローバルに再び有効にされるまで、インタフェース設定は有効になりません。

- Proxy Reporting Status - プロキシ機能を有効にします。(デフォルト: Disabled)
本コマンドを使用してプロキシ機能を有効にすると、スイッチは Last Leave と Query Suppression を含む「IGMP Snooping with Proxy Reporting」（DSL Forum TR-101、2006 年 4 月で定義）を実行します。
Last leave は、最後の受信者がマルチキャストグループを離れるときに代理で IGMP Query メッセージを送信し、Query Suppression は、IGMP Specific Query メッセージがアップストリームマルチキャストルータからこのデバイスのダウンストリームホストに転送されないことを意味します。
プロキシ機能が無効の場合、スイッチが受信したすべての IGMP Report メッセージは、ネイティブでアップストリームマルチキャストルータに転送されます。

- TCN Flood - スパニングツリートポロジ変更通知（TCN）が発生した場合にマルチキャストパケットのフラッディングを有効にします。(デフォルト: Disabled)
スパニングツリーのトポロジ変更が発生すると、スイッチによって学習されたエントリ情報が古くなっている可能性があります。トポロジ変更時、すべての受信者にマルチキャストパケットが確実に配信されるようにするために、トポロジが安定してすべての受信者へのマルチキャストの中継経路が学習されるまでの間、マルチキャストパケットをフラッディングします。
トポロジ変更通知（TCN）が受信され、その後すべてのアップリンクポートが削除されると、マルチキャストルータではすべてのマルチキャストグループがタイムアウトにより削除されます。
新しいアップリンクポートが起動すると、スイッチは新しいアップリンクポートに現在学習しているすべてのマルチキャストグループの IGMP Report メッセージを送信します。
本機能を有効にすると、トポロジの変更が発生した場合、スイッチはただちにマルチキャストパケットをフラッディングします。この場合、多くのマルチキャストグループに加入していると、フラッディングによってスイッチと受信者間の回線に過剰な負荷がかかる可能性があります。これを避けるために本機能を無効にして、マルチキャストパケットのフラッディングを抑制することができます。
トポロジが変更されると、ルートブリッジは代理で IGMP Query メッセージを送信して、マルチキャストグループへの加入状況を迅速に再学習します。

- TCN Query Solicit - スパニングツリートポロジ変更通知（TCN）が発生したときに、IGMP General Query メッセージを送信します。(デフォルト: Disabled)
スパニングツリーのルートブリッジが、IGMP snooping が有効になっている VLAN のトポロジ変更通知を受信すると、IGMP General Query メッセージを要求するために、グローバルな IGMP Leave メッセージを送信します。スイッチはこのメッセージを受信すると、スパニングツリーの変更が発生した VLAN 内のすべてのポートにフラッディングします。上流のマルチキャストルータがこのメッセージを受信すると、IGMP General Query メッセージを即座に送信します。
本機能を有効にすると、スイッチがスパニングツリーのルートブリッジでなくても、トポロジ変更に気付くたびに IGMP Query メッセージを送信します。

- Router Alert Option - Router Alert Option を含まない IGMPv2 / v3 パケットを破棄します。(デフォルト: Disabled)
IGMP バージョン 3 の RFC 3376 のセクション 9.1 で説明されているように、Router Alert Option を使用して DOS 攻撃から保護することができます。DOS 攻撃の一般的な方法の 1 つとして、クエリアに成りすました攻撃者が、大きなソースリストがあり、最大応答時間が大きな値に設定した多数の Group-and-Source Specific Query メッセージを送信して受信者に過負荷をかけます。
この種の攻撃から保護するために、(1) ルータは IGMP Query メッセージを転送すべきではありません。クエリアが Router Alert オプションを持っている場合、これは簡単に実行できます。(2) スイッチが受信者の役割（プロキシ機能を使用している場合など）で動作している場合、Router Alert Option を含まないバージョン 2 または 3 の IGMP Query メッセージは無視する必要があります。

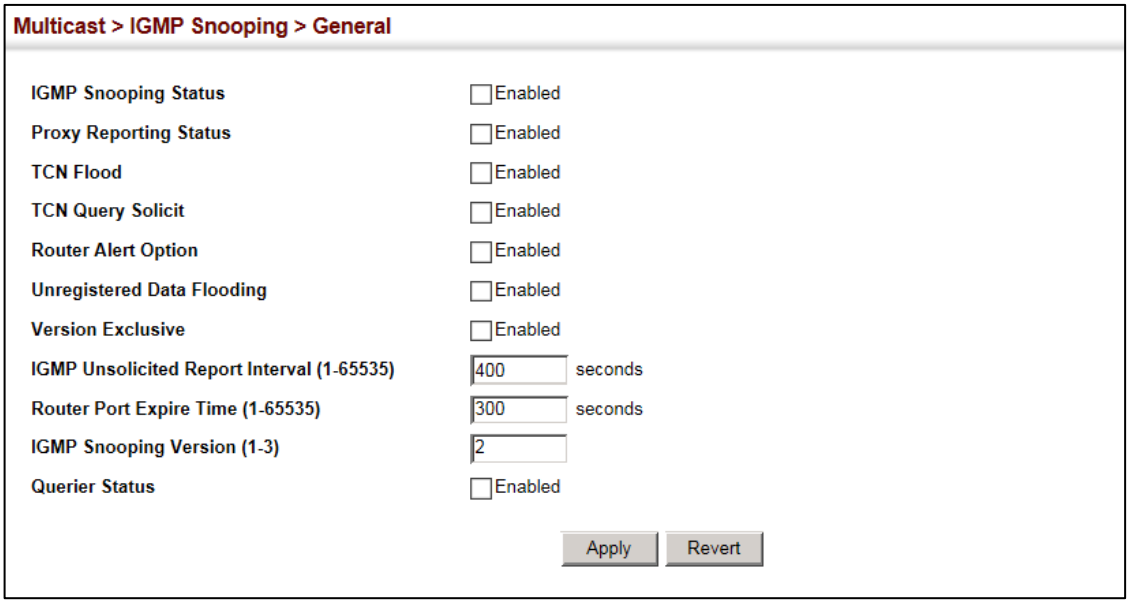
- Unregistered Data Flooding - 未学習のマルチキャストトラフィックを VLAN 内にフラッディングします。(デフォルト: Disabled)
  IGMP snooping のエントリ数が最大数に達すると、新しいエントリは学習されません。接続された VLAN にマルチキャストルータポートが設定されておらず、Unregistered Data Flooding が無効の場合、学習できなかったマルチキャストトラフィックは廃棄されます。それ以外の場合は VLAN 全体にフラッディングされます。
- Version Exclusive - 現在設定されている IGMP バージョンとは異なるバージョンを使用した IGMP メッセージを受信した場合、破棄します。(デフォルト: Disabled)
- IGMP Unsolicited Report Interval - プロキシ機能が有効な場合にマルチキャストルータポートに IGMP Report メッセージを送信する間隔を指定します。(範囲: 1 から 65535 秒、デフォルト：400 秒)
  新しいマルチキャストルータポートが設定されると、スイッチは新しいマルチキャストルータポートに対して、現在学習されているすべてのマルチキャストチャネルの IGMP Report メッセージを送信します。
  このコマンドは、プロキシ機能が有効な場合にのみ適用されます。
- Router Port Expire Time - Dynamic に設定したマルチキャストルータポートが期限切れになるまでの時間です。(範囲: 1 から 65535、推奨される範囲：300 から 500 秒、デフォルト：300)
- IGMP Snooping Version - ネットワーク上の他のデバイスとの互換性のために IGMP バージョンを設定します。スイッチが IGMP Query、Report メッセージを送信するときに使用する IGMP バージョンです。(範囲: 1 から 3、デフォルト：2)
  このアトリビュートは、IGMP snooping で使用される IGMP Report/Query メッセージのバージョンに設定します。バージョン 1 から 3 はすべてサポートされており、バージョン 2 と 3 は下位互換性があるため、使用されている IGMP バージョンに関係なく、スイッチは他のデバイスと連携できます。
- Querier Status - 有効にすると、スイッチはクエリアとして機能し、マルチキャストパケットを受信するかどうかを受信者に問い合わせます。 (デフォルト: Disabled)

Web インタフェース

IGMP snooping の設定を行うには、次の手順を実行します。

1. [Multicast]、[IGMP Snooping]、[General]をクリックします。
2. 必要に応じて IGMP snooping の設定を調整します。
3. [Apply]をクリックします。

図 13-2　IGMP snooping の設定



13.2.2 マルチキャストルータポートの Static 設定

[Multicast]> [IGMP Snooping]> [Multicast Router（Add Static Multicast Router）]ページを使用して、マルチキャストルータポートに設定するインタフェースを Static に設定します。

ネットワーク接続によっては、IGMP snooping が IGMP クエリア（マルチキャストルータ/スイッチ）を検出できないことがあります。この場合、IGMP クエリアを接続しているインタフェース（ポートまたはトランク）が既知であれば、そのインタフェースを手動でマルチキャストルータポートに設定できます。このインタフェースには、すべてのマルチキャストパケットを中継します。

コマンドの使用方法

マルチキャストルータポートを有効にするには、スイッチ上で IGMP snooping をグローバルに有効にする必要があります。

パラメータ

指定した Action ごとに、次のパラメータが表示されます。

Add Static Multicast Router：

- VLAN - マルチキャストルータポートを設定する VLAN を選択します。(範囲: 1 から 4094)
- Interface - ポートまたはトランクのスクロールダウンリストをアクティブにします。
  - Port or Trunk - マルチキャストルータポートに設定するインタフェースを指定します。

Show Static Multicast Router：

- VLAN - 設定済みの Static マルチキャストルータポートを表示する VLAN を選択します。
- Static Multicast Router Interface List - Static マルチキャストルータポートに設定されているインタフェースを表示します。

現在のマルチキャストルータを表示

- VLAN - 現在アクティブなマルチキャストルータポートを表示する VLAN を選択します。
- Interface - マルチキャストルータポートに設定されているインタフェースを表示します。
- Type - このマルチキャストルータポートが Static か Dynamic かを表示します。

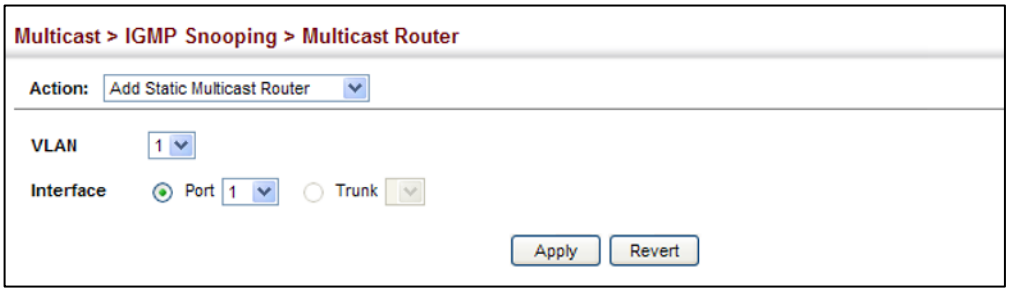
◆ Expire - Dynamic で設定したマルチキャストルータポートが期限切れになるまでの時間を表示します。

Web インタフェース

マルチキャストルータポートを Static に指定する手順は、次のとおりです。

1. [Multicast]、[IGMP Snooping]、[Multicast Router]をクリックします。
2. [Action]リストから[Add Static Multicast Router]を選択します。
3. マルチキャストルータポートを設定する VLAN を選択し、マルチキャストルータポートに設定するポートまたはトランクを選択します。
4. [Apply]をクリックします。

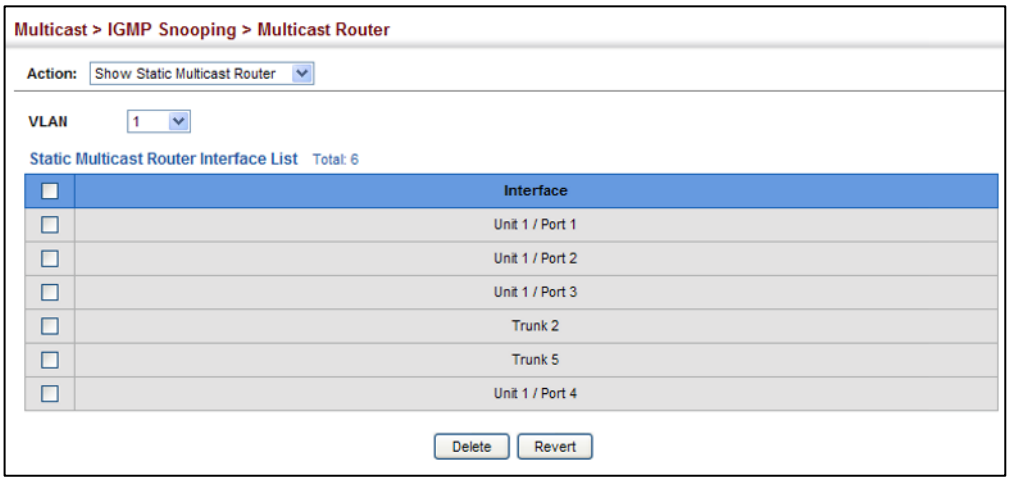
図 13-3　Static マルチキャストルータポートの設定



Static マルチキャストルータポートを表示するには、

1. [Multicast]、[IGMP Snooping]、[Multicast Router]をクリックします。
2. [Action]リストから[Show Static Multicast Router]を選択します。
3. この情報を表示する VLAN を選択します。

図 13-4　Static マルチキャストルータポートの表示



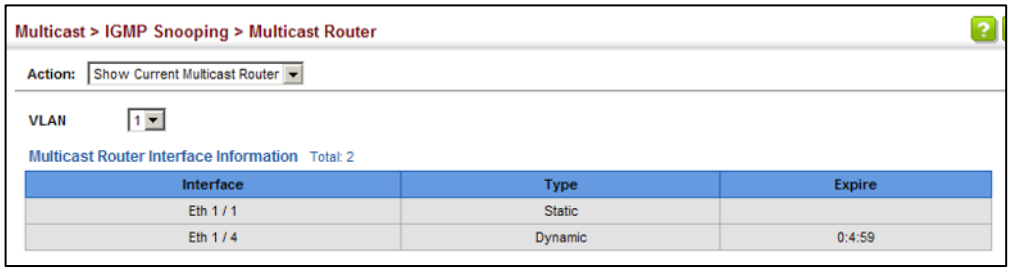
スイッチ上のポートに接続されているマルチキャストルータは、IGMP から取得した情報とマルチキャストルーティングプロトコル（PIM など）を使用して、インターネット上のマルチキャスト中継を実現します。これらのルータを接続するマルチキャストルータポートを設定する方法には、スイッチによって Dynamic に検出する方法と、スイッチ上のインタフェースに Static に設定する方法があります。

すべてのマルチキャストルータポートを表示するには、

1. [Multicast]、[IGMP Snooping]、[Multicast Router]をクリックします。
2. [Action]リストから[Show Current Multicast Router]を選択します。

3. この情報を表示する VLAN を選択します。選択された VLAN 内のマルチキャストルータポートが表示されます。

図 13-5　現在設定されているマルチキャストルータポートを表示



13.2.3 Static エントリの設定

[Multicast]> [IGMP Snooping]> [IGMP Member（Add Static Member）]ページを使用して、Static エントリを設定します。

IGMP Snooping では、IGMP Query および IGMP Report メッセージを使用してエントリを Dynamic に設定できます。ただし、厳重な制御が必要なアプリケーションでは、スイッチ上でマルチキャストサービスを Static に設定する必要があります。Static エントリは VLAN インタフェースに対して、マルチキャストグループと当該マルチキャストグループに加入するインタフェース(ポート/トランク)を設定します。

コマンドの使用方法

- Static エントリは決してエージングアウトされません。
- Static エントリを VLAN インタフェースに設定すると、当該 VLAN で受信した Static エントリに合致するマルチキャストパケットは、Static エントリに設定したポートにのみ転送されます。

パラメータ

指定した Action ごとに、次のパラメータが表示されます。

Add Static Member：

- VLAN - Static エントリを設定する VLAN を指定します。(範囲: 1 から 4094)
- Interface - ポートまたはトランクのスクロールダウンリストをアクティブにします。
  - Port or Trunk - Static エントリに割当てるインタフェースを指定します。
- Multicast IP - Static エントリに設定するマルチキャストアドレスを設定します。

Show Static Member：

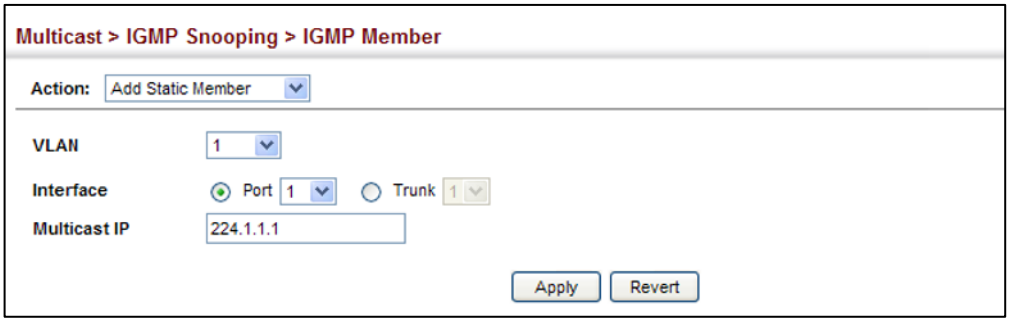
- VLAN - Static エントリを表示する VLAN を指定します。(範囲: 1 から 4094)

Web インタフェース

Static エントリを設定するには、

1. [Multicast]、[IGMP Snooping]、[IGMP Member]をクリックします。
2. [Action]リストから[Add Static Member]を選択します。
3. Static エントリを設定する VLAN を選択し、当該マルチキャストパケットを中継するインタフェースを指定し、マルチキャスト IP アドレスを入力します。
4. [Apply]をクリックします。

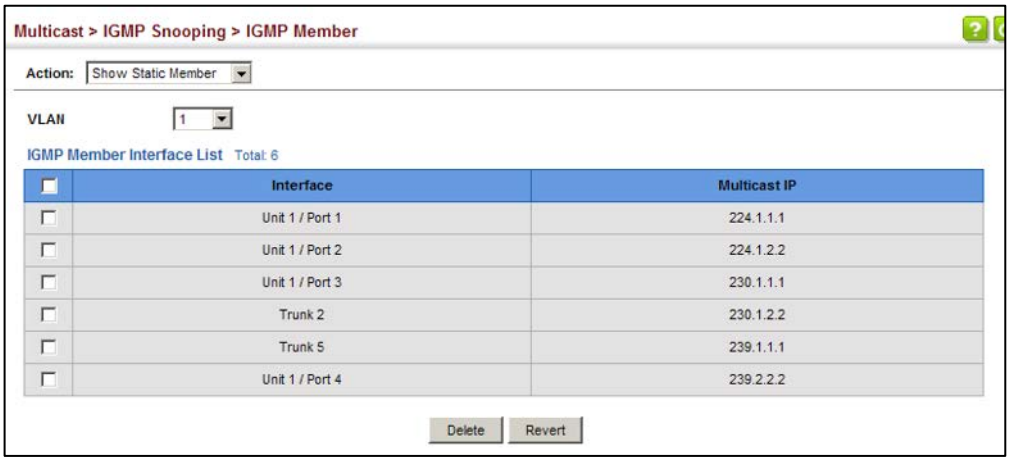
図 13-6　Static エントリの設定



Static エントリを表示:するには、

1. [Multicast]、[IGMP Snooping]、[IGMP Member]をクリックします。
2. [Action]リストから[Show Static Member]を選択します。
3. この情報を表示する VLAN を選択します。

図 13-7　Static エントリの表示



13.2.4 インタフェースごとに IGMP snooping を設定

[Multicast]> [IGMP Snooping]> [Interface（Configure VLAN）]ページを使用して、VLAN に IGMP snooping を設定します。IGMP snooping をグローバルに設定する方法については、「13.2.1　IGMP snooping の設定」を参照してください。

パラメータ

次のパラメータが表示されます。

- VLAN - 設定済みの VLAN の ID です。(範囲: 1 から 4094)
- IGMP Snooping Status - 有効にすると、スイッチは指定の VLAN インタフェースで IGMP snooping を使用します。(デフォルト: Disabled)
  IGMP snooping がグローバルに有効になっている場合、IGMP snooping の VLAN 単位のインタフェース設定が優先されます。
  IGMP snooping をグローバルに無効にすると、VLAN インタフェースごとに IGMP snooping を設定できますが、IGMP snooping がグローバルに再び有効にされるまで、VLAN インタフェースの設定は有効になりません。
- Version Exclusive -現在設定されている IGMP バージョンとは異なるバージョンを使用する IGMP メッセージ（マルチキャストプロトコルパケットを除く）を受信した場合、すべて破棄します。(オプショ

ン: Enabled, Using Global Status; デフォルト: Using Global Status)
VLAN 上で Version Exclusive が無効の場合、この設定は[Multicast]> [IGMP Snooping]> [General]ページで設定されたグローバル設定にもとづいています。VLAN 上で有効になっている場合は、この設定がグローバル設定よりも優先されます。

- Immediate Leave Status - IGMP 即時離脱機能を有効にします。IGMP 即時離脱機能が有効な場合、IGMP Leave メッセージを受信すると、マルチキャストグループから当該ポートを即座に削除します。(デフォルト: Disabled)
  IGMP 即時離脱機能を使用しない場合、マルチキャストルータ（またはクエリア）は、IGMP Leave メッセージを受信すると、IGMP Group-Specific Query メッセージを送信します。ルータ/クエリアは、指定されたタイムアウト時間内に IGMP Group-Specific Query メッセージに応答する受信者がない場合にのみ、そのグループのトラフィックの転送を停止します。このタイムアウトは、RFC 2236 で定義されている Last Member Query Interval * Robustness Variable（2 で固定）に設定されています。
  IGMP 即時離脱機能が有効の場合、スイッチは 1 つの受信者だけがインタフェースに接続されているとみなします。したがって、インタフェースが 1 台の IGMP 対応デバイス（IGMP スヌーピングを実行しているサービスホストまたはネイバー）に接続されている場合のみ、IGMP 即時離脱機能を使用してください。
  このアトリビュートは、IGMP snooping が有効で、IGMPv2 または IGMPv3 で使用されている場合にのみ有効です。
  IGMP 即時離脱機能が有効な場合、次のオプションが提供されます。
  - By Group - スイッチは、1 つのホストだけがインタフェースに接続されていることを前提としています。したがって、インタフェースが 1 台の IGMP 対応デバイス（IGMP スヌーピングを実行しているサービスホストまたはネイバー）が接続されている場合のみ、By Group を指定してください。
  - By Host IP - スイッチは、IGMPv2 / v3 離脱メッセージを受信したときに IGMP Group-Specific Query メッセージを送信しません。しかし、マルチキャストグループに参加している他の受信者があるかどうかを確認します。そのポート上のすべての受信者がグループを離れるときだけ、メンバーポートは削除されます。
- General Query Suppression - 受信者に接続されているポート以外への IGMP General Query メッセージの中継を抑制します。(デフォルト: Disabled)
  デフォルトでは、IGMP General Query メッセージは、受信ポート以外にフラッディングされます。General Query Suppression が有効の場合、IGMP General Query メッセージは受信者を接続しているポートにのみ転送されます。
- Proxy Reporting - プロキシ機能を有効にします。(オプション: Enabled, Disabled, Using Global Status; デフォルト: Using Global Status)
  本コマンドを使用してプロキシ機能を有効にすると、スイッチは Last Leave と Query Suppression を含む「IGMP Snooping with Proxy Reporting」（DSL Forum TR-101、2006 年 4 月で定義）を実行します。Last leave は、最後の受信者がマルチキャストグループを離脱するときに代理で IGMP Query メッセージを送信し、Query Suppression は、アップストリームマルチキャストルータから受信した Specific Query メッセージを受信者に転送しないことを意味します。
  プロキシ機能に使用されるルール：
  プロキシ機能が有効な場合、送信元アドレスは次の基準で設定します。
  - Proxy Query Address が設定されている場合、設定されたアドレスを IGMP Query メッセージ、IGMP Report メッセージおよび IGMP Leave メッセージの送信元アドレスに使用します。
  - Proxy Query Address が設定されていない場合、VLAN の IP アドレスを IGMP Query メッセージに使用し、IGMP Report メッセージおよび IGMP Leave メッセージの送信元アドレスには受信者の IP アドレスを使用します。
- Interface Version - ネットワーク上の他のデバイスとの互換性のために IGMP バージョンを設定しま

す。スイッチが IGMP Query、Report メッセージを送信するために使用する IGMP バージョンです。(オプション: 1-3, Using Global Version; デフォルト: Using Global Version)
このアトリビュートは、IGMP snooping で使用される IGMP Report/Query メッセージのバージョンを設定します。バージョン 1 から 3 はすべてサポートされており、バージョン 2 と 3 は下位互換性があるため、使用されているバージョンに関係なく、スイッチは他のデバイスと連携できます。

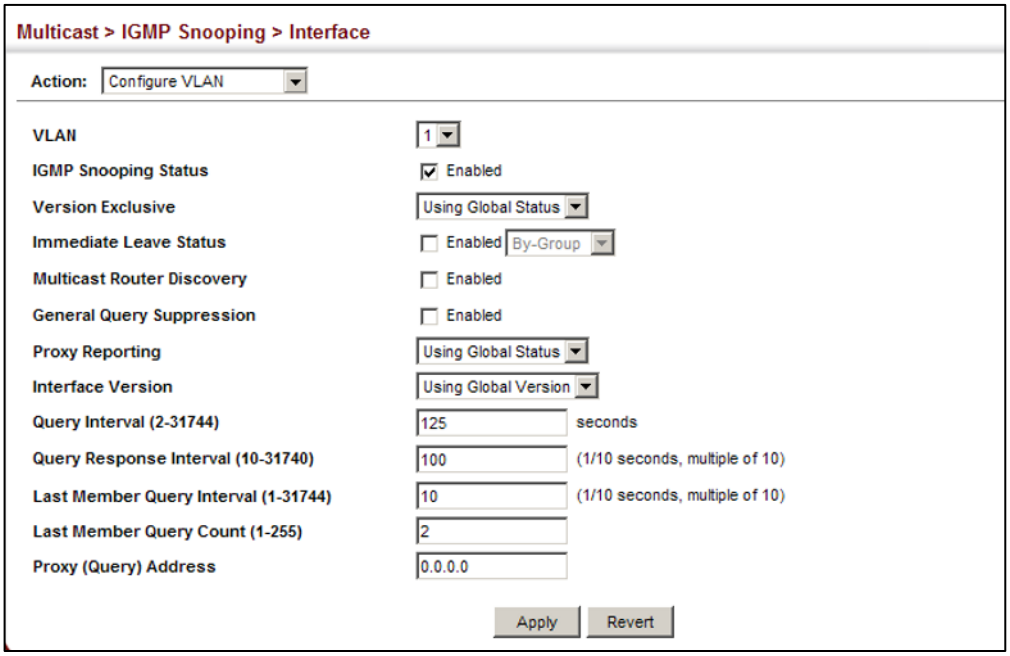
- Query Interval - IGMP General Query メッセージを送信する間隔です。(範囲: 2 から 31744 秒; デフォルト：125 秒)
  IGMP General Query メッセージは、このアトリビュートによって指定された間隔でスイッチによって送信されます。このメッセージがダウンストリームホストによって受信されると、すべての受信者は、参加したマルチキャストグループの IGMP Report メッセージを応答します。
  このアトリビュートは、スイッチがクエリアとして機能している場合、またはプロキシ機能が有効の場合に機能します。Query Interval と Query response Interval を変更する場合、Query response Interval を変更した後、Query Interval を変更してください。
- Query Response Interval - システムが IGMP General Query メッセージへの応答を待機する最大時間です。(範囲: 10 から 31740 秒の 10 分の 1 で 10 の倍数。 デフォルト：10 秒)
  このアトリビュートは、スイッチがクエリアとして機能している場合、またはプロキシ機能が有効の場合に機能します。Query Interval と Query response Interval を変更する場合、Query response Interval を変更した後、Query Interval を変更してください。
- Last Member Query Interval - IGMP Group-Specific Query メッセージまたは IGMP Group-and-Source Specific Query メッセージへの応答を待機する時間です。(範囲: 1 から 31744 秒の 10 分の 1 で 10 の倍数。 デフォルト：1 秒)
  マルチキャストホストがグループを離れると、IGMP Leave メッセージが送信されます。IGMP Leave メッセージがスイッチによって受信されると、IGMP Group-Specific Query メッセージまたは IGMP Group-and-Source Specific Query メッセージを送信して、この受信者が最後にグループを脱退したかどうかを確認し、タイマーを開始します。タイマーの期限が切れるまでに IGMP Report メッセージが受信されない場合、グループレコードは削除されます。
  値を小さくすると、マルチキャストグループの最後のメンバーの損失を検出する時間が短縮されますが、短期間でより多くの IGMP Report メッセージを受信するためバーストトラフィックが発生する可能性があります。
  この属性は、プロキシ機能または IGMP クエリアが有効の場合にのみ有効です。
- Last Member Query Count - システムでローカルメンバーが存在しないとみなされる前に送信される IGMP Group-Specific Query メッセージまたは IGMP Group-and-Source Specific Query メッセージの数です。(範囲: 1 から 255;デフォルト: 2)
  この属性は、プロキシ機能または IGMP クエリアが有効の場合にのみ有効です。
- Proxy (Query) Address - プロキシ機能で送信する IGMP Query メッセージおよび IGMP Report メッセージ用の送信元アドレスです。(範囲: 任意の有効な IP ユニキャストアドレスです。 デフォルト：0.0.0.0)

Web インタフェース

VLAN 上で IGMP snooping を設定するには、次の手順を実行します。

1. [Multicast]、[IGMP Snooping]、[Interface]をクリックします。
2. [Action]リストから[Configure VLAN]を選択します。
3. 必要なパラメータを設定および更新するには、VLAN を選択します。
4. [Apply]をクリックします。

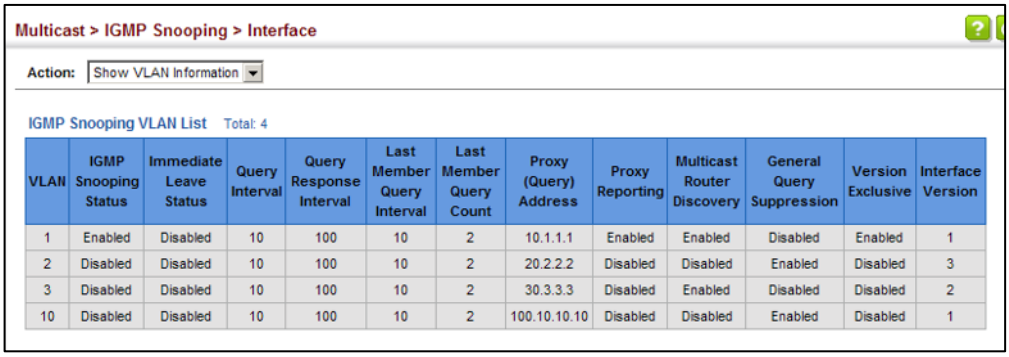
図 13-8　VLAN での IGMP snooping の設定



IGMP snooping のインタフェース設定を表示するには、次の手順を実行します。

1. [Multicast]、[IGMP Snooping]、[Interface]をクリックします。
2. [Action]リストから[Show VLAN Information]を選択します。

図 13-9　VLAN での IGMP snooping 設定の表示



VLAN	IGMP Snooping Status	Immediate Leave Status	Query Interval	Query Response Interval	Last Member Query Interval	Last Member Query Count	Proxy (Query) Address	Proxy Reporting	Multicast Router Discovery	General Query Suppression	Version Exclusive	Interface Version
1	Enabled	Disabled	10	100	10	2	10.1.1.1	Enabled	Enabled	Disabled	Enabled	1
2	Disabled	Disabled	10	100	10	2	20.2.2.2	Disabled	Disabled	Enabled	Disabled	3
3	Disabled	Disabled	10	100	10	2	30.3.3.3	Disabled	Enabled	Disabled	Disabled	2
10	Disabled	Disabled	10	100	10	2	100.10.10.10	Disabled	Disabled	Enabled	Disabled	1

13.2.5 IGMP Query メッセージおよびマルチキャストパケットの廃棄

IGMP Query メッセージを廃棄するインタフェースを設定するには、[Multicast]> [IGMP Snooping]> [Interface（Configure Interface）]ページを使用します。

パラメータ

次のパラメータが表示されます。

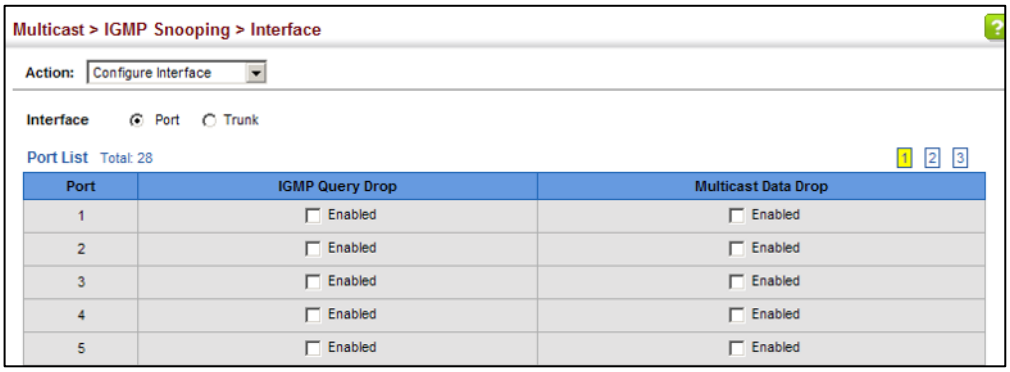
- Interface - ポートまたはトランクの識別子です。
- IGMP Query Drop - 指定されたインタフェースで受信した IGMP Query メッセージを廃棄するように設定します。このスイッチがクエリアとして動作している場合、別のクエリアから受信した IGMP Query メッセージの影響を受けません。
- Multicast Data Drop - 指定されたインタフェースで受信した UDP マルチキャストパケットを廃棄するように設定します。

Web インタフェース

IGMP Query メッセージまたはマルチキャストパケットを廃棄するには、次の手順を実行します。

1. [Multicast]、[IGMP Snooping]、[Interface]をクリックします。
2. [Action]リストから[Configure Interface]を選択します。
3. ポートまたはトランクインタフェースを選択します。
4. 任意のインタフェースに必要なドロップ機能を有効にします。
5. [Apply]をクリックします。

図 13-10　IGMP Query メッセージまたはマルチキャストパケットのドロップの設定



13.2.6 エントリの表示

IGMP snooping で学習したエントリを表示するには、 [Multicast]> [IGMP Snooping]> [Forwarding Entry]ページを使用します。

コマンドの使用方法

エントリに関する情報を表示するには、最初に IGMP snooping をスイッチで有効にする必要があります。

パラメータ

次のパラメータが表示されます。

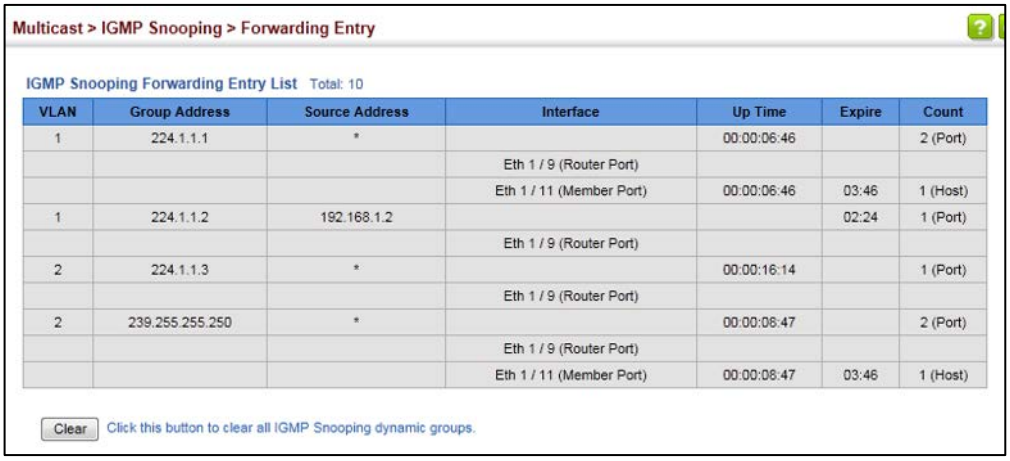
- VLAN - エントリを学習している VLAN です。(範囲: 1 から 4094)
- Group Address - エントリのマルチキャストグループアドレスです。
- Interface - 指定されたマルチキャストグループのトラフィックを受信しているダウンストリームポートまたはトランクです。このフィールドには、Dynamic および Static に設定されたマルチキャストルータポートの両方が含まれます。
- Up Time - このマルチキャストグループを学習してからの経過時間です。
- Expire - このエントリが期限切れになるまでの時間です。
- Count - このエントリの中継先のポート数です。マルチキャストルータポートも含みます。
- Clear - IGMP snooping で動的に学習したマルチキャストグループ情報をクリアします。

Web インタフェース

IGMP snooping によって学習されたエントリを表示するには、

1. [Multicast]、[IGMP Snooping]、[Forwarding Entry]をクリックします。

図 13-11　IGMP snooping のエントリの表示



13.2.7 IGMP snooping 統計情報の表示

[Multicast]> [IGMP Snooping]> [Statistics]ページを使用して、指定されたインタフェースの IGMP snooping 関連の統計情報を表示します。

パラメータ

次のパラメータが表示されます。

Show Query Statistics：

- VLAN - VLAN ID です。(範囲: 1 から 4094)
- Other Querier - このインタフェース上のリモートクエリアの IP アドレスです。
- Other Querier Expire - リモートクエリアが期限切れになるまでの時間です。
- Other Querier Uptime - リモートクエリアを検出してからの経過時間です。
- Self Querier - このインタフェース上のローカルクエリアの IP アドレスです。
- Self Querier Expire - ローカルクエリアが期限切れになるまでの時間です。
- Self Querier Uptime - ローカルクエリアが有効になってからの経過時間です。
- General Query Received - このインタフェースで受信した IGMP General Query メッセージの数です。
- General Query Sent - このインタフェースから送信した IGMP General Query メッセージの数です。
- Specific Query Received - このインタフェースで受信した IGMP Specific Query メッセージの数です。
- Specific Query Sent - このインタフェースから送信した IGMP Specific Query メッセージの数です。
- Warn Rate Limit - 誤ったバージョンの IGMP Query メッセージ受信した場合に、「Vx Warning Count」に加算するための基準となる時間です。表示されている時間内に誤ったバージョンの IGMP Query メッセージを複数受信しても 1 しか加算しません。したがって、「0 Sec」の場合は、誤ったバージョンの IGMP Query メッセージを受信した数だけ「Vx Warning Count」に加算されることに注意してください。
- V1 Warning Count - このインタフェースに設定されたバージョンと一致しない、IGMPv1 Query メッセージを受信した数です。
- V2 Warning Count - このインタフェースに設定されたバージョンと一致しない、IGMPv2 Query メッセージを受信した数です。
- V3 Warning Count - このインタフェースに設定されたバージョンと一致しない、IGMPv3 Query メッセージを受信した数です。

- Clear All - 全ての IGMP snooping の統計情報をクリアします。

Show VLAN Statistics / Show Port Statistics / Show Trunk Statistics：

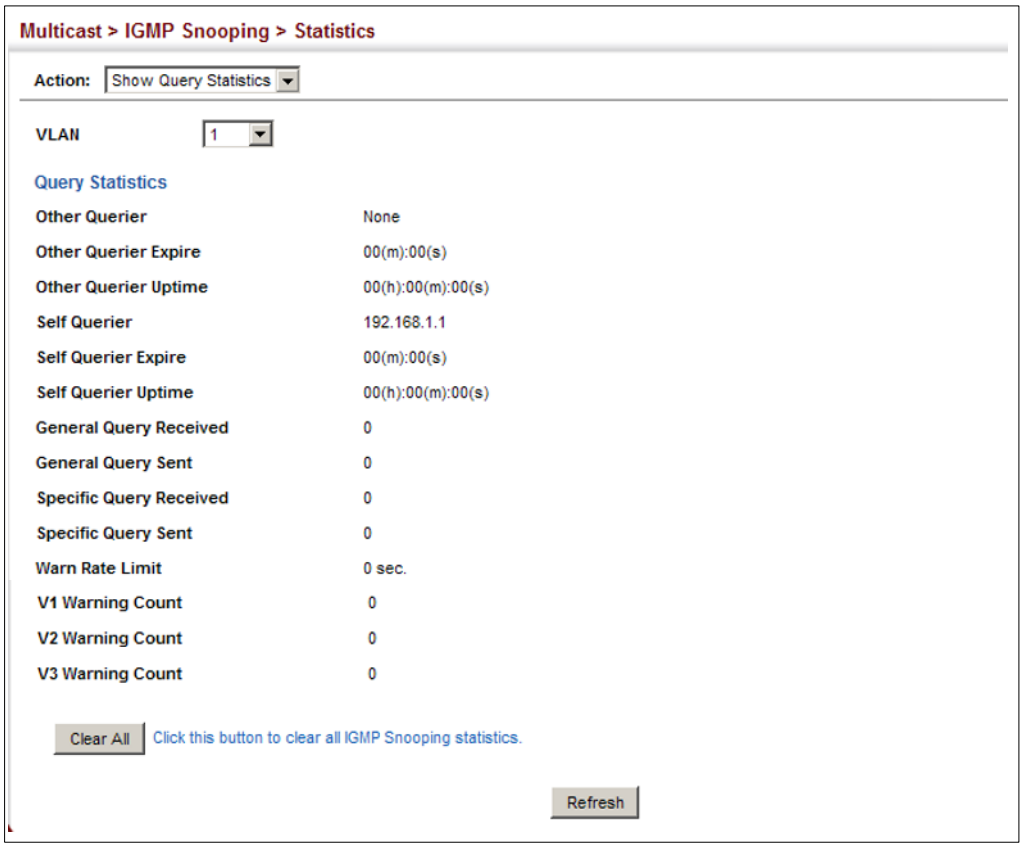
- VLAN - VLAN ID です。(範囲: 1 から 4094)
- Port - ポート番号です。(範囲: 1 から 10)
- Trunk - トランク識別子です。(範囲: 1-8)
- Input Statistics
  - Report - このインタフェースで受信した IGMP Report メッセージの数です。
  - Leave - このインタフェースで受信した IGMP Leave メッセージの数です。
  - G Query - このインタフェースで受信した IGMP General Query メッセージの数です。
  - G(-S)-S Query - このインタフェースで受信した IGMP Group-Specific Query メッセージまたは IGMP Group-and-Source-Specific Query メッセージの数です。
  - Drop - IGMP Query、Report、Leave メッセージがドロップされた回数です。無効な形式、レート制限、パケット内容が許可されていないため、パケットがドロップされる可能性があります。
  - Join Success - マルチキャストグループが正常に参加した回数です。
  - Group - このインタフェースでアクティブな IGMP グループの数です。
- Output Statistics
  - Report - このインタフェースから送信した IGMP Report メッセージの数です。
  - Leave - このインタフェースから送信した IGMP Leave メッセージの数です。
  - G Query - このインタフェースから送信した IGMP General Query メッセージの数です。
  - G(-S)-S Query - このインタフェースから送信した IGMP Group-Specific Query メッセージまたは IGMP Group-and-Source-Specific Query メッセージの数です。
  - Clear - 統計情報をクリアします。
  - Refresh - 統計情報を更新します。

Web インタフェース

クエリアに関連した統計情報を表示するには：

1. [Multicast]、[IGMP Snooping]、[Statistics]をクリックします。
2. [Action]リストから[Show Query Statistics]を選択します。
3. VLAN を選択します。

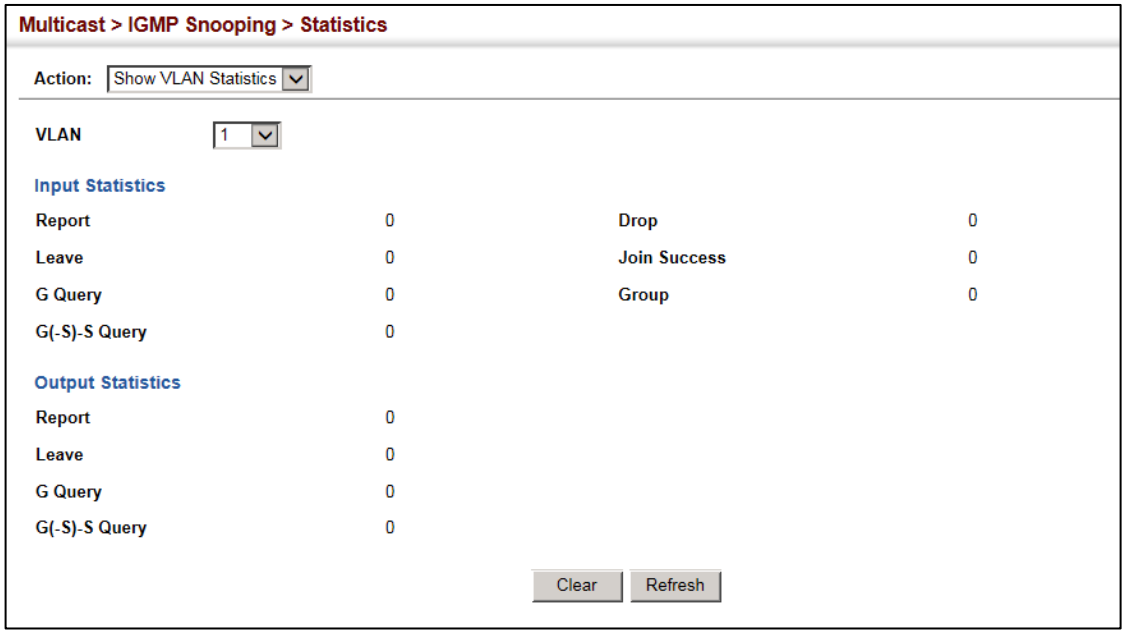
図 13-12　IGMP snooping 統計情報の表示 - クエリア関連



VLAN を指定してプロトコル関連の統計情報を表示するには：

1. [Multicast]、[IGMP Snooping]、[Statistics]をクリックします。
2. [Action]リストから[Show VLAN Statistics]を選択します。
3. VLAN を選択します。

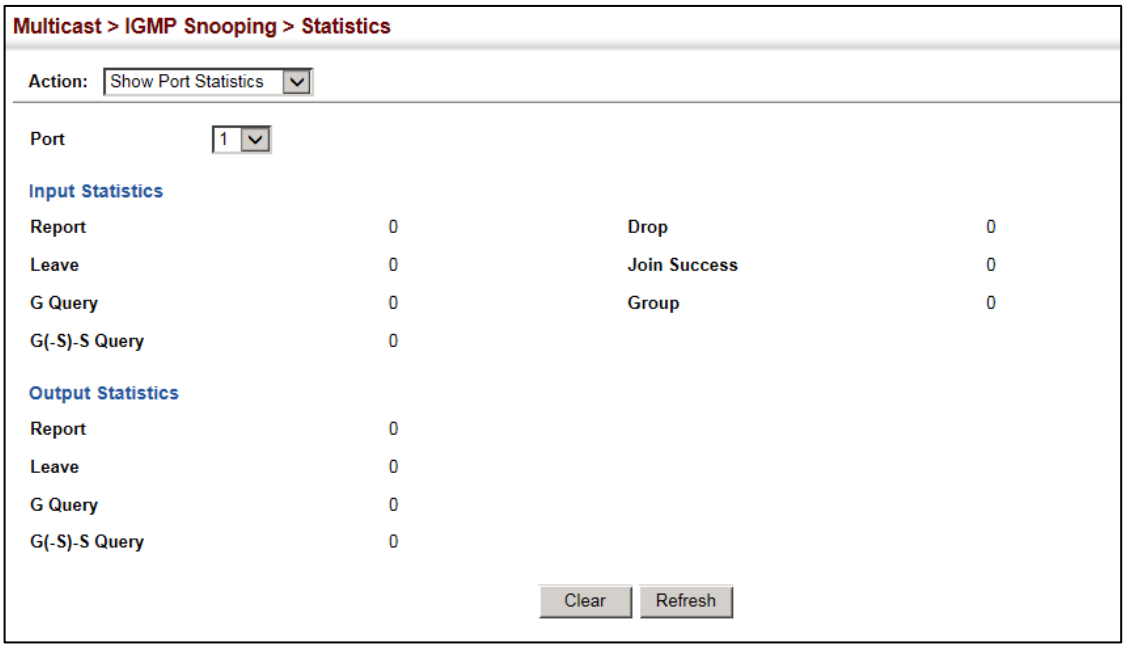
図 13-13　IGMP snooping 統計情報の表示 - VLAN 指定



ポートを指定してプロトコル関連の統計情報を表示するには：

1. [Multicast]、[IGMP Snooping]、[Statistics]をクリックします。
2. [Action]リストから[Show Port Statistics]を選択します。
3. ポートを選択します。

図 13-14　IGMP snooping 統計情報の表示 - ポート指定



13.3 IGMP フィルタリングとスロットリング

特定のスイッチアプリケーションでは、管理者はエンドユーザが使用できるマルチキャストサービスを制御したい場合があります。たとえば、特定のサブスクリプションプランに基づく IP / TV サービスです。IGMP フィルタリングは、スイッチポート上の指定されたマルチキャストサービスへのアクセスを制限することでこの要件を満たし、IGMP スロットリングは、ポートが参加できるマルチキャストグループの同時加入数を制限します。

IGMP フィルタリングを使用すると、ポートで許可または拒否されるマルチキャストグループを指定するスイッチポートにプロファイルを割当てることができます。IGMP フィルタプロファイルには、1 つ以上のアドレスまたはマルチキャストアドレスの範囲を含めることができます。 ポートに割当てられるプロファイルは 1 つだけです。有効にすると、ポートで受信した IGMP Report メッセージがフィルタプロファイルと照合されます。要求されたマルチキャストグループが許可されている場合、IGMP Report メッセージは通常どおり転送されます。要求されたマルチキャストグループが拒否された場合、IGMP Report メッセージは破棄されます。

IGMP スロットリングは、ポートが同時に参加できるマルチキャストグループの最大数を設定します。1 つのポートで最大グループ数に達すると、スイッチは 2 つのアクションのいずれかをとることができます。「Deny」または「Replace」のいずれかです。アクションが Deny に設定されている場合、新しい IGMP Report メッセージはすべて廃棄されます。アクションが Replace に設定されている場合、スイッチはランダムに既存のグループを削除し、新しいマルチキャストグループに置換えます。

13.3.1 IGMP フィルタリングとスロットリングの有効化

[Multicast]> [IGMP Snooping]>[Filter（Configure General）]ページを使用して、スイッチ上で IGMP フィルタリングと IGMP スロットリングをグローバルに有効にします。

パラメータ

次のパラメータが表示されます。

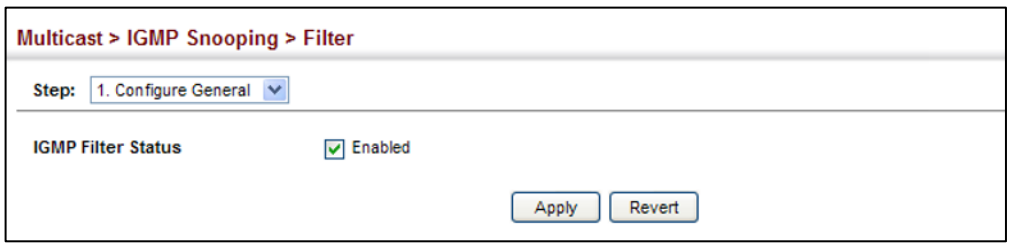
◆ IGMP Filter Status - スイッチの IGMP フィルタリングと IGMP スロットリングをグローバルに有効にします。(デフォルト: Disabled)

Web インタフェース

スイッチ上で IGMP フィルタリングおよび IGMP スロットリングを有効にするには：

1. [Multicast]、[IGMP Snooping]、[Filter]をクリックします。
2. [Step]リストから[Configure General]を選択します。
3. IGMP フィルタステータスを有効にする。
4. [Apply]をクリックします。

図 13-15　IGMP フィルタリングと IGMP スロットリングの有効化



13.3.2 IGMP フィルタプロファイルの設定

IGMP プロファイルを作成し、そのアクセスモードを設定するには、マルチキャスト> IGMP スヌーピング >フィルタ（プロファイルの設定 - 追加）ページを使用します。次に、[Add Multicast Group Range]ページを使用して、フィルタリングするマルチキャストグループを設定します。

コマンドの使用方法

フィルタの対象となるマルチキャストグループの範囲を指定します。指定方法は開始となるアドレスと終了となるアドレスを指定します。範囲の開始と終了に同じ IP アドレスを入力して単一のマルチキャストグループを指定することもできます。

パラメータ

次のパラメータが表示されます。

Add：

- Profile ID - IGMP プロファイルを作成します。(範囲: 1 から 60)
- Access Mode - プロファイルのアクセスモードを設定します。 Permit または Deny のいずれかです。(デフォルト: Deny)
  アクセスモードが Permit に設定されている場合、マルチキャストグループが制御された範囲内に入ると、IGMP Report メッセージが処理されます。アクセスモードが Deny に設定されている場合、IGMP 参加レポートは、マルチキャストグループが設定された範囲にない場合にのみ処理されます。

Add Multicast Group Range：

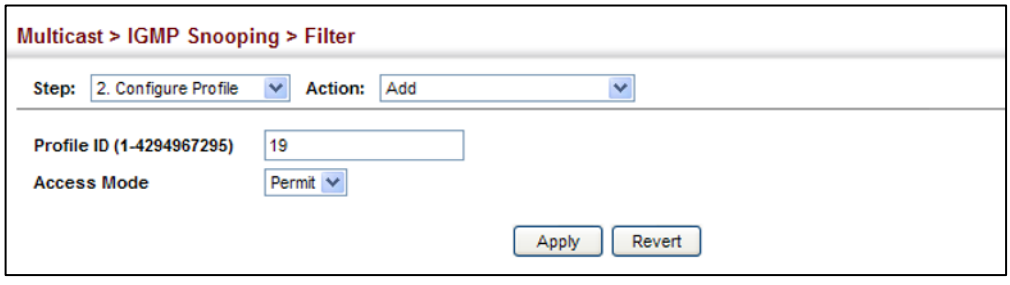
- Profile ID - 設定する IGMP プロファイルを選択します。
- Start Multicast IP Address - マルチキャストグループの範囲の開始アドレスを指定します。
- End Multicast IP Address - マルチキャストグループの範囲の終了アドレスを指定します。

Web インタフェース

IGMP フィルタプロファイルを作成し、そのアクセスモードを設定するには：

1. [Multicast]、[IGMP Snooping]、[Filter]をクリックします。
2. [Step]リストから[Configure Profile]を選択します。
3. [Action]リストから[Add]を選択します。
4. プロファイルの番号を入力し、アクセスモードを設定します。
5. [Apply]をクリックします。

図 13-16　IGMP フィルタリングプロファイルの作成

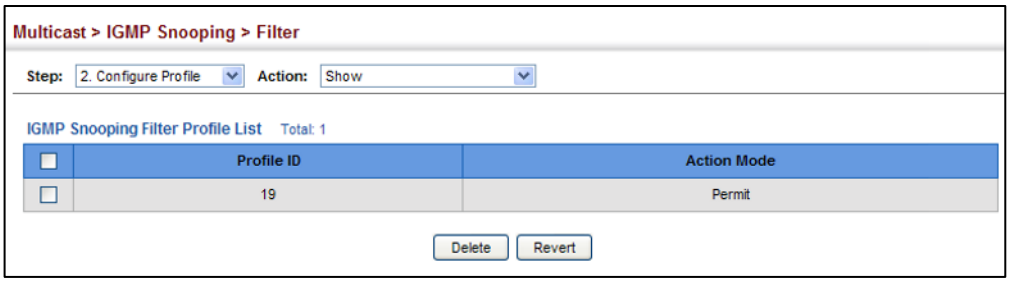


IGMP フィルタプロファイルを表示するには、

1. [Multicast]、[IGMP Snooping]、[Filter]をクリックします。

2. [Step]リストから[Configure Profile]を選択します。
3. [Action]リストから[Show]を選択します。

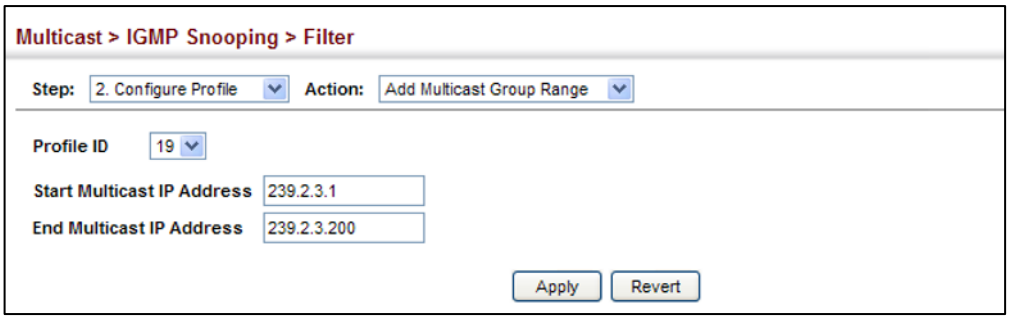
図 13-17　作成された IGMP フィルタリングプロファイルの表示



IGMP フィルタプロファイルにマルチキャストグループの範囲を追加するには、

1. [Multicast]、[IGMP Snooping]、[Filter]をクリックします。
2. [Step]リストから[Configure Profile]を選択します。
3. [Action]リストから[Add Multicast Group Range]を選択します。
4. 設定するプロファイルを選択し、マルチキャストグループアドレスまたはアドレス範囲を追加します。
5. [Apply]をクリックします。

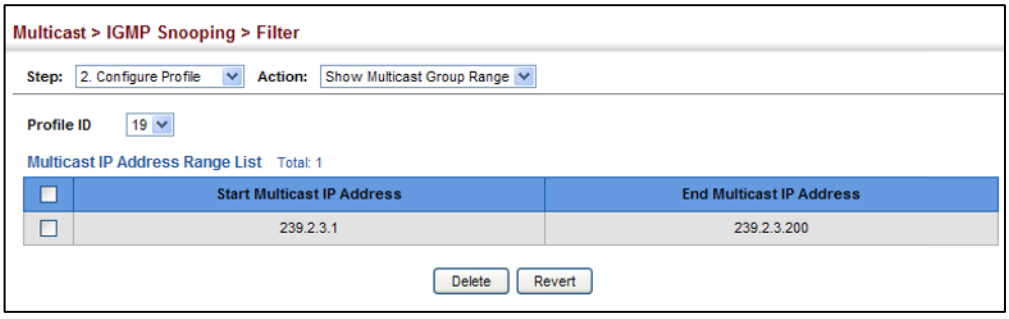
図 13-18　IGMP フィルタリングプロファイルへのマルチキャストグループの追加



IGMP フィルタプロファイル用に設定されたマルチキャストグループを表示するには、次の手順を実行します。

1. [Multicast]、[IGMP Snooping]、[Filter]をクリックします。
2. [Step]リストから[Configure Profile]を選択します。
3. [Action]リストから[Show Multicast Group Range]を選択します。
4. この情報を表示するプロファイルを選択します。

図 13-19　IGMP フィルタリングプロファイルに割当てられたグループの表示



13.3.3 インタフェースの IGMP フィルタリングおよびスロットリングの設定

[Multicast]> [IGMP Snooping]>[Filter（インタフェースの設定）]ページを使用して、スイッチ上のインタフェースに IGMP フィルタプロファイルを割当てたり、インタフェースが同時に参加できるマルチキャストグループの最大数を制限してマルチキャストトラフィックを制御します。

コマンドの使用方法

- IGMP スロットリングは、ポートが同時に参加できるマルチキャストグループの最大数を設定します。1 つのポートで最大グループ数に達すると、スイッチは 2 つのアクションのいずれかをとることができます。 「Deny」または「Replace」のいずれかです。アクションが Deny に設定されている場合、新しい IGMP Report メッセージはすべて削除されます。アクションが Replace に設定されている場合、スイッチはランダムに既存のグループを削除し、新しいマルチキャストグループに置換えます。

パラメータ

次のパラメータが表示されます。

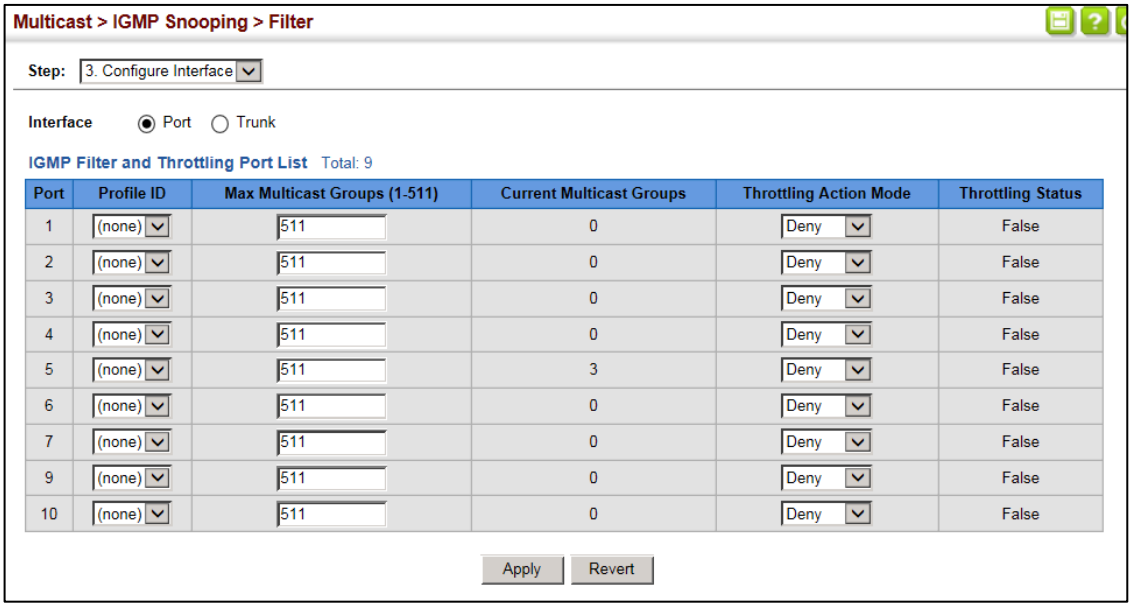
- Interface - ポートまたはトランクの識別子です。
  IGMP プロファイルまたは IGMP スロットリングの設定は、ポートまたはトランクに適用できます。ポートがトランクメンバーとして設定されている場合、トランクはトランクの最初のポートメンバーに適用された設定を使用します。
- Profile ID - インタフェースに割当てる既存のプロファイルを選択します。
- Max Multicast Groups - インタフェースが同時に参加できるマルチキャストグループの最大数を設定します。(範囲: 1 から 511; デフォルト: 511)
- Current Multicast Groups - インタフェースが参加している現在のマルチキャストグループを表示します。
- Throttling Action Mode - インタフェースの最大マルチキャストグループ数を超えた場合に実行するアクションを設定します。(デフォルト: Deny)
  - Deny - 超過後に受信した IGMP Report メッセージを破棄します。
  - Replace - 超過後に受信した IGMP Report メッセージのマルチキャストグループは、既存のグループと置換えます。
- Throttling Status - IGMP スロットリングの状態を表示します。(オプション: True または False)

Web インタフェース

ポートまたはトランクの IGMP フィルタリングまたは IGMP スロットリングを設定するには、次の手順を実行します。

1. [Multicast]、[IGMP Snooping]、[Filter]をクリックします。
2. [Step]リストから[Configure Interface]を選択します。
3. インタフェースに割当てるプロファイルを選択し、マルチキャストグループの最大数と最大マルチキャストグループ数を超えた場合に実行するアクションを設定します。
4. [Apply]をクリックします。

図 13-20　インタフェースへの IGMP フィルタリングおよび IGMP スロットリングの設定



13.4 MLD snooping

MLD snooping は IPv6 ネットワークで動作し、IPv4 の IGMP snooping と同様の機能を実行します。つまり、MLD snooping では、受信者が存在するポートを学習し、IPv6 マルチキャストパケットを受信者を接続するポートにのみ中継します。これにより、指定された VLAN 内の IPv6 マルチキャストパケットのフラッディングを抑制します。

MLD プロトコルには、バージョン 1 とバージョン 2 の 2 つのバージョンがあります。MLDv1 制御パケットには、MLD Query メッセージ、MLD Rewport メッセージ、および MLD Done メッセージ（IGMPv2 Query メッセージ、IGMP Report メッセージ、および IGMP Leave メッセージに相当）が含まれます。MLDv2 メッセージには、MLDv2 Query メッセージおよび MLDv2 Report メッセージ、および MLDv1 Report メッセージおよび MLD Done メッセージが含まれます。

IGMP snooping と MLD snooping は独立した機能なので、同時に機能することができます。

13.4.1 MLD snooping の設定

[Multicast]> [MLD Snooping]>[General]ページを使用して、MLD snooping の設定を行います。MLD Query メッセージおよび MLD Report メッセージにもとづいて、スイッチはマルチキャストパケットを要求するポートにのみ中継します。これにより、スイッチがマルチキャストパケットをフラッディングすることがなくなり、ネットワークのパフォーマンスが低下することを防止します。

パラメータ

次のパラメータが表示されます。

- MLD Snooping Status - 有効にすると、スイッチはネットワークトラフィックを監視して、どの受信者がマルチキャストトラフィックを受信するかを決定します。(デフォルト: Disabled)
- Querier Status - 有効の場合、スイッチは MLDv2 snooping のクエリアとして選択することができます。クエリアは、マルチキャストトラフィックを受信するかどうかをホストに問い合わせます。(デフォルト: Disabled)
  クエリアが選択された場合に動作する VLAN インタフェースに IPv6 アドレスを設定する必要があります。クエリアとして機能する場合、スイッチはこの IPv6 アドレスを MLD Query メッセージの送信元アドレスとして使用します。
  ネットワーク上の IPv6 マルチキャストルータが検出された場合、クエリア機能は起動せず、起動後も自動的に無効になります。
- Robustness – MLD snooping ロバストネス値です。MLD General Query メッセージに多数の受信者が応答して、すべての MLD Report メッセージを受信できなかった場合、当該ポートがエントリから削除されて受信者へのマルチキャスト中継が停止する可能性があります。この場合、ロバストネス値を大きくすることで、エントリを保持する期間(MLD General Query メッセージの送信回数)を延長できるため、マルチキャスト中継停止の可能性を軽減できます。(範囲: 2 から 10 デフォルト：2)
- Query Interval - MLD General Query メッセージを送信する間隔です。(範囲: 60 から 125 秒; デフォルト：125 秒)
  この属性は、スイッチがクエリアとして機能している場合に適用されます。
  MLD General Query メッセージは、このアトリビュートによって指定された間隔でスイッチによって送信されます。このメッセージがダウンストリームホストによって受信されると、すべての受信者は、参加したマルチキャストグループの MLD Report メッセージを応答します。
- Query Max Response Time - MLD General Query メッセージで通知される最大応答時間です。(範囲: 5 から 25 秒; デフォルト：10 秒)
  このアトリビュートは、MLD Query メッセージを受信した受信者が MLD Report メッセージを応答す

るまでの時間を制御します。

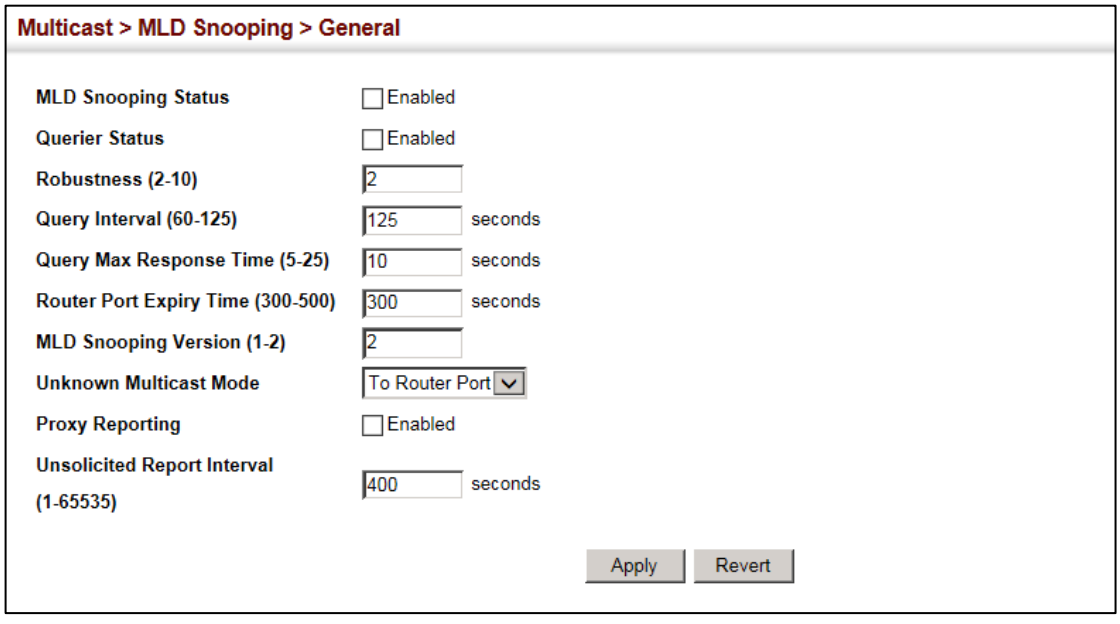
- Router Port Expiry Time - 他装置のクエリアが停止してからマルチキャストルータポート（MLD Query メッセージを受信していたインタフェース）が期限切れになったとみなすまでの時間です。(範囲: 300 から 500 秒; デフォルト：300 秒)
- MLD Snooping Version - ネットワーク上の他のデバイスとの互換性のために使用される MLD バージョンです。また、スイッチが MLD Query メッセージおよび MLD Report メッセージを送信するために使用する MLD バージョンです。(範囲: 1 から 2、デフォルト：2)
- Unknown Multicast Mode - 未学習のマルチキャストパケットを受信した場合の動作を指定します。オプションは次のとおりです。
  - Flood - 未学習の IPv6 マルチキャストパケットを、VLAN 内のすべてのポートにフラッディングします。
  - To Router Port - 未学習の IPv6 マルチキャストパケットをマルチキャストルータポートに転送します。（これがデフォルトの動作です）。
- Proxy Reporting -プロキシ機能を有効にします。(デフォルト: Disabled)
- Unsolicited Report Interval - プロキシ機能が有効な場合にマルチキャストルータポートに IGMP Report メッセージを送信する間隔を指定します。(範囲: 1 から 65535 秒、デフォルト：400 秒)

Web インタフェース

MLD snooping の設定を行うには：

1. [Multicast]、[MLD Snooping]、[General]をクリックします。
2. 必要に応じて設定を調整します。
3. [Apply]をクリックします。

図 13-21　MLD snooping の設定



13.4.2 インタフェースごとの MLD 即時離脱機能の設定

[Multicast]> [MLD Snooping]>[Interface]ページを使用して、VLAN の MLD 即時離脱機能を設定します。

パラメータ

次のパラメータが表示されます。

- VLAN - VLAN ID です。(範囲: 1 から 4094)
- Immediate Leave - そのポートで MLD Done メッセージが受信され、VLAN に対して MLD 即時離脱機能が有効になっている場合、IPv6 マルチキャストサービスのメンバーポートを直ちに削除します。(デフォルト: Disabled)
  MLD 即時離脱機能が使用されない場合、マルチキャストルータ（またはクエリア）は、MLD Done メッセージが受信されたときに MLD Group-Specific Query メッセージを送信します。ルータ/クエリアは、指定されたタイムアウト時間内に MLD Group-Specific Query メッセージに応答する受信者がない場合に限り、そのグループのトラフィックの転送を停止します。
  MLD 即時離脱機能が有効の場合、スイッチは 1 つの受信者だけがインタフェースに接続されているとみなします。したがって、インタフェースが 1 台の MLD 対応デバイス（MLD snooping を実行しているサービスホストまたはネイバー）に接続されている場合のみ、MLD 即時離脱機能を使用してください。
- Immediate Leave By Host - そのポート上のすべての受信者がグループを離れるときだけ、メンバーポートは削除されます。(デフォルト: Disabled)

Web インタフェース

MLD 即時離脱機能を設定するには：

1. [Multicast]、[MLD Snooping]、[Interface]をクリックします。
2. VLAN を選択し、MLD 即時離脱機能のステータスを設定します。
3. [Apply]をクリックします。

図 13-22　MLD 即時離脱機能の設定

13.4.3 マルチキャストルータポートの Static 設定

[Multicast]> [MLD Snooping]>[Multicast Router（Add Static Multicast Router）]ページを使用して、マルチキャストルータポートを Static に設定します。

ネットワーク接続によっては、MLD snooping が MLD クエリアを検出できないことがあります。したがって、MLD クエリアが、スイッチ上のインタフェース（ポートまたはトランク）にネットワーク経由で接続されている既知のマルチキャストルータ/スイッチである場合、そのインタフェースを手動でマルチキャストルータポートに設定することができます。

コマンドの使用方法

マルチキャストルータポートを有効にするには、スイッチ上で MLD snooping をグローバルに有効にする必要があります。

パラメータ

次のパラメータが表示されます。

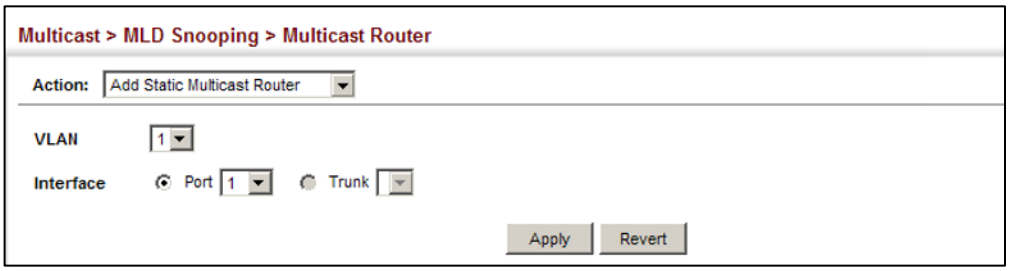
- VLAN - マルチキャストルータポートを設定する VLAN を選択します。(範囲: 1 から 4094)
- Interface - ポートまたはトランクのスクロールダウンリストをアクティブにします。
  - Port or Trunk - マルチキャストルータポートに設定するインタフェースを指定します。

Web インタフェース

マルチキャストルータポートを Static に指定する手順は、次のとおりです。

1. [Multicast]、[MLD Snooping]、[Multicast Router]をクリックします。
2. [Action]リストから[Add Static Multicast Router]を選択します。
3. マルチキャストルータポートを設定する VLAN を選択し、マルチキャストルータポートに設定するポートまたはトランクを選択します。
4. [Apply]をクリックします。

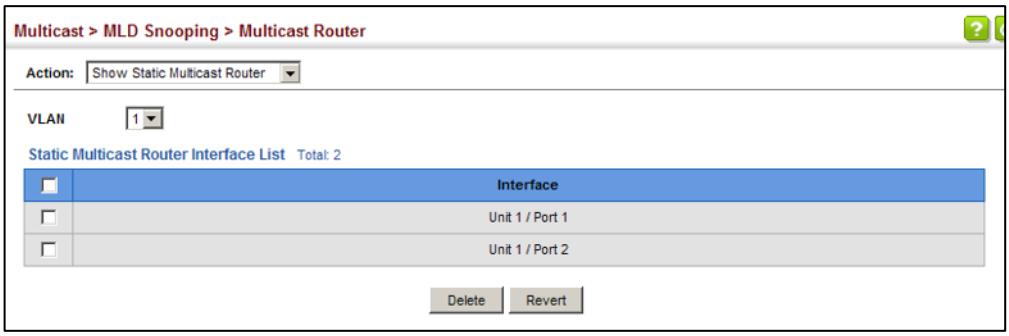
図 13-23　Static マルチキャストルータポートの設定



Static に設定したマルチキャストルータポートを表示するには、

1. [Multicast]、[MLD Snooping]、[Multicast Router]をクリックします。
2. [Action]リストから[Show Static Multicast Router]を選択します。
3. この情報を表示する VLAN を選択します。

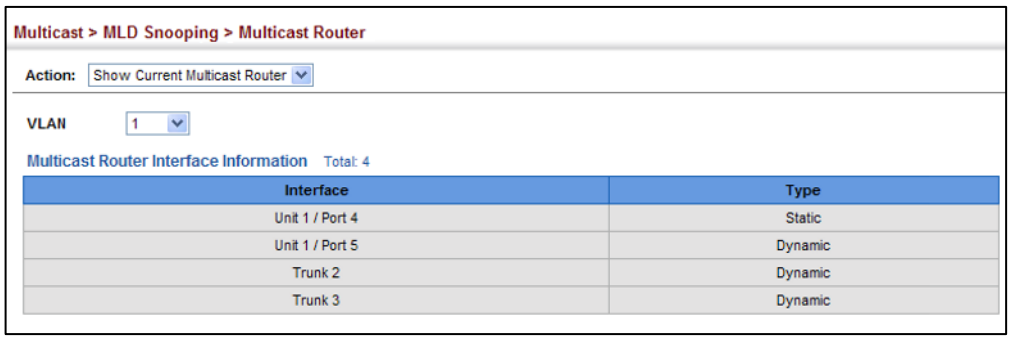
図 13-24　Static マルチキャストルータポートの表示



すべてのマルチキャストルータポートを表示するには、

1. [Multicast]、[MLD Snooping]、[Multicast Router]をクリックします。
2. [Action]リストから[Show Current Multicast Router]を選択します。
3. この情報を表示する VLAN を選択します。選択された VLAN 内のマルチキャストルータポートが表示されます。

図 13-25　現在設定されているマルチキャストルータポートを表示



13.4.4 Static エントリの設定

[Multicast]> [MLD Snooping]> [MLD Member（Add Static Member）]ページを使用して、Static エントリをインタフェースに割当てます。

マルチキャストフィルタリングは、MLD snooping と MLD Query メッセージを使用して Dynamic に設定できます。ただし、厳重な制御が必要なアプリケーションでは、スイッチ上でエントリを Static に設定する必要があります。Static エントリは該当する VLAN にマルチキャストサービスを設定して、当該マルチキャストサービスの受信者を接続しているすべてのポートを割当てます。

コマンドの使用方法

- Static エントリは決してエージングアウトされません。
- Static エントリが VLAN に割当てられると、対応するトラフィックはその VLAN 内の Static エントリに設定したポートにのみ転送されます。

パラメータ

次のパラメータが表示されます。

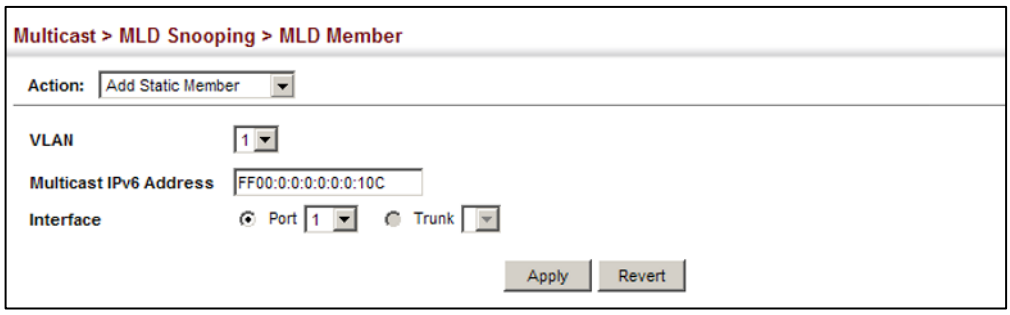
- VLAN - Static エントリを設定する VLAN を指定します。(範囲: 1 から 4094)
- Multicast IPv6 Address - Static エントリのマルチキャストグループアドレスを設定します。
- Interface - ポートまたはトランクのスクロールダウンリストをアクティブにします。
  - Port or Trunk - マルチキャストパケットを中継するインタフェースを指定します。
- Type (Show Current Member) - このマルチキャストストリームが、管理者によって Static に設定されたか、MLD snooping によって Dynamic に設定されたか、または未学習のマルチキャストパケットであるかどうかを示します。

Web インタフェース

インタフェースを IPv6 マルチキャストサービスに Static に設定するには、次の手順を実行します。

1. [Multicast]、[MLD Snooping]、[MLD Member]をクリックします。
2. [Action]リストから[Add Static Member]を選択します。
3. Static エントリ設定する VLAN を選択し、マルチキャストグループアドレスを設定して、当該マルチキャストパケットを中継するインタフェースを指定します。
4. [Apply]をクリックします。

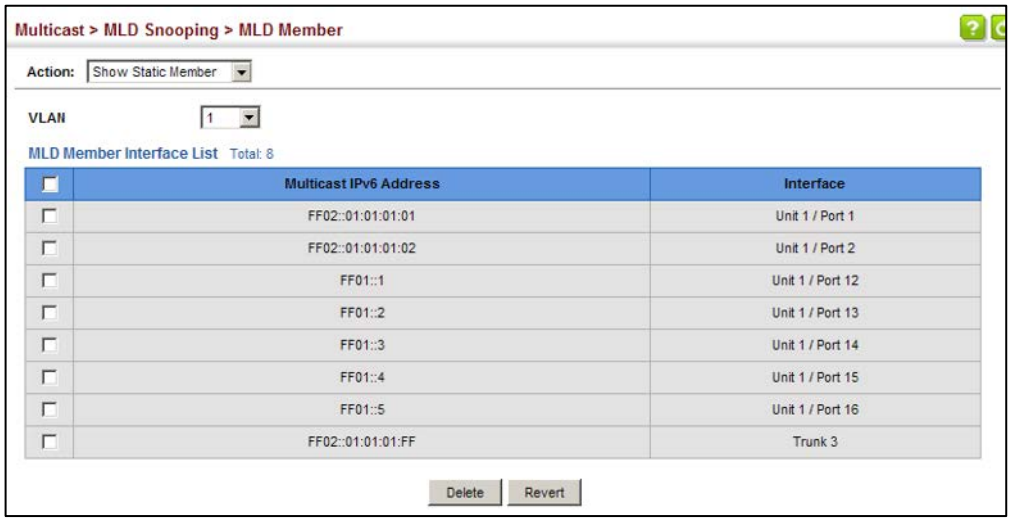
図 13-26　Static エントリの設定



Static エントリを表示するには、

1. [Multicast]、[MLD Snooping]、[MLD Member]をクリックします。
2. [Action]リストから[Show Static Member]を選択します。
3. この情報を表示する VLAN を選択します。

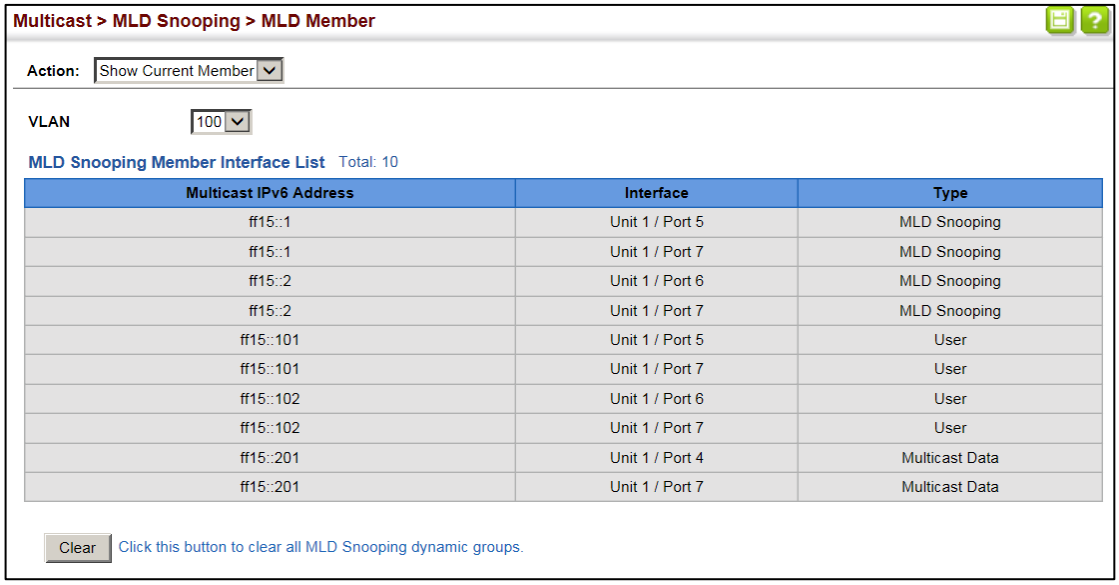
図 13-27　Static エントリの表示



すべての Static エントリに関する情報を表示するには、まずスイッチ上で MLD snooping またはマルチキャストルーティングを有効にする必要があります。Static または Dynamic に割当てられたすべてのエントリを表示するには、次の手順を実行します。

1. [Multicast]、[MLD Snooping]、[MLD Member]をクリックします。
2. [Action]リストから[Show Current Member]を選択します。
3. この情報を表示する VLAN を選択します。

図 13-28　現在学習しているすべてのエントリの表示



13.4.5 エントリとソースリストの表示

[Multicast]> [MLD Snooping]>[Group Information]ページを使用して、学習エントリ、メンバーポート、各グループの学習方法、および対応する送信元リストを表示します。

パラメータ

次のパラメータが表示されます。

- VLAN - VLAN ID です。(範囲: 1 から 4094)
- Interface - ポートまたはトランクの識別子です。
- Group Address - 特定のマルチキャストサービスの IP アドレスです。
- Type - 各グループが学習した手段 - MLD snooping またはマルチキャストデータです。
- Filter Mode - フィルタモードは、マルチキャストアドレスの全リスニング状態を、すべてのノードのリスニング状態が尊重されるような最小限の集合に要約するために使用されます。Include モードでは、ルータは要求リストのみを使用し、指定されたマルチキャストアドレスに送信されたパケットの受信は、ホストの source-list にリストされている IP 送信元アドレスからのみ要求されます。Exclude モードでは、ルータは要求リストと除外リストの両方を使用して、指定されたマルチキャストアドレスに送信されたパケットの受信がすべての IP 送信元アドレスから要求されたことを示します。除外ソースリストにリストされているものと、ソースタイマーのステータスが期限切れになっているその他のソースの場合を除きます。
- Filter Timer Elapse - フィルタタイマーは、特定のマルチキャストアドレスが除外モードの場合にのみ使用されます。これは、マルチキャストアドレスフィルタモードが期限切れになり、Include モードに切り替わる時間を表します。
- Request List - ルータのリクエストリストに含まれるソースです。
- Exclude List - ルータの除外リストに含まれる送信元です。

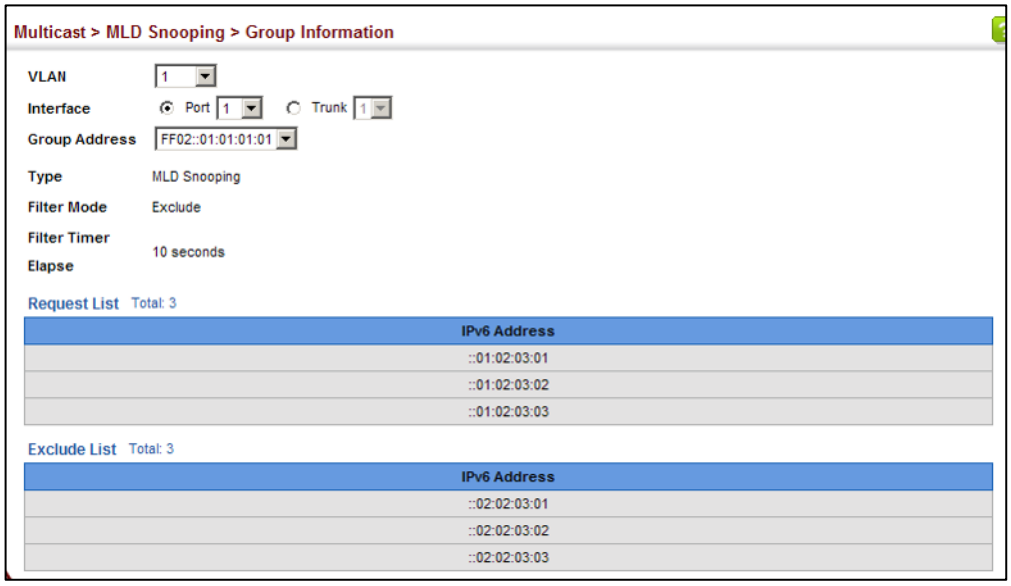
Web インタフェース

学習エントリと送信元情報を表示するには：

1. [Multicast]、[MLD Snooping]、[Group Information]をクリックします。

2. ポートまたはトランクを選択し、そのインタフェースで学習しているマルチキャストグループアドレスを選択します。

図 13-29　学習エントリとそれに対応する送信元情報の表示



13.4.6 MLD snooping 統計情報の表示

MLD snooping 関連の統計情報を表示するには、[Multicast]> [MLD Snooping]>[Statistics]ページを使用します。

パラメータ

次のパラメータが表示されます。

- Type - 表示する統計情報を指定します。「Input」、「Output」、「Query」、「Summary」、「Clear」から選択します。

Input：

次のパラメータが表示されます。

- Interface - ユニット/ポート、トランク識別子または VLAN インタフェースです。
- Report - このインタフェースで受信した MLD Report メッセージの数です。
- Leave - このインタフェースで受信した MLD Done メッセージの数です。
- G Query - このインタフェースで受信した MLD General Query メッセージの数です。
- G(-S)-S Query - このインタフェースで受信した MLD Group-Specific Query メッセージまたは MLD Group-and-Source-Specific Query メッセージの数です。
- Drop - MLD Query、Report、Done メッセージがドロップされた回数です。無効な形式、レート制限、パケット内容が許可されていないため、パケットがドロップされる可能性があります。
- Join Success - マルチキャストグループが正常に参加した回数です。
- Group - このインタフェースでアクティブな MLD グループの数です。

Output：

上記の「Input」のパラメータと同じですが、カウントが送信数である点が異なります。

Query：

次のパラメータが表示されます。

- VLAN - VLAN ID です。(範囲: 1 から 4094)
- Other Querier Address - このインタフェース上のリモートクエリアの IP アドレスです。
- Other Querier Expire - リモートクエリアが期限切れになるまでの時間です。
- Other Querier Uptime - リモートクエリアを検出してからの経過時間です。
- Self Querier Address - ローカルクエリアの IP アドレスです。
- Self Querier Expire Time - ローカルクエリアが期限切れになるまでの時間です。
- Self Querier Uptime - ローカルクエリアに設定してからの経過時間です。
- General Query Received - このインタフェースで受信した MLD General Query メッセージの数です。
- General Query Sent - このインタフェースから送信した MLD General Query メッセージの数です。
- Specific Query Received - このインタフェースで受信した MLD Specific Query メッセージの数です。
- Specific Query Sent - このインタフェースから送信した MLD Specific Query メッセージの数です。

Summary：

次のパラメータが表示されます。

- VLAN - VLAN ID です。(範囲: 1 から 4094)
- Unit - スタックユニットです。(範囲: 1)
- Port - ポート番号です。(範囲: 1 から 10)
- Trunk - トランク識別子です。(範囲: 1-8)

VLAN インタフェース指定時、以下のパラメータを表示します。

- Number of Groups - 指定されたインタフェース上でアクティブな MLD グループの数です。
- Querier
  - Other Querier - このインタフェース上のリモートクエリアの IPv6 アドレスです。
  - Other Uptime - リモートクエリアを検出してからの経過時間です。
  - Other Expire - リモートクエリアが期限切れになるまでの時間です。
  - Self Addr - このインタフェース上のローカルクエリアの IPv6 アドレスです。
  - Self Expire - ローカルクエリアが期限切れになるまでの時間です。
  - Self Uptime - ローカルクエリアが有効になってからの経過時間です。
  - Transmit
    - General - このインタフェースから送信した MLD General Query メッセージの数です。
    - Group Specific - このインタフェースから送信した MLD Group-Specific Query メッセージの数です。
  - Recieved
    - General - このインタフェースで受信した MLD General Query メッセージの数です。
    - Group Specific - このインタフェースで受信した MLD Group-Specific Query メッセージの数です。
- Report & Leave
  - Host Addr - その VLAN に割当てられているリンクローカルまたはグローバル IPv6 アドレスです。
  - Unsolicit Expire - プロキシ機能使用時の MLD Report メッセージを送信するまでの時間です。
  - Transmit
    - Report - このインタフェースから送信した MLD Report メッセージの数です。

- Leave - このインタフェースから送信した MLD Done メッセージの数です。

■ Recieved

- Report - このインタフェースで受信した MLD Report メッセージの数です。
- Leave - このインタフェースで受信した MLD Done メッセージの数です。
- Join Success - マルチキャストグループが正常に参加した回数です。
- Filter Drop - MLD フィルタリングでドロップした MLD メッセージの数です。
- Source Port Drop -マルチキャストルータポートでドロップした MLD メッセージの数です。
- Others Drop - 受信した無効な MLD メッセージの数です。

物理インタフェース（ポート/トランク）指定時、以下のパラメータを表示します。

◆ Number of Groups - 指定されたインタフェース上でアクティブなアクティブ MLD グループの数です。

◆ Querier

■ Transmit

- General - このインタフェースから送信した MLD General Query メッセージの数です。
- Group Specific - このインタフェースから送信した MLD Group-Specific Query メッセージの数です。

■ Recieved

- General - このインタフェースで受信した MLD General Query メッセージの数です。
- Group Specific - このインタフェースで受信した MLD Group-Specific Query メッセージの数です。

◆ Report & Leave

■ Transmit

- Report - このインタフェースから送信した MLD Report メッセージの数です。
- Leave - このインタフェースから送信した MLD Done メッセージの数です。

■ Recieved

- Report - このインタフェースで受信した MLD Report メッセージの数です。
- Leave - このインタフェースで受信した MLD Done メッセージの数です。
- Join Success - マルチキャストグループが正常に参加した回数です。
- Filter Drop - MLD フィルタリングでドロップした MLD メッセージの数です。
- Source Port Drop -マルチキャストルータポートでドロップした MLD メッセージの数です。
- Others Drop - 受信した無効な MLD メッセージの数です。

Clear：

次のパラメータが表示されます。

◆ All - すべての MLD メッセージの統計情報をクリアします。

◆ VLAN - VLAN ID です。(範囲: 1 から 4094)

◆ Unit - スタックユニットです。(範囲: 1)

◆ Port - ポート番号です。(範囲: 1 から 10)

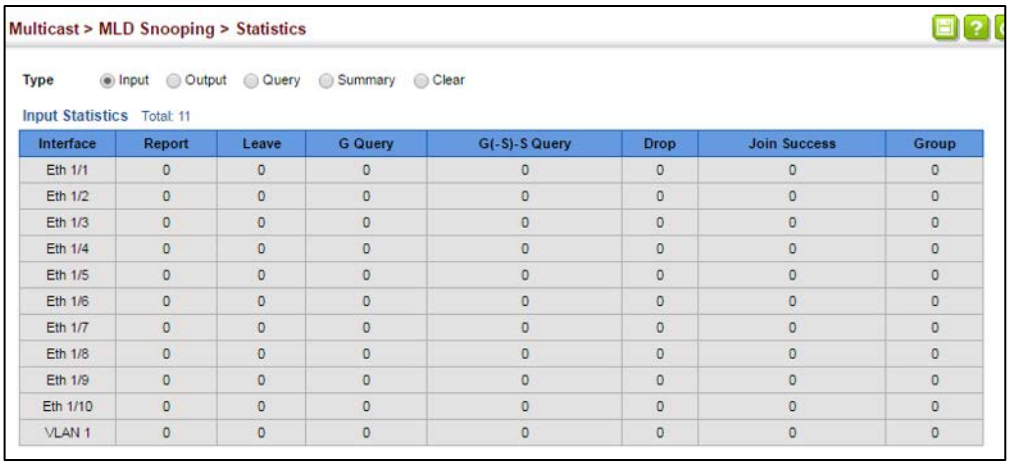
◆ Trunk - トランク ID です。(範囲: 1-8)

Web インタフェース

MLD snooping の入力関連の統計情報を表示するには、次の手順を実行します。

1. [Multicast]、[MLD Snooping]、[Statistics]をクリックします。
2. Input を選択します。

図 13-30　MLD snooping 統計情報の表示 - Input 関連

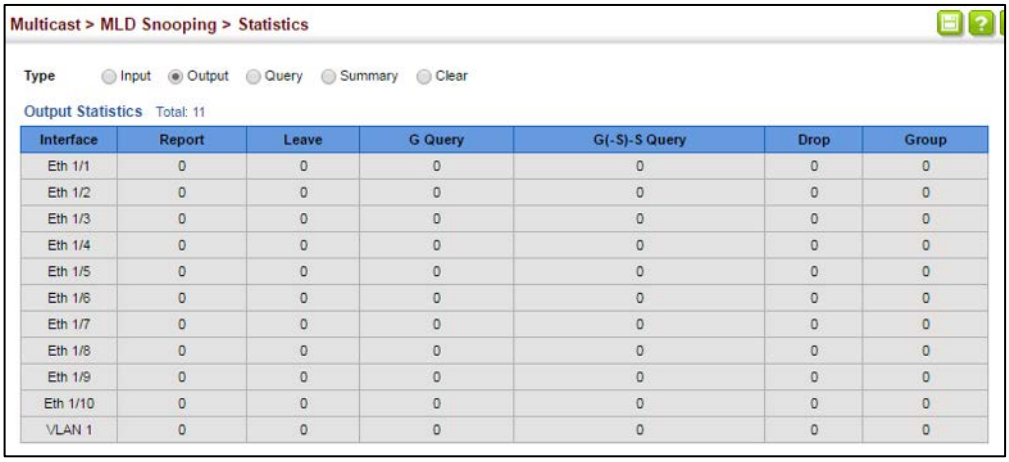


Interface	Report	Leave	G Query	G(-S)-S Query	Drop	Join Success	Group
Eth 1/1	0	0	0	0	0	0	0
Eth 1/2	0	0	0	0	0	0	0
Eth 1/3	0	0	0	0	0	0	0
Eth 1/4	0	0	0	0	0	0	0
Eth 1/5	0	0	0	0	0	0	0
Eth 1/6	0	0	0	0	0	0	0
Eth 1/7	0	0	0	0	0	0	0
Eth 1/8	0	0	0	0	0	0	0
Eth 1/9	0	0	0	0	0	0	0
Eth 1/10	0	0	0	0	0	0	0
VLAN 1	0	0	0	0	0	0	0

MLD スヌーピングの出力関連の統計情報を表示するには、次の手順を実行します。

1. [Multicast]、[MLD Snooping]、[Statistics]をクリックします。
2. Output を選択します。

図 13-31　MLD snooping 統計情報の表示 - Output 関連

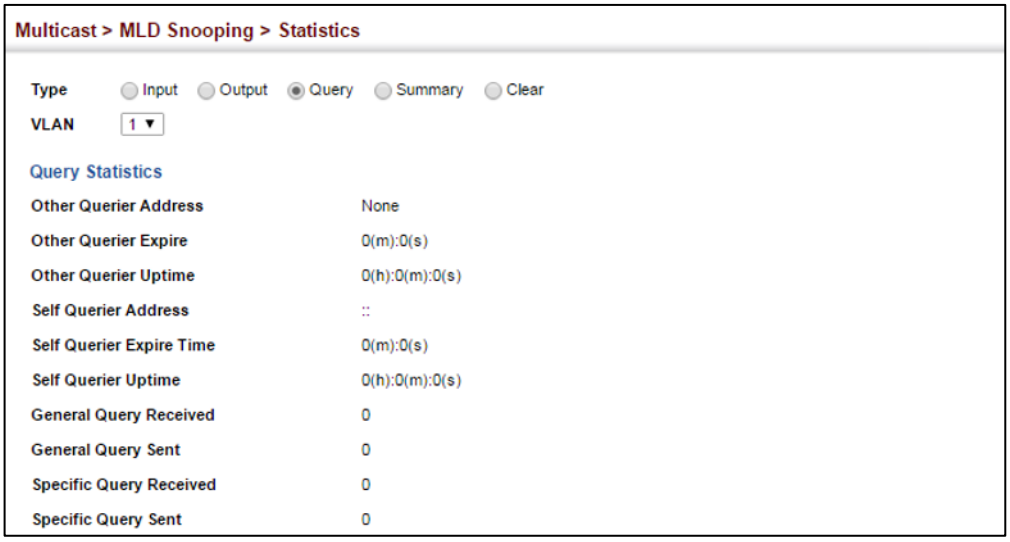


Interface	Report	Leave	G Query	G(-S)-S Query	Drop	Group
Eth 1/1	0	0	0	0	0	0
Eth 1/2	0	0	0	0	0	0
Eth 1/3	0	0	0	0	0	0
Eth 1/4	0	0	0	0	0	0
Eth 1/5	0	0	0	0	0	0
Eth 1/6	0	0	0	0	0	0
Eth 1/7	0	0	0	0	0	0
Eth 1/8	0	0	0	0	0	0
Eth 1/9	0	0	0	0	0	0
Eth 1/10	0	0	0	0	0	0
VLAN 1	0	0	0	0	0	0

MLD Query メッセージの統計情報を表示するには：

1. [Multicast]、[MLD Snooping]、[Statistics]をクリックします。
2. Query を選択します。

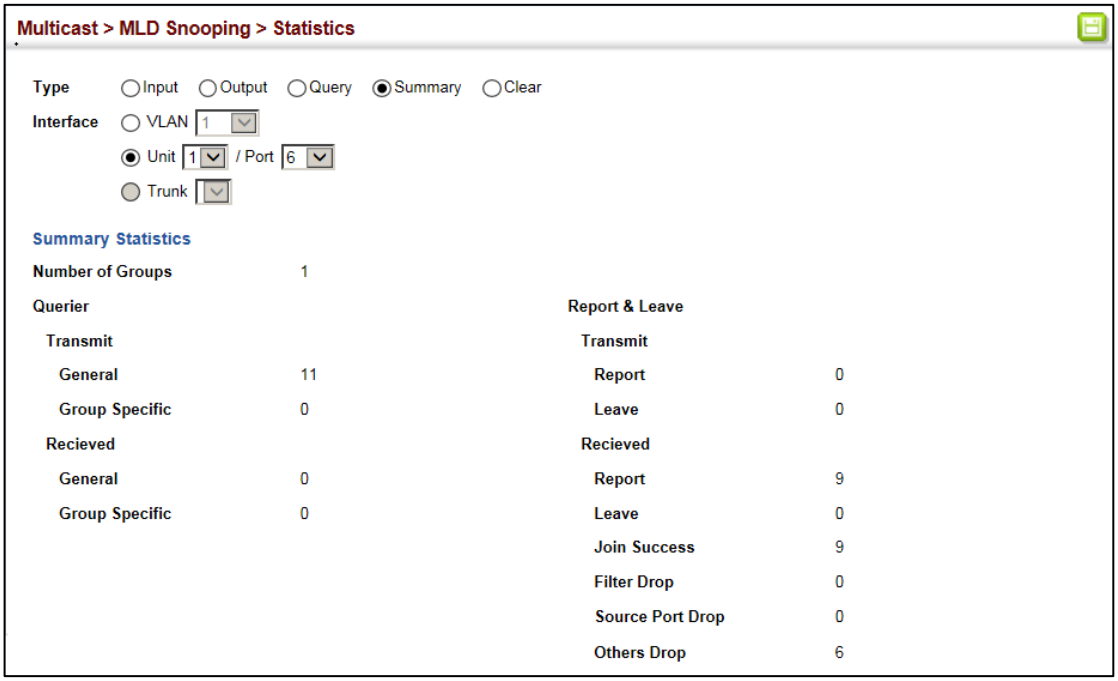
図 13-32　MLD snooping 統計情報の表示 - クエリア関連



ポートまたはトランクの統計情報の Summary を表示するには、次の手順を実行します。

1. [Multicast]、[MLD Snooping]、[Statistics]をクリックします。
2. Summary を選択します。
3. [Unit]/[Port]または[Trunk]を選択します。

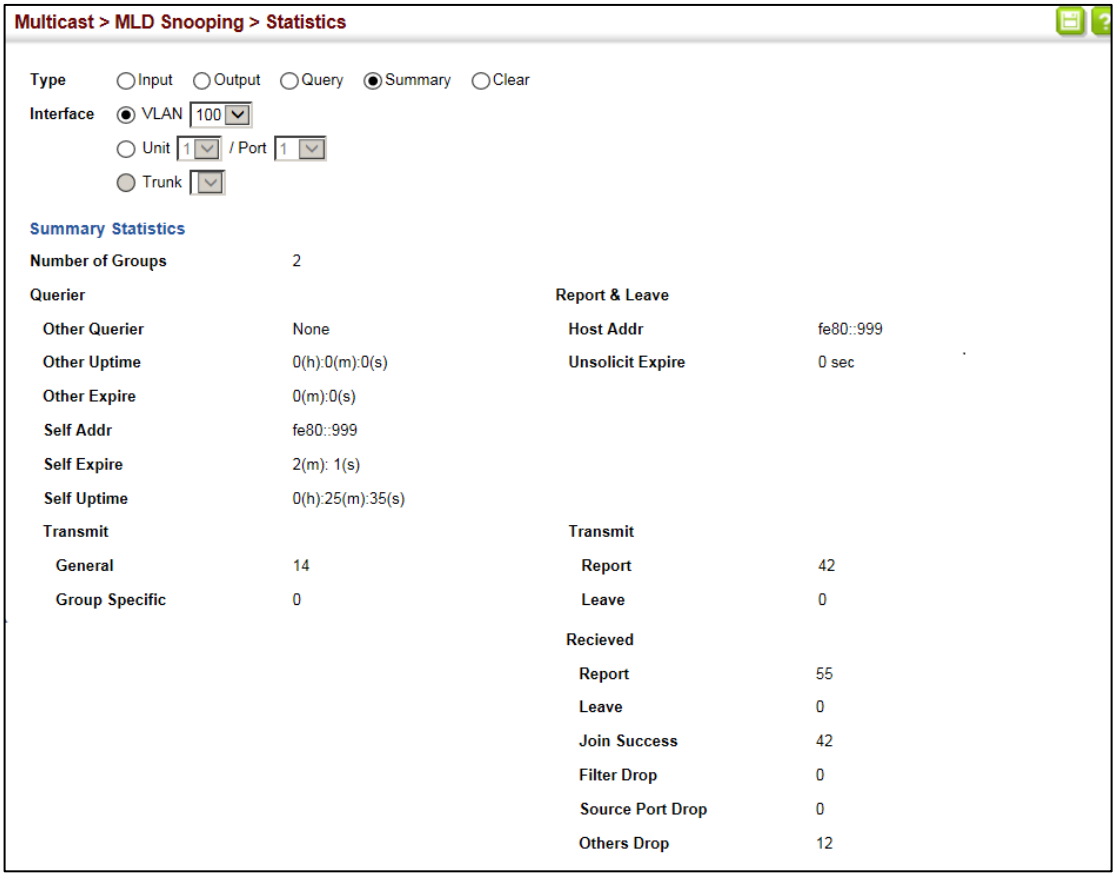
図 13-33　MLD snooping 統計情報の表示 – Summary（ポート/トランク）



VLAN の統計情報の Summary を表示するには、次の手順を実行します。

1. [Multicast]、[MLD Snooping]、[Statistics]をクリックします。
2. Summary を選択します。
3. VLAN を選択します。

図 13-34　MLD snooping 統計情報の表示 - Summary（VLAN）



MLD 統計情報を消去するには：

1. [Multicast]、[MLD Snooping]、[Statistics]をクリックします。
2. Clear を選択します。
3. [All]を選択するか、必要なインタフェースを入力します。
4. [Clear]をクリックします。

図 13-35　MLD snooping 統計情報の消去

13.5 MLD フィルタリングとスロットリング

特定のスイッチアプリケーションでは、管理者はエンドユーザが使用できるマルチキャストサービスを制御したい場合があります。たとえば、特定のサブスクリプションプランに基づく IP / TV サービスです。MLD フィルタリング機能は、スイッチポート上の指定されたマルチキャストサービスへのアクセスを制限することによってこの要件を満たし、MLD スロットリングは、ポートが参加できる同時マルチキャストグループの数を制限します。

MLD フィルタリングを使用すると、ポート上で許可または拒否されるマルチキャストグループを指定するスイッチポートにプロファイルを割当てることができます。MLD フィルタプロファイルには、1 つまたは複数のアドレス、またはマルチキャストアドレスの範囲を含めることができます。 ポートに割当てられるプロファイルは 1 つだけです。有効にすると、ポートで受信した MLD Report メッセージがフィルタプロファイルと照合されます。要求されたマルチキャストグループが許可されている場合、MLD Report メッセージは通常どおり転送されます。要求されたマルチキャストグループが拒否された場合、MLD Report メッセージは破棄されます。

MLD スロットリングは、ポートが同時に参加できるマルチキャストグループの最大数を設定します。1 つのポートで最大グループ数に達すると、スイッチは 2 つのアクションのいずれかをとることができます。「Deny」または「Replace」のいずれかです。アクションが Deny に設定されている場合、新しい MLD Report メッセージはすべて廃棄されます。アクションが Replace に設定されている場合、スイッチはランダムに既存のグループを削除し、新しいマルチキャストグループに置換えます。

13.5.1 MLD フィルタリングとスロットリングの有効化

スイッチ上で MLD フィルタリングと MLD スロットリングをグローバルに有効にするには、[Multicast]> [MLD Snooping]> [Filter（Configure General）]ページを使用します。

パラメータ

次のパラメータが表示されます。

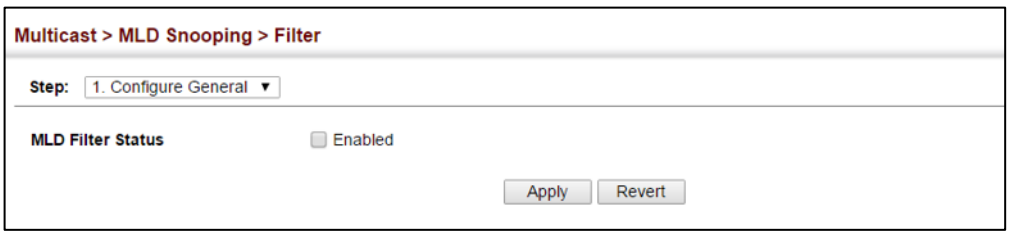
◆ MLD Filter Status - スイッチの MLD フィルタリングと MLD スロットリングをグローバルに有効にします。(デフォルト: Disabled)

Web インタフェース

スイッチ上で MLD フィルタリングおよび MLD スロットリングを有効にするには：

1. [Multicast]、[MLD Snooping]、[Filter]をクリックします。
2. [Step]リストから[Configure General]を選択します。
3. MLD フィルタのステータスを有効にします。
4. [Apply]をクリックします。

図 13-36　MLD フィルタリングと MLD スロットリングの有効化



13.5.2 MLD フィルタプロファイルの設定

[Multicast]> [MLD Snooping]> [Filter（プロファイルの設定 - 追加）]ページを使用して MLD プロファイルを作成し、アクセスモードを設定します。次に、[Add Multicast Group Range]ページを使用して、フィルタリングするマルチキャストグループを設定します。

コマンドの使用方法

フィルタの対象となるマルチキャストグループの範囲を指定します。指定方法は開始となるアドレスと終了となるアドレスを指定します。範囲の開始と終了に同じ IPv6 アドレスを入力して単一のマルチキャストグループを指定することもできます。

パラメータ

指定した Action ごとに、次のパラメータが表示されます。

Add：

- Profile ID - MLD プロファイルを作成します。(範囲: 1 から 40)
- Access Mode - プロファイルのアクセスモードを設定します。 Permit または Deny のいずれかです。(デフォルト: Deny)
  アクセスモードが Permit に設定されている場合、マルチキャストグループが制御された範囲内に入ると、MLD Report メッセージが処理されます。アクセスモードが Deny に設定されている場合、MLD Report メッセージは、マルチキャストグループが設定された範囲にない場合にのみ処理されます。

Add Multicast Group Range：

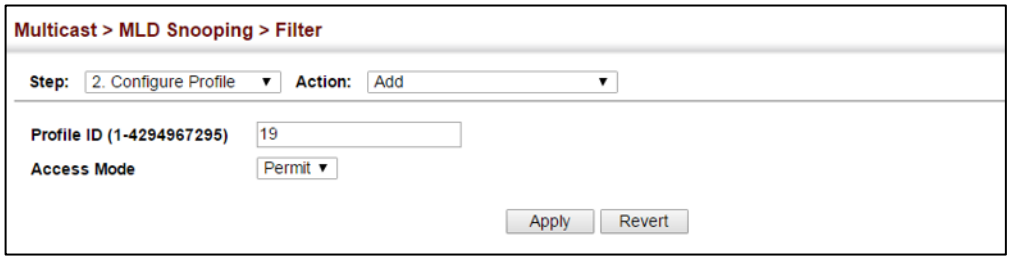
- Profile ID - 設定する MLD プロファイルを選択します。
- Start Multicast IPv6 Address - マルチキャストグループの範囲の開始アドレスを指定します。
- End Multicast IPv6 Address - マルチキャストグループの範囲の終了アドレスを指定します。

Web インタフェース

MLD フィルタプロファイルを作成し、そのアクセスモードを設定するには：

1. [Multicast]、[MLD Snooping]、[Filter]をクリックします。
2. [Step]リストから[Configure Profile]を選択します。
3. [Action]リストから[Add]を選択します。
4. プロファイルの番号を入力し、アクセスモードを設定します。
5. [Apply]をクリックします。

図 13-37　MLD フィルタリングプロファイルの作成

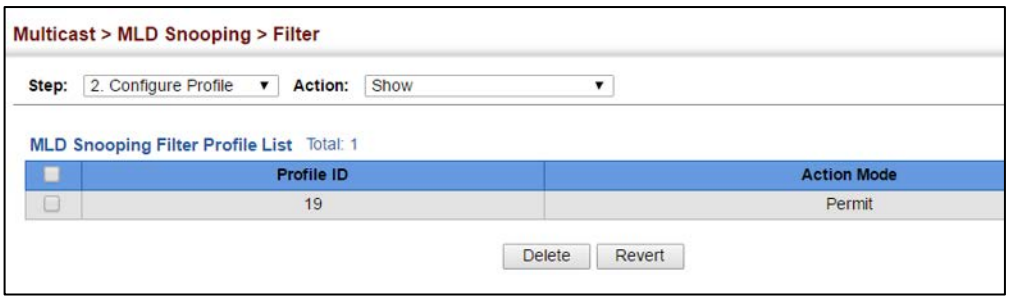


MLD フィルタプロファイルを表示するには：

1. [Multicast]、[MLD Snooping]、[Filter]をクリックします。
2. [Step]リストから[Configure Profile]を選択します。

3. [Action]リストから[Show]を選択します。

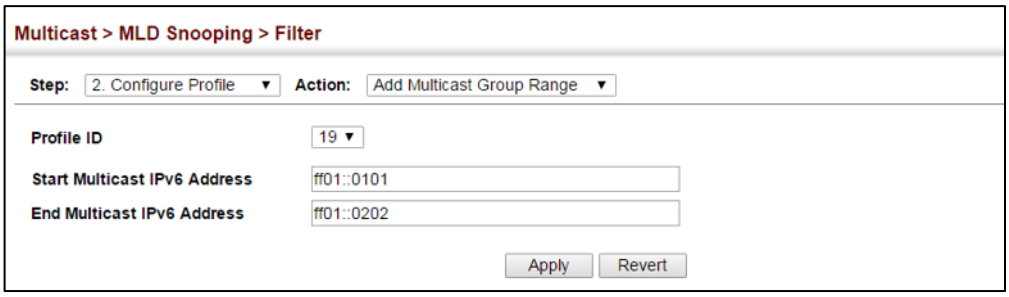
図 13-38　作成された MLD フィルタリングプロファイルの表示



MLD フィルタプロファイルにマルチキャストグループの範囲を追加するには：

1. [Multicast]、[MLD Snooping]、[Filter]をクリックします。
2. [Step]リストから[Configure Profile]を選択します。
3. [Action]リストから[Add Multicast Group Range]を選択します。
4. 設定するプロファイルを選択し、マルチキャストグループアドレスまたはアドレス範囲を追加します。
5. [Apply]をクリックします。

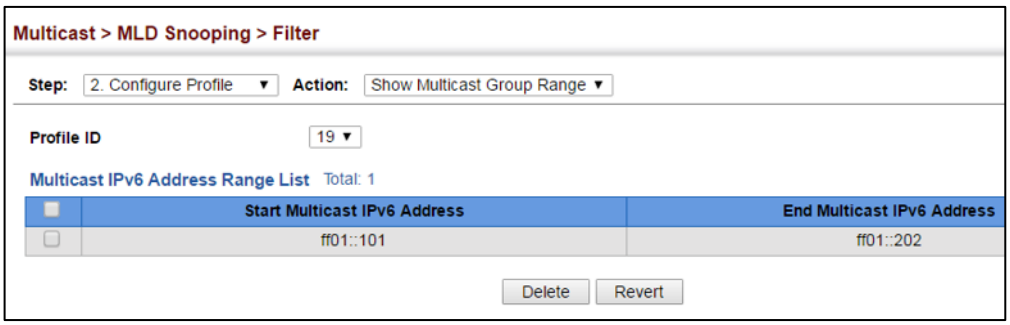
図 13-39　MLD フィルタリングプロファイルへのマルチキャストグループの追加



MLD フィルタプロファイル用に設定されたマルチキャストグループを表示するには：

1. [Multicast]、[MLD Snooping]、[Filter]をクリックします。
2. [Step]リストから[Configure Profile]を選択します。
3. [Action]リストから[Show Multicast Group Range]を選択します。
4. この情報を表示するプロファイルを選択します。

図 13-40　MLD フィルタリングプロファイルに割当てられたグループの表示



13.5.3 インタフェースの MLD フィルタリングおよびスロットリングの設定

[Multicast]> [MLD Snooping]> [Filter（インタフェースの設定）]ページを使用して、スイッチ上のインタフェースに MLD フィルタプロファイルを割当てたり、インタフェースが同時に参加できるマルチキャストグループの最大数を制限してマルチキャストトラフィックを制御します。

コマンドの使用方法

- MLD スロットリングは、ポートが同時に参加できるマルチキャストグループの最大数を設定します。1 つのポートで最大グループ数に達すると、スイッチは 2 つのアクションのいずれかをとることができます。 「Deny」または「Replace」のいずれかです。アクションが Deny に設定されている場合、新しい MLD Report メッセージはすべて削除されます。アクションが Replace に設定されている場合、スイッチはランダムに既存のグループを削除し、新しいマルチキャストグループに置換えます。

パラメータ

次のパラメータが表示されます。

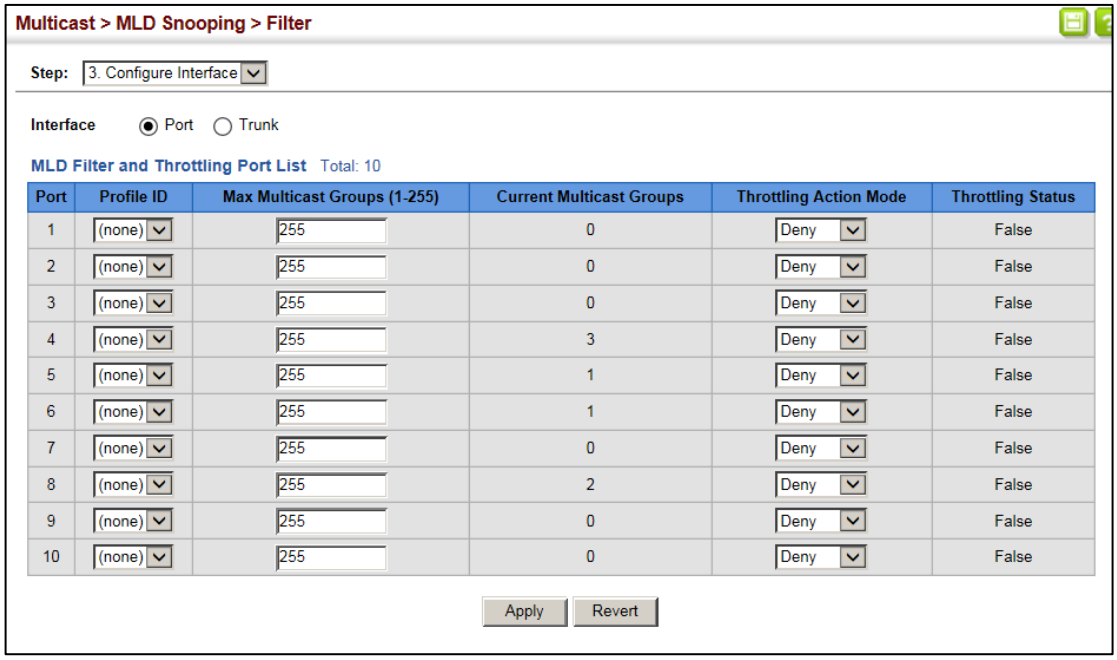
- Interface - ポートまたはトランクの識別子です。
  MLD プロファイルまたは MLD スロットリングの設定は、ポートまたはトランクに適用できます。ポートがトランクメンバーとして設定されている場合、トランクはトランクの最初のポートメンバーに適用された設定を使用します。
- Profile ID - インタフェースに割当てる既存のプロファイルを選択します。
- Max Multicast Groups - インタフェースが同時に参加できるマルチキャストグループの最大数を設定します。(範囲: 1 から 255; デフォルト: 255)
- Current Multicast Groups - インタフェースが参加している現在のマルチキャストグループを表示します。
- Throttling Action Mode - インタフェースの最大マルチキャストグループ数を超えた場合に実行するアクションを設定します。(デフォルト: Deny)
  - Deny - 超過後に受信した MLD Report メッセージを破棄します。
  - Replace - 超過後に受信した MLD Report メッセージのマルチキャストグループは、既存のグループと置換えます。
- Throttling Status - MLD スロットリングの状態を表示します。(オプション: True または False)

Web インタフェース

ポートまたはトランクの MLD フィルタリングまたは MLD スロットリングを設定するには：

1. [Multicast]、[MLD Snooping]、[Filter]をクリックします。
2. [Step]リストから[Configure Interface]を選択します。
3. インタフェースに割当てるプロファイルを選択し、マルチキャストグループの最大数と最大マルチキャストグループ数を超えた場合に実行するアクションを設定します。
4. [Apply]をクリックします。

図 13-41　インタフェースへの MLD のフィルタリングおよび MLD スロットリングの設定



13.5.4 インタフェース上の MLD Query メッセージのフィルタリング

[Multicast]> [MLD Snooping]> [Query Drop]ページを使用して、MLD Query メッセージを廃棄するインタフェースを設定します。

パラメータ

次のパラメータが表示されます。

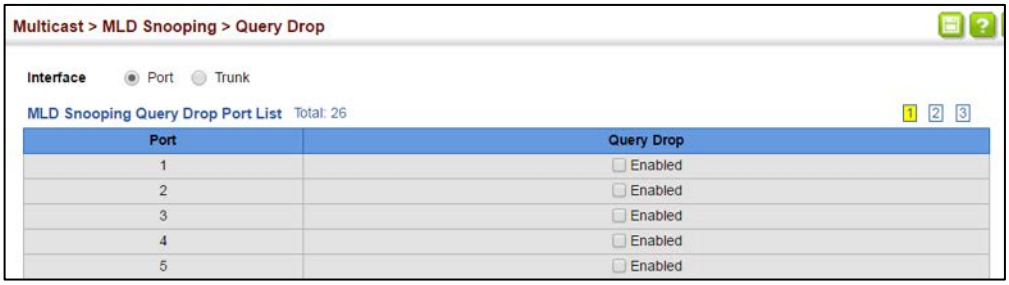
- Interface - ポートまたはトランクの識別子です。
- Query Drop - 受信した MLD Query メッセージをすべて破棄します。(デフォルト: Disabled)
  この機能を使用すると、指定したインタフェースで受信した MLD Query メッセージをすべて破棄できます。このスイッチがクエリアとして動作している場合、別のクエリアから受信した MLD Query メッセージの影響を受けません。

Web インタフェース

MLD Query メッセージを廃棄するには

1. [Multicast]、[MLD Snooping]、[Query Drop]をクリックします。
2. ポートまたはトランクインタフェースを選択します。
3. 任意のインタフェースの Query Drop を Enabled にします。
4. [Apply]をクリックします。

図 13-42　MLD Query メッセージの廃棄



14 IP ツール

この章では、以下を含むネットワーク機能に関する情報を提供します。

- Ping - ping メッセージをネットワーク上の別のノードに送信します。
- Trace Route - 指定された宛先へのパケットのルートを表示します。
- Address Resolution Protocol - プロキシ ARP または静的アドレスを設定する方法、および ARP キャッシュにエントリを表示する方法について説明します。

14.1 ping の使用

[Tools]> [Ping]ページを使用して、ICMP エコー要求パケットをネットワーク上の別のノードに送信します。

パラメータ

次のパラメータが表示されます。

- Host Name/IP Address - ホストのエイリアスまたは IPv4 / IPv6 アドレスです。
- Probe Count - 送信するパケット数です。(範囲: 1 から 16)
- Packet Size - パケットのバイト数です。(範囲: IPv4 の場合は 32 から 512 バイト、IPv6 の場合は 0 から 1500 バイト）
  実際のパケットサイズは、スイッチがヘッダー情報を追加するため、指定されたサイズより 8 バイト大きくなります。

コマンドの使用方法

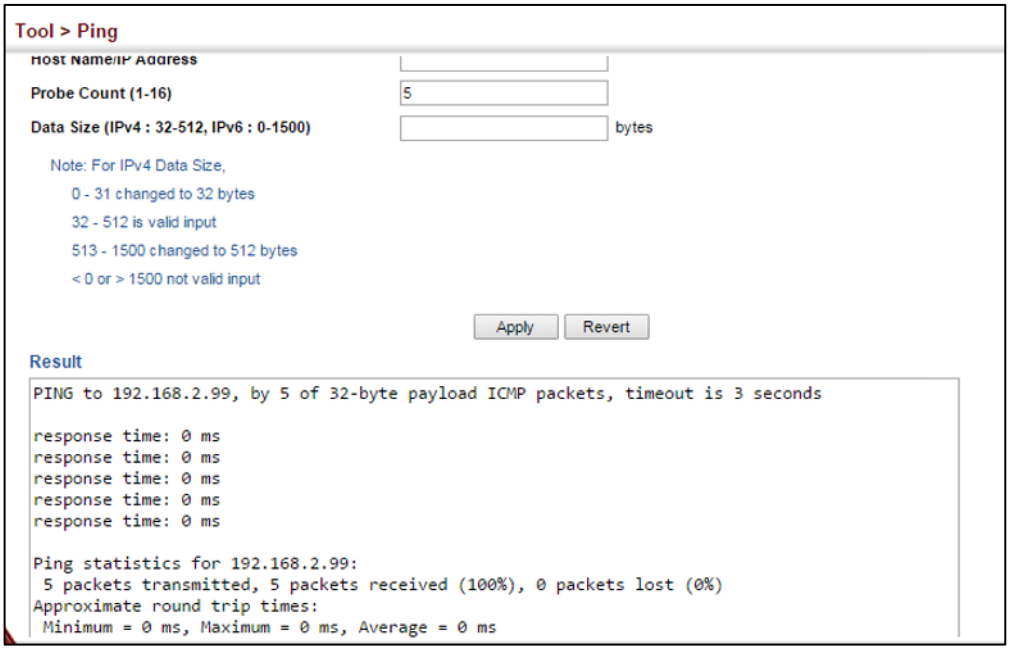
- ping コマンドを使用して、ネットワーク上の他のサイトがネットワークに到達できるかを確認します。
- 以下は、ping コマンドのいくつかの結果です:
  - Normal response - 通常応答がネットワークのトラフィック状態に応じて、0 秒から 10 秒以内に発生します。
  - Destination does not respond - ホストが応答しない場合、“timeout”が 10 秒以内に表示されます。
  - Destination unreachable - 宛先のゲートウェイが、宛先に到達できないことを示しています。
  - Network or host unreachable - ゲートウェイは、ルートテーブルに対応するエントリが見つかりませんでした。
- 同じリンクローカルアドレスは、異なるゾーン（RFC 4007）の異なるインタフェース/ノードによって使用されることがあります。したがって、リンクローカルアドレスを指定する場合は、%デリミタの後に VLAN 識別子を示す zone-id 情報を含めます。たとえば、FE80::7272%1 は VLAN 1 をインタフェースとして識別します。

Web インタフェース

ネットワーク上の別のデバイスに ping を実行するには：

1. [Tools]、[Ping]をクリックします。
2. ターゲットデバイスと ping パラメータを指定します。
3. [Apply]をクリックします。

図 14-1　ネットワークデバイスに ping を実行する



14.2 traceroute の使用

[Tools] > [Trace Route] ページを利用して、 指定された宛先へのルートを確認します。

パラメータ

次のパラメータが表示されます。

- Destination IP Address - ホストのエイリアスまたは IPv4 / IPv6 アドレスです。
- IPv4 Max Failures - トレースルートが終了するまでの最大失敗回数です。（固定：5)
- IPv6 Max Failures - トレースルートが終了するまでの最大失敗回数です。(範囲: 1 から 255; デフォルト：5)

コマンドの使用方法

- トレースルート機能を使用して、指定された宛先に到達するために必要なパスを特定します。
- 宛先が応答した際、最大タイムアウト(TTL)を超過した時、または最大ホップ数を超えた時にトレースが終了します。
- トレースルート機能は、最初に TTL 値が 1 に設定されたプローブデータグラムを送信します。これにより、最初のルータはデータグラムを破棄しエラーメッセージを返します。トレース機能は、その後の各 TTL レベルでいくつかのプローブメッセージを送信し、各メッセージのラウンドトリップ時間を表示します。「ICMP port unreachable」メッセージを返すことによって、すべてのデバイスがプローブに正しく応答するわけではありません。応答が返される前にタイマーがオフになると、トレース機能は一連のアスタリスクと「Request Timed Out」メッセージを出力します。最大タイムアウトに達したときに終了するこれらのメッセージの長いシーケンスは、ターゲットデバイスでこの問題が発生している可能性があります。
- 同一のリンクローカルアドレスは、異なるゾーン（RFC 4007）の異なるインタフェース/ノードによって使用されることがあります。したがって、リンクローカルアドレスを指定する場合は、%デリミタの後に VLAN 識別子を示す zone-id 情報を含めます。

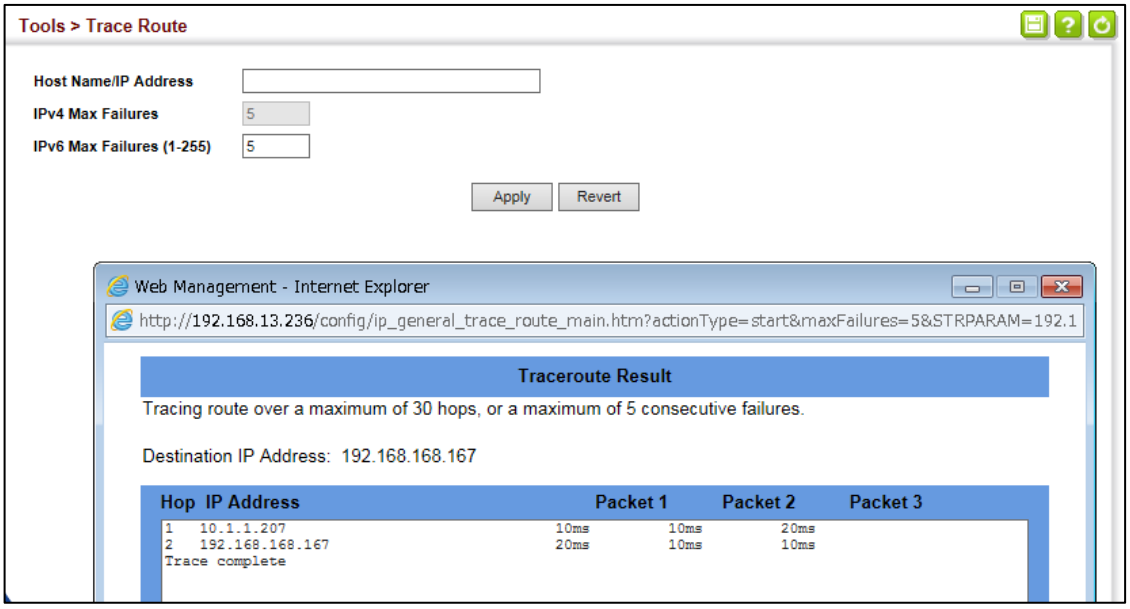
例えば、FE80 :: 7272%1 はトレースルートを送信するインタフェースとして VLAN 1 を識別します。

Web インタフェース

ネットワーク上の別のデバイスに traceroute を実行するには：

1. [Tools]、[Trace Route]をクリックします。
2. ターゲットデバイスを指定します。
3. [Apply]をクリックします。

図 14-2　ネットワークデバイスのルートをトレースする



14.3 アドレス解決プロトコル

IP ルーティングが有効な場合、ルータはルーティングテーブルを使用してルーティングの決定を行い、アドレス解決プロトコル（ARP）を使用して 1 つのホップから次のホップにトラフィックを転送します。ARP は、IP アドレスを物理層（すなわち、MAC）アドレスにマッピングするために使用される。IP フレームがこのルータ（または標準ベースのルータ）によって受信されると、まず ARP キャッシュ内の宛先 IP アドレスに対応する MAC アドレスが検索されます。アドレスが見つかると、ルータは MAC アドレスをフレームヘッダーの適切なフィールドに書き込み、フレームを次のホップに転送します。IP トラフィックは、パケットが最終的な宛先に配信されるまで、各ルーティングデバイスが宛先 IP アドレスを次のホップの宛先に受信者にマッピングするように、この方法で最終的な宛先にパスに沿って渡されます。

ARP キャッシュに IP アドレスのエントリがない場合、ルータはネットワーク上のすべてのデバイスに ARP 要求パケットをブロードキャストします。ARP 要求には、次の例に示すようなフィールドが含まれています。

表 14-1 アドレス解決プロトコル

宛先 IP アドレス	10.1.0.19
宛先 MAC アドレス	?
送信元 IP アドレス	10.1.0.253
送信元 MAC アドレス	00-00-ab-cd-00-00

デバイスはこの要求を受信すると、そのアドレスがメッセージ内の宛先 IP アドレスと一致しない場合にデバイスを破棄します。ただし、一致する場合は、宛先 MAC アドレスフィールドに独自のハードウェアアドレスを書き込み、送信元ハードウェアアドレスにメッセージを戻します。ソースデバイスは応答を受信すると、宛先 IP アドレスと対応する MAC アドレスをキャッシュに書き込み、IP トラフィックを次のホップに転送します。このエントリがタイムアウトしていない限り、ルータは別の ARP 要求をブロードキャストすることなく、この宛先の次ホップに直接トラフィックを転送できます。

また、スイッチが自身の IP アドレスの要求を受信すると、スイッチは応答を返し、ソースデバイスの IP アドレスの MAC もキャッシュします。

14.3.1 基本的な ARP 設定

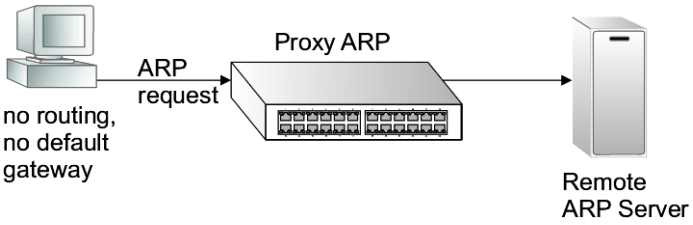
[Tools]> [ARP（Configure General）]ページを使用して、特定の VLAN インタフェースに対してプロキシ ARP を有効にします。

コマンドの使用方法

プロキシ ARP

接続されたサブネットワーク内のノードにルーティングまたはデフォルトゲートウェイが設定されていない場合、プロキシ ARP を使用して ARP 要求をリモートサブネットワークに転送できます。ルータがリモートネットワークの ARP 要求を受信し、プロキシ ARP が有効になっている場合、ルータはリモートネットワークへの最適なルートを持っているかどうかを判断し、要求元のノードに自身の MAC アドレスを送信して ARP 要求に応答します。そのノードは、ルータにトラフィックを送信します。ルータは、ルータ自身のルーティングテーブルを使用して、トラフィックをリモートの宛先に転送します。

図 14-3　プロキシ ARP



パラメータ

次のパラメータが表示されます。

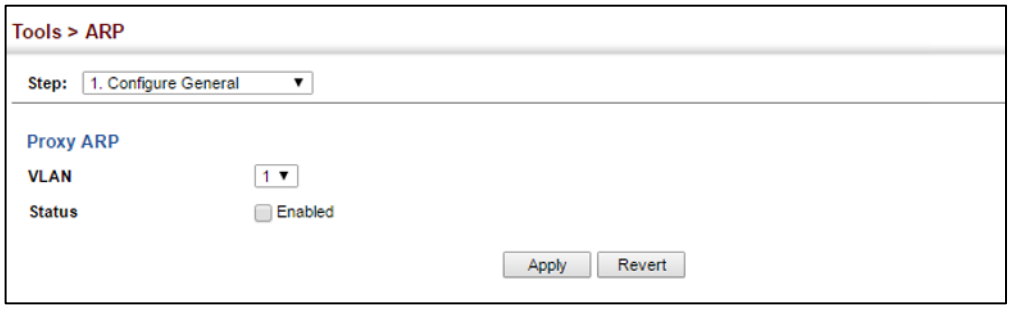
◆ Proxy ARP - 特定の VLAN インタフェースに対してプロキシ ARP を有効または無効にし、ルーティングしていないデバイスが別のサブネットまたはネットワーク上のホストの MAC アドレスを判別できるようにします。(デフォルト: Disabled)
プロキシ ARP を必要とするエンドステーションは、ネットワーク全体を単一のネットワークとして表示する必要があります。したがって、これらのノードは、ルータまたは他の関連ネットワークデバイスによって使用されるよりも小さなサブネットマスクを使用する必要があります。
プロキシ ARP を広範囲に使用すると、ルータのパフォーマンスが低下する可能性があります。これは ARP トラフィックが増加し、大きな ARP アドレステーブルの検索時間が長くなるためです。

Web インタフェース

VLAN（つまり IP サブネットワーク）のプロキシ ARP をイネーブルにするには、次の手順を実行します。

1. [Tools]、[ARP]をクリックします。
2. [Step]リストから[Configure General]を選択します。
3. ルーティングまたはデフォルトゲートウェイを持たないサブネットワークに対してプロキシ ARP を有効にします。
4. [Apply]をクリックします。

図 14-4　ARP の一般設定



14.3.2 動的 ARP エントリまたはローカル ARP エントリの表示

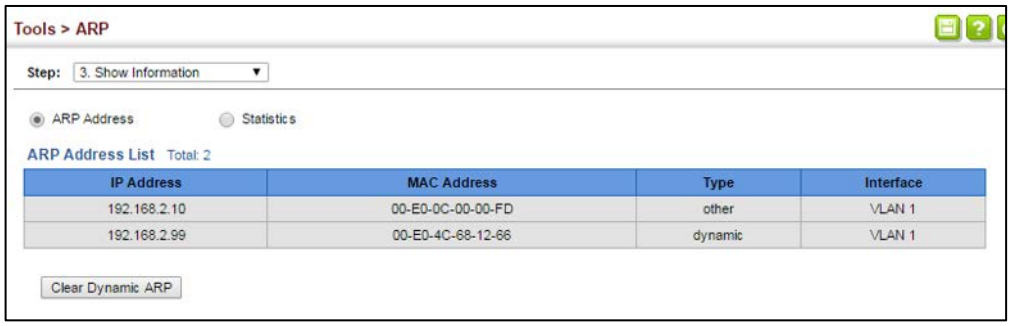
[Tools]> [ARP]ページを使用して、動的エントリまたはローカルエントリを ARP キャッシュに表示します。ARP キャッシュには、静的エントリと、ローカルインタフェースのホストアドレスのエントリが含まれています。ただし、ほとんどのエントリは、ブロードキャストメッセージへの応答を通じて動的に学習されます。

Web インタフェース

ARP キャッシュにすべての動的およびローカルエントリを表示するには、次の手順を実行します。

1. [Tools]、[ARP]をクリックします。
2. [Step]リストから[Show Information]を選択します。
3. [ARP Address]をクリックします。

図 14-5　ARP エントリの表示



14.3.3 ARP 統計情報の表示

このスイッチのすべてのインタフェースを通過する ARP メッセージの統計情報を表示するには、[Tools]> [ARP（Show Information）]ページを使用します。

パラメータ

次のパラメータが表示されます。

表 14-2　ARP 統計

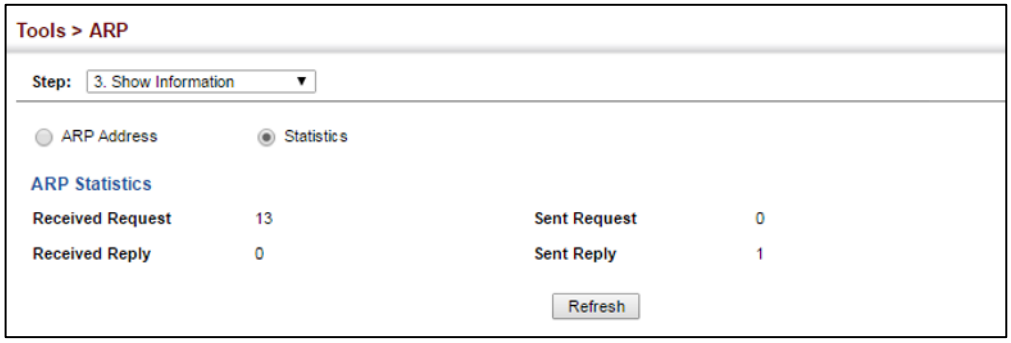
パラメータ	説明
Received Request	ルータが受信した ARP 要求パケットの数
Received Reply	ルータが受信した ARP 応答パケットの数
Sent Request	ルータによって送信された ARP 要求パケットの数
Sent Reply	ルータによって送信された ARP 応答パケットの数

Web インタフェース

ARP 統計を表示するには

1. [Tools]、[ARP]をクリックします。
2. [Step]リストから[Show Information]を選択します。
3. [Statistics]をクリックします。

図 14-6　ARP 統計情報の表示



15 IP コンフィグレーション

この章では、スイッチをネットワーク経由で管理アクセスするための IP インタフェースの設定方法について説明します。このスイッチは、IP バージョン 4 とバージョン 6 の両方をサポートし、これらのアドレスタイプのいずれかを使用して同時に管理することができます。特定の IPv4 または IPv6 アドレスを手動で設定することも、BOOTP または DHCP サーバから IPv4 アドレスを取得するようにスイッチに指示することもできます。IPv6 アドレスは、手動で構成することも動的に生成することもできます。

この章では、以下を含むネットワーク機能に関する情報を提供します。

- IPv4 Configuration - 管理アクセスの IPv4 アドレスを設定します。
- IPv6 Configuration - 管理アクセスの IPv6 アドレスを設定します。

15.1 スイッチの IP アドレスを設定（IP Version 4）

本章では、ネットワーク経由での管理アクセスのための初期 IPv4 インタフェースの設定方法、または複数のサブネットへのインタフェースの作成方法について説明します。このスイッチは IPv4 と IPv6 の両方をサポートしており、これらのアドレスタイプのいずれかを使用して管理できます。特定の IPv4 または IPv6 アドレスを手動で設定するか、BOOTP または DHCP サーバから IPv4 アドレスを取得するようにスイッチに指示できます。IPv6 グローバルユニキャストまたはリンクローカルアドレスを手動で設定することも、リンクローカルアドレスを動的に生成することもできます。

15.1.1 IPv4 インタフェース設定

[IP]> [General]> [Routing Interface（Add Address）]ページを使用して、スイッチの IPv4 アドレスを設定します。IPv4 アドレスは、デフォルトで VLAN 1 に静的アドレスが設定されています。静的アドレスを設定するには、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、別のネットワークセグメントに存在するスイッチと管理ステーションの間に、デフォルトゲートウェイを確立する必要があります。このデバイスをデフォルトゲートウェイとして設定するには、[IP]>[Routing]>[Static Routes（Add）]ページを使用し、宛先アドレスを必要なインタフェースに設定し、ヌルアドレス 0.0.0.0 への次のホップを設定します。

デバイスが BOOTP または DHCP サーバからアドレスを取得するように指示することも、静的 IP アドレスを手動で設定することもできます。有効な IP アドレスは、ピリオドで区切られた 0〜255 の 4 つの 10 進数で構成されます。この形式以外のものは受け入れられません。

コマンドの使用方法

◆ [IP]> [Routing]>[Static Routes（Add）]ページ、または、[IP]>[IPv6 Configuration（Configure Global）]ページを参照してください。

パラメータ

次のパラメータが表示されます。

◆ VLAN - 設定済みの VLAN の ID（1 から 4094）。デフォルトでは、スイッチ上のすべてのポートは VLAN 1 のメンバです。ただし、管理ステーションは、その VLAN に IP アドレスが割当てられている限り、任意の VLAN に属するポートに接続できます。(デフォルト: VLAN 1)

◆ IP Address Mode - 手動構成（ユーザ指定）、Dynamic Host Configuration Protocol（DHCP）、またはブートプロトコル（BOOTP）を使用して IP 機能を有効にするかどうかを指定します。DHCP / BOOTP が有効になっている場合、IP はサーバからの応答を受信するまで機能しません。要求は IP アドレスのスイッチによって定期的にブロードキャストされます。DHCP / BOOTP 応答には、IP アドレス、サブネットマスク、およびデフォルトゲートウェイが含まれます。(デフォルト: DHCP)

◆ IP Address Type - プライマリまたはセカンダリ IP アドレスを指定します。インタフェースでは 1 つの一次 IP アドレスしか持たないものの、多くの二次 IP アドレスを持つことができます。つまり、複数の IP サブネットにこのインタフェースでアクセスできる場合は、二次アドレスを指定する必要があります。初期設定では、このパラメータを Primary に設定します。(オプション: Primary, Secondary; Default: Primary)
一次 IP アドレスを設定する前に二次アドレスを設定することは出来ず、二次アドレスがまだ存在する場合は一次アドレスを削除できないことに留意してください。また、ネットワークセグメント内のルータまたはスイッチがセカンダリアドレスを使用する場合、そのセグメント内の他のすべてのルータ/スイッチも同じネットワークまたはサブネットアドレス空間のセカンダリアドレスを使用する必要があります。

- IP Address - VLAN の IP アドレスです。有効な IP アドレスは、ピリオドで区切られた 0 から 255 の 4 つの数字で構成されます。(デフォルト: None)

Note: 設定済みの任意の IP インタフェースを使用してスイッチを管理できます。

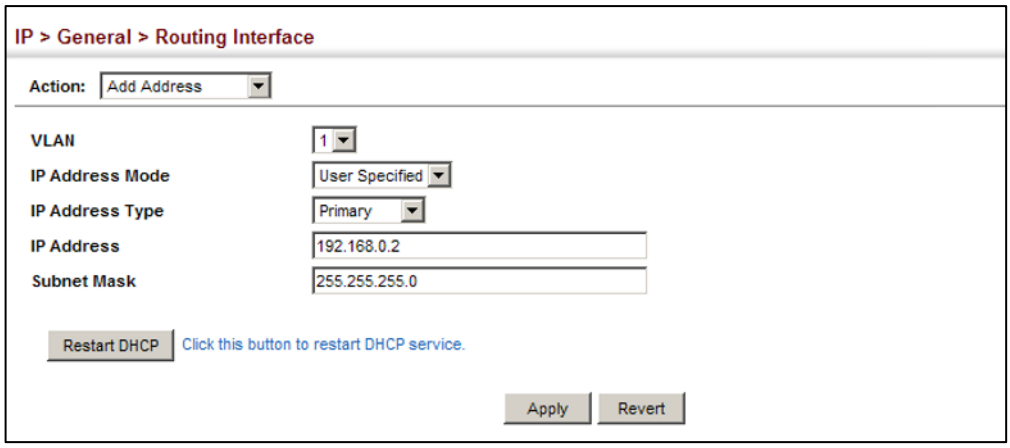
- Subnet Mask - このマスクは、特定のサブネットへのルーティングに使用されるホストアドレスビットを識別します。(デフォルト: None)
- Restart DHCP - DHCP サーバから新しい IP アドレスを要求します。

Web インタフェース

スイッチの静的 IPv4 アドレスを設定するには：

1. [IP]、[General]、[Routing Interface]をクリックします。
2. [Action]リストから[Add Address]を選択します。
3. 設定済みの VLAN を選択し、IP Address Mode を「User Specified」に設定します。このインタフェースにまだアドレスが設定されていない場合は IP Address Type を「Primary」に設定し、IP アドレスとサブネットマスクを入力します。
4. プライマリまたはセカンダリアドレスタイプを選択します。
5. [Apply]をクリックします。

図 15-1　静的 IPv4 アドレスの設定

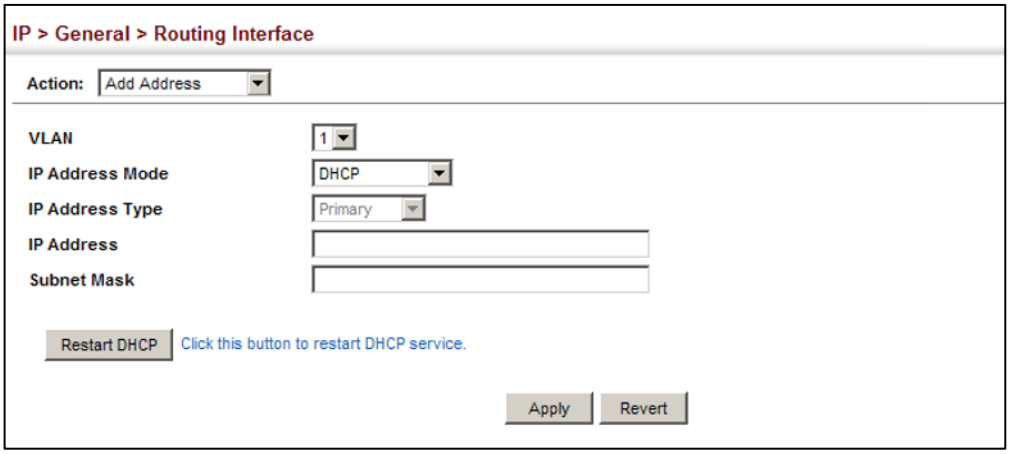


スイッチの DHCP / BOOTP を使って動的な IPv4 アドレスを取得するには：

1. [IP]、[General]、[Routing Interface]をクリックします。
2. [Action]リストから[Add Address]を選択します。
3. 設定済みの VLAN を選択し、IP アドレスモードを「BOOTP」または「DHCP」に設定します。
4. [Apply]をクリックして変更を保存します。
5. 次に、[Restart DHCP]をクリックして、直ちに新しいアドレスを要求します。

IP は有効になりますが、BOOTP または DHCP 応答が受信されるまで機能しません。要求は IP 構成情報が BOOTP または DHCP サーバから取得されるまで、指数バックオフを使用して、数分ごとにブロードキャストされます。

図 15-2　動的 IPv4 アドレスの設定



Note: スイッチはまた、各電源リセット時に IP コンフィグレーションの要求をブロードキャストします。

Note: 管理接続が失われた場合は、スイッチにコンソール接続し、show ip interface と入力して新しいスイッチアドレスを確認します。

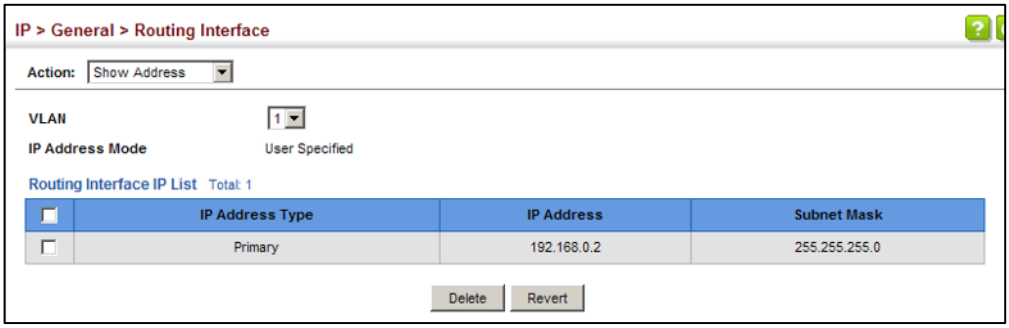
Renewing DCHP - DHCP は、クライアントに無期限に、または特定の期間、アドレスをリースすることがあります。アドレスが期限切れになったり、スイッチが別のネットワークセグメントに移動したりすると、スイッチへの管理アクセスが失われます。この場合、スイッチを再起動するか、CLI を使用して DHCP サービスを再起動するためのクライアント要求を送信できます。

DHCP によって割当てられたアドレスが機能しなくなった場合、Web インタフェース経由で IP 設定を更新することはできません。現在のアドレスがまだ利用可能な場合は、Web インタフェース経由でのみ DHCP サービスを再起動できます。

インタフェース用に設定された IPv4 アドレスを表示するには：

1. [IP]、[General]、[Routing Interface]をクリックします。
2. [Action]リストから[Show Address]を選択します。
3. VLAN リストからエントリを選択します。

図 15-3　インタフェースの設定済み IPv4 アドレスの表示



15.2 スイッチの IP アドレスを設定（IP Version 6）

このセクションでは、ネットワーク経由の管理アクセス用に IPv6 インタフェースを設定する方法、または複数のサブネットへのインタフェースを作成する方法について説明します。このスイッチは IPv4 と IPv6 の両方をサポートしており、これらのアドレスタイプのいずれかを使用して管理できます。

コマンドの使用方法

- IPv6 には、リンクローカルユニキャストとグローバルユニキャストという 2 つの異なるアドレスタイプが含まれています。リンクローカルアドレスは、スイッチが同じローカルサブネットに接続されているすべてのデバイスに対して IPv6 経由でアクセス可能にします。この種のアドレスを使用する管理トラフィックは、サブネット外のルータでは通過できません。リンクローカルアドレスは設定が簡単で、シンプルなネットワークや基本的なトラブルシューティング作業に役立ちます。ただし、複数のセグメントを持つ大規模なネットワークに接続するには、スイッチにグローバルユニキャストアドレスを設定する必要があります。リンクローカルとグローバルの両方のユニキャストアドレスタイプは、（[Configure Interface]ページを使用して）動的に割当てることも、（IPv6 アドレスの追加ページを使用して）手動で設定することもできます。
- IPv6 グローバルユニキャストまたはリンクローカルアドレスは、（IPv6 アドレスの追加ページを使用して）手動で設定することも、（[Configure Interface]ページを使用して）リンクローカルアドレスを動的に生成することもできます。

15.2.1 IPv6 デフォルトゲートウェイの設定

[IP]> [IPv6 Configuration（Configure Global）]ページを使用して、スイッチの IPv6 デフォルトゲートウェイを設定します。

パラメータ

次のパラメータが表示されます。

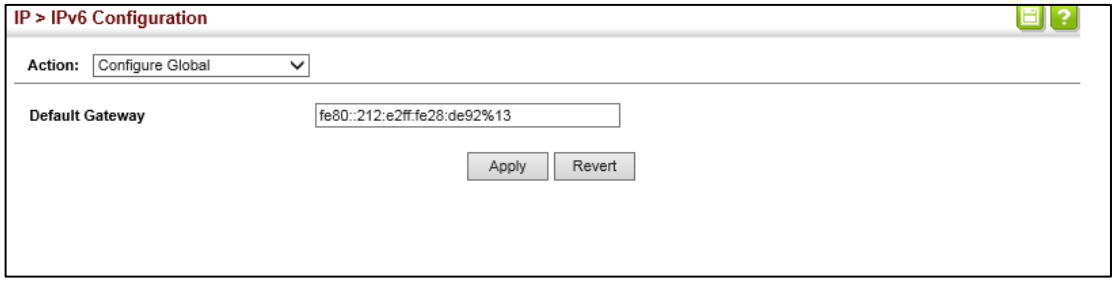
- Default Gateway - IPv6 アドレスに関するルーティング情報が分からない場合に使用する、デフォルトのネクストホップルータの IPv6 アドレスを設定します。
  - スイッチ上で設定されているゲートウェイに、ネットワークインタフェースが直接接続されている場合のみ、IPv6 デフォルトゲートウェイは正常に設定することができます。
  - IPv6 アドレスは、RFC 2373「IPv6 Addressing Architecture」に従って、8 つのコロンで区切られた 16 ビットの 16 進数を使用して構成する必要があります。未定義のフィールドを埋めるために必要な 0 の適切な数を示すために、アドレスに 1 つの二重コロンを使用することができます。

Web インタフェース

スイッチの IPv6 デフォルトゲートウェイを設定するには、次の手順を実行します。

1. [IP]、[IPv6 Configuration]をクリックします。
2. [Action]リストから[Configure Global]を選択します。
3. IPv6 のデフォルトゲートウェイを入力します。
4. [Apply]をクリックします。

図 15-4　IPv6 デフォルトゲートウェイの設定



15.2.2 IPv6 インタフェースの設定

IP> IPv6 Configuration（Configure Interface）ページを使用して、選択した VLAN の一般的な IPv6 を設定します。その中には、グローバルユニキャストインタフェースアドレスの自動設定、およびリンクローカルインタフェースアドレス、MTU サイズ、および、重複アドレス検出および近傍送信間隔の近傍ディスカバリプロトコル設定の明示的な構成などが含まれます。

コマンドの使用方法

- スイッチにリンクローカルアドレスを設定する必要があります。スイッチのアドレス自動設定機能によってリンクローカルアドレスが自動的に作成されます。ルータ広告がローカルインタフェース上で検出された場合は、IPv6 グローバルアドレスも生成されます。
- IPv6 を明示的に有効にするオプションはリンクローカルアドレスを作成しますが、自動設定が有効になっていない場合はグローバル IPv6 アドレスを生成しません。この場合、グローバルユニキャストアドレスを手動で設定することができます。
- IPv6 近傍ディスカバリプロトコルは、IPv6 ネットワークで IPv4 アドレス解決プロトコルに取って代わるものです。同じネットワークセグメント上の IPv6 ノードは、近傍探索を使用して、互いの存在を発見し、互いのリンク層アドレスを決定し、ルータを見つけ、アクティブ近傍への経路に関する到達可能性情報を維持します。このプロセスを容易にするために使用される重要なパラメータは、同じネットワークセグメントに重複アドレスが存在するかどうか、および到達可能性情報を検証するために使用される近傍要請の間の間隔を検証する試行回数です。

パラメータ

次のパラメータが表示されます。

- VLAN - 管理アクセスに使用される設定済み VLAN の ID、またはサブネットの標準インタフェースとして使用されます。デフォルトでは、スイッチ上のすべてのポートは VLAN 1 のメンバです。ただし、管理ステーションは、その VLAN に IP アドレスが割当てられている限り、任意の VLAN に属するポートに接続できます。(範囲: 1 から 4094)
- Address Autoconfig - インタフェース上で IPv6 アドレスのステートレス自動設定をイネーブルにし、そのインタフェースで IPv6 機能をイネーブルにします。アドレスのネットワーク部分は、IPv6 ルータ通知メッセージで受信されたプレフィックスに基づいており、ホスト部分は、インタフェース識別子（すなわち、スイッチの MAC アドレス）の変更された EUI-64 形式を使用して自動的に生成される。
  - リンクローカルアドレスがこのインタフェースにまだ割当てられていない場合、このコマンドは動的にアドレスを生成します。リンクローカルアドレスは、FE80～FEBF の範囲のアドレスプレフィックスと、変更された EUI-64 形式のスイッチの MAC アドレスに基づくホスト部分で作成されます。グローバルプレフィックスが受信されたルータ広告に含まれる場合は、グローバルユニキャストアドレスも生成されます。
  - DHCPv6 が開始されると、スイッチはステートフルアドレス自動設定によって IP アドレスプレ

フィックスを取得しようとする可能性があります。ルータ広告に「その他のステートフルコンフィグレーション」フラグが設定されている場合、スイッチはアドレス以外の設定情報（デフォルトゲートウェイなど）を取得しようとします。

- 自動設定が選択されていない場合は、下記の IPv6 アドレスの追加ページを使用してアドレスを手動で設定する必要があります。

◆ Enable IPv6 Explicitly - インタフェースで IPv6 を有効にし、リンクローカルアドレスを割当てます。明示的なアドレスがインタフェースに割当てられると、IPv6 は自動的に有効になり、割当てられたすべてのアドレスが削除されるまで無効にすることはできません。(デフォルト: Disabled)
このパラメータを無効にしても、IPv6 アドレスで明示的に設定されたインタフェースの IPv6 は無効になりません。

◆ MTU - インタフェース上で送信される IPv6 パケットの最大伝送ユニット（MTU）のサイズを設定します。.(範囲: 1280 から 65535 バイト; デフォルト：1500 バイト）

- このフィールドに設定されている最大値は、現在 1500 バイトに固定されている物理インタフェースの MTU を超えることはできません。
- IPv6 ルータは、他のルータから転送された IPv6 パケットを断片化しません。ただし、IPv6 ルータに接続されたエンドステーションから発信されるトラフィックは断片化する可能性があります。
- 同じ物理メディアのすべてのデバイスは、正確に作動させるために同じ MTU を使用する必要があります。

◆ ND DAD Attempts - 重複アドレス検出中にインタフェース上で送信された連続近傍送信メッセージの数です。(範囲: 0 から 600、デフォルト: 3)

- 値を 0 に設定すると、重複アドレス検出が無効になります。
- 重複アドレス検出は、新しいユニキャスト IPv6 アドレスがネットワークにすでに存在していて、それがインタフェースに割当てられているかどうかを判断します。
- 一時的に停止しているインタフェース上では、重複アドレスの検出が停止されます（「5.1.1 VLAN グループの設定」を参照してください)。インタフェースが中断されている間は、そのインタフェースに割当てられているすべてのユニキャスト IPv6 アドレスが「保留中」の状態になります。インタフェースが管理上再起動されると、重複アドレス検出が自動的に再開されます。
- 再アクティブ化されたインタフェースは、インタフェース上のすべてのユニキャスト IPv6 アドレスに対して重複アドレス検出を再開します。重複したアドレス検出がインタフェースのリンクローカルアドレスで実行されている間、他の IPv6 アドレスは「仮の」状態のままとなります。重複したリンクローカルアドレスが見つからない場合には、残りの IPv6 アドレスに対して重複アドレス検出が開始されます。
- 重複アドレスが検出された場合には、重複状態に設定され警告メッセージがコンソールに送信されます。重複したリンクローカルアドレスが検出されると、IPv6 プロセスはインタフェース上で無効となります。重複するグローバルユニキャストアドレスが検出された場合には使用されません。重複アドレスに関連するすべての設定コマンドは、アドレスが「重複」状態の間は設定されたままとなります。
- インタフェースのリンクローカルアドレスが変更された場合には、重複したアドレス検出が新規のリンクローカルアドレスで実行されますが、インタフェースにすでに関連付けられている IPv6 グローバルユニキャストアドレスのいずれに対しても実施されません。

◆ ND NS Interval - インタフェース上で IPv6 近傍送信要求メッセージを送信する間隔です。(範囲: 1000 から 3600000 ミリ秒）
デフォルト: 1000 ミリ秒は近傍検出操作に使用されます。
このアトリビュートは、アドレスを解決するとき、または近傍の到達可能性をプロービングするときに近傍送信要求メッセージを送信する間隔を指定します。したがって、通常の IPv6 操作には極端に短

い間隔を使用しないでください。

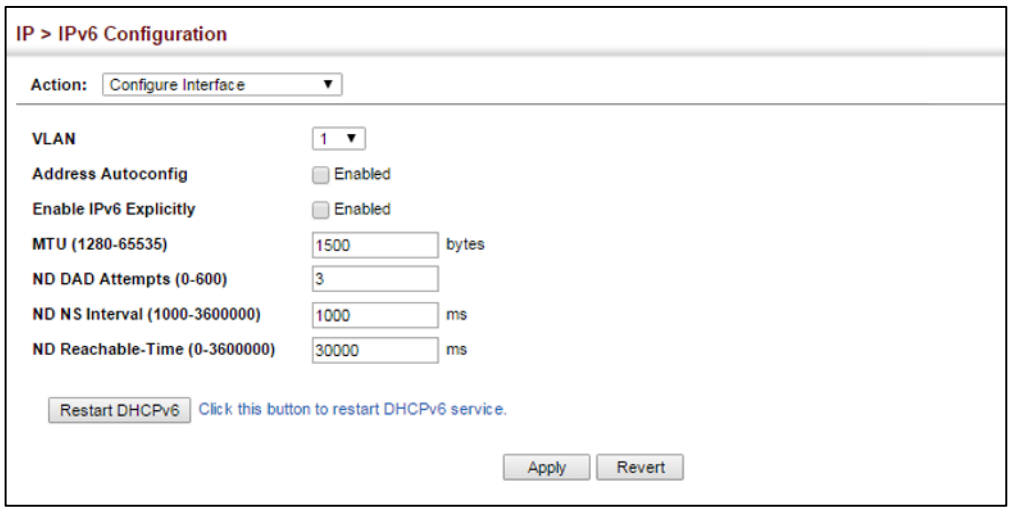
- ND Reachable-Time - 到達可能性確認イベントが発生した後、リモート IPv6 ノードが到達可能であるとみなされる時間です。(範囲: 0 から 3600000 ミリ秒)
  デフォルト: 30000 ミリ秒は近傍検出操作に使用されます。
  - このパラメータで設定された制限時間は、ルータが使用できない近傍を検出できるようにします。近傍検出処理中に、IPv6 ノードは近傍送信要求メッセージをマルチキャストして隣接ノードを検索します。隣接ノードが到達可能であると見なされるためには、隣接ノードに隣接ノード通知メッセージで応答して、確認された隣接ノードになる必要がありその後到達可能タイマーは後続のユニキャスト IPv6 レイヤ通信のために有効とみなされます。
- Restart DHCPv6 - DHCPv6 が再起動されると、スイッチはステートフルアドレス自動設定によって IP アドレスプレフィックスを取得しようとします。ルータ広告に「その他のステートフルコンフィグレーション」フラグが設定されている場合、スイッチは DHCPv6 が再起動されたときに他の非アドレス設定情報（デフォルトゲートウェイなど）を取得しようとすることもあります。
  クライアント要求を DHCPv6 サーバに送信する前に、アドレス自動設定オプションを使用してリンクローカルアドレスでスイッチを設定する必要があります。ルータ通知メッセージで受信した管理アドレス設定フラグ(M フラグ)およびその他のステートフル設定フラグ(O フラグ)の状態によって、このスイッチが DHCPv6 サーバから取得しようとする情報が、以下のように決定されます:
  - M および O フラグの両方が 1 に設定されます:
    DHCPv6 が、アドレスとその他のコンフィグレーションの両方に使用されます。
    この組み合わせは、DHCPv6 ステートフル自動設定と呼ばれ、DHCPv6 サーバがステートフルアドレスを IPv6 ホストに割当てます。
  - M フラグが 0 に設定され、O フラグが 1 に設定されます:
    DHCPv6 は、他のコンフィグレーションに対してのみ使用されます。
    隣接ルータは、IPv6 ホストがステートレスアドレスを取得する非リンクローカルアドレスプレフィックスを通知するように設定されています。
    この組み合わせは、DHCPv6 ステートレス自動設定と呼ばれ、DHCPv6 サーバはステートフルアドレスを IPv6 ホストに割当てず、ステートレスコンフィグレーションを割当てます。

Web インタフェース

スイッチの一般的な IPv6 を設定するには：

1. [IP]、[IPv6 Configuration]をクリックします。
2. [Action]リストから[Configure Interface]を選択します。
3. 設定する VLAN を指定します。
4. アドレスの自動設定を有効にするか、IPv6 を明示的に有効にして、リンクローカルアドレスを自動的に設定し、選択したインタフェースで IPv6 を有効にします。(リンクローカルアドレスを手動で設定するには、[Add IPv6 Address]ページを使用します)。重複アドレス検出メッセージの最大数、近傍送信要求メッセージ間隔、およびリモート IPv6 ノードが到達可能であるとみなされる時間を設定します。
5. [Apply]をクリックします。

図 15-5　IPv6 インタフェースの一般設定



15.2.3 IPv6 アドレスの設定

[IP]> [IPv6 Configuration（Add IPv6 Address）]ページを使用して、ネットワーク経由での管理アクセス、または複数のサブネットへのインタフェース作成用の IPv6 インタフェースを設定します。

コマンドの使用方法

- すべての IPv6 アドレスは、RFC 2373「IPv6 Addressing Architecture」に従って、8 つのコロンで区切られた 16 ビットの 16 進数を使用してフォーマットする必要があります。未定義のフィールドを埋めるために必要な 0 の適切な数を示すために、アドレスに 1 つの二重コロンを使用することができます。
- スイッチは常にリンクローカルアドレスで設定する必要があります。したがって、IPv6 の機能を有効にしたり、アドレスの自動設定や IPv6 IPv6 の明示的な有効化など、グローバルユニキャストアドレスをスイッチに割当てる構成プロセスでは、リンクローカルユニキャストアドレスも自動的に生成されます。リンクローカルアドレスのプレフィックス長は 64 ビットに固定され、デフォルトアドレスのホスト部分は、インタフェース識別子の変更された EUI-64（拡張ユニバーサル識別子）形式に基づいています（すなわち、物理 MAC アドレス）。または、FE80～FEBF の範囲内にネットワークプレフィックスを含む完全なアドレスを入力して、リンクローカルアドレスを手動で設定することもできます。
- 複数のサブネットを持つ大規模なネットワークに接続するには、グローバルユニキャストアドレスを設定する必要があります。このアドレスタイプを設定するには、いくつかの方法があります。
  - グローバルユニキャストアドレスは、ローカルインタフェース上で観察されるルータ広告からネットワークプレフィクスを取得し、修正された EUI-64 形式のインタフェース識別子を使用してアドレスのホスト部分を自動的に作成することによって、自動的に設定できます。
  - ネットワークプレフィックスとプレフィックスの長さ全体を指定し、インタフェース識別子の EUI-64 形式を使用して、アドレスのホスト部分に下位 64 ビットを自動的に作成することによって、手動で構成できます。
  - 完全なアドレスとプレフィックスの長さを入力して、グローバルユニキャストアドレスを手動で設定することもできます。
- インタフェースごとに複数の IPv6 グローバルユニキャストアドレスを設定することができます。しかしながら、1 つのインタフェースに対し 1 つのリンクローカルアドレスのみとなります。
- ローカル・セグメント上で重複したリンクローカルアドレスが検出された場合、このインタフェースは使用不可になり、コンソールに警告メッセージが表示されます。ネットワーク上で重複したグローバルユニキャストアドレスが検出された場合は、このインタフェースでアドレスが無効になり、コン

ソールに警告メッセージが表示されます。

◆ 明示的なアドレスがインタフェースに割当てられると、IPv6 は自動的に有効になり、割当てられたすべてのアドレスが削除されるまで無効にすることはできません。

パラメータ

次のパラメータが表示されます。

◆ VLAN - 管理アクセスに使用される設定済み VLAN の ID、または複数のサブネットへのインタフェースの作成に使用されます。デフォルトでは、スイッチ上のすべてのポートは VLAN 1 のメンバです。ただし、管理ステーションは、その VLAN に IP アドレスが割当てられている限り、任意の VLAN に属するポートに接続できます。(範囲: 1 から 4094)

◆ Address Type - このインタフェースに設定されているアドレスタイプを定義します。

■ Global - ネットワークプレフィックスとホストアドレスビット、スラッシュ、およびアドレスの連続したいくつかのビットが接頭部を構成するビット数を示す 10 進数を含む IPv6 グローバルユニキャストアドレスを構成します　（すなわち、アドレスのネットワーク部分）。

■ EUI-64 (拡張ユニバーサル識別子) - 下位 64 ビットの EUI-64 インタフェース ID を使用して、インタフェースの IPv6 アドレスを設定します。

- アドレスのホスト部分の下位 64 ビットに EUI-64 フォーマットを使用する場合、IPv6 アドレスフィールドに入力された値にはアドレスのネットワーク部分が含まれ、接頭語の長さは接頭辞を構成するアドレスの連続するビット数（左から開始）を示します（すなわち、アドレスのネットワーク部分）。指定されたプレフィックス長が 64 ビット未満の場合、IPv6 アドレスフィールドで指定された値に上位ホストビットの一部が含まれることに注意してください。指定されたプレフィックス長が 64 ビットを超える場合、アドレスのネットワーク部分で使用されるビットがインタフェース識別子よりも優先されます。
- IPv6 アドレスは 16 バイト長で、そのうちの 8 バイトは通常デバイスの MAC アドレスにもとづいて一意のホスト識別子を形成します。EUI-64 仕様は、拡張 8 バイト MAC アドレスを使用するデバイス向けに設計されています。6 バイトの MAC アドレス(EUI-48 フォーマットとも呼ばれます)を使用するデバイスの場合は、アドレスのユニバーサル/ローカルビットを反転し、16 進数の FFFE を MAC アドレスの上位と下位 3 バイトの間に挿入して、EUI-64 フォーマットに変換する必要があります。
  たとえば、デバイスの EUI-48 アドレスが 28-9F-18-1C-82-35 の場合、EUI-64 要件を満たすためにグローバル/ローカルビットを最初に反転する必要があります(例; グローバルに定義されている場合には、1 アドレスは 0、ローカル定義アドレスは 0)、28 を 2A に変更します。その後、2 バイトの FFFE が OUI（すなわち、組織的に固有の識別子、または企業識別子）と残りのアドレスとの間に挿入され、修正された EUI-64 インタフェース識別子が 2A-9F-18-FF-FE-1C-82-35 となります。
- このホストアドレス方式では、これらのインタフェースが異なるサブネットに接続されている場合、同じインタフェース識別子を 1 つのデバイスの複数の IP インタフェースで使用することができます。

■ Link Local - IPv6 リンクローカルアドレスを設定します。

- アドレスプレフィックスは、FE80～FEBF の範囲内でなければなりません。
- インタフェースごとに 1 つのリンクローカルアドレスだけを設定できます。
- 指定されたアドレスは、インタフェース用に自動的に生成されたリンクローカルアドレスを置き換えます。

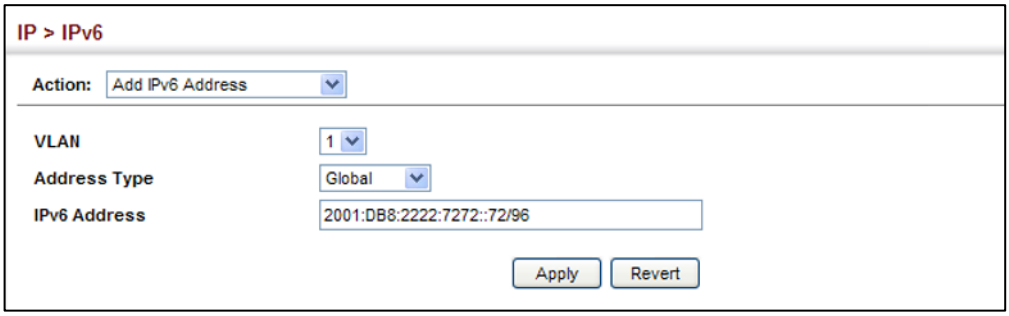
◆ IPv6 Address - このインタフェースに割当てられた IPv6 アドレスです。

Web インタフェース

IPv6 アドレスを設定するには：

1. [IP]、[IPv6 Configuration]をクリックします。
2. [Action]リストから[Add IPv6 Address]を選択します。
3. 設定する VLAN を指定し、アドレスタイプを選択して、IPv6 アドレスとプレフィックス長を入力します。
4. [Apply]をクリックします。

図 15-6　IPv6 アドレスの設定



15.2.4 IPv6 アドレスの表示

[IP]> [IPv6 Configuration（Show IPv6 Address）]ページを使用して、インタフェースに割当てられた IPv6 アドレスを表示します。

パラメータ

次のパラメータが表示されます。

- VLAN - 設定済み VLAN の ID です。.デフォルトでは、スイッチ上のすべてのポートは VLAN 1 のメンバです。ただし、管理ステーションは、その VLAN に IP アドレスが割当てられている限り、任意の VLAN に属するポートに接続できます。(範囲: 1 から 4094)
- IPv6 Address Type - アドレスタイプ（Global、EUI-64、リンクローカル）です。
- IPv6 Address - このインタフェースに割当てられた IPv6 アドレスです。
  インタフェースに割当てられたユニキャストアドレスに加えて、ノードは全ノードマルチキャストアドレス FF01 :: 1（インタフェースローカルスコープ）と FF02 :: 1（リンクローカルスコープ）をリッスンする必要もあります。
  FF01::1/16 は、接続されたすべての IPv6 ノードの一時的なインタフェースローカルマルチキャストアドレスであり、FF02::1/16 は、接続されたすべての IPv6 ノードのリンクローカルマルチキャストアドレスです。インタフェースローカルマルチキャストアドレスは、マルチキャストトラフィックのループバック送信にのみ使用されます。リンクローカルマルチキャストアドレスは以下に説明するように、すべてのノード（FF02::1）、すべてのルータ（FF02::2）、および要請されたノード（FF02::1:FFXX:XXXX）を含むリンクローカルユニキャストアドレスで使用されるのと同じタイプをカバーします。
  またノードは、それが割当てられているすべてのユニキャストおよびエニキャストアドレスについて、関連する要求ノードマルチキャストアドレスを計算して参加させる必要があります。上位ビットのみが異なる IPv6 アドレスとなります。 異なるアグリゲーションに関連付けられた複数の上位プレフィックスが同じ要請ノードアドレスにマッピングされるため、ノードが参加する必要があるマルチキャストアドレスの数が減少します。この例では、FF02::1:FF90:0/104 はアドレスの下位 24 ビットを取り、それらのビットをプレフィックスに付加することによって形成される要請ノードマルチキャス

トアドレスです。
IPv4 のアドレス解決プロトコルで使用されているブロードキャスト方式を IPv6 がサポートしていないため、要請されたノードのマルチキャストアドレス（リンクローカルスコープ FF02）が近傍ノードの MAC アドレスを解決するために使用されることに注意してください。
これらの追加アドレスは、CLI レファレンスガイドの“show ip interface”コマンドで表示されます。

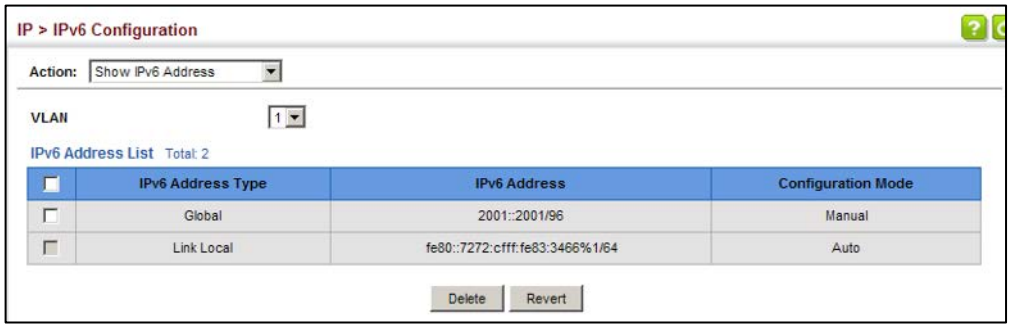
◆ Configuration Mode - このアドレスが自動的に生成されたのか、手動で構成されたのかを示します。

Web インタフェース

設定済みの IPv6 アドレスを表示するには：

1. [IP]、[IPv6 Configuration]をクリックします。
2. [Action]リストから[Show IPv6 Address]を選択します。
3. リストから VLAN を選択します。

図 15-7　設定済みの IPv6 アドレスを表示する



15.2.5 IPv6 近隣キャッシュの表示

[IP]> [IPv6 Configuration（Show IPv6 Neighbor Cache）]ページを使用して、近傍デバイスで検出された IPv6 アドレスを表示します。

パラメータ

次のパラメータが表示されます。

表 15-1　IPv6 近傍を表示する - 表示の説明

フィールド	説明
IPv6 Address	近傍の IPv6 アドレスです。
Age	アドレスが到達可能（秒単位）として確認されてからの時間です。静的エントリは、値 "Permanent"によって示されます。
Link-layer Address	物理レイヤ MAC アドレスです。
State	以下のステートが動的エントリに対して使用されます: ・Incomplete - エントリのアドレス解決が実行されています。近傍送信要求メッセージは、ターゲットのマルチキャストアドレスに送信されていますが、近傍通知メッセージをまだ返していません。 ・Invalid - 無効なマッピングです。状態を無効に設定すると、このエントリで指定されたインタフェースが示されたマッピング(RFC 4293)と関連付けられなくなります。 ・Reachable - 最後の ReachableTime 間隔内に、近傍への順方向パスが機能しているという確かな確認が受信されました。Reachable 状態の間、デバイスはパケットを送信するときに特別な処理を行いません。

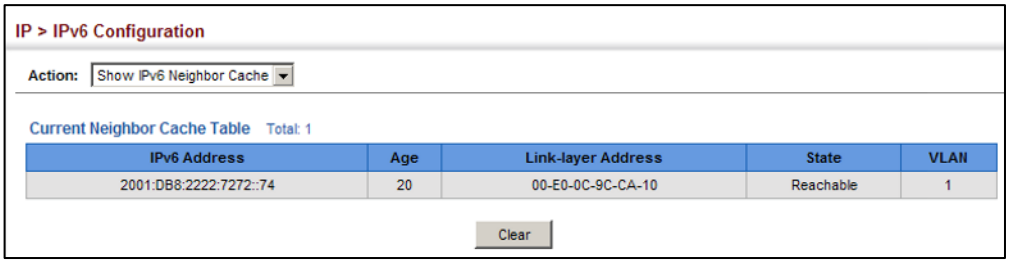
フィールド	説明
	・Stale - 順方向パスが機能していた最後の肯定的な確認が受信されてから、ReachableTime 間隔以上経過しています。Stale 状態の間、デバイスはパケットが送信されるまで何の動作も行いません。 ・Delay - 順方向パスが機能していた最後の肯定的な確認が受信されてから、ReachableTime 間隔以上経過しています。最後の DELAY_FIRST_PROBE_TIME 間隔内にパケットが送信されています。遅延状態に入った後にこの間隔内に到達可能性確認が受信されない場合、スイッチは近傍送信要求メッセージを送信し、状態をプローブに変更します。 ・Probe - 到達可能性の確認が受信されるまで、RetransTimer 間隔ごとに近傍要請メッセージを再送信することによって、到達可能性の確認が積極的に求められる。 ・Unknown - 不明な状態です。 以下のステートが静的エントリに対して使用されます: ・Incomplete - このエントリのインタフェースは停止しています。 ・Permanent - 静的なエントリを示します。 ・Reachable - このエントリのインタフェースが起動しています。IPv6 近傍探索キャッシュの静的エントリに到達可能性の検出は適用されません。
VLAN	アドレスが到達した VLAN インタフェースです。

Web インタフェース

隣接する IPv6 デバイスを表示するには：

1. [IP]、[IPv6 Configuration]をクリックします。
2. [Action]リストから[Show IPv6 Neighbor Cache]を選択します。

図 15-8　IPv6 近傍の表示



15.2.6 IPv6 統計情報の表示

このスイッチを通過する IPv6 トラフィックに関する統計情報を表示するには、[IP]> [IPv6 Configuration（Show Statistics）]ページを使用します。

コマンドの使用方法

このスイッチは、次のトラフィックタイプの統計情報を提供します。

- IPv6 - バージョン 6 アドレス用のインターネットプロトコルは、データブロック（パケットまたはフレームと呼ばれることが多い）を送信元から宛先に送信するためのメカニズムを提供します。これらのネットワークデバイス（つまりホスト）は固定長アドレスで識別されます。また、インターネットプロトコルは、必要であれば、“小規模パケット”ネットワークを介して送信するために、長いパケットの断片化および再構成を提供する。
- ICMPv6 - バージョン 6 アドレスのインターネット制御メッセージプロトコルは、IPv6 パケットを処理する際のエラーを報告するメッセージパケットを送信するネットワークレイヤプロトコルです。した

がって、ICMP はインターネットプロトコルの不可欠な部分です。ICMP メッセージは、データグラムが宛先に到達できない場合、ゲートウェイがデータグラムを転送するバッファリング能力を持たない場合、およびゲートウェイが短いルートでトラフィックを送信するようにホストに指示できる場合など、さまざまな状況を報告するために使用されます。ICMP は、ルータが特定の宛先に使用する、より適切なルート（ネクストホップルータ）に関する情報をフィードバックするためにも使用されます。

- UDP - ユーザデータグラムプロトコルは、パケット交換通信のデータグラムモードを提供します。これは、基本的なトランスポートメカニズムとして IP を使用し、IP ライクなサービスへのアクセスを提供します。UDP パケットは、IP パケットと同様に配信されます。ターゲットに達する前に破棄されるコネクションレスのデータグラムです。UDP は、TCP が複雑すぎる、遅すぎる、または不必要な場合に便利です。

パラメータ

次のパラメータが表示されます。

表 15-2 IPv6 統計情報を表示する - 表示の説明

フィールド	説明
IPv6 Statistics	
IPv6 Received	
Total	エラーで受信したデータグラムを含む、インタフェースによって受信された入力データグラムの総数です。
Header Errors	バージョン番号の不一致、その他のフォーマットエラー、ホップ数超過、IPv6 オプション等、IPv6 ヘッダーエラーのために破棄された入力データグラムの数です。
Too Big Errors	サイズが送信インタフェースのリンク MTU を超過したために転送できなかった、入力データグラムの数です。
No Routes	送信先に送信する経路が見つからなかったために破棄された、入力データグラムの数です。
Address Errors	IPv6 ヘッダーの宛先フィールドの IPv6 アドレスがこのエンティティで受信される有効なアドレスでなかったために廃棄された入力データグラムの数です。このカウントには、無効なアドレス（例：:: 0）とサポートされていないアドレス(未割当てのプレフィックスを持つアドレス等)が含まれます。IPv6 ルータではないため、データグラムを転送しないエンティティの場合、このカウンタには宛先アドレスがローカルアドレスではないため、廃棄されたデータグラムが含まれます。
Unknown Protocols	正常に受信されたものの未知、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、ローカルにアドレス指定されたデータグラムの数です。このカウンタは、これらのデータグラムがアドレス指定されたインタフェースで増分されます。これらのデータグラムは、必ずしもデータグラムの一部の入力インタフェースではない可能性があります。
Truncated Packets	データグラムフレームに十分なデータが格納されていないために破棄された、入力データグラムの数です。
Discards	継続的な処理を妨げるような問題は発生しなかったものの、廃棄された(例; バッファスペースが不足している)入力 IPv6 データグラムの数です。このカウンタには、再組み立てを待つ間に破棄されたデータグラムは含まれないことに留意してください。
Delivers	IPv6 ユーザプロトコル(ICMP を含む)に正常に配信されたデータグラムの総数です。このカウンタは、これらのデータグラムがアドレス指定されたインタフェースで増分されます。これらのデータグラムは、必ずしもデータグラムの一部の入力インタフェースではない可能性があります。
Reassembly Request	受信した IPv6 フラグメントの数です。このインタフェースで再構成する必要

フィールド	説明
Datagrams	があります。このカウンタは、これらのフラグメントがアドレス指定されたインタフェースでインクリメントされます。これらのフラグメントは、必ずしも一部のフラグメントの入力インタフェースではない可能性があります。
Reassembled Succeeded	IPv6 データグラムの数が正常に再構成されています。このカウンタは、これらのデータグラムがアドレス指定されたインタフェースで増分されます。これらのデータグラムは、必ずしも一部のフラグメントの入力インタフェースではない可能性があります。
Reassembled Failed	IPv6 再構成アルゴリズムによって検出された障害の数です(何らかの理由でタイムアウト、エラー等)。これは、一部のアルゴリズム(特に RFC 815 のアルゴリズム)がフラグメントの数を受信時に組み合わせて追跡できなくなるため、必ずしも廃棄された IPv6 フラグメントの数ではありません。このカウンタは、これらのフラグメントがアドレス指定されたインタフェースで増分されるものの、一部のフラグメントの入力インタフェースではない可能性があります。
IPv6 Transmitted	
Forwards Datagrams	このエンティティが受信し最終宛先に転送した出力データグラムの数です。IPv6 ルータとして機能しないエンティティでは、このカウンタにはこのエンティティ経由で送信元ルーティングされたパケットのみが含まれ、送信元ルート処理は成功しています。転送されたデータグラムが正常に転送された場合、発信インタフェースのカウンタが増分されることに留意してください。
Requests	ローカル IPv6 ユーザプロトコル(ICMP を含む)が送信要求で IPv6 に提供された IPv6 データグラムの総数です。このカウンタには、ipv6IfStatsOutForwDatagrams でカウントされたデータグラムは含まれません。
Discards	送信先への送信を妨げるような問題は発生しなかったものの、廃棄された(例;バッファスペースが不足している)出力 IPv6 データグラムの数です。このカウンタは、このようなパケットがこの(任意の)破棄基準を満たしていれば、ipv6IfStatsOutForwDatagrams でカウントされたデータグラムを含むことに留意してください。
No Routes	送信先に送信する経路が見つからなかったために破棄された、入力データグラムの数です。
Generated Fragments	この出力インタフェースでフラグメンテーションの結果生成された、出力データグラムフラグメントの数です。
Fragment Succeeded	この出力インタフェースで正常に断片化された、IPv6 データグラムの数です。
Fragment Failed	この出力インタフェースでフラグメント化する必要があったものの、破棄できなかったために破棄された IPv6 データグラムの数です。
ICMPv6 Statistics	
ICMPv6 received	
Input	ipv6IfIcmpInErrors でカウントされたすべての ICMP メッセージを含むインタフェースによって受信された ICMP メッセージの総数です。このインタフェースは ICMP メッセージがアドレス指定されたインタフェースであり、必ずしもメッセージの入力インタフェースではない可能性があることに注意してください。
Errors	インタフェースが受信したが ICMP 固有のエラー(不良 ICMP チェックサム、長さの不良等)があると判断した、ICMP メッセージの数です。
Destination Unreachable Messages	インタフェースによって受信された、ICMP Destination Unreachable メッセージの数です。
Packet Too Big Messages	インタフェースによって受信された、ICMP Packet Too Big メッセージの数です。
Time Exceeded Messages	インタフェースによって受信された、ICMP Time Exceeded メッセージの数です。

フィールド	説明
Parameter Problem Messages	インタフェースによって受信された、ICMP Parameter Problem メッセージの数です。
Echo Request Messages	インタフェースによって受信された、ICMP Echo (要求)メッセージの数です。
Echo Reply Messages	インタフェースによって受信された、ICMP Echo Reply メッセー時の数です。
Router Solicit Messages	インタフェースによって受信された、ICMP Router Solicit メッセージの数です、
Router Advertisement Messages	インタフェースによって受信された、ICMP Router Advertisement メッセージの数です。
Neighbor Solicit Messages	インタフェースによって受信された、ICMP Neighbor Solicit メッセージの数です。
Neighbor Advertisement Messages	インタフェースによって受信された、ICMP Neighbor Advertisement メッセージの数です。
Redirect Messages	インタフェースによって受信された、Redirect メッセージの数です。このインタフェースで受信した休暇メッセージの数です。
Group Membership Query Messages	インタフェースによって受信された、ICMPv6 Group Membership Query メッセージの数です。
Group Membership Response Messages	インタフェースによって受信された、ICMPv6 Group Membership Response メッセージの数です。
Group Membership Reduction Messages	インタフェースによって受信された、ICMPv6 Group Membership Reduction メッセージの数です。
Multicast Listener Discovery Version 2 Reports	インタフェースによって受信された、MLDv2 レポートの数です。
ICMPv6 Transmitted	
Output	このインタフェースが送信しようとした ICMP メッセージの総数です。このカウンタには、icmpOutErrors でカウントされたすべてのカウンタが含まれていることに留意してください。
Destination Unreachable Messages	インタフェースによって送信された、ICMP Destination Unreachable、メッセージの数です。
Packet Too Big Messages	インタフェースによって送信された、ICMP Packet Too Big メッセージの数です。
Time Exceeded Messages	インタフェースによって送信された、ICMP Time Exceeded メッセージの数です。
Echo Request Messages	インタフェースによって送信された、ICMP Echo (要求)メッセージの数です。
Echo Reply Messages	インタフェースによって送信された、ICMP Echo Reply メッセージの数です。
Router Solicit Messages	インタフェースによって送信された、ICMP Router Solicitation メッセージの数です。
Router Advertisement Messages	インタフェースによって送信された、ICMP Router Advertisement メッセージの数です。
Neighbor Solicit Messages	インタフェースによって送信された、ICMP Neighbor Solicit メッセージの数です。
Neighbor Advertisement Messages	インタフェースによって送信された、ICMP Router Advertisement メッセージの数です。
Redirect Messages	送信された Redirect メッセージの数です。ホストについては、ホストはリダイレクトを送信しないため、このオブジェクトは常に 0 となります。
Group Membership Query Messages	インタフェースによって送信された、ICMPv6 Group Membership Query メッセージの数です。

フィールド	説明
Group Membership Response Messages	送信された ICMPv6 Group Membership Response メッセージの数です。
Group Membership Reduction Messages	送信された ICMPv6 Group Membership Reduction メッセージの数です。
Multicast Listener Discovery Version 2 Reports	インタフェースによって送信された、MLDv2 レポートの数です。
UDP Statistics	
Input	UDP ユーザに運ばれた UDP データグラムの総数です。
No Port Errors	宛先ポートにアプリケーションが無かった受信 UDP データグラムの総数です。
Other Errors	宛先ポートでのアプリケーションの不足以外の理由で配信できなかった、受信 UDP データグラムの数です。
Output	エンティティから送信された UDP データグラムの総数です。

Web インタフェース

IPv6 統計情報を表示するには：

1. [IP]、[IPv6 Configuration]をクリックします。
2. [Action]リストから[Show Statistics]を選択します。
3. [IPv6]、[ICMPv6]または[UDP]をクリックします。

図 15-9　IPv6 の統計情報を表示 (IPv6)

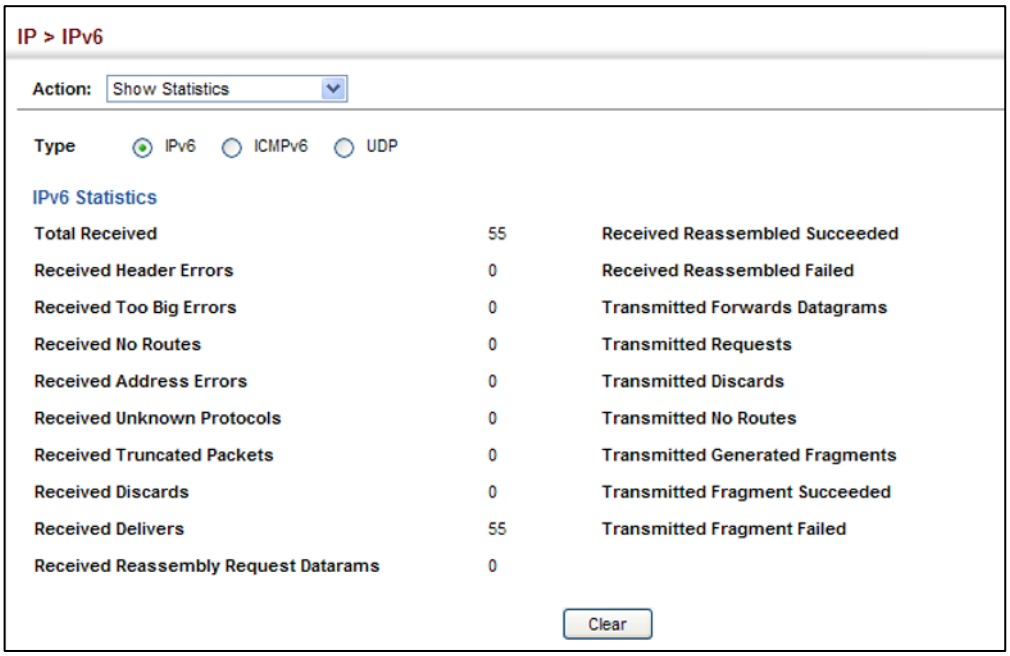


図 15-10　IPv6 の統計情報を表示 (ICMPv6)

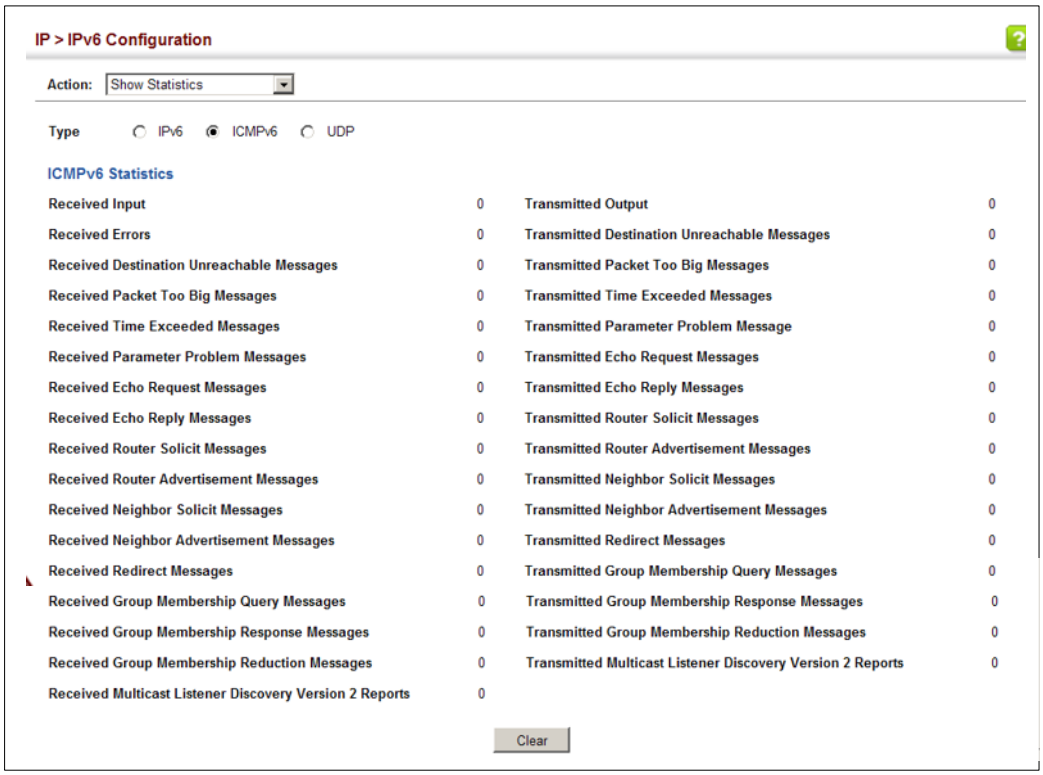
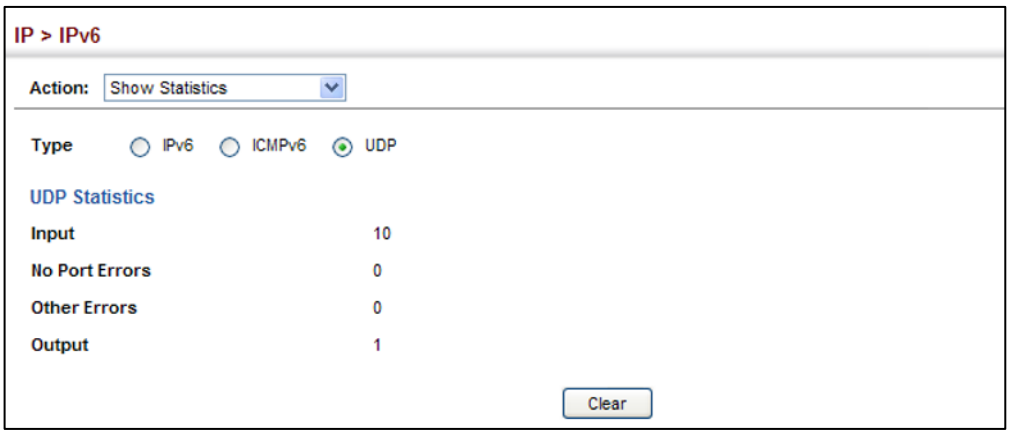


図 15-11　IPv6 の統計情報を表示 (UDP)



15.2.7 応答先の MTU の表示

[IP]> [IPv6 Configuration (ShowMTU）]を使用して、このスイッチへの受け入れ可能な MTU とともに ICMP パケット（大きすぎるメッセージ）を返送した宛先の最大伝送ユニット（MTU）キャッシュを表示します。

パラメータ

次のパラメータが表示されます。

表 15-3　MTU を表示する - 表示の説明

フィールド	説明
MTU	この宛先から返された ICMP パケットの大きすぎるメッセージに含まれる調整済

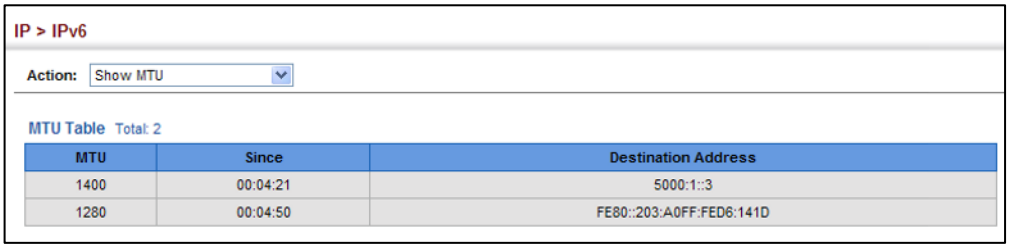
フィールド	説明
	みの MTU です。このパスに沿って送信されたすべてのトラフィックに使用されるようになりました。
Since	この宛先から ICMP パケットが大きすぎるメッセージを受信してからの経過時間です。
Destination Address	ICMP パケットが大きすぎるメッセージを送信したアドレスです。

Web インタフェース

他のデバイスから報告された MTU を表示するには：

1. [IP]、[IPv6 Configuration]をクリックします。
2. [Action]リストから[Show MTU]を選択します。

図 15-12　報告された MTU 値の表示



16 一般的な IP ルーティング

この章では、以下を含むネットワーク機能に関する情報を提供します。

- Static Routes - 他のネットワークセグメントへの静的ルートを設定します。.
- Routing Table - 静的に設定されたエントリによって学習されたルーティングエントリを表示します。

16.1 概要

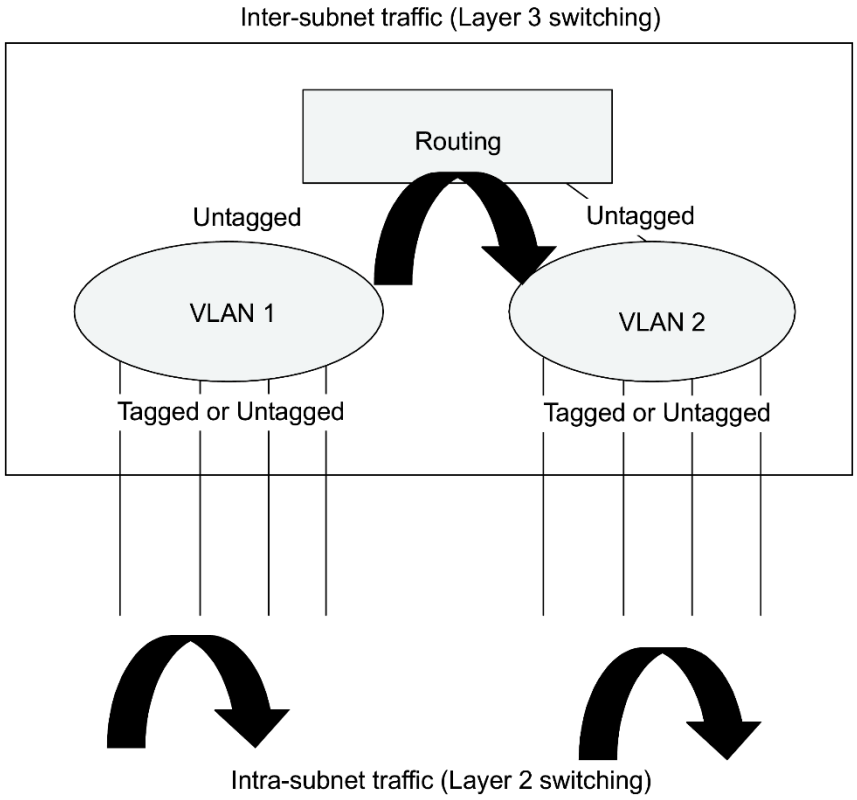
このスイッチは、スタティックルーティング定義と RIP などの動的ルーティングプロトコルによる IP ルーティングおよびルーティングパス管理をサポートします。IP ルーティングが機能している場合、このスイッチはワイヤスピードルータとして機能し、異なる IP インタフェースを持つ VLAN 間でトラフィックを通過させ、トラフィックを外部 IP ネットワークにルーティングします。ただし、スイッチを最初に起動すると、デフォルトルーティングではローカル IP インタフェース間でのみトラフィックを転送できます。すべての従来のルータと同様に、スタティックルーティングは最初に動作するように設定する必要があります。

16.1.1 初期設定

デフォルトでは、すべてのポートが同じ VLAN に属し、スイッチはレイヤ 2 機能のみを提供します。接続されたネットワークをセグメント化するには、最初に一意のユーザーグループまたはアプリケーショントラフィックごとに VLAN を作成し、同じグループに属するすべてのポートをこれらの VLAN に割当て、各 VLAN に IP インタフェースを割当てます。ネットワークを異なる VLAN に分けることで、レイヤ 2 で切断されたサブネットワークに分割できます。同じサブネット内のネットワークトラフィックは、レイヤ 2 スイッチングを使用して切り替えられます。また、VLAN をレイヤ 3 スイッチングと（必要に応じて）相互接続できるようになりました。

各 VLAN はレイヤ 3 への仮想インタフェースを表します。仮想インタフェースごとにネットワークアドレスを指定するだけで、異なるサブネットワーク間のトラフィックはレイヤ 3 スイッチングによってルーティングされます。

図 16-1　仮想インタフェースとレイヤ 3 ルーティング



16.2 IP ルーティングとスイッチング

IP スイッチング（またはパケット転送）には、従来のルーティングと同様に、レイヤ 2 およびレイヤ 3 の両方でパケットを転送するために必要なタスクが含まれます。これらの機能が含まれます:

- レイヤ 2 宛先 MAC アドレスに基づくレイヤ 2 転送（スイッチング）
- レイヤ 3 転送（ルーティング）:
  - レイヤ 3 宛先アドレスに基づいて
  - 各ホップの宛先/送信元 MAC アドレスの置き換え
  - ホップカウントの増分
  - 有効期間の短縮
  - レイヤ 3 チェックサムの確認と再計算

宛先ノードが送信元ネットワークと同じサブネットワーク上にある場合、パケットはルータの助けを借りずに直接送信できます。ただし、MAC アドレスがまだスイッチに認識されていない場合は、宛先 IP アドレスを持つ ARP（Address Resolution Protocol）パケットがブロードキャストされ、宛先 MAC アドレスが宛先ノードから取得されます。IP パケットは宛先 MAC アドレスで直接送信できます。

宛先がこのスイッチ上の別のサブネットに属している場合、そのパケットは直接宛先ノードにルーティングされます。ただし、パケットがこのスイッチに含まれていないサブネットに属している場合は、パケットを次ホップルータに送信する必要があります（宛先 MAC アドレスとして使用されるルータ自体の MAC アドレス、宛先ノードの宛先 IP アドレス ）。ルータはパケットを正しいパスで宛先ノードに転送します。ルータは ARP プロトコルを使用して、必要に応じてネクストホップルータの宛先ノードの MAC アドレスを見つけることもできます。

Note: IP スイッチングを実行するには、他のネットワークノードがスイッチをデフォルトゲートウェイとして設定するか、別のルータから ICMP プロセスを経由してリダイレクトするか、IP ルータとして認識する必要があります。

スイッチが自身の MAC アドレス宛ての IP パケットを受信すると、パケットはレイヤ 3 ルーティングプロセスに従います。宛先 IP アドレスはレイヤ 3 アドレステーブルと照合されます。アドレスがまだ存在しない場合、スイッチは宛先 VLAN 上のすべてのポートに ARP パケットをブロードキャストして宛先 MAC アドレスを検出します。MAC アドレスが検出されると、パケットは再フォーマットされ、宛先に送信されます。再フォーマット処理には、IP ヘッダーの TTL（Time-To-Live）フィールドを減らし、IP ヘッダーチェックサムを再計算し、宛先 MAC アドレスを宛先ノードの MAC アドレスまたは次ホップルーターの MAC アドレスに置き換えます。

同じノード宛ての別のパケットが到着すると、宛先 MAC はレイヤ 3 アドレステーブルから直接取得できます。 パケットは再フォーマットされ、宛先ポートから送出されます。宛先アドレスエントリがすでにレイヤ 3 アドレステーブルにある場合、IP スイッチングはワイヤスピードで実行できます。

スイッチがフレームをルーティングする必要があると判断した場合、ルートはセットアップ中にのみ計算されます。経路が決定されると、現在のフロー内のすべてのパケットが、選択された経路を介して単純に切り替えられるかまたは転送される。これは、パス計算が実行された後に、トラフィックがルーティングエンジンをバイパスできるようにすることにより、高いスループットとスイッチング待ち時間を利用します。

16.2.1 ルーティングパス管理

ルーティングパス管理には、パケット転送に必要なすべてのルーティング情報の決定と更新が含まれます。

- ルーティングテーブルの更新
- レイヤ 3 スイッチングデータベースの更新

16.2.2 ルーティングプロトコル

スイッチはスタティックルーティングをサポートしています。

- 静的ルーティングでは、ルーティング情報を手動で、またはスイッチ外のアプリケーションによって接続が設定されたときにスイッチに格納する必要があります。

16.3 静的ルートの設定

ルーティングテーブルにスタティックルートを入力するには、[IP]>[Routing]>[Static Routes（Add）]ページを使用します。サブネットへの特定のルートの使用を強制するには、静的ルートが必要な場合があります。静的ルートはネットワークトポロジの変更に応じて自動的に変更されないため、ネットワークへのアクセスを確保するために少数の安定したルートを設定する必要があります。

コマンドの使用方法

- 最大 8 の静的ルートを設定することができます。
- 複数のスタティックルートのコストが同じ場合、ルーティングテーブルに格納されている最初のルートが使用されます。

パラメータ

次のパラメータが表示されます。

- Destination IP Address - 宛先ネットワーク、サブネットワーク、またはホストの IP アドレスです。
- Net Mask - 関連する IP サブネットのネットワークマスクです。このマスクは、特定のサブネットへのルーティングに使用されるホストアドレスビットを識別します。
- Next Hop - このルートに使用される次のルータホップの IP アドレスです。
- Distance - このルートが他のルーティング情報によって上書きできることを示す管理ディスタンスです。(範囲: 1 から 255、デフォルト: 1)

Web インタフェース

静的ルートを設定するには：

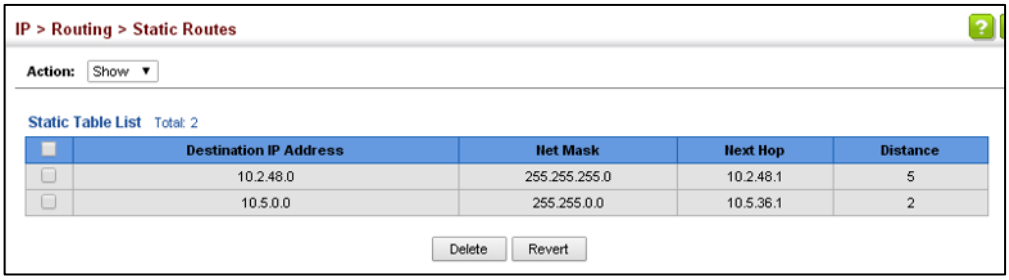
1. [IP]、[Routing]、[Static Routes]をクリックします。
2. [Action]リストから[Add]を選択します。
3. 宛先アドレス、サブネットマスク、ネクストホップルータを入力します。
4. [Apply]をクリックします。

図 16-2　静的ルートの設定

静的ルートを表示するには：

1. [IP]、[Routing]、[Static Routes]をクリックします。
2. [Action]リストから[Show]を選択します。

図 16-3　静的ルートの表示



16.4 ルーティングテーブルの表示

[IP]>[Routing]>[Routing Table]ページを使用して、スタティックルートを介してローカルネットワークインタフェース経由でアクセスできるすべてのルートを表示します。ルート情報がこれらの方法の複数の方法で利用可能な場合、ルート選択の優先順位はローカルであり、次に静的です。また、少なくとも 1 つのアクティブリンクがそのインタフェースに接続されていない限り、ローカルインタフェースのルートは有効ではありません（ルーティングテーブルにリストされています）。

コマンドの使用方法

- 転送情報ベース（FIB）には、IP トラフィックを転送するために必要な情報が含まれています。IP ルーティングテーブルに基づいて、各到達可能な宛先ネットワークプレフィクスのインタフェース識別子と次のホップ情報を含んでいます。ネットワーク内でルーティングまたはトポロジの変更が発生すると、ルーティングテーブルが更新され、それらの変更はすぐに FIB に反映されます。
  FIB は、ルーティングピアから受信したすべてのルーティング情報を保持するルーティングテーブル（または、ルーティング情報ベース-RIB）とは異なります。FIB には一意のパスのみが含まれています。セカンダリパスは含まれません。FIB エントリは、特定のパケットの転送決定を行うために必要な最小限の情報で構成されます。FIB エントリ内の典型的な構成要素は、ネットワークプレフィックス、ルータ（すなわち、VLAN）インタフェース、および次ホップ情報である。
- ルーティングテーブル（および CLI レファレンスガイドで説明されている show ip route コマンド）では、現在転送可能なルートだけが表示されます。ルータは次のホップに直接到達できる必要があるため、どのルートエントリにも関連付けられた VLAN インタフェースが稼動している必要があります。現在、転送にアクセスできないルートは、CLI レファレンスガイドに記載されている show ip route database コマンドを使用して表示できます。

パラメータ

次のパラメータが表示されます。

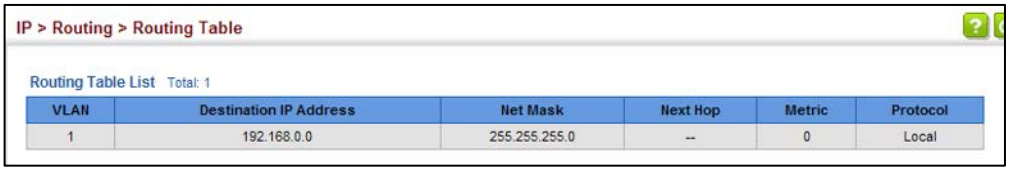
- VLAN - VLAN 識別子（すなわち、有効な IP サブネットとして構成されている）です。
- Destination IP Address - 宛先ネットワーク、サブネットワーク、またはホストの IP アドレスです。アドレス 0.0.0.0 は、このルータのデフォルトゲートウェイを示します。
- Net Mask - 関連する IP サブネットのネットワークマスクです。このマスクは、特定のサブネットへのルーティングに使用されるホストアドレスビットを識別します。
- Next Hop - このルート内の次ホップ（またはゲートウェイ）の IP アドレスです。
- Metric - このインタフェースのコストです。
- Protocol - このルート情報を生成したプロトコルです。(オプション: Local, Static, Others)

Web インタフェース

ルーティングテーブルを表示するには：

1. [IP]、[Routing]、[Routing Table]をクリックします。

図 16-4　ルーティングテーブルの表示



17 IP サービス

この章では、次の IP サービスについて説明します。

- DNS - デフォルトのドメイン名を設定し、動的ルックアップに使用するサーバを特定し、静的エントリを設定する方法を示します。
- Multicast DNS - 専用 DNS サーバを必要とせずにローカルネットワーク上でマルチキャスト DNS ホストの名前からアドレスへのマッピングを設定します。
- DHCP - クライアント、動的プロビジョニングを構成します。

17.1 DNS

このスイッチの DNS サービスを使用すると、静的テーブルエントリを使用するか、ネットワーク上の他のネームサーバへのリダイレクトによって、ホスト名を IP アドレスにマッピングできます。クライアントデバイスがこのスイッチを DNS サーバとして指定すると、クライアントは DNS クエリをスイッチに転送し、応答を待つことでホスト名を IP アドレスに解決しようとします。

ドメイン名を IP アドレスにマッピングしたり、デフォルトのドメイン名を設定したり、ドメイン名の変換に使用する 1 つ以上のネームサーバを指定するために使用される DNS テーブルのエントリを手動で設定できます。

17.1.1 一般的な DNS サービスパラメータの設定

[IP Service]> [DNS]> [General（Configure Global）]ページを使用して、ドメインルックアップを有効にし、デフォルトのドメイン名を設定します。

コマンドの使用方法

- このスイッチで DNS サービスを有効にするには、ドメインルックアップのステータスを有効にし、1 つまたは複数のネームサーバを設定します。
- 1 つ以上のネームサーバが設定されていても DNS がまだ有効になっておらず、スイッチが DNS サーバのリストを含む DNS フィールドを含む DHCP パケットを受信すると、スイッチは自動的に DNS ホストの名前からアドレスへの変換を有効にします。

パラメータ

次のパラメータが表示されます。

- Domain Lookup - DNS ホストの名前からアドレスへの変換を有効にします。(デフォルト: Disabled)
- Default Domain Name - 不完全なホスト名に追加されたデフォルトのドメイン名を定義します。ドメイン名からホスト名を区切る最初のドットは含めないでください。(範囲: 1 から 127 英数字)

Web インタフェース

DNS の一般設定を行うには：

1. [IP Service] > [DNS] > [General]をクリックします。
2. [Action]リストから[Configure Global]を選択します。
3. ドメインの参照を有効にし、既定のドメイン名を設定します。
4. [Apply]をクリックします。

図 17-1　DNS の一般設定

17.1.2 ドメイン名のリストの設定

[IP Service]> [DNS]> [General（Add Domain Name）]ページを使用して、試行するドメイン名のリストを順番に構成します。

コマンドの使用方法

- このページを使用して、不完全なホスト名（クライアントから渡され、ドット区切りで書式設定されていないホスト名）に追加できるドメイン名のリストを定義します。
- ドメインリストがない場合、デフォルトのドメイン名が使用されます。ドメインリストがある場合、システムは対応するエントリを検索します。見つからない場合は、デフォルトのドメイン名が使用されます。
- 不完全なホスト名がこのスイッチの DNS サービスによって受信され、ドメイン名リストが指定されている場合、スイッチはドメインリストを操作し、リスト内の各ドメイン名をホスト名に追加し、指定されたネームサーバで一致するかどうかを確認します。
- すべてのネームサーバが削除された場合、DNS は自動的に無効になります。

パラメータ

次のパラメータが表示されます。

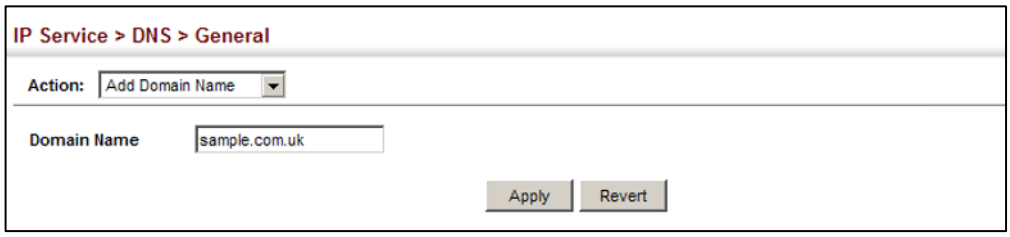
Domain Name - ホスト名です。ドメイン名からホスト名を区切る最初のドットは含めないでください。(範囲: 1 から 127 文字)

Web インタフェース

リストのドメイン名を作成するには：

1. [IP Service] > [DNS] > [General]をクリックします。
2. [Action]リストから[Add Domain Name]を選択します。
3. 一度に 1 つのドメイン名を入力してください。
4. [Apply]をクリックします。

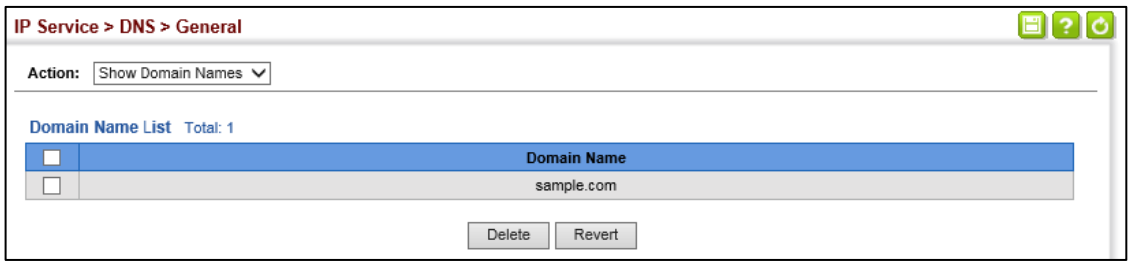
図 17-2　DNS のドメイン名のリストの設定



リストのドメイン名を表示するには：

1. [IP Service] > [DNS] > [General]をクリックします。
2. [Action]リストから[Show Domain Names]を選択します。

図 17-3　DNS のドメイン名のリストを表示



17.1.3 ネームサーバのリストの設定

[IP Service]> [DNS]> [General（Add Name Server）]ページを使用して、ネームサーバのリストを順番に試行するように設定します。

コマンドの使用方法

- このスイッチで DNS サービスを有効にするには、1 つまたは複数のネームサーバを設定し、ドメインルックアップステータスを有効にします。
- 複数のネームサーバが指定されている場合、応答が受信されるか、または応答のないリストの終わりに達するまで、サーバは指定された順序で照会されます。
- すべてのネームサーバが削除された場合、DNS は自動的に無効になります。これは、ドメインルックアップのステータスを無効にすることによって行われます。

パラメータ

次のパラメータが表示されます。

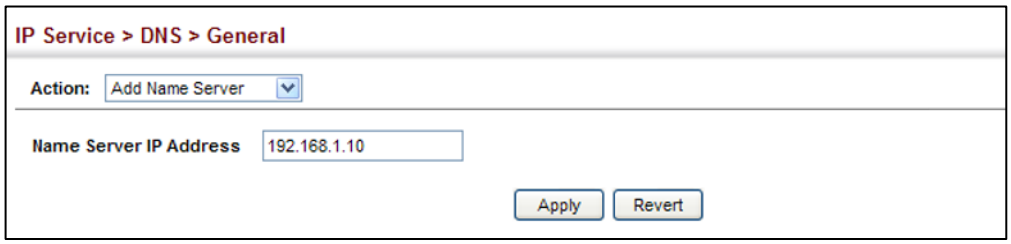
Name Server IP Address - 名前からアドレスへの解決に使用するドメインネームサーバの IPv4 または IPv6 アドレスを指定します。最大 6 つの IP アドレスをネームサーバリストに追加できます。

Web インタフェース

リスト名サーバを作成するには：

1. [IP Service] > [DNS] > [General]をクリックします。
2. [Action]リストから[Add Name Server]を選択します。
3. 一度に 1 つのネームサーバを入力してください。
4. [Apply]をクリックします。

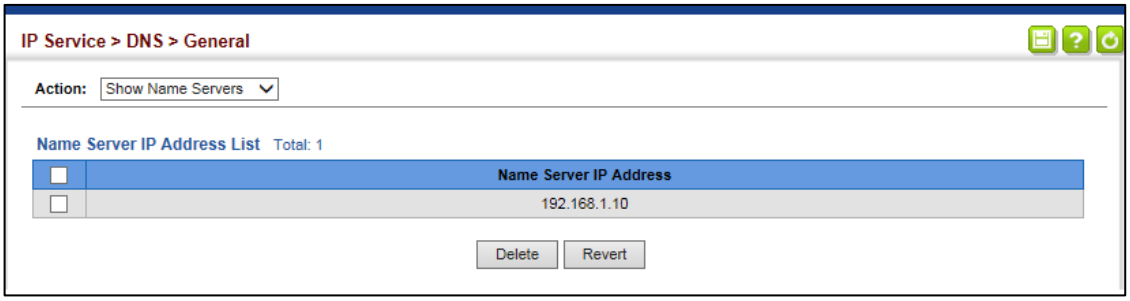
図 17-4　DNS のネームサーバのリストの設定



リストネームサーバを表示するには：

1. [IP Service] > [DNS] > [General]をクリックします。
2. [Action]リストから[Show Name Servers]を選択します。

図 17-5　DNS のネームサーバのリストを表示



17.1.4 エントリをアドレス指定するための静的 DNS ホストの設定

[IP Service]> [DNS]> [Static Host Table（Add）]ページを使用して、ドメイン名を IP アドレスにマッピングするために使用される静的エントリを DNS テーブルに手動で設定します。

コマンドの使用方法

静的エントリは、接続されたネットワークに直接接続されたローカルデバイス、またはネットワーク上の他の場所にある一般的に使用されるリソースに使用できます。

パラメータ

次のパラメータが表示されます。

- Host Name - 1 つ以上の IP アドレスにマップされているホストデバイスの名前です。(範囲: 1 から 127 文字)
- IP Address - ホスト名に関連付けられた IPv4 または IPv6 アドレスです。

Web インタフェース

DNS テーブルに静的エントリを設定するには：

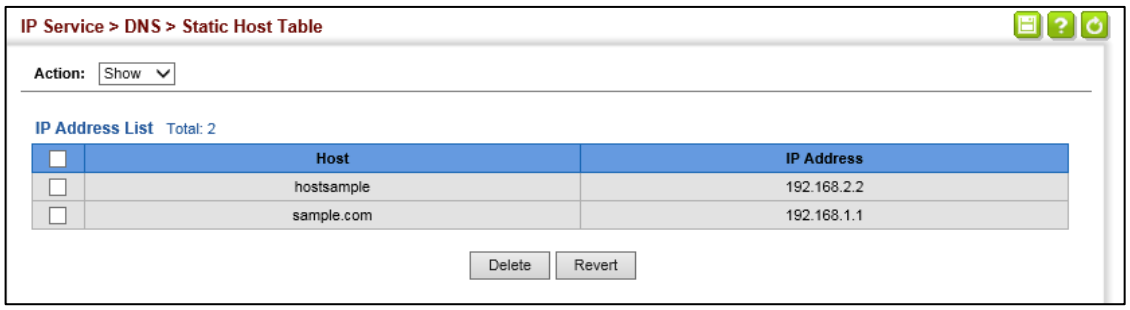
1. [IP Service]、[DNS]、[Static Host Table]をクリックします。
2. [Action]リストから[Add]を選択します。
3. ホスト名と対応するアドレスを入力します。
4. [Apply]をクリックします。

図 17-6　DNS テーブルでの静的エントリの設定

DNS テーブルに静的エントリを表示するには：

1. [IP Service]、[DNS]、[Static Host Table]をクリックします。
2. [Action]リストから[Show]を選択します。

図 17-7　DNS テーブルの静的エントリの表示



17.1.5 DNS キャッシュの表示

[IP Service]> [DNS]> [Cache]ページを使用して、指定されたネームサーバ経由で学習されたエントリを DNS キャッシュに表示します。

コマンドの使用方法

サーバまたは他のネットワーク装置は、複数の IP アドレスを介して 1 つまたは複数の接続をサポートすることができる。複数の IP アドレスがネームサーバから返された情報を介してホスト名に関連付けられている場合、DNS クライアントはターゲットデバイスとの接続を確立するまで、各アドレスを連続して試行できます。

パラメータ

次のパラメータが表示されます。

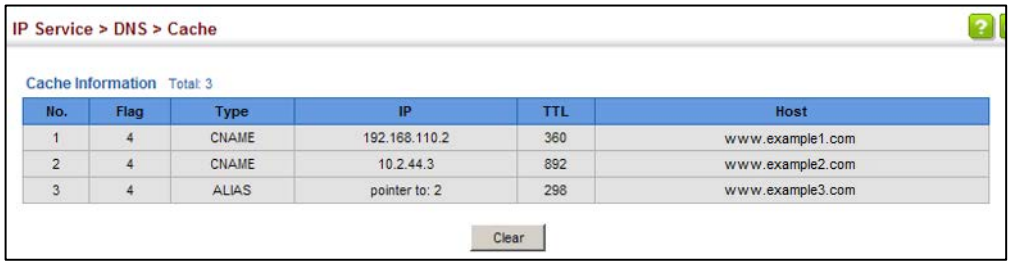
- No. - 各リソースレコードのエントリ番号です。
- Flag - フラグは常にキャッシュエントリを示す "4"であり、したがって信頼できません。
- Type - このフィールドには、所有者のホストアドレスを指定する CNAME と、エイリアスを指定する ALIAS が含まれます。
- IP - このレコードに関連付けられている IP アドレスです。
- TTL - ネームサーバによって報告された生存時間です。
- Host - このレコードに関連付けられたホスト名です。

Web インタフェース

DNS キャッシュにエントリを表示するには：

1. [IP Service]、[DNS]、[Cache]をクリックします。

図 17-8　DNS キャッシュにエントリを表示



17.2 マルチキャスト DNS

[Multicast DNS]ページを使用して、専用 DNS サーバを必要とせずにローカルネットワーク上でマルチキャスト DNS ホストの名前からアドレスへのマッピングを有効にします。

コマンドの使用方法

- マルチキャスト DNS を使用すると、ネットワークデバイスは、ローカル DNS ネームスペース内のドメイン名を選択し、特別なマルチキャスト IP アドレスを使用して通知することができます。これにより、どのユーザも自分のコンピュータに "single-dns-label.local"の形式のリンクローカル mDNS ホスト名を与えることができます。したがって、 ".local。"で終わる任意の名前はリンクローカルであり、このドメイン内の名前は、それらが発信されたリンク上でのみ意味があります。
- 特定のホストの IP アドレスを検索すると、クライアントはローカルネットワークを共有するすべてのホストにシングルショット mDNS IP マルチキャストクエリメッセージを送信します。".local。"で終わる名前の DNS クエリは、mDNS マルチキャストアドレス 224.0.0.251（またはそれに相当する IPv6 の FF02 :: FB）に送信されます。
  対応するホストは、自身をアナウンスするマルチキャストメッセージで応答します。サブネット内のすべてのマシンは、応答メッセージで送信されたホストの情報で mDNS キャッシュを更新できます。
- ホスト名の進行中のキャッシュを維持するには、継続的なマルチキャスト DNS クエリのプロセスが必要です。これはいくつかの段階で行われます。
  - Probing - DNS レスポンダは、各エントリがローカルキャッシュが一意であることを確認するために、プローブメッセージをローカルネットワークに送信します。
  - Announcing - レスポンダは、新しく登録されたすべてのリソースレコード（共有レコードとプロービングステップを完了した固有のレコードの両方）を含む任意の mDNS レスポンスを送信します。
  - Updating - レスポンダは、任意のローカル mDNS レコードのデータが変更されたときにアナウンスステップを繰り返してネイバキャッシュを更新します。

パラメータ

次のパラメータが表示されます。

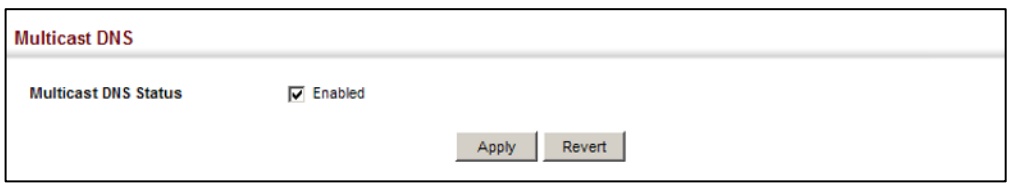
- Multicast DNS Status - ローカルネットワーク上でマルチキャスト DNS ホストの名前からアドレスへのマッピングを有効にします。(デフォルト: Enabled)

Web インタフェース

マルチキャスト DNS を設定するには：

1. [Multicast DNS]をクリックします。
2. チェックボックスをオンにして、必要に応じて mDNS を有効または無効にします
3. [Apply]をクリックします。

図 17-9　マルチキャスト DNS の設定



17.3 DHCP

DHCP（Dynamic Host Configuration Protocol）は、起動時にネットワーククライアントに IP アドレスやその他の構成情報を動的に割当てることができます。

17.3.1 DHCP クライアント識別子の指定

[IP Service]> [DHCP]>[Client]ページを使用して、VLAN インタフェースの DHCP クライアント ID を指定します。

コマンドの使用方法

- クラス識別子は、DHCP サーバへのスイッチのベンダクラスと構成を識別するために使用されます。この情報は、この情報を使用して、クライアントにサービスを提供する方法や返される情報のタイプを決定します。
- この DHCP オプションの一般的なフレームワークは、RFC 2132(オプション 60)に規定されています。この情報は、クライアントに関するコンフィグレーションやその他の識別情報を伝えるために使用されますが、使用する特定の文字列は、サービスプロバイダまたはネットワーク管理者が提供する必要があります。オプション 60,66 および 67 のステートメントをサーバデーモンの構成ファイルに追加することができます。

表 17-1 オプション 60、66 および 67 ステートメント

オプション	ステートメント	
	キーワード	パラメータ
60	vendor-class-identifier	ベンダクラス識別子を示す文字列です。
66	tftp-server-name	tftp サーバ名を示す文字列
67	bootfile-name	bootfile 名を示す文字列

- デフォルトでは、DHCP オプション 66/67 のパラメータは DHCP サーバの応答には含まれません。オプション 66/67 情報で DHCP 応答を要求するには、このスイッチから送信された DHCP クライアント要求に、この情報を要求する“parameter request list”が含まれています。さらに、クライアント要求には、DHCP サーバがデバイスを識別し、ダウンロードするための適切な構成ファイルを選択することを可能にする「ベンダクラス識別子」も含まれています。この情報はオプション 55 および 124 に含まれています。

表 17-2 オプション 55 および 124 ステートメント

オプション	ステートメント	
	キーワード	パラメータ
55	dhcp-parameter-request-list	','で分割されているパラメータリストです。
124	vendor-class-identifier	ベンダクラス識別子を示す文字列です。

- サーバは、TFTP サーバ名とブートファイル名で応答する必要があります。
- ベンダクラス識別子は、テキストまたは 16 進数(ascii コード表記)のいずれかで形成することができますが、クライアントとサーバの両方で使用される形式は同じである必要があります。

パラメータ

次のパラメータが表示されます。

- VLAN - 設定済み VLAN の ID です。

- Vendor Class ID - チェックボックスをオンにしてこの機能を有効にすると、次のオプションがサポートされます。
  - Default - デフォルトの文字列はモデル番号です。
  - Text - テキスト文字列です。(範囲: 1 から 32 文字)
  - Hex - 16 進数の値です。(範囲: 1 から 64 文字)

Web インタフェース

DHCP クライアント識別子を設定するには：

1. [IP Service]、[DHCP]、[Client]をクリックします。
2. この機能を有効にするには、チェックボックスをオンにします。ベンダクラス識別子のデフォルト設定またはフォーマットを選択します。デフォルト以外の値を使用する場合は、テキスト文字列または 16 進数の値を入力します。
3. [Apply]をクリックします。

図 17-10　DHCP クライアント識別子の指定

17.3.2 DHCP ダイナミックプロビジョニング(ゼロタッチプロビジョニング)の有効化

ゼロタッチプロビジョニング(以降、ダイナミックプロビジョニングと呼びます)は、スイッチをネットワークに接続したときに DHCP サーバからコンフィグレーションおよびその他パラメータを自動的にダウンロードする機能です。

[IP Service]> [DHCP]>[Dynamic Provision]を使用して、DHCP によるダイナミックプロビジョニングを有効にします。

DHCPD は、Linux がクライアントシステムの TCP / IP 情報を動的に設定するために使用するデーモンです。DHCP オプション 66/67 をサポートするには、対応するステートメントを DHCPD の構成ファイルに追加する必要があります。このプロセスの完了方法については、CLI レファレンスガイドの説明に従って、“DHCP サーバによって提供される設定ファイルとその他のパラメータのダウンロード”を参照してください。

ダイナミックプロビジョニングプロセスを完了するために DHCPD に追加できるいくつかの代替コマンドについては、CLI レファレンスガイドの ip dhcp dynamic-provision コマンドでも説明しています。

デフォルトでは、DHCP オプション 66/67 のパラメータは DHCP サーバから送られた応答から伝播されません。オプション 66/67 で DHCP 応答を要求するには、クライアントは、「parameter request list」オプションを含む DHCP 要求を送信して、オプション 66/67 に関心があることをサーバに通知できます。これに加えて、クライアントは DHCP サーバがデバイスを識別し、要求するデバイスにどの情報を与えるべきかを決定するために、「vendor class identifier」オプションを含む DHCP 要求をサーバに送信することもできます。

パラメータ

次のパラメータが表示されます。

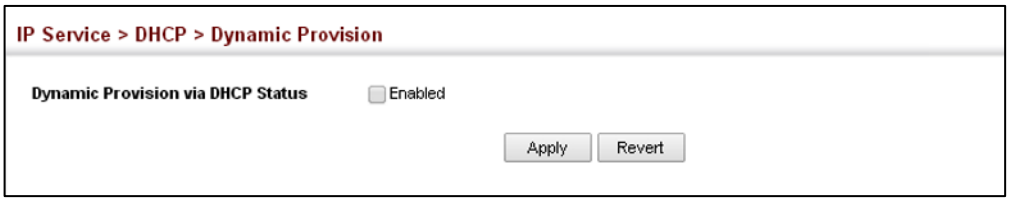
- Dynamic Provision via DHCP Status - DHCP によるダイナミックなプロビジョニングを可能にします。(デフォルト: Enabled)

Web インタフェース

DHCP によるダイナミックプロビジョニングを有効にするには :

1. [IP Service]、[DHCP]、[Dynamic Provision]をクリックします。
2. ダイナミックプロビジョニングが DHCP デーモンで設定されていて、起動に必要な場合は、[Enabled] ボックスにマークを付けます。
3. [Apply]をクリックします。

図 17-11　DHCP によるダイナミックプロビジョニングの有効化



付録

付録A　準拠規格

IEEE 802.1AB Link Layer Discovery Protocol

IEEE 802.1D-2004 Spanning Tree Algorithm and traffic priorities

- Spanning Tree Protocol
- Rapid Spanning Tree Protocol
- Multiple Spanning Tree Protocol

IEEE 802.1p Priority tags

IEEE 802.1Q VLAN

IEEE 802.1v Protocol-based VLANs

IEEE 802.3-2005

- Ethernet, Fast Ethernet, Gigabit Ethernet
- Link Aggregation Control Protocol (LACP)
- Full-duplex flow control (ISO/IEC 8802-3)

IEEE 802.3ac VLAN tagging

ARP (RFC 826)

DHCP Client（RFC 2131）

HTTPS

ICMP (RFC 792)

IGMP (RFC 1112)

IGMPv2 (RFC 2236)

IGMP Proxy（RFC 4541）

IPv4 IGMP (RFC 3228)

MLD Snooping（RFC 4541）

NTP (RFC 1305)

RADIUS+ (RFC 2618)

SNMP (RFC 1157)

SNMPv2c (RFC 1901, 2571)

SNMPv3 (RFC DRAFT 2273, 2576, 3410, 3411, 3413, 3414, 3415)

SNTP (RFC 2030)

SSH (Version 2.0)

TELNET (RFC 854, 855, 856)

TFTP (RFC 1350)

付録B　MIB

Bridge MIB (RFC 1493)

DNS Resolver MIB (RFC 1612)

Entity MIB (RFC 2737)

Ether-like MIB (RFC 2665)

Extended Bridge MIB (RFC 2674)

Extensible SNMP Agents MIB (RFC 2742)

Interface Group（RFC 2233）

Interfaces Evolution MIB (RFC 2863)

IP MIB (RFC 2011)

IP Forwarding Table MIB (RFC 2096)

IP Multicasting related MIB

IPV6-MIB (RFC 2065)

IPV6-ICMP-MIB (RFC 2066)

IPV6-TCP-MIB (RFC 2052)

IPV6-UDP-MIB (RFC2054)

Link Aggregation MIB (IEEE 802.3ad)

MAU MIB (RFC 3636)

MIB II (RFC 1213)

P-Bridge MIB (RFC 2674P)

Port Access Entity Equipment MIB

Power Ethernet MIB (RFC 3621)

Private MIB

Q-Bridge MIB (RFC 2674Q)

QinQ Tunneling　(IEEE 802.1ad Provider Bridges)

Quality of Service MIB

RADIUS Accounting Client MIB (RFC 2620)

RADIUS Authentication Client MIB (RFC 2618)

RMON MIB (RFC 2819)

RMON II Probe Configuration Group (RFC 2021)

SNMP Community MIB (RFC 3584)

SNMP Framework MIB (RFC 3411)

SNMP-MPD MIB (RFC 3412)

SNMP Target MIB、SNMP Notification MIB(RFC 3413)

SNMP User-Based SM MIB (RFC 3414)

SNMP View Based ACM MIB (RFC 3415)

SNMPv2 IP MIB (RFC 2011)

TACACS+ Authentication Client MIB

TCP MIB (RFC 2012)

Trap (RFC 1215)

UDP MIB (RFC 2013)

付録C　トラブルシューティング

付録C.1　管理インタフェースへのアクセスに関する問題

表 C-1　トラブルシューティングチャート

現象	対処方法
Telnet、Web ブラウザ、または SNMP ソフトウェアを使用して接続できません。	・スイッチの電源が入っていることを確認してください。 ・管理ステーションとスイッチ間のネットワークケーブル接続を確認してください。両端が正しく接続され、ケーブルに損傷がないことを確認してください。必要に応じてケーブルをテストします。 ・スイッチとのネットワーク接続が有効で、使用しているポートが無効になっていないことを確認してください。 ・有効な IP アドレス、サブネットマスク、およびデフォルトゲートウェイで管理ステーションが接続されている VLAN インタフェースを設定していることを確認してください。 ・管理ステーションの IP アドレスは、スイッチの IP インタフェースと同じサブネット内にあることを確認してください。 ・タグ付き VLAN グループの IP アドレスを使用してスイッチに接続しようとする場合は、管理ステーションとネットワーク内の中間スイッチを接続するポートに適切なタグを設定する必要があります。 ・Telnet を使用して接続できない場合は、許可されている同時接続可能な Telnet / SSH セッションの最大数を超えている可能性があります。
SSH を使用して接続できません	・SSH を使用して接続できない場合は、許可されている同時接続可能な Telnet / SSH セッションの最大数を超えている可能性があります。 ・スイッチ上で SSH サーバの制御パラメータが正しく設定されていること、および SSH クライアントソフトウェアが管理ステーションで正しく設定されていることを確認してください。 ・スイッチに RSA 公開鍵と DSA 公開鍵の両方を生成し、この鍵を SSH クライアントにエクスポートし、SSH サービスを有効にしてください。別の SSH クライアントを使用するか、SSH クライアントアプリケーションの更新を確認してください。 ・ユーザ名、認証レベル、パスワードなど、各 SSH ユーザのスイッチにアカウントを設定してください。 ・クライアントの公開鍵をスイッチにインポートしたことを確認してください（公開鍵認証が使用されている場合）。
スイッチにシリアルポート接続でアクセスできません。	・ターミナルエミュレータプログラムを VT100 互換、8 データビット、1 ストップビット、パリティなし、およびボーレートを 115200bps に設定しているかどうかを確認してください。

付録C.2　システムログの使用

障害が発生した場合は、「ハードウェア取扱説明書」を参照して、発生した問題が実際にスイッチによって引き起こされていることを確認してください。スイッチによって問題が発生したように見える場合は、次の手順を実行します。

1. ロギングを有効にします。
2. 報告されたエラーメッセージに、すべてのカテゴリを含めるように設定します。

3. SNMP を有効にします。
4. SNMP トラップを有効にします。
5. エラーメッセージを受信する SNMP ホストを指定します。
6. コマンドやエラーにつながる他の一連の動作を繰り返します。
7. 障害につながったコマンドや状況のリストを作成します。また、表示されるエラーメッセージのリストも作成します。
8. すべてのコンソール出力をファイルに取り込むことができるように、端末エミュレーションソフトウェアを設定します。次に、 "show tech-support"コマンドを入力して、このファイルにすべてのシステム設定を記録します。
9. 弊社窓口へご連絡下さい。

下記に例を示します。

```
Console(config)#logging on
Console(config)#logging history flash 7
Console(config)#snmp-server host 192.168.1.23
.
.
.
```

付録D　用語集

ACL（Access Control List）

アクセス制御リスト（ACL）は、ネットワークトラフィックを制限し、特定の IP または MAC（即ち、レイヤ 2）については、各パケットをチェックすることにより、特定のユーザまたはデバイスへのアクセスを制限することができます。

ARP（Address Resolution Protocol）

アドレス解決プロトコル（ARP）は、IP アドレスと MAC アドレスを変換します。ARP は、特定の IP アドレスに対応する MAC アドレスの場所を特定するために使用されます。これにより、スイッチはルーティングの決定に IP アドレスを使用し、対応する MAC アドレスはパケットをあるホップから次のホップに転送します。

BOOTP（Boot Protocol）

ブートプロトコル（BOOTP）は、IP アドレス情報、デバイスのシステムファイルを含む TFTP サーバのアドレス、ブートファイルの名前など、ネットワークデバイスのブートアップ情報を提供するために使用します。

CoS（Class of Service）

サービスクラス（CoS）は、必要なサービスレベルに基づいてパケットに優先順位を付け、適切な出力キューにパケットを配置します。重み付けラウンドロビンサービスを使用してデータがキューから送信され、優先サービスが実行されることで、低レベルキューの閉塞が防止されます。プライオリティは、ポートのデフォルト、パケットのプライオリティビット（VLAN タグ内）、TCP / UDP ポート番号、IP Precedence ビット、または DSCP プライオリティビットに応じて設定できます。

DHCP（Dynamic Host Control Protocol）

動的ホスト制御プロトコル（DHCP）は、TCP / IP ネットワーク上のホストに構成情報を渡すためのフレームワークを提供します。DHCP は Bootstrap Protocol（BOOTP）に基づいており、再利用可能なネットワークアドレスと追加の設定オプションの自動割当て機能が追加されています。

DHCP Option 82

スイッチによって転送された DHCP 要求パケットと DHCP サーバから返信された応答パケットの中で、要求元のクライアント（または中間リレーエージェント）に関する情報を送信するためのリレーオプションです。この情報は、固定 IP アドレスを割当てるために DHCP サーバによって使用されたり、クライアントに他のサービスまたはポリシーを設定したりできます。

DHCP Snooping

DHCP サーバのメッセージをスヌーピングしてホストの物理的な位置を追跡し、ホストが割当てられた IP アドレスのみを使用し、許可された DHCP サーバのみがアクセス可能であることを確認することにより、DHCP サーバへのなりすましや、DHCP サーバへの攻撃を防げます。

DiffServ（Differentiated Services）

差別化サービス（DiffServ）は、さまざまな集約転送動作を構築するための明確に定義されたビルディングブロックを使用することによって、大規模ネットワーク上でサービス品質を提供します。各パ

ケットは、各ホップによって使用される情報（DS バイト）を運び、各ネットワークノードで特定の転送処理またはホップごとの動作を実行します。DiffServ は、トラフィックメーター、シェイパー/ドロッパー、ネットワークの境界にあるパケットマーカーなどのメカニズムを使用して、ネットワーク上のユーザーにさまざまなレベルのサービスを割当てます。

DNS（Domain Name Service）

ドメインネームサービス（DNS）は、ネットワークノードのホスト名を IP アドレスに変換するために使用されるシステムです。

DSCP（Differentiated Services Code Point）

差別化サービスコードポイント（DSCP）は、6 ビットタグを使用して最大 64 の異なる転送動作を提供します。ネットワークポリシーにもとづいて、異なる種類のトラフィックを異なる種類の転送用にマークすることができます。DSCP ビットは、Class of Service カテゴリにマップされ、次に出力キューにマップされます。

EUI（Extended Universal Identifier）

拡張汎用識別子（EUI）は、ネットワークアドレスのホスト部分を識別するための IPv6 で使用されるアドレス形式です。EUI 互換アドレスのインタフェース識別子は、インタフェースのリンクレイヤ（MAC）アドレスに基づいています。グローバルユニキャストおよび他の IPv6 アドレスタイプで使用されるインタフェース識別子は 64 ビット長で、EUI-64 形式で構築できます。変更された EUI-64 形式のインタフェース ID は、リンクレイヤアドレスの上位 3 バイト（OUI フィールド）と下位 3 バイト（シリアル番号）の間に 16 進数の FFFE を挿入することにより、48 ビットのリンクレイヤアドレスから導出されます。選択されたアドレスが固有のイーサネット MAC アドレスからのものであることを保証するため、上位バイトの 7 番目のビットは 1（IEEE Global / Local ビットに相当）に設定され、48 ビットアドレスの一意性を示します。

ICMP（Internet Control Message Protocol）

インターネット制御メッセージプロトコル（ICMP）は、IP パケットを処理する際にエラーを報告するネットワークレイヤプロトコルです。ICMP は、ルーターがより良いルーティング選択に関する情報をフィードバックするためにも使用されます。

IEEE 802.1D

スパニングツリープロトコルを含む MAC ブリッジの一般的な操作方法を指定します。

IEEE 802.1Q

VLAN Tagging - VLAN 情報を伝送するイーサネットフレームタグを定義します。これにより、スイッチは異なる仮想 LAN にエンドステーションを割当てることができ、VLAN がスイッチドネットワークを介して通信するための標準的な方法を定義します。

IEEE 802.1p

イーサネットネットワークでサービス品質（QoS）を提供するための IEEE 標準です。この規格では、最大 8 つのトラフィッククラスを定義するパケットタグを使用し、スイッチがタグ付きプライオリティ値に基づいてパケットを送信できるようにしています。

IEEE 802.1s

マルチプルスパニングツリープロトコル（MSTP）の IEEE 標準は、VLAN グループに独立したスパニングツリーを提供します。

IEEE 802.1w

高速スパニングツリープロトコル（RSTP）の IEEE 標準では、ネットワークトポロジの変更の収束時間を、古い IEEE 802.1D STP 標準で必要とされるものの約 10%に低減します。（現在、IEEE 802.1D-2004 に組み込まれています）

IEEE 802.3ac

VLAN タグ付けのフレーム拡張を定義します。

IEEE 802.3x

全二重リンクのフロー制御に使用されるイーサネットフレームの開始/停止要求とタイマーを定義します。（現在、IEEE 802.3-2002 に組み込まれています）

IGMP（Internet Group Management Protocol）

インターネットグループ管理プロトコル（IGMP）は、ホストがマルチキャストサービスのためにローカルルータに登録するためのプロトコルです。特定のサブネットワーク上に複数のマルチキャストスイッチ/ルータが存在する場合、そのうちの 1 つが「クエリア」になり、グループメンバーシップの追跡を担当します。

IGMP Proxy

プロキシは、ダウンストリームインタフェースでモニタされる IGMP メッセージに基づいて、アップストリームインタフェースにグループメンバーシップ情報をマルチキャストし、その情報に基づいてマルチキャストトラフィックを転送します。IGMP プロキシを使用する単純なツリー内にマルチキャストルーティングプロトコルは必要ありません。

IGMP Query

各サブネットワーク上では、1 つの IGMP 対応デバイスがクエリアとして動作します。つまり、参加したい IP マルチキャストグループまたは既に属している IP マルチキャストグループをすべてのホストに報告するように要求するデバイスです。選択されたクエリアは、サブネットワーク内の IP アドレスが最も小さいデバイスになります。

IGMP Snooping

IP マルチキャストグループのメンバーを識別するために IP マルチキャストルータと IP マルチキャストホストグループとの間で転送される IGMP クエリーおよび IGMP レポートパケットを監視します。

IP Precedence

IPv4 ヘッダーのサービスタイプ（ToS）オクテットには、ネットワーク制御パケットの最高優先順位からルーチントラフィックの最低優先順位までの 8 つの異なる優先レベルを定義する 3 つの優先ビット（IP Precedence）が含まれています。8 つの値は、デフォルトでサービスクラスのカテゴリに 1 対 1 にマッピングされますが、特定のネットワークアプリケーションの要件に合わせて異なるように構成することもできます。

LACP（Link Aggregation Control Protocol）

LACP は、リンク集約制御プロトコルです。ポートが、別のデバイス上の LACP 設定ポートとのトランクリンクを自動的にネゴシエートできるようにします。

Layer 2

ISO 7 層データ通信プロトコルのデータリンク層です。これは、ネットワークデバイスのハードウェアインタフェースに直接関連し、MAC アドレスに基づくトラフィックを通過させます。

Layer 3

ISO 7 層データ通信プロトコルのネットワーク層です。このレイヤーは、1 つのオープンシステムから別のシステムに移動するデータのルーティング機能を処理します。

Link Aggregation

Port Trunk を参照してください。

LLDP（Link Layer Discovery Protocol）

リンク層検出プロトコル（LLDP）は、ローカルブロードキャストドメイン内の隣接デバイスに関する基本情報を検出するために定期的なブロードキャストを使用して、デバイスの識別、機能、および設定の設定などの情報をアドバタイズするために使用されます。

MD5 （Message Digest Algorithm 5）

MD5 は、デジタル署名を作成するために使用されるアルゴリズムです。これは、32 ビットマシンでの使用を意図し、切断された MD4 アルゴリズムより安全です。MD5 は一方向ハッシュ関数です。つまり、メッセージを受け取り、メッセージダイジェストとも呼ばれる固定桁の数字に変換します。

MIB（Management Information Base）

管理情報ベース（MIB）は、特定のデバイスに関する情報を含む一連のデータベースオブジェクトです。

MSTP（Multiple Spanning Tree Protocol）

マルチプルスパニングツリープロトコル（MSTP）は、異なる VLAN に独立したスパニングツリーを提供できます。ネットワーク管理を簡素化し、各リージョンのサイズを制限して RSTP よりも高速なコンバージェンスを実現し、VLAN メンバーが他のグループからセグメント化されないようにします。

NTP（Network Time Protocol）

ネットワークタイムプロトコル（NTP）は、ネットワーク全体の時間を同期させるメカニズムを提供します。タイムサーバは、サブネット内のローカルクロックと有線または無線を介して各国の標準規格とを同期させるために、階層構造を持っております。

Port Mirroring

ロジックアナライザまたは RMON プローブによるトラブルシューティングのために、ターゲットポートのデータをモニタポートに反映させる方法です。

Port Trunk

いくつかの低速物理リンクを組み合わせた単一の高速論理リンクを作成する方法を指定するネットワークリンクアグリゲーションおよびトランキングメソッドを定義します。

QoS（Quality of Service）

サービス品質（QoS）とは、データの優先順位付け、キューイング、輻輳回避、トラフィックシェーピングなどの機能を使用して、選択したトラフィックフローに優れたサービスを提供するネットワークの機能を指します。これらの機能は、1 つのフローの優先順位を上げることによって、または別のフローの優先順位を制限することによって、特定のフローに対して優先的な処理を効果的に提供します。

RADIUS（Remote Authentication Dial-in User Service）

リモート認証ダイヤルインユーザーサービス（RADIUS）は、ネットワーク上の RADIUS 準拠デバイスへのアクセスを制御するために中央サーバ上で実行されるソフトウェアを使用するログオン認証プロトコルです。

RMON（Remote Monitoring）

遠隔モニタリング（RMON）は、包括的なネットワーク監視機能を提供します。標準の SNMP で必要とされるポーリングを排除し、特定のエラータイプを含むさまざまなトラフィック条件でアラームを設定できます。

RSTP（Rapid Spanning Tree Protocol）

高速スパニングツリープロトコル（RSTP）は、ネットワークトポロジ変更の収束時間を、古い IEEE 802.1D STP 標準で要求される収束時間の約 10%に短縮します。

SMTP（Simple Mail Transfer Protocol）

簡易メール転送プロトコル（SMTP）は、TCP（ポート 25）上で動作する標準のホストツーホストメール転送プロトコルです。

SNMP（Simple Network Management Protocol）

簡易ネットワーク管理プロトコル（SNMP）は、ネットワーク管理サービスを提供するインターネットスイートのアプリケーションプロトコルです。

SNTP（Simple Network Time Protocol）

シンプルネットワークタイムプロトコル（SNTP）は、NTP サーバからの定期的な更新に基づいて、デバイスの内部クロックを設定するプロトコルです。内部クロックの更新は、特定の NTP サーバから要求することも、NTP サーバから送信されたブロードキャストを介して受信することもできます。

SSH（Secure Shell）

セキュアシェル（SSH）は、Telnet を含むリモートアクセス機能を安全に置き換えるものです。SSH は暗号鍵でユーザーを認証し、管理クライアントとスイッチ間のデータ接続を暗号化できます。

STA（Spanning Tree Algorithm）

スパニングツリーアルゴリズム（STA）は、ネットワークにループがないかどうかをチェックするテクノロジです。ループは、複雑なまたはバックアップのために冗長化されたネットワークシステムで発生することがよくあります。スパニングツリーは、利用可能な最短経路に沿ってデータを検出して誘導し、ネットワークのパフォーマンスと効率を最大限に高めます。

TACACS+（Terminal Access Controller Access Control System Plus）

ターミナルアクセスコントローラアクセス制御システムプラス（TACACS +）は、ネットワーク上の TACACS 準拠デバイスへのアクセスを制御するために、中央サーバ上で動作するソフトウェアを使用するログオン認証プロトコルです。

TCP/IP（Transmission Control Protocol / Internet Protocol）

伝送制御プロトコル/インターネットプロトコル（TCP/IP）は、プライマリトランスポートプロトコルとして TCP、ネットワークレイヤプロトコルとして IP を含むプロトコルスイートです。

Telnet

TCP / IP を介して端末装置に接続するためのリモート通信機能を定義します。

TFTP（Trivial File Transfer Protocol）

トリビアルファイル転送プロトコル（TFTP）は、ソフトウェアのダウンロードによく使用される TCP / IP プロトコルです。

UDP（User Datagram Protocol）

ユーザデータグラムプロトコル（UDP）は、パケット交換通信のためのデータグラムモードを提供します。これは、IP のようなサービスへのアクセスを提供するための基礎となるトランスポートメカニズムとして IP を使用します。UDP パケットは、IP パケットと同様に配信されます。ターゲットに達する前に破棄されるコネクションレスのデータグラムです。UDP は、TCP が複雑すぎる、遅すぎる、または不必要な場合に便利です。

UTC（Universal Time Coordinate）

ユニバーサルタイムコーディネート（UTC）は、グリニッジ標準時（地球の回転速度のみに基づく）と非常に正確な原子時間を結合する時間スケールです。UTC 自体にはサマータイムがありません。

VLAN（Virtual LAN）

仮想 LAN（VLAN）は、ネットワーク内の物理的な場所または接続ポイントに関係なく、同じコリジョンドメインを共有するネットワークノードの集まりです。VLAN は物理的障壁のない論理的なワークグループとして機能し、ユーザーは同じ LAN 上にあるかのように情報とリソースを共有できます。