

Management Guide

FXC9324XG

Management Guide

FXC9324XG

Management Guide

FXC9324XG

Management Guide

FXC9324XG

Management Guide

FXC9324XG

Management Guide

FXC9324XG

**FXC9324XG
Management Guide**

Management Guide

FXC9324XG

Management Guide

FXC9324XG

Management Guide

FXC9324XG

Management Guide

FXC9324XG

Management Guide

FXC9324XG

Management Guide

FXC9324XG

Management Guide

WEB 設定

本マニュアルについて

- 本マニュアルでは、FXC9324XG の各種設定およびシステムの Web ブラウザによる監視手順について説明します。本製品の設定および監視は、RS-232C シリアルポートまたは、イーサネットポートに設定、監視用の端末接続を行います。



製品取り扱い時のご注意

この度は、お買い上げいただきましてありがとうございます。製品を安全にお使いいただくため、必ず最初にお読みください。

◆ 下記事項は、安全のために必ずお守りください。



- 安全のための注意事項を守る
注意事項をよくお読みください。製品全般の注意事項が記載されています。
- 故障したら使わない
すぐに販売店まで修理をご依頼ください。
- 万一異常が起きたら
 - ◆ 煙が出たら
 - ◆ 異常な音、においがしたら
 - ◆ 内部に水・異物が入ったら
 - ◆ 製品を高所から落としたり、破損したとき

- ①電源を切る（電源コードを抜く）
 - ②接続ケーブルを抜く
 - ③販売店に修理を依頼する
-

- ◆ 下記の注意事項を守らないと、火災・感電などにより死亡や大けがの原因となります。



- 電源ケーブルや接続ケーブルを傷つけない
 - ◆ 電源ケーブルを傷つけると火災や感電の原因となります。
 - ◆ 重いものをのせたり、引っ張ったりしない。
 - ◆ 加工したり、傷つけたりしない。
 - ◆ 熱器具の近くに配線したり、加熱したりしない。
 - ◆ 電源ケーブルを抜くときは、必ずプラグを持って抜く。
 - 内部に水や異物を入れない
 - ◆ 火災や感電の原因となります。
 - ◆ 万一、水や異物が入ったときは、すぐに電源を切り（電源ケーブルを抜き）、販売店に点検・修理をご依頼ください。
 - 内部をむやみに開けない

本体及び付属の機器（ケーブル含む）をむやみに開けたり改造したりすると、火災や感電の原因となります。
 - 落雷が発生したらさわらない

感電の原因となります。また、落雷の恐れがあるときは、電源ケーブルや接続ケーブルを事前に抜いてください。本機が破壊される原因となります。
 - 油煙、湯気、湿気、ほこりの多い場所には設置しない

本書に記載されている使用条件以外の環境でのご使用は、火災や感電の原因となります。
-

- ◆ 下記の注意事項を守らないとけがをしたり周辺の物品に損害を与える原因となります。



- ぬれた手で電源プラグやコネクタに触らない
感電の原因となります。
- 指定された電源コードや接続ケーブルを使う
マニュアルに記載されている電源ケーブルや接続ケーブルを使わないと、火災や感電の原因となります。
- 指定の電圧で使う
マニュアルに記されている電圧の範囲で使わないと、火災や感電の原因となります。
- コンセントや配線器具の定格を超えるような接続はしない
発熱による火災の原因となります。
- 通風孔をふさがない
 - ◆ 通風孔をふさいでしまうと、内部に熱がこもり、火災や故障の原因となります。また、風通しをよくするために次の事項をお守りください。
 - ◆ 毛足の長いジュウタンなどの上に直接設置しない。
 - ◆ 布などでくるまない。
- 移動させるときは、電源ケーブルや接続ケーブルを抜く
接続したまま移動させると、電源ケーブルが傷つき、火災や感電の原因となります。

Web 設定	1
Web インターフェースの使用	2
Web インターフェースへの接続	2
Web ブラウザインターフェースの操作	3
基本的な管理作業.....	25
システム情報の表示	25
スイッチのハードウェアとソフトウェアのバージョンの表示	26
ジャンボフレームのサポートの設定	28
ブリッジ拡張機能の表示	29
システムファイルの管理	31
システムクロックの設定	36
コンソールポートの設定	40
Telnet 設定	42
CPU 使用率の表示	44
メモリ使用量の表示	45
スタック番号の再割り当て	46
システムのリセット	47
インターフェース設定	51
ポート設定	51
トランク設定（リンクアグリゲーション）	66
トラフィックフローのサンプリング	80
トラフィックのセグメント化（プライベート VLAN）	82
VLAN トランッキング	86
VLAN 設定	88
IEEE 802.1Q VLAN	88
IEEE 802.1Q トンネリング	100
プロトコル VLAN	110
IP サブネット VLAN の設定	115
MAC ベースの VLAN の設定	117
アドレステーブル設定	119
MAC アドレス学習の設定	119
スタティックアドレスの設定	121
エージングタイムの変更	123
ダイナミックアドレステーブルの表示	124
ダイナミックアドレステーブルの作成	126
スパニングツリーアルゴリズム	127
概要	127
ループバック検出の設定	130
STA のグローバル設定の設定	132
STA のグローバル設定の表示	137

STA のインターフェース設定の設定	138
STA のインターフェース設定の表示	142
マルチプルスパニングツリー (MSTP) の設定	145
MSTP のインターフェース設定の設定	150
輻輳制御	153
レートリミット	153
ストームコントロール	155
自動トラフィック制御	157
CoS (Class of Service)	163
レイヤ 2 のキューの設定	163
レイヤ 3/4 優先度の設定	170
QoS (Quality of Service)	176
概要	176
QoS ポリシーの作成	181
ポートへのポリシーマップのバインディング	190
VoIP トラフィック設定	191
概要	191
VoIP トラフィックの設定	192
テレフォニー OUI の設定	194
VoIP トラフィックポートの設定	196
セキュリティ対策	198
AAA 認証とアカウント	199
ユーザアカウントの設定	215
Web 認証	218
ネットワークアクセス (MAC アドレス認証)	222
HTTPS の設定	234
セキュアシェルの設定	238
アクセスコントロールリスト	247
ARP インспекション	269
管理アクセスのための IP アドレスフィルタリング	278
ポートセキュリティの設定	280
802.1X ポート認証の設定	282
IP ソースガード	291
DHCP スヌーピング	298
基本的な管理プロトコル	308
イベントログの設定	308
LLDP (Link Layer Discovery Protocol)	315
SNMP (Simple Network Management Protocol)	329
リモートモニタリング (RMON)	354

マルチキャストフィルタリング	365
概要	365
IGMP (Internet Group Management Protocol)	367
レイヤ 2 の IGMP (スヌーピングとクエリ)	368
IGMP グループのフィルタリングとスロットリング	387
レイヤ 3 の IGMP (マルチキャストルーティングと共に使用されるクエリ)	394
MVR (Multicast VLAN Registration)	406
IP 設定	418
スイッチの IP アドレスの設定 (IPv4)	418
スイッチの IP アドレスの設定 (IPv6)	423
一般的な IP ルーティング	441
概要	441
IP ルーティングおよび IP スwitチング	442
IP ルーティングインターフェースの設定	444
アドレス解決プロトコル	449
スタティックルートの設定	457
ルーティングテーブルの表示	459
イコールコストマルチパスルーティング	461
ルータ冗長性の設定	463
VRRP グループの設定	465
VRRP グローバル統計情報の表示	471
VRRP グループに関する統計情報の表示	473
IP サービス	475
ドメインネームサービス	475
ダイナミックホスト設定プロトコル	482
UDP サービス要求の転送	493
ユニキャストルーティング	498
概要	498
RIP (Routing Information Protocol) の設定	499
OSPF プロトコル (バージョン 2) の設定	522
マルチキャストルーティング	561
概要	561
マルチキャストルーティングのグローバル設定の設定	564
IPv4 PIM の設定	568
IPv6 PIM の設定	588

1 Web 設定

ここでは、基本的なスイッチ機能について説明すると共に、Web ブラウザを使用して個々の機能を設定する方法を紹介します。

このセクションは、以下の章から設定されています。

「Web インターフェースの使用」

「基本的な管理作業」

「インターフェース設定」

「VLAN 設定」

「アドレステーブル設定」

「スパニングツリーアルゴリズム」

「輻輳制御」

「CoS (Class of Service)」

「QoS (Quality of Service)」

「VoIP トラフィック設定」

「セキュリティ対策」

「基本的な管理プロトコル」

「マルチキャストフィルタリング」

「IP 設定」

「一般的な IP ルーティング」

「ルータ冗長性の設定」

「IP サービス」

「ユニキャストルーティング」

「マルチキャストルーティング」

Web 設定

Web インターフェースの使用

1.1 Web インターフェースの使用

本製品には HTTP Web エージェントが組み込まれているので、Web ブラウザを使用して、スイッチを設定し、統計値を確認してネットワークアクティビティを監視することができます。Web エージェントには、標準の Web ブラウザ（Internet Explorer 5.0 以上または Mozilla Firefox 2.0.0.0 以上）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することができます。

【注意】 コマンドラインインターフェース（CLI）を使用して、コンソールポートへのシリアル接続経由または Telnet 接続で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、「コマンドラインの設定」を参照してください。

1.1.1 Web インターフェースへの接続

Web ブラウザからスイッチにアクセスする前に、必ず、以下の作業を行ってください。

- (1) コンソール接続、BOOTP プロトコル、または DHCP プロトコルを使用して、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スイッチに指定して設定します（「Setting an IP Address」を参照）。
- (2) コンソール接続を使用して、ユーザ名とパスワードを設定します。Web エージェントへのアクセスは、オンボードの設定プログラムと同じユーザ名とパスワードによって制御されます（「Setting Passwords」を参照）。
- (3) ユーザ名とパスワードを入力すると、システム設定プログラムにアクセスできるようになります。

【注意】 パスワードは 3 回まで入力することができます。間違ったパスワードを 3 回入力すると、接続操作が強制終了されます。

【注意】 Web インターフェースにゲスト（標準の実行権限レベルのユーザ）としてログインすると、設定の設定を表示したり、ゲストパスワードを変更したりすることができます。「admin」（特権付き実行権限レベルのユーザ）としてログインすると、任意のページで設定を変更することができます。

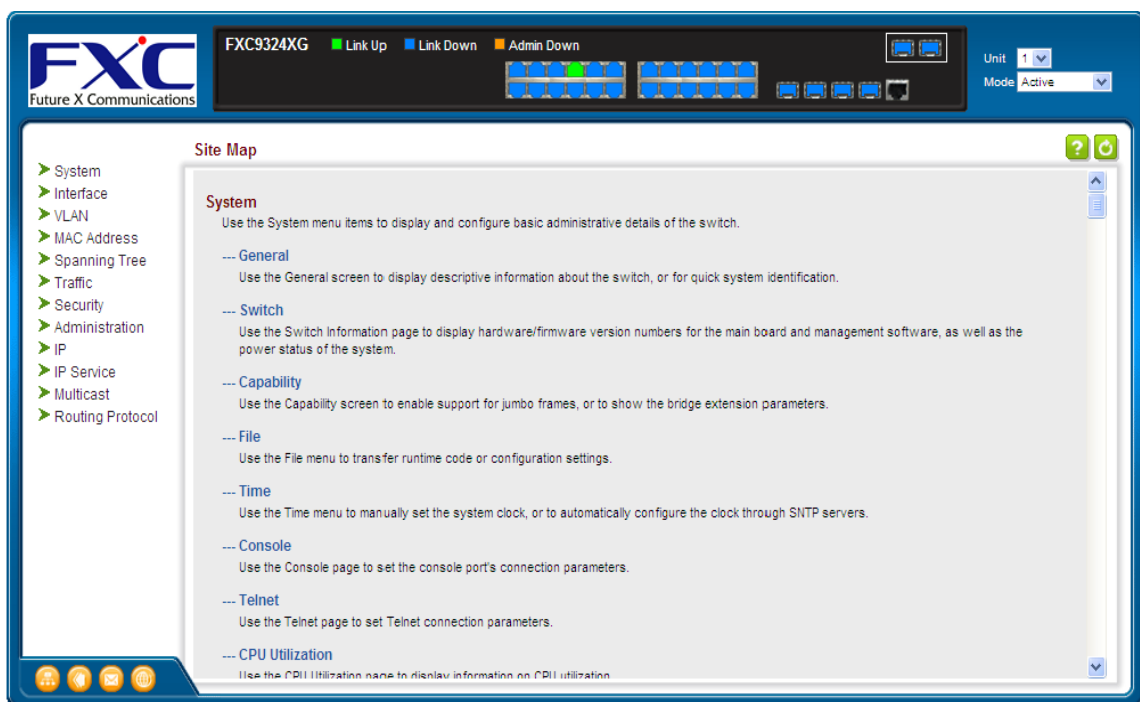
【注意】 管理ステーションと本製品の間の経路がスパニングツリーアルゴリズムを使用するデバイスを経由しない場合は、管理ステーションに接続しているスイッチポートを高速転送に設定し（つまり、管理エッジポートを有効にし）、Web インターフェースを使用して発行される管理コマンドに対するスイッチの応答時間を改善することができます。「STA のインターフェース設定の設定」を参照してください。

1.1.2 Web ブラウザインターフェースの操作

Web ブラウザインターフェースにアクセスするには、最初に、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、すべての設定パラメータと統計値に対する読み取り / 書き込みアクセス権をもちます。管理者のデフォルトのユーザ名とパスワードは「admin」です。

ホームページ

Web ブラウザを使用してスイッチの Web エージェントに接続すると、以下のようなホームページが表示されます。ホームページでは、左側にメインメニューが表示され、右側にシステム情報が表示されます。メインメニューのリンクを使用して他のメニューに移動し、設定パラメータと統計値を表示します。



画面 1-1 : ホームページ

【注意】 画面左上隅に表示される FXC のロゴをクリックすると、ベンダーの Web サイトに接続することができます。

オプション

設定可能なパラメータには、対応する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。ページで設定を変更した場合は、必ず **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。Web ページに表示される設定ボタンは、以下の表のとおりです。

パネルディスプレイ

Web エージェントポートには、スイッチのポートの図が表示されます。ポートに関する各種の情報として、「Active」（「Up」または「Down」）、「Duplex」（「Half Duplex」または「Full Duplex」）、あるいは「Flow Control」（「With Flow Control」または「Without Flow Control」）などが表示されるようにモードを設定することができます。

Web 設定

Web インターフェースの使用

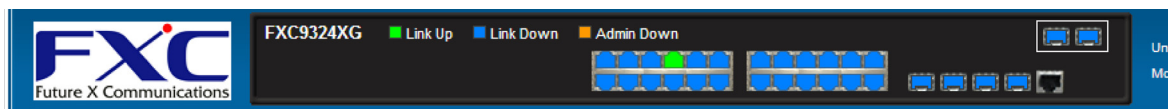


図 5-1：前面パネルのインジケータ

設定ボタンについては、以下のとおりです。

- 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て、< Apply > ボタンをクリックする前の最新の値に戻します。



選択したページのヘルプを表示します。



現在表示されているページの内容を更新します。



最新の設定情報を保存します。



サイトマップを表示します。



管理インターフェースをログアウトします。



ベンダーに電子メールを送信します。



ベンダーの Web サイトにジャンプします。

メインメニュー

オンボードの Web エージェントを使用して、システムパラメータの定義、スイッチとすべてのスイッチポートの管理と制御、またはネットワークの状態の監視を行うことができます。このプログラムで使用できる選択項目の概要は、以下のとおりです。

スイッチのメインメニュー

System

- ・ General 連絡先情報を始めとするシステムに関する基本的な説明を表示します。
- ・ Switch ポート数、ハードウェアのバージョン、電源ステータス、およびファームウェアの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。また、ブリッジ拡張パラメータを表示します。
- ・ File

- ・ Copy ファイルを転送およびコピーすることができます。
- ・ Set Startup 起動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。また、ファイルを削除することができます。
- ・ Automatic Operation Code Upgrade
サーバで新しいバージョンのオペレーションコードが検出された場合に自動的にオペレーションコードをアップグレードします。
- ・ 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: 認証ステータスの有効化と、ポーリング間隔の設定をします。
 - ・ Configure Time ServerSNTP サーバのリストを構成します。
 - ・ 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。
- ・ Console
コンソールポート接続パラメータを設定します。
- ・ Telnet:
接続パラメータを設定します。
- ・ CPU Utilization
CPU 使用状況に関する情報を表示します。
- ・ Memory Status
メモリの使用状況に関するパラメータを表示します。
- ・ Renumbering
スタック内のユニットの番号を再割り当てします。
- ・ Reset
 - Immediately: 即座に再起動します。
 - In: 指定した時刻が経過した場合に再起動します。
 - At: 指定した年月日の時刻になった時点で再起動します。
 - Regularly: 定期的に再起動します。

Interface

Port

- ・ General
 - ・ Configure by Port List: ポートごとの接続設定を行うことができます。
 - ・ Configure by Port Range: 範囲を指定し、指定した範囲のポートを一括で接続設定を行うことができます。
 - ・ Show Information: ポートの接続ステータスを表示します。
- ・ Mirror
 - ・ Add ミラーリングに使用する送信元ポートとターゲットポートを設定します。

Web 設定

Web インターフェースの使用

- ・ Show 構成済みのミラーリングセッションを表示します。
- ・ Statistics インターフェース、Etherlike、RMON、および使用状況といった側面からとらえたポートに関する統計情報を一覧表示します。
- ・ Chart
インターフェース、Etherlike、RMON、および使用状況といった側面からとらえたポートに関する統計情報をグラフ形式で表示します。
- ・ Cable Test
選択したポートのケーブル診断を実行します。ケーブルに関する障害（ショートケーブルやオープンケーブルなど）がないかどうかを確認され、ケーブルの長さが報告されます。

Trunk

Static

- ・ Configure Trunk
 - ・ Add: トランクを最初のポートメンバーと併せて作成します。
 - ・ Show: 設定済みのトランク ID を表示します。
 - ・ Add Member: スタティックトランクにまとめるポートを指定します。
 - ・ 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: トランク接続設定を構成します。
 - ・ Show Information: トランク接続設定を表示します。

Dynamic

- ・ Configure Aggregator: 個々の LACP グループの管理キーを構成します。
- ・ Configure Aggregation Port
 - ・ Configure
 - General: ポートが動的にトランクのメンバーになるか否かの設定が出来ます。
 - Actor: ローカル側のリンクアグリゲーショングループの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アグリゲーショングループのメンバーのパラメータを設定します。
- ・ Configure Trunk
 - ・ Configure 接続設定を構成します。
 - ・ Show ポートの接続ステータスを表示します。

sFlow

送信元ポートと宛先ポートのフローサンプリングを構成します。

Traffic Segmentation

Configure Global

トラフィックのセグメント化をグローバルで有効にします。

- ・ 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ポートとダウンリンクポートを構成します。

- ・ VLAN Trunking: 指定されたインターフェースを不明な VLAN グループが経由できるようにします。

VLAN :

Static

- ・ Add

新しい VLANID を作成できます。

- ・ Show

作成されている VLANID の情報を見ることができます。

- ・ Modify

指定した VLANID の名前とステータスを変更することが出来ます。

Dynamic

- ・ Configure GeneralGVRP VLAN 登録プロトコルをグローバルで有効にします。
- ・ Configure Interface インターフェースごとの GVRP ステータスとタイマーを設定します。
- ・ Show Dynamic VLAN
 - ・ Show VLAN: スイッチが GVRP を使用してメンバーとなった VLAN を表示します。
 - ・ Show VLAN Member: GVRP を使用して VLAN に割り当てられているインターフェースを表示します。

Tunnel – IEEE 802.1Q (QinQ) Tunneling

- ・ Configure Global: スイッチのトンネルモードを設定します。
- ・ Configure Service: SPVLAN マッピングエントリに対する CVLAN を設定します。
- ・ Configure Interface: 該当のインターフェースのトンネルモードを設定します。

Protocol

- ・ Configure Protocol
 - ・ Add: プロトコルグループを作成し、サポートされるプロトコルを指定します。
 - ・ Show: 構成されている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 にマップします。
 - ・ Show: 各 VLAN にマップされているプロトコルグループを表示します。
- ・ IP Subnet
 - ・ Add: IP サブネットトラフィックを VLAN にマップします。
 - ・ Show: IP サブネットと VLAN のマッピングを表示します。
- ・ MAC-Based
 - ・ Add: トラフィックを指定された送信元 MAC アドレスと共に VLAN にマップします。
 - ・ Show: 送信元 MAC アドレスと VLAN のマッピングを表示します。
- ・ MAC Address
 - ・ Learning Status: 選択したインターフェースで学習される MAC アドレスを有効にします。

Web 設定

Web インターフェースの使用

- ・ Static
 - Add: アドレステーブルのスタティックエントリを構成します。
 - Show: アドレステーブルのスタティックエントリを表示します。
- ・ Dynamic
 - ・ Configure Aging: 動的に学習されたエントリの有効期限を設定します。
 - ・ Show Dynamic : MAC アドレステーブルのダイナミックエントリを表示します。
 - ・ Clear Dynamic : MAC 学習されたエントリをすべて転送データベースから削除し、スタティックエントリおよびシステム構成エントリの送信カウントと受信カウントをクリアします。

Spanning Tree

Loopback Detection ループバック検出パラメータを設定します。

STA Spanning Tree Algorithm

- ・ Configure Global
 - ・ ConfigureSTP、RSTP、および MSTP のグローバルブリッジ設定を構成します。
 - ・ Show Information ブリッジに使用されている STA 値を表示します。
- ・ Configure Interface
 - ・ ConfigureSTA のインターフェース設定を構成します。
 - ・ Show InformatonSTA のインターフェース設定を表示します。

MSTP– Multiple Spanning Tree Algorithm

- ・ Configure Global
 - ・ Add: MST インスタンスについて、初期 VLAN メンバーを構成し、優先度を設定します。
 - ・ Show: MST インスタンスのグローバル設定を表示します。
 - ・ Modify: MST インスタンスの優先度を変更します。
 - ・ Add Member: MST インスタンスの VLAN メンバーを追加します。
 - ・ Show Member: MST インスタンスの VLAN メンバーを表示または削除します。
 - ・ Show Information: ブリッジに使用されている MSTP 値を表示します。
- ・ Configure Interface
 - ・ Configure: MST インスタンスのインターフェース設定を構成します。
 - ・ Show Informaton: MST インスタンスのインターフェース設定を表示します。

Traffic

Rate Limit: ポートの入力と出力のレトリミットを設定します。

Storm Control: インターフェースごとのブロードキャストストームしきい値を設定します。

Auto Traffic Control: 構成済みのレトリミットのトリガーまたはポートのシャットダウンに使用できる、ブロードキャストストームおよびマルチキャストストームのしきい値を設定することができます。

Priority

- ・ Default Priority: 各ポートまたはトラックのデフォルトの優先度を設定します。
- ・ Queue: スイッチのキューモードを設定し、重み付きモードまたはハイブリッドモードで使用する各キューのサービスの重みを設定します。

- ・ CoS to QueueCoS: 優先度タグ付きトラフィックに使用される出力キューを指定します。
- ・ IP DSCP to CoS: 内部的な優先度処理のため、イングレスパケットで検出された IP DSCP 優先度を CoS 値にマップします。
- ・ IP Precedence to CoS: 内部的な優先度処理のため、イングレスパケットで検出された IP 優先順位を CoS 値にマップします。
- ・ IP Port to CoS: 内部処理のため、フレームヘッダ内の TCP/UDP 宛先ポート番号によって指定されたネットワークアプリケーションを CoS 値にマップします。

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: 構成されている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: イングレストラフィックの分類に使用される条件を設定します。
 - ・ Show Rule: クラスマップトラフィック分類ルールを表示します。
- ・ Configure Policy
 - ・ Add: 複数のインターフェースに適用されるポリシーマップを作成します。
 - ・ Show: 構成されている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: インバウンドトラフィックの監視に使用される境界パラメータを設定し、ポリシーに準拠しているトラフィックおよびポリシーに準拠していないトラフィックに対するアクションを指定します。
 - ・ Show Rule: ポリシーマップの帯域幅ポリシー設定を強制適用するために使用されるルールを表示します。
- ・ Configure Interface: ポリシーマップをイングレスポートに適用します。

VoIP Voice over IP

- ・ Configure Global: VoIP トラフィックの自動検出を構成し、音声 VLAN を指定し、VLAN のエイジングタイムを設定します。
- ・ Configure OUI
 - ・ Add: イングレスパケットの送信元 MAC アドレスの OUI を VoIP デバイスペンダーにマップします。
 - ・ Show: OUI テレフォニーリストを表示します。
- ・ Configure Interface: ポートを音声 VLAN に追加する方法、非 VoIP パケットのフィルタリング、VoIP トラフィックの検出方法、および音声トラフィックに割り当てられる優先度など、ポートの VoIP トラフィック設定を構成します。

Security

AAA- Authentication, Authorization and Accounting

- ・ System Authentication: ローカル、RADIUS、および TACACS の認証順序を指定します。
- ・ Server
 - ・ Configure Server: RADIUS サーバおよび TACACS サーバに関するメッセージ交換設定を構成します。
 - ・ Configure Group

Web 設定

Web インターフェースの使用

- 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: 請求またはセキュリティのため、要求されたサービスのアカウントリングを有効にします。
 - ・ Configure Global: ローカルアカウントリングサービスがアカウントリングサーバに対して情報を更新する間隔を指定します。
 - ・ Configure Method
 - Add: 各種のサービスのアカウントリングを構成します。
 - Show: 各種のサービスで使用するアカウントリング設定を表示します。
 - ・ Configure Service: コンソールポートの CLI 権限レベル、および Telnet に関し、個々のインターフェースに適用されるアカウントリング方式を設定します。
 - ・ Show Information
 - Summary: 設定されているアカウントリング方式、および特定のインターフェースに適用されているアカウントリング方式を表示します。
 - Statistics: ユーザセッションで記録された基本的なアカウントリング情報を表示します。
- ・ Authorization: 要求されたサービスの承認を有効にします。
 - ・ Configure Method
 - Add: 各種のサービスの承認を構成します。
 - Show: 各種のサービスで使用する承認設定を表示します。
 - ・ Configure Service: コンソールポートおよび Telnet に適用される承認方式を設定します。
 - ・ Configure Method
 - Add: 各種のサービスの承認を構成します。
 - Show: 各種のサービスで使用する承認設定を表示します。
 - ・ Configure Service: コンソールポートおよび Telnet に適用される承認方式を設定します。
 - ・ Show Information: 設定されている承認方式、および特定のインターフェースに適用されている承認方式を表示します。

User Accounts

- ・ Add: ユーザ名、パスワードおよびアクセスレベルを設定します。
- ・ Show: 承認済みユーザを表示します。
- ・ Modify: ユーザ属性を変更します。

Web Authentication

802.1X 認証または MAC 認証が実現できない状況または実用的ではない状況で管理ステーションにおけるサービス承認とネットワークアクセス認証を可能にします。

- ・ Configure Global: Web 認証をグローバルで有効にし、メッセージ交換パラメータを設定します。
- ・ Configure Interface: 指定されたポートで Web 認証を有効にします。

Network Access: MAC アドレスベースのネットワークアクセス認証

- ・ Configure Global: 認証済み MAC アドレスの有効期限を指定し、接続状態の MAC アドレスの再認証が必要になるまでの期間を設定します。

- ・ Configure Interface
 - ・ General: ポートで MAC 認証を有効にし、認証できる MAC アドレスの最大数を設定し、ゲスト VLAN、ダイナミック VLAN、およびダイナミック QoS を指定します。
 - ・ Link Detection: リンクステータスに変更されたことを検出するかどうかを指定し、その場合の対応（トラップの送信またはポートのシャットダウン）を指定します。
- ・ Configure MAC Filter
 - ・ Add: 認証対象から除外される MAC アドレスを指定します。
 - ・ Show: 認証対象から除外される MAC アドレスを一覧表示します。
- ・ Show Information: 認証されている MAC アドレスを一覧表示します。

HTTPS Secure HTTP

- ・ 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 Secure Shell

- ・ Configure Global: SSH サーバ設定を構成します。
- ・ Configure Host Key
 - Generate: ホストキーのペア（公開キーと秘密キー）を生成します。
 - Show: RSA ホストキーと DSA ホストキーを表示または削除します。
- ・ Configure User Key
 - Copy - TFTP サーバからユーザ公開キーをインポートします。
 - Show - RSA ユーザキーと DSA ユーザキーを表示または削除します。

ACL (Access Control List)

- ・ Configure Time Range: ACL の適用期間を設定します。
 - ・ Add: 期間の名前を指定します。
 - ・ Show: 設定されている期間の名前を表示します。
 - ・ Add Rule
 - Absolute: 特定の日時または期間を指定します。
 - Periodic: 定期的な間隔を指定します。
- ・ Show Rule: ルールによって指定されている日時または期間を表示します。

Configure ACL

- ・ Show TCAM: TCAM の使用状況パラメータを表示します。
- ・ Add - IP アドレスまたは MAC アドレスフィルタリングに基づいて ACL を追加します。
- ・ Show: 構成されている ACL の名前とタイプを表示します。
- ・ Add Rule: IP アドレスまたは MAC アドレスおよびその他のパケット属性に基づくパケットフィルタリングを構成します。
- ・ Show Rule: ACL に指定されているルールを表示します。

Configure Interface: 指定された ACL と期間にポートをバインドします。

ARP Inspection

Configure General: ARP インスペクションをグローバルで有効にし、その他のアドレス構成要素の検証を構成し、パケット検査のログメッセージの送信間隔を設定します。

Configure VLAN: 指定された VLAN の ARP インスペクションを有効にします。

Configure Interface: ポートの信頼モードを指定し、パケット検査のレートリミットを設定します。

Show Information

- ・ Show Statistics: ARP インスペクションプロセスに関する統計情報を表示します。
- ・ Show LogARP: インスペクションのログの一覧を表示します。
- ・ IP Filter
 - ・ Add: Web、SNMP、および Telnet による管理アクセスが許可されるクライアントの IP アドレスを設定します。
 - ・ Show: 管理アドレスが許可されるアドレスを表示します。
- ・ Port Security ポートごとのセキュリティ設定（ステータス、セキュリティ侵害への対応、アクセスが許可される MAC アドレスの最大数など）を構成します。
- ・ Port Authentication - IEEE 802.1X
 - ・ Configure Global: 認証および EAPOL パススルーを有効にします。
 - ・ Configure Interface: 個々のポートの認証パラメータを設定します。
 - ・ Show Statistics: 選択したポートのプロトコル統計情報を表示します。
- ・ IP Source Guard - IP ソースガードテーブルのスタティックエントリまたは DHCP スヌーピングテーブルのダイナミック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。
 - ・ Port Configuration : IP ソースガードを有効にし、ポートごとのフィルタリングタイプを選択します。
 - ・ Static Binding
 - Add: ソースガードバインディングテーブルにスタティックアドレスを追加します。
 - Show: ソースガードバインディングテーブルのスタティックアドレスを表示します。
- ・ Dynamic Binding: 選択したインター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。

Administration

- ・ Log
 - ・ System
 - Configure Global: エラーメッセージをローカルメモリに保存します。
 - Show System Logs: ログに記録されている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で記録するメッセージのログを構成します。
 - ・ SMTP: SMTP クライアントメッセージが該当のサーバに送信されるようにします。
- ・ LLDP (Link Layer Discovery Protocol)
 - Configure Global: グローバル LLDP タイミングパラメータを設定します。
- ・ Configure Interface

- Configure General: メッセージ送信モードを設定し、SNMP 通知を有効にし、アドレスを指定する LLDP 属性を設定します。
- Show Local Device Information
 - General: ローカルデバイスに関する全般情報を表示します。
 - Port/Trunk: 各インターフェースに関する情報を表示します。
- Show Remote Device Information
 - Port/Trunk: 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: 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: スイッチに接続されているすべてのリモートデバイスに関する統計情報を表示します。
 - Port/Trunk: 選択したポートまたはトランクのリモートデバイスに関する統計情報を表示します。
- SNMP (Simple Network Management Protocol)
 - Configure Global: SNMP エージェントステータスを有効にし、関連するトラップメッセージを指定します。
 - Configure Engine
 - Set Engine: ID スイッチの SNMPv3 エンジン ID を設定します。
 - Add Remote Engine: リモートデバイスの SNMPv3 エンジン ID を設定します。
 - Show Remote Engine: リモートデバイスに設定されているエンジン ID を表示します。
 - Configure View
 - Add: View: OID MIB の SNMPv3 ビューを追加します。
 - Show View: 構成されている SNMPv3 ビューを表示します。
 - Add OID Subtree: 選択したビューのサブツリーの一部を追加します。
 - Show OID Subtree: それぞれのビューに割り当てられているサブツリーを表示します。
 - Configure Group
 - Add: グループに割り当てられているユーザのアクセスポリシーを追加します。
 - Show: 構成されているグループとアクセスポリシーを表示します。
 - Configure User
 - Add Community: コミュニティストリングスとアクセスモードを設定します。
 - Show Community: コミュニティストリングスとアクセスモードを表示します。
 - Add SNMPv3 Local User: スイッチの SNMPv3 ユーザを構成します。
 - Show SNMPv3 Local User: スイッチで構成されている SNMPv3 ユーザを表示します。
 - Change SNMPv3 Local User Group: ローカルユーザを新規グループに割り当てます。
 - Add SNMPv3 Remote User: リモートデバイスからアクセスする SNMPv3 ユーザを指定します。

Web 設定

Web インターフェースの使用

- Show SNMPv3 Remote User: リモートデバイスからアクセスする SNMPv3 ユーザとして指定されているユーザを表示します。

Configure Trap

- Add: スイッチで発生する重要なイベントに関するメッセージを受信するトラップマネージャを構成します。
- Show: 構成されているトラップマネージャを表示します。

RMON (Remote Monitoring)

- ・ Configure Global

- ・ Add

- Alarm: 監視対象の変数のしきい値を設定します。
 - Event: アラームに対する応答イベントを作成します。

- ・ Show

- Alarm 構成されているすべてのアラームを表示します。
 - Event 構成されているすべてのイベントを表示します。

- ・ Configure Interface

- ・ Add

- History: 物理インターフェースに関する統計情報を定期的にサンプリングします。
 - Statistics: 物理インターフェースに関する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リングデータを表示します。
 - Statistics 統計グループの各エントリのサンプリングデータを表示します。

IP

General

- ・ Routing Interface

Add: VLAN の IP インターフェースを構成します。

Show: VLAN に割り当てられているインターフェースを表示します。

- ・ Ping: ICMP エコー要求パケットをネットワーク上の他のノードに送信します。
- ・ Trace Route: 指定された宛先へのルートパケットを表示します。

ARP (Address Resolution Protocol)

- ・ Configure General: プロトコルのタイムアウトを設定し、指定された VLAN の Proxy ARP を有効または無効にします。

- ・ Configure Static Address

Add 物理アドレスを IP アドレスに静的にマップします。

Show MAC アドレスと IP アドレスのスタティックマッピングテーブルを表示します。

- ・ Show Information

- ・ Dynamic Address: 動的に学習された IP ルーティングテーブルのエントリを表示します。
- ・ Other Address: スイッチで使用されている内部アドレスを表示します。
- ・ Statistics: 送信および受信された ARP 要求に関する統計情報を表示します。

Routing

- ・ Static Routes
 - ・ Add: スタティックルーティングエントリを構成します。
 - ・ Show: スタティックルーティングエントリを表示します。
 - ・ Modify: 選択したスタティックルーティングエントリを変更します。
- ・ Routing Table
 - ・ Show Information: ローカルルート、スタティックルート、およびダイナミックルートを含む、すべてのルーティングエントリを表示します。
 - ・ Configure ECMP Number: ルーティングテーブルにインポートできる、同じ宛先に対するイコールコストパスの最大数を設定します。
- ・ VRRP (Virtual Router Redundancy Protocol)
 - ・ Configure Group ID
 - Add: VRRP グループ ID を VLAN に追加します。
 - Show: VRRP グループ ID リストを表示します。
 - Add IP Address: VRRP グループの仮想 IP アドレスを設定します。
 - Show IP Addresses: VRRP グループに割り当てられている仮想 IP アドレスを表示します。
 - Configure Detail: アドバタイズメント間隔、プリエンプト機能、認証などの詳細設定を構成します。
 - ・ Show Statistics
 - Global Statistics: VRRP プロトコルパケットエラーに関するグローバル統計情報を表示します。
 - Group Statistics: 指定された VRRP グループおよびインターフェースの VRRP プロトコルイベントとエラーに関する統計情報を表示します。

IPv6 Configuration

- ・ Configure Global: 既知のネクストホップがないトラフィックの IPv6 デフォルトゲートウェイを設定します。
- ・ Configure Interface: 自動構成またはリンクローカルアドレスを使用して IPv6 インターフェースアドレスを設定し、関連するプロトコル設定を指定します。
- ・ 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 アドレスをインターフェースに追加します。
- ・ Show IPv6 Address: インターフェースに割り当てられている IPv6 アドレスを表示します。
- ・ Show IPv6 Neighbor CacheIPv6: 近傍検出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: IPv6 メッセージに関する統計情報を表示します。

Web 設定

Web インターフェースの使用

UDP: UDP メッセージに関する統計情報を表示します。

- ・ Show MTUICMP パケットサイズ超過メッセージをスイッチで受信可能な最大転送単位 (MTU) と共に返した宛先の MTU キャッシュを表示します。

IP Service

- DNS (Domain Name Service)

- General

- Configure Global: DNS を有効にし、完全なホスト名に付加されるデフォルトのドメイン名を定義します。
 - Add Domain Name: 完全なホスト名に付加できるドメイン名のリストを定義します。
 - Show Domain Names: 構成されているドメイン名リストを表示します。
 - Add Name Server: ダイナミック検索で使用するネームサーバの 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リストを表示します。

- Static Host Table

- Add: ドメイン名をアドレスにマップするために使用されるスタティックエントリを構成します。
 - Show: スタティック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ているスタティックアドレスを変更します。
- Cache 指定されたネームサーバによって検出されたキャッシュエントリを表示します。

- DHCP (Dynamic Host Configuration Protocol)

- Client インターフェースの DHCP クライアント ID を指定します。

- RelayDHCP リレーサーバを指定します。

- Snooping

- Configure Global: DHCP スヌーピング、MAC アドレスの検証、および情報オプションをグローバルで有効にし、情報ポリシーを設定します。
 - Configure VLAN: VLAN の DHCP スヌーピングを有効にします。
 - Configure Interface: インターフェースの信頼モードを設定します。
 - Show Information: DHCP スヌーピングのバインディング情報を表示します。

- Server

- Configure Global: スイッチの DHCP サービスを有効にします。
 - Configure Excluded Address
 - Add: 除外アドレスを追加します。
 - Show: 除外アドレスを表示します。

- Configure Pool

- Add
 - Network ネットワークグループのアドレスプールを追加します。
 - Host: 指定されたホストのアドレスエントリを追加します。
 - Show: DHCP プールリストを表示します。
 - Modify: 指定されたプールエントリを変更します。

- Show IP Binding: 現在 DHCP クライアントにバインドされているアドレスを表示します。

Web 設定

Web インターフェースの使用

- ・ UDP Helper
 - ・ General: スイッチで UDP ヘルパーをグローバルで有効にします。
 - ・ Forwarding
 - Add: ブロードキャストトラフィックの転送先となる UDP 宛先ポートを指定します。
 - Show: ブロードキャストトラフィックの転送先となる UDP 宛先ポートを一覧表示します。
 - ・ Address
 - Add: 指定された UDP プロトコルパケットの転送先となるサーバを指定します。
 - Show: 指定された UDP プロトコルパケットの転送先となるサーバを表示します。

Multicast

- ・ IGMP Snooping
 - ・ General: マルチキャストフィルタリングを有効にし、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。
- ・ 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るポートを割り当てます。
 - ・ Show Static Multicast Router: 隣接するマルチキャストルータに接続されるものとして静的に構成されているポートを表示します。
 - ・ Show Current Multicast Router: スタティック構成とダイナミック構成のいずれかによって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り当てます。
 - ・ Show Static Member: 選択した VLAN で静的に構成されているマルチキャストアドレスを表示します。
 - ・ Show Current Member: 選択した VLAN にスタティック構成とダイナミック構成のいずれかによって関連付けられているマルチキャストアドレスを表示します。
- ・ Interface
 - ・ Configure VLAN: VLAN インターフェースごとの IGMP スヌーピングを構成します。
 - ・ Show VLAN Information: VLAN インターフェースごとの IGMP スヌーピング設定を表示します。
 - ・ Configure Port : ポート毎に IGMP クエリ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のドロップ設定が出来ます。
 - ・ Configure Trunk : トランクグループ毎に IGMP クエリ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のドロップ設定が出来ます。
 - ・ Forwarding Entry: IGMP スヌーピングを使用して学習された現行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 フィルタリングプロファイルを追加し、アクセスモードを設定します。
 - Show: 構成されている IGMP フィルタリング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り当てます。
- Show Multicast Group Range: プロファイルに割り当てられているマルチキャストグループを表示します。
- Configure Interface: IGMP フィルタリングプロファイルをポートインターフェースに割り当て、スロットリングアクションを設定します。
- IGMP (Internet Group Management Protocol)
 - Proxy: マルチキャストルーティングの IGMP プロキシサービスを構成します。
 - Interface: 選択した VLAN インターフェースのレイヤ 3 の IGMP 設定を構成します。
 - Static Group
 - Add: 指定した VLAN インターフェースでマルチキャストグループのスタティックメンバーとなるルータを指定します。
 - Show: VLAN インターフェースに静的に割り当てられているマルチキャストグループを表示します。

Group Information

- Show Information: 各 VLAN について IGMP スヌーピングを使用して学習された現行のマルチキャストグループを表示します。
- Show Detail: VLAN インターフェースに関連付けられている各マルチキャストグループに関する詳細情報を表示します。
- Multicast Routing
 - General: マルチキャストルーティングをグローバルで有効にします。
 - Information
 - Show Summary: スイッチが学習したそれぞれのマルチキャストルートを表示します。
 - Show Detail: スイッチが学習したそれぞれのマルチキャストルートに関する追加情報（アップストリームルータやダウンストリームインターフェースなど）を表示します。
- MVR (Multicast VLAN Registration)
 - Configure General: MVR をグローバルで有効にし、MVR VLAN を設定します。
 - Configure Group Range
 - Add: マルチキャストストリームアドレスを指定します。
 - Show: マルチキャストストリームアドレスを表示します。
 - Configure Interface: MVR インターフェースタイプと即時脱退ステータスを設定します。
 - Configure Static Group Member
 - Add: MVR マルチキャストストリームをインターフェースに静的に割り当てます。
 - Show: インターフェースに静的に割り当てられている MVR マルチキャストストリームを表示します。
 - Show Member: MVR VLAN に割り当てられているマルチキャストグループに関連付けられているインターフェースに関する情報を表示します。

Routing Protocol

RIP (Routing Information Protocol)

- ・ General
 - ・ Configure: RIP を有効または無効にし、グローバル RIP 属性とタイマー値を設定します。
 - ・ Clear Route: 指定したルートタイプまたはネットワークインターフェースをルーティングテーブルからクリアします。
- ・ Network
 - ・ Add: RIP を使用するネットワークインターフェースを設定します。
 - ・ Show: RIP を使用するネットワークインターフェースを表示します。
- ・ Passive Interface
 - ・ Add: 指定したネットワークインターフェースで RIP ブロードキャストメッセージと RIP マルチキャストメッセージが送信されないようにします。
 - ・ Show: 構成されているパッシブインターフェースを表示します。
- ・ Neighbor Address
 - ・ Add: ルーティング情報をスタティックネイバルータと直接交換するようにルータを構成します。
 - ・ Show: ネイバルータとして構成されている隣接ホストまたはインターフェースを表示します。
- ・ Redistribute
 - ・ Add 外部ルーティング情報を他のルーティングドメイン（つまり、プロトコル）から自律システムにインポートします。
 - ・ Show 他のルーティングドメインからインポートされる外部ルーティング情報を表示します。
- ・ Distance
 - ・ Add: 他のルーティングプロトコルから学習する外部ルートの管理距離を定義します。
 - ・ Show: 他のルーティングプロトコルから学習する外部ルートに割り当てられる管理距離を表示します。
- ・ Interface
 - ・ Add: 各インターフェースの RIP パラメータ（送信バージョンと受信バージョン、認証設定、およびループバック防止策など）を設定します。
 - ・ Show: 各インターフェースに設定されている RIP パラメータを表示します。
 - ・ Modify: インターフェースの RIP パラメータを変更します。

- ・ Statistics
 - ・ Show Interface Information RIP 設定および RIP プロトコルメッセージ統計情報を表示します。
 - ・ Show Peer Information 隣接 RIP ルータに関する情報を表示します。
 - ・ Reset Statistics RIP プロトコルメッセージに関する統計情報をクリアします。

OSPF (Open Shortest Path First)(Version 2)

- ・ Network Area
 - ・ Add: OSPF エリアアドレス、エリア ID、およびプロセス ID を定義します。
 - ・ Show: 構成されているエリアを表示します。
 - ・ Show: Process 構成されているプロセスを表示します。
- ・ System
 - ・ Configure: ルータ ID、グローバル設定、およびデフォルト情報を指定します。
 - ・ Show: LSA 統計情報、管理ステータス、ABR/ASBR、エリアに接続しているルータの数、およびバージョン番号を表示します。
- ・ Area
 - ・ Configure Area
 - ・ Add Area: NSSA またはスタブを追加します。
 - ・ Show Area: 構成されている NSSA またはスタブを表示します。
 - ・ Configure NSSA Area: NSSA に対してインポートまたはインポートするルートに関する設定を指定します。
 - ・ Configure Stub Area: デフォルトのコストを設定し、ルートをスタブにインポートするための設定を指定します。
 - ・ Show Information: 各エリアに関する統計情報（SPF の実行、ABR/ASBR の数、LSA の数、LSA チェックサムなど）を表示します。

Area Range

- ・ Add: エリア境界でアドバタイズされるルートサマリを構成します。
- ・ Show: エリア境界でアドバタイズされるルートサマリを表示します。
- ・ Modify: エリア境界でアドバタイズされるルートサマリを変更します。

Redistribute

- ・ Add: あるルーティングドメインから別のルーティングドメインにルート情報を再配信します。
- ・ Show: 他のドメインに再配信されるルートのタイプを表示します。
- ・ Modify: 再配信されるルートの構成情報を変更します。

Summary Address

- ・ Add: 他の自律システムにアドバタイズするため、他のプロトコルから学習したルート情報を集約します。
- ・ Show: 設定されているサマリアドレスを表示します。

Web 設定

Web インターフェースの使用

Interface

- ・ Show エリア ID、および各インターフェースに指定されているルータ設定を表示します。
- ・ Configure by VLAN: 指定した VLAN の OSPF プロトコル設定と認証設定を指定します。
- ・ Configure by Address: 指定したインターフェースアドレスの OSPF プロトコル設定と認証設定を指定します。
- ・ Show MD5 Key: 各エリアで使用されている MD5 キー ID を表示します。

Virtual Link

- ・ Add: 通過エリアを経由してバックボーンに接続する仮想リンクを構成します。
- ・ Show: 仮想リンクおよびネイバールータのアドレスと状態を表示します。
- ・ Configure Detailed Settings: プロトコルと認証に関する詳細設定を指定します。
- ・ Show MD5 Key: 各ネイバールータで使用されている MD5 キー ID を表示します。

Information

- ・ LSDB: 各種の OSPF リンクステートアドバタイズメント (LSA: Link State Advertisements) に関する情報を表示します。
- ・ Neighbor: 各 OSPF ネイバールータに関する情報を表示します。

PIM (Protocol Independent Multicasting)

- ・ General: スイッチで PIM をグローバルで有効にします。
- ・ Interface: インターフェースごとに PIM を有効にし、モードを「Dense」または「Sparse」に設定します。
- ・ Neighbor: PIM ネイバールータに関する情報を表示します。
- ・ PIM-SM (Protocol Independent Multicasting – Sparse Mode)
 - ・ Configure Global: 登録メッセージの設定、および SPT を使用するかどうかを指定します。
 - ・ BSR Candidate: スイッチを BSR 候補として構成します。
 - ・ RP Address
 - Add: RP のスタティックアドレスと関連付けられているマルチキャストグループを指定します。
 - Show: 各 RP に設定されているスタティックアドレスと関連付けられているマルチキャストグループを表示します。
- ・ RP Candidate
 - ・ Add: 指定したマルチキャストグループの RP 候補としてスイッチを BSR にアドバタイズします。
 - ・ Show: スイッチが自らを RP 候補として BSR にアドバタイズするマルチキャストグループを表示します。
 - ・ Show Information-
 - Show BSR Router: BSR に関する情報を表示します。

- Show RP Mapping: アクティブな RP と関連付けられているマルチキャストルーティングエントリを表示します。

Web 設定

Web インターフェースの使用

- ・ PIM6 (PIM for IPv6)
 - ・ General: スイッチで PIM をグローバルで有効にします。
 - ・ Interface: インターフェースごとに PIM を有効にし、モードを「Dense」または「Sparse」に設定します。
 - ・ Neighbor: PIM ネイバールータに関する情報を表示します。

1.2 基本的な管理作業

本章では、以下のトピックについて説明します。

システム情報の表示 - 連絡先情報を始めとするシステムに関する基本的な説明を表示します。

- ・ スイッチのハードウェアとソフトウェアのバージョンの表示 - ハードウェアバージョン、電源ステータス、およびファームウェアバージョンを表示します。
- ・ ジャンボフレームのサポートの設定 - ジャンボフレームのサポートを有効にします。
- ・ ブリッジ拡張機能の表示 - ブリッジ拡張機能を表示します。
- ・ システムファイルの管理 - オペレーティングソフトウェアや設定ファイルをアップグレードする方法、およびシステムの起動ファイルを設定する方法について説明します。
- ・ システムクロックの設定 - 現在の時刻を手動で、あるいは、指定した NTP サーバまたは SNTP サーバを使用して設定します。
- ・ コンソールポートの設定 - コンソールポートの接続パラメータを設定します。
- ・ Telnet 設定 - Telnet 接続パラメータを設定します。
- ・ CPU 使用率の表示 - CPU 使用率に関する情報を表示します。
- ・ メモリ使用量の表示 - メモリ使用量パラメータを表示します。
- ・ スタック番号の再割り当て - スタック内のユニットの番号を再割り当てします。

1.2.1 システム情報の表示

「System」→「General」を選択すると、デバイス名、設置場所、連絡先などの情報を表示してシステムを特定することができます。

関連する CLI 情報

「System Management Commands」

「SNMP Commands」

パラメータ

以下のパラメータが表示されます。

- ・ System Description - デバイスの種類の簡単な説明。
- ・ 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。
- ・ System Up Time - 管理エージェントの稼働状態が維持されている時間の長さ。
- ・ System Name - スイッチシステムに割り当てられている名前。
- ・ System Location - システムの設置場所。
- ・ System Contact - システムの担当管理者。

Web インターフェース

システム名、連絡先、システムの配置場所の情報を設定するには、以下のようになります。

- (1) 「System」 → 「General」 を選択します。
- (2) システムの名前と設置場所およびシステム管理者の連絡先情報を指定します。
- (3) < Apply > ボタンをクリックします。

The screenshot displays the 'System > General' configuration page. It features a table-like layout with labels on the left and values or input fields on the right. The 'System Name', 'System Location', and 'System Contact' fields are currently empty text boxes. At the bottom right, there are two buttons: 'Apply' and 'Revert'.

System > General	
System Description	FXC9324XG
System Object ID	1.3.6.1.4.1.25574.20.90
System Up Time	0 days, 0 hours, 59 minutes, and 53.23 seconds
System Name	
System Location	
System Contact	

Apply Revert

画面 1-6 : システム情報

1.2.2 スイッチのハードウェアとソフトウェアのバージョンの表示

「System」 → 「Switch」 を選択すると、メインボードと管理ソフトウェアのハードウェアまたはファームウェアのバージョン番号に加え、システムの電源ステータスが表示されます。

関連する CLI 情報

P254 「システム管理」)

パラメータ

以下のパラメータが表示されます。

メインボードに関する情報

- ・ Serial Number – スイッチのシリアル番号。
- ・ Number of Ports – 内蔵ポートの数。
- ・ Hardware Version – メインボードのハードウェアバージョン。
- ・ Internal Power Status – 内部電源のステータス。

管理ソフトウェアに関する情報

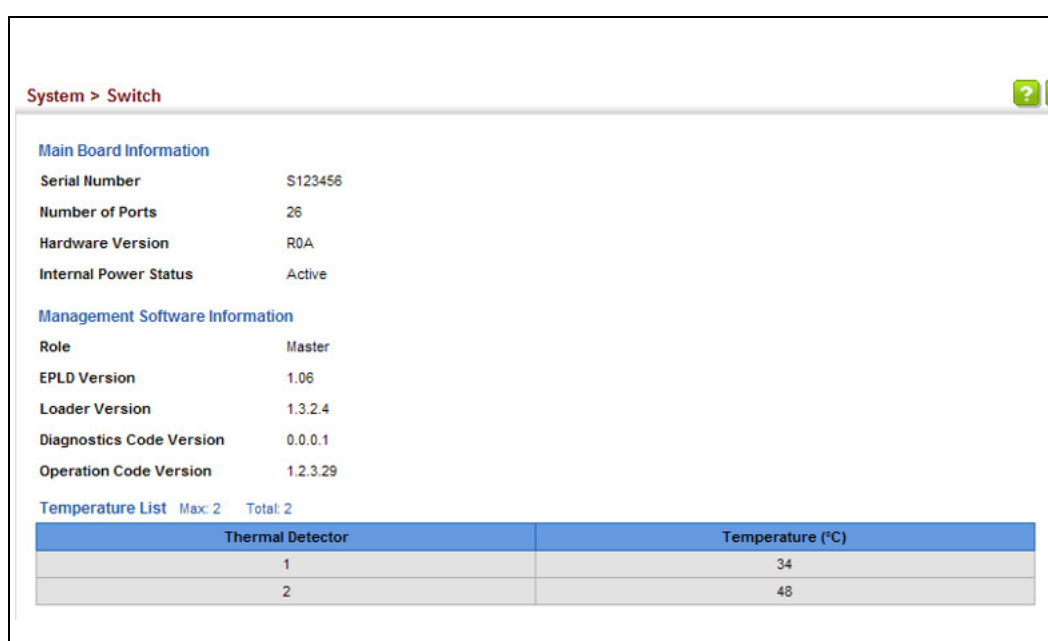
- ・ Role – このスイッチがマスターとスレーブのどちらであるか。
- ・ EPLD Version – EEPROM 書き込み可能デバイスのバージョン番号。
- ・ Loader Version – ロードコードのバージョン番号。

- ・ Diagnostics Code Version – 電源投入時の自己診断テスト（POST: Power-On Self-Test）とブートコードのバージョン。
- ・ Operation Code Version – ランタイムコードのバージョン番号。
- ・ Thermal Detector – 第一温度センサは、通風孔付近にあります。第二温度センサは、スイッチの ASIC 付近にあります。
- ・ Temperature – 所定の温度検出点における温度。

Web インターフェース

ハードウェアとソフトウェアのバージョン情報を表示するには、以下のようにします。

1. 「System」→「Switch」を選択します。



System > Switch

Main Board Information

Serial Number	S123456
Number of Ports	26
Hardware Version	R0A
Internal Power Status	Active

Management Software Information

Role	Master
EPLD Version	1.06
Loader Version	1.3.2.4
Diagnostics Code Version	0.0.0.1
Operation Code Version	1.2.3.29

Temperature List Max: 2 Total: 2

Thermal Detector	Temperature (°C)
1	34
2	48

画面 1-7：スイッチの全般情報

1.2.3 ジャンボフレームのサポートの設定

「System」→「Capability」を選択すると、レイヤ 2 ジャンボフレームのサポートを設定することができます。本製品では、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のポートまたはトランクで最大 9,216bytes のジャンボフレームをサポートすることにより、大容量の連続データ転送で優れたスループット効率を実現します。標準のイーサネットフレームのサイズは最大でも 1,500 bytes ですが、ジャンボフレームを使用すると、プロトコルカプセル化フィールドの処理に必要なパケットごとのオーバーヘッドが大幅に軽減されます。

関連する CLI 情報

「jumbo frame」

「switchport mtu」

使用時のガイドライン

ジャンボフレームを使用するには、送信元と送信先の両方のエンドノード（コンピュータやサーバなど）でジャンボフレーム機能をサポートしている必要があります。また、全二重接続の場合は、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で拡張フレームサイズを受け取ることができなければなりません。また、半二重接続の場合は、コリジョンドメイン内のすべてのデバイスでジャンボフレームをサポートしている必要があります。

このコマンドを使用すると、すべてのギガビットおよび 10 ギガビットのポートとトランクでジャンボフレームのサポートが有効になります。特定のインターフェースの MTU を設定するには、ジャンボフレームを有効にしてから、「Interface」→「Port」→「General」（Configure by Port List または Configure by Port Range）を選択して、必要な MTU サイズを指定します。

パラメータ

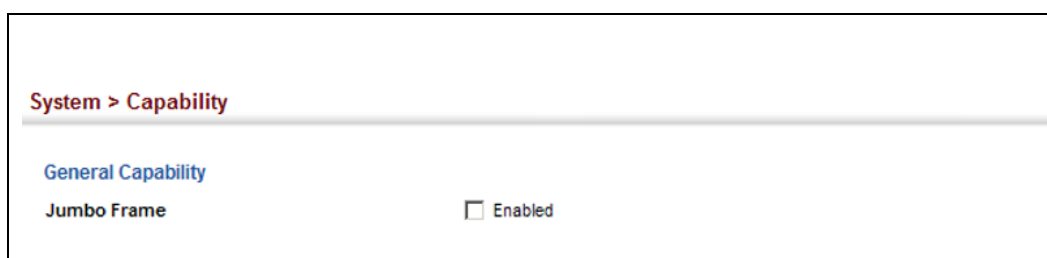
以下のパラメータが表示されます。

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 インターフェース

ジャンボフレームのサポートを設定するには、以下のようにします。

1. 「System」→「Capability」を選択します。
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 > ボタンをクリックします。



画面 1-8：ジャンボフレームのサポートの設定

1.2.4 ブリッジ拡張機能の表示

「System」→「Capability」を選択すると、ブリッジ MIB に基づく設定が表示されます。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、VLAN をサポートする管理対象デバイスのための拡張機能が組み込まれています。それらの拡張機能にアクセスして、主要な変数のデフォルト設定を表示することができます。

関連する CLI 情報

「GVRP and Bridge Extension Commands」

パラメータ

以下のパラメータが表示されます。

- ・ Extended Multicast Filtering Services – 本製品は、GMRP（GARP Multicast Registration Protocol）に基づく個別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 – 本製品は、ユーザの優先順位を複数のトラフィッククラスにマップする機能を備えています（「CoS（Class of Service）」を参照）。
- ・ Static Entry Individual Port – 本製品では、ユニキャストアドレスおよびマルチキャストアドレスにスタティックフィルタリングを使用することができます（「スタティックアドレスの設定」を参照）。
- ・ VLAN Version Number – IEEE 802.1Q に従い、「1」はシングルスパニングツリー（SST）動作のみをサポートするブリッジ、「2」はマルチスパニングツリー（MST）動作をサポートするブリッジを示します。
- ・ VLAN Learning – 本製品では、各ポートが独自のフィルタリングデータベースを保持する IVL（Independent VLAN Learning）方式を採用しています。
- ・ Local VLAN Capable – 本製品は、802.1Q で規定されている VLAN の適用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 – 本製品では、各ポートのデフォルトのポート VLAN ID（フレームタグで使用する PVID）とエグレスステータス（VLAN タグ付き、または、VLAN タグなし）を上書きすることができます（「VLAN 設定」を参照）。
- ・ Max Supported VLAN Numbers – スイッチでサポートする VLAN の最大数。
- ・ Max Supported VLAN ID – スイッチでサポートする設定可能な VLAN ID の最大数。
- ・ GMRP – GMRP（GARP Multicast Registration Protocol）を使用すると、ネットワークデバイスでエンドステーションをマルチキャストグループに登録できるようになります。本製品では、GMRP をサポートしていません。そのため、IGMP（Internet Group Management Protocol）を使用して自動マルチキャストフィルタリングを実現します。

Web 設定

基本的な管理作業

Web インターフェース

ブリッジ拡張機能に関する情報を表示するには、以下のようにします。

1. 「System」 → 「Capability」 を選択します。

The screenshot displays the 'System > Capability' configuration page. It features a breadcrumb trail at the top, followed by a section header 'General Capability'. Below this, there is a table of settings. The 'Jumbo Frame' setting is currently disabled, indicated by an unchecked checkbox. The 'Bridge Extension' section contains several other settings, most of which are enabled or set to default values. At the bottom right of the settings area, there are 'Apply' and 'Revert' buttons.

System > Capability	
General Capability	
Jumbo Frame	☐ Enabled
Bridge Extension	
Extended Multicast Filtering Services	No
Traffic Classes	Enabled
Static Entry Individual Port	Yes
VLAN Version Number	1
VLAN Learning	IVL
Local VLAN Capable	No
Configurable PVID Tagging	Yes
Max Supported VLAN Numbers	4093
Max Supported VLAN ID	4093
GMRP	Disabled

Apply Revert

画面 1-9 : ブリッジ拡張機能の設定の表示

1.2.5 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や設定ファイルをアップグレードする方法、およびシステムの起動ファイルを設定する方法について説明します。

FTP/TFTP または HTTP によるファイルのコピー

「System」→「File」(Copy) を選択して、FTP、TFTP、または HTTP を使用してファームウェアや設定情報をアップロードまたはダウンロードすることができます。ファイルを FTP サーバ、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り、後で、そのファイルをスイッチにダウンロードして動作を復元できるようになります。ファイルの転送方法を（必要な場合はファイルの種類と名前と共に）指定してください。

また、現在のバージョンを上書きすることなく新しいファームウェアまたは設定情報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異なる名前を付けてファイルをダウンロードし、その新規ファイルを起動ファイルとして設定するだけです。

関連する CLI 情報

「copy」

パラメータ

以下のパラメータが表示されます。

- ・ Copy Type - ファームウェアのコピー操作には以下のオプションがあります。
- ・ FTP Upgrade - FTP サーバからスイッチにファイルをコピーします。
- ・ FTP Download - スイッチから FTP サーバにファイルをコピーします。
- ・ HTTP Upgrade - 管理ステーションからスイッチにファイルをコピーします。
- ・ HTTP Download - スイッチから管理ステーションにファイルをコピーします。
- ・ TFTP Upgrade - TFTP サーバからスイッチにファイルをコピーします。
- ・ TFTP Download - スイッチから TFTP サーバにファイルをコピーします。
- ・ FTP/TFTP Server IP Address - FTP サーバまたは TFTP サーバの IP アドレス。
- ・ User Name - FTP サーバアクセスに使用するユーザ名。
- ・ Password - FTP サーバアクセスに使用するパスワード。
- ・ File Type - ファーム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ます。
- ・ File Name - ファイル名にはスラッシュ (¥ または /) を含めないでください。また、ファイル名はピリオド (.) で始まるものであってはならず、ファイル名の最大長はスイッチ上のファイルの場合は 31 文字、サーバ上のファイルの場合は 127 文字（有効な文字は、A～Z、a～z、0～9、ピリオド (.)、マイナス記号 (-)、下線 (_)）です。

[注意] システムソフトウェア（つまり、ランタイムファームウェア）のコピーは 2 つまでスイッチのファイルディレクトリに保存することができます。

[注意] ユーザ定義の設定ファイルの最大数の制限は、使用可能なフラッシュメモリ容量のみによるものです。

[注意] 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、スイッチでコピー先ファイル名として使用することはできません。

Web インターフェース

ファームウェアをコピーするには、以下のようになります。

- (1) 「System」 → 「File」 を選択します。
- (2) 「Step」 リストで「Copy」を選択します。
- (3) ファイル転送方法として、「FTP Upgrade」、「HTTP Upgrade」、または「TFTP Upgrade」を選択します。
- (4) 「FTP Upgrade」または「TFTP Upgrade」を使用する場合は、ファイルサーバの IP アドレスを入力します。
- (5) 「FTP Upgrade」を使用する場合は、FTP サーバのアカウントのユーザ名とパスワードを入力します。
- (6) ファイルの種類を「Operation Code」に設定します。
- (7) ダウンロードするファイルの名前を入力します。
- (8) 上書きするスイッチ上のファイルを選択するか、新しいファイル名を指定します。
- (9) < Apply > ボタンをクリックします。

System > File

Action: Copy

Copy Type: TFTP Upgrade

TFTP Server IP Address: 192.168.0.4

File Type: Operation Code

Source File Name: FB-38_V1.1.0.16.bix

Destination File Name: ☐ FB-38_V1.1.0.15.bix ☒ FB-38_V1.1.0.16.bix

Apply Revert

画面 1-10 : ファームウェアのコピー

現在、起動ファイルとして使用しているファイルを置き換え、新しいファイルを使用して起動する場合は、「System」 → 「Reset」を選択してシステムを Reboot します。

ローカルファイルへの設定情報ファイルの保存

「System」→「File」（Copy）を選択して、現在の設定情報をスイッチのローカルファイルに保存することができます。設定情報は、後でスイッチを Reboot したときに使用可能になるように自動保存されません。設定情報は現在の起動ファイルに保存するか、後で起動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。

関連する CLI 情報

「copy」

パラメータ

以下のパラメータが表示されます。

Copy Type - コピー操作には以下のオプションがあります。

Running-Config - 現在の設定情報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起動ファイルまたは新規ファイルにコピーします。ファイル名にはスラッシュ（\または/）を含めないでください。また、ファイル名はピリオド（.）で始まるものであってはならず、スイッチにおけるファイル名の最大長は 31 文字（有効な文字は、A～Z、a～z、0～9、ピリオド（.）、マイナス記号（-）、下線（_））です。

【注意】 ユーザ定義の設定ファイルの最大数の制限は、使用可能なフラッシュメモリ容量のみによるものです。

Web インターフェース

設定情報ファイルを保存するには、以下のようになります。

- (1) 「System」→「File」を選択します。
- (2) 「Step」リストで「Copy」を選択します。
- (3) 「Copy Type」リストで「Running-Config」を選択します。
- (4) 上書きするスイッチ上の現在の起動ファイルを選択するか、新しいファイル名を指定します。
- (5) < Apply > ボタンをクリックします。

System > File

Action: Copy

Copy Type: Running-Config

Destination File Name: ☒ startup1.cfg ☐

Apply Revert

画面 1-11：設定情報の保存

現在、起動ファイルとして使用しているファイルを置き換え、新しいファイルを使用して起動する場合は、「System」→「Reset」を選択してシステムを Reboot します。

起動ファイルの設定

「System」→「File」(Set Start-Up)を選択して、システムの初期設定に使用するファームウェアまたは設定ファイルを指定することができます。

関連する CLI 情報

「whichboot」

「boot system」

Web インターフェース

システムの初期設定に使用するファイルを設定するには、以下のようになります。

- (1) 「System」→「File」を選択します。
- (2) 「Step」リストで「Set Start-Up」を選択します。
- (3) 起動時に使用するオペレーションコードまたは設定ファイルを選択します。
- (4) < Apply > ボタンをクリックします。

The screenshot shows the 'System > File' configuration page. At the top, there is a breadcrumb 'System > File'. Below it, the 'Action:' dropdown is set to 'Set Start-Up'. A section titled 'File List' indicates 'Max: 18' and 'Total: 3'. It contains a table with the following data:

	File Name	File Type	Start-Up	Size (bytes)
☒	FB-38_V1.1.0.15.bix	Operation Code	Y	14390812
☐	Factory_Default_Config.cfg	Config File	N	455
☒	startup1.cfg	Config File	Y	4718

At the bottom of the table, there are two buttons: 'Apply' and 'Revert'.

画面 1-12 : 起動ファイルの設定

新しいファームウェアまたは設定情報を使用して起動するには、「System」→「Reset」を選択してシステムを Reboot します。

システムファイルの表示

「System」→「File」(Show) を選択して、システムディレクトリ内のファイルを表示または削除することができます。

[注意] 起動ファイルに指定されているファイルおよび Factory_Default_Config.cfg ファイルは削除できません。

関連する CLI 情報

「dir」

「delete」

Web インターフェース

システムファイルを表示するには、以下のようにします。

- (1) 「System」→「File」を選択します。
- (2) 「Step」リストで「Show」を選択します。
- (3) ファイルを削除するには、「File List」でファイルを選択してから < Delete > ボタンをクリックします。

System > File

Action: Show ▼

File List Max: 18 Total: 3

☐	File Name	File Type	Start-Up	Size (bytes)
☐	FB-38_V1.1.0.15.bix	Operation Code	Y	14390812
☐	Factory_Default_Config.cfg	Config File	N	455
☐	startup1.cfg	Config File	Y	4718

画面 1-13 : システムファイルの表示

1.2.6 システムクロックの設定

SNTP（Simple Network Time Protocol）を使用すると、スイッチの内部時刻がタイムサーバ（SNTP または NTP）からの定期的な更新情報に基づいて設定されるようにすることができます。

スイッチの時刻が常に正確になるようにすることで、イベントエントリの正確な日時がシステムログに記録されるようになります。また、時刻は手動で設定することもできます。時刻を手動または SNTP によって設定しない場合は、スイッチの前回の Bootup 時に設定された出荷時のデフォルト値しか記録されません。

SNTP クライアントを有効にすると、設定済みのタイムサーバに対してスイッチから定期的に時刻更新要求が送信されます。タイムサーバの IP アドレスは最大 3 つ設定することができます。スイッチは、設定された順序に従って各サーバにポーリングを試行します。

時刻の手動設定

「System」→「Time」（Configure General - Manual）を選択して、SNTP を使用せずに手動でスイッチのシステム時刻を設定することができます。

関連する CLI 情報

「calendar set」

「show calendar」

パラメータ

以下のパラメータが表示されます。

- ・ Current Time – スイッチで設定されている現在の時刻を表示します。
- ・ Hours – 何時かを設定します（範囲：0 ～ 23、デフォルト：0）。
- ・ Minutes – 何分かを設定します（範囲：0 ～ 59、デフォルト：0）。
- ・ Seconds – 何秒かを設定します（範囲：0 ～ 59、デフォルト：0）。
- ・ Month – 何月かを設定します（範囲：1 ～ 12、デフォルト：1）。
- ・ Day – 何日かを設定します（範囲：1 ～ 31、デフォルト：1）。
- ・ Year – 何年かを設定します（範囲：2001 ～ 2100、デフォルト：2009）。

Web インターフェース

システムクロックを手動で設定するには、以下のようにします。

- (1) 「System」→「Time」を選択します。
- (2) 「Step」リストで「Configure General」を選択します。
- (3) 「Maintain Type」リストで「Manual」を選択します。
- (4) 時間と日付を該当のフィールドに入力します。

(5) < Apply > ボタンをクリックします。

System > Time

Step: 1. Configure General

Current Time 2010-6-22 6:20:46

Maintain Type Manual

6 Hours 20 Minutes 46 Seconds

6 Month 22 Day 2010 Year

Apply Revert

画面 1-14 : システムクロックの手動設定

SNTP ポーリング間隔の設定

「System」→「Time」（Configure General - SNTP）を選択すると、スイッチからタイムサーバへのポーリングの間隔を設定することができます。

関連する CLI 情報

「Time」

パラメータ

以下のパラメータが表示されます。

- ・ Current Time – スイッチで設定されている現在の時刻を表示します。
- ・ SNTP Polling Interval – 時刻更新要求をタイムサーバに送信する間隔を設定します（範囲：16 ～ 16,384 秒、デフォルト：16 秒）。

Web インターフェース

SNTP のポーリング間隔を設定するには、以下のようになります。

- (1) 「System」→「Time」を選択します。
- (2) 「Step」リストで「Configure General」を選択します。
- (3) 「Maintain Type」リストで「SNTP」を選択します。
- (4) 必要な場合は、ポーリング間隔を変更します。

Web 設定

基本的な管理作業

(5) < Apply > ボタンをクリックします。

The screenshot shows a web interface for configuring the system time. At the top, it says 'System > Time'. Below that, there's a 'Step:' dropdown menu set to '1. Configure General'. The 'Current Time' is displayed as '2009-9-14 15:21:12'. The 'Maintain Type' is set to 'SNTP' via a dropdown menu. Under the 'SNTP Configuration' section, the 'SNTP Polling Interval (16-16384)' is set to '16' seconds. At the bottom right, there are 'Apply' and 'Revert' buttons.

画面 1-15 : SNTP のポーリング間隔の設定

SNTP タイムサーバの指定

「System」→「Time」（Configure Time Server）を選択して、SNTP タイムサーバ（最大 3 つ）の IP アドレスを指定することができます。「Step」リストで

関連する CLI 情報

「ntp server」

パラメータ

以下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 アドレスまたは IPv6 アドレスを設定します。スイッチは、時刻の更新を 1 番目のサーバから開始し、失敗すると次のサーバに移る … というように、順に試行します。

Web インターフェース

SNTP タイムサーバを設定するには、以下のようにします。

- (1) 「System」→「Time」を選択します。
- (2) 「Step」リストで「Configure Time Server」を選択します。
- (3) タイムサーバ（最大 3 つ）の IP アドレスを入力します。

(4) < Apply > ボタンをクリックします。

System > Time

Step: 2. Configure Time Server ▼

SNTP Server IP Address 1 10.1.0.19

SNTP Server IP Address 2 137.82.140.80

SNTP Server IP Address 3 128.250.36.2

Apply Revert

画面 1-16 : SNTP タイムサーバの指定

タイムゾーンの設定

「System」→「Time」(Configure Time Server)を選択すると、タイムゾーンを設定することができます。SNTP では、英国のグリニッジを通る地球の本初子午線（経度 0）を基準とする協定世界時が使用されます（協定世界時は、UTC と呼ばれるものであり、正式名称はグリニッジ標準時（GMT）。スイッチに使用場所の現地時刻が表示されるようにするには、タイムゾーンの時刻が UTC の西側（前）か東側（後）かを指定する必要があります。事前に定義されている 80 のタイムゾーンの 1 つを選択するか、または、使用場所のタイムゾーンのパラメータを手動で設定することができます。

関連する CLI 情報

「clock timezone」

パラメータ

以下のパラメータが表示されます。

- ・ Direction – タイムゾーンが UTC の前（西側）か後（東側）かを指定します。
- ・ Name – タイムゾーンに名前を割り当てます（範囲：1 ～ 29 文字）。
- ・ Hours (0-13) – UTC の前または後の時間数。UTC の前の最大値は 12 であり、UTC の後の最大値は 13 です。
- ・ Minutes (0-59) – UTC の前または後の分数。

Web インターフェース

現地時刻のタイムゾーンを設定するには、以下のようになります。

- (1) 「System」→「Time」を選択します。
- (2) 「Step」リストで「Configure Time Zone」を選択します。
- (3) UTC を基準にしてタイムゾーンの補正值（時間と分）を設定します。

(4) < Apply > ボタンをクリックします。

System > Time

Step: 3. Configure Time Zone

Direction: After UTC

Name: UTC

Hours (0-13): 0

Minutes (0-59): 0

Note: The maximum value before UTC is 12:00.
The maximum value after UTC is 13:00.

Apply Revert

画面 1-17 : タイムゾーンの設定

1.2.7 コンソールポートの設定

「System」→「Console」を選択すると、スイッチのコンソールポートの接続パラメータを設定することができます。VT100 対応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により、オンボードの設定プログラムにアクセスできるようになります。コンソールポートによる管理アクセスは、パスワード（CLI からのみ設定可能）、タイムアウト、基本通信設定など、各種のパラメータを使用して制御します。ただし、それらのパラメータを設定できるのは Web インターフェースまたは CLI インターフェースからであるということに注意してください。

関連する CLI 情報

「Line」

パラメータ

以下のパラメータが表示されます。

- ・ Login Timeout – CLI にユーザがログインするまでの待機時間を設定します。タイムアウトで指定されている時間内にログイン操作が実行されたことがシステムで検出されない場合、セッションの接続は強制終了されます（範囲：0 ～ 300 秒、デフォルト：0 秒）。
- ・ Exec Timeout – ユーザ入力検出されるまで待機する時間を設定します。タイムアウトで指定されている時間内にユーザが入力操作を実行したことがシステムで検出されない場合、現行セッションは強制終了されます（範囲：0 ～ 65,535 秒、デフォルト：60 秒）。
- ・ Password Threshold – パスワード侵害のしきい値を設定します。この値によってログイン操作の失敗回数を制限します。ログイン操作のしきい値に達すると、システムインターフェースは、（Silent Time パラメータで）指定された一定時間、応答なくなり、その時間が経過してからでないと、次にログイン操作を実行できるようになりません（範囲：0 ～ 120 回、デフォルト：3 回）。

- ・ Quiet Period – ログイン操作が指定回数を超えて失敗した後、管理コンソールにアクセスできなくなる時間を設定します（範囲：0～65,535 秒、デフォルト：Disabled）。
- ・ Data Bits – コンソールポートで解釈および生成される 1 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る場合は、1 文字あたり 7 データビットを指定してください。パリティ不要の場合は、1 文字あたり 8 データビットを指定してください（デフォルト：8 bits）。
- ・ Stop Bits – 伝送されるバイトあたりのストップビット数を設定します（範囲：1～2、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。一部の端末で提供される通信プロトコルでは特定のパリティビット設定が必要になることがあります。「Even（偶数）」、「Odd（奇数）」、「None（なし）」のいずれかを指定してください（デフォルト：None）。
- ・ Speed – 端末回線の（端末への）送信と（端末からの）受信のボーレートを設定します。シリアルポートに接続しているデバイスのボーレートに対応する速度を設定してください（範囲：9,600、19,200、38,400、57,600 または 115,200 bauds、デフォルト値：115,200 bauds）。

[注意] コンソール接続へのログインのパスワードチェックは、有効または無効にすることができます（「login」を参照）。パスワードコマンドに設定されている単一のグローバルパスワードによる認証、または個々のユーザ名アカウントに設定されているパスワードによる認証を選択することができます。デフォルトは、スイッチで設定されるローカルパスワードです。

Web インターフェース

コンソールポートのパラメータを設定するには、以下のようにします。

- (1) 「System」 → 「Console」を選択します。
- (2) 接続パラメータを必要に応じて指定します。
- (3) < Apply > ボタンをクリックします。

The screenshot shows the 'System > Console' configuration page. The settings are as follows:

Parameter	Value	Unit/Note
Login Timeout (0-300)	0	sec (0: Disabled)
Exec Timeout (0-65535)	0	sec (0: Disabled)
Password Threshold (0-120)	3	(0: Disabled)
Quiet Period (0-65535)	0	sec (0: Disabled)
Data Bits	8	
Stop Bits	1	
Parity Bit	None	
Speed	115200	baud

Buttons: Apply, Revert

画面 1-18 : コンソールポートの設定

1.2.8 Telnet 設定

「System」→「Telnet」を選択すると、Telnet 接続を使用して CLI にアクセスするためのパラメータを設定することができます。Telnet（つまり、仮想端末）を使用してネットワーク経由でオンボードの設定プログラム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有効または無効にすることができます。また、TCP ポート番号、タイムアウト、パスワードなど、その他のパラメータを設定することもできます（ただし、パスワードは CLI からのみ設定することができます）。それらのパラメータは Web インターフェースまたは CLI インターフェースを使用して設定することができます。

関連する CLI 情報

「Line」

パラメータ

以下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 – スイッチの Telnet 用の TCP ポートを設定します（範囲：1 ～ 65,535、デフォルト：23）。
- Max Sessions – 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 ～ 8）。
- Telnet および Secure Shell に対して最大 8 セッションを同時に開くことができます（Telnet と SSH の両方で最大 8 セッションを共有します）。
- Login Timeout – CLI にユーザがログインするまでの待機時間を設定します。タイムアウトで指定されている時間内にログイン操作が実行されたことがシステムで検出されない場合、セッションの接続は強制終了されます（範囲：0 ～ 300 秒、デフォルト：300 秒）。
- Exec Timeout – ユーザ入力が検出されるまで待機する時間を設定します。タイムアウトで指定されている時間内にユーザが入力操作を実行したことがシステムで検出されない場合、現行セッションは強制終了されます（範囲：0 ～ 65,535 秒、デフォルト：60 秒）。
- Password Threshold – パスワード侵害のしきい値を設定します。この値によってログイン操作の失敗回数を制限します。ログイン操作のしきい値に達すると、システムインターフェースは、（Silent Time パラメータで）指定された一定時間、応答なくなり、その時間が経過してからでないと、次にログイン操作を実行できるようになりません（範囲：0 ～ 120 回、デフォルト：3 回）。
- Quiet Period – ログイン操作が指定回数を超えて失敗した後、管理コンソールにアクセスできなくなる時間を設定します（範囲：0 ～ 65,535 秒、デフォルト：Disabled）。

[注意] Telnet接続のパスワードを設定できるのは、CLIからのみです（「password」を参照）。

[注意] コンソール接続へのログインのパスワードチェックは、有効または無効にすることができます（「login」を参照）。パスワードコマンドに設定されている単一のグローバルパスワードによる認証、または個々のユーザ名アカウントに設定されているパスワードによる認証を選択することができます。デフォルトは、スイッチで設定されるローカルパスワードです。

Web インターフェース

コンソールポートのパラメータを設定するには、以下のようにします。

- (1) 「System」 → 「Telnet」 を選択します。
- (2) 接続パラメータを必要に応じて指定します。
- (3) < Apply > ボタンをクリックします。

The screenshot shows the 'System > Telnet' configuration page. It contains several settings with input fields and checkboxes. The 'Telnet Status' is checked and set to 'Enabled'. The 'TCP Port (1-65535)' is set to '23'. The 'Max Session (0-8)' is set to '8'. The 'Login Timeout (1-300)' is set to '300'. The 'Exec Timeout (1-65535)' is set to '600'. The 'Password Threshold (0-120)' is set to '3' with a note '(0: Disabled)'. The 'Quiet Period (0-65535)' is set to '0' with a note 'sec (0: Disabled)'. At the bottom right, there are two buttons: 'Apply' and 'Revert'.

System > Telnet	
Telnet Status	☒ Enabled
TCP Port (1-65535)	23
Max Session (0-8)	8
Login Timeout (1-300)	300
Exec Timeout (1-65535)	600
Password Threshold (0-120)	3 (0: Disabled)
Quiet Period (0-65535)	0 sec (0: Disabled)

Apply Revert

画面 1-19 : Telnet 接続の設定

1.2.9 CPU 使用率の表示

「System」 → 「CPU Utilization」 を選択すると、CPU 使用率に関する情報が表示されます。

関連する CLI 情報

「show process cpu」

パラメータ

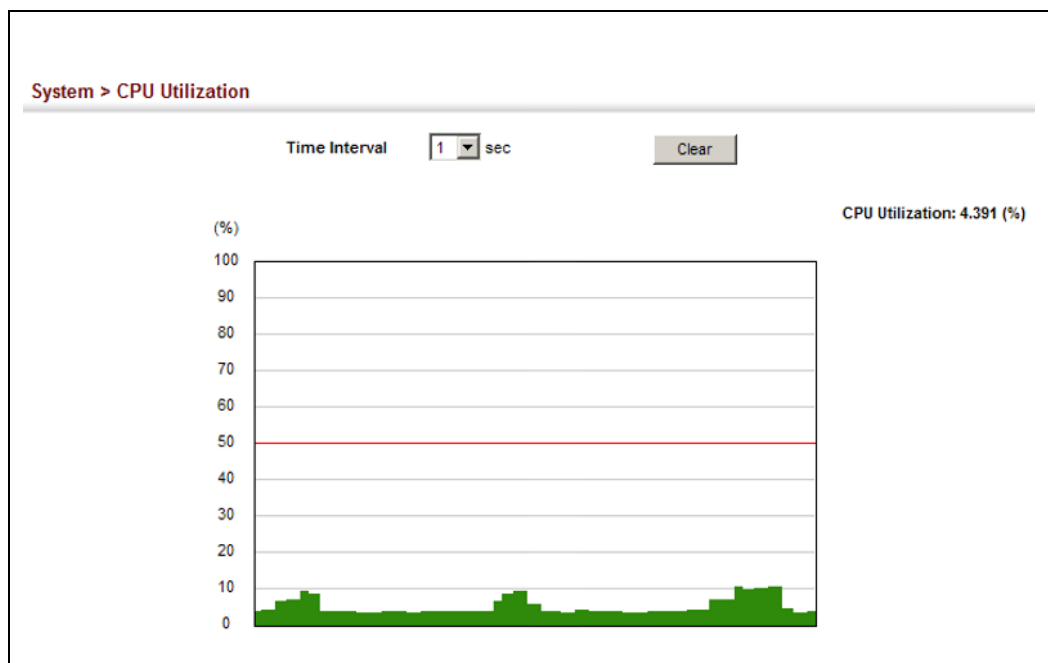
以下のパラメータが表示されます。

- ・ Time Interval
 - 表示されている使用率データの更新間隔（オプション：1、5、10、30、60 秒のいずれか、デフォルト：1 秒）。
- ・ CPU Utilization
 - 指定された間隔における CPU 使用率

Web インターフェース

CPU 使用率を表示するには、以下のようにします。

- (1) 「System」 → 「CPU Utilization」 を選択します。
- (2) 更新間隔を必要に応じて変更します。間隔は、新しい設定を選択すると即座に変更されるので注意してください。



画面 1-20 : CPU 使用率の表示

1.2.10 メモリ使用量の表示

「System」 → 「Memory Status」を選択すると、メモリ使用量パラメータが表示されます。

関連する CLI 情報

「show memory」

パラメータ

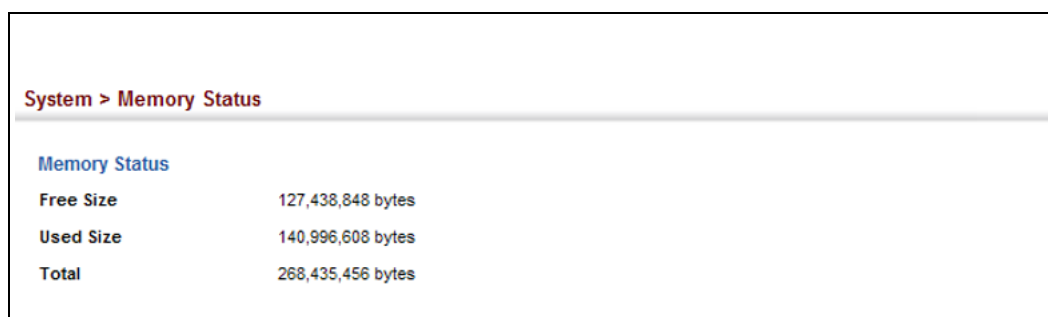
以下のパラメータが表示されます。

- ・ Free Size – 現在使用可能な空きメモリ容量。
- ・ Used Size – アクティブなプロセスに割り当てられているメモリ容量。
- ・ Total – システムメモリの合計容量。

Web インターフェース

メモリ使用量を表示するには、以下のようにします。

- (1) 「System」 → 「Memory Status」を選択します。



System > Memory Status	
Memory Status	
Free Size	127,438,848 bytes
Used Size	140,996,608 bytes
Total	268,435,456 bytes

画面 1-21：メモリ使用量の表示

1.2.11 スタック番号の再割り当て

トポロジが変更されたため、または障害が何回か発生したため、ユニットに連続する番号を割り当てられなくなった場合は、「System」→「Renumbering」を選択してユニット番号をリセットします。その際、スタックマスタの電源をオフにする前に新規設定情報を起動設定ファイルに保存するのを忘れないでください。

関連する CLI 情報

「switch all renumber」

コマンドの使用

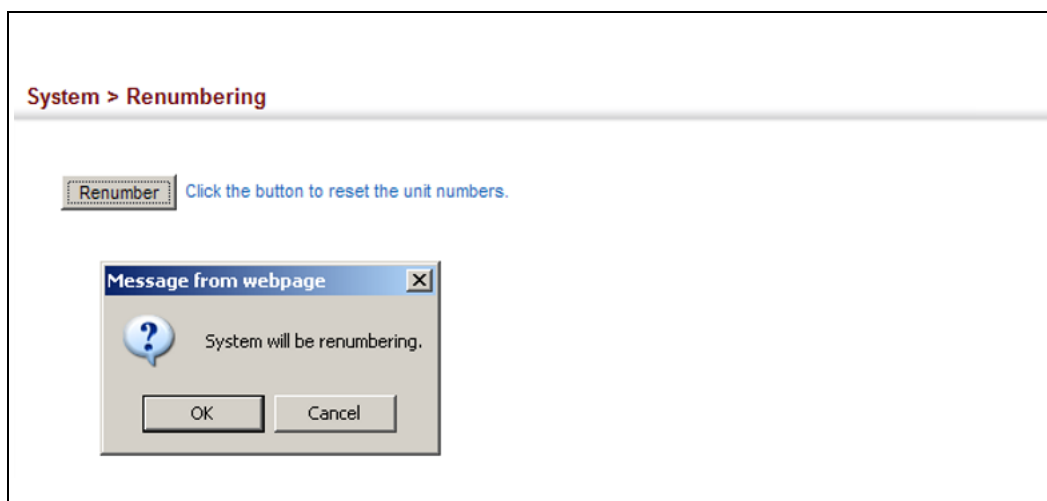
起動設定ファイルは、ユニット ID 番号に基づいて、スタック内の各スイッチに設定情報をマップします。そのため、スタックの番号を再割り当てした後は最新の設定を保存するのを忘れないようにしなければなりません。

回線トポロジの場合、スタックには上から順に番号が付けられます。つまり、スタックの最初のユニットがユニット 1 に指定されます。リングトポロジの場合、マスタユニットがスタックの最初のユニットであるとみなされてユニット 1 という番号が付けられ、その他のすべてのユニットにはリング全体で順に番号が割り当てられます。

Web インターフェース

スタック内のユニットの番号の再割り当てをするには、以下のようにします。

- (1) 「System」→「Renumber」を選択します。
- (2) 確認メッセージが表示されたら < OK > ボタンをクリックします。



画面 1-22 : スタック番号の再割り当て

1.2.12 システムのリセット

「System」→「Reset」を選択すると、スイッチの再起動のタイミングを任意に設定できます。

関連する CLI 情報

「reload (Privileged Exec)」

「reload (Global Configuration)」

「show reload」

コマンドの使用

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、常に電源投入時の自己診断テストが実行されます。

また、copy running-config startup-config コマンドを実行することにより、不揮発性メモリに保存されているすべての設定情報が保持されます（「copy」を参照）。

パラメータ

以下のパラメータが表示されます。

System Reload Information

Reload Settings

- 次回に実行される予定の再読み込みに関する情報、および選択されている再読み込みモードが、以下のように表示されます。

```
The switch will be rebooted at March 9 12:00:00 2012.  
Remaining Time: 0 days, 2 hours, 46 minutes, 5 seconds.  
Reloading switch regularly time: 12:00 everyday.
```

- ・ Refresh - 再読み込みされた情報の表示内容を更新します。コンソールからの変更またはシステム時刻に対する変更がある場合は、最新の設定が表示されるように、表示を更新する必要があります。
- ・ Cancel - 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。

System Reload Configuration

Reset Mode

- スイッチを即座に再起動するか、または、指定された時刻に再起動します。
- ・ Immediately - システムを即座に再起動します。
- ・ In - スイッチの設定が再読み込みされるまでの期間を指定します（再読み込みまでの期間を 24 日以下にする必要があります）。
 - ・ hours - スイッチがリセットされるまでの期間のうちの時間数を示すものとして、分数と組み合わせて指定します（範囲：0 ～ 576）。
 - ・ minutes - スイッチがリセットされるまでの期間のうちの分数を示すものとして、時間数と組み合わせて指定します（範囲：0 ～ 59）。

At - スイッチを再起動する日時を指定します。

- ・ DD - 再読み込みを実行する月の日付（範囲：1 ～ 31）。
- ・ MM - 再読み込みを実行する月（january ～ december）。
- ・ YYYY - 再読み込みを実行する年（範囲：2001 ～ 2050）。
- ・ HH - 再読み込みを実行する時刻の時数（範囲：0 ～ 23）。
- ・ MM - 再読み込みを実行する時刻の分数（範囲：0 ～ 59）。

Regularly - スイッチの設定を定期的に再読み込みする頻度と時刻を指定します。

Time

- ・ HH - 再読み込みを実行する時刻の時数（範囲：0 ～ 23）。
- ・ MM - 再読み込みを実行する時刻の分数（範囲：0 ～ 59）。

Period

- ・ Daily - 毎日。
- ・ Weekly - 再読み込みを実行する曜日（範囲：Sunday ～ Saturday）。
- ・ Monthly - 月に 1 回再読み込みを実行する日付（範囲：1 ～ 31）。

Web インターフェース

スイッチを再起動するには、以下のようになります。

- (1) 「System」 → 「Reset」 を選択します。
- (2) 必要なリセットモードを選択します。
- (3) 即時リセット以外のオプションを選択した場合は、必要なパラメータを指定します。
- (4) < Apply > ボタンをクリックします。

(5) 確認メッセージが表示されたら、スイッチをリセットすることを承認します。

The screenshot shows the 'System > Reset' page. Under 'System Reload Information', it says 'No configured settings for reloading.' with 'Refresh' and 'Cancel' buttons. Under 'System Reload Configuration', the 'Reset Mode' is set to 'Immediately' with a dropdown arrow, and there are 'Apply' and 'Revert' buttons. A modal dialog box titled 'Message from webpage' is displayed in the center, asking 'Do you want to reset the switch immediately?' with 'OK' and 'Cancel' buttons.

画面 1-23 : スイッチの再起動（「Immediately」の場合）

The screenshot shows the 'System > Reset' page. Under 'System Reload Information', it displays: 'The switch will be rebooted at Jan 1 02:54:25 2001. Remaining Time: 0 days, 1 hours, 10 minutes, 0 seconds.', 'Reloading switch in time: 5 hours 26 minutes.', and 'Reloading switch regularity time: 11:20 everyday.' with 'Refresh' and 'Cancel' buttons. Under 'System Reload Configuration', the 'Reset Mode' is set to 'In' with a dropdown arrow. Below it, 'Reload switch in' is set to '1' hours and '30' minutes. A note states: 'Note: The specified time must be equal to or less than 24 days.' There are 'Apply' and 'Revert' buttons at the bottom.

画面 1-24

System > Reset

System Reload Information:
The switch will be rebooted at Jan 1 02:54:25 2001. Remaining Time: 0 days, 1 hours, 10 minutes, 0 seconds.
Reloading switch in time: 5 hours 26 minutes.
Reloading switch regularity time: 11:20 everyday.

System Reload Configuration:
Reset Mode
Reload switch at (DD/MM/YYYY) (HH:MM)
Warning: You have to setup system time first. Otherwise this function won't work.

画面 1-25 : スイッチの再起動（「At」の場合）

System > Reset

System Reload Information:
No configured settings for reloading.

System Reload Configuration:
Reset Mode
Time (HH:MM)
Period
☒ Daily
☐ Weekly
☐ Monthly

Warning: You have to setup system time first. Otherwise this function won't work.

画面 1-26 : スイッチの再起動（「Regularly」の場合）

1.3 インターフェース設定

本章では、以下のトピックについて説明します。

- ・ General – オートネゴシエーション、速度の手動設定、デュプレクスモード、およびフロー制御などの接続設定を設定します。
- ・ Mirror – ローカルスイッチでのミラーリングのための送信元ポートとターゲットポートを設定します。
- ・ Statistics – インターフェース、Etherlike、RMON ポートに関する統計情報を一覧形式またはグラフ形式で表示します。
- ・ Cable Test – 指定したポートのケーブル診断を実行します。
- ・ Trunk – スタティックトランクまたはダイナミックトランクを設定します。
- ・ sFlow – トラフィックフローのサンプリングが定期的に行われるように設定します（プライベート VLAN）。
- ・ Traffic Segmentation – セグメント化されたポートグループに対するアップリンクおよびダウンリンクを設定します。
- ・ VLAN Trunking – 1 つまたは複数の中間スイッチを経由するトンネルを設定して、ある VLAN グループのトラフィックをそのトラフィックが属していない別の VLAN グループに渡すことができます。

1.3.1 ポート設定

ここでは、ポート接続を設定する方法、あるポートから別のポートにトラフィックをミラーリングする方法、およびケーブル診断を実行する方法について説明します。

ポートリストによる設定

「Interface」→「Port」→「General」（Configure by Port List）を選択すると、ポート毎に、インターフェースを有効または無効にすることや、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ーフェース機能を設定することができます。また、速度、デュプレクスモード、およびフロー制御を手動で修正することもできます。

関連する CLI 情報

「Interface Commands」

コマンドの使用

- ・ ギガビット RJ-45 インターフェースで「Speed/Duplex」モードおよび「Flow Control」オプションが使用されるように設定するには、事前にオートネゴシエーションを無効にしておく必要があります。
- ・ オートネゴシエーションを使用すると、リンクパートナーがアドバタイズする機能に基づいて、それらのパートナー間の最適設定がネゴシエーションされます。オートネゴシエーションの対象となる速度、デュプレクスモード、またはフロー制御を設定するには、必要な動作モードをインターフェースの機能リストで指定する必要があります。
- ・ 固定モードは 1000BASE-T 規格および 10GBASE-T 規格ではサポートされていません。オートネゴシエーションは、1000BASE-T または 10GBASE-T のポートあるいはトランクによる接続を確立する場合には常に使用しなければなりません。オートネゴシエー

ションを使用しない場合、他のタイプのスイッチに接続する際にリンクプロセスが正常に完了する保証はありません。

- ・「Speed/Duplex」モードは、ギガビット SFP ポートでは 1000full に固定され、10 ギガビットポートでは 10G full に固定されます。オートネゴシエーションを有効にした場合は、フロー制御や symmetric PAUSE フレームなどの属性のみがアドバタイズされます。

ジャンボフレームの設定方法

- ・「System」→「Capability」を選択して表示されるジャンボフレーム属性を使用して、すべてのギガビットポートおよび 10 ギガビットイーサネットポートでジャンボフレームを有効または無効にすることができます。それから、ポート設定ページで、個々のインターフェースに必要な MTU サイズを指定します。
- ・設定済みポートの MTU に対するパケットサイズの比較では、着信パケットのサイズのみが考慮されます。また、この比較は、イングレスポートがタグ付きポートであるか QinQ イングレスポートであるかということに影響されません。つまり、その他のすべてのサイズ（例えば、チップによって追加される 4 bytes のタグ付きフィールドなど）は、設定されている MTU に対するエグレスパケットのサイズの比率を計算するときには考慮されないということです。
- ・外部デバイスからスイッチへの ping 時には、イーサネットヘッダ用に追加される情報のため、パケットサイズがタグなしパケットの場合は少なくとも 42 bytes、タグ付きパケットの場合は 46 bytes 増加することがあります。調整されたフレームサイズが設定済みポートの MTU を超える場合、スイッチは ping メッセージに応答しません。
- ・他のトラフィックタイプについては、全体的なフレームサイズの計算方法は、追加ヘッダフィールド SA(6) + DA(6) + Type(2) + VLAN-Tag(4)（タグ付きパケットの場合。タグなしパケットの場合、4 bytes フィールドは追加されません）とペイロードを含め、基本的には同じです。全体的なフレームサイズは、すべて、フレームの最後の CRC を含め、設定済みポートの MTU よりも小さくなければなりません。
- ・QinQ についても、全体的なフレームサイズは、上記のように計算され、2 番目のタグの長さはフレームに追加されません。

パラメータ

以下のパラメータが表示されます。

Port - ポート ID。

Type

- ポートタイプを示します（1000BASE-T、1000BASE SFP、10GBASE-T、10GBASE XFP、または 10GBASE SFP+）。

Name

- インターフェースにラベルを付けることができます（範囲：1 ～ 64 文字）。

Admin

- 手動によるインターフェースの無効化を許可します。異常動作（例えば、過剰なコリジョンなど）が発生した場合にはインターフェースを無効にし、問題が解決したら再び有効にすることができます。また、セキュリティ上の理由からインターフェースを無効にする場合もあります。

Media Type

- コンビネーションポートに使用する強制または優先ポートタイプを設定します。
 - ・ Copper-Forced - 常に内蔵 RJ-45 ポートを使用します。

- ・ SFP-Forced – モジュールがインストールされていない場合でも、常に SFP ポートを使用します。
- ・ SFP-Preferred-Auto – 両方のコンビネーションタイプが機能しており、SFP ポートに有効なリンクがある場合、SFP ポートを使用します（これは、ポート 21 ~ 26 のデフォルトです）。

Autonegotiation (Port Capabilities) - オートネゴシエーションを有効または無効にすることができます。オートネゴシエーションを有効にする場合は、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を無効にする場合は、速度、モード、およびフロー制御の設定が強制的に適用されるようにすることができます。サポートされている機能は、以下のとおりです。

- ・ 10h – 10 Mbps 半二重動作をサポートします。
- ・ 10f – 10 Mbps 全二重動作をサポートします。
- ・ 100h – 100 Mbps 半二重動作をサポートします。
- ・ 100f – 100 Mbps 全二重動作をサポートします。
- ・ 1000f (ギガビットポートのみ) – 1000 Mbps 全二重動作をサポートします。
- ・ 10Gf (10 ギガビットポートのみ) – 10 Gbps 全二重動作をサポートします。
- ・ Sym – この項目は、pause フレームを送受信する場合に選択します。
- ・ FC – フロー制御を使用すると、スイッチに直接接続している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の「ブロック」によるフレーム損失が発生しないようにすることができます。フロー制御を有効にした場合、半二重動作にはバックプレッシャが使用され、全二重動作には IEEE 802.3-2005（正式名称は IEEE 802.3x）が使用されます。
- ・ デフォルトで、ギガビットポートおよび 10 ギガビットポートではオートネゴシエーションは有効であり、アドバタイズ機能は以下のように設定されます。
 - 1000BASE-T – 10h、10f、100h、100f、1000f
 - 1000Base-SX/LX/LH (SFP) – 1000f
 - 10GBASE-SR/LR/ER (XFP) – 10Gf
 - 10GBASE-SR/LR (SFP+) – 10Gf
 - 10GBASE-T – 10Gf
- ・ Speed/Duplex – ポート速度およびデュプレクスモードを手動で設定することができます（そのため、オートネゴシエーションは無効になります）。
- ・ Flow Control – フロー制御を自動と手動のどちらにするか選択することができます。
- ・ MTU Size – ギガビットまたは 10 ギガビットイーサネットのポートあるいはトランクを経由するレイヤ 2 パケットについて許可される最大転送単位（MTU: Maximum Transmission Unit）（範囲：1,500 ~ 9,216 bytes、デフォルト：1,518 bytes）。

Web インターフェース

ポートの接続パラメータを設定するには、以下のようになります。

- (1) 「Interface」 → 「Port」 → 「General」を選択します。
- (2) 「Step」 リストで「Configure by Port List」を選択します。
- (3) 必要なインターフェース設定を変更します。

Web 設定

インターフェース設定

(4) < Apply > ボタンをクリックします。

Interface > Port > General

Action: Configure by Port List

Port List Max: 26 Total: 26

Port	Type	Name	Admin	Media Type	Autonegotiation	Speed Duplex	Flow Control	MTU Size (1500-9216)
1	1000BASE-T		☒ Enabled	Copper-Forced	☒ Enabled 10h ☒ 100h ☐ 1000h ☐ 10Gh ☐ Sym 10f ☒ 100f ☒ 1000f ☐ 10Gf ☐ FC	100full	☒ Enabled	1518
2	1000BASE-T		☒ Enabled	Copper-Forced	☒ Enabled 10h ☒ 100h ☐ 1000h ☐ 10Gh ☐ Sym 10f ☒ 100f ☒ 1000f ☐ 10Gf ☐ FC	100full	☒ Enabled	1518
3	1000BASE-T		☒ Enabled	Copper-Forced	☒ Enabled 10h ☒ 100h ☐ 1000h ☐ 10Gh ☐ Sym 10f ☒ 100f ☒ 1000f ☐ 10Gf ☐ FC	100full	☒ Enabled	1518

画面 1-27 : ポートリストに基づく接続の設定

ポート範囲に基づく設定

「Interface」→「Port」→「General」（Configure by Port Range）を選択すると、ポート範囲を指定してインターフェースを有効または無効にすることや、オートネゴシエーションおよびアダプタイズするインターフェース機能を設定することができます。また、速度、デュプレクスモード、フロー制御、または MTU サイズを手動で修正することもできます。

コマンドの使用法に関する詳細およびパラメータの説明については、「ポートリストに基づく設定」を参照してください。

関連する CLI 情報

「Interface Commands」

Web インターフェース

ポートの接続パラメータを設定するには、以下のようにします。

- (1) 「Interface」→「Port」→「General」を選択します。
- (2) 「Step」リストで「Configure by Port Range」を選択します。
- (3) 設定の変更を適用するポート範囲を入力します。
- (4) 必要なインターフェース設定を変更します。

(5) < Apply > ボタンをクリックします。

画面 1-28 : ポート範囲に基づく接続の設定

接続ステータスの表示

「Interface」→「Port」→「General」(Show Information) を選択すると、リンク状態、速度モードとデュプレクスモード、フロー制御、オートネゴシエーションなど、現在の接続ステータスが表示されます。

関連する CLI 情報

「show interfaces status」

パラメータ

以下のパラメータが表示されます。

- ・ Port – ポート ID。
- ・ Type – ポートタイプを示します (1000BASE-T、1000BASE SFP、または 10G)。
- ・ Name – インターフェースラベル。
- ・ Admin – ポートが有効か無効かを示します。
- ・ Oper Status – リンクがアップリンクかダウンリンクを示します。
- ・ Media Type – 使用するメディアタイプ (オプション : Copper-Forced、SFP-Forced または SFP-Preferred-Auto、デフォルト : SFP-Preferred-Auto)。
- ・ 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 – 現行の速度とデュプレクスモードを示します。
- ・ Oper Flow Control – フロー制御が有効か無効かを示します。
- ・ MTU Size – ギガビットまたは 10 ギガビットイーサネットのポートあるいはトランクを経由するレイヤ 2 パケットについて許可される最大転送単位 (MTU: Maximum Transmission Unit)。

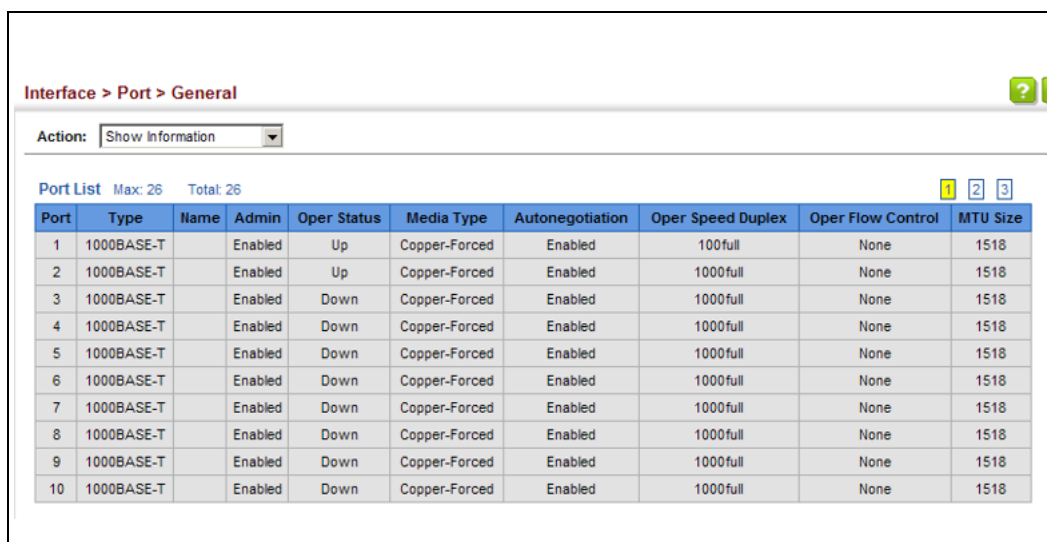
Web 設定

インターフェース設定

Web インターフェース

ポートの接続パラメータを表示するには、以下のようにします。

- (1) 「Interface」 → 「Port」 → 「General」 を選択します。
- (2) 「Step」 リストで 「Show Information」 を選択します。



Interface > Port > General

Action: Show Information

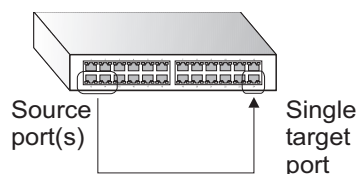
Port List Max: 26 Total: 26

Port	Type	Name	Admin	Oper Status	Media Type	Autonegotiation	Oper Speed Duplex	Oper Flow Control	MTU Size
1	1000BASE-T		Enabled	Up	Copper-Forced	Enabled	100full	None	1518
2	1000BASE-T		Enabled	Up	Copper-Forced	Enabled	1000full	None	1518
3	1000BASE-T		Enabled	Down	Copper-Forced	Enabled	1000full	None	1518
4	1000BASE-T		Enabled	Down	Copper-Forced	Enabled	1000full	None	1518
5	1000BASE-T		Enabled	Down	Copper-Forced	Enabled	1000full	None	1518
6	1000BASE-T		Enabled	Down	Copper-Forced	Enabled	1000full	None	1518
7	1000BASE-T		Enabled	Down	Copper-Forced	Enabled	1000full	None	1518
8	1000BASE-T		Enabled	Down	Copper-Forced	Enabled	1000full	None	1518
9	1000BASE-T		Enabled	Down	Copper-Forced	Enabled	1000full	None	1518
10	1000BASE-T		Enabled	Down	Copper-Forced	Enabled	1000full	None	1518

画面 1-29 ポート情報の表示

ポートのミラーリングの設定

「Interface」→「Port」→「Mirror」を選択すると、リアルタイム分析のために任意の送信元ポートからターゲットポートへのトラフィックをミラーリングすることができます。さらに、論理アナライザまたは RMON プローブをターゲットポートに接続して、送信元ポートで送受信されるトラフィックを、完全に通信の妨げとならない方法で調べることができます。



ローカルポートのミラーリングの設定

関連する CLI 情報

「Local Port Mirroring Commands」

コマンドの使用

- ・ 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 1 つの宛先ポートにミラーリングすることができます。
- ・ 監視ポートの速度は送信元ポートの速度と同等以上でなければなりません。そうでない場合、トラフィックが監視ポートからドロップすることがあります。
- ・ ポートのトラフィックをミラーリングする場合、MSTP を使用するには、ターゲットポートを送信元ポートと同じ VLAN に含める必要があります（「スパンニングツリーアルゴリズム」を参照）。

パラメータ

以下のパラメータが表示されます。

- ・ Source Port - トラフィックをミラーリングするポート（範囲：1 ～ 26）。
- ・ Target Port - 送信元ポートのトラフィックをミラーリングするポート（範囲：1 ～ 26）。
- ・ Type - ターゲットポートにミラーリングするトラフィックを「Rx」（受信）、「Tx」（送信）、「Both」（両方）のいずれかから選択します（デフォルト：Both）。

Web インターフェース

ローカルミラーリングセッションを設定するには、以下のようにします。

- (1) 「Interface」→「Port」→「Mirror」を選択します。
- (2) 「Step」リストで「Add」を選択します。
- (3) 送信元ポートを指定します。
- (4) 監視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 > ボタンをクリックします。

Interface > Port > Mirror

Action: Add

Source Port Unit 1 Port 7

Target Port Unit 1 Port 8

Type Rx

Apply Revert

画面 1-30 : ローカルポートのミラーリングの設定

設定済みのミラーリングセッションを表示するには、以下のようにします。

- (1) 「Interface」 → 「Port」 → 「Mirror」 を選択します。
- (2) 「Step」 リストで 「Show」 を選択します。

Interface > Port > Mirror

Action: Show

Mirror Session List Max: 26 Total: 2

	Source (Unit/Port)	Target (Unit/Port)	Type
☐	1 / 7	1 / 8	Both
☐	1 / 9	1 / 8	Rx

Delete Revert

画面 1-31 : ローカルポートのミラーリングセッションの表示

ポートまたはトランクに関する統計情報の表示

「Interface」 → 「Port/Trunk」 → 「Statistics」 または 「Chart」 を選択すると、インターフェースグループや Etherlike MIB を始めとするネットワークトラフィックに関する標準的な統計情報に加え、RMON MIB に基づくトラフィックの内訳が表示されます。インターフェースおよび Etherlike に関する統計情報には、各ポートを通過するトラフィックのエラーが表示されます。それらの情報は、スイッチに関する潜在的な問題（障害ポートや過度に高い負荷など）を特定するために使用することができます。RMON 統計情報では、各ポートを通過するさまざまなフレームのタイプとサイズの合計数を含め、幅広い統計情報が提供されます。表示されるすべての値は、前回のシステム Reboot 時からの累計値であり、1 秒あたりの数量として表示されます。統計値は、デフォルトで 60 秒ごとに表示更新されます。

[注意] RMON グループ 2、3、9 には、SNMP 管理ソフトウェアを使用することによってのみ、アクセスすることができます。

関連する CLI 情報

「show interfaces counters」

パラメータ

以下のパラメータが表示されます。

パラメータ	説明
Interface Statistics	
Received Octets	インターフェースで受信されたオクテットの総数（フレーミング文字を含む）。
Transmitted Octets	インターフェースから送信されたオクテットの総数（フレーミング文字を含む）
Received Errors	上位プロトコルへの配信の妨げとなったエラーを含むインバウンドパケットの数。
Transmitted Errors	エラーのため送信できなかったアウトバウンドパケットの数。
Received Unicast Packets	上位層プロトコルで受信されたサブネットワークユニキャストパケットの数。
Transmitted Unicast Packets	上位層プロトコルから送信を要求された、サブネットワークユニキャストアドレス宛のパケットの総数（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 Discarded Packets	上位層プロトコルへの配信の妨げとなるエラーがまったく検出されなかったにも関わらず破棄するものとされたインバウンドパケットの数。そのようにパケットが破棄される理由の 1 つとして、バッファ領域を解放するためであることが考えられます。
Transmitted Discarded Packets	送信の妨げとなるエラーがまったく検出されなかったにも関わらず破棄するものとされたアウトバウンドパケットの数。そのようにパケットが破棄される理由の 1 つとして、バッファ領域を解放するためであることが考えられます。
Received Multicast Packets	このサブレイヤから上位（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のパケットの数。
Transmitted Multicast Packets	上位層プロトコルから送信を要求された、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（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	このサブレイヤから上位（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のパケットの数。
Transmitted Broadcast Packets	上位層プロトコルから送信を要求された、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（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 Unknown Packets	このインターフェースを使用して受信され、プロトコルが不明であるため、またはサポートされていないために破棄されたパケットの数。
Etherlike Statistics	

Web 設定

インターフェース設定

Single Collision Frames	コリジョンが 1 つだけ検出された場合に送信が禁止されるフレームのうち、正常に送信されたフレームの数。
Multiple Collision Frames	複数のコリジョンが検出された場合に送信が禁止されるフレームのうち、正常に送信されたフレームの数。
Late Collisions	パケット送信時間に 512 ビット時間を足した時間よりも遅れてコリジョンが検出された回数。
Excessive Collisions	特定のインターフェースで過剰なコリジョンのため送信が失敗したフレームの数。このカウンタの値は、インター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	メディアがビジーであったため特定のインターフェースで最初の送信時に遅延が発生したフレームの数。
Frames Too Long	特定のインターフェースで受信されたフレームのうち、最大許容サイズを超えるフレームの数。
Alignment Errors	アライメントエラー（同期外れデータパケット）の数。
FCS Errors	特定のインターフェースで受信されたフレームのうち、長さは整数オクテットであるが FCS チェックに合格しなかったフレームの数。この数には、Frame-too-long エラーまたは Frame-too-short エラーがある受信フレームは含まれません。
SQE Test Errors	特定のインターフェースについて SQE TEST ERROR メッセージが PLS サブレイヤで生成された回数。
Carrier Sense Errors	フレームの送信時にキャリアセンス状態が失われたか、アサート状態にならなかった回数。
Internal MAC Receive Errors	特定のインターフェースで内部 MAC サブレイヤ受信エラーのため受信が失敗したフレームの数。
Internal MAC Transmit Errors	特定のインターフェースで内部 MAC サブレイヤ送信エラーのため送信が失敗したフレームの数。
RMON Statist	
Drop Events	リソース不足のためパケットがドロップされたイベントの総数。
Jabbers	1,518 octets よりも長く（フレーミングビットを除くが FCS オクテットを含む）、FCS エラーとアラインメントエラーのいずれかをを含む受信フレームの総数。
Fragments	64 octets よりも短く（フレーミングビットを除くが FCS オクテットを含む）、FCS エラーとアラインメントエラーのいずれかをを含む受信フレームの総数。
Collisions	このイーサネットセグメントにおけるコリジョンの総数の最良推定値。
Received Octets	ネットワークで受信されたデータの総オクテット数。この統計値は、イーサネットの使用状況を確認する際の目安として利用することができます。
Received Packets	受信されたパケット（不良、ブロードキャスト、およびマルチキャスト）の総数。
Broadcast Packets	受信された正常パケットのうち、ブロードキャストアドレス宛に送信されたパケットの総数。ただし、この値にはマルチキャストパケットは含まれません。

Multicast Packets	受信された正常パケットのうち、マルチキャストアドレス宛に送信されたパケットの総数。
Undersize Packets	64 octets よりも短い（フレーミングビットを除くが FCS オクテットを含む）がそれ以外は問題のない受信パケットの総数。
Oversize Packets	Packets1518 octets よりも長い（フレーミングビットを除くが FCS オクテットを含む）がそれ以外は問題のない受信パケットの総数。
64 Byte Packets	送受信されたパケットのうち、64 octets（フレーミングビットを除くが FCS オクテットを含む）よりも長いパケット（不良パケットを含む）の総数。 65-127 Byte Packets 128-255 Byte Packets 256-511 Byte Packets 512-1023 Byte Packets 1024-1518 Byte Packets 送受信されたパケットのうち、オクテット数（フレーミングビットを除くが FCS オクテットを含む）が指定された範囲内であるパケットの総数。
Utilization Statistics	
Input Octets per second	このインターフェースが 1 秒間に受け取ったオクテットの数。
Input Packets per second	このインターフェースが 1 秒間に受け取ったパケットの数。
Input Utilization	このインターフェースの入力使用率。
Output Octets per second	このインターフェースから 1 秒間に送り出されたオクテットの数。
Output Packets per second	このインターフェースから 1 秒間に送り出されたパケットの数。
Output Utilization	このインターフェースの出力使用率。

Web インターフェース

ポートに関する統計情報を一覧表示するには、以下のようにします。

- (1) 「Interface」 → 「Port」 → 「Statistics」 を選択します。
- (2) 表示する統計モード（「Interface」、「Etherlike」、または「RMON」）を選択します。
- (3) ポートをドロップダウンリストで選択します。
- (4) 表示内容を更新する場合は、画面の下方にある < Refresh > ボタンをクリックします。または、< Clear > ボタンをクリックして統計情報をリセットします。

The screenshot shows a web interface titled "Interface > Port > Statistics". It features a "Mode" section with radio buttons for "Interface" (selected), "Etherlike", "RMON", and "Utilization". Below this is a "Port" dropdown menu set to "1" and an unchecked "Auto-refresh" checkbox. The main area, titled "Interface Statistics", displays a table of statistics for Port 1. The statistics are organized into two columns: Received and Transmitted. The "Refresh" button is located at the bottom right of the statistics table.

Interface Statistics			
Received Octets	182057	Transmitted Octets	1353652
Received Errors	0	Transmitted Errors	0
Received Unicast Packets	1270	Transmitted Unicast Packets	1700
Received Discarded Packets	0	Transmitted Discarded Packets	0
Received Multicast Packets	9	Transmitted Multicast Packets	838
Received Broadcast Packets	23	Transmitted Broadcast Packets	2
Received Unknown Packets	0		

画面 1-32 : ポートに関する統計情報の表示（一覧）

ポートに関する統計情報をグラフ表示するには、以下のようにします。

- (1) 「Interface」 → 「Port」 → 「Chart」 を選択します。
- (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」、または「RMON」を統計モードとして選択した場合は、ポートをドロップダウンリストで選択します。「All」（ポート）を統計モードとして選択した場合は、表示する統計タイプを選択します。



画面 1-33 : ポートに関する統計情報の表示（グラフ）

ケーブル診断の実行

「Interface」→「Port」→「Cable Test」を選択すると、ポートに接続されているケーブルをテストすることができます。ケーブルテストでは、ケーブルに関するあらゆる障害（ショートケーブルやオープンケーブルなど）がチェックされます。障害が検出されると、障害発生箇所までの距離が報告されます。障害が検出されない場合は、ケーブルの長さが報告されます。このテストは、ケーブル、コネクタおよび終端の品質を判別する場合に使用することができます。オープンケーブル、ショートケーブル、ケーブルインピーダンスの不整合などの問題は、このテストによって診断することができます。

関連する CLI 情報

「Interface Commands」

コマンドの使用

- ・ ケーブル診断は、デジタル信号処理（DSP: Digital Signal Processing）テストモードを使用して実行されます。DSP では、パルス信号をケーブルに送信してからパルスの反射を調べるという方法でケーブルの分析が行われます。
- ・ ケーブル診断は、ツイストペアメディアでのみ実行することができます。
- ・ このケーブルテストは、7 ～ 140 m の長さのケーブルでのみ、正確に実行されます。
- ・ テストには約 5 秒かかります。テストが完了するとすぐに、スイッチに結果が表示され、障害のステータスや障害発生箇所までのおおよその距離に加え、一般的なケーブル障害などを確認することができます。
- ・ 診断で表示される可能性のある状況として、以下のものがあります。
 - ・ OK: 正しく終端されているペア。
 - ・ Open: オープンペア。リンクパートナーなし。
 - ・ Short: ショートペア
 - ・ Not Supported: このメッセージは、ギガビットイーサネットポートが 1,000 Mbps 未満でリンクアップしている場合または 10G イーサネットポートの場合に表示されます。
 - ・ Impedance mismatch: 終端インピーダンスが基準範囲内にありません。
 - ・ ポートは、ケーブル診断の実行中はリンクダウンします。

パラメータ

以下のパラメータが表示されます。

- ・ Port – スイッチポート ID（範囲: 1 ～ 26）。
- ・ Test Result – テストの結果では、障害のステータスや障害発生箇所までのおおよその距離（または、障害が検出されない場合はケーブルのおおよその長さ）に加え、一般的なケーブル障害などを確認することができます。
- ・ Accuracy – 報告される障害発生箇所までの距離の精度（問題がまったく検出されない場合は「0」と表示されます）。
- ・ Last Updated – このポートで前回テストが実行された日時が表示されます。

Web インターフェース

ポートに接続されているケーブルをテストするには、以下のようにします。

- (1) 「Interface」 → 「Port」 → 「Cable Test」 を選択します。
- (2) いずれかのポートの < Test > ボタンをクリックして、ケーブルテストを開始します。

Interface > Port > Cable Test

Cable Test Port List Max: 26 Total: 26 1 2 3

Port	Test Result (Cable/Fault Distance in Meters)				Accuracy(Meters)	Last Updated	Action
	Pair A	Pair B	Pair C	Pair D			
1	OK (1)	OK (2)	Short (1)	Short (2)	0	2010-06-22 01:40:19	Test
2	Not Tested Yet	Not Tested Yet	Not Tested Yet	Not Tested Yet	0		Test
3	Not Tested Yet	Not Tested Yet	Not Tested Yet	Not Tested Yet	0		Test
4	Not Tested Yet	Not Tested Yet	Not Tested Yet	Not Tested Yet	0		Test
5	Not Tested Yet	Not Tested Yet	Not Tested Yet	Not Tested Yet	0		Test
6	Not Tested Yet	Not Tested Yet	Not Tested Yet	Not Tested Yet	0		Test
7	Not Tested Yet	Not Tested Yet	Not Tested Yet	Not Tested Yet	0		Test
8	Not Tested Yet	Not Tested Yet	Not Tested Yet	Not Tested Yet	0		Test
9	Not Tested Yet	Not Tested Yet	Not Tested Yet	Not Tested Yet	0		Test
10	Not Tested Yet	Not Tested Yet	Not Tested Yet	Not Tested Yet	0		Test

画面 1-34 : ケーブルテストの実行

1.3.2 トランク設定（リンクアグリゲーション）

ここでは、スタティックトランクおよびダイナミックトランクを設定する方法について説明します。

複数のリンクをデバイス間で作成し、1つの仮想アグリゲーションリンクとして機能させることができます。ポートトランクは、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を大幅に拡大させるだけでなく、2つのデバイス間でフォールトトレラントなリンクを実現します。1つのスイッチで最大 13 のトランクまたはスタック全体で最大 32 のトランクを作成することができます。

本製品は、スタティックトランキングとダイナミック LACP（Link Aggregation Control Protocol）の両方をサポートしています。スタティックトランクはリンクの両端で手動設定する必要があり、スイッチは Cisco Ether Channel 規格に準拠していなければなりません。一方、LACP が設定されているポートでは、他のデバイスの LACP 設定ポートとのトランクリンクのオートネゴシエーションが可能です。本製品では、既にスタティックトランクの一部として設定されていないポートであれば、いくつでも LACP ポートとして設定することができます。他のデバイスのポートも LACP ポートとして設定されている場合には、スイッチとそのデバイスが相互間のトランクリンクをネゴシエーションします。LACP トランクを設定しているポートの数が 8 つを超えている場合、9 番目以降のすべてのポートは、スタンバイモードになります。トランク内の 1 つのリンクで障害が発生すると、自動的に、スタンバイポートの 1 つがアクティブになって代替ポートとして機能するようになります。

コマンドの使用

トランク内のポート全体で負荷が分散されるだけでなく、トランク内のいずれかのポートで障害が発生した場合には、他のポートが代わりに負荷を引き受けることによって冗長性を提供します。

ただし、デバイス同士を物理的に接続する前に、両端のデバイスで Web インターフェースまたは CLI を使用してトランクを指定する必要があります。

ポートトランクを使用する場合は、以下の点に注意してください。

- ・ ループが発生しないようにするため、スイッチ同士を相応のネットワークケーブルで接続する前にポートトランクの設定を完了させてください。
- ・ 1 つのスイッチ / スタック全体で最大 32 トランク（トランクごとに 8 ポート）を作成することができます。
- ・ 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。
- ・ 異なるタイプのスイッチでスタティックトランクを設定する場合には、それらのスイッチが Cisco Ether Channel 規格に準拠していなければなりません。
- ・ トランクの両端のポートは、通信モード（つまり、速度、デュプレクスモード、およびフロー制御）、VLAN 割り当て、CoS 設定を含め、まったく同じに設定する必要があります。
- ・ 前面パネルの任意のギガビットポート（メディアタイプが異なるポートを含む）を同じトランクに含めることができます。
- ・ トランク内のすべてのポートは、VLAN に対して移動、追加、または削除する場合には、ひとまとまりのものとして取り扱わなければなりません。
- ・ STP、VLAN、および IGMP の各設定は、トランク全体に対してのみ指定することができます。

スタティックトランクの設定

「Interface」→「Trunk」→「Static」を選択すると、トランクを作成し、メンバーポートを割り当て、接続パラメータを設定することができます。

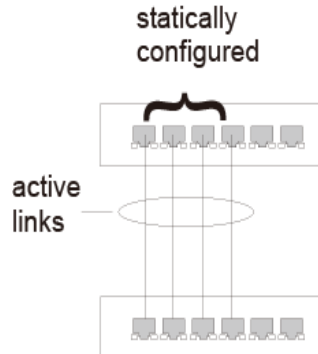


図 1-2: スタティックトランクの設定

関連する CLI 情報

「Link Aggregation Commands」

「Interface Commands」

コマンドの使用

- ・ スタティックトランクを設定する場合、ベンダーが採用している実装方法によっては、異なるタイプのスイッチをリンクできないことがあります。本製品のスタティックトランクは Cisco Ether Channel 規格に準拠しています。
- ・ ネットワークでループが発生しないようにするため、必ず、ポートを設定する前に設定インターフェースを使用してスタティックトランクを追加し、スタティックトランクを削除する前に設定インターフェースを使用してポートを接続解除してください。

パラメータ

以下のパラメータが表示されます。

- ・ Trunk ID – トランク ID（範囲：1 ～ 32）。
- ・ Member – 初期トランクメンバー。「Step」リストで「Add Member」を選択すると、追加メンバーを設定することができます。
- ・ Unit – スタックユニット（範囲：1 ～ 8）。
- ・ Port – ポート ID（範囲：1 ～ 26）。

Web インターフェース

スタティックトランクを作成するには、以下のようになります。

- (1) 「Interface」→「Trunk」→「Static」を選択します。
- (2) 「Step」リストで「Configure Trunk」を選択します。
- (3) 「Step」リストで「Add」を選択します。
- (4) トランク ID を入力します。

Web 設定

インターフェース設定

(5) 初期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 > ボタンをクリックします。

Interface > Trunk > Static

Step: 1. Configure Trunk Action: Add

Trunk ID (1-32) 1

Member Unit 1 Port 5

Apply Revert

画面 1-35 : スタティクトランクの作成

メンバーポートをスタティクトランクに追加するには、以下のようにします。

- (1) 「Interface」 → 「Trunk」 → 「Static」 を選択します。
- (2) 「Step」 リストで 「Configure Trunk」 を選択します。
- (3) 「Step」 リストで 「Add Member」 を選択します。
- (4) トランク ID を選択します。
- (5) 追加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 > ボタンをクリックします。

Interface > Trunk > Static

Step: 1. Configure Trunk Action: Add Member

Trunk 1

Member Unit 1 Port 1

Apply Revert

画面 1-36 : スタティクトランクメンバーの追加

スタティクトランクの接続パラメータを設定するには、以下のようにします。

- (1) 「Interface」 → 「Trunk」 → 「Static」 を選択します。
- (2) 「Step」 リストで 「Configure General」 を選択します。
- (3) 「Step」 リストで 「Configure」 を選択します。

- (4) 必要な インター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、「ポートリストに基づく設定」を参照）。
- (5) < Apply > ボタンをクリックします。

Interface > Trunk > Static ?

Step: 2. Configure General Action: Configure

Static Trunk List Max: 32 Total: 1

Trunk	Type	Name	Admin	Media Type	Autonegotiation					Speed Duplex	Flow Control	MTU Size (1500-9216)
1	1000BASE-T		☒ Enabled	Copper-Forced	☒ Enabled ☒ 10h ☒ 100h ☐ 1000h ☐ 10Gh ☐ Sym ☒ 10f ☒ 100f ☒ 1000f ☐ 10Gf ☐ FC					100full	☐ Disabled	1518

Apply Revert

画面 1-37 : スタティックトランクの接続パラメータの設定

トランクの接続パラメータを表示するには、以下のようにします。

- (1) 「Interface」 → 「Trunk」 → 「Static」 を選択します。
- (2) 「Step」 リストで「Configure General」を選択します。
- (3) 「Step」 リストで「Show Information」を選択します。

Interface > Trunk > Static ?

Step: 2. Configure General Action: Show Information

Static Trunk List Max: 32 Total: 1

Trunk	Type	Name	Admin	Oper Status	Media Type	Autonegotiation	Oper Speed Duplex	Oper Flow Control	MTU Size
1	1000BASE-T		Enabled	Down	Copper-Forced	Enabled	1000full	None	1518

画面 1-38 : スタティックトランクの接続パラメータの表示

ダイナミックトランクの設定

「Interface」→「Trunk」→「Dynamic」（Configure Aggregator）を選択すると、アグリゲーショングループの管理キーを設定する、ポートの LACP を有効にする、ローカルポートとパートナーポートのプロトコルパラメータを設定するといったことができます。

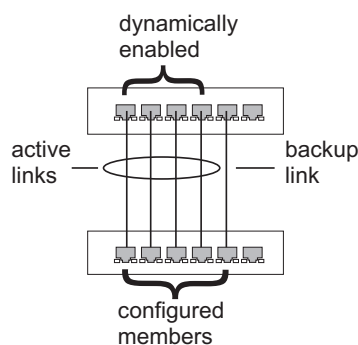


図 1-3: ダイナミックトランクの設定

関連する CLI 情報

「Link Aggregation Commands」

コマンドの使用

- ・ ネットワークでループが発生しないようにするため、必ず、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接続解除してください。
- ・ ターゲットスイッチ上の接続先ポートでも LACP が有効になっている場合には、トランクが自動的にアクティブになります。
- ・ LACP を使用して他のスイッチとの間で形成されたトランクには、最も小さいトランク ID が自動的に割り当てられます。
- ・ 同じターゲットスイッチに 8 つを超えるポートが接続されており、それらのポートで LACP が有効になっている場合、9 番目以降の追加ポートはスタンバイモードになり、いずれかのアクティブリンクで障害が発生したときにのみ有効になります。
- ・ LACP トランクの両端のすべてのポートは、全二重のオートネゴシエーションに対応するように設定する必要があります。
- ・ ポートは、(1) LACP ポートシステム優先度、(2) LACP ポート管理キー、および (3) LAG 管理キー（設定されている場合）がそれぞれ同じである場合にのみ、同じリンクアグリゲーショングループ（LAG: Link Aggregation Group）のメンバーになることができます。ただし、LAG 管理キーが設定されている場合、その管理キーは、グループのメンバーになることが可能なポートと同じ値に設定されていなければなりません。

【注意】 チャンネルグループの形成時に LACP 管理キーが設定されない場合（つまり、Null 値である 0 が設定される場合）、そのキーの動作値は、グループのメンバーであるインターフェースで使用されているポート管理キーと同じ値に設定されます（show lacp internal コマンドの説明を参照）。

パラメータ

以下のパラメータが表示されます。

Configure Aggregator

- ・ Admin Key – スイッチでのローカル LACP セットアップ時に LACP 管理キーを使用して特定の LAG を識別します（範囲：0 ～ 65,535）。

Configure Aggregation Port - General

- ・ Port – ポート ID（範囲：1 ～ 26）。
- ・ LACP Status – ポートで LACP を有効または無効にします。

Configure Aggregation Port - Actor/Partner

- ・ Port – ポート番号（範囲：1 ～ 26）。
- ・ Admin Key – LACP 管理キーは、同じ LAG に属するポートと同じ値に設定する必要があります（範囲：0 ～ 65,535、デフォルト：1）。
- ・ デフォルトでは、「Actor Admin Key」がポートのリンク速度に基づいて判別されて「Oper Key」にコピーされます。「Partner Admin Key」は 0 に割り当てられ、「Oper Key」はパートナーから受信される LACP PDU に基づいて設定されます。
- ・ System Priority – LACP システム優先度を使用して LAG のメンバーであるかどうかを判別され、さらに、LAG ネゴシエーション時にこのデバイスが他のスイッチと区別されます（範囲：0 ～ 65,535、デフォルト：32,768）。
- ・ システム優先度とスイッチの MAC アドレスを組み合わせると LAG ID が作成されます。LAG ID を使用して、他のシステムとの LACP ネゴシエーション時に特定の LAG が示されます。
- ・ Port Priority – リンクがダウンした場合は、LACP ポートの優先度を使用してバックアップリンクが選択されます（範囲：0 ～ 65,535、デフォルト：32,768）。

【 注意 】 ポートの LACP 設定の設定は、管理状態にのみ適用され、動作状態には適用されず、次回にそのポートとアグリゲーションリンクが確立されたときにのみ有効になります。

【 注意 】 ポートパートナーを設定すると、アグリゲーションリンクのリモート側（つまり、接続先デバイスのポート）が設定されます。コマンド属性の意味は、ポートアクターに使用されるものと同じです。

Web インターフェース

ダイナミックトランクの管理キーを設定するには、以下のようになります。

- (1) 「Interface」 → 「Trunk」 → 「Dynamic」を選択します。
- (2) 「Step」リストで「Configure Aggregator」を選択します。
- (3) 必要な LACP グループの管理キーを設定します。

(4) < Apply > ボタンをクリックします。

Interface > Trunk > Dynamic

Step: 1. Configure Aggregator

Trunk List Max: 32 Total: 32

Trunk	Admin Key (0-65535)
1	1
2	0
3	0
4	0
5	0

画面 1-39 : LACP アグリゲータの管理キーの設定

ポートの LACP を有効にするには、以下のようにします。

- (1) 「Interface」 → 「Trunk」 → 「Dynamic」 を選択します。
- (2) 「Step」 リストで 「Configure Aggregation Port」 を選択します。
- (3) 「Step」 リストで 「Configure」 を選択します。
- (4) 「General」 を選択します。
- (5) 必要なポートの LACP を有効にします。
- (6) < Apply > ボタンをクリックします。

Interface > Trunk > Dynamic

Step: 2. Configure Aggregation Port Action: Configure

☒ General ☐ Actor ☐ Partner

Port List Max: 26 Total: 26

Port	LACP Status
1	☐ Enabled
2	☐ Enabled
3	☒ Enabled
4	☒ Enabled
5	☐ Enabled

画面 1-40 : ポートの 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、以下のようにします。

- (1) 「Interface」 → 「Trunk」 → 「Dynamic」 を選択します。

- (2) 「Step」 リストで「Configure Aggregation Port」を選択します。
- (3) 「Step」 リストで「Configure」を選択します。
- (4) 「Actor」または「Partner」を選択します。
- (5) 必要な設定を設定します。
- (6) < Apply > ボタンをクリックします。

Interface > Trunk > Dynamic

Step: 2. Configure Aggregation Port Action: Configure

☐ General ☒ Actor ☐ Partner

Port List Max: 26 Total: 26

Port	Admin Key (0-65535)	System Priority (0-65535)	Port Priority (0-65535)
1	3	32768	32768
2	3	32768	32768
3	3	32768	32768
4	3	32768	32768
5	1	32768	32768

画面 1-41 : ポートの LACP パラメータの設定

ダイナミックトランクのアクティブメンバーを表示するには、以下のようにします。

- (1) 「Interface」 → 「Trunk」 → 「Dynamic」を選択します。
- (2) 「Step」 リストで「Configure Trunk」を選択します。
- (3) 「Step」 リストで「Show Member」を選択します。
- (4) トランクを選択します。

Interface > Trunk > Dynamic

Step: 3. Configure Trunk Action: Show Member

Trunk 1

Member List Total: 3

Member (Unit/Port)
1/1
1/11
2/12

画面 1-42 : ダイナミックトランクのメンバーの表示

Web 設定

インターフェース設定

ダイナミックトランクの接続パラメータを設定するには、以下のようにします。

- (1) 「Interface」 → 「Trunk」 → 「Dynamic」 を選択します。
- (2) 「Step」 リストで 「Configure Trunk」 を選択します。
- (3) 「Step」 リストで 「Configure」 を選択します。
- (4) 必要なインターフェース設定を変更します（インターフェース設定の説明については、「ポートリストに基づく設定」を参照）。
- (5) < Apply > ボタンをクリックします。

Interface > Trunk > Dynamic

Step: 3. Configure Trunk Action: Configure

Dynamic Trunk List Max: 32 Total: 2

Trunk	Type	Name	Admin	Media Type	Autonegotiation	Speed Duplex	Flow Control
1	1000Base-TX		☒ Enabled	Copper-Forced	☒ 10h ☒ 100h ☐ 1000h ☐ Sym ☒ 10f ☒ 100f ☒ 1000f ☐ FC	100full	☒ Enabled
2	1000Base-TX		☒ Enabled	Copper-Forced	☒ 10h ☒ 100h ☐ 1000h ☐ Sym ☒ 10f ☒ 100f ☒ 1000f ☐ FC	100full	☒ Enabled

Apply Revert

画面 1-43 : ダイナミックトランクの接続設定の設定

ダイナミックトランクの接続パラメータを表示するには、以下のようにします。

- (1) 「Interface」 → 「Trunk」 → 「Dynamic」 を選択します。
- (2) 「Step」 リストで 「Configure Trunk」 を選択します。
- (3) 「Step」 リストで 「Show」 を選択します。

Interface > Trunk > Dynamic

Step: 3. Configure Trunk Action: Show

Dynamic Trunk List Max: 32 Total: 1

Trunk	Type	Name	Admin	Oper Status	Media Type	Autonegotiation	Oper Speed Duplex	Oper Flow Control	MTU Size
1	1000BASE-T		Enabled	Up	Copper-Forced	Enabled	1000full	None	1518

画面 1-44 : ダイナミックトランクの接続パラメータの表示

LACP ポートカウンタの表示

「Interface」→「Trunk」→「Dynamic」（「Configure Aggregation Port」→「Show Information」→「Counters」）を選択すると、LACP プロトコルメッセージに関する統計情報が表示されます。

関連する CLI 情報

「show lacp」

パラメータ

以下のパラメータが表示されます。

パラメータ	説明
LACPDU Sent	このチャネルグループから送信された有効な LACPDU の数。
LACPDU Received	このチャネルグループで受信された有効な LACPDU の数。
Marker Sent	このチャネルグループから送信された有効な Marker LACPDU の数。
Marker Received	このチャネルグループで受信された有効な Marker LACPDU の数。
Marker Unknown Pkts	(1) Slow Protocols Ethernet Type 値を伝播するが不明な PDU を含む受信フレームまたは (2) Slow Protocols グループの MAC アドレス宛だが Slow Protocols Ethernet Type 値を伝播しない受信フレームの数。
Marker Illegal Pkts	Slow Protocols Ethernet Type 値を伝播するが PDU の形式が不正または Protocol Subtype の値が無効なフレームの数。

表 1-1: LACP ポートカウンタ

Interface > Trunk > Dynamic

Step: 2. Configure Aggregation Port Action: Show Information

☒ Counters ☐ Internal ☐ Neighbors

Port 3

Trunk ID 2

Port Counters Information

LACPDU Sent	21	LACPDU Receive	20
Marker Sent	0	Marker Receive	0
Marker Unknown Pkts	0	Marker Illegal Pkts	0

Refresh

画面 1-45 : LACP ポートカウンタの表示

Web インターフェース

LACP ポートカウンタを表示するには、以下のようになります。

- (1) 「Interface」 → 「Trunk」 → 「Dynamic」 を選択します。
- (2) 「Step」 リストで 「Configure Aggregation Port」 を選択します。
- (3) 「Step」 リストで 「Show Information」 を選択します。
- (4) 「Counters」 を選択します。
- (5) グループメンバーを 「Port」 リストで選択します。

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」) を選択すると、リンクアグリゲーションのローカル側の設定情報と動作状態が表示されます。

関連する CLI 情報

「show lacp」

パラメータ

以下のパラメータが表示されます。

パラメータ	説明
LACP System Priority	このポートチャネルに割り当てられている LACP システム優先度。
LACP Port Priority	チャネルグループ内でこのインターフェースに割り当てられている LACP ポート優先度。
Admin Key	アグリゲーションポートのキーの現在の管理値。
Oper Key	アグリゲーションポートのキーの現在の動作値。
LACPDUs Interval	受信した LACPDU 情報が無効化されるまでの時間 (秒)。

Admin State, Oper State	アクターの状態パラメータの管理値または動作値であり、以下のいずれかです。 Expired - アクターの受信マシンが期限切れ状態になっています。 Defaulted - アクターの受信マシンはパートナーに対して管理のために設定されているデフォルトの動作パラメータ情報を使用しています。 Distributing - false の場合、このリンクで発信フレームの配信が無効になっています。つまり、配信は、現在、無効になっており、管理情報または受信されたプロトコル情報が変更されない限り、有効にならないものと考えられます。 Collecting - このリンクで着信フレームの収集が有効になっています。つまり、収集は、現在、有効になっており、管理情報または受信されたプロトコル情報が変更されない限り、無効にならないものと考えられます。 Synchronization - このリンクはシステムで IN_SYNC としてみなされています。つまり、このリンクは適切な LAG（互換性を備えたアグリゲータに接続されている LAG）に関連付けられており、LAG の ID が送信されたシステム ID と動作キーの情報に対応しています。 Aggregation - このリンクはシステムで集約可能（つまり、集約の潜在的な候補）であるとみなされています。 Long timeout - 定期的な LACPDU の送信に低い伝送速度が使用されています。 LACP-Activity - このリンクに関するアクティビティ制御値（0: パッシブ、1: アクティブ）。

表 1-2: LACP 内部設定情報

Web インターフェース

ローカル側の LACP 設定とステータスを表示するには、以下のようになります。

- (1) 「Interface」 → 「Trunk」 → 「Dynamic」 を選択します。
- (2) 「Step」 リストで 「Configure Aggregation Port」 を選択します。
- (3) 「Step」 リストで 「Show Information」 を選択します。
- (4) 「Internal」 を選択します。

(5) グループメンバーを「Port」リストで選択します。

The screenshot shows a web interface for configuring network settings. At the top, there is a breadcrumb trail: "Interface > Trunk > Dynamic". Below this, there are two dropdown menus: "Step: 2. Configure Aggregation Port" and "Action: Show Information". Underneath, there are three radio buttons: "Counters", "Internal" (which is selected), and "Neighbors". Below the radio buttons, there is a "Port" dropdown menu showing "2" and a "Trunk ID" field showing "1". The main section is titled "Port Internal Information" and contains a table of LACP parameters and their values.

LACP System Priority	32768
LACP Port Priority	32768
Admin Key	4
Oper Key	4
LACPDUs Interval	30 sec
Admin State	Defaulted, Aggregation, Long timeout, LACP-activity
Oper State	Distributing, Collecting, Synchronization, Aggregation, Long timeout, LACP-activity

画面 1-46 : LACP ポートの内部情報の表示

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」）を選択すると、リンクアグリゲーションのリモート側の設定情報と動作状態が表示されます。

関連する CLI 情報

「show lacp」

パラメータ

以下のパラメータが表示されます。

パラメータ	説明
Partner Admin System	ID ユーザが割り当てた LAG パラメータのシステム ID。
Partner Oper System ID	LACP プロトコルによって割り当てられた LAG パラメータのシステム 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アグリゲーションポートに割り当てられた動作ポート番号。
Partner Oper Port Number	ポートのプロトコルパートナーによってこのアグリゲーションポートに割り当てられた動作ポート番号。
Port Admin Priority	プロトコルパートナーのポート優先度の現在の管理値。

Port Oper Priority	パートナーによってこのアグリゲーションポートに割り当てられた優先度の値。
Admin Key	プロトコルパートナーのキーの現在の管理値。
Oper Key	プロトコルパートナーのキーの現在の動作値。
Admin State	パートナーの状態パラメータの管理値（既出の表を参照）。
Oper State	パートナーの状態パラメータの動作値（既出の表を参照）。

表 1-3: LACP 内部設定情報

Web インターフェース

リモート側の LACP 設定とステータスを表示するには、以下のようになります。

- (1) 「Interface」 → 「Trunk」 → 「Dynamic」 を選択します。
- (2) 「Step」 リストで「Configure Aggregation Port」を選択します。
- (3) 「Step」 リストで「Show Information」を選択します。
- (4) 「Neighbors」を選択します。
- (5) グループメンバーを「Port」リストで選択します。

Interface > Trunk > Dynamic

Step: 2. Configure Aggregation Port
Action: Show Information

☐ Counters
☐ Internal
☒ Neighbors

Port 3
Trunk ID 2

Port Neighbors Information

Partner Admin System ID	32768, 00-00-00-00-00-00
Partner Oper System ID	32768, 00-12-CF-61-24-2F
Partner Admin Port Number	3
Partner Oper Port Number	3
Port Admin Priority	32768
Port Oper Priority	32768
Admin Key	0
Oper Key	3
Admin State	Defaulted, Distributing, Collecting, Synchronization, Long timeout
Oper State	Distributing, Collecting, Synchronization, Aggregation, Long timeout, LACP-activity

画面 1-47 : LACP ポートのリモート情報の表示

1.3.3 トラフィックフローのサンプリング

本製品に組み込まれているフローサンプリング (sFlow) 機能は、リモート sFlow Collector と共に、ネットワーク上に存在するトラフィックのタイプとレベルに関する正確かつ詳細なリアルタイムの情報を管理者に提供します。スイッチを経由するすべてのデータの n 個のパケットから抽出される sFlow Agent サンプル 1 では、サンプルが sFlow ダイアグラムとして再カプセル化されて sFlow Collector に送信されます。従来のプローブではトラフィックが監視対象のインターフェースでサンプリングされるのでトラフィックの状況は部分的にしか確認されませんが、このサンプリングは、すべてのトラフィックが確認される内部ハードウェアレベルで実行されます。それだけでなく、ローカル分析が実行されないため、sFlow エージェントによって課せられるプロセッサとメモリの負荷は最小限に抑えられます。そのため、高いトラフィックレベルでもスイッチのワイヤ速度の伝送特性が維持されます。

sFlow Collector がネットワーク全体の各種の sFlow エージェント（他のスイッチまたはルータ）からストリームを受け取るため、ネットワークの全体的な使用状況とトラフィックフローを適時に確認することができます。sFlow ストリームの分析により、以下の方法で利用できる傾向と情報が明らかになります。

- ・ ネットワークに関する問題の検出、診断、および修正
- ・ リアルタイムでの輻輳管理
- ・ アプリケーションミックス (P2P、Web、DNS など) と変更の把握
- ・ 承認されていないネットワークアクティビティの特定とトレース
- ・ 使用アカウントリング
- ・ 傾向分析およびキャパシティプランニング

sFlow パラメータの設定

「Interface」→「sFlow」を選択すると、サンプリングされるデータの送信元パラメータと宛先パラメータ、ペイロードパラメータ、およびサンプリング間隔を設定することができます。

関連する CLI 情報

「Flow Sampling Commands」

パラメータ

以下のパラメータが表示されます。

- ・ Port - 設定するポートを選択します (範囲: 1 ~ 26、デフォルト: 1)。
- ・ Status - 選択したポートの sFlow を有効にします。
- ・ Receiver Owner - 受信先の名前 (範囲: 1 ~ 256、デフォルト: None)。
- ・ Receiver IP Address - sFlow Collector の IP アドレス。
- ・ Receiver Port - sFlow Collector が sFlow ストリームを listen している UDP ポート (範囲: 0 ~ 65,534、デフォルト: 6,343)。
- ・ Timeout - sFlow プロセスですべての sFlow ポートパラメータをリセットするまで継続的にサンプルを送信する時間 (範囲: 0 ~ 999,999,999 秒 (0 = タイムアウトなし))。このコマンドの影響を受ける sFlow パラメータとして、サンプリング間隔、受信先の名前、アドレス、および UDP ポート、タイムアウト、最大ヘッダサイズ、ならびに最大データグラムサイズなどがあります。

- ・ Max Header Size – sFlow データグラムヘッダの最大サイズ（範囲：64 ～ 256 bytes、デフォルト：128bytes）。
- ・ Max Datagram Size – sFlow データグラムペイロードの最大サイズ（範囲：200 ～ 1,500 bytes、デフォルト：1,400 bytes）。
- ・ Sample Rate – 1 つのサンプルが抽出されるパケットの数（範囲：256 ～ 16,777,215 パケットまたは 0 パケット（= サンプルング無効）、デフォルト：Disabled）。

**1. これらのフィールドを指定する前に、タイムアウトを 0 に設定してサンプルングを無効にする必要があります。

Web インターフェース

フローサンプリングを設定するには、以下のようにします。

- (1) 「Interface」 → 「sFlow」 を選択します。
- (2) フローコレクタ、リセットのためのタイムアウト、ペイロード、およびサンプリングレートのパラメータを設定します。
- (3) < Apply > ボタンをクリックします。

Interface > sFlow

Port	5
Source Status	☒ Enabled
Receiver Owner	Lamar
Receiver IP Address	192.168.0.4
Receiver Port (0-65534)	6343
Timeout (0-10000000)	3880 sec
Max Header Size (64-256)	256 bytes
Max Datagram Size (200-1500)	1500 bytes
Sample Rate (256-16777215)	Sample one packet randomly from 256 packets

Apply Revert

画面 1-48：トラフィックフローのサンプリング

1.3.4 トラフィックのセグメント化（プライベート VLAN）

ローカルネットワークでダウンリンクポートを使用して別々のクライアントからアップリンクポート経由でトラフィックをサービスプロバイダに渡すために高いセキュリティが必要な場合は、ポート単位のトラフィックセグメント化を使用して別々のダウンリンクポートのクライアント間で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では、データトラフィックはアップリンクポートのみに転送され、アップリンクポートのみから転送されます。

各クライアントに属するトラフィックは、割り当てられているダウンリンクポートへと分離されます。ただし、スイッチは、クライアントで割り当てられているアップリンクポートを経由するトラフィックを他のクライアントに割り当てられているアップリンクポートから分離するように設定することも、他のクライアントで使用されているアップリンクポートによってトラフィックを転送するように設定して別々のクライアントがセキュリティ侵害の可能性の低いアップリンクポートへのアクセスを共有できるようにすることもできます。

トラフィックのセグメント化の有効化

「Interface」→「Traffic Segmentation」（Configure Global）を選択すると、トラフィックのセグメント化を有効にすることができます。

関連する CLI 情報

「Configuring Port-based Traffic Segmentation」

パラメータ

以下のパラメータが表示されます。

- ・ Status – ポート単位のトラフィックのセグメント化を有効にします（デフォルト：Disabled）。
- ・ Uplink-to-Uplink Mode – 別々のクライアントセッションに割り当てられているアップリンクポート間でトラフィックを転送できるようにするかどうかを指定します。
- ・ Blocking – 別々のセッションに割り当てられているアップリンクポート間でトラフィックをブロックします。
- ・ Forwarding – 別々のセッションに割り当てられているアップリンクポート間でトラフィックを転送します。

Web インターフェース

トラフィックのセグメント化を有効にするには、以下のようにします。

- (1) 「Interface」→「Traffic Segmentation」を選択します。
- (2) 「Step」リストで「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「Uplink-to-Uplink Mode」を設定します。
- (4) < Apply > ボタンをクリックします。

Interface > Traffic Segmentation

Step:

1. Configure Global

Status

☐ Enabled

Uplink-to-Uplink Mode

Blocking

Apply

Revert

画面 1-49：トラフィックのセグメント化の有効化

アップリンクポートとダウンリンクポートの設定

「Interface」→「Traffic Segmentation」（Configure Session）を選択すると、セグメント化されたグループで使用するダウンリンクポートとアップリンクポートを割り当てることができます。ダウンリンクポートとして指定されたポートは、スイッチのアップリンクポート以外のポートとは通信できません。アップリンクポートは、スイッチの他の任意のポートおよび指定された任意のダウンリンクポートと通信することができます。

関連する CLI 情報

「Configuring Port-based Traffic Segmentation」

コマンドの使用

トラフィックのセグメント化が有効になっている場合、別々のクライアントセッションに割り当てられているアップリンクポートとダウンリンクポートの転送状態は以下のようになります。

宛先セッション 送信元ダウンリンク	Session #1 Downlinks	Session #1 Uplinks	Session #2 Downlinks	Session #2 Uplinks	Normal Ports
Session #1 Downlink Ports	ブロック	転送	ブロック	ブロック	ブロック
Session #1 Uplink Ports	転送	転送	ブロック	ブロック / 転送	転送
Session #2 Downlink Ports	ブロック	ブロック	ブロック	転送	ブロック
Session #2 Uplink Ports	ブロック	ブロック / 転送 **	転送	転送	転送
Normal Ports	転送	転送	転送	転送	転送

** アップリンクポート間の転送状態は、「Configure Global」画面で設定します）。

表 1-4: トラフィックがセグメント化されている場合の転送

Web 設定

インターフェース設定

- ・ トラフィックのセグメント化が無効になっている場合、すべてのポートは、VLAN やスパンニングツリープロトコルなどの他の機能で指定されている設定に基づいて通常の転送モードで動作します。
- ・ ポートをアップリンクリストとダウンリンクリストの両方で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ト化セッションにのみ割り当てることができます。
- ・ ダウンリンクポートが通信できるのは、同じセッションのアップリンクポートのみです。したがって、セッションのアップリンクポートが設定されていない場合、割り当てられているダウンリンクポートは他のいずれのポートとも通信できなくなります。
- ・ セッションのダウンリンクポートが設定されていない場合、割り当てられている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

以下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ト化セッション（範囲：1～4）。
- ・ Direction – 方向をアップリンクとダウンリンクのいずれかに設定して、セグメント化されているグループにインターフェースを追加します（デフォルト：None）。
- ・ Interface – ポートまたはトランクの一覧が表示されます。
 - ・ Port – ポート ID（範囲：1～26）。
 - ・ Trunk – トランク ID（範囲：1～32）。

Web インターフェース

トラフィックセグメント化グループのメンバーを設定するには、以下のようになります。

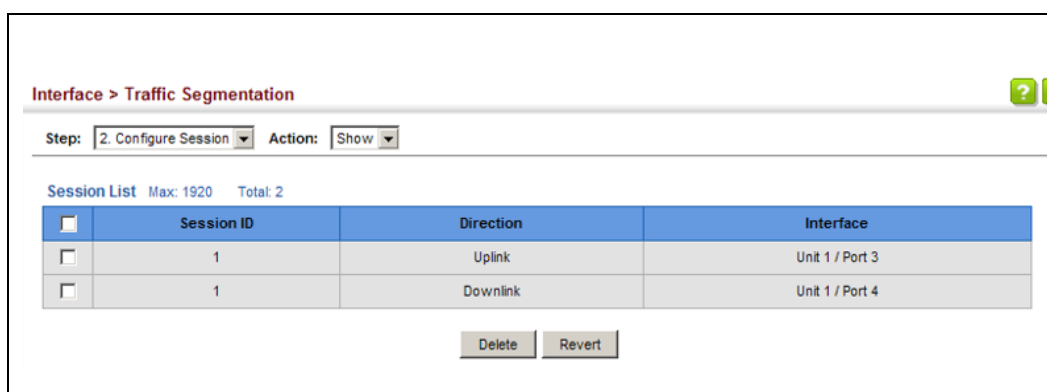
- (1) 「Interface」 → 「Traffic Segmentation」 を選択します。
- (2) 「Step」 リストで 「Configure Session」 を選択します。
- (3) 「Step」 リストで 「Add」 を選択します。
- (4) セッション ID を入力し、アップリンク方向かダウンリンク方向かを設定して、追加するインターフェースを選択します。
- (5) < Apply > ボタンをクリックします。

The screenshot shows the 'Interface > Traffic Segmentation' configuration page. At the top, there's a breadcrumb 'Interface > Traffic Segmentation'. Below it, a 'Step' dropdown is set to '2. Configure Session' and an 'Action' dropdown is set to 'Add'. The main configuration area includes: 'Session ID (1-4)' with a text input field; 'Direction' with a dropdown menu currently showing 'Uplink'; and 'Interface' with two radio buttons: 'Port' (selected) and 'Trunk'. The 'Port' radio button is followed by a dropdown menu showing '1'. The 'Trunk' radio button is followed by a dropdown menu. At the bottom right, there are 'Apply' and 'Revert' buttons.

画面 1-50：トラフィックセグメントのメンバーの設定

トラフィックセグメント化グループのメンバーを表示するには、以下のようにします。

- (1) 「Interface」 → 「Traffic Segmentation」 を選択します。
- (2) 「Step」 リストで 「Configure Session」 を選択します。
- (3) 「Step」 リストで 「Show」 を選択します。



画面 1-51 : トラフィックセグメント化グループのメンバーの表示

1.3.5 VLAN トランキング

「Interface」→「VLAN Trunking」を選択すると、インターフェースを指定して VLAN グループがそのインターフェースを経由できるようにすることができます。

関連する CLI 情報

「vlan-trunking」

コマンドの使用

この機能を使用すると、1つまたは複数の中間スイッチを経由するトンネルを設定して、ある VLAN グループのトラフィックをそのトラフィックが属していない別の VLAN グループに渡すことができます。

以下の図では、スイッチ A とスイッチ B で VLAN 1 と VLAN 2 がそれぞれ設定されており、VLAN トランキングを使用して、それらの VLAN グループのトラフィックがスイッチ C、D、および E を経由して渡されています。

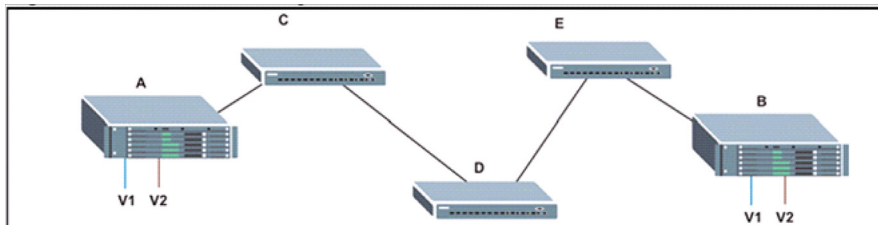


図 1-4: VLAN トランキングの設定

VLAN トランキングを使用しない場合は、すべての中間スイッチ C、D、および E で VLAN 1 と 2 を設定しなければなりません。そのようにしない場合、それらのスイッチでは、不明な VLAN グループタグが含まれているすべてのフレームがドロップされます。ただし、VLAN 1 と 2 を接続するパス上の中間スイッチポートで VLAN トランキングを有効にすることにより、それらの VLAN グループをスイッチ A と B で作成するだけで済むようになります。スイッチ C、D、および E では、VLAN グループタグ 1 と 2（それらのスイッチに対して不明なグループ）を含むフレームが VLAN トランキングポートをパススルーすることが自動的に許可されます。

- ・ スパニングツリーでループが発生しないようにするため、すべての不明な VLAN は、単一のインスタンス（STP/RSTP インスタンスと MSTP のいずれかであり、選択した STA モードによって異なる）宛に送信されます。
- ・ インターフェースで VLAN トランキングとインgress フィルタリングが両方とも無効になっている場合、不明な VLAN タグを含むパケットは、依然としてそのインターフェースに入ることができ、VLAN トランキングが有効になっている他のすべてのポートにフラッドされます（つまり、事実上、不明な VLAN に対して VLAN トランキングが依然として有効になるということです）。

パラメータ

以下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一覧が表示されます。
- ・ Port – ポート ID（範囲：1 ～ 26）。
- ・ Trunk – トランク ID（範囲：1 ～ 32）。
- ・ VLAN Trunking Status – 選択したインターフェースで VLAN トランキングを有効にします。

Web インターフェース

VLAN トランキングをポートまたはトランクで有効にするには、以下のようになります。

- (1) 「Interface」 → 「VLAN Trunking」を選択します。
- (2) 「Port」または「Trunk」を選択してインターフェースタイプを指定します。
- (3) VLAN トランキングを任意のギガビットポートまたはギガビットポートを含むトランクで有効にします。
- (4) < Apply > ボタンをクリックします。

Interface > VLAN Trunking

Interface ☒ Port ☐ Trunk

Port VLAN Trunking List Max: 26 Total: 26 1 2 3

Port	VLAN Trunking Status
1	☒ Enabled
2	☒ Enabled
3	☐ Enabled
4	☐ Enabled
5	☐ Enabled
6	☐ Enabled
7	☐ Enabled
8	☐ Enabled
9	☐ Enabled
10	☐ Enabled

画面 1-52 : VLAN トランキングの設定

1.4 VLAN 設定

本章は、以下のトピックから設定されています。

- ・ IEEE 802.1Q VLAN – スタティック VLAN およびダイナミック VLAN を設定します。
- ・ IEEE 802.1Q トンネリング – QinQ トンネリングを設定して、異なる顧客が同じ内部 VLAN ID を使用する場合でもサービスプロバイダのネットワークで顧客固有の VLAN およびレイヤ 2 プロトコルの設定が保持されるようにします。
- ・ プロトコル VLAN – 指定したプロトコルに基づく VLAN グループを設定します。
- ・ IP サブネット VLAN – 送信元アドレスが IP サブネット –VLAN マッピングテーブルで見つかった場合に、指定された VLAN にタグなしイングレスフレームをマップします。
- ・ MAC ベースの VLAN – 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で見つかった場合に、指定された VLAN にタグなしイングレスフレームをマップします。

1.4.1 IEEE 802.1Q VLAN

大規模ネットワークでは、ルータを使用して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します。本製品は、VLAN を使用して任意のネットワークノードグループを別々のブロードキャストドメインにまとめることにより、同様のサービスをレイヤ 2 で実現します。VLAN を使用すると、ブロードキャストトラフィックが発信元グループに限定されるので、比較的大規模なネットワークでブロードキャストストームが発生するのを防ぐことができます。

また、よりセキュアでクリーンなネットワーク環境を実現することができます。

IEEE 802.1Q VLAN は、ネットワークの任意の場所に配置できるポートグループですが、まるで同じ物理セグメントに属しているように通信します。

VLAN を使用すると、物理接続を変更しなくてもデバイスを新しい VLAN に移動できるので、ネットワーク管理の簡略化に役立ちます。

VLAN は、部署別のグループ（「マーケティング」や「R&D」など）、用途別のグループ（「電子メール」など）、または（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される）マルチキャストグループを示すものとなるように簡単に編成することができます。

VLAN は、ブロードキャストトラフィックを軽減することによって優れたネットワーク効率性を実現します。また、VLAN を使用すると、IP アドレスまたは IP サブネットを更新しなくてもネットワークに変更を加えることができるようになります。VLAN では、トラフィックは、設定されたレイヤ 3 リンクを経由して別の VLAN に到達するので、本質的に、高いレベルのネットワークセキュリティが実現されます。

本製品では、以下の VLAN 機能をサポートしています。

- ・ IEEE 802.1Q 規格に基づく最大 4,093 の VLAN
- ・ 明示的または暗黙のタグ設定と GVRP プロトコルによる複数スイッチにまたがる分散 VLAN 学習
- ・ ポートが複数の VLAN に属することを可能にするポートオーバーラッピング
- ・ 複数の VLAN に属することが可能なエンドステーション

- ・ VLAN 認識デバイスと VLAN 非認識デバイス間のトラフィックの送受信
- ・ 優先度タグの設定

VLAN へのポートの割り当て

スイッチで VLAN を有効にする前に、各ポートをメンバーとなる VLAN グループに割り当てる必要があります。デフォルトでは、すべてのポートが VLAN1 にタグなしポートとして割り当てられます。ポートで 1 つまたは複数の VLAN のトラフィックを伝播するようになるときに、いずれかの中間ネットワークデバイスまたは接続の他端のホストで VLAN をサポートしている場合は、そのポートをタグ付きポートとして追加します。それから、トラフィックを伝播するパス上にある他の VLAN 認識ネットワークデバイスのポートを、手動で、または、GVRP を使用して動的に、同じ VLAN に割り当てます。ただし、本製品のポートが 1 つまたは複数の VLAN のメンバーとなるようにするときに、いずれの中間ネットワークデバイスも接続の他端のホストも VLAN をサポートしていない場合は、そのポートをタグなしのポートとして VLAN に追加してください。

[注意] VLAN タグ付きフレームは、VLAN 認識型または VLAN 非認識型のネットワーク中間デバイスをパススルーすることができますが、VLAN タグ設定をサポートしていないエンドノードホストに渡す場合には、その前に VLAN タグを取り除く必要があります。

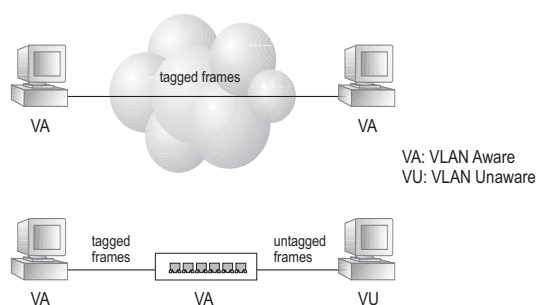


図 1-5: VLAN 対応デバイスと VLAN 非対応デバイス

VLAN クラシフィケーション

スイッチは、フレームを受信すると、2 つの方法のいずれかを使用して分類します。フレームがタグなしの場合、そのフレームは、関連付けられている VLAN（受信ポートのデフォルトの VLAN ID によって識別）に割り当てられます。しかし、フレームがタグ付きの場合には、タグ付きの VLAN ID を使用して、そのフレームのポートブロードキャストドメインが識別されます。

ポートオーバーラッピング

ポートオーバーラッピングを使用すると、異なる VLAN グループでよく共有するファイルサーバやプリンタなどのネットワークリソースにアクセスできるようになります。オーバーラップしない VLAN を実装したが、それらの VLAN と通信する必要がある場合には、本製品でルーティングを有効にすることにより、それらの VLAN を接続することができます。

自動 VLAN 登録

GVRP (GARP VLAN Registration Protocol) は、各エンドステーションが割り当てられるべき VLAN をスイッチが自動的に学習できるシステムを定義します。エンドステーション (または、そのネットワークアダプタ) は、IEEE 802.1Q VLAN プロトコルをサポートしている場合は、メンバーになりたい VLAN グループを示すメッセージをネットワークにブロードキャストするように設定することができます。本製品でそれらのメッセージを受信する場合には、指定された VLAN に受信ポートが自動的に割り当てられてから、メッセージが他のすべてのポートに転送されます。そのメッセージが GVRP をサポートしている他のスイッチで受信されると、そのスイッチも指定された VLAN に受信ポートを割り当て、それから、メッセージを他のすべてのポートに渡します。以上の方法で、VLAN 要件がネットワーク全体に伝搬されます。そのようにすることで、自動的に、エンドステーションの要求のみに基づいて VLAN グループに対する GVRP 対応デバイスが設定できるようにしています。

GVRP をネットワークに実装するには、最初に、(オペレーティングシステムやその他のアプリケーションソフトウェアを使用して) ホストデバイスを必要な VLAN に追加して、それらの VLAN をネットワーク上で伝搬できるようにします。それらのホストデバイスに直接接続されている両方のエッジスイッチ、およびネットワーク内のコアスイッチで、デバイス間のリンクの GVRP を有効にします。また、ネットワーク内のセキュリティ境界を指定してから、境界ポートで GVRP を無効にしてアドバタイズメントが伝搬されないようにするか、それらの境界ポートが制限付き VLAN のメンバーにならないようにしなければなりません。

[注意] 使用するホストデバイスで GVRP をサポートしていない場合は、それらのデバイスに接続しているスイッチポートについてスタティック VLAN またはタグなし VLAN を設定しなければなりません (「VLAN へのスタティックメンバーの追加」の説明を参照)。ただし、さらに、それらのエッジスイッチだけでなく、ネットワーク内のコアスイッチでも GVRP を有効にすることができます。

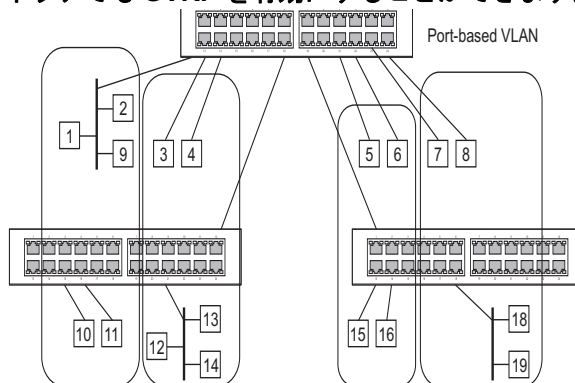


図 1-6: GVRP の使用

タグなし VLAN

VLAN は、一般的に、ブロードキャストトラフィックの削減およびセキュリティの向上のために使用されます。VLAN に割り当てられているネットワークユーザーのグループをメンバーとして、スイッチで設定されている他の VLAN から分離されたブロードキャストドメインが形成されます。パケットは、同じ VLAN に指定されているポート間でのみ転送されます。タグなし VLAN を使用してユーザーグループまたはサブネットを手動で分離することができますが、可能な限り、GVRP を実行する IEEE 802.3 タグ付き VLAN を使用して VLAN 登録が完全に自動化されるようにしてください。

タグ付き / タグなしフレームの転送

単一のスイッチに直接接続されているデバイスについて小規模なポートベースの VLAN を作成する場合は、同じタグなし VLAN にポートを割り当てることができます。

ただし、ポートを複数のスイッチにまたがる VLAN グループのメンバーにするには、そのグループの VLAN を作成し、すべてのポートでタグ設定を有効にしなければなりません。

ポートは複数のタグ付き VLAN またはタグなし VLAN に割り当てることができます。したがって、スイッチの各ポートは、タグ付きまたはタグなしのフレームを渡すことができます。

本製品から VLAN 認識デバイスを含むパスに沿ってフレームを転送する場合は、本製品に VLAN タグを含めなければなりません。本製品から VLAN 認識デバイス（宛先ホストを含む）をまったく含まないパスに沿ってフレームを転送する場合は、最初に本製品で VLAN タグを取り除いてからフレームを転送する必要があります。本製品は、タグ付きフレームを受信すると、フレームタグで示される VLAN にそのフレームを渡します。ただし、VLAN 非認識デバイスからタグなしフレームを受信する場合は、最初にフレームの転送先を判別してから、イングレスポートのデフォルトの VID を示す VLAN タグを挿入します。

VLAN グループの設定

「VLAN」→「Static」（Add）を選択すると、VLAN グループを作成または削除することや、管理ステータスを設定することができます。本製品で使用する 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搬するには、それらのグループのそれぞれの VLAN ID を指定する必要があります。

関連する CLI 情報

「Editing VLAN Groups」

パラメータ

以下のパラメータが表示されます。

- ・ VLAN ID – VLAN または特定の範囲の VLAN の ID（範囲：1 ～ 4,093）。
- ・ VLAN 1 は、デフォルトのタグなし VLAN です。
- ・ Status – 指定した VLAN を有効または無効にします。

Web インターフェース

VLAN グループを作成するには、以下のようになります。

- (1) 「VLAN」→「Static」を選択します。

- (2) 「Step」 リストで「Add」を選択します。
- (3) VLAN ID または ID 範囲を入力します。
- (4) VLAN を稼働状態にするため、「Enabled」チェックボックスをオンにします。
- (5) < Apply > ボタンをクリックします。



画面 1-53 : スタティック VLAN の作成

VLAN へのスタティックメンバーの追加

「VLAN」→「Static」（「Modify VLAN and Member Ports」、「Edit Member by Interface」、または「Edit Member by Interface Range」）を選択すると、選択した VLAN インデックス、インターフェース、またはインターフェース範囲のポートメンバーを設定することができます。ポートメンバーを編集するためのメニューを使用して、動作モード（「Hybrid」または「1Q Trunk」）、デフォルトの VLAN ID（PVID）、受け入れられるフレームタイプ、インGRESS フィルタリングなど、それぞれのインターフェースの VLAN 動作を設定します。ポートは、802.1Q VLAN 対応デバイスに接続されている場合はタグ付きとして割り当て、いかなる VLAN 認識デバイスにも接続されていない場合はタグなしとして割り当てます。あるいは、GVRP を使用してポートが自動的に VLAN に追加されないように、禁止ポートとして設定します。

関連する CLI 情報

「Configuring VLAN Interfaces」

「Displaying VLAN Information」

パラメータ

以下のパラメータが表示されます。

Modify VLAN and Member Ports

- ・ VLAN – 設定済み VLAN の ID（範囲：1 ～ 4,093）。
- ・ VLAN Name – VLAN の名前（1 ～ 32 文字）。
- ・ Status – 指定した VLAN を有効または無効にします。
- ・ Interface – ポートまたはトランクの一覧が表示されます。
- ・ Port – ポート ID（範囲：1 ～ 26）。
- ・ Trunk – トランク ID（範囲：1 ～ 32）。

- ・ Mode – インターフェースの VLAN メンバーシップモードを示します（デフォルト：Hybrid）。
 - ・ Access – タグなしインターフェースとして動作するようにポートを設定します。ポートは、タグなしフレームをシングル VLAN でのみ送受信します。
 - ・ アクセスモードは VLAN トランキングと相互排他です（「VLAN トランキング」を参照）。インターフェースで VLAN トランキングが有効になっている場合、そのインターフェースをアクセスモードに設定することはできません。反対に、インターフェースで VLAN トランキングが無効になっている場合は、そのインターフェースをアクセスモードに設定することができます。
 - ・ Hybrid – ハイブリッド VLAN インターフェースを指定します。ポートでは、タグ付きフレームが送信されることも、タグなしフレームが送信されることもあります。
 - ・ 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 つのスイッチ間のダイレクトリンクであるため、ポートでは、送信元 VLAN を特定するタグ付きフレームが送信されます。ただし、ポートのデフォルト VLAN（つまり、PVID に関連付けられている VLAN）に属するフレームもタグ付きフレームとして送信されることに注意してください。
- ・ PVID – インターフェースで受信されるタグ付きフレームに割り当てられている VLAN ID（デフォルト：1）。アクセスモードを使用している場合にインターフェースが新しい VLAN に割り当てられると、自動的に、そのインターフェースの PVID が新しい VLAN の ID に設定されます。ハイブリッドモードを使用している場合、インターフェースの PVID は、そのインターフェースがタグなしメンバーである任意の VLAN の ID に設定することができます。
- ・ Acceptable Frame Type – タグ付きまたはタグなしフレームを含め、すべてのフレームタイプを受け入れるように、あるいは、タグ付きフレームのみを受け入れるようにインターフェースを設定します。
- ・ すべてのフレームタイプを受信するように設定すると、受信されたすべてのタグなしフレームはデフォルトの VLAN に割り当てられます（オプション：All または Tagged、デフォルト：All）。
- ・ Ingress Filtering – イングレスポートがメンバーではない VLAN のタグが付けられているフレームを処理する方法を指定します（デフォルト：Disabled）。
 - ・ イングレスフィルタリングはタグ付きフレームのみに影響します。
 - ・ イングレスフィルタリングが無効になっており、ポートで、そのポートがメンバーではない VLAN のタグが付けられているフレームを受信すると、それらのフレームは他のすべてのポート（そのポートで明示的に禁止されている VLAN のポートを除く）にフラッドされます。
 - ・ イングレスフィルタリングが有効になっており、ポートで、そのポートがメンバーではない VLAN のタグが付けられているフレームを受信すると、それらのフレームは破棄されます。
 - ・ イングレスフィルタリングは、GVRP や STP などのような VLAN に依存しない BPDU フレームには影響しません。ただし、GMRP などのような VLAN に依存する BPDU フレームには影響します。
- ・ Membership Type – 該当のポートまたはトランクのラジオボタンを選択して、インターフェースごとの VLAN メンバーを指定します。
 - ・ Tagged: インターフェースが VLAN のメンバーとなっています。ポートで送信されるすべてのパケットにタグが付けられる（つまり、タグが伝播される）ので、VLAN または CoS 情報が伝播されます。
 - ・ Untagged: インターフェースが VLAN のメンバーとなっています。ポートで送信されるすべてのパケットにタグが付けられない（つまり、タグが伝播されない）ので、VLAN または CoS 情報は伝播されません。インターフェースは少なくとも 1 つのグループにタグなしポートとして割り当てられなければならないので注意してください。
 - ・ Forbidden: インターフェースが GVRP を使用して自動的に VLAN に追加されないようにします。詳細については、「自動 VLAN 登録」を参照してください。

- ・ None: インターフェースは VLAN のメンバーではありません。この VLAN に関連付けられているパケットはインターフェースで送信されません。

【注意】 VLAN 1 は、スイッチのすべてのポートを含むデフォルトのタグなし VLAN であり、メンバーシップタイプは、最初にポートを他の VLAN に割り当ててからデフォルトのポート VLAN ID を再割り当てするという方法でのみ、変更することができます。

Edit Member by Interface

パラメータは、すべて、上記の「Modify VLAN and Member Ports」セクションで説明されているものと同じです。

Edit Member by Interface Range

パラメータは、以下に記載されているもの以外は、すべて、上記の「Modify VLAN and Member Ports」セクションで説明されているものと同じです。

- ・ Port Range - ポートの一覧が表示されます（範囲：1 ～ 26）。
- ・ Trunk Range - トランクの一覧が表示されます（範囲：1 ～ 32）。

【注意】 指定範囲内のインターフェースごとの PVID、受け入れ可能なフレームタイプ、およびイングレスフィルタリングを「Modify VLAN and Member Ports」画面と「Edit Member by Interface」画面のいずれかで設定する必要があります。

Web インターフェース

スタティックメンバーを VLAN インデックス別に設定するには、以下のようにします。

- (1) 「VLAN」 → 「Static」を選択します。
- (2) 「Step」リストで「Modify VLAN and Member Ports」を選択します。
- (3) 表示されるインターフェースタイプを「Port」または「Trunk」に設定します。
- (4) 任意のインターフェースの設定を必要に応じて変更します。「Membership Type」はインターフェースが他の VLAN に追加されて PVID が 1 以外に変更されるまで変更できないということに留意してください。
- (5) < Apply > ボタンをクリックします。

VLAN > Static

Action: Edit Member by VLAN

VLAN: 1

Interface: ☒ Port ☐ Trunk

Static VLAN Port Member List Max: 26 Total: 26

Port	Mode	PVID	Acceptable Frame Type	Ingress Filtering	Membership Type			
					Tagged	Untagged	Forbidden	None
1	Hybrid	1	All	☐ Enabled	☐	☒	☐	☐
2	Hybrid	1	All	☐ Enabled	☐	☒	☐	☐
3	Hybrid	1	All	☐ Enabled	☐	☒	☐	☐
4	Hybrid	1	All	☐ Enabled	☐	☒	☐	☐
5	Hybrid	1	All	☐ Enabled	☐	☒	☐	☐

画面 1-54 : スタティックメンバーの VLAN インデックス別の設定

スタティックメンバーをインターフェース別に設定するには、以下のようになります。

- (1) 「VLAN」 → 「Static」 を選択します。
- (2) 「Step」 リストで 「Edit Member by Interface」 を選択します。
- (3) 設定するポートまたはトランクを選択します。
- (4) 任意のインターフェースの設定を必要に応じて変更します。
- (5) < Apply > ボタンをクリックします。

VLAN > Static

Action: Edit Member by Interface

Interface: ☒ Port 9 ☐ Trunk

Mode: Hybrid

PVID: 2

Acceptable Frame Type: All

Ingress Filtering: ☐ Enabled

Static VLAN Membership List Max: 4093 Total: 4

VLAN	Membership Type			
	Tagged	Untagged	Forbidden	None
1	☐	☒	☐	☐
2	☐	☒	☐	☐
3	☐	☐	☐	☒
4	☐	☐	☐	☒

Apply Revert

画面 1-55 : スタティック VLAN メンバーのインターフェース別の設定

スタティックメンバーをインターフェース範囲別に設定するには、以下のようになります。

- (1) 「VLAN」 → 「Static」 を選択します。

- (2) 「Step」 リストで「Edit Member by Interface Range」を選択します。
- (3) 表示されるインターフェースタイプを「Port」または「Trunk」に設定します。
- (4) インターフェース範囲を入力します。
- (5) VLAN パラメータを必要に応じて変更します。指定範囲内のインターフェースごとの PVID、受け入れ可能なフレームタイプ、およびイングレスフィルタリングを「Edit Member by VLAN」画面と「Edit Member by Interface」画面のいずれかで設定する必要があるということに留意してください。
- (6) < Apply > ボタンをクリックします。

VLAN > Static

Action: Edit Member by Interface Range

Interface ☒ Port ☐ Trunk

Port Range (1-28) -

Mode Hybrid

VLAN ID (1-4093) -

Membership Type ☐ Tagged ☒ Untagged ☐ Forbidden ☐ None

Apply Revert

画面 1-56 : スタティック VLAN メンバーのインターフェース範囲別の設定

ダイナミック VLAN 登録の設定

「VLAN」→「Dynamic」を選択すると、スイッチで GVRP をグローバルに有効にすることや、GVRP を有効にしてからインターフェースごとにプロトコルタイマーを調整することができます。

関連する CLI 情報

「GVRP and Bridge Extension Commands」

「Configuring VLAN Interfaces」

パラメータ

以下のパラメータが表示されます。

Configure General

- ・ GVRP Status

GVRP は、ネットワーク全体のポートで VLAN メンバーを登録するためにスイッチで VLAN 情報を交換する方法を定義します。VLAN は、ホストデバイスが発行する join メッセージに基づいて動的に設定され、ネットワーク全体に伝搬されます。自動

VLAN 登録が許可されるようにするため、また、ローカルスイッチ外部の VLAN がサポートされるようにするため、GVRP を有効にする必要があります（デフォルト：Disabled）。

Configure Interface

- ・ Interface – ポートまたはトランクの一覧が表示されます。
- ・ Port – ポート ID（範囲：1 ～ 26）。
- ・ Trunk – トランク ID（範囲：1 ～ 32）。
- ・ GVRP Status – インターフェースの GVRP を有効または無効にします。この設定を有効にするには、スイッチの GVRP をグローバルに有効にする必要があります（「Configure General」画面を使用）。無効にすると、このポートで受信されたあらゆる GVRP パケットが破棄され、GVRP 登録情報が他のポートから伝搬されなくなります（デフォルト：Disabled）。
- ・ GVRP は、アクセスモードに設定されているポートでは有効にすることはできません（「VLAN へのスタティックメンバーの追加」を参照）。
- ・ GVRP Timers – タイマーは、次の原則に従って設定してください。
 - ・ 2 x (Join タイマー) < Leave タイマー < LeaveAll タイマー
 - ・ Join – VLAN グループのメンバーとして登録されるために要求または問い合わせを送信する間隔（範囲：20 ～ 1,000 cs、デフォルト：20 cs）。
 - ・ Leave – ポートが VLAN グループから登録解除されるまでの時間。「Join」の 2 倍よりも長い時間を設定する必要があります。そのようにすることで、Leave メッセージまたは LeaveAll メッセージが発行された後、ポートが実際にグループから登録解除される前にアプリケーションで再登録を実行できるようになります（範囲：60 ～ 3,000 cs、デフォルト：60 cs）。
 - ・ LeaveAll – VLAN グループのメンバーの LeaveAll 問い合わせメッセージが送信されてからポートがグループから登録解除されるまでの時間。グループに再登録されるノードによって生成されるトラフィックの量を最小限に抑えるため、この時間は「Leave」よりもかなり長くする必要があります（範囲：500 ～ 18,000 cs、デフォルト：1,000 cs）。

Show Dynamic VLAN - VLAN を表示します。

- ・ VLAN ID – このスイッチが GVRP を使用してメンバーとなった VLAN の ID。
- ・ VLAN Name – このスイッチが GVRP を使用してメンバーとなった VLAN の名前。
- ・ Status – この VLAN が、現在、稼働状態かどうかを示します（表示値：Enabled または Disabled）。

Show Dynamic VLAN - VLAN のメンバーを表示します。

- ・ VLAN – このスイッチが GVRP を使用してメンバーとなった VLAN の ID。
- ・ Interface – 選択した VLAN に GVRP を使用してメンバーとなったポートまたはトランクの一覧が表示されます。

Web インターフェース

スイッチで GVRP を設定するには、以下のようにします。

- (1) 「VLAN」 → 「Dynamic」 を選択します。
- (2) 「Step」 リストで 「Configure General」 を選択します。
- (3) GVRP を有効または無効にします。
- (4) < Apply > ボタンをクリックします。

VLAN > Dynamic

Step: 1. Configure General

GVRP Status ☒ Enabled

Apply Revert

画面 1-57 : GVRP のグローバルステータスの設定

ポートまたはトランクで GVRP ステータスおよびタイマーを設定するには、以下のようにします。

- (1) 「VLAN」 → 「Dynamic」 を選択します。
- (2) 「Step」 リストで 「Configure Interface」 を選択します。
- (3) 表示されるインターフェースタイプを 「Port」 または 「Trunk」 に設定します。
- (4) 任意のインターフェースの GVRP ステータスまたはタイマーを変更します。
- (5) < Apply > ボタンをクリックします。

VLAN > Dynamic

Step: 2. Configure Interface

Interface ☒ Port ☐ Trunk

Port List Max: 26 Total: 26

Port	GVRP Status	GARP Timer (centiseconds)		
		Join (20-1000)	Leave (60-3000)	LeaveAll (500-18000)
1	☐ Enabled	20	60	1000
2	☐ Enabled	20	60	1000
3	☒ Enabled	20	60	1000
4	☐ Enabled	20	60	1000
5	☐ Enabled	20	60	1000

画面 1-58 : インターフェースの GVRP の設定

スイッチがメンバーとなっているダイナミック VLAN を表示するには、以下のようになります。

- (1) 「VLAN」 → 「Dynamic」 を選択します。
- (2) 「Step」 リストで 「Show Dynamic VLAN」 を選択します。
- (3) 「Step」 リストで 「Show VLAN」 を選択します。

VLAN > Dynamic

Step: 3. Show Dynamic VLAN Action: Show VLAN

Dynamic VLAN List Max: 4093 Total: 2

VLAN ID	VLAN Name	Status
120		Enabled
150		Enabled

画面 1-59 : スイッチで登録されているダイナミック VLAN の表示

ダイナミック VLAN のメンバーを表示するには、以下のようになります。

- (1) 「VLAN」 → 「Dynamic」 を選択します。
- (2) 「Step」 リストで 「Show Dynamic VLAN」 を選択します。
- (3) 「Step」 リストで 「Show VLAN Members」 を選択します。

VLAN > Dynamic

Step: 3. Show Dynamic VLAN Action: Show VLAN Member

VLAN 120

Dynamic VLAN Member List Max: 64 Total: 10

Interface
Unit 1 / Port 1
Unit 1 / Port 4
Unit 1 / Port 10
Unit 1 / Port 16
Unit 1 / Port 19

画面 1-60 : ダイナミック VLAN のメンバーの表示

1.4.2 IEEE 802.1Q トンネリング

IEEE 802.1Q トンネリング (QinQ) は、自社のネットワークで複数の顧客のトラフィックを伝播するサービスプロバイダを対象としています。QinQ トンネリングを使用して、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 プロトコルの設定が保持されるようにします。そのようなことを実現するため、顧客のフレームがサービスプロバイダのネットワークに入るときに SPVLAN (Service Provider VLAN) タグを挿入し、フレームがネットワークを出るときに SPVLAN タグを取り除きます。

サービスプロバイダの顧客には、自身の内部 VLAN ID およびサポートする VLAN の数に関して固有の要件があるものと思われます。しかし、同じサービスプロバイダネットワーク内の別々の顧客にとって必要な VLAN 範囲を簡単にオーバーラップさせたり、インフラストラクチャを使用して渡されるトラフィックを混合させたりすることが可能な場合もあります。

それぞれの顧客に固有の範囲の VLAN ID を割り当てると、顧客設定が制限され、VLAN マッピングの集中処理が必要になり、VLAN が容易に上限数である 4,096 を超える可能性があります。

QinQ トンネリングでは、複数の VLAN をもっている顧客に単一の SPVLAN (Service Provider VLAN) を使用します。別々の顧客が同じ顧客別 VLAN ID を使用しても、サービスプロバイダのネットワーク内で顧客の VLAN ID が保持され、それらの顧客からのトラフィックは分離され転送されます。QinQ トンネリングでは、VLAN 内 VLAN 階層を使用し、顧客の元のタグ付きパケットを保持して、SPVLAN タグを各フレームに追加すること (「ダブルタギング」ともいう) により、VLAN 領域を拡大します。

QinQ トンネリングをサポートするように設定されているポートは、トンネルポートモードに設定する必要があります。顧客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ときに使用するエッジスイッチの QinQ トンネルアクセスポートに個々の顧客の SPVLAN ID を割り当てます。顧客ごとに別々の SPVLAN が必要ですが、その SPVLAN で顧客の内部 VLAN 全部をサポートします。トラフィックをエッジスイッチからサービスプロバイダのネットワークに渡す 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。このアップリンクポートを複数の SPVLAN に追加して、サービスプロバイダのネットワークで別々の顧客のインバウンドトラフィックを伝播することができます。

二重タグ付き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スイッチ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の別のトランクポートから出る際に同じ SPVLAN タグが再び付加されます。

パケットがサービスプロバイダのエグレススイッチのトランクポートに入ると、同様に、パケット処理のために外部タグが取り除かれます。ただし、パケットがエッジスイッチ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出される際に SPVLAN タグが付加されません。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る元の VLAN 番号が保持されます。

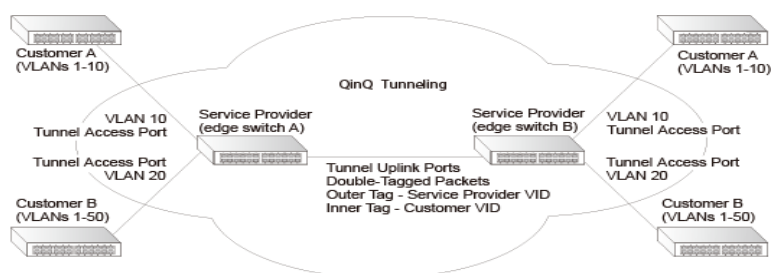


図 1-7: QinQ の運用概念

QinQ トンネルポートでは、タグ付きパケットとタグなしパケットのどちらかが受信されます。着信パケットは、そのタグの数に関係なく、タグ付きパケットとして処理されます。

イングレスプロセスで、ソースルックアップと宛先ルックアップが実行されます。両方のルックアップが正常に完了すると、パケットがメモリに書き込まれます。それから、エグレスプロセスによってパケットが送信されます。QinQ トンネルポートに入るパケットは、以下の方法で処理されます。

SPVLAN タグが SPVLAN インターフェース上のすべてのアウトバウンドパケットに追加されます（それらのパケットに既にタグがいくつかあっても関係ありません）。SPVLAN（外部）タグは、「SPVLAN マッピングエントリに対する CVLAN の作成」で説明されているように定義されていない限り、デフォルトの VLAN ID とタグプロトコル ID（TPID、つまり、イーサタイプのタグ）に基づいて、イングレスプロセスで作成されてパケットに挿入されます。パケットがタグ付きまたは優先度タグ付きのパケットである場合は、内部タグの優先度が外部タグにコピーされます。

1. ソースルックアップと宛先ルックアップが正常に完了すると、イングレスプロセスによって2つのタグが付けられてパケットがスイッチングプロセスに送信されます。着信パケットがタグなしの場合、外部タグは SPVLAN タグであり、内部タグはダミータグ (8100 0000) です。着信パケットがタグ付きの場合、外部タグは SPVLAN タグであり、内部タグは CVLAN タグです。
2. スwitchングプロセスによるパケット分類の後、1つ (外部タグ) または2つ (外部タグと内部タグの両方) のタグと共にパケットがメモリに書き込まれます。
3. スイッチがパケットを適切なエグレスポートに送信します。
4. エグレスポートが SPVLAN のタグなしメンバーである場合は、外部タグが取り除かれます。タグ付きのメンバーである場合は、発信パケットのタグは2つになります。

トンネルアップリンクポートで受信されるパケットのレイヤ2におけるフローアップリンクポートで以下のいずれかのパケットが受信されます。

- ・ タグなし
- ・ シングルタグ (CVLAN または SPVLAN)
- ・ ダブルタグ (CVLAN と SPVLAN の両方)

イングレスプロセスで、ソースルックアップと宛先ルックアップが実行されます。両方のルックアップが正常に完了すると、パケットがメモリに書き込まれます。それから、エグレスプロセスによってパケットが送信されます。QinQ アップリンクポートに入るパケットは、以下の方法で処理されます。

1. 着信パケットがタグなしの場合、PVID VLAN ネイティブタグが付加されます。
2. 着信パケット (シングルタグ付きまたはダブルタグ付き) のイーサタイプがアップリンクポートの TPID と一致しない場合、VLAN タグは CVLAN (Customer VLAN) タグとみなされます。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付加されます。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の学習とスイッチングに使用されます。TPID は、ポート別に設定する必要があり、妥当性検証を無効にすることはできません。
3. 着信パケット (シングルタグ付きまたはダブルタグ付き) のイーサタイプがアップリンクポートの TPID と一致しない場合、新しい VLAN タグは付加されません。アップリンクポートが着信パケットの外部 VLAN のメンバーでない場合、イングレスフィルタリングが有効になっていると、パケットがドロップされます。イングレスフィルタリングが有効になっていなければ、パケットはそのまま転送されます。VLAN が VLAN テーブルに含まれていない場合、パケットはドロップされます。
4. ソースルックアップと宛先ルックアップが正常に完了すると、パケットにダブルタグが付けられます。スイッチでは、0x8100 である TPID を使用して、着信パケットがダブルタグ付きであることを示します。ダブルタグ付き着信パケットの外部タグがポート TPID と一致し、内部タグが 0x8100 である場合、そのパケットはダブルタグ付きパケットとして処理されます。シングルタグ付きパケットの TPID が 0x8100 であり、ポートの TPID が 0x8100 ではない場合は、新しい VLAN タグが付加され、やはり、ダブルタグ付きパケットとして処理されます。
5. 宛先アドレスルックアップが失敗した場合、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、シングルタグ付きパケットまたはダブルタグ付きパケットとして処理されるため、メモリに書き込まれます。
7. スイッチがパケットを適切なエグレスポートに送信します。
8. エグレスポートが SPVLAN のタグなしメンバーである場合は、外部タグが取り除かれます。タグ付きのメンバーである場合は、発信パケットのタグは 2 つになります。

QinQ に関する設定上の制限事項

- ・ アップリンクポートのネイティブ VLAN は、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、そのアップリンクポートは SPVLAN のタグなしメンバーになります。そのため、外部 SPVLAN タグがパケットの送出時に取り除かれます。もう 1 つの理由として、顧客のパケット以外のパケットが SPVLAN に転送されるようになることが挙げられます。
- ・ スタティックトランクポートグループは、QinQ 設定がトランクポート内で一貫している限り、QinQ トンネルポートに対応します。
- ・ ネイティブ VLAN (VLAN 1) は、通常、送信フレームには付加されません。
- ・ 設定エラーによるリスクの軽減のために VLAN 1 を顧客トラフィックの SPVLAN タグとして使用しないようにしてください。その代わりに、VLAN 1 をデータ VLAN ではなく管理 VLAN としてサービスプロバイダネットワークで使用してください。
- ・ レイヤ 2 スイッチングとレイヤ 3 スイッチングには以下のような特性的な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 の QoS (Quality of Service) とレイヤ 3 情報を含むその他の QoS 機能は、トンネルポートでサポートされていません。
 - ・ スパニングツリーの BPDU (Bridge Protocol Data Unit) フィルタリングはトンネルポートでは自動的に無効になります。

QinQ に関する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 TPID (Tag Protocol Identifier) 値を設定します (「Ethernet Type」フィールドを使用)。このステップは、接続先クライアントで 802.1Q タグ付きフレームの識別に非標準の 2 bytes のイーサタイプを使用している場合に実行する必要があります。デフォルトのイーサタイプ値は 0x8100 です (「QinQ トンネリングの有効化」を参照)。
2. SPVLAN (Service Provider VLAN) を作成します (「VLAN グループの設定」を参照)。
3. QinQ トンネルアクセスポートを「Access」モードに設定します (「QinQ トンネルへのインターフェースの追加」を参照)。
4. タグなしメンバーとして SPVLAN に登録されるように QinQ トンネルアクセスポートを設定します (「VLAN へのスタティックメンバーの追加」を参照)。
5. QinQ トンネルアクセスポートで SPVLAN ID をネイティブ VID として設定します (「VLAN へのスタティックメンバーの追加」を参照)。
6. QinQ トンネルアップリンクポートを「Uplink」モードに設定します (「QinQ トンネルへのインターフェースの追加」を参照)。

7. タグ付きメンバーとして SPVLAN に登録されるように QinQ トンネルアップリンクポートを設定します（「VLAN へのスタティックメンバーの追加」を参照）。

スイッチの QinQ トンネリングの有効化

「VLAN」→「Tunnel」（Configure Global）を選択すると、IEEE 802.1Q（QinQ）トンネリングモードで動作するようにスイッチを設定することができます。このトンネリングモードは、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経路でレイヤ2トラフィックを渡すために使用されます。また、接続先クライアントで 802.1Q タグ付きフレームの識別に非標準の 2 bytes のイーサタイプを使用している場合は、トンネルポートのタグプロトコル ID（TPID）値をグローバル設定することもできます。

関連する CLI 情報

「Configuring IEEE 802.1Q Tunneling」

パラメータ

以下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 ID（TPID）は、トンネルポートの着信パケットのイーサタイプを指定します（範囲：16 進数の 0800 ～ 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 のカスタムの 802.1Q イーサタイプ値を設定します。この機能を使用すると、802.1Q タグ付きフレームの識別に標準の 0x8100 イーサタイプを使用しないサードパーティ製スイッチとの互換性を確保できるようになります。例えば、トランクポートでカスタムの 802.1Q イーサタイプとして 0x1234 が設定されている場合、そのイーサタイプを含んでいる着信フレームは、イーサタイプフィールドの直後のタグに含まれている VLAN に割り当てられます。なぜならば、その VLAN には標準の 802.1Q トランクが含まれているものと考えられるからです。ポートで受信されるフレームが他のイーサタイプを含んでいる場合は、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 に割り当てられます。
 - ・ 指定したイーサタイプが「Uplink」モードに設定されているポートのみに適用されます（「QinQ トンネルへのインターフェースの追加」を参照）。ポートが「Normal」モードの場合、TPID は常に 8100 です。ポートが「Access」モードの場合、受信されたパケットはタグなしパケットとして処理されます。

Web インターフェース

スイッチで QinQ トンネリングを有効にするには、以下のようになります。

- (1) 「VLAN」→「Tunnel」を選択します。
- (2) 「Step」リストで「Configure Global」を選択します。
- (3) 「Tunnel Status」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で 802.1Q タグ付きフレームの識別に非標準イーサタイプを使用している場合は、TPID を指定します。
- (4) < Apply > ボタンをクリックします。

VLAN > Tunnel

Step: 1. Configure Global ▼

Tunnel Status ☐ Enabled

Ethernet Type

(800-FFFF, hexadecimal value)

画面 1-61 : QinQ トンネリングの有効化

SPVLAN マッピングエントリに対する CVLAN の作成

「VLAN」→「Tunnel」（Configure Service）を選択すると、SPVLAN マッピングエントリに対する CVLAN を作成することができます。

関連する CLI 情報

「switchport dot1q-tunnel service match cvid」

コマンドの使用

- ・ サービスプロバイダのエッジルータに入る顧客パケットの内部 VLAN タグは、トラフィックを 802.1Q トンネル経由で伝播するサービスプロバイダ VLAN を示す外部タグにマップされます。デフォルトでは、外部タグはエッジルータのイングレスポートのデフォルトの VID に基づいて設定されます。このプロセスは、「IEEE 802.1Q トンネリング」で説明されているように、透過的に実行されます。
- ・ 優先度ビットが内部タグで検出された場合は、それらも外部タグにコピーされます。そのようにすることで、サービスプロバイダが、トンネル全体にわたって、中間ノードで、指定されている優先度と適切なキュー管理方式に基づいてサービスを区別できるようになります。
- ・ 標準サービスパスおよび優先度キューイングに依存せずに、QinQ VLAN マッピングを使用して、指定したインバウンド顧客 VLAN からのトラフィックについて、サービスプロバイダのネットワークを横断する区分化されたサービス経路セットを定義することにより、サービスを強化できます。
- ・ すべての顧客インターフェースはアクセスインターフェース（つまり、ユーザからネットワークへのインターフェース）として設定し、サービスプロバイダインターフェースはアップリンクインターフェース（つまり、ネットワークからネットワークへのインターフェース）として設定しなければならないので注意してください。次のセクションで説明する「Configure Interface」画面を使用して、インターフェースをアクセスモードまたはアップリンクモードに設定してください。

パラメータ

以下のパラメータが表示されます。

- ・ Port – ポート ID（範囲：1 ～ 26）。
- ・ Customer VLAN ID – 内部 VLAN タグの VLAN ID（範囲：1 ～ 4,094）。
- ・ Service VLAN ID – 外部 VLAN タグの VLAN ID（範囲：1 ～ 4,093）。

Web インターフェース

マッピングエントリを設定するには、以下のようにします。

- (1) 「VLAN」→「Tunnel」を選択します。
- (2) 「Step」リストで「Configure Service」を選択します。
- (3) 「Step」リストで「Add」を選択します。
- (4) 「Port」リストでインターフェースを選択します。
- (5) 指定したポートから送出されるパケットの CVID と SVID のマッピングを指定します。

(6) < Apply > ボタンをクリックします。

VLAN > Tunnel

Step: 2. Configure Service Action: Add

Port 1

Customer VLAN ID (1-4094) 2

Service VLAN ID (1-4093) 99

Apply Revert

画面 1-62 : SPVLAN マッピングエントリに対する CVLAN の設定

マッピングテーブルを表示するには、以下のようにします。

- (1) 「VLAN」 → 「Tunnel」 を選択します。
- (2) 「Step」 リストで 「Configure Service」 を選択します。
- (3) 「Step」 リストで 「Show」 を選択します。
- (4) 「Port」 リストで インターフェース を選択します。

VLAN > Tunnel

Step: 2. Configure Service Action: Show

Port 1

Tunnel Service Subscriptions List Total: 2

	Customer VLAN ID	Service VLAN ID
☐	1	1
☐	2	200

Delete Revert

画面 1-63 : SPVLAN マッピングエントリに対する CVLAN の表示

この例では、パケットの CVID が「2」の場合にポート 1 から送出されるエグレスパケットの外部タグで SVID が「200」に設定されています。詳細な例については、switchport dot1q-tunnel service match cidv コマンドの説明を参照してください。

QinQ トンネルへのインターフェースの追加

以降に記載するガイドラインに従って、スイッチで QinQ トンネルをセットアップします。それから、「VLAN」→「Tunnel」（Configure Interface）を選択して、該当のインターフェースのトンネルモードを設定します。

関連する CLI 情報

「Configuring IEEE 802.1Q Tunneling」

コマンドの使用

- トンネル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、「Configure Global」画面でスイッチを「QinQ」モードに設定します（「スイッチの QinQ トンネリングの有効化」を参照）。また、接続先クライアントで 802.1Q タグ付きフレームの識別に非標準の 2 bytes のイーサタイプを使用している場合は、トンネルポートのタグプロトコル ID（TPID）値も設定します。
- 「Configure Interface」画面で、エッジスイッチのアクセスインターフェースを「Tunnel」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しているスイッチでアップリンクインターフェースを「Tunnel Uplink」モードに設定します。

パラメータ

以下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一覧が表示されます。
- Port – ポート ID（範囲：1 ～ 26）。
- Trunk – トランク ID（範囲：1 ～ 32）。
- Mode – ポートの VLAN メンバシップモードを設定します。
 - None – ポートが通常の VLAN モードで動作します（デフォルト）。
 - Access – サービスプロバイダネットワークを経由するトラフィックを分離して顧客 VLAN ID を保持するため、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ます。
 - Uplink – サービスプロバイダネットワーク内の他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 インターフェース

インターフェースを QinQ トンネルに追加するには、以下のようになります。

- 「VLAN」→「Tunnel」を選択します。
- 「Step」リストで「Configure Interface」を選択します。
- 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のモードを「Uplink」に設定します。
- < Apply > ボタンをクリックします。

VLAN > Tunnel ?

Step: 2. Configure Interface ▼

Interface ☒ Port ☐ Trunk

802.1Q Tunnel Port List Total: 26 1 2 3

Port	Mode
1	Uplink ▼
2	Access ▼
3	None ▼
4	None ▼
5	None ▼
6	None ▼
7	None ▼
8	None ▼
9	None ▼
10	None ▼

画面 1-64 : QinQ トンネルへのインターフェースの追加

1.4.3 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、容易に共通の VLAN にグループ化することはできません。そのためには、特定のプロトコルを使用するすべてのデバイスを取り込むために別々の VLAN 間でトラフィックを渡す非標準デバイスが必要になる場合があります。この種の設定では、セキュリティやアクセスの容易性といった、ユーザにとっての VLAN の基本的なメリットが損なわれます。

そのような問題を回避するため、物理ネットワークに必要なプロトコルごとの論理 VLAN グループに分割するプロトコルベースの VLAN を使用するように本製品を設定することができます。フレームがポートで受信されると、インバウンドパケットで使用されているプロトコルタイプに基づいて、そのフレームがどの VLAN に属しているかを判別することができます。

コマンドの使用

- ・ プロトコルベースの VLAN を設定するには、以下のようにします。
 1. 最初に、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、ネットワークで実行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。

この時点ではポートメンバーを追加しないでください。
 2. 「Configure Protocol」(Add) 画面で、VLAN に割り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. 「Configure Interface」(Add) 画面で、各インターフェースのプロトコルを該当の VLAN にマップします。
- ・ MAC ベースの VLAN、IP サブネットベースの VLAN、およびプロトコルベースの VLAN が同時にサポートされる場合、優先順位は、MAC ベース、IP サブネットベース、プロトコルベースの順になり、ポートベースが最後になります。

プロトコル VLAN グループの設定

「VLAN」→「Protocol」(Configure Protocol - Add) を選択すると、プロトコルグループを作成することができます。

関連する CLI 情報

「protocol-vlan protocol-group (Configuring Groups)」

パラメータ

以下のパラメータが表示されます。

- ・ Frame Type - プロトコルで使用するフレームタイプとして、「Ethernet」、「RFC 1042」、または「LLC Other」を選択します。
- ・ Protocol Type - 該当するプロトコルタイプを指定します。指定可能なオプションは、「IP」、「ARP」、「RARP」、および「IPv6」です。「LLC Other」を「Frame Type」として選択した場合、「Protocol Type」で指定可能なオプションは「IPX Raw」のみです。
- ・ Protocol Group ID - プロトコル LAN グループに割り当てられるプロトコルグループ ID (範囲: 1 ~ 2,147,483,647)。

〔注意〕 IP プロトコルイーサネットフレームに対応するトラフィックは、スイッチの管理 IP を指定して設定された VLAN（VLAN 1）にマップされます。IP プロトコルイーサネットトラフィックは他の VLAN にマップしないでください。マップすると、スイッチに対する管理ネットワーク接続が失われます。そのような方法で接続が失われた場合は、コンソールを使用して、問題の原因となっているプロトコル VLAN ルールを削除することにより、再びアクセスが可能になります。あるいは、スイッチをパワーサイクルすることもできますが、その場合、未保存の設定変更が失われます。

Web インターフェース

プロトコルグループを設定するには、以下のようにします。

- (1) 「VLAN」 → 「Protocol」 を選択します。
- (2) 「Step」 リストで 「Configure Protocol」 を選択します。
- (3) 「Step」 リストで 「Add」 を選択します。
- (4) 「Frame Type」 リストで項目を選択します。
- (5) 「Protocol Type」 リストで項目を選択します。
- (6) プロトコルグループの ID を入力します。
- (7) < Apply > ボタンをクリックします。

VLAN > Protocol

Step: 1. Configure Protocol Action: Add

Frame Type Ethernet

Protocol Type 08 06 (ARP)

Protocol Group ID (1-2147483647) 1

Apply Revert

画面 1-65 : 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、以下のようにします。

- (1) 「VLAN」 → 「Protocol」 を選択します。
- (2) 「Step」 リストで 「Configure Protocol」 を選択します。

(3) 「Step」 リストで「Show」を選択します。

VLAN > Protocol

Step: 1. Configure Protocol Action: Show

Protocol to Group Mapping Table Max: 20 Total: 1

	Frame Type	Protocol Type	Protocol Group ID
☐	Ethernet	08 06	1

Delete Revert

画面 1-66 : プロトコル VLAN の表示

インターフェースへのプロトコルグループのマッピング

「VLAN」→「Protocol」（Configure Interface - Add）を選択すると、グループのメンバーとなるインターフェースごとの VLAN にプロトコルグループをマップすることができます。

関連する CLI 情報

「protocol-vlan protocol-group (Configuring Interfaces)」

コマンドの使用

- ・ プロトコルベースの VLAN を作成する場合にインターフェースを割り当てるときには、この設定画面のみを使用してください。「VLAN」→「Static」を選択すると表示される画面など、VLAN 関連の他の画面を使用すると、インターフェースで、関連付けられている VLAN に任意のプロトコルタイプのトラフィックが送信されるようになります。
- ・ フレームは、プロトコル VLAN に割り当てられているポートに入ると、以下の方法で処理されます。
 - ・ フレームがタグ付きの場合、タグ付きフレームに適用される標準ルールに従って処理されます。
 - ・ フレームがタグなしであり、プロトコルタイプが一致する場合、該当の VLAN に転送されます。
 - ・ フレームがタグなしであるだけでなく、プロトコルタイプが一致しない場合、そのインターフェースのデフォルトの VLAN に転送されます。

パラメータ

以下のパラメータが表示されます。

- (1) Interface - ポートまたはトランクの一覧が表示されます。
- (2) Port - ポート ID（範囲：1 ～ 26）。
- (3) Trunk - トランク ID（範囲：1 ～ 32）。
- (4) Protocol Group ID - プロトコル LAN グループに割り当てられるプロトコルグループ ID（範囲：1 ～ 2,147,483,647）。

- (5) VLAN ID - 対応するプロトコルトラフィックの転送先の VLAN (範囲 : 1 ~ 4,093)。

Web インターフェース

プロトコルグループをポートまたはトランクの VLAN にマップするには、以下のようにします。

- (1) 「VLAN」 → 「Protocol」 を選択します。
- (2) 「Step」 リストで 「Configure Interface」 を選択します。
- (3) 「Step」 リストで 「Add」 を選択します。
- (4) ポートまたはトランクを選択します。
- (5) プロトコルグループの ID を入力します。
- (6) プロトコルトラフィックの転送先となる該当の VLAN を入力します。
- (7) < Apply > ボタンをクリックします。

The screenshot shows a web interface for configuring VLAN protocols. At the top, it says "VLAN > Protocol". Below this, there are two dropdown menus: "Step:" set to "2. Configure Interface" and "Action:" set to "Add". Under the "Interface" section, there are two radio buttons: "Port" (selected) and "Trunk". Next to "Port" is a dropdown menu showing "2". Below "Interface", there is a "Protocol Group ID" dropdown menu showing "1". Below that is a "VLAN ID (1-4093)" text input field. At the bottom right, there are two buttons: "Apply" and "Revert".

画面 1-67 : プロトコル VLAN へのインターフェースの割り当て

ポートまたはトランクにマップされているプロトコルグループを表示するには、以下のようになります。

- (1) 「VLAN」 → 「Protocol」 を選択します。
- (2) 「Step」 リストで 「Configure Interface」 を選択します。

(3) 「Step」 リストで「Show」を選択します。

VLAN > Protocol

Step: 2. Configure Interface Action: Show

Interface ☒ Port 3 ☐ Trunk

Port To Protocol Group Mapping Table Max: 3840 Total: 2

☐	Protocol Group ID	VLAN ID
☐	1	10
☐	3	20

Delete Revert

画面 1-68 : インターフェースとプロトコルグループのマッピングの表示

1.4.4 IP サブネット VLAN の設定

「VLAN」→「IP Subnet」を選択すると、IP サブネットベースの VLAN を設定することができます。

ポートベースの分類を使用する場合、ポートで受信されるすべてのタグなしフレームは、VLAN ID（PVID）がそのポートに関連付けられている VLAN に属するものとして分類されます。

IP サブネットベースの VLAN 分類を有効にすると、タグなしイングレスフレームの送信元アドレスが IP サブネット-VLAN マッピングテーブルと照合されます。そのサブネットのエントリが見つかった場合、フレームは、エントリで示されている VLAN に割り当てられます。該当する IP サブネットがない場合、タグなしフレームは、受信ポートの VLAN ID（PVID）に属するものとして分類されます。

関連する CLI 情報

「Configuring IP Subnet VLANs」

コマンドの使用

- ・それぞれの IP サブネットは 1 つの VLAN ID にのみマップすることができます。IP サブネットは IP アドレスとマスクから設定されます。
- ・タグなしのフレームがポートで受信されると、その送信元 IP アドレスが IP サブネット-VLAN マッピングテーブルと照合され、エントリが見つかった場合は、対応する VLAN ID がフレームに割り当てられます。該当するエントリが見つからない場合は、受信ポートの PVID がフレームに割り当てられます。
- ・IP サブネットは、ブロードキャスト IP アドレスまたはマルチキャスト IP アドレスにすることはできません。
- ・MAC ベースの VLAN、IP サブネットベースの VLAN、およびプロトコルベースの VLAN が同時にサポートされる場合、優先順位は、MAC ベース、IP サブネットベース、プロトコルベースの順になり、ポートベースが最後になります。

パラメータ

以下のパラメータが表示されます。

- ・IP Address – サブネットの IP アドレス。有効な IP アドレスは、0 ～ 255 の 10 進数を 4 つ組み合わせ、それぞれをピリオドで区切って設定されます。
- ・Subnet Mask – このマスクによって IP サブネットのホストアドレスビットを識別します。
- ・VLAN – 対応する IP サブネットトラフィックの転送先の VLAN（範囲：1 ～ 4,093）。
- ・Priority – タグなしイングレストラフィックに割り当てられる優先度（範囲：0 ～ 7（7 が最も高い）、デフォルト：0）。

Web インターフェース

IP サブネットを VLAN にマップするには、以下のようにします。

- (1) 「VLAN」→「IP Subnet」を選択します。
- (2) 「Step」リストで「Add」を選択します。
- (3) 「IP Address」フィールドにアドレスを入力します。

- (4) 「Subnet Mask」フィールドにマスクを入力します。
- (5) 「VLAN」フィールドに ID を入力します。ただし、指定する VLAN は、設定済みのものでなくてもかまいません。
- (6) タグなしフレームに割り当てる値を「Priority」フィールドに入力します。
- (7) < Apply > ボタンをクリックします。

VLAN > IP Subnet

Action: Add

IP Address:

Subnet Mask:

VLAN (1-4093):

Priority (0-7):

Apply Revert

画面 1-69 : IP サブネット VLAN の設定

設定済みの IP サブネット VLAN を表示するには、以下のようにします。

- (1) 「VLAN」 → 「IP Subnet」を選択します。
- (2) 「Step」リストで「Show」を選択します。

VLAN > IP Subnet

Action: Show

IP Subnet to VLAN Mapping Table Max: 4093 Total: 1

	IP Address	Subnet Mask	VLAN	Priority
☐	192.168.1.0	255.255.255.0	10	0

Delete Revert

画面 1-70 : IP サブネット VLAN の表示

1.4.5 MAC ベースの VLAN の設定

「VLAN」→「MAC-Based」を選択すると、MAC アドレスに基づいて VLAN を設定することができます。MAC ベースの VLAN 機能は、送信元 VLAN ID を MAC アドレスに従ってタグなしイングレスフレームに割り当てます。

MAC ベースの VLAN 分類が有効になっている場合、ポートで受信される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ている VLAN に割り当てられます。該当する MAC アドレスがない場合、タグなしフレームは、受信ポートのネイティブ VLAN ID (PVID) に割り当てられます。

関連する CLI 情報

「Configuring MAC Based VLANs」

コマンドの使用

- ・ MAC と VLAN のマッピングはスイッチ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 にのみマップすることができます。
- ・ 設定した MAC アドレスをブロードキャストアドレス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 ベースの VLAN、IP サブネットベースの VLAN、およびプロトコルベースの VLAN が同時にサポートされる場合、優先順位は、MAC ベース、IP サブネットベース、プロトコルベースの順になり、ポートベースが最後になります。

パラメータ

以下のパラメータが表示されます。

- ・ MAC Address – 特定の VLAN にマップされる送信元 MAC アドレス。MAC アドレスは xx-xxxx-xx-xx-xx という形式で指定しなければなりません。
- ・ VLAN – 指定された送信元 MAC アドレスに対応するイングレストラフィックの転送先の VLAN (範囲: 1 ~ 4,093)。
- ・ Priority – タグなしイングレストラフィックに割り当てられる優先度 (範囲: 0 ~ 7 (7 が最も高い)、デフォルト: 0)。

Web インターフェース

MAC アドレスを VLAN にマップするには、以下のようにします。

- (1) 「VLAN」→「MAC-Based」を選択します。
- (2) 「Step」リストで「Add」を選択します。
- (3) 「MAC Address」フィールドにアドレスを入力します。
- (4) 「VLAN」フィールドに ID を入力します。ただし、指定する VLAN は、設定済みのものでなくてもかまいません。
- (5) タグなしフレームに割り当てる値を「Priority」フィールドに入力します。

(6) < Apply > ボタンをクリックします。

VLAN > MAC-Based

Action: Add ▼

MAC Address

VLAN (1-4093)

Priority (0-7)

Apply Revert

画面 1-71 : MAC ベースの VLAN の設定

VLAN にマップされている MAC アドレスを表示するには、以下のようにします。

(1) 「VLAN」 → 「MAC-Based」 を選択します。

(2) 「Step」 リストで 「Show」 を選択します。

VLAN > MAC-Based

Action: Show ▼

MAC-Based VLAN List Max: 32 Total: 1

☐	MAC Address	VLAN	Priority
☐	00-AB-CD-11-22-33	10	0

Delete Revert

画面 1-72 : MAC ベースの VLAN の表示

1.5 アドレステーブル設定

スイッチでは、既知のすべてのデバイスのアドレスが保存されます。それらの情報を使用して、トラフィックをアウトバウンドポートとインバウンドポート間で、直接、渡します。トラフィックの監視によって学習されたすべてのアドレスはダイナミック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ているスタティックアドレスを手動で設定することもできます。

本章では、以下のトピックについて説明します。

- ・ MAC アドレス学習の設定 – インターフェースでアドレス学習を有効または無効にします。
- ・ スタティック MAC アドレスの設定 – アドレステーブルのスタティックエントリを設定します。
- ・ エージングタイムの変更 – 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。
- ・ ダイナミックアドレステーブルの表示 – アドレステーブルのダイナミックエントリを表示します。

1.5.1 MAC アドレス学習の設定

「MAC Address」→「Learning Status」を選択すると、MAC アドレス学習をインターフェースで有効または無効にすることができます。

関連する CLI 情報

「mac-learning」

コマンドの使用

- ・ MAC アドレス学習を無効にすると、スイッチは、指定されたインターフェースにおける新しい MAC アドレスの学習を即座に停止します。スタティックアドレステーブルに格納されている送信元アドレスを含んでいる着信トラフィック（「スタティックアドレスの設定」を参照）のみが、そのインターフェースによってネットワークにアクセスすることを許可されたものとして受け入れられるようになります。
- ・ MAC アドレス学習を無効にすると、アドレステーブルに格納されているダイナミックアドレスがシステムからフラッシュされ、以降は、再び MAC アドレス学習が有効になるまで、ダイナミックアドレスが学習されなくなります。スタティックアドレステーブルに含まれていないデバイスは、MAC アドレス学習が無効になった後にインターフェースを使用しようとする、スイッチへのアクセスを妨げられます。
- ・ 以下のいずれかの状況では MAC アドレス学習を無効にできないので注意してください。
 - ・ 802.1X ポート認証がスイッチのグローバル設定で無効になっている場合（「802.1X グローバル設定の設定」を参照）
 - ・ 同じインターフェースでセキュリティステータス（「ポートセキュリティの設定」を参照）が無効になっている場合

パラメータ

以下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一覧が表示されます。
- ・ Port – ポート ID（範囲：1 ～ 26）。
- ・ Trunk – トランク ID（範囲：1 ～ 32）。

Web 設定

アドレステーブル設定

- ・ Status – MAC アドレス学習のステータス（デフォルト : Enabled）。

Web インターフェース

MAC アドレス学習を有効または無効にするには、以下のようにします。

- (1) 「MAC Address」 → 「Learning Status」 を選択します。
- (2) いずれかのインターフェースの学習ステータスを設定します。
- (3) < Apply > ボタンをクリックします。

MAC Address > Learning Status

Interface ☒ Port ☐ Trunk

Port Learning Status List Max: 26 Total: 26

Port	Status
1	☐ Enabled
2	☒ Enabled
3	☒ Enabled
4	☒ Enabled
5	☒ Enabled

画面 1-73 : MAC アドレス学習の設定

1.5.2 スタティックアドレスの設定

「MAC Address」→「Static」を選択すると、スタティック MAC アドレスを設定することができます。スタティックアドレスは、スイッチの特定のインターフェースに割り当てることができます。スタティックアドレスは、割り当てられたインターフェースにバインドされ、移動されません。

スタティックアドレスが他のインターフェースで検出された場合、その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。

関連する CLI 情報

「mac-address-table static」

コマンドの使用

ホストデバイスのスタティックアドレスは、特定の VLAN 内の特定のポートに割り当てることができます。このコマンドを使用して、スタティックアドレスを MAC アドレステーブルに追加します。スタティックアドレスには、以下のような特性があります。

- ・ スタティックアドレスは、割り当てられたインターフェースにバインドされ、移動されません。スタティックアドレスが他のインターフェースで検出された場合、その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。
- ・ スタティックアドレスは、指定されたインターフェースリンクがダウンした場合でもアドレステーブルから削除されません。
- ・ スタティックアドレスは、テーブルから削除されるまで、他のポートで学習できるようにはなりません。

パラメータ

以下のパラメータが表示されます。

- ・ VLAN – 設定済み VLAN の ID（範囲：1 ～ 4,093）。
- ・ Interface – スタティックアドレスが割り当てられているデバイスに関連付けられているポートまたはトランク。
- ・ MAC Address – このインターフェースにマップされているデバイスの物理アドレス。
- ・ アドレスは、xx-xx-xx-xx-xx-xx または xxxxxxxxxxxx という形式で入力してください。
- ・ Static Status – 指定したアドレスを保持する期間を設定します。
 - ・ Delete-on-reset – スイッチがリセットされるまで割り当てを保持します。
 - ・ Permanent – 割り当てを永続的に保持します（これがデフォルトです）。

Web インターフェース

スタティック MAC アドレスを設定するには、以下のようになります。

- (1) 「MAC Address」→「Static」を選択します。
- (2) 「Step」リストで「Add」を選択します。
- (3) VLAN、アドレスの割り当て先のポートまたはトランク、MAC アドレス、およびエントリを保持する時間を指定します。

(4) < Apply > ボタンをクリックします。

MAC Address > Static

Action: **Add**

VLAN: **1**

Interface: ☒ Port **1** ☐ Trunk

MAC Address: **00-12-cf-94-34-da**

Static Status: **Permanent**

Apply **Revert**

画面 1-74 : スタティック MAC アドレスの設定

MAC アドレステーブルのスタティックアドレスを表示するには、以下のようにします。

- (1) 「MAC Address」 → 「Static」 を選択します。
- (2) 「Step」 リストで 「Show」 を選択します。

MAC Address > Static

Action: **Show**

Static MAC Address to Interface Mapping Table Max: 1024 Total: 2

	MAC Address	VLAN	Interface	Type	Life Time
☐	00-00-E8-93-82-A0	1	CPU	CPU	Delete on Reset
☐	00-12-CF-94-34-DA	1	Unit 1 / Port 1	Config	Permanent

Delete **Revert**

画面 1-75 : スタティック MAC アドレスの表示

1.5.3 エージングタイムの変更

「MAC Address」→「Dynamic」(Configure Aging)を選択すると、ダイナミック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ことができます。そのエージングタイムを使用して、動的に学習された転送情報の有効期限を設定します。

関連する CLI 情報

「mac-address-table aging-time」

パラメータ

以下のパラメータが表示されます。

- ・ Aging Status - 機能を有効または無効にします。
- ・ Aging Time - この期間が経過すると、学習されたエントリが破棄されます（範囲：10 ～ 1,000,000 秒、デフォルト：300 秒）。

Web インターフェース

ダイナミック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、以下のようになります。

- (1) 「MAC Address」→「Dynamic」を選択します。
- (2) 「Step」リストで「Configure Aging」を選択します。
- (3) 必要の場合は、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 > ボタンをクリックします。

The screenshot shows a web configuration page titled "MAC Address > Dynamic". Below the title is a "Step:" dropdown menu with "1. Configure Aging" selected. Underneath, there are two settings: "Aging Status" with a checked checkbox labeled "Enabled", and "Aging Time (10-1000000)" with a text input field containing "300" followed by "sec". At the bottom right, there are two buttons: "Apply" and "Revert".

画面 1-76 : アドレスのエージングタイムの設定

1.5.4 ダイナミックアドレステーブルの表示

「MAC Address」→「Dynamic」（Show Dynamic MAC）を選択すると、スイッチに入ってくるトラフィックの送信元アドレスを監視することによって学習された MAC アドレスが表示されます。インバウンドトラフィックの宛先アドレスがデータベースにある場合、そのアドレス宛のパケットは、関連付けられているポートに直接転送されます。データベースにない場合、トラフィックはすべてのポートにフラッドされます。

関連する CLI 情報

「show mac-address-table」

パラメータ

以下のパラメータが表示されます。

- ・ Sort Key – 表示される情報を、MAC アドレス、VLAN、またはインターフェース（ポートまたはトランク）を基準にして並び替えることができます。
- ・ MAC Address – このインターフェースに関連付けられている物理アドレス。
- ・ VLAN – 設定済み VLAN の ID（範囲：1 ～ 4,093）。
- ・ Interface – ポートまたはトランクを示します。
- ・ Type – このテーブルのエントリが学習されたものであることを示します。
- ・ Life Time – 指定したアドレスの保持期間が表示されます。

Web インターフェース

ダイナミックアドレステーブルを表示するには、以下のようにします。

- (1) 「MAC Address」→「Dynamic」を選択します。
- (2) 「Step」リストで「Show Dynamic MAC」を選択します。
- (3) 「Sort Key」で「MAC Address」、「VLAN」、または「Interface」を選択します。
- (4) 検索パラメータ（「MAC Address」、「VLAN」、または「Interface」）を入力します。

(5) < Query > ボタンをクリックします。

MAC Address > Dynamic

Action: Show Dynamic MAC

Query by:

Sort Key: MAC Address

☐ MAC Address

☐ VLAN 1

☐ Interface ☒ Port 1 ☐ Trunk

Query

Dynamic MAC Address List Max: 16384 Total: 2

MAC Address	VLAN	Interface	Type	Life Time
00-60-6E-00-5F-A1	1	Unit 1 / Port 13	Learn	Delete on Timeout
00-E0-29-94-34-65	2	Unit 1 / Port 14	Learn	Delete on Timeout

画面 1-77 : ダイナミック MAC アドレステーブルの表示

1.5.5 ダイナミックアドレステーブルの作成

「MAC Address」→「Dynamic」（Clear Dynamic MAC）を選択すると、学習された任意のエントリを転送データベースから削除することができます。

関連する CLI 情報

「clear mac-address-table dynamic」

パラメータ

以下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、またはポートやトランクに関連付けられているすべてのエントリをクリアすることができます。

Web インターフェース

ダイナミックアドレステーブルのエントリをクリアするには、以下のようになります。

- (1) 「MAC Address」→「Dynamic」を選択します。
- (2) 「Step」リストで「Clear Dynamic MAC」を選択します。
- (3) エントリをクリアする方法（「All」、「MAC Address」、「VLAN」、または「Interface」）を選択します。
- (4) 「MAC Address」、「VLAN」、または「Interface」ごとにエントリをクリアするために必要な情報をその他のフィールドに入力します。
- (5) < Clear > ボタンをクリックします。

The screenshot shows a web interface for clearing dynamic MAC address table entries. At the top, there is a breadcrumb navigation path: "MAC Address > Dynamic". Below this, there is a "Step:" label followed by a dropdown menu showing "3. Clear Dynamic MAC". Underneath, there is a "Clear by:" label followed by a dropdown menu showing "All". At the bottom right of the form, there is a "Clear" button.

画面 1-78 : ダイナミック MAC アドレステーブルのエントリのクリア

1.6 スパニングツリーアルゴリズム

本章では、以下の基本的なトピックについて説明します。

- ・ ループバック検出の設定 – ループバック BPDU の検出とそれらへの対応を設定します。
- ・ STA のグローバル設定 – STP、RSTP、および MSTP のグローバルブリッジを設定します。
- ・ STA のインターフェース設定 – STA のインターフェース（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）を設定します。
- ・ MSTP のインターフェース設定 – MSTP のインターフェース（優先度やパスコストなど）を設定します。

1.6.1 概要

スパニングツリーアルゴリズム（STA: Spanning Tree Algorithm）を使用すると、ネットワークループを検出して無効にすることや、スイッチ、ブリッジ、または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。そのようにすることで、本製品をご使用のネットワーク内の他のブリッジデバイス（つまり、STA 対応のスイッチ、ブリッジ、またはルータ）と通信できるようにしてネットワーク上の任意の 2 つのステーション間でルートが 1 つだけ確保されるようにしたり、プライマリリンクがダウンした場合にその役割を自動的に引き継ぐバックアップリンクが提供されるようにしたりすることが可能になります。

本製品でサポートしているスパニングツリーアルゴリズムには、以下のようなものがあります。

- ・ STP – Spanning Tree Protocol (IEEE 802.1D)
- ・ RSTP – Rapid Spanning Tree Protocol (IEEE 802.1w)
- ・ MSTP – Multiple Spanning Tree Protocol (IEEE 802.1s)

STP

STP では、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 対応のスイッチ、ブリッジ、またはルータ）を選択します。それぞれのブリッジングデバイス（ルートデバイス以外）からルートデバイスにパケットを転送する際にそのデバイスで最小パスコストを実現するルートポートが選択されます。それから、それぞれの LAN からルートデバイスにパケットを転送する際にその LAN で最小パスコストを実現する代表ブリッジングデバイスが選択されます。代表ブリッジングデバイスに接続されているすべてのポートが代表ポートとして割り当てられます。最小コストのスパニングツリーが判別されると、すべてのルートポートと代表ポートが有効になり、その他のすべてのポートが無効になります。そのため、ネットワークパケットがルートポートと代表ポートの間でのみ転送されるようになり、想定されるあらゆるネットワークループが回避されます。

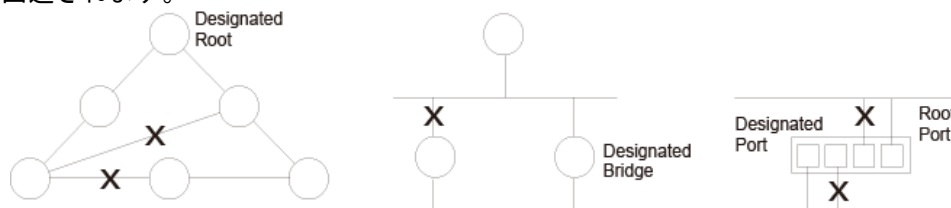


図 1-8: STP ルートポートと代表ポート

安定的なネットワークトポロジが確立されると、すべてのブリッジが、ルートブリッジから送信される Hello BPDU（Bridge Protocol Data Unit）を listen します。

ブリッジは、事前に定義されている期間（Maximum Age）を過ぎても Hello BPDU を取得できない場合は、ルートブリッジへのリンクがダウンしているものとみなします。その場合は、ネットワークを再設定して有効なネットワークトポロジを改めて確立するため、他のブリッジとのネゴシエーションを開始します。

RSTP

RSTP は、低速な従来の STP の一般的な代替プロトコルとして開発されました。RSTP も MSTP に組み込まれています。RSTP では、アクティブポートが学習を開始するまでの状態変更の回数を減らし、ノードやポートで障害が発生した場合に使用できる代替ルートを事前に定義し、再設定時のツリー構造の変化に影響されないポート転送データベースを保持するという方法で、STP よりも極めて速やかに再設定を実現します（STP が 30 秒以上であるのに対し、RSTP は 1 ～ 3 秒）。

MSTP

STP または RSTP を使用する場合、すべての VLAN メンバー間で安定したパスを維持することが難しい状況もあります。ツリー構造が頻繁に変更されると、グループの一部のメンバーが切り離されるということが起こりやすくなります。（速やかな輻輳制御のための RSTP を基盤とする）MSTP は、VLAN グループに基づく独立したスパニングツリーをサポートすることを目的としています。複数のスパニングツリーを使用することで、複数の転送パスを提供し、負荷分散を実現できるようになります。1 つまたは複数の VLAN をグループ化してマルチプルスパニングツリーインスタンス（MSTI: Multiple Spanning Tree Instance）を作成することができます。MSTP では、インスタンスごとに別々のマルチプルスパニングツリー（MST: Multiple Spanning Tree）を構築して、割り当てられている各 VLAN グループ間の接続性を維持します。さらに、MSTP では、一般設定されているすべての MSTP を含む領域の内部スパニングツリー（IST: Internal Spanning Tree）が構築されます。

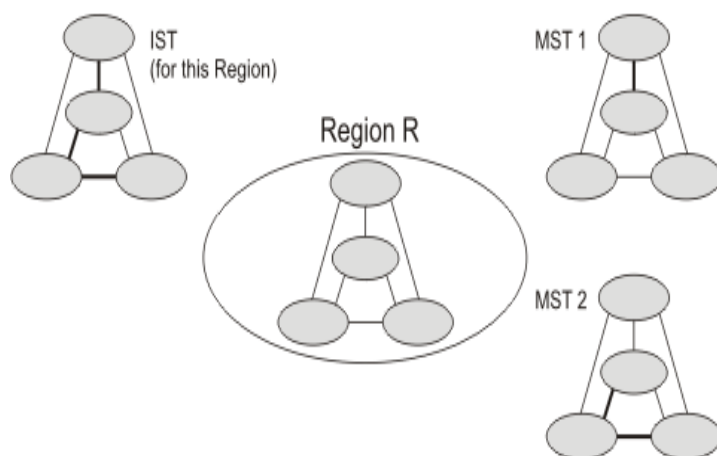


図 1-9: MST 領域、内部スパニングツリー、マルチプルスパニングツリー

MST 領域は、同じ MST 設定 ID（領域名、リビジョンレベル、および設定ダイジェストを含む。「マルチプルスパニングツリー（MSTP）の設定」を参照）をもち、相互接続されているブリッジのグループから設定されます。MST 領域には、複数の MSTP インスタンスを含めることができます。IST を使用して、MST 領域内のすべての MSTP スイッチが接続さ

れます。共通スパニングツリー（CST: Common Spanning Tree）は、隣接するすべての MST 領域を相互接続し、グローバルネットワーク内の STP ノードまたは 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。

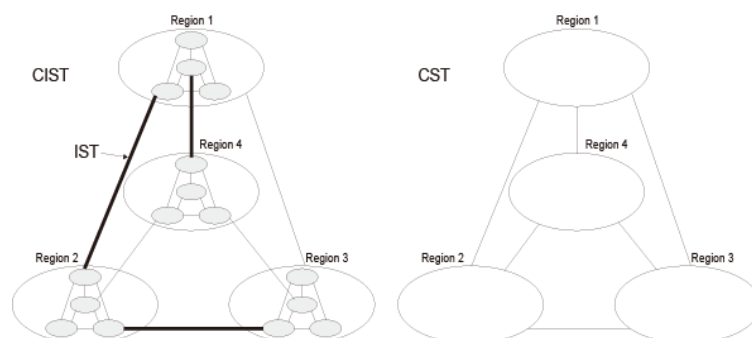


図 1-10: 共通内部スパニングツリー、共通スパニングツリー、内部スパニングツリー

MSTP は、すべてのブリッジおよび LAN セグメントを単一の共通内部スパニングツリー（CIST: Common and Internal Spanning Tree）と接続します。CIST は、STP、RSTP、および MSTP をサポートしているスイッチ間でスパニングツリーアルゴリズムを実行した結果として形成されます。

MSTI に含める VLAN を指定すると、それぞれの VLAN の間の接続性を維持するため、MSTP によって自動的に MSTI ツリーが作成されます。MSTP では、それぞれのインスタンスが CST 内の RSTP ノードとして処理されるので、グローバルネットワークとの通信が維持されます。

1.6.2 ループバック検出の設定

「Spanning Tree」→「Loopback Detection」を選択すると、インターフェースのループバック検出を設定することができます。ループバック検出が有効になっており、ポートまたはトランクでそのポートまたはトランクの BPDU が受信されると、検出エージェントによってループバック BPDU がドロップされ、SNMP トラップが送信されて、インターフェースが破棄モードになります。

このループバック状態は、手動または自動で解除することができます。インターフェースで自動ループバック解除が設定されている場合には、以下のいずれかの条件が満たされときのみ、ポートが転送状態に戻されます。

- ・ インターフェースでそのインターフェースの BPDU 以外の BPDU が受信される
- ・ インターフェースのリンクステータスが、リンクダウンになってから再びリンクアップになる
- ・ インターフェースでそのインターフェースの BPDU の受信が転送待機期間内に停止される

[注意] ループバック検出が有効になっておらず、インターフェースでそのインターフェースの BPDU が受信されると、IEEE 802.1w-2001 9.3.4（注 1）に従い、ループバック BPDU がドロップされます。

[注意] ループバック検出は、スイッチでスパニングツリーが無効になっている場合はアクティブになりません。

[注意] 手動解除モードが設定されている場合、リンクダウンイベントまたはリンクアップイベントが発生してもポートの破棄モードは解除されません。

関連する CLI 情報

「Editing VLAN Groups」

パラメータ

以下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一覧が表示されます。
- ・ Status – このインター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：Enabled）。
- ・ Trap – このインターフェースでループバックイベントに関する SNMP トラップ通知を有効にします（デフォルト：Disabled）。
- ・ Release Mode – インターフェースの自動ループバック解除または手動ループバック解除を設定します（デフォルト：Auto）。
- ・ Release – インターフェースの破棄モードを手動で解除できるようにします。このパラメータは、インターフェースで手動解除モードが設定されている場合にのみ、使用することができます。

Web インターフェース

ループバック検出を設定するには、以下のようにします。

- (1) 「Spanning Tree」 → 「Loopback Detection」 を選択します。
- (2) 「Port」 または 「Trunk」 を選択して必要なインターフェースタイプを表示します。
- (3) 該当のループバック検出属性を変更します。
- (4) < Apply > ボタンをクリックします。

Spanning Tree > Loopback Detection

Interface ☒ Port ☐ Trunk

Loopback Detection Port List Max: 26 Total: 26 1 2 3

Port	Status	Trap	Release Mode	Release
1	☒ Enabled	☐ Enabled	Auto ▼	Release
2	☒ Enabled	☐ Enabled	Auto ▼	Release
3	☒ Enabled	☐ Enabled	Auto ▼	Release
4	☒ Enabled	☐ Enabled	Auto ▼	Release
5	☒ Enabled	☒ Enabled	Manual ▼	Release

画面 1-79 : ポートループバック検出の設定

1.6.3 STA のグローバル設定の設定

「Spanning Tree」→「STA」（Configure Global - Configure）を選択すると、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設定を設定することができます。

関連する CLI 情報

「Spanning Tree Commands」

コマンドの使用

- ・ STP（Spanning Tree Protocol）**2
 - ・ 内部ステートマシンに RSTP を使用しますが、802.1D BPDU のみを送信します。そのようにすると、ネットワーク全体に対して 1 つのスパニングツリーインスタンスが作成されます。複数の VLAN がネットワークに実装されている場合、個々の VLAN メンバー間のパスが何らかの理由でネットワークループを回避するために無効になり、その結果、グループのメンバーが切り離されることがあります。そのため、複数の VLAN を運用する場合は、MSTP オプションを選択することをお勧めします。
- ・ RSTP（Rapid Spanning Tree Protocol）**2

RSTP では、以下のような方法で着信プロトコルメッセージを監視して RSTP ノードで送信されるプロトコルメッセージのタイプを動的に調整することにより、STP ノードと RSTP ノードのいずれかへの接続をサポートします。

 - ・ STP モード - ポートの状態遷移タイマーで設定されている期間を過ぎてから 802.1D BPDU（つまり、STP BPDU）がスイッチで受信されると、そのポートは 802.1D ブリッジに接続されているものとみなされ、802.1D BPDU のみが使用されるようになります。
 - ・ RSTP モード - ポートで 802.1D BPDU が使用されており、状態遷移の待機期間を過ぎてから RSTP BPDU が受信されると、状態遷移待機タイマーがリセットされて、そのポートで RSTP BPDU が使用されるようになります。
- ・ MSTP（Multiple Spanning Tree Protocol）

**2. STP BPDU および RSTP BPDU は、あらゆる VLAN 境界を越えて、タグなしフレームとして送信されます。

MSTP では、インスタンスごとに固有のスパニングツリーが生成されます。そのようにすることで、ネットワーク全体で複数の経路が提供されます。その結果、トラフィックの負荷が分散されるので、単一インスタンス内のブリッジノードで障害が発生した場合に大規模な機能停止状態に陥るのを回避したり、障害が発生したインスタンスの新しいトポロジの速やかな輻輳制御を実現したりできるようになります。

- ・ ネットワーク全体で複数のスパニングツリーを運用できるようにするには、同じ MSTP 設定を使用して関連する一連のスイッチを設定し、それらのスイッチを特定の一連のスパニングツリーインスタンスのメンバーにできるようにする必要があります。
- ・ スパニングツリーインスタンスは、複数の VLAN インスタンスの割り当てが可能なブリッジ上に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際には注意してください。モードを変更すると、直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稼働停止になり、システムが再起動されるので、ユーザトラフィックが一時的に中断されます。

パラメータ

以下のパラメータが表示されます。

Basic Configuration of Global Settings

- ・ 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：Enabled）。
- ・ Spanning Tree Type – このスイッチで使用するスパニングツリーのタイプを指定します。
 - ・ STP: Spanning Tree Protocol (IEEE 802.1D)。このオプションを選択すると、スイッチでは RSTP が強制的に STP モードで使用されるようになります。
 - ・ RSTP: Rapid Spanning Tree (IEEE 802.1w)。RSTP はデフォルトです。
 - ・ MSTP: Multiple Spanning Tree (IEEE 802.1s)。
- ・ Priority – ルートデバイス、ルートポート、および代表ポートの選択時にブリッジの優先度が使用されます。最も優先度が高いデバイスが STA ルート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には、MAC アドレスが最も小さいデバイスがルートデバイスになります（値が小さいほど優先度が高いということに注意してください）。
 - ・ デフォルト：32,768
 - ・ 範囲：0 ～ 61,440（4,096 の倍数）
 - ・ オプション：0、4,096、8,192、12,288、16,384、20,480、24,576、28,672、32,768、36,864、40,960、45,056、49,152、53,248、57,344、61,440
- ・ BPDU Flooding – スパニングツリーがスイッチのグローバル設定で無効になっている場合や特定のポートで無効になっている場合に BPDU がスイッチ上の他のすべてのポートにフラッドされるように設定するか、または、同じ VLAN 内の他のすべてのポートにのみフラッドされるように設定します。
 - ・ To VLAN: BPDU が受信ポートのネイティブ VLAN 内の他のすべてのポート（ポートの PVID によって判別）にフラッドされるようにします。これがデフォルトです。
 - ・ To All: BPDU がスイッチ上の他のすべてのポートにフラッドされるようにします。ポートで BPDU フラディングが無効になっている場合は、この設定は、一切、影響を及ぼしません（「STA のインターフェース設定の設定」を参照）。

Advanced Configuration Settings

以下の属性は、RSTP に基づくものですが、本製品では STP を実装するために RSTP の下位互換サブセットを使用するので、STP にも適用されます。また、規格に従い、RSTP を基盤とする MSTP にも適用されます。

- ・ Path Cost Method – パスコストを使用してデバイス間の最適パスが判別されます。パスコスト方式によって、各インターフェースに割り当てることができる値の範囲が判別されます。
 - ・ Long: 1 ～ 200,000,000 の範囲で 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 ～ 65,535 の範囲で 16 ビットベースの値を指定します。
- ・ Transmission Limit – 連続するプロトコルメッセージの最小送信間隔を設定することにより、BPDU の最大送信レートを指定します（範囲：1 ～ 10、デフォルト：3）。

When the Switch Becomes Root

- ・ Hello Time – ルートデバイスで設定メッセージを送信する間隔（秒単位）。
 - ・ デフォルト：2
 - ・ 最小：1

- ・ 最大: 10 と $[(\text{Message Age} / 2) - 1]$ のいずれか小さい方の値
- ・ Maximum Age – デバイスが設定メッセージを受信せずに待機する最大期間 (秒)。この期間が経過すると、デバイスは再設定を試行します。すべてのデバイスポート (代表ポートを除く) では、設定メッセージが一定の間隔で受信されます。ポートは、(最新の設定メッセージで提供された) STA 情報が期限切れになると、接続している LAN の代表ポートになります。それがルートポートである場合は、ネットワークに接続しているデバイスポートの中から新しいポートが選択されます (このセクションで言うところの「ポート」とは、ポートとトランクの両方を含む「インターフェース」を意味します)。
 - ・ デフォルト: 20
 - ・ 最小: 6 と $[2 \times (\text{Hello Time} + 1)]$ のいずれか大きい方の値
 - ・ 最大: 40 と $[2 \times (\text{Forward Delay} - 1)]$ のいずれか小さい方の値
- ・ Forward Delay – デバイスで状態が変更される (つまり、破棄→学習→転送になる) 前の待機期間 (秒)。すべてのデバイスはフレームの転送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、このような待機が必要になります。さらに、それぞれのポートでは、そのポートを破棄状態にする可能性のある競合情報を listen する必要があります。listen しない場合、一時的なデータループが発生することがあります。
 - ・ デフォルト: 15
 - ・ 最小: 4 と $[(\text{Max. Message Age} / 2) + 1]$ のいずれか大きい方の値
 - ・ 最大: 30

Configuration Settings for MSTP

- ・ Max Instance Numbers – このスイッチの割り当て先にすることができる MSTP インスタンスの最大数。
- ・ Configuration Digest – VLAN ID と MST ID とのマッピングテーブルを含む MD5 署名キー。つまり、このキーは CIST に対するすべての VLAN のマップです。
- ・ Region Revision3 – この MSTI のリビジョン (範囲: 0 ~ 65,535、デフォルト: 0)。
- ・ Region Name3 – この MSTI の名前 (最大長: 32 文字。スイッチの MAC アドレス)。
- ・ Max Hop Count – MST 領域で許可されるホップの最大数。この数を超えると BPDU が破棄されます (範囲: 1 ~ 40、デフォルト: 20)。

Web インターフェース

STA のグローバル設定を設定するには、以下のようにします。

- (1) 「Spanning Tree」 → 「STA」 を選択します。
- (2) 「Step」 リストで 「Configure Global」 を選択します。
- (3) 「Step」 リストで 「Configure」 を選択します。
- (4) 必要な属性のいずれかを変更します。直前のセクションで説明されているように、表示されるパラメータはスパニングツリータイプ（STP、RSTP、または MSTP）によって異なります。
- (5) < Apply > ボタンをクリックします。

**3. MST の名前とバージョン番号は、MST 領域を一意に識別するために両方とも必要です。

Spanning Tree > STA

Step: 1. Configure Global Action: Configure

Spanning Tree Status ☒ Enabled

Spanning Tree Type STP

Priority (0-61440, in steps of 4096) 32768

BPDU Flooding To VLAN

Advanced:

Path Cost Method Long

Transmission Limit (1-10) 3

When the Switch Becomes Root:

Hello Time (1-10) 2 sec

Maximum Age (6-40) 20 sec

Forward Delay (4-30) 15 sec

Note: $2 * (\text{Hello Time} + 1) \leq \text{Max Age} \leq 2 * (\text{Forward Delay} - 1)$

Apply Revert

画面 1-80 : STA のグローバル設定の設定（STP）

Web 設定

スパニングツリーアルゴリズム

Spanning Tree > STA

Step: 1. Configure Global Action: Configure

Spanning Tree Status ☒ Enabled

Spanning Tree Type RSTP

Priority (0-61440, in steps of 4096) 32768

BPDU Flooding To VLAN

Advanced:

Path Cost Method Long

Transmission Limit (1-10) 3

When the Switch Becomes Root:

Hello Time (1-10) 2 sec

Maximum Age (6-40) 20 sec

Forward Delay (4-30) 15 sec

Note: $2 * (\text{Hello Time} + 1) \leq \text{Max Age} \leq 2 * (\text{Forward Delay} - 1)$

Apply Revert

画面 1-81 : STA のグローバル設定の設定 (RSTP)

Spanning Tree > STA

Step: 1. Configure Global Action: Configure

Spanning Tree Status ☒ Enabled

Spanning Tree Type MSTP

Priority (0-61440, in steps of 4096) 32768

BPDU Flooding To VLAN

Advanced:

Path Cost Method Long

Transmission Limit (1-10) 3

When the Switch Becomes Root:

Hello Time (1-10) 2 sec

Maximum Age (6-40) 20 sec

Forward Delay (4-30) 15 sec

Note: $2 * (\text{Hello Time} + 1) \leq \text{Max Age} \leq 2 * (\text{Forward Delay} - 1)$

画面 1-82 : STA のグローバル設定の設定 (MSTP)

1.6.4 STA のグローバル設定の表示

「Spanning Tree」→「STA」（Configure Global - Show Information）を選択すると、スイッチ全体に適用される最新のブリッジ STA 情報の概要が表示されます。

関連する CLI 情報

「show spanning-tree」

「show spanning-tree mst configuration」

パラメータ

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

- ・ Bridge ID - このブリッジの固有の ID です。ブリッジの優先度、MST インスタンス ID（モードが MSTP に設定されている場合は共通スパニングツリーを示す 0）、および MAC アドレス（MAC アドレスがスイッチシステムから取得される場合）から設定されます。
- ・ Designated Root - このスイッチでルートデバイスとして認められている、スパニングツリー内のデバイスの優先度と MAC アドレス。
- ・ Root Port - このスイッチでルートブリッジに最も近いポートの番号。スイッチは、このポートを使用してルートデバイスと通信します。ルートポートがない場合は、このスイッチがスパニングツリーネットワークのルートデバイスとして認められていることを意味します。
- ・ Root Path Cost - このスイッチ上のルートポートからルートデバイスへのパスコスト。
- ・ Configuration Changes - パニングツリーが再設定された回数。
- ・ Last Topology Change - 前回のスパニングツリー再設定からの経過時間。

Web インターフェース

STA のグローバル設定を表示するには、以下のようにします。

- (1) 「Spanning Tree」→「STA」を選択します。
- (2) 「Step」リストで「Configure Global」を選択します。
- (3) 「Step」リストで「Show Information」を選択します。

Spanning Tree > STA

Step: 1. Configure Global Action: Show Information

Spanning Tree Information

Spanning Tree Status	Enabled	Spanning Tree Type	RSTP
Designated Root	32768.0000E89382A0	Bridge ID	32768.0000E89382A0
Root Port	0	Max Age	20 sec
Root Path Cost	0	Hello Time	2 sec
Configuration Changes	2	Forward Delay	15 sec
Last Topology Change	0 days, 3 hours, 51 minutes, 11 seconds		

画面 1-83 : STA のグローバル設定の表示

1.6.5 STA のインターフェース設定の設定

「Spanning Tree」→「STA」（Configure Interface - Configure）を選択すると、個々のインターフェースの RSTP 属性と MSTP 属性（ポートの優先度、パスコスト、リンクタイプ、エッジポートなど）を設定することができます。同じメディアタイプのポートに異なる優先度またはパスコストを使用して優先パスを示し、リンクタイプを使用して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し、エッジポートを使用して接続デバイスで高速転送をサポートできるかどうかを示すことができます（このセクションで言うところの「ポート」とは、ポートとトランクの両方を含む「インターフェース」を意味します）。

関連する CLI 情報

「Spanning Tree Commands」

パラメータ

以下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一覧が表示されます。
- ・ Spanning Tree – このインターフェースで 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になっている場合やスパニングツリーが特定のポートで無効になっている場合の他ポートへの BPDU 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になっている場合、BPDU は、スパニングツリー BPDU フラッディング属性の指定に従って、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ドされます。
- ・ Priority – STP でこのポートに使用される優先度を定義します。スイッチのすべてのポートでパスコストが同じである場合には、優先度が最も高い（つまり、値が最も小さい）ポート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。そのようにすることで、STP でネットワークループが検出される場合に、優先度が高いポートほどブロックされる可能性が低くなるようになっています。最も高い優先度が複数のポートに割り当てられている場合には、ID の値が最も小さいポートが有効になります。
 - ・ デフォルト：128
 - ・ 範囲：0～240（16 の倍数）
- ・ Admin Path Cost – このパラメータは、STA でデバイス間の最適パスを判別するために使用されます。そのため、接続先のメディアが高速であるほどポートに小さい値が割り当てられ、メディアが低速になるにつれてポートに大きい値が割り当てられなければなりません。また、パスコストはポートの優先度よりも優先されるということに注意してください（範囲：自動設定の場合は 0、ショートパスコスト方式 4 の場合は 1～65,535、ロングパスコスト方式の場合は 1～200,000,000）。

デフォルトでは、各ポートで使用されている速度と Duplex モードが自動的に検出され、以下の値に応じてパスコストが設定されます。パスコスト「0」は、自動設定モードを示します。ショートパスコスト方式が選択されており、IEEE 802.1w 規格で推奨されているデフォルトのパスコストが 65,535 より大きい場合、デフォルトは 65,535 に設定されます。

ポートタイプ	IEEE 802.1D-1998	IEEE 802.1w-2001

ギガビットイーサネット	3 ～ 10	2,000 ～ 200,000
10G イーサネット	1 ～ 5	200 ～ 20,000

表 12: 推奨される STA パスコストの範囲

**4. パスコスト方式の設定方法については、「STA のグローバル設定の設定」を参照してください。

ポートタイプ	ショートパスコスト (IEEE 802.1D-1998)	ロングパスコスト (802.1D-2004)
ギガビットイーサネット	10,000	10,000
10G イーサネット	1,000	1,000

表 13: デフォルトの STA パスコスト

- Admin Link Type - このインターフェースに接続されているリンクのタイプ。
 - Point-to-Point - 他の 1 つのブリッジのみに接続しています。
 - Shared - 2 つ以上のブリッジに接続しています。
 - Auto - インターフェースがポイントツーポイントリンクと共有メディアのどちらに接続しているかが自動的に判別されます（これがデフォルトの設定です）。
- Root Guard - STA では、ID が小さいブリッジ（または ID が同じで MAC アドレスが小さいブリッジ）が、随時、ルートブリッジとしての役割を引き継ぐことができます。ルートガードを使用すると、ルートブリッジが 2 番目の候補の場所で形成されないようにすることができます。ルートガードは、低速ブリッジに接続されている代表ポートのうち、ルートポートとしての役割を引き継いで新しいスパニングツリートポロジを形成することによって低速リンクでオーバーロードを発生させる可能性があるポートで有効にします。また、ルートガードは、ネットワークでルートブリッジが許可されている部分の周囲に境界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 - エンドノードは、転送ループを発生させる可能性がないので、直接、スパニングツリー転送状態に移行することができます。
 エッジポートを指定すると、ワークステーションやサーバなどのデバイスの速やかな輻輳制御を実現すること、最新の転送データベースを保持して再設定イベント時のアドレステーブルの再構築に必要なフレームフラッディングの量を削減すること、インターフェースの状態が変更された場合にスパニングツリーで再設定が開始されないようにすること、および、STA 関連のその他のタイムアウト問題を克服することができます。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ているポートに対してのみ有効にしなければならないという点に留意してください（デフォルト：Disabled）。
 - Enabled - 手動でポートをエッジポートとして設定します。
 - Disabled - エッジポート設定を無効にします。
 - Auto - ポートで RSTP BPDU または MSTP BPDU がまったく受信されることなくにエッジ待機期間が過ぎると、そのポートは自動的にエッジポートとして設定されます。エッジ待機期間（802.1D-2004 17.20.4）は、ポートのリンクタイプがポイントツーポイントである場合にはプロトコル移行時間（IEEE 802.3D-2004 17.20.4 で規定されている 3 秒）と等しく、それ以外の場合はスパニングツリーの設定メッ

Web 設定

スパニングツリーアルゴリズム

セージの最大有効期間と等しくなるということに注意してください（最大有効期間については「STA のグローバル設定の設定」を参照）。

- ・ インターフェースは、以下の状況ではエッジポートとして機能しません。
 - ・ スパニングツリーモードが STP に設定されている場合、自動設定を使用してエッジポートモードが自動的に稼働エッジポートモードに遷移することはできません。
 - ・ ループバック検出が有効になっている場合にループバック BPDU が検出されると、インターフェースは、そのループバック状態が解除されるまでエッジポートとして機能することができなくなります。
 - ・ インターフェースが転送状態であり、その役割が変更された場合、そのインターフェースは、エッジ待機期間を過ぎても、引き続きエッジポートとして機能することができなくなります。
 - ・ エッジ待機期間を過ぎてからポートで BPDU が受信されない場合、ポートの役割が代表ポートに変更され、即座にポートが転送状態になります（「STA のインターフェース設定の表示」を参照）。
- ・ BPDU Guard⁵ – この機能は、エッジポートで BPDU が受信されないようにする場合に使用します。BPDU が受信された場合、エッジポートをスパニングツリー破棄状態にする代わりに、シャットダウンします。
- ・ 設定が有効なものであれば、設定されたエッジポートで BPDU が受信されることはありません。エッジポートで BPDU が受信される場合は、承認されていないデバイスへの接続など、無効な設定が存在します。BPDU ガード機能を使用すると、管理者がポートを手動で有効にしなければならないので、無効な設定に対するセキュアな対応が実現します（デフォルト：Disabled）。
- ・ BPDU Filter⁵ – BPDU フィルタリングを使用すると、エンドノードに接続されている設定済みのエッジポートで BPDU が送信されないようにすることができます。デフォルトでは、ポートで管理エッジが有効になっているかどうかに関わらず、STA によって BPDU がすべてのポートに送信されます。BPDU フィルタリングはポートごとに設定します（デフォルト：Disabled）。
- ・ Migration – 本製品では、STP BPDU（設定変更 BPDU またはトポロジ変更 BPDU を含む）が検出されると、必ず、選択されているインターフェースが自動的に STP 対応モードに設定されます。ただし、「Migration」を使用して、選択されているインターフェースで BPDU の送信時に使用されるべき適切な形式（RSTP 対応または STP 対応）を手動で再チェックすることもできます（デフォルト：Disabled）。

Web インターフェース

STA のインターフェース設定を設定するには、以下のようになります。

- (1) 「Spanning Tree」 → 「STA」 を選択します。
- (2) 「Step」 リストで 「Configure Interface」 を選択します。
- (3) 「Step」 リストで 「Configure」 を選択します。
- (4) 必要な属性のいずれかを変更します。
- (5) この機能を使用するには 「Admin Edge Port」 を有効にする必要があります。

(6) < Apply > ボタンをクリックします。

Spanning Tree > STA
■

Step: 2. Configure Interface Action: Configure

Interface Port Trunk

Port List Max: 26 Total: 26 1 2 3

Port	Spanning Tree	BPDU Flooding	Priority (0-240, in steps of 16)	Admin Path Cost (0-200000000, 0: Auto)	Admin Link Type	Root Guard	Admin Edge Port	BPDU Guard	BPDU Filter	Migration
1	☒ Enabled	☒ Enabled	128	0	Auto	☐ Enabled	Auto	☐ Enabled	☐ Enabled	☐ Enabled
2	☒ Enabled	☒ Enabled	128	0	Auto	☐ Enabled	Auto	☐ Enabled	☐ Enabled	☐ Enabled
3	☒ Enabled	☒ Enabled	128	0	Auto	☐ Enabled	Auto	☐ Enabled	☐ Enabled	☐ Enabled
4	☒ Enabled	☒ Enabled	128	0	Auto	☒ Enabled	Auto	☐ Enabled	☐ Enabled	☐ Enabled
5	☒ Enabled	☒ Enabled	128	0	Auto	☐ Enabled	Auto	☐ Enabled	☐ Enabled	☐ Enabled

画面 1-84 : STA のインターフェース設定の設定

1.6.6 STA のインターフェース設定の表示

「Spanning Tree」→「STA」（Configure Interface - Show Information）を選択すると、スパニングツリー内のポートまたはトランクの現在の状態が表示されます。

関連する CLI 情報

「show spanning-tree」

パラメータ

以下のパラメータが表示されます。

- ・ Spanning Tree – このインターフェースで STA が有効になっているかどうかが表示されます。
- ・ BPDU Flooding – スパニングツリーがスイッチのグローバル設定で無効になっている場合や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ドされるかどうかが表示されます。
- ・ STA Status – スパニングツリー内のこのポートの現在の状態が表示されます。
 - ・ Discarding – ポートで STA 確認メッセージが受信されますが、パケットは転送されません。
 - ・ Learning – ポートで競合する情報が受信されることなく、「Forward Delay」パラメータで設定されている間隔で設定メッセージが送信されました。ポートでアドレステーブルがクリアされ、アドレス学習が開始されます。
 - ・ Forwarding – ポートでパケットが転送され、アドレス学習が続行されます。

ポートのステータスを規定する原則は、以下のとおりです。

- ・ 他に STA 対応ブリッジングデバイスが存在しないネットワークセグメント上のポートは常に転送状態になります。
- ・ スwitchの2つのポートが同じセグメントに接続しており、そのセグメントに接続している STA デバイスが他にない場合には、ID の値が小さい方のポートがパケットを転送し、もう一方のポートは破棄状態になります。
- ・ スwitchの Boot 時にはすべてのポートが破棄状態になり、その後、いくつかのポートが学習状態になってから、転送状態になります。
- ・ Forward Transitions – このポートが学習状態から転送状態に遷移した回数。
- ・ 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伝送されるパケットのコスト。メディア速度が遅い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優先度と MAC アドレス。
- ・ Designated Port – このポートがスパニングツリーのルートと通信するために使用する必要がある代表ブリッジングデバイス上のポートの優先度と MAC アドレス。
- ・ Oper Path Cost – このポートが含まれているスパニングツリーのルートへのパスコストに算入される、このポートのコスト。
- ・ Oper Link Type – このインターフェースに接続されている LAN セグメントの稼働時のポイントツーポイントステータス。このパラメータは、STA インターフェース設定の「Admin Link Type」で説明されているように、手動設定または自動検出によって指定されます。

- ・ Oper Edge Port – このパラメータは、STA インターフェース設定の「Admin Edge Port」の値（Enabled、Disabled、または Auto）に初期設定されますが、BPDU が受信されると、他のブリッジがこのポートに接続されていることを示す Disabled に設定されます。
- ・ Port Role – ポートはアクティブトポロジの設定要素であるかどうかに応じて割り当てられます。この役割とは、非ルートブリッジをルートブリッジに接続する最適ポート（ルートポート）、ブリッジを使用して LAN をルートブリッジに接続するポート（代表ポート）、MSTI 領域ポートとなるポート（マスターポート）、あるいは、他のブリッジ、ブリッジポートまたは LAN の障害発生時や削除時に接続性を提供する代替ポートまたはバックアップポートとなるポートです。ポートがスパニングツリー内で何の役割も割り当てられていない場合、役割は無効（無効ポート）に設定されます。

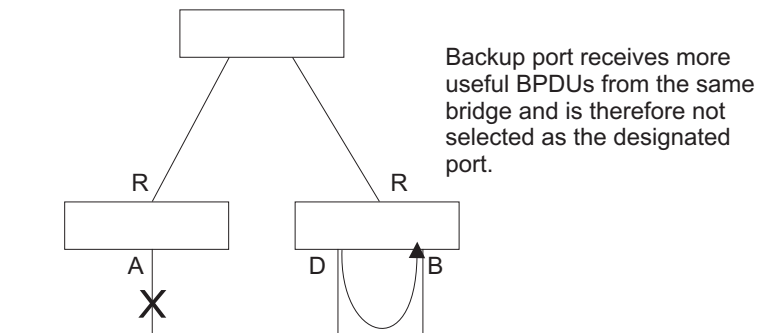


図 1-11: STA ポートの役割

** 図の注釈

代替ポートは、より有効な BPDU を他のブリッジから受信するため、代表ポートとして選択されない。

R: ルートポート

A: 代替ポート

D: 代表ポート

B: バックアップポート

バックアップポートは、より有効な BPDU を同じブリッジから受信するため、代表ポートとして選択されない。

Web インターフェース

STA のインターフェース設定を表示するには、以下のようにします。

- (1) 「Spanning Tree」 → 「STA」 を選択します。
- (2) 「Step」 リストで 「Configure Interface」 を選択します。
- (3) 「Step」 リストで 「Show Information」 を選択します。

Spanning Tree > STA

Step: 2. Configure Interface

Action: Show Information

Interface

☒ Port
 ☐ Trunk

Spanning Tree Port List

Max: 26 Total: 26

1 2 3

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	2	0	32768.0000E89382A0	128.1	100000	Point-to-Point	Disabled	Designated
2	Enabled	Enabled	Discarding	1	0	32768.0000E89382A0	128.2	10000	Point-to-Point	Disabled	Disabled
3	Enabled	Enabled	Discarding	1	0	32768.0000E89382A0	128.3	10000	Point-to-Point	Disabled	Disabled
4	Enabled	Enabled	Discarding	0	0	32768.0000E89382A0	128.4	10000	Point-to-Point	Disabled	Disabled
5	Enabled	Enabled	Discarding	0	0	32768.0000E89382A0	128.5	10000	Point-to-Point	Disabled	Disabled

画面 1-85 : STA のインターフェース設定の表示

1.6.7 マルチプルスパニングツリー（MSTP）の設定

「Spanning Tree」→「MSTP」（Configure Global）を選択すると、MSTP インスタンスを作成することや、VLAN グループを MSTP インスタンスに追加することができます。

関連する CLI 情報

「Spanning Tree Commands」

コマンドの使用

MSTP では、インスタンスごとに固有のスパニングツリーが生成されます。そのようにすることで、ネットワーク全体で複数の経路が提供されます。その結果、トラフィックの負荷が分散されるので、単一インスタンス内のブリッジノードで障害が発生した場合に大規模な機能停止状態に陥るのを回避したり、障害が発生したインスタンスの新しいトポロジの速やかな輻輳制御を実現したりできるようになります。

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）に割り当てられます。本製品でサポートされるインスタンスの最大数は 33 であるため、ご使用のネットワークの同じ共有領域をカバーする 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は同じ一連のインスタンスを指定して設定する必要があり、（各ブリッジの）同じインスタンスは同じ一連の VLAN を指定して設定する必要があるということを忘れないでください。また、RSTP では、各 MSTI 領域は単一のノードとして処理され、すべての領域は共通スパニングツリーに接続されるということにも注意してください。

マルチプルスパニングツリーを使用するには、以下のようにします。

- （1）スパニングツリーのタイプを「MSTP」に設定します。
- （2）選択した MST インスタンスのスパニングツリー優先度を入力します（「Spanning Tree」→「MSTP」（Configure Global - Add）を選択して表示される画面を使用）。
- （3）この MSTI を共有する VLAN を追加します（「Spanning Tree」→「MSTP」（Configure Global - Add Member）を選択して表示される画面を使用）。

【注意】 すべての VLAN が自動的に IST（インスタンス 0）に追加されます。

MSTI がネットワーク全体にわたる接続性を維持できるようにするには、同じ MSTI 設定を使用して、関連する一連のブリッジを設定する必要があります。

パラメータ

以下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 ID（範囲：0 ～ 4,094）。
- ・ VLAN ID - この MST インスタンスに割り当てる VLAN の ID（範囲：1 ～ 4,093）。
- ・ Priority - スパニングツリーインスタンスの優先度（範囲：0 ～ 61,440（4,096 の倍数）、オプション：0、4,096、8,192、12,288、16,384、20,480、24,576、28,672、32,768、36,864、40,960、45,056、49,152、53,248、57,344 または 61,440、デフォルト：32,768）。

Web インターフェース

MSTP のインスタンスを作成するには、以下のようにします。

- (1) 「Spanning Tree」 → 「MSTP」 を選択します。
- (2) 「Step」 リストで 「Configure Global」 を選択します。
- (3) 「Step」 リストで 「Add」 を選択します。
- (4) MST インスタンス ID および最初の VLAN メンバーを指定します。メンバーは、「Spanning Tree」 → 「MSTP」 (Configure Global - Add Member) を選択して表示される画面で追加することができます。優先度が指定されていない場合は、デフォルト値 32,768 が使用されます。
- (5) < Apply > ボタンをクリックします。

Spanning Tree > MSTP

Step: 1. Configure Global Action: Add

MST ID (0-4094) 1

VLAN ID (1-4093) 1

Priority (0-61440, in steps of 4096)

Apply Revert

画面 1-86 : MST インスタンスの作成

MST インスタンスを表示するには、以下のようにします。

- (1) 「Spanning Tree」 → 「MSTP」 を選択します。
- (2) 「Step」 リストで 「Configure Global」 を選択します。

(3) 「Step」 リストで「Show」を選択します。

The screenshot shows the 'Spanning Tree > MSTP' configuration page. At the top, there is a 'Step' dropdown menu set to '1. Configure Global' and an 'Action' dropdown menu set to 'Show'. Below this, the 'MST List' is displayed with 'Max: 33' and 'Total: 10'. The table has two columns: a checkbox column and an 'MST ID' column. The table contains six rows with MST IDs 0 through 5, each with an unchecked checkbox.

	MST ID
☐	0
☐	1
☐	2
☐	3
☐	4
☐	5

画面 1-87 : 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、以下のようにします。

- (1) 「Spanning Tree」 → 「MSTP」 を選択します。
- (2) 「Step」 リストで「Configure Global」を選択します。
- (3) 「Step」 リストで「Modify」を選択します。
- (4) MST インスタンスの優先度を変更します。
- (5) < Apply > ボタンをクリックします。

The screenshot shows the 'Spanning Tree > MSTP' configuration page with the 'Action' dropdown menu set to 'Modify'. Below this, the 'MST Details List' is displayed with 'Max: 33' and 'Total: 10'. The table has two columns: 'MST ID' and 'Priority (0-61440, in steps of 4096)'. The table contains six rows with MST IDs 0 through 5, each with a text input field for the priority value.

MST ID	Priority (0-61440, in steps of 4096)
0	0
1	4096
2	8192
3	0
4	0
5	0

画面 1-88 : MST インスタンスの優先度の変更

MSTP のグローバル設定を表示するには、以下のようにします。

- (1) 「Spanning Tree」 → 「MSTP」 を選択します。
- (2) 「Step」 リストで「Configure Global」を選択します。

Web 設定

スパニングツリーアルゴリズム

- (3) 「Step」 リストで「Show Information」を選択します。
- (4) MST ID を選択します。この画面に表示される属性については、「STA のグローバル設定の表示」で説明しています。

Spanning Tree > MSTP

Step: 1. Configure Global Action: Show Information

MST ID	1		
Priority	0	Designated Root	32768.0030F1245660
Bridge ID	20	Root Port	2
Max Age	15 sec	Root Path Cost	32768.000001010010
Hello Time	23 sec	Configuration Changes	500000
Forward Delay	2 sec	Last Topology Change	0 days, 1 hours, 10 minutes, 0 seconds

画面 1-89 : MST インスタンスのグローバル設定の表示

MSTP インスタンスに VLAN グループを追加するには、以下のようになります。

- (1) 「Spanning Tree」 → 「MSTP」を選択します。
- (2) 「Step」 リストで「Configure Global」を選択します。
- (3) 「Step」 リストで「Add Member」を選択します。
- (4) 「MST ID」リストで MST インスタンスを選択します。
- (5) インスタンスに追加する VLAN グループを「VLAN ID」フィールドに入力します。
指定するメンバーは設定済み VLAN でなくてもかまいません。
- (6) < Apply > ボタンをクリックします。

Spanning Tree > MSTP

Step: 1. Configure Global Action: Add Member

MST ID 1

VLAN ID (1-4093) 2

Apply Revert

画面 1-90 : MST インスタンスへの VLAN の追加

MST インスタンスの VLAN メンバーを表示するには、以下のようにします。

- (1) 「Spanning Tree」 → 「MSTP」 を選択します。
- (2) 「Step」 リストで 「Configure Global」 を選択します。
- (3) 「Step」 リストで 「Show Member」 を選択します。

The screenshot shows a web interface for configuring Spanning Tree > MSTP. At the top, there's a breadcrumb 'Spanning Tree > MSTP' and a help icon. Below that, there are two dropdown menus: 'Step: 1. Configure Global' and 'Action: Show Member'. Underneath, there's a field for 'MST ID' with a dropdown set to '0'. Below this is a 'Member List' section with a total count of 'Total: 4093'. To the right of the list are pagination controls showing numbers 1 through 10. The list itself is a table with two columns: a checkbox column and a 'VLAN' column. The table contains five rows, each with a checked checkbox and a VLAN number (1, 2, 3, 4, 5).

	VLAN
☒	1
☒	2
☒	3
☒	4
☒	5

画面 1-91 : MST インスタンスのメンバーの表示

1.6.8 MSTP のインターフェース設定の設定

「Spanning Tree」→「MSTP」（Configure Interface - Configure）を選択すると、MST インスタンスの STA インターフェース設定を設定することができます。

関連する CLI 情報

「Spanning Tree Commands」

パラメータ

以下のパラメータが表示されます。

- ・ MST Instance ID - 設定するインスタンス ID（デフォルト：0）。
- ・ Interface - ポートまたはトランクの一覧が表示されます。
- ・ STA Status - スパニングツリー内のこのインターフェースの現在の状態が表示されます（詳細については、「STA のインターフェース設定の表示」を参照）。
 - ・ Discarding - ポートで STA 確認メッセージが受信されますが、パケットは転送されません。
 - ・ Learning - ポートで競合する情報が受信されることなく、「Forward Delay」パラメータで設定されている間隔で設定メッセージが送信されました。ポートでアドレステーブルがクリアされ、アドレス学習が開始されます。
 - ・ Forwarding - ポートでパケットが転送され、アドレス学習が続行されます。
- ・ Priority - STP でこのポートに使用される優先度を定義します。スイッチのすべてのポートでパスコストが同じである場合には、優先度が最も高い（つまり、値が最も小さい）ポート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。そのようにすることで、STP でネットワークループが検出される場合に、優先度が高いポートほどブロックされる可能性が低くなるようになっています。最も高い優先度が複数のポートに割り当てられている場合には、ID の値が最も小さいポートが有効になります（デフォルト：128、範囲：0～240（16 の倍数））。
- ・ Admin Path Cost - このパラメータは、MSTP でデバイス間の最適パスを判別するために使用されます。そのため、接続先のメディアが高速であるほどポートに小さい値が割り当てられ、メディアが低速になるにつれてポートに大きい値が割り当てられなければなりません（パスコストがポート優先度よりも優先されます）。「Path Cost Method」が「Short」に設定されている場合は最大パスコストが 65,535 であるということに注意してください。

デフォルトでは、各ポートで使用されている速度と Duplex モードが自動的に検出され、以下の値に応じてパスコストが設定されます。パスコスト「0」は、自動設定モードを示します。ショートパスコスト方式が選択されており、IEEE 8021w 規格で推奨されているデフォルトのパスコストが 65,535 より大きい場合、デフォルトは 65,535 に設定されます。

推奨範囲は、表 12 のとおりです。

デフォルトのパスコストは、表 13（p.219）▲のとおりです。

Web インターフェース

ポートまたはトランクの MSTP パラメータを設定するには、以下のようにします。

- (1) 「Spanning Tree」 → 「MSTP」 を選択します。
- (2) 「Step」 リストで 「Configure Interface」 を選択します。
- (3) 「Step」 リストで 「Configure」 を選択します。
- (4) インターフェースの優先度とパスコストを入力します。
- (5) < Apply > ボタンをクリックします。

Spanning Tree > MSTP

Step: 2. Configure Interface Action: Configure

MST ID: 0

Interface: ☒ Port ☐ Trunk

Spanning Tree Port List Max: 26 Total: 26 1 2 3

Port	STA Status	Priority (0-240, in steps of 16)	Admin MST Path Cost (0-200000000, 0: Auto)
1	Forwarding	128	0
2	Discarding	128	0
3	Discarding	128	0
4	Discarding	0	50
5	Discarding	128	0

画面 1-92 : MSTP インターフェース設定の設定

ポートまたはトランクの MSTP パラメータを表示するには、以下のようにします。

- (1) 「Spanning Tree」 → 「MSTP」 を選択します。
- (2) 「Step」 リストで 「Configure Interface」 を選択します。

Web 設定

スパニングツリーアルゴリズム

(3) 「Step」 リストで「Show Information」を選択します。

Spanning Tree > MSTP

Step: 2. Configure Interface Action: Show Information

MST ID: 0

Interface: ☒ Port ☐ Trunk

Spanning Tree Port List Max: 26 Total: 26

Port	STA Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port	Oper Path Cost	Oper Link Type	Oper Edge Port	Port Role
1	Forwarding	3	0	32768.0.0000E89382A0	128.1	100000	Point-to-Point	Disabled	Designated
2	Discarding	0	0	32768.0.0000E89382A0	128.2	10000	Point-to-Point	Disabled	Disabled
3	Discarding	0	0	32768.0.0000E89382A0	128.3	10000	Point-to-Point	Disabled	Disabled

画面 1-93 : MSTP インターフェース設定の表示

1.7 輻輳制御

本製品では、任意のポートについて送受信時の最大データ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しきい値を設定することにより、トラフィックストームを制御することもできます。さらに、レートリミットの自動トリガーまたはポートのシャットダウンに使用できる、ブロードキャストストームおよびマルチキャストストームのしきい値を設定することもできます。

輻輳制御オプションには、以下のようなものがあります。

- ・ レートリミット – ポートの入力と出力のレートリミットを設定します。
- ・ ストームコントロール – インターフェースごとのトラフィックストームしきい値を設定します。
- ・ 自動トラフィック制御 – 設定済みのレートリミットのトリガーまたはポートのシャットダウンに使用できる、ブロードキャストストームおよびマルチキャストストームのしきい値を設定することができます。

1.7.1 レートリミット

「Traffic」→「Rate Limit」を選択すると、イングレスポートまたはエグレスポートにレートリミットを適用することができます。この機能を使用すれば、ネットワーク管理者は、インターフェースで送受信されるトラフィックの最大レートを制御できるようになります。レートリミットは、ネットワークに出入りするトラフィックを制限するため、ネットワークエッジのインターフェースで設定します。許容トラフィック量を超えるパケットはドロップされます。

レートリミットは、個々のポートまたはトランクに適用することができます。この機能を指定してインターフェースを設定すると、ハードウェアでトラフィックレートが監視されて制限に準拠しているかどうかを検証されます。準拠していないトラフィックはドロップされ、準拠しているトラフィックはそのまま変更されずに転送されます。

関連する CLI 情報

「Rate Limit Configuration」

パラメータ

以下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が表示されます。
- ・ Type – ポートタイプを示します（1000BASE-T、1000BASE SFP、または 10GBASE XFP）。
- ・ Status – レートリミットを有効または無効にします（デフォルト：Disabled）。
- ・ Rate – レートリミットレベルを設定します（範囲：64 ~ 1,000,000 kbps（ギガビットイーサネットポートの場合）または 64 ~ 10,000,000 kbps（10G イーサネットポートの場合））。

Web インターフェース

レートリミットを設定するには、以下のようにします。

- (1) 「Traffic」 → 「Rate Limit」 を選択します。
- (2) インターフェースタイプを「Port」または「Trunk」に設定します。
- (3) 必要なポートまたはトランクのレートリミットの「Status」を有効にします。
- (4) 個々のポートのレートリミットを設定します。
- (5) < Apply > ボタンをクリックします。

Traffic > Rate Limit

Port Rate Limit List Max: 26 Total: 26

Port	Type	Input		Output	
		Status	Rate (kbits/sec)	Status	Rate (kbits/sec)
1	1000Base-TX	☐ Enabled	1000000 (64-1000000)	☐ Enabled	1000000 (64-1000000)
2	1000Base-TX	☐ Enabled	1000000 (64-1000000)	☐ Enabled	1000000 (64-1000000)
3	1000Base-TX	☒ Enabled	600000 (64-1000000)	☒ Enabled	600000 (64-1000000)
4	1000Base-TX	☐ Enabled	1000000 (64-1000000)	☐ Enabled	1000000 (64-1000000)
5	1000Base-TX	☐ Enabled	1000000 (64-1000000)	☐ Enabled	1000000 (64-1000000)

画面 1-94 : レートリミットの設定

1.7.2 ストームコントロール

「Traffic」→「Storm Control」を選択すると、ブロードキャスト、マルチキャスト、および宛先不明ユニキャストのストームコントロールしきい値を設定することができます。トラフィックストームは、ネットワーク上のデバイスが正常に動作していない場合や、アプリケーションプログラムが適切に設計または設定されていない場合に発生する可能性があります。ネットワークのトラフィックが過剰な場合、パフォーマンスが大幅に低下したり、すべての機能が完全に停止したりすることがあります。

ブロードキャスト、マルチキャスト、または宛先不明ユニキャストのトラフィックのしきい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保護することができます。そのようにすると、指定したしきい値を超えるパケットは、すべて、ドロップされます。

関連する CLI 情報

「switchport packet-rate」

コマンドの使用

- ・ 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有効になります。
- ・ トラフィックがブロードキャスト、マルチキャスト、または宛先不明ユニキャストのトラフィックに指定されているしきい値を超えると、レートがそのしきい値を下回るようになるまで、しきい値を超えるパケットがドロップされます。
- ・ トラフィックストームは、ストームコントロール機能を使用してハードウェアレベルで制御することも、各種の制御アクションをトリガーする自動トラフィック制御機能を使用してソフトウェアレベルで制御することもできます。ただし、1つのポートに適用できるのは、それらの制御タイプのうちの1つだけです。ポートでハードウェアレベルのストームコントロールを有効にすると、そのポートでは自動ストームコントロールが無効になります。
- ・ この機能によって設定されるレトリミットは、「Auto Traffic Control」(Configure Interface) 画面で制御アクションがレトリミットに設定されている場合に自動ストームコントロールでも使用されます。
- ・ レトリミットとストームコントロールの両方を同じインターフェースで使用すると、予期せぬ結果を招く可能性があります。例えば、ギガビットイーサネットポートでブロードキャストストームコントロールが 5000 pps に設定され、レトリミットが 200,000 kbps に設定されているとします。200,000 kbps は回線レートの 1/5 であるため、受信レートは実際には 1,000 kbps になります。あるいは、ストームコントロールコマンドで設定された制限値 5,000 kbps の 1/5 になります。以上の理由から、これらの機能の両方を同じインターフェースで使用することはお勧めできません。

パラメータ

以下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一覧が表示されます。
- ・ Type - インターフェースタイプを示します (1000BASE-T、SFP、または 10G)。
- ・ Unknown Unicast - 宛先不明ユニ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。
- ・ 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：ブロードキャストの場合は Enabled、マルチキャストおよび宛先不明ユニキャストの場合は Disabled）。
- ・ Rate – レートとしてのしきい値レベル（パケット数 / 秒）（範囲：500 ～ 14,880,000 pps、デフォルト：宛先不明ユニキャストトラフィックおよびマルチキャストトラフィックの場合は Disabled、ブロードキャストトラフィックの場合は 500 pps）。

Web インターフェース

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、以下のようにします。

- (1) 「Traffic」 → 「Storm Control」 を選択します。
- (2) インターフェースタイプを「Port」または「Trunk」に設定します。
- (3) 「Status」 フィールドでストームコントロールを有効または無効にします。
- (4) 必要なしきい値を設定します。この値をを超えると、スイッチでパケットがドロップされるようになります。
- (5) < Apply > ボタンをクリックします。

Traffic > Storm Control

Interface ☒ Port ☐ Trunk

Port Storm Control List Max: 26 Total: 26 1 2 3

Port	Type	Unknown Unicast		Multicast		Broadcast	
		Status	Rate (packets/sec)	Status	Rate (packets/sec)	Status	Rate (packets/sec)
1	1000Base-T	☐ Enabled	262143 (500-262143)	☐ Enabled	262143 (500-262143)	☒ Enabled	500 (500-262143)
2	1000Base-T	☐ Enabled	262143 (500-262143)	☐ Enabled	262143 (500-262143)	☒ Enabled	500 (500-262143)
3	1000Base-T	☒ Enabled	500 (500-262143)	☐ Enabled	262143 (500-262143)	☐ Enabled	500 (500-262143)
4	1000Base-T	☐ Enabled	262143 (500-262143)	☐ Enabled	262143 (500-262143)	☒ Enabled	500 (500-262143)
5	1000Base-T	☐ Enabled	262143 (500-262143)	☐ Enabled	262143 (500-262143)	☒ Enabled	500 (500-262143)

画面 1-95 : ストームコントロールの設定

1.7.3 自動トラフィック制御

「Traffic」→「Congestion Control」→「Auto Traffic Control」を選択すると、ブロードキャストストームおよびマルチキャストストームのしきい値を設定して、自動的にレートリミットがトリガーされるようにしたり、ポートがシャットダウンされるようにしたりすることができます。

関連する CLI 情報

「Automatic Traffic Control Commands」

コマンドの使用

ATC には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ストームコントロール機能が組み込まれています。以下の図に示すように、それらのトラフィックタイプのいずれについても制御アクションは同じです。

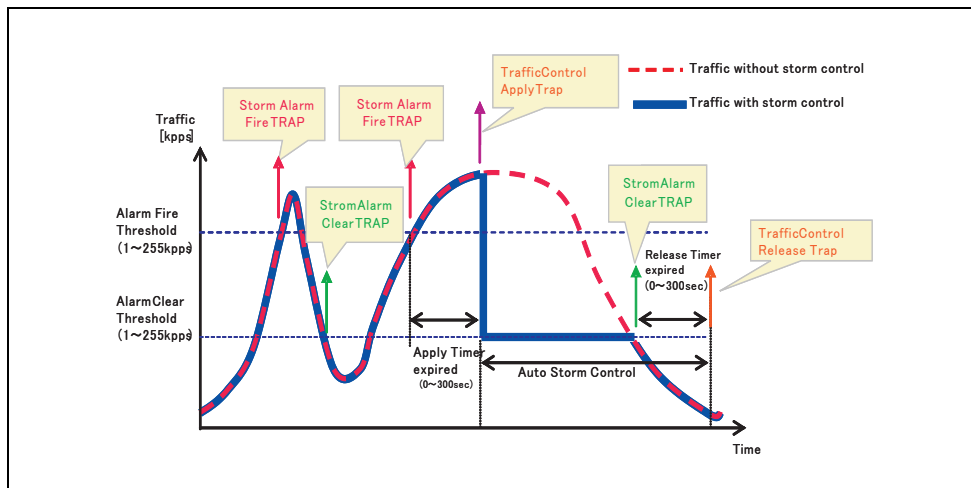


図 1-12: トラフィックレートリミットによるストームコントロール

この図の主要な要素の説明は、以下のとおりです。

- ・ Alarm Fire しきい値 – 最大許容トラフィックレート。イングレストラフィックがこのしきい値を超えると、ATC によって Storm Alarm Fire トラップが送信されてログに記録されます。
- ・ トラフィックが Alarm Fire しきい値を超えてから適用タイマーで設定されている期間が過ぎると、トラフィック制御アクションが適用され、Traffic Control Apply トラップが送信されてログに記録されます。
- ・ Alarm Clear しきい値 – トラフィックがこの下限しきい値を下回ってから解除タイマーで設定されている期間が過ぎると、制御アクションが自動的に停止されます。イングレストラフィックがこのしきい値を下回ると、ATC によって Storm Alarm Clear トラップが送信されてログに記録されます。
- ・ トラフィックが Alarm Clear しきい値を下回ってから解除タイマーで設定されている期間が過ぎると、(レートリミットのための) トラフィック制御が停止され、Traffic Control Release トラップが送信されてログに記録されます。制御アクションによってポートがシャットダウンされている場合、そのポートは、手動制御解除機能を使用して手動でのみ再び有効にすることができます。

- ・ レートリミットのためのトラフィック制御アクションは自動的に解除されるようにすることも、手動で解除することもできます。ポートをシャットダウンする制御アクションは、手動でのみ解除することができます。

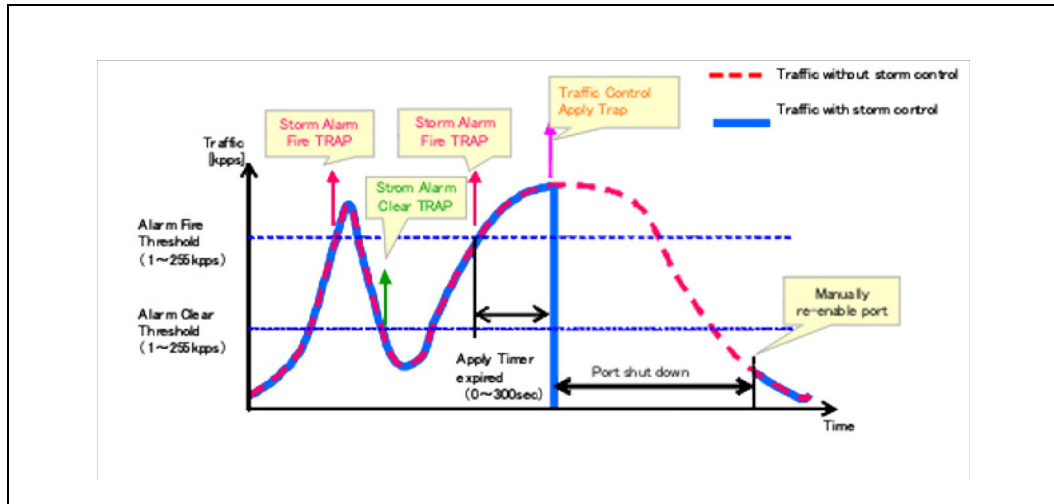


図 1-13: ポートのシャットダウンによるストームコントロール

この図の主要な要素は、制御アクションの自動解除機能が用意されていない点を除き、直前の図に表されているものと同じです。トラフィック制御が適用された場合は、手動でポートを有効にする必要があります。

機能に関する制限事項

自動ストームコントロールは、ソフトウェアレベルの制御機能です。トラフィックストームは、ポートブロードキャスト制御機能またはポートマルチキャスト制御機能を参照）を使用してハードウェアレベルで制御することもできます。ただし、1つのポートに適用できるのは、それらの制御タイプのうちの1つだけです。ポートで自動ストームコントロールを有効にすると、そのポートではハードウェアレベルのストームコントロールが無効になります。

ATC のタイマーの設定

「Traffic」→「Auto Traffic Control」(Configure Global) を選択すると、イングレストラフィックが上限しきい値を超えてから制御アクションが適用されるまでの期間、およびイングレストラフィックが下限しきい値を下回ってから制御アクションが解除されるまでの期間を設定することができます。

関連する CLI 情報

「auto-traffic-control apply-timer」

「auto-traffic-control release-timer」

コマンドの使用

- ・ 適用タイマーで設定されている期間が過ぎると、「Traffic」→「Automatic Traffic Control」(Configure Interface) を選択して表示される画面で指定されている設定を使用して、「(Action)」フィールドで設定されている）制御アクションをトリガーするか、「(Trap Storm Fire)」フィールドで設定されている）トラップメッセージが送信されるかが判別されます。

- ・ 解除タイマーは、「Automatic Traffic Control」(Interface Configuration) 画面の「Action」フィールドで設定されているレート制御アクションのみに適用されます。制御アクションによってポートがシャットダウンされている場合は、手動制御解除機能を使用して手動でポートを再び有効にしなければなりませんを参照)。

パラメータ

以下のパラメータが表示されます。

- ・ Broadcast Apply Timer – 上限しきい値を超えてから制御アクションがブロードキャストストームに適用されるまでの期間 (範囲: 1 ~ 300 秒、デフォルト: 300 秒)。
- ・ Broadcast Release Timer – イングレストラフィックがブロードキャストストームの下限しきい値を下回ってから制御アクションが解除されるまでの期間 (範囲: 1 ~ 900 秒、デフォルト: 900 秒)。
- ・ Multicast Apply Timer – 上限しきい値を超えてから制御アクションがマルチキャストストームに適用されるまでの期間 (範囲: 1 ~ 300 秒、デフォルト: 300 秒)。
- ・ Multicast Release Timer – イングレストラフィックがマルチキャストストームの下限しきい値を下回ってから制御アクションが解除されるまでの期間 (範囲: 1 ~ 900 秒、デフォルト: 900 秒)。

Web インターフェース

自動ストームコントロールの対応タイマーを設定するには、以下のようにします。

- (1) 「Traffic」 → 「Automatic Storm Control」 を選択します。
- (2) 「Step」 リストで 「Configure Global」 を選択します。
- (3) ブロードキャストストームおよびマルチキャストストームの適用タイマーと解除タイマーを設定します。
- (4) < Apply > ボタンをクリックします。

Traffic > Auto Traffic Control

Step: 1. Configure Global

Broadcast Apply Timer (1-300)	300	sec
Broadcast Release Timer (1-900)	900	sec
Multicast Apply Timer (1-300)	300	sec
Multicast Release Timer (1-900)	900	sec

画面 1-96 : ATC タイマーの設定

ATC のしきい値の設定

「Traffic」→「Auto Traffic Control」(Configure Interface) を選択すると、ストームコントロールモード（ブロードキャストまたはマルチキャスト）、トラフィックのしきい値、制御アクション、レートリミット対応の自動解除、または関連する SNMP トラップメッセージの送信を設定することができます。

関連する CLI 情報

「Automatic Traffic Control Commands」

パラメータ

以下のパラメータが表示されます。

- ・ Storm Control – 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自動ストームコントロールを指定します。
- ・ Port – ポート ID。
- ・ State – ブロードキャストストームまたはマルチキャストストームの自動トラフィック制御を有効にします（デフォルト：Disabled）。
- ・ 自動ストームコントロールは、ソフトウェアレベルの制御機能です。トラフィックストームは、「Storm Control」メニューを使用してハードウェアレベルで制御することもできます。ただし、1 つのポートに適用できるのは、これらの制御タイプのうちの 1 つだけです。ポートで自動ストームコントロールを有効にすると、そのポートではハードウェアレベルのストームコントロールが無効になります。
- ・ Action – Alarm Fire しきい値（上限しきい値）を超えてから適用タイマーで設定されている期間が過ぎると、以下のいずれかの制御アクションがトリガーされます。
 - ・ Rate Control – イングレストラフィックのレートを Alarm Clear しきい値で設定されるレベルに制限します。レートリミットは、トラフィックレートが Alarm Clear しきい値（下限しきい値）を下回ってから解除タイマーで設定されている期間を過ぎた場合にのみ、停止されます（これがデフォルトの対応です）。
 - ・ Shutdown – ポートを無効にします。自動トラフィック制御機能によって無効にされたポートは、Manual Control Release 属性を使用して手動でのみ再び有効にすることができます。
- ・ Auto Release Control – 図 104（p.234）▲に示すように、トラフィックが Alarm Clear しきい値を下回ってから解除タイマーで設定されている期間が過ぎるとレートリミットのためのトラフィック制御アクションが自動的に停止されます（デフォルト：Disabled）。トラフィック制御が停止すると、そのイベントがログに記録されます。それから、Traffic Release トラップが送信されることもあります（デフォルト：Disabled）。
- ・ 自動制御の解除が有効になっていない状態でレートリミットのための制御アクションがトリガーされた場合は、Manual Control Release 属性を使用して手動でレートリミット対応を停止することができます。制御アクションによってポートがシャットダウンされている場合、そのポートは、手動制御解除機能を使用して再び有効にすることもできます。
- ・ Alarm Fire Threshold – イングレストラフィックの上限しきい値であり、この値を超えてから適用タイマーで設定されている期間が過ぎるとストームコントロールアクションがトリガーされます（範囲：1 ~ 255 kpps、デフォルト：128 kpps）。トラフィックレートが上限しきい値を超えてから適用タイマーで設定されている期間が過ぎると、トラップメッセージが Trap Storm Fire 属性によって設定されている場合には、その設定されているメッセージが送信されます。

- ・ Alarm Clear Threshold – イングレストラフィックの下限しきい値であり、この値を下回ってから解除タイマーで設定されている期間が過ぎるとレート制御のための制御アクションが解除されます（範囲：1 ～ 255 kpps、デフォルト：128 kpps）。制御アクションとしてレトリミットが設定されており、自動制御解除が有効になっている場合、レトリミットは、トラフィックレートが下限しきい値を下回ってから解除タイマーで設定されている期間を過ぎると停止されます。ただし、制御アクションによってポートがシャットダウンされた場合は自動トラフィック制御によってそのポートが再び有効になることはないので注意してください。その場合は手動制御解除機能を使用して手動でのみ再び有効にすることができます。トラフィックレートが下限しきい値を下回ってから解除タイマーで設定されている期間が過ぎると、トラップメッセージが Trap Storm Clear 属性によって設定されている場合には、その設定されているメッセージが送信されます。
- ・ Trap Storm Fire – トラフィックが自動ストームコントロールの上限しきい値を超えた場合にトラップを送信します（デフォルト：Disabled）。
- ・ Trap Storm Clear – ストームコントロールがトリガーされた後にトラフィックが下限しきい値を下回った場合にトラップを送信します（デフォルト：Disabled）。
- ・ Trap Traffic Apply – トラフィックが自動ストームコントロールの上限しきい値を超えてから適用タイマーで設定されている期間が過ぎた場合にトラップを送信します（デフォルト：Disabled）。
- ・ Trap Traffic Release – ストームコントロールアクションがトリガーされた後にトラフィックが下限しきい値を下回ってから解除タイマーで設定されている期間が過ぎた場合にトラップを送信します（デフォルト：Disabled）。
- ・ Manual Control Release – 指定されているアクションがトリガーされた後にレトリミットまたはポートのシャットダウンのための制御アクションを手動で解除します。この機能をいずれかのポートに対して有効にする場合は、チェックボックスをオンにしてから < Apply > ボタンをクリックします。

Web インターフェース

自動ストームコントロールの対応タイマーを設定するには、以下のようにします。

- (1) 「Traffic」 → 「Automatic Storm Control」 を選択します。
- (2) 「Step」 リストで 「Configure Interface」 を選択します。
- (3) ATC を必要に応じて有効または無効にし、制御アクションを設定して、レトリミットのための制御アクションを自動解除するかどうかを指定し、上限および下限のしきい値を設定し、送信するトラップメッセージを指定します。

(4) < Apply > ボタンをクリックします。

Traffic > Auto Traffic Control ?

Step: 2. Configure Interface

Storm Control ☒ Broadcast ☐ Multicast

Auto Traffic Control Broadcast List Total: 26 1 2 3

Port	State	Action	Auto Release Control	Alarm Fire Threshold (1-255 kpps)	Alarm Clear Threshold (1-255 kpps)	Trap Storm Fire	Trap Storm Clear	Trap Traffic Apply	Trap Traffic Release	Manual Control Release
1	☐ Enabled	Rate Control	☐ Enabled	128	128	☐ Enabled	☐ Enabled	☐ Enabled	☐ Enabled	☐ Enabled
2	☐ Enabled	Rate Control	☐ Enabled	128	128	☐ Enabled	☐ Enabled	☐ Enabled	☐ Enabled	☐ Enabled
3	☐ Enabled	Rate Control	☐ Enabled	128	128	☐ Enabled	☐ Enabled	☐ Enabled	☐ Enabled	☐ Enabled
4	☐ Enabled	Rate Control	☐ Enabled	128	128	☐ Enabled	☐ Enabled	☐ Enabled	☐ Enabled	☐ Enabled
5	☐ Enabled	Rate Control	☐ Enabled	128	128	☐ Enabled	☐ Enabled	☐ Enabled	☐ Enabled	☐ Enabled

画面 1-97 : ATC インターフェース属性の設定

1.8 CoS (Class of Service)

CoS (Class of Service) 機能を使用すると、輻輳のためトラフィックがスイッチのバッファに入れられた場合にどのデータパケットが優先的に処理されるようにするか指定することができます。本製品は、ポートごとに 8 つのレベルの優先度を指定できる CoS 機能をサポートしています。ポートの優先度が高いキューに入れられているデータパケットは、優先度が低いキューのパケットよりも先に送信されます。インターフェースごとにデフォルトの優先度を設定し、フレームの優先度タグとスイッチの優先キューとのマップを設定することができます。

本章では、以下の基本的なトピックについて説明します。

- ・ レイヤ 2 のキューの設定 - デフォルトの優先度、キューモード、キューの重み、タグの CoS 値に基づくキューへのパケットのマッピングを含めた、各キューの設定を指定します。
- ・ レイヤ 3/4 優先度の設定 - TCP ポート、IP 優先順位タグ、または IP DSCP タグを CoS 値にマップします。

1.8.1 レイヤ 2 のキューの設定

ここでは、タグなしフレームのデフォルトの優先度の設定、キューモードの設定、各キューに割り当てられる重みの設定、キューへのタグの CoS 値によるマッピングのそれぞれの方法について説明します。

インターフェースのデフォルトの優先度の設定

「Traffic」→「Priority」→「Default Priority」を選択すると、スイッチの各インターフェースのデフォルトのポート優先度を指定することができます。スイッチに入ってくるすべてのタグなしパケットは、指定されているデフォルトのポート優先度を含むタグが付けられてから、出力ポートの該当の優先度のキューに入れられます。

関連する CLI 情報

「switchport priority default」

コマンドの使用

- ・ 本製品は、ポートごとに 8 つのキューを提供します。本製品は、重み付きラウンドロビン (WRR: Weighted Round Robin) 方式を使用して先頭キューブロッキングを回避しますが、各キューを厳密な順序で処理する (Strict キューイング) ように設定することも、Strict キューイングと重み付き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。
- ・ 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ありフレームの両方を受信する) ように設定されているポートで受信されるタグなしフレームに適用されます。デフォルトの優先度は、IEEE 802.1Q VLAN タグ付きフレームには適用されません。着信フレームが IEEE 802.1Q VLAN タグ付きフレームである場合には、IEEE 802.1p の User Priority ビットが使用されます。
- ・ 出力ポートが、関連付けられている VLAN のタグなしメンバーである場合、IEEE 802.1Q VLAN タグ付きフレームは、すべての VLAN タグを取り除かれてから送信されます。

パラメータ

Web 設定

CoS (Class of Service)

以下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一覧が表示されます。
- ・ CoS – 指定されているインターフェースで受信されたタグなしフレームに割り当てられる優先度（範囲：0～7、デフォルト：0）。

Web インターフェース

キューモードを設定するには、以下のようにします。

- (1) 「Traffic」 → 「Priority」 → 「Default Priority」 を選択します。
- (2) 表示されるインターフェースタイプ（「Port」 または 「Trunk」）を選択します。
- (3) いずれかのインターフェースのデフォルトの優先度を変更します。
- (4) < Apply > ボタンをクリックします。

Traffic > Priority > Default Priority

Interface ☒ Port ☐ Trunk

Port to CoS Mapping Table Max: 26 Total: 26

Port	CoS (0-7)
1	0
2	0
3	5
4	0
5	0

画面 1-98：デフォルトのポート優先度の設定

キューモードの選択

「Traffic」→「Priority」→「Queue」を選択すると、任意のインターフェースのエグレスキューのキューモードを設定することができます。本製品は、優先度の高いキューに入れられているすべてのトラフィックが処理されてから優先度の低いキューが処理されるという厳密なルールに基づいてキューが処理されるように設定することも、各キューのスケジューリングの重みを指定する重み付きラウンドロビン（WRR）キューを使用するように設定することもできます。また、Strict キューイングと重み付きキューイングを組み合わせで使用するように設定することもできます。

関連する CLI 情報

「queue mode」

「show queue mode」

コマンドの使用

- ・ Strict キューイングでは、優先度の高いキューに入れられているすべてのトラフィックが処理されてから優先度の低いキューが処理されます。
- ・ WRR キューイングでは、各キューの相対的な重みを指定します。WRR では、キューごとに事前に定義されている相対的な重みを使用して、スイッチが各キューを処理してから次のキューの処理に移るまでのサービス時間の割合が決まります。そのようにすることで、Strict キューイングを使用した場合に発生することがある（QoS における）HOL ブロッキングを回避します。
- ・ 「Strict and WRR」モードを選択すると、優先度の高いキューには厳密なサービスが使用され、残りのキューには重み付きサービスが使用されます。厳密な優先度を使用するように割り当てられるキューは、「Strict Mode」フィールドパラメータを使用して指定しなければなりません。
- ・ 重みは、それぞれの重み付きキュー（ひいては、対応するトラフィック優先度）に割り当てることができます。この重みによって、各キューが処理のためにポーリングされる間隔が設定されます。また、この重みは、後で、特定の優先度値が割り当てられているソフトウェアアプリケーションの応答時間に影響を及ぼします。
- ・ エグレスポートにおけるサービス時間は、WRR のスケジューリングの重みを定義することによって、または、Strict キューイングと重み付き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 つを指定することによって、共有されます。

パラメータ

以下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一覧が表示されます。
- ・ Queue Mode
 - ・ Strict - エグレスキューを順番に処理します。優先度が高いキューのすべてのトラフィックが送信されてから、優先度が低いキューが処理されます。そのようにすることで、常に、優先度が最も高いパケットが他のすべてのトラフィックよりも先に処理されるようにします。
 - ・ WRR - 重み付きラウンドロビンでは、スケジューリングの重みを使用することにより、また、各キューをラウンドロビン方式で処理することにより、エグレスポートにおける帯域幅の共有を実現します。これは、デフォルトで選択されています。
 - ・ Strict and WRR - 優先度が高いキューについては厳密な優先度を使用し、残りのキューについては WRR を使用します。
- ・ Queue ID - 優先度キューの ID（範囲：0～7）。

Web 設定

CoS (Class of Service)

- ・ Strict Mode - 「Strict and WRR」モードを選択すると、優先度の高いキューには厳密なサービスが使用され、残りのキューには重み付きサービスが使用されます。このパラメータを使用して、厳密な優先度を使用するために割り当てられるキューを指定します（デフォルト: Disabled）。
- ・ Weight - WRR スケジューラで使用される各キューの重みを設定します（範囲: 1 ~ 15、デフォルト: キュー 0 ~ 7 に重み 1、2、4、6、8、10、12、14 がそれぞれ割り当てられています）。

Web インターフェース

キューモードを設定するには、以下のようにします。

- (1) 「Traffic」→「Priority」→「Queue」を選択します。
- (2) 表示されるインターフェースタイプ（「Port」または「Trunk」）を選択します。
- (3) キューモードを設定します。
- (4) いずれかの重み付きキューモードを選択した場合は、必要に応じてキューの重みを変更することができます。
- (5) Strict キューイングと重み付きキューイングの組み合わせを使用するキューモードの 1 つを選択した場合は、表で「Strict Mode」パラメータを有効にして、先に処理されるサービスを指定する必要があります。
- (6) < Apply > ボタンをクリックします。

The screenshot shows a web interface for configuring network settings. At the top, a breadcrumb trail reads "Traffic > Priority > Queue". Below this, there are two sections. The first section is labeled "Interface" and contains two radio buttons: "Port" (which is selected) and "Trunk". Each radio button is followed by a dropdown menu showing the number "1". The second section is labeled "Queue Mode" and contains a dropdown menu with "Strict" selected. At the bottom right of the form, there are two buttons: "Apply" and "Revert".

画面 1-99 : キューモード (Strict) の設定

Traffic > Priority > Queue

Interface ☒ Port 1 ☐ Trunk

Queue Mode

Queue Setting Table Max: 8 Total: 8

Queue ID	Weight (1-15) in ascending order
0	1
1	2
2	4
3	6
4	8
5	10
6	12
7	14

画面 1-100 : キューモード (WRR) の設定

Traffic > Priority > Queue

Interface ☒ Port 1 ☐ Trunk

Queue Mode

Queue Setting Table Max: 8 Total: 8

Queue ID	Strict Mode	Weight (1-15) in ascending order
0	Enabled	1
1	Enabled	2
2	Disabled	4
3	Disabled	6
4	Disabled	8
5	Disabled	10
6	Disabled	12
7	Disabled	14

画面 1-101 : キューモード (Strict and WRR) の設定

出力キューへの CoS 値のマッピング

「Traffic」→「Priority」→「CoS to Queue」を選択すると、CoS (Class of Service) 優先度タグ付きトラフィックに使用されるハードウェア出力キューを指定することができます。

本製品では、ポートごとに 8 つの優先度キューを使用して、または、厳密な優先度に基づくサービススケジュール、重み付きラウンドロビン (WRR)、Strict キューイングと重み付きキューイングの組み合わせのいずれかを使用して、CoS 優先度タグ付きトラフィックを処理します。IEEE 802.1p では、最大 8 つの個別のトラフィック優先度が規定されています。デフォルトの優先レベルは、IEEE 802.1p 規格の推奨事項に従って、以下の表のように割り当てられます。

表 1-1

プライオリティ	0	1	2	3	4	5	6	7
キュー	2	0	1	3	4	5	6	7

表 14: IEEE 802.1p エグレスキューの優先度マッピング

各種のネットワークアプリケーションについて IEEE 802.1p 規格で推奨されている優先レベルは、表 15 のとおりです。ただし、ネットワークのアプリケーショントラフィックが効果的に処理されるように優先レベルをスイッチの出力キューにマップすることができます。

優先レベル	トラフィックタイプ
1	バックグラウンド
2	予備)
0	(デフォルト) ベストエフォート
3	エクセレントエフォート
4	負荷制御
5	ビデオ (ジッタと遅延が 100 ms 未満)
6	音声 (ジッタと遅延が 10 ms 未満)
7	ネットワーク制御

表 15: CoS の優先レベル

関連する CLI 情報

「queue cos-map」

「show queue cos-map」

コマンドの使用

- ・ エグレスパケットは、このコマンドで定義されるマッピングに従ってハードウェアキューに入れられます。
- ・ 指定されたマッピングはすべてのインターフェースに適用されます。

パラメータ

以下のパラメータが表示されます。

- ・ Priority – CoS 値 (範囲 : 0 ~ 7 (7 が最高優先度))。
- ・ Queue – 出力キューバッファ (範囲 : 0 ~ 7 (7 が最高優先度))。

Web インターフェース

CoS 優先度タグ付きトラフィックに使用される出力キューを指定するには、以下のようになります。

- (1) 「Traffic」 → 「Priority」 → 「CoS to Queue」 を選択します。
- (2) 優先度を出力キューに割り当てます。
- (3) < Apply > ボタンをクリックします。

Traffic > Priority > CoS to Queue

CoS to Queue Mapping Table Total: 8

CoS	Queue (0-7)
0	2
1	0
2	1
3	3
4	4
5	5
6	6
7	7

[Restore Default](#) [Click this button to restore default queue values.](#)

[Apply](#) [Revert](#)

画面 1-102 : エグレスキューへの CoS 値のマッピング

1.8.2 レイヤ 3/4 優先度の設定

CoS 値へのレイヤ 3/4 優先度のマッピング

本製品は、アプリケーションの要件を満たすようにレイヤ 3/4 トラフィックの優先度を設定するための一般的な方法をいくつかサポートしています。トラフィックの優先度は、ToS (Type of Service) オクテットの優先度ビットを使用してフレームの IP ヘッダで指定することも、TCP/UDP ポートの番号によって指定することもできます。優先度ビットを使用する際には、ToS オクテットには 3 bits (IP 優先順位の場合) または 6 bits (DSCP (Differentiated Services Code Point) サービスの場合) を含めることができます。それらのサービスを有効にすると、優先度が CoS 値にマップされ、トラフィックが該当の出力キューに送信されるようになります。

トラフィックには異なる優先度情報が含まれていることがあるため、本製品では、以下の方法で優先度値を出力キューにマップします。

- ・ マッピングでは、各種の優先度が、IP ポート優先度、IP 優先順位または DSCP 優先度、デフォルトのポート優先度の順で優先されます。
- ・ IP 優先順位と IP DSCP を両方とも有効にすることはできません。一方の優先度タイプを有効にすると、自動的に、もう一方のタイプが無効になります。

DSCP 優先度のマッピング

「Traffic」→「Priority」→「IP DSCP to CoS」を選択すると、インGRESパケットで検出される IP DSCP 優先度を内部的な優先度処理用の CoS 値にマップすることができます。

関連する CLI 情報

「map ip dscp (Global Configuration)」

「map ip dscp (Global Configuration)」

「show map ip dscp」

コマンドの使用

- ・ DSCP は、6 bits 単位であり、最大 64 の異なる転送動作のコーディングを可能にします。DSCP は、DSCP 非対応のデバイスで DSCP マッピングとの競合が発生しないようにするため、3 bits の優先度ビットとの下位互換性を備えています。ネットワークポリシーに基づき、各種のトラフィックを転送方法別にマーキングすることができます。
- ・ DSCP 優先度値は、IEEE 802.1p 規格の推奨事項に従ってデフォルトの CoS 値にマップされ、後で、8 つのハードウェア優先度キューにマップされます。デフォルトのマッピングは、以下の表のように定義されています。指定されない DSCP 値は、すべて、CoS 値 0 にマップされるということに注意してください。

IP DSCP 値	CoS 値
0	0
8	1
10, 12, 14, 16	2
18, 20, 22, 24	3
26, 28, 30, 32, 34, 36	4

38, 40, 42	5
48	6
46, 56	7

表 1-1: DSCP 優先度値のマッピング

[注意] IP DSCP 設定はすべてのインターフェースに適用されます。

パラメータ

以下のパラメータが表示されます。

- ・ DSCP Mapping Status - IP DSCP 優先度の使用および CoS 値への IP DSCP 優先度値のマッピングを有効または無効にします (デフォルト : Disabled)。
- ・ IP DSCP - 8 bits の DSCP 値 (範囲 : 0 ~ 63)。
- ・ CoS - CoS 値 (範囲 : 0 ~ 7)。

Web インターフェース

IP DSCP を CoS 優先度マップに設定するには、以下のようにします。

- (1) 「Traffic」 → 「Priority」 → 「IP DSCP to CoS」を選択します。
- (2) DSCP テーブルで該当のエントリを見つけ、「CoS」フィールドに値を入力します。
- (3) < Apply > ボタンをクリックします。

Traffic > Priority > IP DSCP to CoS

DSCP Mapping Status ☐ Enabled

IP DSCP to CoS Mapping Table Max: 64 Total: 64

IP DSCP	CoS (0-7)
0	0
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	1
9	1

Apply Revert

画面 1-103 : IP DSCP 優先度値のマッピング

IP 優先順位のマッピング

「Traffic」→「Priority」→「IP Precedence to CoS」を選択すると、イングレスパケットで検出される IP 優先順位を内部的な優先処理用の CoS 値にマップすることができます。

関連する CLI 情報

「map ip precedence (Global Configuration)」

「map ip precedence (Interface Configuration)」

「show map ip precedence」

コマンドの使用

IPv4 ヘッダ内の ToS (Type of Service) オクテットには、最も優先度が高いネットワーク制御パケット用から最も優先度が低い通常トラフィック用まで、8 つの異なる優先レベルを定義する 3 bits の優先度ビットが含まれています。デフォルトの IP 優先順位値は一対一対応で CoS 値にマップされています (優先順位値 0 は CoS 値 0 にマップされ、優先順位値 1 は CoS 値 1 にマップされるというようになっています)。ビット 6 およびビット 7 はネットワーク制御のために使用され、他のビットはさまざまなアプリケーションタイプに使用されます。ToS ビットは、以下の表のように定義されています。

優先度	トラフィックタイプ
0	通常
1	優先度
2	即時
3	フラッシュ
4	フラッシュオーバーライド
5	クリティカル
6	インターネットワーク制御
7	ネットワーク制御

表 1-2: ToS ビット

【注意】 IP 優先度設定はすべてのインターフェースに適用されます。

パラメータ

以下のパラメータが表示されます。

- ・ IP Precedence Mapping Status – IP 優先順位の使用および CoS 値への IP 優先順位値のマッピングを有効または無効にします (デフォルト: Disabled)。
- ・ IP Precedence – 3 bits の優先順位値 (範囲: 0 ~ 7)。
- ・ CoS – CoS 値 (範囲: 0 ~ 7)。

Web インターフェース

IP 優先順位を CoS 優先度マップに設定するには、以下のようにします。

- (1) 「Traffic」 → 「Priority」 → 「IP Precedence to CoS」 を選択します。
- (2) IP 優先度テーブルで該当のエントリを見つけ、「CoS」 フィールドに値を入力します。
- (3) < Apply > ボタンをクリックします。

Traffic > Priority > IP Precedence to CoS
?

Precedence Mapping Status ☐ Enabled

IP Precedence to CoS Mapping Table Max: 8 Total: 8

IP Precedence	CoS (0-7)
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

Apply
Revert

画面 1-104 : IP 優先順位値のマッピング

IP ポート優先度のマッピング

「Traffic」 → 「Priority」 → 「IP Port to CoS」を選択すると、フレームヘッダ内の TCP/UDP 宛先ポート番号によって指定されるネットワークアプリケーションを内部処理のための CoS 値にマップすることができます。

関連する CLI 情報

「map ip port (Global Configuration)」

「map ip port (Interface Configuration)」

「show map ip port」

コマンドの使用

- ・ このマッピングテーブルは、着信パケットのタイプが TCP または UDP である場合にのみ使用されます。比較よく使用される TCP サービスポートとして、例えば、HTTP: 80、FTP: 21、Telnet: 23、および POP3: 110 があります。
- ・ イングレス TCP/UDP ポートタイプについてはデフォルトのマッピングは定義されていません。

[注意] IP ポート優先度設定はすべてのインターフェースに適用されます。

パラメータ

以下のパラメータが表示されます。

- ・ IP Port Mapping Status - TCP/UDP 宛先ポート番号の優先度の使用および CoS 値への TCP/UDP 宛先ポート番号の優先度値のマッピングを有効または無効にします (デフォルト: Disabled)。
- ・ TCP/UDP Port - 16 bits の TCP/UDP 宛先ポート番号 (範囲: 0 ~ 65,535)。
- ・ CoS - CoS 値 (範囲: 0 ~ 7)。

Web インターフェース

TCP/UDP ポート番号を CoS 優先度マップに設定するには、以下のようにします。

- (1) 「Traffic」 → 「Priority」 → 「IP Port to CoS」を選択します。
- (2) 「Step」 リストで 「Add」 を選択します。
- (3) いずれかの TCP または UDP ポートの CoS 優先度を設定します。

(4) < Apply > ボタンをクリックします。

Traffic > Priority > IP Port to CoS

Action: Add

IP Port Mapping Status ☒ Enabled

TCP/UDP Port (1-65535)

CoS (0-7)

Apply Revert

画面 1-105 : IP ポート番号の優先度値のマッピング

TCP/UDP ポート番号と CoS 優先度とのマッピングを表示するには、以下のようにします。

1. 「Traffic」 → 「Priority」 → 「IP Port to DSCP」を選択します。
2. 「Step」 リストで「Show」を選択します。

Traffic > Priority > IP Port to CoS

Action: Show

IP Port Mapping Status Enabled

IP Port to CoS Mapping Table Max: 65535 Total: 1

	IP Port	CoS
☐	21	1

Delete Revert

1.9 QoS (Quality of Service)

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

- ・ クラスマップの設定 – 個々のクラスのトラフィックを特定するためのマップを作成します。
- ・ QoS ポリシーの作成 – インバウンドトラフィックの監視に使用される境界パラメータを設定し、ポリシーに準拠しているトラフィックおよびポリシーに準拠していないトラフィックに対するアクションを指定します。
- ・ ポートへのポリシーマップのバインディング – ポリシーマップをインGRESSポートに適用します。

1.9.1 概要

ここで説明するコマンドは、QoS クラシフィケーションクライテリアおよびサービスポリシーを設定するために使用されます。DiffServ (Differentiated Services) は、ホップ単位で個々のトラフィックタイプの要件を満たすことができるようにネットワークリソースの優先度を設定するためのポリシーベースの管理方式を提供します。それぞれのパケットは、ネットワークに入るときに、アクセスリスト、IP 優先順位、DSCP 値、または VLAN リストに基づいて分類されます。アクセスリストを使用すると、各パケットに含まれているレイヤ 2、レイヤ 3、またはレイヤ 4 情報に基づいてトラフィックを選択できるようになります。設定されているネットワークポリシーに基づき、各種のトラフィックを転送方法別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、分類情報に依存して、同じクラスのパケットに同じ転送処理を提供します。分類情報は、エンドホストによって、あるいはパス上のスイッチまたはルータによって割り当てることができます。それから、一般的なポリシーまたはパケットの詳細な検証に基づいて優先度を割り当てることができます。ただし、パケットの詳細な検証は、コアスイッチおよびコアルータでオーバーロードが発生しないようにするため、ネットワーク付近で実行しなければならないので注意してください。

パス上のスイッチとルータでは、クラス情報を使用して、各種のトラフィッククラスに割り当てられているリソースの優先度を設定することができます。個々のデバイスで DiffServ アーキテクチャを使用してトラフィックを処理する方法を PHB (Per-Hop Behavior) と言います。パス上のすべてのデバイスは、整合性のあるエンドツーエンドの QoS ソリューションを構築するため、一貫した方法で設定されなければなりません。

[注意] クラスマップごとに最大 16 のルールを設定することができます。また、1 つのポリシーマップに複数のクラスを含めることができます。

[注意] 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。作成しない場合、ポリシールール設定画面でクラスマップを選択できなくなります。

コマンドの使用

特定のカテゴリのトラフィックまたはイングレストラフィックのサービスポリシーを作成するには、以下のようにします。

- (1) 「Configure Class」(Add) 画面で、トラフィックの特定のカテゴリのクラス名を指定します。
- (2) 「Configure Class」(Add Rule) 画面で、アクセスリスト、DSCP または IP 優先順位の値、あるいは VLAN に基づいてトラフィックのタイプを指定するクラスごとのルールを編集します。
- (3) 「Configure Policy」(Add) 画面で、イングレストラフィックを処理する特定のポリシー名を指定します。
- (4) 「Configure Policy」(Add Rule) 画面で、1 つまたは複数のクラスをポリシーマップに追加します。トラフィッククラスのマッチングに割り当てられる QoS 値 (CoS または PHB) を「設定」することにより、ポリシールールを各クラスに割り当てます。ポリシールールは、最大スループットおよびバーストレートを監視するために設定することもできます。それから、ルールに準拠するトラフィックに対して実行すべきアクション、またはポリシー違反に対して実行すべきアクションを指定します。
- (5) 「Configure Interface」画面で、ポリシーマップを特定のインターフェースに割り当てます。

クラスマップの設定

クラスマップは、指定されたクラスにパケットをマッチングするために使用されます。「Traffic」→「DiffServ」(Configure Class) を選択すると、クラスマップを設定することができます。

関連する CLI 情報

「Quality of Service Commands」

コマンドの使用

- ・ クラスマップは、特定のインターフェースについて、パケット分類、サービスタグ設定、および帯域幅ポリシー設定を定義するサービスポリシーを作成するため、ポリシーマップと共に使用されます。1 つのポリシーマップには 1 つまたは複数のクラスマップを割り当てることができるという点に注意してください。
- ・ 最大 32 のクラスマップを設定することができます。

パラメータ

以下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 (範囲: 1 ~ 32 文字)。
- ・ Type - クラスマップごとに使用できる match コマンドは match-any のみです。
- ・ Description - クラスマップの簡単な説明 (範囲: 1 ~ 64 文字)。

Add Rule

- ・ Class Name - クラスマップの名前。
- ・ Type - クラスマップごとに使用できる match コマンドは match-any のみです。
- ・ ACL - アクセスコントロールリストの名前。標準または拡張版の IP ACL および MAC ACL を含め、任意のタイプの ACL を指定することができます。
- ・ IP DSCP - DSCP 値 (範囲: 0 ~ 63)。
- ・ IP Precedence - IP 優先順位値 (範囲: 0 ~ 7)。
- ・ IPv6 DSCP - IPv6 パケットに含まれている DSCP 値 (範囲: 0 ~ 63)。
- ・ VLAN ID - VLAN (範囲: 1 ~ 4,093)。

Web インターフェース

クラスマップを設定するには、以下のようにします。

- (1) 「Traffic」 → 「DiffServ」 を選択します。
- (2) 「Step」 リストで 「Configure Class」 を選択します。
- (3) 「Step」 リストで 「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) < Add > ボタンをクリックします。

The screenshot shows a web interface for configuring DiffServ. The breadcrumb is 'Traffic > DiffServ'. Below it, there are two dropdown menus: 'Step' set to '1. Configure Class' and 'Action' set to 'Add'. The main form has three fields: 'Class Name' with the value 'rd-class', 'Type' with a dropdown set to 'Match Any', and 'Description' with the value 'class for software group'. At the bottom right, there are two buttons: 'Apply' and 'Revert'.

画面 1-106 : 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、以下のようにします。

- (1) 「Traffic」 → 「DiffServ」 を選択します。
- (2) 「Step」 リストで 「Configure Class」 を選択します。

(3) 「Step」 リストで「Show」を選択します。

Traffic > DiffServ

Step: 1. Configure Class Action: Show

Class List Max: 32 Total: 1

☐	Class Name	Type	Description
☐	rd-class	Match Any	class for software group

Delete Revert

画面 1-107 : 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、以下のようにします。

- (1) 「Traffic」 → 「DiffServ」 を選択します。
- (2) 「Step」 リストで「Configure Class」を選択します。
- (3) 「Step」 リストで「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 優先順位の値、あるいは VLAN に基づくトラフィックタイプをクラスに対して指定します。イングレストラフィックをクラスマップに割り当てるときにマッチングする最大 16 の項目を指定することができます。
- (6) < Apply > ボタンをクリックします。

Traffic > DiffServ

Step: 1. Configure Class Action: Add Rule

Class Name rd-class

Type Match Any

Rule:

☐ ACL

☒ IP DSCP (0-63) 3

☐ IP Precedence (0-7)

☐ IPv6 DSCP (0-63)

☐ VLAN ID (1-4093)

Apply Revert

画面 1-108 : クラスマップへのルールの追加

Web 設定

QoS (Quality of Service)

クラスマップのルールを表示するには、以下のようにします。

- (1) 「Traffic」 → 「DiffServ」 を選択します。
- (2) 「Step」 リストで 「Configure Class」 を選択します。
- (3) 「Step」 リストで 「Show Rule」 を選択します。

Traffic > DiffServ

Step: 1. Configure Class Action: Show Rule

Class Name: rd-class

Type: Match Any

Rule List Max: 16 Total: 2

☐	Rule
☐	IP DSCP 3
☐	IP Precedence 3

Delete Revert

画面 1-109 : クラスマップのルールの表示

1.9.2 QoS ポリシーの作成

「Traffic」→「DiffServ」(Configure Policy) を選択すると、複数のインターフェースに関連付けることが可能なポリシーマップを作成できます。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のグループ化、サービスタグ設定の変更、および帯域幅ポリシー設定の強制適用に使用します。さらに、サービスポリシーを 1 つまたは複数のインターフェースに割り当てることにより、ポリシーマップをサービスポリシーにバインドすることができます。

QoS ポリシーを設定するためには、いくつかの段階を踏む必要があります。最初に、アクセスリスト、DSCP または IP 優先順位の値、または特定の VLAN のメンバーに従ってどのようにインバウンドパケットをマッチングするかを示すクラスマップを設定する必要があります。それから、インバウンドトラフィックの監視に使用される境界パラメータを示すポリシーマップを設定し、ポリシーに準拠しているトラフィックおよびポリシーに準拠していないトラフィックに対するアクションを指定します。ポリシーマップには、事前に定義されているクラスマップに基づいて 1 つまたは複数のクラスが含まれます。

パケットのマッチングのために CoS または PHB (Per-Hop Behavior) 内部キュー処理に使用される優先度) を割り当てることができます。さらに、以下で説明するように、インバウンドトラフィックのフローレートを監視することや、3 つの別々のポリシー設定方式のいずれかに基づいて準拠トラフィックおよび非準拠トラフィックに対応することができます。

Police Flow Meter

コミットされる情報レート (最大スループット)、コミットされるバーストサイズ (バーストレート)、および準拠トラフィックと非準拠トラフィックに対するアクションを定義します。

ポリシーはバケットの深さ (バケットオーバーフローの前の最大バースト) が「burst」フィールド (BC) によって指定されるトークンバケットに基づいて設定され、バケットから取り除かれる平均レートトークンは「rate」オプション (CIR) によって指定されます。最大スループットを超えないトラフィックまたは最大スループットを超えるトラフィックに対するアクションを実行することができます。

srTCM Police Meter

RFC 2697 で規定されている srTCM (single rate Three Color Marker) 方式に基づいて、分類されたトラフィックのエンフォーサーを定義します。このメータリングポリシーでは、コミットされる情報レート (CIR、つまり最大スループット)、コミットされるバーストサイズ (BC、つまりバーストレート)、および過剰バーストサイズ (BE) に従って、トラフィックストリームを監視し、そのパケットを処理します。最大スループットを超えないトラフィック、最大スループットを超えるトラフィック、または過剰バーストサイズを超えるトラフィックに対するアクションを実行することができます。

- ・ PHB ラベルは、5 bits、PHB 用の 3 bits、およびキューの輻輳制御に使用される 2 bits から設定されます。このコマンドによって定義される送信、DSCP サービス値の再マーキング、またはパケットのドロップのためのアクションに加え、本製品では、処理の優先度を設定するために使用される 2 bits のカラービットによって、パケットが以下で説明するさまざまな色でマーキングされます。パケットは、コミットされる情報レートとバーストサイズを超えていない場合は緑色に、コミットされる情報レートとバーストサイズを超えているが過剰バーストサイズを超えていない場合は黄色に、それ以外の場合は赤色にマーキングされます。

- ・ このメーターは 2 つのいずれかのモードで動作します。カラーブラインドモードでは、パケットストリームが色分けされないものとみなされます。カラー認識モードでは、各パケットを緑色、黄色、赤色のいずれかにマーキングできるように、いくつかの先行エンティティに事前に色でマーキングされている着信パケットストリームが含まれているものとみなされます。メーターの実行結果に従って IP パケットの色がマーキング（または再マーキング）されます。色はパケットの DS フィールド [RFC 2474] でコーディングされます。
- ・ このメーターの動作は、メーターのモードおよび（両方で共通レート CIR を共有する）2 つのトークンバケット C と E に基づいて指定されます。トークンバケット C の最大サイズは BC であり、トークンバケット E の最大サイズは BE です。
- ・ トークンバケット C と E は、最初は満杯です。つまり、トークン数 $T_c(0)$ は BC であり、トークン数 $T_e(0)$ は BE です。その後、トークン数 T_c と T_e は、以下のように、1 秒ごとに CIR の値ずつ更新されます。
 - ・ $T_c < BC$ の場合、 T_c は 1 つずつインクリメントされます。そうでない場合、
 - ・ $T_e < BE$ の場合、 T_e は 1 つずつインクリメントされます。そうでない場合、
 - ・ T_c も T_e もインクリメントされません。

サイズが B bytes のパケットが時刻 t に受信され、srTCM がカラーブラインドモードで動作するように設定されている場合は、以下ようになります。

- ・ $T_c(t) - B \geq 0$ の場合、パケットは緑色にマーキングされ、 T_c は最小値 0 になるまで B ずつデクリメントされます。そうでない場合、
- ・ $T_e(t) - B \geq 0$ の場合、パケットは黄色にマーキングされ、 T_e は最小値 0 になるまで B ずつデクリメントされます。そうでない場合、
- ・ パケットは赤色にマーキングされ、 T_c も T_e もデクリメントされません。

サイズが B bytes のパケットが時刻 t に受信され、srTCM がカラー認識モードで動作するように設定されている場合は、以下ようになります。

- ・ パケットが事前に緑色にマーキングされており、 $T_c(t) - B \geq 0$ の場合、パケットは緑色にマーキングされ、 T_c は最小値 0 になるまで B ずつデクリメントされます。そうでない場合、
- ・ パケットが事前に黄色にマーキングされており、 $T_e(t) - B \geq 0$ の場合、パケットは黄色にマーキングされ、 T_e は最小値 0 になるまで B ずつデクリメントされます。そうでない場合、
- ・ パケットは赤色にマーキングされ、 T_c も T_e もデクリメントされません。

このメータリングポリシーを使用することにより、緑色にマーキングされているパケットの量が CIR および BC に基づいて判別される量よりも決して小さくならない、つまり、指定されている色のトークンが常にその色のパケットで消費されるという一意的な動作が保証されるようになります。srTCM の他の特性の詳細については、RFC 2697 を参照してください。

trTCM Police Meter

RFC 2698 で規定されている trTCM (two rate Three Color Marker) 方式に基づいて、分類されたトラフィックのエンフォースを定義します。このメータリングポリシーでは、コミットされる情報レート (CIR、つまり最大スループット)、ピーク情報レート (PIR)、それらに関連付けられているバーストサイズ (つまり、コミットされるバーストサイズ (BC、つまりバーストレート))、およびピークバーストサイズ (BP) に従って、トラフィックストリームを監視し、そのパケットを処理します。最大スループットを超えないトラフィック、最大スループットを超えるトラフィック、またはピークバーストサイズを超えるトラフィックに対するアクションを実行することができます。

- ・ PHB ラベルは、5 bits、PHB 用の 3 bits、およびキューの輻輳制御に使用される 2 bits から設定されます。このコマンドによって定義される送信、DSCP サービス値の再マーキング、またはパケットのドロップのためのアクションに加え、本製品では、処理の優先度を設定するために使用される 2 bits のカラービットによって、パケットが以下で説明するさまざまな色でマーキングされます。パケットは、PIR を超える場合は赤色にマーキングされます。それ以外の場合、パケットは、CIR を超えるかどうかに応じて、黄色または緑色にマーキングされます。trTCM は、コミットされるレートとは別にピークレートを強制的に適用する必要があるサービスのイングレスポリシー設定で役立ちます。
- ・ このメーターは 2 つのいずれかのモードで動作します。カラーブラインドモードでは、パケットストリームが色分けされないものとみなされます。カラー認識モードでは、各パケットを緑色、黄色、赤色のいずれかにマーキングできるように、いくつかの先行エンティティに事前に色でマーキングされている着信パケットストリームが含まれているものとみなされます。メーターの実行結果に従って IP パケットの色がマーキング (または再マーキング) されます。色はパケットの DS フィールド [RFC 2474] でコーディングされます。このメーターの動作は、メーターのモードおよび (レート PIR と CIR に基づく) 2 つのトークンバケット P と C に基づいて指定されます。トークンバケット P の最大サイズは BP であり、トークンバケット C の最大サイズは BC です。トークンバケット P と C は、最初 (time=0) は満杯です。つまり、トークン数 $Tp(0)$ は BP であり、トークン数 $Tc(0)$ は BC です。
- ・ サイズが B bytes のパケットが時刻 t に受信され、trTCM がカラーブラインドモードで動作するように設定されている場合は、以下ようになります。
 - ・ $Tp(t)-B < 0$ の場合、パケットは赤色にマーキングされます。そうでない場合、
 - ・ $Tc(t)-B < 0$ の場合、パケットは黄色にマーキングされ、 Tp が B ずつデクリメントされます。そうでない場合、
 - ・ パケットは緑色にマーキングされ、 Tp と Tc の両方が B ずつデクリメントされます。

サイズが B bytes のパケットが時刻 t に受信され、trTCM がカラー認識モードで動作するように設定されている場合は、以下ようになります。

- ・ パケットが事前に赤色にマーキングされている場合、または $Tp(t)-B < 0$ の場合、パケットは赤色にマーキングされます。そうでない場合、
- ・ パケットが事前に黄色にマーキングされている場合、または $Tc(t)-B < 0$ の場合、パケットは黄色にマーキングされ、 Tp は B ずつデクリメントされます。そうでない場合、
- ・ パケットは緑色にマーキングされ、 Tp と Tc の両方が B ずつデクリメントされます。
- ・ trTCM は、緑色、黄色、または赤色にマーキングされているパケットに対して徐々に低いレベルの保証 (絶対と相対のいずれか) が適用されるサービスで IP パケットスト

リームのマーキングに使用することができます。trTCM の他の特性の詳細については、RFC 2698 を参照してください。

関連する CLI 情報

「Quality of Service Commands」

コマンドの使用

- ・ ポリシーマップには、同じインターフェースに適用できる 128 のクラスステートメントを含めることができます。イングレスポートに対して最大 26 のポリシーマップを設定することができます。
- ・ ポリシーマップを使用してパケット分類、サービスタグ設定、および帯域幅ポリシー設定を定義した後、それらを有効にするには、サービスポリシーを使用して、そのポリシーマップを特定のインターフェースに割り当てる必要があります。

パラメータ

以下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（範囲：1 ～ 32 文字）。
- ・ Description - ポリシーマップの簡単な説明（範囲：1 ～ 256 文字）。

Add Rule

- ・ Policy Name - ポリシーマップの名前。
- ・ Class Name - ポリシーを適用できるトラフィック分類を定義するクラスマップの名前。
- ・ Action - イングレストラフィックに提供されるサービスを設定します。クラスマップのルール設定に適合するパケットは、以下のように再マーキングされます。
 - ・ Set CoS - 適合するパケットの VLAN タグの優先度ビットを設定します（範囲：0 ～ 7）。
 - ・ Set IP DSCP - （クラスマップのルール設定に）適合するパケットの IP DSCP 値を設定することにより、イングレス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 ～ 63）。
 - ・ Set IP Precedence - （クラスマップのルール設定に）適合するパケットの IP 優先順位値を設定することにより、イングレス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 ～ 63）。
- ・ Meter - このチェックボックスをオンにして、最大スループット、バーストレート、およびポリシー違反の場合に実行されるアクションを定義します。
- ・ Meter Mode - 以下のいずれかのポリシー設定方式を選択します。
 - ・ Flow (Police Flow) - コミットされる情報レート（CIR、つまり最大スループット）、コミットされるバーストサイズ（BC、つまりバーストレート）、および準拠トラフィックと非準拠トラフィックに対するアクションを定義します。ポリシーはパケットの深さ（パケットオーバーフローの前の最大バースト）が「burst」フィールド（BC）によって指定されるトークンバケットに基づいて設定され、バケットから取り除かれる平均レートトークンは「rate」オプションによって指定されます。
 - ・ Committed Information Rate (CIR) - 単位が kbps のレート（範囲：1 ～ 1,000,000 kbps と最大ポート速度のいずれか小さい方）。このレートは、設定されているインターフェース速度よりも大きい値にすることはできません。

- ・ Committed Burst Size (BC) – 単位が bytes のバースト (範囲: 64 ~ 524,288 bytes)。このバーストサイズは、16 Mbytes よりも大きい値にすることはできません。
 - ・ Conform – 最大レート (CIR) に準拠するトラフィックについて、DSCP サービスレベルに一切の変更を加えることなく送信するか、それとも DSCP サービスレベルを変更するかを指定します。
 - ・ Transmit – DSCP サービスレベルに一切の変更を加えることなく準拠トラフィックを送信します。
 - ・ Violate – 最大レート (CIR) を超えるトラフィックをドロップするか、それとも DSCP サービスレベルを下げるかを指定します。
 - ・ Set IP DSCP – 非準拠トラフィックの DSCP 優先度を下げます (範囲: 0 ~ 63)。
 - ・ Drop – 非準拠トラフィックをドロップします。
- ・ srTCM (Police Meter) – コミットされる情報レート (CIR、つまり最大スループット)、コミットされるバーストサイズ (BC、つまりバーストレート)、および過剰バーストサイズ (BE) を定義し、さらに、最大スループットを超えないトラフィック、最大スループットを超えるが過剰バーストサイズを超えないトラフィック、または過剰バーストサイズを超えるトラフィックに対するアクションを定義します。このコマンドによって定義される送信、DSCP サービス値の再マーキング、またはパケットのドロップのためのアクションに加え、本製品では、処理の優先度を設定するために使用される 2 bits のカラービットによって、パケットがさまざまな色でマーキングされます。カラーモードには、パケットストリームが色分けされていないものとみなす「Color-Blind」と、着信パケットが事前に色でマーキングされているものとみなす「Color-Aware」があります。これらのモードの機能面での違いは、前述の「srTCM Police Meter」で説明しています。
 - ・ Committed Information Rate (CIR) – 単位が kbps のレート (範囲: 1 ~ 1,000,000 kbps と最大ポート速度のいずれか小さい方)。
 - ・ このレートは、設定されているインターフェース速度よりも大きい値にすることはできません。
 - ・ Committed Burst Size (BC) – 単位が bytes のバーストサイズ (範囲: 64 ~ 524,288 bytes)。
 - ・ このバーストサイズは、16 Mbytes よりも大きい値にすることはできません。
 - ・ Exceeded Burst Size (BE) – コミットされるバーストサイズを超えるバースト (範囲: 64 ~ 524,288 bytes)。
 - ・ このバーストサイズは、16 Mbytes よりも大きい値にすることはできません。
 - ・ Conform – 最大レート (CIR) に準拠するトラフィックについて、DSCP サービスレベルに一切の変更を加えることなく送信するか、それとも DSCP サービスレベルを変更するかを指定します。
 - ・ Transmit – DSCP サービスレベルに一切の変更を加えることなく準拠トラフィックを送信します。
 - ・ Exceed – 最大レート (CIR) を超えるが過剰バーストサイズ (BE) を超えないトラフィックをドロップするか、それとも DSCP サービスレベルを下げるかを指定します。
 - ・ Set IP DSCP – 非準拠トラフィックの DSCP 優先度を下げます (範囲: 0 ~ 63)。
 - ・ Drop – 非準拠トラフィックをドロップします。
 - ・ Violate – 過剰バーストサイズ (BE) を超えるトラフィックをドロップするか、それとも DSCP サービスレベルを下げるかを指定します。
 - ・ Set IP DSCP – 非準拠トラフィックの DSCP 優先度を下げます (範囲: 0 ~ 63)。
 - ・ Drop – 非準拠トラフィックをドロップします。
- ・ trTCM (Police Meter) – コミットされる情報レート (CIR、つまり最大スループット)、ピーク情報レート (PIR)、それらに関連付けられているバーストサイズ (つまり、コミットされるバーストサイズ (BC、つまりバーストレート)、およびピークバーストサイズ (BP) を定義し、さらに、最大スループットを超えないトラフィック、最大ス

ループットを超えるがピーク情報レートを超えないトラフィック、またはピーク情報レートを超えるトラフィックに対するアクションを定義します。このコマンドによって定義される送信、DSCP サービス値の再マーキング、またはパケットのドロップのためのアクションに加え、本製品では、処理の優先度を設定するために使用される 2 bits のカラービットによって、パケットがさまざまな色でマーキングされます。カラーモードには、パケットストリームが色分けされていないものとみなす「Color-Blind」と、着信パケットが事前に色でマーキングされているものとみなす「Color-Aware」があります。これらのモードの機能面での違いは、前述の「trTCM Police Meter」で説明しています。

- ・ Committed Information Rate (CIR) – 単位が kbps のレート (範囲: 1 ~ 1,000,000 kbps と最大ポート速度のいずれか小さい方)。
このレートは、設定されているインターフェース速度よりも大きい値にすることはできません。
- ・ Peak Information Rate (PIR) – 単位が kbps のレート (範囲: 1 ~ 1,000,000 kbps と最大ポート速度のいずれか小さい方)。
このレートは、設定されているインターフェース速度よりも大きい値にすることはできません。
- ・ Committed Burst Size (BC) – 単位が bytes のバーストサイズ (範囲: 64 ~ 524,288 bytes)。
このバーストサイズは、16 Mbytes よりも大きい値にすることはできません。
- ・ Peak Burst Size (BP) – 単位が bytes のバーストサイズ (範囲: 64 ~ 524,288 bytes)。
このバーストサイズは、16 Mbytes よりも大きい値にすることはできません。
- ・ Conform – 最大レート (CIR) に準拠するトラフィックについて、DSCP サービスレベルに一切の変更を加えることなく送信するか、それとも DSCP サービスレベルを変更するかを指定します。
- ・ Transmit – DSCP サービスレベルに一切の変更を加えることなく準拠トラフィックを送信します。
- ・ Exceed – 最大レート (CIR) を超えるがピーク情報レート (PIR) を超えないトラフィックをドロップするか、それとも DSCP サービスレベルを下げるかを指定します。
 - ・ Set IP DSCP – 非準拠トラフィックの DSCP 優先度を下げます (範囲: 0 ~ 63)。
 - ・ Drop – 非準拠トラフィックをドロップします。
- ・ Violate – ピーク情報レート (PIR) を超えるトラフィックをドロップするか、それとも DSCP サービスレベルを下げるかを指定します。
 - ・ Set IP DSCP – 非準拠トラフィックの DSCP 優先度を下げます (範囲: 0 ~ 63)。
 - ・ Drop – 非準拠トラフィックをドロップします。

Web インターフェース

ポリシーマップを設定するには、以下のようにします。

- (1) 「Traffic」 → 「DiffServ」を選択します。
- (2) 「Step」リストで「Configure Policy」を選択します。
- (3) 「Step」リストで「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) < Add > ボタンをクリックします。

Traffic > DiffServ

Step: 2. Configure Policy Action: Add

Policy Name: rd-policy

Description: for the software group

Apply Revert

画面 1-110 : 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、以下のようにします。

- (1) 「Traffic」 → 「DiffServ」 を選択します。
- (2) 「Step」 リストで 「Configure Policy」 を選択します。
- (3) 「Step」 リストで 「Show」 を選択します。

Traffic > DiffServ

Step: 2. Configure Policy Action: Show

Policy List Max: 32 Total: 1

	Policy Name	Description
☐	rd-policy	for the software group

Delete Revert

画面 1-111 : 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、以下のようにします。

- (1) 「Traffic」 → 「DiffServ」 を選択します。
- (2) 「Step」 リストで 「Configure Policy」 を選択します。
- (3) 「Step」 リストで 「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) マッチするトラフィッククラスに割り当てられる QoS を指定するため、マッチするパケットの CoS または PHB を設定します。いずれかのメーター設定オプションを使用して、最大スループットやバーストレートなどのパラメータを定義します。それから、準拠トラフィックに対するアクション、最大レートを超えるがピーク情報

Web 設定

QoS (Quality of Service)

レートを超えないトラフィックに対するアクション、またはポリシー違反に対するアクションを指定します。

(6) < Apply > ボタンをクリックします。

Traffic > DiffServ

Step: 2. Configure Policy Action: Add Rule

Policy Name: rd-policy

Rule:

Class Name: rd

Action: Set CoS (0-7) 3

☒ Meter

Meter Mode: Flow

Committed Information Rate (1-1000000): 1000000 kbps

Committed Burst Size (64-524288): 4000 bytes

Exceeded Burst Size (64-524288): bytes

Peak Information Rate (1-1000000): kbps

Peak Burst Size (64-524288): bytes

Conform: Transmit

Exceed: Set IP DSCP (0-63)

Violate: Drop

画面 1-112 : 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、以下のようになります。

- (1) 「Traffic」 → 「DiffServ」 を選択します。
- (2) 「Step」 リストで 「Configure Policy」 を選択します。
- (3) 「Step」 リストで 「Show Rule」 を選択します。

Traffic > DiffServ

Step: 2. Configure Policy Action: Show Rule

Policy Name: rd-policy

Rule List Max: 128 Total: 1

	Class Name	Action	Meter Mode	Committed Information Rate (kbps)	Committed Burst Size (bytes)	Exceeded Burst Size (bytes)	Peak Information Rate (kbps)	Peak Burst Size (bytes)	Conform	Exceed	Violate
☐	rd-class	Set CoS 3	Flow	1000000	4000				Transmit		Drop

Delete Revert

画面 1-113 : ポリシーマップのルールを表示

1.9.3 ポートへのポリシーマップのバインディング

「Traffic」→「DiffServ」(Configure Interface) を選択すると、ポリシーマップをインGRESSポートにバインドすることができます。

関連する CLI 情報

「Quality of Service Commands」

コマンドの使用

最初にクラスマップを定義してからポリシーマップを定義し、さらに、必要なインターフェースにサービスポリシーをバインドします。

1つのインターフェースにバインドできるポリシーマップは1つだけです。

本製品では、ポリシーマップをエグレストラフィックのインターフェースにバインドすることはできません。

パラメータ

以下のパラメータが表示されます。

- ・ Port – ポートを指定します。
- ・ Ingress – 選択したルールをイングレストラフィックに適用します。

Web インターフェース

ポリシーマップをポートにバインドするには、以下のようにします。

- (1) 「Traffic」→「DiffServ」を選択します。
- (2) 「Step」リストで「Configure Interface」を選択します。
- (3) 「Ingress」列で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) プルダウンリストでポリシーマップを選択します。
- (5) < Apply > ボタンをクリックします。

Port	Ingress
1	☒ rd-policy
2	☐ rd-policy
3	☐ rd-policy
4	☐ rd-policy
5	☐ rd-policy

画面 1-114 : ポートへのポリシーマップのバインディング

1.10 VoIP トラフィック設定

本章には、以下のトピックが含まれています。

- ・ VoIP トラフィックの設定 – VoIP をグローバルで有効にし、音声 VLAN を設定し、接続されているポートのエージングタイムを指定します。
- ・ テレフォニー OUI の設定 – 指定されている OUI（Organization Unit Identifier）に基づいて VoIP 装置として処理される電話のリストを設定します。
- ・ VoIP トラフィックポートの設定 – ポートを音声 VLAN に追加する方法、非 VoIP パケットのフィルタリング、VoIP トラフィックの検出方法、および音声トラフィックに割り当てられる優先度を設定します。

1.10.1 概要

IP テレフォニーがエンタープライズネットワークで展開されている場合には、VoIP（Voice over IP）トラフィックを他のデータトラフィックから分離することをお勧めします。トラフィックを分離すると、過度のパケット遅延、パケット損失、およびジッタを防いで、より高い音声品質を実現することができます。そのための最善策は、すべての VoIP トラフィックを単一の音声 VLAN に割り当てることです。

音声 VLAN を使用することには、いくつかのメリットがあります。VoIP トラフィックを他のデータトラフィックと分離することにより、セキュリティが提供されます。ネットワーク全体にわたってエンドツーエンドの QoS ポリシーおよび高い優先度を VoIP VLAN トラフィックに適用できるので、必要な帯域幅が確保されます。また、VoIP VLAN を分離することにより、音声品質に重大な影響を及ぼす可能性のある邪魔なブロードキャストトラフィックとマルチキャストトラフィックから VoIP トラフィックが保護されます。

本製品では、ネットワークの音声 VLAN を指定して、VoIP トラフィックの CoS 優先度を設定することができます。パケットの送信元 MAC アドレスを使用して VoIP トラフィックをスイッチポートで検出するか、LLDP（IEEE 802.1AB）を使用して、接続されている VoIP デバイスを検出することができます。設定済されたポートで VoIP トラフィックが検出されると、そのポートは、自動的に、音声 VLAN のタグ付きメンバーとして割り当てられます。あるいは、スイッチポートを手動で設定することができます。

1.10.2 VoIP トラフィックの設定

「Traffic」→「VoIP」（Configure Global）を選択すると、スイッチで VoIP トラフィックを設定することができます。最初に、スイッチポートに接続されている VoIP デバイスの自動検出を有効にしてから、ネットワークの音声 VLAN ID を設定します。また、VoIP トラフィックがポートで受信されることがなくなった場合に音声 VLAN からポートを削除できるようにするため、音声 VLAN のエイジングタイムを設定することもできます。

関連する CLI 情報

「Configuring Voice VLANs」

パラメータ

以下のパラメータが表示されます。

- ・ Auto Detection Status – スイッチポートでの VoIP トラフィックの自動検出を有効にします（デフォルト：Disabled）。
- ・ Voice VLAN – ネットワークの音声 VLAN ID を設定します。サポートされる音声 VLAN は 1 つだけであり、その音声 VLAN は既にスイッチで設定されていなければなりません（範囲：1 ～ 4,093）。
- ・ Voice VLAN Aging Time – VoIP トラフィックがポートで受信されることがなくなった場合、この期間を過ぎると、音声 VLAN からポートが削除されます（範囲：5 ～ 43,200 分、デフォルト：1,440 分）。

[注意] 音声 VLAN ID は、「Auto Detection Status」がグローバルで有効になっている場合には変更することができません。

Web インターフェース

音声 VLAN のグローバル設定を設定するには、以下のようになります。

- (1) 「Traffic」→「VoIP」を選択します。
- (2) 「Step」リストで「Configure Global」を選択します。
- (3) 「Auto Detection Status」の「Enabled」チェックボックスをオンにします。
- (4) 音声 VLAN ID を指定します。
- (5) 必要な場合は音声 VLAN エージングタイムを調整します。

(6) < Apply > ボタンをクリックします。

Traffic > VoIP

Step: 1. Configure Global ▼

Auto Detection Status ☐ Enabled

Voice VLAN 1 ▼

Voice VLAN Aging Time (5-43200) 1440 min

Apply Revert

画面 1-115 : 音声 VLAN の設定

1.10.3 テレフォニー OUI の設定

スイッチに接続されている VoIP デバイスは、受信パケットの送信元 MAC アドレスに含まれているベンダーの OUI（Organizational Unique Identifier）によって識別することができます。OUI 番号は、ベンダーに割り当てられ、デバイスの MAC アドレスの先頭の 3 octets を形成します。VoIP 装置の MAC OUI 番号は、それらの装置からのトラフィックが VoIP トラフィックとして認識されるようにスイッチで設定することができます。「Traffic」→「VoIP」（Configure OUI）を選択すると、この機能を設定することができます。

関連する CLI 情報

「Configuring Voice VLANs」

パラメータ

以下のパラメータが表示されます。

- ・ Telephony OUI – リストに追加する MAC アドレス範囲を指定します。MAC アドレスを 01-23-45-67-89-AB という形式で入力してください。
- ・ Mask – ある範囲の MAC アドレスを特定します。FF-FF-FF-00-00-00 というマスクを設定すると、同じ OUI（先頭の 3 octets）をもつすべてのデバイスが特定されます。他のマスクは、MAC アドレス範囲を制限します。FF-FF-FF-FF-FF-FF というマスクは、単一の MAC アドレスを指定します（デフォルト：FF-FF-FF-00-00-00）。
- ・ Description – VoIP デバイスを特定するユーザ定義のテキスト。

Web インターフェース

VoIP 装置の MAC OUI 番号を設定するには、以下のようになります。

- (1) 「Traffic」→「VoIP」を選択します。
- (2) 「Step」リストで「Configure OUI」を選択します。
- (3) 「Step」リストで「Add」を選択します。
- (4) ネットワーク内の VoIP デバイスの OUI を指定する MAC アドレスを入力します。
- (5) マスクをプルダウンリストで選択して MAC アドレス範囲を定義します。
- (6) デバイスの説明を入力します。

(7) < Apply > ボタンをクリックします。

Traffic > VoIP

Step: 2. Configure OUI Action: Add

Telephony OUI: 00-e0-bb-00-00-00

Mask: FF-FF-FF-00-00-00

Description: old phones

Apply Revert

画面 1-116 : OUI テレフォニーリストの設定

VoIP 装置に使用される MAC OUI 番号を表示するには、以下のようにします。

- (1) 「Traffic」 → 「VoIP」 を選択します。
- (2) 「Step」 リストで 「Configure OUI」 を選択します。
- (3) 「Actio」 リストで 「Show」 を選択します。

Traffic > VoIP

Step: 2. Configure OUI Action: Show

Telephony OUI List Max: 16 Total: 3

☐	Telephony OUI	Mask	Description
☐	00-E0-BB-00-00-00	FF-FF-FF-00-00-00	old phones
☐	00-11-22-33-44-55	FF-FF-FF-00-00-00	new phones
☐	00-98-76-54-32-10	FF-FF-FF-FF-FF-FF	Chris' phone

Delete Revert

画面 1-117 : OUI テレフォニーリストの表示

1.10.4 VoIP トラフィックポートの設定

「Traffic」→「VoIP」（Configure Interface）を選択すると、VoIP トラフィック用のポートを設定することができます。モード（Auto または Manual）を設定し、使用する検出方法を指定し、トラフィックの優先度を設定する必要があります。また、セキュリティフィルタリングを有効にして、VoIP トラフィックのみが音声 VLAN で転送されるようにすることもできます。

関連する CLI 情報

「Configuring Voice VLANs」

パラメータ

以下のパラメータが表示されます。

- ・ Mode – ポートで VoIP トラフィックが検出された場合にそのポートを音声 VLAN に追加するかどうかを指定します（デフォルト：None）。
 - ・ None – ポートの音声 VLAN 機能を無効にします。ポートで VoIP トラフィックが検出されなくなったり、ポートが音声 VLAN に追加されなくなったりします。
 - ・ Auto – ポートで VoIP トラフィックが検出された場合にそのポートをタグ付きメンバーとして音声 VLAN に追加します。VoIP トラフィックを検出する方法として、OUI と 802.1ab（LLDP）のいずれかを選択する必要があります。
 - ・ OUI を選択する場合は、必ず、テレフォニー OUI リストで MAC アドレス範囲を設定してください。
 - ・ Manual – ポートの音声 VLAN 機能が有効になりますが、そのポートを手動で音声 VLAN に追加する必要があります。
- ・ Security – ポートで受信される音声 VLAN ID タグ付きの非 VoIP パケットを破棄するセキュリティフィルタリングを有効にします。
- ・ VoIP トラフィックは、テレフォニー OUI リストで設定されている送信元 MAC アドレスによって、または、スイッチに接続されている VoIP デバイスを検出する LLDP を使用して、特定されます。VoIP 送信元以外の送信元から受信されるパケットはドロップされます（デフォルト：Disabled）。
- ・ Discovery Protocol – ポートで VoIP トラフィックの検出に使用される方式を選択します（デフォルト：OUI）。
 - ・ OUI – VoIP デバイスからのトラフィックが送信元 MAC アドレスの OUI に基づいて検出されます。OUI 番号は、ベンダーに割り当てられ、デバイスの MAC アドレスの先頭の 3 octets を形成します。スイッチでトラフィックが VoIP アドレスからのものであると認識されるようにするため、MAC アドレスの OUI 番号をテレフォニー OUI リストで設定する必要があります。
 - ・ LLDP – LLDP（IEEE 802.1ab）を使用して、ポートに接続されている VoIP デバイスを検出します。LLDP では、System Capability TLV の「Telephone Bit」が有効になっているかどうかチェックされます。LLDP の詳細については、「LLDP（Link Layer Discovery Protocol）」を参照してください。
- ・ Priority – 音声 VLAN のポートトラフィックの CoS 優先度を定義します。ポートの音声 VLAN 機能がアクティブになっている場合は、受信されるあらゆる VoIP パケットの優先度が新しい優先度でオーバーライドされます（範囲：0～6、デフォルト：6）。
- ・ Remaining Age – エントリが期限切れになるまでの期間（秒）。MAC アドレステーブルで OUI の MAC アドレスが期限切れになると、「Remaining Age」のカウントダウンが開始されます。そのため、MAC アドレスのエージングタイムを全体的なエージングタイムに追加する必要があります。例えば、MAC アドレステーブルのエージングタイムを

30 秒にし、音声 VLAN のエージングタイムを 5 分にした場合、5 分 30 秒が経過すると、VoIP トラフィックがポートで受信されなくなったときにポートが音声 VLAN から削除されます。あるいは、MAC アドレステーブルを手動でクリアすると、「Remaining Age」のカウントダウンが開始されます。

Web インターフェース

ポートの VoIP トラフィック設定を設定するには、以下のようになります。

- (1) 「Traffic」 → 「VoIP」 を選択します。
- (2) 「Step」 リストで 「Configure Interface」 を選択します。
- (3) 各ポートの VoIP 設定に対して必要な変更を加えます。
- (4) < Apply > ボタンをクリックします。

Traffic > VoIP

Step: 3. Configure Interface

VoIP Port List Max: 26 Total: 26 1 2 3

Port	Mode	Security	Discovery Protocol	Priority (0-6)	Remaining Age (minutes)
1	Auto	☒ Enabled	☒ OUI ☐ LLDP	6	NA
2	Auto	☒ Enabled	☒ OUI ☐ LLDP	5	NA
3	Manual	☒ Enabled	☒ OUI ☐ LLDP	5	NA
4	Auto	☒ Enabled	☒ OUI ☐ LLDP	6	NA
5	None	☐ Enabled	☒ OUI ☐ LLDP	6	NA

画面 1-118 : 音声 VLAN のポート設定の設定

1.11 セキュリティ対策

本製品は、認証ユーザが管理アクセスのためローカル認証方式またはリモート認証方式でシステムにログインするように設定することができます。

また、アップリンクポートに対する管理アクセスとデータポートに対するクライアントアクセスのいずれかを制御するため、IEEE 802.1X によるポートベースの認証を設定することもできます。本製品は、以下のオプションによって、セキュアなネットワーク管理アクセスを提供します。

- ・ AAA 認証とアカウントिंग – ローカル認証またはリモート認証を使用するため、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トINGを設定します。
- ・ ユーザアカウントの設定 – ユーザを指定してスイッチのアクセス権を手動で設定します。
- ・ Web 認証 – 802.1X 認証またはネットワークアクセス認証が実現できない状況または実用的ではない状況で管理ステーションにおけるサービス承認とネットワークアクセス認証を可能にします。
- ・ ネットワークアクセス – MAC 認証およびダイナミック VLAN 割り当てを設定します。
- ・ HTTPS の設定 – セキュアな Web 接続を提供します。
- ・ セキュアシェルの設定 – (セキュアな Telnet アクセスのための) セキュアシェルを提供します。
- ・ アクセスコントロールリスト – IP フレームのパケットフィルタリング (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 制御コードに基づくフィルタリング) を実現します。
- ・ ARP インспекション – アドレス解決プロトコルパケットについて MAC アドレスのバインディングの妥当性を検証するセキュリティ機能であり、ある種の「中間者」攻撃の足掛かりとなる MAC アドレスと IP アドレスとのバインディングが無効な ARP トラフィックに対する防御策を提供します。
- ・ 管理アクセスのための IP アドレスフィルタリング – Web、SNMP、または Telnet インターフェースへの管理アクセスをフィルタリングします。
- ・ ポートセキュリティの設定 – 個々のポートのセキュアな MAC アドレスを設定します。
- ・ 802.1X ポート認証の設定 – IEEE 802.1X ポート認証を使用して、個々のポートに対するアクセスを制御します。
- ・ IP ソースガード – バインディングおよび DHCP スヌーピングバインディングテーブルの保守によって、非セキュアポートで、信頼できない DHCP メッセージをフィルタリングします。
- ・ DHCP スヌーピング – 非セキュアポートで、DHCP スヌーピングによって送信元アドレスを特定できない IP トラフィックをフィルタリングします。

[注意] フィルタリングコマンドは、ポートセキュリティ、ポート認証、ネットワークアクセス、Web 認証、アクセスコントロールリスト、IP ソースガード、DHCP スヌーピングの順で優先的に実行されます。

1.11.1 AAA 認証とアカウントティング

本製品では、認証、承認、およびアカウントティング（AAA: Authentication, Authorization, and Accounting）機能によって、アクセス制御の基本的な枠組みを提供します。これら 3 つのセキュリティ機能について説明すると、以下のようになります。

- ・ 認証 – 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。
- ・ 承認 – ユーザが個々のサービスにアクセスできるかどうかを判別します。
- ・ アカウントティング – ユーザがネットワークでアクセスしたサービスに関するレポート機能、監査機能、および請求機能を提供します。

AAA 機能では、ネットワーク内の設定済みの RADIUS サーバまたは TACACS+ サーバを使用する必要があります。それらのセキュリティサーバは、一連のグループとして定義して、所定のサービスに対するユーザアクセスを制御するための手段として適用することができます。例えば、スイッチでユーザが認証される場合には、要求が、定義済みのグループの最初のサーバに送信され、応答がなければ 2 番目のサーバに送信されるというようになります。認証が成功または失敗したという応答が返された時点で、プロセスが停止します。

本製品では、以下の AAA 機能をサポートしています。

- ・ スイッチを使用してネットワークにアクセスする IEEE 802.1X 認証済みユーザのアカウントティング
- ・ コンソールまたは Telnet を使用してスイッチの管理インターフェースにアクセスするユーザのアカウントティング
- ・ ユーザが特定の CLI 権限レベルを使用して入力するコマンドのアカウントティング
- ・ コンソールまたは Telnet を使用してスイッチの管理インターフェースにアクセスするユーザの承認

スイッチで AAA を設定するには、以下の汎用プロセスを実行する必要があります。

1. RADIUS サーバおよび TACACS+ サーバのアクセスパラメータを設定します。「ローカルまたはリモートのログオン認証の設定」を参照してください。
2. サービスのアカウントティングと認証をサポートするために RADIUS サーバグループおよび TACACS+ サーバグループを定義します。
3. アカウントティングまたは認証を適用するサービスごとにメソッド名を定義してから、使用する RADIUS サーバグループまたは TACACS+ サーバグループを指定します。
4. メソッド名をポートインターフェースまたは回線インターフェースに適用します。

【注意】 本書では、既に RADIUS サーバおよび 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 サーバおよび TACACS+ サーバの各ソフトウェアの設定は、本書の対象外であるため、それぞれのソフトウェアに付属している資料を参照してください。

ローカルまたはリモートのログオン認証の設定

「Security」→「AAA」→「System Authentication」を選択すると、ローカルまたはリモートの認証を指定することができます。ローカル認証では、スイッチで手動設定されるユーザ名とパスワードに基づいて管理アクセスを制限します。

リモート認証では、RADIUS プロトコルまたは TACACS+ プロトコルに基づいてリモートアクセス認証サーバを使用して、管理アクセスを検証します。

関連する CLI 情報

「Authentication Sequence」

コマンドの使用

- ・ デフォルトでは、管理アクセスは、常に、ローカルスイッチに保存されている認証データベースと照らし合わせてチェックされます。リモート認証サーバを使用する場合は、認証順序を指定する必要があります。それから、「Security」→「AAA」→「Server」を選択して、リモート認証プロトコルに関する該当のパラメータを指定します。ローカルログオン認証およびリモートログオン認証では、コンソールポート、Web ブラウザ、または Telnet を使用して、管理アクセスを制御します。
- ・ いずれのユーザについても最大 3 つの認証方式を指定して認証順序を設定することができます。例えば、(1) RADIUS、(2) TACACS、(3) ローカルというように選択すると、RADIUS サーバ上のユーザ名とパスワードが最初に検証されます。RADIUS サーバが使用できなければ、TACACS+ サーバを使用して認証が試行され、それも不可能であれば、最終的に、ローカルユーザ名とパスワードがチェックされます。

パラメータ

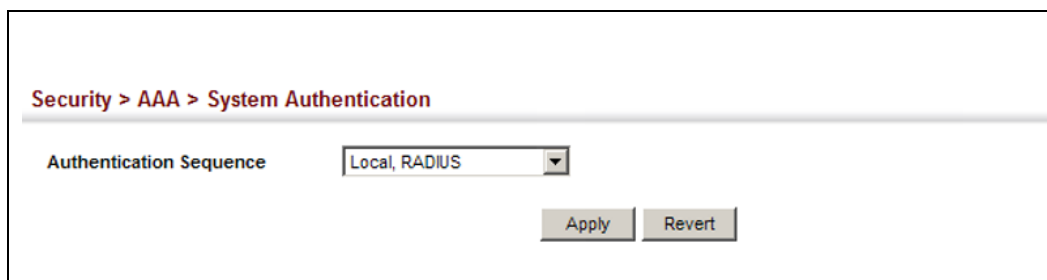
以下のパラメータが表示されます。

- ・ Authentication Sequence – 認証方式を以下の中から選択し、必要な場合は認証順序を指定します。
 - ・ Local – ユーザ認証がスイッチによってローカルのみで実行されます。
 - ・ RADIUS – RADIUS サーバのみを使用してユーザ認証が実行されます。
 - ・ TACACS – TACACS+ サーバのみを使用してユーザ認証が実行されます。
 - ・ [authentication sequence] – 最大 3 つの認証方式を、指定された順序で使用して、ユーザ認証が実行されます。

Web インターフェース

管理アクセスの制御方法を設定するには、以下のようにします。

- (1) 「Security」 → 「AAA」 → 「System Authentication」 を選択します。
- (2) 認証順序（1 ～ 3 つの方式）を指定します。
- (3) < Apply > ボタンをクリックします。



The screenshot shows the 'Security > AAA > System Authentication' configuration page. It features a breadcrumb trail at the top. Below it, the 'Authentication Sequence' is set to 'Local, RADIUS' in a dropdown menu. At the bottom right, there are two buttons: 'Apply' and 'Revert'.

画面 1-119 : 認証順序の設定

リモートログオン認証サーバの設定

「Security」→「AAA」→「Server」を選択すると、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することができます。

RADIUS (Remote Authentication Dial-in User Service) および TACACS+ (Terminal Access Controller Access Control System Plus) は、セントラルサーバで実行されるソフトウェアを使用してネットワーク上の RADIUS 対応デバイスまたは TACACS 対応デバイスに対するアクセスを制御するログオン認証プロトコルです。認証サーバにはデータベースがあり、そのデータベースで、複数組のユーザ名とパスワードが、スイッチに対する管理アクセス権を必要とする各ユーザの権限レベルと関連付けられて保存されます。

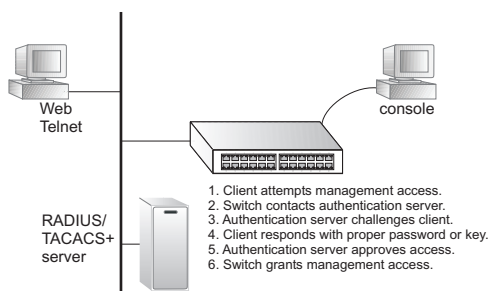


図 1-14: 認証サーバの仕組み

** 図の注釈

RADIUS/TACACS+ サーバ

1. クライアントが管理アクセスを試行する。
2. スイッチが認証サーバとコンタクトする。
3. 認証サーバがクライアントにチャレンジを送信する。
4. クライアントが適切なパスワードまたはキーを返す。
5. 認証サーバがアクセスを承認する。
6. スイッチが管理アクセス権を付与する。

RADIUS では UDP を使用しますが、TACACS+ では TCP を使用します。UDP は単にベストエフォート方式で配信を実現するのみですが、TCP は接続指向のトランスポートを実現します。また、RADIUS ではクライアントからサーバに送信されるアクセス要求パケット内のパスワードのみが暗号化されますが、TACACS+ ではパケット本体全体が暗号されるといふことにも注意してください。

関連する CLI 情報

「RADIUS Client」

「TACACS+ Client」

「AAA」

コマンドの使用

- ・ 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。ローカルログオン認証とリモートログオン認証

のどちらの場合も、コンソールポート、Web ブラウザ、または Telnet を使用して、管理アクセスを制御します。

- ・ RADIUS ログオン認証および TACACS+ ログオン認証では、ユーザ名とパスワードのペアごとに特定の権限レベルが割り当てられます。そのため、認証サーバで、ユーザ名、パスワード、および権限レベルを設定する必要があります。また、認証プロセスで使用する暗号化方式も、設定するか、または、認証サーバとログオンクライアントとの間でネゴシエーションされるようにする必要があります。本製品は、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認証メッセージをサーバとクライアント間で渡すことができます。

パラメータ

以下のパラメータが表示されます。

Configure Server

- ・ RADIUS
 - ・ Global - グローバルで適用できる RADIUS 設定を指定します。
 - ・ Server Index - 設定可能な 5 つの RADIUS サーバの中の 1 つを指定します。スイッチは、指定されている順序でサーバを使用して、認証を試行します。認証プロセスは、サーバがユーザのアクセスを承認または拒否した時点で終了します。
 - ・ Server IP Address - 認証サーバのアドレス（この項目が表示されるようにするには、「Server Index」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（範囲：1 ~ 65,535、デフォルト：1,813）。
 - ・ 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（範囲：1 ~ 65,535、デフォルト：1812）。
 - ・ Authentication Timeout - スイッチが要求を再送する前に RADIUS サーバからの応答を待機する期間（秒）（範囲：1 ~ 65,535、デフォルト：5）。
 - ・ Authentication Retries - スイッチが認証サーバ経由で認証ログオンアクセスを試行する回数（範囲：1 ~ 30、デフォルト：2）。
 - ・ Set Key - 暗号キーを設定または変更する場合は、このチェックボックスをオンにします。
 - ・ Authentication Key - クライアントのログオンアクセスの認証に使用される暗号キー。文字列に空白文字を含めないでください（最大長：48 文字）。
 - ・ Confirm Authentication Key - 入力に誤りがないことを確認するため、直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 2 つのフィールドの入力内容が一致しない場合、暗号キーは変更されません。
- ・ TACACS+
 - ・ Global - グローバルで適用できる TACACS+ 設定を指定します。
 - ・ Server Index - 設定するサーバのインデックス番号を指定します。現時点では、以下の TACACS+ サーバのうちの 1 つだけが本製品でサポートされます。
 - ・ Server IP Address - TACACS+ サーバのアドレス（この項目が表示されるようにするには、「Server Index」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+ サーバ上のネットワーク (TCP) ポート（範囲：1 ~ 65,535、デフォルト：49）。
 - ・ Authentication Timeout - スイッチが要求を再送する前に TACACS+ サーバからの応答を待機する期間（秒）（範囲：1 ~ 540、デフォルト：5）。
 - ・ Authentication Retries - スイッチが認証サーバ経由で認証ログオンアクセスを試行する回数（範囲：1 ~ 30、デフォルト：2）。

Web 設定

セキュリティ対策

- ・ Set Key – 暗号キーを設定または変更する場合は、このチェックボックスをオンにします。
- ・ Authentication Key – クライアントのログオンアクセスの認証に使用される暗号キー。文字列に空白文字を含めないでください（最大長：48 文字）。
- ・ Confirm Authentication Key – 入力に誤りがないことを確認するため、直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 2 つのフィールドの入力内容が一致しない場合、暗号キーは変更されません。

Configure Group

- ・ Server Type – RADIUS サーバまたは TACACS+ サーバを選択します。
- ・ Group Name – RADIUS サーバまたは TACACS+ サーバのグループの名前を定義します（範囲：1 ～ 255 文字）。
- ・ Sequence at Priority – グループに使用する RADIUS サーバとその順序を指定します（範囲：1 ～ 5）。サーバの優先順位を指定する場合は、その前に、サーバインデックスが定義されていなければなりません（「ローカルまたはリモートのログオン認証の設定」を参照）。

Web インターフェース

RADIUS 認証または TACACS+ 認証のパラメータを設定するには、以下のようにします。

- (1) 「Security」 → 「AAA」 → 「System」 を選択します。
- (2) 「Step」 リストで 「Configure Server」 を選択します。
- (3) サーバタイプとして 「RADIUS」 または 「TACACS+」 を選択します。
- (4) 「Global」 を選択して、指定したすべてのサーバにグローバルで適用するパラメータを指定します。または、いずれかの 「Server Index」 を選択して、その特定のサーバに適用するパラメータを指定します。
- (5) 認証キーを設定または変更するには、「Set Key」 チェックボックスをオンにし、キーを入力して、確認用にそのキーを再入力します。

(6) < Apply > ボタンをクリックします。

Security > AAA > Server

Server Type ☒ RADIUS ☐ TACACS+

☐ Global | Server Index: ☒ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

Server IP Address

Accounting Server UDP Port (1-65535)

Authentication Server UDP Port (1-65535)

Authentication Timeout (1-65535) sec

Authentication Retries (1-30)

☒ Set Key

Authentication Key

Confirm Authentication Key

画面 1-120：リモート認証サーバ（RADIUS）の設定

Security > AAA > Server

Step:

Server Type ☐ RADIUS ☒ TACACS+

☐ Global | Server Index: ☒ 1

Server IP Address

Authentication Server TCP Port (1-65535)

Authentication Timeout (1-540) sec

Authentication Retries (1-30)

☒ Set Key

Authentication Key

Confirm Authentication Key

画面 1-121：リモート認証サーバ（TACACS+）の設定

アカウントリングおよび承認に使用するために RADIUS サーバまたは TACACS+ サーバのグループを設定するには、以下のようにします。

- (1) 「Security」 → 「AAA」 → 「System」 を選択します。
- (2) 「Step」 リストで 「Configure Group」 を選択します。
- (3) 「Step」 リストで 「Add」 を選択します。

- (4) サーバタイプとして「RADIUS」または「TACACS+」を選択します。
- (5) グループ名を入力してから、それぞれの優先レベルに使用するサーバのインデックスを指定します。
- (6) < Apply > ボタンをクリックします。

Security > AAA > Server

Step: 2. Configure Group Action: Add

Server Type ☒ RADIUS ☐ TACACS+

RADIUS Group Name: radius

Sequence At Priority 1: 1

Sequence At Priority 2: 3

Sequence At Priority 3: 5

Sequence At Priority 4: 2

Sequence At Priority 5: None

Apply Revert

画面 1-122 : AAA サーバグループの設定

アカウントिंगおよび承認に使用される RADIUS サーバまたは TACACS+ サーバのグループを表示するには、以下のようにします。

- (1) 「Security」 → 「AAA」 → 「System」を選択します。
- (2) 「Step」 リストで「Configure Group」を選択します。
- (3) 「Step」 リストで「Show」を選択します。

Security > AAA > Server

Step: 2. Configure Group Action: Show

Server Type ☒ RADIUS ☐ TACACS+

RADIUS Group List Max: 5 Total: 3

	Group Name	Member Index
☐	radius	1, 2, 3, 5
☐	radius1	3, 5, 1
☐	radius2	1, 2, 5

Delete Revert

画面 1-123 : AAA サーバグループの表示

AAA Accounting の設定

「Security」→「AAA」→「Accounting」を選択すると、請求またはセキュリティのため、要求されたサービスのアカウントリングを有効にすることができます。また、設定されているアカウントリング方式、特定のインターフェースに適用されるアカウントリング方式、およびユーザセッションについて記録されている基本的なアカウントリング情報を表示することもできます。

関連する CLI 情報

「AAA」

コマンドの使用

アカウントリングを有効にする前に、RADIUS サーバまたは TACACS+ サーバによる AAA 認証を有効にする必要があります。

パラメータ

以下のパラメータが表示されます。

Configure Global

- ・ Periodic Update – ローカルアカウントリングサービスでアカウントリングサーバに対するシステム上のすべてのユーザの情報を更新する間隔を指定します（範囲：0 ～ 2,147,483,647 秒（0 = Disabled））。

Configure Method

- ・ Accounting Type – サービスとして、以下のいずれかを指定します。
 - ・ 802.1X – エンドユーザのアカウントリング。
 - ・ Exec – ローカルコンソール接続、Telnet 接続、または SSH 接続の管理アカウントリング。
- ・ Method Name – サービス要求に対するアカウントリング方式を指定します。「デフォルト」以外の方式が定義されていない場合、要求されたサービスにはデフォルトの方式が使用されます（範囲：1 ～ 255 文字）。ここで留意しなければならないのは、この方式名は、指定されている RADIUS サーバまたは TACACS+ サーバで設定されているアカウントリング方式を表わすためにのみ使用されるということです。使用される方式に関する情報は、サーバには、一切、送信されません。
- ・ Accounting Notice – ログイン時点からログオフ時点までのユーザアクティビティを記録します。
- ・ Server Group Name – アカウントリングサーバグループを指定します（範囲：1 ～ 255 文字）。
- ・ グループ名「radius」および「tacacs+」は、設定されているすべての RADIUS ホストおよび TACACS+ ホスト（「ローカルまたはリモートのログオン認証の設定」を参照）を表わします。その他のすべてのグループ名は、「Security」→「AAA」→「Server」（Configure Group）で表示される画面で設定されるサーバグループを表わします。

Configure Service

- ・ Accounting Type – 直前のセクションで説明しているように、サービスとして「802.1X」または「Exec」を指定します。
 - ・ 802.1X

- ・ Method Name – インターフェースに適用するユーザ定義のアカウントティング方式名を指定します。この方式は、「Configure Method」画面で定義する必要があります（範囲：1～255文字）。
- ・ Exec
 - ・ Console Method Name – コンソール接続に適用するユーザ定義のアカウントティング方式名を指定します。
 - ・ Telnet Method Name – Telnet 接続に適用するユーザ定義のアカウントティング方式名を指定します。

Show Information - Summary

- ・ Accounting Type – アカウントティングサービスが表示されます。
- ・ Method Name – ユーザ定義またはデフォルトのアカウントティング方式が表示されます。
- ・ Server Group Name – アカウントティングサーバグループが表示されます。
- ・ Interface – 指定したルールの適用先となるポート、コンソール、またはTelnetの各インターフェースが表示されます（このフィールドは、アカウントティング方式および関連付けられるサーバグループがインターフェースに割り当てられていない場合にはNullになります）。

Show Information - Statistics

- ・ User Name – 登録されているユーザ名が表示されます。
- ・ Accounting Type – アカウントティングサービスが表示されます。
- ・ Interface – ユーザがスイッチにアクセスするために使用した受信ポートの番号が表示されます。
- ・ Time Elapsed – この入力データがアクティブになるまでにかかった時間が表示されます。

Web インターフェース

AAA Accounting のグローバル設定を設定するには、以下のようにします。

- (1) 「Security」 → 「AAA」 → 「Accounting」 を選択します。
- (2) 「Step」 リストで 「Configure Global」 を選択します。
- (3) 必要な更新間隔を入力します。
- (4) < Apply > ボタンをクリックします。

Security > AAA > Accounting

Step: 1. Configure Global

Periodic Update (1-2147483647) 10 min (0: Disabled)

Apply Revert

画面 1-124 : AAA Accounting のグローバル設定の設定

各種のサービスタイプおよびそれらに割り当てられているサーバグループに適用されるアカウント方式を設定するには、以下のようにします。

- (1) 「Security」 → 「AAA」 → 「Accounting」 を選択します。
- (2) 「Step」 リストで 「Configure Method」 を選択します。
- (3) 「Step」 リストで 「Add」 を選択します。
- (4) アカウントタイプ（「802.1X」または「Exec」）を選択します。
- (5) アカウント方式名およびサーバグループ名を指定します。
- (6) < Apply > ボタンをクリックします。

Security > AAA > Accounting

Step: 2. Configure Method Action: Add

Accounting Type: 802.1X

Method Name: default

Accounting Notice: Start-Stop

Server Group Name: ☒ radius ☐

Apply Revert

画面 1-125 : AAA Accounting 方式の設定

各種のサービスタイプおよびそれらに割り当てられているサーバグループに適用されるアカウント方式を表示するには、以下のようにします。

- (1) 「Security」 → 「AAA」 → 「Accounting」 を選択します。
- (2) 「Step」 リストで 「Configure Method」 を選択します。

(3) 「Step」 リストで「Show」を選択します。

Security > AAA > Accounting

Step: 2. Configure Method Action: Show

Method List Max: 26 Total: 21

☐	Accounting Type	Method Name	Accounting Notice	Server Group Name
☐	802.1X	default	Start-Stop	radius
☐	802.1X	aaa	Start-Stop	aaaRadius
☐	Command 0	default	Start-Stop	tacacs+
☐	Command 1	default	Start-Stop	tacacs+

画面 1-126 : AAA Accounting 方式の表示

個々のインターフェース、個々の権限レベルで入力されるコンソールコマンド、およびローカルコンソール接続、Telnet 接続または SSH 接続に適用されるアカウントング方式を設定するには、以下のようにします。

- (1) 「Security」 → 「AAA」 → 「Accounting」 を選択します。
- (2) 「Step」 リストで「Configure Service」を選択します。
- (3) アカウントタイプ（「802.1X」または「Exec」）を選択します。
- (4) 必要なアカウントング方式を入力します。
- (5) < Apply > ボタンをクリックします。

Security > AAA > Accounting

Step: 3. Configure Service

Accounting Type ☒ 802.1X ☐ EXEC

Port Method List Max: 26 Total: 26

Port	Method Name
1	
2	
3	
4	
5	

画面 1-127 : 802.1X サービスの AAA Accounting サービスの設定

Security > AAA > Accounting

Step: 3. Configure Service

Accounting Type ☐ 802.1X ☒ EXEC

Console Method Name

Telnet Method Name

Apply Revert

画面 1-128 : Exec サービスの AAA Accounting サービスの設定

指定されているサービスタイプについて、設定されているアカウントング方式の概要と割り当てられているサーバグループを表示するには、以下のようにします。

- (1) 「Security」 → 「AAA」 → 「Accounting」 を選択します。
- (2) 「Step」 リストで 「Show Information」 を選択します。
- (3) 「Summary」 を選択します。

Security > AAA > Accounting

Step: 4. Show Information

☒ Summary ☐ Statistics

Method List Max: 26 Total: 20

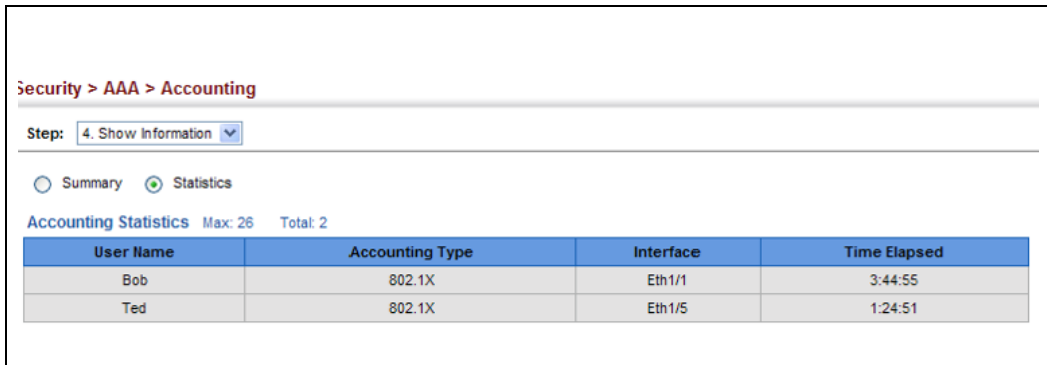
Accounting Type	Method Name	Server Group Name	Interface
802.1X	default	tacacs+	Eth 1/1, Eth 1/2, Eth 1/3, Eth 1/4
EXEC	default	tacacs+	Console, Telnet
Command 0	default	tacacs+	Console, Telnet
Command 1	default	tacacs+	Console, Telnet
Command 2	default	tacacs+	Console, Telnet

画面 1-129 : 適用されている AAA Accounting 方式の概要の表示

ユーザセッションについて、基本アカウントング情報と記録されている統計情報を表示するには、以下のようにします。

- (1) 「Security」 → 「AAA」 → 「Accounting」 を選択します。
- (2) 「Step」 リストで 「Show Information」 を選択します。

(3) 「Statistics」を選択します。



Security > AAA > Accounting			
Step: 4. Show Information			
☐ Summary ☒ Statistics			
Accounting Statistics Max: 26 Total: 2			
User Name	Accounting Type	Interface	Time Elapsed
Bob	802.1X	Eth1/1	3:44:55
Ted	802.1X	Eth1/5	1:24:51

画面 1-130 : AAA Accounting セッションに関する統計情報の表示

AAA 承認の設定

「Security」→「AAA」→「Authorization」を選択すると、要求されるサービスの承認を有効にすることができます。また、設定されている承認方式および個々のインターフェースに適用される承認方式を表示することもできます。

関連する CLI 情報

「AAA」

コマンドの使用

- ・ この機能は、ユーザが Exec シェルの実行を許可されているかどうかを判別するために承認を実行します。
- ・ 承認を有効にする前に、RADIUS サーバまたは TACACS+ サーバによる AAA 認証を有効にする必要があります。

パラメータ

以下のパラメータが表示されます。

Configure Method

- ・ Authorization Type – ローカルコンソール、Telnet、SSH のいずれかの接続の管理承認であることを示す「Exec」をサービスとして指定します。
- ・ Method Name – サービス要求に対する承認方式を指定します。「デフォルト」以外の方式が定義されていない場合、要求されたサービスにはデフォルトの方式が使用されます（範囲：1 ～ 255 文字）。
- ・ Server Group Name – 承認サーバグループを指定します（範囲：1 ～ 255 文字）。グループ名「tacacs+」は、設定されているすべての TACACS+ ホスト（「ローカルまたはリモートのログオン認証の設定」を参照）を表わします。その他のすべてのグループ名は、TACACS+ グループ設定画面で設定されるサーバグループを表わします。承認は TACACS+ サーバでのみサポートされます。

Configure Service

- ・ Console Method Name - コンソール接続に適用するユーザ定義のアカウントティング方式名を指定します。
- ・ Telnet Method Name - Telnet 接続に適用するユーザ定義のアカウントティング方式名を指定します。

Show Information

- ・ Authorization Type - 承認サービスが表示されます。
- ・ Method Name - ユーザ定義またはデフォルトのアカウントティング方式が表示されます。
- ・ Server Group Name - 承認サーバグループが表示されます。
- ・ Interface - 指定したルールの適用先となるコンソールインターフェースまたは Telnet インターフェースが表示されます（このフィールドは、アカウントティング方式および関連付けられるサーバグループがインターフェースに割り当てられていない場合には Null になります）。

Web インターフェース

Exec サービスタイプおよびそれに割り当てられているサーバグループに適用される承認方式を設定するには、以下のようにします。

- (1) 「Security」 → 「AAA」 → 「Authorization」 を選択します。
- (2) 「Step」 リストで 「Configure Method」 を選択します。
- (3) 「Step」 リストで 「Add」 を選択します。
- (4) 承認方式名およびサーバグループ名を指定します。
- (5) < Apply > ボタンをクリックします。

Security > AAA > Authorization

Step: 1. Configure Method Action: Add

Authorization Type: EXEC

Method Name: default

Server Group Name: ☒ tacacs+ ☐

Apply Revert

画面 1-131 : AAA 承認方式の設定

Exec サービスタイプおよびそれに割り当てられているサーバグループに適用される承認方式を表示するには、以下のようにします。

- (1) 「Security」 → 「AAA」 → 「Authorization」 を選択します。
- (2) 「Step」 リストで 「Configure Method」 を選択します。
- (3) 「Step」 リストで 「Show」 を選択します。

Security > AAA > Authorization

Step: 1. Configure Method Action: Show

Method List Max: 5 Total: 2

☐	Authorization Type	Method Name	Server Group Name
☐	EXEC	default	tacacs+
☐	EXEC	aaa	tacacs1

Delete Revert

画面 1-132 : AAA 承認方式の表示

ローカルコンソール、Telnet、SSH のいずれかの接続に適用される承認方式を設定するには、以下のようにします。

- (1) 「Security」 → 「AAA」 → 「Authorization」 を選択します。
- (2) 「Step」 リストで 「Configure Service」 を選択します。
- (3) 必要な承認方式を入力します。
- (4) < Apply > ボタンをクリックします。

Security > AAA > Authorization

Step: 2. Configure Service

Console Method Name tps-auth

VTY Method Name tps-auth

Apply Revert

画面 1-133 : Exec サービスの AAA 承認方式の設定

Exec サービスタイプについて、設定されているアカウンティング方式と割り当てられているサーバグループを表示するには、以下のようにします。

(1) 「Security」 → 「AAA」 → 「Authorization」 を選択します。

(2) 「Step」 リストで 「Show Information」 を選択します。

Authorization Type	Method Name	Server Group Name	Interface
EXEC	default	tacacs+	
EXEC	console	tacacs+	Console
EXEC	telnet	tacacs+	Telnet

画面 1-134 : 適用されている AAA 承認方式の表示

1.11.2 ユーザアカウントの設定

「Security」 → 「User Accounts」 を選択すると、手動設定されているユーザ名とパスワードに基づいてスイッチに対する管理アクセスを制御することができます。

関連する CLI 情報

「User Accounts」

コマンドの使用

- ・ デフォルトのゲスト名は「guest」であり、対応するパスワードは「guest」です。デフォルトの管理者名は「admin」であり、対応するパスワードは「admin」です。
- ・ ゲストは、大部分の設定パラメータについては読み取り専用アクセス権しかもっていません。しかし、管理者は、オンボードエージェントを制御するすべてのパラメータに対する書き込みアクセス権をもっています。そのため、管理者は、新規の管理者に可能な限り速やかにパスワードを割り当て、そのパスワードを安全な場所に保管しなければなりません。

パラメータ

以下のパラメータが表示されます。

- ・ User Name - ユーザの名前（最大長：8 文字、最大ユーザ数：16）。
- ・ Access Level - ユーザレベルを指定します（オプション：0（通常）または 15（特権））。
- ・ 通常レベルの場合、スイッチの現在のステータスを表示するコマンドおよびデータベースのクリアやリセットのための機能のうち、アクセスできるものが限られます。特権レベルの場合、すべてのコマンドにフルアクセスすることができます。
- ・ Password Type - 以下のオプションを指定します。
 - ・ No Password - 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 - 非暗号化プレーンテキストパスワード。

Web 設定

セキュリティ対策

- ・ Encrypted Password – 暗号化パスワード。暗号化パスワードは、システム起動時に設定ファイルを読み込むときに従来のパスワード設定（プレーンテキストパスワードまたは非暗号化パスワード）との互換性を確保するために必要です。暗号化パスワードの手動設定は不要です。
- ・ Password – ユーザパスワードを指定します（範囲：0～8文字のプレーンテキスト（大文字と小文字の区別あり））。
- ・ Confirm Password – 入力に誤りがないことを確認するため、直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2つのフィールドの入力内容が一致しない場合、パスワードは変更されません。

Web インターフェース

ユーザアカウントを設定するには、以下のようになります。

- (1) 「Security」 → 「User Accounts」 を選択します。
- (2) 「Step」 リストで 「Add」 を選択します。
- (3) ユーザ名を指定し、ユーザのアカウントレベルを選択して、パスワードと確認用パスワードを入力します。
- (4) < Apply > ボタンをクリックします。

Security > User Accounts

Action:

User Name:

Access Level:

Password Type:

Password:

Confirm Password:

画面 1-135 : ユーザアカウントの設定

ユーザアカウントを表示するには、以下のようになります。

- (1) 「Security」 → 「User Accounts」 を選択します。

(2) 「Step」 リストで「Show」を選択します。

Security > User Accounts

Action: Show ▾

User Account List Max: 16 Total: 3

☐	User Name	Access Level
☐	admin	15
☐	guest	0
☐	bob	15

Delete Revert

画面 1-136 : ユーザアカウントの表示

1.11.3 Web 認証

Web 認証は、802.1X 認証またはネットワークアクセス認証が実現できない状況または実用的ではない状況で管理ステーションにおけるサービス承認とネットワークアクセス認証を可能にします。Web 認証機能を使用すれば、非認証ホストが、DHCP によって割り当てられる IP アドレスを要求して受信し、DNS クエリを実行できるようになります。その他のトラフィック（ただし、HTTP プロトコルトラフィックは除く）は、すべて、ブロックされます。スイッチは、HTTP プロトコルトラフィックをインターセプトして、RADIUS によるユーザ名とパスワードの認証を容易にするためにスイッチで生成された Web ページにリダイレクトします。認証が正常に完了すると、元々要求された Web ページに転送され、そのページの内容が Web ブラウザに表示されるようになります。認証が正常に完了した場合、その認証は、ポートに接続されているすべてのホストについて有効になります。

[注意] Web 認証機能が正しく機能するには、RADIUS 認証がアクティブになっており、正しく設定されていなければなりません（「ローカルまたはリモートのログオン認証の設定」を参照）。

[注意] Web 認証はトランクポートでは設定できません。

Web 認証のグローバル設定の設定

「Security」→「Web Authentication」（Configure Global）を選択すると、Web 認証のグローバルパラメータを編集することができます。

関連する CLI 情報

「Web Authentication」

パラメータ

以下のパラメータが表示されます。

- ・ Web Authentication Status – スイッチの Web 認証を有効または無効にします（デフォルト : Disabled）。

[注意] この機能は必要なあらゆるポート（「Step」リストで「Configure Interface」を選択した場合に表示されるべきポート）について有効にしなければならないので注意してください。

- ・ Session Timeout – 認証されたセッションがアクティブな状態に維持される期間。この期間を過ぎると再認証が必要になります（範囲 : 300 ~ 3,600 秒、デフォルト : 3,600 秒）。
- ・ Quiet Period – ホストが最大許容ログイン失敗回数を超えてから再び認証を試行するまで待機しなければならない期間（範囲 : 1 ~ 180 秒、デフォルト : 60 秒）。
- ・ Login Attempts – サプリカントが認証を試行して失敗できる回数。この回数を超えると、サプリカントは「Quiet Period」で指定されている期間、待機しなければなりません（範囲 : 1 ~ 3 回、デフォルト : 3 回）。

Web インターフェース

Web 認証のグローバルパラメータを設定するには、以下のようにします。

- (1) 「Security」 → 「Web Authentication」 を選択します。
- (2) 「Step」 リストで 「Configure Global」 を選択します。
- (3) スイッチで Web 認証をグローバルで有効にし、必要に応じて、いずれかのプロトコルパラメータを調整します。
- (4) < Apply > ボタンをクリックします。

Security > Web Authentication

Step: 1. Configure Global ▼

Web Authentication Status ☐ Enabled

Session Timeout (300-3600) sec

Quiet Period (1-180) sec

Login Attempts (1-3)

Apply Revert

画面 1-137 : Web 認証のグローバル設定の設定

Web 認証のインターフェース設定の設定

「Security」→「Web Authentication」（Configure Interface）を選択すると、ポートの Web 認証を有効にすることや、接続されている任意のホストの情報を表示することができます。

関連する CLI 情報

「Web Authentication」

パラメータ

以下のパラメータが表示されます。

- ・ Port – 設定するポートを示します。
- ・ Status – ポートの Web 認証ステータスを指定します。
- ・ Host IP Address – 接続されている各ホストの IP アドレスを示します。
- ・ Remaining Session Time – ホストについて認証されている現行のセッションが期限切れになるまでの残り時間を示します。
- ・ Apply – 「Status」チェックボックスがオンになっている場合、Web 認証を有効にします。また、「Authenticated Host List」で選択されているホスト IP アドレスについて認証済みのすべての Web セッションを終了し、ユーザに再認証を実行するように求めます。
- ・ Revert – 直前の設定情報に戻します。
- ・ Re-authenticate – 「Authenticated Host List」で選択されているホスト IP アドレスについて認証済みのすべての Web セッションを終了し、ユーザに再認証を実行するように求めます。

Web インターフェース

ポートの Web 認証を有効にするには、以下のようにします。

- (1) 「Security」→「Web Authentication」を選択します。
- (2) 「Step」リストで「Configure Interface」を選択します。
- (3) Web 認証を必要とするいずれかのポートを「Port」で指定してから、「Status」で「Enabled」チェックボックスをオンにします。
- (4) 再認証が必要なホストアドレスのチェックボックスをオンにします。

(5) < Apply > ボタンをクリックします。

Security > Web Authentication

Step: 2. Configure Interface

Port: 1

Status: ☒ Enabled

Apply Revert

Authenticated Host List Max: 8 Total: 2

	Host IP Address	Remaining Session Time (sec)
☐	10.1.1.1	300
☐	10.2.2.2	100

Re-authenticate Revert

画面 1-138 : Web 認証のインターフェース設定の設定

1.11.4 ネットワークアクセス（MAC アドレス認証）

スイッチポートに接続されているデバイスによっては、ハードウェアまたはソフトウェアに関する制限のため、802.1X 認証がサポートされないことがあります。そのような状況は、ネットワークプリンタや IP フォンなどのデバイスおよび一部の無線アクセスポイントでよく発生します。本製品では、セントラル RADIUS サーバを使用してデバイスの MAC アドレスを認証するという方法で、それらのデバイスからのネットワークアクセスを制御することができます。

[注意] MAC アドレス認証機能が正しく機能するには、RADIUS 認証がアクティブになっており、正しく設定されていなければなりません（「リモートログオン認証サーバの設定」を参照）。

[注意] MAC アドレス認証はトランクポートでは設定できません。

関連する CLI 情報

「Network Access (MAC Address Authentication)」

コマンドの使用

- ・ MAC アドレス認証では、スイッチポートに接続しようとする各ホストの MAC アドレスを認証することにより、ネットワークへのアクセスを制御します。特定の MAC アドレスから受信されるトラフィックは、送信元 MAC アドレスがセントラル RADIUS サーバによって正常に認証される場合にのみ、転送されます。MAC アドレスの認証の進行中は、認証が完了するまで、すべてのトラフィックがブロックされます。必要に応じて、認証が正常に完了した後にスイッチポートの VLAN 設定と QoS 設定が RADIUS サーバによって割り当てられるようにすることもできます。
- ・ ポートで認証が有効になっている場合、認証プロセスでは、PAP (Password Authentication Protocol) 要求が、設定済みの RADIUS サーバに送信されます。ユーザ名とパスワードは、両方とも、認証される MAC アドレスと等しくなります。そのため、RADIUS サーバでは、PAP ユーザ名とパスワードを XX-XX-XX-XX-XX-XX（すべて大文字）というように、MAC アドレス形式で設定する必要があります。
- ・ 認証された MAC アドレスは、スイッチのセキュアな MAC アドレステーブルにダイナミックエントリとして保存され、期限切れになると削除されます。このスイッチシステムでサポートされる送信元 MAC アドレスの最大数は 1,024 です。
- ・ 設定されているスタティック MAC アドレスは、スイッチポートで検出されると、セキュアなアドレステーブルに追加されます。スタティックアドレスは、要求が RADIUS サーバに送信されることなく、認証済みアドレスとして処理されます。
- ・ ポートがダウン状態になると、そのポートにマップされているすべての MAC アドレスがセキュアな MAC アドレステーブルからクリアされます。スタティック VLAN 割り当ては復元されません。
- ・ 必要に応じて、スイッチポートに適用される VLAN ID リストが RADIUS サーバによって返すようにすることもできます。その場合は、RADIUS サーバで以下の属性を設定する必要があります。
 - ・ Tunnel-Type = VLAN
 - ・ Tunnel-Medium-Type = 802
 - ・ Tunnel-Private-Group-ID = 1u,2t [VLAN ID リスト]

VLAN ID リストは、RADIUS の「Tunnel-Private-Group-ID」属性によって伝播されます。VLAN リストには、複数の VLAN ID を「1u,2t,3u」という形式で含めることができます（「u」はタグなし VLAN、「t」はタグ付き VLAN を示します）。

- ・ 必要に応じて、認証されたユーザのスイッチポートに適用されるダイナミック QoS 割り当てが RADIUS サーバによって返されるようにすることもできます。以下の QoS 情報を渡すように「Filter-ID」属性（属性 11）を RADIUS サーバで設定することができます。

プロファイル	属性の構文	例
DiffServ	service-policy-in= ポリシーマップ名	service-policy-in=p1
Rate Limit	rate-limit-input= レート	rate-limit-input=100（単位：kbps）
802.1p	switchport-priority-default= 値	switchport-priority-default=2
IP ACL	IP ACLip-access-group-in=IP ACL 名	ip-access-group-in=ipv4acl
IPv6 ACL	IPv6 ACLipv6-access-group-in=IPv6 ACL 名	ipv6-access-group-in=ipv6acl
MAC ACL	MAC ACLmac-access-group-in=MAC ACL 名	mac-access-group-in=macAcl

表 1-4: ダイナミック QoS プロファイル

- ・ Filter-ID 属性では、セミコロンを使用して各プロファイルを区切ることにより、複数のプロファイルを指定することができます。
- ・ 例えば、属性「service-policy-in=pp1;rate-limitinput=100」は、DiffServ プロファイル名として「pp1」を、また、イングレスレートリミットプロファイル値として 100 kbps を指定します。
- ・ 重複するプロファイルが Filter-ID 属性で渡された場合は、最初のプロファイルのみが使用されます。
- ・ 例えば、属性が「service-policy-in=p1;service-policy-in=p2」である場合、スイッチは DiffServ プロファイル「p1」のみを適用します。
- ・ サポートされていないプロファイルが Filter-ID 属性に含まれている場合、それらのプロファイルは、すべて、無視されます。
- ・ 例えば、属性が「map-ip-dscp=2:3;service-policy-in=p1」である場合、スイッチは「map-ip-dscp」プロファイルを無視します。
- ・ 認証が正常に完了した場合に、以下のいずれかの状況のため、RADIUS サーバからダイナミック QoS 情報が渡されないことがあります（認証結果は変更されません）。
 - ・ ユーザプロファイルを伝播するための Filter-ID 属性を検出できない。
 - ・ Filter-ID 属性が空である。
 - ・ ダイナミック QoS 割り当てに関する Filter-ID 属性の形式が認識不可能である

Security > Network Access

Step: 1. Configure Global

Aging Status ☒ Enabled

Reauthentication Time (120-1000000) 30000 sec

Apply

Revert

は
全体を認識できない。

- ・ 以下の状況では、ダイナミック QoS 割り当てが失敗し、認証結果が成功から失敗に変わります。

Web 設定

セキュリティ対策

- ・ プロファイル値で不正な文字が検出される（例えば、802.1p プロファイル値で数字以外の文字が検出される場合など）。
- ・ 受信されるプロファイルが認証対象のポートで設定されていない。
- ・ ダイナミック QoS が割り当てられているポートで最後のユーザがログオフすると、ポートの元の QoS 設定が復元されます。
- ・ 返されたダイナミック QoS プロファイルを使用してユーザがネットワークにログインしようとしたときに、そのプロファイルが同じポートにログインするときに既に使用されたものと異なる場合、ユーザはアクセスを拒否されます。
- ・ ポートにはダイナミック QoS プロファイルが割り当てられていますが、QoS 設定に手動で加えられた変更は、すべてのユーザがポートからログオフした後にのみ有効になります。

ネットワークアクセスのグローバル設定の設定

MAC アドレス認証はポートごとに設定されますが、スイッチのすべてのポートにグローバルで適用される設定可能パラメータが 2 つあります。「Security」→「Network Access」(Configure Global) を選択すると、MAC アドレス認証の有効期限と再認証が必要になるまでの期間を設定することができます。

関連する CLI 情報

「Network Access (MAC Address Authentication)」

パラメータ

以下のパラメータが表示されます。

- ・ Aging Status – セキュアな MAC アドレステーブルに保存されている認証済み MAC アドレスの有効期限設定を有効にします (デフォルト: Disabled)。このパラメータは、このセクションで説明している MAC アドレス認証プロセスで設定される認証済み MAC アドレスだけでなく、「802.1X Operation Mode」で説明している「Single-Host」、「Multi-Host」、または「MAC-Based」認証) に関係なく、802.1X によって認証されるあらゆるセキュアな MAC アドレスに適用されます。認証された MAC アドレスは、スイッチのセキュアな MAC アドレステーブルにダイナミックエントリとして保存され、期限切れになると削除されます。このスイッチシステムでサポートされる送信元 MAC アドレスの最大数は 1,024 です。
- ・ Reauthentication Time – 接続しているホストの再認証が必要になるまでの期間を設定します。セキュアな MAC アドレスは、この期間が過ぎると、RADIUS サーバによって再認証されます。再認証プロセスの間、依然としてポートを経由するトラフィックには影響ありません (デフォルト: 1,800 秒、範囲: 120 ~ 1,000,000 秒)。

Web インターフェース

MAC アドレス認証の有効期限ステータスと再認証までの期間を設定するには、以下のようになります。

- (1) 「Security」→「Network Access」を選択します。
- (2) 「Step」リストで「Configure Global」を選択します。
- (3) セキュアなアドレスの有効期限を有効または無効にし、必要に応じて、再認証までの期間を変更します。
- (4) < Apply > ボタンをクリックします。



画面 1-139 : ネットワークアクセスのグローバル設定の設定

ポートのネットワークアクセスの設定

「Security」→「Network Access」（Configure Interface - General）を選択すると、スイッチポートの MAC 認証を設定することができます。例えば、アドレス認証を有効にする、MAC アドレスの最大数を設定する、ダイナミック VLAN 割り当てまたはダイナミック QoS 割り当てを有効にしたりすることが可能です。

関連する CLI 情報

「Network Access (MAC Address Authentication)」

パラメータ

以下のパラメータが表示されます。

- ・ MAC Authentication
 - ・ Status – ポートで MAC 認証を有効にします（デフォルト：Disabled）。
 - ・ Intrusion – MAC 認証失敗時のポートでの対応として、ポートへのアクセスのブロックとトラフィックのパススルーのいずれかを設定します（オプション：Block または Pass、デフォルト：Block）。
 - ・ Max MAC Count6 – MAC 認証（つまり、このセクションで説明しているネットワークアクセスプロセス）によってポートで認証できる MAC アドレスの最大数を設定します（範囲：1～1,024、デフォルト：1,024）。

**6. ポートごとの MAC アドレスの最大数は 1,024 であり、スイッチシステムでサポートされるセキュアな MAC アドレスの最大数は 1,024 です。制限値に達すると、新しい MAC アドレスは、すべて、認証に失敗したものととして処理されます。

- ・ Network Access Max MAC Count6 – あらゆる形式の認証（ネットワークアクセス認証や IEEE 802.1X 認証など）によってポートインターフェースで認証できる MAC アドレスの最大数を設定します（範囲：1～1,024、デフォルト：1,024）。
- ・ Guest VLAN – 802.1X 認証が失敗した場合にポートに割り当てられる VLAN を指定します（範囲：0～4,093（0 = Disabled）、デフォルト：Disabled）。VLAN は既に作成され、アクティブになっていなければなりません（「VLAN グループの設定」を参照）。また、802.1X 認証と共に使用する場合は、「Guest VLAN」について、侵害発生時のアクションを設定する必要があります（「802.1X のポート設定の設定」を参照）。
- ・ Dynamic VLAN – 認証されたポートのダイナミック VLAN 割り当てを有効にします。有効にすると、RADIUS サーバによって返されるあらゆる VLAN ID がポートに適用され、スイッチで既に作成されている VLAN が提供されるようになります（GVRP による VLAN の作成は使用されません）（デフォルト：Enabled）。ポートには、最初に認証される MAC アドレスによって指定される VLAN 設定が実装されます。ポートで認証されるその他の MAC アドレスの VLAN 設定は同じでなければなりません。同じでない場合、それらの MAC アドレスは認証に失敗したものととして処理されます。
- ・ ダイナミック VLAN 割り当てがポートで有効になっており、VLAN 設定が RADIUS サーバによって一切返されない場合でも、認証は成功したものととして処理され、ホストはデフォルトのタグなし VLAN に割り当てられます。ポートでダイナミック VLAN 割り当てのステータスが変更されると、すべての認証済みアドレスがセキュアな MAC アドレステーブルからクリアされます。
- ・ Dynamic QoS – 認証されたポートのダイナミック QoS 割り当てを有効にします（デフォルト：Disabled）。

- ・ MAC Filter ID – MAC フィルタをポートに割り当てられるようにします。選択した MAC フィルタテーブル内で検出される MAC アドレスまたは MAC アドレス範囲は、指定したポートの認証対象から除外されます（「MAC アドレスフィルタの設定」▲の説明を参照）（範囲：1 ～ 64、デフォルト：None）。

Web インターフェース

スイッチポートの MAC 認証を設定するには、以下のようにします。

- (1) 「Security」 → 「Network Access」 を選択します。
- (2) 「Step」 リストで 「Configure Interface」 を選択します。
- (3) < General > ボタンをクリックします。
- (4) ポートでアドレス認証を有効にするために必要なあらゆる設定変更を行ってから、サポートされるセキュアな MAC アドレスの最大数、MAC 認証または 802.1X 認証が失敗した場合に使用されるゲスト VLAN、およびダイナミック VLAN 割り当てとダイナミック QoS 割り当てを設定します。
- (5) < Apply > ボタンをクリックします。

Security > Network Access

Step: 2. Configure Interface

General Link Detection

Port List Max: 26 Total: 26

Port	MAC Authentication			Network Access Max MAC Count (1-1024)	Guest VLAN (0-4093, 0: Disabled)	Dynamic VLAN	Dynamic QoS	MAC Filter ID (1-64)
	Status	Intrusion	Max MAC Count (1-1024)					
1	☐ Enabled	Block	1024	1024	0	☒ Enabled	☐ Enabled	☐
2	☒ Enabled	Pass	1024	1024	2	☒ Enabled	☐ Enabled	☐
3	☐ Enabled	Block	1024	1024	0	☒ Enabled	☐ Enabled	☐
4	☒ Enabled	Block	1024	1024	0	☒ Enabled	☐ Enabled	☐
5	☐ Enabled	Block	1024	1024	0	☒ Enabled	☐ Enabled	☐

画面 1-140：ネットワークアクセスのインターフェース設定の設定

ポートのリンク検出の設定

「Security」→「Network Access」（Configure Interface - Link Detection）を選択すると、リンクイベントが発生した場合に SNMP トラップが送信されるようにしたり、ポートのシャットダウンが可能になります。

関連する CLI 情報

「Network Access (MAC Address Authentication)」

パラメータ

以下のパラメータが表示されます。

- ・ Link Detection Status - ポートのリンク検出を有効にするか無効にするかを指定します。
- ・ Condition - ポートのアクションをトリガーするリンクイベントのタイプ。
 - ・ Link up - リンクアップイベントが発生した場合にのみ、ポートのアクションのトリガーになります。
 - ・ Link down - リンクダウンイベントが発生した場合にのみ、ポートのアクションのトリガーになります。
 - ・ Link up and down - リンクアップイベントが発生した場合も、リンクダウンイベントが発生した場合も、ポートのアクションのトリガーになります。
- ・ Action - スイッチは、以下の 3 つの方法でリンクアップイベントまたはリンクダウンイベントに対応することができます。
 - ・ Trap - SNMP トラップを送信します。
 - ・ Trap and shutdown - SNMP トラップを送信し、ポートをシャットダウンします。
 - ・ Shutdown - ポートをシャットダウンします。

Web インターフェース

スイッチポートのリンク検出を設定するには、以下のようになります。

- (1) 「Security」→「Network Access」を選択します。
- (2) 「Step」リストで「Configure Interface」を選択します。
- (3) < Link Detection > ボタンをクリックします。
- (4) リンク検出ステータス、トリガー条件、およびポートの対応を変更します。

(5) < Apply > ボタンをクリックします。

Security > Network Access

Step: 2. Configure Interface

General Link Detection

Port List Max: 26 Total: 26

Port	Link Detection Status	Condition	Action
1	☐ Enabled	Link down	Trap
2	☒ Enabled	Link up and down	Trap
3	☐ Enabled	Link down	Trap
4	☐ Enabled	Link down	Trap
5	☐ Enabled	Link down	Trap

画面 1-141 : ネットワークアクセスのリンク検出の設定

MAC アドレスフィルタの設定

「Security」→「MAC Authentication」（Configure MAC Filter）を選択すると、認証対象から除外する特定の MAC アドレスまたは MAC アドレス範囲を指定することができます。ポートでアクティブになっている MAC フィルタテーブルで検出される MAC アドレスは、そのポートで事前に認証されているものとして処理されます。

関連する CLI 情報

「Network Access (MAC Address Authentication)」

コマンドの使用

- ・ 指定した MAC アドレスは認証対象から除外されます。
- ・ 最大 65 のフィルタテーブルを定義することができます。
- ・ フィルタテーブルで使用されるエントリの数に制限はありません。

パラメータ

以下のパラメータが表示されます。

- ・ Filter ID – 指定したフィルタのフィルタルールを追加します。
- ・ MAC Address – フィルタルールを使用して、入力された MAC アドレスまたは（「MAC Address Mask」で定義される）MAC アドレス範囲と照らし合わせてインGRES パケットがチェックされます。
- ・ MAC Address Mask – フィルタルールを使用して、MAC ビットマスクで定義されている MAC アドレス範囲がチェックされます。マスクの指定を省略すると、完全に一致するデフォルトのマスクがシステムによって割り当てられます（範囲：0000000000000 ~ FFFFFFFF、デフォルト：FFFFFFFF）。

Web インターフェース

MAC 認証の MAC アドレスフィルタを追加するには、以下のようになります。

- (1) 「Security」→「Network Access」を選択します。
- (2) 「Step」リストで「Configure MAC Filter」を選択します。
- (3) 「Step」リストで「Add」を選択します。
- (4) フィルタ ID、MAC アドレス、およびマスク（任意指定）を入力します。

(5) < Apply > ボタンをクリックします。

Security > Network Access

Step: 3. Configure MAC Filter Action: Add

Filter ID (1-64) 22

MAC Address 11-22-33-44-55-66

MAC Address Mask FFFFFFFF

Apply Revert

画面 1-142 : ネットワークアクセスの MAC アドレスフィルタの設定

MAC 認証の MAC アドレスフィルタテーブルを表示するには、以下のようにします。

- (1) 「Security」 → 「Network Access」 を選択します。
- (2) 「Step」 リストで 「Configure MAC Filter」 を選択します。
- (3) 「Step」 リストで 「Show」 を選択します。

Security > Network Access

Step: 3. Configure MAC Filter Action: Show

MAC Filter List Max: 65 Total: 1

	Filter ID	MAC Address	MAC Address Mask
☐	22	11-22-33-44-55-66	FF-FF-FF-FF-FF-FF

Delete Revert

画面 1-143 : ネットワークアクセスの MAC アドレスフィルタテーブルの表示

セキュアな MAC アドレス情報の表示

「Security」→「Network Access」(Show Information) を選択すると、セキュアな MAC アドレステーブルに保存されている認証済みの MAC アドレスを表示することができます。

セキュアな MAC エントリに関する情報を表示することや、選択したエントリをテーブルから削除することができます。

関連する CLI 情報

「Network Access (MAC Address Authentication)」

パラメータ

以下のパラメータが表示されます。

- ・ Query By - MAC アドレスクエリで使用するパラメータを指定します。
 - ・ Sort Key - 表示される情報を、MAC アドレス、ポートインターフェース、または属性を基準にして並び替えます。
 - ・ MAC Address - 特定の MAC アドレスを指定します。
 - ・ Interface - ポートインターフェースを指定します。
 - ・ Attribute - スタティックアドレスとダイナミックアドレスのどちらを表示するかを指定します。
- ・ Authenticated MAC Address List
 - ・ MAC Address - 認証済みの MAC アドレス。
 - ・ Interface - セキュアな MAC アドレスに関連付けられているポートインターフェース。
 - ・ RADIUS Server - MAC アドレスを認証した RADIUS サーバの IP アドレス。
 - ・ Time - MAC アドレスが最後に認証された日時。
 - ・ Attribute - スタティックアドレスとダイナミックアドレスのどちらであることを示します。

Web インターフェース

セキュアな MAC アドレステーブルに保存されている認証済み MAC アドレスを表示するには、以下のようにします。

- (1) 「Security」→「Network Access」を選択します。
- (2) 「Step」リストで「Show Information」を選択します。
- (3) 「Sort Key」を使用して、MAC アドレス、ポートインターフェース、または属性を基準にして情報が表示されるようにします。
- (4) 「MAC Address」フィールドに特定のアドレスを入力するか、「Interface」フィールドでポートを指定するか、「Attribute」フィールドでアドレスタイプを「Static」または「Dynamic」に設定して、表示されるアドレスを絞り込みます。

(5) < Query > ボタンをクリックします。

Security > Network Access

Step: 4. Show Information

Query by:

Sort Key: MAC Address

☐ MAC Address

☐ Interface: 1

☐ Attribute: Static

Query

Authenticated MAC Address List Max: 2048 Total: 8

	MAC Address	Interface	RADIUS Server	Time	Attribute
☐	00-00-86-45-F2-23	Unit 1 / Port 23	10.2.2.10	2008y 20m 12d 11h 16m 12s	Dynamic
☐	00-00-E8-5E-E1-DD	Unit 1 / Port 23	10.2.2.10	2008y 20m 12d 11h 32m 24s	Dynamic
☐	00-00-E8-81-93-30	Unit 1 / Port 23	10.2.2.10	2008y 20m 12d 11h 40m 32s	Dynamic
☐	00-01-80-31-B8-30	Unit 1 / Port 23	10.2.2.10	2008y 20m 12d 11h 18m 51s	Dynamic
☐	00-01-80-36-95-08	Unit 1 / Port 23	10.2.2.10	2008y 20m 12d 11h 32m 22s	Dynamic

画面 1-144 : ネットワークアクセスが認証されているアドレスの表示

1.11.5 HTTPS の設定

HTTPS (Secure Hypertext Transfer Protocol) over SSL (Secure Socket Layer) を有効にするようにスイッチを設定して、セキュアアクセス (つまり、暗号化接続) がスイッチの Web インターフェースに提供されるようにすることができます。

HTTPS のグローバル設定の設定

「Security」→「HTTPS」(Configure Global) を選択すると、HTTPS を有効または無効にすることや、HTTPS サービスで使用される UDP ポートを指定することができます。

関連する CLI 情報

「Web Server」

コマンドの使用

- ・ HTTP サービスと HTTPS サービスは、両方とも、スイッチで個別に有効にすることができます。ただし、両方のサービスで同じ UDP 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 で `ip http server` コマンドを使用することによってのみ、設定することができます)。
- ・ HTTPS を有効にする場合は、ブラウザの URL に `https:// デバイス [: ポート番号]` というように表示されるように指定して、HTTPS が有効になっていることを示す必要があります。
- ・ HTTPS サービスを開始すると、接続が以下の方法で確立されます。
 - ・ クライアントがサーバのデジタル証明書を使用してサーバを認証します。
 - ・ クライアントとサーバが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ションします。
 - ・ クライアントとサーバがデータの暗号化と復号化のためのセッションキーを生成します。
- ・ クライアントとサーバがセキュアな暗号化接続を確立します。
- ・ Internet Explorer 5.x 以降および Mozilla Firefox 2.0.0.0 以降の場合はステータスバーに南京錠アイコンが表示されます。
- ・ 現在、HTTPS は、以下の Web ブラウザとオペレーティングシステムでサポートされています。

Web ブラウザ	オペレーティングシステム
Internet Explorer 5.0 以降	Windows 98、Windows NT (Service Pack 6a 適用済み)、Windows 2000、Windows XP、Windows 7
Mozilla Firefox 2.0.0.0 以降	Windows 2000、Windows XP、Linux

表 1-5: HTTPS システムのサポート

パラメータ

以下のパラメータが表示されます。

- ・ HTTPS Status – スイッチの HTTPS サーバ機能を有効または無効にすることができます（デフォルト：Enabled）。
- ・ HTTPS Port – スイッチの Web インターフェースへの HTTPS 接続で使用する UDP ポート番号を指定します（デフォルト：ポート 443）。

Web インターフェース

HTTPS を設定するには、以下のようにします。

- (1) 「Security」 → 「HTTPS」 を選択します。
- (2) 「Step」 リストで 「Configure Global」 を選択します。
- (3) HTTPS を有効にし、必要な場合は、ポート番号を指定します。
- (4) < Apply > ボタンをクリックします。

The screenshot shows a web configuration page titled "Security > HTTPS". Below the title, there is a section labeled "Action:" with a dropdown menu set to "Configure Global". Underneath, there are two configuration items: "HTTPS Status" with a checked checkbox and the text "Enabled", and "UDP Port (1-65535)" with a text input field containing the value "443". At the bottom right of the configuration area, there are two buttons: "Apply" and "Revert".

画面 1-145 : HTTPS の設定

デフォルトのセキュアサイト証明書の置き換え

「Security」→「HTTPS」(Copy Certificate)を選択すると、デフォルトのセキュアサイト証明書を置き換えることができます。

(セキュアアクセスのため) HTTPS を使用して Web インターフェースにログオンすると、スイッチの SSL (Secure Sockets Layer) 証明書が表示されます。デフォルトで、Internet Explorer に表示される証明書は、サイトがセキュアサイトとして認識されていないという警告に関連付けられます。なぜならば、証明書には、公認の認証局によって署名が付けられていないからです。この警告を、スイッチへの接続がセキュアなものであることを認めるメッセージに置き換える場合は、認定されている認証局から、固有の証明書および秘密キーとパスワードを取得する必要があります。

[注意] 最大限のセキュリティを実現するため、可能な限り速やかに、固有の SSL 証明書を取得することをお勧めします。なぜならば、スイッチのデフォルトの証明書は、購入されたハードウェアに固有のものではないからです。

それらを取得したら、TFTP サーバに保存し、スイッチに転送してデフォルト (認識されない) 証明書を認定されている証明書に置き換えます。

[注意] 新しい証明書をアクティブにするには、スイッチをリセットする必要があります。スイッチをリセットするには、「システムのリセット」を参照するか、コマンドプロンプトで「reload」と入力します (例: Console#reload)。

関連する CLI 情報

「Web Server」

パラメータ

以下のパラメータが表示されます。

- ・ TFTP Server IP Address - 証明書ファイルが保存されている TFTP サーバの IP アドレス。
- ・ 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。
- ・ Private Key Source File Name - TFTP サーバに保存されている秘密キーファイルの名前。
- ・ Private Password - 秘密キーファイルに保存されているパスワード。このパスワードは、証明書の権限を検証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検証されます。
- ・ Confirm Password - 入力に誤りがないことを確認するため、直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 2 つのフィールドの入力内容が一致しない場合、証明書はスイッチにダウンロードされません。

Web インターフェース

デフォルトのセキュアサイト証明書を置き換えるには、以下のようになります。

- (1) 「Security」 → 「HTTPS」 を選択します。
- (2) 「Step」 リストで 「Copy Certificate」 を選択します。
- (3) TFTP サーバ、証明書と秘密キーのファイルの名前、および秘密キーのパスワードを入力します。
- (4) < Apply > ボタンをクリックします。

The screenshot shows a web interface for configuring HTTPS security. The title is "Security > HTTPS". Below the title, there is a dropdown menu labeled "Action:" with "Copy Certificate" selected. Below this, there are five input fields arranged in a table-like structure:

TFTP Server IP Address	192.168.0.4
Certificate Source File Name	ES3628BT-site-certificate
Private Key Source File Name	ES3628BT-private-key
Private Password	*****
Confirm Password	*****

At the bottom right of the form, there are two buttons: "Apply" and "Revert".

画面 1-146 : セキュアサイト証明書のダウンロード

1.11.6 セキュアシェルの設定

カリフォルニア大学バークレー校で開発された BSD には、元々、UNIX システム用に考案されたリモートアクセスツールが含まれています。それらのツールの一部は、Microsoft Windows およびその他の環境にも実装されています。rlogin（リモートログイン）、rsh（リモートシェル）、および rcp（リモートコピー）などのコマンドを含むそれらのツールは、不正な攻撃に対してセキュアではありません。

セキュアシェル（SSH: Secure Shell）には、古いバークレーリモートアクセスツールに代わるセキュアなツールとして、クライアント / サーバアプリケーションが組み込まれています。また、本製品では、SSH を使用することにより、Telnet に代わるセキュアな手段としてリモート管理アクセスが実現されます。クライアントが SSH プロトコルを使用してスイッチにコンタクトすると、クライアントがアクセス認証でローカルユーザ名とパスワードと共に使用する公開キーがスイッチによって生成されます。また、SSH を使用することにより、スイッチと SSH 対応管理ステーションクライアントとの間で転送されるすべてのデータが暗号化され、ネットワーク経由で送信されるデータが途中で変更せずに到着するようになります。

[注意] SSH プロトコルによる管理のためスイッチにアクセスするには、SSH クライアントを管理ステーションにインストールする必要があります。

[注意] 本製品は SSH V1.5 と V2.0 の両方のクライアントをサポートしています。

コマンドの使用

スイッチ上の SSH サーバは、パスワードによる認証と公開キーによる認証の両方をサポートします。パスワード認証が SSH クライアントによって指定される場合は、パスワードがローカルで認証されるようにするか、それとも、RADIUS または TACACS+ リモート認証サーバを使用して認証されるようにするか、「System Authentication」画面で設定することができます。公開キー認証が SSH クライアントによって指定される場合は、以下のセクションの説明に従って、認証キーをクライアントとスイッチの両方で設定する必要があります。ただし、公開キー認証とパスワード認証のどちらを使用するかに関係なく、依然として、認証キーをスイッチで生成して（SSH ホストキー設定）、SSH サーバを有効にする（認証設定）必要があるということに注意してください。

SSH サーバを使用するには、以下の手順を実行します。

1. ホストキーペアの生成 - SSH ホストキー設定画面で、ホストの公開キーと秘密キーのペアを作成します。
2. クライアントへのホストの公開キーの提供 - 多くの SSH クライアントプログラムでは、スイッチとの初期接続セットアップ時に自動的にホストの公開キーがインポートされます。自動的にインポートされない場合は、既知のホストのファイルを管理ステーションで手動作成し、そのファイルにホストの公開キーを入れる必要があります。既知のホストのファイル内の公開キーのエントリは、以下の例のようになります。

```
10.1.0.54 1024 35
```

```
15684995401867669259333946775054617325313674890836547254
```

```
15020245593199868544358361651999923329781766065830956
```

```
10825913212890233 76546801726272571413428762941301196195566782
```

```
59566410486957427888146206519417467729848654686157177393901647
79355942303577413098022737087794545240839717526463580581767167
09574804776117
```

3. スイッチへのクライアントの公開キーのインポート - 「ユーザの公開キーのインポート」を参照するか、`copy tftp public-key` コマンドを使用して、すべての SSH クライアントに付与されているスイッチに対する管理アクセス権の公開キーを含むファイルをコピーします（それらの SSH クライアントは、p.291 ▲で説明されている「User Accounts」画面を使用して、スイッチでローカルに設定する必要があるということに注意してください）。SSH クライアントは、後で、それらの公開キーを使用して認証されます。現行のファームウェアは、(RSA V1 のキーの例として以下に示されているような) 標準の UNIX フォーマットに基づく公開キーファイルのみを受け入れます。

```
1024 35
13410816856098939210409449201554253476316419218729589211431738
80055536161631051775940838686311092912322268285192543746031009
37187721199696317813662774141689851320491172048303392543241016
37997592371449011938006090253948408482717819437228840253311595
2134861022902978982721353267131629432532818915045306393916643
steve@192.168.1.19
```

4. オプションパラメータの設定 - 「SSH」設定画面で、認証タイムアウト、再試行回数、サーバキーのサイズなどのオプションパラメータを設定します。
5. SSH サービスの有効化 - 「SSH」設定ページで、スイッチの SSH サーバを有効にします。
6. 認証 - 以下のいずれかの認証方式が使用されます。
 - パスワード認証 (SSH V1.5 または V2 クライアントの場合)
 - a. クライアントが自らのパスワードをサーバに送信します。
 - b. スイッチがクライアントのパスワードとメモリに保存されているパスワードを照合します。
 - c. マッチするものが検出されると、接続が許可されます。

[注意] SSH でパスワード認証のみを使用する場合でも、ホストの公開キーが、初期接続時に、または、既知のホストのファイルへの手動入力によって、クライアントに提供されるようにしなければなりません。ただし、クライアントのキーを設定する必要はありません。

公開キー認証

SSH クライアントがスイッチにコンタクトしようとする、SSH サーバは、ホストキーのペアを使用して、セッションキーおよび暗号化方式をネゴシエーションします。スイッチに保存されている公開キーに対応する秘密キーをもつクライアントのみが、スイッチにアクセスすることができます。このプロセスの間、以下のような情報交換が実行されます。

SSH V1.5 クライアントの認証

- a. クライアントが自らの RSA 公開キーをスイッチに送信します。
- b. スイッチがクライアントの公開キーとメモリに保存されている秘密キーを照合します。
- c. マッチするものが検出されると、スイッチは、その秘密キー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、ユーザの公開キーを使用してその文字列を暗号化してからクライアントに送信します。
- d. クライアントは、その秘密キーを使用してチャレンジ文字列を復号し、MD5 チェックサムを計算して、そのチェックサムをスイッチに戻します。
- 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を、送信した元の文字列について計算されたチェックサムと比較します。2 つのチェックサムが一致する場合は、クライアントの秘密キーが認証済みの公開キーと対応していることを意味し、クライアントが認証されます。

SSH V2 クライアントの認証

- a. クライアントは、最初に、望ましいアルゴリズムによる DSA 公開キー認証が許可されるかどうかを判別するため、スイッチに対して問い合わせを実行します。
- b. スイッチは、指定されたアルゴリズムをサポートしている場合には、クライアントに対し、認証プロセスを続行するように通知します。サポートしていない場合は、要求を拒否します。
- c. クライアントは、秘密キー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、そのメッセージを受信すると、提供されたキーが認証で受け入れられるかどうかをチェックし、受け入れられる場合は、署名が正しいものであるかどうかをチェックします。両方のチェックが正常に完了すると、クライアントが認証されます。

[注意] 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、現行の Telnet セッションと SSH セッションの両方が含まれます。

[注意] SSH サーバには、スイッチの任意の設定済み IPv4 インターフェースアドレスまたは IPv6 インター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。

SSH サーバの設定

「Security」→「SSH」（Configure Global）を選択すると、SSH サーバを有効にすることや、認証の基本設定を設定することができます。

【注意】 SSH サーバを有効にする前に、ホストキーのペアをスイッチで設定する必要があります。「ホストキーのペアの生成」を参照してください。

関連する CLI 情報

「Secure Shell」

パラメータ

以下のパラメータが表示されます。

- ・ SSH Server Status – スイッチで SSH サーバを有効または無効にすることができます（デフォルト：Disabled）。
- ・ Version – SSH のバージョン番号。画面図ではバージョン 2.0 が表示されていますが、本製品では、SSHV1.5 と V2.0 のいずれかのクライアントによる管理アクセスをサポートしています。
- ・ Authentication Timeout – 認証の試行時にクライアントからの応答を SSH サーバが待機する時間（秒）を指定します（範囲：1 ～ 120 秒、デフォルト：120 秒）。
- ・ Authentication Retries – クライアントが許可される認証の試行回数を指定します。この回数を超えると、認証が失敗し、クライアントは認証プロセスを再び開始しなければなりません（範囲：1 ～ 5 回、デフォルト：3 回）。
- ・ Server-Key Size – SSH サーバキーのサイズを指定します（範囲：512 ～ 896 bits、デフォルト：768 bits）。
- ・ SSH サーバキーは、スイッチの外部で共有されることのない秘密キーです。
- ・ ホストキーは、SSH クライアントと共有され、1024 bits に固定されます。

Web インターフェース

SSH サーバを設定するには、以下のようにします。

- (1) 「Security」→「SSH」を選択します。
- (2) 「Step」リストで「Configure Global」を選択します。
- (3) SSH サーバを有効にします。
- (4) 認証パラメータを必要に応じて調整します。

(5) < Apply > ボタンをクリックします。

The screenshot shows a web interface for configuring the SSH server. The breadcrumb navigation at the top reads "Security > SSH". Below this, a "Step:" dropdown menu is set to "1. Configure Global". The main configuration area contains the following settings:

SSH Server Status	☒ Enabled
Version	2.0
Authentication Timeout (1-120)	120 sec
Authentication Retries (1-5)	3
Server-Key Size (512-896)	768

At the bottom right of the configuration area, there are two buttons: "Apply" and "Revert".

画面 1-147 : SSH サーバの設定

ホストキーのペアの生成

「Security」→「SSH」（Configure Host Key – Generate）を選択すると、SSH クライアントとスイッチとの間でセキュアな接続を実現するために使用されるホストの公開キーと秘密キーのペアを生成することができます。キーペアを生成したら、「ユーザの公開キーのインポート」の説明に従って、ホストの公開キーを SSH クライアントに提供し、クライアントの公開キーをスイッチにインポートする必要があります。

【注意】 SSH サーバを有効にする前に、ホストキーのペアをスイッチで設定する必要があります。「SSH サーバの設定」を参照してください。

関連する CLI 情報

「Secure Shell」

パラメータ

以下のパラメータが表示されます。

- ・ Host-Key Type – ホストキーのペア（公開キーと秘密キー）を生成するために使用されるキータイプ（範囲：RSA (V1)、DSA (V2) または Both、デフォルト：Both）。
- ・ SSH サーバは、クライアントが初めてスイッチとの接続を確立するときに RSA または DSA を使用してキーを交換してから、データ暗号化に DES（56 bits）と 3DES（168 bits）のどちらを使用するかクライアントとネゴシエーションします。

【注意】 本製品では、SSH V1.5 クライアントには RSA V1 のみを、SSH V2 クライアントには DSA V2 のみを使用します。

- ・ Save Host-Key from Memory to Flash – RAM（つまり、揮発性メモリ）内のホストキーをフラッシュメモリに保存します。保存しない場合、ホストキーのペアは、デフォルトで、RAM に保存されます。この項目はホストキーのペアを生成する前に選択する必要がありますということに注意してください（デフォルト：Disabled）。

Web インターフェース

SSH ホストキーのペアを生成するには、以下のようになります。

- (1) 「Security」→「SSH」を選択します。
- (2) 「Step」リストで「Configure Host Key」を選択します。
- (3) 「Step」リストで「Generate」を選択します。
- (4) ドロップダウンリストでホストキーのタイプを選択します。
- (5) 必要な場合は、ホストキーをメモリからフラッシュメモリに保存するためのオプションを選択します。

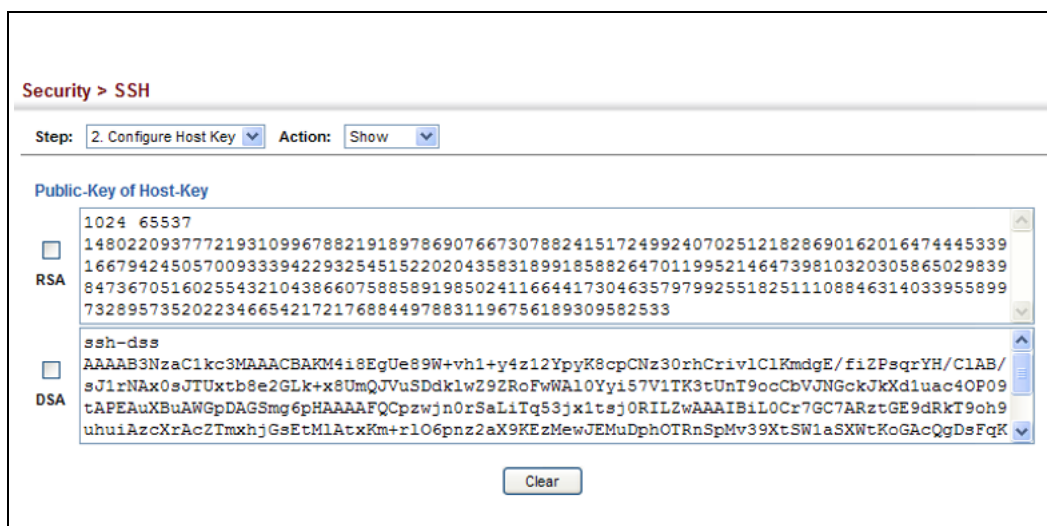
(6) < Apply > ボタンをクリックします。



画面 1-148 : SSH ホストキーのペアの生成

SSH ホストキーのペアを表示またはクリアするには、以下のようにします。

- (1) 「Security」 → 「SSH」 を選択します。
- (2) 「Step」 リストで 「Configure Host Key」 を選択します。
- (3) 「Step」 リストで 「Show」 を選択します。
- (4) クリアするホストキーのタイプを選択します。
- (5) < Clear > ボタンをクリックします。



画面 1-149 : SSH ホストキーのペアの表示

ユーザの公開キーのインポート

「Security」→「SSH」（Configure User Key - Copy）を選択すると、ユーザの公開キーをスイッチにアップロードすることができます。この公開キーは、ユーザが公開キー認証メカニズムを使用してログインできるようにするため、スイッチに保存する必要があります。ユーザの公開キーがスイッチ上に存在しない場合、SSH は、対話型パスワード認証メカニズムに戻って認証を終了します。

関連する CLI 情報

「Secure Shell」

パラメータ

以下のパラメータが表示されます。

- ・ User Name - 公開キーを管理するユーザをドロップダウンリストから選択します。先に「User Accounts」画面でユーザを作成する必要があるということに注意してください（「ユーザアカウントの設定」を参照）。
- ・ User Key Type - アップロードする公開キーのタイプ。
 - ・ RSA: RSA V1 暗号化公開キーをスイッチで受け入れます。
 - ・ DSA: DSA V2 暗号化公開キーをスイッチで受け入れます。SSH サーバは、クライアントが初めてスイッチとの接続を確立するときに RSA または DSA を使用してキーを交換してから、データ暗号化に DES（56 bits）と 3DES（168 bits）のどちらを使用するかクライアントとネゴシエーションします。
本製品では、SSH V1.5 クライアントには RSA V1 のみを、SSH V2 クライアントには DSA V2 のみを使用します。
- ・ TFTP Server IP Address - インポートする公開キーファイルが保存されている TFTP サーバの IP アドレス。
- ・ Source File Name - アップロードする公開キーファイル。

Web インターフェース

SSH ユーザの公開キーをコピーするには、以下のようにします。

- (1) 「Security」→「SSH」を選択します。
- (2) 「Step」リストで「Configure User Key」を選択します。
- (3) 「Step」リストで「Copy」を選択します。
- (4) ユーザ名と公開キータイプをそれぞれドロップダウンリストから選択し、TFTP サーバの IP アドレスおよび公開キーのソースファイルの名前を入力します。

(5) < Apply > ボタンをクリックします。

The screenshot shows the 'Security > SSH' configuration page. The 'Step' dropdown is set to '3. Configure User Key' and the 'Action' dropdown is set to 'Copy'. The 'User Name' is 'steve', 'User-Key Type' is 'RSA', 'TFTP Server IP Address' is '192.168.0.61', and 'Source File Name' is 'rsa.pub'. 'Apply' and 'Revert' buttons are at the bottom right.

画面 1-150 : SSH ユーザの公開キーのコピー

SSH ユーザの公開キーを表示またはクリアするには、以下のようにします。

- (1) 「Security」 → 「SSH」 を選択します。
- (2) 「Step」 リストで 「Configure User Key」 を選択します。
- (3) 「Step」 リストで 「Show」 を選択します。
- (4) ユーザを 「User Name」 リストで選択します。
- (5) クリアするホストキーのタイプを選択します。
- (6) < Clear > ボタンをクリックします。

The screenshot shows the 'Security > SSH' configuration page with 'Step' set to '3. Configure User Key' and 'Action' set to 'Show'. The 'User Name' is 'admin'. Under 'Public-Key of User-Key', there are two sections: 'RSA' and 'DSA'. The 'RSA' section shows a long public key string. The 'DSA' section shows a long public key string. A 'Clear' button is at the bottom right.

画面 1-151 : SSH ユーザの公開キーの表示

1.11.7 アクセスコントロールリスト

アクセスコントロールリスト (ACL: Access Control Lists) は、IPv4 パケットフィルタリング、(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 制御コードに基づく) フィルタリング、IPv6 パケット (アドレス、次のヘッダのタイプ、またはフローラベルに基づく) フィルタリング、あるいは 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実現します。着信パケットをフィルタリングするには、最初にアクセスコントロールリストを作成し、必要なルールを追加してから、リストを特定のポートにバインドします。

アクセスコントロールリストの設定

ACL は、IP アドレス、MAC アドレス、またはその他のより詳細な基準に適用される一連の許可条件または拒否条件のリストです。本製品では、イングレスパケットを ACL 内の条件と 1 つずつ照らし合わせてテストします。パケットは、許可ルールにマッチすると受け入れられ、拒否ルールにマッチするとドロップされます。マッチするルールがない場合、パケットは受け入れられません。

コマンドの使用

- ・ ACL には、以下の制限事項が適用されます。
- ・ ACL の最大数は 32 です。
- ・ ACL ごとのルールの最大数は 96 です。
- ・ ポートにバインドできるルールの最大数は、ACL タイプごと、つまり、MAC ACL、IP ACL (標準 ACL と拡張 ACL を含む)、IPv6 標準 ACL、および IPv6 拡張 ACL のそれぞれで 96 です。

ここで紹介しているルール (アクセス制御エントリ (ACE: Access Control Entry)) の最大数は、ワーストケースシナリオの場合の数です。実際には、スイッチでは TCAM (ACE を保存するために使用されるハードウェアテーブル) 内の ACE が圧縮されますが、見込まれる ACE の実際の最大数は、非常に多くの要素によって左右されるため、正確に見極めることはできません。その数は、ランタイム時に ACE のために確保されるハードウェアリソースの量によって決まります。

自動 ACE 圧縮機能は、ハードウェアリソースがより効率的に利用されるように、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。圧縮機能を使用しない場合、1 つの ACE によって TCAM 内の一定数のエントリが占領されてしまう可能性があります。つまり、ある ACL に 25 の ACE が含まれている場合、その ACL には TCAM 内の (25 x n) のエントリが必要になるということです (「n」は、1 つの ACL に必要な一定数の TCAM エントリ)。圧縮機能を使用すると、必要な TCAM エントリ数を減らすため、ACE が、TCAM に書き込まれる前にソフトウェアによって圧縮されます。例えば、ある ACL に、連続する IP アドレス範囲 (192.168.1.0 ~ 255 など) を分類する 128 の ACE が含まれているとします。圧縮が無効になっている場合、この ACL は TCAM 内の (128 x n) のエントリを占領し、ハードウェアリソースのほぼすべてを使用することになります。圧縮を使用すると、128 の ACE が IP アドレスを 192.168.1.0/24 として分類する 1 つの ACE に圧縮されるので、TCAM で必要なエントリは「n」個だけになります。以上は、理想的なケースにおける圧縮の例です。ワーストケースでは、ACE をまったく圧縮できず、使用される TCAM エントリ数が圧縮機能を使用しない場合と同じになることもあります。また、ACE を処理するために必要な時間が増える可能性もあります。

- ・ リストの最後に到達するまでにマッチするエントリが検出されない場合、トラフィックは拒否されます。そのため、頻繁にヒットするエントリがリストの先頭にくるよう

にしなければなりません。明示的に許可されないトラフィックは暗黙的に拒否されます。また、単一エントリの ACL に拒否エントリが 1 つだけ含まれている場合は、すべてのトラフィックが拒否されることになるので注意してください。そのため、ACL では少なくとも 1 つの許可ステートメントを使用する必要があります。使用しない場合、すべてのトラフィックがブロックされます。スイッチはマッチする最初のエントリを検出した時点でテストを停止するので、条件の順序は重要です。マッチ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 がチェックされる順序は、以下のとおりです。

1. イングレスポートの IP ACL 内と MAC ACL 内のユーザ定義のルールは同時にチェックされます。
2. 1 つの ACL 内のルールは、設定されている順序どおり、上から下にチェックされます。
3. IP ACL のチェックの結果がパケットを許可するものであるが、同じパケットに対する MAC ACL のチェックの結果がそれを拒否するものである場合、そのパケットは拒否されます（なぜならば、セキュリティ上の理由により、パケットの拒否決定の方が優先されるためです）。また、IP ACL によって拒否され、MAC ACL によって許可される場合にも、パケットは拒否されます。

期間の設定

「Security」 → 「ACL」（Configure Time Range）を選択すると、ACL 機能が適用される期間を設定することができます。

関連する CLI 情報

「Time Range」

パラメータ

以下のパラメータが表示されます。

Add

- ・ Time-Range Name – 期間の名前（範囲：1 ～ 30 文字）。

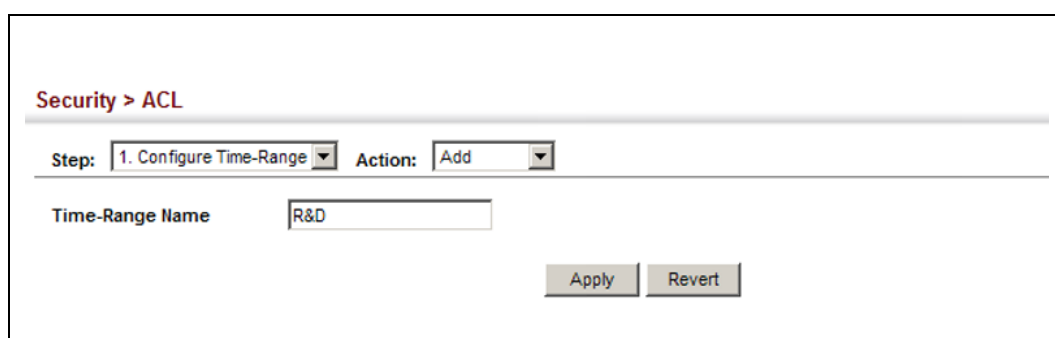
Add Rule

- ・ Time-Range – 期間の名前。
- ・ Mode
 - ・ Absolute – 特定の日時または期間を指定します。
 - ・ Start/End – 適用を開始または終了する年月日と時刻（時間と分）を指定します。
 - ・ Periodic – 定期的な間隔を指定します。
 - ・ Start/To – 適用を開始または終了する曜日と時刻（時間と分）を指定します。

Web インターフェース

期間を設定するには、以下のようになります。

- (1) 「Security」 → 「ACL」を選択します。
- (2) 「Step」 リストで「Configure Time Range」を選択します。
- (3) 「Step」 リストで「Add」を選択します。
- (4) 期間の名前を入力します。
- (5) < Apply > ボタンをクリックします。



Security > ACL

Step: 1. Configure Time-Range Action: Add

Time-Range Name R&D

Apply Revert

画面 1-152：期間の名前の設定

期間を一覧表示するには、以下のようにします。

- (1) 「Security」 → 「ACL」 を選択します。
- (2) 「Step」 リストで 「Configure Time Range」 を選択します。
- (3) 「Step」 リストで 「Show」 を選択します。

The screenshot shows the 'Security > ACL' configuration page. At the top, there is a breadcrumb 'Security > ACL'. Below it, a 'Step:' dropdown is set to '1. Configure Time-Range' and an 'Action:' dropdown is set to 'Show'. Underneath, a 'Time-Range List' is displayed with 'Max: 16' and 'Total: 1'. The list contains one entry with a checkbox and the name 'R&D'. At the bottom of the list are 'Delete' and 'Revert' buttons.

画面 1-153 : 期間の一覧表示

期間のルールを設定するには、以下のようにします。

- (4) 「Security」 → 「ACL」 を選択します。
- (5) 「Step」 リストで 「Configure Time Range」 を選択します。
- (6) 「Step」 リストで 「Add Rule」 を選択します。
- (7) ドロップダウンリストで期間の名前を選択します。
- (8) モードオプションとして 「Absolute」 または 「Periodic」 を選択します。
- (9) 選択したモードに関する必要なパラメータを指定します。
- (10) < Apply > ボタンをクリックします。

The screenshot shows the 'Security > ACL' configuration page with the 'Add Rule' form. The 'Step:' dropdown is '1. Configure Time-Range' and the 'Action:' dropdown is 'Add Rule'. The form includes a 'Time-Range' dropdown set to 'R&D' and a 'Mode' dropdown set to 'Periodic'. Below these are two columns of settings: 'Start' and 'To'. The 'Start' column has 'Days of the week' set to 'Weekend', 'Hours (0-23)' set to '5', and 'Minutes (0-59)' set to '30'. The 'To' column has 'Days of the week' set to 'Sunday', and empty fields for 'Hours (0-23)' and 'Minutes (0-59)'. At the bottom are 'Apply' and 'Revert' buttons.

画面 1-154 : 期間へのルールの追加

期間について設定されているルールを表示するには、以下のようになります。

- (1) 「Security」 → 「ACL」 を選択します。
- (2) 「Step」 リストで 「Configure Time Range」 を選択します。
- (3) 「Step」 リストで 「Show Rule」 を選択します。

The screenshot shows the 'Security > ACL' configuration page. At the top, there is a breadcrumb 'Security > ACL'. Below it, there are two dropdown menus: 'Step: 1. Configure Time-Range' and 'Action: Show Rule'. Underneath, there is a 'Time-Range' dropdown menu set to 'time1'. Below that, there is a section titled 'Time-Range Rule List' with 'Max: 8' and 'Total: 4'. This section contains a table with four columns: a checkbox, 'Mode', 'Start', and 'End'. The table lists four rules: an Absolute rule from 2009-01-01 10:05 to 2010-01-31 20:10, and three Periodic rules: Daily 10:05 to 20:10, Monday 10:05 to Tuesday 20:10, and Monday 00:00 to Tuesday 23:59. At the bottom of the table, there are 'Delete' and 'Revert' buttons.

☐	Mode	Start	End
☐	Absolute	2009-01-01 10:05	2010-01-31 20:10
☐	Periodic	Daily 10:05	Daily 20:10
☐	Periodic	Monday 10:05	Tuesday 20:10
☐	Periodic	Monday 00:00	Tuesday 23:59

画面 1-155 : 期間について設定されているルールの表示

TCAM の使用状況の表示

「Security」→「ACL」（Configure ACL - Show TCAM）を選択すると、使用されているポリシー制御エントリの数、空きエントリの数、TCAM の全体的な使用率など、TCAM（Ternary Content Addressable Memory）の使用状況パラメータを表示することができます。

関連する CLI 情報

「show access-list tcam-utilization」

コマンドの使用

ポリシー制御エントリ（PCE: Policy Control Entry）は、ACL、IP ソースガードフィルタリングルール、QoS プロセス、トラップなど、ルールに基づく検索に依存する各種のシステム機能で使用されます。

例えば、ACL をポートにバインドする場合は ACL 内のそれぞれのルールで 2 つの PCE が使用され、ポートの IP ソースガードのフィルタリングルールを設定する場合にもシステムで 2 つの PCE が使用されます。

パラメータ

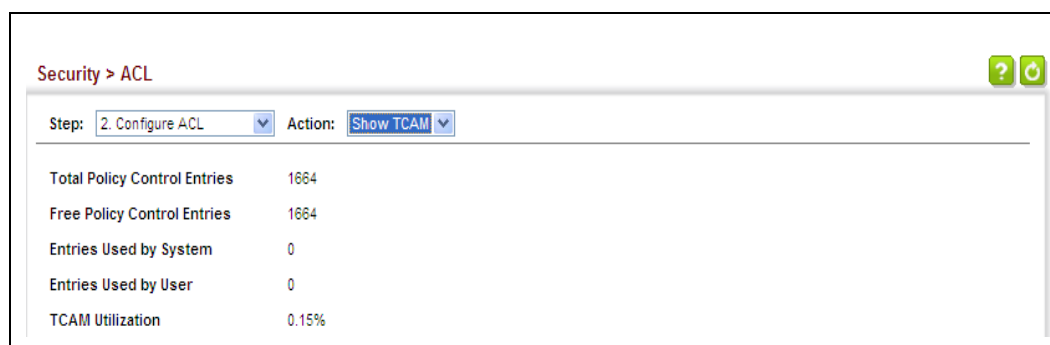
以下のパラメータが表示されます。

- ・ Total Policy Control Entries – 使用されているポリシー制御エントリの数。
- ・ Free Policy Control Entries – 使用可能なポリシー制御エントリの数。
- ・ Entries Used by System – オペレーティングシステムで使用されているポリシー制御エントリの数。
- ・ Entries Used by User – ACL などの設定情報で使用されているポリシー制御エントリの数。
- ・ TCAM Utilization – TCAM の全体的な使用率。

Web インターフェース

TCAM の使用状況に関する情報を表示するには、以下のようになります。

- (1) 「Security」→「ACL」を選択します。
- (2) 「Step」リストで「Configure ACL」を選択します。
- (3) 「Step」リストで「Show TCM」を選択します。



画面 1-156 : TCAM の使用状況の表示

ACL の名前とタイプの設定

「Security」→「ACL」（Configure ACL - Add）を選択すると、ACL を作成することができます。

関連する CLI 情報

「access-list ip」

「show ip access-list」

パラメータ

以下のパラメータが表示されます。

- ・ ACL Name - ACL の名前（最大長：32 文字）。
- ・ Type - 以下のフィルタリングモードがサポートされています。
 - ・ IP Standard: 送信元 IPv4 アドレスに基づいてパケットをフィルタリングする IPv4 ACL モード。
 - ・ IP Extended: 送信元または宛先 IPv4 アドレスに加え、プロトコルタイプおよびプロトコルポート番号に基づいてパケットをフィルタリングする IPv4 ACL モード。「TCP」プロトコルを指定する場合は、TCP 制御コードに基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: 送信元 IPv6 アドレスに基づいてパケットをフィルタリングする IPv6 ACL モード。
 - ・ IPv6 Extended: 送信元または宛先 IPv6 アドレスに加え、次のヘッダのタイプおよびフローラベル（IPv6 ルータによる特別な処理の要求）に基づいてパケットをフィルタリングする IPv6 ACL モード。
 - ・ MAC - 送信元または宛先 MAC アドレスおよびイーサネットフレームタイプ（RFC 1060）に基づいてパケットをフィルタリングする MAC ACL モード。
 - ・ ARP - ARP インスペクションで使用される IP と MAC アドレスとのスタティックバインディングを指定する ARP ACL（「ARP インスペクション」を参照）。

Web インターフェース

ACL の名前とタイプを設定するには、以下のようになります。

- (1) 「Security」→「ACL」を選択します。
- (2) 「Step」リストで「Configure ACL」を選択します。
- (3) 「Step」リストで「Add」を選択します。
- (4) 「ACL Name」フィールドを指定し、ACL のタイプを選択します。

(5) < Apply > ボタンをクリックします。

Security > ACL

Step: 2. Configure ACL Action: Add

ACL Name R&D

Type IP Standard

Apply Revert

画面 1-157 : ACL の作成

ACL を一覧表示するには、以下のようにします。

- (1) 「Security」 → 「ACL」 を選択します。
- (2) 「Step」 リストで 「Configure ACL」 を選択します。
- (3) 「Step」 リストで 「Show」 を選択します。

Security > ACL

Step: 2. Configure ACL Action: Show

ACL List Max: 2048 Total: 1

	ACL Name	Type
☐	R&D	IP Standard

Delete Revert

画面 1-158 : ACL の一覧表示

標準 IPv4 ACL の設定

「Security」 → 「ACL」 (Configure ACL - Add Rule - IP Standard) を選択すると、標準 IPv4 ACL を設定することができます。

関連する CLI 情報

「permit, deny (Standard IP ACL)」
「show ip access-list」
「Time Range」

パラメータ

以下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 - 選択されたタイプにマッチする ACL の名前が表示されます。
- ・ Action - ACL には任意の組み合わせの許可ルールと拒否ルール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。「Any」の場合は使用可能なすべてのアドレスを含めることができ、「Host」の場合は特定のホストアドレスを「Address」フィールドで指定することができ、「IP」の場合はアドレス範囲を「Address」フィールドと「Subnet Mask」フィールドで指定することができます（オプション：Any、Host または IP、デフォルト：Any）。
- ・ Source IP Address - 送信元 IP アドレス。
- ・ Source Subnet Mask - それぞれピリオドで区切られた 0 から 255 までの範囲内の 4 つの整数を含むサブネットマスク。サブネットマスクでは、1 bit は「match」を示し、0 bit は「ignore」を示します。サブネットマスクと指定された送信元 IP アドレスとのビット論理積が求められ、ACL が割り当てられているポートに入ってくる各 IP パケットのアドレスと比較されます。
- ・ Time Range - 期間の名前。

Web インターフェース

標準 IPv4 ACL にルールを追加するには、以下のようにします。

- (1) 「Security」→「ACL」を選択します。
- (2) 「Step」リストで「Configure ACL」を選択します。
- (3) 「Step」リストで「Add Rule」を選択します。
- (4) 「Type」リストで「IP Standard」を選択します。
- (5) 「Name」リストで ACL の名前を選択します。
- (6) アクション（「Permit」または「Deny」）を選択します。
- (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およびアドレス範囲のマスクを入力します。

(9) < Apply > ボタンをクリックします。

Security > ACL

Step: 2. Configure ACL Action: Add Rule

Type: ☒ IP Standard ☐ IP Extended ☐ MAC ☐ IPv6 Standard ☐ IPv6 Extended ☐ ARP

Name: R&D

Action: Permit

Address Type: Host

Source IP Address: 10.1.1.21

Source Subnet Mask: 255.255.255.255

☒ Time-Range: R&D

Apply Revert

画面 1-159 : 標準 IPv4 ACL の設定

拡張 IPv4 ACL の設定

「Security」→「ACL」(Configure ACL - Add Rule - IP Extended) を選択すると、拡張 IPv4 ACL を設定することができます。

関連する CLI 情報

「permit, deny (Extended IPv4 ACL)」

「show ip access-list」

「Time Range」

パラメータ

以下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 - 選択されたタイプにマッチする ACL の名前が表示されます。
- ・ Action - ACL には任意の組み合わせの許可ルールと拒否ルールを含めることができます。
- ・ Source/Destination Address Type - 送信元または宛先 IP アドレスを指定します。「Any」の場合は使用可能なすべてのアドレスを含めることができ、「Host」の場合は特定のホストアドレスを「Address」フィールドで指定することができ、「IP」の場合はアドレス範囲を「Address」フィールドと「Subnet Mask」フィールドで指定することができます (オプション: Any、Host または IP、デフォルト: Any)。
- ・ Source/Destination IP Address - 送信元または宛先 IP アドレス。
- ・ Source/Destination Subnet Mask - 送信元アドレスまたは宛先アドレスのサブネットマスクの説明を参照)。

- ・ Source/Destination Port – 指定したプロトコルタイプの送信元ポートまたは宛先ポートの番号（範囲：0 ～ 65,535）。
- ・ Source/Destination Port Bit Mask – マッチするポートビットを表わす 10 進数（範囲：0 ～ 65,535）。
- ・ Protocol – マッチするプロトコルタイプとして「TCP」、「UDP」、または「Others」を指定します。「Others」は特定のプロトコル番号（0 ～ 255）であることを示します（オプション：TCP、UDP または Others、デフォルト：TCP）。
- ・ Service Type – 以下の基準に基づくパケットの優先度設定。
 - ・ ToS – ToS レベル（範囲：0 ～ 15）。
 - ・ Precedence – IP 優先レベル（範囲：0 ～ 7）。
 - ・ DSCP – DSCP 優先レベル（範囲：0 ～ 63）。
- ・ Control Code – TCP ヘッダの第 14 バイト目でフラグビットを指定する（ビット文字列を表わす）10 進数（範囲：0 ～ 63）。
- ・ Control Code Bit Mask – マッチするコードビットを表わす 10 進数（範囲：0 ～ 63）。制御ビットマスクとは、制御コードに適用される（同等のバイナリビットマスクの）10 進数です。10 進数を入力します。同等のバイナリビット「1」はビットがマッチすることを意味し、「0」はビットを無視することを意味します。指定できるビットは、以下のとおりです。
 - ・ 1 (fin) – 完了
 - ・ 2 (syn) – 同期
 - ・ 4 (rst) – リセット
 - ・ 8 (psh) – プッシュ
 - ・ 16 (ack) – 肯定応答
 - ・ 32 (urg) – 緊急ポインタ例えば、以下のようにコード値とマスクを使用して、フラグが設定されているパケットを取得することができます。
 - ・ SYN フラグ有効、制御コード 2 を使用、制御ビットマスク 2
 - ・ SYN と ACK が共に有効、制御コード 18 を使用、制御ビットマスク 18
 - ・ SYN が有効で ACK が無効、制御コード 2 を使用、制御ビットマスク 18
- ・ Time Range – 期間の名前。

Web インターフェース

拡張 IPv4 ACL にルールを追加するには、以下のようにします。

- (1) 「Security」 → 「ACL」 を選択します。
- (2) 「Step」 リストで 「Configure ACL」 を選択します。
- (3) 「Step」 リストで 「Add Rule」 を選択します。
- (4) 「Type」 リストで 「IP Extended」 を選択します。
- (5) 「Name」 リストで ACL の名前を選択します。
- (6) アクション（「Permit」 または 「Deny」）を選択します。
- (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および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、制御コードなど、その他の必要な基準を設定します。
- (10) < Apply > ボタンをクリックします。

The screenshot shows the 'Security > ACL' configuration page. The 'Step' is '2. Configure ACL' and the 'Action' is 'Add Rule'. The 'Type' is 'IP Extended'. The 'Name' is 'R&D#2'. The 'Action' is 'Permit'. The 'Source Address Type' is 'IP' with 'Source IP Address' '10.7.1.0' and 'Source Subnet Mask' '255.255.255.0'. The 'Destination Address Type' is 'Any' with 'Destination IP Address' '0.0.0.0' and 'Destination Subnet Mask' '0.0.0.0'. The 'Protocol' is 'TCP (6)'. The 'Service Type' is 'ToS (0-15)'. The 'Time-Range' is 'R&D'. The 'Apply' and 'Revert' buttons are at the bottom.

Security > ACL

Step: 2. Configure ACL Action: Add Rule

Type ☐ IP Standard ☒ IP Extended ☐ MAC ☐ IPv6 Standard ☐ IPv6 Extended ☐ ARP

Name R&D#2

Action Permit

Source Address Type IP Destination Address Type Any

Source IP Address 10.7.1.0 Destination IP Address 0.0.0.0

Source Subnet Mask 255.255.255.0 Destination Subnet Mask 0.0.0.0

Source Port (0-65535)

Source Port Bit Mask (0-65535)

Destination Port (0-65535)

Destination Port Bit Mask (0-65535)

Protocol ☒ TCP (6) ☐ UDP (17) ☐ Others

Service Type ☒ ToS (0-15) ☐ DSCP (0-63) Precedence (0-7)

Control Code (0-63)

Control Code Bit Mask (0-63)

☐ Time-Range R&D

Apply Revert

画面 1-160 : 拡張 IPv4 ACL の設定

標準 IPv6 ACL の設定

「Security」→「ACL」（Configure ACL - Add Rule - IPV6 Standard）を選択すると、標準 IPv6 ACL を設定することができます。

関連する CLI 情報

「permit, deny (Standard IPv6 ACL)」

「show ipv6 access-list」

「Time Range」

パラメータ

以下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 - 選択されたタイプにマッチする ACL の名前が表示されます。
- ・ Action - ACL には任意の組み合わせの許可ルールと拒否ルール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。「Any」の場合は使用可能なすべてのアドレスを含めることができ、「Host」の場合は特定のホストアドレスを「Address」フィールドで指定することができ、「IPv6-prefix」の場合はアドレス範囲を「Address」フィールドと「Subnet Mask」フィールドで指定することができます（オプション：Any、Host または IPv6-prefix、デフォルト：Any）。
- ・ Source IPv6 Address - 送信元 IPv6 アドレスまたはネットワーククラス。アドレスは、コロンで区切られた 16 bits の 16 進数値を 8 つ使用して、RFC 2373 「IPv6 Addressing Architecture」に準拠する形式で指定しなければなりません。アドレスでダブルコロンを 1 つ使用して、未定義フィールドを埋めるために必要な該当数の 0（ゼロ）を示すこともできます。
- ・ Source Prefix-Length - プレフィックス（つまり、アドレスのネットワーク部）を設定するアドレスの（先頭からの）連続ビットの数を示す 10 進数。
- ・ Time Range - 期間の名前。

Web インターフェース

標準 IPv6 ACL にルールを追加するには、以下のようになります。

- (1) 「Security」→「ACL」を選択します。
- (2) 「Step」リストで「Configure ACL」を選択します。
- (3) 「Step」リストで「Add Rule」を選択します。
- (4) 「Type」リストで「IPv6 Standard」を選択します。
- (5) 「Name」リストで ACL の名前を選択します。
- (6) アクション（「Permit」または「Deny」）を選択します。
- (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長を入力します。

(9) < Apply > ボタンをクリックします。

Security > ACL

Step: 2. Configure ACL Action: Add Rule

Type: ☐ IP Standard ☐ IP Extended ☐ MAC ☒ IPv6 Standard ☐ IPv6 Extended ☐ ARP

Name: R&D#6S

Action: Permit

Source Address Type: Host

Source IPv6 Address: 2009:DB9:2229::79

Source Prefix Length (0-128): 128

☐ Time-Range R&D

Apply Revert

画面 1-161 : 標準 IPv6 ACL の設定

拡張 IPv6 ACL の設定

「Security」→「ACL」（Configure ACL - Add Rule - IPv6 Extended）を選択すると、拡張 IPv6 ACL を設定することができます。

関連する CLI 情報

「permit, deny (Extended IPv6 ACL)」

「show ipv6 access-list」

「Time Range」

パラメータ

以下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 - 選択されたタイプにマッチする ACL の名前が表示されます。
- ・ Action - ACL には任意の組み合わせの許可ルールと拒否ルールを含めることができます。
- ・ Destination Address Type - 宛先 IP アドレスを指定します。「Any」の場合は使用可能なすべてのアドレスを含めることができ、「IPv6-prefix」の場合はアドレス範囲を指定することができます（オプション：Any または IPv6-prefix、デフォルト：Any）。
- ・ Destination IPv6 Address - IPv6 アドレスまたはネットワーククラス。アドレスは、コロンで区切られた 16 bits の 16 進数値を 8 つ使用して、RFC 2373 「IPv6 Addressing

Architecture」に準拠する形式で指定しなければなりません。アドレスでダブルコロンを1つ使用して、未定義フィールドを埋めるために必要な該当数の0（ゼロ）を示すこともできます（本製品は、宛先アドレスの先頭の64 bitsのみをチェックします）。

- ・ Destination Prefix-Length – プレフィックス（つまり、アドレスのネットワーク部）を設定するアドレスの（先頭からの）連続ビットの数を示す10進数（範囲：0～64 bits）。
- ・ DSCP – DSCP トラフィッククラス（範囲：0～63）。
- ・ Next Header – IPv6 ヘッダの次のヘッダのタイプを特定します（範囲：0～255）。オプションのインターネットレイヤ情報は、エンコードされて、パケット内でIPv6ヘッダと上位レイヤの間に配置される別のヘッダに入れます。そのような拡張ヘッダはいくつかあり、それぞれが別々のNext Header値によって識別されます。IPv6では、RFC 1700のIPv4プロトコルフィールドについて定義される値がサポートされ、よく使用される以下のヘッダがパケットに含められます。
 - 0：ホップバイホップオプション（RFC 2460）
 - 6：TCP上位ヘッダ（RFC 1700）
 - 17：UDP上位ヘッダ（RFC 1700）
 - 43：ルーティング（RFC 2460）
 - 44：フラグメント（RFC 2460）
 - 50：セキュリティペイロードのカプセル化（RFC 2406）
 - 51：認証（RFC 2402）
 - 60：宛先オプション（RFC 2460）
- ・ Flow Label – 送信者が、デフォルト以外のQoSや「リアルタイム」サービスなど（RFC 2460を参照）、IPv6ルータによる特別な処理を要求する特定のトラフィック「フロー」に属するパケットのラベル（範囲：0～1,048,575）。フローラベルは、フローの送信元ノードによってフローに割り当てられます。新規のフローラベルは、1～FFFFFF（16進数）の範囲で疑似ランダムかつ一様に選択されなければなりません。そのようなランダム割り当ての目的は、Flow Labelフィールド内のあらゆるビットセットを、フローに関連付けられている状態を検索するためのハッシュキーとしてルータが使用するのに適したものとなるようにすることにあります。フローラベルによって、仲介ルータによる特別な処理を必要とする特定の（ユニキャストまたはマルチキャストの）宛先に特定の送信元から送信されるパケットの順序が識別されます。その特別な処理の性質は、RSVP（ReSource ReserVation Protocol）などの制御プロトコルによって、または、フローのパケット自体（例えば、ホップバイホップオプション内など）に含まれている情報によってルータに伝達されることがあります。フローは、送信元アドレスと非ゼロのフローラベルの組み合わせによって一意に識別されます。フローに属さないパケットは値0（ゼロ）のフローラベルを伝播します。フローラベルによって指定される機能をサポートしていないホストまたはルータは、パケットの発信時にはフィールドを0（ゼロ）に設定し、パケットの転送時にはフィールドを変更せずに渡し、パケットの受信時にはフィールドを無視しなければなりません。

Web インターフェース

拡張 IPv6 ACL にルールを追加するには、以下のようになります。

- (1) 「Security」 → 「ACL」 を選択します。
- (2) 「Step」 リストで 「Configure ACL」 を選択します。
- (3) 「Step」 リストで 「Add Rule」 を選択します。

- (4) 「Type」 リストで「IPv6 Extended」を選択します。
- (5) 「Name」 リストで ACL の名前を選択します。
- (6) アクション（「Permit」または「Deny」）を選択します。
- (7) アドレスタイプ（「Any」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、次のヘッダ、フローラベルなど、その他の必要な基準を設定します。
- (10) < Apply > ボタンをクリックします。

Security > ACL

Step: 2. Configure ACL Action: Add Rule

Type ☐ IP Standard ☐ IP Extended ☐ MAC ☐ IPv6 Standard ☒ IPv6 Extended ☐ ARP

Name R&D#6E

Action Permit

Destination Address Type IPv6-Prefix

Destination IPv6 Address 2009:DB9:2229::79

Destination Prefix Length (0-64) 48

DSCP (0-63)

Next-Header (0-255)

Flow-Label (0-1048575)

☐ Time-Range R&D

Apply Revert

画面 1-162 : 拡張 IPv6 ACL の設定

MAC ACL の設定

「Security」→「ACL」（Configure ACL - Add Rule - MAC）を選択すると、ハードウェアアドレス、パケットのフォーマット、およびイーサネットタイプに基づいて MAC ACL を設定することができます。

関連する CLI 情報

「permit, deny (MAC ACL)」

「show ip access-list」

「Time Range」

パラメータ

以下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 - 選択されたタイプにマッチする ACL の名前が表示されます。
- ・ Action - ACL には任意の組み合わせの許可ルールと拒否ルールを含めることができます。
- ・ Source/Destination Address Type - 「Any」の場合は使用可能なすべてのアドレスを含めることができ、「Host」の場合は特定の MAC アドレスを指定することができ、「MAC」の場合はアドレス範囲を「Address」フィールドと「Bit Mask」フィールドで指定することができます（オプション：Any、Host または 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 進数マスク。
- ・ Packet Format - この属性には、以下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。
 - ・ Untagged-eth2 - タグなしイーサネット II パケット。
 - ・ Untagged-802.3 - タグなしイーサネット 802.3 パケット。
 - ・ tagged-eth2 - タグ付きイーサネット II パケット。
 - ・ Tagged-802.3 - タグ付きイーサネット 802.3 パケット。
- ・ VID - VLAN ID（範囲：1 ～ 4,094）。
- ・ VID Bit Mask - VLAN ビットマスク（範囲：1 ～ 4,094）。
- ・ Ethernet Type - このオプションは、イーサネット II フォーマットのパケットをフィルタリングするためにのみ使用することができます（範囲：600 ～ FFFF（16 進数））。
- ・ イーサネットプロトコルタイプの詳細な一覧は RFC 1060 で確認することができます。
- ・ 比較的によく使用されるタイプとして、0800 (IP)、0806 (ARP)、8137 (IPX) などがあります。
- ・ Ethernet Type Bit Mask - プロトコルのビットマスク（範囲：600 ～ FFFF（16 進数））。
- ・ Time Range - 期間の名前。

Web インターフェース

MAC ACL にルールを追加するには、以下のようにします。

- (1) 「Security」 → 「ACL」 を選択します。
- (2) 「Step」 リストで 「Configure ACL」 を選択します。
- (3) 「Step」 リストで 「Add Rule」 を選択します。
- (4) 「Type」 リストで 「MAC」 を選択します。
- (5) 「Name」 リストで ACL の名前を選択します。
- (6) アクション（「Permit」 または 「Deny」）を選択します。
- (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、ベースアドレスおよびアドレス範囲のビットマスク（16 進数）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 > ボタンをクリックします。

The screenshot shows the 'Security > ACL' configuration page. The 'Step' dropdown is set to '2. Configure ACL' and the 'Action' dropdown is set to 'Add Rule'. Under the 'Type' section, the 'MAC' radio button is selected. The 'Name' dropdown is set to 'R&D#3'. In the 'Action' section, the 'Permit' dropdown is selected. The 'Source Address Type' is set to 'Any'. The 'Source MAC Address' and 'Source Bit Mask' fields both contain '00-00-00-00-00-00'. The 'Destination Address Type' is set to 'Any'. The 'Destination MAC Address' and 'Destination Bit Mask' fields both contain '00-00-00-00-00-00'. The 'Packet Format' dropdown is set to 'Any'. The 'VID (1-4094)' field contains '12'. The 'VID Bit Mask (1-4094)' field contains '4094'. The 'Ethernet Type' field is empty, with '(600-FFFF, hexadecimal value)' as a hint. The 'Ethernet Type Bit Mask' field is empty, with '(600-FFFF, hexadecimal value)' as a hint. The 'Time-Range' checkbox is unchecked, and the 'rd' dropdown is set to 'rd'. At the bottom, there are 'Apply' and 'Revert' buttons.

画面 1-163 : MAC ACL の設定

ARP ACL の設定

「Security」→「ACL」(Configure ACL - Add Rule - ARP)を選択すると、ARP メッセージアドレスに基づいて ACL を設定することができます。それから、それらの ACL を ARP インスペクションで使用して、疑わしいトラフィックをフィルタリングすることができます(「ARP インスペクションのグローバル設定の設定」を参照)。

関連する CLI 情報

「permit, deny (ARP ACL)」

「show ip access-list」

「Time Range」

パラメータ

以下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 - 選択されたタイプにマッチする ACL の名前が表示されます。
- ・ Action - ACL には任意の組み合わせの許可ルールと拒否ルールを含めることができます。
- ・ Packet Type - ARP 要求、ARP 応答、または両方のタイプを示します(範囲: Request、Response または All、デフォルト: Request)。
- ・ Source/Destination IP Address Type - 送信元または宛先 IPv4 アドレスを指定します。「Any」の場合は使用可能なすべてのアドレスを含めることができ、「Host」の場合は特定のホストアドレスを「Address」フィールドで指定することができ、「IP」の場合はアドレス範囲を「Address」フィールドと「Subnet Mask」フィールドで指定することができます(オプション: Any、Host または IP、デフォルト: Any)。
- ・ Source/Destination IP Address - 送信元または宛先 IP アドレス。
- ・ Source/Destination IP Subnet Mask - 送信元アドレスまたは宛先アドレスのサブネットマスクのサブネットマスクの説明を参照)。
- ・ Source/Destination MAC Address Type - 「Any」の場合は使用可能なすべてのアドレスを含めることができ、「Host」の場合は特定の MAC アドレスを指定することができ、「MAC」の場合はアドレス範囲を「Address」フィールドと「Bit Mask」フィールドで指定することができます(オプション: Any、Host または 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 MAC Bit Mask - 送信元 MAC アドレスまたは宛先 MAC アドレスの 16 進数マスク。
- ・ Log - パケットがアクセス制御エントリとマッチする場合は、そのパケットをログに記録します。

Web インターフェース

ARP ACL にルールを追加するには、以下のようになります。

- (1) 「Security」 → 「ACL」 を選択します。
- (2) 「Step」 リストで 「Configure ACL」 を選択します。
- (3) 「Step」 リストで 「Add Rule」 を選択します。
- (4) 「Type」 リストで 「ARP」 を選択します。
- (5) 「Name」 リストで ACL の名前を選択します。
- (6) アクション（「Permit」 または 「Deny」）を選択します。
- (7) パケットタイプ（「Request」、「Response」、または 「All」）を選択します。
- (8) アドレスタイプ（「Any」、「Host」、または 「IP」）を選択します。
- (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、ベースアドレスおよびアドレス範囲のビットマスク（16 進数）を入力します。
- (10) 必要な場合は、ログを有効にします。
- (11) < Apply > ボタンをクリックします。

Security > ACL

Step: 2. Configure ACL Action: Add Rule

Type: ☐ IP Standard ☐ IP Extended ☐ MAC ☐ IPv6 Standard ☐ IPv6 Extended ☒ ARP

Name: R&D#7ARP

Action: Permit

Packet Type: All

Source IP Address Type: Any

Destination IP Address Type: Any

Source IP Address: 0.0.0.0

Destination IP Address: 0.0.0.0

Source IP Subnet Mask: 0.0.0.0

Destination IP Subnet Mask: 0.0.0.0

Source MAC Address Type: Any

Destination MAC Address Type: Any

Source MAC Address: 00-00-00-00-00-00

Destination MAC Address: 00-00-00-00-00-00

Source MAC Bit Mask: 00-00-00-00-00-00

Destination MAC Bit Mask: 00-00-00-00-00-00

☐ Log

Apply Revert

画面 1-164 : ARP ACL の設定

アクセスコントロールリストへのポートのバインディング

ACL を設定した後、「Security」→「ACL」（Configure Interface）を選択すると、トラフィックをフィルタリングする必要があるポートを該当の ACL にバインドすることができます。

関連する CLI 情報

「ip access-group」

「ipv6 access-group」

「show ip access-group」

「show ipv6 access-group」

「mac access-group」

「show mac access-group」

「Time Range」

コマンドの使用

- ・ 本製品は、イングレスフィルタリングについてのみ、ACL をサポートしています。
- ・ イングレスフィルタリングのため、1 つの ACL のみを任意のポートにバインドすることができます。

パラメータ

以下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 のタイプを指定します。
- ・ Port – ポート ID。
- ・ ACL – イングレスパケットに使用される ACL。
- ・ Time Range – 期間の名前。

Web インターフェース

ACL をポートにバインドするには、以下のようにします。

- (1) 「Security」→「ACL」を選択します。
- (2) 「Step」リストで「Configure Interface」を選択します。
- (3) 「Type」リストで「IP」または「MAC」を選択します。
- (4) 「ACL」リストで ACL の名前を選択します。

(5) < Apply > ボタンをクリックします。

Security > ACL

Step: 3. Configure Interface

Type ☒ IP ☐ MAC ☐ IPv6

Port 1

Ingress

ACL ☒ ips

Time-Range ☐ R&D

Apply Revert

画面 1-165 : ACL へのポートのバインディング

1.11.8 ARP インспекション

ARP インспекションは、アドレス解決プロトコルパケットについて MAC アドレスのバインディングの妥当性を検証するセキュリティ機能です。ARP インспекションは、ある種の「中間者」攻撃の足掛かりとなる MAC アドレスと IP アドレスとのバインディングが無効な ARP トラフィックに対する防御策を提供します。そのための方法として、ローカルの ARP キャッシュが更新される前、またはパケットが該当の宛先に転送される前に、すべての ARP 要求と ARP 応答をインターセプトし、それらのパケットをそれぞれ検証します。無効な ARP パケットはドロップされます。

ARP インспекションでは、DHCP スヌーピングバインディングデータベース（「DHCP スヌーピング設定」を参照）という、信頼できるデータベースに保存されている有効な IP アドレスと MAC アドレスとのバインディング情報に基づいて、ARP パケットの妥当性が判別されます。このデータベースは、DHCP スヌーピングによって作成されます（ただし、スイッチで DHCP スヌーピングがグローバルで有効になっており、必要な VLAN で有効になっていなければなりません）。また、ARP インспекションでは、静的に設定されたアドレスをもつホストのユーザ定義の ARP ACL（「ARP ACL の設定」を参照）と照らし合わせて ARP パケットの妥当性を検証することもできます。

コマンドの使用

ARP インспекションの有効化と無効化

- ・ ARP インспекションは、グローバルで制御することも、VLAN 単位で制御することもできます。
- ・ デフォルトでは、ARP インспекションは、グローバルでも、すべての VLAN でも無効になっています。
 - ・ ARP インспекションは、グローバルで有効になっている場合には、ARP インспекションが有効になっている VLAN でのみ、アクティブになります。
 - ・ ARP インспекションがグローバルで有効になっている場合、ARP インспекションが有効になっている VLAN では、すべての ARP 要求パケットと ARP 応答パケットが CPU にリダイレクトされ、それらのパケットのスイッチング動作は ARP インспекションエンジンによって処理されます。
 - ・ ARP インспекションは、グローバルで無効になっている場合には、すべての VLAN（ARP インспекションが有効になっている VLAN を含む）で無効になります。
 - ・ ARP インспекションが無効になっている場合、すべての ARP 要求パケットと ARP 応答パケットは ARP インспекションエンジンをバイパスし、それらのパケットのスイッチング動作は他のすべてのパケットのものと一致するようになります。
 - ・ グローバル ARP インспекションを無効にしてから再び有効にしても、いずれの VLAN の ARP インспекション設定にも影響しません。
 - ・ ARP インспекションがグローバルで無効になっている場合でも、個々の VLAN の ARP インспекションを設定することができます。そのような設定変更は、ARP インспекションが再びグローバルで有効にされた場合にのみ、アクティブになります。
- ・ 現行のファームウェアバージョンの ARP インспекションエンジンは、トランクポートでの ARP インспекションをサポートしていません。

ARP インспекションのグローバル設定の設定

「Security」→「ARP Inspection」（Configure General）を選択すると、各パケット内のアドレス情報の妥当性を検証するためにスイッチの ARP インспекションをグローバルで有効にすることや、ログを設定することができます。

関連する CLI 情報

「ARP Inspection」

コマンドの使用

ARP インспекションによる妥当性検証

- ・ デフォルトでは、ARP インспекションによる妥当性検証は無効になっています。
- ・ 以下の妥当性検証を少なくとも 1 つ指定すると、ARP インспекションによる妥当性検証がグローバルで有効になります。以下のチェックを任意に組み合わせて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内の宛先 MAC アドレスを ARP パケット本体内のターゲット MAC アドレスと照らし合わせてチェックします。このチェックは ARP 応答に対して実行されます。有効にすると、異なる MAC アドレスが含まれているパケットは、無効なものとして分類され、ドロップされます。
 - ・ IP – ARP パケット本体に無効な IP アドレスおよび予期されない IP アドレスが含まれていないかチェックします。そのようなアドレスとして、例えば、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などがあります。送信者 IP アドレスはすべての ARP 要求と ARP 応答でチェックされますが、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内の送信元 MAC アドレスを ARP パケット本体内の送信者 MAC アドレスと照らし合わせてチェックします。このチェックは ARP 要求と ARP 応答の両方に対して実行されます。有効にすると、異なる MAC アドレスが含まれているパケットは、無効なものとして分類され、ドロップされます。

ARP インспекションのログ記録

- ・ ARP インспекションのログ記録は、デフォルトで有効になっており、無効にすることはできません。
- ・ 管理者は、ログファシリティレートを設定することができます。
- ・ スイッチでパケットがドロップされる場合は、エントリがログバッファに保存され、システムメッセージがレート制御ベースで生成されます。システムメッセージが生成された後、エントリがログバッファからクリアされます。
- ・ それぞれのログエントリには、受信先 VLAN、ポート番号、送信元 IP アドレスと宛先 IP アドレス、送信元 MAC アドレスと宛先 MAC アドレスなどのフロー情報が含まれます。
- ・ 同一の有効な ARP パケットが複数同時に同じ VLAN で受信された場合は、ログファシリティによってログバッファのエントリが 1 つだけ生成され、対応するシステムメッセージが 1 つ生成されます。ログバッファが満杯になっている場合は、最も古いエントリが最も新しいエントリに置き換えられます。

パラメータ

以下のパラメータが表示されます。

- ・ ARP Inspection Status – ARP インспекションをグローバルで有効にします（デフォルト：Disabled）。
- ・ ARP Inspection Validation – 以下のいずれかのオプションが有効な場合に拡張 ARP インспекションによる妥当性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内の宛先 MAC アドレスを ARP 応答本文内のターゲット MAC アドレスと照らし合わせて妥当性を検証します。
 - ・ IP – ARP パケット本体に無効な IP アドレスおよび予期されない IP アドレスが含まれていないかチェックします。送信者 IP アドレスはすべての ARP 要求と ARP 応答でチェックされますが、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。
 - ・ Src-MAC – イーサネットヘッダ内の送信元 MAC アドレスを ARP パケット本体内の送信者 MAC アドレスと照らし合わせて妥当性を検証します。このチェックは ARP 要求と ARP 応答の両方に対して実行されます。
- ・ Log Message Number – ログメッセージ内に保存されるエントリの最大数（範囲：0 ～ 256、デフォルト：5）。
- ・ Log Interval – ログメッセージの送信間隔（範囲：0 ～ 86,400 秒、デフォルト：1 秒）。

Web インターフェース

ARP インспекションのグローバル設定を設定するには、以下のようになります。

- (1) 「Security」 → 「ARP Inspection」 を選択します。
- (2) 「Step」 リストで 「Configure General」 を選択します。
- (3) ARP インспекションをグローバルで有効にして、いずれかのアドレス妥当性検証オプションを有効にし、必要に応じてログパラメータを調整します。
- (4) < Apply > ボタンをクリックします。

Security > ARP Inspection

Step: 1. Configure General

ARP Inspection Status ☒ Enabled

ARP Inspection Validate ☒ Dst-MAC ☐ IP ☐ Src-MAC

Log Message Number (0-256)

Log Interval (0-86400) sec

Apply Revert

画面 1-166 : ARP インспекションのグローバル設定の設定

ARP インспекションの VLAN 設定の設定

「Security」→「ARP Inspection」（Configure VLAN）を選択すると、任意の VLAN について ARP インспекションを有効にすることや、使用する ARP ACL を指定することができます。

関連する CLI 情報

「ARP Inspection」

コマンドの使用

ARP インспекションの VLAN フィルタ（ACL）

- ・ デフォルトでは、ARP インспекションの ACL は、一切、設定されておらず、ARP インспекションは無効になっています。
- ・ ARP インспекションの ACL は、「ARP ACL 設定画面」を参照）で設定します。
- ・ ARP インспекションの ACL は、任意の設定済み VLAN に適用することができます。
- ・ ARP インспекションでは、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 アドレスと MAC アドレスとのバインディングのリストに使用します。ARP ACL は、DHCP スヌーピングバインディングデータベース内のエントリに優先します。本製品では、最初に、ARP パケットを、指定されているあらゆる ARP ACL と照合します。
- ・ 「Static」が指定されている場合、選択された ACL のみに基づいて ARP パケットの妥当性が検証されます。パケットは、マッチするルールに従ってフィルタリングされ、いずれのルールにもマッチしないパケットはドロップされて、DHCP スヌーピングバインディングデータベースによる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、最初に、選択された ACL に基づいて ARP パケットの妥当性が検証され、マッチする ACL ルールがない場合は、DHCP スヌーピングバインディングデータベースに基づいて ARP パケットの妥当性が判別されます。

パラメータ

以下のパラメータが表示されます。

- ・ ARP Inspection VLAN ID – 任意の設定済み VLAN を選択します（デフォルト：1）。
- ・ ARP Inspection VLAN Status – 選択した VLAN の ARP インспекションを有効にします（デフォルト：Disabled）。
- ・ ARP Inspection ACL Name
 - ・ ARP ACL – 任意の設定済み ARP ACL を選択することができます（デフォルト：None）。
 - ・ Static – ARP ACL が選択され、「Static」モードも選択されている場合は、ARP インспекションのみが実行され、DHCP スヌーピングバインディングデータベースに基づく妥当性検証はバイパスされます。ARP ACL が選択されているが、「Static」モードは選択されていない場合は、最初に ARP インспекションが実行されてから、DHCP スヌーピングバインディングデータベースに基づく妥当性検証が実行されます（デフォルト：Disabled）。

Web インターフェース

ARP インспекションの VLAN 設定を設定するには、以下のようになります。

- (1) 「Security」 → 「ARP Inspection」 を選択します。
- (2) 「Step」 リストで 「Configure VLAN」 を選択します。
- (3) 必要な VLAN について ARP インспекションを有効にし、設定済みアドレスを
チェックするための ARP ACL フィルタを選択してから、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によるチェックがバイパスされるように
「Static」 オプションを選択します。
- (4) < Apply > ボタンをクリックします。

Security > ARP Inspection

Step: 2. Configure VLAN

ARP Inspection VLAN ID: 1

ARP Inspection VLAN Status: ☒ Enabled

ARP Inspection ACL Name: ☒ aaa ☐ Static

Apply Revert

画面 1-167 : ARP インспекションの VLAN 設定の設定

ARP インспекションのインターフェース設定の設定

「Security」 → 「ARP Inspection」 (Configure Interface) を選択すると、ARP インспекションが必要なポートを選択することや、パケット検査レートを調整することができます。

関連する CLI 情報

「ARP Inspection」

パラメータ

以下のパラメータが表示されます。

- ・ Port – ポート ID。
- ・ Trust Status – ポートを信頼できるポートとして、または信頼できないポートとして設定します (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に ARP パケットレートリミットが適用され、すべての信頼できるポートは ARP パケットレートリミットの適用対象から除外されます。信頼できるインターフェースで受信されるパケットは、すべての ARP インспекションと ARP インспекションによる妥当性検証をバイパスし、常に転送されます。一方、信頼できないインターフェースで受信されるパケットは、設定されているすべての ARP インспекションによるテストを受けなければなりません。
- ・ Packet Rate Limit – 信頼できないポートで CPU によって処理できる 1 秒あたりの ARP パケットの最大数 (範囲: 0 ~ 2,048、デフォルト: 15)。このレートリミットは、信頼できるポートと信頼できないポートの両方に適用されます。レートリミットを「0」に設定するということは、CPU によって処理できる ARP パケットの数が制限されないこ

とを意味します。スイッチで設定されている ARP-packets-per-second レートリミットを超えてポートで受信された ARP パケットは、すべて、ドロップされます。

Web インターフェース

ARP インспекションのインターフェース設定を設定するには、以下のようにします。

- (1) 「Security」 → 「ARP Inspection」 を選択します。
- (2) 「Step」 リストで 「Configure Interface」 を選択します。
- (3) ARP インспекションが必要な信頼できないポートを指定し、パケット検査レートを調整します。
- (4) < Apply > ボタンをクリックします。

Port	Trust Status	Packet Rate Limit (0-2048 pps)
1	☒ Enabled	☒ 15
2	☐ Enabled	☒ 15
3	☐ Enabled	☒ 15
4	☐ Enabled	☒ 15
5	☐ Enabled	☒ 15

画面 1-168 : ARP インспекションのインターフェース設定の設定

ARP インスペクションに関する統計情報の表示

「Security」→「ARP Inspection」（Show Information - Show Statistics）を選択すると、処理された ARP パケットの数やさまざまな理由でドロップされた ARP パケットの数に関する統計情報を表示することができます。

関連する CLI 情報

「show ip arp inspection statistics」

パラメータ

以下のパラメータが表示されます。

パラメータ	説明
Received ARP packets before ARP inspection rate limit	ARP インスペクションのレートリミットを超えることなく受信された ARP パケットの数。
Dropped ARP packets in the process of ARP inspection rate limit	ARP インスペクションのレートリミットを超えて受信され（そして、ドロップされ）た ARP パケットの数。
ARP packets dropped by additional validation (IP)	IP アドレステストに合格しなかった ARP パケットの数。
ARP packets dropped by additional validation (Dst-MAC)	宛先 MAC アドレステストに合格しなかった ARP パケットの数。
Total ARP packets processed by ARP inspection	ARP インスペクションエンジンによって処理された ARP パケットの総数。
ARP packets dropped by additional validation (Src-MAC)	送信元 MAC アドレステストに合格しなかった ARP パケットの数。
ARP packets dropped by ARP ACLs	ARP ACL のルールに基づく妥当性検証に合格しなかった ARP パケットの数。
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基づく妥当性検証に合格しなかった ARP パケットの数。

表 1-6: ARP インスペクションに関する統計情報

Web インターフェース

ARP インスペクションに関する統計情報を表示するには、以下のようにします。

1. 「Security」 → 「ARP Inspection」 を選択します。
2. 「Step」 リストで 「Show Information」 を選択します。
3. 「Step」 リストで 「Show Statistics」 を選択します。

Security > ARP Inspection

Step: 4. Show Information ▼ Action: Show Statistics ▼

Received ARP packets before ARP inspection rate limit	1000
Dropped ARP packets in processing ARP inspection rate limit	5
Total ARP packets processed by ARP inspection	200
ARP packets dropped by additional validation (Src-MAC)	300
ARP packets dropped by additional validation (Dst-MAC)	2000
ARP packets dropped by additional validation (IP)	100
ARP packets dropped by ARP ACLs	5
ARP packets dropped by DHCP snooping	5

画面 1-169 : ARP インスペクションに関する統計情報の表示

ARP インспекションのログの表示

「Security」→「ARP Inspection」（Show Information - Show Log）を選択すると、関連付けられている VLAN、ポート、アドレスコンポーネントなど、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ことができます。

関連する CLI 情報

「show ip arp inspection log」

パラメータ

以下のパラメータが表示されます。

パラメータ	説明
VLAN ID	パケットが検出された VLAN。
Port	パケットが検出されたポート。
Src. IP Address	パケット内の送信元 IP アドレス。
Dst. IP Address	パケット内の宛先 IP アドレス。
Src. MAC Address	パケット内の送信元 MAC アドレス。
Dst. MAC Address	パケット内の宛先 MAC アドレス。

表 1-7: ARP インспекションのログ

Web インターフェース

ARP インспекションのログを表示するには、以下のようになります。

1. 「Security」→「ARP Inspection」を選択します。
2. 「Step」リストで「Show Information」を選択します。
3. 「Step」リストで「Show Log」を選択します。

Security > ARP Inspection

Step: 4. Show Information Action: Show Log

ARP Inspection Log List Max: 256 Total: 2

VLAN ID	Port	Src. IP Address	Dst. IP Address	Src. MAC Address	Dst. MAC Address
1	15	192.168.1.1	192.168.1.5	11-22-33-44-55-66	AA-BB-CC-DD-EE-FF
1	17	192.168.1.3	192.168.1.23	11-4E-33-75-55-BB	A0-3B-C9-DD-4E-1F

画面 1-170 : ARP インспекションのログの表示

1.11.9 管理アクセスのための IP アドレスフィルタリング

「Security」→「IP Filter」を選択すると、Web、SNMP、または Telnet インターフェースによるスイッチへの管理アクセスが許可される最大 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することができます。

関連する CLI 情報

「Management IP Filter」

コマンドの使用

- ・ 管理インターフェースは、デフォルトで、すべての IP アドレスに対して開かれています。エントリをフィルタリストに追加すると、該当のインターフェースに対するアクセスが特定のアドレスにのみ許可されるようになります。
- ・ 誰かが無効なアドレスからスイッチ上の管理インターフェースにアクセスしようとすると、接続が拒否され、イベントメッセージがシステムログに記録されて、トラップメッセージがトラップマネージャに送信されます。
- ・ IP アドレスは、SNMP、Web、Telnet のそれぞれのアクセスについて設定することができます。それらのグループは、それぞれ、最大 5 つの異なるアドレスセット（個々のアドレスとアドレス範囲のいずれか）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、重複するアドレス範囲は受け入れられません。別のグループのアドレスを入力する場合、重複するアドレス範囲は受け入れられます。
- ・ 指定したアドレス範囲から個々のアドレスを削除することはできません。範囲全体を削除してから、アドレスを再入力する必要があります。
- ・ アドレス範囲は、開始アドレスを指定するだけで削除することも、開始アドレスと終了アドレスの両方を指定して削除することもできます。

パラメータ

以下のパラメータが表示されます。

- ・ Mode
 - ・ 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。
- ・ Start IP Address – 単一の IP アドレス、またはアドレス範囲の開始アドレス。
- ・ End IP Address – アドレス範囲の終了アドレス。

Web インターフェース

管理アクセスが許可される IP アドレスのリストを作成するには、以下のようにします。

- (1) 「Security」→「IP Filter」を選択します。
- (2) 「Step」リストで「Add」を選択します。
- (3) フィルタリングする管理インターフェース（「Web」、「SNMP」、または「Telnet」）を選択します。

(4) インターフェースへの管理アクセスが許可される IP アドレスまたは IP アドレス範囲を入力します。

(5) < Apply > ボタンをクリックします。

Security > IP Filter

Action: Add ▼

Mode ☒ Web ☐ SNMP ☐ Telnet

Start IP Address 10.1.2.3

End IP Address

Apply Revert

画面 1-171 : 管理アクセスのための IP アドレスフィルタの作成

管理アクセスが許可される IP アドレスのリストを表示するには、以下のようにします。

(1) 「Security」 → 「IP Filter」を選択します。

(2) 「Step」 リストで「Show」を選択します。

Security > IP Filter

Action: Show ▼

Mode ☐ Web ☒ SNMP ☐ Telnet

SNMP IP Filter List Max: 5 Total: 1

	Start IP Address	End IP Address
☐	10.1.2.3	10.1.2.3

Delete Revert

画面 1-172 : 管理アクセスが許可される IP アドレスの表示

1.11.10 ポートセキュリティの設定

「Security」→「Port Security」を選択すると、スイッチポートで学習できるデバイス MAC アドレス、アドレステーブルに保存できるデバイス MAC アドレス、およびネットワークへのアクセスが許可されるデバイス MAC アドレスのそれぞれの最大数を設定することができます。

ポートセキュリティが有効になっている場合、スイッチで設定されている MAC アドレスの最大数に達すると、指定されているポートで新しい MAC アドレスが学習されなくなります。既にアドレステーブルに保存されている送信元アドレスを含んでいる着信トラフィックのみが、そのポートからのネットワークへのアクセスを許可されます。許可されていない MAC アドレスをもつデバイスがスイッチポートを使用しようとすると、ネットワーク侵入として検知され、アクション（ポートの無効化またはトラップメッセージの送信、あるいは、その両方）がスイッチによって自動的に実行されます。

関連する CLI 情報

「Port Security」

コマンドの使用

- ・セキュアポートで許可される MAC アドレスのデフォルトの最大数は 0 (= Disabled) です。ポートセキュリティを使用するには、ポートで許可されるアドレスの最大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するには、まず、ポートセキュリティを無効にしてから、許可されるダイナミックアドレスの最大数を指定します。スイッチでは、ポートで受信されるフレームについて、許可されているアドレスペア〈送信元 MAC アドレス, VLAN〉の最大数になるまでアドレスが学習されます。MAC アドレスの最大数に達すると、ポートで新しいアドレスが学習されなくなります。既にアドレステーブル内にある MAC アドレスは保持され、期限切れにはなりません。
ただし、スタティックアドレステーブルを使用して、手動でセキュアアドレスをポートに追加することができます。
- ・ポートセキュリティの状態が Enabled から Disabled 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になっており、許可されるアドレスの最大数が 0（ゼロ）以外に設定されている場合、アドレスがアドレステーブルに含まれていないデバイスがポートを使用しようとすると、スイッチへのアクセスが拒否されます。
- ・セキュリティ違反のため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」で表示される画面を使用して手動でポートを再び有効にする必要があります。
- ・セキュアポートには、以下の制限事項があります。
 - ・スタティックトランクまたはダイナミックトランクのメンバーとして使用することはできません。
 - ・ネットワーク相互接続デバイスに接続してはなりません。

パラメータ

以下のパラメータが表示されます。

- ・ Port - ポート番号。
- ・ Security Status - ポートセキュリティを有効 / 無効に設定します（デフォルト設定では、Disabled）。

- ・ Port Status - ステータスは以下のとおりです。
 - ・ Secure/Down - ポートセキュリティを無効にします。
 - ・ Secure/Up - ポートセキュリティを有効にします。
 - ・ Shutdown - ポートセキュリティへの違反により、ポートをシャットダウンします。
- ・ Action - ポートセキュリティ違反が検出された場合に実行されるアクションを示します。
 - ・ None: アクションは実行されません（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（範囲: 0 ~ 1,024 (0 = Disabled)）。最大アドレス数は、ポートセキュリティが有効になっている場合も無効になっている場合も適用されますが、「Security Status」が「Disabled」の場合にのみ設定することができます。
- ・ Current MAC Count - 現在関連のある MAC アドレス数
- ・ Mac Filter - MAC アドレスフィルタリング機能の設定の有無が表示されます。
- ・ Filter ID - MAC アドレスフィルタリングの識別子
- ・ Last Intrusion MAC - 最後に検出された認証されていない MAC アドレス
- ・ Last Time Detected Intrusion MAC - 認証されていない MAC アドレスが最後に検出された時間。

Web インターフェース

ポートセキュリティを設定するには、以下のようにします。

- (1) 「Security」 → 「Port Security」を選択します。
- (2) 選択したポートでポートセキュリティを有効にする場合は、「Security Status」のメニューをチェックしてセキュリティを有効にします。次に、無効なアドレスがポートで検出された場合に実行されるアクションを設定し、ポートで許可される MAC アドレスの最大数を設定します。
- (3) < Apply > ボタンをクリックします。

Port Security List Total: 26									
Port	Security Status	Port Status	Action	Max MAC Count (0-1024)	Current MAC Count	MAC Filter	MAC Filter ID	Last Intrusion MAC	Last Time Detected Intrusion MAC
1	☐ Enabled	Secure/Down	None	0	32	Disabled	0	NA	NA
2	☐ Enabled	Secure/Down	None	0	0	Disabled	0	NA	NA
3	☐ Enabled	Secure/Down	None	0	0	Disabled	0	NA	NA
4	☐ Enabled	Secure/Down	None	0	0	Disabled	0	NA	NA
5	☐ Enabled	Secure/Down	None	0	0	Disabled	0	NA	NA
6	☐ Enabled	Secure/Down	None	0	0	Disabled	0	NA	NA

画面 1-173 : ポートセキュリティの設定

1.11.11 802.1X ポート認証の設定

ネットワークスイッチでは、クライアント PC を接続するだけで、ネットワークリソースに対するオープンかつ簡単なアクセスが提供されます。そのような自動設定とアクセスは理想的な機能ですが、未承認ユーザがネットワークに簡単に侵入して機密データにアクセスすることを許してしまう可能性もあります。

IEEE 802.1X (dot1X) 規格では、最初に認証のための証明書を提示するようにユーザに要求することによってネットワークへの未承認アクセスを防ぐポートベースのアクセス制御プロシージャが規定されています。ネットワーク内のすべてのスイッチポートへのアクセスをサーバから集中管理することができます。つまり、承認ユーザは、ネットワーク内の任意の場所から同じ資格情報を使用して認証を受けることが可能であるということです。

本製品では、EAPOL (Extensible Authentication Protocol over LAN) を使用して認証プロトコルメッセージをクライアントと交換し、リモート RADIUS 認証サーバを使用してユーザ ID とアクセス権を検証することもできます。クライアント (サブリカント) がスイッチポートに接続すると、スイッチ (オーセンティケータ) は EAPOL ID 要求を送信します。クライアントが自らの ID (ユーザ名など) を EAPOL 要求に含めてスイッチに提示し、スイッチはその ID を RADIUS サーバに転送します。RADIUS サーバはクライアント ID を検証し、アクセスチャレンジをクライアントに送信します。RADIUS サーバから送信される EAP パケットには、チャレンジだけでなく、使用される認証方式に関する情報も含まれます。クライアントは、クライアントソフトウェアと RADIUS サーバの設定に応じて、その認証方式を拒否して別の方式を要求することができます。認証メッセージを渡すために使用される暗号化方式は、MD5 (Message-Digest 5)、TLS (Transport Layer Security)、PEAP (Protected Extensible Authentication Protocol)、または TTLS (Tunneled Transport Layer Security) にすることができます。クライアントは、資格情報 (パスワードや証明書など) と共に、適切な認証方式に関する情報を RADIUS サーバに送信します。RADIUS サーバは、クライアントの資格情報を検証し、許可パケットまたは拒否パケットを返します。認証が正常に完了すると、スイッチはクライアントにネットワークへのアクセスを許可します。認証が正常に完了しない場合、ポートで受信される非 EAP トラフィックは、ブロックされるか、または、「intrusion-action」設定に基づいてゲスト VLAN に割り当てられます。「multi-host」モードでは、ポートに接続されているホストのうちの 1 つだけが正常に認証されれば、他のすべてのホストにもネットワークアクセス権が付与されます。同様に、接続されているホストの 1 つが再認証に失敗するか、EAPOL ログオフメッセージを送信すると、すべてのホストがポートで非承認になります。

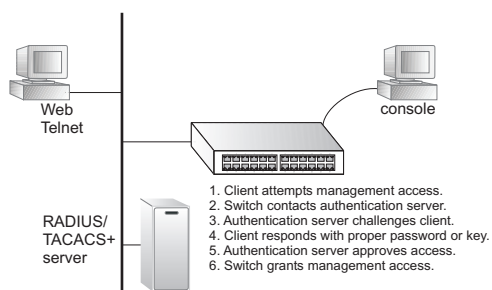


図 1-15: ポートセキュリティの設定

** 図の注釈

1. クライアントがスイッチポートにアクセスしようとする。

2. スイッチがクライアントに ID 要求を送信する。
3. クライアントが ID 情報を返す。
4. スイッチがそれを認証サーバに転送する。
5. 認証サーバがクライアントにチャレンジを送信する。
6. クライアントが適切な資格情報を返す。
7. 認証サーバがアクセスを承認する。
8. スイッチがポートへのアクセス権をクライアントに付与する。

スイッチで 802.1X を運用するには、以下の条件を満たす必要があります。

- ・ スイッチに IP アドレスが割り当てられていること。
- ・ スイッチで RADIUS 認証が有効になっており、RADIUS サーバの IP アドレスが指定されていること。
- ・ スイッチで 802.1X がグローバルで有効になっていること。
- ・ 使用される各ポートが dot1X モード（「Auto」認証モード）に設定されていること。
- ・ 認証される必要があるデバイスで dot1X クライアントソフトウェアがインストールされて適切に設定されていること。
- ・ RADIUS サーバおよび 802.1X クライアントで EAP をサポートしていること（本製品は、EAP パケットをサーバからクライアントに渡すため、EAPOL のみをサポートしています）。
- ・ RADIUS サーバおよびクライアントが同じ EAP 認証タイプ（MD5、PEAP、TLS、TTLS のいずれか）をサポートしていること（これらの暗号化方式は、Windows XP および Windows 2000（Service Pack 4 適用済み）でネイティブサポートされています。それらの暗号化方式を Windows 95 および Windows 98 でサポートするには、AEGIS dot1x クライアントまたは互換性を備えたその他のクライアントソフトウェアを使用することができます）。

802.1X グローバル設定の設定

「Security」→「Port Authentication」(Configure Global) を選択すると、IEEE 802.1X ポート認証を設定することができます。ポートの設定をアクティブにする前に、スイッチシステムで 802.1X プロトコルをグローバルで有効にする必要があります。

関連する CLI 情報

「802.1X Port Authentication」

パラメータ

以下のパラメータが表示されます。

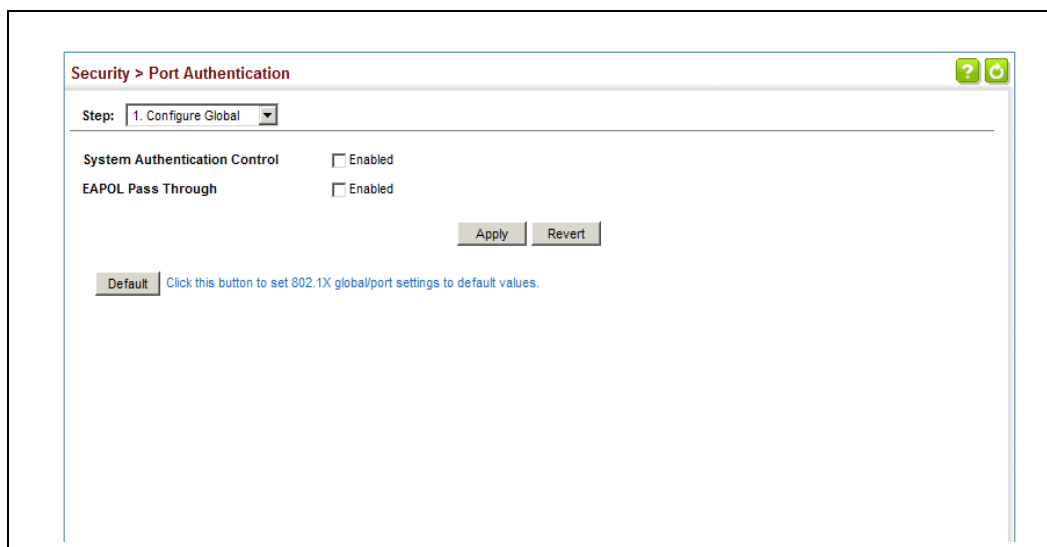
- ・ Port Authentication Status – 802.1X のグローバル設定を指定します (デフォルト: Disabled)。
- ・ EAPOL Pass Through – dot1x がグローバルで無効になっている場合に EAPOL フレームをすべてのポートにパススルーします (デフォルト: Disabled)。本製品がネットワークで中間ノードとして機能しており、dot1x 認証を実行する必要がない場合は、「EAPOL Pass Through」を「Enabled」にして、EAPOL フレームを他のスイッチから認証サーバに転送できるようにし、認証プロセスがネットワークエッジにあるスイッチで引き続き実行されるようにすることができます。本製品がエッジスイッチとして機能しているが、接続するクライアントの認証が必要ない場合は、「EAPOL Pass Through」を「Disabled」にして、不要な EAPOL トラフィックが破棄されるようにすることができます。

Web インターフェース

802.1X のグローバル設定を設定するには、以下のようにします。

- (1) 「Security」→「Port Authentication」を選択します。
- (2) 「Step」リストで「Configure Global」を選択します。
- (3) スwitchの 802.1X をグローバルで有効にし、必要に応じて「EAPOL Pass Through」を設定します。それから、スイッチが認証サーバからの MD5 チャレンジに応答するときに使用するユーザ名とパスワードを設定します。

(4) < Apply > ボタンをクリックします。



画面 1-174 : 802.1X ポート認証のグローバル設定の設定

802.1X のポート設定の設定

「Security」→「Port Authentication」（Configure Interface）を選択すると、スイッチをローカルオーセンティケータとして使用するために 802.1X ポートを設定することができます。802.1X を有効にする場合は、クライアントとスイッチ（オーセンティケータ）との間で実行される認証プロセスのパラメータに加え、スイッチと認証サーバとの間で実行されるクライアント ID ルックアッププロセスのパラメータを設定する必要があります。

関連する CLI 情報

「802.1X Port Authentication」

コマンドの使用

スイッチに接続するサブリカントデバイスと認証サーバとの間のローカルオーセンティケータとしてスイッチが機能するようにする場合は、オーセンティケータとクライアントとの間の EAP メッセージの交換に関するパラメータを設定します。

パラメータ

以下のパラメータが表示されます。

- ・ Port – ポート番号。
- ・ Status – ポートで認証が有効になっているか無効になっているかを示します。制御モードが「Force-Authorized」に設定されている場合、「Status」は「Disabled」になります。
- ・ Authorized – 接続されているクライアントの 802.1X 認証ステータスが表示されます。
 - ・ Yes – 接続されているクライアントは認証されています。
 - ・ No – 接続されているクライアントは認証されていません。
- ・ Supplicant – 接続されているクライアントの MAC アドレスを示します。
- ・ Control Mode – 認証モードを以下のいずれかに設定します。
 - ・ Auto – dot1x 対応クライアントが認証サーバによって認証される必要があります。dot1x 対応ではないクライアントはアクセスが拒否されます。
 - ・ Force-Authorized – dot1x 対応であるか dot1x 非対応であるかに関わらず、ポートに対するアクセス権がすべてのクライアントに付与されます（これがデフォルトの設定です）。
 - ・ Force-Unauthorized – dot1x 対応であるか dot1x 非対応であるかに関わらず、すべてのクライアントがポートへのアクセスを拒否されます。
- ・ Operation Mode – 単一または複数のホスト（クライアント）が 802.1X 認証済みポートに接続できるようにします（デフォルト：Single-Host）。
 - ・ Single-Host – 単一のホストのみがポートに接続できるようにします。
 - ・ Multi-Host – 複数のホストがポートに接続できるようにします。このモードでは、ポートに接続されているホストのうちの 1 つだけが正常に認証されれば、他のすべてのホストにもネットワークアクセス権が付与されます。同様に、接続されているホストの 1 つが再認証に失敗するか、EAPOL ログオフメッセージを送信すると、すべてのホストがポートで非承認になります。
 - ・ MAC-Based – 複数のホストがこのポートに接続できるようにすると共に、それぞれのホストについて認証が必要とされるようにします。このモードでは、ポートに接続されている各ポートが認証に成功する必要があります。このモードで動作するポートへのアクセスを許可されるホストの数は、セキュアアドレステーブル（最大 1,024 アドレス）の使用可能スペースのみによって制限されます。
- ・ Max MAC Count – 「Multi-Host」動作モードが選択されている場合にポートに接続できるホストの最大数（範囲：1 ～ 1,024、デフォルト：5）。
- ・ Max Request – 認証セッションがタイムアウトする前にスイッチポートが EAP Request パケットをクライアントに再送する最大回数を設定します（範囲：1 ～ 10、デフォルト：2）。
- ・ Quiet Period – 「Max Request Count」を超えた後、新しいクライアントを取得しようとする前にスイッチポートが待機する期間を設定します（範囲：1 ～ 65,535 秒、デフォルト：60 秒）。
- ・ Tx Period – 認証セッションでスイッチが EAP パケットを再送する前に待機する期間を設定します（範囲：1 ～ 65,535 秒、デフォルト：30 秒）。

- ・ Tx Period – スイッチポートが EAP パケットを再送する前に EAP 要求に対するクライアントからの応答を待機する期間を設定します（範囲：1 ～ 65,535 秒、デフォルト：30 秒）。
- ・ このコマンド属性は、EAP Request/ID フレーム以外の EAP Request フレームのタイムアウトを設定します。dot1x 認証がポートで有効になっている場合、ポートのリンク状態が Up になると、スイッチが認証を開始します。認証情報に関する 1 つまたは複数の要求が後に続く EAP Request/ID フレームをクライアントに送信して、クライアントの ID を要求します。また、アクティブ接続の間、再認証が必要になった場合には、その他の EAP Request フレームがスイッチから送信されることもあります。
- ・ Server Timeout – スイッチポートが EAP パケットを再送する前に EAP 要求に対する認証サーバからの応答を待機する期間を設定します（固定設定：10 秒）。
- ・ Re-authentication Status – 「Re-authentication Period」で指定されている期間を過ぎるとクライアントが再認証されるように設定します。再認証は、新しいデバイスがスイッチポートにプラグインされたかどうかを確認するために使用することができます（デフォルト：Disabled）。
- ・ Re-authentication Period – 接続されているクライアントの再認証が必要になるまでの期間を設定します（範囲：1 ～ 65,535 秒、デフォルト：3,600 秒）。
- ・ Re-authentication Max Retries – 認証セッションがタイムアウトする前にスイッチポートが EAP Request/ID パケットをクライアントに再送する最大回数を設定します（範囲：1 ～ 10、デフォルト：2）。
- ・ Intrusion Action – 認証が失敗した場合のポートの対応を設定します。
 - ・ Block Traffic – ポートのすべての非 EAP トラフィックをブロックします（これがデフォルトの設定です）。
 - ・ Guest VLAN – ポートのすべてのトラフィックをゲスト VLAN に割り当てます。ゲスト VLAN は、別途、設定して（「VLAN グループの設定」を参照）、各ポートでマップする（「ポートのネットワークアクセスの設定」を参照）必要があります。

Authenticator PAE State Machine

- ・ State – 現在の状態（Initialize、Disconnected、Connecting、Authenticating、Authenticated、Aborting、Held、Force_Authorized、Force_Unauthorized など）。
- ・ Reauth Count – Connecting 状態に戻った回数。
- ・ Current Identifier – 認証サーバによって各 EAP Success、EAP Failure、または EAP Request パケットで送信された ID。

Backend State Machine

- ・ State – 現在の状態（Request、Response、Success、Fail、Timeout、Idle、Initialize など）。
- ・ Request Count – 応答が受信されずにサブリカントに送信された EAP Request パケットの数。
- ・ Identifier (Server) – 認証サーバから受信された最新の EAP Success、EAP Failure、または EAP Request パケットで伝播された ID。

Reauthentication State Machine

- ・ State – 現在の状態（Initialize、Re-authenticate など）。

Web インターフェース

802.1X オーセンティケータポート設定を設定するには、以下のようにします。

- (1) 「Security」 → 「Port Authentication」 を選択します。
- (2) 「Step」 リストで 「Configure Interface」 を選択します。
- (3) 「Port」 でオーセンティケータポートを選択します。
- (4) 各ポートの認証設定を必要に応じて変更します。
- (5) < Apply > ボタンをクリックします。

Security > Port Authentication

Step: 2. Configure Interface

Port	1
Status	Disabled
Authorized	Yes
Control Mode	Auto
Operation Mode	Single-Host
Max MAC Count (1-1024)	5
Max Request (1-10)	2
Quiet Period (1-65535)	60 sec
Tx Period (1-65535)	30 sec
Supplicant Timeout (1-65535)	30 sec
Server Timeout	10 sec
Re-authentication Status	☐ Enabled
Re-authentication Period (1-65535)	3600 sec
Re-authentication Max Retries (1-10)	2
Intrusion Action	Block Traffic

画面 1-175 : 802.1X オーセンティケータポートのインターフェース設定の設定

802.1Xに関する統計情報の表示

「Security」→「Port Authentication」（Show Statistics）を選択すると、任意のポートについて dot1x プロトコル交換に関する統計情報を表示することができます。

関連する CLI 情報

「show dot1x」

パラメータ

以下のパラメータが表示されます。

パラメータ	説明
Rx EAPOL Start	このオーセンティケータで受信された EAPOL Start フレームの数。
Rx EAPOL Logoff	このオーセンティケータで受信された EAPOL Logoff フレームの数。
Rx EAPOL Invalid	このオーセンティケータで受信された EAPOL フレームのうち、フレームタイプが認識されなかったものの数。
Rx EAPOL Total	このオーセンティケータで受信された、あらゆるタイプの有効な EAPOL フレームの数。
Rx Last EAPOLVer	このオーセンティケータで受信された最新の EAPOL フレームに含まれているプロトコルバージョン番号。
Rx Last EAPOLSrc	このオーセンティケータで受信された最新の EAPOL フレームに含まれている送信元 MAC アドレス。
Rx EAP Resp/Id	このオーセンティケータで受信された EAP Response/ID フレームの数。
Rx EAP Resp/Oth	このオーセンティケータで受信された（EAP Response/ID フレーム以外の）有効な EAPOL Response フレームの数。
Rx EAP LenError	このオーセンティケータで受信された EAPOL フレームのうち、Packet Body Length フィールドが無効なものの数。
Tx EAP Req/Id	このオーセンティケータで送信された EAP Request/ID フレームの数。
Tx EAP Req/Oth	このオーセンティケータで送信された（EAP Request/ID フレーム以外の）EAP Request/ID フレームの数。
Tx EAPOL Total	このオーセンティケータで送信された、あらゆるタイプの EAPOL フレームの数。

表 1-8: 802.1X に関する統計情報

Web インターフェース

802.1X オーセンティケーターポートに関する統計情報を表示するには、以下のようになります。

- (1) 「Security」 → 「Port Authentication」 を選択します。
- (2) 「Step」 リストで 「Show Statistics」 を選択します。
- (3) 「Port」 でオーセンティケーターポートを選択します。

Security > Port Authentication

Step: 3. Show Statistics ▼

Port 1 ▼

Port Authentication Authenticator Statistics

Rx EAPOL Start	11154	Rx EAP Resp/Id	2533664
Rx EAPOL Logoff	2115542	Rx EAP Resp/Oth	11123
Rx EAPOL Invalid	533	Rx EAP LenError	1
Rx EAPOL Total	1000	Tx EAP Req/Id	5222
Rx Last EAPOLVer	255	Tx EAP Req/Oth	1222
Rx Last EAPOLSrc	00-02-44-51-C2-90	Tx EAPOL Total	1

Refresh

画面 1-176 : 802.1X オーセンティケーターポートに関する統計情報の表示

1.11.12 IP ソースガード

IP ソースガードは、手動で設定された IP ソースガードテーブルのエントリまたは（DHCP スヌーピングが有効になっている場合は）DHCP スヌーピングテーブルのダイナミックエントリ（「DHCP スヌーピング」を参照）に基づいてネットワークインターフェースで 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、ホストが近隣ホストの IP アドレスを利用してネットワークにアクセスしようとした場合に発生するトラフィック攻撃を防ぐために使用することができます。ここでは、IP ソースガードの使用方法について説明します。

IP ソースガードのためのポートの設定

「Security」→「IP Source Guard」→「Port Configuration」を選択すると、送信元 IP アドレスまたは送信元 IP アドレスと MAC アドレスの組み合わせに基づいてフィルタリングタイプを設定することができます。

ネットワークやファイアウォールの外部からメッセージを受信し、そのために近隣ホストの IP アドレスを利用しようとするホストによって引き起こされるトラフィック攻撃にさらされる可能性がある非セキュアポートでトラフィックをフィルタリングする場合は、IP ソースガードを使用することができます。

関連する CLI 情報

「ip source-guard」

コマンドの使用

- ・ IP ソースガードモードを「SIP」（送信元 IP）または「SIP-MAC」（送信元 IP と送信元 MAC）に設定すると、選択したポートで IP ソースガード機能が有効になります。「SIP」オプションは、VLAN ID、送信元 IP アドレス、およびポート番号をバインディングテーブル内のすべてのエントリと照らし合わせてチェックする場合に使用します。「SIP-MAC」オプションは、それらのパラメータに加え、送信元 MAC アドレスをチェックする場合に使用します。マッチするエントリがない場合、パケットはドロップされます。

【注意】 IP ソースガードではマルチキャストアドレスを使用できません。

- ・ IP ソースガードを有効にすると、DHCP スヌーピングによって学習されたダイナミックエントリ（「DHCP スヌーピング」を参照）、または IP ソースガードバインディングテーブルで設定されているスタティックアドレスに基づいて、トラフィックがフィルタリングされます。
- ・ IP ソースガードが有効になっている場合、インバウンドパケットの IP アドレス（「SIP」オプションが選択されている場合）または着信パケットの IP アドレスとそれに対応する MAC アドレスの両方（「SIPMAC」オプションが選択されている場合）がバインディングテーブルと照らし合わせてチェックされます。マッチするエントリがない場合、パケットはドロップされます。
- ・ フィルタリングルールは、以下のように実装されます。
 - ・ DHCP スヌーピングが無効になっている場合を参照）、IP ソースガードでは、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」オプションが選択されている場合）がチェックされます。マッチするエントリがバインディングテーブルで検出され、エントリタイプがスタティック IP ソースガードバインディングである場合は、パケットが転送されます。
 - ・ DHCP スヌーピングが有効になっている場合、IP ソースガードでは、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

ションが選択されている場合) がチェックされます。マッチするエントリがバインディングテーブルで検出され、エントリタイプがスタティック IP ソースガードバインディングまたはダイナミック DHCP スヌーピングバインディングである場合は、パケットが転送されます。

- ・ まだ IP ソースバインディングが設定されていない (IP ソースガードバインディングテーブルのスタティックエントリと DHCP スヌーピングによって学習されるダイナミックエントリのどちらも設定されていない) インターフェースで IP ソースガードが有効になっている場合、そのポートでは DHCP パケット以外のすべての IP トラフィックがドロップされます。

パラメータ

以下のパラメータが表示されます。

- ・ Filter Type – 送信元 IP アドレスまたは送信元 IP アドレスとそれに対応する MAC アドレスの組み合わせに基づいてインバウンドトラフィックがフィルタリングされるようにスイッチを設定します (デフォルト: None)。
 - ・ None – ポートの 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保存されている IP アドレスに基づく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保存されている IP アドレスとそれらに対応する MAC アドレスに基づくトラフィックフィルタリングを有効にします。
- ・ Max Binding Entry – インターフェースにバインドできるエントリの最大数 (範囲: 1 ~ 5、デフォルト: 5)。このパラメータは、バインディングテーブルでインター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。この場合の最大数は、DHCP スヌーピングによって検出されるダイナミックエントリ (「DHCP スヌーピング」を参照) と IP ソースガードで設定されるスタティックエントリ (「IP ソースガードのスタティックバインディングの設定」を参照) の両方を含めたものです。

Web インターフェース

ポートの IP ソースガードのフィルタリングタイプを設定するには、以下のようにします。

- (1) 「Security」 → 「IP Source Guard」 → 「Port Configuration」 を選択します。
- (2) ポートごとに必要なフィルタリングタイプを設定します。
- (3) < Apply > ボタンをクリックします。

Security > IP Source Guard > Port Configuration

Port Configuration List Max: 26 Total: 26 1 2 3

Port	Filter Type	Max Binding Entry (1-5)
1	None	5
2	None	5
3	None	5
4	None	5
5	SIP	3
6	None	5
7	None	5
8	None	5
9	None	5
10	None	5

画面 1-177 : IP ソースガードのフィルタリングタイプの設定

IP ソースガードのスタティックバインディングの設定

「Security」→「IP Source Guard」→「Static Configuration」を選択すると、スタティックアドレスをポートにバインドすることができます。テーブルエントリには、MAC アドレス、IP アドレス、リースタイム、エントリタイプ（Static または Dynamic）、VLAN ID、およびポート ID が含まれます。すべてのスタティックエントリのリースタイムは無期限（テーブルでの値が 0）に設定されます。

関連する CLI 情報

「ip source-guard binding」

コマンドの使用

- ・ IP ソースガードバインディングテーブルに入力されたスタティックエントリのリースタイムは、自動的に無期限に設定されます。DHCP スヌーピングによって学習されるダイナミックエントリは、DHCP サーバ自体によって設定されます。
- ・ スタティックバインディングは、以下のように処理されます。
 - ・ 同じ VLAN ID と MAC アドレスを含むエントリが存在しない場合、「スタティック IP ソースガードバインディング」というタイプ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 VLAN ID と MAC アドレスを含むエントリが存在し、エントリのタイプがスタティック IP ソースガードバインディングである場合、新しいエントリによって古いエントリが置き換えられます。
 - ・ 同じ VLAN ID と MAC アドレスを含むエントリが存在し、エントリのタイプがダイナミック DHCP スヌーピングバインディングである場合、新しいエントリによって古いエントリが置き換えられ、エントリのタイプがスタティック IP ソースガードバインディングに変更されます。
 - ・ スタティックバインディングについて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

以下のパラメータが表示されます。

- ・ Port – スタティックエントリのバインド先のポート。
- ・ VLAN – 設定済み VLAN の ID（範囲：1 ～ 4,093）。
- ・ MAC Address – 有効なユニキャスト MAC アドレス。
- ・ IP Address – 有効なユニキャスト IP アドレス（クラス A、B、または C など）。

Web インターフェース

IP ソースガードのスタティックバインディングを設定するには、以下のようになります。

- (1) 「Security」→「IP Source Guard」→「Static Configuration」を選択します。
- (2) 「Step」リストで「Add」を選択します。
- (3) ポートごとに必要なバインディング情報を入力します。

(4) < Apply > ボタンをクリックします。

Security > IP Source Guard > Static Binding

Action: Add ▼

Port: 1 ▼

VLAN: 1 ▼

MAC Address: 00-10-B5-F4-00-01

IP Address: 10.2.44.96

Apply Revert

画面 1-178 : IP ソースガードのスタティックバインディングの設定

IP ソースガードのスタティックバインディングを表示するには、以下のようにします。

- (1) 「Security」 → 「IP Source Guard」 → 「Static Configuration」 を選択します。
- (2) 「Step」 リストで 「Show」 を選択します。

Security > IP Source Guard > Static Binding

Action: Show ▼

Static Binding List Max: 140 Total: 1

	VLAN	MAC Address	Interface	IP Address	Lease Time (sec)
☐	1	00-10-B5-F4-00-01	Unit 1 / Port 1	192.168.0.23	0

Delete Revert

画面 1-179 : IP ソースガードのスタティックバインディングの表示

ダイナミック IP ソースガードバインディングに関する情報の表示

「Security」→「IP Source Guard」→「Dynamic Binding」を選択すると、インターフェースを選択してソースガードバインディングテーブルを表示することができます。

関連する CLI 情報

「show ip dhcp snooping binding」

パラメータ

以下のパラメータが表示されます。

Query by

- ・ Port – スイッチのポート。
- ・ VLAN – 設定済み VLAN の ID（範囲：1 ～ 4,093）。
- ・ MAC Address – 有効なユニキャスト MAC アドレス。
- ・ IP Address – 有効なユニキャスト IP アドレス（クラス A、B、または C など）。

Dynamic Binding List

- ・ VLAN – エントリのバインド先の VLAN。
- ・ MAC Address – エントリに関連付けられている物理アドレス。
- ・ Interface – エントリのバインド先のポート。
- ・ IP Address – クライアントに対応する IP アドレス。
- ・ Lease Time – IP アドレスがクライアントにリースされる期間。

Web インターフェース

IP ソースガードバインディングテーブルを表示するには、以下のようになります。

- (1) 「Security」→「IP Source Guard」→「Dynamic Binding」を選択します。
- (2) 検索条件のチェックボックスをオンにして、必要な値を入力します。

(3) < Query > ボタンをクリックします。

Security > IP Source Guard > Dynamic Binding

Query by:

☐ Port

☐ VLAN

☐ MAC Address

☐ IP Address

Dynamic Binding List Max: 140 Total: 3

VLAN	MAC Address	Interface	IP Address	Lease Time (sec)
1	00-10-B5-F4-00-01	Unit 1 / Port 2	10.2.44.96	5
1	00-10-B5-F4-00-02	Unit 1 / Port 4	10.2.44.97	25
2	00-10-B5-F4-00-03	Unit 1 / Port 7	10.2.44.98	47

画面 1-180 : IP ソースガードバインディングテーブルの表示

1.11.13 DHCP スヌーピング

非セキュアなポートで DHCP クライアントに割り当てられているアドレスは、DHCP スヌーピングによって登録されるダイナミックバインディングを使用して（または、IP ソースガードで設定されるスタティックバインディングを使用して）、詳細に制御することができます。スイッチで DHCP スヌーピングを使用すると、認証されていない DHCP サーバ、またはポート関連の情報を DHCP サーバに送信するその他のデバイスからネットワークを保護することができます。ポート関連の情報は、IP アドレスを物理ポートまでさかのぼって追跡する場合に利用することができます。

コマンドの使用

DHCP スヌーピングプロセス

- ・ 不正な DHCP メッセージが外部送信元から受信されると、ネットワークトラフィックが妨げられる可能性があります。DHCP スヌーピングを使用して、非セキュアなインターフェースでネットワークやファイアウォールの外部から受信される DHCP メッセージをフィルタリングすることができます。DHCP スヌーピングをスイッチでグローバルで有効にし、VLAN インターフェースで有効にすると、信頼できないインターフェースでは、DHCP スヌーピングテーブルに含まれていないデバイスから受信された DHCP メッセージがドロップされるようになります。
- ・ テーブルには、信頼できるインターフェースのみについて学習されたエントリが保存されます。エントリは、クライアントが IP アドレスを DHCP サーバから受け取ったり、DHCP サーバにリリースしたりすると、動的に DHCP スヌーピングテーブル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、リースタイム、VLAN ID、およびポート ID が含まれます。スイッチで処理できる DHCP メッセージのレートリミットは、100 パケット / 秒です。この制限を超えると、すべての DHCP パケットがドロップされます。
- ・ DHCP スヌーピングが有効になっている場合、信頼できないインターフェースに入ってくる DHCP メッセージは、DHCP スヌーピングによって学習されたダイナミックエントリに基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、以下のように実装されます。
 - ・ グローバル DHCP スヌーピングが無効になっている場合、すべての DHCP パケットが転送されます。
 - ・ DHCP スヌーピングがグローバルで有効になっており、DHCP パケットが受信される VLAN でも有効になっている場合、信頼できるポートについては、すべての DHCP パケットが転送されます。また、受信されたパケットが DHCP ACK メッセージである場合は、ダイナミック DHCP スヌーピングエントリが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で有効になっており、DHCP パケットが受信される VLAN でも有効になっているが、ポートが信頼できるポートではない場合、DHCP パケットは以下のように処理されます。DHCP パケットが DHCP サーバからの返信パケット（OFFER、ACK、または NAK メッセージなど）である場合、そのパケットはドロップされます。DHCP パケットがクライアントからのもの（DECLINE メッセージや RELEASE メッセージなど）である場合、対応するエントリがバインディングテーブルで検出されたときにのみ、そのパケットは転送されます。

- ・ DHCP パケットがクライアントからのもの（DISCOVER、REQUEST、INFORM、DECLINE、RELEASE メッセージなど）である場合、MAC アドレス検証が無効になっていると、そのパケットは転送されます。ただし、MAC アドレス検証が有効になっていると、DHCP パケットに保存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内の送信元 MAC アドレスと同じであれば、そのパケットは転送されます。
- ・ DHCP パケットが認識されないタイプである場合、そのパケットはドロップされます。
- ・ 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条件を満たす場合、そのパケットは同じ VLAN 内の信頼できるポートのみに転送されます。
- ・ DHCP パケットがサーバからのものであり、信頼できるポートで受信された場合、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どちらにも転送されます。
- ・ DHCP スヌーピングがグローバルで無効になると、すべてのダイナミック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その他の考慮事項として、スイッチがクライアント要求を DHCP サーバに送信するときに使用するポートは信頼できるポートとして設定されていなければならないということが挙げられます。スイッチで ACK メッセージが DHCP サーバから受信された場合、そのスイッチ自体のダイナミックエントリはバインディングテーブルに追加されないので注意してください。また、スイッチが自らの DHCP クライアントパケットを送信する場合にはフィルタリングは実行されません。ただし、スイッチが何らかのメッセージを DHCP サーバから受信する場合には、信頼できないポートから受信されたパケットは、すべて、ドロップされます。

DHCP Snooping Option 82

- ・ DHCP Option 82 は、DHCP クライアントに関する情報を送信するための中継メカニズム、または中継エージェント自体を、DHCP サーバに提供します。この機能をサポートしている DHCP サーバは、IP アドレスを割り当てる場合、またはクライアントに関する他のサービスやポリシーを設定するため、DHCP クライアントに関する情報を使用することができます。また、DHCP Option 82 は、IP スヌーピング、クライアント ID スヌーピング、MAC アドレススヌーピング、アドレス消費などの DHCP サービスで、攻撃されたクライアントからの悪意あるネットワーク攻撃を防ぐ場合にも有効です。
- ・ 要求パケットに挿入される Option 82 情報について DHCP スヌーピングを有効にする必要があります。
- ・ Option 82 情報の DHCP スヌーピングが有効になっている場合、スイッチによって転送される DHCP 要求パケットおよび DHCP サーバから返される返信パケットによって、要求元のクライアント（または、自らの情報を記述するために Option 82 情報フィールドを使用した中継エージェント）を特定することができます。Option 82 情報によって、要求元デバイス（つまり、この場合はスイッチ）の MAC アドレスまたは IP アドレスを特定することもできます。また、本製品では、デフォルトで、DHCP クライアント要求を受け取るときに使用されるローカルインターフェースを示す情報（ポートや VLAN ID など）が Option 82 Circuit ID フィールドに入れられます。そのようにすると、DHCP クライアントサーバ交換メッセージを、VLAN 全体にフラッドさせることなく、サーバとクライアント間で転送することができます。
- ・ スイッチで Option 82 情報の DHCP スヌーピングが有効になっている場合は、（DHCP スヌーピングフィルタリングルールに従って）VLAN 経由で受信される DHCP 要求パケットに情報を挿入することもできます。中継されるパケットに挿入される情報には、回線 ID およびリモート ID だけでなく、ゲートウェイインターネットアドレスも含まれます。

Web 設定

セキュリティ対策

- ・ 既に DHCP Option 82 情報を含んでいる DHCP パケットをスイッチで受信する場合は、それらのパケットに関するアクションポリシーを設定することができます。スイッチで、DHCP パケットをドロップするか、既存の情報を維持するか、既存の情報をスイッチの中継情報に置き換えることができます。

DHCP スヌーピング設定

「IP Service」→「DHCP」→「Snooping」（Configure Global）を選択すると、スイッチで DHCP スヌーピングをグローバルで有効にすることや、MAC アドレス検証を設定することができます。

関連する CLI 情報

「DHCP Snooping」

パラメータ

以下のパラメータが表示されます。

- ・ DHCP Snooping Status - DHCP スヌーピングをグローバルで有効にします（デフォルト : Disabled）。
- ・ DHCP Snooping MAC-Address Verification - MAC アドレス検証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異なる場合、パケットはドロップされます（デフォルト : Enabled）。
- ・ DHCP Snooping Information Option Status - DHCP Option 82 情報の中継を有効または無効にします（デフォルト : Disabled）。
- ・ DHCP Snooping Information Option Policy - 既に Option 82 情報を含んでいる DHCP クライアント要求パケットの処理方法を指定します。
 - ・ Drop - クライアントの要求パケットを中継せずにドロップします。
 - ・ Keep - クライアント要求に含まれている Option 82 情報を保持し、信頼できるポートにパケットを転送します。
 - ・ Replace - クライアントの要求に含まれている Option 82 情報の circuit-id フィールドおよび remote-id フィールドを、中継エージェント自体に関する情報に置き換え、中継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になっている場合）、信頼できるポートにパケットを転送します（これがデフォルトです）。

Web インターフェース

DHCP スヌーピングのグローバル設定を設定するには、以下のようになります。

- (1) 「Security」→「IP Source Guard」→「DHCP Snooping」を選択します。
- (2) 「Step」リストで「Configure Global」を選択します。
- (3) 全般的な DHCP スヌーピングプロセスと DHCP Option 82 情報ポリシーに関して必要なオプションを選択します。

(4) < Apply > ボタンをクリックします。

The screenshot shows a web configuration page for DHCP Snooping. The breadcrumb navigation at the top reads "IP Service > DHCP > Snooping". Below this, a "Step:" dropdown menu is set to "1. Configure Global". The page is divided into two sections: "General" and "Information". In the "General" section, "DHCP Snooping Status" and "DHCP Snooping MAC-Address Verification" are both checked and set to "Enabled". In the "Information" section, "DHCP Snooping Information Option Status" is checked and set to "Enabled", and "DHCP Snooping Information Option Policy" is set to "Replace" via a dropdown menu. At the bottom right of the configuration area, there are two buttons: "Apply" and "Revert".

IP Service > DHCP > Snooping

Step: 1. Configure Global ▼

General

DHCP Snooping Status ☒ Enabled

DHCP Snooping MAC-Address Verification ☒ Enabled

Information

DHCP Snooping Information Option Status ☒ Enabled

DHCP Snooping Information Option Policy Replace ▼

Apply Revert

画面 1-181 : DHCP スヌーピングのグローバル設定の設定

DHCP スヌーピングの VLAN 設定

「IP Service」→「DHCP」→「Snooping」（Configure VLAN）を選択すると、特定の VLAN で DHCP スヌーピングを有効または無効にすることができます。

関連する CLI 情報

「ip dhcp snooping vlan」

コマンドの使用

- ・ スイッチで DHCP スヌーピングがグローバルで有効になっており、指定された VLAN で有効になっている場合、VLAN 内のあらゆる信頼できないポートでは、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で無効になっている場合でも、個々の VLAN について DHCP スヌーピングを設定することはできますが、DHCP スヌーピングが再びグローバルで有効にならない限り、そのような変更は適用されません。
- ・ DHCP スヌーピングがグローバルで有効になっている場合に、ある VLAN で DHCP スヌーピングが無効にされると、その VLAN について学習されたすべてのダイナミック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

以下のパラメータが表示されます。

- ・ VLAN – 設定済み VLAN の ID（範囲：1 ～ 4,093）。
- ・ 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。スイッチで DHCP スヌーピングがグローバルで有効になっており、指定された VLAN で有効になっている場合、VLAN 内のあらゆる信頼できないポートでは、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 インターフェース

DHCP スヌーピングの VLAN 設定を設定するには、以下のようになります。

- (1) 「IP Service」→「DHCP」→「Snooping」を選択します。
- (2) 「Step」リストで「Configure VLAN」を選択します。
- (3) いずれかの既存の VLAN で DHCP スヌーピングを有効にします。
- (4) < Apply > ボタンをクリックします。

IP Service > DHCP > Snooping

Step: 2. Configure VLAN

VLAN 1

DHCP Snooping Status ☒ Enabled

Apply Revert

画面 1-182 : VLAN の DHCP スヌーピングの設定

DHCP スヌーピングのためのポートの設定

「IP Service」→「DHCP」→「Snooping」(Configure Interface) を選択すると、スイッチポートを信頼できるポートまたは信頼できないポートとして設定することができます。

関連する CLI 情報

「ip dhcp snooping trust」

コマンドの使用

- ・ 信頼できるインターフェースとは、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ているインターフェースです。信頼できないインターフェースとは、ネットワークやファイアウォールの外部からのメッセージを受信するように設定されているインターフェースです。
- ・ DHCP スヌーピングがグローバルで有効になっており、VLAN でも有効になっている場合、VLAN 内のあらゆる信頼できないポートでは、DHCP パケットフィルタリングが実行されます。
- ・ 信頼できないポートが信頼できるポートに変更されると、そのポートに関連付けられているすべてのダイナミック DHCP スヌーピングバインディングが削除されます。
- ・ ローカルネットワークやファイアウォールの内部の DHCP サーバに接続されているすべてのポートは、Trusted 状態に設定してください。また、ローカルネットワークやファイアウォールの外部にある他のすべてのポートは、Untrusted 状態に設定してください。

パラメータ

以下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有効または無効にします (デフォルト: Disabled)。

Web インターフェース

DHCP スヌーピングのポートモードを設定するには、以下のようにします。

- (1) 「IP Service」→「DHCP」→「Snooping」を選択します。
- (2) 「Step」リストで「Configure Interface」を選択します。
- (3) ローカルネットワーク内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ポートに設定します。

(4) < Apply > ボタンをクリックします。

IP Service > DHCP > Snooping

Step: 3. Configure Interface

Interface ☒ Port ☐ Trunk

DHCP Snooping Port List Max: 26 Total: 26

Port	Trust Status
1	☐ Enabled
2	☐ Enabled
3	☐ Enabled
4	☐ Enabled
5	☒ Enabled

画面 1-183 : DHCP スヌーピングのポートモードの設定

DHCP スヌーピングのバインディング情報の表示

「IP Service」→「DHCP」→「Snooping」(Show Information) を選択すると、バインディングテーブルのエントリを表示することができます。

関連する CLI 情報

「show ip dhcp snooping binding」

パラメータ

以下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ている物理アドレス。
- ・ IP Address – クライアントに対応する IP アドレス。
- ・ Lease Time (seconds) – IP アドレスがクライアントにリースされる期間。
- ・ Type – 以下のエントリタイプ。
 - ・ DHCP-Snooping – ダイナミックスヌーピング。
 - ・ Static-DHCPSPNP – スタティックスヌーピング。
- ・ VLAN – エントリのバインド先の VLAN。
- ・ Interface – エントリのバインド先のポートまたはトランク。
- ・ 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、現時点で学習済みのダイナミック DHCP スヌーピングエントリをフラッシュメモリに保存することができます。それらのエントリは、スイッチのリセット時に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ダイナミックエントリについて表示されるリースタイムは有効なものではなく、注意してください。
- ・ 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 インターフェース

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、以下のようにします。

- (1) 「IP Service」 → 「DHCP」 → 「Snooping」 を選択します。
- (2) 「Step」 リストで 「Show Information」 を選択します。
- (3) 必要な場合は、「Store」 機能または 「Clear」 機能を使用します。

IP Service > DHCP > Snooping

Step: 4. Show Information

DHCP Snooping Binding List Max: 115 Total: 6

MAC Address	IP Address	Lease Time (seconds)	Type	VLAN	Interface
00-10-B5-F4-00-01	10.2.44.96	5	DHCP-Snooping	1	Trunk 1
00-10-B5-F4-00-02	10.3.44.96	15	Static-DHCPSPNP	1	Unit 1 / Port 2
00-10-B5-F4-00-03	10.4.44.96	25	DHCP-Snooping	1	Unit 1 / Port 3
00-10-B5-F4-00-04	10.5.44.96	10	Static-DHCPSPNP	1	Trunk 4
00-10-B5-F4-00-05	10.6.44.96	10	DHCP-Snooping	1	Unit 1 / Port 5
00-10-B5-F4-00-06	10.7.44.96	5	Static-DHCPSPNP	1	Unit 1 / Port 6

Store

Click the button to Store DHCP Snooping binding entries to flash.

Clear

Click the button to Clear DHCP Snooping binding entries from flash.

画面 1-184 : DHCP スヌーピングのバインディングテーブルの表示

1.12 基本的な管理プロトコル

本章では、以下の基本的な管理作業について説明します。

- ・ イベントログの設定 – イベントメッセージのログがシステムメモリまたはフラッシュメモリに記録される条件を設定し、トラップメッセージがリモートログサーバに送信される条件を設定し、SMTP (Simple Mail Transfer Protocol) を使用してリモートホストに応答として送信されるトラップを設定します。
- ・ LLDP (Link Layer Discovery Protocol) – ローカルスイッチに関する基本情報のアドバタイズメント、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。
- ・ SNMP (Simple Network Management Protocol) – SNMPv1、SNMPv2c、SNMPv3 によるスイッチの管理を設定します。
- ・ リモートモニタリング (RMON) – SNMP を使用して取得される詳細な統計情報またはイベント情報のローカルでの収集を設定します。

1.12.1 イベントログの設定

本製品では、エラーメッセージのログ記録を制御することができます。例えば、スイッチのメモリに記録されるイベントのタイプの指定、リモートシステムログ (syslog) サーバへのログの記録、最新のイベントメッセージの一覧表示といったことが可能です。

システムログの設定

「Administration」→「Log」→「System」(Configure Global) を選択すると、イベントのログ記録を有効または無効にすることや、RAM またはフラッシュメモリに記録されるログのレベルを指定することができます。

フラッシュメモリにログとして記録される重大なエラーメッセージは、永続的にスイッチに保存され、ネットワークに関する問題のトラブルシューティングに役立ちます。フラッシュメモリには最大 4,096 のログエントリを保存することができ、使用可能なログメモリ (256K bytes) の空き領域がなくなると、最も古いエントリから順に上書きされます。

「Administration」→「Log」→「System」で表示される画面では、フラッシュメモリまたは RAM にログとして記録されるシステムメッセージを指定および限定することができます。デフォルトでは、レベル 0～3 のイベントのログはフラッシュメモリに記録され、レベル 0～7 のイベントのログは RAM に記録されます。

関連する CLI 情報

「Event Logging」

パラメータ

以下のパラメータが表示されます。

- ・ System Log Status – ログ記録プロセスのため、デバッグまたはエラーメッセージのログを有効または無効にします (デフォルト: Enabled)。
- ・ Flash Level – 指定したレベルまでのすべてのレベルのログメッセージのみがスイッチのフラッシュメモリに永続的に保存されます。例えば、レベル 3 が指定されている場合、レベル 0～3 のすべてのメッセージのログがフラッシュメモリに記録されます (範囲: 0～7、デフォルト: 3)。

表 1-1

レベル	重大度	説明
7	Debug	デバッグメッセージ
6	Informational	情報提供のみを目的とするメッセージ
5	Notice	正常だが連絡が必要な状態（コールドスタートなど）
4	Warning	警告状態（例：False が返される、予期しない値が返される）
3	Error	エラー状態（例：無効な入力）（これがデフォルトとして使用されます）
2	Critical	クリティカルな状態（例：メモリ割り当て、空きメモリエラー（リソース不足））
1	Alert	アラート迅速な対応が必要
0	Emergency	アラート迅速な対応が必要

* 現行のファームウェアリリースで用意されているのは、レベル 2、5、および 6 のエラーメッセージのみです。

表 1-9: ログレベル

RAM Level - 指定したレベルまでのすべてのレベルのログメッセージのみがスイッチの RAM に一時的に保存されます。例えば、レベル 7 が指定されている場合、レベル 0 ～ 7 のすべてのメッセージのログが RAM に記録されます（範囲：0 ～ 7、デフォルト：7）。

【注意】「Flash Level」の値は「RAM Level」の値と同等またはそれ以下でなければなりません。

Web インターフェース

システムメモリへのエラーメッセージのログ設定を設定するには、以下のようにします。

- (1) 「Administration」 → 「Log」 → 「System」を選択します。
- (2) 「Step」リストで「Configure Global」を選択します。
- (3) システムログを有効または無効にし、フラッシュメモリと RAM に記録されるイベントメッセージのログのレベルを設定します。

Web 設定

基本的な管理プロトコル

(4) < Apply > ボタンをクリックします。

Administration > Log > System

Step: 1. Configure Global

System Log Status ☒ Enabled

Flash Level 3 - Error

RAM Level 7 - Debugging

Note: The Flash Level must be equal to or less than the RAM Level.

Apply Revert

画面 1-185 : システムメモリログ設定の設定

システムメモリに記録されているエラーメッセージのログを表示するには、以下のようになります。

- (1) 「Administration」 → 「Log」 → 「System」 を選択します。
- (2) 「Step」 リストで 「Show System Logs」 を選択します。
- (3) 「RAM」 または 「Flash」 を選択します。

この画面では、ログに記録されているシステムメッセージとイベントメッセージをスクロールして確認することができます。本製品では、一時保存領域（RAM）（電源のリセット時に消去されるメモリ）には最大 2,048 のログエントリを保存し、フラッシュメモリには最大 4,096 のログエントリを保存することができます。

Administration > Log > System

Step: 2. Show System Logs

Log Type ☒ Ram ☐ Flash

System Ram Logs

```
[10] 01:33:45 2010-06-22
"User(admin/Web) (::FFFF:192.168.0.5), login successful."
level: 6, module: 5, function: 1, and event no: 1
-----
[9] 01:33:26 2010-06-22
"Fan Recover, unit=[1], fanIndex=[3]."
level: 6, module: 5, function: 1, and event no: 1
-----
[8] 01:33:23 2010-06-22
"Unit 1, fan 3 fail."
level: 6, module: 5, function: 1, and event no: 1
```

画面 1-186 : システムメモリに記録されているエラーメッセージのログの表示

システムログの設定

「Administration」→「Log」→「Remote」を選択すると、ログメッセージが syslog サーバまたはその他の管理ステーションに送信されるようにすることができます。また、指定したレベルよりも低いレベルのイベントメッセージのみが送信されるようにすることもできます。

関連する CLI 情報

「Event Logging」

パラメータ

以下のパラメータが表示されます。

- ・ Remote Log Status – リモートログ記録プロセスのため、デバッグまたはエラーメッセージのロ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グのファシリティタイプを設定します。ファシリティタイプは、ログメッセージを該当のサービスに送信するために syslog サーバで使用されます。この属性によって、syslog メッセージで送信されるファシリティタイプのタグ（RFC 3164 を参照）を指定します。ファシリティタイプはスイッチで報告されるメッセージの種類には影響を及ぼしません。ただし、syslog サーバによるメッセージの処理（該当のデータベースでのメッセージの並び替えや保存など）に使用することもできます（範囲：16～23、デフォルト：23）。
- ・ Logging Trap Level – 指定したレベルまでのすべてのレベルのログメッセージのみがリモート syslog サーバに送信されます。例えば、レベル 3 が指定されている場合、レベル 0～3 のすべてのメッセージのログがリモートサーバに送信されます（範囲：0～7、デフォルト：7）。
- ・ Server IP Address – syslog メッセージの送信先となるリモートサーバの IPv4 アドレスまたは IPv6 アドレスを指定します。

Web インターフェース

リモートサーバへのエラーメッセージのログ設定を設定するには、以下のようになります。

- (1) 「Administration」→「Log」→「Remote」を選択します。
- (2) リモートログを有効にし、syslog メッセージに使用されるファシリティタイプを指定して、リモートサーバの IP アドレスを入力します。

Web 設定

基本的な管理プロトコル

(3) < Apply > ボタンをクリックします。

Administration > Log > Remote

Remote Log Status	☒ Enabled
Logging Facility	23 - Local use 7 ▼
Logging Trap Level	0 - System unusable ▼
Server IP Address 1	192.168.0.4
Server IP Address 2	
Server IP Address 3	
Server IP Address 4	
Server IP Address 5	

Apply Revert

画面 1-187 : エラーメッセージのリモートログ設定の設定

SMTP (Simple Mail Transfer Protocol) アラートの送信

「Administration」→「Log」→「SMTP」を選択すると、指定したレベルのイベントのログが記録された場合に SMTP 電子メールメッセージが送信されるようにして、システム管理者に通知することができます。メッセージは、ネットワーク上の指定の SMTP サーバに送信され、POP クライアントまたは IMAP クライアントを使用して取得することができます。

関連する CLI 情報

「SMTP Alerts」

パラメータ

以下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 - アラートメッセージのトリガーに使用するシステムログ重大度のしきい値レベル (表を参照) を設定します。このレベル以上のすべてのイベントが、指定された電子メール受信者に報告されます。例えば、レベル 7 に設定すると、レベル 0 ~ 7 のすべてのイベントが報告されます (デフォルト: レベル 7)。
- ・ Email Source Address - アラートメッセージの「From」フィールドに使用される電子メールアドレスを設定します。スイッチを特定するシンボリック電子メールアドレスを使用することも、スイッチの担当管理者のアドレスを使用することもできます。
- ・ Email Destination Address - アラートメッセージの電子メール受信者を指定します。最大 5 名の受信者を指定することができます。
- ・ Server IP Address - 最大 3 つの受信者 SMTP サーバを指定します。スイッチは、最初のサーバへの接続が失敗すると、次に指定されているサーバに接続しようとします。

Web インターフェース

SMTP アラートメッセージ設定を設定するには、以下のようにします。

- (1) 「Administration」→「Log」→「SMTP」を選択します。
- (2) SMTP を有効にし、送信元の電子メールアドレスを指定して、重大度の最低レベルを選択します。送信元電子メールアドレスと宛先電子メールアドレスを指定し、1 つまたは複数の SMTP サーバを指定します。

Web 設定

基本的な管理プロトコル

(3) < Apply > ボタンをクリックします。

The screenshot shows a web interface for configuring SMTP alert messages. The breadcrumb navigation at the top reads "Administration > Log > SMTP". The configuration area contains the following fields:

SMTP Status	☒ Enabled
Severity	3 - Error
E-mail Source Address	big-wheels@matel.com
E-mail Destination Address 1	chris@matel.com
E-mail Destination Address 2	
E-mail Destination Address 3	
E-mail Destination Address 4	
E-mail Destination Address 5	
Server IP Address 1	192.168.1.4
Server IP Address 2	
Server IP Address 3	

At the bottom right of the form are two buttons: "Apply" and "Revert".

画面 1-188 :SMTP アラートメッセージ設定の設定

1.12.2 LLDP (Link Layer Discovery Protocol)

LLDP は、ローカルブロードキャストドメインにある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、レイヤ 2 プロトコルであり、定期的なブロードキャストを使用して送信元デバイスに関する情報をアドバタイズします。アドバタイズされる情報は、IEEE 802.1ab 規格に基づく TLV (Type Length Value) 形式で表されます。それらの情報には、デバイスの ID、機能、設定情報などの詳細情報を含めることができます。また、LLDP は、検出した隣接ネットワークノードに関して収集された情報をどのようにし保存して保持するかを定義します。

LLDP タイミング属性の設定

「Administration」→「LLDP」(Configure Global) を選択すると、一般的な LLDP 機能の属性を設定することができます。例えば、LLDP をスイッチでグローバルに有効にする、メッセージの有効期間を設定する、一般的なアドバタイズメントまたは LLDP MIB の変更に関するレポートのブロードキャストの頻度を設定するといったことができます。

関連する CLI 情報

「LLDP Commands」

パラメータ

以下のパラメータが表示されます。

- ・ LLDP – LLDP をスイッチでグローバルに有効にします (デフォルト: Enabled)。
- ・ Transmission Interval – LLDP アドバタイズメントの定期送信間隔を設定します (範囲: 5 ~ 32,768 秒、デフォルト: 30 秒)。
- ・ Hold Time Multiplier – 以下の計算式で示すように、LLDP アドバタイズメントで送信される TTL (Time To Live) 値を設定します (範囲: 2 ~ 10、デフォルト: 4)。

TTL は、更新情報が適宜送信されない場合に受信先 LLDP エージェントが送信元 LLDP エージェントに関するすべての情報を保持する期間を指定します。

TTL (単位: 秒) は、以下の式に従って求めます。

最小値 ((Transmission Interval x Hold time Multiplier) または 65,535)

したがって、デフォルトの TTL は $30 \times 4 = 120$ 秒です。

- ・ Delay Interval – ローカル LLDP MIB 変数が変更された場合に発行されるアドバタイズメントの連続送信時の遅延時間を設定します (範囲: 1 ~ 8,192 秒、デフォルト: 2 秒)。この送信遅延は、ローカル LLDP MIB オブジェクトが頻繁に変更された場合に LLDP アドバタイズメントが短時間に連続して送信されないようにするため、また、可能な限り 1 回の送信で 1 つだけではなく複数の変更が報告されるようにするために使用します。この属性は、以下の原則に従うものでなければなりません。($4 \times \text{Delay Interval} \leq \text{Transmission Interval}$)
- ・ Reinitialization Delay – LLDP ポートが無効になった場合またはリンクがダウンした場合に再初期設定が実行されるまでの遅延時間を設定します (範囲: 1 ~ 10 秒、デフォルト: 2 秒)。ポートで LLDP が再初期設定されると、リモートシステム LLDP MIB 内でのそのポートに関連付けられているすべての情報が削除されます。

Web 設定

基本的な管理プロトコル

- ・ Notification Interval – LLDP MIB の変更に関する SNMP 通知の許容送信間隔を設定します（範囲：5 ～ 36,000 秒、デフォルト：5 秒）。このパラメータは、LLDP MIB に保存されているデータをネットワークの監視または管理に使用する SNMP アプリケーションのみに適用されます。SNMP 通知と SNMP 通知との間に LLDP 隣接デバイス情報に関する変更が発生しても、その情報は送信されません。送信される情報に含まれるのは、通知時に検出されている状態変更のみです。したがって、SNMP エージェントは、スロットリングまたは送信損失のために通知されなかった lldpRemTablesChange 通知イベントを検出できるように、定期的に lldpStatsRemTableLastChangeTime の値をチェックしなければなりません。
- ・ MED Fast Start Count – LLDP-MED Fast Start メカニズムのアクティブ化プロセスで送信される LLDP-MED Fast Start LLD PDU の量を設定します（範囲：1 ～ 10 パケット、デフォルト：4 パケット）。MED Fast Start Count パラメータは、LLDP-MED Fast Start メカニズムがポートでアクティブになるようにするためのタイマー設定の一部として機能します。LLDP-MED Fast Start は、LLDP をタイムリーに実行するために極めて重要であり、したがって、緊急呼び出しサービスを速やかに使用可能にするために不可欠です。

Web インターフェース

LLDP タイミング属性を設定するには、以下のようになります。

- (1) 「Administration」 → 「LLDP」を選択します。
- (2) 「Step」リストで「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を変更します。
- (4) < Apply > ボタンをクリックします。

Administration > LLDP

Step: 1. Configure Global

LLDP ☒ Enabled

Transmission Interval (5-32768) sec

Hold Time Multiplier (2-10)

Delay Interval (1-8192) sec

Reinitialization Delay (1-10) sec

Notification Interval (5-3600) sec

Note: The Transmission Interval must be greater than or equal to 4 times the Delay Interval.

Apply Revert

画面 1-189 :LLDP タイミング属性の設定

LLDP インターフェース属性の設定

「Administration」→「LLDP」(Configure Interface - Configure General)を選択すると、個々のインターフェースのメッセージ属性を指定することができます。例えば、メッセージを送信、受信、または送受信するかどうか、SNMP 通知を送信するかどうかといったことや、アドバタイズする情報のタイプを指定することができます。

関連する CLI 情報

「LLDP Commands」

パラメータ

以下のパラメータが表示されます。

- ・ Admin Status – LLDP PDU (Protocol Data Unit) の LLDP メッセージの送信モードと受信モードを有効にします。(オプション: Tx only、Rx only、Tx Rx または 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: Disabled)。このオプションを設定すると、SNMP トラップ通知が既出の「Notification Interval」で設定されている間隔で指定のターゲットステーションに送信されます。トラップ通知には、LLDP-MIB (IEEE 802.1AB)、LLDP-MED MIB (ANSI/TIA-1057)、またはベンダー固有の LLDP-EXT-DOT1 と LLDP-EXT-DOT3 MIB の状態変更に関する情報が含まれます。SNMP トラップの宛先の定義に関する情報については、「トラップマネージャの指定」を参照してください。
- ・ SNMP 通知と SNMP 通知との間に LLDP 隣接デバイス情報に関する変更が発生しても、その情報は送信されません。送信される情報に含まれるのは、トラップ通知時に検出されている状態変更のみです。したがって、SNMP エージェントは、スロットリングまたは送信損失のために通知されなかった lldpRemTablesChange 通知イベントを検出できるように、定期的に lldpStatsRemTableLastChangeTime の値をチェックしなければなりません。
- ・ Basic Optional TLVs – アドバタイズされるメッセージの 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には、スイッチの IPv4 アドレスが含まれます。使用できる管理アドレスがない場合は、CPU の MAC アドレスまたはアドバタイズメントを送信するポートの MAC アドレスを管理アドレスにしてください。また、管理アドレスの TLV フィールドには、アドレスに関連付けられている特定のインターフェースに関する情報、およびアドレスに関連付けられているハードウェアコンポーネントまたはプロトコルエンティティのタイプを示すオブジェクト ID を含めることもできます。インターフェース番号および OID を TLV フィールドに含めて、検索に使用されるエンタープライズ固有の開始点またはその他の開始点 (インターフェースやエンティティ MIB など) を示すことにより、SNMP アプリケーションのネットワーク検出パフォーマンスを向上させることができます。通常、レイヤ 3 デバイスには多種多様なアドレスが関連付けられるため、個々の LLDP PDU に複数のアドレス TLV に含まれていることがあります。その特定のポートを使用してプロトコル VLAN でアクセスできるアドレスを伝えるあらゆる管理アドレス TLV には、その TLV によって伝えられる管理アドレスに関連付けられている VLAN ID (VID) を示す、ポートとプロトコル VLAN の組み合わせの TLV が付加されます。
 - ・ Port Description – このポートの説明は、ifDescr オブジェクト (RFC 2863) から取得され、ベンダー、製品名、およびインターフェースのハードウェアまたはソフトウェアのバージョンに関する情報を提供します。
 - ・ System Capabilities – システム性能は、システムの主要機能、およびそれらの主要機能が有効になっているかどうかที่กำหนดされます。この TLV によってアドバタイズされる情報は、IEEE 802.1AB で規定されています。
 - ・ System Description – このシステムの説明は、sysDescr オブジェクト (RFC 3418) から取得され、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

Web 設定

基本的な管理プロトコル

システム、およびネットワークソフトウェアのそれぞれのフルネームとバージョン ID などの情報を提供します。

- ・ System Name – このシステム名は、sysName オブジェクト (RFC 3418) から取得され、管理のためにシステムに割り当てられている名前を示します。システム名の設定については、「システム情報の表示」を参照してください。
- ・ Basic Optional TLVs – アドバタイズされるメッセージの TLV フィールドに含まれる IEEE 802.1 情報を設定します。
 - ・ Protocol Identity – このインターフェースを使用してアクセスできるプロトコル (「プロトコル VLAN」を参照)。
 - ・ VLAN ID – ポートのデフォルトの VLAN ID (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 (「IEEE 802.1Q VLAN」を参照)。
 - ・ VLAN Name – このインターフェースが割り当てられているすべての VLAN の名前 (「IEEE 802.1Q VLAN」および「プロトコル VLAN」を参照)。
 - ・ Port and Protocol VLAN ID – このインターフェースで設定されているポートベースのプロトコル VLAN (「IEEE 802.1Q VLAN」および「プロトコル VLAN」を参照)。
- ・ 802.3 Organizationally Specific TLVs – アドバタイズされるメッセージの TLV フィールドに含まれる IEEE 802.3 情報を設定します。
 - ・ Legatink Aggrion – リンクアグリゲーション機能、リンクのアグリゲーションステータス、および IEEE 802.3 アグリゲーションポート ID (インターフェースが現在リンクアグリゲーションメンバーである場合)。
 - ・ Max Frame Size – 最大フレームサイズ (スイッチの最大フレームサイズの設定については、「ジャンボフレームのサポートの設定」を参照)。
 - ・ MAC/PHY Configuration/Status – オートネゴシエーションのサポートと機能および動作可能な MAU (Multistation Access Unit) タイプに関する情報を含めた、MAC/PHY 設定とステータス。

Web インターフェース

LLDP インターフェース属性を設定するには、以下のようにします。

- (1) 「Administration」 → 「LLDP」を選択します。
- (2) 「Step」リストで「Configure Interface」を選択します。
- (3) 「Port」リストまたは「Trunk」リストでインターフェースを選択します。
- (4) 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 メッセージでアドバタイズする情報を選択します。

(5) < Apply > ボタンをクリックします。

The screenshot displays the 'Administration > LLDP' configuration page. At the top, a breadcrumb trail shows 'Administration > LLDP' with a help icon and a refresh icon. Below this, a 'Step:' dropdown menu is set to '2. Configure Interface'. The main configuration area includes several sections: 'Interface' with radio buttons for 'Port' (selected) and 'Trunk', and a dropdown for '1'; 'Admin Status' with a 'Tx Rx' dropdown; 'SNMP Notification' with an 'Enabled' checkbox; 'Basic Optional TLVs' with checkboxes for 'Management Address', 'Port Description', 'System Capabilities', 'System Description', and 'System Name'; '802.1 Organizationally Specific TLVs' with checkboxes for 'Protocol Identity', 'VLAN ID', 'VLAN Name', and 'Port and Protocol VLAN ID'; and '802.3 Organizationally Specific TLVs' with checkboxes for 'Link Aggregation', 'Max Frame Size', and 'MAC/PHY Configuration/Status'. At the bottom right, there are 'Apply' and 'Revert' buttons.

画面 1-190 :LLDP インターフェース属性の設定

LLDP ローカルデバイス情報の表示

「Administration」→「LLDP」（Show Local Device Information）を選択すると、スイッチに関する情報を表示することができます。例えば、スイッチの MAC アドレス、シャーシ ID、管理 IP アドレス、ポート情報などを確認することができます。

関連する CLI 情報

「show lldp info local-device」

パラメータ

以下のパラメータが表示されます。

グローバル設定

- Chassis Type - 送信元 LLDP エージェントに関連付けられている IEEE 802 LAN エンティティを含むシャーシを示します。シャーシを示す方法はいくつかあります。また、シャーシ ID サブタイプを使用して、Chassis ID フィールドで参照されるコンポーネントのタイプが表示されます。

ID の基本情報	参照
Chassis component	EntPhysicalAlias (entPhysClass の値が「chassis(3)」である場合 (IETF RFC 2737))
Interface alias	ifAlias (IETF RFC 2863)
Port component	EntPhysicalAlias (entPhysicalClass の値が「port(10)」または「backplane(4)」である場合 (IETF RFC 2737))
MAC address	MAC アドレス (IEEE Std 802-2001)
Network address	networkAddress
Interface name	ifName (IETF RFC 2863)
Locally assigned	ローカルで割り当てられる値ローカルで割り当てられる値

表 1-10: シャーシ ID サブタイプ

- Port Description - ポートの説明を表わす文字列。RFC 2863 が実装されている場合、このフィールドには ifDescr オブジェクトが使用されます。
- Chassis ID - 本システムの特定のシャーシの固有の ID を示すオクテット文字列。
- System Name - 管理のためにシステムに割り当てられている名前を示す文字列（「システム情報の表示」を参照）。
- System Description - ネットワークエンティティの説明。このフィールドは、show system コマンドを使用して表示することもできます。
- System Capabilities Supported - システムの主要機能を規定するシステム性能。

ID の基本情報	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

表 1-11: システム性能

- ・ System Capabilities Enabled – 現在有効になっているシステムの主要機能（上記の表を参照してください）。
- ・ Management Address – 管理アドレスプロトコルパケットには、スイッチの IPv4 アドレスが含まれます。使用できる管理アドレスがない場合は、CPU の MAC アドレスまたはアドバタイズメントを送信するポートの MAC アドレスを管理アドレスにしてください。

インターフェース設定

以下の属性は、ポートタイプとトランクタイプの両方のインターフェースに適用されます。「trunk」と記載されている場合、説明は、トランクの最初のポートに関するものです。

- ・ Port/Trunk Description – ポートまたはトランクの説明を表わす文字列。RFC 2863 が実装されている場合、このフィールドには ifDescr オブジェクトが使用されます。
- ・ Port/Trunk ID – LLD PDU を送信したポートまたはトランクの固有の ID を含む文字列。

Web インターフェース

ローカルデバイスの LLDP 情報を表示するには、以下のようになります。

- (1) 「Administration」 → 「LLDP」を選択します。
- (2) 「Step」 リストで 「Show Local Device Information」を選択します。
- (3) 「General」、「Port」、または 「Trunk」を選択します。

Administration > LLDP

Step: 3. Show Local Device Information

☒ General
☐ Port
☐ Trunk

LLDP Local Device Information

Chassis Type	MAC Address
Chassis ID	00-00-E8-93-82-A0
System Name	
System Description	FXC9324XG
System Capabilities Supported	Bridge, Router
System Capabilities Enabled	Bridge, Router
Management Address	192.168.0.4 (IPv4)

画面 1-191 : ローカルデバイスの LLDP 情報の表示（全般）

Port	Port Description	Port ID
1	Ethernet Port on unit 1, port 1	00-00-E8-93-82-A1
2	Ethernet Port on unit 1, port 2	00-00-E8-93-82-A2
3	Ethernet Port on unit 1, port 3	00-00-E8-93-82-A3
4	Ethernet Port on unit 1, port 4	00-00-E8-93-82-A4
5	Ethernet Port on unit 1, port 5	00-00-E8-93-82-A5

画面 1-192 : ローカルデバイスの LLDP 情報の表示（ポート）

LLDP リモートデバイス情報の表示

「Administration」→「LLDP」（Show Remote Device Information）を選択すると、LLDP を使用して情報をアドバタイズするスイッチポートに直接接続されているデバイスに関する情報を表示することや、ローカルスイッチ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することができます。

関連する CLI 情報

「show lldp info remote-device」

パラメータ

以下のパラメータが表示されます。

Port

- ・ 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。
- ・ Chassis ID – 本システムの特定のシャーシの固有の ID を示すオクテット文字列。
- ・ Port ID – LLD PDU を送信したポートの固有の ID を含む文字列。
- ・ System Name – 管理のためにシステムに割り当てられている名前を示す文字列。

Port Details

- ・ Port – ローカルスイッチ上のポートの ID。
- ・ 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。
- ・ Chassis Type – 送信元 LLDP エージェントに関連付けられている IEEE 802 LAN エンティティを含むシャーシを示します。シャーシを示す方法はいくつかあります。また、シャーシ ID サブタイプを使用して、Chassis ID フィールドで参照されるコンポーネントのタイプが示されます（表 24 「シャーシ ID サブタイプ」を参照）。
- ・ Chassis ID – 本システムの特定のシャーシの固有の ID を示すオクテット文字列。
- ・ System Name – システムに割り当てられている名前を示す文字列。

- ・ System Description – ネットワークエンティティの説明。
- ・ Management Address – リモートデバイスの IPv4 アドレス。使用できる管理アドレスがない場合は、CPU の MAC アドレスまたはアドバタイズメントを送信するポートの MAC アドレスを管理アドレスにしてください。
- ・ Port Type – 「Port ID」フィールドに表示されている ID の基になる情報を示します。

ID の基本情報	参照
インターフェースエイリアス	ifAlias (IETF RFC 2863)
シャーシコンポーネント	EntPhysicalAlias (entPhysClass の値が「chassis(3)」である場合 (IETF RFC 2737))
ポートコンポーネント	EntPhysicalAlias (entPhysicalClass の値が「port(10)」または「backplane(4)」である場合 (IETF RFC 2737))
MAC アドレス	MAC アドレス (IEEE Std 802-2001)
ネットワークアドレス	networkAddress
インターフェース名	ifName (IETF RFC 2863)
エージェント回線	IDagentCircuitID (IETF RFC 3046)
ローカルで割り当てられる値	割り当てられる値

表 1-12: ポート ID サブタイプ

- ・ Port Description – ポートの説明を表わす文字列。RFC 2863 が実装されている場合、このフィールドには ifDescr オブジェクトが使用されます。
- ・ Port ID – LLD PDU を送信したポートの固有の ID を含む文字列。
- ・ System Capabilities Supported – システムの主要機能を規定するシステム性能（表 25 「システム性能」を参照）。
- ・ System Capabilities Enabled – 現在有効になっているシステムの主要機能（表 25 「システム性能」を参照）。
- ・ Management Address List – デバイスの管理アドレス。通常、レイヤ 3 デバイスには多種多様なアドレスが関連付けられるため、個々の LLDP PDU に複数のアドレス TLV に含まれていることがあります。
- ・ 使用できる管理アドレスがない場合は、CPU の MAC アドレスまたはアドバタイズメントを送信するポートの MAC アドレスを管理アドレスにしてください。

Port Details - 802.1 Extension Information

- ・ Remote Port VID – ポートのデフォルトの VLAN ID (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 – このインターフェースで設定されている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) 指定のポートがポート VLAN とプロトコル VLAN をサポートしているかどうか、リモートシステムに関連付けられている指定のポートでポート VLAN とプロトコル VLAN が有効になっているかどうかが表示されます。
- ・ Remote VLAN Name List – ポートに関連付けられている VLAN の名前。
- ・ Remote Protocol Identity List – ポートを使用してアクセスできる個々のプロトコルに関する情報。このオブジェクトは、特定のプロトコル ID を示すためにエージェントで使

用され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ているプロトコルを示すために使用されるオクテット文字列を表わします。

Port Details - 802.3 Extension Port Information

- Remote Port Auto-Neg Supported - (リモートシステムに関連付けられている) 指定のポートがオートネゴシエーションをサポートしているかどうかを示します。
- Remote Port Auto-Neg Adv-Capability - リモートシステム上のポートに関連付けられている ifMauAutoNegCapAdvertisedBits オブジェクト (IETF RFC 3636 で規定) の値 (ビットマップ)。

bit	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	半二重リンクの非同期ポーズ信号
10	半二重リンクの同期ポーズ信号
11	全二重リンクの非同期ポーズ信号と同期ポーズ信号
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

表 1-13: リモートポートのオートネゴシエーションアドバタイズメント機能

- Remote Port Auto-Neg Status - リモートシステムに関連付けられている指定のポートでポートオートネゴシエーションが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 MAU タイプを示す整数値。このオブジェクトは、対応する dot3MauType (IETF RFC 3636 を参照) の優先順位から取得される整数値を含み、個々の dot3MauType OID の末尾の数値と等しくなります。

Port Details - 802.3 Extension Power Information

- Remote Power Class - リモートシステム (給電側装置 (PSE: Power Sourcing Equipment) または受電側装置 (PD: Powered Device)) に関連付けられている指定のポートのポートクラス。
- Remote Power MDI Status - リモートシステムに関連付けられている指定のポートで 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」は予備ペアのみが使用中であることを意味します。
- Remote Power MDI Supported - リモートシステムに関連付けられている指定のポートで 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 Controlable – リモートシステムに関連付けられている指定のポートで給電に関してペアの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、Power over LAN (PoE) ネットワーク上の各種の端末にそれぞれの電力消費に応じてタグを付けるために使用されます。IP フォンなどのデバイスや WLAN アクセスポイントといったものが、それぞれの電力要件に応じて分類されます。

Port Details - 802.3 Extension Trunk Information

- ・ Remote Link Aggregation Capable – リモートポートがリンクアグリゲーション状態ではないかどうか、また、リンクアグリゲーション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。
- ・ Remote Link Aggregation 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ているポートコンポーネントの ifIndex の ifNumber から取得される IEEE 802.3 アグリゲーションポート ID、つまり aAggPortID (IEEE 802.3-2002, 30.7.2.1.1) が含まれます。リモートポートがリンクアグリゲーション状態ではない場合やリンクアグリゲーションをサポートしていない場合、この値は 0 (ゼロ) になります。

Port Details - 802.3 Extension Frame Information

- ・ Remote Max Frame Size – リモートシステムに関連付けられているポートコンポーネントでサポートされている最大フレームサイズ (単位: octet) を示す整数値。

Web インターフェース

リモートポートの LLDP 情報を表示するには、以下のようにします。

- (1) 「Administration」→「LLDP」を選択します。
- (2) 「Step」リストで「Show Remote Device Information」を選択します。
- (3) 「General」、「Port Details」、「Trunk」、または「Trunk Details」を選択します。

The screenshot shows the 'Administration > LLDP' page. The 'Step' dropdown is set to '4. Show Remote Device Information'. Below this, there are four tabs: 'Port' (selected), 'Port Details', 'Trunk', and 'Trunk Details'. The 'LLDP Remote Device Port List' is displayed with the following data:

Local Port	Chassis ID	Port ID	System Name
1	00-E0-0C-10-90-00	00-E0-0C-10-90-06	
2	00-E0-0C-9C-CA-10	00-E0-0C-9C-CA-11	

Web 設定

基本的な管理プロトコル

画面 1-193 : リモートデバイスの LLDP 情報の表示（ポート）

Remote VLAN Name List Total: 1

VLAN	Name
1	DefaultVlan

Remote Protocol Identity List Total: 1

Remote Protocol Identity
88-CC

802.3 Extension Port Information

Remote Port Auto-Neg Supported	Yes	Remote Port Auto-Neg Status	Enabled
Remote Port Auto-Neg Adv-Capability	6C01	Remote Port MAU Type	30

802.3 Extension Trunk Information

Remote Link Aggregation Capable	Yes	Remote Link Aggregation Status	Disabled
Remote Link Port ID	0		

802.3 Extension Frame Information

Remote Max Frame Size	1518		

Administration > LLDP

Step: 4. Show Remote Device Information

☐ Port ☒ Port Details ☐ Trunk ☐ Trunk Details

Port 2

LLDP Remote Device Port Information

Local Port	2	Port Type	MAC Address
Chassis Type	MAC Address	Port Description	Ethernet Port on unit 1, port 1
Chassis ID	00-E0-0C-9C-CA-10	Port ID	00-E0-0C-9C-CA-11
System Name		System Capabilities Supported	Bridge, Router
System Description		System Capabilities Enabled	Bridge, Router

Management Address List Total: 1

Address	Address Type
192.168.0.3	IPv4 Address

802.1 Extension Information

Remote Port VID	1

画面 1-194 : リモートデバイスの LLDP 情報の表示（ポート詳細情報）

デバイス統計情報の表示

「Administration」→「LLDP」(Show Device Statistics)を選択すると、スイッチに接続されている LLDP 対応デバイスおよびすべてのローカルインターフェースで送受信される LLDP プロトコルメッセージに関する統計情報を表示することができます。

関連する CLI 情報

「show lldp info statistics」

パラメータ

以下のパラメータが表示されます。

リモートデバイスに関する全般的な統計情報

- ・ Neighbor Entries List Last Updated – LLDP 隣接デバイスエントリリストの前の更新からの経過時間。
- ・ New Neighbor Entries Count – まだリモート TTL が期限切れになっていない LLDP 隣接デバイスエントリの数。
- ・ Neighbor Entries Deleted Count – 何らかの理由で LLDP リモートシステムの MIB から削除された LLDP 隣接デバイスエントリの数。
- ・ Neighbor Entries Dropped Count – リソース不足のためスイッチのリモートデータベースで LLD PDU がドロップされた回数。
- ・ Neighbor Entries Age-out Count – リモート TTL タイマーで設定されている期間を過ぎたため LLDP リモートシステムの MIB から隣接デバイスの情報が削除された回数。

ポートまたはトランクに関する統計情報

- ・ Frames Discarded – 一般的な妥当性検証ルールだけでなく、特定の TLV について定義されている特定の使用ルールに準拠していないため破棄されたフレームの数。
- ・ Frames Invalid – 1 つまたは複数の検出可能エラーと共に受信された LLD PDU の総数。
- ・ Frames Received – 受信された LLDP PDU の数。
- ・ Frames Sent – 送信された LLDP PDU の数。
- ・ TLVs Unrecognized – 受信先 LLDP ローカルエージェントで認識されなかった TLV の総数。
- ・ TLVs Discarded – 受信された後にメモリ領域不足やシーケンス属性の欠落などのために破棄された LLD PDU の総数。
- ・ Neighbor Ageouts – リモート TTL タイマーで設定されている期間を過ぎたため LLDP リモートシステムの MIB から隣接デバイスの情報が削除された回数。

Web インターフェース

スイッチに接続されている LLDP 対応デバイスに関する統計情報を表示するには、以下のようになります。

- (1) 「Administration」 → 「LLDP」 を選択します。
- (2) 「Step」 リストで 「Show Device Statistics」 を選択します。
- (3) 「General」、「Port」、または 「Trunk」 を選択します。

The screenshot shows the 'Administration > LLDP' page. The 'Step' dropdown is set to '5. Show Device Statistics'. Under the 'General' tab, the 'LLDP Device Statistics' section displays the following data:

Neighbor Entries List Last Updated	2 sec
New Neighbor Entries Count	20
Neighbor Entries Deleted Count	20
Neighbor Entries Dropped Count	0
Neighbor Entries Age-out Count	20

画面 1-195 :LLDP デバイスに関する統計情報の表示（全般）

The screenshot shows the 'Administration > LLDP' page with the 'Port' tab selected. The 'Step' dropdown is set to '5. Show Device Statistics'. The 'Port' dropdown is set to '3'. The 'LLDP Device Port Statistics' section displays the following data:

Frames Discarded	0	TLVs Unrecognized	0
Frames Invalid	0	TLVs Discarded	0
Frames Received	97	Neighbor Ageouts	0
Frames Sent	104		

A 'Refresh' button is located at the bottom right of the statistics table.

画面 1-196 :LLDP デバイスに関する統計情報の表示（ポート）

1.12.3 SNMP (Simple Network Management Protocol)

SNMP は、特にネットワークにおけるデバイスの管理を目的として開発された通信プロトコルです。一般的に SNMP を使用して管理される機器は、スイッチ、ルータ、ホストコンピュータなどです。SNMP は、通常、それらの機器がネットワーク環境で適切に動作するように設定するため、また、それらの機器を監視してパフォーマンスを評価したり潜在的な問題を検出したりするために使用されます。

SNMP をサポートしている管理対象デバイスには、デバイスでローカルに実行されるエージェントと呼ばれるソフトウェアが組み込まれています。定義されている一連の変数（管理対象オブジェクト）が、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。そ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的なプレゼンテーションを示す管理情報ベース（MIB: Management Information Base）で定義されます。SNMP は、それらの情報にネットワーク経由でアクセスするために使用される MIB 仕様のフォーマットとプロトコルの両方を定義します。

本製品には、SNMPv1、SNMPv2c、および SNMPv3 をサポートするオンボードエージェントが組み込まれています。このエージェントは、スイッチのハードウェアのステータスだけでなく、スイッチのポートを経由するトラフィックを継続的に監視します。ネットワーク管理ステーションは、ネットワーク管理ソフトウェアを使用して、それらの情報にアクセスすることができます。

SNMPv1 および SNMPv2c を使用するクライアントからオンボードエージェントへのアクセスは、コミュニティストリングスによって管理されます。スイッチと通信するため、管理ステーションは、最初に、有効なコミュニティストリングスを送信して認証を受ける必要があります。

SNMPv3 を使用するクライアントからスイッチにアクセスでは、メッセージの整合性、認証、および暗号化などの追加のセキュリティ機能が提供されるだけでなく、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 セキュリティ構造は、それぞれ独自のセキュリティレベルをもつ複数のセキュリティモデルから設定されています。規定されているセキュリティモデルは、SNMPv1、SNMPv2c、SNMPv3 の 3 つです。ユーザは、セキュリティモデルおよび指定されるセキュリティレベルによって定義される「グループ」に割り当てられます。各グループは、一連の MIB オブジェクトに対する読み取りと書き込みのための定義済みのセキュリティアクセス権（「ビュー」）をもっています。本製品では、セキュリティモデル v1 と v2c について、デフォルトのビュー（すべての MIB オブジェクト）とデフォルトグループが定義されています。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は、以下の表のとおりです。

モデル	レベル	グループ	読み取りビュー	書き込みビュー	通知ビュー	セキュリティ
v1	noAuthNoPriv	public（読み取り専用）	デフォルトビュー	なし	なし	コミュニティストリングスのみ
v1	noAuthNoPriv	private（読み取り / 書き込み）	デフォルトビュー	デフォルトビュー	なし	コミュニティストリングスのみ
v1	noAuthNoPriv	ユーザ定義	ユーザ定義	ユーザ定義	ユーザ定義	コミュニティストリングスのみ

Web 設定

基本的な管理プロトコル

v2c	noAuthNoPriv	ユーザ定義	デフォルトビュー	デフォルトビュー	なし	コミュニティストリングスのみ
v2c	noAuthNoPriv	ユーザ定義	デフォルトビュー	デフォルトビュー	なし	コミュニティストリングスのみ
v2c	noAuthNoPriv	ユーザ定義	ユーザ定義	ユーザ定義	ユーザ定義	コミュニティストリングスのみ
v3	noAuthNoPriv	ユーザ定義	ユーザ定義	ユーザ定義	ユーザ定義	ユーザ名のマッチングのみ
v3	noAuthNoPriv	ユーザ定義	ユーザ定義	ユーザ定義	ユーザ定義	MD5 または SHA アルゴリズムによるユーザ認証
v3	noAuthNoPriv	ユーザ定義	ユーザ定義	ユーザ定義	ユーザ定義	MD5 または SHA アルゴリズムによるユーザ認証および DES 56 ビット暗号化によるデータプライバシー

表 1-14:SNMPv3 セキュリティモデルとレベル

【注意】 事前定義のデフォルトのグループとビューをシステムから削除し、アクセス権を必要とする SNMP クライアントのため、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

SNMPv1 または SNMPv2c 管理アクセスの設定

スイッチに対する SNMPv1 または SNMPv2c 管理アクセスを設定するには、以下の手順を実行します。

1. 「Administration」 → 「SNMP」 (Configure Global) を選択し、スイッチの SNMP を有効にして、トラップメッセージを有効にします。
2. 「Administration」 → 「SNMP」 (Configure User - Add Community) を選択し、管理アクセスのために承認されるコミュニティストリングスを設定します。
3. 「Administration」 → 「SNMP」 (Configure Trap) を選択し、重要なイベントが管理ステーションに報告されるようにするため、トラップメッセージを指定します。

SNMPv3 管理アクセスの設定

1. 「Administration」 → 「SNMP」 (Configure Global) を選択し、スイッチの SNMP を有効にして、トラップメッセージを有効にします。
2. 「Administration」 → 「SNMP」 (Configure Trap) を選択し、重要なイベントが管理ステーションに報告されるようにするため、トラップメッセージを指定します。
3. 「Administration」 → 「SNMP」 (Configure Engine) を選択し、ローカルエンジン ID を変更します。デフォルトのローカルエンジン ID を変更する場合は、他のパラメータを指定する前に変更しなければなりません。
4. 「Administration」 → 「SNMP」 (Configure View) を選択し、スイッチの MIB ツリーの読み取りビューと書き込みビューを指定します。
5. 「Administration」 → 「SNMP」 (Configure User) を選択し、必要なセキュリティモデル (SNMPv1、SNMPv2c、または SNMPv3) とセキュリティレベル (authentication または privacy) を指定して SNMP ユーザグループを設定します。
6. 「Administration」 → 「SNMP」 (Configure Group) を選択し、SNMP ユーザをグループに割り当てると共に、ユーザ固有の認証パスワードとプライバシーパスワードを指定します。

SNMP のグローバル設定の設定

「Administration」 → 「SNMP」 (Configure Global) を選択し、すべての管理クライアント (SNMPv1、SNMPv2c、および SNMPv3) について SNMPv3 サービスを有効にして、トラップメッセージを有効にします。

関連する CLI 情報

「snmp-server」

「snmp-server enable traps」

パラメータ

以下のパラメータが表示されます。

- ・ Agent Status – スwitchの SNMP を有効にします (デフォルト: Enabled)。
- ・ Authentication Traps7 – SNMP アクセス認証プロセスで無効なコミュニティストリングスが送信されるたびに、指定された IP トラップマネージャ宛の通知メッセージを発行します (デフォルト: Enabled)。
- ・ Link-up and Link-down Traps7 – ポートリンクが確立または切断されるたびに通知メッセージを発行します (デフォルト: Enabled)。

※ 次ページ「**7」参照

Web インターフェース

SNMP のグローバル設定を設定するには、以下のようにします。

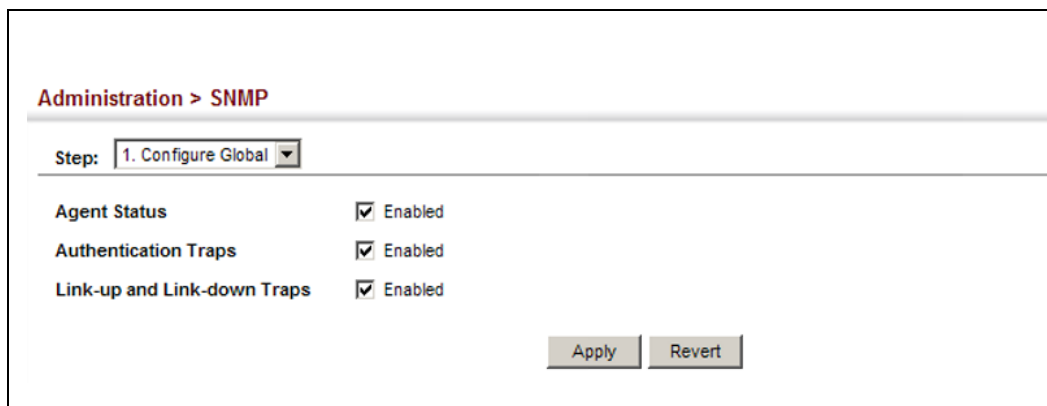
- (1) 「Administration」 → 「SNMP」 を選択します。
- (2) 「Step」 リストで 「Configure Global」 を選択します。

Web 設定

基本的な管理プロトコル

(3) SNMP および必要なトラップタイプを有効にします。

(4) < Apply > ボタンをクリックします。



The screenshot shows a web interface for configuring SNMP. At the top, it says "Administration > SNMP". Below this, there is a "Step:" label followed by a dropdown menu showing "1. Configure Global". Underneath, there are three settings, each with a checked checkbox and the word "Enabled": "Agent Status", "Authentication Traps", and "Link-up and Link-down Traps". At the bottom right of the settings area, there are two buttons: "Apply" and "Revert".

Setting	Status
Agent Status	☒ Enabled
Authentication Traps	☒ Enabled
Link-up and Link-down Traps	☒ Enabled

画面 1-197 :SNMP のグローバル設定の設定

ローカルエンジン ID の設定

「Administration」→「SNMP」（Configure Engine - Set Engine ID を選択すると、ローカルエンジン ID を変更することができます。SNMPv3 エンジンには、スイッチに常駐する独立型 SNMP エージェントであり、メッセージの返信、遅延、およびリダイレクトに関する保護機能を提供します。また、エンジン ID は、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する際に、ユーザパスワードと組み合わせて使用されます。

関連する CLI 情報

「snmp-server engine-id」

コマンドの使用

- ローカル ID は、スイッチ固有の ID であり、自動的に生成されます。この ID は、デフォルトのエンジン ID とみなされます。ローカルエンジン ID が変更または削除されると、すべての SNMP ユーザがクリアされ、既存のすべてのユーザを再設定しなければなりません。

**7. これらは、レガシー通知であり、そのため、SNMPv3 ホストに使用する場合は、通知ビューの該当のエントリと併せて有効にする必要があります。

パラメータ

以下のパラメータが表示されます。

- Engine ID - 9 ～ 64 文字の 16 進数文字（16 進数形式で 5 ～ 32 octets）を入力して、新規エンジン ID を指定することができます。奇数の文字数を指定すると、最後のオクテットを埋めるため、値の末尾に 0 が付加されます。例えば、値「123456789」は「1234567890」と同等です。

Web インターフェース

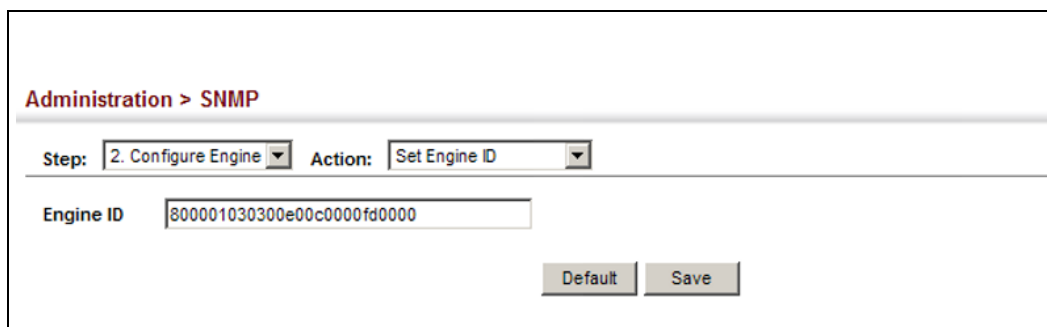
ローカル SNMP エンジン ID を設定するには、以下のようにします。

- （1）「Administration」→「SNMP」を選択します。
- （2）「Step」リストで「Configure Engine」を選択します。
- （3）「Step」リストで「Set Engine ID」を選択します。
- （4）9 文字以上の 16 進数文字の ID を入力します。

Web 設定

基本的な管理プロトコル

(5) < Apply > ボタンをクリックします。



画面 1-198 :SNMP 用のローカルエンジン ID の設定

リモートエンジン ID の設定

「Administration」→「SNMP」（Configure Engine - Add Remote Engine）を選択すると、リモート管理ステーションのエンジン ID を設定することができます。リモートデバイスの SNMPv3 ユーザからの管理アクセスを許可するには、最初に、ユーザが使用しているリモートデバイスの SNMP エージェントのエンジン ID 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のユーザと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。

関連する CLI 情報

「snmp-server engine-id」

コマンドの使用

- ・ SNMP パスワードは、優先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ます。情報メッセージの場合、優先 SNMP エージェントはリモートエージェントです。そのため、リモートエージェントにプロキシ要求または情報メッセージを送信するには、その前に、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（「リモート SNMPv3 ユーザの設定」を参照）。

パラメータ

以下のパラメータが表示されます。

- ・ Remote Engine ID – このエンジン ID は、9 ～ 64 文字の 16 進数文字（16 進数形式で 5 ～ 32 octets）を入力して指定することができます。奇数の文字数を指定すると、最後のオクテットを埋めるため、値の末尾に 0 が付加されます。例えば、値「123456789」は「1234567890」と同等です。
- ・ Remote IP Host – 指定したエンジン ID を使用しているリモート管理ステーションの IP アドレス。

Web インターフェース

リモート SNMP エンジン ID を設定するには、以下のようにします。

- (1) 「Administration」 → 「SNMP」 を選択します。
- (2) 「Step」 リストで 「Configure Engine」 を選択します。
- (3) 「Step」 リストで 「Add Remote Engine」 を選択します。
- (4) 9 文字以上の 16 進数文字の ID を入力し、リモートホストの IP アドレスを入力します。
- (5) < Apply > ボタンをクリックします。

The screenshot shows the 'Administration > SNMP' configuration page. The 'Step' dropdown is set to '2. Configure Engine' and the 'Action' dropdown is set to 'Add Remote Engine'. There are two input fields: 'Remote Engine ID' with the value '5432100000' and 'Remote IP Host' with the value '192.168.1.19'. At the bottom right, there are 'Apply' and 'Revert' buttons.

画面 1-199 :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、以下のようにします。

1. 「Administration」 → 「SNMP」 を選択します。
2. 「Step」 リストで 「Configure Engine」 を選択します。
3. 「Step」 リストで 「Show Remote Engine」 を選択します。

The screenshot shows the 'Administration > SNMP' configuration page with the 'Action' dropdown set to 'Show Remote Engine'. Below the dropdowns, it says 'SNMPv3 Remote Engine List Max: 5 Total: 1'. There is a table with two columns: 'Remote Engine ID' and 'Remote IP Host'. The table contains one row with the values '5432100000' and '192.168.1.19'. At the bottom right, there are 'Delete' and 'Revert' buttons.

	Remote Engine ID	Remote IP Host
☐	5432100000	192.168.1.19

画面 1-200 :SNMP 用のリモートエンジン ID の表示

SNMPv3 ビューの設定

「Administration」→「SNMP」（Configure View）を選択すると、MIB ツリーの指定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 ビューを設定することができます。事前定義ビュー「defaultview」には MIB ツリー全体へのアクセス権が含まれています。

関連する CLI 情報

「snmp-server view」

パラメータ

以下のパラメータが表示されます。

Add View

- ・ View Name - SNMP ビューの名前（範囲：1 ～ 64 文字）。
- ・ OID Subtree - MIB ツリー内のブランチの初期オブジェクト ID を指定します。ワイルドカードを使用して OID 文字列の特定の部分をマスクすることができます。「Add OID Subtree」画面を使用して、オブジェクト ID を追加設定することができます。
- ・ Type - MIB ツリー内のブランチのオブジェクト ID が SNMP ビューで表示されるか、非表示にされるかを示します。

Add OID Subtree

- ・ View Name - 「Add View」画面で設定された SNMP ビューが表示されます。
- ・ OID Subtree - MIB ツリー内のブランチのオブジェクト ID を、選択したビューに追加します。ワイルドカードを使用して OID 文字列の特定の部分をマスクすることができます。
- ・ Type - MIB ツリー内のブランチのオブジェクト ID が SNMP ビューで表示されるか、非表示にされるかを示します。

Web インターフェース

スイッチの MIB データベースの SNMP ビューを設定するには、以下のようになります。

- (1) 「Administration」→「SNMP」を選択します。
- (2) 「Step」リストで「Configure View」を選択します。
- (3) 「Step」リストで「Add View」を選択します。
- (4) ビューの名前を入力し、ビューで表示または非表示にするスイッチの MIB データベース内の初期 OID サブツリーを指定します。「Add OID Subtree」画面を使用して、オブジェクト ID ブランチをビューに追加します。

(5) < Apply > ボタンをクリックします。

Administration > SNMP

Step: 3. Configure View Action: Add View

View Name: ifEntry.a

OID Subtree: 1.3.6.1.2.1.2.2.1.1.*

Type: Included

Apply Revert

画面 1-201 :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、以下のようにします。

1. 「Administration」 → 「SNMP」 を選択します。
2. 「Step」 リストで 「Configure View」 を選択します。
3. 「Step」 リストで 「Show View」 を選択します。

Administration > SNMP

Step: 3. Configure View Action: Show View

SNMPv3 View List Max: 32 Total: 2

☐	View Name
☐	ifEntry.a
☐	defaultview

Delete Revert

画面 1-202 :SNMP ビューの表示

オブジェクト ID をスイッチの MIB データベースの既存の SNMP ビューに追加するには、以下のようにします。

1. 「Administration」 → 「SNMP」 を選択します。
2. 「Step」 リストで 「Configure View」 を選択します。
3. 「Step」 リストで 「Add OID Subtree」 を選択します。
4. ビューの名前を既存のビューのリストで選択し、そのビューに対して追加または除外するスイッチの MIB データベース内の OID サブツリー（初期 OID サブツリー以外）を指定します。

Web 設定

基本的な管理プロトコル

5. < Apply > ボタンをクリックします。

Administration > SNMP

Step: 3. Configure View Action: Add OID Subtree

View Name: ifEntry.a

OID Subtree: 1.3.6.1.2.1.2.2.1.2.*

Type: Included

Apply Revert

画面 1-203 :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 ビューについて設定されている OID ブランチを表示するには、以下のようにします。

1. 「Administration」 → 「SNMP」 を選択します。
2. 「Step」 リストで 「Configure View」 を選択します。
3. 「Step」 リストで 「Show OID Subtree」 を選択します。
4. ビューの名前を既存のビューのリストで選択します。

Administration > SNMP

Step: 3. Configure View Action: Show OID Subtree

View Name: ifEntry.a

SNMPv3 View OID Subtree List Max: 32 Total: 2

	OID Subtree	Type
☐	1.3.6.1.2.1.2.2.1.1.*	Included
☐	1.3.6.1.2.1.2.2.1.2.*	Included

Delete Revert

画面 1-204 :SNMP ビューについて設定されている OID ブランチの表示

SNMPv3 グループの設定

「Administration」→「SNMP」（Configure Group）を選択すると、SNMPv3 グループを追加することができます。SNMPv3 グループを使用して、グループに割り当てられているユーザのアクセスポリシーを設定することにより、それらのユーザが特定の読み取りビュー、書き込みビュー、および通知ビューのみにアクセスできるようにします。事前に定義されているデフォルトグループを使用するか、新規グループを作成して、一連の SNMP ユーザを SNMP ビューにマップすることができます。

関連する CLI 情報

「show snmp group」

パラメータ

以下のパラメータが表示されます。

- ・ Group Name - ユーザを割り当てる SNMP グループの名前（範囲：1 ～ 32 文字）。
- ・ Security Model - ユーザセキュリティモデル（SNMPv1、SNMPv2c、または SNMPv3）。
- ・ Security Level - 以下のセキュリティレベルは、SNMP セキュリティモデルに割り当てられるグループのみに使用されます。
 - ・ noAuthNoPriv - SNMP 通信で認証または暗号化が使用されません（これがデフォルトのセキュリティレベルです）。
 - ・ AuthNoPriv - SNMP 通信で認証が使用されますが、データは暗号化されません。
 - ・ AuthPriv - SNMP 通信で認証と暗号化の両方が使用されます。
- ・ Read View - 読み取りアクセスのための設定済みビュー（範囲：1 ～ 64 文字）。
- ・ Write View - 書き込みアクセスのための設定済みビュー（範囲：1 ～ 64 文字）。
- ・ Notify View - 通知のための設定済みビュー（範囲：1 ～ 64 文字）。

モデル	レベル	グループ
RFC 1493 Traps		
newRoot	1.3.6.1.2.1.17.0.1	送信元エージェントがスパニングツリーの新規ルートになったことを示します。このトラップは、送信元エージェントが新規ルートとして選択されるとすぐに、ブリッジによって送信されます。
topologyChange	1.3.6.1.2.1.17.0.2	設定されているブリッジポートが Learning 状態から Forwarding 状態に変わった場合または Forwarding 状態から Discarding 状態に変わった場合にブリッジによって送信されます。このトラップは、同じ状態の変化について newRoot トラップが送信される場合には送信されません。
SNMPv2 Traps		

Web 設定

基本的な管理プロトコル

coldStart	1.3.6.1.6.3.1.1.5.1	エージェントとして機能している SNMPv2 エンティティが再初期設定中であり、そのため、その設定が変更された可能性があることを通知します。
warmStart	1.3.6.1.6.3.1.1.5.2	エージェントとして機能している SNMPv2 エンティティが再初期設定中であるため、その設定が変更されたことを通知します。
inkDown*	1.3.6.1.6.3.1.1.5.3	エージェントとして機能している SNMP エンティティが、自らの通信リンクの 1 つで ifOperStatus オブジェクトが他の何らかの状態（ただし、notPresent 状態以外）からダウン状態になろうとしていることを検出した場合に発行されます。この「他の何らかの状態」は、ifOperStatus に含まれる値によって示されます。
linkUp*	1.3.6.1.6.3.1.1.5.4	エージェントとして機能している SNMP エンティティが、自らの通信リンクの 1 つで ifOperStatus オブジェクトがダウン状態から他の何らかの状態（ただし、notPresent 状態以外）に移行したことを検出した場合に発行されます。この「他の何らかの状態」は、ifOperStatus に含まれる値によって示されます。
authentication Failure*	1.3.6.1.6.3.1.1.5.5	エージェントとして機能している SNMPv2 エンティティが、適切に認証されていないというプロトコルメッセージを受信したことを通知します。このトラップは、すべての SNMPv2 実装環境で発行可能ですが、発行されるかどうかは snmpEnableAuthenTraps オブジェクトによって示されます。
RMON Events (V2)		
risingAlarm	1.3.6.1.2.1.16.0.1	アラームエントリの上限しきい値を超えた場合に生成されるイベントがトリガーの SNMP トラップ。
fallingAlarm	1.3.6.1.2.1.16.0.2	アラームエントリの下限しきい値を下回った場合に生成されるイベントがトリガーの SNMP トラップ。
Private Traps		
swPowerStatusChangeTrap	1.3.6.1.4.1.25574.20.90.2.1.0.1	電源状態が変化した場合に送信されます。

swPortSecurityTrap	1.3.6.1.4.1.25574.20.90.2.1.0.36	ポート侵入が発生している場合に送信されます。このトラップは、portSecActionTrap トラップが有効になっている場合にのみ、送信されます。
swIpfFilterRejectTrap	1.3.6.1.4.1.25574.20.90.2.1.0.40	IP フィルタによって不正な IP アドレスが拒否された場合に送信されます。
swSmtplibConnFailureTrap	1.3.6.1.4.1.25574.20.90.2.1.0.41	SMTP システムがメールサーバへの接続を正常に開けないことがトリガーとなります。
swMainBoardVersionMismatchNotification	1.3.6.1.4.1.25574.20.90.2.1.0.56	スレーブボードのバージョンがマスターボードのバージョンと一致しない場合に送信されます。このトラップは、2 つのオブジェクトをバインドします。1 番目のオブジェクトはマスターバージョンを示し、2 番目のオブジェクトはスレーブバージョンを示します。
swAtcBcastStormAlarmFireTrap	1.3.6.1.4.1.25574.20.90.2.1.0.70	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た場合に発行されます。
swAtcBcastStormAlarmClearTrap	1.3.6.1.4.1.25574.20.90.2.1.0.71	ブロードキャストストームが通常トラフィックとして検出された場合に発行されます。
swAtcBcastStormTcApplyTrap	1.3.6.1.4.1.25574.20.90.2.1.0.72	ATC がアクティブになった場合に発行されます。
swAtcBcastStormTcReleaseTrap	1.3.6.1.4.1.25574.20.90.2.1.0.73	ATC がリリースされた場合に発行されます。
swAtcMcastStormAlarmFireTrap	1.3.6.1.4.1.25574.20.90.2.1.0.74	マルチキャストトラフィックがストームとして検出された場合に発行されます。
swAtcMcastStormAlarmClearTrap	1.3.6.1.4.1.25574.20.90.2.1.0.75	マルチキャストストームが通常トラフィックとして検出された場合に発行されます。
swAtcMcastStormTcApplyTrap	1.3.6.1.4.1.25574.20.90.2.1.0.76	ATC がアクティブになった場合に発行されます。
swAtcMcastStormTcReleaseTrap	1.3.6.1.4.1.25574.20.90.2.1.0.77	ATC がリリースされた場合に発行されます。
swLoopbackDetectionTrap	1.3.6.1.4.1.25574.20.90.2.1.0.95	ループバック BPDU が検出された場合に送信されます。
networkAccessPortLinkDetectionTrap	1.3.6.1.4.1.25574.20.90.2.1.0.96	networkAccessPortLinkDetection イベントがトリガーされた場合に送信されます。

Web 設定

基本的な管理プロトコル

swCpuUtiRisingNotification	1.3.6.1.4.1.25574.20.90.2.1.0.107	CPU 使用率が cpuUtiRisingThreshold を超えたことを示します。
swCpuUtiFallingNotification	1.3.6.1.4.1.25574.20.90.2.1.0.108	CPU 使用率が cpuUtiFallingThreshold を超えたことを示します。
swMemoryUtiRisingThresholdNotification	1.3.6.1.4.1.25574.20.90.2.1.0.109	メモリ使用率が memoryUtiRisingThreshold を超えたことを示します。
swMemoryUtiFallingThresholdNotification	1.3.6.1.4.1.25574.20.90.2.1.0.110	メモリ使用率が memoryUtiFallingThreshold を超えたことを示します。
swLoginFailureTrap	1.3.6.1.4.1.25574.20.90.2.1.0.139	コンソール、Telnet、または Web によるログインが失敗した場合に送信されます。
swLoginSuccessfulTrap	1.3.6.1.4.1.25574.20.90.2.1.0.140	コンソール、Telnet、または Web によるログインが成功した場合に送信されます。

表 1-14: サポートされている通知メッセージ

Web インターフェース

SNMP グループを設定するには、以下のようにします。

- (1) 「Administration」 → 「SNMP」 を選択します。
- (2) 「Step」 リストで 「Configure Group」 を選択します。
- (3) 「Step」 リストで 「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り当ててから、読み取りビュー、書き込みビュー、および通知ビューを選択します。
- (5) < Apply > ボタンをクリックします。

Administration > SNMP

Step: 4. Configure Group Action: Add

Group Name

secure-users

Security Model

v3

Security Level

authPriv

Read View

☒ ifEntry.a ☐

Write View

☒ ifEntry.a ☐

Notify View

☒ ifEntry.a ☐

Apply

Revert

画面 1-205 :SNMP グループの作成

SNMP グループを表示するには、以下のようにします。

1. 「Administration」 → 「SNMP」 を選択します。
2. 「Step」 リストで 「Configure Group」 を選択します。
3. 「Step」 リストで 「Show」 を選択します。

Administration > SNMP

Step: 4. Configure Group Action: Show

SNMPv3 Group List Max: 26 Total: 5

	Group Name	Model	Level	Read View	Write View	Notify View
☐	public	v1	noAuthNoPriv	defaultview	none	none
☐	public	v2c	noAuthNoPriv	defaultview	none	none
☐	private	v1	noAuthNoPriv	defaultview	defaultview	none
☐	private	v2c	noAuthNoPriv	defaultview	defaultview	none
☐	secure-users	v3	authPriv	ifEntry.a	ifEntry.a	ifEntry.a

Delete Revert

画面 1-206 :SNMP グループの表示

コミュニティアクセス文字列の設定

「Administration」 → 「SNMP」 (Configure User - Add Community) を選択すると、SNMPv1 および SNMPv2c を使用するクライアントによる管理アクセスのために承認されるコミュニティストリングスを最大 5 つ設定することができます。セキュリティ上の理由から、デフォルトの文字列は削除するようにしてください。

関連する CLI 情報

「snmp-server community」

パラメータ

以下のパラメータが表示されます。

- Community String - パスワードと同じような役割を果たし、SNMP プロトコルに対するアクセス許可に使用される文字列。
範囲: 1 ~ 32 文字 (大文字と小文字の区別あり)
デフォルト文字列: public (読み取り専用)、private (読み取り / 書き込み)
- Access Mode - コミュニティストリングスに対応するアクセス権として、以下のいずれかを指定します。
 - Read-Only - 承認された管理ステーションは MIB オブジェクトの取得のみを行うことができます。

Web 設定

基本的な管理プロトコル

- ・ Read/Write – 承認された管理ステーションは MIB オブジェクトの取得と変更の両方を行うことができます。

Web インターフェース

コミュニティストリングスを設定するには、以下のようにします。

- (1) 「Administration」 → 「SNMP」 を選択します。
- (2) 「Step」 リストで 「Configure User」 を選択します。
- (3) 「Step」 リストで 「Add Community」 を選択します。
- (4) 必要に応じて新規のコミュニティストリングスを追加し、それらに対応するアクセス権を 「Access Mode」 リストで選択します。
- (5) < Apply > ボタンをクリックします。

Administration > SNMP

Step: 5. Configure User Action: Add Community

Community String: spiderman

Access Mode: Read/Write

Apply Revert

画面 1-207 : 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、以下のようにします。

1. 「Administration」 → 「SNMP」 を選択します。
2. 「Step」 リストで 「Configure User」 を選択します。
3. 「Step」 リストで 「Show Community」 を選択します。

Administration > SNMP

Step: 5. Configure User Action: Show Community

SNMP Community String List Max: 5 Total: 3

	Community String	Access Mode
☐	public	Read-Only
☐	private	Read/Write
☐	spiderman	Read/Write

Delete Revert

画面 1-208 : コミュニティアクセス文字列の表示

ローカル SNMPv3 ユーザの設定

「Administration」→「SNMP」（Configure User - Add SNMPv3 Local User）を選択すると、SNMPv3 クライアントの管理アクセスの認証方式や、ローカルスイッチから送信される SNMPv3 トラップメッセージの送信元を指定することができます。それぞれの SNMPv3 ユーザは一意の名前で定義されます。ユーザを設定するときには、グループに割り当てられている特定のセキュリティレベルを指定する必要があります。SNMPv3 グループに応じて、ユーザが特定の読み取りビュー、書き込みビュー、および通知ビューのみにアクセスできるようになります。

関連する CLI 情報

「snmp-server user」

パラメータ

以下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（範囲：1 ～ 32 文字）。
- ・ Group Name - ユーザを割り当てる SNMP グループの名前（範囲：1 ～ 32 文字）。
- ・ Security Model - ユーザセキュリティモデル（SNMPv1、SNMPv2c、または SNMPv3）。
- ・ Security Level - 以下のセキュリティレベルは、SNMP セキュリティモデルに割り当てられるグループのみに使用されます。
 - ・ noAuthNoPriv - SNMP 通信で認証または暗号化が使用されません（これがデフォルトのセキュリティレベルです）。
 - ・ AuthNoPriv - SNMP 通信で認証が使用されますが、データは暗号化されません。
 - ・ AuthPriv - SNMP 通信で認証と暗号化の両方が使用されます。
- ・ Authentication Protocol - ユーザ認証方式（オプション：MD5 または SHA、デフォルト：MD5）。
- ・ Authentication Password - 最小 8 文字のプレーンテキストを指定する必要があります。
- ・ Privacy Protocol - データプライバシーのために使用される暗号化アルゴリズム（現時点では 56 ビット DES のみ、使用可能）。
- ・ Privacy Password - 最小 8 文字のプレーンテキストを指定する必要があります。

Web インターフェース

ローカル SNMPv3 ユーザを設定するには、以下のようになります。

- (1) 「Administration」→「SNMP」を選択します。
- (2) 「Step」リストで「Configure User」を選択します。
- (3) 「Step」リストで「Add SNMPv3 Local User」を選択します。
- (4) 名前を入力し、その名前をグループに割り当てます。セキュリティモデルを「SNMPv3」に設定し、セキュリティレベルを「authNoPriv」または「authPriv」に設定する場合は、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。また、

Web 設定

基本的な管理プロトコル

セキュリティレベルが「authPriv」の場合は、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 > ボタンをクリックします。

The screenshot shows the 'Administration > SNMP' configuration page. The 'Step' is set to '5. Configure User' and the 'Action' is 'Add SNMPv3 Local User'. The form includes the following fields:

- SNMPv3 User**
 - User Name:
 - Group Name: ☐ public ☒ r&d
 - Security Model:
 - Security Level:
- User Authentication**
 - Authentication Protocol:
 - Authentication Password:
- Data Privacy**
 - Privacy Protocol:
 - Privacy Password:

At the bottom right, there are 'Apply' and 'Revert' buttons.

画面 1-209 : 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、以下のようにします。

1. 「Administration」 → 「SNMP」 を選択します。
2. 「Step」 リストで 「Configure User」 を選択します。
3. 「Step」 リストで 「Show SNMPv3 Local User」 を選択します。

The screenshot shows the 'Administration > SNMP' configuration page with the 'Action' set to 'Show SNMPv3 Local User'. It displays a table of local SNMPv3 users.

	User Name	Group Name	Model	Level	Authentication	Privacy
☐	chris	r&d	v3	authPriv	MD5	DES56

At the bottom right, there are 'Delete' and 'Revert' buttons.

画面 1-210 : ローカル SNMPv3 ユーザの表示

リモート SNMPv3 ユーザの設定

「Administration」→「SNMP」（Configure User - Add SNMPv3 Remote User）を選択すると、リモートデバイスから送信される SNMPv3 情報メッセージの送信元を指定することができます。それぞれの SNMPv3 ユーザは一意の名前で定義されます。ユーザを設定するときには、グループに割り当てられている特定のセキュリティレベルを指定する必要があります。SNMPv3 グループに応じて、ユーザが特定の読み取りビュー、書き込みビュー、および通知ビューのみにアクセスできるようになります。

関連する CLI 情報

「snmp-server user」

コマンドの使用

- ・ リモートデバイスの SNMPv3 ユーザに管理アクセスを付与するには、最初に、ユーザが使用しているリモートデバイスの SNMP エージェントのエンジン ID 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と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（「トラップマネージャの指定」および「リモートエンジン ID の設定」を参照）。

パラメータ

以下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（範囲：1 ～ 32 文字）。
- ・ Group Name - ユーザを割り当てる SNMP グループの名前（範囲：1 ～ 32 文字）。
- ・ Remote IP - ユーザが使用するリモートデバイスの IP アドレス。
- ・ Security Model - ユーザセキュリティモデル（SNMPv1、SNMPv2c、または SNMPv3）（デフォルト：v3）。
- ・ Security Level - 以下のセキュリティレベルは、SNMP セキュリティモデルに割り当てられるグループのみに使用されます。
 - ・ noAuthNoPriv - SNMP 通信で認証または暗号化が使用されません（これがデフォルトのセキュリティレベルです）。
 - ・ AuthNoPriv - SNMP 通信で認証が使用されますが、データは暗号化されません。
 - ・ AuthPriv - SNMP 通信で認証と暗号化の両方が使用されます。
- ・ Authentication Protocol - ユーザ認証方式（オプション：MD5 または SHA、デフォルト：MD5）。
- ・ Authentication Password - 最小 8 文字のプレーンテキストを指定する必要があります。
- ・ Privacy Protocol - データプライバシーのために使用される暗号化アルゴリズム（現時点では 56 ビット DES のみ、使用可能）。
- ・ Privacy Password - 最小 8 文字のプレーンテキストを指定する必要があります。

Web インターフェース

リモート SNMPv3 ユーザを設定するには、以下のようにします。

- (1) 「Administration」→「SNMP」を選択します。
- (2) 「Step」リストで「Configure User」を選択します。

Web 設定

基本的な管理プロトコル

- (3) 「Step」 リストで「Add SNMPv3 Remote User」を選択します。
- (4) 名前を入力し、その名前をグループに割り当てます。リモートデバイスから送信される SNMPv3 情報メッセージの送信元がわかるようにするための IP アドレスを入力します。セキュリティモデルを「SNMPv3」に設定し、セキュリティレベルを「authNoPriv」または「authPriv」に設定する場合は、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。また、セキュリティレベルが「authPriv」の場合は、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 > ボタンをクリックします。

The screenshot shows the 'Administration > SNMP' configuration page. At the top, there is a breadcrumb trail 'Administration > SNMP'. Below it, a 'Step:' dropdown is set to '5. Configure User' and an 'Action:' dropdown is set to 'Add SNMPv3 Remote User'. The main configuration area is titled 'SNMPv3 User' and contains the following fields:

- User Name:** A text input field containing 'mark'.
- Group Name:** Two radio buttons are present. The first is labeled 'public' and is unselected. The second is labeled 'r&d' and is selected.
- Remote IP:** A dropdown menu showing '192.168.1.19'.
- Security Model:** A dropdown menu showing 'v3'.
- Security Level:** A dropdown menu showing 'authPriv'.
- User Authentication:** A section header.
- Authentication Protocol:** A dropdown menu showing 'MD5'.
- Authentication Password:** A text input field containing 'greenpeace'.
- Data Privacy:** A section header.
- Privacy Protocol:** A dropdown menu showing 'DES56'.
- Privacy Password:** A text input field containing 'einstien'.

At the bottom right of the form, there are two buttons: 'Apply' and 'Revert'.

画面 1-211：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、以下のようにします。

- (1) 「Administration」 → 「SNMP」を選択します。
- (2) 「Step」 リストで「Configure User」を選択します。

(3) 「Step」 リストで「Show SNMPv3 Remote User」を選択します。

Administration > SNMP

Step: 5. Configure User Action: Show SNMPv3 Remote User

SNMPv3 Remote User List Max: 5 Total: 1

	User Name	Group Name	Engine ID	Model	Level	Authentication	Privacy
☐	mark	r&d	543210000	v3	authPriv	MD5	DES56

Delete Revert

画面 1-212 : リモート SNMPv3 ユーザの表示

トラップマネージャの指定

「Administration」→「SNMP」(Configure Trap)を選択すると、トラップの送信先のホストデバイスおよび送信するトラップのタイプを指定することができます。ステータスが変わったことを示すトラップは、スイッチから、指定されたトラップマネージャに発行されます。重要なイベントが（ネットワーク管理ソフトウェアを使用して）スイッチから管理ステーションに報告されるようにするため、トラップマネージャを指定する必要があります。認証失敗メッセージやその他のトラップメッセージをスイッチから受信する管理ステーションを最大5つ指定することができます。

関連する CLI 情報

「snmp-server host」

「snmp-server enable traps」

コマンドの使用

- デフォルトで、通知はトラップメッセージとしてスイッチから送信されます。トラップメッセージの受信先は応答をスイッチに送信しません。したがって、トラップは、受信確認要求を含む情報メッセージほど信頼性は高くありません。情報メッセージは、重大な情報がホストで受信されるようにするために使用することができます。ただし、情報メッセージは、応答が受信されるまでメモリに保存されるので、トラップに比べて多くのシステムリソースを消費するということに注意してください。また、情報メッセージはネットワークトラフィックを増加させます。通知をトラップとして送信するか情報メッセージとして送信するか決める際には、これらのことを考慮してください。

情報メッセージを SNMPv2c ホストに送信するには、以下の手順を実行します。

- SNMP エージェントを有効にします。
- 必要な通知メッセージを指定してビューを作成します。
- 必要な通知ビューが含まれるようにグループを設定します。このグループは、「Configure Trap」(「Step」リスト)→「Add」(「Action」リスト)を選択して表示される画面で指定したコミュニティストリングスに対応するグループです。

4. 以降に記載されている説明に従って、情報メッセージを有効にします。

情報メッセージを SNMPv3 ホストに送信するには、以下の手順を実行します。

1. SNMP エージェントを有効にします。
2. メッセージ交換プロセスで使用するローカル SNMPv3 ユーザを作成します。トラップ設定画面で指定されたユーザが存在しない場合は、指定されたローカルユーザの名前、ならびに読み取りビュー、書き込みビュー、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を指定して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. 以降に記載されている説明に従って、情報メッセージを有効にします。

パラメータ

以下のパラメータが表示されます。

SNMPv1

- ・ IP Address – 通知メッセージを受信する新規の管理ステーション（対象の受信先）の IP アドレス。
- ・ Version – 通知を SNMPv1 トラップ、SNMPv2c トラップ、SNMPv3 トラップのうちのどれとして送信するかを指定します（デフォルト：v1）。
- ・ Community String – 新規トラップマネージャエントリについて有効なコミュニティストリングスを指定します（範囲：1～32 文字（大文字と小文字の区別あり））。
- ・ この文字列は「Configure Trap」（「Step」リスト）→「Add」（「Action」リスト）を選択して表示される画面で設定することができますが、「Configure User」（「Step」リスト）→「Add Community」（「Action」リスト）を選択して表示される画面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が使用する UDP ポート番号を指定します（デフォルト：162）。

SNMPv2c

- ・ IP Address – 通知メッセージを受信する新規の管理ステーション（対象の受信先）の IP アドレス。
- ・ Version – 通知を SNMPv1 トラップ、SNMPv2c トラップ、SNMPv3 トラップのうちのどれとして送信するかを指定します。
- ・ Notification Type
 - ・ Traps – 通知をトラップメッセージとして送信します。
 - ・ Inform – 通知を情報メッセージとして送信します。このオプションは SNMPv2c ホストおよび SNMPv3 ホストの場合にのみ使用可能であるという点に注意してください（デフォルト：Traps）。
 - Timeout – 情報メッセージを再送する前に受信確認を待機する期間（範囲：0～2,147,483,647 センチ秒、デフォルト：1,500 センチ秒）
 - Retry times – 受信先からの受信確認がない場合の情報メッセージの最大再送回数（範囲：0～255、デフォルト：3）。

- ・ Community String – 新規トラップマネージャエントリについて有効なコミュニティストリングスを指定します（範囲：1～32文字（大文字と小文字の区別あり））。この文字列は「Configure Trap」（「Step」リスト）→「Add」（「Action」リスト）を選択して表示される画面で設定することができますが、「Configure User」（「Step」リスト）→「Add Community」（「Action」リスト）を選択して表示される画面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が使用する UDP ポート番号を指定します（デフォルト：162）。

SNMPv3

- ・ IP Address – 通知メッセージを受信する新規の管理ステーション（対象の受信先）の IP アドレス。
- ・ Version – 通知を SNMPv1 トラップ、SNMPv2c トラップ、SNMPv3 トラップのうちのどれとして送信するかを指定します。
- ・ Notification Type
 - ・ Traps – 通知をトラップメッセージとして送信します。
 - ・ Inform – 通知を情報メッセージとして送信します。このオプションは SNMPv2c ホストおよび SNMPv3 ホストの場合にのみ使用可能であるという点に注意してください（デフォルト：Traps）。
 - Timeout – 情報メッセージを再送する前に受信確認を待機する期間（範囲：0～2,147,483,647 センチ秒、デフォルト：1,500 センチ秒）。
 - Retry times – 受信先からの受信確認がない場合の情報メッセージの最大再送回数（範囲：0～255、デフォルト：3）。
- ・ Local User Name – ローカルスイッチから送信される SNMPv3 トラップメッセージの送信元を特定するために使用されるローカルユーザ名（範囲：1～32文字）。指定されたユーザのアカウントが作成されていない場合は、アカウントが自動的に生成されます。
- ・ Remote User Name – リモートスイッチから送信される SNMPv3 情報メッセージの送信元を特定するために使用されるローカルユーザ名（範囲：1～32文字）。指定されたユーザのアカウントが作成されていない場合は、アカウントが自動的に生成されます。
- ・ UDP Port – トラップマネージャが使用する UDP ポート番号を指定します（デフォルト：162）。
- ・ Security Level – 「v3」を選択した場合は、以下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（デフォルト：noAuthNoPriv）。
 - ・ noAuthNoPriv – SNMP 通信で認証または暗号化が使用されません。
 - ・ AuthNoPriv – SNMP 通信で認証が使用されますが、データは暗号化されません。
 - ・ AuthPriv – SNMP 通信で認証と暗号化の両方が使用されます。

Web 設定

基本的な管理プロトコル

Web インターフェース

トラップマネージャを設定するには、以下のようにします。

- (1) 「Administration」 → 「SNMP」 を選択します。
- (2) 「Step」 リストで 「Configure Trap」 を選択します。
- (3) 「Step」 リストで 「Add」 を選択します。
- (4) 選択した SNMP バージョンに基づいて必要なパラメータを指定します。
- (5) < Apply > ボタンをクリックします。

The screenshot shows the 'Administration > SNMP' configuration page. At the top, there is a breadcrumb 'Administration > SNMP'. Below it, a 'Step:' dropdown is set to '6. Configure Trap' and an 'Action:' dropdown is set to 'Add'. The main form contains the following fields: 'IP Address' with the value '192.168.0.3', 'Version' with a dropdown set to 'v1', 'Community String' with the value 'private', and 'UDP Port (1-65535)' with the value '162'. At the bottom right, there are two buttons: 'Apply' and 'Revert'.

画面 1-213 : トラップマネージャの設定 (SNMPv1)

The screenshot shows the 'Administration > SNMP' configuration page for SNMPv2c. At the top, there is a breadcrumb 'Administration > SNMP'. Below it, a 'Step:' dropdown is set to '6. Configure Trap' and an 'Action:' dropdown is set to 'Add'. The main form contains the following fields: 'IP Address' with the value '192.168.2.9', 'Version' with a dropdown set to 'v2c', 'Notification Type' with a dropdown set to 'Inform', 'Timeout (0-2147483647)' with an empty field and the unit 'centiseconds' to its right, 'Retry Times (0-255)' with an empty field, 'Community String' with the value 'venus', and 'UDP Port (1-65535)' with an empty field. At the bottom right, there are two buttons: 'Apply' and 'Revert'.

画面 1-214 : トラップマネージャの設定 (SNMPv2c)

Administration > SNMP

Step: 6. Configure Trap Action: Add

IP Address: 192.168.2.9

Version: v3

Notification Type: Inform

Timeout (0-2147483647): centiseconds

Retry Times (0-255):

Remote User Name:

UDP Port (1-65535):

Security Level: authPriv

Apply Revert

画面 1-215 : トラップマネージャの設定 (SNMPv3)

設定されているトラップマネージャを表示するには、以下のようにします。

1. 「Administration」 → 「SNMP」 を選択します。
2. 「Step」 リストで 「Configure Trap」 を選択します。
3. 「Step」 リストで 「Show」 を選択します。

Administration > SNMP

Step: 6. Configure Trap Action: Show

SNMP Trap Manager List Max: 5 Total: 5

☐	IP Address	Version	Community String/User Name	UDP Port	Security Level	Timeout	Retry Times
☐	192.168.0.4	v3	steve	162	noAuthNoPriv		
☐	192.168.0.5	v3	bobby	162	noAuthNoPriv		
☐	192.168.0.6	v3	betty	162	authNoPriv		
☐	192.168.2.9	v2c	venus	162		1600	5
☐	192.168.5.8	v3	margaret	162	authPriv	1600	5

Delete Revert

画面 1-216 : トラップマネージャの表示

1.12.4 リモートモニタリング (RMON)

RMON を使用すると、リモートデバイスで情報を収集したり、指定したイベントに対して個別にアクションが実行可能にします。本製品は、RMON 対応デバイスであり、さまざまなタスクを個別に実行して、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。継続的に診断を実行し、ネットワークパフォーマンスに関する情報をログに記録することが可能です。イベントがトリガーされた場合は、自動的に、障害がネットワーク管理者に通知され、イベントの履歴情報が提供されます。本製品は、管理エージェントに接続できない場合には、指定されたタスクを引き続き実行し、次回、接続できたときにデータを管理ステーションに渡します。

本製品は、Statistics、History、Event、および AlarmThe の各グループから設定される mini-RMON をサポートしています。RMON を有効にすると、システムによって物理インターフェースに関する情報が徐々に作成され、該当の RMON データベースグループに保存されます。管理エージェントは、SNMP プロトコルを使用して定期的にスイッチと通信します。ただし、スイッチでクリティカルなイベントが発生した場合に自動的にトラップメッセージが管理ステーションに送信されるようにすることができ、管理エージェントは（そのように設定されていれば）そのイベントに対するアクションを実行します。

RMON アラームの設定

「Administration」→「RMON」(Configure Global - Add - Alarm) を選択すると、応答イベントを生成する個々の条件を定義することができます。アラームを設定して、指定した間隔でデータがテストされるようにすることや、絶対変化値または相対変化値（例えば、統計カウンタが特定の値に達したことや、指定された期間内に特定の数値の分だけ統計値が変化したことなど）を監視することができます。また、アラームを設定して、上限しきい値を超えた場合または下限しきい値を下回った場合にアクションが実行されるようにすることもできます（ただし、アラームは、トリガーされると、統計値が反対の境界しきい値を超えてから再びトリガーしきい値に達するまで再度トリガーされないという点に注意してください）。

関連する CLI 情報

「Remote Monitoring Commands」

コマンドの使用

- あるインデックスについて既にアラームが定義されている場合は、そのエントリを削除してからでないと、何らかの変更を加えることはできません。

パラメータ

以下のパラメータが表示されます。

- Index - エントリのインデックス（範囲：1 ～ 65,535）。
- Status - アラームエントリのステータス（表示されるデータ：Valid、createRequest、underCreation、または Invalid）。
- Variable - サンプリングされる MIB 変数のオブジェクト ID。サンプリングできるのは etherStatsEntry.n.n というタイプの変数のみです。
etherStatsEntry.n は MIB 変数を一意に定義し、etherStatsEntry.n.n は MIB 変数に加えて etherStatsIndex を定義するという点に注意してください。例えば、1.3.6.1.2.1.16.1.1.1.6.1 は etherStatsBroadcastPkts と値 1 の etherStatsIndex を表わします。
- Interval - ポーリング間隔（範囲：1 ～ 31,622,400 秒）。

- ・ Sample Type – 指定した変数の絶対変化と相対変化が確認されます。
 - ・ Absolute – 変数が、そのまま、サンプリング期間の終了時のしきい値と比較されます。
 - ・ Delta – 最新の値から前回のサンプリング値が差し引かれ、その差分がしきい値と比較されます。
- ・ Rising Threshold – 最新の値が上限しきい値以上であり、前回のサンプリング値が上限しきい値よりも小さかった場合にアラームが生成されます。上限しきい値を超えたことを示すイベントが生成された場合、同様のイベントは、サンプリング値が上限しきい値を下回ってから下限しきい値に達した後に再び上限しきい値に達するまで生成されません（範囲：1 ～ 65,535）。
- ・ Rising Event Index – 監視対象の変数が上限しきい値以上になったことによってアラームがトリガーされた場合に使用されるイベントのインデックス。該当するエントリがイベント制御テーブルにない場合、イベントは生成されません（範囲：1 ～ 65,535）。
- ・ Falling Threshold – 最新の値が下限しきい値以下であり、前回のサンプリング値が下限しきい値よりも大きかった場合にアラームが生成されます。下限しきい値を下回ったことを示すイベントが生成された場合、同様のイベントは、サンプリング値が下限しきい値を上回ってから上限しきい値に達した後に再び下限しきい値に達するまで生成されません（範囲：1 ～ 65,535）。
- ・ Falling Event Index – 監視対象の変数が下限しきい値以下になったことによってアラームがトリガーされた場合に使用されるイベントのインデックス。該当するエントリがイベント制御テーブルにない場合、イベントは生成されません（範囲：1 ～ 65,535）。
- ・ Owner – エントリを作成したユーザの名前（範囲：1 ～ 127 文字）。

Web インターフェース

RMON アラームを設定するには、以下のようにします。

- (1) 「Administration」 → 「RMON」 を選択します。
- (2) 「Step」 リストで 「Configure Global」 を選択します。
- (3) 「Step」 リストで 「Add」 を選択します。
- (4) 「Alarm」 を選択します。
- (5) インデックス番号、ポーリング対象の MIB オブジェクト（etherStatsEntry.n.n）、ポーリング間隔、サンプリングタイプ、しきい値、およびトリガーされるイベントを入力します。

Web 設定

基本的な管理プロトコル

(6) < Apply > ボタンをクリックします。

Administration > RMON

Step: 1. Configure Global Action: Add

☒ Alarm ☐ Event

Index (1-65535) 1

Variable 6.1

Interval (1-31622400) 15 sec

Sample Type Delta

Rising Threshold (0-2147483647) 100

Rising Event Index (0-65535) 30

Falling Threshold (0-2147483647) 1

Falling Event Index (0-65535) 2

Owner bill

Apply Revert

画面 1-217 :RMON アラームの設定

設定されている RMON アラームを表示するには、以下のようにします。

- (1) 「Administration」 → 「RMON」 を選択します。
- (2) 「Step」 リストで 「Configure Global」 を選択します。
- (3) 「Step」 リストで 「Show」 を選択します。
- (4) 「Alarm」 を選択します。

Administration > RMON

Step: 1. Configure Global Action: Show

☒ Alarm ☐ Event

RMON Alarm List Max: 896 Total: 26

☐	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	bill
☐	2	Valid	1.3.6.1.2.1.16.1.1.1.6.2	30	Delta	0	892800	0	446400	0	bill
☐	3	Valid	1.3.6.1.2.1.16.1.1.1.6.3	30	Delta	0	892800	0	446400	0	bill
☐	4	Valid	1.3.6.1.2.1.16.1.1.1.6.4	30	Delta	0	892800	0	446400	0	bill
☐	5	Valid	1.3.6.1.2.1.16.1.1.1.6.5	30	Delta	0	892800	0	446400	0	bill

画面 1-218 : 設定されている RMON アラームの表示

RMON イベントの設定

「Administration」→「RMON」（Configure Global - Add - Event）を選択すると、アラームがトリガーされた場合に実行されるアクションを設定することができます。アクションには、アラームのログ記録やトラップマネージャへのメッセージの送信などがあります。アラームとそれらに対応するイベントを指定することにより、クリティカルなネットワーク障害に即座に対応できるようになります。

関連する CLI 情報

「Remote Monitoring Commands」

コマンドの使用

- ・ あるインデックスについて既にアラームが定義されている場合は、そのエントリを削除してからでないと、何らかの変更を加えることはできません。
- ・ デフォルトのイベントは、以下のように設定されています。

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

以下のパラメータが表示されます。

- ・ Index – エントリのインデックス（範囲：1 ～ 65,535）。
- ・ 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 – イベントがトリガーされた場合に RMON ログエントリが生成されます。ログメッセージは、イベントログの現在の設定情報に基づいて処理されます（「システムログの設定」を参照）。
 - ・ Trap – 指定されているトラップマネージャにトラップメッセージが送信されます（「トラップマネージャの指定」を参照）。
 - ・ Log and Trap – イベントのログが記録され、トラップメッセージが送信されます。
- ・ Community – パスワードと同じような役割を果たすコミュニティストリングスであり、SNMPv1 ホストおよび SNMPv2c ホストに対するトラップ操作で送信されます。コミュニティストリングスは、この設定画面で設定できますが、事前に SNMP トラップ設定画面で定義することをお勧めします（「コミュニティアクセス文字列の設定」を参照）（範囲：1 ～ 32 文字）。
- ・ Description – イベントについて説明するコメント（範囲：1 ～ 127 文字）。
- ・ Owner – エントリを作成したユーザの名前（範囲：1 ～ 127 文字）。

Web インターフェース

RMON イベントを設定するには、以下のようにします。

- (1) 「Administration」 → 「RMON」 を選択します。
- (2) 「Step」 リストで 「Configure Global」 を選択します。
- (3) 「Step」 リストで 「Add」 を選択します。
- (4) 「Event」 を選択します。
- (5) 索引番号、開始するイベントのタイプ、トラップメッセージと共に送信するコミュニティストリングスストリングス、イベントを作成したユーザの名前、およびイベントの簡単な説明を入力します。
- (6) < Apply > ボタンをクリックします。

The screenshot shows a web interface for configuring RMON events. At the top, it says "Administration > RMON". Below this, there are two dropdown menus: "Step: 1. Configure Global" and "Action: Add". Underneath, there are two radio buttons: "Alarm" (unselected) and "Event" (selected). Below the radio buttons, there are several input fields: "Index (1-65535)" with the value "2", "Type" with a dropdown menu showing "Log and Trap", "Community" with the value "private", "Description" with the value "for software group", and "Owner" with the value "david". At the bottom right, there are two buttons: "Apply" and "Revert".

画面 1-219 :RMON イベントの設定

設定されている RMON イベントを表示するには、以下のようにします。

1. 「Administration」 → 「RMON」 を選択します。
2. 「Step」 リストで 「Configure Global」 を選択します。
3. 「Step」 リストで 「Show」 を選択します。

4. 「Event」を選択します。

Administration > RMON

Step: 1. Configure Global Action: Show

☐ Alarm ☒ Event

RMON Event List Max: 448 Total: 1

☐	Index	Status	Type	Community	Description	Owner	Last Fired
☐	2	Valid	Log and Trap	private	for software group	david	00:00:00

Delete Revert

画面 1-220 : 設定されている RMON イベントの表示

RMON 履歴サンプリングの設定

「Administration」→「RMON」（Configure Interface - Add - History）を選択すると、ネットワークの使用状況、パケットタイプ、およびエラーを監視するために物理インターフェースに関する統計情報が収集されるようにすることができます。アクティビティの履歴レコードを使用して、断続的に発生する問題を追跡することができます。また、履歴レコードを使用して、標準的な基準アクティビティを設定することもできます。そのようにすることで、大量トラフィックやブロードキャストストームなどの例外的なイベントに伴って発生する問題が明らかになる可能性があります。さらに、履歴レコードに基づいてネットワークトラフィックの増加を予測し、ネットワークで過度のオーバーロードが発生する前にネットワークの拡張計画を立てることもできます。

関連する CLI 情報

「Remote Monitoring Commands」

コマンドの使用

それぞれのインデックス番号はスイッチのポートと同じ番号です。

- あるインターフェースで既に履歴情報の収集が有効になっている場合は、そのエントリを削除してからでないと、何らかの変更を加えることはできません。
- それぞれのサンプリングで収集される情報には、以下のようなものがあります。
- 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、サイズ不足パケット、サイズ超過パケット、フラグメント、ジャバー、CRC アライメントエラー、コリジョン、ドロップイベント、ネットワークの使用状況
- 「Show Details」画面に表示される統計情報の説明については、「ポートまたはトランクに関する統計情報の表示」を参照してください。

パラメータ

以下のパラメータが表示されます。

- Port - スwitchのポート番号。
- Index - エントリのインデックス（範囲：1～65,535）。
- Interval - ポーリング間隔（範囲：1～3,600 秒、デフォルト：1,800 秒）。

Web 設定

基本的な管理プロトコル

- ・ Buckets – エントリに関して要求されるバケットの数（範囲：1 ～ 65,536、デフォルト：50）。
- ・ 付与されたバケットの数は「Show」画面に表示されます。
- ・ Owner – エントリを作成したユーザの名前（範囲：1 ～ 127 文字）。

Web インターフェース

ポートに関する統計を定期的にサンプリングするには、以下のようにします。

- (1) 「Administration」 → 「RMON」 を選択します。
- (2) 「Step」 リストで 「Configure Interface」 を選択します。
- (3) 「Step」 リストで 「Add」 を選択します。
- (4) 「History」 を選択します。
- (5) データソースとなるポートをリストで選択します。
- (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、およびエントリのオーナーの名前を入力します。
- (7) < Apply > ボタンをクリックします。

The screenshot shows a web interface for configuring RMON. The breadcrumb is 'Administration > RMON'. Below it, 'Step: 2. Configure Interface' and 'Action: Add' are shown in dropdown menus. There are two radio buttons: 'History' (selected) and 'Statistics'. A 'Port' dropdown menu shows '2'. Below this are four input fields: 'Index (1-65535)' with value '100', 'Interval (1-3600)' with value '60' and 'sec' unit, 'Buckets (1-65535)' with value '10', and 'Owner' with value 'david'. At the bottom right are 'Apply' and 'Revert' buttons.

画面 1-221 :RMON 履歴サンプリングの設定

設定されている RMON 履歴サンプリングを表示するには、以下のようにします。

- (1) 「Administration」 → 「RMON」 を選択します。
- (2) 「Step」 リストで 「Configure Interface」 を選択します。
- (3) 「Step」 リストで 「Show」 を選択します。
- (4) ポートをドロップダウンリストから選択します。

(5) 「History」を選択します。

Administration > RMON

Step: 2. Configure Interface Action: Show

☒ History ☐ Statistics

Port 2

RMON History Port List Max: 1344 Total: 3

☐	Index	Status	Interval	Requested Buckets	Granted Buckets	Owner
☐	3	Valid	1800	8	8	
☐	4	Valid	30	8	8	
☐	100	Valid	60	10	8	david

Delete Revert

画面 1-222 : 設定されている RMON 履歴サンプリングの表示

収集された RMON 履歴サンプリング情報を表示するには、以下のようにします。

- (1) Administration → 「RMON」を選択します。
- (2) 「Step」リストで「Configure Interface」を選択します。
- (3) 「Step」リストで「Show Details」を選択します。
- (4) ポートをドロップダウンリストから選択します。
- (5) 「History」を選択します。

Administration > RMON

Step: 2. Configure Interface Action: Show Details

☒ History ☐ Statistics

Port 2

RMON History Details Port List Max: 24 Total: 14

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
4	303	02:31:06	38438	99	0	17	0	0	0	0	0	0	0	0
4	304	02:31:36	28267	72	1	17	0	0	0	0	0	0	0	0
4	305	02:32:06	27950	70	0	16	0	0	0	0	0	0	0	0
100	1	02:31:24	66705	171	1	34	0	0	0	0	0	0	0	0

Refresh

画面 1-223 : 収集された RMON 履歴サンプリング情報の表示

RMON 統計サンプリングの設定

「Administration」→「RMON」（Configure Interface - Add – Statistics）を選択すると、ポートに関する統計情報が収集されるようにすることができます。後で、それらの情報を使用して、一般的なネットワークエラーや全体的なトラフィックレートを監視することができます。

関連する CLI 情報

「Remote Monitoring Commands」

コマンドの使用

- ・ あるインターフェースで既に統計情報の収集が有効になっている場合は、そのエントリを削除してからでないと、何らかの変更を加えることはできません。
- ・ それぞれのエントリについて収集される情報には、以下のようなものがあります。
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、サイズ不足パケット、サイズ超過パケット、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、さまざまなサイズのフレーム

パラメータ

以下のパラメータが表示されます。

- ・ Port – スイッチのポート番号。
- ・ Index – エントリのインデックス（範囲：1 ～ 65,535）。
- ・ Owner – エントリを作成したユーザの名前（範囲：1 ～ 127 文字）。

Web インターフェース

ポートに関する統計情報の定期的なサンプリングを有効にするには、以下のようにします。

- (1) 「Administration」→「RMON」を選択します。
- (2) 「Step」リストで「Configure Interface」を選択します。
- (3) 「Step」リストで「Add」を選択します。
- (4) 「Statistics」を選択します。
- (5) データソースとなるポートをリストで選択します。
- (6) インデックス番号およびエントリのオーナーの名前を入力します。

(7) < Apply > ボタンをクリックします。

The screenshot shows the 'Administration > RMON' page. The 'Step' dropdown is set to '2. Configure Interface' and the 'Action' dropdown is set to 'Add'. Under the 'Statistics' tab, the 'Port' dropdown is set to '2'. The 'Index (1-65535)' field contains '100' and the 'Owner' field contains 'mary'. At the bottom right, there are 'Apply' and 'Revert' buttons.

画面 1-224 :RMON 統計サンプリングの設定

設定されている RMON 統計サンプリングを表示するには、以下のようにします。

1. 「Administration」 → 「RMON」 を選択します。
2. 「Step」 リストで 「Configure Interface」 を選択します。
3. 「Step」 リストで 「Show」 を選択します。
4. ポートをドロップダウンリストから選択します。
5. 「Statistics」 を選択します。

The screenshot shows the 'Administration > RMON' page. The 'Step' dropdown is set to '2. Configure Interface' and the 'Action' dropdown is set to 'Show'. Under the 'Statistics' tab, the 'Port' dropdown is set to '2'. Below the form, there is a table titled 'RMON Statistics Port List' with 'Max: 448' and 'Total: 2'. The table has columns for 'Index', 'Status', and 'Owner'. There are two rows of data: one with Index '2' and Status 'Valid', and another with Index '100' and Status 'Valid', both with Owner 'mary'. At the bottom right, there are 'Delete' and 'Revert' buttons.

	Index	Status	Owner
☐	2	Valid	mary
☐	100	Valid	mary

画面 1-225 : 設定されている RMON 統計サンプリングの表示

収集された RMON 統計サンプリング情報を表示するには、以下のようにします。

1. 「Administration」 → 「RMON」 を選択します。
2. 「Step」 リストで 「Configure Interface」 を選択します。
3. 「Step」 リストで 「Show Details」 を選択します。

Web 設定

基本的な管理プロトコル

4. ポートをドロップダウンリストから選択します。

5. 「Statistics」を選択します。

Administration > RMON

Step: 2. Configure Interface Action: Show

☐ History ☒ Statistics

Port 2

RMON Statistics Port List Max: 448 Total: 2

☐	Index	Status	Owner
☐	2	Valid	
☐	100	Valid	mary

Delete Revert

画面 1-226 : 収集された RMON 統計サンプリング情報の表示

1.13 マルチキャストフィルタリング

本章では、以下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。

- ・ レイヤ 2 の IGMP - スヌーピングパラメータおよびクエリパラメータを設定します。
- ・ IGMP グループのフィルタリングとスロットリング - マルチキャストサービスを指定してフィルタリングされるようにしたり、スロットリングによってインターフェースで許可されるマルチキャストグループの最大数を制限したりします。
- ・ レイヤ 3 の IGMP - マルチキャストルーティングと共に使用されるクエリを設定します。
- ・ MVR (Multicast VLAN Registration) - 他の一般的な VLAN またはプライベート VLAN グループにアサインされているホストにより構成された特定のグループ宛てのマルチキャストトラフィックのみを対象とした VLAN となり、セキュリティを確保し、データを分離します。

1.13.1 概要

マルチキャストは、ビデオ会議やオーディオストリーミング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。マルチキャストサーバは、各クライアントとの接続を別途に確立する必要はなく、マルチキャストサービスをネットワークにブロードキャストするだけで済みます。そうすれば、そのサービスを受けるホストが自らのローカルマルチキャストスイッチまたはルータを登録します。この手法を使用すると、マルチキャストサーバのネットワークオーバーヘッドを削減することができますが、それぞれのマルチキャストスイッチまたはマルチキャストルータを経由するブロードキャストトラフィックを慎重に絞り込んで、それらのトラフィックがサービスに加入しているホストのみに渡されるようにしなければなりません。

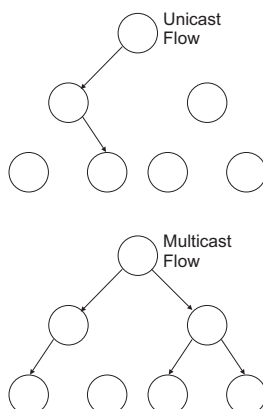


図 1-16: マルチキャストフィルタリングの概念

本製品では、IGMP (Internet Group Management Protocol) を使用してマルチキャストトラフィックをフィルタリングすることができます。また、IGMP スヌーピングを使用すれば、接続ホストと IGMP 対応デバイス (マルチキャストルータなど) との間のデータ交換をパッシブに監視 (つまり、「スヌーピング」) することができます。そのようにすることで、マルチキャストグループへの加入を希望しているホストを検出したり、そのためのフィルターを設定したりできるようになります。

Web 設定

マルチキャストフィルタリング

ローカルサブネットに接続しているマルチキャストルータがない状況では、マルチキャストトラフィックおよびクエリメッセージをスイッチで受信できない場合があります。そのような場合には、IGMP クエリを使用して、接続しているホストに対し、特定のマルチキャストサービスを受けるかどうかをアクティブに問い合わせることができます。そのように IGMP クエリを使用することにより、マルチキャストサービスへの加入を要求しているホストに接続しているポートが特定され、それらのポートのみにデータが送信されるようになります。ホストは、自らが引き続きマルチキャストサービスを受けられるようにするため、サービス要求を、隣接するマルチキャストスイッチまたはマルチキャストルータに伝搬します。

IP マルチキャストフィルタリングの目的はスイッチドネットワークのパフォーマンスを最適化することです。そのため、トラフィックをサブネット（VLAN）内のすべてのポートにフラッドせず、マルチキャストグループホスト、マルチキャストルータ、またはマルチキャストスイッチに接続しているポートのみにマルチキャストパケットを送信します。

本製品は、IGMP クエリ、レポートメッセージ、およびマルチキャストルーティングプロンプトメッセージをパッシブに監視することによって IP マルチキャストフィルタリングをサポートして、エンドステーションをマルチキャストグループメンバーとして登録します。それだけでなく、マルチキャストトラフィックを他のサブネットに転送するために必要な PIM（Protocol Independent Multicasting）もサポートしています。

また、他の標準 VLAN グループまたはプライベート VLAN グループに常駐しているホストによって共有される単一のネットワークワイド VLAN を設定して、セキュリティを確保し、データを分離することもできます（「MVR (Multicast VLAN Registration)」を参照）。

1.13.2 IGMP (Internet Group Management Protocol)

IGMP は、ホストとそれらに直接隣接するマルチキャストルータまたはマルチキャストスイッチとの間で実行されます。IGMP は、ホストが特定のマルチキャストグループ宛の送信データの受信を希望することをローカルルータに通知できるようにするマルチキャストホスト登録プロトコルです。マルチキャスト対応のルータまたはスイッチは、ホストに対し、マルチキャストトラフィックの受信を希望するかどうかを定期的に問い合わせることができます。LAN 上に IP マルチキャストを実行する複数のルータまたはスイッチがある場合には、それらの 1 つが（レイヤ 3 の）「クエリア」として選択され、グループメンバーについてホストに問い合わせる役割を果たします。ホストは、自らが引き続きマルチキャストサービスを受けられるようにするため、サービス要求を、隣接するマルチキャストスイッチまたはマルチキャストルータに伝搬します。IGMP を使用して学習されるグループメンバーシップ情報に基づき、ルータまたはスイッチは、自らのそれぞれのポートにどのマルチキャストトラフィック（存在する場合）を転送する必要があるかどうかを判別します。レイヤ 3 では、マルチキャストルータは、インターネットでの IP マルチキャストをサポートするため、この情報を PIM (Protocol Independent Multicasting) などのマルチキャストルーティングプロトコルと共に使用します。ただし、IGMP では IP マルチキャストパケットについてアラートが発行されることもルーティングが実行されることもないという点に注意してください。マルチキャストルーティングプロトコルは、異なるサブネットワークにまたがって IP マルチキャストパケットを配信する場合に使用する必要があります。したがって、スイッチ上のサブネットについて PIM ルーティングを有効にすると、自動的に IGMP が有効になります。

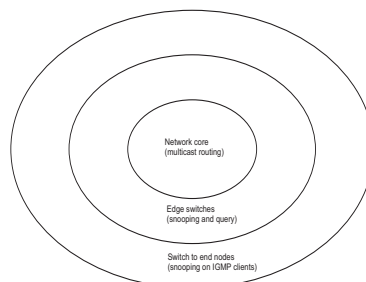


図 1-17:IGMP (Internet Group Management Protocol)

**** 図の注釈**

ネットワークコア（マルチキャストルーティング）

エッジスイッチ（スヌーピングとクエリ）

エンドノードに接続しているスイッチ（IGMP クライアントでのスヌーピング）

1.13.3 レイヤ 2 の IGMP（スヌーピングとクエリ）

IGMP スヌーピングとクエリ - マルチキャストルーティングがネットワーク内の他のスイッチでサポートされていない場合には、IGMP スヌーピングとクエリを使用して、マルチキャストクライアントとマルチキャストサーバとの間で渡される IGMP サービス要求を監視し、マルチキャストトラフィックを転送する必要があるスイッチポートを動的に設定することができます。IGMP スヌーピングを使用すると、特定のマルチキャストサービスを受けることを希望しているノードが存在していないネットワークセグメントで帯域幅を節約することができます。スイッチでマルチキャストルーティングをサポートしていない場合や、既にマルチキャストルーティングがローカルネットワーク内の他のスイッチで有効になっている場合、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サービスは IGMP スヌーピングのみです。

IGMPv3 スヌーピングを使用する場合、IGMPv1、v2、または v3 ホストからのサービス要求は、すべて、アップストリームルータに IGMPv3 レポートとして転送されます。IGMPv3 スヌーピングによって提供される主な拡張機能は、ダウンストリーム IGMPv3 ホストが要求または拒否した特定のマルチキャストサービスの送信元に関する情報の追跡です。本製品では、マルチキャストグループとマルチキャストチャネルの両方に関する情報が保持されます。この場合、グループはホストが特定の送信元を要求しなかったマルチキャストフローを示し、チャネルはホストが特定の送信元からのサービスを要求したフローを示します。IGMPv1 ホストまたは IGMPv2 ホストの場合、チャネルの送信元アドレスは常に Null（任意の送信元を許可）ですが、IGMPv3 ホストの場合、必要に応じて特定のアドレスを含めることができます。

IGMPv3 ホストのみが特定のマルチキャスト送信元からのサービスを要求することができます。ダウンストリームホストが特定の送信元からのマルチキャストサービスを要求する場合、それらの送信元は、すべて、Include リストに含まれ、トラフィックは、それらの送信元のそれぞれからホストに転送されます。また、IGMPv3 ホストは、指定されている以外の送信元からサービスが転送されるように要求することもできます。その場合、トラフィックは、Exclude リストの送信元に基いてフィルタリングされ、その他の使用可能なすべての送信元から転送されます。

[注意] IGMPv3 スヌーピングを使用するようにスイッチを設定する場合、各 VLAN で検出される IGMP クエリパケットのバージョンに応じて、スヌーピングのバージョンを v2 または v1 にダウングレードすることもできます。

[注意] IGMP スヌーピングは、マルチキャストルータポートがスイッチで有効になっていない場合は機能しません。マルチキャストルータポートは、2 つのいずれかの方法で有効にすることができます。1 つは、スタティックルータポートを手動で設定する方法です（「マルチキャストルータのスタティックインターフェースの指定」を参照）。この方法を使用する場合、ルータポートは、タイムアウトになることなく、明示的に削除されるまで継続して機能します。もう 1 つの方法は、スイッチに依存して、ポート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 クエリパケットが検出されるたびにマルチキャストルーティングポートが動的に作成されるようにすることです。

[注意] IGMP スヌーピングとマルチキャストルーティングの両方が有効になっている場合は、それらの両方について最大 1,024 のマルチキャストエントリを保持することができます。テーブルがいっぱいになると、新しいエントリは学習されなくなります。それ以降は、テーブルで検出されないマルチキャストトラフィックは、未登録によるフラッドイングが無効（デフォルトの動作）になっており、接続している VLAN

でルータポートが設定されていない場合にはドロップされ、未登録によるフラッディングが有効になっている場合（「IGMP スヌーピングとクエリのパラメータの設定」を参照）には VLAN 全体にフロードされます。

スタティック IGMP ルータインターフェース - IGMP スヌーピングによって IGMP クエリアを見つけられない場合は、ネットワーク経由でスイッチのインターフェースに接続されている既知の IGMP クエリア（マルチキャストルータまたはマルチキャストスイッチ）を手動で指定することができます。そのようにすると、マルチキャストトラフィックがスイッチ内の該当のすべてのインターフェースに渡されるようにするため、接続されているスイッチまたはルータでサポートされている現行のすべてのマルチキャストグループがインターフェースで結合されます。

Static IGMP Host Interface

より慎重に制御する必要があるマルチキャストアプリケーションについては、マルチキャストサービスをスイッチの特定のインターフェースに手動で割り当てることができます。

IGMP Snooping with Proxy Reporting

本製品は、Last leave およびクエリ抑止（2006 年 4 月の DSL フォーラム TR-101 で規定）をサポートしています。

- ・ Last leave: IGMP ホストから送信される IGMP 脱退メッセージをインターセプト、吸収、および要約します。IGMP 脱退メッセージは、必要な場合（つまり、マルチキャストグループから最後のユーザが脱退した場合）にのみ、アップストリームに中継されます。
- ・ クエリ抑制: IGMP 固有のクエリがクライアントポートに送信されない方法で IGMP クエリをインターセプトして処理します。

TR-101 との唯一の相違点は、レポート抑制、およびスイッチから発信される IGMP トラフィックの優先度ビットによるマーキング（R-250 で規定）がサポートされていないことです。

IGMP スヌーピングとクエリのパラメータの設定

「Multicast」→「IGMP Snooping」→「General」を選択すると、マルチ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することができます。スイッチは、IGMP クエリメッセージとレポートメッセージに基づいて、マルチトラフィックを、要求しているポートのみに転送します。そのようにすることで、スイッチがトラフィックをすべてのポートにブロードキャストしないようにし、場合によっては、ネットワークのパフォーマンスに悪影響が及ぶことも防ぎます。

関連する CLI 情報

「IGMP Snooping」

コマンドの使用

- ・ IGMP Snooping – 本製品では、IP マルチキャストグループのメンバーを特定するため、IP マルチキャストルータまたはスイッチと IP マルチキャストグループとの間で伝送される IGMP Query パケットと IGMP Report パケットをパッシブにスヌーピングすることができます。パススルーされる IGMP パケットが監視され、グループ登録情報が取得されて、その情報に応じてマルチキャストフィルタが設定されます。

[注意] ルータポートを指定して設定された VLAN に不明なマルチキャストトラフィックが入ってきた場合、トラフィックは、そのルータポートに転送されます。ただし、ルータポートが VLAN 上に 1 つも存在していない場合には、未登録によるフラッディングが無効（デフォルトの動作）になっているとトラフィックはドロップされ、未登録によるフラッディングが有効（コマンドパラメータ「Unregistered Data Flood」の説明を参照）になっているとトラフィックは VLAN 全体にフロードされます。

- ・ IGMP クエリア – マルチキャスト対応のルータまたはスイッチは、ホストに対し、マルチキャストトラフィックの受信を希望するかどうかを定期的に問い合わせることができます。LAN 上に IP マルチキャストを実行する複数のルータまたはスイッチがある場合には、それらの 1 つが「クエリア」として選択され、グループメンバーについてホストに問い合わせる役割を果たします。ホストは、自らが引き続きマルチキャストサービスを受けられるようにするため、サービス要求をアップストリームマルチキャストスイッチまたはマルチキャストルータに伝搬します。

[注意] マルチキャストルータは、インターネットでの IP マルチキャストをサポートするため、IGMP スヌーピングレポートおよび IGMP クエリレポートによって取得される情報を PIM などのマルチキャストルーティングプロトコルと共に使用します。

パラメータ

以下のパラメータが表示されます。

- ・ IGMP Snooping Status – このパラメータが有効になっている場合、スイッチは、ネットワークトラフィックを監視して、どのホストがマルチキャストトラフィックの受信を希望しているかを判別します。これを IGMP スヌーピングと言います（デフォルト：Enable）。
- IGMP スヌーピングがグローバルで有効になっている場合は、VLAN インターフェースごとの IGMP スヌーピング設定が優先されます（「インターフェースごとの IGMP スヌーピングステータスの設定」を参照）。

IGMP スヌーピングがグローバルで無効になっている場合でも、個々の VLAN について IGMP スヌーピングを設定することはできますが、IGMP スヌーピングが再びグローバルで有効にならない限り、そのインターフェース設定は適用されません。

- ・ Proxy Reporting Status – プロキシレポートによる IGMP スヌーピング (IGMP Snooping with Proxy Reporting) を有効にします (デフォルト: Disabled)。

このコマンドを使用してスイッチでプロキシレポートを有効にすると、Last leave とクエリ抑止を含め、(2006 年 4 月の DSL フォーラム TR-101 で規定されている)「プロキシレポートによる IGMP スヌーピング」が実行されます。

Last leave は、マルチキャストグループの最後のメンバーが脱退した場合にプロキシクエリを送信する機能です。クエリ抑止とは、特定のクエリがスイッチのアップストリームマルチキャストルータからダウンストリームホストに転送されないようにすることを意味します。

スイッチでプロキシレポートが無効になっている場合、受信されたすべての IGMP レポートはアップストリームマルチキャストルータにネイティブに転送されます。

- ・ TCN Flood – スパニングツリーのトポロジ変更通知 (TCN: Topology Change Notification) が発行された場合のマルチキャストトラフィック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 TCN が発行された場合には、スイッチが学習したマルチキャストメンバーシップ情報が古くなって使えなくなることがあります。例えば、トポロジ変更 (TC: Topology Change) の前にあるポートにリンクしていたホストが変更後には別のポートに移動されていることがあります。マルチキャストデータがすべての受信者に配信されるようにするため、デフォルトで、(ルートブリッジによって) TC ビットが設定されるブリッジプロトコルデータユニット (BPDU: Bridge Protocol Data Unit) を受信する (IGMP スヌーピングが有効になっている) VLAN 内のスイッチは、トポロジが安定してすべてのマルチキャスト受信先の新しいロケーションが学習されるまで、しばらくの間、「マルチキャストフラッディングモード」になります。

TCN が受信されると、すべてのアップリンクポートが削除され、その時点で学習されているすべてのマルチキャストチャネルがタイムアウトメカニズムを使用して削除されます。

新しいアップリンクポートが始動すると、その時点で学習されているすべてのチャネルに関する非要請レポートが、その新しいアップリンクポートを使用して、スイッチから送信されます。

デフォルトで、スイッチは、スパニングツリーのトポロジ変更が発生するとすぐに「マルチキャストフラッディングモード」になります。このモードでは、マルチキャストトラフィックがすべての VLAN ポートにフロードされます。異なるマルチキャストグループに加入しているポートが多数ある場合には、フラッディングによってスイッチとエンドホストとの間のリンクで過度のパケット損失が発生する可能性があります。そのようなことが起こらないようにするため、フラッディングを無効にして、マルチキャストグループメンバーが学習されているポートのみにマルチキャストトラフィックが配信されるようにすることもできます。フラッディングを無効にしない場合は、フラッディングモードとなる期間を手動設定して、過度の負荷が発生しないようにすることができます。

スパニングツリートポロジが変更されると、ルートブリッジは、マルチキャストチャネルのホストメンバーシップまたはポートの関係が速やかに学習されるようにするため、プロキシクエリを送信します。また、ルートブリッジは、VLAN 内のマルチキャストルータのロケーションを速やかに突き止めるため、非要請のマルチキャストルータ検出 (MRD: Multicast Router Discovery) 要求も送信します。

プロキシクエリおよび非要請 MRD 要求は、該当のパケットがスイッチで受信されると、受信先ポート以外のすべての VLAN ポートにフロードされます。

- ・ TCN Query Solicit – スパニングツリーの TCN が発行された場合に IGMP 一般クエリ要請を送信します（デフォルト：Disabled）。

スパニングツリー内のルートブリッジは、IGMP スヌーピングが有効になっている VLAN の TCN を受信すると、グローバル IGMP 脱退メッセージ（クエリ要請）を発行します。スイッチは、この要請を受信すると、それを、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ロードします。アップストリームマルチキャストルータは、この要請を受信すると、即座に IGMP 一般クエリを発行します。

クエリ要請は、スイッチがスパニングツリー内のルートブリッジでなくても、スイッチがトポロジ変更を通知するときには常に送信されるようにすることができます。

- ・ Router Alert Option – Router Alert オプションを含んでいない IGMPv2 パケットまたは IGMPv3 パケットを破棄します（デフォルト：Disabled）。

IGMPv3 に関する RFC 3376 の 9.1 で規定されているように、Router Alert オプションは、DOS 攻撃を防ぐために使用することができます。一般的な攻撃手法の 1 つとして、侵入者がクエリアの役割を乗っ取って、（それぞれ、送信元リストのサイズが大きく、Maximum Response Time が大きな値が設定されている）GSS（Group and Source Specific）クエリを大量に送信することにより、マルチキャストホストでオーバーロードを発生させるというものがあります。

この種の攻撃を防ぐ方法は、第一に、ルータがクエリを転送しないようにすることです。この方法は、クエリに Router Alert オプションが含まれる場合は比較的簡単に実装することができます。第二の方法は、スイッチがマルチキャストホストとして機能している場合（例えば、プロキシルーティングを使用している場合など）に Router Alert オプションを含んでいない IGMPv2 クエリまたは IGMPv3 クエリを無視するというものです。

- ・ Unregistered Data Flooding – 接続している VLAN に未登録のマルチキャストトラフィックをフロードします（デフォルト：Disabled）。

IGMP スヌーピングと IGMP マルチキャストルーティングのためのマルチキャストエントリが保存されているテーブルがいっぱいになると、新しいエントリが学習されなくなります。ただし、接続している VLAN でルータポートが 1 つも設定されていない場合、未登録によるフラディングが無効になっていると以降のトラフィックはすべてドロップされ、未登録によるフラディングが有効になっているとトラフィックは VLAN 全体にフロードされます。

- ・ Version Exclusive – IGMP Version 属性で設定されている現行のバージョンと異なるバージョンが使用されている受信 IGMP メッセージを破棄します（デフォルト：Disabled）。
- ・ IGMP Unsolicited Report Interval – プロキシレポートが有効になっている場合にアップストリームインターフェースで非要請 IGMP レポートを送信する間隔を指定します（範囲：1 ～ 65,535 秒、デフォルト：400 秒）。

新しいアップストリームインターフェース（つまり、アップリンクポート）が始動すると、その時点で学習されているすべてのマルチキャストチャネルに関する非要請レポートが、その新しいアップストリームインターフェースを使用して、スイッチから送信されます。

このコマンドは、プロキシレポートが有効になっている場合にのみ適用されます。

- ・ Router Port Expire Time – クエリアが停止してから期限切れになったとみなすまでスイッチが待機する時間（範囲：1 ～ 65,535 秒、推奨範囲：300 ～ 500 秒、デフォルト：300 秒）。
- ・ IGMP Snooping Version – ネットワーク上の他のデバイスとの互換性を確保するため、プロトコルバージョンを設定します。これは、スイッチがスヌーピングレポートを送信するときに使用する IGMP バージョンです（範囲：1 ～ 3、デフォルト：2）。

この属性は、IGMP スヌーピングで使用される IGMP レポートまたはクエリのバージョンを指定します。バージョン 1 ～ 3 が、すべて、サポートされています。バージョン 2 と 3 は、使用されるスヌーピングのバージョンに関係なくスイッチが他のデバイスと連携できるように、下位互換性を確保するために用意されています。

- ・ Querier Status – 有効にすると、スイッチは、ホストにマルチキャストトラフィックの受信を希望するかどうかを問い合わせるクエリアとして機能することができます。この機能は IGMPv3 スヌーピングではサポートされていません（デフォルト：Disabled）。

Web インターフェース

IGMP スヌーピングとクエリの全般設定を設定するには、以下のようにします。

- (1) 「Multicast」 → 「IGMP Snooping」 → 「General」 を選択します。
- (2) IGMP 設定を必要に応じて調整します。
- (3) < Apply > ボタンをクリックします。

Multicast > IGMP Snooping > General	
IGMP Snooping Status	☒ Enabled
Proxy Reporting Status	☒ Enabled
TCN Flood	☐ Enabled
TCN Query Solicit	☐ Enabled
Router Alert Option	☐ Enabled
Unregistered Data Flooding	☐ Enabled
Version Exclusive	☐ Enabled
IGMP Unsolicited Report Interval (1-65535)	400 seconds
Router Port Expire Time (1-65535)	300 seconds
IGMP Snooping Version (1-3)	2
Querier Status	☐ Enabled

画面 1-227 :IGMP スヌーピングの全般設定の設定

マルチキャストルータのスタティックインターフェースの指定

Web 設定

マルチキャストフィルタリング

「Multicast」→「IGMP Snooping」→「Multicast Router」（Add Static Multicast Router）を選択すると、インターフェースをマルチキャストルータまたはマルチキャストスイッチに静的に接続することができます。

ネットワーク接続によっては、IGMP スヌーピングで必ずしも IGMP クエリアを見つけられないことがあります。そのため、IGMP クエリアがスイッチ上のインターフェース（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またはスイッチである場合には、接続しているルータでサポートされている現行のすべてのマルチキャストグループを結合するように、そのインターフェース（および指定した VLAN）を手動設定することができます。そのようにすることで、マルチキャストトラフィックがスイッチの該当のすべてのインターフェースに渡されるようになります。

関連する CLI 情報

「Static Multicast Routing」

コマンドの使用

- ・ マルチキャストルータポートが機能するようにするには、事前にスイッチで IGMP スヌーピングをグローバルに有効にする必要があります（「IGMP スヌーピングとクエリのパラメータの設定」を参照）。

パラメータ

以下のパラメータが表示されます。

- ・ VLAN – 接続しているマルチルータから送信されるすべてのマルチキャストトラフィックを伝搬する VLAN を選択します（範囲：1 ～ 4,093）。
- ・ Interface – 「Port」または「Trunk」を選択してドロップ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に接続されているインターフェースを指定します。

Web インターフェース

マルチキャストルータに接続されているスタティックインターフェースを指定するには、以下のようになります。

- (1) 「Multicast」→「IGMP Snooping」→「Multicast Router」を選択します。
- (2) 「Step」リストで「Add Static Multicast Router」を選択します。
- (3) 該当するすべてのマルチキャストトラフィックを転送する VLAN を選択し、マルチキャストルータに接続されているポートまたはトランクを選択します。

(4) < Apply > ボタンをクリックします。

画面 1-228 : マルチキャストルータのスタティックインターフェースの設定

マルチキャストルータに接続されているスタティックインターフェースを表示するには、以下のようになります。

1. 「Multicast」 → 「IGMP Snooping」 → 「Multicast Router」を選択します。
2. 「Step」 リストで「Show Static Multicast Router」を選択します。
3. 該当の情報を表示する VLAN を選択します。

Static Multicast Router Interface List	
	Interface
☐	Unit 1 / Port 1
☐	Unit 1 / Port 2
☐	Unit 1 / Port 3
☐	Trunk 2
☐	Trunk 5
☐	Unit 1 / Port 4

画面 1-229 : マルチキャストルータに接続されているスタティックインターフェースの表示

スイッチのポートに接続されているマルチキャストルータは、インターネットでの IP マルチキャストリングをサポートするため、IGMP によって取得される情報を PIM などのマルチキャストルーティングプロトコルと共に使用します。それらのルータは、スイッチで動的に検出したり、スイッチのインターフェースに静的に割り当てたりすることができます。マルチキャストルータに接続されているすべてのインターフェースを表示するには、以下のようになります。

Web 設定

マルチキャストフィルタリング

1. 「Multicast」 → 「IGMP Snooping」 → 「Multicast Router」 を選択します。
2. 「Step」 リストで 「Current Multicast Router」 を選択します。
3. 該当の情報を表示する VLAN を選択します。隣接するマルチキャストルータまたはマルチキャストスイッチに接続している選択した VLAN 内のポートが表示されます。

Multicast > IGMP Snooping > Multicast Router

Action: Show Current Multicast Router

VLAN 1

Multicast Router Interface Information Max: 32 Total: 4

Interface	Type
Unit 1 / Port 4	Static
Unit 1 / Port 5	Dynamic
Trunk 2	Dynamic
Trunk 3	Dynamic

画面 1-230 : マルチキャストルータに接続されている現行のインターフェースの表示

マルチキャストサービスへのインターフェースの割り当て

「Multicast」→「IGMP Snooping」→「IGMP Member」（Add Static Member）を選択すると、マルチキャストサービスをインターフェースに静的に割り当てることができます。

マルチキャストフィルタリングは、IGMP スヌーピングメッセージと IGMP クエリメッセージを使用して動的に設定することができます（「IGMP スヌーピングとクエリのパラメータの設定」を参照）。ただし、比較的厳密な管理が要求される特定のアプリケーションについては、スイッチでマルチキャストサービスを静的に設定することが必要になる場合もあります。最初に、該当のホストに接続されているすべてのポートを共通 VLAN に追加してから、マルチキャストサービスをその VLAN グループに割り当てます。

関連する CLI 情報

「ip igmp snooping vlan static」

コマンドの使用

- ・ スタティックマルチキャストアドレスは、テーブルから削除されることはありません。
- ・ マルチキャストアドレスが特定の VLAN 内のインターフェースに割り当てられている場合、該当するトラフィックは、その VLAN 内のポートのみに転送することができます。

パラメータ

以下のパラメータが表示されます。

- ・ VLAN – マルチキャストサービスを伝搬する VLAN を指定します（範囲：1 ～ 4,093）。
- ・ Interface – 「Port」または「Trunk」を選択してドロップダウンリストをアクティブにします。
- ・ Port or Trunk – マルチキャストグループに割り当てられているインターフェースを指定します。
- ・ Multicast IP – 特定のマルチキャストサービス用の IP アドレス。

Web インターフェース

インターフェースをマルチキャストサービスに静的に割り当てするには、以下のようになります。

- (1) 「Multicast」→「IGMP Snooping」→「IGMP Member」を選択します。
- (2) 「Step」リストで「Add Static Member」を選択します。
- (3) マルチキャストサービスを伝搬する VLAN を選択し、（IGMP 対応スイッチまたはマルチキャストルータを使用して）マルチキャストサービスに接続されているインターフェースを指定し、マルチキャスト IP アドレスを入力します。

Web 設定

マルチキャストフィルタリング

(4) < Apply > ボタンをクリックします。

Multicast > IGMP Snooping > IGMP Member

Action: Add Static Member

VLAN: 1

Interface: ☒ Port 1 ☐ Trunk 1

Multicast IP: 224.1.1.1

Apply Revert

画面 1-231 : マルチキャストサービスへのインターフェースの割り当て

マルチキャストサービスに割り当てられているスタティックインターフェースを表示するには、以下のようにします。

1. 「Multicast」 → 「IGMP Snooping」 → 「IGMP Member」を選択します。
2. 「Step」 リストで「Show Static Member」を選択します。
3. 該当の情報を表示する VLAN を選択します。

Multicast > IGMP Snooping > IGMP Member

Action: Show Static Member

VLAN: 1

IGMP Member Interface List Max: 1024 Total: 6

☐	Interface	Multicast IP
☐	Unit 1 / Port 1	224.1.1.1
☐	Unit 1 / Port 2	224.1.2.2
☐	Unit 1 / Port 3	230.1.1.1
☐	Trunk 2	230.1.2.2
☐	Trunk 5	239.1.1.1
☐	Unit 1 / Port 4	239.2.2.2

Delete Revert

画面 1-232 : マルチキャストサービスに割り当てられている
スタティックインターフェースの表示

すべてのマルチキャストグループに関する情報を表示するには、事前に IGMP スヌーピングまたはマルチキャストルーティングをスイッチで有効にする必要があります。マルチキャストサービスにスタティックまたは動的に割り当てられているすべてのインターフェースを表示するには、以下のようになります。

1. 「Multicast」 → 「IGMP Snooping」 → 「IGMP Member」を選択します。
2. 「Step」 リストで「Show Current Member」を選択します。
3. 該当の情報を表示する VLAN を選択します。

Multicast > IGMP Snooping > IGMP Member

Action: Show Current Member

VLAN: 1

IGMP Member Interface List Max: 1024 Total: 6

Interface	Multicast IP	Type
Unit 1 / Port 1	224.1.1.1	Dynamic
Unit 1 / Port 2	224.1.2.2	Static
Unit 1 / Port 3	230.1.1.1	Static
Trunk 2	230.1.2.2	Static
Trunk 5	239.1.1.1	Dynamic
Unit 1 / Port 4	239.2.2.2	Dynamic

画面 1-233 : マルチキャストサービスに割り当てられている 現行のインターフェースの表示

インターフェースごとの IGMP スヌーピングステータスの設定

「Multicast」 → 「IGMP Snooping」 → 「Interface」（Configure VLAN）を選択すると、VLAN インターフェースの IGMP スヌーピング属性を設定することができます。スヌーピングをグローバルで設定するには、「IGMP スヌーピングとクエリのパラメータの設定」を参照してください。

関連する CLI 情報

「IGMP Snooping」

コマンドの使用

マルチキャストルータ検出

マルチキャスト送信元データとグループメンバーシップレポートは、セグメント上のすべてのマルチキャストルータで受信される必要があります。クエリ抑止も実現するため、グループメンバーシッププロトコルクエリメッセージを使用してマルチキャストルータを検出するだけでは不十分です。そのため、MRD は、特定のマルチキャストルーティングプロトコルに依存せずにマルチキャストルータを特定するための標準的な方法を提供します。

【注意】 本製品では、MRD ドラフトで推奨されているデフォルト値が適用されています。

MRD では、以下の 3 つのメッセージタイプを使用してマルチキャストルータを検出します。

Web 設定

マルチキャストフィルタリング

- ・ マルチキャストルータアドバタイズメント - IP マルチキャスト転送が有効になっていることをアドバタイズするため、アドバタイズメントがルータによって送信されます。このメッセージは、マルチキャスト転送が有効になっているすべてのルータインターフェースで、要請がなくても定期的に送信されます。なお、このメッセージは、以下のイベントが発生したときにも送信されます。
 - ・ 定期（ライダム化）タイマーの期限切れ時
 - ・ ルータの起動プロセスの実行中
 - ・ マルチキャスト転送インターフェースの再起動中
 - ・ 要請メッセージの受信時
- ・ マルチキャストルータ要請 - デバイスが、マルチキャストルータからのアドバタイズメントメッセージを要請するため、要請メッセージを送信します。このメッセージを使用して、直接接続しているリンク上にあるマルチキャストルータが検出されます。また、要請メッセージは、マルチキャスト転送インターフェースが初期設定または再初期設定されるたびに送信されます。ルータは、IP マルチキャスト転送と MRD が有効になっているインターフェースで要請メッセージを受信すると、アドバタイズメントを送信して応答します。
- ・ マルチキャストルータ終端 - このメッセージは、以下のように、マルチキャストルータでインターフェースの IP マルチキャストルーティング機能が停止している場合に送信されます。
 - ・ マルチキャスト転送がインターフェースで無効になっている場合
 - ・ インターフェースが管理者によって無効にされている場合
 - ・ ルータが正常にシャットダウンされた場合

アドバタイズメントメッセージおよび終端メッセージは、All-Snoopers マルチキャストアドレスに送信されます。要請メッセージは、All-Routers マルチキャストアドレスに送信されます。

[注意] MRD メッセージは、IGMP スヌーピングまたは IGMP ルーティングが有効になっている VLAN 内のすべてのポートにフロードされます。MRD をサポートしていない古いスイッチもマルチキャストルータポートを学習できるようにするため、本製品は、Null 送信元アドレス (0.0.0.0) が含まれていない IGMP 一般クエリパケットを、接続している VLAN 内のすべてのポートにフロードします。Null 送信元アドレスが含まれている IGMP パケットは、システムがマルチキャストフラッディングモードで実行されている場合（例えば、新規 VLAN または新規ルータポートが作成中の場合や、スパンニングツリーの変更が発生した場合など）にのみ、VLAN 内のすべてのポートにフロードされます。それ以外の場合には、この種のパケットは、既知のマルチキャストルーティングポートのみに転送されます。

パラメータ

以下のパラメータが表示されます。

- ・ VLAN - 設定済み VLAN の ID（範囲：1 ～ 4,093）。
- ・ IGMP Snooping Status - このパラメータが有効になっている場合、スイッチは、指定された VLAN インターフェースにおけるネットワークトラフィックを監視して、どのホストがマルチキャストトラフィックの受信を希望しているかを判別します。これを IGMP スヌーピングと言います（デフォルト：Enable）。
IGMP スヌーピングがグローバルで有効になっている場合は、VLAN インターフェースごとの IGMP スヌーピング設定が優先されます。

IGMP スヌーピングがグローバルで無効になっている場合でも、個々の VLAN について IGMP スヌーピングを設定することはできますが、IGMP スヌーピングが再びグローバルで有効にならない限り、そのインターフェース設定は適用されません。

- ・ Version Exclusive – IGMP Version 属性で設定されている現行のバージョンと異なるバージョンが使用されている受信 IGMP メッセージ（ただし、マルチキャストプロトコルパケットに関するものを除く）を破棄します（デフォルト：Disabled）。

バージョンに基づく除外が VLAN で無効になっている場合、この設定は、「Multicast」→「IGMP Snooping」→「General」で表示される画面で設定されるグローバル設定に基づくものになります。バージョンに基づく除外が VLAN で有効になっている場合、この設定は、グローバル設定に優先します。

- ・ Immediate Leave Status – Leave パケットがマルチキャストサービスのメンバーポートで受信され、親 VLAN で immediate leave が有効になっている場合は、そのメンバーポートを即座に削除します（デフォルト：Disabled）。

immediate leave が使用されていない場合には、マルチキャストルータ（またはクエリア）は、IGMPv2 グループ脱退メッセージを受信すると、GS（Group Specific）クエリメッセージを送信します。ルータまたはクエリアは、指定されているタイムアウト期間内にクエリに対するホストからの応答がない場合にのみ、そのグループのトラフィックの転送を停止します。このタイムアウト期間は、「Last Member Query Interval x Robustness Variable（RFC 2236 に従い、2 に固定）」という計算式によって定義されます。

immediate leave が有効になっている場合、スイッチは、1 つのホストのみがインターフェースに接続しているものとみなします。したがって、immediate leave は、インターフェースが 1 つの IGMP 対応デバイス（サービスホストと IGMP スヌーピングを実行している隣接ホストのいずれか）のみに接続している場合に限り、有効にすることができます。

この属性は、IGMP スヌーピングが有効になっており、IGMPv2 スヌーピングが使用されている場合にのみ、適用されます。

- ・ Multicast Router Discovery – マルチキャストルータに接続しているインターフェースを検出するため、MRD が使用されます（デフォルト：Enabled）。
- ・ General Query Suppression – ダウンストリームマルチキャストホストに接続しているポート以外について、一般クエリを抑制します（デフォルト：Disabled）。デフォルトでは、一般クエリメッセージは、それらのメッセージの受信時に使用されるマルチキャストルータを除くすべてのポートにフロードされます。

一般クエリ抑制が有効になっている場合、一般クエリメッセージは、マルチキャストサービスに加入しているダウンストリームポートのみに転送されます。

- ・ Proxy Reporting – プロキシレポートによる IGMP スヌーピングを有効にします（デフォルト：グローバル設定に基づく値）。

このコマンドを使用してスイッチでプロキシレポートを有効にすると、Last leave とクエリ抑止を含め、（2006 年 4 月の DSL フォーラム TR-101 で規定されている）「プロキシレポートによる IGMP スヌーピング」が実行されます。

Last leave は、マルチキャストグループの最後のメンバーが脱退した場合にプロキシクエリを送信する機能です。クエリ抑止とは、特定のクエリがスイッチのアップストリームマルチキャストルータからダウンストリームホストに転送されないようにすることを意味します。

- ・ Interface Version – ネットワーク上の他のデバイスとの互換性を確保するため、プロトコルバージョンを設定します。これは、スイッチがスヌーピングレポートを送信するときに使用する IGMP バージョンです（範囲：1～3、デフォルト：2）。

この属性は、IGMP スヌーピングで使用される IGMP レポートまたはクエリのバージョンを指定します。バージョン 1～3 が、すべて、サポートされています。バージョン 2 と 3 は、使用されるスヌーピングのバージョンに関係なくスイッチが他のデバイスと連携できるように、下位互換性を確保するために用意されています。

- ・ Query Interval – IGMP プロキシ一般クエリの送信間隔（範囲：2～31,744 秒、デフォルト：125 秒）。
- ・ IGMP 一般メッセージは、この属性で指定される間隔でスイッチから送信されます。IGMP 一般メッセージがダウンストリームホストで受信されると、すべての受信先で、それらの受信先が加入しているマルチキャストグループに関する IGMP レポートが作成されます。

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または IGMP スヌーピングプロキシレポートが有効になっているときにプロキシホストとして機能している場合に適用されます。

- ・ Query Response Interval – 一般クエリに対する応答をシステムで待機する最大時間（範囲：1～31,74 秒、デフォルト：10 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または IGMP スヌーピングプロキシレポートが有効になっているときにプロキシホストとして機能している場合に適用されます。

- ・ Last Member Query Interval – GS または GSS クエリメッセージに対する応答を待機する期間（範囲：1～31,744（1/10 秒単位かつ 10 の倍数）、デフォルト：1 秒）。

マルチキャストホストは、グループを脱退すると、IGMP 脱退メッセージを送信します。スイッチは、脱退メッセージを受信すると、IGMP GS または IGMP GSS クエリメッセージを送信することにより、そのホストがグループの最後のメンバーであるかどうかをチェックし、タイマーをスタートさせます。タイマーに設定されている時間が経過するまでにレポートが受信されない場合には、グループのレコードが削除され、レポートがアップストリームマルチキャストルータに送信されます。

この値を減らすと、グループまたは送信元の最後のメンバーが脱退したことを検出するための時間を短縮することができますが、バーストラフィックが発生する可能性が高くなります。

この属性は、IGMP スヌーピングプロキシレポートが有効になっている場合にのみ、適用されます。

- ・ Last Member Query Count – IGMP GS または IGMP GSS クエリメッセージの数であり、この数を超えると、システムは、ローカルメンバーが存在しなくなったものとみなします（範囲：1～255、デフォルト：2）。

この属性は、IGMP スヌーピングプロキシレポートまたは IGMP クエリアが有効になっている場合にのみ、適用されます。

- ・ Proxy Query Address – IGMP プロキシレポートで使用するためにローカルで生成されるクエリメッセージとレポートメッセージのスタティック送信元アドレス（範囲：任意の有効な IP ユニキャストアドレス、デフォルト：0.0.0.0）。

IGMP スヌーピングでは、選択されたクエリアではないことを示すためにダウンストリームホストに送信される IGMP クエリメッセージの送信元に Null の IP アドレス（0.0.0.0）が使用されますが、RFC 4541 に従い、それらのメッセージはプロキシ経由でのみ送信されます。また、本製品では、アップストリームポートに送信される IGMP レポートにも Null アドレスが使用されます。

多くのホストでは、RFC 4541 が実装されていないため、0.0.0.0 という送信元アドレスのクエリメッセージは認識されません。したがって、それらのホストは、クエリに応

答せず、その結果、マルチキャストルータは、それらのホストへのトラフィックの送信を停止します。

この問題を解決するため、プロキシ経由で送信される IGMP クエリメッセージに含まれる送信元アドレスを任意の有効なユニキャストアドレス（ルータ自体のアドレス以外のアドレス）に置き換えることができます。

Web インターフェース

IGMP スヌーピングを VLAN で設定するには、以下のようにします。

- (1) 「Multicast」→「IGMP Snooping」→「Interface」を選択します。
- (2) 「Step」リストで「Configure VLAN」を選択します。
- (3) VLAN を選択して必要なパラメータを設定および更新します。
- (4) < Apply > ボタンをクリックします。

The screenshot shows the 'Multicast > IGMP Snooping > Interface' configuration page. At the top, the 'Action' dropdown is set to 'Configure VLAN'. Below this, various settings for VLAN 1 are displayed:

- VLAN:** 1
- IGMP Snooping Status:** ☒ Enabled
- Version Exclusive:** ☐ Enabled
- Immediate Leave Status:** ☐ Enabled
- Multicast Router Discovery:** ☐ Enabled
- General Query Suppression:** ☐ Enabled
- Proxy Reporting:** Disabled
- Interface Version (1-3):** 2
- Query Interval (2-31744):** 125 seconds
- Query Response Interval (10-31740):** 100 (1/10 seconds, multiple of 10)
- Last Member Query Interval (1-31744):** 10 (1/10 seconds, multiple of 10)
- Last Member Query Count (1-255):** 2
- Proxy (Query) Address:** 0.0.0.0

At the bottom right, there are 'Apply' and 'Revert' buttons.

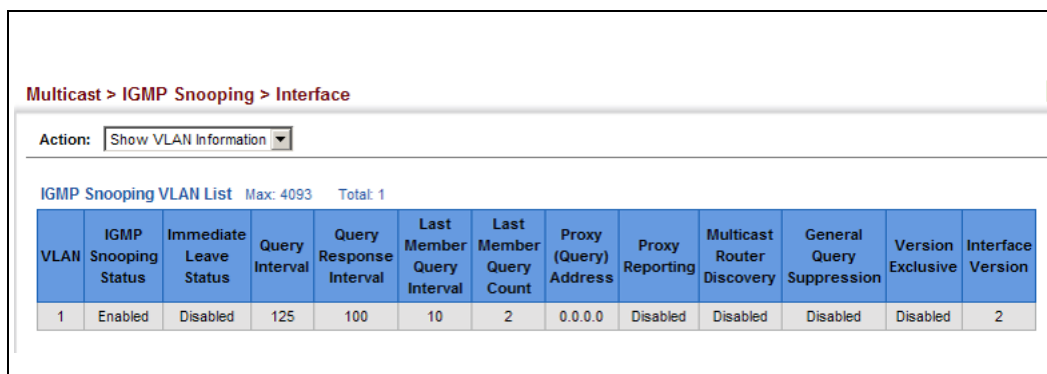
画面 1-234 : インターフェースの IGMP スヌーピングの設定

Web 設定

マルチキャストフィルタリング

インターフェースの IGMP スヌーピング設定を表示するには、以下のようにします。

1. 「Multicast」 → 「IGMP Snooping」 → 「Interface」 を選択します。
2. 「Step」 リストで 「Show VLAN Information」 を選択します。



Action: Show VLAN Information												
IGMP Snooping VLAN List Max: 4093 Total: 1												
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	125	100	10	2	0.0.0.0	Disabled	Disabled	Disabled	Disabled	2

画面 1-235 : インターフェースの IGMP スヌーピング設定の表示

IGMP クエリパケットとマルチキャストデータのフィルタリング

「Multicast」 → 「IGMP Snooping」 → 「Interface」 (Configure Port/Trunk) を選択すると、IGMP クエリパケットまたは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ーフェースを設定することができます。

関連する CLI 情報

「ip igmp query-drop」

「ip multicast-data-drop」

パラメータ

以下のパラメータが表示されます。

- ・ IGMP Query Drop - 受信するあらゆる IGMP クエリパケットをドロップするようにインターフェースを指定して設定します。スイッチがクエリアとして機能している場合は、そのようにすることで、スイッチが他のクエリアから受信するメッセージに影響されないようになります。
- ・ Multicast Data Drop - 接続しているユーザにマルチキャストサービスを転送しないようにダウンストリームポート（つまり、このコマンドで指定するインターフェース）を設定します。

Web インターフェース

IGMP クエリパケットまたはマルチキャストデータパケットがドロップされるようにするには、以下のようにします。

- (1) 「Multicast」 → 「IGMP Snooping」 → 「Interface」 を選択します。
- (2) 「Step」 リストで 「Configure Port」 または 「Configure Trunk」 を選択します。
- (3) いずれかのインターフェースについて必要なドロップ機能を有効にします。

(4) < Apply > ボタンをクリックします。

Multicast > IGMP Snooping > Interface

Action: Configure Port

Port List Max: 26 Total: 26

Port	IGMP Query Drop	Multicast Data Drop
1	☐ Enabled	☐ Enabled
2	☐ Enabled	☐ Enabled
3	☐ Enabled	☐ Enabled
4	☐ Enabled	☐ Enabled
5	☐ Enabled	☐ Enabled

画面 1-236 :IGMP クエリパケットまたはマルチキャストデータパケットのドロップ

IGMP スヌーピングによって検出されたマルチキャストグループの表示

「Multicast」→「IGMP Snooping」→「Forwarding Entry」を選択すると、IGMP スヌーピングによって学習された転送エントリを表示することができます。

関連する CLI 情報

「show ip igmp snooping group」

コマンドの使用

すべてのマルチキャストグループに関する情報を表示するには、事前に IGMP スヌーピングをスイッチで有効にする必要があります。

パラメータ

以下のパラメータが表示されます。

- ・ VLAN – 指定されたマルチキャストグループアドレスのダウンストリームポートにトラフィックを転送しているスイッチのインターフェース。
- ・ Group Address – スイッチに直接接続しているサブスクライバまたはスイッチのダウンストリームのサブスクライバを含んでいる IP マルチキャストグループのアドレス、あるいは、インターフェースに割り当てられているスタティックマルチキャストグループのアドレス。
- ・ Source Address – 指定されたグループにトラフィックを送信しているマルチキャストサーバの 1 つのアドレス。
- ・ 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。このフィールドには、動的に設定されたマルチキャストルータポートと静的に設定されたマルチキャストルータポートのどちらも表示されます。

Web 設定

マルチキャストフィルタリング

Web インターフェース

IGMP スヌーピングによって学習されたマルチキャストグループを表示するには、以下のようになります。

- (1) 「Multicast」 → 「IGMP Snooping」 → 「Forwarding Entry」 を選択します。
- (2) 該当の情報を表示する VLAN を選択します。

Multicast > IGMP Snooping > Forwarding Entry

VLAN

IGMP Snooping Forwarding Entry List Max: 1024 Total: 9

Group Address	Source Address	Interface
224.1.1.1	10.1.1.1	Unit 1 / Port 4
224.1.1.1	10.1.1.1	Unit 1 / Port 5
224.1.1.1	10.1.1.1	Trunk 3
224.1.1.1	10.1.1.1	Trunk 8
224.1.1.2	10.1.1.1	Unit 1 / Port 3
224.1.2.1	10.1.1.1	Unit 1 / Port 5
224.1.2.1	10.1.1.1	Unit 1 / Port 7
224.3.1.1	10.1.1.1	Trunk 2
224.3.1.2	10.1.1.1	Trunk 5

画面 1-237 :IGMP スヌーピングによって学習されたマルチキャストグループの表示

1.13.4 IGMP グループの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、エンドユーザが使用できるマルチキャストサービスを管理者が制御することが必要な場合もあります。そのような例として、特定の加入プランに基づく IP/TV サービスが挙げられます。IGMP フィルタリング機能を使用すれば、スイッチポートで所定の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、そのような要件を満たすことができます。また、IGMP スロットリング機能によってポートが同時に加入できるマルチキャストグループの数を制限することもできます。

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プロファイルスイッチポートに割り当てることができるようになります。IGMP フィルタプロファイルには、1つまたは複数のアドレスあるいは特定の範囲のマルチキャストアドレスを含めることができますが、1つのポートに割り当てることができるプロファイルは1つだけです。IGMP フィルタリングが有効になっている場合、ポートで受信される IGMP 加入レポートがフィルタプロファイルと照らし合わせてチェックされます。要求されたマルチキャストグループが許可される場合は、IGMP 加入レポートが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る場合は、IGMP 加入レポートがドロップされます。

IGMP スロットリングでは、ポートが同時に加入できるマルチキャストグループの最大数が設定されます。スイッチでは、ポートにおけるグループの最大数に達した場合に2つのアクションのうちの1つ（「拒否」と「置換」のどちらか）を実行することができます。アクションが「拒否」に設定されている場合には、新規の IGMP 加入レポートはドロップされます。アクションが「置換」に設定されている場合には、既存のグループがランダムに削除されて新規のマルチキャストグループに置き換えられます。

IGMP フィルタリングと IGMP スロットリングの有効化

「Multicast」→「IGMP Snooping」→「Filter」（Configure General）を選択すると、スイッチで 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することができます。

関連する CLI 情報

「ip igmp filter (Global Configuration)」

パラメータ

以下のパラメータが表示されます。

- ・ IGMP Filter Status - スwitchの IGMP フィルタリングと IGMP スロットリングをグローバルで有効にします（デフォルト：Disabled）。

Web インターフェース

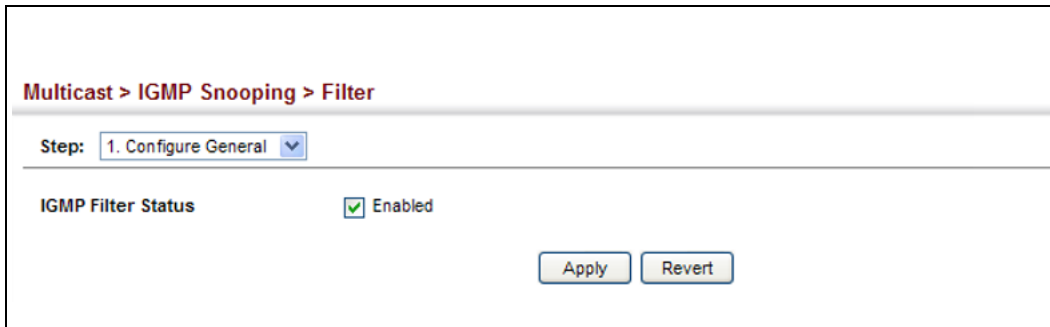
スイッチで IGMP フィルタリングと IGMP スロットリングを有効にするには、以下のようになります。

- (1) 「Multicast」→「IGMP Snooping」→「Filter」を選択します。
- (2) 「Step」リストで「Configure General」を選択します。
- (3) 「IGMP Filter Status」を有効にします。

Web 設定

マルチキャストフィルタリング

(4) < Apply > ボタンをクリックします。



画面 1-238 :IGMP フィルタリングと IGMP スロットリングの有効化

IGMP フィルタリングプロファイルの設定

「Multicast」→「IGMP Snooping」→「Filter」(Add) を選択すると、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ことができます。それから、「Step」リストで「Add Multicast Group Range」を選択すると表示される画面で、フィルタリングするマルチキャストグループを指定します。

関連する CLI 情報

「IGMP Filtering and Throttling」

コマンドの使用

開始 IP アドレスと終了 IP アドレスを入力して特定の範囲のマルチキャストグループを指定するか、範囲の開始 IP アドレスと終了 IP アドレスに同じ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します。

パラメータ

以下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 ~ 4,294,967,295)。

Access Mode - プロファイルのアクセスモードとして、「Permit」と「Deny」のどちらかを設定します (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は、マルチキャストグループが制御対象の範囲に該当すると、IGMP 加入レポートが処理されます。

アクセスモードが「Deny」に設定されている場合は、マルチキャストグループが制御対象の範囲に該当しないときにのみ、IGMP 加入レポートが処理されます。

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 - 特定の範囲のマルチキャストグループの開始アドレスを指定します。

End Multicast IP Address - 特定の範囲のマルチキャストグループの終了アドレスを指定します。

Web インターフェース

IGMP フィルタプロファイルを作成してそのアクセスモードを設定するには、以下のようになります。

- (1) 「Multicast」 → 「IGMP Snooping」 → 「Filter」 を選択します。
- (2) 「Step」 リストで 「Configure Profile」 を選択します。
- (3) 「Step」 リストで 「Add」 を選択します。
- (4) プロファイルの番号を入力し、そのアクセスモードを設定します。
- (5) < Apply > ボタンをクリックします。

Multicast > IGMP Snooping > Filter

Step: 2. Configure Profile Action: Add

Profile ID (1-4294967295) 19

Access Mode Permit

Apply Revert

画面 1-239 :IGMP フィルタリングプロファイルの作成

IGMP フィルタリングプロファイルを表示するには、以下のようになります。

1. 「Multicast」 → 「IGMP Snooping」 → 「Filter」 を選択します。
2. 「Step」 リストで 「Configure Profile」 を選択します。
3. 「Step」 リストで 「Show」 を選択します。

Multicast > IGMP Snooping > Filter

Step: 2. Configure Profile Action: Show

IGMP Snooping Filter Profile List Max: 480 Total: 1

	Profile ID	Action Mode
☐	19	Permit

Delete Revert

画面 1-240 : 作成されている IGMP フィルタリングプロファイルの表示

Web 設定

マルチキャストフィルタリング

特定の範囲のマルチキャストグループを IGMP フィルタリングプロファイルに追加するには、以下のようにします。

- (1) 「Multicast」 → 「IGMP Snooping」 → 「Filter」 を選択します。
- (2) 「Step」 リストで 「Configure Profile」 を選択します。
- (3) 「Step」 リストで 「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のアドレスまたはアドレス範囲を追加します。
- (5) < Apply > ボタンをクリックします。

Multicast > IGMP Snooping > Filter

Step: 2. Configure Profile Action: Add Multicast Group Range

Profile ID 19

Start Multicast IP Address 239.2.3.1

End Multicast IP Address 239.2.3.200

Apply Revert

画面 1-241 :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 フィルタリングプロファイルについて設定されているマルチキャストグループを表示するには、以下のようにします。

1. 「Multicast」 → 「IGMP Snooping」 → 「Filter」 を選択します。
2. 「Step」 リストで 「Configure Profile」 を選択します。
3. 「Step」 リストで 「Show Multicast Group Range」 を選択します。
4. 該当の情報を表示するプロファイルを選択します。

Multicast > IGMP Snooping > Filter

Step: 2. Configure Profile Action: Show Multicast Group Range

Profile ID 19

Multicast IP Address Range List Max: 1024 Total: 1

	Start Multicast IP Address	End Multicast IP Address
☐	239.2.3.1	239.2.3.200

Delete Revert

画面 1-242 :IGMP フィルタリングプロファイルに割り当てられている

マルチキャストグループの表示

インターフェースの IGMP フィルタリングと IGMP スロットリングの設定

「Multicast」→「IGMP Snooping」→「Filter」（Configure Interface）を選択すると、IGMP フィルタリングプロファイルをスイッチのインターフェースに割り当てることや、インターフェースが同時に加入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がスロットリングされるようにすることができます。

関連する CLI 情報

「IGMP Filtering and Throttling」

コマンドの使用

- ・ IGMP スロットリングでは、ポートが同時に加入できるマルチキャストグループの最大数が設定されます。スイッチでは、ポートにおけるグループの最大数に達した場合に 2 つのアクションのうちの 1 つ（「拒否」と「置換」のどちらか）を実行することができます。アクションが「拒否」に設定されている場合には、新規の IGMP 加入レポートはドロップされます。アクションが「置換」に設定されている場合には、既存のグループがランダムに削除されて新規のマルチキャストグループに置き換えられます。

パラメータ

以下のパラメータが表示されます。

- ・ Interface – ポート ID またはトランク ID。
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することができます。ポートがトランクメンバーとして設定されている場合、トランクでは、トランク内の最初のポートメンバーに適用される設定が使用されます。
- ・ Profile ID – インターフェースに割り当てる既存のプロファイルを選択します。
- ・ Max Multicast Groups – インターフェースが同時に加入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 ～ 1,024、デフォルト：1,024）。
- ・ Current Multicast Groups – インターフェースが加入している現在のマルチキャストグループが表示されます。
- ・ Throttling Action Mode – インターフェースのマルチキャストグループの最大数を超えた場合に実行されるアクションを設定します（デフォルト：Deny）。
 - ・ Deny – 新規のマルチキャストグループ加入レポートがドロップされます。
 - ・ Replace – 新規のマルチキャストグループによって既存のグループが置き換えられます。
- ・ Throttling Status – スロットリングアクションがインターフェースに実装されているかどうかを示します（オプション：True または False）。

Web インターフェース

ポートまたはトランクの IGMP フィルタリングや IGMP スロットリングを設定するには、以下のようになります。

- (1) 「Multicast」→「IGMP Snooping」→「Filter」を選択します。
- (2) 「Step」リストで「Configure Interface」を選択します。
- (3) インターフェースに割り当てるプロファイルを選択し、許可されるマルチキャストグループの最大数を設定して、スロットリングアクションを設定します。

(4) < Apply > ボタンをクリックします。

Multicast > IGMP Snooping > Filter

Step: 3. Configure Interface ▼

Interface ☒ Port ☐ Trunk

IGMP Filter and Throttling Port List Max: 26 Total: 26 1 2 3

Port	Profile ID	Max Multicast Groups (1-1024)	Current Multicast Groups	Throttling Action Mode	Throttling Status
1	19 ▼	64	0	Deny ▼	False
2	(none) ▼	1024	0	Deny ▼	False
3	(none) ▼	1024	0	Deny ▼	False
4	(none) ▼	1024	0	Deny ▼	False
5	(none) ▼	1024	0	Deny ▼	False

画面 1-243 : インターフェースの IGMP フィルタリングと
IGMP スロットリングの設定

1.13.5 レイヤ 3 の IGMP（マルチキャストルーティングと共に使用されるクエリ）

IGMP Snooping - IGMP スヌーピングは、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一連の機能の中核を成しています。マルチキャストクライアントからの IGMP サービス要求をパッシブに監視するため、また、マルチキャストトラフィックを転送する必要があるスイッチポートを動的に設定するために使用されます。

IGMP Query - マルチキャストクエリは、既知のマルチキャストグループをそれぞれポーリングしてアクティブなメンバーを確認するため、また、マルチキャストトラフィックを転送する必要があるスイッチポートを動的に設定するために使用されます。以降で説明するように、レイヤ 3 の IGMP クエリは、レイヤ 2 の IGMP スヌーピングと IGMP マルチキャストルーティングの両方と併せて使用されます。

IGMP - このプロトコルには、特にマルチキャストルーティングと連携するように設計されたマルチキャストクエリのフォームが組み込まれています。ルータは、ホストに対し、マルチキャストトラフィックの受信を希望するかどうかを定期的に問い合わせます。ホストは、自らが引き続きマルチキャストサービスを受けられるようにするため、サービス要求をアップストリームマルチキャストルータに伝搬します。IGMP は、VLAN インターフェースごとに有効にすることができます。

[注意] : MRD プロトコルを使用して、マルチキャストルータに接続しているインターフェースが検出されます（このプロトコルの説明については、「マルチキャストルータ検出」を参照）。

IGMP Proxy - デバイスは、ダウンストリームインターフェースに接続しているホストのマルチキャストサービス要件を学習し、そのグループメンバーシップ情報をアップストリームルータにプロキシ経由で送信して、その情報に基づいてマルチキャストパケットが転送されるようにすることができます。

IGMP プロキシルーティングの設定

「Multicast」→「IGMP」→「Proxy」を選択すると、IGMP プロキシルーティングを設定することができます。

簡易なネットワークポロジでは、デバイスがダウンストリームインターフェースのマルチキャスト要件を学習してそのメンバーシップ情報をアップストリームルータにプロキシ経由で送信するだけで十分です。そのようにすれば、その情報のみに基づいて、マルチキャストパケットをダウンストリームに転送されるようにすることができます。このメカニズムをIGMP プロキシルーティングと言います。本システムでIGMP プロキシルーティングを使用すると、標準のIGMP インターフェースによって検出されたホストに代わってIGMP ホストメッセージを発行できるようになります。

関連する CLI 情報

「IGMP Proxy Routing」

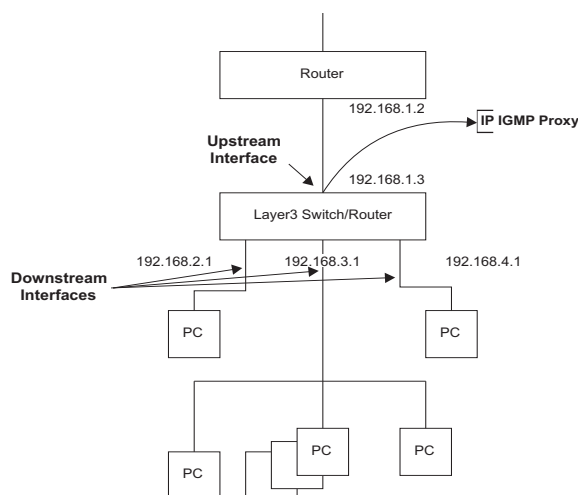


図 1-18:IGMP プロキシルーティング

IGMP プロキシルーティングを使用してエッジスイッチでマルチキャストトラフィックを転送すると、PIMのような比較的複雑なマルチキャストプロトコルを実行しなくても済むようになるので、エッジスイッチの処理負荷が大幅に軽減されます。また、プロキシデバイスがコアルータで使用されるマルチキャストルーティングプロトコルに依存すること也不再行します。

IGMP プロキシルーティングでは、(上記の図でインターネットに接続するアップストリームインターフェースのように) ツリーのルートがマルチキャストインフラストラクチャ全体に接続するツリートポロジを使用します。そのように簡易なトロポジでは、学習したグループメンバーシップ情報をアップストリームに送信し、その情報に基づいてマルチキャストパケットがダウンストリームホストに転送されるようにするだけで十分です。本製品の場合、IGMP プロキシルーティングによって、コアネットワーク側へのアップストリーム接続が1つだけ確立され、顧客側へのダウンストリーム接続が、複数、確立されます。

IGMP プロキシルーティングツリーは、各プロキシデバイスでアップストリームインターフェースを1つとダウンストリームインターフェースを複数指定して、手動で設定する必要があります。プロキシデバイス以外の他のマルチキャストルータがツリー内には存在しては

ならず、ツリーのルートは、より大規模なマルチキャストインフラストラクチャに接続していなければなりません。IGMP は単一の管理ドメインの場合にのみ使用できるという点に注意してください。

トポロジがツリー型ではない複雑なシナリオ（例えば、複数の送信元に接続する多様なパスがある場合など）では、より堅牢なフェイルオーバーメカニズムを使用する必要があります。複数の管理ドメインが関連する場合には、IGMP プロキシではなく、マルチキャストルーティングプロトコルを使用してください。

IGMP プロキシサービスを有効にするには、以下の手順を実行します。

1. ルータで IP マルチキャストリングをグローバルに有効にします（「マルチキャストルーティングのグローバル設定の設定」を参照）。
2. プロキシマルチキャストサービスを必要とするダウンストリームインターフェースで IGMP を有効にします（「IGMP インターフェースパラメータの設定」を参照）。
3. アップストリームマルチキャストルータに接続しているインターフェースで、このセクションで紹介されているプロキシ設定を使用して、IGMP プロキシを有効にします。
4. （任意指定）このセクションで以降に記載されている説明に従って、「Multicast」→「IGMP」→「Proxy」を選択すると表示される画面で、非要請レポートをアップストリームルータに送信する頻度を指定します。

コマンドの使用

- ・ IGMP プロキシをインターフェースで有効にすると、そのインターフェースがアップストリームインターフェース（ホストインターフェース）として認識されます。このインターフェースでは、IGMP メンバーシップレポートを送信することによって、IGMP のホスト部分の機能のみを実行します。そのため、自動的に IGMP ルータ機能が無効になります。
- ・ IGMP が有効になっているがマルチキャストツリーのルート方向に位置していないインターフェースは、ダウンストリームインターフェース（ルータインターフェース）として認識されます。このインターフェースは、自らが保有しているすべての IGMP サブスクライバのデータベースを保守することによって、標準の IGMP ルータ機能を実行します。そのため、プロキシマルチキャストサービスを必要とするすべてのインターフェースで IGMP を有効にする必要があります。
- ・ 本システムでは、定期的にマルチキャストルートテーブルの ASM（Any-Source Multicast）（*G）転送エントリがチェックされます。ダウンストリーム IGMP グループに関する変更が発生すると、IGMP 状態変更レポートが作成されて、アップストリームルータに送信されます。
- ・ アップストリームネットワーク上に IGMPv1 クエリアまたは IGMPv2 クエリアがある場合、プロキシデバイスは、アップストリームインターフェースで IGMPv1 ホストまたは IGMPv2 ホストとして機能し、VLAN 内にアクティブな IGMPv1 クエリアまたは IGMPv2 クエリアが存在していることを示すため、v1/v2 クエリア存在確認タイマーを設定します。アップストリームネットワーク上に IGMPv1 クエリアまたは IGMPv2 クエリアがない場合、プロキシデバイスは IGMPv3 ホストとして機能します。
- ・ マルチキャストルーティングプロトコルは、IGMP プロキシサービスが有効になっている場合はサポートされません。
- ・ 本システムでサポートされるアップストリームインターフェースは1つだけです。

- ・ サポートされるマルチキャストエントリの最大数は 1,024 です。

パラメータ

以下のパラメータが表示されます。

- ・ VLAN – IGMP プロキシサービスを設定する VLAN インターフェース（範囲：1 ～ 4,093）。
- ・ IGMP Proxy Status – マルチキャストルーティングの IGMP プロキシサービスを有効にして、ダウンストリームインターフェースで監視される IGMP メンバーシップ情報が要約レポートで示されるアップストリームインターフェースに転送されるようにします（デフォルト：Disabled）。
- ・ Unsolicited Report Interval – アップストリームインターフェースで非要請 IGMP レポートを送信する間隔を指定します（範囲：1 ～ 65,535 秒、デフォルト：400 秒）。

Web インターフェース

IGMP プロキシルーティングを設定するには、以下のようになります。

- (1) 「Multicast」 → 「IGMP」 → 「Proxy」 を選択します。
- (2) アップストリームインターフェースを選択して、「IGMP Proxy Status」を有効にし、必要に応じて非要請 IGMP レポートの送信間隔を変更します。
- (3) < Apply > ボタンをクリックします。

The screenshot shows the 'Multicast > IGMP > Proxy' configuration page. It contains three settings: 'VLAN' set to 1, 'IGMP Proxy Status' checked and labeled 'Enabled', and 'Unsolicited Report Interval (1-65535)' set to 400 seconds. At the bottom right are 'Apply' and 'Revert' buttons.

Multicast > IGMP > Proxy	
VLAN	1
IGMP Proxy Status	☒ Enabled
Unsolicited Report Interval (1-65535)	400 seconds
Apply Revert	

画面 1-244 :IGMP プロキシルーティングの設定

IGMP インターフェースパラメータの設定

「Multicast」→「IGMP」→「Interface」を選択すると、IGMP のインターフェース設定を設定することができます。

本製品では、IGMP (Internet Group Management Protocol) を使用して、接続しているホストに対し、特定のマルチキャストサービスを受けることを希望するかどうかを問い合わせます。ホストからは、いくつかのタイプの IP マルチキャストメッセージが応答として返されます。ホストは、加入を希望するグループまたは既に加入しているグループを示すレポートメッセージを送信してクエリに応答します。ルータは、指定されている期間内にレポートメッセージを受信できない場合には、そのインターフェースをマルチキャストツリーから除外します。また、ホストは、ルータからのクエリを待たずに、随時、加入メッセージを送信することができます。さらに、ホストは、特定のグループについてトラフィックを受信する必要がなくなった場合は、グループ脱退メッセージを送信して通知することができます。

LAN 上に IP マルチキャストを実行する複数のルータがある場合には、それらの 1 つが「クエリア」として選択され、グループメンバーを問い合わせる役割を果たします。ホストは、自らが引き続きマルチキャストサービスを受けられるようにするため、サービス要求を、隣接するマルチキャストルータに伝搬します。このセクションで紹介しているパラメータは、レイヤ 3 の IGMP 機能とクエリ機能を制御するために使用します。

[注意] :IGMP Protocol Status」は、(このセクションの説明に従って) ダウンストリームマルチキャストホストをサポートする必要があるすべてのインターフェースで有効にしなければなりません。

[注意] :IGMP は、マルチキャストルーティングが無効になっている場合は、無効になります (「グローバルでのマルチキャストルーティングの有効化」を参照)。

関連する CLI 情報

「IGMP (Layer 3)」

パラメータ

以下のパラメータが表示されます。

- ・ VLAN – プライマリ IP アドレスにバインドされている VLAN インターフェース (範囲: 1 ~ 4,093)。
- ・ IGMP Protocol Status – (IGMP クエリ機能を含めて) IGMP を VLAN インターフェースで有効にします (デフォルト: Disabled)。
- ・ PIM などのマルチキャストルーティングプロトコルが有効になっている場合は、IGMP も有効になります。
- ・ IGMP Version – インターフェースで使用する IGMP バージョンを設定します (オプション: Version 1 ~ 3、デフォルト: Version 2)。
- ・ Robustness Variable – インターフェースの信頼性 (パケット損失の期待値) を指定します。この信頼性の値は、「Group Membership Interval」、「Other Querier Present Interval」、「Startup Query Count」(RFC 2236) など、他の IGMP 変数の適性範囲を求めるときに使用されます (範囲: 1 ~ 255、デフォルト: 2)。

ルータでは、最新の受信クエリから取得される信頼性値 f が採用されます。クエリアの信頼性値 (QRV: Querier's Robustness Variable) が 0 の場合は、QRV フィールドで信頼性値が宣言されていないことを意味し、信頼性変数は、このコマンドによって静的に設定される値に設定されます。QRV は、7 (QRV フィールドの最大値) よりも大

きい場合には、0 に設定されます。値 0 は、以降に送信されるクエリメッセージでは QRV がアダプタイズされないことを意味します。

- ・ Query Interval – ホストクエリメッセージの送信間隔を指定します（範囲：1 ～ 255 秒、デフォルト：125 秒）。

マルチキャストルータは、特定のマルチキャストサービスを要求しているダウンストリームホストに接続しているインターフェースを判別するため、ホストクエリメッセージを送信します。ホストクエリメッセージを送信するのは、サブネットの代表マルチキャストルータのみです。ホストクエリメッセージは、マルチキャストアドレス 224.0.0.1 宛に、TTL（Time-To-Live）値 1 を使用して送信されます。

IGMPv1 の場合、代表ルータは、LAN で実行されているマルチキャストルーティングプロトコルに応じて選択されます。一方、IGMPv2 および IGMPv3 の場合には、サブネットで IP アドレスが最も小さいマルチキャストルータが代表クエリアになります。

- ・ Query Max Response Time – IGMP クエリでアダプタイズされる最大応答時間を指定します（範囲：0 ～ 255（1/10 秒単位）、デフォルト：10 秒）。

IGMPv1 の場合、クエリメッセージの最大応答時間は、指定不可であり、10 秒に固定されます。

「Query Max Response Time」の値を変更することにより、サブネットで渡される IGMP メッセージのバースト性を調整することができます。値が大きいほど、応答間隔が長くなるのでホスト応答の到達範囲が広がるため、トラフィックでバーストが発生する可能性は低くなります。

最大応答時間の値は、「Query Interval」よりも小さくしなければなりません。

- ・ Last Member Query Interval – IGMP GS または IGMPv3 GSS 脱退メッセージが受信されたかどうかに関係なく IGMP GS または IGMPv3 GSS クエリメッセージが送信される間隔（範囲：1 ～ 255（1/10 秒単位）、デフォルト：1 秒）。

スイッチは、マルチキャストグループ、送信元、またはチャネルから脱退するホストから IGMPv2 または IGMPv3 脱退メッセージを受信すると、「Last Member Query Count」で指定されている数の GS または GSS クエリメッセージをこの「Last Member Query Interval」で指定されている間隔で送信します。この間隔よりも長い間、応答がスイッチで受信されない場合、グループ、送信元、またはチャネルのトラフィックの転送が停止されます。

- ・ Querier – 現在、マルチキャストサービスの IGMP クエリアとして機能しているデバイス。クエリアは、IGMP マルチキャストリングが有効になっており、このエントリの VLAN が Up 状態であり、有効な IP アドレスを指定して設定されている場合にのみ、表示されます。

Web インターフェース

IGMP インターフェース設定を設定するには、以下のようになります。

- (1) 「Multicast」→「IGMP」→「Interface」を選択します。
- (2) IGMP（レイヤ 3）をサポートするインターフェースをそれぞれ選択して、必要な IGMP パラメータを設定します。

Web 設定

マルチキャストフィルタリング

(3) < Apply > ボタンをクリックします。

Multicast > IGMP > Interface

VLAN	1
IGMP Protocol Status	☒ Enabled
IGMP Version (1-3)	2
Robustness Variable (1-255)	1
Query Interval (1-255)	125 seconds
Query Max Response Time (0-255)	100 * 0.1 seconds
Last Member Query Interval (1-255)	10 * 0.1 seconds
Querier	192.168.1.254

Apply Revert

画面 1-245 :IGMP インターフェース設定の設定

スタティック IGMP グループメンバーシップの設定

「Multicast」→「IGMP」→「Static Group」を選択すると、個々のマルチキャストグループからのトラフィックが指定の VLAN インターフェースに伝搬されるように手動で設定することができます。

関連する CLI 情報

「ip igmp static-group」

コマンドの使用

- ・ マルチキャストグループアドレスの全範囲内のグループアドレスを指定することができます。ただし、SSM (Source-Specific Multicast) アドレス範囲 (デフォルトは 232/8) 内のアドレスが指定されているが、送信元アドレスがコマンドに含まれていない場合、逆方向パスツリー内の次のノードで該当のグループが特定の送信元アドレスに静的にマップされていない限り、マルチキャストグループ加入要求は失敗します。また、SSM アドレス範囲外のアドレスが指定されており、特定の送信元アドレスがコマンドに含まれている場合、逆方向パスツリー内の次のノードで PIMSSM プロトコルが有効になっていると、やはり、マルチキャストグループ加入要求が失敗します。
- ・ ASM (*,G) のためのスタティックグループを設定すると、以降は、該当のエントリを削除しない限り、そのグループについて送信元アドレスを定義することができなくなります。
- ・ 1 つまたは複数の SSM (S,G) についてスタティックグループを設定すると、以降は、関連付けられている SSM (S,G) エントリをすべて削除しない限り、そのグループについて ASM (*,G) を定義することができなくなります。
- ・ 本製品は最大 64 のスタティックグループエントリをサポートします。

パラメータ

以下のパラメータが表示されます。

- ・ VLAN – 指定するマルチキャストグループのスタティックメンバーとして割り当てる VLAN インターフェイス（範囲：1 ～ 4,093）。
- ・ Static Group Address – IP マルチキャストグループアドレス（224.0.0.1 ～ 239.255.255.255 の範囲内のグループアドレスを指定することはできません）。
- ・ Source Address – 指定されたグループにトラフィックを送信しているマルチキャストサーバの送信元アドレス。

Web インターフェース

スタティック IGMP グループを設定するには、以下のようにします。

- (1) 「Multicast」 → 「IGMP」 → 「Static Group」 を選択します。
- (2) 「Step」 リストで 「Add」 を選択します。
- (3) スタティックマルチキャストグループのメンバーとして割り当てる VLAN インターフェースを選択し、マルチキャストグループを指定します。SSM が、指定したマルチキャストグループの逆方向パスツリー内のネクストホップルータでサポートされている場合には、送信元アドレスも指定してください。
- (4) < Apply > ボタンをクリックします。

The screenshot shows the 'Multicast > IGMP > Static Group' configuration page. At the top, there is a breadcrumb trail 'Multicast > IGMP > Static Group'. Below it, the 'Action:' dropdown is set to 'Add'. The 'VLAN' dropdown is set to '1'. The 'Static Group Address' text box contains '239.2.3.1'. The 'Source Address' text box contains '192.168.1.200' with '(optional)' text to its right. At the bottom right, there are 'Apply' and 'Revert' buttons.

画面 1-246 : スタティック IGMP グループの設定

設定されているスタティック IGMP グループを表示するには、以下のようにします。

1. 「Multicast」 → 「IGMP」 → 「Static Group」 を選択します。
2. 「Step」 リストで 「Show」 を選択します。

Web 設定

マルチキャストフィルタリング

3. < Apply > ボタンをクリックします。

Multicast > IGMP > Static Group

Action: Show

VLAN 1

IGMP Static Group List Max: 64 Total: 1

☐	Static Group Address	Source Address
☐	239.2.3.1	192.168.1.200

Apply Revert

画面 1-247 : スタティック IGMP グループの表示

マルチキャストグループに関する情報の表示

IGMP（レイヤ 3）がスイッチで有効になっている場合は、「Multicast」→「IGMP」→「Group Information」を選択すると、IGMP を使用して学習された現行のマルチキャストグループを表示することができます。IGMP（レイヤ 3）が無効になっており、IGMP（レイヤ 2）が有効になっている場合には、「Multicast」→「IGMP Snooping」→「Forwarding Entry」を選択すると、アクティブなマルチキャストグループを表示することができます。

コマンドの使用

マルチキャストグループに関する情報を表示するには、最初に、グループが割り当てられているインターフェースで IGMP を有効にして（「IGMP インターフェースパラメータの設定」を参照）から、システムでマルチキャストルーティングをグローバルに有効にする（「マルチキャストルーティングのグローバル設定の設定」を参照）必要があります。

関連する CLI 情報

「show ip igmp groups」

パラメータ

以下のパラメータが表示されます。

Show Information

- ・ VLAN – VLAN ID。選択するエントリは、設定済みの IP インターフェースでなければなりません（範囲：1 ～ 4,093）。
- ・ Group Address – スイッチに直接接続するサブスクリバまたはスイッチのダウンストリームのサブスクリバを含むグループの IP マルチキャストアドレス。
- ・ Last Reporter – 指定されたインターフェースで指定されたマルチキャストグループアドレスについて最後に受信されたメンバーシップレポートの送信元の IP アドレス。
- ・ Up Time – エントリが作成されてから経過した時間（経過時間に応じて、w（週）、d（日）、h（時間）、m（分）、s（秒）が表示されます）。
- ・ Expire – エントリが期限切れになるまでの残り時間（デフォルト：260 秒）。
- ・ 「Group Mode」が「Include」の場合、このパラメータには「Stopped」と表示されます。
- ・ V1 Timer – インターフェースに接続している IP サブネットに IGMPv1 メンバーがいなくなったものとみなされるまでの残り時間。
 - ・ スイッチは、IGMPv1 メンバーシップレポートを受信すると、レポートが受信されたグループのメンバーである IGMPv1 ホストが存在していることを示すため、タイマーを設定します。
 - ・ 特定のグループについて IGMPv1 ホストが存在する場合、スイッチは、そのグループについて受信するあらゆるグループ脱退メッセージを無視します。

Show Detail

この画面では、以下の追加情報も確認することができます。

- ・ VLAN – VLAN ID。選択するエントリは、設定済みの IP インターフェースでなければなりません（範囲：1 ～ 4,093）。
- ・ Group Address – スイッチに直接接続しているサブスライバまたはスイッチのダウンストリームのサブスライバを含んでいる IP マルチキャストグループのアドレス、あるいは、インターフェースに割り当てられているスタティックマルチキャストグループのアドレス。
- ・ Interface – スイッチでマルチキャストグループアドレス宛のトラフィックを受信したインターフェース。
- ・ Up Time – エントリが作成されてから経過した時間（経過時間に応じて、w（週）、d（日）、h（時間）、m（分）、s（秒）が表示されます）。
- ・ Group Mode – 「Include」の場合、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、source-list パラメータで指定される IP 送信元アドレスのみから要求されます。「Exclude」の場合、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、source-list パラメータで指定されている IP 送信元アドレスおよび送信元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 IP 送信元アドレス以外のすべての IP 送信元アドレスから要求されます。
- ・ Group Source List – マルチキャストの受信を要求する IP ユニキャストアドレスまたはマルチキャストの受信を要求しない IP ユニキャストアドレス（フィルタモードによって異なる）が 0 個以上含まれているリスト。
 - ・ Source Address – 指定されたグループにトラフィックを送信しているマルチキャストサーバの 1 つのアドレス。
 - ・ Up Time – エントリが作成されてから経過した時間（経過時間に応じて、w（週）、d（日）、h（時間）、m（分）、s（秒）が表示されます）。
 - ・ Expire – エントリが期限切れになるまでの残り時間（デフォルトは 260 秒）。「V3 Expire」というように「V3」が付いている場合は、IGMPv3 によって学習された送信元に関する時間のみが表示されていることを意味します（デフォルトは 260 秒）。
 - ・ Forward – マルチキャスト送信元からのトラフィックが転送されるかどうかを示します。

Web インターフェース

IGMP を使用して学習された現行のマルチキャストグループを表示するには、以下のようにします。

- (1) 「Multicast」 → 「IGMP」 → 「Group Information」 を選択します。
- (2) 「Step」 リストで 「Show Information」 を選択します。
- (3) VLAN を選択します。選択するエントリは、設定済みの IP インターフェースでなければなりません。

Multicast > IGMP > Group Information

Action: Show Information

VLAN: 1

IGMP Group Information List Max: 1024 Total: 1

Group Address	Last Reporter	Up Time	Expire	V1 Timer
224.0.17.17	192.168.1.0	0:00:01	0:04:19	0:00:00

画面 1-248 :IGMP を使用して学習されたマルチキャストグループの表示
(Show Information)

IGMP を使用して学習された現行のマルチキャストグループの詳細情報を表示するには、以下のようにします。

1. 「Multicast」 → 「IGMP」 → 「Group Information」 を選択します。
2. 「Step」 リストで 「Show Details」 を選択します。
3. VLAN を選択します。選択するエントリは、設定済みの IP インターフェースでなければなりません。

Multicast > IGMP > Group Information

Action: Show Detail

VLAN: 1

Group Address: 224.1.1.1

Interface: VLAN 1

Up Time: 0h:12m:42s

Group Mode: Exclude

Last Reporter: 0.0.0.0

Group Source List Max: 64 Total: 3

Source Address	Up Time	V3 Expire	Forward
10.2.2.2	0h:1m:7s	10:20:00	YES
11.2.2.2	0h:1m:7s	10:20:00	YES
12.2.2.2	0h:1m:7s	10:20:00	NO

画面 1-249 : IGMP を使用して学習されたマルチキャスト
グループの表示 (Show Details)

1.13.6 MVR (Multicast VLAN Registration)

MVR は、マルチキャストトラフィック（TV チャンネルやビデオオンデマンドのトラフィック）をサービスプロバイダーのネットワーク経由で送信する場合に最もよく使用されている単一のネットワークワイド VLAN に対するアクセスを制御するプロトコルです。MVR VLAN に入るあらゆるマルチキャストトラフィックは、その VLAN に接続しているすべてのサブスクリバに送信されます。このプロトコルを使用すると、平均的なマルチキャスト VLAN の配信ツリーを動的に監視および確立するために必要な処理オーバーヘッドを大幅に削減することができます。その結果、マルチキャストルーティングプロトコルを一切使用しなくても、一般的なマルチキャストサービスをネットワーク内の広い範囲でサポートすることが可能になります。

MVR では、サブスクリバが属している他の VLAN のみにトラフィックを渡すことにより、VLAN セグレーションで実現されるユーザ分離とデータセキュリティが維持されます。共通のマルチキャストストリームが MVR VLAN から別々の VLAN グループに渡されますが、異なる IEEE 802.1Q VLAN またはプライベート VLAN 内のユーザは、（上位のルーティングサービスを使用しない限り）情報を交換することはできません。

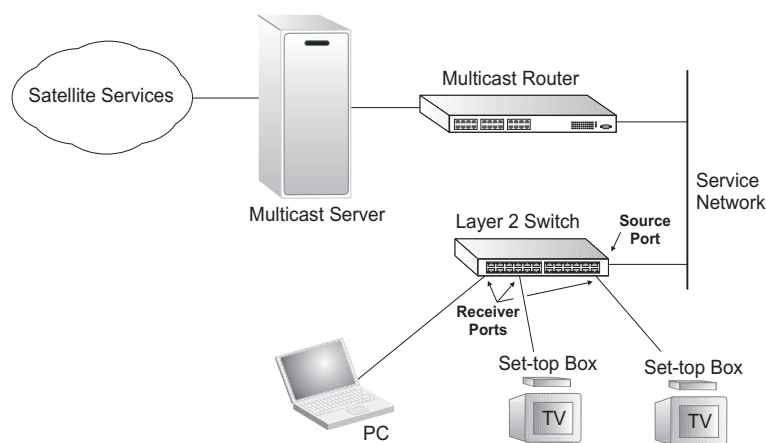


図 1-19:MVR の概念

** 図の注釈

衛星サービスマルチキャストルータ
マルチキャストサーバ
サービスネットワーク
レイヤ 2 スイッチ送信元ポート
受信先ポート
セットトップボックスセットトップボックス
PCTVTV

コマンドの使用

MVR に関する一般的な設定ガイドライン：

1. スイッチで MVR をグローバルに有効にし、MVR VLAN を選択して、接続しているホストにトラフィックをストリーミングするマルチキャストグループを追加します（「MVR のグローバル設定の設定」を参照）。

2. MVR に加入するインターフェースを送信元ポートまたは受信先ポートとして設定します（「MVR インターフェースステータスの設定」を参照）。
 3. 長期的に実行され、一定の一連のホストに関連付けられるマルチキャストストリームについては、マルチキャストグループを加入インターフェースに静的にバインドすることができます（「インターフェースへのスタティック MVR マルチキャストグループの割り当て」を参照）。
- ・ MVR は IGMP スヌーピングの基礎となるメカニズム上で動作しますが、2つの機能は、相互に単独で動作します。一方の動作に影響を及ぼすことなく、もう一方を有効または無効にすることができます。ただし、IGMP スヌーピングと MVR を両方とも有効にした場合、MVR は、MVR について設定されているマルチキャストグループからの加入メッセージと脱退メッセージのみに反応します。他のすべてのマルチキャストグループからの加入メッセージと脱退メッセージは IGMP スヌーピングによって管理されます。また、マルチキャスト加入メッセージまたは脱退メッセージを発行できるのは IGMPv2 ホストまたは IGMPv3 ホストのみであるという点にも注意してください。

MVR のグローバル設定の設定

「Multicast」→「MVR」（Configure Domain）を選択すると、スイッチで MVR をグローバルに有効にし、サービスプロバイダーがサポートしている共通マルチキャストストリーム用の唯一のチャンネルとして機能する VLAN を選択することができます。

関連する CLI 情報

「Multicast VLAN Registration」

パラメータ

以下のパラメータが表示されます。

- ・ MVR Status - MVR をスイッチで有効にすると、MVR グループに関連付けられているマルチキャストデータは、すべての代表送信元ポートから送信され、そのグループからのデータを受け取るために登録されているすべての受信先ポートで受信されます（デフォルト：Disabled）。
- ・ MVR VLAN - MVR を使用してマルチキャストサービスをストリーミングするチャンネルとして機能する VLAN の ID。MVR 送信元ポートは MVR VLAN のメンバーとして設定されていなければなりません（「VLAN へのスタティックメンバーの追加」を参照）が、MVR 受信先ポートをその VLAN のメンバーとして手動で設定する必要はありません（デフォルト：1）。
- ・ MVR Running Status - MVR 環境で必要なすべての条件が満たされているかどうかを示します。この実行ステータスは、MVR が有効であり、指定されている MVR VLAN が存在し、有効なリンクをもつ送信元ポートが設定されていれば、「Active」になります（「MVR インターフェースステータスの設定」を参照）。
- ・ MVR Current Learned Groups - 現在ドメインに割り当てられている MVR グループの数。
- ・ Upstream Source IP - アップストリームに送信されるすべての MVR 制御パケットに割り当てられている送信元 IP アドレス（デフォルト：Null 送信元 IP アドレス）。

Web 設定

マルチキャストフィルタリング

Web インターフェース

MVR のグローバル設定を設定するには、以下のようにします。

- (1) 「Multicast」 → 「MVR」 を選択します。
- (2) 「Step」 リストで 「Configure Domain」 を選択します。
- (3) スイッチで MVR をグローバルに有効にし、MVR VLAN を選択し、必要に応じて、アップストリームに送信されるすべての制御パケットの送信元 IP アドレスを設定します。
- (4) < Apply > ボタンをクリックします。

Multicast > MVR

Step: 1. Configure General

MVR Status	☒ Enabled
MVR VLAN	1
MVR Running Status	Inactive
MVR Current Learned Groups	0
Upstream Source IP	192.168.1.99

Apply Revert

画面 1-250 :MVR のグローバル設定の設定

MVR グループ範囲の設定

「Multicast」→「MVR」（Configure Profile）を選択すると、各サービスのマルチキャストグループアドレスを MVR VLAN に割り当てることができます。

関連する CLI 情報

「Multicast VLAN Registration」

コマンドの使用

- ・ 「Configure Profile」画面で、MVR VLAN に加入するすべてのマルチキャストグループのアドレスを静的に設定することができます。MVR グループに関連付けられているあらゆるマルチキャストグループは、スイッチ上のすべての送信元ポートから送信され、そのマルチキャストアドレスのデータを受信するために選択されているすべての受信先ポートで受信されます。
- ・ マルチキャストストリームには、IP アドレス範囲 224.0.0.0 ～ 239.255.255.255 が使用されます。MVR グループアドレスには、予約 IP マルチキャストアドレス範囲 224.0.0.x に該当するアドレスを使用することはできません。
- ・ IGMP スヌーピングと MVR で最大 1,024 のグループを共有します。この上限値を超えて受信されたマルチキャストストリームは、関連付けられている VLAN 内のすべてのポートにフロードされます。

パラメータ

以下のパラメータが表示されます。

- ・ Start IP Address – MVR マルチキャストグループの開始 IP アドレス（範囲：224.0.1.0 ～ 239.255.255.255）。
- ・ End IP Address – MVR マルチキャストグループの終了 IP アドレス（範囲：224.0.1.0 ～ 239.255.255.255）。

Web インターフェース

MVR VLAN のマルチキャストグループを設定するには、以下のようになります。

- (1) 「Multicast」→「MVR」を選択します。
- (2) 「Step」リストで「Configure Profile」を選択します。
- (3) 「Step」リストで「Add」を選択します。
- (4) トラフィックを加入ホストにストリーミングするマルチキャストグループを追加します。

(5) < Apply > ボタンをクリックします。

Multicast > MVR

Step: 2. Configure Profile Action: Add

Profile Name: Video

Start IP Address: 228.1.23.1

End IP Address: 228.1.23.10

Apply Revert

画面 1-251 :MVR のグループ範囲の設定

MVR VLAN に割り当てられているマルチキャストグループを表示するには、以下のようになります。

1. 「Multicast」 → 「MVR」 を選択します。
2. 「Step」 リストで 「Configure Group Range」 を選択します。
3. 「Step」 リストで 「Show」 を選択します。

Multicast > MVR

Step: 2. Configure Profile Action: Show

MVR Profile List Total: 1

	Profile Name	Start IP Address	End IP Address
☐	Video	228.1.23.1	228.1.23.10

Delete Revert

画面 1-252 :MVR について設定されているグループ範囲の表示

MVR インターフェースステータスの設定

「Multicast」→「MVR」(Configure Interface)を選択すると、送信元ポートまたは受信先ポートとして MVR プロトコルサービスに加入する各インターフェースを設定することができます。インターフェースに接続している 1 つのサブスクリバのみがマルチキャストサービスを受けることが確実である場合には、immediate leave 機能を有効にすることができます。

関連する CLI 情報

「Multicast VLAN Registration」

コマンドの使用

- ・ MVR 受信先ポートまたは MVR 送信元ポートとして設定されているポートは、MVR について設定されているマルチキャストグループに対して加入または脱退することができます。ただし、それらのポートは、IGMP スヌーピングを使用して、マルチキャストフィルタリングの標準ルールが適用されている他のマルチキャストグループに加入または脱退することもできるので、注意してください。
- ・ 受信先ポートは、異なる VLAN に属することができますが、MVR VLAN のメンバーとして設定しないでください。MVR を使用することにより、受信先ポートは、MVR VLAN 内のマルチキャストグループに対して動的に加入または脱退できるようになります。また、マルチキャストグループを動的に受信先ポートに割り当てることもできます（「インターフェースへのスタティック MVR マルチキャストグループの割り当て」を参照）。
- ・ 受信先ポートは MVR VLAN のスタティックメンバーとして設定しないでください。そのように設定すると、MVR のステータスが非アクティブになります。
- ・ 1 つまたは複数のインターフェースを MVR 送信元ポートとして設定することができます。1 つの送信元ポートで、設定されている MVR グループまたは静的に割り当てられている MVR グループ（「インターフェースへのスタティック MVR マルチキャストグループの割り当て」を参照）のデータの送信と受信の両方を行うことができます。

すべての送信元ポートは MVR VLAN に属していなければなりません。

サブスクリバは送信元ポートに直接接続しないでください。

- ・ immediate leave は受信先ポートのみに適用されます。immediate leave が有効になっている場合には、受信先ポートは、脱退メッセージで示されるマルチキャストグループから即座に削除されます。immediate leave が無効になっている場合には、スイッチは、標準のルールに従って、クエリメッセージを受信先ポートに送信し、マルチキャストグループに残っているサブスクリバがないかどうかを確認するために応答を待機してから、ポートをグループリストから削除します。
 - ・ immediate leave は、脱退に伴う遅延を減らすのに役立ちますが、同じインターフェースに接続している他のグループメンバーに対するサービスが妨げられることがないようにするため、1 つのマルチキャストサブスクリバに接続しているポートでのみ、有効にしてください。
 - ・ immediate leave はポートに静的に割り当てられているマルチキャストグループには適用されません。

パラメータ

以下のパラメータが表示されます。

- ・ Port – ポート ID。
- ・ Type – 以下のインターフェースタイプがサポートされています。
- ・ Source – MVR VLAN に割り当てられているグループのマルチキャストデータを送受信できるアップリンクポート。送信元ポートは手動で MVR VLAN のメンバーとして設定する必要があるので注意してください（「VLAN へのスタティックメンバーの追加」を参照）。
- ・ Receiver – MVR VLAN によって送信されるマルチキャストデータを受信できるサブスクライバポート。受信先ポートとして設定されているあらゆるポートは、MVR VLAN でサポートされている指定のマルチキャストサービスを要求する接続ホストからの IGMP レポートまたは加入メッセージを転送するときに、動的にその MVR VLAN に追加されます。マルチキャスト加入メッセージまたは脱退メッセージを発行できるのは IGMPv2 ホストまたは IGMPv3 ホストのみであるという点に注意してください。IGMPv1 ホストについて MVR を設定する必要がある場合は、マルチキャストグループを静的に割り当てなければなりません（「インターフェースへのスタティック MVR マルチキャストグループの割り当て」を参照）。
- ・ Non-MVR – MVR VLAN に加入しないインターフェース（これがデフォルトのタイプです）。
- ・ Oper. Status – リンクステータスが表示されます。
- ・ MVR Status – MVR ステータスが表示されます。送信元ポートの MVR ステータスは、MVR がスイッチでグローバルに有効になっている場合に「Active」になります。受信先ポートの MVR ステータスは、MVR グループのうちの 1 つからマルチキャストトラフィックを受信するサブスクライバがいる場合、またはマルチキャストグループが静的にインターフェースに割り当てられている場合にのみ、「Active」になります。
- ・ Immediate Leave – MVR グループについて脱退メッセージを受信した場合に即座にインターフェースをマルチキャストストリームから除外するようにスイッチを設定します（このオプションは、MVR 受信先ポートとして設定されているインターフェースのみに適用されます）。

Web インターフェース

MVR のインターフェース設定を設定するには、以下のようになります。

- (1) 「Multicast」 → 「MVR」 を選択します。
- (2) 「Step」 リストで 「Configure Interface」 を選択します。
- (3) 「Step」 リストで 「Configure Port」 または 「Configure Trunk」 を選択します。
- (4) MVR プロトコルサービスに加入する各ポートを送信元ポートまたは受信先ポートとして設定し、必要に応じて、サブスクライバが 1 つだけ接続している受信先ポートで 「Immediate Leave」 を有効にします。

Web 設定

マルチキャストフィルタリング

(5) < Apply > ボタンをクリックします。

Multicast > MVR

Step: 3. Configure Interface Action: Configure Port

Port List Max: 26 Total: 26 1 2 3

Port	Type	Oper. Status	MVR Status	Immediate Leave
1	Source	Up	Inactive	☐ Enabled
2	Receiver	Up	Inactive	☒ Enabled
3	Non-MVR	Down	Inactive	☐ Enabled
4	Non-MVR	Down	Inactive	☐ Enabled
5	Non-MVR	Down	Inactive	☐ Enabled

画面 1-253 :SNMP のインターフェース設定の設定

インターフェースへのスタティック MVR マルチキャストグループの割り当て

「Multicast」→「MVR」(Configure Static Group Member) を選択すると、永続的に実行され、一定の一連のホストに関連付けられているマルチキャストストリームを受信するポートにマルチキャストグループを静的にバインドすることができます。

関連する CLI 情報

「mvr vlan group」

コマンドの使用

- ・ この設定画面を使用して、マルチキャストグループを受信先ポートに静的に割り当てることができます。
- ・ マルチキャストストリームには、IP アドレス範囲 224.0.0.0 ～ 239.255.255.255 が使用されます。MVR グループアドレスには、予約 IP マルチキャストアドレス範囲 224.0.0.x に該当するアドレスを使用することはできません。
- ・ マルチキャスト加入メッセージまたは脱退メッセージを発行できるのは IGMPv2 ホストまたは IGMPv3 ホストのみです。IGMPv1 ホストについて MVR を設定する必要がある場合は、マルチキャストグループを静的に割り当てなければなりません。
- ・ MVR VLAN をスタティックバインディングのための受信側 VLAN として指定することはできません。

パラメータ

以下のパラメータが表示されます。

- ・ Port - ポート ID。
 - ・ VLAN - VLAN ID。
- Group IP Address - 選択したポートに送信されるマルチキャストサービスを定義します。割り当てるマルチキャストグループは、「Configure General」画面で設定する MVR グループ範囲に含まれているグループでなければなりません。

Web インターフェース

スタティック MVR グループをポートに割り当てるには、以下のようになります。

- (1) 「Multicast」→「MVR」を選択します。
- (2) 「Step」リストで「Configure Static Group Member」を選択します。
- (3) 「Step」リストで「Add」を選択します。
- (4) マルチキャストストリームを受信する VLAN とポートメンバーを選択し、マルチキャストグループアドレスを入力します。

Web 設定

マルチキャストフィルタリング

(5) < Apply > ボタンをクリックします。

Multicast > MVR

Step: 3. Configure Static Group Member Action: Add

Port: 1

VLAN: 1

Group IP Address: 224.1.1.1

Apply Revert

画面 1-254 : ポートへのスタティック MVR グループの割り当て

ポートに割り当てられているスタティック MVR グループを表示するには、以下のようになります。

1. 「Multicast」 → 「MVR」 を選択します。
2. 「Step」 リストで 「Configure Static Group Member」 を選択します。
3. 「Step」 リストで 「Show」 を選択します。
4. 該当の情報を表示するポートを選択します。

Multicast > MVR

Step: 3. Configure Static Group Member Action: Show

Port: 2

MVR Static Group Member List Max: 16 Total: 3

	VLAN	Group IP Address
☐	2	224.1.1.1
☐	2	224.1.1.2
☐	3	224.1.1.3

Delete Revert

画面 1-255 : ポートに割り当てられているスタティック MVR グループの表示

MVR 受信先グループの表示

「Multicast」→「MVR」(Show Member) を選択すると、各インターフェースで MVR 受信先グループにスタティックまたは動的に割り当てられているマルチキャストグループを表示することができます。

関連する CLI 情報

「show mvr」

パラメータ

以下のパラメータが表示されます。

- ・ Group IP Address – MVR VLAN に割り当てられているマルチキャストグループ。
- ・ VLAN – サービスの受信に使用される VLAN。この VLAN は、グループアドレスが静的に割り当てられている場合は MVR VLAN と異なることがあるという点に注意してください。
- ・ Port – インターフェースが、MVR VLAN を使用して提供されるマルチキャストサービスのサブスクライバと共に表示されます。
- ・ Up Time – 接続しているクライアントにサービスが転送された時間。
- ・ Expire – 現在アクティブなクライアントまたは新規のクライアントからメンバーシップレポートが受信されない場合にエントリが期限切れになるまでの時間。
- ・ Count – 現在 MVR VLAN から転送されているマルチキャストサービスの数。

Web インターフェース

ポートに割り当てられているすべての MVR グループを表示するには、以下のようになります。

- (1) 「Multicast」→「MVR」を選択します。
- (2) 「Step」リストで「Show Member」を選択します。

Multicast > MVR					
Step: 5. Show Member					
MVR Member List Total: 8					
Group IP Address	VLAN	Port	Up Time	Expire	Count
224.1.1.1	2		00:00:30		2 (Port)
	2	Unit 1 / Port 1 (Source)			
224.1.1.2	1	Unit 1 / Port 2 (Receiver)	00:01:10	00:00	4 (Host)
	4		00:00:50		4 (Port)
	4	Unit 1 / Port 3 (Source)			
	5	Unit 1 / Port 4 (Receiver)			
	6	Unit 1 / Port 5 (Source)			
	7	Unit 1 / Port 6 (Receiver)	00:01:10	00:00	1 (Host)

画面 1-256 :MVR 受信先グループの表示

1.14 IP 設定

本章では、スイッチに対するネットワーク経由での管理アクセスのための初期 IP インターフェースを設定する方法について説明します。本製品は、IPv4 と IPv6 の両方をサポートしており、両方のアドレスタイプを使用して管理することができます。特定の IPv4 アドレスを手動で設定することも、スイッチの電源投入時に IPv4 アドレスが BOOTP または DHCP から取得されるように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、手動で設定するか、リンクローカルアドレスを動的に生成することができます。

本章は、以下のネットワーク機能に関する情報を提供します。

- ・ スwitchの IP アドレスの設定 (IPv4) – 管理アクセスに使用する IPv4 アドレスを設定します。
- ・ スwitchの IP アドレスの設定 (IPv6) – 管理アクセスに使用する IPv6 アドレスを設定します。

1.14.1 スwitchの IP アドレスの設定 (IPv4)

「IP」→「General」→「Routing Interface」(Add) を選択すると、スイッチの IPv4 アドレスを設定することができます。IPv4 アドレスは、デフォルトで、DHCP を使用して VLAN 1 から取得されます。スタティック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に対応する値に変更する必要があります。また、スイッチと別のネットワークセグメントに存在する管理ステーションとの間でデフォルトのゲートウェイが確立されるようにしなければならないこともあります（有効になっているルーティングプロトコルがない場合）。

アドレスを BOOTP サーバまたは DHCP サーバから取得するようにスイッチを設定するか、スタティック IP アドレスを手動で設定することができます。有効な IP アドレスは、0 ～ 255 の 10 進数を 4 つ組み合わせ、それぞれをピリオドで区切って設定されます。それ以外の形式は認められません。

関連する CLI 情報

「Basic IPv4 Configuration」

「DHCP Client」

コマンドの使用

- ・ ここでは、スイッチへの初期アクセスに使用される単一のローカルインターフェースを設定する方法について説明します。複数の IP インターフェースを設定するには、VLAN ごとに IP インターフェースをセットアップしてください。
- ・ IP アドレスがインターフェースに割り当てられると、スイッチ上の異なるインターフェース間でのルーティングが有効になります。
- ・ スwitchで定義されているインターフェースと外部ネットワークインターフェースとの間のルーティングを有効にするには、スタティックルートを設定するか、ダイナミックルーティング（RIP、OSPFv2、または OSPFv3）を使用する必要があります。
- ・ IP インターフェースを設定する場合は、「IP」→「General」→「Routing Interface」(Add) で表示される画面でのインターフェースを設定する、スタティックルートを定義する、ダイナミックルーティングを設定するという順序で作業を進めます。

パラメータ

以下のパラメータが表示されます。

- ・ VLAN – 設定済み VLAN の ID (範囲: 1 ~ 4,093)。デフォルトでは、スイッチ上のすべてのポートが VLAN 1 のメンバーになります。ただし、管理ステーションは任意の VLAN に属するポートに接続することができます (その場合、VLAN に IP アドレスが割り当てられていることが前提になります)。
- ・ IP Address Mode – IP 機能を手動設定 (Static)、DHCP (Dynamic Host Configuration Protocol)、ブートプロトコル (BOOTP) のうちのどの方法を使用して有効にするかを指定します。「DHCP」または「BOOTP」を選択した場合、IP は、サーバから応答が受信されるまで機能しません。IP アドレス要求は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 応答または 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 IP アドレスまたはセカンダリ IP アドレスを指定します。1 つのインターフェースについて指定できるプライマリ IP アドレスは 1 つだけですが、セカンダリ IP アドレスは複数指定することができます。言い換えれば、インターフェースを使用して複数の IP サブネットにアクセスできるようにする場合にはセカンダリ IP アドレスを指定する必要があるということです。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 または Secondary、デフォルト: Primary)。
- ・ ここで注意しなければならないのは、セカンダリ IP アドレスはプライマリ IP アドレスを設定してからでないと指定することができず、プライマリ IP アドレスはセカンダリ IP アドレスが存在している限り削除することができないという点です。また、ネットワークセグメント内のいずれかのルータがセカンダリ IP アドレスを使用している場合、そのセグメント内の他のすべてのルータも同じネットワークアドレス領域またはサブネットアドレス領域のセカンダリ IP 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。有効な IP アドレスは、0 ~ 255 の数値を 4 つ組み合わせ、それぞれをピリオドで区切って設定されます (デフォルト: 0.0.0.0)。

[注意] : スイッチは、任意の設定済み IP インターフェースを使用して管理することができます。

- ・ Subnet Mask – このマスクは、個々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示します。
- ・ Restart DHCP – 有効になっているすべての VLAN について、新規 IP アドレスを DHCP サーバに要求します。

Web インターフェース

スイッチのスタティックアドレスを設定するには、以下のようにします。

- (1) 「IP」 → 「General」 → 「Routing Interface」を選択します。
- (2) 「Step」リストで「Add」を選択します。
- (3) 任意の設定済み VLAN を選択し、「IP Address Mode」を「Static」に設定して、(インターフェースについて設定されているアドレスがない場合は)「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) < Apply > ボタンをクリックします。

IP > General > Routing Interface

Action: Add ▼

VLAN 1 ▼

IP Address Mode Static ▼

IP Address Type Primary ▼

IP Address

Subnet Mask

Restart DHCP [Click the button to restart DHCP service.](#)

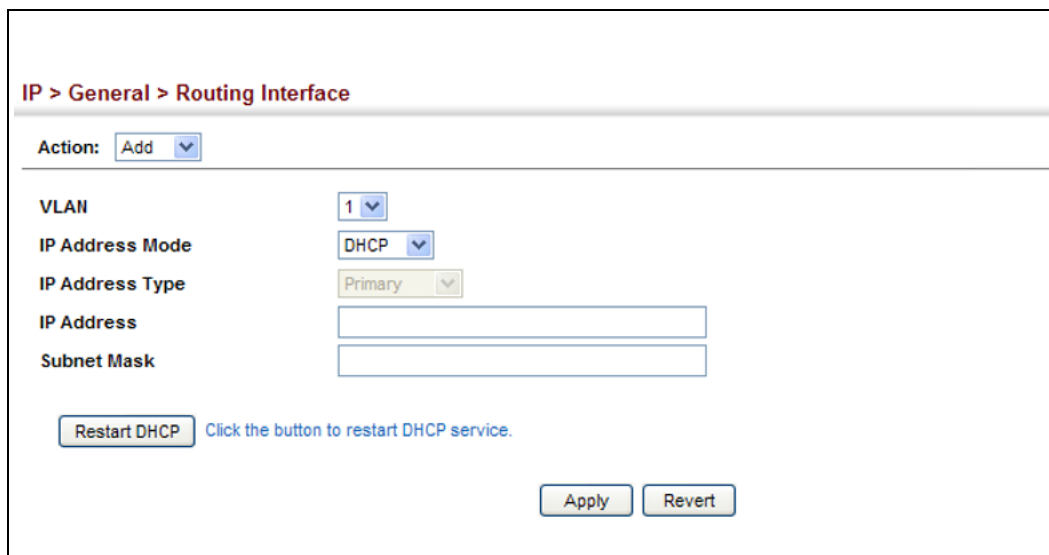
Apply Revert

画面 1-257 : スタティック IPv4 アドレスの設定

スイッチで DHCP または BOOTP を使用してダイナミックアドレスを取得するには、以下のようになります。

1. 「IP」 → 「General」 → 「Routing Interface」 を選択します。
2. 「Step」 リストで 「Add」 を選択します。
3. 任意の設定済み VLAN を選択し、「IP Address Mode」を「BOOTP」または「DHCP」に設定します。
4. < Apply > ボタンをクリックして変更を保存します。

IP は、有効になりますが、BOOTP 応答または DHCP 応答が受信されるまで機能しません。IP 設定情報が BOOTP サーバまたは DHCP サーバから取得されるまで、IP 設定情報要求が数分間隔でブロードキャストされます。



画面 1-258 : ダイナミック IPv4 アドレスの設定

[注意] : IP 設定情報要求は、スイッチの電源がリセットされたときにも、その都度にブロードキャストされます。

[注意] : 管理接続が失われた場合には、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てください。

Renewing DHCP

DHCP では、アドレスがクライアントに無期限でリースされることも、特定の期間リースされることもあります。アドレスの有効期限が切れたり、スイッチが他のネットワークセグメントに移動されたりすると、スイッチに対する管理アクセスが失われます。

その場合は、スイッチを Reboot するか、DHCP サービスを再始動するためのクライアント要求を CLI から送信することができます。

DHCP によって割り当てられているアドレスが機能しなくなった場合には、IP 設定を Web インターフェースから更新できなくなります。Web インターフェースから DHCP サービスを再始動できるのは、現在のアドレスが使用可能な状態になっている場合のみです。

インターフェースについて設定されているアドレスを表示するには、以下のようになります。

1. 「IP」 → 「General」 → 「Routing Interface」を選択します。
2. 「Step」 リストで 「Add」 を選択します。

3. 「VLAN」リストで項目を選択します。

IP > General > Routing Interface

Action: Show

VLAN 1

IP Address Mode Static

Routing Interface IP List Max: 10 Total: 1

☐	IP Address Type	IP Address	Subnet Mask
☐	Primary	192.168.1.2	255.255.255.0

Apply Revert

画面 1-259 : インターフェースについて設定されているアドレスの表示

1.14.2 スイッチの IP アドレスの設定 (IPv6)

ここでは、ネットワーク経由での管理アクセスのため、または、複数のサブネットに接続するインターフェースを作成するため、初期 IPv6 インターフェースを設定する方法について説明します。本製品は、IPv4 と IPv6 の両方をサポートしており、それらのアドレスタイプのいずれかを使用して管理することができます。IPv4 アドレスを指定してスイッチを設定する方法については、「スイッチの IP アドレスの設定 (IPv4)」を参照してください。

コマンドの使用

- IPv6 には 2 つのまったく異なるアドレスタイプがあります。1 つはリンクローカルユニキャストアドレスであり、もう 1 つはグローバルユニキャストアドレスです。リンクローカルアドレスを使用すると、同じローカルサブネットに接続しているすべてのデバイスに IPv6 によってスイッチにアクセスできるようになります。この種のアドレスを使用する管理トラフィックは、サブネット外部のルータ経由で渡すことができません。リンクローカルアドレスは、セットアップが容易であり、簡易ネットワークや基本的なトラブルシューティング作業の場合に役立ちます。ただし、複数のセグメントがある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指定してスイッチを設定する必要があります。
- 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、「Step」リストで「Add IPv6 Address」を選択して）手動で設定するか、「Step」リストで「Configure Interface」を選択して）リンクローカルアドレスを動的に生成することができます。

IPv6 デフォルトゲートウェイの設定

「IP」→「IPv6 Configuration」(Configure Global) を選択すると、スイッチの IPv6 デフォルトゲートウェイを設定することができます。

関連する CLI 情報

「ipv6 default-gateway」

パラメータ

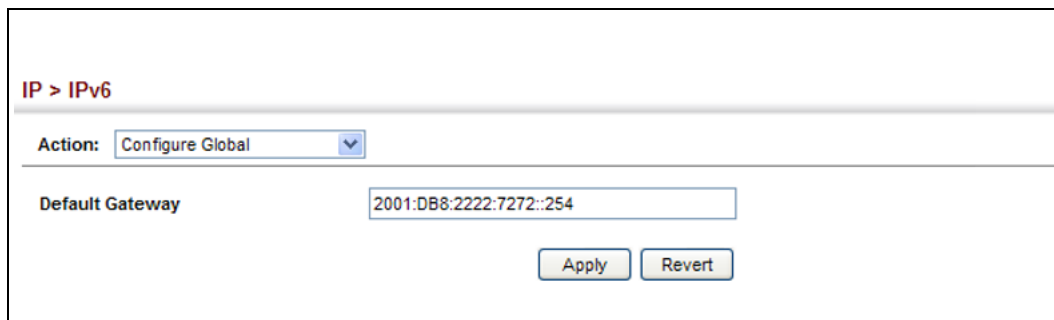
以下のパラメータが表示されます。

- Default Gateway - IPv6 に関して認識されているルーティング情報がない場合に使用され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。
 - 有効になっているルーティングプロトコルがない場合や定義されているスタティックルートがない場合、ターゲットデバイスが別のサブネット内に存在しているときには、ゲートウェイを定義する必要があります。
 - ルーティングプロトコルが有効になっている場合でも、指定されているアドレスまたはサブネット宛のトラフィックが優先ゲートウェイをパススルーするために、スタティックルートを定義することができます。
 - IPv6 デフォルトゲートウェイは、そのゲートウェイに直接接続するネットワークインターフェースがスイッチで設定されている場合にのみ、正常に設定することができます。

Web インターフェース

スイッチの IPv6 デフォルトゲートウェイを設定するには、以下のようにします。

- (1) 「IP」 → 「IPv6 Configuration」 を選択します。
- (2) 「Step」 リストで 「Configure Global」 を選択します。
- (3) IPv6 デフォルトゲートウェイを入力します。
- (4) < Apply > ボタンをクリックします。



The screenshot shows a web interface for IPv6 configuration. At the top, it says "IP > IPv6". Below that, there is a dropdown menu labeled "Action:" with "Configure Global" selected. Underneath, there is a text input field labeled "Default Gateway" containing the value "2001:DB8:2222:7272::254". At the bottom right, there are two buttons: "Apply" and "Revert".

画面 1-260 :IPv6 デフォルトゲートウェイの設定

IPv6 インターフェース設定の設定

「IP」 → 「IPv6 Configuration」 (Configure Interface) を選択すると、VLAN を選択して全般的な IPv6 設定を設定することができます。例えば、リンクローカルインターフェースアドレスの明示的設定、MTU サイズ、重複するアドレスを検出するための NDP (Neighbor Discovery Protocol) 設定、近傍要請間隔などを指定することができます。

関連する CLI 情報

「IPv6 Interface」

「DHCP Client」

コマンドの使用

- ・ スイッチは、リンクローカルアドレスを指定して設定する必要があります。IPv6 を明示的に有効にするオプションを指定すると、リンクローカルアドレスが作成されますが、グローバル IPv6 アドレスは生成されません。グローバルユニキャストアドレスは手動で設定する必要があります (「IPv6 アドレスの設定」を参照)。
- ・ IPv6 ネットワークでは、IPv6 NDP が IPv4 アドレス解決プロトコル (ARP: Address Resolution Protocol) に優先します。同じネットワークセグメント上の IPv6 ノードは、NDP を使用して、相互の存在を確認する、相互のリンクレイヤアドレスを判別する、ルータを検出する、隣接ノードへのパスに関する到達可能性情報を管理するといったことを行います。このプロセスを促進するために使用される主要なパラメータは、同じネットワークセグメントに重複アドレスが存在しているかどうかを確認する回数、および、到達可能性情報の検証に使用される近傍要請の送信間隔です。

パラメータ

以下のパラメータが表示されます。

- ・ VLAN – 管理アクセスのため、またはサブネットの標準インターフェースとして使用される設定済み VLAN の ID。デフォルトでは、スイッチ上のすべてのポートが VLAN 1 のメンバーになります。ただし、管理ステーションは任意の VLAN に属するポートに接続することができます（その場合、VLAN に IP アドレスが割り当てられていることが前提になります）（範囲：1 ～ 4,093）。
- ・ Enable IPv6 Explicitly – インターフェースの IPv6 を有効にします。明示的なアドレスがインターフェースに割り当てられている場合は IPv6 が自動的に有効になり、割り当てられているすべてのアドレスが削除されない限り無効にすることができなくなるので注意してください（デフォルト：Disabled）。
- ・ このパラメータを無効にしても、IPv6 アドレスを指定して明示的に設定されたインターフェースの IPv6 は無効になりません。
- ・ MTU – インターフェースで送信される IPv6 パケットの最大転送単位（MTU: Maximum Transmission Unit）のサイズを設定します（範囲：1,280 ～ 65,535 bytes、デフォルト：1,500 bytes）。
 - ・ このコマンドで設定する最大値は、物理インターフェースの MTU（現在は 1,500 bytes に固定）を超えてはなりません。
 - ・ デフォルト以外の値を設定すると、このデバイスから送信されるルータアドバタイズメントに MTU オプションが含まれます。このオプションは、（そのようにしないとリンク MTU が十分に認識されない場合に）リンク上のすべてのノードが同じ MTU 値を使用するようにするために用意されています。
 - ・ IPv6 ルータは、他のルータから転送される IPv6 パケットをフラグメント化しません。ただし、IPv6 ルータに接続しているエンドステーションから発信されるトラフィックはフラグメント化することができます。
 - ・ 同じ物理メディア上のすべてのデバイスは、正しく動作するには、同じ MTU を使用する必要があります。
 - ・ MTU を設定できるようにするため、先に IPv6 を有効にしなければなりません。IPv6 アドレスがスイッチに割り当てられていない場合は、「MTU」フィールドに「N/A」と表示されます。
- ・ ND DAD Attempts – 重複アドレスを検出するときにインターフェースで連続して送信される近傍要請メッセージの数（範囲：0 ～ 600、デフォルト：2）。
 - ・ 値 0 を指定すると、重複アドレスの検出が無効になります。
 - ・ 重複アドレスの検出によって、新規ユニキャスト IPv6 アドレスをインターフェースに割り当てる前に、そのアドレスが既にネットワーク上に存在しているかどうかを確認されます。
 - ・ 重複アドレスの検出は、サスペンドになっているインターフェース（「VLAN グループの設定」を参照）では停止されます。
 - ・ インターフェースがサスペンドになっている間は、そのインターフェースに割り当てられているすべてのユニキャスト IPv6 アドレスが「Pending」状態になります。インターフェースが管理者によって再びアクティブにされると、自動的に重複アドレスの検出が再開されます。
 - ・ 再アクティブ化されたインターフェースでは、そのインターフェース上のすべてのユニキャスト IPv6 アドレスに対する重複アドレスの検出が再開されます。インターフェースのリンクローカルアドレスに対する重複アドレスの検出が実行されている間、他の IPv6 アドレスは「Tentative」状態に維持されます。重複するリンクローカルアドレスが検出されなかった場合は、残りの IPv6 アドレスに対する重複アドレスの検出が開始されます。
 - ・ 重複するアドレスが検出されると、そのアドレスが「Duplicate」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。重複するものとして検出されたアドレスがリンクローカルアドレスである場合、そのインターフェースで IPv6 プロセスが無効になります。重複するものとして検出されたアドレスがグローバルユニキャストアドレスである場合、そのアドレスは使用されません。重複アドレスに関連付けられているすべての設定コマンドは、そのアドレスが「Duplicate」状態の間は設定された状態に維持されます。

Web 設定

IP 設定

- ・ インターフェースのリンクローカルアドレスが変更された場合、新規のリンクローカルアドレスについては重複アドレスの検出が実行されますが、既にそのインターフェース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については重複アドレスの検出は実行されません。
- ・ ND NS Interval – インターフェースにおける IPv6 近傍要請メッセージの送信間隔（範囲：1,000 ～ 3,600,000 ms）。
近傍検出動作にはデフォルトの 1,000 ms が使用され、0 ms がルータアダプタイズメントでアダプタイズされます。
この属性は、アドレスの解決時または隣接ノードの到達可能性の検証時に近傍要請メッセージを送信する間隔を指定します。そのため、通常の IPv6 動作には極めて短い間隔を使用しないようにしてください。
デフォルト以外の値を指定すると、その指定した間隔がルータアダプタイズメントとルータ自体の両方で使用されます。
- ・ ND Reachable-Time – いくつかの到達可能性確認イベントが発生してからリモート IPv6 ノードが到達可能であるとみなされるまでの時間（範囲：0 ～ 3,600,000 ms）。
 - ・ 近傍検出動作にはデフォルトの 30,000 ms が使用され、0 ms がルータアダプタイズメントでアダプタイズされます。
 - ・ このパラメータで時間制限を指定することによって、使用不可になっている隣接ノードをルータが検出できるようになります。
 - ・ この制限時間は、同じリンク上のノードで同じ時間値が使用されるようにするため、インターフェース経由で送信されるすべてのルータアダプタイズメントに含まれます。
 - ・ 時間制限を 0 に設定するということは、ルータについて時間制限を指定しないことを意味します。

Web インターフェース

スイッチの全般的な IPv6 設定を設定するには、以下のようにします。

- (1) 「IP」 → 「IPv6 Configuration」 を選択します。
- (2) 「Step」 リストで 「Configure Interface」 を選択します。
- (3) 設定する VLAN を指定します。
- (4) 「Enable IPv6 Explicitly」 チェックボックスをオンにすると、選択したインターフェースで、自動的に、リンクローカルアドレスが設定され、IPv6 が有効になります（リンクローカルアドレスを手動で設定するには、「Step」 リストで 「Add IPv6 Address」 を選択します）。MTU サイズ、重複アドレス検出メッセージの最大数、近傍要請メッセージの送信間隔、およびリモート IPv6 ノードが到達可能とみなされるまでの時間を設定します。

(5) < Apply > ボタンをクリックします。

IP > IPv6 Configuration

Action: Configure Interface

VLAN 1

Enable IPv6 Explicitly ☒ Enabled

MTU (1280-65535) 1500 bytes

ND DAD Attempts (0-600) 2

ND NS Interval (1000-3600000) 1000 ms

ND Reachable-Time (0-3600000) 30000 ms

Apply Revert

画面 1-261 :IPv6 インターフェースの全般設定の設定

IPv6 アドレスの設定

「IP」→「IPv6 Configuration」(Add IPv6 Address) を選択すると、ネットワーク経由での管理アクセスのため、または、複数のサブネットに接続するインターフェースを作成するため、初期 IPv6 インターフェースを設定することができます。

関連する CLI 情報

「IPv6 Interface」

コマンドの使用

- すべての IPv6 アドレスは、コロンで区切られた 16 bits の 16 進数値を 8 つ使用して、RFC 2373 「IPv6 Addressing Architecture」に準拠する形式で指定しなければなりません。アドレスでダブルコロンを 1 つ使用して、未定義フィールドを埋めるために必要な該当数の 0 (ゼロ) を示すこともできます。
- スイッチは、常にリンクローカルアドレスを指定して設定する必要があります。また、IPv6 を明示的に有効にする (「IPv6 インターフェース設定の設定」を参照) か、グローバルユニキャストアドレスを手動で割り当てると、リンクローカルユニキャストアドレスが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 bits に固定され、デフォルトアドレスのホスト部は修正版 EUI-64 (Extended Universal Identifier) 形式のインターフェース ID (つまり、物理 MAC アドレス) に基づいて設定されます。あるいは、FE80 ~ FEBF の範囲で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。
- 複数のサブネットがある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、以下のように、いくつかの方法があります。
- ネットワークプレフィックス全体とプレフィックス長を指定し、EUI-64 形式のインターフェース ID を使用してアドレスのホスト部の下位 64 bits が自動的に作成されるようにすることによって、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ができます。

- ・ 完全なアドレスとプレフィックス長を入力することによっ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。
- ・ 1つのインターフェースに対して複数の 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が、リンクローカルアドレスは1つしか設定できません。
- ・ 重複するリンクローカルアドレスがローカルセグメントで検出された場合、インターフェースは無効になり、警告メッセージがコンソールに表示されます。重複するグローバルアドレスがネットワークで検出された場合、インターフェースでそのアドレスが無効になり、警告メッセージがコンソールに表示されます。
- ・ 明示的なアドレスがインターフェースに割り当てられている場合は IPv6 が自動的に有効になり、割り当てられているすべてのアドレスが削除されない限り無効にすることができなくなります。

パラメータ

以下のパラメータが表示されます。

- ・ VLAN – 管理アクセスのため、または複数のサブネットに接続するインターフェースを作成するために使用される設定済み VLAN の ID。デフォルトでは、スイッチ上のすべてのポートが VLAN 1 のメンバーになります。ただし、管理ステーションは任意の VLAN に属するポートに接続することができます（その場合、VLAN に IP アドレスが割り当てられていることが前提になります）（範囲：1 ～ 4,093）。
- ・ Address Type – インターフェースに対して設定するアドレスの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を含む完全な IPv6 アドレスの後にスラッシュ (/) を付け、アドレスの（先頭から）いくつ目までの連続ビットがプレフィックス（アドレスのネットワーク部）を設定するかを示す 10 進数値を指定して、IPv6 グローバルユニキャストアドレスを設定します。
 - ・ EUI-64 (Extended Universal Identifier) – 下位 64 bits に EUI-64 インターフェース ID を使用して、インターフェースの IPv6 アドレスを設定します。
 - ・ EUI-64 形式をアドレスのホスト部の下位 64 bits に使用する場合、「IPv6 Address」フィールドに入力される値にはアドレスのネットワーク部が含まれ、プレフィックス長はプレフィックス（アドレスのネットワーク部）を設定するアドレスの（先頭からの）連続ビット数を示します。ただし、指定するプレフィックス長が 64 bits 未満の場合は、「IPv6 Address」フィールドに指定する値に上位ホストビットの一部を含めることができます。指定するプレフィックス長が 64 bits を超える場合、アドレスのネットワーク部に使用されるビットはインターフェース ID に優先します。
 - ・ IPv6 アドレスの長さは 16 bytes であり、そのうちの下位 8 bytes は、通常、デバイスの MAC アドレスに基づく固有のホスト ID を形成します。EUI-64 仕様は、8 bytes の拡張 MAC アドレスを使用するデバイスを対象としています。（EUI-48 形式としても知られる）従来の 6 bytes の MAC アドレスを使用するデバイスについては、アドレスのユニバーサルビットまたはローカルビットを反転させて MAC アドレスの上位 3 bytes と下位 3 bytes との間に 16 進数値 FFFE を挿入することにより、MAC アドレスを EUI-64 形式に変換する必要があります。
例えば、デバイスの EUI-48 アドレスが 28-9F-18-1C-82-35 である場合は、最初に、EUI-64 要件が満たされるようにする（つまり、グローバルに定義されているアドレスについては 1、ローカルに定義されているアドレスについては 0 となるようにする）ため、グローバルビットまたはローカルビットを反転させて、28 を 2A に変更します。2 bytes の FFFE が OUI（組織ごとに固有の ID、または企業 ID）とアドレスの残りの部分の間に挿入されて、修正版の EUI-64 ID である 2A-9F-18-FF-FE-1C-82-35 となります。
- ・ このホストアドレス指定方式を使用すると、単一のデバイスの複数の IP インターフェースで同じインターフェース ID を使用できるようになります（ただ

し、それらのインターフェースが異なるサブネットに接続していることが前提となります)。

- ・ Link Local – IPv6 リンクローカルアドレスを設定します。
- ・ アドレスのプレフィックスは FE80 ～ FEBF の範囲でなければなりません。

1 つのインターフェースに対して指定できるリンクローカルアドレスは 1 つだけです。

インターフェースについて自動的に生成されたリンクローカルアドレスが、指定したアドレスに置き換えられます。

- ・ IPv6 Address – インターフェースに割り当てられている IPv6 アドレス。

Web インターフェース

IPv6 アドレスを設定するには、以下のようにします。

- (1) 「IP」 → 「IPv6 Configuration」 を選択します。
- (2) 「Step」 リストで 「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 > ボタンをクリックします。

The screenshot shows a web configuration page titled "IP > IPv6". Below the title, there is a section for "Action:" with a dropdown menu set to "Add IPv6 Address". Below this, there are three rows of configuration fields: "VLAN" with a dropdown set to "1", "Address Type" with a dropdown set to "Global", and "IPv6 Address" with a text input field containing "2001:DB8:2222:7272::72/96". At the bottom right of the form, there are two buttons: "Apply" and "Revert".

画面 1-262 :IPv6 アドレスの設定

IPv6 アドレスの表示

「IP」→「IPv6 Configuration」(Show IPv6 Address)を選択すると、インターフェースに割り当てられている IPv6 アドレスを表示することができます。

関連する CLI 情報

「show ipv6 interface」

パラメータ

以下のパラメータが表示されます。

- ・ VLAN – 管理アクセスのため、または複数のサブネットに接続するインターフェースを作成するために使用される設定済み VLAN の ID。デフォルトでは、スイッチ上のすべてのポートが VLAN 1 のメンバーになります。ただし、管理ステーションは任意の VLAN に属するポートに接続することができます（その場合、VLAN に IP アドレスが割り当てられていることが前提になります）（範囲：1 ～ 4,093）。
- ・ IP Address Type – アドレスタイプ（オプション：Global、EUI-64、または Link Local）。
- ・ IP Address – インターフェースに割り当てられている IPv6 アドレス。

ノードは、インターフェースに割り当てられているユニキャストアドレスに加え、全ノードマルチキャストアドレス FF01::1（インターフェースローカル範囲）と FF02::1（リンクローカル範囲）も listen する必要があります。

FF01::1/16 は、接続されているすべての IPv6 ノードの一時インターフェースローカルユニキャストアドレスであり、FF02::1/16 は、接続されているすべての 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。インター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のみに使用されます。リンクローカルマルチキャストアドレスは、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く、全ノード（FF02::1）、全ルータ（FF02::2）、要請ノード（FF02::1:FFXX:XXXX）といったタイプをカバーします。これらについては、以降で説明します。

また、ノードでは、そのノードが割り当てられているあらゆるユニキャストアドレスおよびエニーキャストアドレスについて、関連付けられている要請ノードのマルチキャストアドレスを計算し、それらを結合する必要があります。異なるアグリゲーションリンクに複数の上位プレフィックスが関連付けられていることなどが原因で上位ビットのみが異なる IPv6 アドレスは、同じ要請先ノードアドレスにマップされるので、ノードで結合しなければならないマルチキャストアドレスの数が削減されます。この例の場合、FF02::1:FF90:0/104 が要請ノードのマルチキャストアドレスであり、アドレスの下位 24 bits を取り出してそれをプレフィックスに付加することによって形成されています。

IPv6 では IPv4 のアドレス解決で使用するブロードキャスト方式がサポートされないため、要請ノードのマルチキャストアドレス（リンクローカル範囲 FF02）を使用して隣接ノードの MAC アドレスが解決されるので注意してください。

それらの追加アドレスは、CLI を使用して確認することができます（「show ip interface」を参照）。

- ・ Configuration Mode – アドレスが自動的に生成されたものか、手動で設定されたものかを示します。

Web インターフェース

設定されている IPv6 アドレスを表示するには、以下のようになります。

- (1) 「IP」 → 「IPv6 Configuration」 を選択します。
- (2) 「Step」 リストで 「Show IPv6 Address」 を選択します。
- (3) リストで 「VLAN」 を選択します。

The screenshot shows the 'IP > IPv6' configuration page. The 'Action' dropdown is set to 'Show IPv6 Address'. The 'VLAN' dropdown is set to '1'. Below this, the 'IPv6 Address List' is displayed with a maximum of 10 entries and a total of 3 entries. The list contains three rows: EUI-64, Global, and Link Local, each with its corresponding IP address and configuration mode. At the bottom, there are 'Apply' and 'Revert' buttons.

☐	IP Address Type	IP Address	Configuration Mode
☐	EUI-64	2001:DB8::1:200:E8FF:FE93:82A0/64	Manual
☐	Global	2001:DB8:2222:7272::72/96	Manual
☐	Link Local	FE80::200:E8FF:FE93:82A0%1/64	Auto

画面 1-263 : 設定されている IPv6 アドレスの表示

IPv6 近傍キャッシュの表示

「IP」→「IPv6 Configuration」(Show IPv6 Neighbor Cache)を選択すると、隣接デバイスについて検出された IPv6 アドレスを表示することができます。

関連する CLI 情報

「show ipv6 neighbors」

パラメータ

以下のパラメータが表示されます。

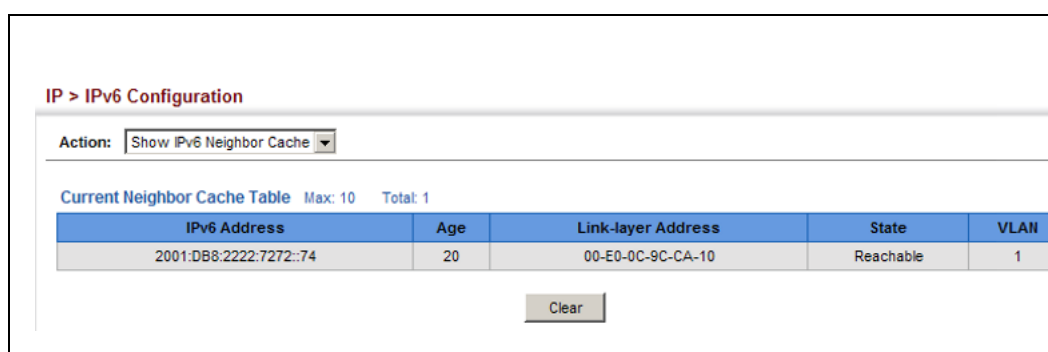
パラメータ	説明
IPv6 Address	隣接デバイスの IPv6 アドレス。
Age	アドレスが到達可能であると確認されてからの経過時間（単位：秒）。スタティックエントリは値「Permanent」で示されます。
Link-layer Address	物理レイヤの MAC アドレス。
State	ダイナミックエントリについては以下の状態が使用されます。 ・ Incomplete - エントリに対するアドレス解決の実行中です。近傍要請メッセージがターゲットのマルチキャストアドレスに送信されましたが、まだ近傍アドバタイズメントメッセージが返されていません。 ・ Invalid - 無効なマッピング。状態が「Invalid」になると、このエントリによって特定されるインターフェースのマッピング（RFC 4293）が解除されます。 ・ Reachable - 隣接デバイスへの転送パスが機能していた前回の ReachableTime 内に肯定応答が受信されました。デバイスは、Reachable 状態の間は、パケットの送信時に何も特別なアクションを実行しなくなります。 ・ Stale - 転送パスが機能しているという肯定応答が前回受信されてから ReachableTime を超える時間が経過しています。デバイスは、Stale 状態の間は、パケットが送信されるまで何のアクションも実行しなくなります。 ・ Delay - 転送パスが機能しているという肯定応答が前回受信されてから ReachableTime を超える時間が経過しています。パケットが前回の DELAY_FIRST_PROBE_TIME 内に送信されました。Delay 状態になってからこの期間が経過するまでに到達可能性確認メッセージを受信しない場合、スイッチは、近傍要請メッセージを送信して、Probe 状態になります。 ・ Probe - 到達可能性確認メッセージが受信されるまで、近傍要請メッセージが RetransTimer の間隔で再送されて、到達可能性確認メッセージがアクティブに探索されます。 - Unknown - 不明な状態。 スタティックエントリについては以下の状態が使用されます。 ・ Incomplete - エントリで示されているインターフェースが Down 状態になっています。 ・ Permanent - スタティックエントリであることを示します。 ・ Incomplete - エントリで示されているインターフェースが Up 状態になっています。到達可能性の検出は、IPv6 近傍探索キャッシュ内のスタティックエントリには適用されません。
VLAN	VLAN 到達先アドレスの VLAN インターフェース。

表 1-15:IPv6 近傍キャッシュの表示（表示内容の説明）

Web インターフェース

隣接 IPv6 デバイスを表示するには、以下のようにします。

- (1) 「IP」 → 「IPv6 Configuration」 を選択します。
- (2) 「Step」 リストで 「Show IPv6 Neighbors」 を選択します。



The screenshot shows the 'IP > IPv6 Configuration' page. Under the 'Action:' dropdown, 'Show IPv6 Neighbor Cache' is selected. Below this, a table titled 'Current Neighbor Cache Table' is displayed. The table has columns for IPv6 Address, Age, Link-layer Address, State, and VLAN. One entry is shown with IPv6 Address 2001:DB8:2222:7272::74, Age 20, Link-layer Address 00-E0-0C-9C-CA-10, State Reachable, and VLAN 1. A 'Clear' button is located below the table.

IPv6 Address	Age	Link-layer Address	State	VLAN
2001:DB8:2222:7272::74	20	00-E0-0C-9C-CA-10	Reachable	1

画面 1-264 :IPv6 隣接デバイスの表示

IPv6 統計情報の表示

「IP」 → 「IPv6 Configuration」 (Show Statistics) を選択すると、スイッチを経由する IPv6 トラフィックに関する統計情報を表示することができます。

関連する CLI 情報

「show ipv6 traffic」

コマンドの使用

本製品は、以下のトラフィックタイプに関する統計情報を提供します。

- ・ IPv6 – IPv6 アドレスは、固定長アドレスによってネットワークデバイス（つまり、ホスト）が特定される場合に（一般的にはパケットまたはフレームと呼ばれる）データブロック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。また、IPv6 を使用することにより、「スモールパケット」ネットワークによる送信のため、必要に応じて、ロングパケットをフラグメント化して再アセンブルできるようになります。
- ・ ICMPv6 – ICMPv6 (Internet Control Message Protocol for Version 6) は、IPv6 パケット処理エラーを報告するために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において欠くことのできない要素です。ICMP メッセージは、さまざまな状況、例えば、データグラムが宛先に到達できない、ゲートウェイにデータグラムを転送するためのバッファリング容量がない、より短いルートでトラフィックを送信するためにゲートウェイがホストをダイレクトできるといった状況を報告するために使用することができます。また、ICMP は、特定の宛先についてより望ましいルート（つまり、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ルータで使用されることもあります。
- ・ UDP – UDP (User Datagram Protocol) は、パケットスイッチング通信でデータグラムモードを実現します。基礎となるトランスポートメカニズムとして IP を使用して、IP-like サービスへのアクセスを可能にします。UDP パケットは、IP パケットと同様、ターゲットに到達する前に破棄される可能性のあるコネクションレスデータグラムと

して配信されます。UDP は、TCP を使用すると複雑すぎる場合や遅すぎる場合、または TCP が不要である場合に役立ちます。

パラメータ

以下のパラメータが表示されます。

パラメータ	説明
IPv6 Statistics	
IPv6 Received	
Total	インターフェースで受信された入力データグラムの総数（エラーとして受信されたものを含む）。
Header Errors	IPv6 ヘッダに、バージョン番号の不一致、フォーマット違いエラー、過剰ホップ数、IPv6 オプションなどのエラーが含まれていたために破棄された入力データグラムの数。
Too Big Errors	サイズが発信インターフェースのリンク MTU を超えていたため転送できなかった入力データグラムの数。
No Routes	宛先に送信するためのルートを検出できなかったために破棄された入力データグラムの数。
Address Errors	IPv6 ヘッダの宛先フィールド内の 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はなかったために破棄された入力データグラムの数。この数には、無効なアドレス（例：::0）およびサポートされていないアドレス（例：割り当てられていないプレフィックスをもつアドレス）をもつデータグラムが含まれます。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、この数には、宛先アドレスがローカルアドレスではないために破棄されたデータグラムが含まれます。
Unknown Protocols	正常に受信されたが、プロトコルが不明であるため、またはサポートされていないために破棄されたローカルアドレス宛のデータグラムの数。この値は、該当のデータグラムの宛先インターフェース（データグラムによっては必ずしも入力インターフェースとはならない）でインクリメントされます。
Truncated Packets	データグラムのフレームに十分なデータが含まれていなかったために破棄された入力データグラムの数。
Discards	処理の続行を妨げる問題は検出されなかったが（バッファ領域不足などのために）破棄された入力 IPv6 データグラムの数。ただし、この数には、再アセンブリの待機中に破棄されたデータグラムは含まれません。
Delivers	IPv6 ユーザプロトコル（ICMP を含む）について正常に配信されたデータグラムの総数。この値は、該当のデータグラムの宛先インターフェース（データグラムによっては必ずしも入力インターフェースとはならない）でインクリメントされます。
Reassembly Request Datagrams	インターフェースで再アセンブリする必要があった受信 IPv6 フラグメントの数。この値は該当のフラグメントの宛先インターフェース（フラグメントによっては必ずしも入力インターフェースとはならない）でインクリメントされるという点に注意してください。
Reassembled Succeeded	正常に再アセンブリされた IPv6 データグラムの数。この値は該当のデータグラムの宛先インターフェース（データグラムによっては必ずしも入力インターフェースとはならない）でインクリメントされるという点に注意してください。

Reassembled Failed	IPv6 再アセンブリアルゴリズムによって検出された（タイムアウトやエラーなど、何らかの原因による）問題の数。この数は必ずしも破棄された IPv6 フラグメントの数ではないので注意してください。なぜならば、アルゴリズムによっては（特に、RFC 815 のアルゴリズムでは）フラグメントが受信時に結合されるのでフラグメントの数を追跡できないからです。この値は、該当のフラグメントの宛先インターフェース（フラグメントによっては必ずしも入力インターフェースとはならない）でインクリメントされます。
IPv6 Transmitted	
Forwards Datagrams	このエンティティで受信されて最終的な宛先に転送された出力データグラムの数。IPv6 ルータとして使用されていないエンティティの場合、この数には、エンティティ経由でソースルーティングされ、ソースルーティングプロセスが正常に完了したパケットのみが含まれます。正常に転送されたデータグラムについては、この数は発信インターフェースでインクリメントされるので注意してください。
Requests	ローカル IPv6 ユーザプロトコル (ICMP を含む) によって送信要求時に IPv6 に提供された IPv6 データグラムの総数。この数には <code>ipv6IfStatsOutForw</code> データグラムでカウントされるデータグラムは含まれないので注意してください。
Discards	宛先への送信を妨げる問題は検出されなかったが（バッファ領域不足などのために）破棄された出力 IPv6 データグラムの数。該当のパケットが（任意指定の）破棄条件を満たす場合はこの数に <code>ipv6IfStatsOutForw</code> データグラムでカウントされるデータグラムが含まれるので注意してください。
No Routes	宛先に送信するためのルートを検出できなかったために破棄された入力データグラムの数。
Generated Fragments	出力インターフェースでのフラグメント化の結果として生成された出力データグラムフラグメントの数。
Fragment Succeeded	出力インターフェースで正常にフラグメント化された IPv6 データグラムの数。
Fragment Failed The	出力インターフェースでフラグメント化する必要があったがフラグメント化できなかったために破棄された IPv6 データグラムの数。
ICMPv6 Statistics	
ICMPv6 received	
Input	インターフェースで受信された ICMP メッセージの総数（ <code>ipv6IfIcmpInErrors</code> でカウントされるすべてのメッセージを含む）。この場合のインターフェースは ICMP メッセージの宛先インターフェース（データグラムによっては必ずしも入力インターフェースとはならない）であるという点に注意してください。
Errors	インターフェースで受信された ICMP メッセージの総数（ <code>ipv6IfIcmpInErrors</code> でカウントされるすべてのメッセージを含む）。この場合のインターフェースは ICMP メッセージの宛先インターフェース（データグラムによっては必ずしも入力インターフェースとはならない）であるという点に注意してください。
Destination Unreachable Messages	インターフェースで受信された ICMP 宛先到達不能（Destination Unreachable）メッセージの数。
Packet Too Big Messages	インターフェースで受信された ICMP パケットサイズ超過（Packet Too Big）メッセージの数。

Web 設定

IP 設定

Time Exceeded Messages	インターフェースで受信された ICMP 時間切れ (Time Exceeded) メッセージの数。
Parameter Problem Messages	インターフェースで受信された ICMP パラメータ障害 (Parameter Problem) メッセージの数。
Echo Request Messages	インターフェースで受信された ICMP エコー (要求) (Echo (request)) メッセージの数。
Echo Reply Messages	インターフェースで受信された ICMP エコー応答 (Echo Reply) メッセージの数。
Router Solicit Messages	インターフェースで受信された ICMP ルータ要請 (Router Solicit) メッセージの数。
Router Advertisement Messages	インターフェースで受信された ICMP ルータアドバタイズメント (Router Advertisement) メッセージの数。
Neighbor Solicit Messages	インターフェースで受信された ICMP 近傍要請 (Neighbor Solicit) メッセージの数。
Neighbor Advertisement Messages	インターフェースで受信された ICMP 近傍アドバタイズメント (Neighbor Advertisement) メッセージの数。
Redirect Messages	インターフェースで受信されたりダイレクトメッセージの数。
Group Membership Query Messages	インターフェースで受信された ICMPv6 グループメンバーシップクエリ (Group Membership Query) メッセージの数。
Group Membership Response Messages	インターフェースで受信された ICMPv6 グループメンバーシップ応答 (Group Membership Response) メッセージの数。
Group Membership Reduction Messages	インターフェースで受信された ICMPv6 グループメンバーシップ脱退 (Group Membership Reduction) メッセージの数。
Multicast Listener Discovery Version 2 Reports	インターフェースで受信された MLDv2 レポートの数。
ICMPv6 Transmitted	
Output	インターフェースが送信しようとした ICMP メッセージの総数。この数には icmpOutErrors でカウントされるすべてのメッセージが含まれるので注意してください。
Destination Unreachable Messages	インターフェースで送信された ICMP 宛先到達不能 (Destination Unreachable) メッセージの数。
Packet Too Big Messages	インターフェースで送信された ICMP パケットサイズ超過 (Packet Too Big) メッセージの数。
Time Exceeded Messages	インターフェースで送信された ICMP 時間切れ (Time Exceeded) メッセージの数。

Echo Request Messages	インターフェースで送信された ICMP エコー（要求）（Echo (request)）メッセージの数。
Echo Reply Messages	インターフェースで送信された ICMP エコー応答（Echo Reply）メッセージの数。
Router Solicit Messages	インターフェースで送信された ICMP ルータ要請（Router Solicit）メッセージの数。
Router Advertisement Messages	インターフェースで送信された ICMP ルータアドバタイズメント（Router Advertisement）メッセージの数。
Neighbor Solicit Messages	インターフェースで送信された ICMP 近傍要請（Neighbor Solicit）メッセージの数。
Neighbor Advertisement Messages	インターフェースで送信された ICMP 近傍アドバタイズメント（Neighbor Advertisement）メッセージの数。
Redirect Messages	送信されたりダイレクトメッセージの数。ホストの場合、リダイレクトは送信されないので、このオブジェクトは常にゼロになります。
Group Membership Query Messages	インターフェースで送信された ICMPv6 グループメンバーシップクエリ（Group Membership Query）メッセージの数。
Group Membership Response Messages	送信された ICMPv6 グループメンバーシップ応答（Group Membership Response）メッセージの数。
Group Membership Reduction Messages	送信された ICMPv6 グループメンバーシップ脱退（Group Membership Reduction）メッセージの数。
Multicast Listener Discovery Version 2 Reports	インターフェースで送信された MLDv2 レポートの数。
UDP Statistics	
Input	UDP ユーザに配信された UDP データグラムの総数。
No Port Errors	宛先ポートにアプリケーションがなかった受信 UDP データグラムの総数。
Other Errors	宛先ポートにアプリケーションがないこと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。
Output	このエンティティから送信された UDP データグラムの総数。

表 1-16:IPv6 統計情報の表示（表示内容の説明）

Web インターフェース

IPv6 統計情報を表示するには、以下のようにします。

- (1) 「IP」 → 「IPv6 Configuration」 を選択します。
- (2) 「Step」 リストで 「Show Statistics」 を選択します。
- (3) 「IPv6」、「ICMPv6」、または 「UDP」 を選択します。

IP > IPv6

Action: Show Statistics

Type ☒ IPv6 ☐ ICMPv6 ☐ UDP

IPv6 Statistics

Total Received	55	Received Reassembled Succeeded
Received Header Errors	0	Received Reassembled Failed
Received Too Big Errors	0	Transmitted Forwards Datagrams
Received No Routes	0	Transmitted Requests
Received Address Errors	0	Transmitted Discards
Received Unknown Protocols	0	Transmitted No Routes
Received Truncated Packets	0	Transmitted Generated Fragments
Received Discards	0	Transmitted Fragment Succeeded
Received Delivers	55	Transmitted Fragment Failed
Received Reassembly Request Datagrams	0	

Clear

画面 1-265 :IPv6 統計情報の表示 (IPv6)

IP > IPv6 Configuration

Action: Show Statistics

Type ☐ IPv6 ☒ ICMPv6 ☐ UDP

ICMPv6 Statistics

Received Input	0	Transmitted Output	0
Received Errors	0	Transmitted Destination Unreachable Messages	0
Received Destination Unreachable Messages	0	Transmitted Packet Too Big Messages	0
Received Packet Too Big Messages	0	Transmitted Time Exceeded Messages	0
Received Time Exceeded Messages	0	Transmitted Parameter Problem Message	0
Received Parameter Problem Messages	0	Transmitted Echo Request Messages	0
Received Echo Request Messages	0	Transmitted Echo Reply Messages	0
Received Echo Reply Messages	0	Transmitted Router Solicit Messages	0
Received Router Solicit Messages	0	Transmitted Router Advertisement Messages	0
Received Router Advertisement Messages	0	Transmitted Neighbor Solicit Messages	0
Received Neighbor Solicit Messages	0	Transmitted Neighbor Advertisement Messages	0
Received Neighbor Advertisement Messages	0	Transmitted Redirect Messages	0
Received Redirect Messages	0	Transmitted Group Membership Query Messages	0

画面 1-266 :IPv6 統計情報の表示 (ICMPv6)

IP > IPv6

Action: Show Statistics

Type ☐ IPv6 ☐ ICMPv6 ☒ UDP

UDP Statistics

Input	10
No Port Errors	0
Other Errors	0
Output	1

Clear

画面 1-267 :IPv6 統計情報の表示 (UDP)

応答した宛先の MTU の表示

「IP」→「IPv6 Configuration」(Show MTU) を選択すると、ICMP パケットサイズ超過メッセージをスイッチで受信可能な MTU と共に返した宛先の MTU キャッシュを表示することができます。

関連する CLI 情報

「show ipv6 mtu」

パラメータ

以下のパラメータが表示されます。

パラメータ	説明
MTU	宛先から返された ICMP パケットサイズ超過メッセージに含まれていた調整済みの MTU であり、現在は、このパスで送信されるすべてのトラフィックに使用されている MTU。
Since	ICMP パケットサイズ超過メッセージが宛先から返された時点からの経過時間。
Destination Address	ICMP パケットサイズ超過メッセージの送信元アドレス。

表 1-17:MTU の表示 (表示内容の説明)

Web インターフェース

他のデバイスから報告された MTU を表示するには、以下のようになります。

- (1) 「IP」→「IPv6 Configuration」を選択します。
- (2) 「Step」リストで「Show MTU」を選択します。

IP > IPv6		
Action: Show MTU		
MTU Table Max: 10 Total: 2		
MTU	Since	Destination Address
1400	00:04:21	5000:1::3
1280	00:04:50	FE80::203:A0FF:FED6:141D

画面 1-268 : 報告された MTU 値の表示

1.15 一般的な IP ルーティング

本章は、以下のネットワーク機能に関する情報を提供します。

- ・ ping 機能の使用 – ping メッセージをネットワーク上の他のノードに送信します。
- ・ トレースルート機能の使用 – ICMP エコー要求パケットをネットワーク上の他のノードに送信します。
- ・ アドレス解決プロトコル – ARP エージングタイム、Proxy ARP、またはスタティックアドレスの設定方法を説明します。また、ARP キャッシュ内のダイナミックエントリを表示する方法も示します。
- ・ スタティックルートの設定 – 他のネットワークセグメントへのスタティックルートを設定します。
- ・ ルーティングテーブルの表示 – ダイナミックルーティングによって学習されたルーティングエントリおよび静的に設定されたルーティングエントリを表示します。
- ・ イコールコストマルチパスルーティング – 同じ宛先にトラフィックを送信できるイコールコストパスの最大数を設定します。

1.15.1 概要

本製品は、スタティックルーティングの定義とダイナミックルーティングプロトコル（RIP や OSPF など）による IP ルーティングとルーティングパス管理をサポートしています。IP ルーティングが機能している場合、スイッチは、ワイヤスピードルータとしての役割を果たし、異なる IP インターフェースを使用する VLAN 間でトラフィックを渡し、トラフィックを外部 IP ネットにルーティングします。ただし、スイッチの初回 Boot 時のデフォルトルーティングでは、ローカル IP インターフェース間でトラフィックを転送することしかできません。従来のルータと同様、まずは、スタティックルーティング機能とダイナミックルーティング機能が使用できる状態になるように設定する必要があります。

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 の機能のみを提供します。接続する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それらの VLAN に割り当て、IP インターフェースをそれぞれの VLAN に割り当てます。ネットワークを別々の VLAN に分割することにより、レイヤ 2 では接続されないサブネットワークに区切ることができます。同じサブネット内のネットワークトラフィックは、引き続きレイヤ 2 スイッチングを使用してスイッチングされます。そして、VLAN は、レイヤ 3 スイッチングを使用して（必要に応じて）相互に接続できるようになります。

それぞれの VLAN はレイヤ 3 への仮想インターフェースを表わします。それぞれの仮想インターフェースの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がレイヤ 3 スイッチングを使用してルーティングされるようになります。

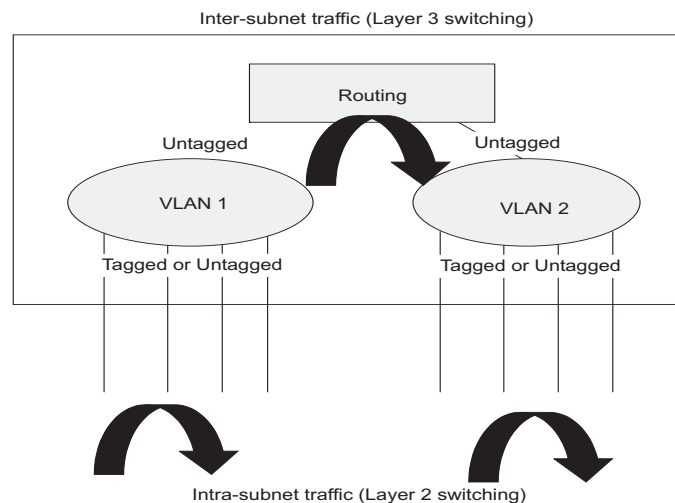


図 1-20: 仮想インターフェースとレイヤ 3 ルーティング

1.15.2 IP ルーティングおよび IP スイッチング

IP スイッチング（パケット転送）には、従来のルーティングに加え、レイヤ 2 とレイヤ 3 の両方についてパケットを転送するために必要なタスクが伴います。それらには、以下のものが含まれます。

- ・ 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く
 - ・ 各ホップの宛先 / 送信元 MAC アドレスの置き換え
 - ・ ホップカウンタのインクリメント
 - ・ TLV（Time-To-Live）のデクリメント
 - ・ レイヤ 3 チェックサムの検証と再計算

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にある場合には、パケットは、ルータによる中継を必要とせずに直接送信することができます。ただし、MAC アドレスがスイッチにとって不明なものである場合は、宛先 MAC アドレスを宛先ノードから取得するため、宛先 IP アドレスを含むアドレス解決プロトコル（ARP: Address Resolution Protocol）パケットがブロードキャストされます。すると、その宛先 MAC アドレスを使用して、IP パケットを直接送信できるようになります。

宛先がスイッチ上の他のサブネットに属している場合には、パケットを宛先ノードに直接ルーティングすることができます。一方、宛先がスイッチ上にはないサブネットに属している場合は、（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、および宛先ノードの宛先 IP アドレスを含む）パケットをネクストホップルータに送信しなければなりません。そのようにすると、ルータが適切なパスを使用してパケットを宛先ノードに転送できるようになります。また、ルータは、必要に応じて、ARP を使用してネクストホップルータの宛先ノードの MAC アドレスを検出することができます。

[注意] : IP スイッチングを実行するには、スイッチが他のネットワークノードで IP ルータとして認識されるようにしなければなりません。そのためには、スイッチをデフォルトゲートウェイとして設定するか、ICMP プロセスによる別のルータからのリダイレクトを使用します。

スイッチでそのスイッチ自体の MAC アドレス宛の IP パケットが受信された場合には、パケットはレイヤ 3 ルーティングプロセスに従って処理されます。まず、宛先 IP アドレスがレイヤ 3 アドレステーブルと照合されます。アドレスがまだレイヤ 3 アドレステーブル内にはない場合は、スイッチは、宛先 MAC アドレスを検出するため、ARP パケットを宛先 VLAN 上のすべてのポートにブロードキャストします。宛先 MAC アドレスが検出されると、パケットが再フォーマットされて、宛先に送信されます。再フォーマットプロセスでは、IP ヘッダの TTL (Time-To-Live) フィールド値がデクリメントされ、IP ヘッダのチェックサムが再計算されて、宛先 MAC アドレスが宛先ノードの MAC アドレスまたはネクストホップルータの MAC アドレスに置き換えられます。

以降は、同じノード宛の別のパケットが到着した場合には、宛先 MAC アドレスをレイヤ 3 アドレステーブルから直接取得することができ、パケットが再フォーマットされて宛先ポートに送信されます。IP スwitチングは、宛先アドレスエントリが既にレイヤ 3 アドレステーブル内にあれば、ワイヤスピードで実行されます。

スイッチでパケットをルーティングする必要があると判断された場合、ルートはセットアップ時にのみ計算されます。ルートが判別されたら、現行フローのすべてのパケットが、単にスウィッチングされるか、または、選択されたパスを経由して転送されます。この方法の場合、パスの計算がいったん実行されれば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なるので、優れたスループットとスウィッチングの低遅延が実現されるというメリットがあります。

ルーティングパス管理

ルーティングパス管理では、パケット転送に必要なすべてのルーティング情報を判別して更新しなければなりません。その一環として、以下のようなことが行われます。

- ・ ルーティングプロトコルの処理
- ・ ルーティングテーブルの更新
- ・ レイヤ 3 スウィッチングデータベースの更新

ルーティングプロトコル

本製品は、スタティックルーティングとダイナミックルーティングの両方をサポートしています。

- ・ スタティックルーティングでは、ルーティング情報をスイッチに手動で保存するか、接続のセットアップ時にスイッチ外部のアプリケーションによってルーティング情報がスイッチに保存されるようにする必要があります。
- ・ ダイナミックルーティングでは、ルーティングプロトコルを使用して、ルーティング情報の交換、ルーティングテーブルの計算、および、ネットワークのステータスまたは負荷が変化した場合の応答が実行されます。

1.15.3 IP ルーティングインターフェースの設定

ローカルインターフェースとリモートインターフェースの設定

「IP」→「General」→「Routing Interface」を選択すると、直接接続する IPv4 サブネット（「スイッチの IP アドレスの設定（IPv4）」を参照）のルーティングインターフェースを設定することができます。または、「IP」→「IPv6 Configuration」を選択して、直接接続する IPv6 サブネット（「スイッチの IP アドレスの設定（IPv6）」を参照）のルーティングインターフェースを設定することができます。

スイッチがルータとして特定のサブネットに割り当てられるエンドノードデバイスに直接接続している場合（または、共有メディアを使用してエンドノードに接続している場合）は、ルーティングをサポートする VLAN ごとにルータインターフェースを作成する必要があります。ルータインターフェースのアドレスは IP アドレスとサブネットマスクから設定されます。インターフェースアドレスは、ルータインターフェースが接続するネットワークのブリフィックス番号とそのネットワークにおけるルータのホスト番号の両方を定義します。つまり、ルータインターフェースアドレスは、インターフェースに接続されるネットワークセグメントを定義し、ルータに対する IP パケットの送受信を可能にするということです。

ルータに直接接続する IP サブネットを指定するには、IP アドレスを各 VLAN に手動で割り当てるか、BOOTP または DHCP を使用して動的に IP アドレスが各 VLAN に割り当てられるようにします。ルータに直接接続しない IP サブネットを指定するには、スタティックルートを設定するか、RIP または OSPF ダイナミックルーティングプロトコルを使用してネットワーク上の他のルータとプロトコルメッセージを交換して他のインターフェースへのルートが特定されるようにします。

IP インターフェースが設定されると、スイッチはマルチレイヤルーティングスイッチとして機能し、必要に応じてレイヤ 2 とレイヤ 3 のどちらかで動作するようになります。すべての IP パケットは、ローカルインターフェース間では直接ルーティングされ、ローカルインターフェースとリモートインターフェース間ではスタティックルーティングとダイナミックルーティングのどちらかを使用して間接的にルーティングされます。IP 以外のプロトコル（例えば、NetBuei、NetWare、AppleTalk など）を使用するすべてのパケットは、MAC アドレスに基づいてスイッチングされます。

リモート IP インターフェース間でトラフィックをルーティングするには、スイッチが他のネットワークノードで IP ルータとして認識されるようにしなければなりません。そのためには、自らをデフォルトゲートウェイとしてアドバタイズするようにスイッチを設定するか、ICMP プロセスによる別のルータからのリダイレクトを使用します。

自らをデフォルトゲートウェイとしてアドバタイズするようにスイッチが設定されている場合でも、宛先が不明であれば（パケットにマッチするエントリがルーティングテーブルにない）、ルーティングプロトコルを使用してネクストホップルータを判断する必要があります。他のルータがデフォルトゲートウェイとして指定されている場合には、スイッチは、ホストまたはサブネットが不明であれば、パケットをネクストホップルータに渡します。

IPv4 のデフォルトゲートウェイを設定するには、スタティックルーティングテーブルを参照）を使用して、IP アドレスとサブネットマスクに 0.0.0.0 を入力し、スイッチ自体または

他のルータをゲートウェイとして指定します。IPv6 のゲートウェイを設定するには、「IPv6 デフォルトゲートウェイの設定」を参照してください。

ping 機能の使用

「IP」→「General」→「Ping」を選択すると、ICMP エコー要求パケットをネットワーク上の他のノードに送信できるようになります。

関連する CLI 情報

「ping」

パラメータ

以下のパラメータが表示されます。

- ・ IP Address – ホストの IP アドレス。
- ・ Probe Count – 送信されるパケットの数（範囲:1 ～ 16）。
- ・ Packet Size – パケットのバイト数（範囲: 32 ～ 512 bytes）。

実際のパケットサイズは、ここで指定するサイズよりも 8 bytes 大きくなります。なぜならば、スイッチによってヘッダ情報が追加されるからです。

コマンドの使用

- ・ ping コマンドを使用して、ネットワーク上の他のサイトに到達できるかどうかを確認します。
- ・ ping コマンドを実行すると、以下のような結果が得られます。
 - ・ Normal response – 正常な応答が、ある時間内（1/10 秒単位）に発生します（この時間は、ネットワークトラフィックの状況によって異なります）。
 - ・ Destination does not respond – ホストが応答しない場合は、ある時間内（1/10 秒単位）に「timeout」と表示されます。
 - ・ Destination unreachable – 宛先が到達不能であることがその宛先のゲートウェイによって通知されます。
 - ・ Network or host unreachable – 該当するエントリがルーティングテーブルにないことがゲートウェイによって確認されました。

Web 設定

一般的な IP ルーティング

Web インターフェース

ネットワーク上の他のデバイスに対して ping を実行するには、以下のようにします。

- (1) 「IP」 → 「General」 → 「Ping」 を選択します。
- (2) ターゲットデバイスの IP アドレスおよび ping パラメータを指定します。
- (3) < Apply > ボタンをクリックします。

The screenshot shows the 'IP > General > Ping' configuration page. It includes input fields for 'IP Address' (192.168.2.61), 'Probe Count (1-16)' (16), and 'Packet Size (32-512)' (64 bytes). There are 'Apply' and 'Revert' buttons. Below the configuration fields is a 'Result' section displaying the output of a ping command: 'PING to 192.168.2.61, by 16 of 64-byte payload ICMP packets, timeout is 3 seconds'. The results show response times: 10 ms, 0 ms, 0 ms, 10 ms, 20 ms, 10 ms, 10 ms, 10 ms, 10 ms, 10 ms, 10 ms, 10 ms, 10 ms, 10 ms, 10 ms.

Field	Value
IP Address	192.168.2.61
Probe Count (1-16)	16
Packet Size (32-512)	64 bytes

Buttons: Apply, Revert

Result:

```
PING to 192.168.2.61, by 16 of 64-byte payload ICMP packets, timeout is 3 seconds
response time: 10 ms
response time: 0 ms
response time: 0 ms
response time: 10 ms
response time: 20 ms
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 10 ms
```

画面 1-269 : ネットワークデバイスの ping

トレースルート機能の使用

「IP」→「General」→「Trace Route」を選択すると、指定した宛先へのルートパケットを表示することができます。

関連する CLI 情報

「traceroute」

パラメータ

以下のパラメータが表示されます。

Destination IP Address - ホストの IP アドレス。

コマンドの使用

- ・ トレースルート機能を使用して、指定した宛先に到達するパスを判別します。
- ・ トレースは、宛先から応答が返された場合、タイムアウト期間（TTL）を超えた場合、または最大ホップ数を超えた場合、終了されます。
- ・ トレースルート機能では、最初に、TTL 値が 1 に設定されているプローブデータグラムが送信されます。すると、そのデータグラムが最初のルータで破棄され、エラーメッセージが返されます。次に、以降のそれぞれの TTL レベルのプローブメッセージがいくつか送信され、メッセージごとのラウンドトリップ時間が表示されます。すべてのデバイスが「ICMP Port Unreachable (ICMP ポート到達不能)」メッセージを返して正常に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に設定されている時間が経過すると、トレース機能によって一連のアスタリスク (*) と「Request Timed Out (要求タイムアウト)」メッセージがプリントされます。それらの長い一連のメッセージは、最大タイムアウト時間に達したときにのみ終了し、ターゲットデバイスに関する問題が発生している可能性あることを示します。

Web インターフェース

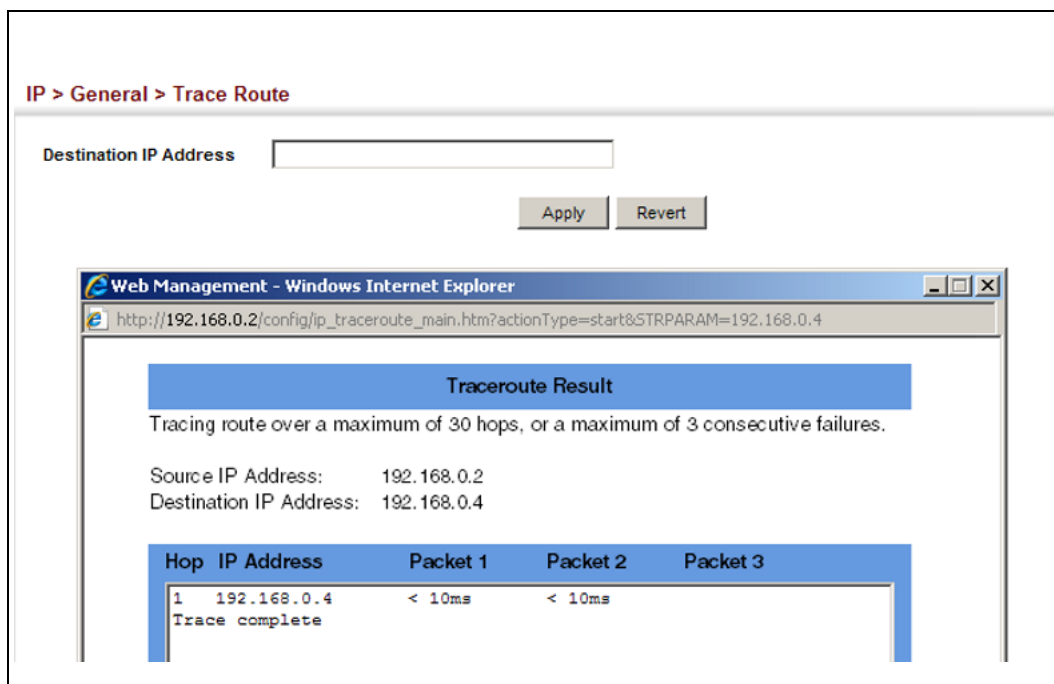
ネットワーク上の他のデバイスへのルートをトレースするには、以下のようにします。

- (1) 「IP」→「General」→「Trace Route」を選択します。
- (2) ターゲットデバイスの IP アドレスを指定します。

Web 設定

一般的な IP ルーティング

(3) < Apply > ボタンをクリックします。



画面 1-270 : ネットワークデバイスへのルートのトレース

1.15.4 アドレス解決プロトコル

IP ルーティングが有効になっている場合、ルータは、自らのルーティングテーブルを使用してルートを決し、アドレス解決プロトコル（ARP: Address Resolution Protocol）を使用してワンホップ手前のルータからのトラフィックを次のルータに転送します。ARP は、IP アドレスを物理レイヤ（つまり、MAC）アドレスにマップするために使用されます。ルータ（または、何らかの標準ベースのルータ）は、IP フレームを受信すると、最初に、宛先アドレスに対応する MAC アドレスを ARP キャッシュで検索します。MAC アドレスが見つかり、ルータは、その MAC アドレスをフレームヘッダ内の該当のフィールドに書き込み、そのフレームをネクストホップに転送します。パケットが最終的な宛先に配信されるまで、それぞれのルーティングデバイスが宛先 IP アドレスを受信先方向のネクストホップの MAC アドレスにマップするという方法で、IP トラフィックが最終的な宛先への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まったくない場合には、ルータは、ARP 要求パケットをネットワーク上のすべてのデバイスにブロードキャストします。ARP 要求には、以下の例に示すようなフィールドが含まれます。

パラメータ	説明
destination IP address	10.1.0.19
destination MAC address	?
source IP address	10.1.0.253
source MAC address	00-00-ab-cd-00-00

表 1-18: アドレス解決プロトコル

デバイスは、ARP 要求を受信すると、自らのアドレスがメッセージ内の宛先 IP アドレスにマッチしない場合は破棄します。ただし、マッチする場合には、自らのハードウェアアドレスを destination MAC address フィールドに書き込み、メッセージを送信元ハードウェアアドレスに送り返します。送信元デバイスは、応答を受信すると、宛先 IP アドレスと対応する MAC アドレスを自らのキャッシュに書き込み、IP トラフィックをネクストホップに転送します。キャッシュのエントリがタイムアウトにならない限り、ルータは、改めて ARP 要求をブロードキャストしなくても、エントリに対応する宛先については、トラフィックをネクストホップに直接転送できるようになります。

また、スイッチは、自らの IP アドレスに関する要求を受信した場合は、応答を送り返し、また、送信元デバイスの IP アドレスの MAC をキャッシュに書き込みます。

基本的な ARP 設定

「IP」→「ARP」（Configure General）を選択すると、ARP キャッシュエントリのタイムアウトを指定することや、個々の VLAN インターフェースの Proxy ARP を有効にすることができます。

関連する CLI 情報

「arp timeout」

「ip proxy-arp」

コマンドの使用

Proxy ARP

接続しているサブネット内のノードで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は、Proxy 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することができます。ルータは、リモートネットワークに関する ARP 要求を受信し、Proxy ARP が有効になっている場合は、それがリモートネットワークへの最適なルートがあるかどうかを判別し、自らの MAC アドレスを要求元ノードに送信して ARP 要求に応答します。すると、要求元ノードがトラフィックをルータに送信し、ルータは、自ら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。

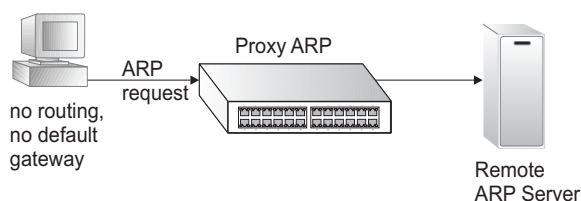


図 1-21:Proxy ARP

パラメータ

以下のパラメータが表示されます。

- ・ Timeout – ARP キャッシュのダイナミックエントリのエージングタイムを設定します（範囲：300 ～ 86,400 秒、デフォルト：1,200 秒（つまり 20 分））。

ARP のエージングタイムを設定することができます。

エージングタイムによってダイナミックエントリがキャッシュで保持される期間が決まります。タイムアウトまでの期間が短すぎると、ルータが、最近テーブルから消去されたアドレスに関する ARP 要求を繰り返し送信して、リソースを独占してしまう可能性があります。

ARP エントリは期限切れになるとキャッシュから削除され、再び MAC アドレスを取得するために ARP 要求パケットが送信されます。

- ・ Proxy ARP – 指定した VLAN の Proxy ARP を有効して、非ルーティングデバイスが他のサブネットまたはネットワークのホストの MAC アドレスを判別できるようにします（デフォルト：Disabled）。

Proxy ARP を必要とするエンドステーションでは、ネットワーク全体が単一のネットワークとしてみなされなければなりません。そのため、ルータやその他の該当のネットワークデバイスで使用するよりも小さいサブネットマスクを使用する必要があります。

Proxy ARP を過度に使用すると、ARP トラフィックが増加し、ARP アドレステーブルが大きくなって検索に時間がかかるようになるため、ルータのパフォーマンスが低下することがあります。

Web インターフェース

ARP キャッシュのタイムアウトを設定したり、VLAN（IP サブネットワーク）の Proxy ARP を有効にしたりするには、以下のようにします。

- (1) 「IP」 → 「ARP」 を選択します。
- (2) 「Step」 リストで 「Configure General」 を選択します。
- (3) タイムアウトを ARP キャッシュに適した値に設定するか、ルーティングまたはデフォルトゲートウェイがないサブネットワークの Proxy ARP を有効にします。
- (4) < Apply > ボタンをクリックします。

The screenshot shows the 'IP > ARP' configuration page. At the top, there is a breadcrumb 'IP > ARP'. Below it, a 'Step:' dropdown menu is set to '1. Configure General'. The main configuration area includes a 'Timeout (300-86400)' field with the value '1200' and a 'sec' unit. Below this, the 'Proxy ARP' section is visible, containing a 'VLAN' dropdown set to '1' and a 'Status' checkbox labeled 'Enabled' which is currently unchecked. At the bottom right, there are two buttons: 'Apply' and 'Revert'.

画面 1-271 :ARP の全般設定の設定

スタティック ARP アドレスの設定

ARP 要求に応答しないか、タイムアウトが発生する前に応答しないデバイスに関しては、IP アドレスを物理アドレスにマップできないため、トラフィックがドロップされます。そのようなことが発生する場合は、「IP」→「ARP」(Configure Static Address - Add)を選択して、ARP キャッシュで IP アドレスを対応する物理アドレスに手動でマップします。

関連する CLI 情報

「arp」

コマンドの使用

- ・ ARP キャッシュは、32 bits の IP アドレスを 48 bits のハードウェアアドレス（つまり、MAC）にマップするために使用されます。ARP キャッシュには、ルータで定義されているローカルネットワークインターフェース上のホストおよび他のルータのエントリが含まれます。
- ・ 最大 128 のスタティックエントリを ARP キャッシュで定義することができます。
- ・ スタティックエントリは、ARP ブロードキャストメッセージに対する応答がないときに使用することが必要になる場合があります。例えば、アプリケーションによっては ARP 要求に応答できない場合や、応答が到着するのが遅すぎる場合があります、その結果、ネットワークオペレーションがタイムアウトすることがあります。
- ・ スタティックエントリは、期限切れになったり、電源リセット時に削除されたりしません。

パラメータ

以下のパラメータが表示されます。

- ・ IP Address – 物理 MAC アドレスに静的にマップされる IP アドレス（有効な IP アドレスは、0 ～ 255 の数値を 4 つ組み合わせ、それぞれをピリオドで区切って設定されます）。
- ・ MAC Address – 対応する IP アドレスに静的にマップされる MAC アドレス（有効な MAC アドレスは、xx-xx-xx-xx-xx-xx という形式の 16 進数です）。

Web インターフェース

Web インターフェースを使用して ARP キャッシュで IP アドレスを対応する物理アドレスにマップするには、以下のようにします。

- (1) 「IP」→「ARP」を選択します。
- (2) 「Step」リストで「Configure Static Address」を選択します。
- (3) 「Step」リストで「Add」を選択します。
- (4) IP アドレスおよび対応する MAC アドレスを入力します。

(5) < Apply > ボタンをクリックします。

The screenshot shows the 'IP > ARP' configuration page. At the top, there is a breadcrumb 'IP > ARP'. Below it, the 'Step' is set to '2. Configure Static Address' and the 'Action' is 'Add'. There are two input fields: 'IP Address' with the value '10.2.78.105' and 'MAC Address' with the value '00-e0-0c-00-00-fd'. At the bottom right, there are 'Apply' and 'Revert' buttons.

画面 1-272 : スタティック ARP エントリの設定

ARP キャッシュ内のスタティックエントリを表示するには、以下のようにします。

1. 「IP」 → 「ARP」 を選択します。
2. 「Step」 リストで 「Configure Static Address」 を選択します。
3. 「Step」 リストで 「Show」 を選択します。

The screenshot shows the 'IP > ARP' configuration page with the 'Action' set to 'Show'. Below the configuration fields, there is a table titled 'Static Address List' with the following data:

	IP Address	MAC Address	Interface
☐	10.2.78.105	00-E0-0C-00-00-FD	VLAN 1
☐	10.2.78.254	00-12-D9-75-DC-5B	VLAN 1

At the bottom right, there are 'Delete' and 'Revert' buttons.

画面 1-273 : スタティック ARP エントリの表示

ダイナミック ARP エントリまたはローカル ARP エントリの表示

ARP キャッシュには、スタティックエントリおよびローカルインターフェースのエントリ（サブネット、ホスト、およびブロードキャストのそれぞれのアドレスを含む）が保存されます。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に対する応答によって動的に学習されます。「IP」→「ARP」（Show Information）を選択すると、ARP キャッシュ内のダイナミックエントリまたはローカルエントリを表示することができます。

関連する CLI 情報

「show arp」

Web インターフェース

ARP キャッシュ内のすべてのダイナミックエントリを表示するには、以下のようにします。

- (1) 「IP」→「ARP」を選択します。
- (2) 「Step」リストで「Show Information」を選択します。
- (3) 「Dynamic Address」を選択します。

The screenshot shows the 'IP > ARP' configuration page. Under the 'Step' dropdown, '3. Show Information' is selected. Below this, there are three radio buttons: 'Dynamic Address' (selected), 'Other Address', and 'Statistics'. A 'Dynamic Address List' is displayed with the following data:

IP Address	MAC Address	Interface
192.168.2.61	00-60-6E-00-5F-A1	VLAN 1

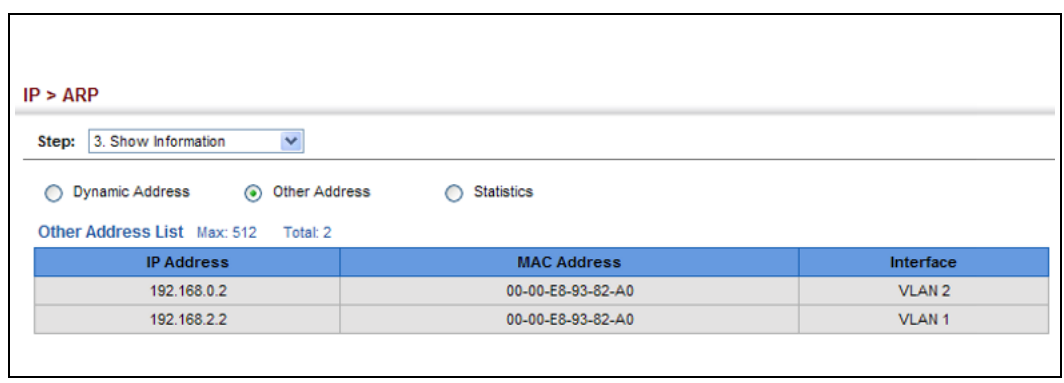
A 'Clear' button is located at the bottom right of the table.

画面 1-274 : ダイナミック ARP エントリの表示

ARP キャッシュ内のダイナミックエントリ以外のすべてのローカルエントリを表示するには、以下のようにします。

1. 「IP」→「ARP」を選択します。
2. 「Step」リストで「Show Information」を選択します。

3. 「Other Address」を選択します。



画面 1-275 : ローカル ARP エントリの表示

ARP に関する統計情報の表示

「IP」→「ARP」(Show Information) を選択して表示される画面で「Statics」オプションを選択すると、ルータのすべてのインターフェースを経由する ARP メッセージに関する統計情報を表示することができます。

関連する CLI 情報

「show ip traffic」

パラメータ

以下のパラメータが表示されます。

パラメータ	説明
Received Request	ルータで受信された ARP Request パケットの数。
Received Reply	ルータで受信された ARP Reply パケットの数。
Sent Request	ルータで送信された ARP Request パケットの数。
Sent Reply	ルータで送信された ARP Reply パケットの数。

表 1-19:ARP に関する統計情報

Web インターフェース

ARP に関する統計情報を表示するには、以下のようになります。

- (1) 「IP」→「ARP」を選択します。
- (2) 「Step」リストで「Show Information」を選択します。

Web 設定

一般的な IP ルーティング

(3) 「Statistics」を選択します。

The screenshot shows a web interface for IP configuration. At the top, it says "IP > ARP". Below this is a "Step:" dropdown menu set to "3. Show Information". There are three radio buttons: "Dynamic Address", "Other Address", and "Statistics". The "Statistics" radio button is selected. Below the radio buttons, the section "ARP Statistics" is displayed. It contains two columns of statistics: "Received Request" (31), "Received Reply" (5), "Sent Request" (5), and "Sent Reply" (16). At the bottom right of the statistics section is a "Refresh" button.

ARP Statistics			
Received Request	31	Sent Request	5
Received Reply	5	Sent Reply	16

画面 1-276 :ARP に関する統計情報の表示

1.15.5 スタティックルートの設定

本製品は、ルータとして、ダイナミックルーティングプロトコル（RIP や OSPF など）を使用して他のネットワークセグメントへのルートを動的に設定することができます。ただし、「IP」→「Routing」→「Static Routes」（Add）を選択して、手動でスタティックルートをルーティングテーブルに入力することもできます。スタティックルートは、ダイナミックルーティングをサポートしていないネットワークセグメントにアクセスする場合に必要なことがあります。または、スタティックルートは、ダイナミックルーティングを使用する代わりに、サブネットに対する特定のルートが使用されるようにする場合に設定することができます。スタティックルートは、ネットワークトポロジの変化に応じて自動的に変更されないため、ネットワークのアクセシビリティが確保されるようにするため、ごくわずかな数の安定したルートのみを設定してください。

関連する CLI 情報

「ip route」

コマンドの使用

- ・ 最大 512 のスタティックルートを設定することができます。
- ・ スタティックルーティングについては最大 8 つのイコールコストマルチパス（ECMP: Equal-Cost Multipath）を設定することができます（「イコールコストマルチパスルーティング」を参照）。
- ・ スタティックルートの管理距離が定義されており、ダイナミックルートを使用するとより短い管理距離で同じ宛先に到達できる場合は、ダイナミックルートが使用されます。
- ・ スタティックパスとダイナミックパスの両方の最低コストが同じ場合は、ルーティングテーブルに保存されている順序が先の方のルートが使用されます（静的に設定されているルートか、ルーティングプロトコルを使用して動的に学習されたルートかは関係ありません）。
- ・ スタティックルート情報は、ルータによって定期的送信される RIP および OSPF 更新パケットに含まれます（ただし、この機能が RIP または OSPF で有効にされている場合）。

パラメータ

以下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、ホストのいずれかの IP アドレス。
- ・ Netmask / Prefix Length - 関連付けられている IP サブネットのネットワークマスク。このマスクは、個々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示します。
- ・ Next Hop - ルートで使用されるネクストホップルータの IP アドレス。
- ・ Distance - 管理距離であり、ダイナミックルートの距離がスタティックルートについて設定されている距離よりも短い場合は、ルートをダイナミックルーティング情報によって上書きできることを示します。ただし、ダイナミックユニキャストルーティングプロトコルで使用されるデフォルトの管理距離は、OSPF の場合は 110 であり、RIP の場合は 120 であるという点に注意してください（範囲：1 ～ 255、デフォルト：1）。

Web 設定

一般的な IP ルーティング

Web インターフェース

スタティックルートを設定するには、以下のようにします。

- (1) 「IP」 → 「Routing」 → 「Static Routes」 を選択します。
- (2) 「Step」 リストで 「Add」 を選択します。
- (3) 宛先アドレス、サブネットマスク、およびネクストホップルータを入力します。
- (4) < Apply > ボタンをクリックします。

The screenshot shows the 'IP > Routing > Static Routes' configuration page. The 'Action' dropdown is set to 'Add'. The form contains the following fields:

Destination IP Address	10.2.48.0
Net Mask / Prefix Length	255.255.255.0
Next Hop	10.2.48.1
Distance (1-255)	5 (Optional)

At the bottom right, there are 'Apply' and 'Revert' buttons.

画面 1-277 : スタティックルートの設定

スタティックルートを表示するには、以下のようにします。

1. 「IP」 → 「Routing」 → 「Static Routes」 を選択します。
2. 「Step」 リストで 「Show」 を選択します。

The screenshot shows the 'IP > Routing > Static Routes' configuration page. The 'Action' dropdown is set to 'Show'. Below the form, there is a table titled 'Static Table List' with the following data:

	Destination IP Address	Net Mask / Prefix Length	Next Hop	Distance
☐	10.2.48.2	255.255.255.0	10.2.48.1	5
☐	10.5.36.123	255.255.0.0	10.5.36.1	2
☐	5566::	60	7788::12	1

At the bottom, there are 'Delete' and 'Revert' buttons.

画面 1-278 : スタティックルートの表示

1.15.6 ルーティングテーブルの表示

「IP」→「Routing」→「Routing Table」を選択すると、ローカルネットワークインターフェース、スタティックルート、または動的に学習されたルートを使用してアクセスできるすべてのルートを表示することができます。それらのうちの複数の方法を使用してルート情報を取得できる場合、ルート選択の優先順位は、ローカルルート、スタティックルート、ダイナミックルートの順になります（ただし、ダイナミックルートの距離パラメータがスタティックルートの距離よりも優先される値に設定されている場合を除きます）。また、ローカルインターフェースのルートは、そのインターフェースに接続されているアクティブなリンクが少なくとも 1 つなければ、有効になりません（つまり、ルーティングテーブルに含まれません）。

関連する CLI 情報

「show ip route」

コマンドの使用

- ・ 転送情報ベース（FIB: Forwarding Information Base）には、IP トラフィックを転送するのに必要な情報が含まれます。それらの情報とは、IP ルーティングテーブルに基づく到達可能な宛先ネットワークのプレフィックスごとのインターフェース ID とネクストホップ情報です。ネットワーク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、それらの変更が即座に FIB に反映されます。
FIB は、ルーティングピアから受信されたすべてのルーティング情報が保持されるルーティングテーブル（つまり、ルーティング情報ベース（RIB: Routing Information Base））とは個別のものです。FIB には、一意のパスのみが含まれ、セカンダリパスは一切含まれません。FIB エントリは、特定のパケットの転送に関する決定を行うために必要な最小限の情報から設定されています。FIB エントリの代表的な設定要素は、ネットワークプレフィックス、ルータ（VLAN）インターフェース、およびネクストホップ情報です。
- ・ 「Routing Table」（または show ip route コマンドを実行した場合）には、その時点で転送のためにアクセスできるルートのみが表示されます。ルータはネクストホップに直接到達できなければならないので、ダイナミックルートエントリまたはスタティックルートエントリに関連付けられている VLAN は Up 状態でなければなりません。show ip route database コマンドを使用した場合はその時点で転送のためにアクセスできないルートも表示されることがあるので注意してください。

パラメータ

以下のパラメータが表示されます。

- ・ VLAN – VLAN ID（有効な IP サブネットとして設定されているもの）。
- ・ Destination IP Address – 宛先ネットワーク、サブネットワーク、ホストのいずれかの IP アドレス。アドレス 0.0.0.0 はルータのデフォルトゲートウェイを示すということに注意してください。
- ・ Net Mask / Prefix Length – 関連付けられている IP サブネットのネットワークマスク。このマスクは、個々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示します。
- ・ Next Hop – ルートのネクストホップ（またはゲートウェイ）の IP アドレス。
- ・ Metric – インターフェースのコスト。
- ・ Protocol – ルート情報を生成するときに使用されたプロトコル（オプション：Local、Static、RIP、OSPF、Others）。

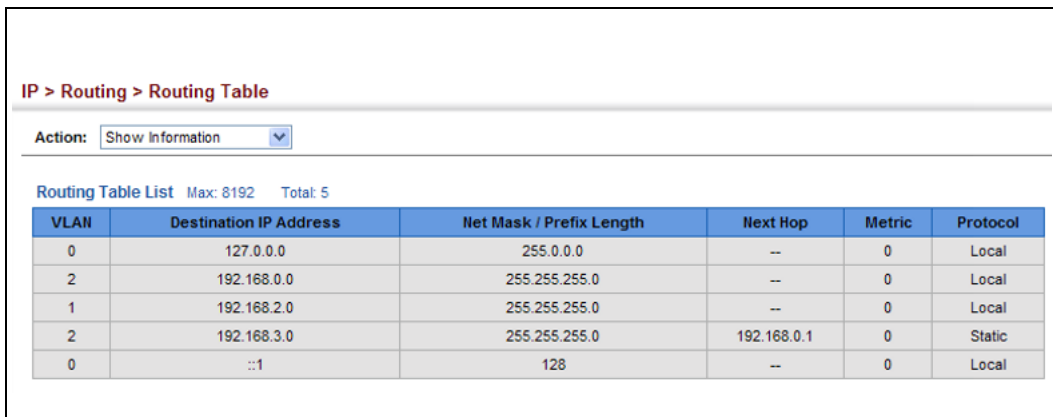
Web 設定

一般的な IP ルーティング

Web インターフェース

ルーティングテーブルを表示するには、以下のようにします。

- (1) 「IP」 → 「Routing」 → 「Routing Table」 を選択します。
- (2) 「Step」 リストで 「Show Information」 を選択します。



IP > Routing > Routing Table					
Action: Show Information					
Routing Table List Max: 8192 Total: 5					
VLAN	Destination IP Address	Net Mask / Prefix Length	Next Hop	Metric	Protocol
0	127.0.0.0	255.0.0.0	--	0	Local
2	192.168.0.0	255.255.255.0	--	0	Local
1	192.168.2.0	255.255.255.0	--	0	Local
2	192.168.3.0	255.255.255.0	192.168.0.1	0	Static
0	::1	128	--	0	Local

画面 1-279 : ルーティングテーブルの表示

1.15.7 イコールコストマルチパスルーティング

「IP」→「Routing」→「Routing Table」（Configure ECMP Number）を選択すると、トラフィックを同じ宛先に送信できるイコールコストパスの最大数を設定することができます。ECMP アルゴリズムは、同じ宛先に渡されるデータについて複数のイコールコストパスでの負荷共有をサポートする手法です。同じ宛先に対するパスコストが等価である複数のパスがルーティングテーブルで検出されると常に、ECMP まず、そのコストがルーティングテーブル内の他のどのエントリよりも少ないかがアルゴリズムによってチェックされます。コストがテーブル内のエントリで最も少なければ、スイッチは、最低コストが同じ最大 8 つのパスを使用して、宛先に転送されるトラフィックの負荷を分散させます。

ECMP では、スタティックルーティングテーブルで手動設定されるイコールコストマルチパスと OSPF（Open Shortest Path First）アルゴリズムによって動的に生成されるイコールマルチパスのいずれかが使用されます。つまり、スタティックエントリと OSPF エントリのいずれかが使用され、両方が使用されることはないということです。通常のユニキャストルーティングでは、単に、宛先までのパスの中でコストが最も低いものが選択されるだけです。

マルチキャストルーティングでは、やはり、最低コストのパスが選択されますが、最低コストのパスが複数ある場合は、それらを使用してトラフィックを転送することができます。本製品では、ECMP はデフォルトで有効になっています。宛先への最低コストパスが 1 つしかない場合は、そのパスを使用してすべてのトラフィックが転送されます。スタティックルーティングテーブルで設定される（「スタティックルートの設定」を参照）か、OSPFv2 によって動的に生成される（「OSPF プロトコル（バージョン 2）の設定」を参照）最低コストパスが複数ある場合は、最低コストが等価である最大 8 つのパスを使用してトラフィックを宛先に転送することができます。

関連する CLI 情報

「maximum-paths」

コマンドの使用

- ・ ECMP では、同じプロトコルタイプのパスのみが選択されます。同じ宛先についてスタティックパスとダイナミックパスの両方を同時に適用することはできません。スタティックパスとダイナミックパスの両方の最低コストが等価である場合は、スタティックパスがダイナミックパスに優先します。
- ・ ルーティングテーブルでは、同じ宛先に対して最低コストが等価であるパスごとに 1 つのエントリを使用してルーティング情報が記録されます。つまり、パスが 8 つあるルートについてはエントリが 8 つ使用されるということです。
- ・ スタティックルーティングとダイナミックルーティングで共通の宛先についてルーティングテーブルに保持できるエントリ数は、それぞれ最大 8 つです。ただし、本システムでは、ファストスイッチングについては ASIC で最大合計 256 の ECMP エントリをサポートし、さらに、その他にソフトウェアルーティングによって処理されるエントリをサポートします。
- ・ 同じ宛先についてコストが等価である複数のパスが存在する場合、システムは、それらのパスの 1 つを選択し、負荷分割アルゴリズムを適用して各パケットを宛先に転送します。

ハッシュ値が、各パケットの destination IP address フィールドと source IP address フィールドに基づいて、複数のパスの 1 つに対する間接インデックスとして計算されます。それぞれのトラフィックフローを特定できるパケットヘッダ情報に基づいてハッシュ値が計算されるので、この手法を使用すると、個々のフローについてパスが変更される回数を最小限に抑えることができます。一般的に、個々のフローに関する

Web 設定

一般的な IP ルーティング

パス変更は、マルチパスグループに対してパスが追加または削除された場合にのみ発生します。

パラメータ

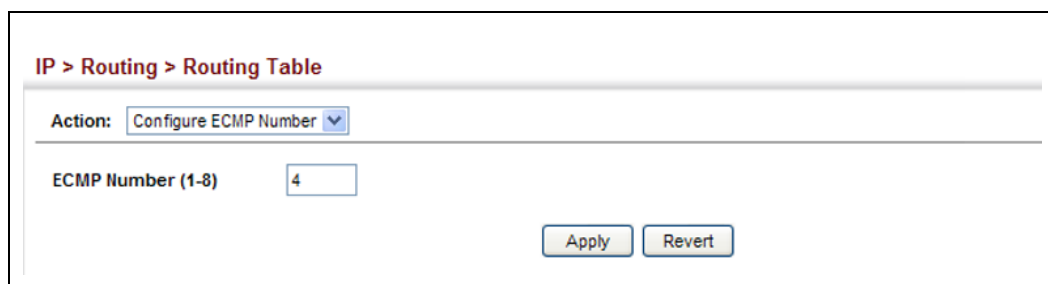
以下のパラメータが表示されます。

- ・ ECMP Number - ルーティングテーブルにインポートできる、同じ宛先に対するイコールコストパスの最大数を設定します（範囲：1～8、デフォルト：4）。

Web インターフェース

ECMP の最大数を設定するには、以下のようにします。

- (1) 「IP」 → 「Routing」 → 「Routing Table」 を選択します。
- (2) 「Step」 リストで 「Configure ECMP Number」 を選択します。
- (3) 同じ宛先へのトラフィックのルートに使用されるイコールコストパスについてスイッチで許可される最大数を入力します。
- (4) < Apply > ボタンをクリックします。



The screenshot shows a web interface for configuring ECMP Number. The breadcrumb navigation at the top reads "IP > Routing > Routing Table". Below this, there is a section titled "Action:" with a dropdown menu set to "Configure ECMP Number". Underneath, the label "ECMP Number (1-8)" is followed by a text input field containing the value "4". At the bottom right of the form, there are two buttons: "Apply" and "Revert".

画面 1-280 :ECMP の最大数の設定

1.16 ルータ冗長性の設定

ルータ冗長プロトコルは、仮想 IP アドレスを使用して、1つのプライマリルータと複数のバックアップルータをサポートします。バックアップルータは、マスタールータで障害が発生した場合にワークロードを引き継ぐように設定したり、トラフィックの負荷を共有するように設定したりすることができます。ルータ冗長化の主要な目的は、固定ゲートウェイを指定して設定されたホストデバイスが、プライマリゲートウェイがダウンした場合にネットワークの接続性を保持できるようにすることです。

本製品は、仮想ルータ冗長プロトコル（VRRP: Virtual Router Redundancy Protocol）をサポートしています。VRRP を使用すると、仮想グループに加入しているルータの1つのインターフェースのアドレスをマスタ仮想ルータのアドレスとして指定したり、マスタ仮想ルータについて任意のアドレスを設定したりすることができます。そのようにすると、指定されている仮想ルータの優先度に基づいてバックアップルータが選択されるようになります。

ルータ冗長化は、以下のうちの任意の方法でセットアップすることができます。これらの例では、加入ルータの1つのアドレスをマスタールータのアドレスとして使用しています。仮想ルータ IP アドレスが実アドレスではない場合は、マスタールータが優先度に基づいて選択されます。いくつかのルータの優先度が同じ場合は、IP アドレスの値が最も大きいルータがマスタとして選択されます。

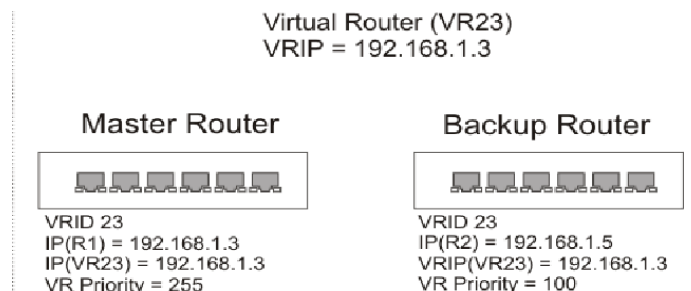


図 1-22: マスタ仮想ルータとバックアップルータ

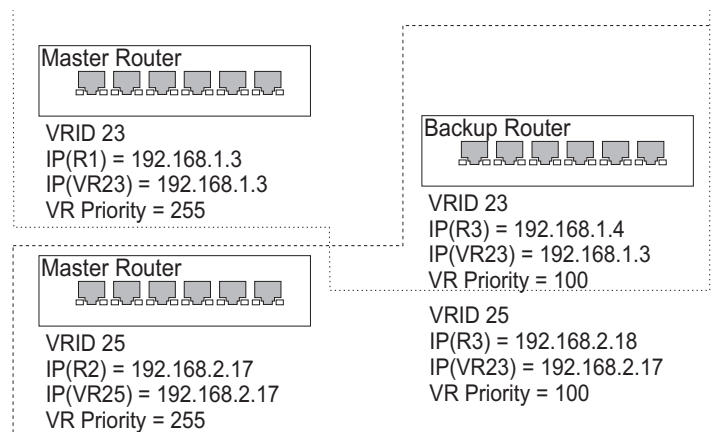


図 1-23: バックアップルータを使用する複数のマスタ仮想ルータ

Web 設定

ルータ冗長性の設定

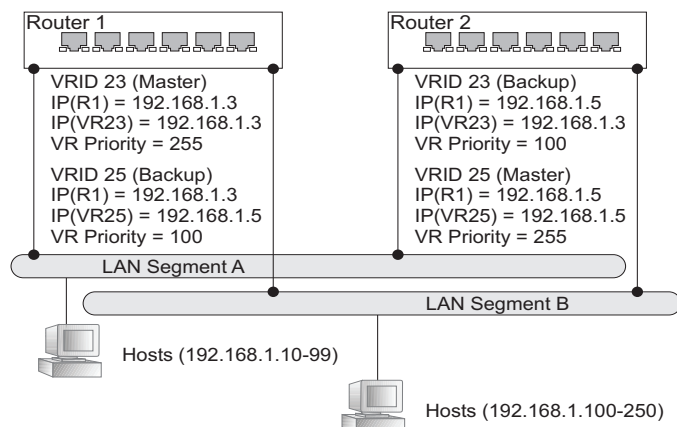


図 1-24: 相互バックアップと負荷共有を実現するように設定された複数のマスタ仮想ルータ

[注意] : 負荷共有は、DHCP サーバを使用してアドレスのサブセットを別々のホストアドレスプールに割り当てることによって実現できます（「アドレスプールの設定」を参照）。

1.16.1 VRRP グループの設定

「IP」→「VRRP」を選択すると、VRRP を設定することができます。VRRP グループを設定するには、マスタールータまたはバックアップルータとしてプロトコルサービスに加入するグループ内の各ルータでインターフェースを 1 つ選択します。特定のデバイスがマスタールータとして選択されるようにするには、そのデバイスのインターフェースのアドレスをグループの仮想ルータアドレスとして設定します。それから、同じ仮想アドレスと優先度をバックアップルータに設定し、認証文字列を指定します。また、プリエンプト機能を有効にして、ルータがオンラインになったときにそのルータがその時点でアクティブなマスタールータよりも優先度が高ければ代わりにマスタールータとなるようにすることもできます。

関連する CLI 情報

「VRRP Commands」

コマンドの使用

アドレスの割り当て

- ・ 特定の仮想ルータを VRRP マスタとして指定するには、その仮想ルータに割り当てられる IP アドレスがグループアドレスのオーナーとなるルータで事前に設定されていなければなりません。つまり、仮想ルータの IP アドレスが仮想ルータグループ内のただ 1 つのルータ上に存在し、仮想ルータアドレスのネットワークマスクがグループアドレスのオーナーから取得されるということです。また、オーナーはグループ内のマスタ仮想ルータの役割を果たします。
- ・ ルータグループのいずれのルータ上にもない仮想アドレスがグループに割り当てられている場合には、マスタールータは優先度に基づいて選択されます。グループ内のいくつかのルータの優先度が同じ場合は、IP アドレスの値が最も大きいルータがマスタールータとしてグループから選択されます。
- ・ 複数のセカンダリアドレスを現行の VLAN インターフェースで設定している場合は、それらのアドレスのうち、任意のものを仮想ルータグループに追加することができます。
- ・ 仮想ルータグループに加入しているすべてのルータのインターフェースは同じ IP サブネット内になければなりません。
- ・ VRRP では、標準プリフィックスに基づいてマスタールータの仮想 MAC アドレスが作成されます（末尾のオクテットはグループ ID と同じになります）。バックアップルータは、マスタールータの役割を引き継いだ場合は、この仮想 MAC アドレス宛のトラフィックの転送を継続します。ただし、IP アドレスのオーナーがオフラインであるため、仮想グループに関連付けられているアドレスに送信される ICMP ping には応答できません。

仮想ルータの優先度

- ・ 仮想 IP アドレスのオーナーには、自動的に、使用可能な最高優先度である 255 が割り当てられます。現行のマスタで障害が発生すると、優先度が最も高いバックアップルータがマスタールータになります。ただし、仮想 IP アドレスのオーナーの優先度が最も高いため、元々のマスタールータは、回復すると必ずアクティブなマスタになります。
- ・ 2 つ以上のルータに同じ VRRP 優先度が設定されている場合、現行のマスタールータで障害が発生したときには、IP アドレスが最も大きいルータが新しいマスタールータとして選択されます。

アクティブマスタのプリエンプト

- ・ 仮想 IP アドレスのオーナーは、優先度が最も高いため、他のルータがプリエンプトすることはできず、また、オンライン状態に戻ると必ずマスタ仮想ルータとして制御を取り戻します。プリエンプト機能では、バックアップルータは、グループ内に仮想 IP アドレスのオーナーであるルータがない場合にのみ、マスタルータ（または、一時的にグループマスタとして機能している他のバックアップルータ）の役割を引き継ぐことができます。プリエンプト機能が有効になっている場合には、あるルータが現在マスタとして機能しているルータよりも優先度が高ければ、そのルータは、オンラインになると、グループのマスタとしての役割を引き継ぎます。
- ・ プリエンプト機能の遅延期間を指定して、制御を引き継ぐ前に現行のマスタからのアドバタイズメントメッセージを受信するための猶予時間が設けられるようにすることができます。そのように遅延期間を設定すると、マスタになろうとしているルータがオンラインになったときにも役立ちます。ルータは、その時点でアクティブになっているマスタルータを実際にプリエンプトする前に、自らのルーティングテーブルのための情報を収集する時間を確保できるようになります。

パラメータ

以下のパラメータが表示されます。

VRRP グループの追加

- ・ VRID – VRRP グループ ID（範囲：1 ～ 255）。
- ・ VLAN – IP インターフェースを指定して設定されている VLAN の ID（範囲：1 ～ 4,093、デフォルト：1）。

仮想 IP アドレスの追加

- ・ VLAN – IP インターフェースを指定して設定されている VLAN の ID（範囲：1 ～ 4,093）。
- ・ VRID – VRRP グループ ID（範囲：1 ～ 255）。
- ・ IP Address – グループの仮想 IP アドレス。

ルータ上の実インターフェースの IP アドレスを使用して、そのインターフェースをグループのマスタ仮想ルータにします。あるいは、既存のグループの仮想アドレスを使用して、そのグループをバックアップルータにするか、または、グループアドレスのオーナーとして設定されている他のメンバーがない場合には指定されている優先度に基づいてマスタが選択されるようにします。

詳細設定の設定

- ・ VLAN ID – IP インターフェースを指定して設定されている VLAN の ID（範囲：1 ～ 4,093）。
- ・ VRID – VRRP グループ ID（範囲：1 ～ 255）。
- ・ Advertisement Interval – マスタ仮想ルータが自らのマスタとしての状態を通知するアドバタイズメントを送信する間隔（範囲：1 ～ 255 秒、デフォルト：1 秒）。
- ・ 現行のマスタ仮想ルータからの VRRP アドバタイズメントには、そのルータの優先度とマスタとしての現在の状態に関する情報が含まれます。
- ・ VRRP アドバタイズメントはマルチキャストアドレス 224.0.0.8 宛に送信されます。マルチキャストアドレスを使用することにより、指定された VRRP グループのメンバーではないネットワークデバイスが処理するトラフィックの量を減らします。

- ・ マスタルータがアドバタイズメントの送信を停止すると、バックアップルータが優先度に基づいてマスタルータになります。マスタとしての役割を引き継ぐ前の猶予期間は、hello 期間の 3 倍に 0.5 秒を加えたものになります。
- ・ Priority - VRRP グループにおけるルータの優先度（範囲：1 ～ 254、デフォルト：100）。
 - ・ VRRP グループアドレスのオーナーの優先度は自動的に 255 に設定されます。
 - ・ バックアップルータの優先度は、現行のマスタルータで障害が発生した場合にマスタとしての役割を引き継ぐルータを判別するために使用されます。
- ・ Preempt Mode - バックアップルータが現在マスタ仮想ルータとして機能しているルータ（グループアドレスオーナーではないマスタルータ、または以前のマスタから役割を引き継いだバックアップルータ）よりも優先度が高い場合にマスタとしての役割を引き継ぐことができるようにします。（デフォルト：Enabled）。
- ・ Preempt Delay Time - マスタとなることを宣言するメッセージを送信する前の待機時間（範囲：0 ～ 120 秒、デフォルト：0 秒）。
- ・ Authentication Mode - 他のルータから受信した VRRP パケットの検証に使用される認証モード（オプション：None または Simple Text、デフォルト：None）。

認証モードとして「Simple Text」を選択する場合は、認証文字列も入力する必要があります。

同じ VRRP グループのすべてのルータには、同じ認証モードを設定し、同じ認証文字列を指定しなければなりません。

プレーンテキスト認証を使用しても、実質的にはセキュリティは確保されません。プレーンテキスト認証は、正しく設定されていないルータが VRRP グループに加入しないようにすることのみを目的としてサポートされています。
- ・ Authentication String - 他のルータから受信した VRRP パケットの認証に使用されるキー（範囲：1 ～ 8 文字の英数字）。

あるルータがグループ内の他のルータから VRRP パケットを受信した場合、その送信元ルータの認証文字列が、受信先ルータで設定されている認証文字列と照合されます。文字列がマッチすると、メッセージが受け入れられます。マッチしない場合は、パケットが破棄されます。
- ・ State - VRRP ルータの役割（値：Master または Backup）。
- ・ Virtual MAC Address - グループの仮想 MAC アドレス。
- ・ Master Router - グループのプライマリルータとして機能するルータ。
- ・ Master Priority - マスタルータの優先度。
- ・ Master Advertisement Interval - マスタルータが自らをグループマスタとしてアドバタイズするメッセージを送信する間隔。
- ・ Master Down Interval - このパラメータで設定されている時間を過ぎてもマスタルータからのアドバタイズメントメッセージが受信されない場合、バックアップルータはマスタルータがダウンしているものとみなし、グループマスタとなるバックアップルータの選定が開始されます。

Web インターフェース

VRRP を設定するには、以下のようにします。

- (1) 「IP」 → 「VRRP」 を選択します。
- (2) 「Step」 リストで 「Configure Group ID」 を選択します。
- (3) 「Step」 リストで 「Add」 を選択します。
- (4) VRID グループ番号を入力し、グループが担当する VLAN（つまり、IP サブネット）を選択します。
- (5) < Apply > ボタンをクリックします。

The screenshot shows the 'IP > VRRP' configuration page. The 'Step' dropdown is set to '1. Configure Group ID' and the 'Action' dropdown is set to 'Add'. Below these, there is a text input field for 'VRID (1-255)' containing the value '1', and a dropdown menu for 'VLAN' also set to '1'. At the bottom right, there are 'Apply' and 'Revert' buttons.

画面 1-281 :VRRP グループ ID の設定

設定されている VRRP グループを表示するには、以下のようにします。

1. 「IP」 → 「VRRP」 を選択します。
2. 「Step」 リストで 「Configure Group ID」 を選択します。
3. 「Step」 リストで 「Show」 を選択します。

The screenshot shows the 'IP > VRRP' configuration page with the 'Action' dropdown set to 'Show'. Below the configuration fields, there is a table titled 'VRRP Group ID List' with 'Max: 16' and 'Total: 2'. The table has three columns: a checkbox, 'VRID', and 'VLAN'. It lists two configured groups: VRID 1 on VLAN 1 and VRID 2 on VLAN 1. At the bottom right, there are 'Delete' and 'Revert' buttons.

	VRID	VLAN
☐	1	1
☐	2	1

画面 1-282 : 設定されている VRRP グループの表示

VRRP グループの仮想ルータアドレスを設定するには、以下のようになります。

1. 「IP」 → 「VRRP」 を選択します。
2. 「Step」 リストで 「Configure Group ID」 を選択します。
3. 「Step」 リストで 「Add IP Address」 を選択します。
4. VLAN および VRRP グループ ID を選択し、仮想ルータの IP アドレスを入力します。
5. < Apply > ボタンをクリックします。

The screenshot shows the 'IP > VRRP' configuration page. The 'Step' dropdown is set to '1. Configure Group ID' and the 'Action' dropdown is set to 'Add IP Address'. Below these, there are three input fields: 'VLAN ID' with a value of '1', 'VRID' with a value of '1', and 'IP Address' with the value '192.168.2.9'. At the bottom right, there are two buttons: 'Apply' and 'Revert'.

画面 1-283 :VRRP グループの仮想ルータアドレスの設定

VRRP グループに割り当てられている仮想 IP アドレスを表示するには、以下のようになります。

1. 「IP」 → 「VRRP」 を選択します。
2. 「Step」 リストで 「Configure Group ID」 を選択します。
3. 「Step」 リストで 「Show IP Addresses」 を選択します。
4. VLAN および VRRP グループ ID を選択します。

The screenshot shows the 'IP > VRRP' configuration page. The 'Step' dropdown is set to '1. Configure Group ID' and the 'Action' dropdown is set to 'Show IP Addresses'. Below these, there are two input fields: 'VLAN ID' with a value of '1' and 'VRID' with a value of '1'. Below these fields, there is a section titled 'VRRP Group IP List' with 'Max: 1' and 'Total: 1'. This section contains a table with two columns: a checkbox column and an 'IP Address' column. The table has one row with a checked checkbox and the IP address '192.168.2.9'. At the bottom right, there are two buttons: 'Delete' and 'Revert'.

画面 1-284 :VRRP グループに割り当てられている仮想アドレスの表示

Web 設定

ルータ冗長性の設定

VRRP グループの詳細設定を設定するには、以下のようにします。

1. 「IP」 → 「VRRP」 を選択します。
2. 「Step」 リストで「Configure Group ID」を選択します。
3. 「Step」 リストで「Configure Detail」を選択します。
4. VRRP グループ ID を選択し、必要に応じていずれかの VRRP プロトコルパラメータを設定します。
5. < Apply > ボタンをクリックします。

IP > VRRP

Step: 1. Configure Group ID Action: Configure Detail

VLAN ID	1
VRID	1
Advertisement Interval (1-255)	1 sec
Priority (1-254)	255
Preempt Mode	☒ Enabled
Preempt Delay Time (0-120)	0 sec
Authentication Mode	None
Authentication String	
State	Master
Virtual MAC Address	00-00-5E-00-01-01
Master Router	192.168.0.2
Master Priority	255
Master Advertisement Interval	1 sec
Master Down Interval	3

画面 1-285 :VRRP グループの詳細設定の設定

1.16.2 VRRP グローバル統計情報の表示

「IP」→「VRRP」(Show Statis - Global Statistics)を選択すると、VRRP プロトコルパケットで検出されたエラーのカウントを表示することができます。

関連する CLI 情報

「show vrrp router counters」

パラメータ

以下のパラメータが表示されます。

- ・ VRRP Packets with Invalid Checksum - 無効な VRRP チェックサム値を含む受信 VRRP パケットの総数。
- ・ VRRP Packets with Unknown Error - 不明なバージョン番号またはサポートされていないバージョン番号を含む受信 VRRP パケットの総数。
- ・ VRRP Packets with Invalid VRID - 仮想ルータの無効な VRID を含む受信 VRRP パケットの総数。

Web インターフェース

VRRP プロトコルパケットで検出されたエラーのカウントを表示するには、以下のようになります。

- (1) 「IP」→「VRRP」を選択します。
- (2) 「Step」リストで「Show Statistics」を選択します。
- (3) 「Global Statistics」を選択します。

IP > VRRP

Step: 1. Configure Group ID Action: Configure Detail

VLAN ID	1
VRID	1
Advertisement Interval (1-255)	1 sec
Priority (1-254)	255
Preempt Mode	☒ Enabled
Preempt Delay Time (0-120)	0 sec
Authentication Mode	None
Authentication String	
State	Master
Virtual MAC Address	00-00-5E-00-01-01
Master Router	192.168.0.2
Master Priority	255
Master Advertisement Interval	1 sec
Master Down Interval	3

Web 設定

ルータ冗長性の設定

IP > VRRP

Step: 2. Show Statistics

☒ Global Statistics ☐ Group Statistics

Global Statistics

VRRP Packets with Invalid Checksum	0
VRRP Packets with Unknown Error	3
VRRP Packets with Invalid VRID	0

画面 1-286 :VRRP パケットで検出されたエラーのカウンタの表示

1.16.3 VRRP グループに関する統計情報の表示

「IP」→「VRRP」(Show Statistics - Group Statistics) を選択すると、特定のインターフェースで発生した VRRP プロトコルイベントとエラーのカウンタを表示することができます。

関連する CLI 情報

「show vrrp interface counters」

パラメータ

以下のパラメータが表示されます。

- ・ VLAN ID - IP インターフェースを指定して設定されている VLAN の ID (範囲: 1 ~ 4,093)。
- ・ VRID - VRRP グループ ID (範囲: 1 ~ 255)。

表示される統計値は、以下のとおりです。

パラメータ	説明
Times Transitioned to Master	ルータがマスタになった回数。
Received Advertisement Packets	ルータで受信された VRRP アドバタイズメントの数。
Received Error Advertisement Interval Packets	ローカル仮想ルータについて設定されている間隔とは異なる間隔で受信された VRRP アドバタイズメントの数。
Received Authentication Failure Packets	認証チェックに合格しなかった受信 VRRP パケットの数。
Received Error IP TTL VRRP Packets	IP TTL (Time-To-Live) が 255 ではない仮想ルータで受信された VRRP パケットの数。
Received Priority 0 VRRP Packets	優先度が 0 に設定されている仮想ルータで受信された VRRP パケットの数。
Sent Priority 0 VRRP Packets	優先度が 0 に設定されている仮想ルータで送信された VRRP パケットの数。優先度 0 は、グループマスタが VRRP サービスへの加入を停止していることを示し、マスタのタイムアウトを待たずに速やかにバックアップ装置をマスタモードにするために使用します。
Received Invalid Type VRRP Packets	仮想ルータで受信された VRRP パケットのうち、「type」フィールドの値が無効なもの数。
Received Error Address List VRRP Packets	アドレスリストが仮想ルータについてローカルで設定されているリストとマッチしない受信パケットの数。
Received Invalid Authentication Type VRRP Packets	不明な認証タイプの受信パケットの数。
Received Mismatch Authentication Type VRRP Packets	「Auth Type」がローカルで設定されている認証方式と一致しない受信パケットの数。

Web 設定

ルータ冗長性の設定

Received Error Packets Length VRRP Packets	パケット長が VRRP ヘッダ長よりも短い受信パケットの数。

表 1-20:VRRP グループに関する統計情報

Web インターフェース

特定の VRRP インターフェースで発生した VRRP プロトコルイベントとエラーのカウンタを表示するには、以下のようにします。

- (1) 「IP」 → 「VRRP」 を選択します。
- (2) 「Step」 リストで 「Show Statistics」 を選択します。
- (3) 「Group Statistics」 を選択します。

IP > VRRP

Step: 2. Show Statistics

Group Statistics

VLAN ID	1
VRID	1
Times Transitioned to Master	1
Received Advertisement Packets	0
Received Error Advertisement Interval Packets	0
Received Authentication Failure Packets	0
Received Error IP TTL VRRP Packets	0
Received Priority 0 VRRP Packets	0
Sent Priority 0 VRRP Packets	0
Received Invalid Type VRRP Packets	0
Received Error Address List VRRP Packets	0
Received Invalid Authentication Type VRRP Packets	0
Received Mismatch Authentication Type VRRP Packets	0
Received Error Packets Length VRRP Packets	0

画面 1-287 :VRRP グループで検出されたエラーのカウンタの表示

1.17 IP サービス

本章では、以下の IP サービスについて説明します。

- ・ ドメインネームサービス - デフォルトのドメイン名を設定し、ダイナミック検索で使用するサーバを指定し、スタティックエントリを設定する方法を表示します。
- ・ DHCP クライアント ID の指定 - インターフェースの DHCP クライアント ID を指定します。
- ・ DHCP リレーサービスの設定 - DHCP リレーサービスを有効にし、クライアント要求の転送先となるサーバを定義します。
- ・ DHCP サーバの設定 - ネットワークまたは個々のホストに割り当てられるアドレスを設定します。
- ・ UDP ヘルパーの有効化 - ホストアプリケーションから発信される UDP ブロードキャストパケットをネットワークの別の部分に転送するようにスイッチを設定します。

1.17.1 ドメインネームサービス

本製品の DNS サービスでは、スタティックテーブルエントリを使用するか、ネットワーク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 アドレスにマップすることができます。クライアントデバイスは、このスイッチを DNS サーバとして指定している場合は、DNS クエリをスイッチに転送して応答を待機し、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 アドレスにマップするのに使用される DNS テーブルのエントリを手動で設定するか、デフォルトのドメイン名を設定するか、ドメイン名からアドレスへの変換に使用される 1 つまたは複数のネームサーバを指定することができます。

DNS サービスの全般パラメータの設定

「IP Service」→「DNS - General」（Configure Global）を選択すると、ドメイン検索を有効にして、デフォルトのドメイン名を設定することができます。

関連する CLI 情報

「ip domain-lookup」

「ip domain-name」

コマンドの使用

- ・ スwitchの DNS サービスを有効にするには、ドメイン検索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（「ネームサーバのリストの設定」を参照）。

パラメータ

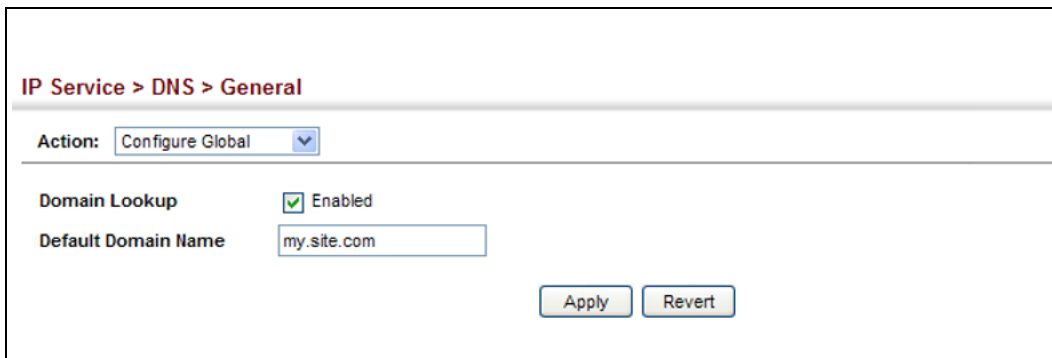
以下のパラメータが表示されます。

- ・ Domain Lookup - DNS ホスト名からアドレスへの変換を有効にします（デフォルト：Enabled）。
- ・ Default Domain Name - 不完全なホスト名に付加されるデフォルトのドメイン名を定義します。ホスト名をドメイン名と区切る先頭ドットは含めないでください（範囲：1 ～ 127 文字の英数字）。

Web インターフェース

DNS の全般設定を設定するには、以下のようにします。

- (1) 「IP Service」 → 「DNS」 を選択します。
- (2) 「Step」 リストで 「Configure Global」 を選択します。
- (3) ドメイン検索を有効にし、デフォルトのドメイン名を設定します。
- (4) < Apply > ボタンをクリックします。



IP Service > DNS > General

Action: Configure Global

Domain Lookup ☒ Enabled

Default Domain Name

Apply Revert

画面 1-288 :DNS の全般設定の設定

ドメイン名のリストの設定

「IP Service」 → 「DNS」 → 「General」 (Add Domain Name) を選択すると、列挙されている順序に従って問い合わせが試行されるドメイン名のリストを設定することができます。

関連する CLI 情報

「ip domain-list」

「show dns」

コマンドの使用

- ・ この画面を使用して、不完全なホスト名（ドット付き表記になっていない状態でクライアントから渡されるホスト名）に付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は、デフォルトのドメイン名が使用されます（「DNS サービスの全般パラメータの設定」を参照）。ドメインリストがある場合は、該当するエントリがそのリストで検索されます。該当するエントリが見つからなければ、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スイッチの DNS サービスで受信され、ドメイン名リストが指定されている場合、スイッチはそのドメイン名リストを調べて、リスト内のそれぞれのドメイン名をその不完全なホスト名に付加し、指定されているネームサーバにマッチするものがあるかどうかをチェックします（「ネームサーバのリストの設定」を参照）。

パラメータ

以下のパラメータが表示されます。

- ・ Domain Name – ホストの名前。ホスト名をドメイン名と区切る先頭ドットは含めないでください（範囲：1 ～ 68 文字）。

Web インターフェース

ドメイン名のリストを作成するには、以下のようにします。

- (1) 「IP Service」 → 「DNS」 を選択します。
- (2) 「Step」 リストで 「Add Domain Name」 を選択します。
- (3) ドメイン名を 1 つずつ入力します。
- (4) < Apply > ボタンをクリックします。

The screenshot shows the 'IP Service > DNS > General' configuration page. Under the 'Action:' dropdown, 'Add Domain Name' is selected. Below this, the 'Domain Name' field contains the text 'goggle.com'. At the bottom right, there are 'Apply' and 'Revert' buttons.

画面 1-289 :DNS 用のドメイン名のリストの設定

ドメイン名のリストを表示するには、以下のようにします。

1. 「IP Service」 → 「DNS」 を選択します。
2. 「Step」 リストで 「Show Domain Names」 を選択します。

The screenshot shows the 'IP Service > DNS > General' configuration page. Under the 'Action:' dropdown, 'Show Domain Names' is selected. Below this, there is a section titled 'Domain Name List' with 'Max: 3' and 'Total: 2'. It contains a table with two rows of domain names: 'google.com' and 'hinet.net'. Each row has a checkbox on the left. At the bottom right, there are 'Delete' and 'Revert' buttons.

	Domain Name
☐	google.com
☐	hinet.net

画面 1-290 :DNS 用のドメイン名のリストの表示

ネームサーバのリストの設定

「IP Service」→「DNS」→「General」(Add Name Server)を選択すると、列挙されている順序に従って問い合わせが試行されるネームサーバのリストを設定することができます。

関連する CLI 情報

「ip name-server」

「show dns」

コマンドの使用

- ・ スイッチの 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、ドメイン検索ステータスを有効にします（「DNS サービスの全般パラメータの設定」を参照）。
- ・ 複数のネームサーバが指定されている場合は、応答が受信されるまで、または、応答がなくリストの最後に到達するまで、指定されている順序に従ってそれらのサーバに対する問合せが実行されます。
- ・ すべてのネームサーバが削除されると、DNS が自動的に無効になります。また、DNS は、ドメイン検索ステータスが Disabled になった場合にも無効になります。

パラメータ

以下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されるドメインネームサーバの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することができます。

Web インターフェース

ネームサーバのリストを作成するには、以下のようになります。

- (1) 「IP Service」→「DNS」を選択します。
- (2) 「Step」リストで「Add Name Server」を選択します。
- (3) ネームサーバを 1 つずつ入力します。
- (4) < Apply > ボタンをクリックします。

The screenshot shows a web configuration page with the breadcrumb 'IP Service > DNS > General'. Below the breadcrumb, there is a section titled 'Action:' with a dropdown menu set to 'Add Name Server'. Underneath, there is a label 'Name Server IP Address' followed by a text input field containing the value '192.168.1.10'. At the bottom right of the form, there are two buttons: 'Apply' and 'Revert'.

画面 1-291 :DNS 用のネームサーバのリストの設定

ネームサーバのリストを表示するには、以下のようにします。

1. 「IP Service」 → 「DNS」 を選択します。
2. 「Step」 リストで 「Show Name Servers」 を選択します。

IP Service > DNS > General

Action: Show Name Servers ▼

Name Server IP Address List Max: 6 Total: 3

☐	Name Server IP Address
☐	192.168.1.10
☐	140.113.5.7
☐	10.7.231.5

Delete Revert

画面 1-292 :DNS 用のネームサーバのリストの表示

スタティック DNS ホストに対応するアドレスエントリの設定

「IP Service」 → 「DNS - Static Host Table」 (Add) を選択すると、ドメイン名を IP アドレスにマップするために使用される DNS テーブルのスタティックエントリを手動で設定することができます。

関連する CLI 情報

「ip host」

「show hosts」

コマンドの使用

スタティックエントリは、接続先のネットワークに直接接続しているローカルデバイス、またはネットワーク上の他の場所にあるよく利用されるリソースに使用することができます。

パラメータ

以下のパラメータが表示されます。

- ・ Host Name - 1 つまたは複数の IP アドレスにマップされるホストデバイスの名前（範囲：1 ～ 127 文字）。
- ・ IP Address - ホスト名に関連付けられる IPv4 アドレスまたは IPv6 アドレス。

Web インターフェース

DNS テーブルのスタティックエントリを設定するには、以下のようにします。

- (1) 「IP Service」 → 「DNS」 → 「Static Host Table」 を選択します。
- (2) 「Step」 リストで 「Add」 を選択します。

(3) ホスト名とそれに対応するアドレスを入力します。

(4) < Apply > ボタンをクリックします。

IP Service > DNS > Static Host Table

Action: Add

Host Name: yahoo.com

IP Address 1: 10.2.78.3

IP Address 2:

IP Address 3:

IP Address 4:

IP Address 5:

IP Address 6:

IP Address 7:

IP Address 8:

Apply Revert

画面 1-293 :DNS テーブルのスタティックエントリの設定

DNS テーブルのスタティックエントリを表示するには、以下のようにします。

1. 「IP Service」 → 「DNS」 → 「Static Host Table」を選択します。
2. 「Step」 リストで「Show」を選択します。

IP Service > DNS > Static Host Table

Action: Show

IP Address List Max: 16 Total: 3

☐	Host Name	IP Address
☐	yahoo.com	10.2.78.3 5.6.7.8
☐	hinet.net	124.29.31.155 1.2.3.4
☐	google.com	133.45.211.18 9.9.9.9

Delete Revert

画面 1-294 :DNS テーブルのスタティックエントリの表示

DNS キャッシュの表示

「IP Service」→「DNS」→「Cache」を選択すると、指定したネームサーバについて学習された DNS キャッシュ内のエントリを表示することができます。

コマンドの使用

- ・ サーバまたはその他のネットワークデバイスは、複数の IP アドレスを使用して1つまたは複数の接続をサポートすることもあります。ネームサーバから返される情報によって複数の IP アドレスが1つのホスト名に関連付けられる場合、DNS クライアントは、ターゲットデバイスとの接続が確立されるまで、それぞれのアドレスを連続して試すことができます。

パラメータ

以下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。
- ・ Flag - このフラグは、常に、キャッシュエントリを示す「4」になります。
- ・ Type - このフィールドには、オーナーのホストアドレスを指定する CNAME およびエイリアスを指定する ALIAS が含まれます。
- ・ IP - レコードに関連付けられている IP アドレス。
- ・ TTL - ネームサーバから報告された TTL。
- ・ Domain - レコードに関連付けられているドメイン名。

Web インターフェース

DNS キャッシュ内のエントリを表示するには、以下のようになります。

- (1) 「IP Service」→「DNS」→「Cache」を選択します。

IP Service > DNS > Cache					
Cache Information Max: 2560 Total: 3					
No.	Flag	Type	IP	TTL	Domain
1	4	CNAME	192.168.110.2	360	www.sina.com.cn
2	4	CNAME	10.2.44.3	892	www.yahoo.akadns.new
3	4	ALIAS	pointer to: 2	298	www.yahoo.com
Clear					

画面 1-295 :DNS キャッシュ内のエントリの表示

1.17.2 ダイナミックホスト設定プロトコル

ダイナミックホスト設定プロトコル（DHCP: Dynamic Host Configuration Protocol）を使用すると、ネットワーククライアントのブートアップ時に IP アドレスおよびその他の設定情報をそれらのクライアントに動的に割り当てることができます。サブネットにまだ BOOTP サーバまたは DHCP サーバが含まれていない場合は、DHCP クライアント要求を別のサブネットの DHCP サーバに中継するか、該当のサブネットをサポートするようにスイッチで DHCP サーバを設定することができます。

スイッチで DHCP サーバを設定する場合は、一意のインターフェースごとにアドレスプールを設定するか、クライアントのハードウェアアドレスまたはクライアント ID に基づいてスタティック IP アドレスをクライアントに手動で割り当てることができます。DHCP サーバは、ホストの IP アドレス、ドメイン名、ゲートウェイルータ、および DNS サーバ、ならびにホストの Boot イメージに関する情報（ダウンロード時にアクセスする TFTP サーバ、および Boot ファイル名など）または NetBIOS Windows Internet Naming Service（WINS）の Boot 情報を提供することができます。

DHCP クライアント ID の指定

「IP Service」→「DHCP」→「Client」を選択すると、VLAN インターフェースの DHCP クライアント ID を指定することができます。

関連する CLI 情報

「ip dhcp client class-id」

コマンドの使用

- ・ クラス ID は、スイッチのベンダークラスおよび設定を DHCP サーバが識別するために使用され、DHCP サーバは、それらの情報を使用して、クライアントへのサービスの提供方法または返すべき情報のタイプを決定します。
- ・ この DHCP オプションの全体的な枠組みは、RFC 2132（Option 60）で規定されています。これらの情報を使用してクライアントに関する設定情報やその他の ID 情報が伝達されますが、使用され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によって指定されます。

パラメータ

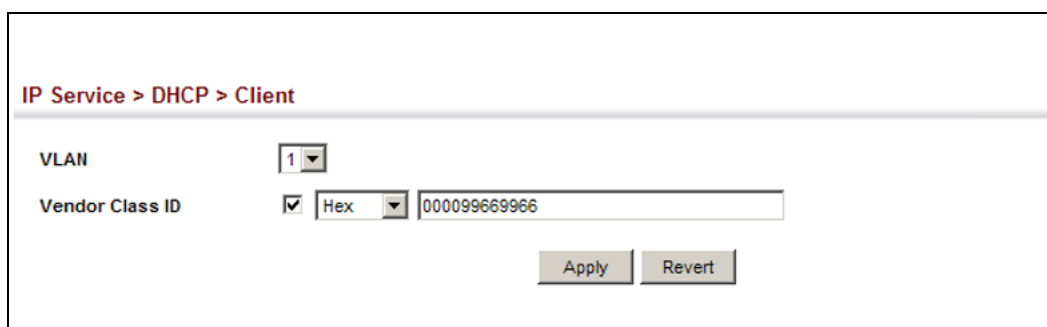
以下のパラメータが表示されます。

- ・ VLAN – 設定済み VLAN の ID。
- ・ 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、以下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 FXC9324XG です。
 - ・ Text – テキスト文字列（範囲：1 ～ 32 文字）。
 - ・ Hex – 16 進数値（範囲：1 ～ 64 文字）。

Web インターフェース

DHCP クライアント ID を指定するには、以下のようになります。

- (1) 「IP Service」 → 「DHCP」 → 「Client」 を選択します。
- (2) チェックボックスをオンにして、この機能を有効します。デフォルトの設定を選択するか、または、ベンダークラス ID の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 進数値を入力します。
- (3) < Apply > ボタンをクリックします。



IP Service > DHCP > Client

VLAN

Vendor Class ID ☒ Hex

画面 1-296 :DHCP クライアント ID の指定

DHCP リレーサービス

「IP Service」 → 「DHCP」 → 「Relay」 を選択すると、接続しているホストデバイスの DHCP リレーサービスを設定することができます。DHCP リレーを有効にしている場合、スイッチは、DHCP 要求がブロードキャストされているのを見つけると、クライアントが存在しているサブネットを DHCP サーバが認識できるようにするため、自らの IP アドレスをその要求に挿入します。それから、パケットを DHCP サーバに転送します。サーバは、DHCP 要求を受信すると、DHCP クライアントのサブネットについて定義されている範囲内の DHCP クライアントのフリー IP アドレスを割り当ててから、DHCP 要求を DHCP リレーエージェント（つまり、スイッチ）に戻します。スイッチは、サーバから受信した DHCP 要求をクライアントにブロードキャストします。

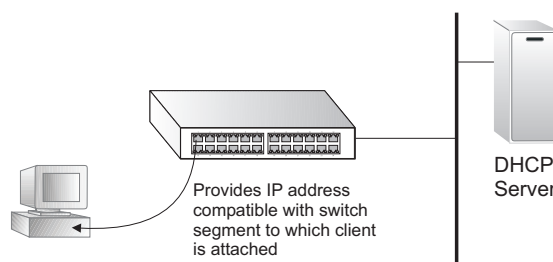


図 1-25: レイヤ 3 の DHCP リレーサービス

** 図の注釈

クライアントが接続しているスイッチセグメントに適合する IP アドレスを指定

関連する CLI 情報

「ip dhcp relay server」

「ip dhcp restart relay」

コマンドの使用

- ・ 少なくとも 1 つの DHCP サーバの IP アドレスを指定する必要があります。指定しない場合、スイッチの DHCP リレーエージェントはクライアント要求を DHCP サーバに転送しません。
- ・ DHCP リレー設定は、アクティブな DHCP サーバが同じネットワークセグメントで検出されると無効になります。

パラメータ

以下のパラメータが表示されます。

- ・ VLAN ID - 設定済み VLAN の ID。
- ・ Server IP Address - 望ましい順にスイッチの DHCP リレーエージェントで使用される DHCP サーバのアドレス。
- ・ Restart DHCP Relay - このボタンは、DHCP リレーサービスを再初期設定する場合に使用します。

Web インターフェース

DHCP リレーサービスを設定するには、以下のようにします。

- (1) 「IP Service」 → 「DHCP」 → 「Relay」を選択します。
- (2) いずれかの VLAN の IP アドレスを最大 5 つ入力します。
- (3) < Apply > ボタンをクリックします。

IP Service > DHCP > Relay

Note: DHCP relay configuration will be disabled if an active DHCP server is detected on the same network segment.

DHCP Server by VLAN List Max: 4093 Total: 1

VLAN	Server IP Address
1	192.168.2.33
	0.0.0.0
	0.0.0.0
	0.0.0.0
	0.0.0.0

Click the button to restart DHCP Relay service.

画面 1-297 :DHCP リレーサービスの設定

DHCP サーバの設定

本製品には、サービスを要求する接続ホストに一時 IP アドレスを割り当てることができる DHCP (Dynamic Host Configuration Protocol) サーバ機能が組み込まれています。このサーバは、ドメイン名、デフォルトゲートウェイ、ドメインネームサーバ (DNS: Domain Name Server)、WINS (Windows Internet Naming Service) ネームサーバなどのネットワーク設定、またはダウンロードするホストデバイスのブートアップファイルに関する情報を提供します。

スイッチの特定の IP インターフェースについて設定されている共通アドレスプールからアドレスをクライアントに割り当てるか、クライアントの ID コードまたは MAC アドレスに基づいて固定アドレスをホストに割り当てることができます。

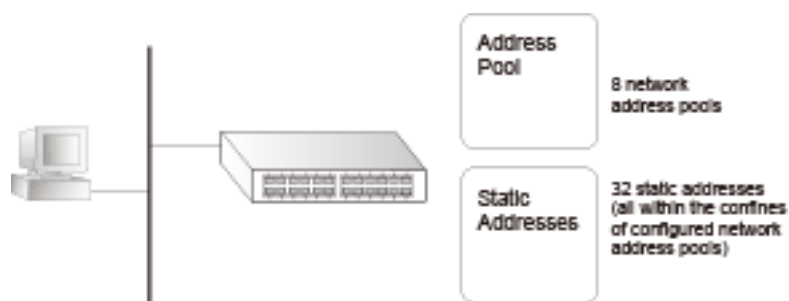


図 1-26:DHCP サーバ

** 図の注釈

アドレスプール 8 つのネットワークアドレスプール

スタティックアドレス 32 個のスタティックアドレス (すべて、設定されているネットワークアドレスプールの範囲内)

コマンドの使用

- ・ 最初に、スイッチのアドレスを含めた、除外アドレスを指定します。
- ・ 次に、ネットワークインターフェースのアドレスプールを設定します。最大 8 つのアドレスプールを設定することができます。また、必要な場合は、手動でアドレスを特定のクライアントにバインドすることもできます。ただし、固定アドレスは、既存のネットワークアドレスプールの範囲内のものでなければなりません。最大 32 の固定ホストアドレスを設定することができます (プールごとにアドレスを 4 つ入力)。
- ・ DHCP サーバを実行している場合、設定に関する変更を実装するには、その DHCP サーバを無効にしてから再び有効にする必要があります。そのための操作は、「IP Service」→「DHCP」→「Server」(Configure Global) を選択して表示される画面で実行することができます。

サーバの有効化

「IP Service」→「DHCP」→「Server」(Configure Global) を選択すると、DHCP サーバを有効にすることができます。

関連する CLI 情報

「service dhcp」

パラメータ

以下のパラメータが表示されます。

- ・ DHCP Server – スイッチで DHCP サーバを有効または無効にします（デフォルト：Disabled）。

Web インターフェース

DHCP サーバを有効するには、以下のようにします。

- (1) 「IP Service」 → 「DHCP」 → 「Server」 を選択します。
- (2) 「Step」 リストで 「Configure Global」 を選択します。
- (3) 「Enabled」 チェックボックスをオンにします。
- (4) < Apply > ボタンをクリックします。

IP Service > DHCP > Server

Step: 1. Configure Global

DHCP Server ☒ Enabled

Note:
You must configure an address pool before enabling the DHCP server.
If the DHCP server is running, you must restart it to implement any configuration changes.

Apply Revert

画面 1-298 :DHCP サーバの有効化

除外するアドレスの設定

「IP Service」→「DHCP」→「Server」（Configure Excluded Addresses - Add）を選択すると、クライアントに割り当てられないようにする IP アドレスを指定することができます。

関連する CLI 情報

「ip dhcp excluded-address」

パラメータ

以下のパラメータが表示されます。

- ・ Start IP Address - DHCP サーバが DHCP クライアントに割り当てないようにする単一の IP アドレス、または IP アドレス範囲の最初のアドレスを指定します。
- ・ End IP Address - DHCP サーバが DHCP クライアントに割り当てないようにする IP アドレス範囲の最後のアドレスを指定します。

【注意】：必ず、スイッチおよびその他の主要なネットワークデバイスのアドレスを除外してください。

Web インターフェース

DHCP クライアントへの割り当てから除外される IP アドレスを設定するには、以下のようになります。

- (1) 「IP Service」→「DHCP」→「Server」を選択します。
- (2) 「Step」リストで「Configure Excluded Addresses」を選択します。
- (3) 「Step」リストで「Add」を選択します。
- (4) 単一のアドレスまたはアドレス範囲を入力します。
- (5) < Apply > ボタンをクリックします。

IP Service > DHCP > Server

Step: 2. Configure Excluded Address Action: Add

Start IP Address 10.1.0.250

End IP Address 10.1.0.254 (optional)

Apply Revert

画面 1-299 :DHCP サーバにおける除外アドレスの設定

DHCP クライアントへの割り当てから除外される IP アドレスを表示するには、以下のようになります。

1. 「IP Service」→「DHCP」→「Server」を選択します。
2. 「Step」リストで「Configure Excluded Addresses」を選択します。
3. 「Step」リストで「Show」を選択します。

IP Service > DHCP > Server

Step: 2. Configure Excluded Address Action: Show

DHCP Excluded Address List Max: 5 Total: 1

	Start IP Address	End IP Address
☐	10.1.0.250	10.1.0.254

Delete Revert

画面 1-300 :DHCP サーバにおける除外アドレスの表示

アドレスプールの設定

「IP Service」→「DHCP」→「Server」(Configure Pool - Add) を選択すると、DHCP サーバを使用して接続クライアントにアドレスを提供する各インターフェースの IP アドレスプールを設定することができます。

関連する CLI 情報

「DHCP Server」

コマンドの使用

- ・ 最初に、ネットワークインターフェースのアドレスプールを設定します。それから、必要な場合は、手動でアドレスを特定のクライアントにバインドすることができます。ただし、スタティックホストアドレスは既存のネットワークアドレスプールの範囲内のものでなければならないという点に注意してください。最大 8 つのネットワークアドレスプールを設定し、最大 32 のホストアドレスを手動でプールにバインドすることができます (ホストプールごとにアドレス 4 つ)。ただし、ホストアドレスプールで指定されるあらゆるアドレスは、設定されているネットワークアドレスプールの範囲内のものでなければならないという点に注意してください。
- ・ スイッチは、クライアント要求を受信すると、最初に、要求を発信したゲートウェイにマッチするネットワークアドレスプールがあるかどうかをチェックします (要求がリレーサーバによって転送された場合)。クライアント要求にゲートウェイ情報が含まれていない場合 (要求がリレーサーバによって転送されていない場合) には、スイッチは、クライアント要求の受信時に使用されたインターフェースにマッチするネットワークプールを検索します。それから、マッチするネットワークプールで、手動設定されているホストアドレスを検索します。手動設定されているホストアドレスが見つからなければ、マッチするネットワークアドレスプールからアドレスが割り当てられます。ただし、マッチするアドレスプールが見つければ、要求は無視されます。
- ・ 手動でバインドされたホストアドレスを検索する場合、スイッチは、DHCP クライアントのクライアント ID と照合してから、ハードウェアアドレスと照合します。BOOTP クライアントはクライアント ID を送信できないので、該当のホストタイプのハードウェアアドレスを設定する必要があります。ハードウェアアドレスまたはクライアン

ト ID に手動でバインドされているホストエントリがない場合は、最初にマッチするネットワークプールからアドレスが割り当てられます。

- ・ ネットワークアドレスプールまたはホストアドレスプールのサブネットマスクが指定されていない場合は、クラス A、B、または C のナチュラルマスクが使用されます（「ネットワークインターフェースの指定」を参照）。DHCP サーバは、すべてのホストアドレスが使用可能であると仮定します。「IP Service」→「DHCP」→「Server」（Configure Excluded Addresses - Add）を選択して表示される画面を使用して、アドレス領域のサブセットを除外することができます。

パラメータ

以下のパラメータが表示されます。

新規アドレスプールの作成

- ・ Pool Name - 文字列または整数（範囲：1 ～ 8 文字）。
- ・ Type - アドレスプールのタイプを「Network」または「Host」に設定します。

ネットワークプールのパラメータの設定

- ・ IP - DHCP アドレスプールの IP アドレス。
- ・ Subnet Mask - ネットワーク（または、サブネット）および DHCP アドレスプールのホスト部を識別するために使用されるビットの組み合わせ。

スタティックホストのパラメータの設定

- ・ IP - ホストに割り当てられる IP アドレス。
- ・ Subnet Mask - クライアントのネットワークマスクを指定します。
- ・ Client-Identifier - クライアントデバイスを一意に特定するものであり、テキスト文字列（1 ～ 15 文字）と 16 進数値のいずれかです。この ID に含まれる情報は、RFC 2132 の Option 60 に基づくものであり、同じ管理ドメイン内のすべてのクライアントで一貫でなければなりません。
- ・ Hardware Address - クライアントで使用される MAC アドレスおよびプロトコルを指定します（オプション：Ethernet、IEEE802、FDDI または None、デフォルト：Ethernet）。

オプションパラメータの設定

- ・ Default Router - プライマリおよび代替のゲートウェイルータの IP アドレス。ルータの IP アドレスは、クライアントと同じサブネットになければなりません。
- ・ DNS Server - プライマリおよび代替の DNS サーバの IP アドレス。
- ・ ホスト名を IP アドレスにマップするため、DHCP クライアントに対応する DNS サーバを指定する必要があります。
- ・ Netbios Server - Microsoft DHCP クライアントに対して使用されるプライマリおよび代替の WINS（NetBIOS Windows Internet Naming Service）ネームサーバの IP アドレス。
- ・ Netbios Type - Microsoft DHCP クライアントの NetBIOS ノードタイプ（オプション：Broadcast、Hybrid、Mixed または Peer to Peer、デフォルト：Hybrid）。
- ・ Domain Name - クライアントのドメイン名（範囲：1 ～ 128 文字）。
- ・ Bootfile - DHCP クライアントのデフォルトの Boot イメージ。このファイルは、「Next Server」として指定される TFTP（Trivial File Transfer Protocol）サーバ上に置く必要があります。
- ・ Next Server - Boot プロセスにおけるネクストサーバの IP アドレスであり、通常は、TFTP サーバです。

- ・ Lease Time - IP アドレスが DHCP クライアントに割り当てられている期間（オプション：Finite または Infinite、デフォルト：Infinite）。

Web インターフェース

DHCP アドレスプールを設定するには、以下のようになります。

- (1) 「IP Service」 → 「DHCP」 → 「Server」 を選択します。
- (2) 「Step」 リストで 「Configure Pool」 を選択します。
- (3) 「Step」 リストで 「Add」 を選択します。
- (4) プールのタイプを 「Network」 または 「Host」 に設定します。
- (5) ネットワークプールまたはホストの IP アドレスとサブネットマスクを入力します。
ホストのスタティックバインディングを設定する場合は、クライアントデバイスのクライアント ID またはハードウェアアドレスを入力します。ゲートウェイサーバや DNS サーバなどのオプションパラメータを設定します。
- (6) < Apply > ボタンをクリックします。

IP Service > DHCP > Server

Step: 3. Configure Pool Action: Add

Pool Name

tps

Type

Network

IP

10.1.0.0

Subnet Mask

255.255.255.0

<<Option>>

Default Router

10.1.0.253

DNS Server

10.2.3.4

Netbios Server

10.1.0.33

Netbios Type

Hybrid

Bootfile

wme.bat

Lease Time

Infinite

Default Router 2

DNS Server 2

Netbios Server 2

Domain Name

example.com

Next Server

10.1.0.21

画面 1-301 :DHCP サーバアドレスプールの設定（ネットワーク）

IP Service > DHCP > Server

Step: 3. Configure Pool Action: Add

Pool Name: mgr

Type: Host

IP: 10.1.0.19

Subnet Mask: 255.255.255.0

Client Identifier: Text bear

Hardware Address: Ethernet 00-e0-29-94-34-28

<<Option>>

Default Router	10.1.0.253	Default Router 2	
DNS Server	10.2.3.4	DNS Server 2	
Netbios Server	10.1.0.33	Netbios Server 2	
Netbios Type	Hybrid	Domain Name	example.com
Bootfile	wme.bat	Next Server	10.1.0.21
Lease Time	Infinite		

画面 1-302 :DHCP サーバアドレスプールの設定（ホスト）

設定されている DHCP アドレスプールを表示するには、以下のようにします。

1. 「IP Service」 → 「DHCP」 → 「Server」を選択します。
2. 「Step」 リストで「Configure Pool」を選択します。
3. 「Step」 リストで「Show」を選択します。

IP Service > DHCP > Server

Step: 3. Configure Pool Action: Show

DHCP Pool List Max: 40 Total: 2

	Pool Name	Pool Type	IP	Subnet Mask
☐	mgr	Host	10.1.0.19	255.255.255.0
☐	tps	Network	10.1.0.0	255.255.255.0

Delete Revert

画面 1-303 : 設定されている DHCP サーバアドレスプールの表示

アドレスバインディングの表示

「IP Service」→「DHCP」→「Server」（Show IP Binding）を選択すると、スイッチの DHCP サーバから IP アドレスを取得したホストを表示することができます。

関連する CLI 情報

「show ip dhcp binding」

パラメータ

以下のパラメータが表示されます。

- ・ IP Address – ホストに割り当てられている IP アドレス。
- ・ MAC Address – ホストの MAC アドレス。
- ・ Lease Time – ホストで IP アドレスを使用できる期間。
- ・ Start Time – アドレスがスイッチによって割り当てられた日時。

Web インターフェース

DHCP クライアントに割り当てられているアドレスを表示するには、以下のようになります。

- (1) 「IP Service」→「DHCP」→「Server」を選択します。
- (2) 「Step」リストで「Show IP Binding」を選択します。

The screenshot shows the 'IP Service > DHCP > Server' configuration page. Under the 'Step' dropdown, '4. Show IP Binding' is selected. Below this, there is a table titled 'IP Binding List' with 'Max: 512' and 'Total: 1'. The table has five columns: a checkbox, 'IP Address', 'MAC Address', 'Lease Time', and 'Start Time'. One row is displayed with the values: checkbox (unchecked), '192.168.2.61', '00-60-6E-00-5F-A1', 'Infinite', and 'Dec 7 12:20:50 2009'. At the bottom of the table, there are 'Delete' and 'Revert' buttons.

☐	IP Address	MAC Address	Lease Time	Start Time
☐	192.168.2.61	00-60-6E-00-5F-A1	Infinite	Dec 7 12:20:50 2009

画面 1-304 :DHCP サーバによって割り当てられたアドレスの表示

1.17.3 UDP サービス要求の転送

ここでは、ローカルアプリケーションサーバが使用できない場合にスイッチがホストアプリケーションから発信される UDP ブロードキャストパケットをネットワークの別の部分に転送できるようにする方法について説明します。

コマンドの使用

- ・ ネットワークホストでは、UDP ブロードキャストを使用して、アドレス設定やドメイン名のマッピングなどの情報を判別することがあります。それらのブロードキャストは、ローカルサブネット内でのみ送信され、全ホストブロードキャスト（all-ones ブロードキャスト - 255.255.255.255）とダイレクトサブネットブロードキャスト（例：10.10.10.255 など）のどちらかになります。マルチセグメントネットワーク内に展開されるアプリケーションサーバの数を減らすため、UDP ヘルパーを使用して、指定した UDP アプリケーションポートのブロードキャストパケットが別のネットワークセグメント内のリモートサーバに転送されるようにすることができます。
- ・ UDP ヘルパーを設定するには、それをグローバルで有効にし（「DNS サービスの全般パラメータの設定」を参照）、ブロードキャストトラフィックの転送先となる UDP 宛先ポートを指定して（「UDP 宛先ポートの指定」を参照）、リモートアプリケーションサーバまたはサーバがあるサブネットを指定します（「ターゲットサーバまたはサブネットの指定」を参照）。

UDP ヘルパーの有効化

「IP Service」→「UDP Helper」→「General」を選択すると、UDP ヘルパーをスイッチでグローバルに有効にすることができます。

関連する CLI 情報

「ip helper」

パラメータ

以下のパラメータが表示されます。

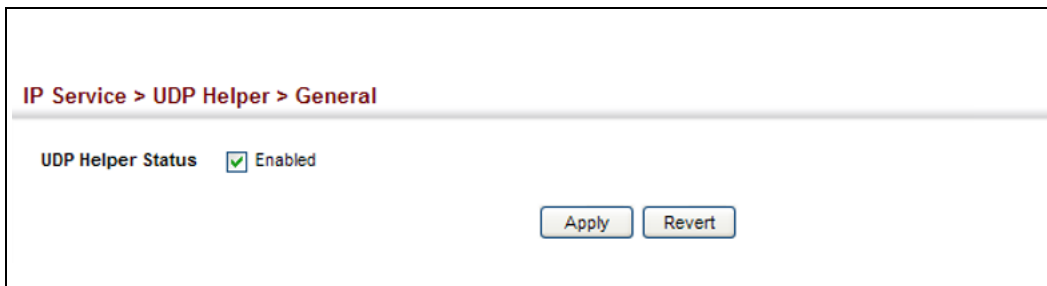
- ・ UDP Helper Status - UDP ヘルパーを有効または無効にします（デフォルト：Disabled）。

Web インターフェース

DHCP ヘルパーを有効するには、以下のようにします。

- (1) 「IP Service」→「UDP Helper」→「General」を選択します。
- (2) 「Enabled」チェックボックスをオンにします。

(3) < Apply > ボタンをクリックします。



IP Service > UDP Helper > General

UDP Helper Status ☒ Enabled

Apply Revert

画面 1-305 :UDP ヘルパーの有効化

UDP 宛先ポートの指定

「IP Service」→「UDP Helper」→「Forwarding」を選択すると、UDP ヘルパーが有効になっている場合にブロードキャストトラフィックの転送先となる UDP 宛先ポートを指定することができます。

関連する CLI 情報

「ip forward-protocol udp」

コマンドの使用

- このコマンドでは、1 つまたは複数のリモートサーバにトラフィックを転送するため、最大 100 の UDP ポートを指定することができます。

パラメータ

以下のパラメータが表示されます。

- Destination UDP Port - UDP サービス要求が転送される UDP アプリケーションポート (範囲: 1 ~ 65,535)。

UDP ヘルパーが有効になっている場合には、以下の UDP ポートが転送リストに含まれ、リモートサーバアドレスが設定されます。

BOOTP クライアント	ポート 67
BOOTP サーバ	ポート 68
ドメインネームサービス	ポート 53
IEN-116 ネームサービス	ポート 42
NetBIOS データグラムサーバ	ポート 138
NetBIOS ネームサーバ	ポート 137
NTP	ポート 37
TACACS サービス	ポート 49
TFTP	ポート 69

Web インターフェース

転送に使用される UDP 宛先ポートを指定するには、以下のようにします。

- (1) 「IP Service」 → 「UDP Helper」 → 「Forwarding」 を選択します。
- (2) 「Step」 リストで 「Add」 を選択します。
- (3) サービス要求がリモートアプリケーションサーバに転送される UDP 宛先ポート番号を入力します。
- (4) < Apply > ボタンをクリックします。

IP Service > UDP Helper > Forwarding

Action: Add ▼

Destination UDP Port (1-65535)

Apply Revert

画面 1-306 :UDP 宛先ポートの指定

指定されている UDP 宛先ポートを表示するには、以下のようにします。

1. 「IP Service」 → 「UDP Helper」 → 「Forwarding」 を選択します。
2. 「Step」 リストで 「Show」 を選択します。

IP Service > UDP Helper > Forwarding

Action: Show ▼

UDP Helper Forwarding Port List Max: 100 Total: 1

	Destination UDP Port
☐	547

Delete Revert

画面 1-307 :UDP 宛先ポートの表示

ターゲットサーバまたはサブネットの指定

「IP Service」→「UDP Helper」→「Address」を選択すると、指定した UDP ブロードキャストパケットの転送先となるアプリケーションサーバまたは（ダイレクトブロードキャストアドレスによって示される）サブネットを指定することができます。

関連する CLI 情報

「ip helper-address」

コマンドの使用

- ・ 最大 20 のヘルパーアドレスを指定することができます。
- ・ UDP ヘルパーを使用して UDP パケットを転送するには、選択されたインターフェースにクライアントが接続されており、そのインターフェースが IP アドレスを指定して設定されていなければなりません。
- ・ 転送される UDP パケットは、「IP Service」→「UDP Helper」→「Forwarding」を選択して表示される画面で指定する必要がある、以下の条件を満たすものでなければなりません。
 - ・ 受信されるフレームの MAC アドレスが all-ones ブロードキャストアドレス (ffff.ffff.ffff) であること。
 - ・ IP 宛先アドレスは、以下のいずれかであること。
 - all-ones ブロードキャスト (255.255.255.255)
 - 受信先インターフェースのサブネットブロードキャスト
 - ・ IP TTL (Time To Live) 値が 2 以上であること。
 - ・ IP が UDP(17) であること。
 - ・ UDP 宛先ポートは、TFTP、DNS、Time、NetBIOS、BOOTP、または DHCP ポート、つまり、「IP Service」→「UDP Helper」→「Forwarding」を選択して表示される画面で指定されている UDP ポートでなければなりません。
- ・ この画面でヘルパーアドレスが指定されているにもかかわらず「IP Service」→「UDP Helper」→「Forwarding」を選択して表示される画面で UDP ポートが指定されていない場合には、p.534 ▲で説明されているように、デフォルトで、いくつかの UDP プロトコルタイプのブロードキャストトラフィックが転送されるようになります。

パラメータ

以下のパラメータが表示されます。

- ・ VLAN ID – VLAN 識別子（範囲：1 ～ 4,093）。
- ・ IP Address – ブロードキャストパケットの転送先のホストアドレスまたはダイレクトブロードキャストアドレス（範囲：1 ～ 65,535）。

Web インターフェース

UDP 要求パケットを転送するためのターゲットサーバまたはサブネットを指定するには、以下のようになります。

- (1) 「IP Service」→「UDP Helper」→「Address」を選択します。
- (2) 「Step」リストで「Add」を選択します。

(3) UDP 要求パケットの転送先となるリモートサーバまたはサブネットのアドレスを入力します。

(4) < Apply > ボタンをクリックします。

IP Service > UDP Helper > Address

Action: Add ▼

VLAN ID 1 ▼

IP Address 192.168.2.255

Apply Revert

画面 1-308 :UDP 要求のターゲットサーバまたはサブネットの指定

UDP 要求パケットを転送するためのターゲットサーバまたはサブネットを表示するには、以下のようにします。

1. 「IP Service」 → 「UDP Helper」 → 「Address」 を選択します。
2. 「Step」 リストで「Show」を選択します。

IP Service > UDP Helper > Address

Action: Show ▼

VLAN ID 1 ▼

UDP Helper Address List Max: 1024 Total: 1

	IP Address
☐	192.168.2.255

Delete Revert

画面 1-309 :UDP 要求のターゲットサーバまたはサブネットの表示

1.18 ユニキャストルーティング

本章では、以下のユニキャストルーティングプロトコルを設定する方法について説明します。

- ・ RIP（Routing Information Protocol）の設定 - RIP を設定します。
- ・ OSPF プロトコル（バージョン 2）の設定 - IPv4 用の OSPFv2 を設定します。

1.18.1 概要

本製品は、RIP（Routing Information Protocol）または OSPF（Open Shortest Path First）プロトコルを使用してユニキャストトラフィックを別々のサブネットワークにルーティングすることができ、RIPv1、RIPv2、および OSPFv2 ダイナミックルーティングをサポートしています。それらのプロトコルを使用して、ルーティング情報の交換、ルーティングテーブルの計算、および、ネットワークのステータスまたは負荷が変化した場合の応答が実行されます。

RIPv1 および RIPv2 ダイナミックルーティングプロトコル

RIP は、最も汎用的に使用されているルーティングプロトコルです。RIP では、距離ベクトルに基づく手法を使用してルーティングが実行されます。ルータは、送信コストの概算を示すものとして役立つ距離ベクトル（ホップ数）を最小限に抑えることを基準にして決定されます。各ルータは、アドバタイズメントを自らのルーティングテーブルの更新情報と共に 30 秒ごとにブロードキャストします。そのようにすることで、ネットワーク上のすべてのルータで学習される、該当のサブネットへのネクストホップリンクのテーブルの一貫性を確保できるようになります。

[注意] : IPv6 をサポートする RIPng は、今後のリリースでサポートされる予定です。

OSPFv2 ダイナミックルーティングプロトコル

OSPF は、RIP のすべての問題を打開します。OSPF では、リンクステートルーティングプロトコルを使用して最短パスツリーを生成してから、そのツリーに基づいてルーティングテーブルが構築されます。OSPF を使用すると、関連ルータがネットワークに関する変更に対して、予測どおり、かつ同時に反応するので、最適なルートが RIP よりも素早く導き出されるため、より安定したネットワークを実現することができます。それだけでなく、宛先に対して等価コストルートがいくつかある場合は、それらのルートにトラフィックが均等に分散されるようにすることができます。

非 IP ルーティング

本製品でサポートしているのは、IP ルーティングのみです。IP 以外の IPX や Appletalk などのプロトコルについては、本製品でトラフィックをルーティングすることができないので、外部ルータによってブリッジされない限り、それらのローカル VLAN グループ内でしか使用できません。

マルチレイヤスイッチで構築されるネットワークと共存するには、非 IP サブネットワークは、IP サブネットワークと同じ論理境界に沿って存在していなければなりません。そうすれば、個別のマルチプロトコルルータを使用して、ネットワーク上の使用可能な各 VLAN から 1 つのポートに接続し、サブネットワークにリンクすることができます。

1.18.2 RIP (Routing Information Protocol) の設定

RIP は、最も汎用的に使用されているルーティングプロトコルです。RIP では、距離ベクトルに基づく手法を使用してルーティングが実行されます。ルータは、送信コストの概算を示すものとして役立つ距離ベクトル（ホップ数）を最小限に抑えることを基準にして決定されます。各ルータは、アドバタイズメントを自らのルーティングテーブルの更新情報と共に 30 秒ごとにブロードキャストします。そのようにすることで、ネットワーク上のすべてのルータで学習される、該当のサブネットへのネクストホップリンクのテーブルの一貫性を確保できるようになります。

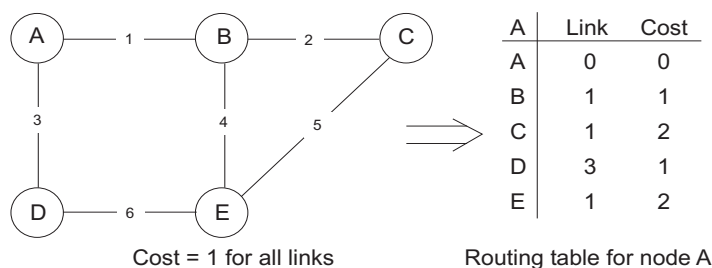


図 1-27:RIP の設定

** 図の注釈

- コスト = すべてのリンクで 1
- ノード A のルーティングテーブル

コマンドの使用

- ・ レイヤ 2 スイッチでループを防ぐためにスパニングツリーを使用するのと同じように、ルータでも、データトラフィックの無限再送信を発生させる可能性があるループを防ぐための手法を使用します。RIP では、以下の 3 つの方法を利用して、ループの発生を防ぎます。
 - ・ スプリットホライズン - ルート情報が取得元のインターフェースポートに伝搬されなくなります。
 - ・ ポイズンリバー - ルート情報が取得元のインターフェースポートに伝搬されますが、距離ベクトルメトリックが infinity に設定されます（そのようにすることで、収束が迅速化されます）。
 - ・ トリガーアップデート - ルートが変更された場合、一定の時間ではなく、ランダムで短い遅延時間が経過してから更新メッセージをブロードキャストします。
- ・ RIPv2 は、RIPv1 のアップグレード版であり、RIPv1 との互換性を備えています。RIPv2 を使用すると、プレーンテキスト認証、複数の独立 RIP ドメイン、可変長のサブネットマスク、およびルートアドバタイズメントのためのマルチキャスト伝送 (RFC 1723) に関する便利な機能が追加されます。
- ・ RIP については考慮すべき重大な問題がいくつかあります。第 1 に、RIPv1 ではサブネットは認識されず、RIPv1 と RIPv2 のどちらも、リンクまたはルータで障害が発生してから新規ルートが収束されるまで時間がかかることがあります、その間、ルーティングループが発生する可能性があります。また、ホップ数がわずか 15 に制限されるので、小規模なネットワークにしか使用できません。さらに、RIPv1 では、ルーティング情報がブロードキャストによって伝搬されるので、貴重なネットワーク帯域幅が無駄に消費され、また、最適なルートを決断する際に考慮されるネットワーク変数の数が少なすぎます。

プロトコルの全般設定の設定

「Routing Protocol」→「RIP」→「General」（Configure）を選択すると、RIP の全般設定と基本タイマーを設定することができます。

RIP は、ルータでルート情報を交換する方法を指定するために使用されます。RIP をルータで有効にすると、RIP メッセージがネットワーク内のすべてのデバイスに 30 秒（デフォルト）ごとに送信され、他のルータからの RIP メッセージが受信されるとルーティングテーブルが更新されます。RIP を使用して他のルータと正しく通信できるようにするため、ルータでグローバルに使用される RIP バージョンだけでなく、個々のインターフェースで使用する RIP の送信バージョンと受信バージョンも指定する必要があります（「RIP ネットワークインターフェースの設定」を参照）。

関連する CLI 情報

「Routing Information Protocol（RIP）」

コマンドの使用

RIP は、ルータでルート情報を交換する方法を指定するために使用されます。RIP をルータで有効にすると、RIP メッセージがネットワーク内のすべてのデバイスに 30 秒（デフォルト）ごとに送信され、他のルータからの RIP メッセージが受信されるとルーティングテーブルが更新されます。RIP を使用して他のルータと正しく通信できるようにするため、ルータでグローバルに使用される RIP バージョンだけでなく、個々のインターフェースで使用する RIP の送信バージョンと受信バージョンも指定する必要があります。

パラメータ

以下のパラメータが表示されます。

グローバル設定

- ・ RIP Routing Process – RIP ルーティングをグローバルで有効にします。また、「ネットワークインターフェースの指定」で説明しているように、RIP は、ルーティングプロセスに関与する各ネットワークインターフェースでも有効にする必要があります（デフォルト：Disabled）。
- ・ Global RIP Version – ルータでグローバルに使用される RIP のバージョンを指定します（オプション：Version 1、Version 2 または By Interface、デフォルト：By Interface）。

「Global RIP Version」を指定する場合は、事前に特定の「Receive Version」または「Send Version」が設定されていない VLAN インターフェースについて、以下の値を設定することができます。

- ・ RIP Version 1 – 該当のインターフェースは、RIPv1 対応プロトコルメッセージを送信し、RIPv1 と RIPv2 のいずれかのプロトコルメッセージを受信ようになります。
- ・ RIP Version 2 – 該当のインターフェースは、プロトコルメッセージの送信と受信の両方に RIPv2 を使用ようになります。

インターフェース設定画面で設定される RIP の「Receive Version」または「Send Version」は、常に、「Global RIP Version」に優先します。ただし、「Global RIP Version」が「By Interface」に設定されている場合には、事前に特定の「Receive Version」または「Send Version」が設定されていない VLAN インターフェースについては、以下のデフォルト値が設定されます。

- ・ Receive – RIPv1 または RIPv2 パケットを受け入れます。

- ・ Send - RIPv2 を使用してルート情報が他のルータにブロードキャストされます。
- ・ RIP Default Metric - 他のプロトコルからインポートされた外部ルートに割り当てられるデフォルトのメトリックを設定します（範囲：1～15、デフォルト：1）。

デフォルトのメトリックは、互換性のないメトリックを使用している外部ルートの再配信の問題を解決するために使用する必要があります。

他のプロトコルからのルート情報をRIPに再配信するときには低いメトリック値を使用することをお勧めします。大きいメトリック値を使用すると、RIPに再配信される外部ルート情報の有用性が制限されます。例えば、再配信されるルート情報のメトリックを10に定義した場合、それらのルートは、最大5つ先のホップまでしかアドバタイズすることができません（その時点で、メトリックが最大ホップ数である15に達するからです）。メトリックを1に定義すれば、トラフィックは、RIPドメイン内で許可されている最大ホップ数まで、インポートされたルートをたどることができます。ただし、小さいメトリック値を使用するとルーティングループが発生する可能性が高くなるので注意してください。そのようなことが発生する状況として、例えば、複数の再配信ポイントがあり、ルータが発信元から学習する外部ネットワークのメトリック値よりも再配信ポイントから学習する同じ外部ネットワークのメトリック値の方が妥当な場合などが挙げられます。

「Redistribute」画面で設定されるメトリック値（「ルート情報の再配信の設定」を参照）は、デフォルトのメトリックによって上書きされません。メトリック値が「Redistribute」画面で設定されていない場合は、デフォルトメトリックによって、インポートされたすべての外部ルートに使用されるメトリック値が設定されます。

- ・ RIP Max Prefix - ルーティングテーブルにインポートできる RIP ルートの最大数を設定します（範囲：1～7,168、デフォルト：7,168）。
- ・ Default Information Originate - ローカルの RIP 自律システムに対するデフォルトの外部ルートを生成します（デフォルト：Disabled）。
- ・ デフォルトルートは、RIP が有効になっているすべてのレイヤ3インターフェースに設定されます。外部クエリに対する応答パケットでは、アクティブなそれぞれの RIP インターフェースが IP アドレス 0.0.0.0 のデフォルトルータとしてマークされます。
- ・ Default Distance - 他のルーティングプロトコルから学習する外部ルートの管理距離を定義します。外部ルートとは、最適パスがローカル RIP 自律システム外部のネイバールータから学習されるルートです。管理距離が 255 のルートは、ルーティングテーブルにはインポートされません（範囲：1～255、デフォルト：120）。

管理距離は、同じ宛先に対して異なるルーティングプロトコルから学習した異なるルートが2つ以上存在する場合にルータが優先パスを選択するために使用します。管理距離が短いほど、プロトコルの信頼性が高いということになります。

「Routing Protocol」→「RIP」→「Distance」を選択すると、特定のネットワークアドレスに対する管理距離を設定することや、ルーティング情報を提供するルータの IP アドレスに応じてネットワークをフィルタリングするアクセスリストを設定することができます。

- ・ Number of Route Changes - IP ルートデータベースに対して RIP によって加えられた変更の回数。
- ・ Number of Queries - RIP クエリに対して他のシステムから送信された応答の数。

基本タイマー設定

[注意] : タイマーは、ネットワーク内のすべてのルータで同じ値に設定する必要があります。

- ・ Update - 更新メッセージの送信間隔を設定します。これは、すべての基本的な RIP プロセスの制御に使用される基本タイマーです (範囲: 5 ~ 2,147,483,647 秒、デフォルト: 30 秒)。

更新タイマーの設定間隔を短くすると、ルータで更新メッセージの処理に大幅な時間が費やされることになる可能性があります。反対に、間隔が長すぎると、ネットワーク設定の変更に対するルーティングプロトコルの反応が鈍くなります。

- ・ Timeout - ここで指定されている期間、ルータがダウンしていることを宣言する更新メッセージが発行されなかったことを示します。この期間を過ぎると、ルートは、アクセス不能としてマークされ (つまり、メトリックが infinite に設定され)、到達不能としてアドバタイズされます。ただし、該当のルートでのパケットの転送は続行されます (範囲: 90 ~ 360 秒、デフォルト: 180 秒)。
- ・ Garbage Collection - 「Timeout」タイマーに設定されている期間が経過した後、ルータは、この「Garbage Collection」タイマーで設定されている期間が経過してから、該当のエントリをルーティングテーブルから削除します。このタイマーを使用することにより、ネイバールータがルートをパージする前に無効なルートを認識できるようになります (範囲: 60 ~ 240 秒、デフォルト: 120 秒)。

Web インターフェース

RIP の全般設定を設定するには、以下のようにします。

- (1) 「Routing Protocol」→「RIP」→「General」を選択します。
- (2) 「Step」リストで「Configure Global」を選択します。
- (3) RIP を有効にし、事前に特定の「Receive Version」または「Send Version」が指定されていないインターフェースで使用される RIP バージョンを「RIPv1」または「RIPv2」に設定してから、外部ルートに割り当てられるデフォルトのメトリック、システムで許可される最大ルート数、および基本タイマーを設定します。

(4) < Apply > ボタンをクリックします。

Routing Protocol > RIP > General

Action: Configure

Global

RIP Routing Process	☒ Enabled
Global RIP Version	By interface
RIP Default Metric (1-15)	1
RIP Max Prefix (1-7168)	7168
Default Information Originate	☐ Enabled
Default Distance (1-255)	120
Number of Route Changes	0
Number of Queries	0

Basic Timer

Update (5-2147483647)	30 sec
Timeout (90-360)	180 sec
Garbage Collection (60-240)	120 sec

Apply Revert

画面 1-310 :RIP の全般設定の設定

ルーティングテーブルのエントリのクリア

「Routing Protocol」→「RIP」→「General」（Clear Route）を選択すると、ルーティングテーブルのエントリをルートタイプまたは特定のネットワークアドレスに基づいてクリアすることができます。

関連する CLI 情報

「clear ip rip route」

コマンドの使用

クリアするタイプを「All」にすると RIP テーブル内のすべてのルートが削除されます。RIP ネットワーク全体が削除されないようにするには、「Routing Protocol」→「RIP」→「Redistribute」を選択して表示される画面で、RIP ネットワークに接続しているルートの情報が再配信されるようにします。ネイバールータから学習した RIP ルートを削除するが RIP ネットワークはそのままにする場合は、タイプが「RIP」のルートをルーティングテーブルからクリアします。

パラメータ

以下のパラメータが表示されます。

- ・ Clear Route By Type - 以下のタイプに基づいて RIP ルーティングテーブルのエントリをクリアします。
 - ・ All - ルーティングテーブルからすべてのエントリを削除します。
 - ・ Connected - 現在接続しているエントリをすべて削除します。
 - ・ OSPF - OSPF を使用して学習したすべてのエントリを削除します。
 - ・ RIP - RIP を使用して学習したすべてのエントリを削除します。
 - ・ Static - すべてのスタティックエントリを削除します。
- ・ Clear Route By Network - 特定のルートをその IP アドレスとプレフィクス長に基づいてクリアします。
 - ・ Network IP Address - 指定されたネットワークアドレスに関連付けられているすべてのエントリを削除します。
 - ・ Prefix Length - アドレスのネットワーク部を設定するアドレスの（先頭からの）連続ビットの数を示す 10 進数。

Web インターフェース

エントリを RIP ルーティングテーブルからクリアするには、以下のようになります。

- (1) 「Routing Protocol」→「RIP」→「General」を選択します。
- (2) 「Step」リストで「Clear Route」を選択します。
- (3) タイプに基づいてルートをクリアする場合は、必要なタイプをドロップダウンリストから選択します。ネットワーク別のルートをクリアする場合は、有効なネットワークアドレスとプレフィックス長を入力します。

(4) < Apply > ボタンをクリックします。

Routing Protocol > RIP > General

Action: Clear Route ▼

Clear Route by ☐ Type ☒ Network

Network IP Address 192.168.1.0

Prefix Length (1-32) 24

Apply Revert

画面 1-311 : ルーティングテーブルのエントリのクリア

ネットワークインターフェースの指定

「Routing Protocol」→「RIP」→「Network」(Add) を選択すると、RIP ルーティングプロセスに含まれるネットワークインターフェースを指定することができます。

関連する CLI 情報

「network」

コマンドの使用

- ・ RIP では、指定されたインターフェースに関する更新メッセージのみが送受信されます。ネットワークが指定されていない場合、そのネットワーク内のインターフェースはいずれの RIP 更新メッセージでもアドバタイズされません。
- ・ デフォルトでは、ネットワークはまったく指定されていません。

パラメータ

以下のパラメータが表示されます。

- ・ By Address – ネットワークを RIP ルーティングプロセスに追加します。
 - ・ Subnet Address – ルータに直接接続しているネットワークの IP アドレス（デフォルト：ネットワークの指定なし）。
 - ・ Prefix Length – アドレスのネットワーク部を設定するアドレスの（先頭からの）連続ビットの数を示す 10 進数。このマスクは、関連付けられるルーティングエントリに使用されるホストアドレスビットを示します。
- ・ By VLAN – レイヤ 3 の VLAN を RIP ルーティングプロセスに追加します。VLAN は IP アドレスを指定して設定されていなければなりません（範囲：1 ～ 4,093）。

Web インターフェース

ネットワークインターフェースを RIP に追加するには、以下のようにします。

- (1) 「Routing Protocol」→「RIP」→「Network」を選択します。
- (2) 「Step」リストで「Add」を選択します。
- (3) RIP プロセスに関与するインターフェースを追加します。
- (4) < Apply > ボタンをクリックします。

The screenshot shows a web configuration page titled "Routing Protocol > RIP > Network". Below the title bar, there is a section for "Action:" with a dropdown menu set to "Add". Underneath, there are two radio buttons: "By IP Address" (which is selected) and "By VLAN". Below these, there are two input fields: "Subnet Address" with the value "10.1.0.0" and "Prefix Length (1-32)" with the value "16". At the bottom right of the form, there are two buttons: "Apply" and "Revert".

画面 1-312 :RIP プロセスへのネットワークインターフェースの追加

RIP を使用するネットワークインターフェースを表示するには、以下のようにします。

1. 「Routing Protocol」→「RIP」→「Network」を選択します。
2. 「Step」リストで「Show」を選択します。
3. 「IP Address」または「VLAN」を選択します。

Routing Protocol > RIP > Network

Action: Show

By: ☒ IP Address ☐ VLAN

RIP Network Address List Total: 1

	Subnet Address	Prefix Length
☐	10.1.0.0	16

Delete Revert

画面 1-313 :RIP を使用するネットワークインターフェースの表示

パッシブインターフェースの指定

「Routing Protocol」→「RIP」→「Passive Interface」(Add) を選択すると、RIP によって特定のインターフェースに関するルーティング情報更新メッセージが送信されないようにすることができます。

関連する CLI 情報

「passive-interface」

コマンドの使用

- ・ ネットワークインターフェースは、RIP ブローとキャストメッセージとマルチキャストメッセージを送信しないように設定することができます。ルーティング情報更新メッセージの送信がインターフェースでブロックされている場合でも、接続されているサブネットは引き続き他のインターフェースにアドバタイズされ、指定されたインターフェースに関する他のルータからの更新情報が引き続き受信され、処理されます。
- ・ この機能は、個々のネイバルルータに送信されるルーティング情報更新メッセージを制御するため、スタティックネイバルルータ指定機能（次のセクションを参照）と組み合わせて使用することができます。

パラメータ

以下のパラメータが表示されます。

- ・ VLAN – RIP 更新メッセージの送信を停止する VLAN インターフェース（範囲：1 ～ 4,093）。

Web インターフェース

パッシブ RIP インターフェースを指定するには、以下のようにします。

- (1) 「Routing Protocol」 → 「RIP」 → 「Passive Interface」 を選択します。
- (2) 「Step」 リストで「Add」を選択します。
- (3) RIP 更新メッセージの送信を停止するインターフェースを追加します。
- (4) < Apply > ボタンをクリックします。

Routing Protocol > RIP > Passive Interface

Action:

VLAN ID (1-4093)

Link State Router List Total: 2

Area ID	Link ID	Adv Router	Age	Sequence	Checksum
0.0.0.0	192.168.0.4	192.168.0.4	702	0x80000003	0xE6B4
0.0.0.0	192.168.1.2	192.168.1.2	355	0x80000005	0xDDBC

Link State Network List Total: 1

Area ID	Link ID	Adv Router	Age	Sequence	Checksum
0.0.0.0	192.168.0.4	192.168.0.4	702	0x80000001	0x8F16

Link State Summary List Total: 1

Area ID	Link ID	Adv Router	Age	Sequence	Checksum
0.0.0.0	192.168.1.0	192.168.1.2	638	0x80000001	0x99EB

Link State ASBR Summary List Total: 0

Area ID	Link ID	Adv Router	Age	Sequence	Checksum

Link State External List Total: 0

Area ID	Link ID	Adv Router	Age	Sequence	Checksum

Link State NSSA External List Total: 0

Area ID	Link ID	Adv Router	Age	Sequence	Checksum

画面 1-314 : パッシブ RIP インターフェースの指定

パッシブ RIP インターフェースを表示するには、以下のようにします。

1. 「Routing Protocol」 → 「RIP」 → 「Passive Interface」 を選択します。
2. 「Step」 リストで「Show」を選択します。

Routing Protocol > RIP > Passive Interface

Action:

VLAN ID List Max: 4093 Total: 1

☐	VLAN ID
☐	1

画面 1-315 : パッシブ RIP インターフェースの表示

スタティックネイバルータの指定

「Routing Protocol」→「RIP」→「Passive Interface」(Add)を選択すると、RIPによって生成されるブロードキャストメッセージまたはマルチキャストメッセージに依存せずに、(特に、ポイントツーポイントリンクについて)ルーティング情報をスタティックネイバルータと直接交換するようにルータを設定することができます。この機能は、個々のネイバルータに送信されるルーティング情報更新メッセージを制御するため、パッシブインターフェース指定機能(直前のセクションを参照)と組み合わせて使用することができます。

関連する CLI 情報

「neighbor」

パラメータ

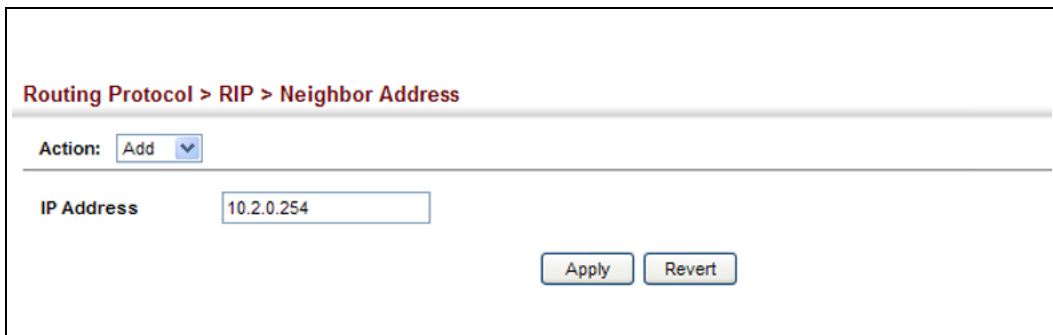
以下のパラメータが表示されます。

- ・ IP Address - ルーティング情報を交換するスタティックネイバルータの IP アドレス。

Web インターフェース

スタティック RIP ネイバルータを指定するには、以下のようになります。

- (1) 「Routing Protocol」→「RIP」→「Neighbor Address」を選択します。
- (2) 「Step」リストで「Add」を選択します。
- (3) RIP を使用して容易に検出できないことがあるスタティックネイバルータのアドレスを追加します。
- (4) < Apply > ボタンをクリックします。



Routing Protocol > RIP > Neighbor Address

Action: Add ▼

IP Address 10.2.0.254

Apply Revert

画面 1-316 : スタティック RIP ネイバルータの指定

スタティック RIP ネイバルータを表示するには、以下のようになります。

1. 「Routing Protocol」→「RIP」→「Neighbor Address」を選択します。

2. 「Step」 リストで「Show」を選択します。

Routing Protocol > RIP > Neighbor Address

Action: Show

Neighbor Address List Total: 1

	IP Address
☐	10.2.0.254

Delete Revert

画面 1-317 : スタティック RIP ネイバールータの表示

ルート情報の再配信の設定

「Routing Protocol」→「RIP」→「Redistribute」(Add)を選択すると、外部ルーティング情報（直接接続ルート、プロトコル、スタティックルート）を他のルーティングドメインからこの自律システムにインポートすることができます。

関連する CLI 情報

「redistribute」

パラメータ

以下のパラメータが表示されます。

- Protocol – インポートできるルートのタイプとして、以下のようなものがあります。
 - Connected – インターフェースで IP を有効にするだけで自動的に確立されるルートをインポートします。
 - Static – スタティックルートがこのルーティングドメインにインポートされます。
 - OSPF – 外部ルートが OSPF プロトコルからこのルーティングドメインにインポートされます。
- Metric – 指定されたプロトコルのすべての外部ルートに割り当てられるメトリック（範囲：0 ～ 16、デフォルト：「プロトコルの全般設定の設定」で説明されているデフォルトメトリック）。

ルートメトリックは、互換性のないメトリックを使用している外部ルートの再配信の問題を解決するために使用する必要があります。

メトリック値がこの画面で設定されていない場合は、デフォルトメトリックによって、インポートされたすべての外部ルートに使用されるメトリック値が決まります。

他のプロトコルからのルート情報をRIPに再配信するときには低いメトリック値を使用することをお勧めします。大きいメトリック値を使用すると、RIP に再配信される外部ルート情報の有用性が制限されます。例えば、再配信されるルート情報のメトリックを 10 に定義した場合、それらのルートは、最大 5 つ先のホップまでしかアドバタイズすることができません（その時点で、メトリックが最大ホップ数である 15 に達するからです）。メトリックを 1 に定義すれば、トラフィックは、RIP ドメイン内で許可されている最大ホップ数まで、インポートされたルートをたどることができます。ただし、小さいメトリック値を使用するとルーティングループが発生する可能性が高くなります。そのようなことが発生する状況として、例えば、複数の再配信ポイントがあり、ルータが発信元から学習する外部ネットワークのメトリック値よりも再配信

Web 設定

ユニキャストルーティング

ポイントから学習する同じ外部ネットワークのメトリック値の方が妥当な場合などが挙げられます。

Web インターフェース

外部ルーティング情報を他のルーティングドメインからインポートするには、以下のようになります。

- (1) 「Routing Protocol」 → 「RIP」 → 「Redistribute」 を選択します。
- (2) 「Step」 リストで 「Add」 を選択します。
- (3) 外部ルートをインポートするプロトコルのタイプ（Directly Connected、OSPF、または Static） およびそれらのルートに割り当てるメトリックを指定します。
- (4) < Apply > ボタンをクリックします。

Routing Protocol > RIP > Redistribute

Action: Add ▼

Protocol: OSPF ▼

Metric (1-16): 3 (Optional)

Apply Revert

画面 1-318 :RIP への外部ルート情報の再配信

RIP にインポートされた外部ルートを表示するには、以下のようになります。

1. 「Routing Protocol」 → 「RIP」 → 「Redistribute」 を選択します。
2. 「Step」 リストで 「Show」 を選択します。

Routing Protocol > RIP > Redistribute

Action: Show ▼

Redistribute List Max: 3 Total: 1

	Protocol	Metric
☐	OSPF	3

Delete Revert

画面 1-319 :RIP に再配信された外部ルート情報の表示

管理距離の指定

「Routing Protocol」→「RIP」→「Distance」を選択すると、他のルーティングプロトコルから学習する外部ルート of 管理距離を定義することができます。

関連する CLI 情報

「distance」

コマンドの使用

- ・ 管理距離は、同じ宛先に対して異なるルーティングプロトコルから学習した異なるルートが 2 つ以上存在する場合にルータが優先パスを選択するために使用します。管理距離が短いほど、プロトコルの信頼性が高いということになります。
- ・ アクセスリストを使用して、ルーティング情報を提供するルータの IP アドレスに応じてネットワークをフィルタリングすることができます。例えば、管理制御によって、ルータが信頼性の高くないルーティング情報を受け取らないようにすることができます。
- ・ 管理距離は、指定されたネットワークについて学習されたすべてのルートに適用されます。

パラメータ

以下のパラメータが表示されます。

- ・ Distance - 外部ルートの管理距離。外部ルートとは、最適パスがローカル RIP 自律システム外部のネイバールータから学習されるルートです。管理距離が 255 のルートは、ルーティングテーブルにはインポートされません（範囲：1 ～ 255）。
- ・ IP Address - ルートエントリの IP アドレス。
- ・ Subnet Mask - このマスクは、関連付けられるルーティングエントリに使用されるホストアドレスビットを示します。
- ・ ACL Name - アクセスコントロールリストの名前。標準または拡張版の IP ACL および MAC ACL を含め、任意のタイプの ACL を指定することができます（範囲：1 ～ 16 文字）。

Web インターフェース

他のルーティングプロトコルから学習する外部ルートの管理距離を定義するには、以下のようになります。

- (1) 「Routing Protocol」→「RIP」→「Distance」を選択します。
- (2) 「Step」リストで「Add」を選択します。
- (3) 距離および外部ルートを入力し、必要な場合は、ルーティング情報を提供するルータの IP アドレスに応じてネットワークをフィルタリングする ACL の名前を入力します。

(4) < Apply > ボタンをクリックします。

Routing Protocol > RIP > Distance

Action: Add ▼

Distance (1-255) 120

IP Address 192.168.3.0

Subnet Mask 255.255.255.0

ACL Name ☐ ▼

Apply Revert

画面 1-320：外部ルートに割り当てられる管理距離の設定

他のルーティングプロトコルから学習する外部ルートに割り当てられる管理距離を表示するには、以下のようにします。

1. 「Routing Protocol」→「RIP」→「Distance」を選択します。
2. 「Step」リストで「Show」を選択します。

Routing Protocol > RIP > Distance

Action: Add ▼

Distance (1-255) 120

IP Address 192.168.3.0

Subnet Mask 255.255.255.0

ACL Name ☐ ▼

Apply Revert

画面 1-321：外部ルートに割り当てられる管理距離の表示

RIP ネットワークインターフェースの設定

「Routing Protocol」→「RIP」→「Distance」(Add) を選択すると、RIP ルーティングプロセスに各インターフェースの送信バージョンと受信バージョン、認証設定、およびループバック防止策を指定することができます。

関連する CLI 情報

「ip rip receive version」

「ip rip send version」

「ip rip authentication mode」

「ip rip authentication string」

「ip rip split-horizon」

コマンドの使用

- ・ 受信プロトコルと送信プロトコルのタイプの指定
- ・ 各 RIP インターフェースの受信プロトコルメッセージタイプ（つまり、RIP バージョン）および送信プロトコルメッセージのタイプ（つまり、RIP バージョンまたは互換モード）を指定します。

インターフェースの RIP の「Receive Version」または「Send Version」を設定すると、RIP 全般設定画面で指定されたグローバル設定が上書きされます（「プロトコルの全般設定の設定」を参照）。

- ・ 「Send Version」は、以下のオプションに基づいて指定することができます。
 - ・ ローカルネットワーク内のすべてのルータが RIPv1 または RIPv2 に基づくものである場合は、それぞれ、「RIPv1」または「RIPv2」を選択します。
 - ・ 「RIPv1 Compatible」を選択すると、通常 RIPv2 で必要とされるマルチキャストの代わりに RIPv2 アドバタイズメントリストを使用してネットワーク上の他のルータにブロードキャストすることにより、ルート情報が伝搬されるようになります（このモードを使用すると、RIP ブロードキャストメッセージのみを受信する古い RIPv1 ルータで RIPv2 によって提供されるすべての情報（サブネットマスク、ネクストホップ、認証情報など）を受信できるようになります）（これがデフォルトの設定です）。
 - ・ 「Do Not Send」を選択すると、ネットワークに接続している他のルータによってアドバタイズされるルート情報をパッシブに監視することができます。
- ・ 「Receive Version」は、以下のオプションに基づいて指定することができます。
 - ・ ローカルネットワーク内のすべてのルータが RIPv1 または RIPv2 に基づくものである場合は、それぞれ、「RIPv1」または「RIPv2」を選択します。
 - ・ ローカルネットワーク内の一部のルータは RIPv2 を使用している一方でまだ RIPv1 を使用している古いルータもいくつかある場合は、「RIPv1 and RIPv2」を選択します（これがデフォルトの設定です）。
 - ・ ダイナミックエントリをインターフェースのルーティングテーブルに追加する必要がない場合は、「Do Not Receive」を選択します（例えば、特定のインターフェースでスタティックルートのみが許可されている場合など）。

プロトコルメッセージ認証

RIPv1 はセキュアなプロトコルではありません。UDP ポート 520 からプロトコルメッセージを送信するあらゆるデバイスは、ネイバルルータからは、ルータであるとみなされます。認証を一切不要にすると、不正なプロトコルメッセージや迷惑プロトコルメッセージが、容易にネットワーク全体に伝搬されてしまいます。

RIPv2 は、簡易パスワードまたは MD5 キー暗号化による認証をサポートしています。ルータは、認証メッセージを交換するように設定されている場合は、すべての送信プロトコルパケットにパスワードを挿入し、すべての受信パケットをチェックして、承認されたパスワードが受信パケットに含まれていることを確認します。着信プロトコルメッセージに正しいパスワードが含まれていない場合、それらのメッセージは、そのままドロップされます。

認証が正常に機能するようにするため、送信インターフェースと受信インターフェースの両方が同じパスワードまたは認証キーを指定して設定されていなければなりません。

ループバックの防止

レイヤ 2 スイッチでループを防ぐためにスパニングツリーを使用するのと同じように、ルータでも、データトラフィックの無限再送信を発生させる可能性があるループを防ぐための手法を使用します。プロトコルパケットがループに陥ると、リンクが輻輳し、その結果、プロトコルパケットが失われることがあります。ただし、ネットワークは、ゆっくりと新しい状態に収束します。RIP では、ネットワークトポロジが変更された場合の収束を迅速化し、ループがほとんど発生しないようにすることができる手法がいくつかサポートされています。

パラメータ

以下のパラメータが表示されます。

- ・ VLAN ID - レイヤ 3 の VLAN インターフェイス。このインターフェイスは、IP アドレスを指定して設定されており、アクティブなリンクをもっていなければなりません（範囲：1 ～ 4,093）。
- ・ Send Version - インターフェイスでの送信に使用される RIP バージョン。
 - ・ RIPv1 - RIPv1 パケットのみを送信します。
 - ・ RIPv2 - RIPv2 パケットのみを送信します。
 - ・ RIPv1 Compatible - RIPv2 を使用してルート情報を他のルータにブロードキャストします。
 - ・ Do Not Send - RIP 更新メッセージを送信しません。ネットワークに接続している他のルータによってアドバタイズされるルート情報をパッシブに監視します。

デフォルトは、「Global RIP Version」の設定（「プロトコルの全般設定の設定」を参照）によって異なります。

Receive Version - インターフェイスでの受信に使用される RIP バージョン。

RIPv1 - RIPv1 パケットのみを受け入れます。

RIPv2 - RIPv2 パケットのみを受け入れます。

RIPv1 or RIPv2 - RIPv1 または RIPv2 パケットを受け入れます。

Do Not Receive - 着信 RIP パケットを受け入れません。このオプションを指定すると、インターフェイスのルーティングテーブルにダイナミックエントリが、一切、追加されなくなります。

デフォルトは、「Global RIP Version」の設定（「プロトコルの全般設定の設定」を参照）によって異なります。

- ・ Authentication Type - RIPv2 プロトコルメッセージの交換に必要な認証のタイプを指定します（デフォルト：No Authentication）。
 - ・ No Authentication - 認証は不要です。
 - ・ Simple Password - 承認されたパスワードに基づいてインターフェイスがルーティング情報を他のルータと交換するようにします（ただし、認証は RIPv2 のみに適用されるという点に注意してください）。
 - ・ MD5 - DM 5（Message Digest 5）認証。

MD5 は、認証キーを取得して 128 bits のメッセージダイジェスト（「フィンガープリント」）を生成する一方向ハッシュアルゴリズムです。MD5 は、コンピュータ上を使用して、同じメッセージダイジェストを含む 2 つのメッセージを作成することや、何らかの事前指定のターゲットメッセージダイジェストを含むメッセージを生成することを不可能にします。
- ・ Authentication Key - RIPv2 パケットの認証に使用されるキーを指定します。認証が正常に機能するようにするため、送信インターフェイスと受信インターフェイスの両方が

同じパスワードを使用するようにしなければなりません（範囲:1～16文字（大文字と小文字の区別あり））。

- ・ Instability Prevention – ネットワークトポロジ変更時の輻輳時間を短縮し、RIP メッセージが送信元ルータにループバックされないようにするための方法を指定します。
 - ・ スプリットホライズン – ルート情報が取得元のインターフェイスポートに伝搬されなくなります。
 - ・ ポイズンリバーズ – ルート情報が取得元のインターフェイスポートに伝搬されますが、距離ベクトルメトリックが infinity に設定されます。そのようにすることで、収束が迅速化されます（これがデフォルトの設定です）。
 - ・ None – ループバック防止策を使用しません。防止策を使用せずにループが発生する場合は、ルートのホップ数が徐々にインクリメントされ、ルートが到達不能とみなされる前に、infinity（つまり、16）になります。

Web インターフェース

RIP のネットワークインターフェース設定を指定するには、以下のようにします。

- (1) 「Routing Protocol」 → 「RIP」 → 「Interface」 を選択します。
- (2) 「Step」 リストで 「Add」 を選択します。
- (3) RIP プロセスに参与するレイヤ 3 の VLAN インターフェースを選択します。送信および受信される RIP プロトコルメッセージタイプを選択します。RIP 認証方式とパスワードを選択します。それから、ループバック防止策を設定します。
- (4) < Apply > ボタンをクリックします。

Routing Protocol > RIP > Interface

Action: Add

VLAN ID (1-4093): 1

Send Version: RIPv1 Compatible

Receive Version: RIPv1 and RIPv2

Authentication Type: Simple Password

Authentication Key: mighty

Instability Prevention: Poison Reverse

Apply Revert

画面 1-322 :RIP のネットワークインターフェースの設定

RIP について指定されているネットワークインターフェース設定を表示するには、以下のようになります。

1. 「Routing Protocol」 → 「RIP」 → 「Interface」 を選択します。

2. 「Step」 リストで「Show」を選択します。

Routing Protocol > RIP > Interface

Action: Show ▼

Interface Settings List Max: 4093 Total: 2

☐	VLAN ID	Send Version	Receive Version	Authentication Type	Authentication Key	Instability Prevention
☐	1	RIPv1 Compatible	RIPv1 and RIPv2	Simple Password	mighty	Poison Reverse
☐	2	RIPv1 Compatible	RIPv1 and RIPv2	No Authentication		Poison Reverse

Delete Revert

画面 1-323 :RIP ネットワークインターフェース設定の表示

RIP インターフェース設定の表示

「Routing Protocol」→「RIP」→「Statistics」(Show Interface Information) を選択すると、RIP インターフェースの設定情報を表示することができます。

関連する CLI 情報

「show ip rip」

パラメータ

以下のパラメータが表示されます。

- ・ Interface - RIP ルータインターフェースの送信元 IP アドレス。
- ・ Auth Type - RIPv2 プロトコルメッセージの交換に使用された認証のタイプ。
- ・ Send Version - インターフェースでの送信に使用された RIP バージョン。
- ・ Receive Version - インターフェースでの受信に使用された RIP バージョン。
- ・ Rcv Bad Packets - 受信された不良 RIP パケットの数。
- ・ Rcv Bad Routes - 受信された不良ルート情報の件数。
- ・ Send Updates - ルートの変更回数。

Web インターフェース

RIP インターフェースの設定情報を表示するには、以下のようにします。

- (1) 「Routing Protocol」→「RIP」→「Statistics」を選択します。
- (2) 「Step」リストで「Show Interface Information」を選択します。

Routing Protocol > RIP > Statistics						
Action: Show Interface Information						
Interface Information Max: 4093 Total: 3						
Interface	Auth Type	Send Version	Receive Version	Rcv Bad Packets	Rcv Bad Routes	Send Updates
1.2.3.4	No Authentication	Do Not Send	RIPv1 and RIPv2	10	2	124
10.1.0.1	Simple Password	RIPv1	Do Not Receive	3	4	23
140.113.1.3	MD5	RIPv1 Compatible	RIPv2	5	5	65

画面 1-324 :RIP インターフェース設定の表示

ピアルータ情報の表示

「Routing Protocol」→「RIP」→「Statistics」（Show Peer Information）を選択すると、隣接 RIP ルータに関する情報を表示することができます。

関連する CLI 情報

「show ip protocols rip」

パラメータ

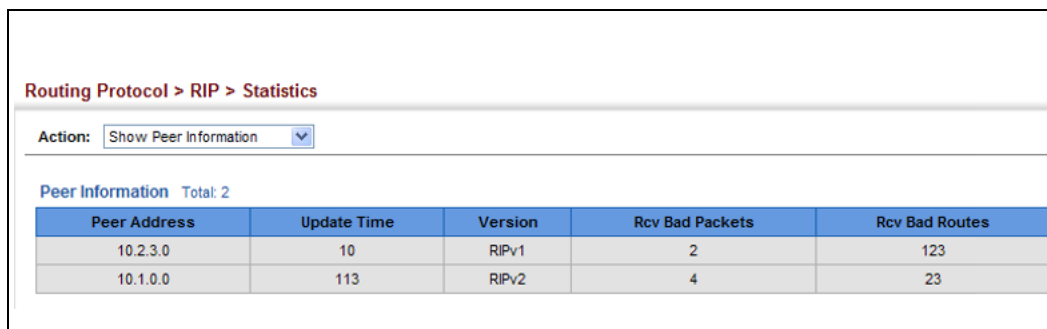
以下のパラメータが表示されます。

- ・ Peer Address - 隣接 RIP ルータの IP アドレス。
- ・ Update Time - 前回、ピアからルート更新メッセージが受信された時刻。
- ・ Version - ピアから RIPv1 パケットと RIPv2 パケットのどちらが受信されたかを示します。
- ・ Rcv Bad Packets - ピアから受信された不良 RIP パケットの数。
- ・ Rcv Bad Routes - ピアから受信された不良ルート情報の件数。

Web インターフェース

隣接 RIP ルータに関する情報を表示するには、以下のようにします。

- (1) 「Routing Protocol」→「RIP」→「Statistics」を選択します。
- (2) 「Step」リストで「Show Peer Information」を選択します。



Routing Protocol > RIP > Statistics				
Action: Show Peer Information				
Peer Information Total: 2				
Peer Address	Update Time	Version	Rcv Bad Packets	Rcv Bad Routes
10.2.3.0	10	RIPv1	2	123
10.1.0.0	113	RIPv2	4	23

画面 1-325 :RIP ピア情報の表示

RIP に関する統計情報のリセット

「Routing Protocol」→「RIP」→「Statistics」(Reset Statistics) を選択すると、RIP プロトコルメッセージに関するすべての統計情報をリセットすることができます。

関連する CLI 情報

該当するコマンドなし。

Web インターフェース

RIP に関する統計情報をリセットするには、以下のようにします。

- (1) 「Routing Protocol」→「RIP」→「Statistics」を選択します。
- (2) 「Step」リストで「Reset Statistics」を選択します。
- (3) < Reset > ボタンをクリックします。

Routing Protocol > RIP > Statistics						
Action: Show Interface Information ▼						
Interface Information Max: 4093 Total: 3						
Interface	Auth Type	Send Version	Receive Version	Rcv Bad Packets	Rcv Bad Routes	Send Updates
1.2.3.4	No Authentication	Do Not Send	RIPv1 and RIPv2	10	2	124
10.1.0.1	Simple Password	RIPv1	Do Not Receive	3	4	23
140.113.1.3	MD5	RIPv1 Compatible	RIPv2	5	5	65

画面 1-326 :RIP に関する統計情報のリセット

1.18.3 OSPF プロトコル（バージョン 2）の設定

OSPF（Open Shortest Path First）は、リンクの変更が頻繁に発生する広域ネットワークに比較的適している手法です。また、RIP に比べ、サブネットの取り扱いにも適しています。OSPF プロトコルでは、ネイバルルータに対する各リンクのステータスがアクティブに確認されて、最短パスツリーが生成され、その情報に基づいてルーティングテーブルが作成されます。それから、IP マルチキャストを使用して、ルーティング情報が伝搬されます。ルーティングトラフィックをさらに減らすため、別のルーティングエリアスキーマも使用されます。

【注意】 本製品に実装されている OSPF プロトコルは RFC 2328（バージョン 2）に基づいています。また、本製品は、古い OSPF ルータが存在している場合にネットワーク全体で同じ方法を使用してサマリルートコストが計算されるようにするため、Not-So-Stubby-Area オプション（RFC 3101）に加え、RFC 1583（初期の OSPFv2）互換モードもサポートしています。

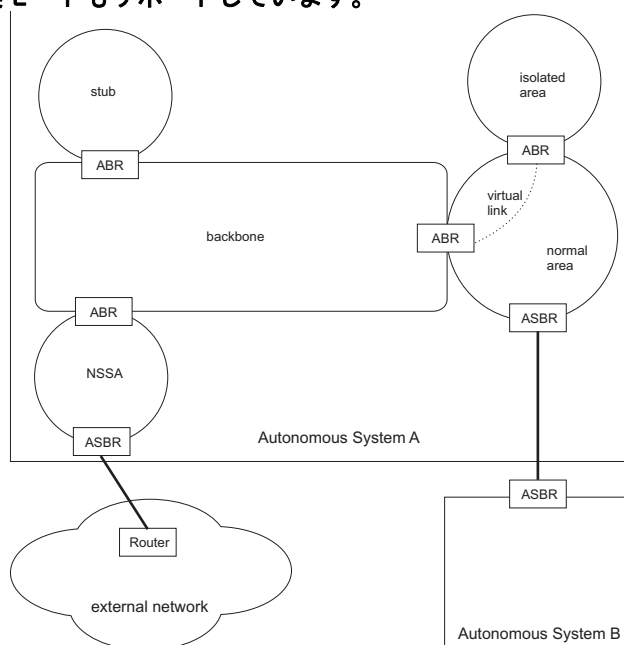


図 1-28:OSPF の設定

コマンドの使用

- ・ OSPF では、単純なホップ数が確認されるだけではありません。いずれかのノードへの最短パスをツリーに追加するときには、遅延、スループット、および接続性に基づいて最適パスが選択されます。OSPF では、IP マルチキャストを使用して、ルーティングパスに関する更新メッセージを送信または受信する際に必要となるルーティングトラフィックの量を減らします。OSPF で使用される分離ルーティングエリアスキーマによって、さらにルーティングトラフィックの量が減らされ、必然的に、ルーティング保護のレベルが向上します。それだけでなく、すべてのルーティングプロトコルメッセージの交換が認証されるようにすることができます。さらに、OSPF アルゴリズムは、TCP/IP イントラネットでの効率的な動作のために調整されています。
- ・ OSPFv2 は、OSPFv1 のアップグレード版であり、OSPFv1 との互換性を備えています。OSPFv2 では、プロトコルメッセージ認証の強化や、非ブロードキャストネットワークでの OSPF の実行を可能にするポイントツーマルチポイントインターフェースの追加といった機能に加え、重複するエリア範囲がサポートされるようになりました。

- ・ OSPF を使用する場合は、ネットワーク（自律システム）を、標準エリア、Stubby エリア（スタブ）、Not-So-Stubby エリアにまとめる必要があります。リンクステートアドバタイズメント（LSA: Link State Advertisement）によって集約できるサブネットアドレスの範囲を設定し、OSPF バックボーンに物理的に直接アクセスできないエリアの仮想リンクを設定します。
- ・ 大規模ネットワークで OSPF を実装するには、第 1 に、ネットワークを論理エリアにまとめて、LSA をアクティブに交換する OSPF ルータの数が制限されるようにします。第 2 に、ルータで設定されている IP インターフェースをそれらのエリアの 1 つに割り当てることにより、OSPF インターフェースを定義します。この OSPF インターフェースを使用して、隣接 OSPF ルータに対する OSPF トラフィックの送受信が行われます。
- ・ また、多数のサブネットワークアドレスをカバーするエリア範囲を指定して、OSPF トラフィックの交換をさらに最適化することができます。これは、エリア境界ルータ（ABR: Area Border Router）間で交換されるトラフィックの量を制限するための重要な手法です。
- ・ 最後に、OSPF バックボーンに物理的に接続しない OSPF エリアへの仮想リンクを指定する必要があります。仮想リンクは、隣接するエリアが分断されないようにするため、または、バックボーンエリアを結合するため、隣接エリア間で冗長リンクを実現する場合にも使用することができます（ただし、仮想リンクはスタブエリアまたは NSSA ではサポートされないので注意してください）。

アドレスに基づくネットワークエリアの定義

OSPF プロトコルブロードキャストメッセージ（つまり、リンクステートアドバタイズメント（LSA））は、ネットワークパフォーマンスへの影響を抑えるため、エリア単位で制限されます。

大規模ネットワークは、ネットワークの安定性を向上させるため、また、ルーティング情報をよりコンパクトなメッセージにまとめることによってプロトコルトラフィックを減らすため、別々の OSPF エリアに分割する必要があります。エリア内の各ルータからは、ネットワークトポロジ（エリアリンク、直接接続エリアのルートサマリ、他のエリアへの外部リンクなど）が同じように見えます。

「Routing Protocol」→「OSPF」→「Network Area」（Add）を選択すると、OSPF エリアおよびそのエリア内で動作するインターフェースを定義することができます。エリア ID が 0.0.0.0 のバックボーンエリアを指定して、自律システムを設定する必要があります。デフォルトでは、他のすべてのエリアは標準の通過エリアとして作成されます。

標準エリア内のルータは、個々のノードに関するルーティング情報をインポートまたはエクスポートすることができます。ネットワークにフロードされるルーティングトラフィックの量を減らすため、エリア内の広範なネットワークアドレスをカバーする単一のサマリルートをエクスポートするようにエリアを設定することができます。エリア間で渡されるルート情報の量を減らすため、エリアを Stubby エリアまたは Not-So-Stubby エリアとして設定することができます。

標準エリア - 大規模な OSPF ドメインは、ネットワークの安定性を向上させるため、また、ある範囲のアドレスを単一ルートに集約するルートサマリを使用して必要なルーティングトラフィックの量を減らすため、いくつかのエリアに分割する必要があります。バックボーンまたは標準エリアは、他のエリア同士の間でトラフィックを渡すことができ、そのため、通過エリアとして知られています。エリア内の各ルータは、同一のルーティングテーブルを保有します。それらのテーブルには、自律システムのトポロジを表わすエリアリンク、サマリリンク、または外部リンクが含まれます。

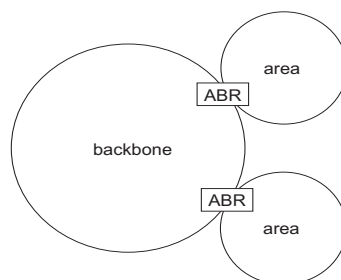


図 1-29: OSPF エリア

関連する CLI 情報

「router ospf」

「network area」

コマンドの使用

- ・ 各 OSPF ブロードキャストエリアのエリア ID とそれに対応するネットワークアドレス範囲を指定します。各エリアは、ネットワークトポロジに対する認識が共通のものであることを確認するため、LSA をアクティブに交換する OSPF ルータの論理グループを示します。
- ・ 各エリアはバックボーンエリアに接続されていなければなりません。バックボーンエリアは、自律システム内の他のエリア同士の間でルーティング情報を渡します。すべてのルータはバックボーンに接続していなければなりません。直接接続することも、物理的に直接接続できない場合は仮想リンクを使用することもできます。
- ・ すべてのエリアは、「Network Area」(Add) 画面で標準の通過エリアとして作成されます。標準エリア (または通過エリア) では、外部 LSA を送受信することができます。必要であれば、エリアは、外部ルート情報を自らのエリアにインポートできる Not-So-Stubby エリア (NSSA) として設定することも、Stubby エリアとして設定することもできます。
- ・ エリアには、ある範囲のサブネットワークアドレスが割り当てられなければなりません。エリアとそれに対応するアドレス範囲はルーティングインターフェースを形成します。形成されるルーティングインターフェースは、該当のすべてのサブネットワークアドレスからの LSA を集約してその情報をネットワーク内の他のルータと交換するように設定することができます (「エリア範囲 (ABR のルートサマリ) の設定」) を参照)。
- ・ アドレス範囲が他のネットワークエリアと重複している場合には、ルータは、アドレス範囲がインターフェースアドレスに最もマッチするネットワークエリアを使用します。また、アドレス範囲がエリアから削除された場合、削除されたものほどではないが該当のエリアをおおまかにカバーしているアドレス範囲が指定されていれば、その範囲に属するインターフェースはアクティブなままになるので注意してください。

パラメータ

以下のパラメータが表示されます。

- ・ Process ID - 複数のルーティングインターフェースを区別するために使用されるプロトコル ID (範囲: 1 ~ 65,535)。
- ・ IP Address - エリアに追加されるインターフェースのアドレス。
- ・ Netmask - エリアに追加されるアドレス範囲のネットワークマスク。
- ・ Area ID - 指定されたアドレスまたは範囲が割り当てられるエリア。OSPF エリアは、同じルーティング情報を共有するルータのグループを示します。エリア ID の形式は、IPv4 アドレス形式にすることも、4 octets の符号なし整数 (範囲は 0 ~ 4,294,967,295) にすることもできます。

エリアに 1 つまたは複数のインターフェースを追加するには、ネットワークマスクを使用してネットワークセグメント上のすべてのルータのエリア ID を同じ値に設定します。

Web インターフェース

OSPF エリアおよびそのエリア内で動作するインターフェースを定義するには、以下のようになります。

- (1) 「Routing Protocol」 → 「OSPF」 → 「Network Area」 を選択します。
- (2) 「Step」 リストで 「Add」 を選択します。
- (3) ネットワーク内の他のすべてのエリアに隣接するバックボーンエリアを設定し、他のすべての OSPF インターフェースに対するエリアを設定します。
- (4) < Apply > ボタンをクリックします。

Routing Protocol > OSPF > Network Area

Action: Add

Process ID (1-65535)	1
IP Address	192.168.0.0
Netmask	255.255.255.0
Area ID	0.0.0.0

Apply
Revert

画面 1-327 : アドレスに基づく OSPF ネットワークエリアの定義

OSPF エリアとそれらに割り当てられているインターフェースを表示するには、以下のようになります。

- (1) 「Routing Protocol」 → 「OSPF」 → 「Network Area」 を選択します。

(2) 「Step」 リストで「Show」を選択します。

Routing Protocol > OSPF > Network Area

Action: Show

Process ID: 1

Network Area Address List Max: 16 Total: 2

☐	IP Address	Netmask	Area ID
☐	192.168.0.0	255.255.255.0	0.0.0.0
☐	192.168.1.0	255.255.255.0	192.168.1.0

Apply Revert

画面 1-328 :OSPF ネットワークエリアの表示

OSPF プロセス ID を表示するには、以下のようにします。

1. 「Routing Protocol」 → 「OSPF」 → 「Network Area」 を選択します。
2. 「Step」 リストで「Show Process」を選択します。

Routing Protocol > OSPF > Network Area

Action: Show Process

Process List Max: 65535 Total: 1

☐	Process ID
☐	1

Apply Revert

画面 1-329 :OSPF プロセス ID の表示

プロトコルの全般設定の設定

ダイナミック OSPF ルーティングを実装するには、最初に、ルータが接続する各 IP サブネットに VLAN グループを割り当てて（直前のセクションを参照）から、「Routing Protocol」→「OSPF」→「System」（Configure）を選択して表示される画面で、ルータ ID をルータに割り当てて、他の基本的なプロトコルパラメータを設定します。

関連する CLI 情報

「Open Shortest Path First (OSPFv2)」

パラメータ

以下のパラメータが表示されます。

- ・ Process ID - 「Routing Protocol」→「OSPF」→「Network Area」（Add）を選択して表示される画面で設定されるプロトコル ID（範囲：1 ～ 65,535）。

General Information

- ・ RFC1583 Compatible - ルーティングドメイン内の 1 つまたは複数のルータが初期の OSPFv2 を使用している場合は、すべてのルータで同じ RFC に基づいてサマリルートコストが計算されるようにするため、本製品では RFC 1583（初期の OSPFv2）互換モードを使用しなければなりません。このフィールドを有効にすると、RFC 1583 に基づいてサマリルートコストが計算されるようになります（デフォルト：Disabled）。

RFC 1583 互換モードが有効になっている場合、同じ宛先をアドバタイズする複数の AS 外部 LSA ルートから 1 つを選択するときにはコストのみが使用されます。無効になっている場合、優先順位はパスのタイプに基づいて決まり、コストは順位が同じ場合にのみ使用されます（RFC 2328 を参照）。

サマリ情報を交換するエリア内に OSPFv2（RFC 2328）にアップグレードされていない OSPF ルータ（特に、ABR）がある場合は、依然として古い OSPFv2 コードを実行しているルータとの互換性を確保するため、アップグレードされている OSPFv2 ルータで RFC 1583 を使用しなければなりません。

- ・ OSPF Router ID - 現行の OSPF プロセスに関して自律システム内で一意のルータ ID を本製品に割り当てます。

ルータ ID は、自律システム内のすべてのルータで一意でなければなりません。ただし、ルータ ID は 255.255.255.255 に設定することもできるという点に注意してください。本製品に既にネイバールータが登録されている場合は、本製品を Reboot するか、no router ospf コマンドに続けて router ospf コマンドを実行して手動で再始動すると、新しいルータ ID が使用されるようになります。

- ・ Auto Cost - 基準帯域幅をインターフェース帯域幅で割ってインターフェースのコストが計算されます。基準帯域幅は、Mbps/ 秒単位で定義されます（範囲：1 ～ 4,294,967）。デフォルトでは、ギガビットポートのコストは 0.1、10 ギガビットポートのコストは 0.01 です。アグリゲーションリンクについては、基準帯域幅の値を大きくして、コストの低いリンクとして優先的に使用されるようにすることができます。
- ・ SPF Hold Time - SPF 計算を 2 回連続して実行する場合の保留時間（範囲：0 ～ 65,535 秒、デフォルト：10 秒）。

この「SPF Hold Time」を 0 に設定すると、計算と計算の間で遅延が発生しないことを意味します。

- ・ SPF Delay Time – トポロジ変更通知を受信してから SPF 計算を開始するまでの遅延時間（範囲：0 ～ 65,535 秒、デフォルト：5 秒）。
遅延および保留時間の値を小さくすると、新しいパスに素早く切り替えられるようになりますが、CPU 処理時間は長くなります。
- ・ Default Metric – 他のプロトコルからインポートされる外部ルートへのデフォルトのメトリック（範囲：0 ～ 16,777,214、デフォルト：20）。
デフォルトメトリックは、互換性のないメトリックを使用している他のプロトコルから学習した外部ルートの再配信の問題を解決するために使用する必要があります。
「Redistribute」設定画面で設定されるメトリック値は、このデフォルトのメトリックによって上書きされません。メトリック値が「Redistribute」画面で設定されていない場合は、「System」設定画面で設定されるデフォルトメトリックによって、インポートされたすべての外部ルートに使用されるメトリック値が設定されます。

Default Information

- ・ Originate Default Route8 – 自律システムに対するデフォルトの外部ルートを生成します。ただし、「Advertise Default Route」フィールドに適切な値が指定されていないと注意してください（デフォルト：Disabled）。
この機能を使用してルート情報をルーティングドメイン（つまり、自律システム）に再配信すると、本製品が自動的に自律システム境界ルータ（ASBR: Autonomous System Boundary Router）になります。そのようにすることで、本製品が接続する他の自律システム内の境界ルータとルーティング情報を交換できるようになります。ルータが ASBR として機能している場合には、自律システム内の他のそれぞれのルータが、そのルータから外部ルートに関する情報を学習することができます。

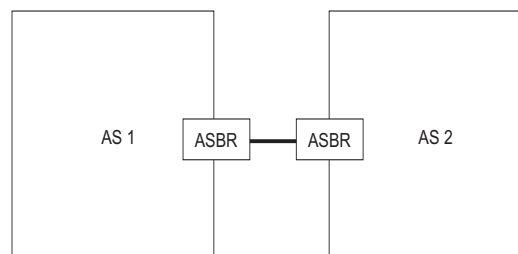


図 1-30:AS 境界ルータ

- ・ Advertise Default Route8 – ルータがデフォルトの外部ルートを自律システム（AS: Autonomous System）にアドバタイズすることができます（オプション：Not Always または Always、デフォルト：Not Always）。
 - ・ Always – ルータは、デフォルトの外部ルートが実際には存在しなくても、自らのローカル AS のデフォルトの外部ルートをアドバタイズします（デフォルトのルートを定義するには、「スタティックルートの設定」を参照）。
 - ・ NotAlways – RIP を使用して外部ルートをインポートするように設定されているか、スタティックルートが設定されており、そのようなルートが既知のものである場合には、デフォルトの外部ルートを AS のみにアドバタイズすることができます（「外部ルート情報の再配信」を参照）。

- ・ External Metric Type8 – デフォルトルートのアドバタイズに使用される外部リンクのタイプ。「Type 1」のルートアドバタイズメントでは、内部コストが外部ルートのメトリックに追加されます。「Type 2」のルートアドバタイズメントでは、内部コストはメトリックは追加されません。内部コストは、「Type 2」のルートと比較するときにルートコストが同じ「Type2」のルートが複数ある場合にのみ、ルートを決断するための要素として使用されます（デフォルト：Type 2）。
- ・ Default External Metric8 – デフォルトルートに割り当てられるメトリック（範囲：0 ～ 16,777,215、デフォルト：20）。

このデフォルトの外部ルートのメトリックを使用して、AS 内の他のルータから ASBR 経由で渡されるトラフィックのパスコストが計算されます。

他のプロトコルから学習したルーティング情報の再配信は、再配信機能によって制御します。

Web インターフェース

OSPF の全般設定を設定するには、以下のようにします。

- (1) 「Routing Protocol」→「OSPF」→「System」を選択します。
- (2) 「Step」リストで「Configure」を選択します。
- (3) 「Process ID」および「Router ID」を指定してから、必要に応じて、他のグローバル属性を指定します。例えば、「Auto Cost」を 10,000 に設定すると、インターフェースの使用コストは、ギガビットポートの場合は 10、ギガビットポートの場合は 1 に設定されます。
- (4) < Apply > ボタンをクリックします。

Routing Protocol > OSPF > System

Action: Configure

Process ID: 1

General Information

RFC 1583 Compatible: ☒ Enabled

OSPF Router ID: 192.168.1.2

Auto Cost (1-4294967): 10000 mbps

SPF Hold Time (0-65535): 10 sec

SPF Delay Time (0-65535): 5 sec

Default Metric (0-16777215): 20

Default Information

Originate Default Route: ☒ Enabled

Advertise Default Route: Always

External Metric Type: 2

Default External Metric (0-16777215): 20

Apply Revert

画面 1-330 :OSPF の全般設定の設定

管理設定と統計情報の表示

「Routing Protocol」→「OSPF」→「System」（Show）を選択すると、OSPF に関する全般的な管理設定と統計情報を表示することができます。

関連する CLI 情報

「show ip ospf」

「show ip protocols ospf」

パラメータ

以下のパラメータが表示されます。

Router ID Type	ルータ ID が手動設定されたものか、システムで自動生成されたものかを示します。
Rx LSAs	受信されたリンクステートアドバタイズメント（LSA）の数。
Originate LSAs	発信された新規の LSA の数。
AS LSA Count	リンクステートデータベース内の自律システム LSA の数。
External LSA Count	リンクステートデータベース内の外部 LSA の数。
External LSA Checksum	外部リンクステートアドバタイズメントデータベースのチェックサム。
Admin Status	アクティブなインターフェース（つまり、有効になっており、Up 状態になっているレイヤ 3 インターフェース）をもつ構成済み OSPF エリアが 1 つまたは複数あるかどうかを示します。
ABR Status (Area Border Router)	ルータが 2 つ以上のエリア内のネットワークに直接接続しているかどうかを示します。エリア境界ルータは、個別のコピーの SPF アルゴリズムを実行して、エリアごとに別々のルーティングデータベースを保持します。
ASBR Status (Autonomous System Boundary Router)	ルータが接続する他の自律システム内の境界ルータとルーティング情報を交換できるかどうかを示します。ルータが ASBR として有効になっている場合には、自律システム内の他のそれぞれのルータが、このルータから外部ルートに関する情報を学習することができます。
Restart Status	OSPF プロセスがグレースフルリスタート状態であるかどうかを示します。
Area Number	ルータに接続している構成済みエリアの数。
Version Number	OSPF バージョン番号。本製品に実装されている OSPF プロトコルは RFC 2328（バージョン 2）に基づいています。また、RFC 1583（初期の OSPFv2）互換モードもサポートされています。

表 1-21:OSPF システム情報

Web インターフェース

OSPF の全般設定を表示するには、以下のようになります。

- (1) 「Routing Protocol」→「OSPF」→「System」を選択します。
- (2) 「Step」リストで「Show」を選択します。

(3) 「Process ID」を指定します。

Routing Protocol > OSPF > System

Action:

Process ID

OSPF System Information

Router ID Type	Auto	Admin Status	Enabled
Rx LSAs	5	ABR Status	Disabled
Originate LSAs	5	ASBR Status	Disabled
AS LSA Count	0	Restart Status	Disabled
External LSA Count	1	Area Number	2
External LSA Checksum	CD97	Version Number	2

画面 1-331 :OSPF の全般設定の表示

NSSA またはスタブの追加

「Routing Protocol」→「OSPF」→「Area」（Configure Area - Add Area）を選択すると、Not-So-Stubby エリア（NSSA）または Stubby エリア（スタブ）を追加することができます。

関連する CLI 情報

「router ospf」

「area stub」

「area nssa」

コマンドの使用

本製品は、最大 5 つのスタブまたは NSSA をサポートします。

パラメータ

以下のパラメータが表示されます。

- ・ Process ID - 「Routing Protocol」→「OSPF」→「Network Area」（Add）を選択して表示される画面で設定されるプロトコル ID（範囲：1 ～ 65,535）。
- ・ Area ID - NSSA またはスタブの ID。エリア ID の形式は、IPv4 アドレス形式にすることも、4 octets の符号なし整数（範囲は 0 ～ 4,294,967,295）にすることもできます。
- ・ エリアに 1 つまたは複数のインターフェースを追加するには、ネットワークマスクを使用してネットワークセグメント上のすべてのルータのエリア ID を同じ値に設定します。
- ・ Area Type - 「NSSA」または「Stub」を選択します。

Web インターフェース

NSSA またはスタブを OSPF 管理ドメインに追加するには、以下のようにします。

- (1) 「Routing Protocol」→「OSPF」→「Area」を選択します。
- (2) 「Step」リストで「Configure Area」を選択します。
- (3) 「Step」リストで「Add Area」を選択します。
- (4) 「Process ID」を指定し、「Area ID」を入力して、「Area Type」として「NSSA」または「Stub」を選択します。
- (5) < Apply > ボタンをクリックします。

Routing Protocol > OSPF > Area

Step: 1. Configure Area Action: Add Area

Process ID: 1

Area ID: 3

Area Type: NSSA

Apply Revert

画面 1-332 :NSSA またはスタブの追加

指定した OSPF ドメインに追加された NSSA またはスタブを表示するには、以下のようにします。

1. 「Routing Protocol」→「OSPF」→「Area」を選択します。
2. 「Step」リストで「Configure Area」を選択します。
3. 「Step」リストで「Show Area」を選択します。
4. 「Process ID」を指定します。

Routing Protocol > OSPF > Area

Step: 1. Configure Area Action: Show Area

Process ID: 1

Area List Max: 5 Total: 2

	Area ID	Area Type
☐	3	NSSA
☐	4	Stub

Apply Revert

画面 1-333 :NSSA またはスタブの表示

NSSA 設定の設定

「Routing Protocol」→「OSPF」→「Area」（Configure Area - Configure NSSA Area）を選択すると、NSSA のプロトコル設定を設定することができます。

NSSA は、エリア境界ルータ（ABR: Area Border Routers）および自律システム境界ルータ（ASBR: Autonomous System Boundary Routers）のデフォルトルートと、他のルーティングドメインから学習されて ABR 経由でインポートされた外部ルートのどちらを使用するか制御するように設定することができます。

NSSA はスタブよりも小規模です。NSSA は、ほとんどの外部ルーティング情報をブロックし、ルータが ABR である場合に AS において NSSA と他のエリアとの間で渡されるトラフィックの単一のデフォルトルートをアドバタイズするように設定することができます。

また、NSSA では、AS に含まれていない 1 つまたは複数のルーティングドメインから外部ルート情報（RIP ドメインや、ローカルに設定されたスタティックルートなど）をインポートすることもできます。そのような外部 AS ルート情報は、NSSA の ASBR によって生成され、NSSA 内でのみアドバタイズされます。デフォルトでは、それらのルートは、ABR によってバックボーンまたは他のエリアにフロードされません。ただし、NSSA の ABR は、NSSA 外部 LSA（Type 7）を、AS 内の他のエリアに伝搬される外部 LSA（Type 5）に変換します。

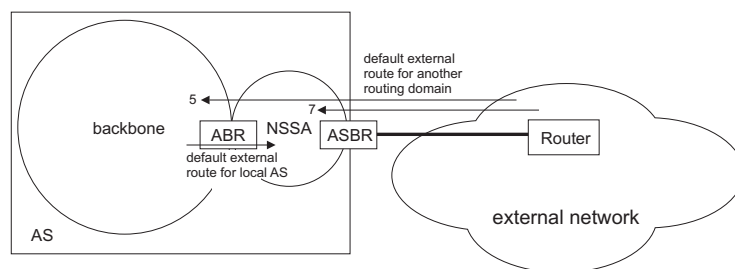


図 1-31:OSPF NSSA

** 図の注釈

- ローカル外部ネットワークのデフォルトの外部ルート
- バックボーンルータ
- 他のルーティングドメインのデフォルトの外部ルート

関連する CLI 情報

「router ospf」

「area default-cost」

「area nssa」

コマンドの使用

- ・ NSSA を作成するには、最初に、その NSSA のアドレス範囲を指定します（「アドレスに基づくネットワークエリアの定義」を参照）。それから、「NSSA またはスタブの追加」の説明に従って NSSA を作成します。
- ・ NSSA は、通過エリアとして使用することはできません。したがって、ルーティングドメインのエッジに配置しないでください。

- ・ NSSA には複数の ABR またはエグジットポイントを含めることができます。ただし、外部宛先ごとにエグジットポイントを判別しなくても済むようにするため、すべてのエグジットポイントとローカルルータには同じ外部ルーティングデータが含まれていなければなりません。
- ・ OSPF スタブには外部ルートがないため、他のプロトコルから学習したルート情報をスタブに再配信することはできません。一方、NSSA では、他のプロトコルから学習した外部ルート情報を自らのエリアに再配信して、隣接エリアにリークすることができます。
- ・ NSSA 外部 LSA によってアドバタイズできるルートとしては、OSPF を使用して学習される AS 外部のネットワーク宛先、デフォルトルート、スタティックルート、RIP などの他のルーティングプロトコルから導き出されるルート、または OSPF を実行していないネットワークに直接接続するルートなどがあります。
- ・ NSSA は、OSPF を使用するセントラルサイトを別のルーティングプロトコルを使用するリモートサイトに接続する場合に管理を容易するために利用することができます。OSPF は、セントラルルータとリモートルータとの間のエリアを NSSA として定義することによってリモート接続をカバーするように、簡単に拡張することができます。

パラメータ

以下のパラメータが表示されます。

- ・ Process ID - 「Network Area」設定画面をで指定されたのと同じプロセス ID。
- ・ Area ID - NSSA の ID。
- ・ Translator Role - Type 7 外部 LSA を Type 5 外部 LSA に変換するための NSSA-ABR トランスレータロールを示します。トランスレータロールには、以下のものがあります。
 - ・ Never - NSSA LSA を Type 5 外部 LSA に変換しません。
 - ・ Always - 常に NSSA LSA を Type 5 外部 LSA に変換します。
 - ・ Candidate - トランスレータとして選択されている場合には NSSA LSA を Type 5 外部 LSA に変換します。
- ・ Redistribute - ルータが NSSA エリア境界ルータ (ABR: Area Border Router) であり、ルートを標準エリアのみにインポートする (「外部ルート情報の再配信」を参照) 必要があり、NSSA にはインポートする必要がない場合は、このオプションを無効にしてください。つまり、NSSA ABR が (他のエリア内のルータから学習した) 外部ルーティング情報を NSSA にアドバタイズするのを防ぐため、再配信を無効にする必要があるということです (デフォルト: Enabled)。
- ・ Originate Default Information - ルータが NSSA ABR または NSSA ASBR である場合、このオプションを有効にすると、NSSA に対する Type 7 のデフォルト LSA が生成されます。このデフォルトの LSA は、NSSA ABR の場合は AS 内の他のエリアへのルート情報を、NSSA ASBR の場合は AS 外部のエリアへのルート情報を提供します (デフォルト: Disabled)。

ルータが ABR である場合、この「Originate Default Information」オプションを使用したときには、AS 内の他のエリアへのデフォルトルートを NSSA に送信できるようになるので、NSSA とスタブではほぼ違いはありません。ただし、ルータが ASBR である場合は、このオプションを使用すると、(NSSA に隣接しているが OSPF AS 内にはないルーティングプロトコルドメインの) デフォルトの外部 AS ルートを NSSA にインポートできるようになるので、NSSA とスタブとでは違いがあります。
- ・ Metric Type - 「Type 1」または「Type 2」の外部ルート。「Type 2」を選択すると、ルータで内部コストが外部ルートのメトリックに追加されなくなります (デフォルト: Type 2)。

Web 設定

ユニキャストルーティング

- ・ Metric – Type 7 のデフォルト LSA に割り当てられるメトリック（範囲：0 ～ 16,777,214、デフォルト：1）。
- ・ Default Cost – ABR から NSSA に送信されるデフォルトのサマリルートのコスト（範囲：0 ～ 16,777,215、デフォルト：0）。
- ・ このデフォルトのコストを「0」に設定するとルータは接続している NSSA にデフォルトルートをアドバタイズしなくなるので注意してください。
- ・ Summary – サマリルートの使用を制御します（デフォルト：Summary）。
 - ・ Summary – スタブとは異なり、常に内部ルートが Type 7 NSSA 外部ルートよりも優先的に選択されるようにするため、すべての Type 3 サマリ LSA が NSSA にインポートされます。
 - ・ No Summary – エリアで標準の NSSA 機能が保持されるようにする一方で、エリア間ルート（Type 3 および Type 4 のサマリルート）がエリアに注入されないようにします。その代わりに、デフォルトルートを Type 3 LSA としてアドバタイズします。

Web インターフェース

NSSA のプロトコル設定を設定するには、以下のようになります。

- (1) 「Routing Protocol」→「OSPF」→「Area」を選択します。
- (2) 「Step」リストで「Configure Area」を選択します。
- (3) 「Step」リストで「Configure NSSA Area」を選択します。
- (4) 「Process ID」を指定し、NSSA のルーティング動作を変更します。
- (5) < Apply > ボタンをクリックします。

Routing Protocol > OSPF > Area

Step: 1. Configure Area Action: Configure NSSA Area

Process ID: 1

NSSA Area List Max: 5 Total: 1

Area ID	Translator Role	Redistribute	Originate Default Information	Metric Type	Metric (0-16777215)	Default Cost (0-16777215)	Summary
192.168.2.0	Candidate	Enabled	Enabled	2	34	0	Summary

Apply Revert

画面 1-334 :NSSA のプロトコル設定の設定

スタブ設定の設定

「Routing Protocol」→「OSPF」→「Area」（Configure Area - Configure Stub Area）を選択すると、スタブのプロトコル設定を設定することができます。

スタブは外部ルーティング情報を受け取りません。その代わりに、スタブに隣接する ABR を、ローカルエリア外部または自律システム外部のすべての宛先に対するデフォルト外部ルートに関する情報をスタブに送信するように設定することができます。また、そのデフォルトの外部ルートは、スタブに入ってくるトラフィックの単一のエントリポイントとしてアドバタイズされます。スタブを使用すると、ネットワーク上で交換しなければならないトポロジデータの量を大幅に減らすことができます。

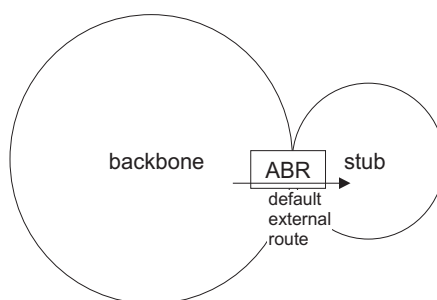


図 1-32: OSPF スタブ

バックボーンデフォルトの外部ルートスタブ

デフォルトでは、スタブは、デフォルトの外部ルートを使用して、自律システム内の他のエリアのみにトラフィックを渡すことができます。ただし、自律システム内のどこか他の場所にあるサブネットワークに関する Type 3 サマリリンクアドバタイズメントをスタブに送信するように ABR を設定することもできます。

関連する CLI 情報

「router ospf」

「area default-cost」

「area stub」

コマンドの使用

- ・ スタブを作成するには、最初に、そのスタブのアドレス範囲を指定します（「アドレスに基づくネットワークエリアの定義」を参照）。それから、「NSSA またはスタブの追加」の説明に従ってスタブを作成します。
- ・ スタブは、通過エリアとして使用することはできません。したがって、ルーティングドメインのエッジに配置しないでください。
- ・ スタブには複数の ABR またはエグジットポイントを含めることができます。ただし、外部宛先ごとにエグジットポイントを判別しなくても済むようにするため、すべてのエグジットポイントとローカルルータには同じ外部ルーティングデータが含まれていなければなりません。

パラメータ

以下のパラメータが表示されます。

- ・ Process ID - 「Network Area」 設定画面で指定されたのと同じプロセス ID。
- ・ Area ID - スタブの ID。
- ・ Default Cost - ABR からスタブに送信されるデフォルトのサマリルートのコスト（範囲：0 ～ 16,777,215、デフォルト：0）。
- ・ このデフォルトのコストを「0」に設定するとルータは接続しているスタブにデフォルトルートをアドバタイズしなくなるので注意してください。
- ・ Summary - サマリルートの使用を制御します。
 - ・ Summary - ABR がサマリリンクアドバタイズメントをスタブに送信できるようにします。
 - ・ No Summary - ABR がサマリリンクアドバタイズメントをスタブに送信しないようにします。

Type 4 の AS サマリ LSA と Type 5 の 外部 LSA をブロックすることにより、ルーティングテーブルスペースを節約できます。また、このオプションを使用して、ローカルエリア外部または自律システム外部の宛先のデフォルトルートをアドバタイズする Type 3 の サマリ LSA が ABR から送信されないようにすることにより、スタブを完全に分離することもできます。

エリアは、そのエリア内のルータが他のエリアからのサマリ LSA を必要としない場合にのみ、完全に Stubby なエリア（スタブ）として定義してください。

Web インターフェース

スタブのプロトコル設定を設定するには、以下のようになります。

- (1) 「Routing Protocol」 → 「OSPF」 → 「Area」 を選択します。
- (2) 「Step」 リストで 「Configure Area」 を選択します。
- (3) 「Step」 リストで 「Configure Stub Area」 を選択します。
- (4) 「Process ID」 を指定し、スタブのルーティング動作を変更します。
- (5) < Apply > ボタンをクリックします。

Routing Protocol > OSPF > Area

Step: 1. Configure Area Action: Configure Stub Area

Process ID: 1

Stub Area List Max: 5 Total: 1

Area ID	Default Cost (0-16777215)	Summary
192.168.3.0	1	Summary

Apply Revert

画面 1-335 : スタブのプロトコル設定の設定

NSSA とスタブに関する情報の表示

「Routing Protocol」→「OSPF」→「Area」(Show Information) を選択すると、NSSA とスタブに関するプロトコル情報を表示することができます。

関連する CLI 情報

「show ip ospf」

パラメータ

以下のパラメータが表示されます。

- ・ Process ID - 「Network Area」設定画面で指定されたのと同じプロセス ID。
- ・ Area ID - NSSA またはスタブの ID。
- ・ SPF Runs - エリアに対して SPF アルゴリズムが実行された回数。
- ・ ABR Count - エリアに接続しているエリア境界ルータ (ABR) の数。
- ・ ASBR Count - エリアに接続している自律システム境界ルータ (ASBR) の数。
- ・ LSA Count - 発信された新規のリンクステートアドバタイズメント (LSA) の数。
- ・ LSA Checksum Sum - エリアのリンクステートデータベースに含まれている LSA の LS チェックサムの合計。

Web インターフェース

NSSA とスタブに関する情報を表示するには、以下のようにします。

- (1) 「Routing Protocol」→「OSPF」→「Area」を選択します。
- (2) 「Step」リストで「Show Information」を選択します。
- (3) 「Process ID」を指定します。

Routing Protocol > OSPF > Area					
Step: 2. Show Information					
Process ID 1					
Area Information List Max: 256 Total: 4					
Area ID	SPF Runs	ABR Count	ASBR Count	LSA Count	LSA Checksum Sum
0.0.0.1	0	0	0	0	0
0.0.0.2	0	0	0	0	0
0.0.0.3	10	10	10	10	10
0.0.0.4	0	0	0	0	0

画面 1-336 :NSSA とスタブに関する情報の表示

エリア範囲（ABR のルートサマリ）の設定

OSPF エリアには多数のノードを含めることができます。それらのノードのそれぞれのルート情報を ABR でアドバタイズしなければならないとなると、多くの帯域幅とプロセッサ時間が無駄に消費されることになります。そのようにする代わりに、「Routing Protocol」→「OSPF」→「Area Range」（Add）を選択して表示される画面で、エリア内の個々のネットワークすべてをカバーする単一のサマリルートアドバタイズするように ABR を設定することができます。ルートサマリを使用すると、ローカルでの変更を他のエリアルータに伝搬しなくても済むようになります。そのため、比較的大規模なネットワークで簡単に OSPF を規模に合わせて調整することができ、より安定したネットワークトポロジが実現されます。

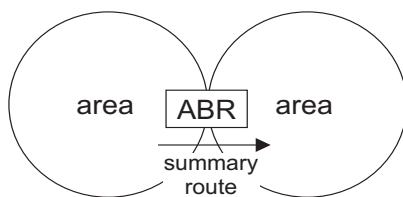


図 1-33: ABR のルートサマリ

関連する CLI 情報

「router ospf」

「area range」

コマンドの使用

- ・ 「Area Range」設定画面を使用すると、エリア内のルートをまとめ、その情報を ABR 経由で他のエリアにアドバタイズすることができます。エリアのサマリルートは IP アドレスとネットワークマスクによって定義されます。そのため、エリア内のすべてのルートが簡単に指定できる範囲に収まるように、各エリアが連続する一連のアドレスをもつように設定する必要があります。連続する一連のアドレスを使用できない場合は、複数のエリア範囲についてルートをまとめることができます。また、本製品は、可変長サブネットマスク（VLSM: Variable Length Subnet Mask）もサポートしているので、ネットワークアドレスの任意のビット境界でアドレス範囲をまとめることができます。
- ・ 自律システム（ローカルルーティングドメイン）にインポートされた外部 LSA をまとめるには、「Summary Address」設定画面を使用します。
- ・ 本製品は、エリア範囲に対して最大 5 つのサマリルートをサポートします。

パラメータ

以下のパラメータが表示されます。

- ・ Process ID - 「Network Area」設定画面で指定されたのと同じプロセス ID。
- ・ Area ID - ルートをサマリルートにまとめるエリアを指定します。エリア ID の形式は、IPv4 アドレス形式にすることも、4 octets の符号なし整数（範囲は 0 ～ 4,294,967,295）にすることもできます。
- ・ Range Network - サマリルートにまとめるルートのベースアドレス。
- ・ Range Netmask - サマリルートのネットワークマスク。

- ・ Advertising - サマリルートアドバタイズするかどうかを示します。ルートがアドバタイズされるように設定すると、ルータは、指定されたアドレス範囲ごとに Type 3 のサマリを発行します。サマリルートがアドバタイズされない場合には、指定されたサマリルートはネットワークの残りの部分からは見えない状態で維持されます（デフォルト：Advertise）。

Web インターフェース

エリア範囲のルートサマリを設定するには、以下のようにします。

- (1) 「Routing Protocol」 → 「OSPF」 → 「Area Range」 を選択します。
- (2) 「Step」 リストで 「Add」 を選択します。
- (3) プロセス ID、エリア ID、およびベースアドレスとネットワークマスクを指定して、サマリルートを実他のエリアにアドバタイズするかどうかを選択します。
- (4) < Apply > ボタンをクリックします。

Routing Protocol > OSPF > Area Range

Action: Add

Process ID 1

Area ID 192.168.0.0

Range Network 192.168.0.0

Range Netmask 255.255.0.0

Advertising Advertise

Apply Revert

画面 1-337 : エリア範囲のルートサマリの設定

設定されているルートサマリを表示するには、以下のようにします。

1. 「Routing Protocol」 → 「OSPF」 → 「Area Range」 を選択します。
2. 「Step」 リストで 「Show」 を選択します。

Web 設定

ユニキャストルーティング

3. 「Process ID」を指定します。

Routing Protocol > OSPF > Area Range

Action:

Process ID:

Area Range List Max: 5 Total: 1

☐	Area ID	Range Network	Range Netmask	Advertising
☐	192.168.0.0	192.168.0.0	255.255.0.0	Advertise

画面 1-338 : 設定されているルートサマリの表示

外部ルート情報の再配信

「Routing Protocol」→「OSPF」→「Redistribute」(Add) を選択すると、他のルーティングプロトコルから学習した外部ルーティング情報、スタティックルート、または直接接続ルートを自律システムにインポートすることや、AS 外部 LSA を生成することができます。

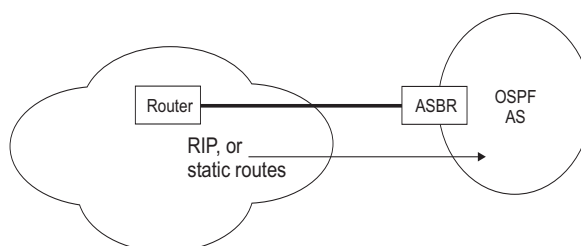


図 1-34: 外部ルート情報の再配信

関連する CLI 情報

「router ospf」

「redistribute」

コマンドの使用

- ・ 本製品は、現在接続しているルート、RIP を使用して学習されたエントリ、およびスタティックルートのすべてについて再配信をサポートしています。
- ・ 外部ルート情報を OSPF AS に再配信すると、ルータは自動的に ASBR となります。
- ・ ただし、「General Configuration」画面を使用してルータが ASBR として設定されていても再配信が有効になっていない場合、ルータは、「常に (Always)」デフォルトの外部ルートをアドバタイズするように設定されていると、外部ルートが実際には存在しなくても、AS への「デフォルト」の外部ルートのみを生成します。

パラメータ

以下のパラメータが表示されます。

- ・ Process ID - 「Network Area」設定画面で指定されたのと同じプロセス ID。
- ・ Protocol Type - ルーティング情報をローカルルーティングドメインに再配信する外部ルーティングプロトコルのタイプを指定します（オプション：RIP または Static、デフォルト：RIP）。
- ・ Metric Type - 外部ルートコストの計算に使用される方法を示します（オプション：Type 1 または Type 2、デフォルト：Type 1）。

この「Metric Type」によって、外部 LSA を使用してルートを AS システムの外部の宛先にアドバタイズする方法を指定します。「Type 1」を指定すると、内部コストが外部ルートのメトリックに追加されます。つまり、AS 内のあらゆるルータからのルートのコストが、アドバタイズ元の ASBR に関連付けられているコストに外部ルートのコストを足したものと等しくなるということです。「Type 2」を指定すると、外部ルートのメトリックのみがアドバタイズされます。

- ・ Metric - 指定されたプロトコルのすべての外部ルートに割り当てられるメトリック（範囲：1 ～ 65,535、デフォルト：10）。

再配信されるルートに関して指定されるメトリック値は、「Routing Protocol」→「OSPF」→「System」を選択すると表示される画面で指定される「Default External Metric」に優先します。

- ・ Tag - 特定の外部ルーティングドメインを示すため、または、追加情報をルータ間で渡すため、AS 外部 LSA に挿入されるタグ（範囲：0 ～ 4,294,967,295）。

タグは、別の外部 AS（他のルーティングプロトコル）から学習した個々のルートを区別するために使用することができます。例えば、ルーティングドメインに 2 つの ASBR、A と B があるとします。ASBR A は RIP ドメイン 1（Tag 1 によって識別）から学習したルートを再配信するように設定し、ASBR B は RIP ドメイン 2（Tag 2 によって識別）から学習したルートを再配信するように設定することができます。

Web インターフェース

外部ルーティング情報をインポートするようにルータを設定するには、以下のようになります。

- (1) 「Routing Protocol」→「OSPF」→「Redistribute」を選択します。
- (2) 「Step」リストで「Add」を選択します。
- (3) プロセス ID、インポートするプロトコルタイプ、メトリックタイプ、パスコスト、およびオプションのタグを指定します。

Web 設定

ユニキャストルーティング

(4) < Apply > ボタンをクリックします。

Routing Protocol > OSPF > Redistribute

Action: Add

Process ID: 1

Protocol Type: RIP

Metric Type: 1

Metric (0-16777214): 3

Tag (0-4294967295): 1

Apply Revert

画面 1-339 : 外部ルートのインポート

インポートされた外部ルートのタイプを表示するには、以下のようにします。

1. 「Routing Protocol」→「OSPF」→「Redistribute」を選択します。
2. 「Step」リストで「Show」を選択します。
3. 「Process ID」を指定します。

Routing Protocol > OSPF > Redistribute

Action: Show

Process ID: 1

Redistribute List Max: 2 Total: 1

	Protocol Type	Metric Type	Metric	Tag
☐	RIP	1	3	1

Apply Revert

画面 1-340 : インポートされた外部ルートのタイプの表示

(外部 AS ルートの) サマリアドレスの設定

他のプロトコルのルート情報を OSPF エリアに再配信する場合、通常は、直前のセクションで説明したように、ルータが外部 LSA によって各ルートを個別にアドバタイズする必要があります。それらの外部ルート情報の再配信に必要なプロトコルメッセージの数を減らすため、代わりに、他のプロトコルから学習したルートを接続先のすべての AS に再配信するように ASBR を設定することができます。

他の AS に送信される外部 LSA の量を減らすには、「Routing Protocol」→「OSPF」→「Summary Address」(Add) を選択すると表示される画面を使用して、広範にわたる外部アドレスを統合するアグリゲーションルートをアドバタイズするようにルータを設定します。そのようにすると、アドバタイズされる外部 LSA の数と OSPF リンクステートデータベースのサイズの両方を減らすのに役立ちます。

関連する CLI 情報

「router ospf」

「summary-address」

コマンドの使用

統合するアドレス範囲が明確にわからない場合は、まず、「Redistribute」設定画面を使用して外部ルート情報の再配信を有効にし、ルーティングテーブルにインポートされたルートを確認してから、ルーティングテーブルのサイズを減らすため、また、それらの外部ルートを統合してからローカルドメインにアドバタイズするため、1 つまたは複数のサマリアドレスを設定します。

OSPF エリア間でルーティング情報が送信されるルートをサマリルートにまとめるには、「Area Range Configuration」画面を使用します。

本製品は、最大 20 の Type 5 のサマリルートをサポートします。

パラメータ

以下のパラメータが表示されます。

- ・ Process ID - 「Network Area」設定画面で指定されたのと同じプロセス ID。
- ・ IP Address - ある範囲のアドレスをカバーするサマリアドレス。
- ・ Netmask - サマリルートのネットワークマスク。

Web インターフェース

外部ルーティング情報のサマリを作成するようにルータを設定するには、以下のようにします。

- (1) 「Routing Protocol」→「OSPF」→「Summary Address」を選択します。
- (2) 「Step」リストで「Add」を選択します。
- (3) プロセス ID、およびベースアドレスとネットワークマスクを指定します。

(4) < Apply > ボタンをクリックします。

Routing Protocol > OSPF > Summary Address

Action: Add ▼

Process ID: 1 ▼

IP Address:

Netmask:

Apply Revert

画面 1-341 : 外部ルートのサマリルートの作成

外部ルートのサマリアドレスを表示するには、以下のようにします。

1. 「Routing Protocol」 → 「OSPF」 → 「Summary Address」 を選択します。
2. 「Step」 リストで 「Show」 を選択します。
3. 「Process ID」 を指定します。

Routing Protocol > OSPF > Summary Address

Action: Show ▼

Process ID: 1 ▼

Summary Address List Max: 20 Total: 1

	IP Address	Netmask
☐	192.168.0.0	255.255.0.0

Apply Revert

画面 1-342 : 外部ルートのサマリアドレスの表示

OSPF インターフェースの設定

ルータまたはネットワーク内のどこかにある他のネットワークセグメントと通信する必要があります。あるローカルサブネットのルーティングインターフェースを指定しなければなりません。最初に、ルータに直接接続する各サブネットの VLAN を設定し、IP インターフェースを各 VLAN に割り当てて（1 つのプライマリインターフェースと 1 つまたは複数のセカンダリインターフェース）から、「Network Area」設定画面を使用して、インターフェースアドレス範囲を OSPF エリアに割り当てます。

ルータインターフェースを OSPF エリアに割り当てた後、「Routing Protocol」→「OSPF」→「Interface」（Configure by VLAN）または（Configure by Address）を選択して表示される画面で、優先パスの選択で使用するコストの設定、代表ルータの選択、LSA のタイミングの制御、およびルーティングメッセージの認証方法の指定のために OSPF で使用されるインターフェースごとのパラメータを設定します。

関連する CLI 情報

「Open Shortest Path First (OSPFv2)」

コマンドの使用

- ・「Configure by VLAN」画面を使用して、「Network Area」（Add）画面で VLAN に割り当てられたすべてのエリアの OSPF インターフェース設定を指定します。
- ・「Configure by Address」画面を使用して、「Network Area」（Add）画面で VLAN に割り当てられた特定のエリアの OSPF インターフェース設定を指定します。

パラメータ

以下のパラメータが表示されます。

- ・ VLAN ID - IP インターフェースが割り当てられている VLAN。
- ・ IP Address - 「Network Area」（Add）画面で VLAN に割り当てられたインターフェースのアドレス。

このパラメータは「Configure by Address」画面のみに適用されます。

- ・ Cost - インターフェースのプロトコルパケット送信コストを設定します。値が大きいほど、ポート速度が遅くなります（範囲：1 ～ 65,535、デフォルト：1）。

このインターフェースコストは、特定のインターフェース経由でパケットを送信するために必要なオーバーヘッドを示します。この値は、ルータの LSA でリンクコストとしてアドバタイズされます。

ルートには、ルート内の各インターフェースのすべてのメトリックの合計と同等のメトリックが割り当てられます。

本製品では、すべてのポートについて、デフォルトコストである 1 が使用されます。そのため、10 ギガビットモジュールをインストールする場合は、実際のインターフェース帯域幅が反映されるようにするため、すべての 1 Gbps ポートのコストを 1 よりも大きい値にリセットする必要があります。

- ・ Router Priority - ルータのインターフェース優先度を設定します（範囲：0 ～ 255、デフォルト：1）。

この優先度によって、各 OSPF エリアの代表ルータ（DR: Designated Router）およびバックアップ代表ルータ（BDR: Backup Designated Router）が決まります。DR は、ルーティングトポロジ情報を交換するため、エリア内の他のすべてのルータとアク

ティブな隣接関係を形成します。何らかの理由により DR で障害が発生すると、BDR が DR の役割を引き継ぎます。

ルータが DR または BDR として選択されないようにするには、優先度を 0 (ゼロ) に設定します。0 以外の値に設定した場合は、優先度が最も高いルータが DR になり、次に優先度が高いルータが BDR になります。優先度が最も高いルータが 2 つ以上ある場合は、ID の値が最も大きいルータが DR として選択されます。

インターフェースが Up 状態になったときに既にエリアの DR が存在している場合には、新しいルータは、自らの優先度に関係なく、その時点における DR を受け入れます。DR は、次回に選択プロセスが開始されるまで変更されません。

ルータ優先度は、マルチアクセスネットワークでのみ設定し、ポイントツーポイントネットワークでは設定しないでください。

- ・ Hello Interval – インターフェースにおける hello パケットの送信間隔を設定します。この間隔は、ネットワーク上のすべてのルータで同じ値に設定する必要があります (範囲: 1 ~ 65,535 秒、デフォルト: 10 秒)。

hello パケットは、送信元ルータがアクティブな状態に維持されていることを他のルータに通知するために使用されます。「Hello Interval」を小さい値に設定すると、トポロジ変更の検出時の遅延時間を短縮することができますが、ルーティングトラフィックが増加します。

- ・ Dead Interval – ここで設定されている期間内に hello パケットが検出されない場合、ルータはダウンしているものとしてネイバールータによって宣言されます。この期間は、ネットワーク上のすべてのルータで同じ値に設定する必要があります (範囲: 1 ~ 65,535 秒、デフォルト: 40 秒または「Hello Interval」の 4 倍)。

「Dead Interval」はルータの hello パケットでアドバタイズされます。「Dead Interval」の値は、「Hello Interval」の倍数であり、なおかつ、該当のネットワーク上のすべてのルータで同じでなければなりません。

- ・ Transmit Delay – インターフェースでのリンク状態更新パケットの送信にかかる推定時間を設定します (範囲: 1 ~ 65,535 秒、デフォルト: 1 秒)。

LSA の送信までの期間が、この遅延値の分だけ、延長されます。この遅延値を見積もる場合は、インターフェースの送信遅延と伝搬遅延の両方を考慮に入れる必要があります。送信遅延はリンク速度に応じて設定してください。リンク速度が遅いほど、大きい値を使用します。

この遅延値を追加しない場合、LSA をリンクで送信するのに必要な時間は、ルーティングプロセスで考慮されなくなります。低速リンクでは、デバイスが受信できるよりも速い速度でルータからパケットが送信される可能性があります。そのような問題が発生しないようにするため、「Transmit Delay」を使用して、ルータが送信から次の送信までの間、指定された時間の分だけ待機するようにすることができます。

- ・ Retransmit Interval – LSA の再送信間隔を設定します (範囲: 1 ~ 65,535 秒、デフォルト: 5 秒)。

ルータは、この「Retransmit Interval」を過ぎても肯定応答を受信できない場合は、LSA をネイバールータに再送信します。ルーティング情報のフローのために十分な時間を確保する一方で不要なプロトコルトラフィックが発生しないようにするため、「Retransmit Interval」は控えめな値に設定しなければなりません。この値は仮想リンクの場合は大きめの値にする必要があるということに注意してください。

再送信が不必要に発生しないようにするため、この間隔は、接続先のネットワーク上のいずれか 2 つのルータ間のラウンドトリップ遅延よりも大きい値に設定してください。

- ・ Authentication Type – インターフェースで使用する認証タイプを指定します（オプション：None、Simple または MD5、デフォルト：None）。

ルータが意図せずに非承認エリアに参入するのを防ぐため、認証を使用してください。同じエリア内のルータは同じパスワード（またはキー）を指定して設定してください。同じネットワーク上にあり、同じパスワードを使用するすべてのネイバルルータで、ルーティングデータが交換されます。

簡易パスワード認証を使用すると、パスワードがパケットに含まれます。そのパスワードが受信ルータで設定されているパスワードと一致しなければ、パケットは破棄されます。この方法では、ルーティングプロトコルパケットのスヌーピングによって認証キーを学習することが可能であるため、セキュリティはほとんど確保されません。

MD5（Message-Digest 5）認証を使用する場合、ルータは、MD5 アルゴリズムに基づいて、認証キーから 128 bits のメッセージダイジェストを作成することにより、データの整合性を検証します。適切なキーとキー ID がなければ、事前に指定されているターゲットメッセージダイジェストに一致するメッセージを作成することは、ほぼ不可能です。

「Message Digest Key ID」と「Authentication Key」は、自律ネットワーク全体で同じものを使用する必要があります。

- ・ Authentication Key – ルーティングプロトコルメッセージの信頼性を検証するためにネイバルルータが使用するプレーンテキストパスワードを割り当てます（範囲：1～8 文字（簡易パスワードの場合）または 1～16 文字（MD5 認証の場合）、デフォルト：キーなし）。

プレーンテキスト認証または直前の項目で説明されている MD5 認証が有効になっている場合には、ルーティングプロトコルパケットが本製品から発信されるときに、このパスワード（キー）が OSPF ヘッダに挿入されます。

それぞれのネットワークインターフェースに異なるパスワードを割り当てることができますが、パスワードはネットワーク（自律システム）のすべてのネイバルルータで同じものを使用する必要があります。同じネットワーク上にあり、同じパスワードを使用するすべてのネイバルルータで、ルーティングデータが交換されます。

- ・ Message Digest Key ID – ネイバルルータに送信されるルーティングプロトコルメッセージの信頼性を検証するために認証キーと併せて使用されるキー ID を割り当てます（範囲：1～255、デフォルト：なし）。

通常は、インターフェースごとにキーを 1 つだけ使用して、アウトバウンドパケットの認証情報を生成し、着信パケットを認証します。ネイバルルータは、同じキー ID とキー値を使用する必要があります。

新しいキーに変更する場合には、ルータはすべてのプロトコルメッセージの複数のコピー（1 つには古いキーが含まれ、もう 1 つには新しいキーが含まれているもの）を送信します。すべてのネイバルルータが新しいキーを使用してプロトコルメッセージをルータに返信し始めると、ルータは古いキーの使用を停止します。このようなロールオーバープロセスを使用することにより、ネットワーク管理者は、ネットワークの接続性に影響を及ぼすことなく、ネットワーク上のすべてのルータを更新する時間を確保できるようになります。セキュリティ上の理由から、すべてのネットワークルータが新しいキーを使用するように更新されたら、古いキーは削除してください。

Web 設定

ユニキャストルーティング

新しいキー ID を設定する前に、「Show MD5 Key」画面を使用して、現行のキーを削除する必要があります。

Web インターフェース

VLAN に割り当てられているすべてのエリアの OSPF インターフェースを設定するには、以下のようになります。

- (1) 「Routing Protocol」 → 「OSPF」 → 「Interface」 を選択します。
- (2) 「Step」 リストで 「Configure by VLAN」 を選択します。
- (3) 「VLAN ID」 を指定して、必要なインターフェース設定を設定します。
- (4) < Apply > ボタンをクリックします。

Routing Protocol > OSPF > Interface

Action: Configure by VLAN

VLAN ID: 1

Cost (1-65535): 1

Router Priority (0-255): 1

Hello Interval (1-65535): 10 sec

Dead Interval (1-65535): 40 sec

Transmit Delay (1-65535): 1 sec

Retransmit Interval (1-65535): 5 sec

Authentication Type: MD5

Message Digest Key ID: 1

Authentication Key: aiebel

Clear Click the button to clear the configuration of this VLAN.

Apply Revert

画面 1-343 :VLAN に割り当てられているすべてのインターフェースの設定の設定

VLAN に割り当てられている特定のエリアのインターフェース設定を設定するには、以下のようになります。

1. 「Routing Protocol」 → 「OSPF」 → 「Interface」 を選択します。
2. 「Step」 リストで 「Configure by Address」 を選択します。
3. 「VLAN ID」 を指定して、エリアに割り当てられるアドレスを入力し、必要なインターフェース設定を設定します。

4. < Apply > ボタンをクリックします。

Routing Protocol > OSPF > Interface

Action: Configure by Address

VLAN ID: 1

IP Address: 192.168.0.2

Cost (1-65535): 1

Router Priority (0-255): 1

Hello Interval (1-65535): 10 sec

Dead Interval (1-65535): 40 sec

Transmit Delay (1-65535): 1 sec

Retransmit Interval (1-65535): 5 sec

Authentication Type: MD5

Message Digest Key ID: 2

Authentication Key: bobby_martin

Clear [Click the button to clear the configuration of this IP address.](#)

Apply Revert

画面 1-344 :VLAN に割り当てられている特定エリアの設定の設定

OSPF インターフェースの設定情報を表示するには、以下のようにします。

1. 「Routing Protocol」 → 「OSPF」 → 「Interface」 を選択します。
2. 「Step」 リストで 「Show」 を選択します。
3. 「VLAN ID」 を指定します。

Routing Protocol > OSPF > Interface

Action: Show

VLAN ID: 1

Interface List Max: 512 Total: 4

Interface IP	Area ID	State	Designated Router IP	Designated Router ID	Backup Designated Router IP	Backup Designated Router ID
192.168.1.2/24	192.168.1.0	Up	192.168.1.2	192.168.1.2	0.0.0.0	0.0.0.0
192.168.10.2/24	192.168.10.0	Up	192.168.10.2	192.168.1.2	0.0.0.0	0.0.0.0
192.168.100.2/24	192.168.100.0	Up	192.168.100.2	192.168.1.2	0.0.0.0	0.0.0.0
192.168.110.2/24	192.168.110.0	Up	192.168.110.2	192.168.1.2	0.0.0.0	0.0.0.0

画面 1-345 :OSPF インターフェースの表示

インターフェースについて設定されている MD5 認証キーを表示するには、以下のようにします。

Web 設定

ユニキャストルーティング

1. 「Routing Protocol」→「OSPF」→「Interface」を選択します。
2. 「Step」リストで「Show MD5 Key」を選択します。
3. 「VLAN ID」を指定します。

Routing Protocol > OSPF > Interface

Action: Show MD5 Key

VLAN ID: 1

Interface MD5 List Max: 512 Total: 2

	Area ID	Key ID
☐	0.0.0.0	1
☐	192.168.10.0	2

Apply Revert

画面 1-346 :MD5 認証キーの表示

仮想リンクの設定

「Routing Protocol」→「OSPF」→「Virtual Link」(Add) および (Configure Detailed Settings) を選択すると、OSPF バックボーンに物理的に直接接続しないエリアからの仮想リンクを設定することができます。

すべての OSPF エリアは、バックボーンに接続していなければなりません。エリアがバックボーンに物理的に直接接続できない場合は、バックボーンへの論理パスを提供する仮想リンクを設定することができます。分離エリアをバックボーンに接続するため、論理パスは、単一の非バックボーンエリア（通過エリア）を経由してバックボーンに到達することができます。このパスを定義するには、分離エリアを共通の通過エリアに接続するエンドポイントとして機能する ABR を設定し、その共通の通過エリアをバックボーン自体に接続する反対側のエンドポイントで隣接 ABR を指定する必要があります（スタブまたは NSSA を経由する仮想リンクを設定することはできないので注意してください）。

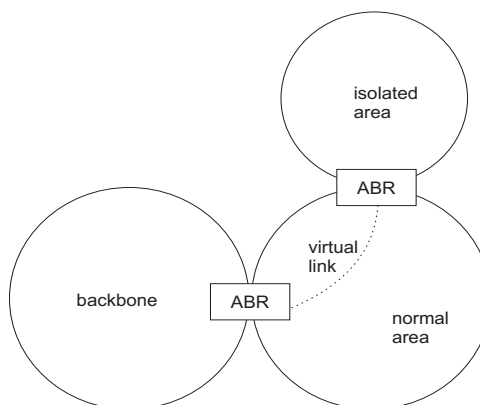


図 1-35:OSPF 仮想リンク

分離エリア

バックボーン標準エリア仮想リンク

また、仮想リンクを使用して、パーティション化を防ぐのに役立つように任意のエリアとバックボーンとの間の冗長リンクを作成したり、2つの既存のバックボーンエリアを共通バックボーンに接続したりすることができます。

バックボーンから分離されているあらゆるエリアには、通過エリア ID、およびバックボーンに隣接する仮想リンクネイバルータのルータ ID が含まれていなければなりません。

本製品は、最大 5 つの仮想リンクをサポートします。

関連する CLI 情報

「router ospf」

「area virtual-link」

コマンドの使用

- ・ 「Add」画面で仮想リンクを作成してから、「Configure Detailed Settings」画面でそのリンクのプロトコルタイマーと認証設定を指定します。「Configure Detailed Settings」画面で設定するパラメータについては、「OSPF インターフェースの設定」で説明しています。

パラメータ

以下のパラメータが表示されます。

- ・ Process ID – 「Network Area」設定画面で指定されたのと同じプロセス ID。
- ・ Area ID – 仮想リンクの通過エリアを示します。エリア ID の形式は、IPv4 アドレス形式にするか、4 octets の符号なし整数（範囲は 0 ～ 4,294,967,295）にしなければなりません。
- ・ Neighbor – 仮想リンクネイバルータのルータ ID。このパラメータは、仮想リンクの他端の ABR を指定します。仮想リンクを作成するには、リンクの両端で ABR の仮想リンクを設定する必要があります。ABR の 1 つは、分離エリアおよびリンクの一端の通過エリアに隣接していなければなりません。もう 1 つの ABR は、リンクの他端の通過エリアおよびバックボーンに隣接していなければなりません。

Web インターフェース

仮想リンクを作成するには、以下のようにします。

- (1) 「Routing Protocol」→「OSPF」→「Virtual Link」を選択します。
- (2) 「Step」リストで「Add」を選択します。
- (3) プロセス ID、エリア ID、およびネイバルータ ID を指定します。

(4) < Apply > ボタンをクリックします。

Routing Protocol > OSPF > Virtual Link

Action: Add

Process ID: 1

Area ID: 192.168.10.0

Neighbor: 192.168.10.3

Apply Revert

画面 1-347：仮想リンクの追加

仮想リンクを表示するには、以下のようにします。

1. 「Routing Protocol」 → 「OSPF」 → 「Virtual Link」 を選択します。
2. 「Step」 リストで 「Show」 を選択します。
3. 「Process ID」 を指定します。

Routing Protocol > OSPF > Virtual Link

Action: Show

Process ID: 1

Virtual Link List Max: 5 Total: 2

	Transit Area ID	Neighbor ID	State	Local Address	Remote Address	Hello Due	Adjacency State
☐	0.0.0.1	10.2.0.0	Down	192.168.1.1	192.168.2.1	Inactive	Full
☐	0.0.0.2	10.3.0.0	Waiting	*	*		Down

Delete Revert

画面 1-348：仮想リンクの表示

仮想リンクの詳細設定を設定するには、以下のようにします。

1. 「Routing Protocol」 → 「OSPF」 → 「Virtual Link」 を選択します。
2. 「Step」 リストで 「Configure Detailed Settings」 を選択します。
3. 「Process ID」 を指定してから、必要に応じてプロトコルタイマーと認証設定を変更します。

4. < Apply > ボタンをクリックします。

Routing Protocol > OSPF > Virtual Link

Action: Configure Detailed Settings

Process ID 1

Virtual Link List Max: 5 Total: 1

Transit Area ID	Neighbor ID	Transmit Delay (1-65535)	Retransmit Interval (1-65535)	Hello Interval (1-65535)	Dead Interval (1-65535)	Auth Key Type	MD5 Key ID	Auth Key
192.168.10.0	192.168.10.3	1	5	10	40	Simple		Gaibel

Apply Revert

画面 1-349 : 仮想リンクの詳細設定の設定

仮想リンクについて設定されている MD5 認証キーを表示するには、以下のようにします。

1. 「Routing Protocol」 → 「OSPF」 → 「Interface」 を選択します。
2. 「Step」 リストで 「Show MD5 Key」 を選択します。
3. 「VLAN ID」 を指定します。

Routing Protocol > OSPF > Virtual Link

Action: Show MD5 Key

Process ID 1

Virtual Link MD5 List Max: 5 Total: 6

☐	Transit Area ID	Neighbor ID	Key ID
☐	0.0.0.1	10.2.0.0	1
☐	0.0.0.1	10.2.0.0	4
☐	0.0.0.2	10.3.0.0	3
☐	0.0.0.2	10.3.0.0	5
☐	0.0.0.2	10.3.0.0	9
☐	0.0.0.2	10.3.0.0	13

Delete Revert

画面 1-350 : MD5 認証キーの表示

リンクステートデータベース情報の表示

「Routing Protocol」→「OSPF」→「Information」（LSDB）を選択すると、ルートをアドバタイズする OSPF ルータで送信されるリンクステートアドバタイズメント（LSA: Link State Advertisements）を表示することができます。ルーティンターフェースが接続しているエリアから収集する LSA をすべてまとめたものをリンクステートデータベースといいます。複数のインターフェースに接続するルータは、エリアごとに異なるデータベースを保有します。同じエリア内の各ルータには、そのエリアのトポロジを表わす同一のデータベース、および外部の宛先への最短パスがなければなりません。

新規ルータが検出されるとすぐに、データベース全体の情報がネイバルルータ間で交換されます。以降は、ルーティングテーブルで発生したあらゆる変更は、高信頼フラッディングと呼ばれるプロセスを通じて、ネイバルルータと同期されるようになります。ルータのデータベースに保存されているさまざまな LSA に関する情報を表示することができます。それらの情報には、以下のいずれかのタイプが含まれています。

- ・ Router (Type 1) – OSPF エリア内のすべてのルータが、そのルータのアクティブなインターフェースの状態とコストおよびネイバルルータを表わすルータ LSA を発信します。
- ・ Network (Type 2) – 各エリアの代表ルータが、現在のネットワークセグメントに接続しているすべてのルータを表わすネットワーク LSA を発信します。
- ・ Summary (Type 3) – ABR が、エリア外部にあるサブネットワークまでのコストを示すサマリ LSA を生成することができます。
- ・ AS Summary (Type 4) – ABR が、自律システム境界ルータ（ASBR）までのコストを示す AS サマリ LSA を生成することができます。
- ・ AS External (Type 5) – ASBR が、AS 外部の既知のそれぞれのネットワーク宛先の AS 外部 LSA を生成することができます。
- ・ NSSA External (Type 7) – NSSA 内の ASBR が、AS 外部の既知のそれぞれのネットワーク宛先の NSSA 外部 LSA を生成します。

関連する CLI 情報

「show ip ospf database」

パラメータ

以下のパラメータが表示されます。

- ・ Process ID – 「Network Area」設定画面で指定されたのと同じプロセス ID。
- ・ Query by – 以下の条件を使用して LSA データベースを検索することができます。
 - ・ Self-Originate – ルータで生成された LSA。
 - ・ Link ID – 特定のリンクをアドバタイズする LSA。
 - ・ Adv Router – 特定のルータによってアドバタイズされた LSA。
- ・ Link State Type – すべての LSA タイプについて、または、特定のタイプについて、クエリによって返された情報を表示することができます（デフォルト: All）。

LSA エントリごとに表示される情報として、以下のようなものがあります。

- ・ Area ID – 表示される LSA 情報に対して定義されているエリア。
- ・ Link ID – LSA によって表されるネットワーク部。「Link ID」は、以下のいずれかになります。

- ・ Type 3 のサマリ LSA および Type 5 の AS 外部 LSA の場合は、IP ネットワーク番号 (Type 5 の AS 外部 LSA がデフォルトルートを表わすものである場合、その「Link ID」はデフォルトの宛先 0.0.0.0 に設定されます)。
- ・ ルータ LSA、ネットワーク LSA、および Type 4 の AS サマリ LSA の場合は、ルータ ID。
- ・ Adv Router – アドバタイズ元ルータの IP アドレス。
- ・ Age – LSA の有効期限 (秒)。
- ・ Sequence – LSA の連続番号 (重複する LSA がある場合に古い方の LSA を見極めるために使用)。
- ・ Checksum – LSA のすべての内容のチェックサム。

Web インターフェース

リンクステートデータベース内の情報を表示するには、以下のようにします。

- (1) 「Routing Protocol」→「OSPF」→「Information」を選択します。
- (2) 「LSDB」を選択します。
- (3) 「Process ID」を指定します。
- (4) 必要な検索条件 (自己発信 LSA、特定のリンク ID を含む LSA、特定のルータによってアドバタイズされた LSA など) を指定します。

(5) LSA タイプに基づいて表示するデータベースエントリを選択します。

Routing Protocol > OSPF > Information

Type ☒ LSDB ☐ Neighbor

Process ID 1

Query by:

☐ Self-Originate

☐ Link ID

☐ Adv Router

Link State Type All

Link State Router List Total: 2

Area ID	Link ID	Adv Router	Age	Sequence	Checksum
0.0.0.0	192.168.0.4	192.168.0.4	702	0x80000003	0xE6B4
0.0.0.0	192.168.1.2	192.168.1.2	355	0x80000005	0xDDBC

Link State Network List Total: 1

Area ID	Link ID	Adv Router	Age	Sequence	Checksum
0.0.0.0	192.168.0.4	192.168.0.4	702	0x80000001	0x8F16

Link State Summary List Total: 1

Area ID	Link ID	Adv Router	Age	Sequence	Checksum
0.0.0.0	192.168.1.0	192.168.1.2	638	0x80000001	0x99EB

Link State ASBR Summary List Total: 0

Area ID	Link ID	Adv Router	Age	Sequence	Checksum

Link State External List Total: 0

Area ID	Link ID	Adv Router	Age	Sequence	Checksum

Link State NSSA External List Total: 0

Area ID	Link ID	Adv Router	Age	Sequence	Checksum

画面 1-351 : リンクステートデータベース内の情報の表示

ネイバルータに関する情報の表示

「Routing Protocol」→「OSPF」→「Information」(Neighbor)を選択すると、インターフェースごとにネイバルータに関する情報を表示することができます。

関連する CLI 情報

「show ip ospf neighbor」

パラメータ

以下のパラメータが表示されます。

- ・ Process ID - 「Network Area」設定画面で指定されたのと同じプロセス ID。
- ・ ID - ネイバルータのルータ ID。
- ・ Priority - ネイバルータの優先度。

State - OSPF の状態と ID フラグ。

- ・ 状態には、以下のようなものがあります。
- ・ Down - 接続がダウンしています。
- ・ Attempt - 接続がダウンしていますが、通信が試行されています（非ブロードキャストネットワーク）。
- ・ Init - hello パケットは受信されましたが、まだ通信は確立されていません。
- ・ Two-way - 双方向通信が確立されています。
- ・ ExStart - ネイバルータ間の隣接関係の初期化中です。
- ・ Exchange - データベース記述の交換中です。
- ・ Loading - LSA データベース情報の交換中です。
- ・ Full - ネイバルータが完全に隣接状態になりました。

ID フラグには、以下のようなものがあります。

- ・ D - ダイナミックネイバルータ
- ・ S - スタティックネイバルータ
- ・ DR - 代表ルータ
- ・ BDR - バックアップ代表ルータ
- ・ Address - インターフェースの IP アドレス。
- ・ Interface - OSPF が有効になっているレイヤ 3 インターフェース。

Web インターフェース

リンクステートデータベースに保存されているネイバルータに関する情報を表示するには、以下のようにします。

- (1) 「Routing Protocol」→「OSPF」→「Information」を選択します。
- (2) 「Neighbor」を選択します。

Web 設定

ユニキャストルーティング

(3) 「Process ID」を指定します。

Routing Protocol > OSPF > Information 

Type ☐ LSDB ☒ Neighbor

Process ID

Neighbor Information List Max: 256 Total: 2

Neighbor ID	Priority	State	Address	Interface
10.10.10.50	1	Full / DR	10.10.10.50	VLAN 1
10.10.10.50	1	Full / Backup	10.10.10.50	VLAN 2

画面 1-352 : リンクステートデータベースに保存されているネイバールータ情報の表示

1.19 マルチキャストルーティング

本章では、以下のマルチキャストルーティングに関するトピックについて説明します。

- ・ グローバルでのマルチキャストルーティングの有効化 – マルチキャストルーティングをグローバルで有効にする方法について説明します。
- ・ マルチキャストルーティングテーブルの表示 – マルチキャストルーティングテーブルを表示する方法について説明します。
- ・ IPv4 PIM の設定 – IPv4 PIM-DM と PIM-SM を設定する方法について説明します。
- ・ IPv6 PIM の設定 – IPv6 PIM-DM（バージョン 6）を設定する方法について説明します。

1.19.1 概要

本製品は、IPv4 PIM-DM または PIM-SM（Protocol-Independent Multicasting - Dense Mode または Sparse Mode）だけでなく、IPv6 PIM-DM を使用して、マルチキャストトラフィックを別々のサブネットワークにルーティングすることができます。IPv4 PIM（本書では PIMv4 と記述）では、IGMP 対応レイヤ 2 スイッチおよびホストから送信されるメッセージに依存して、ホストがマルチキャストグループに対する加入または脱退を希望しているかどうかを判別されます。IPv6 PIM（本書では PIMv6 と記述）では、IPv6 と同等の IGMPv2 である MLDv1（Multicast Listener Discovery）を使用します。PIM-DM は、ローカルネットワークなどのように、マルチキャストグループメンバーを使用する可能性が高いネットワークを対象としています。PIM-DM は、インターネットなどのように、マルチキャストグループメンバーを使用する可能性が低いネットワークを対象としています。

また、本製品で PIM が有効になっていない場合や、ネットワークで他のマルチキャストルーティングプロトコルが使用されている場合は、マルチキャストルータに接続されているスイッチポートを、マルチキャストトラフィックを転送するように設定することができます（「マルチキャストルータのスタティックインターフェースの指定」を参照）。

PIM-DM の設定

PIM-DM は、マルチキャストトラフィックをダウンストリームにフロードし、それぞれの送信元ホストグループと宛先ホストグループとの間の最短パスのソースルーティング配信ツリーを導き出します。DVMRP などのような他のマルチキャストルーティングプロトコルでは、独自のソースルーティングマルチキャスト配信ツリー（つまり、個別のルーティングテーブル）を作成して、ループを防止したり、マルチキャストトラフィックの送信元への最短パスを判別したりします。PIM-DM でもマルチキャストソースごとにソースルーティングマルチキャスト配信ツリーを作成しますが、独自のマルチキャストテーブルを保持するのではなく、ルータのユニキャストルーティングテーブルからの情報を使用するので、ルーティングプロトコルに依存しません。

PIM-DM は、フロードとプルーンを使用して、マルチキャストソースグループペアごとのソースルーティングマルチキャスト配信ツリーを作成する簡易マルチキャストルーティングプロトコルです。前述のように、PIM-DM は、独自のルーティングテーブルを保持しませんが、その代わりに、ルータインターフェースで有効になっている任意のユニキャストルーティングプロトコルによって提供されるルーティングテーブルを使用します。ルータがソースグループペアのマルチキャストパケットを受信すると、PIM-DM によって、インバウンドインターフェースのユニキャストルーティングテーブルがチェックされ、そのインターフェースがユニキャストパケットをマルチキャストソースネットワークにルーティングするために使用されたのと同じインターフェースであるかどうかを判別されます。同じインターフェースではない場合は、ルータがパケットをドロップし、Assert メッセージを送信元インターフェースに返します。それから、その送信元からのトラフィックの転送を続行するため、Assert Winner が選択されます。一方、インバウンドインターフェースがユニキャスト

プロトコルで使われたのと同じインターフェースである場合には、ルータは、その特定のソースグループペアについてまだ Prune メッセージを受信したことがない他のすべてのインターフェースにパケットのコピーを転送します。

DVMRP では Prune 状態が約 2 時間維持されますが、PIM-DM では Prune 状態は 3 分程度しか維持されません。そのため、PIM-DM の場合、DVMRP に比べてフロードが発生する確率が高くなりますが、主なデメリットはそれだけであり、その代わりに、処理オーバーヘッドが軽減され、設定が容易になるというメリットが得られます。

PIM-SM の設定

PIM-SM では、ルータのローカルユニキャストルーティングテーブルを使用して、マルチキャストトラフィックが（フロードされるのではなく）ルーティングされます。マルチキャストトラフィックが転送されるのは、ローカルホストまたはダウンストリームホストから要求された場合のみです。ホストからサービスを要求された場合、PIM-SM では、逆方向パスツリー（RPT: Reverse Path Tree）を使用して、それぞれの送信元からのマルチキャストトラフィックをローカル PIM-SM ドメイン内の単一のランデブーポイント（RP: Rendezvous Point）経由でチャネリングすることができます。それから、そのトラフィックを、ホストが接続しているローカルネットワークセグメント内の代表ルータ（DR: Designated Router）に転送します。ただし、特定の送信元からのマルチキャスト負荷が極めて高く、そうすることが妥当であると思われる場合には、RP をバイパスして DR から送信元に直接接続する最短パスツリー（SPT: Shortest Path Tree）を作成するように PIMSM を設定して、アクティブなホストのサービス遅延と新規ホストのセットアップ時間を短縮することができます。

PIM-SM では、マルチキャストトラフィックをグループの受信先に接続されているポートのみに転送することによって、マルチキャストトラフィックの量を減らします。マルチキャストトラフィックのフィルタリングのための重要な要素は、以下のとおりです。

共通ドメイン

すべてのマルチキャストルータが同じ基本 PIM-SM 設定を使用して設定されている共通ドメインをセットアップする必要があります。

ブートストラップルータ（BSR）

共通ドメインをセットアップした後、その共通ドメインからブートストラップルータが選出されます。PIM-SM ルータがブートアップされるたびに、または、PIM-SM を有効にするためにマルチキャストモードが再設定されるたびに、ブートストラップルータ候補のルータが自らのすべてのインターフェースでブートストラップメッセージのフロードを開始します（逆方向転送を使用するとネットワークへの影響を抑えることができます）。ネイバールータは、ブートストラップメッセージを受信すると、そのメッセージを処理してから、すべてのインターフェース（ただし、メッセージを受信時に使用されたものを除く）を使用して転送します。ルータは、自らの BSR 優先度よりも高い BSR 優先度を含むブートストラップメッセージを受信すると、自らを BSR の候補としてアドバタイズするのをやめます。最終的には、BSR 優先度が最も高いルータがブートストラップメッセージを送信し続けることになります。

ランデブーポイント（RP）

ルータは、指定されたグループアドレスについて自らを RP 候補であるとアドバタイズする PIMv2 メッセージを BSR に定期的に送信することもできます。すると、その BSR は、すべての RP 候補に関する情報を、以降送信されるブートストラップメッセージに挿入するようになります。BSR、およびそれらのメッセージを受信するすべてのルータは、同じハッシュアルゴリズムを使用して、それぞれのマルチキャストグループの RP を選出します。そ

それぞれのルータが適切に設定されていれば、選出プロセスの結果はそれぞれのルータで同じになります。選出されたそれぞれの RP は、1 つまたは複数のマルチキャストグループの共有配信ツリーのルートとして機能するようになります。

代表ルータ (DR)

Hello メッセージで最高の優先度をアドバタイズする DR が、それぞれのサブネットで選出されます。DR は、グループに対する加入または脱退を希望しているマルチキャストクライアントに関する情報をサブネットから収集する役割を果たします。各グループの DR (受信先) から Join メッセージが RP へと送信され、マルチキャストソースからのデータが RP に送信されます。その時点で、受信先は、クライアントグループ宛のトラフィックを RP から受信できるようになります。または、送信元を特定して、必要に応じて、最短パスツリー (SPT) による送信元への直接接続をセットアップします (ただし、そのような切り替えに伴う負荷が相応なものである場合)。

共有ツリー

多数の受信先がグループに加入する場合は、それらの受信先の Join メッセージは、RP で収束され、それらのメッセージに基づいて、その RP でルーティングされるグループの配信ツリーが形成されます。このツリーは、逆方向ツリー (RPT) と呼ばれます。または、該当のグループ宛にデータを送信するすべての送信元によって共有されることから、共有ツリーとも呼ばれます。あるグループ宛のデータをマルチキャストソースが送信すると、そのソースのローカル DR がそれらのデータパケットを受け取り、ユニキャストカプセル化してから、RP に送信します。RP は、それらのカプセル化されたデータパケットを受信すると、カプセル化を解除して、共有ツリーに転送します。それらのパケットは、RP ツリー上のルータで保持されるグループマッピングに従って処理され、RP ツリーが分岐するたびにレプリケートされて、最終的には、そのマルチキャストグループのすべての受信先に到達します。共有ツリー上のすべてのルータは PIM-SM を使用するので、マルチキャストフローは共有ツリー内にとどめられます。また、複数のフローを同じ共有ツリーに沿って伝播することができますが、それぞれのフローを担当する RP は 1 つだけであるということにも注意してください。

最短パスツリー (SPT)

共有ツリーを使用する場合、マルチキャストトラフィックは共有ツリー内にとどめられます。ただし、共有ツリーにはいくつか欠点があります。RP でトラフィックをカプセル化解除してマルチキャストパケットにする処理には、大量のリソースが必要になります。プロトコルでは、RP の選出時にグループメンバーのロケーションは考慮されないため、RP から受信先へのパスが常に最適なものになるとは限りません。それだけでなく、共有ツリーをセットアップして送信元への戻りパスを確立する前に RP が DR からの Register メッセージを待機しなければならないため、グループに加入しようとしているホストで大幅な遅延が発生する可能性があります。また、送信元でバーストが発生しやすくなるという問題もあります。送信元で頻繁にタイムアウトが発生すると、そのたびに共有ツリーを再作成しなければならないので、その結果、トラフィックを受信先に送信する際の遅延時間が増加します。全体的なネットワークパフォーマンスを向上させるため、スイッチは、送信元から最初に受け取ったパケットのみを RP を使用して受信先に転送します。最初のパケットを転送した後、受信先と送信元との間の最短パスを求め、以降は、SPT を使用して、送信元からのすべてのパケットを受信先に直接送信します。RP は、最初のパケットが最短パス経由でネイティブに到着すると、登録停止メッセージを送信元付近の DR に返します。DR は、登録停止メッセージを受信すると、RP への Register メッセージの送信を停止します。共有ツリーを使用している送信元が他にない場合は、共有ツリーも削除されます。SPT をセットアップする場合、共有ツリーを使用する場合よりも多くのメモリが必要になりますが、グループへの加入時とデータ送信時の遅延が大幅に緩和されます。また、スイッチは、特定のマルチキャスト

Web 設定

マルチキャストルーティング

トグループについてのみ SPT を使用するように設定したり、特定のグループについて SPT への切り替えを無効にするように設定したりすることができます。

1.19.2 マルチキャストルーティングのグローバル設定の設定

本製品でマルチキャストルーティングを使用するには、最初に、このセクションの説明に従ってマルチキャストルーティングをグローバルで有効にし、それから、マルチキャストルーティングプロトコルを採用するインターフェースを指定します。ただし、いずれのインターフェースでも有効することができる IPv4 マルチキャストルーティングプロトコルは 1 つだけですが、同じインターフェースで PIMv4 と PIMv6 の両方を有効にすることができるということに注意してください。

グローバルでのマルチキャストルーティングの有効化

「Multicast」→「Multicast Routing」→「General」を選択すると、IP マルチキャストルーティングをスイッチでグローバルに有効にすることができます。

関連する CLI 情報

「ip multicast-routing」

パラメータ

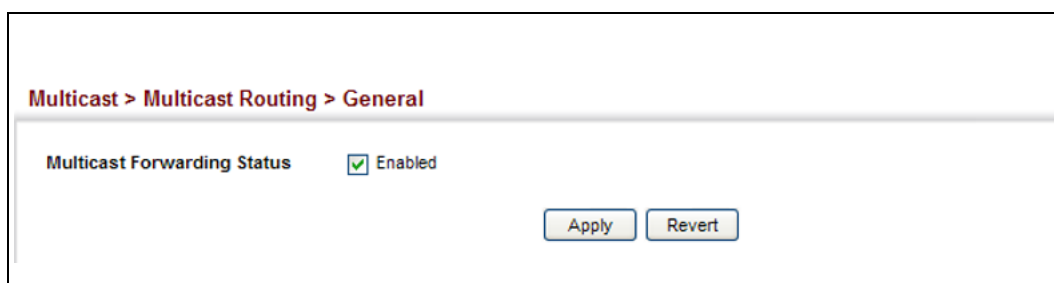
以下のパラメータが表示されます。

- ・ Multicast Forwarding Status – IP マルチキャストルーティングを有効にします（デフォルト : Disabled）。

Web インターフェース

マルチキャストルーティングを有効にするには、以下のようになります。

- (1) 「Multicast」→「Multicast Routing」→「General」を選択します。
- (2) 「Multicast Forwarding Status」で「Enabled」チェックボックスをオンにします。
- (3) < Apply > ボタンをクリックします。



The screenshot shows a web configuration page for Multicast. The breadcrumb trail at the top is "Multicast > Multicast Routing > General". Below this, there is a section titled "Multicast Forwarding Status" with a checkbox labeled "Enabled" that is checked. At the bottom right of the section, there are two buttons: "Apply" and "Revert".

画面 1-353 : マルチキャストルーティングの有効化

マルチキャストルーティングテーブルの表示

「Multicast」→「Multicast Routing」→「Information」を選択すると、PIM を使用して学習された各マルチキャストルートに関する情報を表示することができます。ルータは、マルチキャストルートをネイバールータから学習し、また、それらのルートをネイバールータにアドバタイズします。ルータは、実際のグループメンバーシップメッセージや Prune メッセージを考慮に入れずに、自らが学習したパスと他のルータが学習したパスすべてのエントリを保存します。したがって、ルーティングテーブルからは、テーブルに含まれている特定のどの送信元からのマルチキャストトラフィックをルータが処理したかがわかりません。ルータは、直接接続しているサブネットワーク上またはダウンストリームルータに接続しているサブネットワーク上にグループのメンバーが存在している場合にのみ、ルーティングテーブルのルートを使用してマルチキャストトラフィックを転送します。

関連する CLI 情報

「show ip mroute」

パラメータ

以下のパラメータが表示されます。

Show Summary

- ・ Group Address – マルチキャストサービス用の IP グループアドレス。
- ・ Source Address – IP マルチキャストソースを含むサブネットワーク。
- ・ Source Mask – IP マルチキャストソースのネットワークマスク（ただし、本製品ではソースマスクを検出することができないので、このフィールドには「255.255.255.255」と表示されます）。
- ・ Interface – アップストリームネイバールータへのインターフェース。

PIM では、ユニキャストルーティングテーブルに基づいてマルチキャストルーティングツリーが作成されます。関連するユニキャストルーティングテーブルが存在しない場合でも、マルチキャストルーティングエントリが作成され、アップストリームインターフェースが表示されて、そのエントリが有効であるということが示されます。また、このフィールドには、「Register」と表示されることもあり、その場合は、PIM-SM Register パケットの受信に疑似インターフェースが使用されていることを示します。そのようなことは、逆方向パスツリー（RPT）のルートであるランデブーポイント（RP）の場合に発生します。その場合は、Register パケットを受信するいずれかの VLAN が登録インターフェースに変換されます。
- ・ Owner – 関連付けられているマルチキャストプロトコル（PIM-DM、PIM-SM、IGMP Proxy）。
- ・ Flags – それぞれのルーティングエントリに関連付けられるフラグであり、以下のことを示します。
 - ・ Forward – アップストリームインターフェースで受信されたトラフィックが、このインターフェースに転送されています。
 - ・ Local – これは、発信インターフェースです。
 - ・ Pruned – このインターフェースは、トラフィックを受信する必要がなくなったダウンストリームネイバールータによってブルーニングされました。

Show Details

- ・ Group Address - マルチキャストサービス用の IP グループアドレス。
- ・ Source Address - IP マルチキャストソースを含むサブネットワーク。
- ・ Source Mask - IP マルチキャストソースのネットワークマスク。
- ・ Upstream Neighbor - グループのアップストリーム側の直近のマルチキャストルータ (RPF ネイバールータ)。
- ・ Upstream Interface - アップストリームネイバールータへのインターフェース。
- ・ Up Time - エントリ作成からの経過時間。
- ・ Owner - 関連付けられているマルチキャストプロトコル (PIM-DM、PIM-SM、IGMP Proxy)。
- ・ Flags - それぞれのルーティングエントリに関連付けられるフラグであり、以下のことを示します。
 - ・ Dense - PIM Dense モードを使用中です。
 - ・ Sparse - PIM Sparse モードを使用中です。
 - ・ Connected - 送信元に直接接続されているルートです。
 - ・ Pruned - 使用終了になったルートです。
 - ・ Register - マルチキャストソースへの登録中です。
 - ・ RPT-bit set - (S,G) エントリはランデブーポイント (RP) をポイントするものであり、通常は、特定の送信元の共有ツリーでプルーンされた状態であることを示します。
 - ・ SPT-bit set - マルチキャストパケットが最短パスツリー上の送信元から受信されました。
 - ・ Join SPT - 共有ツリー経由で到着するトラフィックのレートが、このグループの SPT しきい値を超えました。(*,G) エントリに SPT フラグが設定されている場合、次回、(S,G) パケットが受信されると、ルータが最短パスツリーに追加されます。(S,G) エントリに SPT フラグが設定されている場合、ルータは即座に最短パスツリーに追加されます。

Downstream Interface List -

- ・ Interface - マルチキャストサブスクライバが記録されたインターフェース。
- ・ State - それぞれのダウンストリームインターフェースに関連付けられるフラグであり、以下のことを示します。
 - ・ Forward - アップストリームインターフェースで受信されたトラフィックが、このインターフェースに転送されています。
 - ・ Local - このダウンストリームインターフェースで、同じサブネット内のホストから IGMP レポートメッセージが受信されました。
 - ・ Pruned - 使用終了になったルートです。
 - ・ Registering - マルチキャストソースへの登録中です。

Web インターフェース

マルチキャストルーティングテーブルを表示するには、以下のようにします。

1. 「Multicast」 → 「Multicast Routing」 → 「Information」 を選択します。
2. 「Step」 リストで 「Show Summary」 を選択します。

Multicast > Multicast Routing > Information

Action: Show Summary

Multicast Routing Summary List Max: 255 Total: 3

Group Address	Source Address	Source Mask	Interface	Owner	Flags
224.0.17.17	192.168.2.1	255.255.255.255	VLAN 1	PIM-DM	Forward
224.1.1.1	10.1.1.0	255.255.255.0	VLAN 2	DVMRP	Pruned
224.1.1.2	10.1.1.0	255.255.255.0	VLAN 3	DVMRP	Forward

画面 1-354 : マルチキャストルーティングテーブルの表示

マルチキャストルーティングテーブル内の特定のフローに関する詳細情報を表示するには、以下のようにします。

1. 「Multicast」 → 「Multicast Routing」 → 「Information」 を選択します。
2. 「Step」 リストで 「Show Details」 を選択します。
3. 「Group Address」 ドロップダウンリストでグループアドレスを選択します。
4. 「Source Address」 ドロップダウンリストでソースアドレスを選択します。

Multicast > Multicast Routing > Information

Action: Show Detail

Group Address 224.0.17.17

Source Address 192.168.2.1

Source Mask 255.255.255.255

Upstream Neighbor 192.168.2.2

Upstream Interface VLAN 1

Up Time 00:00:05

Owner PIM-DM

Flags Dense

Downstream Interface List Max: 256 Total: 3

Interface	State
VLAN 1	Forward
VLAN 2	Pruned
VLAN 3	Forward

画面 1-355 : マルチキャストルーティングテーブルの詳細エントリの表示

Web 設定

マルチキャストルーティング

1.19.3 IPv4 PIM の設定

ここでは、IPv4 PIM-DM と PIM-SM を設定する方法について説明します。

グローバルでの PIM の有効化

「Routing Protocol」→「PIM」→「General」を選択すると、IPv4 PIM ルーティングをルータでグローバルに有効にすることができます。

関連する CLI 情報

「router pim」

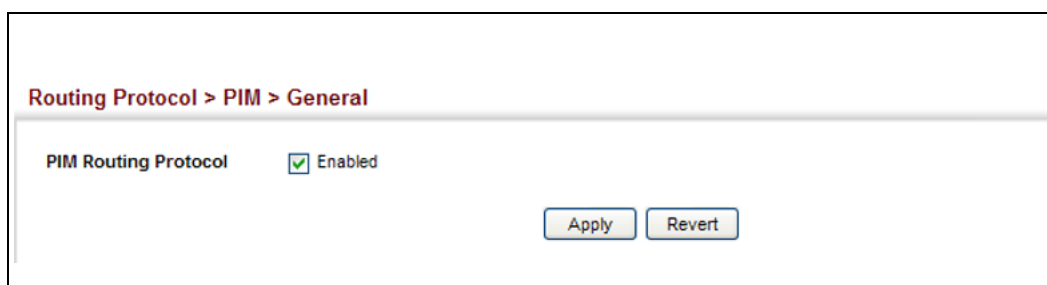
コマンドの使用

- ・ この機能は、PIM-DM および PIM-SM をルータでグローバルに有効にします。その際、マルチキャストルーティングをサポートするインターフェースごとに PIM-DM または PIM-SM を有効にし、マルチキャストプロトコルパラメータに適宜変更を加えることも必要になります。
- ・ PIM を使用するには、スイッチで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（「グローバルでのマルチキャストルーティングの有効化」を参照）。

Web インターフェース

PIM マルチキャストルーティングを有効にするには、以下のようにします。

- (1) 「Routing Protocol」→「PIM」→「General」を選択します。
- (2) 「PIM Routing Protocol」で「Enabled」チェックボックスをオンにします。
- (3) < Apply > ボタンをクリックします。



The screenshot shows a web configuration page for 'Routing Protocol > PIM > General'. It features a section for 'PIM Routing Protocol' with a checked checkbox labeled 'Enabled'. At the bottom right, there are two buttons: 'Apply' and 'Revert'.

画面 1-356 :PIM マルチキャストルーティングの有効化

PIM インターフェース設定の設定

「Routing Protocol」→「PIM」→「Interface」を選択すると、それぞれのインターフェースのルーティングプロトコルの機能属性を設定することができます。

関連する CLI 情報

「IPv4 PIM Commands」

コマンドの使用

- ・ この画面のほとんどの属性は、PIM-DM と PIM-SM で共通です。「Dense」モードまたは「Sparse」モードを選択すると、選択したモードに該当する属性が共通属性と共に表示されます。
- ・ PIM プロキシと IGMP プロキシを併用することはできません。インターフェースが PIM Dense モードまたは PIM Sparse モードを使用するように設定されている場合には、本製品のいずれのインターフェースでも IGMP を有効にすることはできません（「IGMP スヌーピングとクエリのパラメータの設定」を参照）。また、あるインターフェースで IGMP を有効にしている場合は、いずれのインターフェースでも PIM を有効にすることはできません。

PIM-DM

- ・ PIM-DM は、アクティブなマルチキャストサーバからのトラフィックを定期的にネットワークにフロードして、DVMRP と同じように機能します。また、PIM-DM では、IGMP を使用して、マルチキャストグループメンバーが存在しているかどうかが判別されます。DVMRP との主な違いは、PIM-DM では、ルータのユニキャストルーティングテーブルを使用して、パケットの受信に使用されたインターフェースが送信元への最短パスを提供するかどうかを判別されるということです。
- ・ Dense モードインターフェースは、デフォルトで、マルチキャストフラッディングに従い、グループメンバーまたはダウンストリームルータが存在していないことがルータによって確認された場合、または、Prune メッセージがダウンストリームルータから受信された場合にのみ、マルチキャストルーティングテーブルから削除されます。

PIM-SM

- ・ PIM-SM インターフェースは、Join メッセージがダウンストリームルータから受信された場合、または、グループメンバーがインターフェースに直接接続している場合にのみ、マルチキャストトラフィックを転送するために使用されます。ルータは、マルチキャストフローの受信を希望する場合には、RP に Join メッセージを定期的に送信し、その後、指定された RP への戻りフローの共有パスに追加されます。ルータは、SPT を使用する送信元パスへの加入を希望する場合は、送信元に Join メッセージを定期的に送信します。また、ルータは、SPT によって自らが送信元に接続された後、または、該当のインターフェースに接続するグループメンバーがいなくなった場合に、RP に Prune メッセージを送信して、共有パスが削除されるようにします。

パラメータ

以下のパラメータが表示されます。

Common Attributes

- ・ VLAN – レイヤ 3 の VLAN インターフェイス（範囲：1 ～ 4,093）。
- ・ Mode – PIM ルーティングモード（オプション：Dense、Sparse、None）。
- ・ IP Address – 選択された VLAN に割り当てられているプライマリ IP アドレス。
- ・ Hello Holdtime – PIM ネイバルータがダウンしていることを宣言する前にそのルータからの Hello メッセージを待機する時間を設定します。この「Hello Holdtime」は、「Hello Interval」の値と同じか、それ以上でなければならず、そうでない場合は自動的に「Hello Interval」の 3.5 倍に設定されます（範囲：1 ～ 65,535 秒、デフォルト：105 秒または「Hello Interval」（設定されている場合）の 3.5 倍）。
- ・ Hello Interval – すべてのインターフェイスにおける PIM Hello メッセージの送信間隔を設定します（範囲：1 ～ 65,535 秒、デフォルト：30 秒）。

Hello メッセージは、受信したプローブの送信元の PIM ネイバルータに送信され、それらのネイバルータがまだマルチキャストツリーのアクティブなメンバーであるかどうかを確認するために使用されます。PIM-SM ルータは、Hello メッセージを、ネイバルータが存在しているかどうかを確認するためだけでなく、各 LAN セグメントのどのルータが代表ルータ（DR）として稼働しているかを判別するためにも使用します。

ルータは、Boot 時、または PIM を使用するように最初に設定されたときには、初回 Hello メッセージを送信し、それから、Hello タイマーを指定の値に設定します。

「Hello Holdtime」で指定されている期間、ネイバルータからメッセージが送信されてこなければ、ルータは、そのネイバルータをドロップします。この保留時間の値は、ネイバルータから受信する各 Hello メッセージに含まれています。また、Hello メッセージにはメッセージの送信元のルータの DR 優先度も含まれるということにも注意してください。

「Hello Holdtime」が既に設定されており、「Hello Interval」が「Hello Holdtime」よりも大きい場合、このコマンドは失敗します。

- ・ Join/Prune Holdtime – Prune 状態を維持する期間を設定します（範囲：1 ～ 65,535 秒、デフォルト：210 秒）。
 - ・ PIM-DM – 特定の送信元から初めてマルチキャストストリームを受信したマルチキャストインターフェイスは、そのトラフィックをルータ上の他のすべての PIM-DM インターフェイスに転送します。そのインターフェイスにトラフィックを要求しているグループがない場合、リーフノードは、Prune メッセージをアップストリームに送信し、そのマルチキャストストリームについて Prune 状態になります。Prune 状態は、「Join/Prune Holdtime」が経過するまで、または、転送先エントリに関する Graft メッセージが受信されるまで、維持されます。
 - ・ PIM-SM – 特定の送信元から初めてマルチキャストストリームを受信したマルチキャストインターフェイスは、そのトラフィックを、ルータ上で、該当のグループへの加入を要求しているインターフェイスのみに転送します。そのインターフェイスにトラフィックを要求しているグループが既に存在していない場合、リーフノードは、Prune メッセージをアップストリームに送信し、そのマルチキャストストリームについて Prune 状態になります。この (S, G)（送信元とグループ）の組み合わせについて、現在の Join 状態と Pending RPT Prune 状態の両方が、「Join/Prune Holdtime」が経過するまで維持されます。
- ・ LAN Prune Delay – このデバイスが Prune 要求を受信してからフローをブールンするまでの待機時間がダウンストリームルータに通知されるようにします（デフォルト：Disabled）。

同じ VLAN 上の他のダウンストリームルータは、このアップストリームルータが Prune 要求を受信したことを通知された場合、フローを引き続き受信したければ、この

「LAN Prune Delay」期間が経過する前に Join メッセージを送信して Prune メッセージをオーバーライドする必要があります。このコマンドによって生成されるメッセージを使用すると、フローを受信したホストをダウンストリームのネイバルータに通知して、それらのルータが Join メッセージを返すという処理が効率的に実行されるようになります。この「LAN Prune Delay」期間を過ぎても Join メッセージが受信されない場合、ルータはフローをプルーンします。

「LAN Prune Delay」は、「Override Interval」と「Propagation Delay」の合計に基づいて求められます。

- ・ Override Interval – ダウンストリームルータが LAN Prune Delay メッセージで示されているフローを引き続き受信する場合に Join メッセージを戻すことによって LAN Prune Delay メッセージに応答するために必要な時間（範囲：500 ～ 6,000 ms、デフォルト：2,500 ms）。

「LAN Prune Delay」は、「Override Interval」と「Propagation Delay」に基づいて求められます。この「Override Interval」は、LAN Prune Delay メッセージで示されているフローを引き続き受信したいグループメンバーがダウンストリームルータにいる場合に、ダウンストリームルータが LAN Prune Delay メッセージを処理してから Join メッセージを送信することによってアップストリームルータに応答してフローが終了されないようにするために必要な時間を表わします。

- ・ Propagation Delay – LAN Prune Delay メッセージがダウンストリームルータに到達するために必要な時間（範囲：100 ～ 5,000 ms、デフォルト：500 ms）。

「LAN Prune Delay」は、「Override Interval」と「Propagation Delay」に基づいて求められます。この「Propagation Delay」は、LAN Prune Delay メッセージで示されているフローを引き続き受信したいグループメンバーがダウンストリームルータにいる場合に、LAN Prune Delay メッセージがアップストリームルータから同じ VLAN インターフェースに接続しているすべてのダウンストリームルータに伝搬されるために必要な時間を表わします。

- ・ Trigger Hello Delay – ルータが Reboot されてから、またはインターフェースで PIM が有効化されてからトリガーされた PIM Hello メッセージの送信が開始されるまでの最大時間（範囲：0 ～ 5 秒、デフォルト：5 秒）。

ルータを初めて始動するか、インターフェースで PIM を有効にすると、Hello 遅延が 0 から「Trigger Hello Delay」の間のランダムな値に設定されます。そのようにすることで、複数のルータが同時に電源オンにされた場合にマルチアクセスリンクで Hello メッセージが同期されないようにしています。

また、ルータは、新規ルータから Hello メッセージを受信すると、0 から「Trigger Hello Delay」の間のランダムな値に設定されている遅延期間が経過してから自らの Hello メッセージを送信します。

Dense-Mode Attributes

- ・ Graft Retry Interval – Graft メッセージを再送信する前に Graft 肯定応答メッセージを待機する期間（範囲：1 ～ 10 秒、デフォルト：3 秒）。

Graft メッセージは、Prune 状態を解除するためにルータが送信します。ルータは、Graft メッセージを受信した場合には、Graft 肯定応答メッセージを返す必要があります。肯定応答メッセージがない場合、Graft メッセージを送信したルータは、何回か（「Max. Graft Retries」で指定されている回数）Graft メッセージ再送信します。

- ・ Max. Graft Retries – 肯定応答がない場合の Graft メッセージの最大再送回数（範囲：1 ～ 10、デフォルト：3）。
- ・ State Refresh Origination Interval – PIM-DM State Refresh Control（PIM-DM 状態リフレッシュ制御）メッセージの送信間隔（範囲：1 ～ 100 秒、デフォルト：60 秒）。

Prune 状態は約 3 分間ごとにタイムアウトになり、マルチキャストパケットと Prune メッセージが PIM-DM ネットワーク全体に再びフロードされます。状態リフレッシュ機能では、制御メッセージを配信ツリーのダウンストリームへ定期的に転送することにより、ツリー内の各ルータの発信インターフェースの Prune 状態をリフレッシュして、Prune 状態がタイムアウトにならないようにします。また、そのようにすると、デフォルトの 3 分間のタイムアウト期間が経過する前に PIM ルータがトポロジの変更（マルチキャストグループに対する送信元の加入または脱退）を認識できるようになります。

このコマンドは、マルチキャストグループの送信元メンバーに直接接続するファーストホップの PIM-DM ルータのインターフェースについてのみ、有効です。

Sparse-Mode Attributes

- ・ DR Priority – ルータが自らを代替ルータ（DR）の候補として宣言する際にアドバタイズする優先度を設定します（範囲：0 ～ 4,294,967,294、デフォルト：1）。

Ethernet LANやその他の共有メディアLANに複数のPIM-SMが接続していることがあります。マルチキャストホストがLANに直接接続している場合は、ルータが1つだけがDRとして選出されて、マルチキャストホストに代わってJoinメッセージやPruneメッセージを各グループのグループ固有のRPへ定期的に送信します。DRは、簡易な選出プロセスを使用してインターフェース（LANなど）ごとに1つずつ選出されます。

インターフェースで設定されている最も高い優先度をもつルータがDRとして選択されます。インターフェースに接続している複数のルータの優先度が同じ場合には、最上位のIPアドレスをもつDRとして選出されます。

ルータが自らの優先度をHelloメッセージでアドバタイズしない場合は、最も高い優先度をもつものとみなされ、DRとして選出されます。複数のルータが自らの優先度をアドバタイズしない場合には、最上位のIPアドレスをもつルータがDRとして選出されます。

- ・ Join/Prune Interval – Join メッセージと Prune メッセージの送信間隔を設定します（範囲：1 ～ 65,535 秒、デフォルト：60 秒）。

デフォルトでは、スイッチは、60 秒ごとに Join メッセージまたは Prune メッセージを送信して、どのクライアントがマルチキャストグループに対する加入または脱退を希望しているかを PIM-SM ルータに通知します。

「Join/Prune Interval」は、同じ PIM-SM ドメイン内のすべての PIM-SM ルータで同じ値に設定してください。同じ値を使用しない場合、ルーティングプロトコルのパフォーマンスに悪影響を及ぼします。

特定の送信元から初めてマルチキャストストリームを受信したマルチキャストインターフェースは、そのトラフィックを、ルータ上で、該当のグループへの加入を要求しているインターフェースのみに転送します。そのインターフェースにトラフィックを要求しているグループが既に存在していない場合、リーフノードは、Prune メッセージをアップストリームに送信し、そのマルチキャストストリームについて Prune 状態になります。この (S, G) (送信元とグループ) の組み合わせについて、現在の Join 状態と Pending RPT Prune 状態の両方が、「Join/Prune Holdtime」が経過するまで維持されます。

Web インターフェース

PIM インターフェース設定を設定するには、以下のようにします。

- (1) 「Routing Protocol」→「PIM」→「Interface」を選択します。
- (2) プロトコルパラメータを必要に応じて変更します。
- (3) < Apply > ボタンをクリックします。

Routing Protocol > PIM > Interface

VLAN	1	
Mode	Dense	
IP Address	192.168.0.2	
Hello Holdtime (1-65535)	105	sec
Hello Interval (1-65535)	30	sec
Join/Prune Holdtime (1-65535)	210	sec
LAN Prune Delay	☐ Enabled	
Override Interval (500-6000)	2500	msec
Propagation Delay (100-5000)	500	msec
Trigger Hello Delay (0-5)	5	sec
Graft Retry Interval (1-10)	3	sec
Max. Graft Retries (1-10)	3	
State Refresh Origination Interval (1-100)	60	sec

Apply
Revert

画面 1-357 :PIM インターフェース設定の設定 (Dense モード)

Web 設定

マルチキャストルーティング

Routing Protocol > PIM > Interface

VLAN	1
Mode	Sparse
IP Address	192.168.0.2
Hello Holdtime (1-65535)	105 sec
Hello Interval (1-65535)	30 sec
Join/Prune Holdtime (1-65535)	210 sec
LAN Prune Delay	☐ Enabled
Override Interval (500-6000)	2500 msec
Propagation Delay (100-5000)	500 msec
Trigger Hello Delay (0-5)	5 sec
DR Priority (0-4294967294)	1
Join/Prune Interval (1-65535)	60 sec

Apply Revert

画面 1-358 :PIM インターフェース設定の設定 (Sparse モード)

ネイバールータに関する情報の表示

「Routing Protocol」→「PIM」→「Neighbor」を選択すると、すべての PIM ネイバールータを表示することができます。

関連する CLI 情報

「show ip pim neighbor」

パラメータ

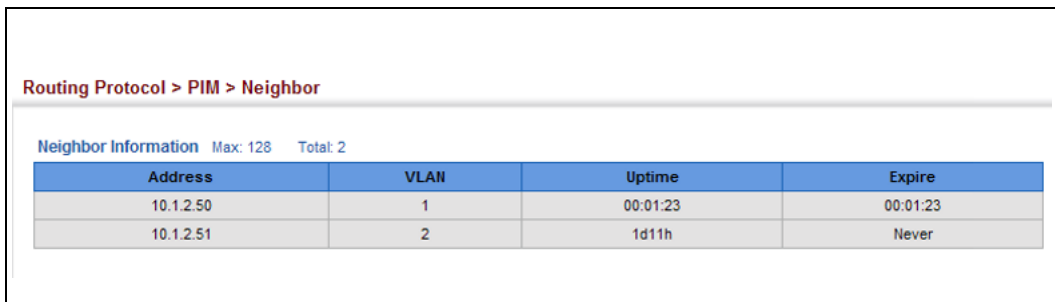
以下のパラメータが表示されます。

- ・ IP Address – ネクストホップルータの IP アドレス。
- ・ VLAN – ネイバールータに接続している VLAN。
- ・ Uptime – このエントリがアクティブな期間。
- ・ Expire – このエントリが削除されるまでの時間。

Web インターフェース

PIM ネイバールータを表示するには、以下のようにします。

- (1) 「Routing Protocol」→「PIM」→「Neighbor」を選択します。



Routing Protocol > PIM > Neighbor			
Neighbor Information Max: 128 Total: 2			
Address	VLAN	Uptime	Expire
10.1.2.50	1	00:01:23	00:01:23
10.1.2.51	2	1d11h	Never

画面 1-359 :PIM ネイバールータの表示

PIM-SM のグローバル設定の設定

「Routing Protocol」→「PIM」→「SM」(Configure Global) を選択すると、Register メッセージの送信間隔、Register メッセージの送信元、および最短パスツリー (SPT) への切り替えを設定することができます。

関連する CLI 情報

「IPv4 PIM Commands」

パラメータ

以下のパラメータが表示されます。

- Register Rate Limit – それぞれの (S,G) エントリの代表ルータ (DR) によって Register メッセージが送信される間隔 (範囲: 1 ~ 65,535 パケット / 秒、デフォルト: Disabled)。

このパラメータを使用すると、代表ルータ (DR) およびランデブーポイント (RP) の負荷を緩和することができます。ただし、Register メッセージは制限値を超えるとドロップされるので、ビジーな送信元から Register メッセージが送信される場合、最初の数秒間に一部の受信先でデータパケット損失が発生する可能性があります。

- Register Source – Register メッセージの IP 送信元アドレスを、RP への戻り時の DR の発信インターフェイスアドレス以外のものに設定します (範囲: VLAN 1 ~ 4,094、デフォルト: RP への戻り時の DR の発信インターフェイスの IP アドレス)。

Register メッセージの送信元アドレスが中間ネットワークデバイスによってフィルタリングされるか、RP がパケットを送信できるアドレスに一意にルーティングされる場合には、RP から送信元アドレスに送信される応答が DR に到達できず、その結果、PIM-SM プロトコル障害が発生します。この種の問題は、Register メッセージの送信元アドレスを RP への戻り時のインターフェイスのアドレスに手動で設定することによって克服することができます。

- SPT Threshold – PIM-SM ラストホップルータが SPT モードに切り替わらないようにします (オプション: Infinity または Reset、デフォルト: Reset (つまり、SPT を使用))。

マルチキャストソースから受信先へのパケットのデフォルトパスは RP を経由します。ただし、RP を経由するパスが必ずしも最短パスであるとは限りません。そのため、新規のマルチキャストグループから最初に受け取ったパケットのみを RP を使用して受信先に転送します。最初のパケットを転送した後、受信先と送信元との間の最短パスを求め、以降は、共有ツリーではなく、最短パスツリー (SPT) を使用して、送信元からのすべてのパケットを受信先に直接送信します。SPT しきい値がこのコマンドによって設定されていない場合、PIM リーフルータは、新規の送信元から最初のパケットを受信した直後に SPT に追加されます。

「SPT Threshold」を指定すると、ルータで、すべてのマルチキャストグループに、または、指定されたマルチキャストグループのみに共有ツリーが使用されるようになります。

- Group Address – IP マルチキャストグループアドレス。グループアドレスが指定されていない場合、すべてのマルチキャストグループに共有ツリーが使用されます。
- Group Mask – グループアドレスに使用されるサブネットマスク。

Web インターフェース

PIM-SM のグローバル設定を設定するには、以下のようにします。

- (1) 「Routing Protocol」 → 「PIM」 → 「SM」 を選択します。
- (2) 「Step」 リストで 「Configure Global」 を選択します。
- (3) 「Register Rate Limit」 を設定し、必要な場合は 「Register Source」 を指定します。
また、SPT に切り替えずに共有ツリーを使用してルーティングする必要があるマルチキャストグループも指定します。
- (4) < Apply > ボタンをクリックします。

The screenshot shows the 'Routing Protocol > PIM > SM' configuration page. The 'Step' dropdown is set to '1. Configure Global'. The configuration options are as follows:

Parameter	Value	Unit / Note
Register Rate Limit (1-65535)	500	packets/sec
Register Source	Enabled, VLAN 1	
SPT Threshold	Infinity	
Group Address	224.1.0.0	(Optional)
Group Mask	255.255.0.0	(Optional)

At the bottom right, there are 'Apply' and 'Revert' buttons.

画面 1-360 :PIM-SM のグローバル設定の設定

BSR 候補の設定

「Routing Protocol」→「PIM」→「SM」(BSR Candidate)を選択すると、スイッチをブートストラップルータ (BSR) 候補として設定することができます。

関連する CLI 情報

「ip pim bsr-candidate」

コマンドの使用

- ・ 本製品を BSR 候補として設定すると、ブートストラップメッセージがすべての PIM-SM ネイバルータに送信されるようになります。代表 VLAN のプライマリ IP アドレスが候補の BSR アドレスとして送信されます。ブートストラップメッセージを受信するそれぞれのネイバルータは、その BSR アドレスと以前に受信したメッセージのアドレスとを比較します。現行のアドレスが同じアドレスまたは上位のアドレスである場合は、そのブートストラップメッセージを受け入れて転送します。そうでない場合は、メッセージをドロップします。
- ・ ルータは、優先度が高い（または、優先度が同じで IP アドレスが大きい）他の候補からメッセージを受信するまで、BSR として稼働し続けます。
- ・ より優れたフェイルオーバーリカバリを実現するため、別々の場所にある少なくとも 2 つのコアルータを選択して、それぞれ、BSR 候補と RP 候補の両方として稼働させることをお勧めします。また、それらのルータの 1 つをプライマリ BSR と RP の両方としてセットアップすることも推奨されます。

パラメータ

以下のパラメータが表示されます。

- ・ BSR Candidate Status - スイッチをブートストラップルータ (BSR) 候補として設定します (デフォルト: Disabled)。
- ・ VLAN ID - 設定済み VLAN の ID (範囲: 1 ~ 4,093)。
- ・ Hash Mask Length - RP 選出プロセスで使用されるハッシュマスク長 (bit 単位) (「ステックランデブーポイントの設定」および「RP 候補の設定」を参照)。この「Hash Mask Length」によって指定されるハッシュ部分はグループアドレスと AND 計算されます。

したがって、ハッシュ機能がいずれかの BSR で実行されると、同じシードハッシュをもつすべてのグループが同じ RP にマップされます。マスク長が 32 bits 以上の場合には、ハッシュの先頭部分のみが使用され、1 つの RP が複数のグループに対して定義されます (範囲: 0 ~ 32、デフォルト: 10)。

- ・ Priority - 選出プロセスで BSR 候補によって使用される優先度。この「Priority」の値が最も大きい BSR 候補が優先されます。「Priority」の値が同じ場合には、IP アドレスが大きい方の候補が BSR になるものとして選出されます。「Priority」を 0 に設定すると、そのルータが BSR として稼働する資格がなくなります。PIM-SM ドメイン内の少なくとも 1 つのルータに 0 よりも大きい値を設定する必要があります (範囲: 0 ~ 255、デフォルト: 0)。

Web インターフェース

スイッチを BSR 候補として設定するには、以下のようにします。

- (1) 「Routing Protocol」 → 「PIM」 → 「SM」 を選択します。
- (2) 「Step」 リストで 「BSR Candidate」 を選択します。
- (3) ルータが BSR 候補であることを宣言する VLAN インターフェース、このルータが BSR として選出されるかどうかを決めるために後で RP 選出プロセスで使用されるハッシュマスク長、および BSR 選出のための優先度を指定します。
- (4) < Apply > ボタンをクリックします。

The screenshot shows the configuration page for BSR Candidate. The breadcrumb is 'Routing Protocol > PIM > SM'. The 'Step' dropdown is set to '2. BSR Candidate'. The configuration fields are as follows:

Field	Value
BSR Candidate Status	☒ Enabled
VLAN ID	1
Hash Mask Length (0-32)	20
Priority (0-255)	200

At the bottom right, there are two buttons: 'Apply' and 'Revert'.

画面 1-361 :BSR 候補の設定

スタティックランデブーポイントの設定

「Routing Protocol」→「PIM」→「SM」(RP Address) を選択すると、スタティックアドレスを特定のマルチキャストグループのランデブーポイント (RP) のアドレスとして設定することができます。

関連する CLI 情報

「ip pim rp-address」

コマンドの使用

- ・ マルチキャストグループが指定されていない場合、ルータは、ローカル PIM-SM ドメイン内のすべてのマルチキャストグループの RP として機能します。スタティック RP は、全マルチキャストグループ範囲 224/4 と特定のグループ範囲のいずれかに対して設定することができます。
- ・ 以前に RP で使用されていた IP アドレスを指定した場合には、古い方のエントリが置き換えられます。
- ・ さまざまな RP をさまざまなグループまたはグループ範囲に対して定義することができます。1 つのグループが複数のエントリにマッチする場合、ルータは、グループプレフィックス長が長い方に関連付けられている RP を使用します。プレフィックス長が同じ場合は、IP アドレスが最も大きいスタティック RP が選択されます。
- ・ スタティック RP アドレスは、ブートストラップルータ (BSR) によって動的に学習される RP アドレスと併せて使用することもできます。あるグループ範囲に対して、BSR によって学習された RP アドレスとこのコマンドを使用して静的に設定された RP アドレスの両方を使用できる場合は、このコマンドを使用して静的に設定された RP アドレスではなく、BSR によって学習された RP アドレスの方が選択されます。
- ・ 同じ PIM-SM ドメイン内のすべてのルータは同じ RP を指定して設定する必要があります。そのため、ダイナミック選出プロセスによる RP の選出は、ほとんどの状況で望ましいものとなります。また、ダイナミック RP 選出プロセスを使用すると、アクティブな RP ルータが使用不可になった場合に自動的にバックアップ RP ルータがその役割を引き継ぐことができるようになります。

パラメータ

- ・ 以下のパラメータが表示されます。
- ・ RP Address - 指定されたマルチキャストグループの RP となるルータのスタティック IP アドレス。
- ・ Group Address - IP マルチキャストグループアドレス。グループアドレスが指定されていない場合、この RP は、すべてのマルチキャストグループで使用されます。
- ・ Group Mask - グループアドレスに使用されるサブネットマスク。

Web インターフェース

スタティックランデブーポイントを設定するには、以下のようになります。

- (1) 「Routing Protocol」→「PIM」→「SM」を選択します。
- (2) 「Step」リストで「RP Address」を選択します。
- (3) マルチキャストグループに使用されるスタティック RP アドレスまたはグループ範囲を指定します (グループ範囲の場合はサブネットマスクも指定します)。

(4) < Apply > ボタンをクリックします。

Routing Protocol > PIM > SM

Step: 3. RP Address Action: Add

RP Address: 192.168.1.1

Group Address: 224.9.0.0 (Optional)

Group Mask: 255.255.255.0 (Optional)

Apply Revert

画面 1-362 : スタティックランデブーポイントの設定

スタティックランデブーポイントを表示するには、以下のようにします。

1. 「Routing Protocol」 → 「PIM」 → 「SM」 を選択します。
2. 「Step」 リストで 「RP Address」 を選択します。
3. 「Step」 リストで 「Show」 を選択します。

Routing Protocol > PIM > SM

Step: 3. RP Address Action: Show

PIM-SM RP Address List Total: 1

	RP Address	Group Address	Group Mask
☐	192.168.1.1	224.9.0.0	255.255.255.0

Delete Revert

画面 1-363 : スタティックランデブーポイントの表示

RP 候補の設定

「Routing Protocol」→「PIM」→「PIM-SM」(RP Candidate)を選択すると、自らをランデブーポイント (RP) としてブートストラップルータ (BSR) にアドバタイズするようにスイッチを設定することができます。

関連する CLI 情報

「ip pim rp-candidate」

コマンドの使用

- ・ 本製品は、RP 候補として設定すると、指定されたグループアドレスについて自らを RP 候補であるとアドバタイズする PIMv2 メッセージを BSR に定期的送信します。代表 VLAN の IP アドレスが候補の BSR アドレスとして送信されます。すると、その BSR は、すべての RP 候補に関する情報を、以降送信されるブートストラップメッセージに挿入するようになります。BSR は、RP 選出ハッシュアルゴリズムを使用して、それぞれのグループ範囲に対してアクティブな RP を選出します。選出プロセスは、BSR が自ら使用するためにのみ、実行します。RP 候補のリストを BSR から受け取るそれぞれの PIM-SM ルータも、同じ選出プロセスを使用して、それぞれのグループ範囲に対してアクティブな RP を選出します。
- ・ 各グループの選出プロセスの基準は、以下のとおりです。
 - ・ 最も明確なグループ範囲が指定されている RP をすべて検出
 - ・ 優先度が最も高い（優先度値が最も小さい）RP を選択
 - ・ ブートストラップメッセージに含まれているグループアドレス、RP アドレス、優先度、およびハッシュマスクに基づいてハッシュ値を計算
 - ・ ハッシュ値が同じ場合には、IP アドレスの値が最も大きい RP 候補を使用
- ・ この分散選出プロセスを使用すると、RP で障害が発生した場合に、収束を迅速に実現し、サービスの中断期間を最小限に抑えることができます。また、グループを複数の RP に分散させるので、負荷分散にも役立ちます。それだけでなく、RP で障害が発生した場合に、それぞれのルータで処理を担当する RP が改めて選出され、グループが自動的に残りの RP に分散されます。
- ・ より優れたフェイルオーバーリカバリを実現するため、別々の場所にある少なくとも 2 つのコアルータを選択して、それぞれ、BSR 候補と RP 候補の両方として稼働させることをお勧めします。また、それらのルータの 1 つをプライマリ BSR と RP の両方としてセットアップすることも推奨されます。

パラメータ

以下のパラメータが表示されます。

- ・ VLAN – 設定済み VLAN の ID（範囲：1 ～ 4,093）。
- ・ Interval – ルータが自らを RP 候補としてアドバタイズする間隔（範囲：60 ～ 16,383 秒、デフォルト：60 秒）。
- ・ Priority – 選出プロセスで RP 候補によって使用される優先度。この「Priority」の値が最も大きい RP 候補が優先されます。「Priority」の値が同じ場合には、IP アドレスが大きい方の候補が RP になるものとして選出されます。「Priority」を 0 に設定すると、そのルータが RP として稼働する資格がなくなります（範囲：0 ～ 255、デフォルト：0）。
- ・ Group Address – IP マルチキャストグループアドレス。指定しない場合、デフォルトのアドレスである 224.0.0.0/4（つまり、IPv4 マルチキャストグループ全体）が使用されます。

- ・ Group Mask - グループアドレスに使用されるサブネットマスク。

Web インターフェース

スイッチを RP 候補としてアドバタイズするには、以下のようにします。

- (1) 「Routing Protocol」 → 「PIM」 → 「PIM-SIM」 を選択します。
- (2) 「Step」 リストで 「RP Candidate」 を選択します。
- (3) VLAN インターフェース、ルータが自らを RP 候補としてアドバタイズする間隔、選出プロセスで使用される優先度、ルータが RP 候補であることを宣言するグループを示すマルチキャストグループアドレスとアドレスマスクを指定します。
- (4) < Apply > ボタンをクリックします。

The screenshot shows a web configuration page titled "Routing Protocol > PIM > SM". Below the title, there is a "Step:" dropdown menu set to "4. RP Candidate" and an "Action:" dropdown menu set to "Add". The main configuration area contains several fields: "VLAN" with a value of "1", "Interval (60-16383)" with a value of "60" and "sec (Optional)", "Priority (0-255)" with a value of "100" and "(Optional)", "Group Address" with a value of "224.0.0.0" and "(Optional)", and "Group Mask" with a value of "255.0.0.0" and "(Optional)". At the bottom, there is a note: "Note: If the group prefix is not defined, the default 224.0.0.0 240.0.0.0 is used." and two buttons: "Apply" and "Revert".

画面 1-364 :RP 候補の設定

RP 候補の設定を表示するには、以下のようにします。

1. 「Routing Protocol」 → 「PIM」 → 「PIM-SIM」 を選択します。
2. 「Step」 リストで 「RP Candidate」 を選択します。
3. 「Step」 リストで 「Show」 を選択します。

Web 設定

マルチキャストルーティング

4. 「VLAN」リストでインターフェースを選択します。

Routing Protocol > PIM > SM

Step: 4. RP Candidate Action: Show

VLAN 1

Interval 60

Priority 100

PIM-SM RP Candidate Group List Max: 128 Total: 1

Group Address	Group Mask
224.0.0.0	255.0.0.0

Delete

画面 1-365 :RP 候補の設定の表示

ブートストラップルータの表示

「Routing Protocol」→「PIM」→「SM」(Show Information - Show BSR Router) を選択すると、ブートストラップルータ (BSR) に関する情報を表示することができます。

関連する CLI 情報

「show ip pim bsr-router」

パラメータ

以下のパラメータが表示されます。

- ・ IP Address - BSR として設定されているインターフェースの IP アドレス。
- ・ Uptime - BSR が稼働状態になってからの時間。
- ・ Priority - BSR 候補で使用されている優先値。
- ・ Hash Mask Length - この BSR 候補によるマルチキャストグループ比較マスクで使用されている上位ビットの数。
- ・ Expire - BSR がダウンしているものとして宣言されるまでの時間。
- ・ Role - BSR 候補であるかどうか。
- ・ State⁹ - BSR の稼働状態として、以下のものが表示されます。
 - ・ No information - 情報が一切保存されていない状態です。
 - ・ Accept Any - アクティブな BSR を認識していない状態であり、最初に受信するブートストラップメッセージに新しい BSR の ID と RP-set (RP 候補のリスト) が含まれているものとみなし、そのメッセージを受け入れます。
 - ・ Accept Preferred - 現行の BSR の ID を認識しており、その BSR から提供される RP-set を使用しています。その BSR からのブートストラップメッセージまたは、現行の BSR よりも重みが大きい C-BSR からのブートストラップメッセージのみが受け入れられます。
 - ・ Candidate BSR - 選出プロセスに参加中です。
 - ・ Pending-BSR - このルータは RP-set で BSR となる候補です。現在、他に優先される BSR はありませんが、まだ BSR として選出されていません。
 - ・ Elected BSR - BSR として稼働するように選出されました。

Web インターフェース

BSR に関する情報を表示するには、以下のようにします。

- (1) 「Multicast」→「Multicast Routing」→「SM」を選択します。
- (2) 「Step」リストで「Show Information」を選択します。
- (3) 「Step」リストで「Show BSR Router」を選択します。

Web 設定

マルチキャストルーティング

**9. これらのパラメータは RFC 5059 に基づくものです。

Routing Protocol > PIM > SM

Step: 5. Show Information ▼ Action: Show BSR Router ▼

IP Address	10.10.11.35
Uptime	00:11:12
Priority	0
Hash Mask Length	10
Expire	00:01:32
Role	Non-Candidate BSR
State	Accept Preferred

画面 1-366 :BSR に関する情報の表示

RP マッピングの表示

「Routing Protocol」→「PIM」→「SM」(Show Information – Show RP Mapping) を選択すると、アクティブな RP とそれに関連付けられているマルチキャストルーティングエントリを表示することができます。

関連する CLI 情報

「show ip pim rp mapping」

パラメータ

以下のパラメータが表示されます。

- ・ Groups – マルチキャストグループアドレス。
- ・ RP Address – 表示されているマルチキャストグループの RP の IP アドレス。
- ・ Information Source – マッピング、RP が選出された方法 (「Static」または「Bootstrap」)、および選出プロセスで使用される優先度をアドバタイズした RP。
- ・ Uptime – RP が稼働状態になってからの時間。
- ・ Expire – このエントリが削除されるまでの時間。

Web インターフェース

マルチキャストグループにマップされている RP を表示するには、以下のようになります。

- (1) 「Multicast」→「Multicast Routing」→「SM」を選択します。
- (2) 「Step」リストで「Show Information」を選択します。
- (3) 「Step」リストで「Show RP Mapping」を選択します。

Routing Protocol > PIM > SM

Step: 5. Show Information Action: Show RP Mapping

RP Mapping Information List Total: 2

Groups	RP Address	Information Source	Uptime	Expire
172.16.0.0/16	10.6.6.6	10.6.6.6, via bootstrap, priority 0	22:36:49	00:02:04
192.168.0.0/24	10.9.9.9	10.9.9.9, via bootstrap, priority 0	22:36:20	00:03:27

Clear

画面 1-367 :RP マッピングの表示

1.19.4 IPv6 PIM の設定

ここでは、IPv6 PIM-DM を設定する方法について説明します。

グローバルでの PIM の有効化

「Routing Protocol」→「PIM6」→「General」を選択すると、IPv6 PIM ルーティングをルータでグローバルに有効にすることができます。

関連する CLI 情報

「router pim6」

コマンドの使用

- ・ この機能は、IPv6 PIM-DM をルータでグローバルに有効にします。その際、マルチキャストルーティングをサポートするインターフェースごとに PIM-DM を有効にし、マルチキャストプロトコルパラメータに適宜変更を加えることも必要になります。
- ・ PIMv6 を使用するには、スイッチで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（「グローバルでのマルチキャストルーティングの有効化」を参照）。
- ・ マルチキャストルーティングを使用する場合は、デバイスのいずれのインターフェースでも MLD プロキシを有効にすることはできません（「MLD Proxy Routing」を参照）。

Web インターフェース

PIMv6 マルチキャストルーティングを有効にするには、以下のようになります。

- (1) 「Routing Protocol」→「PIM6」→「General」を選択します。
- (2) 「PIM6 Routing Protocol」で「Enabled」チェックボックスをオンにします。
- (3) < Apply > ボタンをクリックします。



Routing Protocol > PIM6 > General

PIM6 Routing Protocol ☒ Enabled

Apply Revert

画面 1-368 :PIMv6 マルチキャストルーティングの有効化

PIM インターフェース設定の設定

「Routing Protocol」→「PIM6」→「Interface」を選択すると、それぞれのインターフェースのルーティングプロトコルの機能属性を設定することができます。

関連する CLI 情報

「IPv6 PIM-DM Commands」

コマンドの使用

- ・ PIM-DM は、アクティブなマルチキャストサーバからのトラフィックを定期的にネットワークにフロードして、DVMRP と同じように機能します。また、PIM-DM では、MLD を使用して、マルチキャストグループメンバーが存在しているかどうかを判別されます。DVMRP との主な違いは、PIM-DM では、ルータのユニキャストルーティングテーブルを使用して、パケットの受信に使用されたインターフェースが送信元への最短パスを提供するかどうかを判別されるということです。
- ・ Dense モードインターフェースは、デフォルトで、マルチキャストフラッディングに従い、グループメンバーまたはダウンストリームルータが存在していないことがルータによって確認された場合、または、Prune メッセージがダウンストリームルータから受信された場合にのみ、マルチキャストルーティングテーブルから削除されます。
- ・ PIMv6 プロキシと MLD プロキシを併用することはできません。PIMv6 Dense モードを使用するようにインターフェースを設定する場合は、デバイスのいずれのインターフェースでも MLD プロキシを有効にすることはできません（「MLD Proxy Routing」を参照）。また、あるインターフェースで MLD プロキシが有効になっている場合には、いずれのインターフェースでも PIMv6 を有効にすることはできません。

パラメータ

以下のパラメータが表示されます。

- ・ VLAN – レイヤ 3 の VLAN インターフェース（範囲：1 ～ 4,093）。
- ・ Mode – PIMv6 ルーティングモード（オプション：Dense、Sparse、None）。
- ・ IP Address – 選択された VLAN に割り当てられている IPv6 リンクローカルアドレス。
- ・ Hello Holdtime – PIM ネイバールータがダウンしていることを宣言する前にそのルータからの Hello メッセージを待機する時間を設定します。この「Hello Holdtime」は、「Hello Interval」の値と同じか、それ以上でなければならず、そうでない場合は自動的に「Hello Interval」の 3.5 倍に設定されます（範囲：1 ～ 65,535 秒、デフォルト：105 秒または「Hello Interval」（設定されている場合）の 3.5 倍）。
- ・ Hello Interval – すべてのインターフェースにおける PIM Hello メッセージの送信間隔を設定します（範囲：1 ～ 65,535 秒、デフォルト：30 秒）。

Hello メッセージは、受信したプローブの送信元の PIM ネイバールータに送信され、それらのネイバールータがまだマルチキャストツリーのアクティブなメンバーであるかどうかを確認するために使用されます。PIM-SM ルータは、Hello メッセージを、ネイバールータが存在しているかどうかを確認するためだけでなく、各 LAN セグメントのどのルータが代表ルータ（DR）として稼働しているかを判別するためにも使用します。

ルータは、Boot 時、または PIM を使用するように最初に設定されたときには、初回 Hello メッセージを送信し、それから、Hello タイマーを指定の値に設定します。「Hello Holdtime」で指定されている期間、ネイバールータからメッセージが送信されてこなければ、ルータは、そのネイバールータをドロップします。この保留時間の値は、ネイバールータから受信する各 Hello メッセージに含まれています。また、Hello

メッセージにはメッセージの送信元のルータの DR 優先度も含まれるということにも注意してください。

「Hello Holdtime」が既に設定されており、「Hello Interval」が「Hello Holdtime」よりも大きい場合、このコマンドは失敗します。

- ・ Join/Prune Holdtime – Prune 状態を維持する期間を設定します（範囲：1 ～ 65,535 秒、デフォルト：210 秒）。
 - ・ PIM-DM – 特定の送信元から初めてマルチキャストストリームを受信したマルチキャストインターフェースは、そのトラフィックをルータ上の他のすべての PIM-DM インターフェースに転送します。そのインターフェースにトラフィックを要求しているグループがない場合、リーフノードは、Prune メッセージをアップストリームに送信し、そのマルチキャストストリームについて Prune 状態になります。Prune 状態は、「Join/Prune Holdtime」が経過するまで、または、転送先エントリに関する Graft メッセージが受信されるまで、維持されます。
 - ・ PIM-SM – 特定の送信元から初めてマルチキャストストリームを受信したマルチキャストインターフェースは、そのトラフィックを、ルータ上で、該当のグループへの加入を要求しているインターフェースのみに転送します。そのインターフェースにトラフィックを要求しているグループが既に存在していない場合、リーフノードは、Prune メッセージをアップストリームに送信し、そのマルチキャストストリームについて Prune 状態になります。この (S, G) (送信元とグループ) の組み合わせについて、現在の Join 状態と Pending RPT Prune 状態の両方が、「Join/Prune Holdtime」が経過するまで維持されます。
- ・ LAN Prune Delay – このデバイスが Prune 要求を受信してからフローをプルーンするまでの待機時間がダウンストリームルータに通知されるようにします（デフォルト：Disabled）。

同じ VLAN 上の他のダウンストリームルータは、このアップストリームルータが Prune 要求を受信したことを通知された場合、フローを引き続き受信したければ、この「LAN Prune Delay」期間が経過する前に Join メッセージを送信して Prune メッセージをオーバーライドする必要があります。このコマンドによって生成されるメッセージを使用すると、フローを受信したホストをダウンストリームのネイバルルータに通知して、それらのルータが Join メッセージを返すという処理が効率的に実行されるようになります。この「LAN Prune Delay」期間を過ぎても Join メッセージが受信されない場合、ルータはフローをプルーンします。

「LAN Prune Delay」は、「Override Interval」と「Propagation Delay」の合計に基づいて求められます。

- ・ Override Interval – ダウンストリームルータが LAN Prune Delay メッセージで示されているフローを引き続き受信する場合に Join メッセージを戻すことによって LAN Prune Delay メッセージに応答するために必要な時間（範囲：500 ～ 6,000 ms、デフォルト：2,500 ms）。

「LAN Prune Delay」は、「Override Interval」と「Propagation Delay」に基づいて求められます。この「Override Interval」は、LAN Prune Delay メッセージで示されているフローを引き続き受信したいグループメンバーがダウンストリームルータにいる場合に、ダウンストリームルータが LAN Prune Delay メッセージを処理してから Join メッセージを送信することによってアップストリームルータに回答してフローが終了されないようにするために必要な時間を表わします。

- ・ Propagation Delay – LAN Prune Delay メッセージがダウンストリームルータに到達するために必要な時間（範囲：100 ～ 5,000 ms、デフォルト：500 ms）。

「LAN Prune Delay」は、「Override Interval」と「Propagation Delay」に基づいて求められます。この「Propagation Delay」は、LAN Prune Delay メッセージで示されているフローを引き続き受信したいグループメンバーがダウンストリームルータにいる場合に、LAN Prune Delay メッセージがアップストリームルータから同じ VLAN インターフェイスに接続しているすべてのダウンストリームルータに伝搬されるために必要な時間を表わします。

- ・ Trigger Hello Delay – ルータが Reboot されてから、またはインターフェイスで PIM が有効化されてからトリガーされた PIM Hello メッセージの送信が開始されるまでの最大時間（範囲：0 ～ 5 秒、デフォルト：5 秒）。

ルータを初めて始動するか、インターフェイスで PIM を有効にすると、Hello 遅延が 0 から「Trigger Hello Delay」の間のランダムな値に設定されます。そのようにすることで、複数のルータが同時に電源オンにされた場合にマルチアクセスリンクで Hello メッセージが同期されないようにしています。

また、ルータは、新規ルータから Hello メッセージを受信すると、0 から「Trigger Hello Delay」の間のランダムな値に設定されている遅延期間が経過してから自らの Hello メッセージを送信します。

- ・ Graft Retry Interval – Graft メッセージを再送信する前に Graft 肯定応答メッセージを待機する期間（範囲：1 ～ 10 秒、デフォルト：3 秒）。

Graft メッセージは、Prune 状態を解除するためにルータが送信します。ルータは、Graft メッセージを受信した場合には、Graft 肯定応答メッセージを返す必要があります。肯定応答メッセージがない場合、Graft メッセージを送信したルータは、何回か（「Max. Graft Retries」で指定されている回数）Graft メッセージ再送信します。

- ・ Max. Graft Retries – 肯定応答がない場合の Graft メッセージの最大再送回数（範囲：1 ～ 10、デフォルト：3）。

- ・ State Refresh Origination Interval – PIM-DM State Refresh Control（PIM-DM 状態リフレッシュ制御）

メッセージの送信間隔（範囲：1 ～ 100 秒、デフォルト：60 秒）。

Prune 状態は約 3 分間ごとにタイムアウトになり、マルチキャストパケットと Prune メッセージが PIM-DM ネットワーク全体に再びフローされます。状態リフレッシュ機能では、制御メッセージを配信ツリーのダウンストリームへ定期的に転送することにより、ツリー内の各ルータの発信インターフェイスの Prune 状態をリフレッシュして、Prune 状態がタイムアウトにならないようにします。また、そのようにすると、デフォルトの 3 分間のタイムアウト期間が経過する前に PIM ルータがトポロジの変更（マルチキャストグループに対する送信元の加入または脱退）を認識できるようになります。

このコマンドは、マルチキャストグループの送信元メンバーに直接接続するファーストホップの PIM-DM ルータのインターフェイスについてのみ有効です。

Web インターフェース

PIMv6 インターフェース設定を設定するには、以下のようにします。

- (1) 「Routing Protocol」 → 「PIMv6」 → 「Interface」 を選択します。
- (2) プロトコルパラメータを必要に応じて変更します。
- (3) < Apply > ボタンをクリックします。

Routing Protocol > PIM6 > Interface

VLAN	1
Mode	Dense
IPv6 Address	FE80::200:E8FF:FE90:0
Hello Holdtime (1-65535)	105 sec
Hello Interval (1-65535)	30 sec
Join/Prune Holdtime (1-65535)	210 sec
LAN Prune Delay	☐ Enabled
Override Interval (500-6000)	2500 msec
Propagation Delay (100-5000)	500 msec
Trigger Hello Delay (0-5)	5 sec
Graft Retry Interval (1-10)	3 sec
Max. Graft Retries (1-10)	3
State Refresh Origination Interval (1-100)	60 sec

画面 1-369 :PIMv6 インターフェース設定の設定（Dense モード）

ネイバールータに関する情報の表示

「Routing Protocol」→「PIM6」→「Neighbor」を選択すると、すべての PIM6 ネイバールータを表示することができます。

関連する CLI 情報

「show ip pim neighbor」

パラメータ

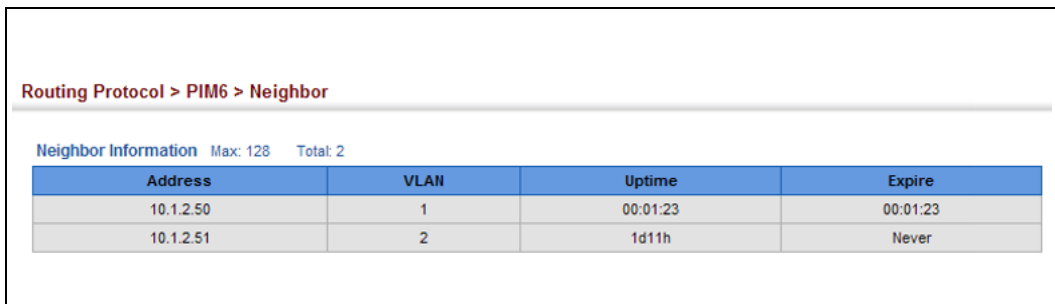
以下のパラメータが表示されます。

- ・ IP Address – ネクストホップルータの IP アドレス。
- ・ VLAN – ネイバールータに接続している VLAN。
- ・ Uptime – このエントリがアクティブな期間。
- ・ Expire – このエントリが削除されるまでの時間。

Web インターフェース

PIMv6 ネイバールータを表示するには、以下のようにします。

- (1) 「Routing Protocol」→「PIM6」→「Neighbor」を選択します。



Routing Protocol > PIM6 > Neighbor			
Neighbor Information Max: 128 Total: 2			
Address	VLAN	Uptime	Expire
10.1.2.50	1	00:01:23	00:01:23
10.1.2.51	2	1d11h	Never

画面 1-370 :PIMv6 ネイバールータの表示

Web 設定

マルチキャストルーティング

FXC9324XG Management Guide(WEB) (FXC13-DC-200028-R1.1)

初版

2013 年 11 月

- ◆ 本ユーザマニュアルは、FXC 株式会社が制作したもので、全ての権利を弊社が所有します。弊社に無断で本書の一部、または全部を複製 / 転載することを禁じます。
 - ◆ 改良のため製品の仕様を予告なく変更することがありますが、ご了承ください。
 - ◆ 予告なく本書の一部または全体を修正、変更することがありますが、ご了承ください。
 - ◆ ユーザマニュアルの内容に関しましては、万全を期しておりますが、万一ご不明な点がございましたら、弊社サポートセンターまでご相談ください。
-

**Management Guide
FXC9324XG**

**Management Guide
FXC9324XG**

**Management Guide
FXC9324XG**

**Management Guide
FXC9324XG**

**Management Guide
FXC9324XG**

**Management Guide
FXC9324XG**

**Management Guide
FXC9324XG**

**Management Guide
FXC9324XG**

**Management Guide
FXC9324XG**

**Management Guide
FXC9324XG**

**Management Guide
FXC9324XG**

**Management Guide
FXC9324XG**

**Management Guide
FXC9324XG**