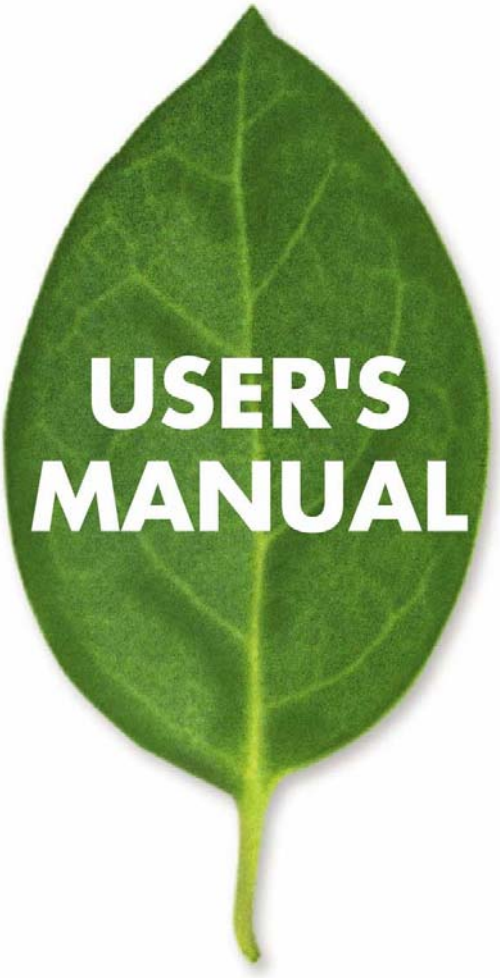



24 ポートスタッカブルスイッチ

# SF-0224FS

PLANEX COMMUNICATIONS INC.

# 第1章 はじめに

本製品は、レイヤ2スイッチング機能を幅広く取り揃えており、本書にて解説している各機能を設定するための管理エージェントを搭載しています。本製品の提供する機能のほとんどは、初期設定の状態でもご利用いただけますが、必要に応じて各機能のオプション設定を変更することにより、ご利用のネットワーク環境において最大限の性能を発揮できるようになります。

## 1-1 特長

表1-1 主な機能

| 機能 | 内容 |
|---|---|
| 設定のバックアップおよび復元 | TFTPサーバに設定内容をバックアップ及び復元します。(TFTPサーバへのアップ/ダウンロード) |
| 認証 | • コンソール、TelnetおよびWEB:ユーザ名/パスワード、RADIUSおよびTACACS+<br>• Web:SSL/HTTPS<br>• Telnet:SSH<br>• SNMP v1/2c:コミュニティストリング<br>• ポート:IEEE802.1X、MACアドレスフィルタリング |
| ACL (アクセスコントロールリスト) | 最大88個のIPないしMAC ACLに対応 |
| DHCPクライアント | 対応 |
| ポート設定 | 速度、デュープレックスモードおよびフローコントロールを設定可能 |
| 速度制限 | ポートごとに入出力の各速度を制限可能 |
| ポートミラーリング | いずれか一つのポート上の内容を他の分析用ポート(×1)にミラーリング |
| ポートトランキング | 固定ないし動的トランク(LACP)、最大4トランクまで対応(IEEE802.3ad対応) |
| ブロードキャストストームコントロール | 対応 |
| 固定アドレス | フォワーディング(転送)テーブル内にて最大8000個までのMACアドレスに対応 |
| IEEE802.1Dブリッジング | 動的なデータスイッチングならびにアドレス学習に対応 |
| ストア・アンド・フォワードスイッチング | 不良フレームを排除しつつワイヤスピードでの |

| | |
|---|---|
| | スイッチングを実現 |
| スパニングツリーアルゴリズム | 標準のSTPならびにRSTP(ラピッドスパニングツリープロトコル)に対応 |
| VLAN | IEEE802.1Qポートベース/プライベートVLAN、最大255までのVLANに対応 |
| トラフィックの優先度設定 | ポート初期優先度、トラフィッククラスマップ、キュースケジュール、IP優先度ないしDSCP(差別サービスコードポイント)およびTCP/UDPポート |
| マルチキャストフィルタリング | IGMPスヌーピングおよびクエリに対応 |

# ソフトウェア搭載機能

本製品は、通信性能を向上させるための機能を幅広く取り揃えております。

フローコントロールは、ポート上でパケットが一杯となること(ボトルネック)により起こるパケットの損失を回避するほか、ブロードキャストストーム抑制(制御)はブロードキャストトラフィックストームによってネットワークが圧倒されてしまうといった事態を防止します。ポートベース/プライベートVLANならびに自動GVRP VLAN登録機能は、トラフィックを保護し、またネットワーク帯域幅のより効率的な利用を可能とします。CoS優先度別キュー機能は、リアルタイム性の要求されるマルチメディアデータをネットワーク上で移動する際の遅延を最小限にとどめます。また、マルチキャストフィルタリングはリアルタイム性の求められるネットワークアプリケーションに対応します。以下に、本製品に搭載されている管理機能のいくつかを簡単に紹介します。

■設定のバックアップおよび復元
現在の設定内容をファイルとしてTFTPサーバに保存し、後で同設定が必要となったときにこれをダウンロードし、設定を復元します。

■認証
本製品は、コンソールポート、Telnetおよびブラウザを介し管理アクセスを認証します。

ユーザ名およびパスワードはローカルで設定できるほか、リモート認証サーバ(RADIUS、TACACS+など)にて認証することも可能となっています。IEEE802.1Xプロトコルを使ったポートベースの認証にも対応しております。同プロトコルはEAPOLを使用することにより802.1Xクライアントに対しユーザ認証情報を要求し、認証サーバを介して同クライアントのネットワークに対するアクセス権限を確認します。

他の認証オプションとしては、

1)WEB経由での安全な管理アクセスを実現するHTTPS

2)Telnet同等接続での安全な管理アクセスを可能とするSSH

3)SNMP/WEB/Telnet管理アクセス用のIPアドレスフィルタリング

4)ポートアクセス用のMACアドレスフィルタリング

などが含まれます。

■ACL (アクセス制御リスト)
ACLは、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、TCP/UDP番号ないしTCP制御モードのいずれかに基づく)ないし、すべてのフレームのパケットフィルタリング(MACアドレスないしイーサネットの種類に基づく)を行います。ACLは、不要なネットワークトラフィックを遮断することにより、また特定のネットワーク資源やプロトコルへのアクセスを限定するセキュリティ管理を行うことにより、ネットワークの通信性能を改善します。

■ポート設定

特定ポートの速度、デュープレックスモードおよびフローコントロール設定を手動で変更できるようになっているほか、オートネゴシエーションを使って最適な設定内容を自動的に検出することも可能です。可能な限り、ポートでは全二重モードを有効にしてスイッチ接続上のスループットを倍増させたほうがよいでしょう。またフローコントロールを有効にすると、通信が混雑している間ネットワークトラフィックを制御したり、ポートバッファ限界量の超過によるパケットの損失をあらかじめ防止する、といったことが可能となります。本製品は、IEEE802.3x標準に基づいたフローコントロールに対応しています。

■速度制限

指定インタフェース上における、トラフィックの最大送受信速度を制御します。

ネットワークを出入りするトラフィックを制限するため、速度制限(Rate Limiting)はネットワークの末端にあたるインタフェース上で設定を行います。速度制限を下回るトラフィックは送信が許可され、逆に許容量を超えるパケットは廃棄されるかたちになります。

■ポートミラーリング

本製品は、いずれか指定のポートからモニタ(観測用)ポートに流れるトラフィックを透過的にミラーリング(コピー)することが可能です。同モニタポートにプロトコルアナライザかRMONプローブを接続することにより、トラフィックを解析し接続の整合性を確認することが可能となります。

■ポートトランキング

ポートを複数束ねることによりトランク接続を構成します。

トランクは手動で構成できるようになっているほか、IEEE802.3ad LACPにて動的に構成することも可能です。複数のポートを使った接続となるため、通常の単一ポートを使った場合

と比べスループットが飛躍的に向上するほか、トランク内のポートいずれかが動作不能となっても残りのポートが送信を引き継ぐため、冗長性も同時に確保します。

■固定アドレス

本製品上の指定インタフェース上に固定のアドレスを割り当てます。

割り当てられたアドレスは該当インタフェース固定となり、移動することはありません。他インタフェース上で固定アドレスが認められた場合、同アドレスは無視されアドレステーブルにも書き込まれません。固定アドレスは、特定ポートを使った既知のホストへのアクセスを制限することによりご使用ネットワークのセキュリティをさらに強化します。

■IEEE802.1Dブリッジング

本製品はIEEE802.1D透過ブリッジングに対応しています。

アドレステーブルは、アドレスを学習し、さらに同情報に基づきトラフィックをフィルタないし転送することによりデータスイッチングを円滑に行います。アドレステーブルは8000個までのアドレスに対応しています。

■ストア・アンド・フォワーディングスイッチ方式

本製品は各フレームを他ポートに転送する前にそのコピーをメモリ上に保管します。

このため、フレームがすべてイーサネット標準のサイズであること、またCRCチェックに合格した整合性のあるものであることが確認できるようになっています。結果、ネットワークに不良フレームが混入し帯域幅が無駄に失われる、といった事態を防ぐことが可能です。

混雑の発生するポート上でフレームの損失を避けるため、本製品は8MBのフレームバッファを搭載しています。同バッファにより、混雑しているネットワーク上で送信待ちとなっているパケットを順番に並べ確保することが可能となります。

■スパニングツリーアルゴリズム

本製品は以下のスパニングツリー機能をサポートしています。

・スパニングツリープロトコル(STP、IEEE802.1D)

ループの検出を行うほか、LANセグメント2点間において2つないしそれ以上の冗長接続を設けることにより経路を復帰させることが可能です。セグメント間に物理経路が複数存在する場合、本プロトコルはこのうちいずれか1つの経路を選択し、残りすべての経路を無効とし、ネットワーク上のステーション2台の間で常に経路が1つだけ存在するようにします。このためネットワーク上でループの発生(作成)を予め防止することが可能となります。ただし選択された経路が何らかの理由により動作不能となった場合は、代行用の経路いずれか1つを有効にし、接続を維持します。

・ラピッドスパニングツリープロトコル(RSTP、IEEE802.1w)

従来のIEEE802.1D STP規格は、ネットワークのトポロジが変化する際の収束時間として30秒ほどを要しますが、RSTPでは同時間がわずか3～5秒となります。RSTPはSTPに完全に取って代わる後継プロトコルとして設計されていますが、接続先機器上で従来のSTPプロトコル用メッセージを検出した場合は該当ポートをSTP準拠用として自動的に再設定しますので、従来のSTP規格との相互運用も可能です。

■VLAN

本製品は最大255個までのVLANグループに対応しています。

VLANとは、ネットワーク内における実際の物理的な場所や接続ポイントの位置に関わりなく、同一のコリジョンドメインを共有するネットワークノードを集めたものを指します。本製品はIEEE802.1Q標準に基づいたタグ付きVLANをサポートしています。VLANグループのメンバーはGVRPにて自動的に学習できるようになっているほか、手動で特定のVLANに割り当てることも可能です。VLANを使用することにより、本製品側でトラフィックをユーザの割り当てられているVLANにのみに制限することが可能となります。ネットワークを複数のVLANに分割することにより以下の利点が得られます。

・通常のネットワークにおいて通信性能を著しく低下させるブロードキャストストームを排除します。

・ノードの変更および移動などを行った際のネットワークの管理が大幅に簡単になります。いずれのポートにおいてもそのVLANメンバー構成を遠隔で設定できますので、実際にネットワーク上の各接続地点に出向いて手動で変更する、といった手間をすべて省くことが可能です。

・トラフィックをすべて発信源であるVLAN内に限定できるため、扱うデータに対しセキュリティを設けることが可能です。
・プライベートVLANを使用することにより、トラフィックをデータポートならびにアップリンクポートのみに制限して通すことが可能です。結果、同一VLAN内で隣接しているポートを隔離し、設定が必要なVLANの合計数を一定数に制限することが可能となります。

## ■トラフィック優先度

本製品はサービスの要求レベルに応じて各パケットに優先度を設定します。

優先度設定は、ストリクト/ウェイトラウンドロビンキュー方式にて4つの優先度キューを使用して行います。その際本製品は、末端ステーション上のアプリケーションからの入力に基づき、IEEE802.1pおよび802.1Qタグを使って着信トラフィックの優先度付けを行います。これらの機能を使用することにより、遅延の許されないデータおよびベストエフォート式データに対し個別に優先度を設定することが可能です。

本製品はまた、レイヤ3/4トラフィックに優先度付けを行いアプリケーション側の要求を満たすための、より一般的な方式いくつかをサポートしています。トラフィックはIPフレームのToS(タイプオブサービス)オクテット内の優先度ビットに基づき、またTCP/UDPポートのポート番号に基づき優先度付けすることが可能です。これらのサービスが有効となっている場合、優先度は本製品によりCoS(クラスオブサービス)値としてマッピングされ、トラフィックも対応する出力キューに送信されるかたちになります。

■マルチキャストフィルタリング

特定のマルチキャストトラフィックを同トラフィック自身のVLANに割り当てることにより、通常のネットワークトラフィックへの干渉が回避できるほか、指定VLAN用の必要な優先度レベルを設定することによりリアルタイムでの転送(配信)が可能となります。本製品はIGMPスヌーピングおよびクエリを使用しマルチキャストグループの登録管理を行います。

# システム初期設定

本製品のシステム初期設定は設定ファイル「Factory_Default_Config.cfg」内に保存されています。システム初期設定をリセットする場合は、同ファイルをスタートアップ設定ファイルとして設定する必要があります(詳細は51ページをご覧ください)。

以下に、基礎的なシステム初期設定値のいくつかを紹介します。

| 表1-2システム初期設定 | | |
|---|---|---|
| 機能 | パラメータ | 初期設定 |
| コンソールポート接続 | Baud Rate<br>ボーレート | 9600 |
| | Data bits<br>データビット | 8 |
| | Stop bits<br>ストップビット | 1 |
| | Parity<br>パリティ | None (なし) |
| | Local Console Timeout<br>ローカルコンソールタイムアウト | 0 (無効) |
| 認証 | Privileged Exec Level<br>優先Execレベル | ユーザ名:admin |
| | | パスワード:admin |
| | Normal Exec Level<br>通常Execレベル | ユーザ名:guest |
| | | パスワード:guest |
| | Enable Privileged Exec from Normal Exec Level (Normal Exec LevelからPrivileged Execを有効にする) | パスワード:super |
| | RADIUS Authentication<br>RADIUS認証 | Disabled (無効) |
| | TACACS Authentication<br>TACACS認証 | Disabled (無効) |
| | 802.1X Port Authentication<br>802.1Xポート認証 | Disabled (無効) |
| | HTTPS | Enabled (有効) |
| | SSH | Disabled (無効) |
| | Port Security<br>ポートセキュリティ | Disabled (無効) |

| | | |
|---|---|---|
| | IP Filtering<br>IPフィルタリング | Disabled (無効) |
| WEB管理 | HTTP Server<br>HTTPサーバ | Enabled (有効) |
| | HTTP Port Number<br>HTTPポート番号 | 80 |
| | HTTP Secure Server<br>HTTPセキュアサーバ | Enabled (有効) |
| | HTTP Secure Port Number<br>HTTPセキュアポート番号 | 443 |
| SNMP | Community Strings<br>コミュニティストリング | public (リードオンリー)<br>private (リード/ライト) |
| | Traps<br>トラップ | Authentication traps(認証とラップ):enabled (有効)<br>Link-up-down events (リンクアップ/ダウンイベント):enabled (有効) |
| ポート設定 | Admin Status<br>管理ステータス | Enabled (有効) |
| | Auto-negotiation<br>オートネゴシエーション | Enabled (有効) |
| | Flow Control<br>フローコントロール | Disabled (無効) |
| 速度制限 | Input and Output Limits<br>入力/出力制限 | Disabled (無効) |
| ポートトランク | Static Trunks<br>固定トランク | None (なし) |
| | LACP (全ポート) | Disabled (無効) |
| ブロードキャストストーム防止 | Status<br>ステータス | Disabled (無効) |
| | Broadcast Limit Rate<br>ブロードキャスト制限速度 | 32,000 octets per second<br>32,000オクテット/秒 |

| | | |
|---|---|---|
| スパニングツリーアルゴリズム | Status<br>ステータス | Enabled (有効)<br>(初期設定:全ての値はIEEE802.1wに準拠) |
| | Fast Forwarding (Edge Port)<br>高速転送(エッジポート) | Disabled (無効) |
| アドレステーブル | Aging Time<br>エージングタイム | 300 seconds (300秒) |
| VLAN | Default VLAN<br>初期VLAN | 1 |
| | PVID | 1 |
| | Acceptable Frame Type<br>許容フレームタイプ | All<br>すべて |
| | Ingress Filtering<br>着信フィルタリング | Disabled (無効) |
| | Switchport Mode (Egress Mode)<br>スイッチポートモード(送信モード) | Hybrid:tagged/untagged frames<br>ハイブリッド:タグ付/タグ無しフレーム |
| | GVRP(global)<br>GVRP(グローバル) | Disabled (無効) |
| | GVRP(port interface)<br>GVRP(ポートインタフェース) | Disabled (無効) |
| トラフィック優先度 | Ingress Port Priority<br>着信ポート優先度 | 0 |
| | Weighted Round Robin<br>ウェイトラウンドロビン | キュー:0 1 2 3<br>重量:1 2 4 6 |
| | IP Precedence Priority<br>IP優先度 | Disabled (無効) |
| | IP DSCP Priority<br>IP DSCP優先度 | Disabled (無効) |
| | IP Port Priority<br>IPポート優先度 | Disabled (無効) |
| IP設定 | IP Address<br>IPアドレス | 0.0.0.0 |

| | | |
|---|---|---|
| | Subnet Mask<br>サブネットマスク | 255.0.0.0 |
| | Default Gateway<br>デフォルトゲートウェイ | 0.0.0.0 |
| | DHCP | クライアント:Enabled (有効) |
| | BOOTP | Disabled (無効) |
| マルチキャストフィルタリング | IGMP Snooping<br>IGMPスヌーピング | スヌーピング:有効<br>クエリア:有効 |
| システムログ | Status<br>ステータス | Enabled (有効) |
| | Messages Logged<br>記録済みメッセージ | レベル0-7 (すべて) |
| | Messages logged to Flash<br>フラッシュに記録されたメッセージ | レベル0-3 |
| SMTP電子メール警告 | Event Handler<br>イベントハンドラ | Enabled(有効:ただしサーバは無定義) |
| SNTP | Clock Synchronization<br>クロック同調 | Disabled (無効) |

# 第2章　初めて設定を行う場合

## 2-1　本製品に接続する

### 2-1-1　設定オプション

本製品にはネットワーク管理エージェントが内蔵されています。

同エージェントはSNMP、RMONおよびWEBベースインタフェースを含む管理オプションを幅広く取り揃えています。またPCを本製品に直接接続して、設定およびCLI（コマンドラインインタフェース）コマンドによる監視などを行うことも可能です。

注意：

本製品用のIPアドレスは、初期設定ではDHCPにより入手するようになっています。

同アドレスを変更する場合は、p.16の「IPアドレスの変更」をご覧ください。

本製品はHTTP WEBエージェントを搭載しているため、スイッチパラメータの設定やポート接続の監視、統計情報の表示といった作業をMicrosoft Internet Explorer 5.0以上などの標準WEBブラウザを介して実行できるようになっています。本製品のWEB管理インタフェースは、ネットワークに接続されているどのPCからでもアクセス可能です。

CLIプログラムは、本製品上のRS-232シリアルコンソールポートと直接接続してアクセスできるほか、Telnet接続を使いネットワーク経由で遠隔地からアクセスすることも可能となっています。

本製品の管理エージェントはSNMPもサポートしています。

SNMPエージェントを利用することにより、HP OpenViewなどのネットワーク管理ソフトウェアを使って本製品のネットワーク上のどのシステムからでも本製品の管理が可能となります。

本製品のWEBインタフェース、CLI設定プログラムならびにSNMPエージェントを使用することにより、以下の管理機能が利用できるようになります。

- ユーザ名およびパスワードを最大16ユーザ分まで設定
- どのVLANにもIPインタフェースを設定
- SNMPパラメータの設定
- 指定ポートの有効/無効化設定
- 指定ポートの速度/デュープレックス設定を変更

- ポートの入出力速度を制限することによりその帯域幅を制御
- IEEE802.Xセキュリティないし固定アドレスフィルタリングを行うことでポートへのアクセスを制御
- ACLを使ってパケットのフィルタリングを実行
- IEEE802.1Q VLANを最大255グループまで作成
- GVRP自動VLAN登録の有効化
- ユニキャストトラフィック用としてIPルーティングを設定
- IGMPマルチキャストフィルタリングの設定
- システムファームウェアソフトウェアをTFTP経由でダウンロード/アップロード
- スイッチ設定ファイルをTFTP経由でダウンロード/アップロード
- スパニングツリー用パラメータの設定
- CoS優先度キューの設定
- 最大4つまで固定トランクないしLACPトランクを設定
- ポートミラーリングの有効化
- 指定ポート上でブロードキャストストーム制限を実施（設定）
- システム情報ならびに統計を表示
- 同一IPアドレス経由でいずれのスタックユニットも設定可能

## 2-1-2 シリアルポートの接続

本製品上のRS-232シリアルポートにPCないし端末を接続し、本製品の監視および設定を行うことが可能です。本製品パッケージにはヌルモデム・コンソールケーブルが同梱されています。

注意：

スタックの設定を行う場合は、マスタユニットのコンソールポートに接続してください。

VT100互換端末かターミナルエミュレーションプログラムが実行可能なPCを接続します。接続には、本製品に同梱されているコンソールケーブルか、インストールガイドに記載されている配線仕様を満たすヌルモデムケーブルをお使いいただけます。

以下に、コンソールポートに端末を接続する手順を示します。

1. コンソールケーブルを端末か、ターミナルエミュレーションソフトウェアが実行可能なPCのシリアルポートに接続します。次にシリアルコネクタ上の固定用ネジを締めます。（固定用ネジが無い場合もあります）
2. ケーブルのもう一端を本製品のRS-232シリアルポートに接続します。
3. ターミナルエミュレーションソフトウェアが以下のように設定されていることをご確認ください。

- 適切なシリアルポートをお選びください（COMポート1か2）。
- ボーレート：9600bps
- データフォーマット：8データビット、1ストップビット、パリティなし
- フローコントロール：なし
- エミュレーションモード：VT100
- ハイパーターミナルご利用時は、Windowsキーではなくターミナルキーをお使いください。

注意：

1. Windows2000上でハイパーターミナルをお使いの場合は、Windows2000サービスパック2ないしそれ以降のものがインストールされていることをご確認ください。サービスパック2では、ハイパーターミナルのVT100エミュレーション実行時に矢印キーが正常に動作しない不具合が修正されています。Windows2000サービスパック各種につきましては、www.microsoft.comをご覧ください。

2. P.245の「回線コマンド」をご覧の上、コンソール設定オプションの詳細をご確認ください。

3. 端末が正しく設定された時点で、コンソールのログイン画面が表示されます。

CLIの利用方法につきましてはp.235の「コマンドラインインタフェースの使用」をご覧ください。CLIコマンドの一覧および利用方法の詳細についてはp.244の「コマンドグループ」をご覧ください。

## 2-1-3 リモート接続

ネットワーク接続経由で本製品内蔵のエージェントにアクセスする前に、本製品に有効なIPアドレス、サブネットマスクおよびデフォルトゲートウェイを設定しておく必要があります。設定にはコンソール接続、DHCPないしBOOTPプロトコルを使用します。

初期設定では、本製品のIPアドレスはDHCPにより入手されるようになっています。同アドレスを手動で設定する場合や、DHCPないしBOOTPによるダイナミックアドレス割当を有効にする場合は、p.16の「IPアドレスの設定」をご覧ください。

**注意**：　本製品では、TelnetまたはSSHセッションを最大で4セッションまで同時に実行することが可能です。

本製品の各IPパラメータの設定が完了した時点で、接続されているネットワーク内であればどこからでも本製品内蔵の設定プログラムにアクセスすることが可能となります。同設定プログラムはネットワークに接続されているPCいずれかからTelnetにてアクセスできるようになっています。また、本製品はInternet Explorer 5.0以降のWEBブラウザ経由で管理できるほか、SNMPネットワーク管理ソフトウェアを使いネットワーク（上の）PCから管理することも可能です。

注意：

内蔵プログラムでは、基本的な設定機能のみ利用可能となっています。

SNMP管理機能すべてにアクセスする場合は、SNMPベースのネットワーク管理ソフトウェアを使用する必要があります。

## 2-2 スタックの利用

インストレーションガイドにて解説されているように、最大8台までのスイッチをスタックできるようになっています。同スタック内のスイッチのうち1台はマスタとして動作し、設定やファームウェア更新などの役目を担います。スタック内の残りのスイッチはすべてスレーブモードで動作します。

スタック内のユニットいずれかを設定する場合は、マスタユニットから数えた場合のユニット番号をまず確認し、WEBないしコンソール管理インタフェース上で同ユニット番号を選択してください。

### 2-2-1 スタックマスタの選択

ユニットの番号付けを行う際は以下の点にご注意ください。

- スタックに最初に電源を入れた時点で、マスタユニットはユニット1として指定されます。スタックは単純に上から下に向かって番号付けがなされるようになっており、スタック内の最初のユニットがユニット1となります。同ユニット認識番号は、WEBインタフェース上のフロントパネル画像上およびCLI上で選択可能です。
- 本製品前面パネル上のマスタプッシュボタンを使って2台ないしそれ以上のスイッチがマスタとして選択されている場合、スタックは機能しませんのでご注意ください。
- スタック内のユニットいずれか1台が故障するとスタックとして動作しなくなります。故障したユニットは正常なものと好感し、スタックケーブルを接続しなおしてリングトポロジを回復する必要があります。
- スタック内のユニットいずれか1台が故障するかスタックから取り外されても、スタック内の各ユニット番号は変化しません。このため、スタック内でいずれか1台を交換した場合は、故障したユニットのもともとの設定内容がその交換機上で復元されるかたちになります。

### 2-2-2 スタック故障後およびトポロジ変更後の回復手段

スタック内のリンクないしユニットが故障すると、トラップメッセージが送信され故障（不具合）イベントが記録されます。システム上で故障ないしトポロジ変更が発生した時点でスタックは再起動されます。スタックの再起動には2～3分ほどかかります。なお、スタック内のユニットいずれか1台の電源を切ったり、新規にユニットを追加した場合もスタックは再起動するようになっています。

### 2-2-2-1 回復力の強い管理アクセス用IPインタフェース

スタックは、管理および設定を目的とした一体型のシステムとして動作します。このため、IPアドレスの割り当てられているVLAN内のポートであればどのポートでもスタックの管理が行えるようになっています。マスタユニットは、管理アクセスで使用されるVLANインタフェース内の動作中（アクティブ）ポートメンバーを含む（持つ）必要がありません。ただし、管理アクセスを通常行うユニットが故障し、かつ当VLANインタフェース内の他ユニット上でアクティブなポートメンバーが存在しない場合、当IPアドレスは利用できなくなります。故障などのイベント発生時も管理アクセス用の固定IPアドレスを保持する場合は、スタック管理で使用されるプライマリVLAN内のユニットいくつかのポートメンバーをあらかじめ含めておく必要があります。

# 2-3 基本設定

## 2-3-1 コンソール接続

CLIプログラムでは、通常アクセスレベル(Normal Exec)および優先アクセスレベル(Privileged Exec)の2つコマンドレベルが利用できるようになっています。

Normal Execレベルで利用可能なコマンドはPrivileged Execレベルで利用可能なものより数が制限されているほか、基本的なユーティリティのみ使用可能となっており、情報も表示のみとなります。本製品のパラメータすべてに対し設定変更を行う場合は、Privileged Execレベルにて CLIからアクセスを行う必要があります。

これらのCLIレベルはいずれも、ユーザ名およびパスワードで制御を行っています。各レベル用に初期ユーザ名およびパスワードが設定されております。Privileged Execレベルにて、初期ユーザ名ならびにパスワードを使ってCLIにログインする場合は以下の操作を行ってください。

1. Enterキーを押してコンソール接続を開始します。「User Access Verification(ユーザアクセス認証)」プロシージャが始まります。
2. ユーザ名プロンプトで「admin」と入力します。
3. パスワードプロンプトで「admin」と入力します。（入力されたパスワードの内容はコンソール画面上では表示されません。）
4. セッションが開始され、CLIは「Console#」プロンプトを表示します。これでPrivileged Execレベルでのアクセスが可能となります。

## 2-3-2 パスワードの設定

注意：

CLIプログラムに最初にログインする場合は、どちらの初期ユーザ名用のパスワードも

「username」コマンドを使って新しく設定しなおし、同パスワードを記録した上で安全な場所に保存してください。

パスワードは8文字までの半角英数字を使って設定できるようになっています。なお、大文字・小文字の区別を行いますのでご注意ください。本製品への不正アクセスを防止するためにも、以下の手順にてパスワードを設定するようにしてください。

1. コンソールインタフェースを起動し、初期ユーザ名およびパスワード「admin」を使ってPrivileged Execレベルでアクセスします。
2. 「configure」と入力しEnterキーを押します。
3. Normal Execレベル用のパスワードを変更する場合は「username guest password 0 *パスワード*」と入力しEnterキーを押してください。(*パスワード*:新しいパスワード)
4. Privileged Execレベル用のパスワードを変更する場合は「username admin password 0 *パスワード*」と入力しEnterキーを押してください。(*パスワード*:新しいパスワード)

注意: 「0」は通常テキストでパスワードを指定することを意味します。「7」は、パスワードを暗号化形式で指定することを示します。

```
Username: admin
Password:

   CLI session with the 24PORT STACKABLE SWITCH is opened.
   To end the CLI session, enter [Exit].

Console#configure
Console(config)#username guest password 0 [password]
Console(config)#username admin password 0 [password]
Console(config)#
```

## 2-3-3 IPアドレスの設定

ネットワーク経由で本製品に対し管理アクセスを行う場合は、あらかじめ本製品にIPアドレスを設定しておく必要があります。設定は以下のいずれかの方法で行えるようになっています。

■手動設定

IPアドレスおよびサブネットマスクなどを含む情報を入力します。ご使用の管理用ステーションのIPサブネットが本製品のものと異なる場合は、デフォルトゲートウェイルータの指定も行う必要があります。

■動的(自動)設定

本製品は、ネットワーク上のBOOTPないしDHCPアドレス割当サーバに対しIP設定要求を送信します。

### 2-3-3-1 手動設定

本製品に手動でIPアドレスを設定します。また、本製品と他ネットワークセグメント上に存在する管理ステーションとの間に存在するデフォルトゲートウェイの指定が必要となる場合もあります。有効なIPアドレスは、0～255までの10進数数字4つをピリオドで区切ったものとなります。他の形式は当CLIプログラム上で認識されませんのでご注意ください。

**注意**:　　初期設定では、本製品のIPアドレスはDHCPにて入手されるようになっています。

本製品にIPアドレスを割り当てる前に、ネットワーク管理者から以下の情報をあらかじめ入手しておいてください。

- 本製品のIPアドレス
- ネットワークのデフォルトゲートウェイ
- ネットワークのネットワークマスク

以下に、本製品にIPアドレスを割り当てる手順を示します。

1. Privileged Execレベルグローバル設定モードプロンプトで「interface vlan 1」と入力し、インタフェース設定モードにアクセスします。Enterキーを押してください。

2. 「ip address *IPアドレス ネットマスク*」と入力しEnterキーを押してください（*IPアドレス*: 本製品のIPアドレス、*ネットマスク*: ネットワークのネットワークマスク）。

3. 「exit」と入力します。グローバル設定モードプロンプトに戻りますのでEnterキーを押してください。

4. 本製品の所属するネットワークのデフォルトゲートウェイ用IPアドレスを設定する場合は、「ip default-gateway *ゲートウェイ*」と入力しEnterキーを押してください（*ゲートウェイ*: デフォルトゲートウェイのIPアドレス）。

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.5 255.255.255.0
Console(config-if)#exit
Console(config)#ip default-gateway 192.168.1.254
Console(config)#
```

### 2-3-3-2 自動設定

「bootp」ないし「dhcp」オプションを選択した場合、IPは有効となりますがBOOTPないしDHCP応答が受信されるまで機能しないかたちになります。このため、「ip dhcp restart」コマンドを使ってサービス要求をブロードキャスト送信を開始する必要があります。IP設定情報を入手する目的で、要求は定期的に送信されるようになっています。(BOOTPおよびDHCP値には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。)

「bootp」および「dhcp」オプションが起動設定ファイル(startup-configファイル：ステップ6)に保存されていると、本製品は電源投入と同時にサービス要求のブロードキャスト送信を開始します。

ネットワーク上でBOOTPないしDHCPアドレス割当サーバと通信し自動的に本製品の設定を行う場合は、以下の操作を行ってください。

1. グローバル設定モードプロンプトで「interface vlan 1」と入力しインタフェース設定モードにアクセスします。Enterキーを押してください。

2. インタフェース設定モードプロンプトで、以下のうちいずれか1つのコマンドをお使いください。

   - DHCP経由でIP設定を取得する場合は「ip address dhcp」と入力してEnterキーを押してください。
   - BOOTP経由でIP設定を取得する場合は「ip address bootp」と入力しEnterキーを押してください。

3. 「end」と入力してください。Privileged Execモードに戻りますのでEnterキーを押してください。

4. 「ip dhcp restart」と入力し、サービス要求のブロードキャスト送信を開始してください。Enterキーを押してください。

5. 数分ほどお待ちください。次に「show ip interface」コマンドを入力しEnterキーを押して、IP設定内容をご確認ください。

6. 「copy running-config startup-config」と入力し、設定の変更内容を保存してください。起動ファイル名(startupファイル名)を入力し、Enterキーを押してください。

```
Console(config)#interface vlan 1
Console(config-if)#ip address dhcp
Console(config-if)#end
Console#ip dhcp restart
Console#show ip interface
 IP address and netmask: 192.168.1.54 255.255.255.0 on VLAN 1,
 and address mode: User specified.
Console#copy running-config startup-config
Startup configuration file name []: startup
\Write to FLASH Programming.

\Write to FLASH finish.
Success.
```

## 2-3-4 SNMP管理アクセスを有効にする

本製品は、HP OpenviewなどのSNMPアプリケーションからの管理コマンドを受け付けるよう設定できるようになっています。本製品は、

1)SNMP要求に応答するよう設定

2)SNMPトラップを生成するよう設定

とすることが可能です。

SNMP管理ステーションが本製品に対し(情報を返すため、またパラメータ設定などの目的で)要求を送ると、本製品は要求されたデータを返信するか、指定されたパラメータの設定を行います。本製品はまた、(マネージャから要求されなくとも)トラップメッセージを通じて情報をSNMPマネージャに送信するよう設定することが可能です。トラップメッセージは、何らかのイベントが発生したことをマネージャに伝えます。

## 2-3-4-1 コミュニティストリング

コミュニティストリングは、SNMPステーションへの管理アクセスの制御で使用されているほか、本製品からのトラップメッセージを受信するようSNMPステーションに対し許可する働きを持ちます。このため、指定ユーザないしユーザグループに対しコミュニティストリングを設定し、かつアクセスレベルを決定する必要があります。

以下に、初期状態で設定されているストリングを示します。

- public:アクセス権限はリードオンリーとなります。認可された管理ステーションはMIBオブジェクトの取り出しのみ行えます。
- private:アクセス権限はリード/ライトとなります。認可された管理ステーションはMIBオブジェクトの取り出しおよび改変が行えます。

**注意**: SNMPを使用しない場合は、上記の初期コミュニティストリングを両方とも削除することをおすすめいたします。コミュニティストリングが存在しない場合、本製品へのSNMP管理アクセスは無効となります。

SNMPを使った本製品への不正アクセスを避けるためにも、初期状態で設定されているコミュニティストリングを別のものに変更することをおすすめします。

以下に、コミュニティストリングを設定する際の手順を示します。

1. Privileged Execレベルグローバル設定モードプロンプトで、「snmp-server community *ストリング モード*」と入力します(*ストリング*:コミュニティアクセスストリング、*モード*:rw(リード/ライト)かro(リードオンリー))。Enterキーを押してください。なお、初期状態ではリードオンリーに設定されています。

2. 既存のストリングを削除する場合は、「no snmp-server community *ストリング*」と入力します(*ストリング*:削除するコミュニティアクセスストリング)。Enterキーを押してください。

```
Console(config)#snmp-server community admin rw
Console(config)#snmp-server community private
Console(config)#
```

## 2-3-4-2 トラップ受信者

本製品から送信されるトラップを受信するSNMPステーションを指定します。

以下に、トラップ受信者を設定する際の手順を示します。

1. Privileged Execレベルグローバル設定モードプロンプトで「snmp-server host *ホストアドレス コミュニティストリング*」と入力します（*ホストアドレス*:トラップ受信者のIPアドレス、*コミュニティストリング*:同ホストに関連付けられているストリング）。Enterキーを押してください。

2. 本製品からSNMP通知を送信するよう設定するには、最低でも1つのsnmp-server enable trapsコマンドを入力する必要があります。「snmp-server enable traps *タイプ*」と入力してください(*タイプ*:authenticationかlink-up-down)。Enterキーを押してください。

```
Console(config)#snmp-server enable traps link-up-down
Console(config)#
```

## 2-3-5 設定内容の保存

設定コマンドは現在実行されている設定ファイルの内容の変更のみ行います。また、変更後の設定内容は本製品を再起動した時点で保存されません。変更後の内容を不揮発性ストレージに保存する場合は、「copy」コマンドをお使いの上、現在実行中の設定ファイルを起動設定ファイル(start-up configuration file)にコピーする必要があります。”

以下に、現在の設定内容を保存する際の手順を示します。

1. Privileged Execモードプロンプトで「copy running-config startup-config」と入力してEnterキーを押してください。

2. Start-upファイルのファイル名を入力し、Enterキーを押してください。

```
Console#copy running-config startup-config
Startup configuration file name []: startup
\Write to FLASH Programming.

\Write to FLASH finish.
Success.

Console#
```

# 2-4 システムファイルの管理

本製品のフラッシュメモリは、CLIプログラム、WEBインタフェースおよびSNMPで管理可能な3種類のシステムファイルに対応しています。本製品のファイルシステムでは、ファイルのアップロード、ダウンロード、コピー、削除が行えるほか、同ファイルを起動（start-up）ファイルとして設定することも可能となっています。

以下に、上記の3種類のファイルについて解説します。

■Configuration (設定)

システム設定情報を保管するファイルで、設定内容を保存する際に作成されます。保存された設定ファイルはシステム起動(start-up)ファイルとして選択できるほか、TFTP経由でサーバにバックアップ用としてアップロードすることも可能です。
「Factory_Default_Config.cfg」ファイルはシステムのすべての初期設定を含んでおり、システムから削除することはできません。詳細についてはP.47の「設定内容の保存および復元」をご覧ください。

■Operation Code (実行コード)

システム起動後に実行されるシステムソフトウェアで、ランタイムコードとも呼ばれます。本製品の動作を実行するコードとなっており、CLIおよびWEB管理インタフェースがご利用いただけます。詳細についてはP.43の「ファームウェアの管理」をご覧ください。

■Diagnostic Code (診断コード)

システム起動時に実行されるソフトウェアで、POST(電源投入時の自己診断)とも呼ばれます。

フラッシュメモリの容量が制限されているため、本製品では実行コードを最大で2つまでのみサポートしています。ただし診断コードおよび設定ファイルは、フラッシュメモリの容量が許すかぎりいくらでも保持することが可能です。

システムのフラッシュメモリ内では、各種類のうち1ファイルを起動(start-up)ファイルとして設定しておく必要があります。システムの起動中、start-upファイルとして指定されている診断コードおよび実行コードが実行され、次いでstart-upファイルと指定されている設定ファイルがロードされるかたちになります。

なお設定ファイルは、ファイル設定の内容および利用を示すファイル名を使ってダウンロードする必要があります。Running-configに直接ダウンロードした場合、システムは再起動しますが、その後設定はrunning-configから保存可能な(固定)ファイルにコピーする必要があります。

# 第3章 スイッチの設定

## 3-1 WEBインタフェースを利用する

本製品は埋め込み式のHTTP WEBエージェントを採用しているため、WEBブラウザを使って本製品の設定や統計情報の確認、ならびにネットワーク上の活動の監視などが行えるようになっています。WEBエージェントは、ネットワーク上のコンピュータであればどの端末からでも標準のWEBブラウザ(Internet Explorer 5.0以降など)を使ってアクセスすることが可能です。

**注意**: コンソールポートとのシリアル接続経由で行うCLI(コマンドラインインタフェース)および、Telnet経由でも本製品の管理を行うことが可能です。CLIの利用に関する詳細については、第4章「CLI」をご覧ください。

WEBブラウザ経由で本製品にアクセスする前に、以下の作業を事前に行ってください。

1. 帯域外シリアル接続、BOOTPないしDHCPプロトコルをお使いの上、本製品に有効なIPアドレス、サブネットマスクならびにデフォルトゲートウェイを設定してください。(設定方法の詳細についてはp.16の「IPアドレスの設定」をご覧ください。)

2. 帯域外シリアル接続をお使いの上、ユーザ名およびパスワードを設定してください。WEBエージェントへのアクセスを制限するユーザ名およびパスワードは、内蔵設定プログラムのそれと同じです。(P.16の「パスワードの設定」をご覧ください。)

3. ユーザ名およびパスワードが終わりましたら、次にシステム設定プログラムにアクセスする必要があります。

**注意:** 1. パスワード入力時は、3回まで入力が許可されています。3回続けて正しいパスワードの入力に失敗した場合、その時点の接続は切断されます。

2. WEBインタフェースにゲスト(Normal Execレベル)でログインした場合は、設定内容の参照およびゲストパスワードの変更が行えます。「admin」(Privileged Execレベル)でログインした場合は、すべてのページ上で設定を変更することが可能です。

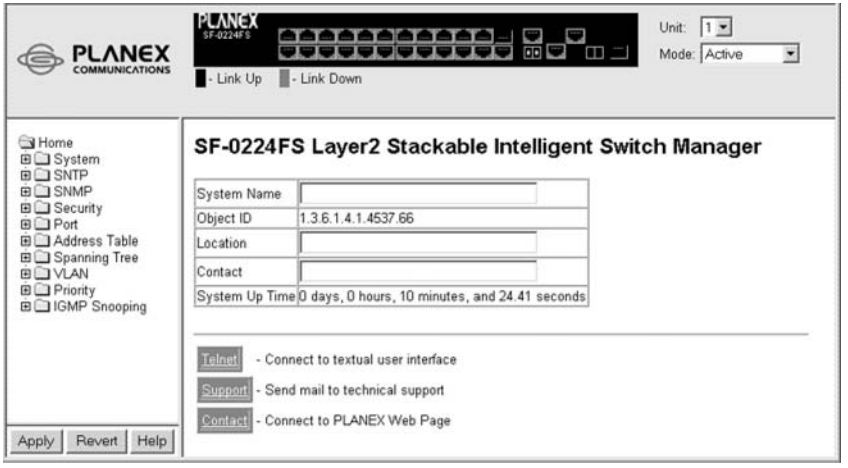
3. 管理ステーションと本製品との間の経路上にSTA(スパニングツリーアルゴリズム)を使用する機器が何も存在しない場合は、管理ステーションに接続されている本製品上のポートを高速転送に設定し(fast forwarding、Admin Edge Portを有効に設定し)、WEBインタフェースを通じて発行される管理コマンドに対する本製品の応答時間を短縮することが可能です。P.175の「インタフェース設定の変更」をご覧ください。

# 3-2 WEBブラウザインタフェースを使用する

WEBブラウザインタフェースにアクセスするためには、まずユーザ名および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ならびに統計情報に対しリード/ライトアクセス権限を持ちます。初期状態で設定されている管理者用のユーザ名およびパスワードは、どちらも「admin」となります。

## 3-2-1 ホームページ

ご使用のWEBブラウザが本製品のWEBエージェントに接続した時点で、以下のホームページが表示されます（下図参照）。ホームページでは、画面左側ではメインメニューが、また右側ではシステム情報が表示されます。メインメニュー上のリンクは、他メニューへの移動する際、また設定パラメータおよび統計情報を表示する場合に使用します。



## 3-2-2 設定オプション

設定可能なパラメータには、ダイアログボックスかドロップダウンリストが表示されます。

いずれかのページ上で何か設定に変更を加えた場合は、「適用(Apply)」ボタンをクリックして新しい設定を必ず確定するようにしてください。

以下に、WEBページ上の設定ボタンの一覧を示します。

表3-1 設定オプション

| ボタン | 動作 |
|---|---|
| Revert (戻す) | 「適用(Apply)」を押す前の時点であれば、指定された値を取り消して現在の値を復元 |
| Apply (適用) | 指定された値をシステムに適用 |
| Help (ヘルプ) | WEBhelpに直接リンク |

**注意:** 1. 画面内容が適度に更新されるよう、ご使用のInternet Explorer 5.x以降を以下のように設定してください。ツール→インターネットオプション→全般→インターネット一時ファイル→設定と選び、「保存しているページの新しいバージョンの確認」項目が「ページを表示するごとに確認する」となっていることをご確認ください。

2. Internet Explorer 5.0をお使いの場合は、ブラウザの更新ボタンを直接押して画面内容を手動で更新する必要があります。

## 3-2-3 パネル表示

WEBエージェントでは、本製品上の各ポートを示す画像が表示されます。Mode(モード)設定を変更することにより、ポートに関する情報を切り替えて表示することが可能です。表示内容には、Active (アクティブ:アップ/ダウン)、Duplex(デュープレックス:half (半二重)/full duplex (全二重))、Flow Control (フローコントロール:with (あり)/ without (なし))などが含まれます。P.121にて解説されておりますように、ポートの画像を直接クリックするとPort Configuration (ポート設定)ページが開くようになっています。

## 3-2-4 メインメニュー

本製品に内蔵されているWEBエージェントを使用することにより、システムパラメータの設定、本製品ならびに各ポートの管理および制御、そしてネットワークの利用状況の監視といった作業を行うことが可能となります。

以下の表は、同プログラムで選択可能な内容を簡単に紹介しています。

表3-2 メインメニュー

| メニュー | 内容 | ページ |
|---|---|---|
| System (システム) | | 32 |
| System Information (システム情報) | 管理者(contact)情報などを含む、システムに関する基本的な情報を示します。 | 32 |
| Switch Information (スイッチ情報) | ポート数、ハードウェア/ソフトウェアバージョンおよび電源の状態を示します。 | 35 |
| Bridge Extension (ブリッジ拡張) | ブリッジ拡張パラメータを示します。 | 37 |
| IP Configuration (IP設定) | 管理アクセス用のIPアドレスを設定します。 | 39 |
| File (ファイル) | | 43 |
| Copy (コピー) | ファイルの転送およびコピーを許可します。 | 45 |
| Delete (削除) | フラッシュメモリ上のファイルの削除を許可します。 | 46 |
| Set Startup (Startup設定) | 起動(startup)ファイルの設定を行います。 | 50 |
| Line (ライン) | | 51 |
| Console (コンソール) | コンソールポートの接続パラメータを設定します。 | 51 |
| Telnet | Telnet接続パラメータを設定します。 | 54 |
| Log (ログ) | | 56 |
| Logs (ログ) | エラーメッセージの保管および表示を行います。 | 56 |
| System Logs (システムログ) | エラーメッセージをログプロセスに送信します。 | 56 |
| Remote Logs (リモートログ) | 遠隔地のログプロセスに対し、メッセージのログ(記録)を設定します。 | 58 |
| SMTP Logs (SMTPログ) | 特定のサーバに対しSMTPクライアントメッセージを送信します。 | 61 |

| | | |
|---|---|---|
| Static List<br>(固定リスト) | VLANグループの作成および削除で使用 | 187 |
| Static Membership by Port<br>(ポート別固定メンバーシップ) | インタフェースのメンバーシップ種類設定をタグ付き、タグ無しおよび禁止のいずれかに指定 | 189 |
| Port Configuration<br>(ポート設定) | 初期PVIDおよびVLAN属性を設定 | 192 |
| Trunk Configuration<br>(トランク設定) | 初期トランクVIDおよびVLAN属性を指定 | 192 |
| Private VLAN<br>(プライベートVLAN) | | 197 |
| Information<br>(情報) | プライベートVLAN機能情報を表示 | 199 |
| Configuration<br>(設定) | プライマリ/コミュニティVLANの作成/削除で使用 | 201 |
| Association<br>(関連付け) | コミュニティVLANはどれもプライマリVLANと関連付ける必要があります | 203 |
| Port Information<br>(ポート情報) | VLANポートの種類および関連付けられているプライマリ/セカンダリVLANを表示 | 204 |
| Port Configuration<br>(ポート設定) | プライベートVLANインタフェースの種類を設定し、同インタフェースをプライベートVLANと関連付けます | 206 |
| Trunk Information<br>(トランク情報) | VLANポートの種類および関連付けられているプライマリ/セカンダリVLANを表示 | 204 |
| Trunk Configuration<br>(トランク設定) | プライベートVLANインタフェースの種類を設定し、同インタフェースをプライベートVLANと関連付けます。 | 207 |
| Priority (優先度) | | 208 |
| Default Port Priority<br>(ポート初期優先度) | 各ポートの初期優先度を設定 | 208 |
| Default Trunk Priority<br>(トランク初期優先度) | 各トランクの初期優先度を設定 | 208 |
| Traffic Classes<br>(トラフィッククラス) | IEEE802.1p優先度タグを出力キューにマッピング | 210 |
| Traffic Classes Status<br>(トラフィッククラスステータス) | トラフィッククラス優先度の有効/無効を設定(未実装) | |
| Queue Mode<br>(キューモード) | キューモードを厳密な優先度(strict priority)かウェイトラウンドロビン(Weighted Round-Robin)に設定 | 212 |

# 3-3 基本設定

## 3-3-1 システム情報を表示する

機器名、場所および担当者連絡先を表示することによりシステムを簡単に識別できるようになっています。

### 3-3-1-1 フィールド項目

- System Name (システム名):当スイッチシステムに割り当てられている名称です。
- Object ID(オブジェクトID):本製品のネットワーク管理サブシステム用MIB IIオブジェクトIDです。
- Location (場所):システムの場所を指定します。
- Contact(連絡先):当システムの管理担当者です。
- System Up Time(システム稼働時間):管理エージェントが稼動している期間です。

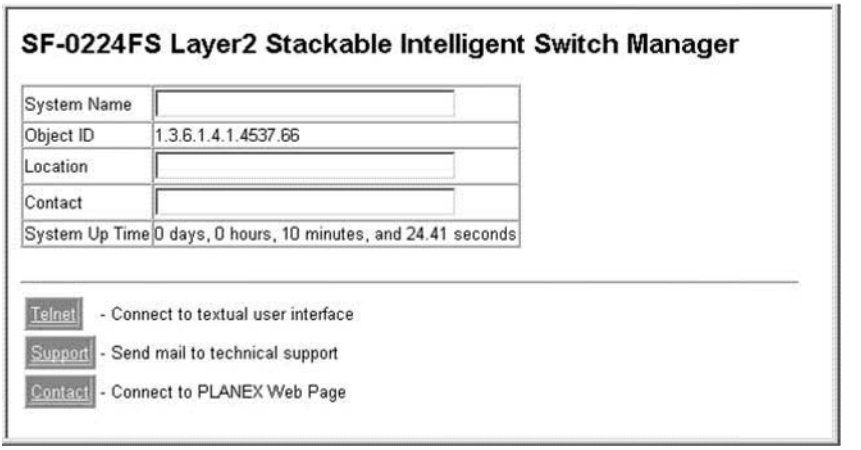
なお、CLIでは以下のパラメータが追加で表示されます。

- MAC Address (MACアドレス):本製品の物理レイヤアドレスです。
- WEB server (WEBサーバ):HTTP経由での管理アクセスが有効となっているかどうかを示します。
- WEB server port (WEBサーバポート):WEBインタフェースで使用しているTCPポートの番号です。
- WEB secure server(WEBセキュアサーバ):HTTPS経由での管理アクセスが有効となっているかどうかを示します。
- WEB secure server port (WEBセキュアサーバポート):HTTPSインタフェースで使用しているTCPポートを示します。
- Telnet server (Telnetサーバ):Telnet経由での管理アクセスが有効となっているかどうかを示します。
- Telnet port (Telnetポート):Telnetインタフェースで使用しているTCPポートを示します。
- Jumbo Frame (ジャンボフレーム):ジャンボフレームが有効となっているかどうかを示します。
- POST result (POST結果):電源投入時の自己診断の結果を示します。

WEB：

System（システム）→System Information（システム情報）と選択してください。

次に、システム名、場所および連絡先情報を指定し、Apply(適用)をクリックしてください。（当ページには、Telnet経由でのCLI（コマンドラインインタフェース）へのアクセスを許可するTelnetボタンも含まれます。）



CLI:

ホスト名、位置および連絡先情報を指定します。

```
Console(config)#hostname R&D 5                                          4-25
Console(config)#snmp-server location WC 9                               4-104
Console(config)#snmp-server contact Ted                                 4-104
Console(config)#exit
Console#show system                                                     4-62
System description: SF-0224FS Layer2 Stackable Intelligent Switch
System OID string: 1.3.6.1.4.1.4537.66
System information
 System Up time:          0 days, 2 hours, 4 minutes, and 7.13 seconds
 System Name:             R&D 5
 System Location:         WC 9
 System Contact           Ted
 MAC address              00-90-CC-12-34-56
 Web server:              enabled
 Web server port:         80
 Web secure server:       enabled
 Web secure server port:  443
 Telnet server:           enabled
 Telnet port:             23
 Jumbo Frame:             Disabled
 POST result
DUMMY Test 1.................PASS
UART LOOP BACK Test..........PASS
DRAM Test....................PASS
Timer Test...................PASS
RTC Initialization...........PASS
Switch Int Loopback test.....PASS

Done All Pass.
Console#
```

## 3-3-2ハードウェアおよびソフトウェアのバージョンを表示する

Switch Information (スイッチ情報)では、本製品メインボードならびに管理ソフトウェアのハードウェア/ソフトウェアバージョンを表示することが可能なほか、電源状態の確認も行えるようになっています。

フィールド項目:

■メインボード

- Serial Number (シリアル番号)
  本製品のシリアル番号です。
- Number of Ports (ポート数)
  内蔵RJ-45ポートのポート数です。

- Hardware Version (ハードウェアバージョン)
  メインボードのハードウェアバージョンです。
- Internal Power Status (内部電源ステータス)
  内部電源の状態を示します。

■管理ソフトウェア

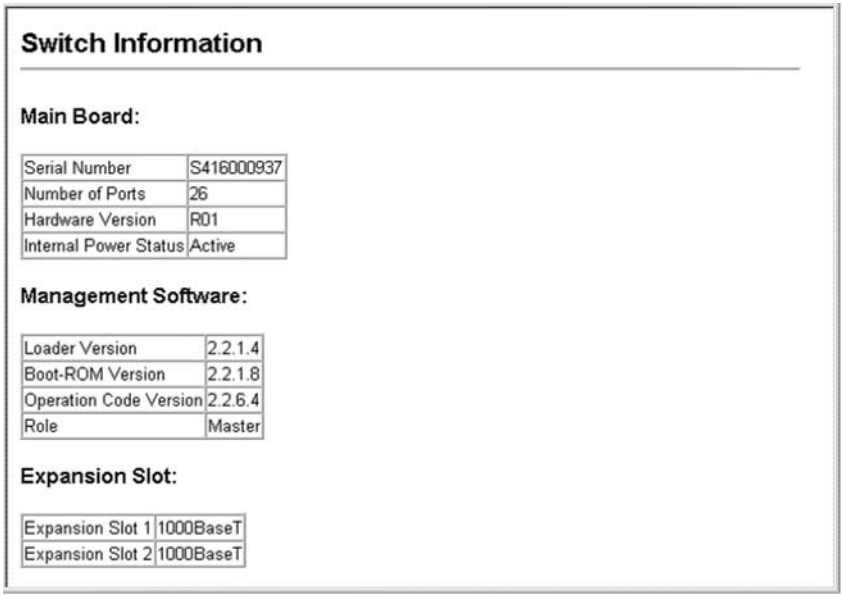
- Loader Version (ローダバージョン)
  ローダコードのバージョンです。
- Boot-ROM Version (Boot ROMバージョン)
  POSTおよびブートコードのバージョンです。
- Operation Code Version (実行コードバージョン)
  ランタイムコードのバージョンです。
- Role(M/S)
  本製品がマスタ、スレーブのどちらで動作しているのかを示します。

■拡張スロット

- Expansion Slot 1/2 (拡張スロット1/2)
  RJ-45/SFPコンビネーションポートです。
- Unit ID (ユニットID)
  スタック内のユニット番号です。
- Redundant Power Status (冗長電源ステータス)
  冗長電源の状況を示します。

WEB：

System（システム）→Switch Information(スイッチ情報)と選択します。



## Switch Information

### Main Board:

| | |
|---|---|
| Serial Number | S416000937 |
| Number of Ports | 26 |
| Hardware Version | R01 |
| Internal Power Status | Active |

### Management Software:

| | |
|---|---|
| Loader Version | 2.2.1.4 |
| Boot-ROM Version | 2.2.1.8 |
| Operation Code Version | 2.2.6.4 |
| Role | Master |

### Expansion Slot:

| | |
|---|---|
| Expansion Slot 1 | 1000BaseT |
| Expansion Slot 2 | 1000BaseT |

CLI：

バージョン情報を表示する場合は以下のコマンドを入力してください。

```
Console#show version                                          4-63
Unit 1
 Serial number:            S416000937
 Service tag:
 Hardware version:         R01
 Module A type:            1000BaseT
 Module B type:            1000BaseT
 Number of ports:          26
 Main power status:        up
 Redundant power status    :not present

Agent (master)
 Unit ID:                  1
 Loader version:           2.2.1.4
 Boot ROM version:         2.2.1.8
 Operation code version:   2.2.6.4

Console#
```

## 3-3-3 ブリッジ拡張機能を表示する

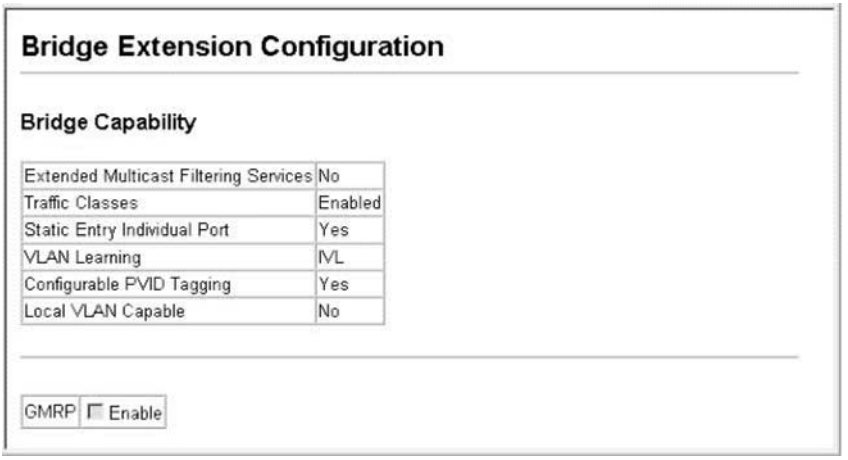
ブリッジMIBは、マルチキャストフィルタリング、トラフィッククラスおよびVLANに対応した管理危機用の拡張機能を備えています。これらの拡張にアクセスし、主な変数の初期設定を表示することが可能です。

フィールド項目：

- Extended Multicast Filtering Services（拡張マルチキャストフィルタリングサービス）
  本製品は、GMRP(GARPマルチキャスト拡張登録)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には対応しておりません。
- Traffic Classes（トラフィッククラス）
  本製品では、複数のトラフィッククラスに対しユーザの優先度をマッピング（割り当てる）ことが可能です。（p.208の「CoS設定」をご覧ください。）
- Static Entry Individual Port（固定エントリ個別ポート）
  本製品では、ユニキャストおよびマルチキャストアドレスの固定フィルタリングに対応しています。（p.156の「固定アドレスの設定」をご覧下さい。）
- VLAN Learning（VLAN学習）
  本製品では、各ポートが自身のフィルタリングデータベースを保持する独自VLAN学習(IVL)を採用しています。
- Configurable PVID Tagging（設定変更対応PVIDタギング）
  本製品では、各ポートの
  1)初期ポートVLAN ID（フレームタグで使用されるPVID）
  2)送信ステータス（タグ付きVLANかタグ無しのいずれか）
  を上書きすることが可能です（p.178の「VLAN設定」をご覧ください。）
- Local VLAN Capable（ローカルVLAN対応）
  本製品は、802.1Qで定義されているVLAN以外の複数の（多重）ローカルブリッジには対応していません。
- GMRP
  本製品は、マルチキャストグループを持つ末端ステーションの登録をネットワーク機器に許可するGARPマルチキャスト登録プロトコル(GMRP)には対応しておりません。本製品はIGMPを使用して自動マルチキャストフィルタリングを行います。

WEB：

System (システム)→Bridge Extension Configuration(ブリッジ拡張設定)と選択します。




CLI：

以下のコマンドを入力してください。

```
Console#show bridge-ext                                          4-165
 Max support VLAN numbers:              255
 Max support VLAN ID:                   4094
 Extended multicast filtering services: No
 Static entry individual port:          Yes
 VLAN learning:                         IVL
 Configurable PVID tagging:             Yes
 Local VLAN capable:                    No
 Traffic classes:                       Enabled
 Global GVRP status:                    Disabled
 GMRP:                                  Disabled
Console#
```

## 3-3-4 本製品のIPアドレスを設定する

当セクションでは、ネットワーク経由で管理アクセスを行う際に使用するIPインタフェースの設定手順を解説します。初期設定では、本製品用のIPアドレスはDHCP経由で取得するようになっています。アドレスを手動で設定する場合は、本製品の初期設定(IPアドレス:0.0.0.0、ネットマスク:255.0.0.0)をご使用ネットワークで利用可能な値に変更する必要があります。また、本製品と、他ネットワークセグメント上に存在する管理ステーションとの間でデフォルトゲートウェイの設定が必要となる場合もあります。

特定のIPアドレスを手動で設定できるほか、BOOTPやDHCPサーバからアドレスを取得するよう設定することも可能です。有効なIPアドレスは0から255までの十進数4個をピリオドで区切ったものとなります。CLIプログラムは、当形式以外の値は受け付けませんのでご注意ください。

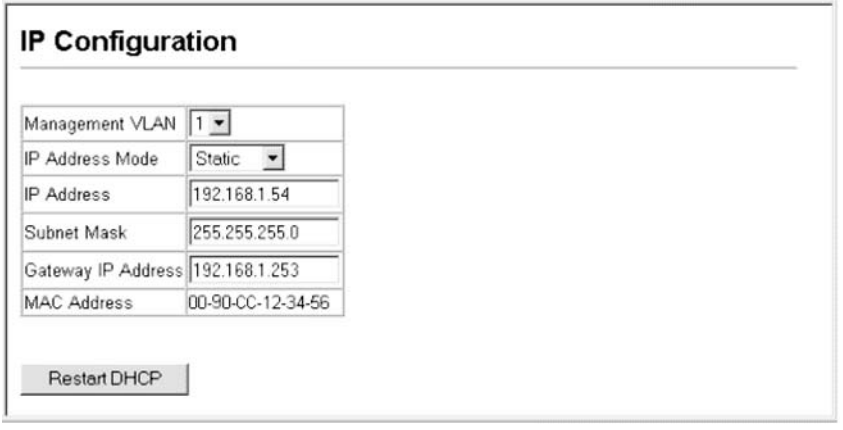
コマンド解説:

- Management VLAN (管理VLAN)
  設定済VLANのIDで、範囲は1～4094となります。なおIDの戦闘でゼロは使えません。初期設定では、本製品のすべてのポートはVLAN 1のメンバーとなっています。ただしいずれのVLANに所属するポートであっても、同VLANにIPアドレスが割り当てられてさえいえれば同ポートに管理ステーションを接続することが可能です。
- IP Address Mode (IPアドレスモード)
  手動設定(Static)、DHCP(DHCP)ないしBOOTP(BOOTP)経由でIP機能を有効にするかどうかを指定します。DHCP/BOOTPが有効となっている場合、サーバから応答があるまでIPは機能しません。本製品は、IPアドレス用の要求を定期的にブロードキャスト送信します。(DHCP/BOOTP値には、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。)
- IP Address (IPアドレス)
  管理アクセスを許可されているVLANインタフェースのアドレスです。有効なIPアドレスは0から255までの十進数4個をピリオドで区切ったものとなります。(初期設定:0.0.0.0)
- Subnet Mask (サブネットマスク)
  特定のサブネットにルーティングする際に使用するホストアドレスビットを示します。(初期設定:255.0.0.0)
- Gateway IP address (ゲートウェイIPアドレス)
  本製品と、他ネットワークセグメント上に存在する管理ステーションとの間にあるゲートウェイルータのIPアドレスです。(初期設定:0.0.0.0)
- MAC Address (MACアドレス)
  本製品の物理レイヤアドレスです。
- Restart DHCP (DHCP再起動)

DHCPサーバに対しIPアドレスを新規に要求します。

WEB:

System (システム)→IP Configuration (IP設定)と選択し、管理ステーションが接続されているVLANを選んでください。IP Address Mode (IPアドレスモード)を「Static(固定)」に設定し、IPアドレス、サブネットマスクおよびゲートウェイを入力してApply(適用)をクリックしてください。




CLI:

管理インタフェース、IPアドレスならびにデフォルトゲートウェイを指定してください。

```
Console#config
Console(config)#interface vlan 1                                    4-108
Console(config-if)#ip address 10.1.0.254 255.255.255.0              4-190
Console(config-if)#exit
Console(config)#ip default-gateway 192.168.1.254                    4-191
Console(config)#
```

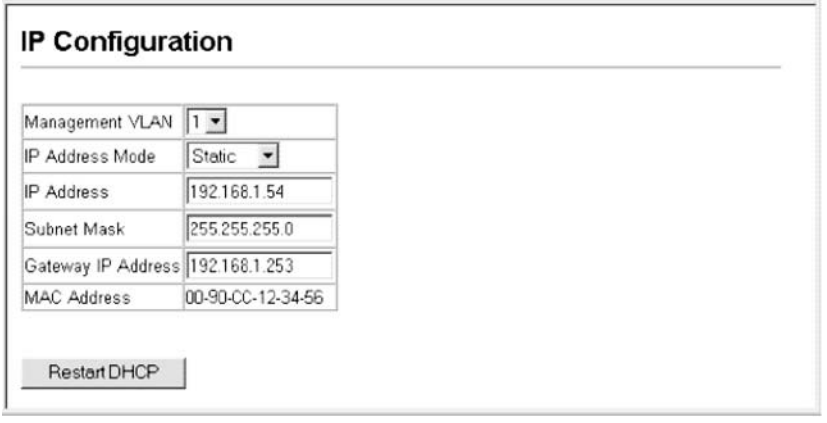
## 3-3-5 DHCP/BOOTPを使用する

ご使用ネットワークでDHCP/BOOTPサービスが提供されている場合は、これらのサービスにより本製品を動的に設定するよう、本製品自体を設定することが可能です。

WEB:

System (システム)→IP Configuration (IP設定)と選択します。

管理ステーションが接続されているVLANを指定し、IP Address Mode (IPアドレスモード)をDHCPかBOOTPに設定してください。設定が済みましたらApply(適用)ボタンをクリックして新しい設定内容を保存してください。次に、「Restart DHCP(DHCP再起動)」をクリックしてください。この操作で、新規アドレスを即座に要求するかたちになります。なお本製品は、電源リセット時もIP設定内容の要求をブロードキャスト送信するようになっています。




**注意**: 管理接続が失われた場合は、端末接続をお使いの上「show ip interface 」と入力し、本製品の新しいアドレスをご確認ください。

CLI:

管理インタフェースを指定し、IPアドレスモードをDHCPかBOOTPに設定してください。次に「ip dhcp restart」コマンドを入力してください。

```
Console#config
Console(config)#interface vlan 1                                    4-108
Console(config-if)#ip address dhcp                                  4-190
Console(config-if)#end
Console#ip dhcp restart                                             4-192
Console#show ip interface                                           4-192
 IP address and netmask: 192.168.1.54 255.255.255.0 on VLAN 1,
 and address mode: User specified.
Console#
```

Renewing DHCP (DHCPの更新):

DHCPは、クライアントに対しアドレスを永久に残す場合もあれば、一定期間に限って残す場合もあります。アドレスが期限切れとなるか本製品が他ネットワークセグメントに移動すると、本製品への管理アクセスは失われます。このような場合は、本製品を再起動するか、CLI経由でDHCPサービスを再起動するようクライアント要求を発行してください。

WEB:

DHCPより割り当てられたアドレスが機能しなくなった場合は、WEBインタフェースを通じてIP設定を更新することが不可能となります。DHCPサービスは、現在のアドレスが利用可能な場合のみ、WEBインタフェース経由で再起動することが可能です。

CLI:

DHCPサービスを再起動する場合は以下のコマンドを入力してください。

```
Console#ip dhcp restart                                             4-192
Console#
```

# 3-4 ファームウェアの管理

スタック内のスイッチユニットとTFTPサーバとの間で、ファームウェアのアップロード、ダウンロードおよびコピーが行えます。ランタイムコードをファイルとしてTFTPサーバに保存し、同ファイルを後でダウンロードしてスイッチの動作を復元することが可能です。また既存のファームウェアを上書きすることなく、新しいファームウェアを使用するよう本製品を設定することも可能です。ファイル転送の形式、ファイルの種類ならびにファイル名を指定する必要があります。

コマンド解説：

- File Transfer Method (ファイル転送形式)
  ファームウェアのコピー操作には以下のオプションが含まれます。
  - file to file (ファイル→ファイル)
    本製品のディレクトリ内に、新しいファイル名を使って既存のファイルをコピーします。
  - file to tftp (ファイル→TFTP)
    ファイルを本製品からTFTPサーバにコピーします。
  - tftp to file (TFTP→ファイル)
    TFTPサーバから本製品にファイルをコピーします。
  - file to unit (ファイル→スイッチ)
    本製品から、スタック内の他ユニットに対しファイルをコピーします。
  - unit to file (スイッチ→ファイル)
    スタック内の他ユニットから本製品に対しファイルをコピーします。
- TFTP Server IP Address (TFTPサーバIPアドレス)
  TFTPサーバのIPアドレスです。
- File Type (ファイルの種類)
  opcode (オペレーショなるコード)を指定してファームウェアをコピーしてください。
- File Name (ファイル名)
  ファイル名内ではスラッシュ(/および右下がりのマークも含む)を使用することはできません。またファイル名をピリオド(「.」)で開始することはできませんのでご注意ください。TFTPサーバ上のファイル名は最大127文字までとなっているほか、本製品上のファイル名は最大31文字までとなります。いずれも、使用可能な文字は半角英数字(A-Z, a-z, 0-9, - , - , _)となります。
- Source/Destination Unit (コピー元/コピー先スイッチ)
  スタック内のスイッチのユニット番号を指定してください。

**注意**:　本製品上のファイルディレクトリ内には、システムソフトウェア(例:ランタイムファームウ

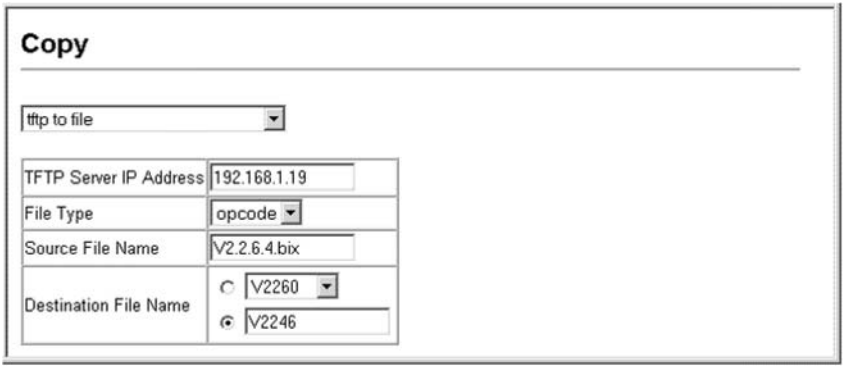
ェア)を最大で2つまでそのコピーを保存することが可能です。同ファイルの、現時点で指定されている起動(startup)バージョンは削除できません。

## 3-4-1 サーバからシステムソフトウェアをダウンロードする

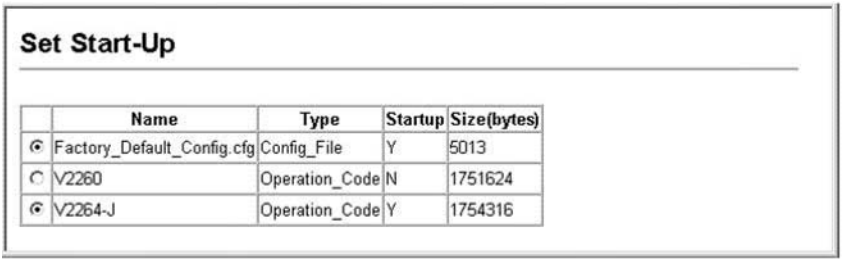
ランタイムコードをダウンロードする場合は、現在のイメージと置き換えるコピー先ファイル名を指定するか、現在のランタイムコードファイルとは別の名前でファイルをまずダウンロードし、同ファイルをstartup (起動)ファイルとして指定する必要があります。

WEB:

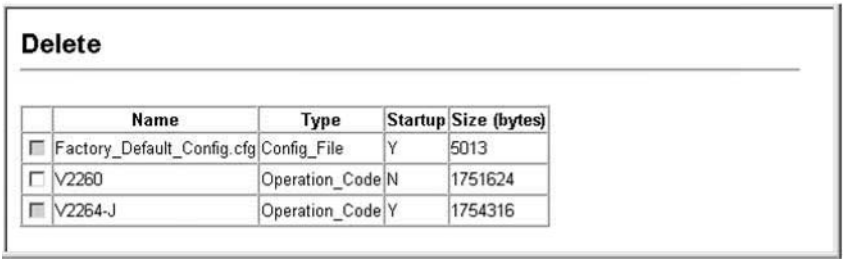
System (システム)→File Management (ファイル管理)→Copy Operation (コピー)と選択します。ファイル転送方法として「tftp to file (TFTP→ファイル)」を選び、TFTPサーバのIPアドレスを入力してください。次にファイルの種類を「opcode」に設定し、ダウンロードするファイルのファイル名を入力した上で、置き換え(上書き)対象となる本製品上のファイルを指定するか、新規にファイル名を指定してください。この状態でApply(適用)をクリックしてください。起動(startup)で使用されている現在のファームウェアを別のものと置き換えており、かつ新しい実行(operation)コードを使って本製品を再起動する場合は、System(システム)/Reset (リセット)メニューにて本製品を再起動してください。




新規のコピー(保存)先ファイルとしてダウンロードしている場合は、System/File/Set Start-Up (システム/ファイル/起動ファイルの設定)メニューにてstartup(起動)時に使用する実行コードを選び、Apply (適用)をクリックしてください。新しいファームウェアを開始する場合はSystem/Reset (システム/リセット)メニューにて本製品を再起動してください。



ファイルを削除する場合はSystem/File/Delete (システム/ファイル/削除)と選択し、表示されるファイル一覧の中から削除するファイルを選んでチェックマークを付けてApply(適用)ボタンをクリックしてください。なお、現時点においてstartupコードとして指定されているファイルは削除できませんのでご注意ください。



**Delete**

| | Name | Type | Startup | Size (bytes) |
|---|---|---|---|---|
| ☐ | Factory_Default_Config.cfg | Config_File | Y | 5013 |
| ☐ | V2260 | Operation_Code | N | 1751624 |
| ☐ | V2264-J | Operation_Code | Y | 1754316 |

CLI:

TFTPサーバから新しいファームウェアをダウンロードする場合は、TFTPサーバのIPアドレスを入力し、ファイルの種類として「opcode」を指定した上でダウンロード元(source)およびダウンロード先(destination)のファイル名を入力してください。ファイルのダウンロードが完了しましたら、同(新)ファイルをstartupファイルとして設定し本製品を再起動してください。

新ファームウェアを開始する場合は、「reload」コマンドを使用するか、本製品を再起動してください。

```
Console#copy tftp file                                          4-65
TFTP server ip address: 192.168.1.23
Choose file type:
 1. config:  2. opcode: <1-2>: 2
Source file name: V2.2.6.4.bix
Destination file name: V2264
\Write to FLASH Programming.
-Write to FLASH finish.
Success.
Console#config
Console(config)#boot system opcode:V2264                        4-70
Console(config)#exit
Console#reload                                                  4-22
```

# 3-5 設定内容の保存および復元

TFTPサーバに対し設定内容をアップロードし、また同サーバから設定内容をダウンロードすることが可能となっているほか、スタック内のスイッチとTFTPサーバとの間でファイルのコピーが行えます。後で設定ファイルをダウンロードし、スイッチ設定を復元することが可能です。

コマンド解説：

- File Transfer Method (ファイル転送方式)
  設定のコピーに関する操作は以下の通りです。
  - file to file (ファイル→ファイル)
    スイッチディレクトリ内でファイルをコピーします。コピー先のファイルには新しいファイル名が割り当てられます。
  - file to running-config (ファイル→実行中の設定)
    本製品内のファイルを、現在実行中の設定にコピーします。
  - file to startup-config (ファイル→起動(startup)設定)
    本製品内のファイルをstartup設定にコピーします。
  - file to tftp (ファイル→TFTP)
    ファイルを本製品からTFTPサーバにコピーします。
  - running-config to file (実行中設定→ファイル)
    現在実行中の設定をファイルにコピーします。
  - running-config to startup-config (実行中設定→起動(startup)設定)
    現在実行中のファイルをstartup設定にコピーします。
  - running-config to tftp (実行中設定→TFTP)
    現在実行中の設定をTFTPサーバにコピーします。
  - startup-config to file (起動(startup)設定→ファイル)
    startup設定を本製品上のファイルにコピーします。
  - startup-config to running-config (起動(startup)設定→実行中設定)
    startup設定を現在実行中の設定にkピーします。
  - startup-config to tftp (起動(startup)設定→TFTP)
    startup設定をTFTPサーバにコピーします。
  - tftp to file (TFTP→ファイル)
    ファイルをTFTPサーバから本製品にコピーします。
  - tftp to running-config (TFTP→実行中設定)
    ファイルをTFTPサーバから現在実行中の設定にコピーします。
  - tftp to startup-config (TFTP→起動(startup)設定)
    ファイルをTFTPサーバからstartup設定にコピーします。

- file to unit (ファイル→ユニット)
  本製品上のファイルをスタック内の他スイッチにコピーします。
- unit to file (ユニット→ファイル)
  スタック内の他スイッチから本製品に対しファイルをコピーします。

・ TFTP Server IP Address (TFTPサーバIPアドレス)
TFTPサーバのIPアドレスです。

・ File Type (ファイルの種類)
設定内容をコピーする場合はconfig(設定)と指定してください。

・ File Name (ファイル名)
ファイル名内ではスラッシュ(/および右下がりのマークも含む)を使用することはできません。またファイル名をピリオド(「.」)で開始することはできませんのでご注意ください。TFTPサーバ上のファイル名は最大127文字までとなっているほか、本製品上のファイル名は最大31文字までとなります。いずれも、使用可能な文字は半角英数字(A-Z, a-z, 0-9, - , - , _)となります。

・ Source/Destination Unit (コピー元/コピー先ユニット)
スタック内のユニット番号で指定します。

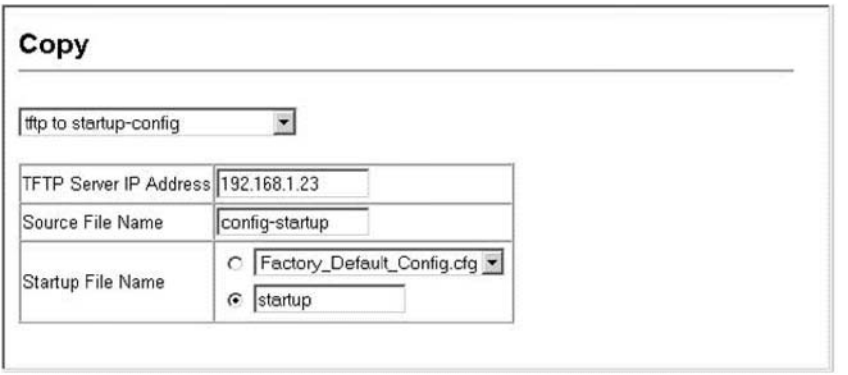
**注意**: ユーザ側で定義する設定ファイルは、フラッシュメモリ内の空き容量が許す限り複数保存することが可能です(他の要素により、保存可能最大数が制限されることはありません)。

## 3-5-1 サーバから設定内容をダウンロードする

設定ファイルを新規ファイル名でダウンロードし、同ファイルをstartupファイルとして設定できるほか、現在のstartup設定ファイルをコピー先ファイルとして指定して直接置き換えることも可能となっています。なお「Factory_Default_Config.cfg」ファイルをTFTPサーバにコピーすることは可能ですが、同ファイルを本製品上のコピー先ファイル（destination）として利用することはできまえんのでご注意ください。

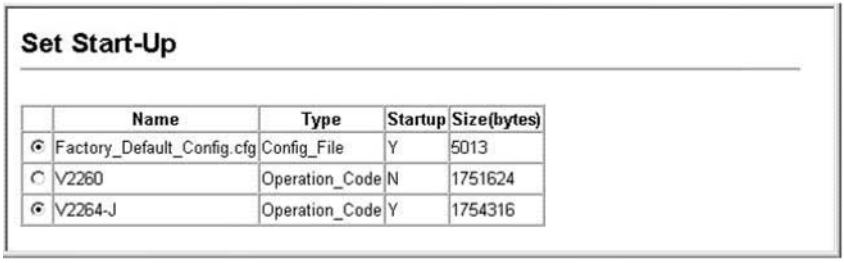
WEB：

System（システム）→File（ファイル）→Copy（コピー）と選び、「tftp to startup-config」または「tftp to file」を選択した上でTFTPサーバのIPアドレスを入力してください。次にダウンロードするファイルのファイル名を指定し、本製品上で上書きするファイル名を選択するか、新規ファイル名を指定してください。設定が完了しましたらApply（適用）をクリックしてください。



「tftp to startup-config」ないし「tftp to file」を使って新しいファイルをダウンロードした場合は、同ファイルは自動的にstartup設定ファイルとして指定されます。新しい設定を利用する場合はSystem/Reset(システム/リセット)メニューにて本製品を再起動してください。

なおSystem/File/Set Start-Up (システム/ファイル/Start-Upの設定)ページを使用することにより、いずれの設定ファイルも起動(startup)設定ファイルとして指定することが可能です。




CLI:

TFTPサーバのIPアドレスを入力し、サーバ上のコピー元(source)ファイルを指定してください。次に本製品上のstartupファイル名を設定した上で本製品を再起動してください。

```
Console#copy tftp startup-config                                    4-65
TFTP server ip address: 192.168.1.19
Source configuration file name: config-startup
Startup configuration file name [] : startup
\Write to FLASH Programming.
-Write to FLASH finish.
Success.

Console#reload
```

他の設定ファイルをstartup設定として選択する場合は、boot systemコマンドをお使いの上本製品を再起動してください。

```
Console#config
Console(config)#boot system config: startup                         4-70
Console(config)#exit
Console#reload                                                      4-22
```

# 3-6 コンソールポート設定

VT100互換機器を本製品のシリアルコンソールポートに接続することにより、本製品内蔵の設定プログラムにアクセスすることが可能となります。同コンソールポート経由での管理アクセスは、パスワード、タイムアウトおよび基本コミュニティストリングなどを含むいくつかのパラメータにより制限されています。同パラメータはWEBおよびCLIインタフェースで設定可能です。

コマンド解説：

- Login Timeout（ログインタイムアウト）
  CLIに対しユーザがログインするまでの間、システムが待機する時間を設定します。同待機時間以内にログインが行われない場合、該当セッションの接続は切断されます。（範囲：0～300秒、初期設定：0）
- Exec Timeout（Execタイムアウト）
  ユーザからの入力が検出されるまでの間システムが待機する待ち時間を設定します。同待機時間以内にログインが行われない場合、現在のセッションとの接続は切断されます。（範囲：0～65535秒、初期設定：0）
- Password Threshold（パスワード入力試行回数）
  パスワード入力を許可する回数を設定します。同設定を行うことにより、失敗可能なログオン回数を制限することが可能となります。当パラメータで設定する回数に到達すると、システムインタフェースは、指定された期間の間沈黙状態となります（沈黙期間はSilent Timeパラメータにて設定）。同期間が経過するまでは、再びログオンすることはできません。（範囲：0～120、初期設定：3回）
- Silent Time（沈黙期間）
  一定回数以上ログオンに失敗した際に管理コンソールがアクセス不可能となる期間を設定します。（範囲：0～65535、初期設定：0）
- Data Bits（データビット）
  コンソールポートにより解釈および生成される、文字ごとのデータビット数を設定します。パリティを生成する場合は、文字ごとのデータビット数として7データビットを指定してください。パリティが不要な場合は8データビット/文字を指定してください（初期設定：8ビット）。
- Parity（パリティ）
  パリティビットの設定変更を行います。端末によっては、使用する通信プロトコルで特定のパルティビット設定が必要となる場合があります。Even（偶数）、Odd(奇数)およびNone(なし)のいずれかを設定してください。（初期設定：なし）
- Speed（速度）
  端末回線の、端末との送受信ボーレートを設定します。シリアルポートと接続している機器のボーレートと合致する速度を設定してください。（範囲：9600、19200、38400、57600および115200ボー　初期設定：9600bps）

・ Stop Bits (ストップビット)

バイトごとに送信するストップビットの数を指定します。(範囲:1～2、初期設定:1ストップビット)

・ Password (パスワード)

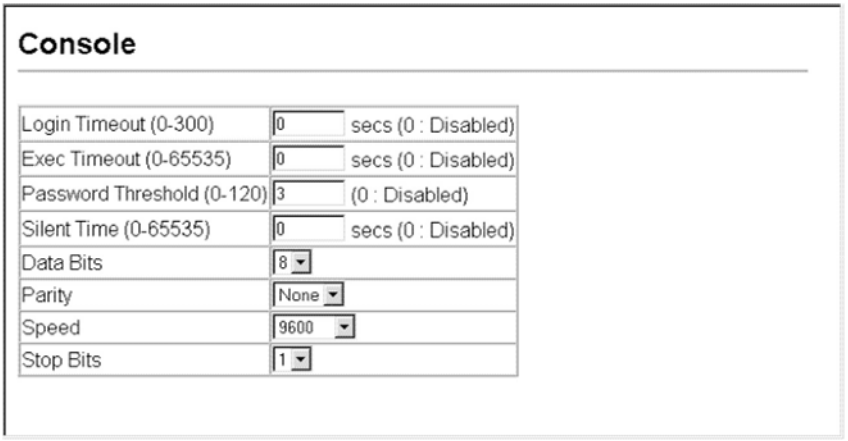
回線接続のパスワードを指定します。パスワードで保護されている回線で接続を開始した場合、システムはパスワードの入力を要求します。正しいパスワードが入力された時点でプロンプトが表示されます。(初期設定:No password (パスワード無し))

・ Login (ログイン)

ログイン時にパスワードを確認するようになります。Passwordパラメータ用に設定されている単一のグローバルパスワードでの認証が選べるほか、特定のユーザ名アカウント用に設定されているパスワードでの認証を行うよう設定することも可能です。(初期設定:Local(ローカル))

WEB:

System(システム)→Line(回線)→Console(コンソール)と選び、必要に応じて各コンソールポート接続パラメータの設定を行ってください。最後にApply(適用)をクリックしてください。



CLI:

コンソール用のLine Configuration(回線設定)モードに移行し、必要に応じて接続パラメータの設定を行ってください。現在のコンソールポート設定を表示する場合は、Normal Execレベルにてshow lineコマンドを実行してください。

```
Console(config)#line console                                    4-10
Console(config-line)#login local                                4-11
Console(config-line)#password 0 secret                          4-12
Console(config-line)#timeout login response 0                   4-13
Console(config-line)#exec-timeout 0                             4-13
Console(config-line)#password-thresh 3                          4-14
Console(config-line)#silent-time 60                             4-15
Console(config-line)#databits 8                                 4-15
Console(config-line)#parity none                                4-16
Console(config-line)#speed 115200                               4-17
Console(config-line)#stopbits 1                                 4-17
Console(config-line)#end
Console#show line                                               4-18
 Console configuration:
  Password threshold:  3 times
  Interactive timeout: Disabled
  Login timeout:       Disabled
  Silent time:         60
  Baudrate:            115200
  Databits:            8
  Parity:              none
  Stopbits:            1

 VTY configuration:
  Password threshold:  3 times
  Interactive timeout: 600 sec
  Login timeout:       300 sec
Console#
```

# 3-7 Telnet設定

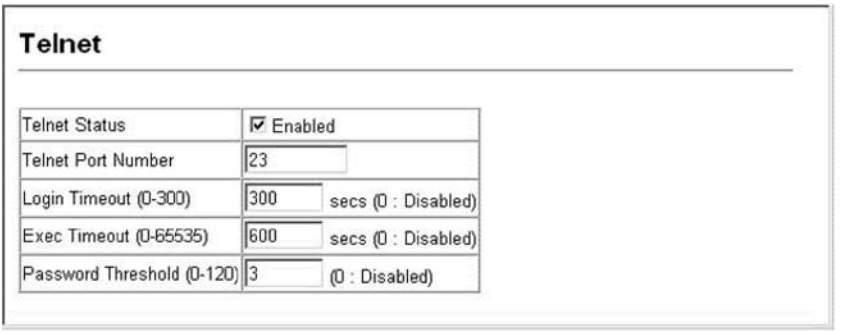
Telnet（仮想ターミナル）を使って、ネットワーク経由で本製品内蔵の設定プログラムにアクセスすることが可能です。Telnet経由での管理アクセスを有効/無効に設定できるほか、TCPポート番号、タイムアウトおよびパスワードを含む様々なパラメータの設定変更が可能です。同パラメータはWEBおよびCLIインタフェースで設定できるようになっています。

コマンド解説：

- Telnet Status（Telnetステータス）
  本製品に対するTelnetでのアクセスを有効/無効に設定します。（初期設定：有効）
- Telnet Port Number(Telnetポート番号)
  本製品でTelnet利用時に使用するTCPポート番号を設定します。（初期設定：23）
- Login Timeout(ログインタイムアウト)
  ユーザがCLIにログインするまでの間システムが待機する時間を設定します。同待機時間内にログインが行われない場合、該当セッションの接続は切断されます。（範囲：0～300秒、初期設定：300秒）
- Exec Timeout(Execタイムアウト)
  ユーザからの入力が検出されるまでの間システムが待機する待ち時間を設定します。同待機時間以内にログインが行われない場合、現在のセッションとの接続は切断されます。（範囲：0～65535秒、初期設定：600秒）
- Password Threshold(パスワード入力試行回数)
  パスワード入力を許可する回数を設定します。同設定を行うことにより、失敗可能なログオン回数を制限することが可能となります。当パラメータで設定する回数に到達すると、システムインタフェースは、指定された期間の間沈黙状態となります（沈黙期間はSilent Timeパラメータにて設定）。同期間が経過するまでは、再びログオンすることはできません。（範囲：0～120、初期設定：3回）
- Password（パスワード）
  回線接続のパスワードを指定します。パスワードで保護されている回線で接続を開始した場合、システムはパスワードの入力を要求します。正しいパスワードが入力された時点でプロンプトが表示されます。（初期設定：No password（パスワード無し））
- Login（ログイン）
  ログイン時にパスワードを確認するようになります。Passwordパラメータ用に設定されている単一のグローバルパスワードでの認証が選べるほか、特定のユーザ名アカウント用に設定されているパスワードでの認証を行うよう設定することも可能です。（初期設定：Local(ローカル)）

WEB：

System（システム）→Line(回線)→Telnetと選択し、Telnetアクセス用のパラメータを指定してください。最後にApply(適用)をクリックしてください。




CLI：

仮想端末アクセス用としてLine Configuration(回線設定)モードに移行し、必要に応じて接続パラメータの設定を行ってください。現在の仮想端末設定を表示する場合は、Normal Execレベルにてshow lineコマンドを実行してください。

```
Console(config)#line vty                                          4-10
Console(config-line)#login local                                  4-11
Console(config-line)#password 0 secret                            4-12
Console(config-line)#timeout login response 300                   4-13
Console(config-line)#exec-timeout 600                             4-13
Console(config-line)#password-thresh 3                            4-14
Console(config-line)#end
Console#show line                                                 4-18
 Console configuration:
  Password threshold:  3 times
  Interactive timeout: Disabled
  Login timeout:       Disabled
  Silent time:         Disabled
  Baudrate:            9600
  Databits:            8
  Parity:              none
  Stopbits:            1

 VTY configuration:
  Password threshold:  3 times
  Interactive timeout: 600 sec
  Login timeout: 300 sec
Console#
```

# 3-8 イベントログの設定

本製品では、エラーメッセージの記録方法を設定することが可能です。

記録対象となる情報には、スイッチメモリに記録されるイベントの種類、遠隔地のSystem Log(syslog)サーバへのログイン履歴などが含まれます。最近発生したイベントメッセージを一覧表示することも可能です。

## 3-8-1 システムログ設定

イベントログ（履歴記録）を有効/無効に設定するほか、RAMないしフラッシュメモリに対し、どのレベルを記録するかを指定します。

フラッシュメモリに記録された重大なエラーメッセージは、ネットワーク関連の問題のトラブルシューティングを円滑に行えるようにするため、本製品内に永久に保存されるかたちになります。フラッシュメモリには最大4096までのログエントリを保存することが可能となっているほか、利用可能なログメモリ(256KB)を超過した場合はもっとも古いエントリから上書きします。

System Logs（システムログ）ページでは、フラッシュかRAMメモリに記録されるシステムメッセージの設定変更ならびに、制限設定が変えられるようになっています。初期設定では、イベントレベル0～3はフラッシュに記録し、レベル0～7はRAMに記録するかたちになります。

コマンド解説：

- System Log Status（システムログ状況）
  デバッグ/エラーメッセージのログ（記録）機能を有効/無効に設定します。（初期設定：Enabled(有効)）
- Flash Level（フラッシュレベル）
  本製品の固定フラッシュメモリに保存するログメッセージのレベルを制限します。例：レベル3を指定した場合、レベル0～3までのメッセージすべてがフラッシュメモリに書き込まれるかたちになります。（範囲：0～7、初期設定：3）

表3-3 ログレベル

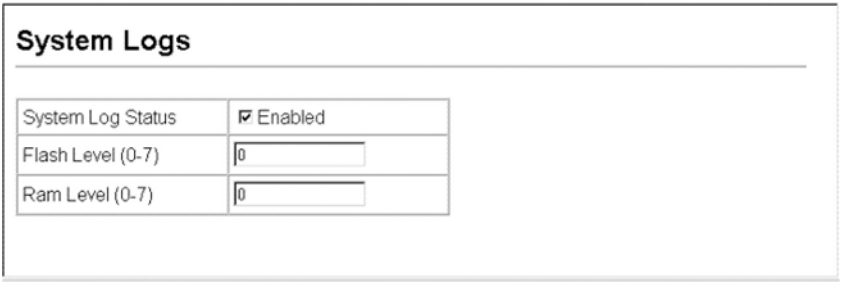
| レベル | 重大性カテゴリ | 内容 |
|---|---|---|
| 7 | Debug(デバッグ) | デバッグメッセージ |
| 6 | Informational(情報) | 情報メッセージのみ |
| 5 | Notice(通知) | コールドスタートなど、正常ではあるものの注意が必要な状態を示します |
| 4 | Warning(警告) | 警告を要する状態(例:return false(応答失敗)、unexpected return(予期せぬ応答)など) |
| 3 | Error(エラー) | エラー状態(例:不正な入力、初期設定の使用など) |
| 2 | Critical(重大) | 重大な状況(例:メモリ割当ないしフリーメモリエラー、リソース不足状態など) |
| 1 | Alert (緊急) | 即座に対応することが必要な状況です |
| 0 | Emergency(非常事態) | システムが利用不可となっています |

- 現時点で利用可能なファームウェアで対応しているエラーメッセージは、レベル2、5および6のみとなります。
- RAM Level (RAMレベル):指定されたレベルまでのログメッセージを、本製品の一時利用RAMメモリに保存します。例:レベル7が指定されている場合、レベル0～7までのすべてのメッセージがRAMに書き込まれるかたちになります。(範囲:0～7、初期設定:6)

**注意:** フラッシュレベルは、RAMレベルと同じであるかそれ以下である必要があります。

WEB:

System (システム)→Log(ログ)→System Log(システムログ)と選択し、System Log Status (システムログ状況)を選んでください。次にRAMおよびフラッシュメモリに記録するメッセージのレベルをそれぞれ必要に応じて変更し、Apply (適用)をクリックしてください。



CLI:

システムのログ機能を有効にし、またRAMおよびフラッシュ目メモリに保存するメッセージのレベルを設定します。現在の設定を表示する場合はshow loggingコマンドを実行してください。

```
Console(config)#logging on                                    4-43
Console(config)#logging history ram 0                         4-44
Console(config)#end
Console#show logging flash                                    4-47
Syslog logging: Enabled
History logging in FLASH: level emergencies
Console#
```

## 3-8-2 リモートログ設定

Remote Logs (リモートログ)ページでは、syslogサーバないしその他管理ステーションに送信されるメッセージの履歴保存(ログ)設定を変更します。送信するエラーメッセージのレベルを特定レベル以下に制限することも可能です。

コマンド解説:

- Remote Log Status (リモートログ状況)
  リモートログプロセスに対し、デバッグ/エラーメッセージを記録する機能を有効/無効に設定します。(初期設定:Enabled(有効))
- Logging Facility (ログ設備)
  syslogメッセージを遠隔保存(remote logging)する際使用する設備の種類を指定します。設定可能な施設は8種類となり、16～23まで値で設定します。syslogサーバはこの情報を使用し、ログメッセージを適切なサービスに発信します。
  当情報は、syslogメッセージにて送信される設備種類のタグを指定します(RFC 3164を参照)。当種類(type)情報は、本製品により報告されるメッセージには何ら影響を与えません。一方、同情報はsyslogサーバがメッセージを処理する際に使用されます。具体的には、メッセージを該当データベース内で分類ないし保存する処理などが含まれます。
  (範囲:16～23、初期設定:23)
- Logging Trap (トラップの記録)
  リモートsyslogサーバに送信されるメッセージを特定レベル以下のものに制限します。
  例:レベル3が指定されている場合、レベル0～3までのすべてのメッセージがリモートサーバに送信されるかたちになります。(範囲:0～7、初期設定:6)
- Host IP List(ホストIPリスト)
  syslogメッセージを受信するリモートサーバのIPアドレスを一覧表示します。アドレス数は最大で5となります。
- Host IP Address (ホストIPアドレス)
  ホストIPリストに新規に追加するサーバのIPアドレスを指定します。

WEB：

System (システム)→Log(ログ)→Remote Log(リモートログ)と選択します。

ホストIPリストにIPアドレスを追加する場合はHost IP Address(ホストIPアドレス)ボックスに新規IPアドレスを入力してAdd(追加)をクリックしてください。IPアドレスを削除する場合は、ホストIPリスト上の該当アドレスをクリックしてRemove (削除)をクリックしてください。


CLI：

syslogサーバのホストIPアドレスを入力し、設備の種類(facility type)を選択してlogging trap (記録トラップ)を設定してください。

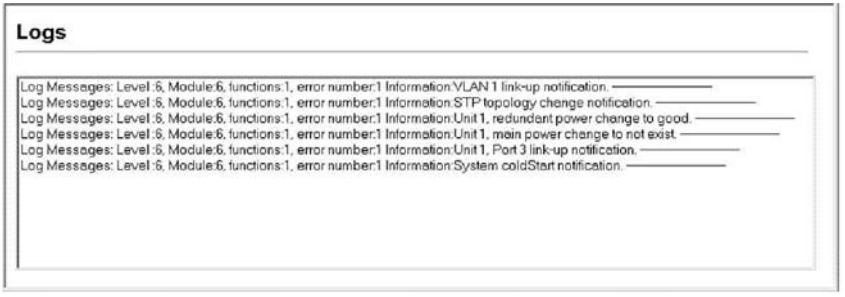
```
Console(config)#logging host 192.168.1.15                    4-45
Console(config)#logging facility 23                          4-45
Console(config)#logging trap 4                               4-46
Console(config)#end
Console#show logging trap                                    4-46
Syslog logging:               Enabled
REMOTELOG status:             Enabled
REMOTELOG facility type:      local use 7
REMOTELOG level type:         Warning conditions
REMOTELOG server ip address: 192.168.1.15
REMOTELOG server ip address: 0.0.0.0
REMOTELOG server ip address: 0.0.0.0
REMOTELOG server ip address: 0.0.0.0
REMOTELOG server ip address: 0.0.0.0
Console#
```

## 3-8-3 ログメッセージの表示

ログページでは、記録されているシステムメッセージならびにイベントメッセージをスクロール表示することが可能です。本製品では、一時利用RAM(次回電源リセット時にメモリ内容は失われます)に最大で2048までのログエントリを保管できるようになっています。また、固定フラッシュメモリには最大4096エントリまで保存可能です。

WEB:

System (システム)→Log(ログ)→Logs(ログ内容)と選びます。




CLI:

以下の例では、RAM内に保存されているイベントメッセージを表示しています。

```
Console#show log ram                                                    4-47
[1] 00:01:37 2001-01-01
   "DHCP request failed - will retry later."
   level: 4, module: 9, function: 0, and event no.: 10
[0] 00:00:35 2001-01-01
   "System coldStart notification."
   level: 6, module: 6, function: 1, and event no.: 1
Console#
```

## 3-8-4 SMTP警告を送信する

本製品から管理者に対し警告を発する仕組みとして、本製品ではSMTPを使用しています。あらかじめ指定したレベルのイベントが記録されると同時に、これを引き金としてe-mailメッセージを送信します。メッセージはネットワーク上の指定SMTPサーバに対し送信されるほか、POPおよびIMAPクライアント側でも取得することが可能となっています。

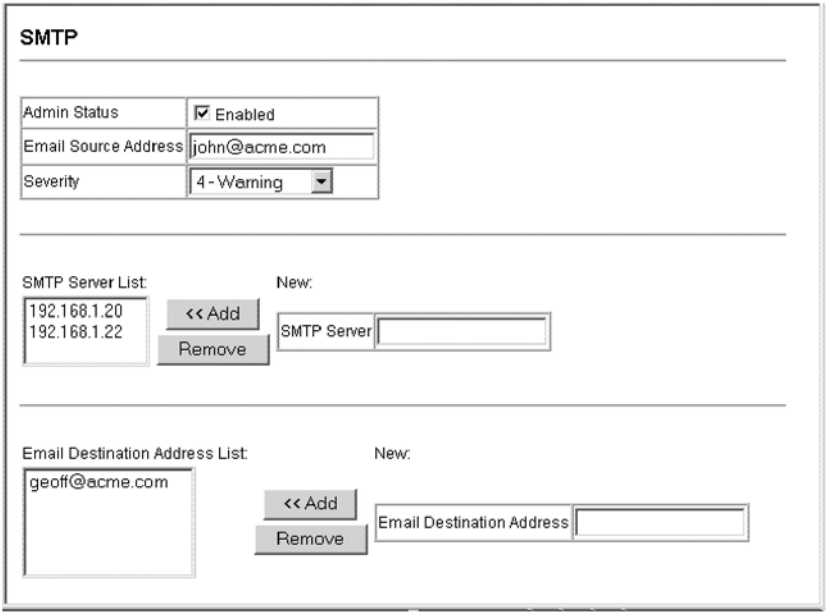
コマンド解説:

- Admin Status (管理ステータス)
  SMTP機能を有効/無効に設定します。(初期設定:Enabled (有効))
- Email Source Address (E-mail送信元アドレス)
  警告メッセージの「From」フィールドで使用するe-mailアドレスを指定します。本製品を識別するための記号的なe-mailアドレスを設定できるほか、本製品の管理担当者のアドレスを指定することも可能です。
- Severity (重要度)
  警告メッセージを発信する際に使用するsyslog重要度判断レベル(p.57の表を参照)です。このレベルないしそれ以上のレベルのイベントはすべて、あらかじめ指定されているe-mail受信者に対し送信されます。例:レベル7と設定した場合、レベル7～0までのイベントすべてが送信されるかたちになります(数値が少ないレベルほど高レベルとなります)。(初期設定:レベル7)
- SMTP Server List (SMTPサーバリスト)
  受信する側となるSMTPサーバを最大で3つまで備えたリストを指定します。リスト上の1番目のサーバに接続できない場合、本製品はリスト上の他のサーバへの送信を試みます。New SMTP Server (新規SMTPサーバ)テキストフィールドおよびAdd/Remove (追加/削除)ボタンをお使いの上、リストを設定してください。
- Email Destination Address List (E-mail送信先アドレスリスト)
  警告メッセージ(e-mail)の受信者を指定します。受信者は最大で5名まで設定可能です。New E-mail Destination Address (新規E-mail送信先アドレス)テキストフィールドおよびAdd/Remove (追加/削除)ボタンをお使いの上、リストを設定してください。

WEB：

System(システム)→Log(ログ)→SMTPと選択してください。

次にSMTPを有効にし(enable)、送信元e-mailアドレスを指定した上で重要度の最小レベルを選択してください。SMTPサーバリストにIPアドレスを追加する場合は、SMTP Server (SMTPサーバ)フィールドに新しいIPアドレスを入力してAdd(追加)をクリックしてください。IPアドレスを削除する場合は、SMTPサーバリスト上で該当エントリをクリックしてRemove (削除)をクリックしてください。警告メッセージを受信するe-mailアドレスは最大で5アドレスまで設定可能です。設定が完了しましたらApply (適用)をクリックしてください。



CLI:

まず、SMTPサーバのIPアドレスを少なくとも1つ入力する必要があります。

次にe-mailメッセージを送信する条件となる、syslog重要度レベル(syslog severity level、送信元となるスイッチおよび受信(送信先)e-mail アドレスを指定してください。同アドレスは最大5つまで設定することが可能です。login sendmailコマンドにてSMTPを有効に設定してください。これで設定は完了となります。現時点でのSMTP設定を表示する場合はlogging sendmailコマンドをお使いください。

```
Console(config)#logging sendmail host 192.168.1.200                    4-49
Console(config)#logging sendmail level 4                               4-50
Console(config)#logging sendmail source-email john@acme.com            4-51
Console(config)##logging sendmail destination-email geoff@acme.com     4-51
Console(config)#logging sendmail                                       4-52
Console(config)#exit
Console#show logging sendmail                                          4-52
SMTP servers
-----------------------------------------------
  1. 192.168.1.200

SMTP minimum severity level: 4

SMTP destination email addresses
-----------------------------------------------
  1. geoff@acme.com

SMTP source email address:   john@acme.com

SMTP status:                 Enabled
Console#
```

## 3-8-5 システムのリセット

WEB:

本製品を再起動する場合は、System (システム)→Reset (リセット)と選択してください。

本当にリセットしてもよいのか確認するメッセージが表示されますので、リセットをこのまま実行する場合はResetボタン本をクリックしてください。


CLI:

本製品をリセットする場合はReloadコマンドをお使いください。

本当にリセットを行ってよいか確認する画面が表示されますので、リセットの要・不要をお確かめの上リセットを続行してください。

```
Console#reload                                                    4-22
System will be restarted, continue <y/n>? y
```

**注意:** システム再起動時は、毎回必ずPOST(起動時自己診断)を実行するようになっています。

## 3-8-6 システムクロックの設定

SNTP(簡易ネットワーク時間プロトコル)を使用することにより、本製品では時間確認用サーバ(SNTPないしNTP)からの定期更新情報に基づき、内蔵クロックの設定が行えるようになっています。本製品上で正確な時刻設定を保つことにより、システム側でも正しい時刻情報を使ってイベントを記録することが可能となります。なお、CLIを使ってクロック設定を手動で設定することも可能です(p.303のcalendar setをご覧ください)。クロックの設定を行わない場合、本製品は最後に起動された際に設定されている工場出荷時の初期設定時間に基づき記録を行います。

SNTPクライアントが有効となっている場合、本製品は設定されている時刻確認用サーバに対し定期的に時間情報の更新要求を送信します。時刻確認用サーバのIPアドレスは、最大で3個まで設定可能です。本製品は、設定されている順番に沿って各サーバに対しアクセスを試みます。

## 3-8-6-1 SNTPの設定

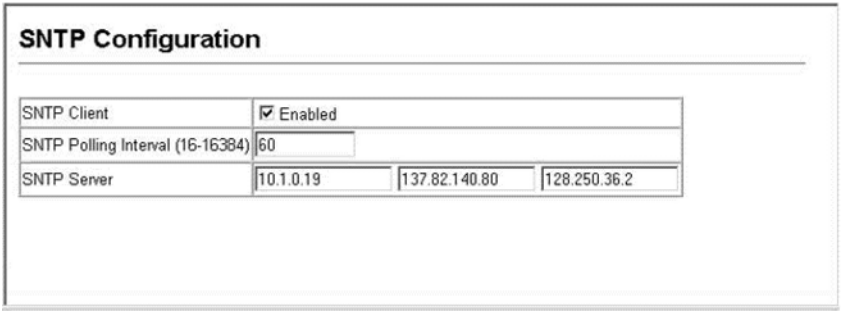
時刻確認用サーバに対し、時間同期要求を送信するよう本製品を設定することが可能です。

コマンド解説：

- SNTP Client (SNTPクライアント)
  本製品がSNTPクライアントとして動作するよう設定します。SNTP Server Field(SNTPサーバフィールド)に、時刻確認用サーバを最低でも1つ指定する必要があります。(初期設定：Disabled (無効))
- SNTP Poll Interval (SNTP要求間隔)
  時刻確認用サーバに対し時間情報の更新要求を送信する間隔を設定します。(範囲：16～16284秒、初期設定：16秒)
- SNTP Server (SNTPサーバ)
  最大で3箇所まで時刻確認用サーバのIPアドレスを設定することが可能です。本製品はまず、1番目のサーバに対し時間更新要求の送信を試みます。これに失敗した場合はリスト上の次のサーバに対し送信を試みます。

WEB：

SNTP→Configuration(設定)と選択し、必要に応じてパラメータを変更してApply(適用)をクリックしてください。



CLI:

以下の例では、本製品をSNTPユニキャストクライアントとして動作するよう設定し、さらに現在の時刻および設定を表示しています。

```
Console(config)#sntp server 10.1.0.19 137.82.140.80 128.250.36.2     4-54
Console(config)#sntp poll 60                                         4-55
Console(config)#sntp client                                          4-53
Console(config)#exit
Console#show sntp
Current time:  Jan  6 14:56:05 2004
Poll interval: 60
Current  mode:  unicast
SNTP status : Enabled
SNTP server 10.1.0.19 137.82.140.80 128.250.36.2
Current server: 128.250.36.2
Console#
```

### 3-8-6-2 タイムゾーンの設定

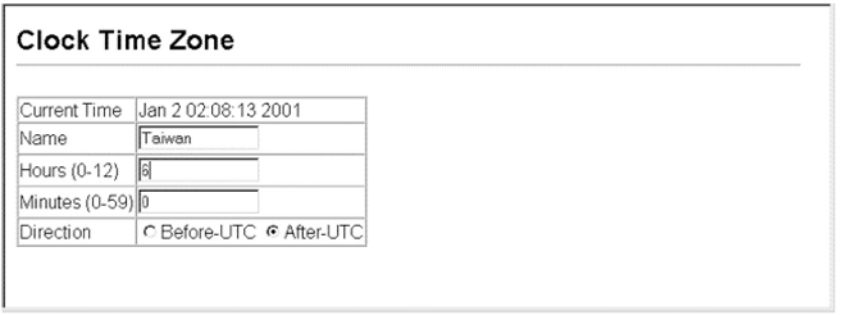
SNTPでは、UTC(協定世界時)の時刻情報が使用されています。お住まい地域のタイムゾーンがUTCより何時間何分1)進んでいるのか(east)、あるいは2)遅れているのか(west)を指定することにより、お住まいの地域の時間に合った時刻を表示させることが可能となります。

コマンド解説:

- Current Time (現在の時刻)
  現在の時刻を表示します。
- Name (タイムゾーン名)
  タイムゾーン名を1～29文字の範囲で設定します。
- Hours(0-12) (時間 (0-12))
  UTCより何時間進んでいるか(遅れているか)を設定します。
- Minutes (0-59)(分(0-59)
  UTCより何分進んでいるか(遅れているか)を設定します。
- Direction (方向)
  タイムゾーンがUTCより進んでいるか、それとも遅れているのかを設定します。

WEB:

SNTP→Clock Time Zone(クロックタイムゾーン)と選択し、UTCと比べた場合のお住まい地域のタイムゾーン値を設定してApply(適用)をクリックしてください。




CLI:

以下の例では、システムクロックにタイムゾーンを設定する方法を示しています。

```
Console(config)#clock timezone Taiwan hours 6 minute 0 after-UTC     4-56
Console(config)#
```

# 3-9 SNMP

SNMP通信プロトコルは、ネットワーク上の機器を管理する目的で設計されています。

通常SNMPで管理されている機器には、スイッチ、ルータおよびホストコンピュータなどが含まれます。SNMPは、これらの機器がネットワーク環境内で正常に動作するよう設定する際に通常使用されているほか、同機器を監視してその性能を確認したり、異常を検出したりする目的でもよく利用されます。

本製品はSNMPエージェントを内蔵しています。

エージェントは自身のハードウェアの状況ならびに、同ハードウェア上のポートを通過するトラフィックを絶え間なく監視します。ネットワーク管理ステーションは、HP OpenViewなどのソフトウェアを使って同情報にアクセスすることが可能です。内蔵エージェントへのアクセス権は、コミュニティストリングにより制限を行っています。本製品と通信を行う際、管理ステーションはまず有効なコミュニティストリングを送信し認証を受ける必要があります。以下に、コミュニティストリングおよびトラップ機能の設定オプションならびに、特定のIPアドレスを持つクライアントにのみアクセスを許可する際の設定オプションを示します。

## 3-9-1 コミュニティアクセスストリングの設定

本製品では、管理アクセスを行う権限を持つコミュニティストリングを最大で5つまで設定できるようになっています。IP Trap Managers(IPトラップマネージャ)で使用するコミュニティストリングは、すべて同テーブル内に一覧表示されます。セキュリティを向上させるためにも、初期設定されているストリングを削除することをおすすめします。

コマンド解説：

- SNMP Community Capability (SNMPコミュニティ対応)
  本製品が最大で5つのコミュニティストリングに対応していることを示します。
- Community String (コミュニティストリング)
  パスワードの役割を担い、SNMPプロトコルへのアクセスを許可するコミュニティストリングの設定を行います。
  - 初期設定：public (リードオンリー)、private (リード/ライト)
  - 範囲：1～32文字、大文字/小文字の区別あり

- Access Mode (アクセスモード)：
  - Read-Only (リードオンリー)
    読み込みのみ可能であることを意味します。同アクセスモード(権限)を持つ管理ステーションは、MIBオブジェクトの取得のみ行えます。

- Read/Write (リード/ライト)
  読み込み、書き込みの両方が行えることを示します。同権限を持つ管理ステーションは、MIBオブジェクトの取得ならびに変更が行えます。

WEB:

SNMP→Configuration (設定)と選び、必要に応じてコミュニティストリングの追加を行ってください。Access Mode(アクセスモード)ドロップダウンリストからアクセス権限を選び、Add(追加)ボタンをクリックしてください。


CLI:

以下の例では、リード/ライト権限を持つストリング「spiderman」を追加しています。

```
Console(config)#snmp-server community spiderman rw              4-103
Console(config)#
```

## 3-9-2 トラップマネージャおよびトラップ種別の指定

指定されているトラップマネージャに対し、本製品は状態の変化を示すトラップを発行します。本製品から管理ステーションに対し主要イベントの報告を行うためには、トラップマネージャをあらかじめ設定しておく必要があります。（設定には、HP OpenViewなどのネットワーク管理プラットフォームを使用します。）本製品から認証失敗メッセージならびにその他のトラップメッセージを受信する管理ステーションは、最大で5つまで指定することが可能です。

コマンド属性：

- Trap Manager Capability（トラップマネージャ対応）
  本製品は最大で5つのトラップマネージャに対応しています。
- Current（現在の設定）
  現在設定されているトラップマネージャを一覧表示します。
- Trap Manager IP Address（トラップマネージャIPアドレス）
  受信対象となるホストのIPアドレスです。
- Trap Manager Community String（トラップマネージャコミュニティストリング）
  通知を行う際に一緒に送信されるコミュニティストリングです。（範囲：1～32文字、大文字/小文字の区別あり）
- Trap Version（トラップバージョン）
  SNMP v1とv2cのどちらで通知内容を送信するかを設定します。（初期設定：Version 1）

- Enable Authentication Traps（認証トラップを有効にする）
  SNMPアクセス認証実行時において、不正なコミュニティストリングが送信されるたびにトラップメッセージを発行します。（初期設定：Enabled（有効））
- Enable Link-up and Link-down Traps（リンクアップ/リンクダウンとラップを有効にする）
  ポートリンクが確立/消失するたびにトラップメッセージを発行します。（初期設定：Enabled（有効））

WEB：

SNMP→Configuration（設定）と選びます。メッセージを受信する各トラップマネージャのIPアドレスおよびコミュニティストリングを入力し、SNMPバージョンを指定してください。次に必要となるトラップの種別（trap type）にマークを入れてAdd(追加)をクリックしてください。


CLI：

以下の例では、トラップマネージャを追加し、さらに認証ならびにリンクアップ/リンクダウンとラップを有効に設定しています。

```
Console(config)#snmp-server host 192.168.1.19 private version 2c    4-105
Console(config)#snmp-server enable traps                             4-106
```

# 3-10 ユーザ認証

本製品に対する管理アクセスを制限するための、各オプションを設定します。

- User Accounts (ユーザアカウント)
  指定されたユーザにつき、本製品へのアクセス権を手動で設定します。
- Authentication Settings (認証設定)
  リモート(遠隔)認証にてアクセス権を設定します。
- HTTPS Settings (HTTPS設定)
  安全なWEB接続を提供します。
- SSH Settings (SSH設定)
  セキュアシェルを提供します(安全なTelnetアクセスを実現)。
- Port Security (ポートセキュリティ)
  各ポート個別のセキュア(安全な)アドレスを設定します。
- 802.1X
  IEEE802.1Xポート認証を使用し、特定ポートへのアクセスを制御します。
- IP Filter (IPフィルタ)
  WEB、SNMPないしTelnetインタフェースに対する管理アクセスのフィルタリングを行います。

## 3-10-1 ユーザアカウントの設定

ゲスト(guest)は、ほとんどの設定パラメータにおいてリード(読み込み)アクセス権限しか持ちません。一方管理者は、内蔵エージェントの管理するすべてのパラメータにつきライト(書き込み)アクセス権限を持っています。このため、出来うる限り早急に管理者用のパスワードを新規に設定し、同情報を安全な場所に保管するようにしてください。

ゲスト名は初期設定でguestとなっており、パスワードも同じguestとなります。管理者名は初期設定でadminとなっており、こちらもパスワードはadminとなります。

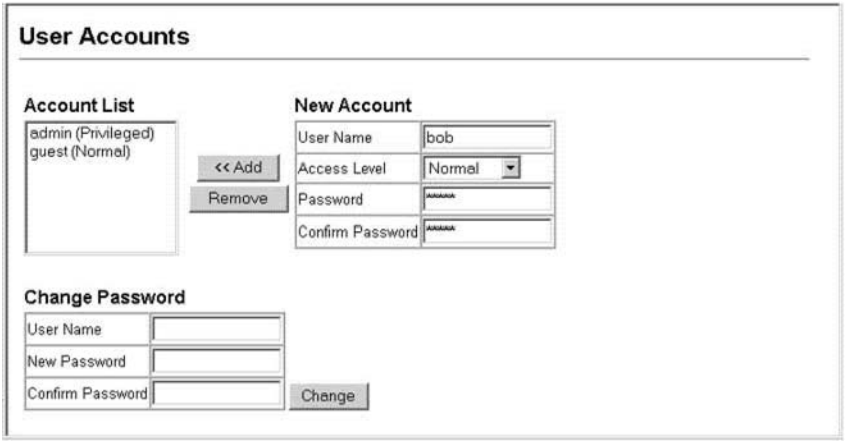
コマンド属性:

- Account List (アカウントリスト)
  現時点でのユーザアカウントおよび関連付けられているレベルを一覧表示します。(初期設定:adminおよびguest)
- New Account (新規アカウント)
  新規アカウントの設定内容を表示します。
  - User Name (ユーザ名)
    ユーザ名を最大8文字までの範囲で設定します。
  - Access Level (アクセスレベル)
    ユーザレベルを指定します。(NormalないしPrivilegedのいずれかの設定可能)
  - Password (パスワード)
    ユーザパスワードを指定します。(範囲:0～8文字までの半角英数字、大文字/小文字の区別有り)
- Change Password(パスワードの変更)
  指定したユーザ名に新規パスワードを設定します。
- Add/Remove (追加/削除)
  リストからアカウントを追加/削除します。

WEB：

Security（セキュリティ）→User Accounts(ユーザアカウント)と選択します。

新規にユーザアカウントを設定する場合は、ユーザ名を指定し、ユーザのアクセスレベルを選択した上でパスワードを入力してください。確認のため再度同じパスワードを入力し、Add(追加)ボタンをクリックしてください。これで新規ユーザアカウントの情報が保存され、同時にアカウントリストに追加されるかたちになります。いずれかのユーザのパスワードを変更する場合は、ユーザ名ならびに新規パスワードを入力し、確認のためもう一度同じパスワードを入力した上でApply(適用)をクリックしてください。




CLI：

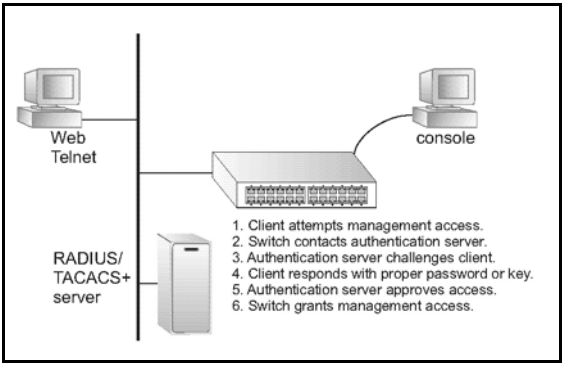
以下の例では、ユーザ（名）にアクセスレベル15(例：管理者)を割り当てた上でパスワードを指定しています。

```
Console(config)#username bob access-level 15                    4-26
Console(config)#username bob password 0 smith
Console(config)#
```

## 3-10-2 ローカル/リモートログオン認証の設定

Authentication Settings (認証設定)メニューを使って、管理アクセスを指定ユーザ名ならびにパスワードに基づいて制限することが可能です。本製品を使って手動でアクセス権限を設定できるほか、RADIUS/TACACS+プロトコルに準拠したリモートアクセス認証サーバを使用することも可能です。

RADIUS(リモート認証ダイアルインユーザサービス)およびTACACS+(端末アクセスコントローラアクセス制御システムプラス)は、中央のサーバで実行されているソフトウェアを使ってネットワーク上のRADIUS/TACACS対応機器へのアクセスを制御するログオン認証プロトコルです。認証サーバは複数のユーザ名/パスワードのペア情報を含んだデータベースを備えています。同情報には、本製品への管理アクセスを必要とする各ユーザ用に関連付けられている権限(特権)レベルも含まれます。




1. クライアントから管理アクセスを試行
2. スイッチから認証サーバに接続
3. 認証サーバはクライアントに対しチャレンジ(認証)実行
4. クライアントは正しいパスワードないしキーを応答
5. 認証サーバはアクセスを承認
6. スイッチは管理アクセスを許可

RADIUSがUDPを使用するのに対し、TACACS+はTCPを使用します。UDPはベストエフォート式の配信のみ提供しますが、TCPは接続志向の配信を提供します。またRADIUSはクライアントからサーバに送られるアクセス要求パケット内のパスワードのみ暗号化を行いますが、TACACS+はパケット全体を暗号化します。

コマンド利用：

- 初期設定では、管理アクセスはローカルスイッチ上に保存されている認証データベースの情報と常に比較し確認が行われるかたちになります。リモート認証サーバを使用する場合は、認証シーケンスならびに、リモート認証プロトコルに対応するパラメータを指定する必要があります。ローカルおよびリモートのログオン認証は、コンソールポート、WEBブラウザおよびTelnetを介する管理アクセスを制御（制限）します。
- RADIUSおよびTACACS+ログオン認証は、各ユーザ名/パスワードペアに対し特定の権限レベルを割り当てます。ユーザ名、パスワードおよび権限（privilege）レベルは認証サーバ上で設定する必要があります。
- いずれのユーザに対しても、最大で3つの認証方式を指定して認証シーケンス（手順）を設定することが可能です。例：(1)RADIUS、(2)TACACSおよび(3)Localと選択した場合は、RADIUSサーバ上のユーザ名およびパスワードが最初に確認されます。RADIUSサーバが利用できない場合、認証プロセスはTACACS+サーバに対し接続を試み、こちらも利用不可であった場合は最後にローカルユーザ名およびパスワードを確認します。

コマンド解説：

- Authentication（認証）
  必要となる認証ないし認証シーケンスを選択します。
  - Local（ローカル）
    本製品側でローカルのユーザ認証を行います。
  - Radius(RADIUS)
    ユーザ認証をRADIUSサーバのみ使って実行します。
  - TACACS
    TACACS+サーバのみ使ってユーザ認証を行います。
  - [authentication sequence（認証順番）]
    指定されている順番にて、最大3種の認証方式を使ってユーザ認証を行います。
- RADIUS Settings（RADIUS設定）
  - -Global（グローバル）
    グローバル（全体）に適用可能なRADIUS設定となります。
  - ServerIndex(サーバインデックス)
    5つのRADIUSサーバのうち、設定可能なもの1つを指定します。本製品は、リスト上の順番に沿ってサーバを使用し認証を試みます。サーバがユーザに対し、アクセスを承認ないし拒否した時点で同プロセスは終了します。
  - Server IP Address（サーバIPアドレス）
    認証サーバのアドレスです。（初期設定：10.1.0.1）
  - Server Port Number（サーバポート番号）
    認証メッセージで使用する、認証サーバ上のネットワークポート（UDP）です。（範囲：1～65535、初期設定：1812）

- Secret Txt String(暗号キー)

  クライアントのログオンアクセスを認証する際に使用する暗号キーです。キー(文字列)内では空白は使わないでください。(最大長:20文字)
- Number of Server Transmits (サーバ送信数)

  本製品が認証サーバ経由でログオンアクセスの認証を試みる回数です。(範囲:1～30、初期設定:2)
- Timeout for a reply (応答タイムアウト)

  本製品が要求を再送信する前に、RADIUSサーバからの応答を待つ待機時間を秒数で設定します。(範囲:1～65535、初期設定:5)

・ TACACS設定

- Server IP Address (サーバIPアドレス)

  TACACS+サーバのIPアドレスです。(初期設定:10.11.12.13)
- Server Port Number (サーバポート番号)

  認証メッセージで使用するTACACS+サーバ上のネットワークポート(TCP)です。(範囲:1～65535、初期設定:49)
- Secret Text String (暗号キー)

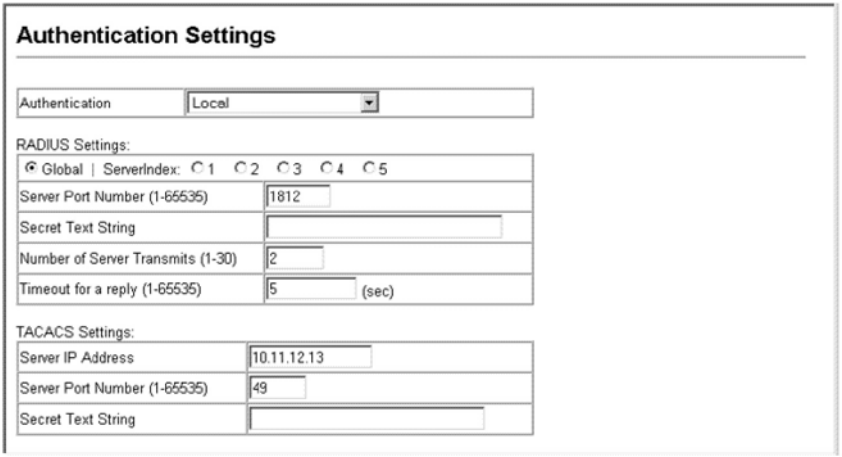
  クライアントのログオンアクセスを認証する際に使用する暗号キーです。キー(文字列)内では空白は使わないでください。(最大長:20文字)

**注意**: ローカルスイッチのユーザデータベースは、CLIを使って手動でユーザ名およびパスワードを入力する必要があります。(p.264の「username (ユーザ名)」をご覧ください。)

WEB：

Security（セキュリティ）→Authentication Settings（認証設定）と選択します。

ご希望のローカルないしリモートの認証設定を行う場合は、認証手順（1～3種類の認証方法）を指定してください。RADIUSないしTACACS*が選択されている場合は、該当するパラメータを入力してください。最後にApply（適用）をクリックしてください。



CLI:

ログオン認証を有効にするため必要となるパラメータをすべて設定します。

```
Console(config)#authentication login radius                          4-71
Console(config)#radius-server port 181                               4-74
Console(config)#radius-server key green                              4-74
Console(config)#radius-server retransmit 5                           4-75
Console(config)#radius-server timeout 10                             4-75
Console(config)#radius-server 1 host 192.168.1.25                    4-73
Console(config)#end
Console#show radius-server                                           4-76

Remote RADIUS server configuration:

Global settings:
 Communication key with RADIUS server: *****
 Server port number:                   181
 Retransmit times:                     5
 Request timeout:                      10

Server 1:
 Server IP address: 192.168.1.25
 Communication key with RADIUS server: *****
 Server port number: 1812
 Retransmit times: 2
 Request timeout: 5
```

```
Console#configure
Console(config)#authentication login tacacs                          4-71
Console(config)#tacacs-server host 10.20.30.40                       4-77
Console(config)#tacacs-server port 200                               4-77
Console(config)#tacacs-server key green                              4-78
Console#show tacacs-server                                           4-78
Server IP address: 10.20.30.40
 Communication key with tacacs server: green
 Server port number: 200
Console(config)#
```

## 3-10-3 HTTP設定

SSL(セキュアソケットレイヤ)を介したHTTPS(セキュア・ハイパーテキスト転送プロトコル)を本製品上で有効に設定し、本製品のWEBインタフェースへのアクセスをより安全なものとすることが可能です(暗号化された接続を利用します)。

コマンド利用:

- HTTPSおよびHTTPSサービスは、それぞれ本製品上で個別に有効にすることが可能です。ただし、二つ以上のサービスで同じUDPポートを使用するように設定することはできません。
- HTTPSを有効にする場合は、ご使用のブラウザのURLフィールドに
  https://機器名 [:ポート番号]
  と入力する必要があります。
- HTTPSを開始すると、接続は以下の順序で行われます。
  - クライアントはサーバのデジタル証明を使ってサーバを認証します。
  - クライアントおよびサーバは、接続で使用するセキュリティプロトコルいくつかにおいてネゴシエーションを行います。
  - クライアントおよびサーバは、データの暗号化および解読で使用するセッションキーを発行します。
- クライアントおよびサーバは、暗号化された安全な接続を確立します。Internet Explorer 5.x以降などのブラウザでは、安全性を示す錠前アイコンが表示されます。
- 以下に、現時点においてHTTPSに対応しているブラウザおよびOSを示します。

表3-4 HTTPS対応表

| WEBブラウザ | OS(オペレーティングシステム) |
|---|---|
| Internet Explorer 5.0以降 | Windows 98、Windows NT(サービスパック6a)、Windows 2000およびWindows XP |

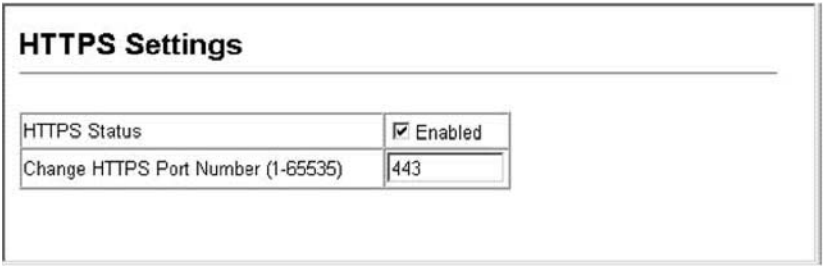
- セキュアサイト証明を指定する場合は、p.82の「セキュアサイト初期証明を置き換える」をご覧ください。

コマンド解説：

- HTTPS Status (HTTPステータス)
  本製品上でHTTPSサーバ機能を有効/無効に設定します。(初期設定：Enabled(有効))
- Change HTTPS Port Number (HTTPSポート番号の変更)
  本製品のWEBインタフェースに接続する際HTTPS/SSLが使用するUDPポートのポート番号となります。(初期設定：ポート443)

WEB：

Security(セキュリティ)→HTTPS Settings(HTTPS設定)と選択します。HTTPSを有効に設定し、ポート番号を指定してApply(適用)をクリックしてください。




CLI：

以下の例では、HTTPSセキュアサーバを有効に設定した上でポート番号を変更しています。

```
Console(config)#ip http secure-server                                    4-31
Console(config)#ip http secure-port 443                                  4-32
Console(config)#
```

### 3-10-3-1 セキュアサイトの初期証明を置き換える

安全のためHTTPSを使ってWEBインタフェースに対しログオンした場合は、本製品用のSSL(セキュアソケットレイヤ)証明が表示されます。初期設定では、Internet Explorer上などで表示される証明は「当サイトは安全なサイトとして認識されていません」といった主旨の警告メッセージと関連付けられています。これは同証明が、認可されている認証団体(権限)により署名されていないためとなります。同警告内容を本製品への接続が安全であることを承認するメッセージに置き換える場合は、まず、認可されている認証団体から固有の証明、プライベートキーならびにパスワードを取得する必要があります。

重要:

最大限の安全を確保するためにも、固有のSSL証明を出来うる限り早期に取得されることをおすすめします。これは、本製品の初期状態の(デフォルト)証明がお客様の購入されたハードウェア固有のものではないためとなります。

上記の各内容/情報が取得できましたら、同内容をTFTPサーバに保管し、以下のコマンドを本製品のCLI画面にて入力して初期(認知されていない)証明を、許可を受けている証明と置き換えてください。

```
Console#copy tftp https-certificate                                    4-65
TFTP server ip address: <server ip-address>
Source certificate file name: <certificate file name>
Source private file name: <private key file name>
Private password: <password for private key>
```

**注意**: 新規の証明を有効とする場合は、本製品をいったんリセットする必要があります。本製品のリセットを行う場合は Console#reloadと入力してください。

## 3-10-4 セキュアシェルの設定

バークリー標準には、もともとUnixシステム用として設計されたリモートアクセスツールが含まれています。これらのツールのうちいくつかはMicrosoft Windowsおよびその他環境でも導入されています。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これらのツールは、敵意ある攻撃の対象となる恐れがあります。

SSH8セキュアシェル)は、従来のバークリーリモートアクセスツールに取って代わる、より安全なサーバ/クライアントアプリケーションを含みます。SSHはまた本製品に対し、Telnetに代わるより安全なリモート管理アクセスを提供します。クライアントがSSHプロトコルを通じて本製品に通信を行うと、本製品はパブリックキーを発行します。クライアントは、アクセス認証時にこのパブリックキーならびにローカルのユーザ名およびパスワードを使用します。SSHはまた、本製品とSSH対応管理ステーションクライアントとの間でやりとりするデータ転送すべてを暗号化します。このためネットワーク経由で送信されるデータに対する改ざんを防止し、その整合性を確保することが可能となります。

なお、SSHプロトコル経由で本製品に対し管理アクセスを行う場合は、アクセスを行う管理ステーション側でSSHクライアントをインストールする必要があります。

**注意**:　本製品はSSHバージョン1.5および2.0の両者に対応しています。

コマンド利用:

本製品上のSSHサーバは、パスワード認証とパブリックキーによる認証の両者に対応しています。SSHクライアント側でパスワード認証が指定されている場合、パスワードはAuthentication Settings (認証設定:p.75)の設定内容に基づき、ローカルまたはRADIUS/TACACS+リモート認証サーバ経由で認証されるかたちになります。クライアントによりパブリックキー認証が指定されている場合は、以下の説明をご覧の上、クライアントおよび本製品の両者上で認証キーを必ず設定してください。なおパブリックキーとパスワード認証のどちらを使用するかに関わらず、本製品上では認証キーを発行し(SSH Host Key Settings(SSHホストキー設定))、かつSSHサーバを有効にする必要があります(Authentication Settings(認証設定))。

SSHサーバを使用する場合は以下の操作を行ってください。

1. ホストキー・ペアの発行

   SSH Host Key Settings(SSHホストキー設定)ページ上でホストのパブリック/プライベートキー・ペアを作成してください。

2. ホストパブリックキーをクライアントに提供

SSHクライアントプログラムの多くは、本製品との接続の初期化中にホストパブリックキーを自動的にインポートするようになっています。その他の場合は、管理ステーション上で既知ホストのファイルを手動で作成し、ホストパブリックキーを同ファイル内に入れる必要があります。以下の例では、既知のホストファイル内でパブリックキーがどのように表示されるかを示しています。

```
10.1.0.54 1024 35 156849954018676692593339467750546173253136748908365472541502024559319986854435836165199992332978176606583095610825913212890233765468017262725714134287629413011961955667825956641048695742788814620651941746772984865468615717739390164779355942303577413098022737087794545240839717526463580581767167095748047761171
```

3. クライアントのパブリックキーを本製品にインポートする

copy tftp public-keyコマンドを使って、SSHクライアントから本製品への管理アクセスを許可するためのパブリックキーが含まれているファイルをコピーしてください。(なお、これらのクライアントはUser Accounts (ユーザアカウント)ページ経由で本製品上ローカルで設定する必要があります。詳しくはp.73をご覧ください。)同クライアントはどれも、これらのキーを使って後で認証されるかたちになります。現時点において、ファームウェアは標準UNIX形式に基づくパブリックキーのみ受け付けるようになっています。以下の例では、RSAバージョン1キーを使用しています。

```
1024 35 134108168560989392104094492015542534763164192187295892114317388005553616163105177594083868631109291232226828519254374603100937187721199696317813662774141689851320491172048303392543241016379975923714490119380060902539484084827178194372288402533115952134861022902978982721353267131629432532818915045306393916643 steve@192.168.1.19
```

4. オプションパラメータの設定

SSH Settings (SSH設定)ページにて、認証タイムアウト、リトライ数およびサーバキーサイズなどを含むオプションパラメータの設定を行ってください。

5. SSHサービスを有効にする

SSH Settings (SSH設定)ページにて、本製品上のSSHサーバを有効に設定してください。

6. チャレンジ・レスポンス認証

SSHクライアントが本製品への接続を試みた時点で、SSHサーバはホストキー・ペアを使ってセッションキーならびに暗号化方式の確認(ネゴシエーション)を行います。本製品上に保存されているパブリックキーに対応するプライベートキーを所有するクライアントのみがアクセス可能となります。同プロセス中の流れは以下のようになります。

a クライアントから本製品に対しパブリックキーを送信します。

b　本製品はクライアントのパブリックキーと自身のメモリ内に保存されているキーとを比較します。

c　両者が合致した場合、本製品は同パブリックキーを使って複数バイトのランダムシーケンスを暗号化し同ストリングをクライアントに送信します。

d　クライアントは自身のプライベートキーを使って同バイトを複合化し、複合化されたバイトを本製品に送信します。

e　本製品は複合化されたバイトと、自身が最初に送った元々のバイトを比較します。両者が合致した場合は、その時点でクライアントのプライベートキーが正当なパブリックキーに対応するものであることが証明されるため、クライアントも認証します。

**注意:** 1. SSHをパスワード認証のみでお使いになる場合は、ホストパブリックキーをクライアントに提供する必要があります。同キーの提供は初期接続中に行うか、既知ホストファイル内に手動で入力するかたちになります。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。

2. SSHサーバは、最大4セッションまでのクライアントセッションに対応しています。同最大数には、現在のTelnetセッション数およびSSHセッション数の両者が含まれます。

### 3-10-4-1 ホストキー・ペアを発行する

パブリック/プライベートキー・ペアを使用することにより、SSHクライアントと本製品との間で安全に通信を行うことが可能となります。同キー・ペアを発行した後は、ホストパブリックキーをSSHクライアントに提供し、またクライアントのパブリックキーを本製品に提供する必要があります。詳細については、前述の「コマンド利用」をご覧ください。

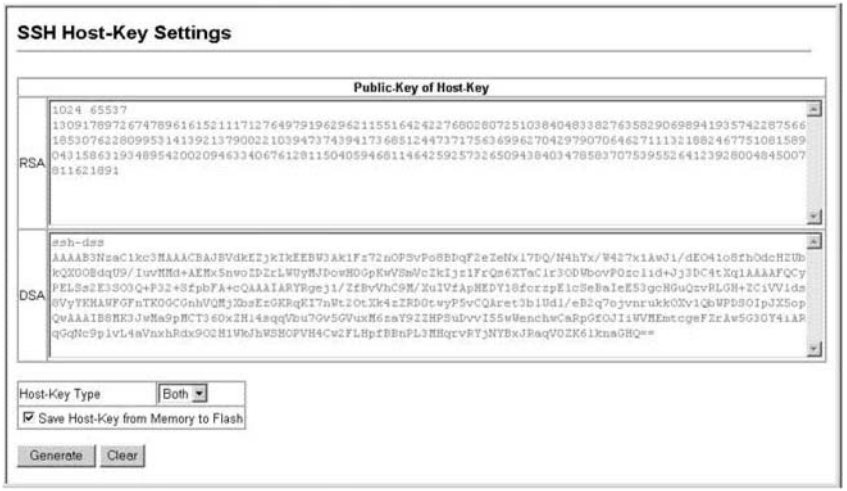
フィールド解説:

- Public-Key of Host-Key (ホストキーのパブリックキー)
  ホストのパブリックキーです。
  - RSA (バージョン1)
    1番目のフィールドはホストキーのサイズを示し(例:1024)、2番目のフィールドは符号化されたパブリック指数(例:65537)、最後のストリングは符号化された係数を示します。
  - DSA(バージョン2)
    1番目のフィールドは、SSHで使用されている暗号化方式がDSS(デジタル署名標準)に基づいていることを示します。最後のストリングは符号化された係数となります。
- Host-Key Type (ホストキーの種類)
  ホストキー・ペア(パブリック/プライベートキー)を発行する際に使用するキーの種類です。(範囲:RSA(バージョン1)、DSA(バージョン2)、両方　初期設定:RSA)
- クライアントが最初に本製品と接続を確立する際、SSHサーバはRSAないしDSAを使ってキー交換を行い、次いでクライアントとネゴシエーションを行ってデータ暗号化用としてDES(56ビット)または3DES(168ビット)を選択します。
- Save Host-Key from Memory to Flash (ホストキーをメモリからフラッシュに保存する)
  ホストキーをRAMからフラッシュメモリに保存します。この他の場合、初期設定により、ホストキー・ペアはRAMに保管されるようになっています。なお当設定オプションは、ホストキー・ペアを発行する前に設定しておく必要があります。
- Generate (発行)
  ホストキー・ペアを発行する際に使用するキーです。なお、SSH Server Settings(SSHサーバ設定)ページ上でSSHサーバを有効にする前にまずホストキー・ペアを発行する必要があります。
- Clear (消去)
  RAMおよびフラッシュメモリの両者からホストキーを消去します。

WEB:

Security(セキュリティ)→SSH→Host-Key Settings(ホストキー設定)と選択します。

次にドロップダウンリストからホストキーの種類を選択してください。必要に応じて、「Save the host key from memory to flash (キー発行前にホストキーをメモリからフラッシュに保存)」オプションをお選びください。最後にGenerate (発行)をクリックしてください。




CLI:

以下の例では、RSAとDSAの両アルゴリズムを使ってホストキー・ペアを発行し、同キーをフラッシュメモリーに保存した上でホストのパブリックキーを表示しています。

```
Console#ip ssh crypto host-key generate                                    4-36
Console#ip ssh save host-key                                               4-36
Console#show public-key host                                               4-36
Host:
RSA:
1024 65537 1272509225449264021313365145461311896790551923600760286530067618
2409690947448320102524878965977592168322225584652387791546479807396314033
8692579310510576521224305280786588548578927260293786608923684142327591212 7
6032591968369705343933643844522333518828717389689451172929051081391964202 5
1909321043285790457648 91
DSA:
ssh-dss AAAAB3NzaC1kc3MAAACBAN6zwIqCqDb3869jYVXlME1sHL0EcE/Re6hlasfEthIwmj
hLY4O0jqJZpcEQUgCfYlum0Y2uoLka+Py9ieGWQ8f2gobUZKIICuKg6vjO9XTs7XKc05xfzkBi
KviDa+2OrIz6UK+6vFOgvUDFedlnixYTVo+h5v8r0ea2rpnO6DkZAAAAFQCNZn/x17dwpW8RrV
DQnSWw4Qk+6QAAAIEAptkGeB6B5hwagH4gUOCY6i1TmrmSiJgfwO9OqRPUMbCAkCC+uzxatOo7
drnIZypMx+Sx5RUdMGgKS+9ywsa1cWqHeFY5ilc3lDCNBueeLykZzVS+RS+azTKIk/zrJh8GLG
Nq375R55yRxFvmcGIn/Q7IphPqyJ3o9MK8LFDfmJEAAACAL8A6tESiswP2OFqX7VGoEbzVDSOI
RTMFy3iUXtvGyQAOVSy67Mfc3lMtgqPRUOYXDiwIBp5NXgilCg5z7VqbmRm28mWc5a//f8TUAg
PNWKV6W0hqmshQdotVzDR1e+XKNTZj0uTwWfjO5Kytdn4MdoTHgrbl/DMdAfjnte8MZZs=

Console#
```

### 3-10-4-2 SSHサーバの設定

SSHサーバには、認証用の基本設定が含まれます。

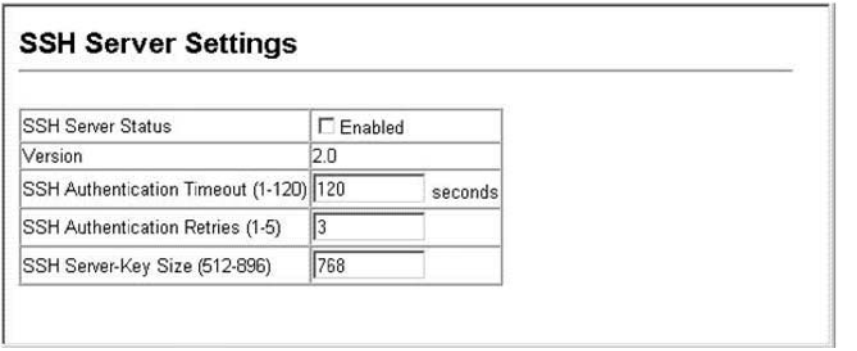
フィールド解説:

- SSH Server Status(SSHサーバステータス)
  本製品上でSSHサーバを有効/無効に設定します。(初期設定:Disabled(無効))
- Version (バージョン)
  セキュアシェルのバージョンです。表示内容はVersion 2.0となりますが、本製品はSSHバージョン1.5および2.0のいずれのクライアントからの管理アクセスにも対応しています。
- SSH Authentication Timeout(SSH認証タイムアウト)
  認証中に、クライアントからの応答があるまでSSHサーバが待機する時間を秒で設定します。(範囲:1～120秒、初期設定:120秒)
- SSH Authentication Retries (SSH認証リトライ数)
  認証失敗と判定されるまでにクライアントが認証を試行できる回数です。失敗と判定された時点でクライアントは認証プロセスを最初からやり直すかたちになります。(範囲:1～5回、初期設定:3)
- SSH Server-Key Size (SSHサーバキーサイズ)
  SSHサーバキーのサイズを指定します。(範囲:512～896ビット、初期設定:768)
  - サーバキーとは、本製品の外部ではけして共有されないプライベートキーを指します。
  - ホストキーはSSHクライアントと共有されるほか、1024ビットで固定されています。

WEB:

Security (セキュリティ)→Settings(設定)と選択します。

SSHを有効に設定し、必要に応じて認証パラメータを調整してApply(適用)をクリックしてください。なお、SSHサーバを有効にする前に必ずSSH Host-Key Settings(SSHホストキー設定)ページ上でホストキー・ペアを発行する必要があります。




CLI:

以下の例では、SSHを有効にし認証パラメータの設定を行った上で現在の設定を表示しています。同内容は、管理者がSSH経由での接続を確立した上で接続を無効にしている様子を示しています。

```
Console(config)#ip ssh server                                          4-36
Console(config)#ip ssh timeout 100                                     4-37
Console(config)#ip ssh authentication-retries 5                        4-37
Console(config)#ip ssh server-key size 512                             4-38
Console(config)#end
Console#show ip ssh                                                    4-40
SSH Enabled - version 2.0
Negotiation timeout: 120 secs; Authentication retries: 5
Server key size: 512 bits
Console#show ssh                                                       4-41
Connection Version State                Username Encryption
  0          2.0   Session-Started      admin    ctos aes128-cbc-hmac-md5
                                                  stoc aes128-cbc-hmac-md5
Console#disconnect 0                                                   4-18
Console#
```

## 3-10-5 ポートセキュリティの設定

ポートセキュリティ機能を使用することにより、本製品をいずれか1つのスイッチポート経由で設定することが可能となります。同ポートを経由したネットワークへのアクセスを許可された、1つないしそれ以上の機器MACアドレスを備えています。

ポート上でポートセキュリティを有効にした場合、あらかじめ設定された最大(アドレス)数に達した時点で、本製品は同ポート上における新規MACアドレスの学習を停止します。着信トラフィックのうち、送信元(ソース)アドレスが動的/固定アドレステーブル上にすでに存在するもののみが、同ポート経由でネットワークにアクセスすることを許可されるかたちとなります。許可を受けていないMACアドレスを持つ機器が同スイッチポートへのアクセス(侵入)を試みた場合、本製品は同行為を検出し、自動的に該当ポートを無効に設定してトラップメッセージを発信します。

ポートセキュリティを使用する場合は、ポート上で許可するアドレスの最大数を指定し、同ポート上で受信されるフレームの＜source MAC address, VLAN(送信元MACアドレス、VLAN)＞ペアを本製品側で動的に学習するよう設定する必要があります。なお、Static Address Table (固定アドレステーブル、p.156)を使って手動で安全なアドレスを追加することも可能です。同ポート上でMACアドレスの最大数に達した場合、同ポートはアドレスの学習を停止します。アドレステーブル上にすでに存在するMACアドレスはそのまま保管され、エージアウトすることはありません。他のいかなる機器が同ポートの使用を試みても、本製品へのアクセスは拒否されるかたちになります。

コマンド利用:

- セキュアポートは以下の制約を受けます。
    - ポート監視(モニタリング)は使用できません。
    - 複数のVLANを使用するポートとしては利用できません。
    - 固定/動的トランクのメンバーポートとしては利用できません。
    - ネットワーク間の相互接続を行う機器とは接続できません。
- セキュアポート上で許可されているMACアドレス最大数は、初期設定では0となっています。同ポート上でアクセスを許可する場合は、同最大数設定を1～1024の範囲で指定する必要があります。
- ポートがセキュリティ侵害のため無効(シャットダウン)されている場合は、「インタフェースの接続設定」(p.121)より、手動にて再度同ポートを有効に設定する必要があります。

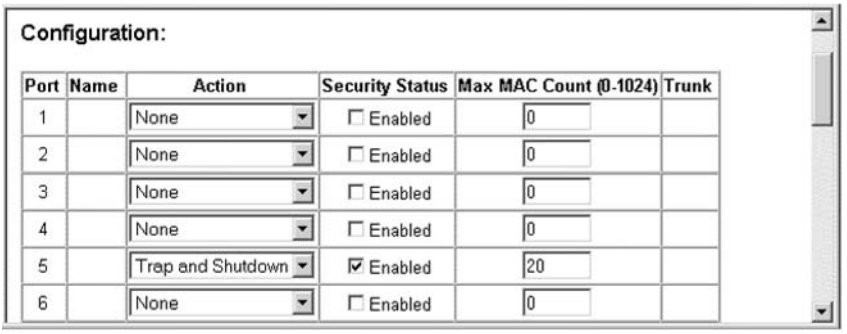
コマンド解説：

- Port (ポート)
  ポート番号です。
- Name (名称)
  説明文です(p.367)。
  - Action (対処)
    ポートへのセキュリティ侵害が検出された際に実行する内容を示します。
  - None (なし)
    なにも行動しません。(初期設定)
  - Trap (トラップ)
    SNMPトラップメッセージを送信します。
  - Shutdown (シャットダウン)
    ポートを無効に設定します。
  - Trap and Shutdown (トラップを送信しシャットダウン)
    SNMPトラップメッセージを送信してポートを無効に設定します。
- Security Status(セキュリティステータス)
  ポート上でポートセキュリティを有効/無効に設定します。(初期設定：Disabled(無効))
- Max MAC Count(最大MACアドレスカウント数)
  ポート上で学習可能なMACアドレスの最大数です。(範囲：0～1024、0=無効)
- Trunk (トランク)
  ポートが所属するトランクの番号です(該当時)(p.125-126)

WEB：

Security (セキュリティ) →Port Security(ポートセキュリティ)と選択します。

ポート上でセキュリティを有効にする場合は、Status(ステータス)欄のチェックボックスにチェックマークを入れた上で、同ポート上で許可するMACアドレスの最大数を指定しApply(適用)をクリックしてください。



CLI:

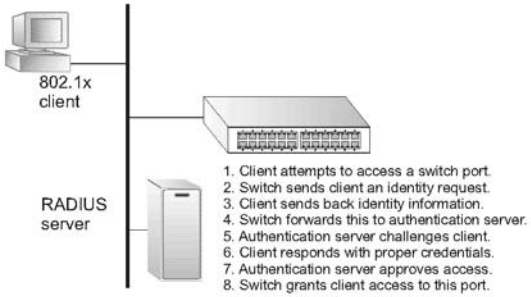
以下の例ではまず対象（ターゲット）ポートを選択し、同ポートのセキュリティ対処設定を「トラップ送信後ポートを無効にする」とし、同ポート上で許可するMACアドレスの最大数を指定した上で同ポート上でポートセキュリティを有効に設定しています。

```
Console(config)#interface ethernet 1/5
Console(config-if)#port security action trap-and-shutdown          4-79
Console(config-if)#port security max-mac-count 20                  4-79
Console(config-if)#port security                                   4-79
Console(config-if)#
```

## 3-10-6 802.1Xポート認証の設定

ネットワークスイッチは、クライアントPCを接続するだけでネットワーク上の資源に対するオープンかつ簡単なアクセス手段を提供することが可能です。設定およびアクセスが自動で行える点は非常に便利ですが、このままでは、不正利用者も簡単にネットワークに侵入し重要なデータに接触できてしまうことになります。

IEEE802.1X(ドット1X)標準はポートベースのアクセス制御プロシージャを定義しており、ユーザに対しまず認証用の信用情報の提出を要求することで、ネットワークへの不正アクセスを阻止することが可能となっています。ネットワーク上の全スイッチポートへのアクセスはサーバにて集中的に制御することが可能となっています。つまり許可を受けているユーザであれば、ネットワーク内どこからでも同じ認証用の信用情報を使うことが可能となります。




本製品はEAPOLを使って認証プロトコルメッセージをクライアントと交換するほか、リモートRADIUS認証サーバを使ってユーザの識別およびアクセス権限の確認を行います。クライアント(サプリカント＝認証依頼者)がスイッチポートに接続すると、本製品(認証者)はEAPOL識別要求を同クライアントに対し返信します。クライアントは自身の識別情報(ユーザ名など)を本製品へのEAPOL応答にて示し、次いで本製品は同情報をRADIUSサーバに転送します。RADIUSサーバはクライアントの識別情報を確認し、アクセスチャレンジをクライアントに対し送信します。RADIUSサーバから送られるEAPパケットはチャレンジだけでなく、使用する認証方式も含んでいます。クライアントソフトウェアおよびRADIUSサーバの設定により、クライアントは認証方式を拒否し別途要求を送信することが可能です。なお認証方式はMD5となっていなければなりません。クライアントは適切な方式に対し自身の信用情報(パスワードや証明など)を返答します。RADIUSサーバはクライアントの信用情報を確認し、受理ないし拒否パケットにて返答します。認証が成功した場合、本製品はクライアントに対しネットワークへのアクセスを許可します。その他の場合、ネットワークへのアクセスは拒否されポートも遮断状態のままとなります。

本製品上で802.1Xを使用する場合は以下の条件を満たす必要があります。

- 本製品にはIPアドレスを割り当てておく必要があります。
- RADIUS認証は、本製品ならびに指定されたRADIUSサーバのIPアドレス上で有効と設定する必要があります。
- 802.1Xは本製品全体で(グローバルに)有効に設定しておく必要があります。

・ 使用するポートはすべて、ドット1X「オート(auto)」モードに設定する必要があります。
・ 認証を必要とするクライアントにはすべて、ドット1Xクライアントソフトウェアをあらかじめインストールし適切に設定しておく必要があります。
・ RADIUSサーバおよび802.1Xクライアントは EAPに対応している必要があります。(本製品は、サーバからクライアントに対しEAPパケットを渡すためEAPOLのみに対応しています。)
・ RADIUSサーバおよびクライアントは、どちらも同じEAP認証タイプ(MD5)に対応している必要があります。(クライアントによってはWindows上ですでに同タイプに対応しているものがあります。その他の場合はドット1Xクライアント側でサポートする必要があります。)

### 3-10-6-1 802.1Xグローバル設定の表示

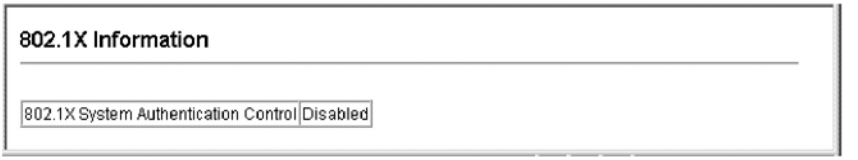
802.1Xプロトコルはクライアント認証機能を提供します。

コマンド解説：

・ 802.1X System Authentication Control (802.1Xシステム認証制御)
802.1Xのグローバル(スイッチ全体での)設定です。

WEB：

Security(セキュリティ)→802.1X→Information(情報)と選択します。




CLI：

以下の例では、802.1Xの初期グローバル設定を表示しています。

```
Console#show dot1x                                                    4-86
Global 802.1X Parameters
 system-auth-control: enable

802.1X Port Summary

Port Name  Status         Operation Mode   Mode               Authorized
1/1        disabled       Single-Host      ForceAuthorized    n/a
1/2        disabled       Single-Host      ForceAuthorized    n/a
:
802.1X Port Details

802.1X is disabled on port 1/1
:
802.1X is disabled on port 1/26
Console#
```

### 3-10-6-2 802.1Xグローバル設定の変更

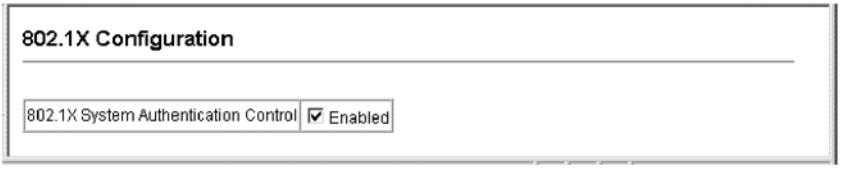
802.1Xプロトコルはクライアント認証機能を提供します。

コマンド解説:

- 802.1X System Authentication Control (802.1Xシステム認証制御)
  802.1Xのグローバル設定を変更します。(初期設定:Disabled(無効))

WEB:

Security(セキュリティ)→802.1X→Configuration(設定)と選択します。802.1Xを本製品全体で(グローバルに)有効に設定し、Apply(適用)をクリックしてください。




CLI:以下の例では、802.1Xを本製品全体で有効に設定しています。

```
Console(config)#dot1x system-auth-control                    4-81
Console(config)#
```

### 3-10-6-3 802.1X用にポートを設定する

802.1Xを有効にした場合は、1)クライアントと本製品(認証者)との間で行われる認証プロセス用の各パラメータの設定ならびに2)本製品と認証サーバとの間で行われるクライアント識別確認プロセス用のパラメータの設定を行う必要があります。以下に、該当パラメータを解説します。

コマンド解説:

- Port (ポート)
  ポート番号です。
- Status (ステータス)
  ポート上で認証が有効ないし無効になっていることを示します。(初期設定:Disabled(無効))
- Operation Mode (実行モード)
  802.1Xで認証を受けているポート1ポートに対し、単一ないし複数のホスト(クライアント)の接続を許可します。(オプション:Single-Host (単一ホスト)、Multi-Host(複数ホスト)

初期設定：Single-Host）

- Max Count（最大カウント）

  Multi-Host(複数ホスト)実行モード選択時に、ポートに接続することのできるホストの最大数となります。（範囲：1～1024、初期設定：5）

- Mode（モード）

  認証モードを以下のいずれかの設定します。

  - Auto（自動）

    ドット1X対応クライアントに対し、認証サーバから許可（認証）を得るよう要求します。ドット1X非対応のクライアントはアクセスを拒否されるかたちになります。

  - Force-Unauthorized（すべて未許可）

    クライアントがドット1X対応・非対応のどちらであるかにかかわらず、すべてのクライアントに対しアクセスを拒否するようポートを設定します。

- Re-authen（再認証）

  Re-authentication Period(再認証期間)で指定された時間が経過した時点でクライアントを再度認証するよう設定します。Re-authentication(再認証)機能は、スイッチポートいずれかに新しく機器が接続されているかどうか確認する場合に利用可能です。（初期設定：Disabled(無効)）

- Max-Req（最大要求回数）

  認証セッションがタイムアウトする前に、スイッチポートがクライアントに対し再度EAP要求パケットを送信する最大回数を設定します。（範囲：1～10、初期設定：2）

- Quiet Period（沈黙期間）

  Max Request Count(最大要求回数)を超過した後、スイッチポートが新しくクライアントを取得する前に待機する時間を設定します。（範囲：1～65535秒、初期設定：60秒）

- Re-authen Period（再認証期間）

  この時間が経過した時点で、接続されているクライアントは再度（必ず）認証されるかたちになります。（範囲：1～65535秒、初期設定：3600秒）

- TX Period（送信期間）

  認証セッション中、本製品が再度EAPパケットを送信する前に待機する時間を設定します。（範囲：1～65535秒、初期設定：30秒）

- Authorized（許可ステータス）

  - Yes（許可済）

    接続されているクライアントはすでに許可を受けています。

  - No（未許可）

    接続されているクライアントは許可されていません。

  - 空白状態

    ポート上でドット1Xが無効となっている場合は何も表示されません。

- Supplicant（サプリカント/許可依頼者）

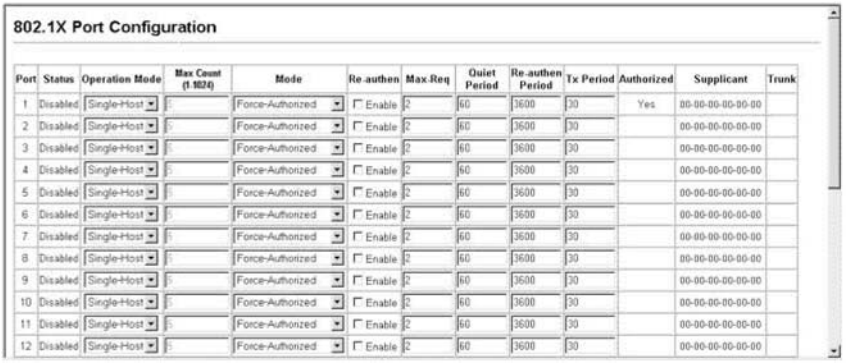
  接続されているクライアントのMACアドレスを示します。

・ Trunk (トランク)
ポートがトランクポートとして設定されていることを示します。

WEB:

Security (セキュリティ)→802.1X→Port Configuration (ポート設定)と選択します。

必要に応じてパラメータ設定を変更し、Apply(適用)をクリックしてください。



CLI:

以下の例では、ポート2上で802.1Xパラメータの設定を行っています。表示されている各フィールドの詳細については、p.337の「show dot1x(ドット1X情報の表示)」をご覧ください。

```
Console(config)#interface ethernet 1/2                                  4-108
Console(config-if)#dot1x port-control auto                              4-82
Console(config-if)#dot1x re-authentication                              4-84
Console(config-if)#dot1x max-req 5                                      4-82
Console(config-if)#dot1x timeout quiet-period 30                        4-84
Console(config-if)#dot1x timeout re-authperiod 1800                     4-85
Console(config-if)#dot1x timeout tx-period 40                           4-85
Console(config-if)#exit
Console(config)#exit
Console#show dot1x                                                      4-86
Global 802.1X Parameters
 system-auth-control: enable

802.1X Port Summary

Port Name  Status         Operation Mode   Mode                Authorized
1/1        disabled       Single-Host      ForceAuthorized     n/a
1/2        enabled        Single-Host      auto                yes
:
1/26       disabled       Single-Host      ForceAuthorized     n/a

802.1X Port Details

802.1X is disabled on port 1/1

802.1X is enabled on port 1/2
 reauth-enabled: Enable
 reauth-period:  1800
 quiet-period:   30
 tx-period:      40
 supplicant-timeout:   30
 server-timeout: 10
 reauth-max:     2
 max-req:        5
Status              Authorized
Operation mode      Single-Host
Max count           5
Port-control        Auto
Supplicant          00-90-cc-49-5e-dc
Current Identifier  3

Authenticator State Machine
State               Authenticated
Reauth Count        0

Backend State Machine
State               Idle
Request Count       0
Identifier(Server)  2

Reauthentication State Machine
State               Initialize
:
802.1X is disabled on port 1/26
Console#
```

### 3-10-6-4 802.1X統計情報の表示

本製品は、各ポート上におけるドット1X関連の統計情報を表示することが可能です。

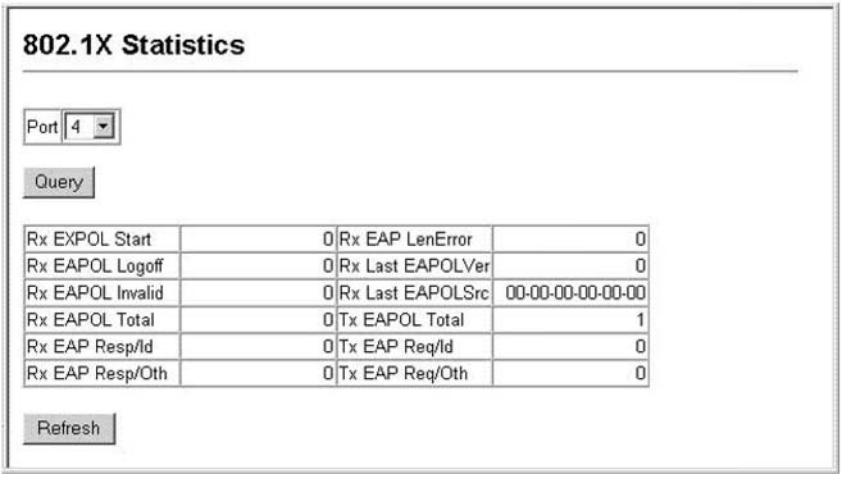
表3-5 802.1X統計情報

| パラメータ | 内容 |
|---|---|
| Rx EAPOL Start | 当Authenticator(認証者)がこれまで受信した、EAPOL Startフレームの数を示します。 |
| Rx EAPOL Logoff | 当Authenticator(認証者)がこれまで受信した、EAPOL Logoffフレームの数を示します。 |
| Rx EAPOL Invalid | 当Authenticator(認証者)がこれまで受信したEAPOLフレームのうち、フレームの種類が認識できなかったものの数を示します。 |
| Rx EAPOL Total | フレームの種類を問わず、当Authenticator(認証者)がこれまで受信した正常なEAPOL フレームの数を示します。 |
| Rx EAP Resp/Id | 当Authenticator(認証者)がこれまで受信した、EAP Resp/Idフレームの数を示します。 |
| Rx EAP Resp/Oth | 当Authenticator(認証者)がこれまで受信したEAP Response負フレームのうち、Resp/Idフレームを除いたものの数を示します。 |
| Rx EAP LenError | 当Authenticator(認証者)がこれまで受信したEAPOLフレームのうち、Packet Body Lengthフィールドが不正なものの数を示します。 |
| Rx Last EAPOLVer | もっとも最近受信されたEAPOLフレーム内で見られた、プロトコルバージョンとなります。 |
| Rx Lst EAPOLSrc | もっとも最近受信されたEAPOLフレーム内で見られた、送信元MACアドレスとなります。 |
| Tx EAP Req/Id | 当Authenticator(認証者)によりこれまで送信された、EAP Req/Idフレームの数を示します。 |
| Tx EAP Req/Oth | 当Authenticator(認証者)によりこれまで送信されたEAP Requestフレームのうち、Req/Idフレームを除いたものの数を示します。 |

WEB：

Security(セキュリティ)→802.1X→Statistics (統計)と選択します。

統計を参照するポートを選び、Query(照会)をクリックしてください。統計情報を更新する場合はRefresh(更新)をクリックしてください。




CLI：

以下の例では、ポート4の802.1X統計情報を表示しています。

```
Console#show dot1x statistics interface ethernet 1/4                4-86

Eth 1/4
Rx: EAPOL      EAPOL      EAPOL      EAPOL      EAP        EAP        EAP
    Start      Logoff     Invalid    Total      Resp/Id    Resp/Oth LenError
        2           0          0       1007       672          0        0

    Last       Last
EAPOLVer      EAPOLSrc
       1      00-90-CC-98-73-21

Tx: EAPOL       EAP        EAP
    Total      Req/Id     Req/Oth
     2017      1005         0
Console#
```

### 3-10-6-5 管理アクセス用IPアドレスのフィルタリング

WEBインタフェース、SNMPおよびTelnet経由で本製品への管理アクセスを許可するIPアドレスないしIPアドレスグループは、最大で16個までリスト内に登録することが可能となっています。

コマンド利用：

- 初期設定では、管理インタフェースはすべてのIPアドレスに対し解放（オープン）されています。フィルタリストにエントリ（アドレス）を何か追加した時点で、同インタフェースへのアクセスは指定されたアドレスのみに限定されます。
- 不正なアドレスから本製品上の管理インタフェースに対しアクセスが試みられた場合、本製品は該当する接続を拒絶し、システムログ内にイベントメッセージを記録した上でトラップメッセージをトラップマネージャに送信します。
- IPアドレスはSNMP用、WEB用およびTelnet用というようにそれぞれ設定することが可能です。各グループとも、最大で5つまでの異なるアドレスセットを設定することが可能です。アドレスは個別のアドレスないしアドレスの範囲を指定するかたちになります。
- 複数のアドレスを同一グループ(SNMP、WEBないしTelnet)に入力する場合、本製品はアドレスの範囲が重複するものは受け付けないようになっています。異なるグループ複数に対しアドレスを入力する場合は、アドレス範囲が重複していても本製品は同アドレスを受け付けます。
- 指定された範囲からアドレスを個別に削除することはできません。範囲全体をいったん削除した上でアドレスを再度入力してください。
- アドレス範囲の削除は開始アドレスのみ指定するだけで実行できるようになっています。また開始アドレスと終了アドレスの両者を指定して削除することも可能です。

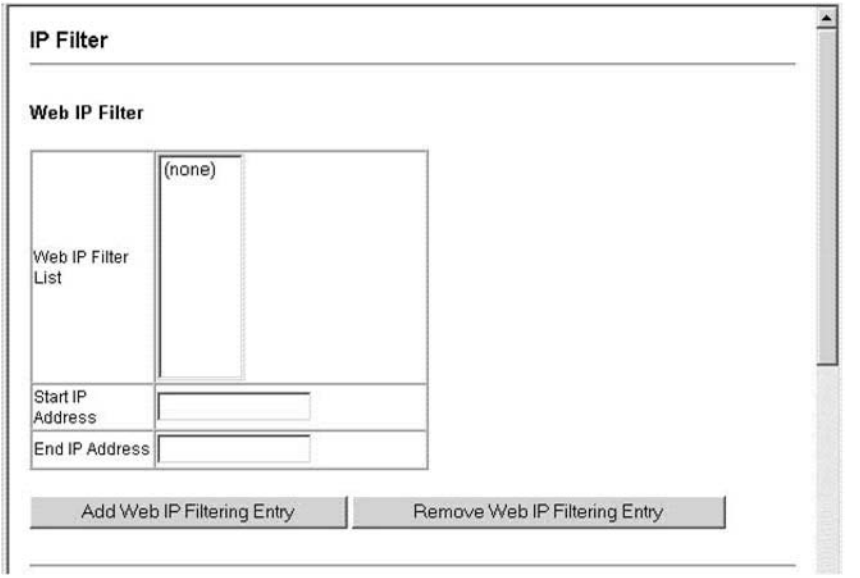
コマンド解説：

- WEB IP Filter (WEB IPフィルタ)
  WEBグループのIPアドレスを設定します。
- SNMP IP Filter (SNMP IPフィルタ)
  SNMPグループのIPアドレスを設定します。
- Telnet IP Filter( Telnet IPフィルタ)
  TelnetグループのIPアドレスを設定します。
- IP Filter List (IPフィルタリスト)
  当インタフェースに対する管理アクセスを許可されているIPアドレスを表示します。
- Start IP Address (開始IPアドレス)
  単一のIPアドレスか、指定範囲の先頭となるIPアドレスを表示します。
- End IP Address (終了IPアドレス)
  指定範囲の最後にあたるIPアドレスです。

・ Add/Remove Filtering Entry (フィルタリングエントリの追加/削除)
一覧上のIPアドレスの追加/削除を行います。

WEB:

Security(セキュリティ)→IP Filter(IPフィルタ)と選択します。インタフェースに対する管理アクセスを許可するIPアドレスないしアドレス範囲を指定し、Add IP Filtering Entry (IPフィルタリングエントリの追加)をクリックしてください。



CLI:

以下の例では、指定ポートに対しSNMPアクセスを許可しています。

```
Console(config)#management snmp-client 10.1.2.3                    4-28
Console(config)#end
Console#show management all-client
Management IP Filter
 HTTP-Client:
  Start IP address  End IP address
-----------------------------------------------

SNMP-Client:
 Start IP address  End IP address
-----------------------------------------------
1. 10.1.2.3       10.1.2.3

TELNET-Client:
 Start IP address  End IP address
-----------------------------------------------

Console#
```

## 3-10-7 ACL(アクセス制御リスト)

ACLは、IPフレームのパケットフィルタリング機能(アドレス、プロトコル、レイヤ4プロトコルポート番号ないしTCP制御コードなどに基づくもの)およびその他フレームのパケットフィルタリング機能(MACアドレスないしイーサネットタイプに基づくもの)を提供します。着信パケットのフィルタリングを行う場合は、アクセスリストをまず作成し、フィルタリングで使用するルールを追加した上で同リストを特定のポートにバインド(固定)する必要があります。

## 3-10-7-1 ACLの設定

ACLとは、IPアドレス、MACアドレスないしその他の指定基準を用いた許可/拒否条件を順番に定めたリストを指します。本製品は着信/発信パケットに対し、ACL上の条件を一つ一つ当てはめ確認（試験）を行います。パケットはいずれかの許可ルールとの合致が認められた時点で受理されるほか、いずれかの拒否ルールと一致した時点で即座に破棄されるかたちになります。リスト上のどの許可ルールとも合致しない場合、該当パケットは破棄されます。一方、リスト上のどの拒否ルールとも合致しない場合、該当パケットは受理されます。

コマンド利用：

ACLには以下の制限が適用されます。

- 各ACLとも、設定可能なルールは32個までとなります。
- ACLは最大で88個まで設定可能となっています。
- ただしリソース制限の理由上、ポートにバインドするルールは平均で20個を越えないようにする必要があります。
- 本製品は、着信(ingress)フィルタリング用のACLにのみ対応します。ただし着信フィルタリングにつき、いずれのポートに対してもバインド可能なIP ACLは1つのみとなり、本製品全体（グローバル）でバインド可能なMAC ACLも1つのみとなります。つまり、1つのインタフェースに対しバインド可能なACLの数は1)着信IP ACLおよび2)着信MAC ACLの2つのみとなります。

有効な（アクティブとなっている）ACLは、以下の順番にて確認が行われます。

1. 着信ポート用の着信MAC ACL内のユーザ定義ルール
2. 着信ポート用の着信IP ACL内のユーザ定義ルール
3. 着信ポート用の着信IP ACL内の明示（Explicit）初期設定ルール(permit any any: any any)
4. 着信ポート用の着信MAC ACL内の明示（Explicit）初期設定ルール(permit any any: any any)
5. いずれの明示ルールとも合致しない場合、暗示（implicit）初期設定はpermit all（すべて許可)となります。

### 3-10-7-2 ACL名および種類の設定

ACL Configuration (ACL設定)ページにてACLの名称および種類を指定することが可能です。

コマンド解説:

- Name (名称)
  ACLの名称を16文字以内で設定します。
- Type (種類)
  以下の3種類のフィルタリングモードが選択可能です。
  - Standard (標準)
    送信元IPアドレスをもとにパケットをフィルタリングするIP ACLモードです。
  - Extended (拡張)
    送信先IPアドレス、プロトコルの種類ならびにプロトコルポート番号に基づきパケットのフィルタリングを行うIP ACLモードです。「TCP」プロトコルが指定されている場合は、TCP制御モードに基づきパケットのフィルタリングを行うことも可能です。
  - MAC
    送信元ないし送信先MACアドレスおよびイーサネットフレームタイプ(RFC 1060)に基づきパケットのフィルタリングを行うMAC ACLモードです。

WEB:

Security (セキュリティ)→ACL→Configuration (設定)と選択します。

Name (名称)フィールドにACL名を入力し、種類をIP Standard (IP標準)、Extended(拡張)およびMACの中から選んでください。最後にAdd(追加)をクリックし、新規リスト用の設定ページを開いてください。

CLI:

以下の例では、「david」という名称の標準IP ACLを作成しています。

```
Console(config)#access-list ip standard david                    4-90
Console(config-std-acl)#
```

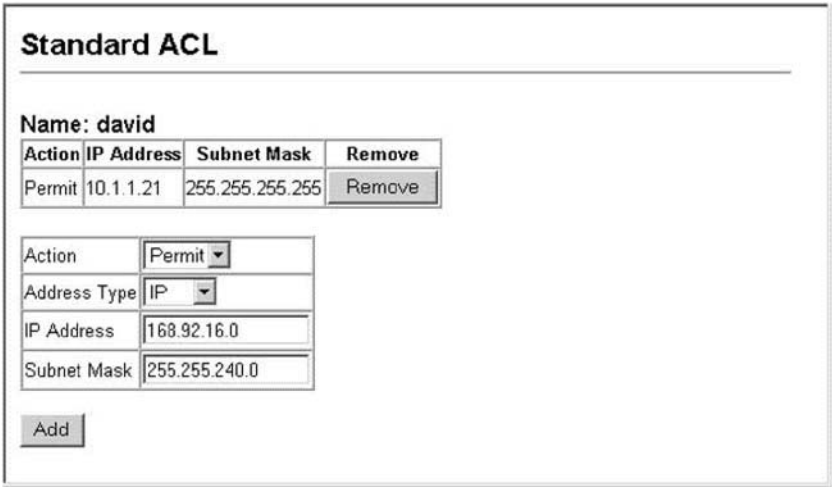
## 3-10-7-3 標準IP ACL(Standard IP ACL)の設定

コマンド解説：

- Action(対処)
  許可(permit)ルールと拒否(deny)ルールとを様々に組み合わせてACL内に設定することが可能です。
- Address Type (アドレス種別)
  送信元(ソース)IPアドレスを指定します。すべてのアドレスを指定する場合は「Any(すべて)」を選んでください。Address(アドレス)フィールド内に特定のホストアドレスを指定する場合は「Host(ホスト)」をお選びください。また、Address(アドレス)フィールドおよびSubMask(サブマスク)フィールドにアドレスの範囲を指定する場合は「IP」を選んでください。(選択肢：Any（すべて）、Host(ホスト)およびIP　初期設定：Any)
- P Address(IPアドレス)
  送信元IPアドレスです。
- Subnet Mask(サブネットマスク)
  0～255までの整数4つをピリオドで区切ったものとなります。マスクは1ビットを使って「合致」を、また0ビットにて「無視」を示します。マスクはビット面で指定送信元アドレスと論理積で繋がれており(ANDed)、当ACLが割り当てられているポートに到着する各IPパケットのアドレスと比較されるかたちになります。

WEB：

対処(Permit(許可)かDeny(拒否))を指定し、アドレス種別(Any(すべて)、Host(ホスト)ないしIP)を選択してください。「Host(ホスト)」を選択した場合は該当するアドレスを入力してください。「IP」を選択した場合は、サブネットアドレスならびにアドレス範囲のマスクを入力してください。最後にAdd(追加)をクリックしてください。



CLI:

以下の例では、指定アドレス10.1.1.21用の許可ルールを1つ設定し、さらにアドレス範囲168.92.16.x～168.92.31.xにてビットマスクを使ったルールを別途設定しています。

```
Console(config-std-acl)#permit host 10.1.1.21                    4-91
Console(config-std-acl)#permit 168.92.16.0 255.255.240.0
Console(config-std-acl)#
```

### 3-10-7-4 拡張(Extended) IP ACLの設定

コマンド解説：

- Action(対処)
  許可(permit)ルールと拒否(deny)ルールとを様々に組み合わせてACL内に設定することが可能です。
- Source/Destination Address Type (送信元/送信先アドレス種別)
  送信元(ソース)ないし送信先IPアドレスを指定します。すべてのアドレスを含む場合は「Any(すべて)」を選んでください。Address(アドレス)フィールド内に特定のホストアドレスを指定する場合は「Host(ホスト)」をお選びください。また、Address(アドレス)フィールドおよびSubMask(サブマスク)フィールドにアドレスの範囲を指定する場合は「IP」を選んでください。(選択肢：Any(すべて)、Host(ホスト)およびIP　初期設定：Any)
- Source/Destination IP Address(送信元/送信先IPアドレス)
  送信元ないし送信先IPアドレスです。
- Source/Destination Subnet Mask(送信元/送信先サブネットマスク)
  送信元ないし送信先アドレスのサブネットマスクです。(p.108のサブネットマスクについての解説をご覧ください。)
- Service Type (サービス種別)
  以下の条件に基づいた、パケットの優先度設定です。
  - Precedence (優先度)
    IP優先レベルです。(範囲：0～7)
  - TOS
    TOS(サービス種別)レベルです。(範囲：0～15)
  - DSCP
    DSCP優先レベルです。(範囲：0～63)
- Protocol (プロトコル)
  合致するプロトコル種別をTCP、UDPないしOthers(その他)のいずれかに指定します。「Others(その他)」は、0～255の範囲内のプロトコル番号を示します。(選択肢：TCP、UDPおよびOthers(その他)、初期設定：TCP)
- Source/Destination Port (送信元/送信先ポート)
  指定プロトコル種別の送信元/送信先ポート番号です。(範囲：0～65535)
- Control Code (制御コード)
  合致するコードビットを表す十進数数値となります。Control bitmask(制御ビットマスク)とは、制御コードに適用される十進数(同等のバイナリビットマスク用)を指します。十進数数値を入力してください。なお、同等のバイナリビット「1」はビットとの合致を、また「0」はビットの無視を意味します。設定可能なビットは以下のとおりです。
  - 1(fin) – Finish (終了)
  - 2(syn) – Synchronize (同期化)
  - 4(rst) – Reset (リセット)

- 8(psh) – Push (プッシュ)
- 16(ack) – Acknowledgement (承認)
- 32(urg) – Urgent pointer (緊急ポインタ)

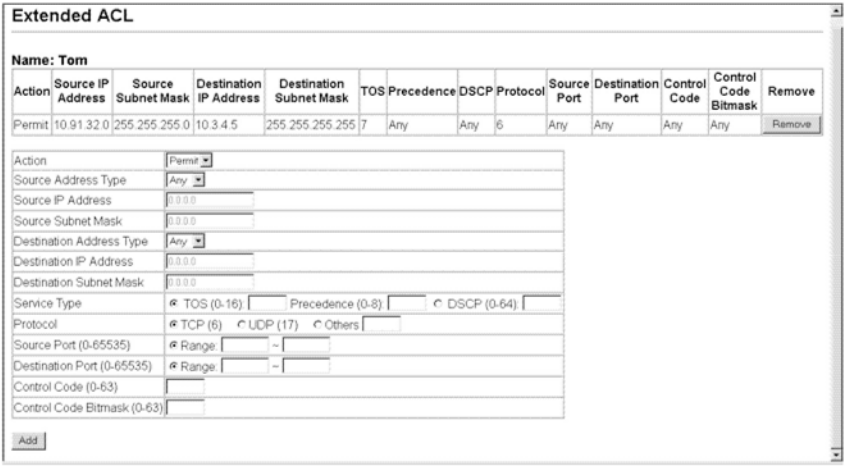
例えば、コード値とマスクを使って以下のフラグセットを持つパケットを捕らえることが可能です。

- SYN flag valid, use control-code 2, control bitmask 2
- Both SYN and ACK valid, use control-code 18, control bitmask 18
- SYN valid and ACK invalid, use control-code 2, control bitmask 18

WEB:

対処(Permit(許可)かDeny(拒否))ならびに、送信元/送信先アドレスを指定してください。

次にアドレス種別(Any(すべて)、Host(ホスト)ないしIP)を選んでください。「Host(ホスト)」を指定した場合は該当アドレスを、また「IP」を選んだ場合はサブネットアドレスならびにアドレス範囲のマスクを入力してください。サービス種別、プロトコル種別ないしTCP制御コードなど、その他必要となる条件を設定し、Add(追加)をクリックしてください。



CLI:

以下の例では2つのルールを追加しています。

(1) 送信元アドレスがサブネット10.7.1.x内にある着信パケットはすべて受理する

(例:ルールが合致した場合(ルール(10.7.1.0 & 255.255.255.0) = マスクされているアドレス(10.7.1.2 & 255.255.255.0))、パケットは通過します。

(2) 送信先TCPポート80に設定されている場合(例:HTTP)、クラスCアドレス192.168.1.0からのTCPパケットはいずれの送信先アドレスに対しても(～アドレスへの送信も)許可する

(3) クラスCアドレス192.168.1.0からのTCPパケットでTCP制御コードが「SYN」に設定されているものはすべて許可する

```
Console(config-ext-acl)#permit 10.7.1.1 255.255.255.0 any            4-92
Console(config-ext-acl)#permit tcp 192.168.1.0 255.255.255.0 any
  destination-port 80
Console(config-ext-acl)#permit tcp 192.168.1.0 255.255.255.0 any
  control-flag 2 2
Console(config-std-acl)#
```

## 3-10-7-5 MAC ACLの設定

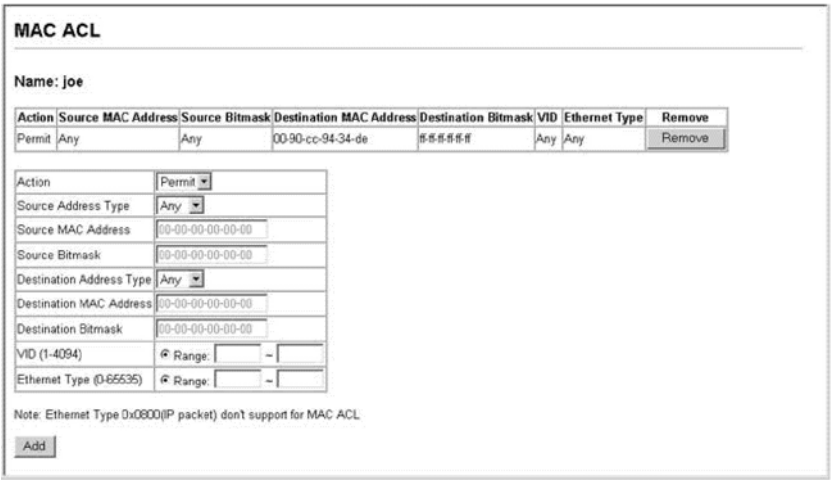
コマンド解説：

- Action(対処)
  許可(permit)ルールと拒否(deny)ルールとを様々に組み合わせてACL内に設定することが可能です。
- Source/Destination Address Type（送信元/送信先アドレス種別）
  すべてのアドレスを含む場合は「Any(すべて)」を選んでください。Address(アドレス)フィールド内に特定のMACアドレスを指定する場合は「Host(ホスト)」をお選びください。また、Address(アドレス)フィールドおよびBitmask(ビットマスク)フィールドにアドレスの範囲を指定する場合は「MAC」を選んでください。（選択肢：Any（すべて）、Host(ホスト)およびMAC　初期設定：Any）
- Source/Destination MAC Address(送信元/送信先MACアドレス)
  送信元ないし送信先MACアドレスです。
- Source/Destination Bitmask(送信元/送信先ビットマスク)
  送信元ないし送信先MACアドレスの16進数マスクです。
- VID
  VLAN IDです。（範囲：1～4094）
- Ethernet Type（イーサネット種別）
  イーサネットII形式パケットのフィルタリングを行う場合のみ利用可能な項目です。（範囲：0～65535）

各イーサネットプロトコル種別のより詳細な情報は、RFC1060にてご確認いただけます。よく見かけられる種別としては0800(IP)、0806(ARP)および8137(IPX)などがあります。

WEB：

Action（対処)を指定してください（「Permit(許可)」、「Deny(拒否)」など）。次に送信元/送信先アドレスを指定し、アドレス種別(Any(すべて)、Host(ホスト)ないしMAC)を選んでください。「Host(ホスト)」を選択した場合は該当するアドレスを入力してください（例：11-22-33-44-55-66など）。「MAC」を選択した場合は、アドレス範囲のベースアドレスならびに16進数ビットマスクを入力してください。必要に応じて、VIDおよびEthernet type（イーサネット種別)などの条件も設定してください。最後にAdd(追加)をクリックしてください。




CLI：

以下のルールは、いかなる送信元MACアドレスからのパケットに対しても、イーサネット種別が0800である送信先アドレス00-e0-29-94-34-deへの送信を許可します。

```
Console(config-mac-acl)#permit any host 00-90-cc-94-34-de
  ethertype 0800                                          4-98
Console(config-mac-acl)#
```

## 3-10-8 ポートをACLにバインド(固定)する

ACLの設定完了後は、トラフィックのフィルタリングが必要となるポートに対し同ACLをバインドする必要があります。IPアクセスリストは、いずれのポートに対しても1つ割り当てることが可能です。一方、MACアクセスリストは本製品内の全ポートに対して1つのみ割り当てられるようになっています。

コマンド利用:

- 本製品は、着信(ingress)フィルタリング用のACLのみ対応しています。
  着信フィルタリングにつき、いずれのポートに対してもIP ACLを1つ割り当てることが可能となっているほか、本製品全体でMAC ACLを1つ割り当てられるようになっています。

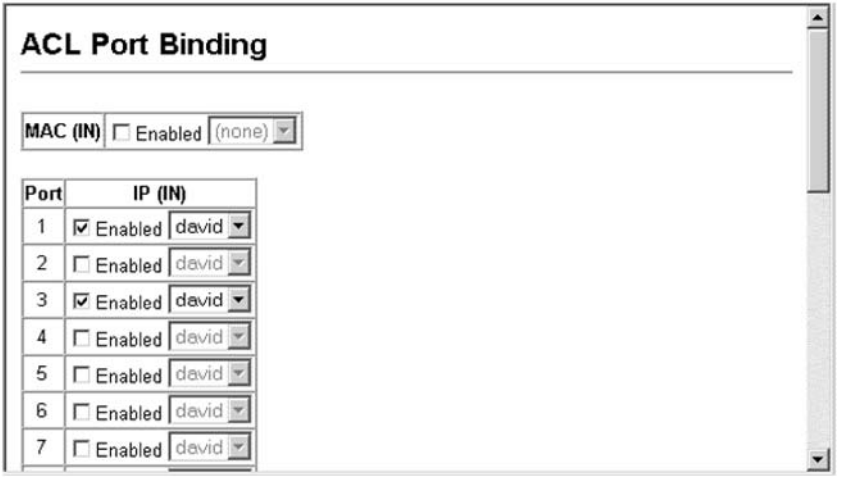
コマンド解説:

- Port (ポート)
  固定ポートないしSFPモジュールとなります。(範囲:1～26)
- IP
  ポート上で有効にするIPアクセスリストを指定します。
- MAC
  本製品全体で有効にする、MACアクセスリストを指定します。
- IN
  着信(ingress)パケット用のACLです。
- ACL名
  ACLの名称です。

WEB：

Security（セキュリティ）→ACL→Port Binding(ポートバインド)と選択します。

ACLにバインドするポートのEnabled（有効)フィールドにチェックマークを入れ、ドロップダウンリストから必要となる（該当する）ACLを選択してApply（適用)をクリックしてください。




CLI：

以下の例では、ポート1に対しIPおよびMACアクセスリストを、またポート3に対しIPアクセスリストを割り当てています。

```
Console(config)#interface ethernet 1/1                          4-108
Console(config-if)#ip access-group david in                     4-94
Console(config-if)#mac access-group jerry in                    4-99
Console(config-if)#exit
Console(config)#interface ethernet 1/3
Console(config-if)#ip access-group david in
Console(config-if)#
```

# 3-11 ポート設定

## 3-11-1 接続ステータスの表示

Port Information（ポート情報）ならびにTrunk Information(トランク情報)ページにて現時点での接続状況を表示することが可能です。表示内容には、リンク状態、速度/デュープレックスモード、フローコントロールならびにオートネゴシエーションの状態などが含まれます。

フィールド解説(WEB)：

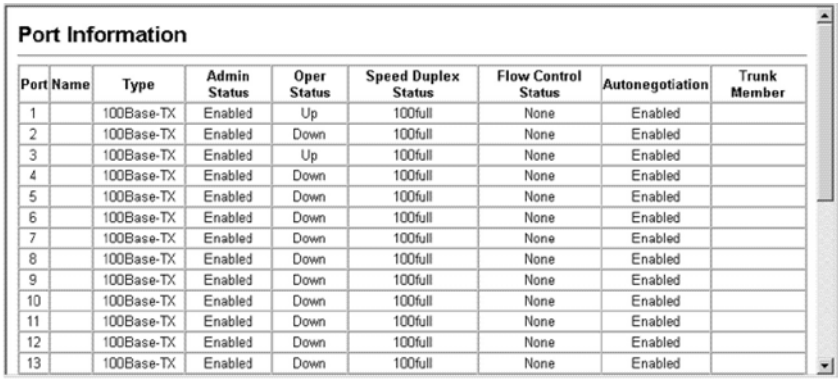
- Name（名称）
  インタフェースのラベル（名称）です。
- Type（種別）
  ポートの種類を示します。（100BASE-TX、1000BASE-TないしSFP）
- Admin Status（管理状況）
  該当インタフェースが有効/無効となっていることを示します。
- Oper Status（動作状況）
  リンクのUP/Down状態を示します。
- Speed Duplex Status（速度/デュープレックス状態）
  現在の速度およびデュープレックスモードを示します。(Auto(自動)ないしFixed（固定)のいずれかが選択可能))
- Flow Control Status（フローコントロール状況）
  現在使用されているフローコントロールの種類を示します。（IEEE802.3x、Back Pressure(バックプレッシャー)ないしNone（なし））
- Autonegotiation（オートネゴシエーション）
  オートネゴシエーションが有効/無効となっていることを示します。
- Trunk Member（*1)(トランクメンバー）
  ポートがトランクメンバーであることを示します。
- Creation（*2）（設定手段）
  トランクの設定（作成）が、1)手動によるものか、それとも2)LACPによる動的な設定によるものかどうかを示します。

  *1：ポート情報のみとなります。

  *2：トランク情報のみとなります。

WEB:

Port (ポート)→Port Information(ポート情報)またはTrunk Information(トランク情報)と選択してください。



**Port Information**

| Port | Name | Type | Admin Status | Oper Status | Speed Duplex Status | Flow Control Status | Autonegotiation | Trunk Member |
|---|---|---|---|---|---|---|---|---|
| 1 | | 100Base-TX | Enabled | Up | 100full | None | Enabled | |
| 2 | | 100Base-TX | Enabled | Down | 100full | None | Enabled | |
| 3 | | 100Base-TX | Enabled | Up | 100full | None | Enabled | |
| 4 | | 100Base-TX | Enabled | Down | 100full | None | Enabled | |
| 5 | | 100Base-TX | Enabled | Down | 100full | None | Enabled | |
| 6 | | 100Base-TX | Enabled | Down | 100full | None | Enabled | |
| 7 | | 100Base-TX | Enabled | Down | 100full | None | Enabled | |
| 8 | | 100Base-TX | Enabled | Down | 100full | None | Enabled | |
| 9 | | 100Base-TX | Enabled | Down | 100full | None | Enabled | |
| 10 | | 100Base-TX | Enabled | Down | 100full | None | Enabled | |
| 11 | | 100Base-TX | Enabled | Down | 100full | None | Enabled | |
| 12 | | 100Base-TX | Enabled | Down | 100full | None | Enabled | |
| 13 | | 100Base-TX | Enabled | Down | 100full | None | Enabled | |

フィールド解説(CLI):

Basic Information(基本情報)

- Port type (ポート種別):ポートの種別を示します。(100BASE-TX、1000BASE-Tないし SFP)
- MAC address (MACアドレス):当ポートの物理レイヤアドレスです。(WEB上で当紅毛にアクセスする場合は、p.39の「スイッチのIPアドレスを設定する」をご覧ください。)

Configuration (設定)

- Name (名称)
  インタフェースの名称です。
- Port admin(ポート管理)
  インタフェースが有効(up)ないし無効(down)となっていることを示します。
- Speed-duplex(速度/デュープレックス)
  現在の速度およびデュープレックスモード設定です。(Auto(自動)ないしfixed(固定))
- Capabilities(対応機能)
  オートネゴシエーション実行中に、相手側機器に通知(advertise)するポート情報です。(当項目にWEB経由でアクセスする場合は、p.175の「インタフェース接続の設定」をご覧ください。本製品は以下の各機能に対応しています。
  - 10half (10半二重)
    10Mbps半二重通信に対応します。
  - 10full (10全二重)
    10Mbps全二重通信に対応します。

- 100half (100半二重)
  100Mbps半二重通信に対応します。
- 100full (100全二重)
  100Mbps全二重通信に対応します。
- 1000full (1000全二重)
  1000Mbps全二重通信に対応します。
- Sym (ポーズフレーム)
  フローコントロール用のポーズフレームの送受信を行います。
- FC (フローコントロール)
  フローコントロールに対応します。

・ Broadcast storm (ブロードキャストストーム)
ブロードキャストストーム制御の有効/無効を示します。
・ Broadcast storm limit(ブロードキャストストーム制限)
ブロードキャストストームのしきい値(限界値)を示します。(64～95232000オクテット/秒)
・ Flow Control (フローコントロール)
フローコントロールの有効/無効を示します。
・ LACP
LACPの有効/無効を示します。
・ Port Security (ポートセキュリティ)
ポートセキュリティの有効/無効を示します。
・ Max MAC count (最大MACカウント)
ポートで学習可能なMACアドレスの最大数を示します。(0～1024アドレス)
・ Port security action (ポートセキュリティ対策)
セキュリティ侵害が検出された際に実行する内容です。(Shutdown(シャットダウン)、trap(トラップ送信)、trap-and-shutdown(トラップ送信の後シャットダウン)ないしnone(なし))

Current Status (現在の状況):

・ Link Status (リンクステータス)
リンクのアップ/ダウン状態を示します。
・ Port Operation Status(ポート実行ステータス)
ポート状態の詳細な情報を示します。(リンクがアップ状態のときのみ表示)
・ Operation speed-duplex(実行速度/デュープレックス設定)
現在の速度ならびにデュープレックスモードを示します。
・ Flow control type (フローコントロール種別)
現在使用しているフローコントロールの種類を示します。(IEEE802.13x、Back-Pressure(バックプレッシャー)またはnone(なし))

CLI:

以下の例では、ポート5の接続状態を示しています。

```
Console#show interfaces status ethernet 1/5                    4-115
Information of Eth 1/5
 Basic information:
  Port type:              100TX
  Mac address:            00-90-CC-12-34-61
 Configuration:
  Name:
  Port admin:             Up
  Speed-duplex:           Auto
  Capabilities:           10half, 10full, 100half, 100full
  Broadcast storm:        Enabled
  Broadcast storm limit:  32000 octets/second
  Flow control:           Disabled
  Lacp:                   Disabled
  Port security:          Disabled
  Max MAC count:          0
  Port security action:   None
 Current status:
  Link status:            Down
  Operation speed-duplex: 100full
  Flow control type:      None
Console#
```

## 3-11-2 インタフェースの接続設定

Port Configuration (ポート設定)およびTrunk Configuration (トランク設定)ページではインタフェースの有効/無効設定、オートネゴシエーションの設定、インタフェース機能の通知(宣伝)が行えるほか、速度・デュープレックスモードならびにフローコントロール設定を手動で変更することが可能となっています。

コマンド解説:

- Name (名称)
  インタフェースに名称を設定することが可能です。(範囲:1～64文字)
- Admin(管理)
  インタフェースを手動で無効に設定します。過剰なコリジョンが検出された場合など、異常が認められた時点でインタフェースを無効にし、障害が取り除かれたあとでまた同インタフェースを有効に設定しなおすことが可能です。その他セキュリティ上の理由でインタフェースを無効にすることも可能です。
- Speed/Duplex(速度/デュープレックス)
  ポートの速度およびデュープレックスモードを手動で設定することが可能です(オートネゴシエーションが無効設定されている場合など)。
- Flow Control (フローコントロール)
  フローコントロールの自動/手動設定の選択が可能です。
- Autonegotiation(オートネゴシエーション:ポート機能)
  オートネゴシエーションを有効/無効に設定します。有効となっている場合は、通知(宣伝)する機能を指定する必要があります。無効となっている場合は、速度、モードおよびフローコントロールの各設定を強制的に設定することが可能です。本製品は以下の機能に対応しています。
  - 10half (10半二重)
    10Mbps半二重通信に対応します。
  - 10full (10全二重)
    10Mbps全二重通信に対応します。
  - 100half (100半二重)
    100Mbps半二重通信に対応します。
  - 100full (100全二重)
    100Mbps全二重通信に対応します。
  - 1000full (1000全二重)
    1000Mbps全二重通信に対応します。
  - Sym (ポーズフレーム:ギガビットのみ)
    ポーズフレームの送受信を行う場合はチェックマークを入れてください。送信者と受信者との間で、非対称ポーズフレームのオートネゴシエーションを行う場合はチェックマークを外してください。

（現時点において、本製品内蔵チップは対象ポーズフレームにのみ対応しています。）

- FC（フローコントロール）

  フローコントロールに対応します。
  フローコントロールが有効となっていると、本製品上のバッファが一杯となった時点で本製品に直接接続されている末端ステーションないしセグメントから送られてくるトラフィックが遮断されるため、フレームの損失を防止することが可能となります。有効となっている場合は、半二重通信ではバックプレッシャーが、また全二重通信ではIEE802.3xを使用します。（ハブに接続されているポート上では、何か問題を解決するためフローコントロールが必要となっている場合などを除き、通常はフローコントロールを使用しないようにしてください。特に必要がない場合にハブと接続しているポート上でフローコントロールを有効にすると、バックプレッシャーのジャミング信号のため、該当ハブに接続されているセグメント全体の通信性能が劣化する恐れがあります。
  （初期設定：オートネゴシエーション有効

  100BASE-TXでの通知（宣伝）機能

  10half(10半二重)、10full(10全二重)、100half（100半二重)および100full(100全二重)

  1000BASE-Tでの通知（宣伝）機能

  10half(10半二重)、10full(10全二重)、100half（100半二重)、100full(100全二重)ならびに1000full(1000全二重)

  1000BASE-SX/LX/LHでの通知（宣伝）機能

  1000full（1000全二重）

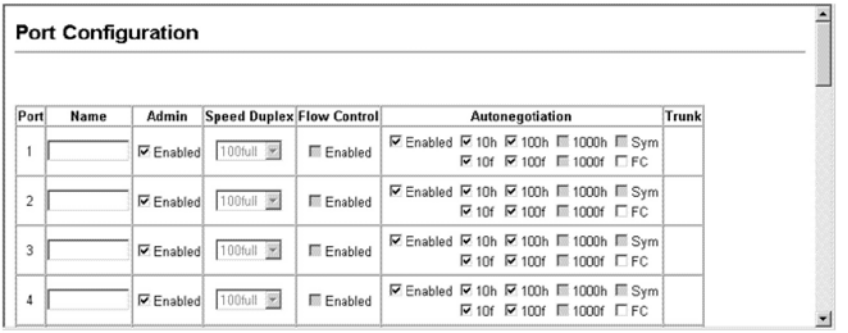
・ Trunk（トランク）

  ポートがトランクのメンバーとなっているかどうかを示します。トランクを作成しポートメンバーを選択する手順については、p.123の「トランクグループの作成」をご覧ください。

**注意**：　インタフェース上で強制的に速度/デュープレックス設定ないしフローコントロール設定を変更する場合は、必ずあらかじめオートネゴシエーションを無効に設定しておいてください。

WEB：

Port(ポート)→Port Configuration(ポート設定)ないしTrunk Configuration(トランク設定)を選択します。必要に応じてインタフェース設定を変更し、Apply (適用)をクリックしてください。




CLI：

インタフェースを選択し、必要に応じて設定を入力してください。

```
Console(config)#interface ethernet 1/13                    4-108
Console(config-if)#description RD SW#13                    4-109
Console(config-if)#shutdown                                4-113
.
Console(config-if)#no shutdown
Console(config-if)#no negotiation                          4-110
Console(config-if)#speed-duplex 100half                    4-109
Console(config-if)#flowcontrol                             4-112
.
Console(config-if)#negotiation
Console(config-if)#capabilities 100half                    4-111
Console(config-if)#capabilities 100full
Console(config-if)#capabilities flowcontrol
```

## 3-11-3 トランクグループの作成

機器間の複数のリンクを束ねて一つの大きな仮想リンク(トランク)として使用することが可能です。ボトルネックの存在するネットワークセグメントにおいてポートトランクは帯域幅を飛躍的に増大させることが可能なほか、機器間の物理リンクいずれか1つが使用不可となっても通信を維持するため、耐故障性(フォールトトレランス)も提供します。本製品では、同時に最大4つまでトランクを作成することが可能です。

本製品は、固定トランクおよび動的なLACP(Link Aggregation Control Protocol)の両者に対応しています。固定トランクはリンクの両端で手動で設定する必要があるほか、リンクで使用するスイッチはすべてCisco EtherChannel標準への対応が必須となります。一方LACPの設定されているポートは、相手側機器上のLACP設定ポートと自動的にネゴシエーションを行ってトランクリンクを形成します。固定トランクに既に設定されているポートでな

ければ、本製品上ではどのポートもポート数に制限なくLACPに設定することが可能です。LACPトランクに8ポート以上が含まれる場合、その他のポートはすべて待機（スタンバイ）モードとなります。トランク内のリンクいずれか1つが使用不可となった時点で、スタンバイモード中のポートのうちいずれか1つが有効となり、故障ポートと置き換えられるかたちになります。

コマンド利用：

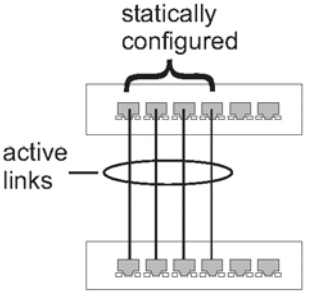
トランク内で各ポートの負荷を平均化する以外に、他のポートは、トランク内のポートいずれか1つが使用不可となった時点でそのポートの負荷を引き継ぎます。このためトランクは通信における冗長性を提供します。ただし機器間で物理的な接続を何か行う前に、WEBインタフェースないしCLIを使ってリンクの両端にあたる機器上でトランクを指定する必要があります。ポートトランクを使用する場合は以下の点にご注意ください。

- ループの形成を避けるためにも、該当するネットワークケーブルで両機器を接続する前に必ずポートトランクの設定を完了させておいてください。
- 本製品では最大4個までトランクを作成することが可能です。各トランクには、最大で8ポートまで参加させることが可能です。
- 接続の両端にあたるポートは、トランクポートとして設定しておく必要があります。
- 機種の異なるスイッチ間で固定トランクを設定する場合は、両機器ともCisco EtherChannel標準に準拠していることをあらかじめご確認ください。
- トランクの両端に該当するポートは、通信モード(速度、デュープレックスモードおよびコントロール)、VLAN割当設定ならびにCoS設定もすべて含め、完全に同じように設定する必要があります。
- トランク内のポートをVLANに追加ないしVLANから削除する場合、トランク内のポートはすべて一まとめにして取り扱う必要があります。
- STP、VLANならびにIGMP設定はトランク全体に適用されます（トランク内の任意のポートのみ異なる設定を行うことはできません）。

## 3-11-3-1 固定トランクの設定

コマンド利用：

- 固定トランクを設定する際は、異なる種類のスイッチ間でリンクを形成できない場合があります（各製造元で採用している仕様が異なる場合など）。ただし、本製品において固定トランクはCisco EtherChannel互換となっています。
- ネットワーク上でループの形成を防止するためにも、実際にポート同士を接続する前に、設定インタフェースにてあらかじめ固定トランクを追加するようにしてください。固定トランクを削除する場合も、設定インタフェースにてあらかじめポートを切断するようにしてください。




statically configured：(固定設定

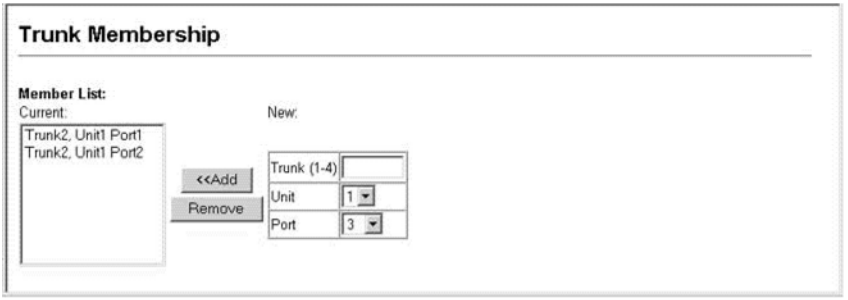
active links：アクティブリンク

コマンド解説：

- Member List (メンバー一覧)(Current：現在)
  設定済みのトランクを表示します（トランクID、ユニットおよびポート）
- New (新規)
  新規にトランクを作成する際に使用するフィールド（空白状態）を含みます。
  - Trunk (トランク)
    トランクIDを1～4の間で設定します。
  - Unit (ユニット)
    スタックユニットです。（範囲：1～8）
  - Port (ポート)
    ポートIDです。（範囲：1～26）

WEB：

Port (ポート)→Trunk Membership(トランクメンバーシップ)と選択します。Trunk(トランク)フィールドに、1～4の範囲でトランクIDを入力してください。次に、スクロールダウンリスト上でスイッチポートいずれかを選択しAdd (追加)をクリックしてください。メンバーリストにポートが追加できた時点でApply(適用)をクリックしてください。




CLI：

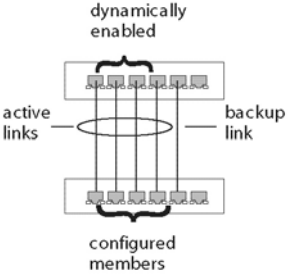
以下の例では、ポート1および2を使ってトランク2を構成しています。これらのポートを、相手側機器の固定トランクポート(2ポート)にそのまま接続してトランクを構成してください。

```
Console(config)#interface port-channel 2                          4-108
Console(config-if)#exit
Console(config)#interface ethernet 1/1                            4-108
Console(config-if)#channel-group 2                                4-124
Console(config-if)#exit
Console(config)#interface ethernet 1/2
Console(config-if)#channel-group 2
Console(config-if)#end
Console#show interfaces status port-channel 2                     4-115
Information of Trunk 2
 Basic information:
  Port type:              100TX
  Mac address:            00-90-CC-12-34-84
 Configuration:
  Name:
  Port admin:             Up
  Speed-duplex:           Auto
  Capabilities:           10half, 10full, 100half, 100full
  Flow control:           Disabled
  Port security:          Disabled
  Max MAC count:          0
 Current status:
  Created by:             User
  Link status:            Up
  Port operation status:  Up
  Operation speed-duplex: 100full
  Flow control type:      None
  Member Ports: Eth1/1, Eth1/2,
Console#
```

### 3-11-3-2 選択ポート上でLACPを有効にする

コマンド利用:

- ネットワーク上でのループの形成を避けるためにも、ポートを接続する前にあらかじめLACPを有効に設定してください。またLACPを無効にする前にポート接続を切断する(取り外す)ようにしてください。
- 接続ポート上において相手側スイッチでもLACPが有効となっている場合は、トランクが自動的に形成されます。
- LACPを使って他スイッチとの間で形成されたトランクには、次に利用可能なトランクIDが自動的に割り当てられます。




dynamically enabled:自動的に有効設定

active links:アクティブリンク

backup link:バックアップリンク

configured members:設定済みメンバー

- 同じ相手側スイッチに接続されているポートでLACPが有効となっているものが8ポート以上存在する場合、(9ポート目以降の)追加ポートはスタンバイモードに移行します。同ポートは、アクティブリンクいずれか1つが利用不可となった場合に有効となります。
- LACPトランクの両端上にあるポートはすべて全二重に設定する必要があります。設定手段は、強制モード(forced mode)とオートネゴシエーションのどちらでも構いません。
- LACPにて自動的に形成されたトランクは、Trunk Membership(トランクメンバー)メニュー上のMember List(メンバー一覧:p.126)内にも表示されます。

コマンド解説:

- Member List(メンバー一覧)(Current(現在))

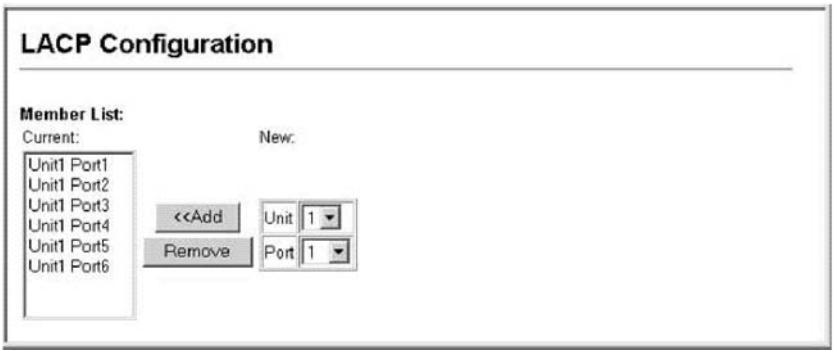
設定済みのトランクを表示します（ユニット、ポート）

- New（新規）
  新規にトランクを作成する際に使用するエントリフィールドを含みます。
  - Unit（ユニット）
    スタックユニットです。（範囲：1～8）
  - Port（ポート）
    ポートIDです。（範囲：1～26）

WEB：

Port（ポート）→LACP→Configuration(設定)と選択します。

ポートのスクロールダウンリストからスイッチポートを選び、Add(追加)をクリックしてください。
メンバーリストにポートが追加された時点でApply(適用)をクリックしてください。



CLI:

以下の例では、ポート1および6でLACPを有効に設定しています。相手側スイッチ上のLACPが有効となっているポートに、これらのポートをそのまま接続してトランクを構成してください。

```
Console(config)#interface ethernet 1/1                                    4-108
Console(config-if)#lacp                                                   4-125
Console(config-if)#exit
:
Console(config)#interface ethernet 1/6
Console(config-if)#lacp
Console(config-if)#end
Console#show interfaces status port-channel 1                             4-115
Information of Trunk 1
 Basic information:
  Port type:              100TX
  Mac address:            00-90-CC-12-34-89
 Configuration:
  Name:
  Port admin:             Up
  Speed-duplex:           Auto
  Capabilities:           10half, 10full, 100half, 100full
  Flow control status:    Disabled
  Port security:          Disabled
  Max MAC count:          0
 Current status:
  Created by:             Lacp
  Link status:            Up
  Port operation status:  Up
  Operation speed-duplex: 100full
  Flow control type:      None
  Member Ports: Eth1/1, Eth1/2, Eth1/3, Eth1/4, Eth1/5, Eth1/6,
Console#
```

## 3-11-4 LACPパラメータの設定

### 3-11-4-1 ポートチャネルを自動的に作成する

一般(共通)のポートチャネルに割り当てるポートは、以下の条件を満たす必要があります。

- ポートはどれも、LACP System Priority(LACPシステム優先度)が同じとなっていること
- ポートはどれも、同じLACP port Admin Key (LACPポート管理キー)を持っていること
- ただし「port channel(ポートチャネル)」Admin Key (管理キー)が設定されている場合は、チャネルグループへの参加を許可するポートに対しても同じport Admin Key(ポート管理キー)を設定する必要があります。

**注意**: チャネルグループ形成時にポートチャネル管理キー(lacp admin key)がCLI経由で設定されていない場合(ヌル値である0となっている場合)、同キーは、同グループに参加しているインタ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(本項およびp.388で解説されているlacp admin key(LACP管理キーとなります)。

コマンド解説:

Set Port Actor (ポートアクターの設定)

ローカル側(本製品上)の集合リンクの設定を行うメニューです。

- Port (ポート)
  ポート番号です。(範囲:1～26)
- System Priority (システム優先度)
  LAG(リンクアグリゲーショングループ)ネゴシエーションを行う際本製品は、LACPシステム優先度をもとに1)LAGメンバー所属情報の決定ならびに2)本機器の他スイッチへの識別(照合)を行います。(範囲:0～65535、初期設定:32768)
  - ポートは、参加するLAGと同じシステム優先度に設定する必要があります。
  - システム優先度と、本製品のMACアドレスとを組み合わせたものがLAG ID (識別子)となります。他システムとLACPネゴシエーションを行う際は、同IDを使って特定のLAGを示すかたちになります。
- Admin Key (管理キー)
  同一のLAGに所属するポートにはすべて、同じLACP管理キーを割り当てる必要があります。(範囲:0～65535、初期設定:1)
- Port Priority (ポート優先度)
  リンクが使用不可となった場合は、LACPポート優先度をもとにバックアップリンクを選択します。(範囲:0～65535、初期設定:32768)

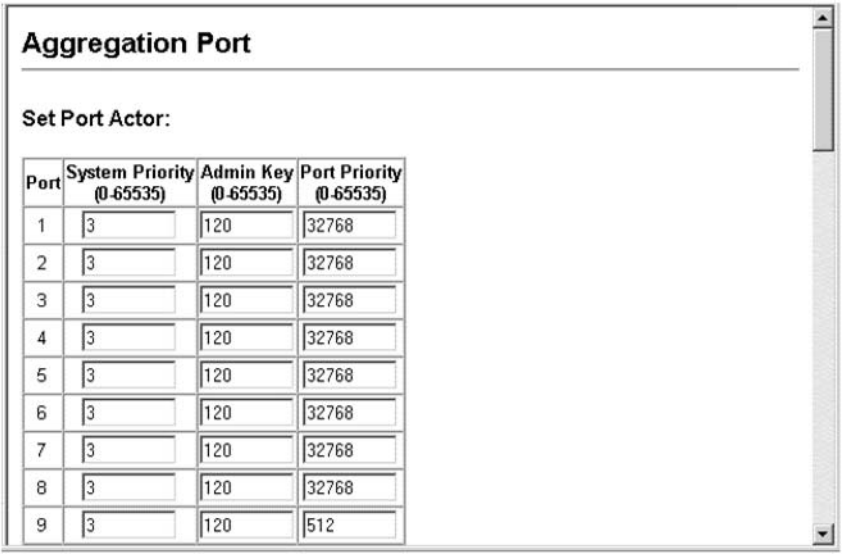
Set Port Partner(ポートパートナーの設定)

集合リンクの、相手側(接続されている機器側)の設定を行うメニューです。コマンド内容は、

ポートアクターで使用するものと同じとなります。ただしパートナー用のLACP設定はその管理ステート(状態)にのみ適用するものであり、動作ステートには適用しません。このため実際に効果が反映されるのは、同パートナーとの間で集合リンクが次に確立した時点となります。

WEB:

Port (ポート)→LACP→Aggregation Port (集合ポート)と選択します。ポートアクターの、システム優先度、管理キーならびにポート優先度を設定してください。また必要な場合は、ポートパートナー用にこれらの項目を設定することも可能です(省略可)。(なお、同設定内容はパートナーの管理ステートにのみ影響を与えるものとなります。このため同設定内容が実際に反映されるのは、同機器との間で集合リンクが次に確立した時点以降となります。)
ポートのLACPパラメータの設定が完了しましたら、Apply(適用)をクリックしてください。



CLI:

以下の例では、ポート1～4にてLACPパラメータの設定を行っています。ポート1～4は、LAG内において有効な(アクティブな)メンバーポートとして使用されます。

```
Console(config)#interface ethernet 1/1                                    4-108
Console(config-if)#lacp actor system-priority 3                           4-126
Console(config-if)#lacp actor admin-key 120                               4-127
Console(config-if)#lacp actor port-priority 128                           4-129
Console(config-if)#exit
:
Console(config)#interface ethernet 1/4
Console(config-if)#lacp actor system-priority 3
Console(config-if)#lacp actor admin-key 120
Console(config-if)#lacp actor port-priority 512
Console(config-if)#end
Console#show lacp sysid                                                   4-129
Port Channel     System Priority    System MAC Address
-------------------------------------------------------------------------------
           1                   3     00-90-CC-31-31-31
           2               32768     00-90-CC-31-31-31
           3               32768     00-90-CC-31-31-31
           4               32768     00-90-CC-31-31-31

Console#show lacp 1 internal                                              4-129
Port channel : 1
-------------------------------------------------------------------------------
Oper Key : 120
Admin Key : 0
Eth 1/1
-------------------------------------------------------------------------------
  LACPDUs Internal:     30 sec
  LACP System Priority: 3
  LACP Port Priority:   128
  Admin Key:            120
  Oper Key:             120
  Admin State : defaulted, aggregation, long timeout, LACP-activity
  Oper State:           distributing, collecting, synchronization,
                        aggregation, long timeout, LACP-activity
:
:
```

## 3-11-5 LACPポートカウンタを表示する

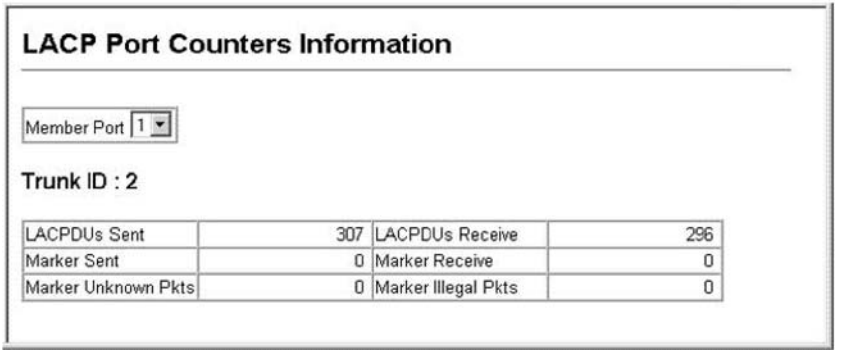
LACPプロトコルメッセージの統計情報を表示します。

表3-6 LACPポートカウンタ

| フィールド名 | 内容 |
|---|---|
| LACPDUs Sent (送信済LACPDU数) | 当チャネルグループから送信されている、有効なLACPDUの数を示します。 |
| LACPDUs Received (受信済LACPDU数) | 当チャネルグループで受信された、有効なLACPDUの数を示します。 |
| Market Sent (送信済マーカー数) | 当チャネルグループから送信されている、有効なMarket PDUの数を示します。 |
| Market Received (受信済マーカー数) | 当チャネルグループで受信された、有効なMarker PDUの数を示します。 |
| LACPDUs Unknown Pkts (LACPDU不明パケット数) | 受信フレーム数のうち、以下に該当するものを指します。1)Slow Protocols Ethernet Type値を持つものの、不明なPDUも含まれるもの 2)Slow ProtocolsグループのMACアドレス宛となっているものの、Slow Protocols Ethernet Typeを持たないもの |
| LACPDUs Illegal Pkts (LACPDU不正パケット数) | 受信フレーム数のうち、Slow Protocols Ethernet Type値を持つものの、正常に構成されていないPDUを含んでいるか、不正なProtocol Subtype値を持つものを指します。 |

WEB:

Port (ポート)→LACP→Port Counters Information(ポートカウンタ情報)と選択します。情報を表示するメンバーポートを選んでください。



CLI:

以下の例では、LACPカウンタの表示を行っています。

```
Console#show lacp counters                                          4-129
Port channel : 1
---------------------------------------------------------------------------
Eth 1/ 1
---------------------------------------------------------------------------
  LACPDUs Sent:          91
  LACPDUs Receive:       43
  Marker Sent:           0
  Marker Receive:        0
  LACPDUs Unknown Pkts: 0
  LACPDUs Illegal Pkts: 0
:
```

## 3-11-6 ローカル側の状況およびLACP設定を表示する

集合リンクのローカル側の設定内容および動作状況を表示します。

表3-7 LACP内部設定情報

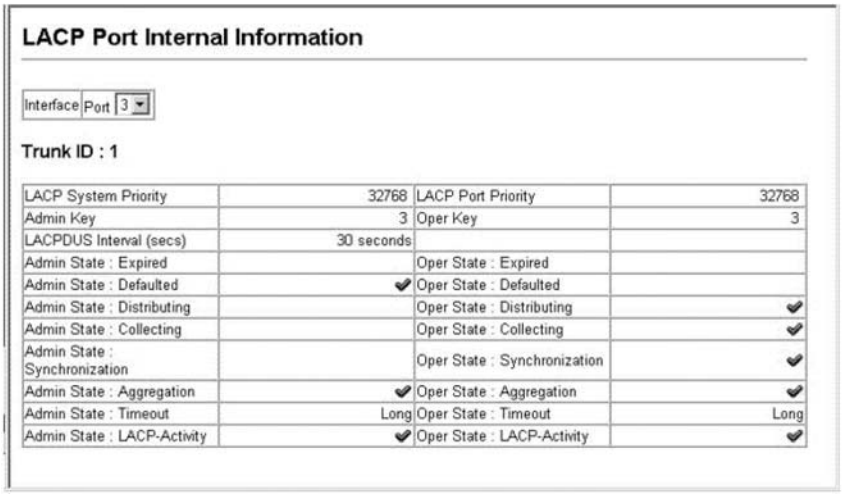
| フィールド | 内容 |
|---|---|
| Oper Key<br>(動作キー) | 集合ポート用キーの、現時点における動作値です。 |
| Admin Key<br>(管理キー) | 集合ポート用キーの、現時点における管理値です。 |
| LACPDUs Internal<br>(LACPDU内部設定) | 受信したLACPDU情報を無効とする前に待機する時間を秒単位で表示します。 |
| LACP System Priority<br>(LACPシステム優先度) | 当ポートチャネルに割り当てられている、LACPシステム優先度です。 |
| LACP Port Priority<br>(LACPポート優先度) | チャネルグループ内の当インタフェースに割り当てられているLACPポート優先度です。 |
| Admin State, Oper State<br>(管理状態、動作状態) | アクターの状態を示すパラメータの、管理ないし動作値を示します。<br>・ Expired (期限切れ)<br>アクターの受信機器は期限切れ状態となっています。<br>・ Defaulted (初期設定)<br>アクターの受信機器は、パートナー用に管理上設定されている、デフォルト(初期設定)の動作パートナー情報を使用しています。<br>(訳注:Defaulted は不履行などの意味を示す単語ですが、ここでは意味が通じなくなるのでデフォルト＝初期設定の訳にしています)<br>・ Distributing (配信)<br>フォールス(否)状態となっている場合、当リンクから発信するフレームの配信は無効となります。(配信が現在無効となっており、管理上の変更や受信プロトコル情報内での変更がない限り有効となることはありません)<br>・ Collecting (収集)<br>当リンク上における、着信フレームの収集は有効となっています。(収集は現在有効となっており、管理上の変更や受信プロトコル情報内での変更がない限り無効となることはありません) |

| | |
|---|---|
| | · Synchronization (同調)<br>システムは、当リンクをIN_SYNC状態にあると見なします。(同リンクは正しいLAG(リンクアグリゲーショングループ)に割り当てられており、当グループは互換性のあるAggregator (集合)と関連付けられています。またLAGの識別情報と、送信されているシステムIDならびに動作キー情報との間に矛盾は見つかっていません。)<br>· Aggregation (集合)<br>システムは当リンクを集合化可能と見なしています。(集合ポートに含むポートの候補となります。)<br>· Long timeout (長時間タイムアウト)<br>定期的にLACPDUを送信する際は、低い送信速度を使用します。<br>· LACP-Activity(LACP動作)<br>当リンクにおける、動作(activity)制御値です。(0:Passive (非アクティブ)、1:Active(アクティブ) |

WEB:

Port (ポート)→LACP→Port Internal Information(ポート内部情報)と選択します。

表示するポートチャネルを選んでください。



CLI:

以下の例では、ポートチャネル1ローカル側の設定内容および動作状態を表示しています。

```
Console#show lacp 1 internal                                          4-129
Port channel : 1
------------------------------------------------------------------------------
Oper Key : 120
Admin Key : 0
Eth 1/1
------------------------------------------------------------------------------
  LACPDUs Internal:     30 sec
  LACP System Priority: 3
  LACP Port Priority:   128
  Admin Key:            120
  Oper Key:             120
  Admin State : defaulted, aggregation, long timeout, LACP-activity
  Oper State:           distributing, collecting, synchronization,
                        aggregation, long timeout, LACP-activity
:
:
```

## 3-11-7 リモート側のLACP設定およびステータスを表示する

集合リンクのリモート側の設定内容および動作状況を表示します。

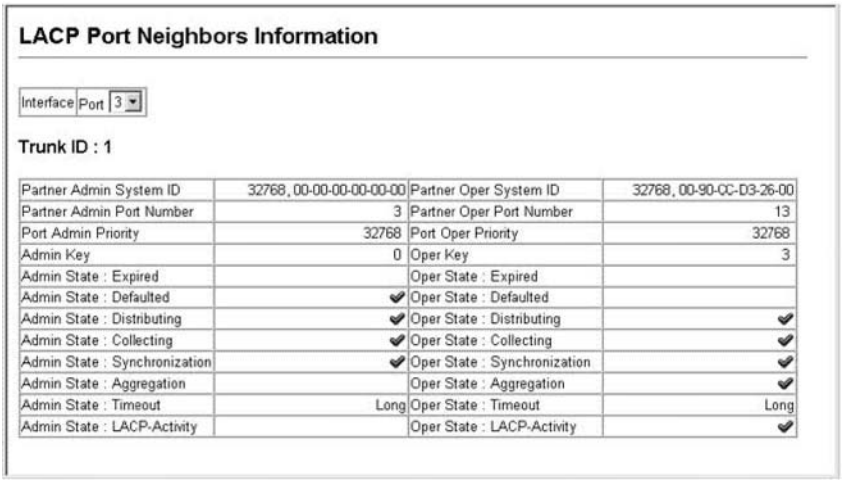
表3-8 LACP相手側設定情報

| フィールド | 内容 |
|---|---|
| Partner Admin System ID<br>（パートナー管理システムID） | ユーザより割り当てられている、LAGパートナーのシステムIDです。 |
| Partner Oper System ID<br>（パートナー動作システムID） | LACPプロトコルより割り当てられている、LAGパートナーのシステムIDです。 |
| Partner Admin Port Number<br>（パートナー管理ポート番号） | プロトコルパートナー用のポート番号の、現時点における管理上の値となります。 |
| Partner Oper Port Number<br>（パートナー動作ポート番号） | ポートのプロトコルパートナーから当集合ポートに対し割り当てられた、動作上のポート番号となります。 |
| Port Admin Priority<br>（ポート管理優先度） | プロトコルパートナー用ポート優先度の、現時点における管理上の値となります。 |
| Admin Key（管理キー） | プロトコルパートナー用キーの、現時点における管理上の値となります。 |
| Oper Key（動作キー） | プロトコルパートナー用キーの、現時点における動作上の値となります。 |
| Admin State(管理ステート) | パートナー用ステート（状態）パラメータの管理上の値となります（前述の表をご覧ください）。 |
| Oper State（動作ステート） | パートナー用ステート（状態）パラメータの動作上の値となります（前述の表をご覧ください）。 |

WEB：

Port (ポート)→LACP→Port Neighbors Information(相手側ポートの情報)と選択します。

情報を表示するポートチャネルを選んでください。



**LACP Port Neighbors Information**

Interface Port 3

**Trunk ID : 1**

| | | | |
|---|---|---|---|
| Partner Admin System ID | 32768, 00-00-00-00-00-00 | Partner Oper System ID | 32768, 00-90-CC-D3-26-00 |
| Partner Admin Port Number | 3 | Partner Oper Port Number | 13 |
| Port Admin Priority | 32768 | Port Oper Priority | 32768 |
| Admin Key | 0 | Oper Key | 3 |
| Admin State : Expired | | Oper State : Expired | |
| Admin State : Defaulted | ✔ | Oper State : Defaulted | |
| Admin State : Distributing | ✔ | Oper State : Distributing | ✔ |
| Admin State : Collecting | ✔ | Oper State : Collecting | ✔ |
| Admin State : Synchronization | ✔ | Oper State : Synchronization | ✔ |
| Admin State : Aggregation | | Oper State : Aggregation | ✔ |
| Admin State : Timeout | Long | Oper State : Timeout | Long |
| Admin State : LACP-Activity | | Oper State : LACP-Activity | ✔ |

CLI：

以下の例では、ポートチャネル1のリモート側のLACP設定内容および動作状態を表示しています。

```
Console#show lacp 1 neighbors                                        4-129
Port channel 1 neighbors
------------------------------------------------------------------------
Eth 1/1
------------------------------------------------------------------------
  Partner Admin System ID:   32768, 00-00-00-00-00-00
  Partner Oper System ID:    3, 00-90-CC-CE-2A-20
  Partner Admin Port Number: 5
  Partner Oper Port Number:  3
  Port Admin Priority:       32768
  Port Oper Priority:        128
  Admin Key:                 0
  Oper Key:                  120
  Admin State:               defaulted, distributing, collecting,
                             synchronization, long timeout,
  Oper State:                 distributing, collecting, synchronization,
                             aggregation, long timeout, LACP-activity
:
```

# 3-12 ブロードキャストストームしきい値の設定

ご使用ネットワーク上の機器いずれかが正常に動作していなかったり、またアプリケーションプログラムが正しく設計ないし設定されていない場合はブロードキャストストームが発生する恐れがあります。ネットワーク上でブロードキャストトラフィックが過剰に発生すると、通信性能が著しく低下し場合によっては完全に停止することもあります。

ブロードキャストトラフィックのしきい値（制限値）を設定することにより、ご使用のネットワークをブロードキャストストームから保護することが可能となります。このしきい値を超過するブロードキャストパケットはすべて破棄されます。

コマンド利用：

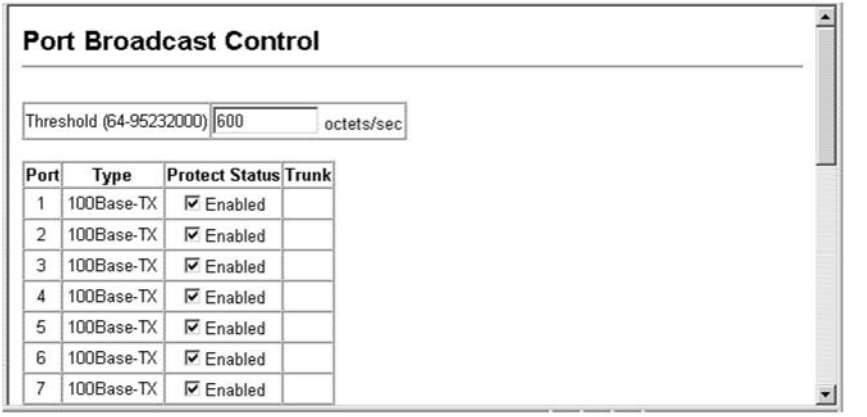
- 初期状態では、ブロードキャストストーム制御(Broadcast Storm Control)は有効に設定されています。
- ブロードキャスト制御はIPマルチキャストトラフィックに対しては何ら影響を与えません。
- 指定されたしきい値は、本製品上のすべてのポートに対して適用されます。

コマンド解説：

- Port (ポート)(*1)
  ポート番号です。
- Trunk (トランク)(*2)
  トランク番号です。
- Threshold (しきい値)
  しきい値を、ポート帯域幅の％単位で設定します。(訳注：「％」部分は以下内容と矛盾しますが念のためこのまま残しておきます)(範囲：64～95232000、初期設定：32000オクテット/秒)
- Protect Status(保護状況)
  ブロードキャストストーム制御が有効となっているかどうかを示します。(初期状態：Enabled(有効))

WEB：

Port (ポート)→Port/Trunk Broadcast Control (ポート/トランクブロードキャスト制御)と選択します。該当するインタフェース上でしきい値を設定し、Enabled(有効)フィールドにチェックマークを入れてApply(適用)をクリックしてください。




*1 ポートブロードキャスト制御

*2 トランクブロードキャスト制御

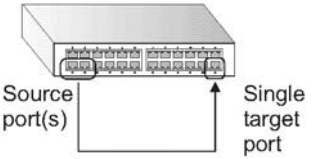
CLI:

インタフェースを指定し、しきい値を入力してください。以下の例では、ポート1上でブロードキャストストーム制御を無効に設定した上で、ポート2上でブロードキャスト抑制（制御）を600オクテット/秒に設定しています。なお、ポート2上の設定は全ポートに対し適用されます。

```
Console(config)#interface ethernet 1/1                                  4-108
Console(config-if)#no switchport broadcast                              4-114
Console(config-if)#exit
Console(config)#interface ethernet 1/2
Console(config-if)#switchport broadcast octet-rate 600                  4-114
Console(config-if)#end
Console#show interfaces switchport ethernet 1/2                         4-117
Information of Eth 1/2
 Broadcast threshold:           Enabled, 600 octets/second
 Lacp status:                   Enabled
 Ingress rate limit: disable, Level: 30
 Egress rate limit: disable, Level: 30
 VLAN membership mode:          Hybrid
 Ingress rule:                  Disabled
 Acceptable frame type:         All frames
 Native VLAN:                   1
 Priority for untagged traffic: 0
 Gvrp status:                   Disabled
 Allowed Vlan:                  1(u),
 Forbidden Vlan:
 Private-VLAN mode:             NONE
 Private-VLAN host-association: NONE
 Private-VLAN mapping:          NONE
Console#
```

# 3-13 ポートミラーリングの設定

いずれのソース(ミラー元)ポート上のトラフィックも、ターゲットポートにミラーリング(コピー)することが可能です。ターゲットポートにROMプローブやロジックアナライザなどを接続することで、ミラーリングされたトラフィックを完全に邪魔にならない方法でリアルタイムに解析することが可能となります。




Source ports (ソースポート)

Single target port (単一のターゲットポート)

コマンド利用:

- モニタポートの速度は、ソースポートの速度と同じであるかこれを上回っている必要があります。その他の場合、トラフィックはモニタポート上で破棄されるかたちになります。
- ミラーセッションはすべて、同一の送信先ポートを共有する必要があります。
- ポート上のトラフィックのミラーリングを行う場合、ターゲットポートとソースポートはどちらも同じVLANに所属している必要があります。

コマンド解説:

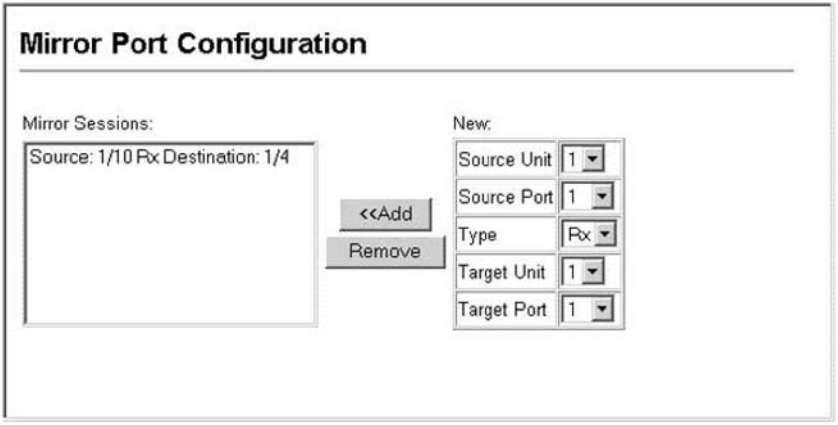
- Mirror Sessions (ミラーセッション)
  現時点において存在するミラーセッションを一覧表示します。
- Source Unit (ソース機器)
  この機器のポート上のトラフィックを監視します。
- Source Port (ソースポート)
  このポート上のトラフィックを監視します。
- Type (種別)
  ターゲットポートに対しミラーリングするトラフィックの種類を、Rx(受信)かTx(送信)のいずれかに設定します。
- Target Unit (ターゲット機器)
  ソースポート上のトラフィックは、当機器上のポートにて複写(ミラーリング)されます。
- Target Port (ターゲットポート)

ソースポート上のトラフィックをミラーリングするポートです。

WEB：

Port (ポート)→Mirror Port Configuration (ミラーポート設定)と選択します。

ソースポート/機器、ミラーリングするトラフィックの種別ならびにミラーポート/機器をそれぞれ指定し、Add(追加)をクリックしてください。




CLI：

interfaceコマンドを使用してモニタポートを選択し、port monitorコマンドを使ってソースポートならびにトラフィックの種類を指定してください。

```
Console(config)#interface ethernet 1/10                    4-108
Console(config-if)#port monitor ethernet 1/13 tx           4-119
Console(config-if)#
```

# 3-14 速度制限の設定

当機能を使用することにより、ネットワーク管理者はポート上で受信するトラフィックの最大速度を制御することが可能となります。ネットワークの末端に位置するポート上で速度制限を設定することで、ネットワークを行き来するトラフィックの速度を制御できるようになります。速度制限の範囲内のトラフィックが送信される一方で、許容量を超えるパケットは破棄されるかたちになります。

速度制限は個別のポートないしトランクごとに設定可能です。インタフェース上で当機能を設定(有効)にした場合は、本製品ハードウェア側でトラフィックの速度を監視し、指定条件に必ず合致するようにします。条件を満たさないトラフィックは破棄し、条件に合致するトラフィックは何ら変更を加えない状態でそのまま転送します。

## 3-14-1 速度制限精度(Rate Limit Granularity)

速度制限精度機能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上のトラフィックをさらに効率よく制御することが可能となります。「速度制限精度(rate limit granularity)」に「速度制限レベル(rate limit level)をかけ合わせた値が、インタフェースに対し実際に設定される速度制限値となります。同精度は本製品全体に適用(グローバル適用)されるため、イーサネットインタフェースに設定を行った場合はすべてのファストイーサネットインタフェース上で同じ設定が、またギガビットイーサネットインタフェースに対し設定を行った場合はすべてのギガビットイーサネットインタフェース上で同じ設定が適用されます。

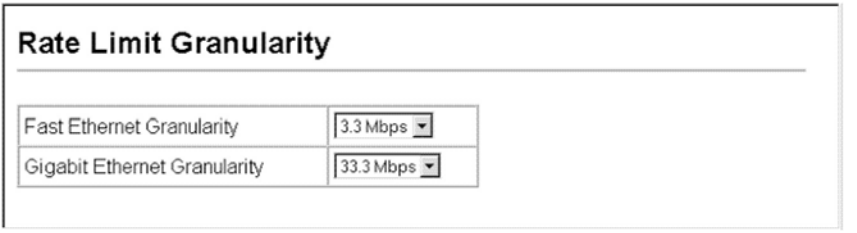
コマンド利用:

- ファストイーサネットインタフェースの場合、速度制限精度は512Kbps、1Mpbsないし3.3Mbpsのいずれかに設定可能です。
- ギガビットイーサネットインタフェースの場合、設定可能な速度制限精度は33.3Mbpsとなります。

WEB:

Port (ポート)→Rate Limit(速度制限)→Granularity(精度)と選択します。

ファストイーサネットないしギガビットイーサネットに適用する速度制限精度を選び、Apply(適用)をクリックしてください。



CLI:

以下の例では、ファストイーサネットおよびギガビットイーサネット用の速度制限精度を設定し、また同内容を表示しています。

```
Console(config)#rate-limit fastethernet granularity 512              4-122
Console(config)#rate-limit gigabitethernet granularity 33300         4-122
console#show rate-limit                                              4-122

Fast ethernet granularity:  512

Gigabit ethernet granularity:  33300
Console#
```

## 3-14-2 速度制限の設定(Rate Limit Configuration)

速度制限設定(rate limit configuration)ページにて速度制限設定を適用します。

コマンド利用:

- 個別のインタフェースごとに入力/出力速度制限を有効/無効に設定することが可能です。

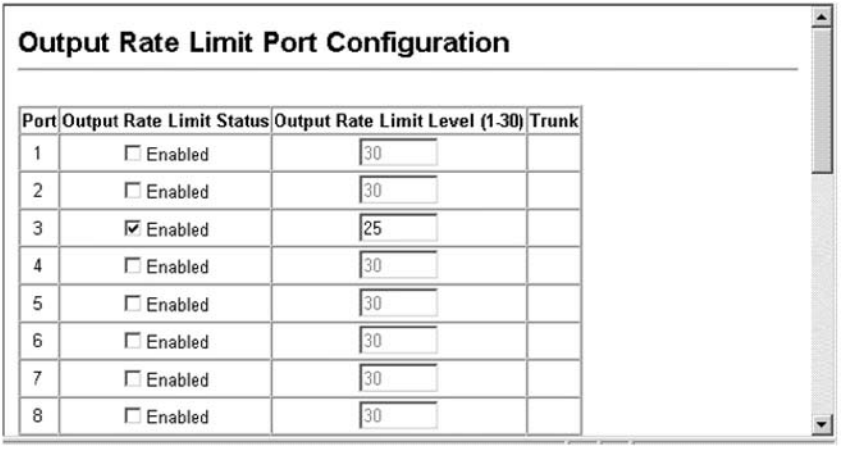
コマンド解説:

- Port/Trunk (ポート/トランク)
  ポート番号を表示します。
- Rate Limit Status(速度制限ステータス)
  速度制限を有効/無効に設定します。(初期設定:無効)
- Rate Limit Level (速度制限レベル)
  速度制限レベルを設定します。(範囲:1～30、初期設定:30)

**注意**:　実際の速度制限＝速度制限レベル×精度

WEB:

Port (ポート)→Rate Limit (速度制限)→Input/Output Port/Trunk Configuration(入出力ポート/トランク設定)と選択します。該当するインタフェース上でRate Limit Status(速度制限ステータス)を有効に設定し、速度制限レベルを指定した上でApply(適用)をクリックしてください。



CLI:

以下の例では、ポート3を通過する入出力トラフィックの速度制限レベルを設定しています。

```
Console(config)#interface ethernet 1/3                                  4-108
Console(config-if)#rate-limit input level 25                            4-121
Console(config-if)#rate-limit output level 25                           4-121
Console(config-if)#
```

# 3-15 ポート統計の表示

インタフェースグループおよびイーサネットタイプの各MIBを使ってネットワークトラフィックの一般的な統計情報が表示できるようになっているほか、RMON MIBをもとにトラフィックのさらに詳細な情報を表示することも可能です。インタフェースおよびイーサネットタイプの統計は、各ポートを通過するトラフィック上のエラーを表示します。同情報を使用することにより、不良ポートや過剰の負荷といった、問題となり得る要因を識別することが可能となります。RMON統計は、各ポートを通過するレームの種類、サイズならびにカウント数といった、より広範囲の統計情報を提供します。表示される値はすべて毎秒ごとのカウント数であるほか、最後に本製品を再起動した時点からの累計となっています。初期設定では、統計情報は60秒ごとに自動的に更新されるようになっています。

注意: RMONグループ2、3および9は、HP OpenViewなどのSNMP管理ソフトウェアを使用した場合のみアクセス可能となります。

表3-9 ポート統計

| パラメータ | 内容 |
|---|---|
| Interface Statistics (インタフェース統計) | |
| Received Octets (受信オクテット数) | 当インタフェース上で受信した、フレーミングキャラクタも含めたオクテット数です。 |
| Received Unicast Packets<br>(受信ユニキャストパケット数) | より高位層のプロトコルに対し送信されたサブネットワーク-ユニキャストパケットの数です。 |
| Received Multicast Packets<br>(受信マルチキャストパケット数) | 当下位レイヤから上位(下位)レイヤに対し送信されたパケットのうち、当下位レイヤにおいてマルチキャストアドレスに対し通知が行われたものの数です。 |
| Received Broadcast Packets<br>(受信ブロードキャストパケット数) | 当下位レイヤから上位(下位)レイヤに対し送信されたパケットのうち、当下位レイヤにおいてブロードキャストアドレスに対し通知が行われたものの数です。 |
| 受信破棄パケット数 | より高位層のプロトコルへ送信するにあたり何ら問題が検出されなかったものの、破棄するよう選択された着信パケットの数です。バッファ領域を開放するため、これら正常なパケットを破棄している可能性があります。 |
| Received Unknown Packets }<br>(受信未知パケット数) | インタフェース経由で受信したパケットのうち、未知ないし未対応のプロトコルであったため破棄されたものの数です。 |

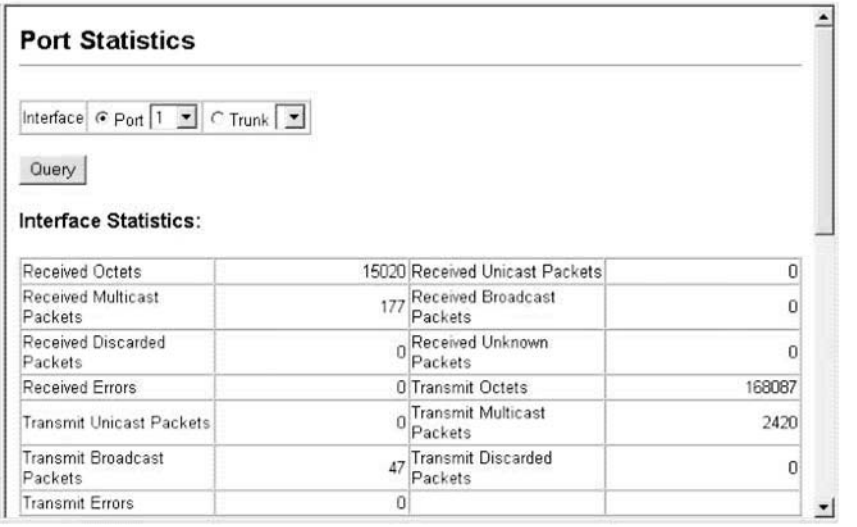
| | |
|---|---|
| Received Errors (受信エラー数) | エラーを含んでいるため、より高位層のプロトコルに対し送信が行えない着信パケットの数です。 |
| Transmit Octets (送信オクテット数) | 当インタフェースから送信されている、フレーミングキャラクタも含めたオクテットの総数です。 |
| Transmit Unicast Packets<br>(送信ユニキャストパケット数) | 高位層プロトコルにより、サブネットワーク-ユニキャストアドレスへの送信が要求されたパケットの総数です。破棄されたか、送信されなかったパケットも含みます。 |
| Transmit Multicast Packets<br>(送信マルチキャストパケット数) | 高位層プロトコルにより送信が要求されており、また当下位レイヤにおけるマルチキャストアドレスへの通知が行われているパケットの総数です。破棄されたか、送信されなかったパケットも含みます。 |
| Transmit Broadcast Packets<br>(送信ブロードキャストパケット数) | 高位層プロトコルにより送信が要求されており、また当下位レイヤにおけるブロードキャストアドレスへの通知が行われているパケットの総数です。破棄されたか、送信されなかったパケットも含みます。 |
| Transmit Discarded Packets<br>(送信破棄パケット数) | より高位層のプロトコルへ送信するにあたり何ら問題が検出されなかったものの、破棄するよう選択された送信パケットの数です。バッファ領域を開放するため、これら正常なパケットを破棄している可能性があります |
| Transmit Errors (送信エラー数) | エラーのため送信できなかった、外部宛(送信)パケットの数です。 |
| Etherlike Statistics (イーサ関連統計) | |
| Alignment Errors (アラインメントエラー) | アラインメントエラー(同期のとれなかったデータパケット)の数です。 |
| Late Collisions (遅延コリジョン数) | パケット送信後、512ビットタイムより後にコリジョンが検出された回数です。 |
| FCS Errors (FCSエラー数) | インタフェース上で受信したフレームのうち、長さがオクテット整数分あるもののFCSチェックに合格しなかったフレームのカウント数です。同カウントには、frame-too-long/short(フレームサイズ超過/不足)エラーを持つパケットは含まれません。 |
| Excessive Collisions (過剰コリジョン数) | 過剰なコリジョンのため、特定インタフェース上での送信に失敗しているフレームのカウント数です。なお、インタフェースが全二重モードで動作している場合同カウントは増加しません。 |

| | |
|---|---|
| Single Collision Frames<br>(単一コリジョンフレーム数) | 送信が、一回のコリジョンによってのみ妨害されている場合において送信が正常に行われているフレームの数です。 |
| Internal MAC Transmit Errors<br>（内部MAC送信エラー数） | 内部MACサブレイヤ（下位層）送信エラーのため、特定インタフェース上での送信に失敗しているフレームのカウント数です。 |
| Multiple Collision Frames<br>（複数回コリジョンフレーム数） | 送信が一回以上のコリジョンにより妨害されているフレームのうち、正常に送信されたもののカウント数です。 |
| Carrier Sense Errors<br>(キャリアセンスエラー数) | フレーム送信を試みた際にキャリアセンス（察知）状態が喪失したか、有効状態にならなかった回数です。 |
| SQE Test Errors (SQEテストエラー数) | 特定インタフェース用のPLSサブレイヤにてSQE TEST ERRORメッセージが発生した回数です。 |
| Frames Too Long<br>（フレームサイズ超過） | 特定インタフェース上で受信されたフレーム数のうち、許容されている最大フレームサイズを超過したもののカウント数です。 |
| Deferred Transmissions (送信延期数) | 特定インタフェース上において、通信メディアがビジー状態であるため初回の送信が延期されたフレームのカウント数です。 |
| Internal MAC Receive Errors<br>（内部MAC受信エラー数） | 特定インタフェース上において、内部MACサブレイヤ受信エラーのため受信に失敗したフレームのカウント数です。 |
| RMON Statistics (RMON統計) | |
| Drop Events (破棄イベント数) | リソース不足のためパケットが破棄されることとなったイベントの総数です。 |
| Jabbers (ジャバー数) | 受信フレームのうち、サイズが1518オクテット（フレーミングビットは除くがFCSオクテットは含む）を超えるもので、FCSないしアラインメントエラーのいずれかを備えるフレームの総数です。 |
| Received Bytes (受信バイト数) | ネットワーク上で受信したバイトの総数です。同情報は、イーサネット使用率を把握する場合などに利用することが可能です。 |
| Collisions （コリジョン数） | 当イーサネットセグメント上における、コリジョン総数の最も信頼できる予測値です。 |
| Received Frames (受信フレーム数) | 受信したフレームの総数です。不良フレーム、ブロードキャストならびにマルチキャストフレームも含みます。 |
| Broadcast Frames<br>（ブロードキャストフレーム数） | 受信した正常なフレームのうち、ブロードキャストアドレスに宛てられたものの総数です。マルチキ |

| | |
|---|---|
| | ャストパケットは含まれません。 |
| Multicast Frames<br>（マルチキャストフレーム数） | 受信した正常フレームのうち、当マルチキャストアドレスに対し宛てられたものの総数です。 |
| CRC/Alignment Errors<br>（CRCアライメントエラー数） | CRCエラーおよびアライメントエラーの数です。 |
| Undersize Frames（過小フレーム数） | 受信フレームのうち、サイズが64オクテット(フレーミングビットを除くがFCSオクテットは含む)に満たないほかは問題の認められなかったものの総数です。 |
| Oversize Frames | 受信フレームのうち、サイズが1518オクテット(フレーミングビットを除くがFCSオクテットは含む)を超過しているほかは問題の認められなかったものの総数です。 |
| Fragments（フラグメント数） | 受信フレームのうち、サイズが64オクテット(フレーミングビットを除くがFCSオクテットは含む)に満たず、またFCSエラーかaアラインメントエラーを持つフレームの総数です。 |
| 64 Bytes Frames（64バイトフレーム数） | 不良パケットを含む送受信フレームのうち、サイズが64オクテット(フレーミングビットを除くがFCSオクテットは含む)のものの総数です。 |
| 65-127 Byte Frames<br>（65-127バイトフレーム数）<br>128-255 Byte Frames<br>（128-255バイトフレーム数）<br>256-511 Byte Frames<br>（256-511バイトフレーム数）<br>512-1023 Byte Frames<br>（512-1023バイトフレーム数）<br>1024-1518 Byte Frames<br>（1024-1528バイトフレーム数）<br>1519-1536 Byte Frames<br>（1519-1536バイトフレーム数） | 不良パケットを含む送受信フレームのうち、サイズが指定範囲内(フレーミングビットを除くがFCSオクテットは含む)のものの総数です。 |

WEB：

Port (ポート)→Port Statistics (ポート統計)と選択します。該当するインタフェースを選び、Query(クエリ)をクリックしてください。画面内容を更新する場合は、画面最下部のRefresh(更新)ボタンをクリックしてください。



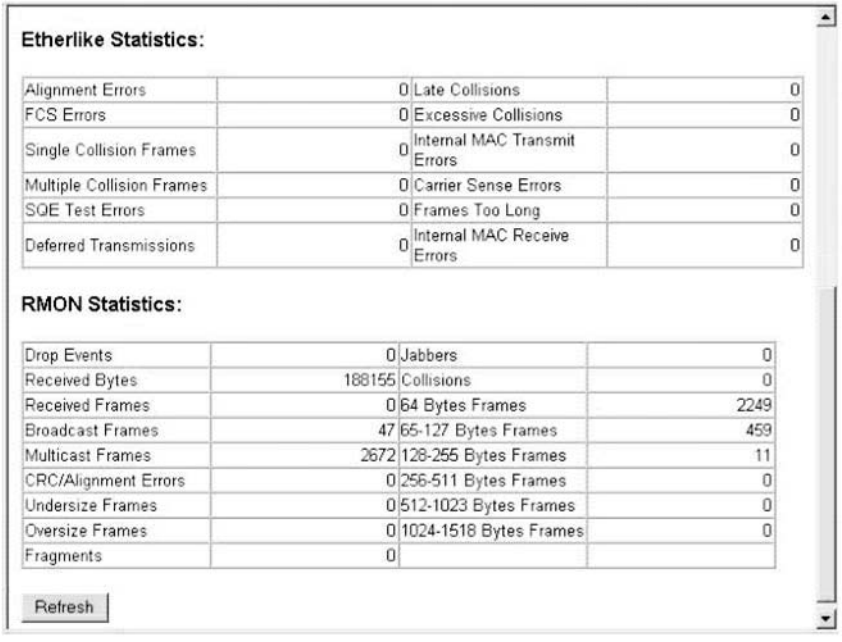
**Port Statistics**

Interface ◉ Port 1 ○ Trunk

Query

**Interface Statistics:**

| | | | |
|---|---|---|---|
| Received Octets | 15020 | Received Unicast Packets | 0 |
| Received Multicast Packets | 177 | Received Broadcast Packets | 0 |
| Received Discarded Packets | 0 | Received Unknown Packets | 0 |
| Received Errors | 0 | Transmit Octets | 168087 |
| Transmit Unicast Packets | 0 | Transmit Multicast Packets | 2420 |
| Transmit Broadcast Packets | 47 | Transmit Discarded Packets | 0 |
| Transmit Errors | 0 | | |



**Etherlike Statistics:**

| | | | |
|---|---|---|---|
| Alignment Errors | 0 | Late Collisions | 0 |
| FCS Errors | 0 | Excessive Collisions | 0 |
| Single Collision Frames | 0 | Internal MAC Transmit Errors | 0 |
| Multiple Collision Frames | 0 | Carrier Sense Errors | 0 |
| SQE Test Errors | 0 | Frames Too Long | 0 |
| Deferred Transmissions | 0 | Internal MAC Receive Errors | 0 |

**RMON Statistics:**

| | | | |
|---|---|---|---|
| Drop Events | 0 | Jabbers | 0 |
| Received Bytes | 188155 | Collisions | 0 |
| Received Frames | 0 | 64 Bytes Frames | 2249 |
| Broadcast Frames | 47 | 65-127 Bytes Frames | 459 |
| Multicast Frames | 2672 | 128-255 Bytes Frames | 11 |
| CRC/Alignment Errors | 0 | 256-511 Bytes Frames | 0 |
| Undersize Frames | 0 | 512-1023 Bytes Frames | 0 |
| Oversize Frames | 0 | 1024-1518 Bytes Frames | 0 |
| Fragments | 0 | | |

Refresh

CLI:

以下の例では、ポート13の統計情報を表示しています。

```
Console#show interfaces counters ethernet 1/13                          4-116
Ethernet 1/13
 Iftable stats:
  Octets input: 868453, Octets output: 3492122
  Unicast input: 7315, Unitcast output: 6658
  Discard input: 0, Discard output: 0
  Error input: 0, Error output: 0
  Unknown protos input: 0, QLen output: 0
 Extended iftable stats:
  Multi-cast input: 0, Multi-cast output: 17027
  Broadcast input: 231, Broadcast output: 7
 Ether-like stats:
  Alignment errors: 0, FCS errors: 0
  Single Collision frames: 0, Multiple collision frames: 0
  SQE Test errors: 0, Deferred transmissions: 0
  Late collisions: 0, Excessive collisions: 0
  Internal mac transmit errors: 0, Internal mac receive errors: 0
  Frame too longs: 0, Carrier sense errors: 0
  Symbol errors: 0
 RMON stats:
  Drop events: 0, Octets: 4422579, Packets: 31552
  Broadcast pkts: 238, Multi-cast pkts: 17033
  Undersize pkts: 0, Oversize pkts: 0
  Fragments: 0, Jabbers: 0
  CRC align errors: 0, Collisions: 0
  Packet size <= 64 octets: 25568, Packet size 65 to 127 octets: 1616
  Packet size 128 to 255 octets: 1249, Packet size 256 to 511 octets: 1449
  Packet size 512 to 1023 octets: 802, Packet size 1024 to 1518 octets: 871
Console#
```

# 3-16 アドレステーブル設定

スイッチは、既知の機器すべてのアドレスを保管しています。

同情報を使用することで、着信ポートと送信ポートとの間で直接トラフィックを受け渡すことが可能となります。トラフィックを監視する際に学習したアドレスはすべて、ダイナミックアドレステーブルに保管されています。特定のポートにバインド（固定）されている、固定アドレスを手動で設定することも可能です。

## 3-16-1 固定アドレスの設定

本製品上の特定のインタフェースに対し、固定アドレスを割り当てることが可能です。固定アドレスは指定されたインタフェースに固定されており、移動することはありません。固定アドレスが他インタフェース上で見られた場合、同アドレスは無視されアドレステーブルにも書き込まれることはありません。

コマンド解説：

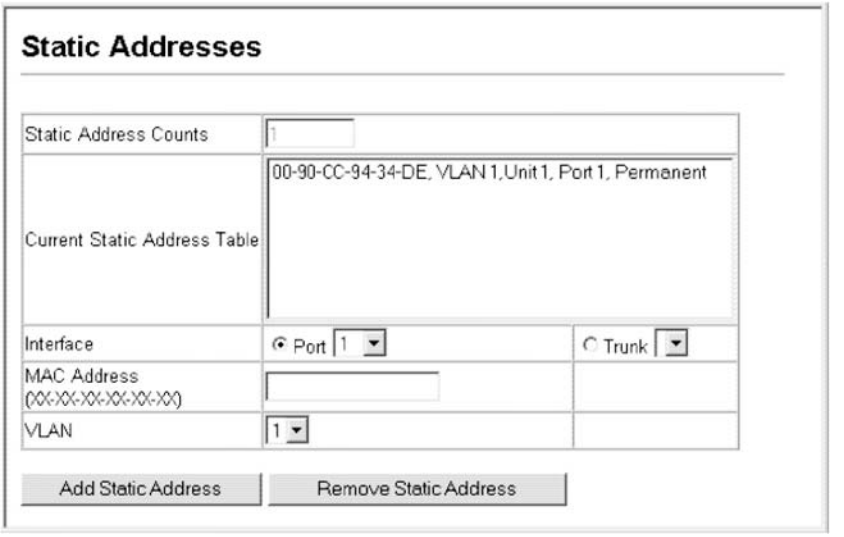
- Static Address Counts (*1) (固定アドレスカウント)
  手動で設定されているアドレスの数です。
- Current Static Address Table (現在の固定アドレステーブル)
  固定アドレスをすべて一覧表示します。
- Interface (インタフェース)
  固定アドレスに割り当てられている機器と関連付けられているポートないしトランクです。
- MAC Address (MACアドレス)
  当インタフェースにマッピングされている機器の物理アドレスです。
- VLAN
  設定されているVLANのIDです（範囲：1～4094）。

*1：WEBのみ

WEB：

Address Table(アドレステーブル)→Static Addresses (固定アドレス)と選択します。

インタフェース、MACアドレスならびにVLANを指定し、Add Static Address (固定アドレスの追加)をクリックしてください。




CLI：

以下の例では、アドレスを固定アドレステーブルに追加した後、本製品をリセットした時点で同アドレスを削除するよう設定しています。

```
Console(config)#mac-address-table static 00-90-cc-94-34-de interface
  ethernet 1/1 vlan 1 delete-on-reset                          4-134
Console(config)#
```

## 3-16-2 アドレステーブルの表示

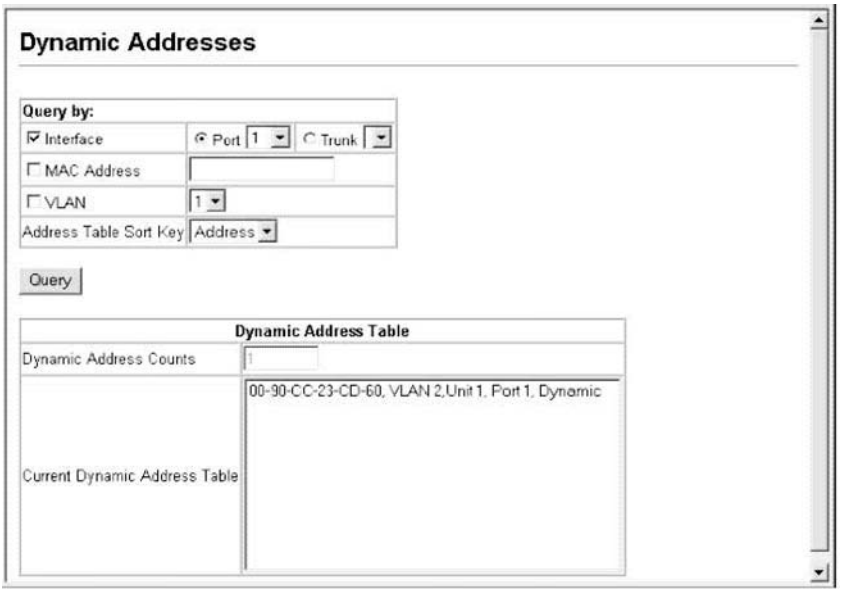
ダイナミックアドレステーブルは、本製品に届いたトラフィックの送信元（ソース）アドレスを監視する際に学習したMACアドレスを保管しています。着信トラフィックの送信先アドレスがデーベース内で見つかった場合、同アドレスに宛てられたパケットは直接、関連付けられているポートに対し転送されます。その他の場合、トラフィックは前ポートに対しフラッド送信されます。

コマンド解説：

- Interface（インタフェース）
  ポートないしトランクを示します。
- MAC Address（MACアドレス）
  当インタフェースと関連付けられている物理アドレスです。
- VLAN
  設定されているVLANのIDです（範囲：1～4094）。
- Address Table Sort Key（アドレステーブルソートキー）
  MACアドレス、VLANないしインタフェース（ポートかトランク）いずれかの順に情報を並べ替えて表示することが可能です。
- Dynamic Address Counts（動的アドレスカウント数）
  動的に学習したアドレスの数です。
- Current Dynamic Address Table（現在のダイナミックアドレステーブル）
  動的（ダイナミック）アドレスをすべて一覧表示します。

WEB：

Address Table (アドレステーブル)→Dynamic Addresses(ダイナミックアドレス)と選択します。検索種別を指定し(インタフェース、MACアドレスないしVLANの各チェックボックスにマークを入れるなど)、表示するアドレスのソート方式を選んでQuery(クエリ)をクリックしてください。




CLI：

以下の例では、ポート1のアドレステーブルエントリを表示しています。

```
Console#show mac-address-table interface ethernet 1/1                4-135
 Interface Mac Address       Vlan Type
 --------- ----------------- ---- -----------------
  Eth 1/ 1 00-90-CC-94-34-DE    1 Delete-on-reset
  Eth 1/ 1 00-90-CC-23-CD-60    2 Learned
Console#
```

## 3-16-3 エージング期間の変更

ダイナミックアドレステーブル内のエントリのエージング期間を設定します。

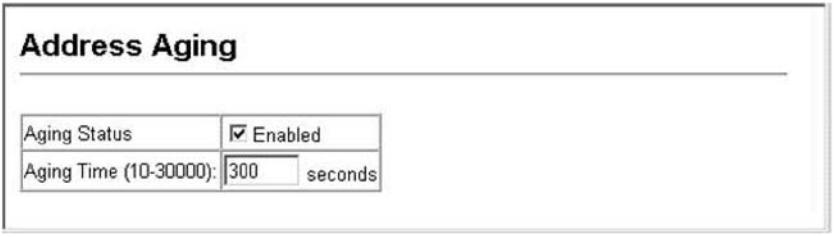
コマンド解説：

- Aging Status（エージング状態）
  当機能を有効/無効に設定します。
- Aging Time（エージング期間）
  この時間が経過した時点で、学習したエントリが1つ破棄されるかたちになります。（範囲：10～30000秒、初期設定：300秒）

WEB：

Address Table（アドレステーブル）→Address Aging（アドレスエージング）と選択します。

新規にエージング期間を指定しApply(適用)をクリックしてください。




CLI：

以下の例では、エージング期間を300秒に設定しています。

```
Console(config)#mac-address-table aging-time 300                    4-136
Console(config)#
```

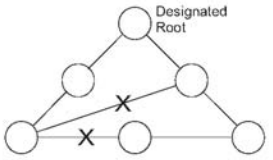
# 3-17 スパニングツリーアルゴリズムの設定

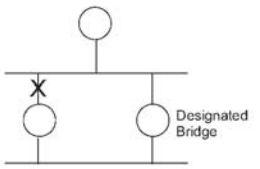
スパニングツリーアルゴリズム(STA)を使用することにより、ネットワークループの検出および無効化が行えるようになるほか、複数のスイッチ、ブリッジないしルータ間でバックアップ用のリンクを確保することが可能となります。このため本製品は、他のSTA対応ブリッジやルータなどのブリッジング機器と相互に交信し、ネットワーク内においていずれの二つの機器間においても経路が常に一つだけ存在する状態を保ちます。通常のリンク(通信経路)が利用不可となった場合もバックアップ用のリンクが自動的に通信を続行するかたちになります。

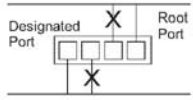
本製品で対応しているSTAバージョンは以下の通りです。

- STP:スパニングツリープロトコル(IEEE 802.1D)
- RSTP:ラピッドスパニングツリープロトコル(IEEE802.1w)

STAは分散型アルゴリズムを使用することにより、スパニングツリーネットワークのルート(根幹)として動作するブリッジング機器(STA対応スイッチ、ブリッジないしルータなど)を選択します。STAはまた、各ブリッジング機器(ルート機器を除く)上でルートポートを選択します。同ポートは、同機器からルート機器に対しパケットを転送する際のパスコストが最も低くなるものとなります。この時点でSTAは、各LANから指定ブリッジング機器(designated bridging device)を選択します。同機器は、同LANからルート機器に対しパケットを転送する際のパスコストが最も低くなるものとなります。指定ブリッジング機器に接続されているポートはすべて、指定ポート(designated port)として割り当てられます。コストの最も低いスパニングツリーを決定した後、STAはすべてのルートポートならびに指定ポートを有効にし、同時にその他のポートすべてを無効に設定します。この結果ネットワークパケットはルートポートと指定ポートとの間でのみ転送されるようになるため、ネットワークループの発生そのものを阻止することが可能となります。




Designated Root:指定ルート

Designated Bridge:指定ブリッジ

Designated Port :指定ポート

Root Port:ルートポート)

安定したネットワークトポロジが一端構築されると、ブリッジはすべて、ルートブリッジからHello BPDU (ブリッジプロトコルデータユニット)が送信されていないかどうかを確認します。

あらかじめ設定されている一定期間（Maximum Age）の間Hello BPDUがまったく届かない場合、ブリッジは、ルートブリッジとのリンクが利用不可となっているものと見なします。同ブリッジは次に他のブリッジとの間でネゴシエーションを開始し、有効なネットワークトポロジの再構成を試みます。

RSTPは、従来のより低速なSTPの後継となるよう設計されています。RSTPはまた、再構成にかかる時間を大幅に縮小しています。（例：STPでは30秒以上かかりますがRSTPでは1～3秒のみとなります。）縮小に貢献している要素としては、1）アクティブなポートが学習を開始する前の段階での状態変化（ステートの変化）回数を減らしていること、2）ノードないしポートが利用不可となった場合に使用する代替経路を事前に設定すること、および3)再構成が発生した際にツリー構造の変化と無関係な（無反応な）ポートの情報を転送データベース内に保存しこれを保持していることが挙げられます。

## 3-17-1 グローバル設定の表示

STA Information(STA情報)画面では、本製品全体で適用されている現時点でのブリッジSTA情報の概要を表示することが可能です。

フィールド解説：

- Spanning Tree State(スパニングツリーの状態)
  STA対応ネットワークへの参加が有効となっているかどうかを示します。
- Bridge ID (ブリッジID)
  ブリッジ優先度およびMACアドレスから成る、当ブリッジを識別するIDです。(アドレスは本製品システムのものを使用します。)
- Max Age (最大待機時間)
  再構成を試みる前に、機器が設定メッセージを受信するため待機する最大時間を秒単位で設定します。指定ポートを除くすべての機器ポートは、定期的に設定メッセージを受信するようになっています。最後に届いた設定メッセージにて提供されているSTA情報がエージアウト(期限切れ)となったポートはすべて、接続されているLANの指定ポートとなります。同ポートがルートポートの場合、機器ポートの中から新たにルートポートが選出されるかたちになります。(ここで言う「ポート」は、ポートならびにトランクまで含めた「インタフェース」を指します。)
- Hello Time (ハロータイム)
  ルート機器が設定メッセージを送信する時間間隔を秒単位で設定します。
- Forward Delay (転送ディレイ)
  ルート機器がその状態(ステート)を変更する前に待機する最大時間を秒単位で設定します。ステートはdiscarding(破棄)→learning(学習)→forwarding(転送)と変化します。どの機器もフレームを転送する前にトポロジの変化についての情報を受信する必要があるため、同ディレイ設定が必要となります。またどのポートも、discarding(破棄)ステートへと戻すような矛盾する情報がないか確認する時間が必要となります。この確認を行わない場合は一時的なデータループが発生する恐れがあります。
- Designated Root (指定ルート)
  スパニングツリー内において本製品がルート機器として認めた機器の、優先度およびMACアドレスです。
    - Root Port (ルートポート)
      当スイッチ上のポートのうち、ルートに最も近いもののポート数です。当スイッチは、このポートを通してルート機器との通信を行います。ルートポートが存在しない場合は、同スイッチがスパニングツリー内のルート機器として認められます。
    - Root Path Cost (ルートパスコスト)
      当スイッチ上のルートポートからルート機器までのパスコストです。
- Configuration Changes (構成変更数)
  スパニングツリーがこれまで再構成された回数を示します。

・トポロジ変更後の経過時間
スパニングツリーが最後に再構成されてから経過している時間です。
以下のパラメータはCLIでのみ表示可能です。

・Spanning tree mode (スパニングツリーモード)
当スイッチ上で使用するスパニングツリーの種類を指定します。
  - STP
    スパニングツリープロトコル(IEEE 802.1D)
  - RSTP
    ラピッドスパニングツリー(IEEE802.1w)

・Priority (優先度)
ルート機器、ルートポートおよび指定ポートを選択する際に使用するブリッジ優先度です。最も高い優先度を持つ機器がSTAルート機器となります。ただしすべての機器が同じ優先度を有する場合は、最も低いMACアドレスを備えたものがルート機器となります。

・Root Hello Time (ルートハロータイム)
当機器が設定メッセージを送信する時間間隔を秒単位で示します。

・Root Maximum Age (ルート最大エージング時間)
再構成を試みる前に、当機器が設定メッセージを受信するため待機する最大時間を秒単位で示します。指定ポートを除くすべての機器ポートは、定期的に設定メッセージを受信するようになっています。最後に届いた設定メッセージにて提供されているSTA情報がルートポート上でエージアウト(期限切れ)となった時点で、ネットワークに接続されている機器ポートの中から新規にルートポートが選出されます。(ここで言う「ポート」は、ポートならびにトランクまで含めた「インタフェース」を指します。)

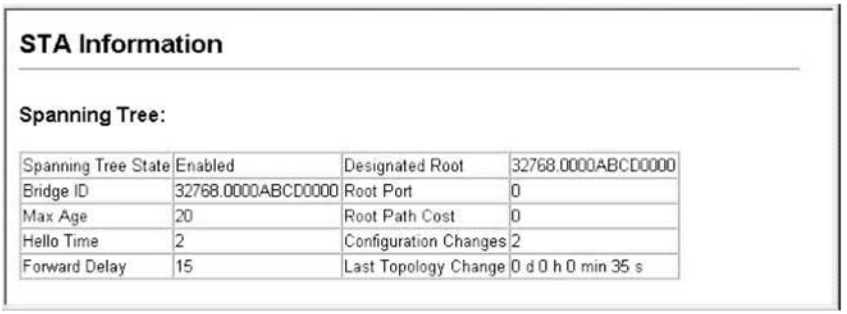
・Root Forward Delay (ルート転送ディレイ)
当機器がその状態(ステート)を変更する前に待機する最大時間を秒単位で設定します。ステートはdiscarding(破棄)→learning(学習)→forwarding(転送)と変化します。どの機器もフレームを転送する前にトポロジの変化についての情報を受信する必要があるため、同ディレイ設定が必要となります。またどのポートも、discarding(破棄)ステートへと戻すような矛盾する情報がないか確認する時間が必要となります。この確認を行わない場合は一時的なデータループが発生する恐れがあります。

・Transmission limit (送信制限)
連続してRSTP BPDUを送信する際に設けられる、最小限の送信間隔です。

・Path Cost Method (パスコスト方式)
本製品は、パスコストをもとに機器間で最も適切な経路(パス)を決定します。パスコスト方式は、各インタフェースに割り当てることが可能な値の範囲を決定する際に使用します。

WEB:

Spanning Tree (スパニングツリー9→STA→Information(情報)と選択します。



**STA Information**

**Spanning Tree:**

| | | | |
|---|---|---|---|
| Spanning Tree State | Enabled | Designated Root | 32768.0000ABCD0000 |
| Bridge ID | 32768.0000ABCD0000 | Root Port | 0 |
| Max Age | 20 | Root Path Cost | 0 |
| Hello Time | 2 | Configuration Changes | 2 |
| Forward Delay | 15 | Last Topology Change | 0 d 0 h 0 min 35 s |

CLI:

当コマンドは、グローバルSTA設定を表示した後、それぞれのポートの設定を表示します。

```
Console#show spanning-tree                                          4-147
Spanning-tree information
---------------------------------------------------------------
 Spanning tree mode                :RSTP
 Spanning tree enable/disable      :enabled
 Priority                          :32768
 Bridge Hello Time (sec.)          :2
 Bridge Max Age (sec.)             :20
 Bridge Forward Delay (sec.)       :15
 Root Hello Time (sec.)            :2
 Root Max Age (sec.)               :20
 Root Forward Delay (sec.)         :15
 Designated Root                   :32768.0.0000ABCD0000
 Current root port                 :1
 Current root cost                 :200000
 Number of topology changes        :1
 Last topology changes time (sec.):13380
 Transmission limit                :3
 Path Cost Method                  :long
:
:
```

**注意**:　　当機器がネットワークに接続されていない場合は、current root port (現在のルートポート)ならびにcurrent root cost(現在のルートコスト)はいずれも0と表示されます。

## 3-17-2 グローバル設定の変更

グローバル設定は本製品全体に適用されます。

コマンド利用：

- Spanning Tree Protocol (スパニングツリープロトコル)
  内部ステート機器(internal state machine)用としてはRSTPを使用しますが、802.1D BPDUのみ送信します。
- Rapid Spanning Tree Protocol (ラピッドSTP) (*1)
  RSTPは着信プロトコルメッセージを監視しまたRSTPノードの発信するプロトコルメッセージの種類を自動的に調整することにより、STPおよびRSTP両者のノードへの接続に対応します(以下参照)。
  - STP Mode (STPモード)
    ポートの移行(migration)ディレイタイマが期限切れとなった後で802.1D BPDU (STP BPDU)を受信した場合、本製品は自身が802.1Dブリッジと接続されているものと見なし、802.1D BPDUのみ使用するようになります。
  - RSP Mode (RSTPモード)
    RSTPが802.1D BPDUをポート上で使用しており、かつ移行ディレイが期限切れとなった後でRSTP BPDUを受信した場合、RSTPは移行ディレイタイマを再開始するとともに同ポート上でRSTP BPDUを使用するようになります。

コマンド解説：

Basic Configuration of Global Settings (グローバル設定の基本設定)

- Spanning Tree State (スパニングツリーの状態)
  本製品上でSTAを有効/無効に設定します。(初期設定：有効(enabled))
- Spanning Tree Type (スパニングツリー種別)
  本製品で使用するスパニングツリーの種類を指定します。
  - STP
    スパニングツリープロトコル(IEEE 802.1D) 当オプションを選択した場合、本製品は、STP強制互換モードに設定されているRSTPを利用します。
  - RSTP
    ラピッドスパニングツリー(IEEE 802.1w)：RSTPが初期設定となります。
- Priority (優先度)
  ルート機器、ルートポートおよび指定ポートを選択する際に使用するブリッジ優先度です。最も高い優先度を持つ機器がSTAルート機器となります。ただしすべての機器が同じ優先度を有する場合は、最も低いMACアドレスを備えたものがルート機器となります。(なお、数値的に低いものがより高い優先度を持つかたちになります。)
  - 初期設定：32768
  - 範囲：0～61440 (4096ごとに増減)

- オプション：0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440

Root Device Configuration（ルート機器設定）

・ Hello Time（ハロータイム）
ルート機器が設定メッセージを送信する時間間隔を秒単位で設定します。
  - 初期設定：2
  - 最小設定：1
  - 最大設定：10か、[(Max. Message Age（最大メッセージエイジング時間))/2]-1]のうちより小さい値

*1 STPおよびRSTP BPDUはタグ無しフレームとして送信されるほか、いかなるVLAN境界をも越えて移動することが可能です。

・ Maximum Age（最大エージング時間）
再構成を試みる前に、機器が設定メッセージを受信するため待機する最大時間を秒単位で示します。指定ポートを除くすべての機器ポートは、定期的に設定メッセージを受信するようになっています。最後に届いた設定メッセージにて提供されているSTA情報がエージアウト（期限切れ）となったポートは、接続しているLANの指定ポートとなります。同ポートがルートポートの場合、ネットワークに接続されている機器ポートの中から新規にルートポートが選出されます。（ここで言う「ポート」は、ポートならびにトランクまで含めた「インタフェース」を指します。）
  - 初期設定：20
  - 最小設定：6と [2 x（ハロータイム+1)]のうち数値の高いもの
  - 最大設定：40と[2 x（転送ディレイ-1)]のうち数値の低いもの

・ Forward Delay（転送ディレイ）
当機器がその状態（ステート）を変更する前に待機する最大時間を秒単位で設定します。ステートはdiscarding(破棄)→learning(学習)→forwarding(転送)と変化します。どの機器もフレームを転送する前にトポロジの変化についての情報を受信する必要があるため、同ディレイ設定が必要となります。またどのポートも、discarding(破棄)ステートへと戻すような矛盾する情報がないか確認する時間が必要となります。この確認を行わない場合は一時的なデータループが発生する恐れがあります
  - 初期設定：15
  - 最小設定：4と[(Max. Message Age(最大メッセージエイジング時間)/2)+1]のうち数値の高いもの
  - 最大設定：30

Configuration Settings for RSTP(RSTP設定の変更)

・ Path Cost Method (パスコスト方式)

本製品は、パスコストをもとに機器間で最も適切な経路(パス)を決定します。パスコスト方式は、各インタフェースに割り当てることが可能な値の範囲を決定する際に使用します。

- Long (長)

  32ビットベースの値を指定します。範囲は1～200,000,000となります。当設定が初期設定となります。

- Short (短)

  16ビットベースの値を指定します。範囲は1～65535となります。

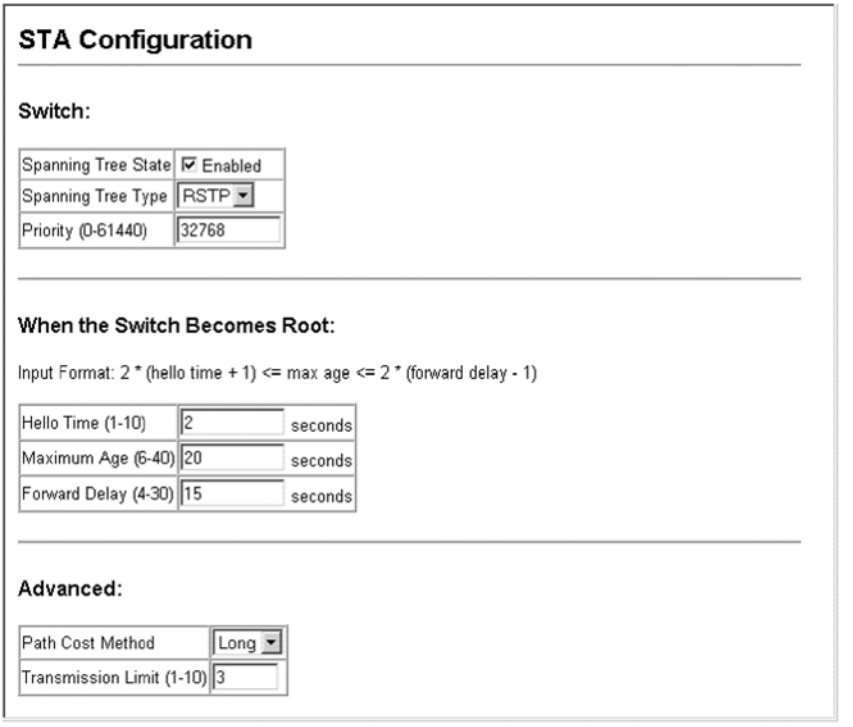
・ Transmission Limit (送信制限)

BPDUの最大送信速度は、プロトコルメッセージを連続で送信する際の最小送信間隔により指定されます。(範囲:1～10、初期設定:3)

WEB：

Spanning Tree (スパニングツリー)→STA→Configuration(設定)と選択します。

必要に応じて設定を変更し、Apply(適用)をクリックしてください。




CLI：

以下の例では、STPを有効にしモードをRSTPに設定した上でSTAならびにRSTPのパラメータを設定しています。

```
Console(config)#spanning-tree                                    4-137
Console(config)#spanning-tree mode rstp                          4-138
Console(config)#spanning-tree priority 45056                     4-141
Console(config)#spanning-tree hello-time 5                       4-139
Console(config)#spanning-tree max-age 38                         4-140
Console(config)#spanning-tree forward-time 20                    4-139
Console(config)#spanning-tree pathcost method long               4-141
Console(config)#spanning-tree transmission-limit 4               4-142
Console(config)#
```

## 3-17-3 インタフェース設定の表示

STA Port Information (STAポート情報)およびSTA Trunk Information (STAトランク情報)ページは、スパニングツリー内における現在のポートおよびトランクの状況を表示します。

フィールド解説:

- Spanning Tree (スパニングツリー)
  当インタフェース上でSTAが有効となっているかどうかを示します。
- STA Status (STAステータス)
  スパニングツリー内における、当ポートの現在の状態を示します。
  - Discarding (破棄)
    ポートはSTA設定メッセージを受信しますが、パケットの転送は行いません。
  - Learning (学習)
    ポートは、Forward Delay(転送ディレイ)パラメータで設定されている期間の間、矛盾する情報を受信することなく設定メッセージを送信しています。ポートアドレステーブルが消去され、同ポートはアドレスの学習を開始します。
  - Forwarding (転送)
    ポートはパケットを送信した上でアドレスの学習を続行します。
- ポートステータスを決定するルールは以下の通りです。
  - ほかにSTA互換ブリッジング機器が存在しないネットワークセグメント上のポートが常に転送を行っていること
  - 同一スイッチ上で二つのポートが同じセグメントに接続されており、同セグメントにほかにSTA機器が接続されていない場合、より値の低いIDを持つポートがパケットの転送を行い、もう一方のポートは破棄を行います。
  - 本製品が軌道した際、すべてのポートは破棄状態となります。このうちいくつかのポートが学習ステートへと移行し、さらに転送ステートへと移行します。
- Forward Transitions (転送への移行回数)
  当ポートが学習ステートから転送ステートまで移行した回数です。
- Designated Cost (指定コスト)
  現在のスパニングツリー構成の中で、パケットが当ポートからルートまで移動する際のコストです。メディアがより低速なほどコストは高くなります。
- Designated Bridge (指定ブリッジ)
  当ポートがスパニングツリーのルートと通信する際、経由しなければならない機器のブリッジ優先度ならびにMACアドレスです。
- Designated Port (指定ポート)
  本製品がスパニングツリーのルートと通信する際に経由しなければならない、指定ブリッジ機器上のポートのポート優先度ならびにポート数です。

・ Oper Link Type (実行リンク種別)

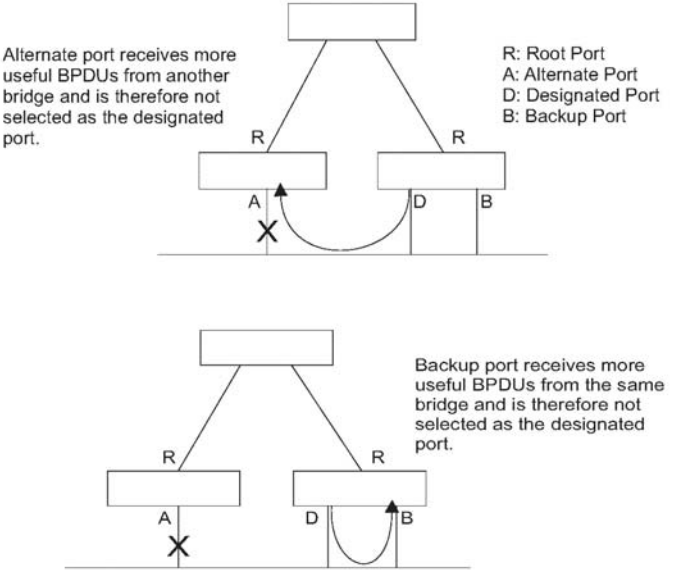
当インタフェースに接続しているLANセグメントの、実行上のポイントツーポイント状態です。P.173「インタフェース設定の表示」のAdmin Link Type (管理リンク種別)にて解説されているように、当パラメータは手動で決定(設定)できるようになっているほか、自動検出することも可能です。

・ Oper Edge Port (実行エッジポート)

当パラメータの初期設定は、p.175の「STAポート設定」内のAdmin Edge Port (管理エッジポート)の設定どおり(trueないしfalse)となりますが、当ポートに他ブリッジが接続されるなどしてBPDUが受信された場合はfalseとなります。

・ Port Role (ポートの役割)

ポートに対し割り当てられるRole(役割)は以下の通りです。ブリッジをルートブリッジに接続している稼働中(アクティブ)のトポロジの一部である場合はルート(root)ポートとなります。ブリッジを介しLANをルートブリッジに接続している場合は指定(designated)ポートとなります。他のブリッジやブリッジポート、ないしLANが利用不可または外された場合において接続を提供する場合は代替(alternate)ポートないしバックアップ(backup)ポートとなります。スパニングツリー内で何ら役割を担わないポートは無効(disabled)ポートとして設定されます。




Alternate…. port: 代替ポートは他ブリッジからより有益なBPDUを受信するため、指定ポートとしては選ばれません。

R:ルートポート

A:代替ポート

D：指定ポート

B：バックアップポート

Backup…. port ：バックアップポートは同じブリッジからより有益なBPDUを受信するため指定ポートとしては選ばれません。

・ Trunk Member(トランクメンバー)

ポートがトランクのメンバーであるかどうかを示します。(STA Port Information(STAポート情報)画面のみ))

以下のパラメータはCLIでのみ表示可能となっています。

・ Admin status (管理ステータス)

インタフェースが有効となっているかどうかを示します。

・ Path cost(パスコスト)

STAは、当パラメータを使って機器間における最適な経路を決定します。このため、より高速なメディアに接続しているポート対してはより低い値を、またより低速なメディアのポートに対してはより高い値を割り当てる必要があります。(Path costは、port priority (ポート優先度)より優先されます。)

・ Priority (優先度)

STA内における、当ポートの優先度を設定します。スイッチ上のポートすべてのpath cost(パスコスト)が同じである場合、最もpriority(優先度)の高い(値の最も低い)ポートがスパニングツリー内において有効な(アクティブな)リンクとして設定されます。このためSTAがネットワークループを削除する際においても、より優先度の高いポートが遮断される可能性を低くすることが可能となります。複数のポートに対して最も高い優先度が割り当てられている場合は、IDの値の最も低いポートが有効となります。

・ Designated root (指定ルート)

本製品がルート機器として認めたスパニングツリー内の機器の、優先度およびMACアドレスです。

・ Fast Forwarding (高速転送)

Admin Edge port (管理エッジポート)と同じ情報を表示します。本製品より前に発売されている機器との互換性を保つ目的でのみ搭載されています。

・ Admin Edge Port (管理エッジポート)

ブリッジされているLANの末端部分ないし、末端ノードに位置するLANセグメントにインタフェースが接続されている場合は、当オプションを有効に設定することが可能です。末端ノードでは転送ループが発生することがないため、スパニングツリーの転送ステートに直接移行できるようになっています。エッジポートを指定することにより、1)ワークステーションやサーバなどの機器をより高速に収束(集中管理)することが可能となる、2)現在の転送データベースを維持し、再構成イベント中にアドレステーブルを再度作成する際に発生するフレームフラッディングの量を縮小できるようになる、3)インタフェースのステートが変わってもスパニングツリーが再構成しなくなる、また4)STA関連のタイムアウト問題を克服できるようになる、といった利点を得ることが可能となります。ただし、エッジポートは末端ノード機器に接続されているポート上でしか有効にできませんのでご注意ください。

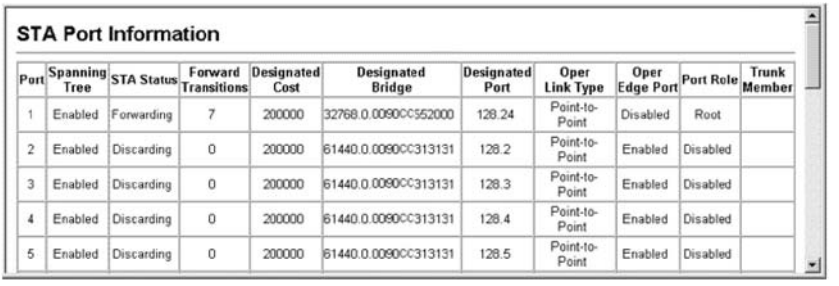
・ Admin Link Type (管理リンク種別)

当インタフェースに接続されているリンクの種類です。

- Point-to-Point (ポイントツーポイント)
  他のブリッジ一台のみとの接続です。
- Shared (共有)
  2台ないしそれ以上のブリッジとの接続です。
- Auto (自動)
  本製品は、当インタフェースがポイントツーポイントのリンクと接続されているか、それとも共有メディアと接続されているのかどうかを自動的に判断します。

WEB:

Spanning Tree (スパニングツリー)→STA→Port Information (ポート情報)ないしSTA Trunk Information(STAトランク情報)と選択します。



**STA Port Information**

| Port | Spanning Tree | STA Status | Forward Transitions | Designated Cost | Designated Bridge | Designated Port | Oper Link Type | Oper Edge Port | Port Role | Trunk Member |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Enabled | Forwarding | 7 | 200000 | 32768.0.0090CC552000 | 128.24 | Point-to-Point | Disabled | Root | |
| 2 | Enabled | Discarding | 0 | 200000 | 61440.0.0090CC313131 | 128.2 | Point-to-Point | Enabled | Disabled | |
| 3 | Enabled | Discarding | 0 | 200000 | 61440.0.0090CC313131 | 128.3 | Point-to-Point | Enabled | Disabled | |
| 4 | Enabled | Discarding | 0 | 200000 | 61440.0.0090CC313131 | 128.4 | Point-to-Point | Enabled | Disabled | |
| 5 | Enabled | Discarding | 0 | 200000 | 61440.0.0090CC313131 | 128.5 | Point-to-Point | Enabled | Disabled | |

CLI:

以下の例では、ポート5のSTA属性を表示しています。

```
Console#show spanning-tree ethernet 1/5                                    4-147
Eth  1/ 5 information
--------------------------------------------------------------
 Admin status          : enabled
 Role                  : designate
 State                 : discarding
 Path cost             : 10000
 Priority              : 128
 Designated cost       : 0
 Designated port       : 128.5
 Designated root       : 61440.0.0090CC313131
 Designated bridge     : 61440.0.0090CC313131
 Fast forwarding       : disabled
 Forward transitions   : 0
 Admin edge port       : disabled
 Oper edge port        : disabled
 Admin Link type       : auto
 Oper Link type        : point-to-point
 Spanning Tree Status  : enabled
Console#
```

## 3-17-4 インタフェース設定の変更

ポート優先度、パスコスト、リンク種別およびエッジポートなどを含む、RSTP属性設定をインタフェースごとに変更することが可能です。同一メディア上の複数のポートに対し、それぞれ1）異なる優先度やパスコストを設定して優先的に使用する経路（パス）を指定することが可能なほか、2）リンク種別を設定してポイントツーポイント接続と共有メディア接続のどちらを使用するかを決定したり、3）エッジポートの設定を行って接続先の機器が高速転送に対応しているかどうか示すことなどが可能です。（当項において「ポート」とは、ポートならびにトランクを含めた「インタフェース」を指します。）

コマンド解説：

以下の属性はリードオンリーとなっており、変更することはできません。

- STA State（STA状態）
  スパニングツリー内における、当ポイントの現在の状態を示します。（p.170の「Displaying Interface Settings（インタフェース設定の表示）」をご覧ください。）
  - Discarding（破棄）
    ポートはSTA設定メッセージを受信しますが、パケットの転送は行いません。
  - Learning（学習）
    ポートは、Forward Delay(転送ディレイ)パラメータで設定されている期間の間、矛盾する情報を受信することなく設定メッセージを送信しています。ポートアドレステーブルが消去され、同ポートはアドレスの学習を開始します。
  - Forwarding（転送）
    ポートはパケットを転送した上でアドレスの学習を続行します。
- Trunk（トランク）
  ポートがトランクのメンバーであるかどうかを示します（STA Port Configuration(STAポート設定)のみ）。

以下のインタフェース属性は変更可能となっています。

- Spanning Tree（スパニングツリー）
  当インタフェース上でSTAを有効/無効に設定します。（初期設定：Enabled（有効））
- Priority（優先度）
  STA内における、当ポートの優先度を設定します。スイッチ上のポートすべてのpath cost(パスコスト)が同じである場合、最もpriority(優先度)の高い（値の最も低い）ポートがスパニングツリー内において有効な（アクティブな）リンクとして設定されます。このためスパニングツリープロトコルがネットワークループを検出した場合でも、より優先度の高いポートが遮断される可能性を低くすることが可能となります。複数のポートに対して最も高い優先度が割り当てられている場合は、IDの値の最も低いポートが有効となります。
  - 初期設定：128
  - 範囲：0～240、16単位で増減

・ Path cost (パスコスト)

STPは、当パラメータを使って機器間における最適な経路を決定します。このため、より高速なメディアに接続しているポート対してはより低い値を、またより低速なメディアのポートに対してはより高い値を割り当てる必要があります。(パスコストは、port priority (ポート優先度)より優先されます。)なお、Path Cost Method (パスコスト方式)がshort(短)に設定されている場合、最大パスコストは65,535となります。

- - 範囲
  - イーサネット:200,000～20,000,000
  - ファストイーサネット:20,000～2,000,000
  - ギガビットイーサネット:2,000～200,000
- - 初期設定:
  - -イーサネット:半二重/2,000,00、全二重/1,000,000、トランク/500,000
  - -ファストイーサネット:半二重/200,000、全二重/100,000、トランク/50,000
  - -ギガビットイーサネット:全二重/10,000、トランク/5,000

・ Admin Link Type (管理リンク種別)

当インタフェースに接続されているリンクの種類です。

- Point-to-Point (ポイントツーポイント)

  他のブリッジ一台のみとの接続です。
- Shared (共有)

  2台ないしそれ以上のブリッジとの接続です。
- Auto (自動)

  本製品は、当インタフェースがポイントツーポイントのリンクと接続されているか、それとも共有メディアと接続されているのかどうかを自動的に判断します。(これが初期設定となります。)

・ Admin Edge Port (管理エッジポート)(高速転送)

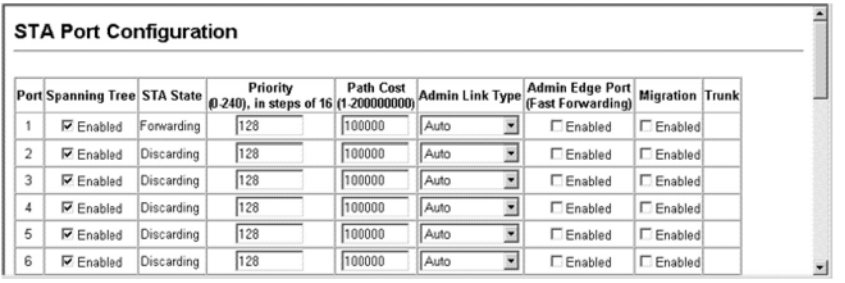
ブリッジされているLANの末端部分ないし、末端ノードに位置するLANセグメントにインタフェースが接続されている場合は、当オプションを有効に設定することが可能です。末端ノードでは転送ループが発生することがないため、スパニングツリーの転送ステートに直接移行できるようになっています。エッジポートを指定することにより、1)ワークステーションやサーバなどの機器をより高速に収束(集中管理)することが可能となる、2)現在の転送データベースを維持し、再構成イベント中にアドレステーブルを再度作成する際に発生するフレームフラッディングの量を縮小できるようになる、3)インタフェースのステートが変わってもスパニングツリーが再構成しなくなる、また4)STA関連のタイムアウト問題を克服できるようになる、といった利点を得ることが可能となります。ただし、エッジポートは末端ノード機器に接続されているポート上でしか有効にできませんのでご注意ください。(初期設定:無効)

・ Migration (移行)

設定BPDUやトポロジ変更通知BPDUなどのSTP BPDUを検出した時点で、本製品は、選択されているインタフェースを自動的に強制STP互換モードに設定します。ただしProtocol Migration(プロトコル移行)ボタンを使って、選択されているインタフェースに対し送信するのにふさわしいBPDU形式(RSTPないしSTP互換)を手動で再度確認することが可能です。(初期設定:無効)

WEB:

Spanning Tree (スパニングツリー)→STA→Port Configuration (ポート設定)ないしTrunk Configuration(トランク設定)と選択します。必要に応じて属性値を変更し、Apply(適用)をクリックしてください。




CLI:

以下の例では、ポート7のSTA属性を設定しています。

```
Console(config)#interface ethernet 1/7                          4-108
Console(config-if)#spanning-tree port-priority 0                4-143
Console(config-if)#spanning-tree cost 50                        4-142
Console(config-if)#spanning-tree link-type auto                 4-145
Console(config-if)#no spanning-tree edge-port                   4-144
Console(config-if)#
```

# 3-18 VLAN設定

## 3-18-1 IEEE802.1Q VLANについて

大規模ネットワークにおいて、ルータは各サブネット用のブロードキャストトラフィックを別々のドメインに隔離する役目を担っています。本製品でもレイヤ2にて同様のサービスを提供することが可能となっています。具体的には、VLANを使ってネットワーク上のノードグループを個別のブローキャストドメインへと編成しなおすことが可能です。VLANはブロードキャストトラフィックをその発信元グループのみに限定して送信できるようになっているため、大規模ネットワークにおいてブロードキャストストームを排除し、より安全で整然としたネットワーク環境を提供することが可能です。

IEEE802.1Q VLAN（VLANグループ）を構成するポートはネットワーク内において物理的にどの場所に位置していてもよいほか、グループ内のポートはあたかもすべて同一の物理セグメントに所属しているかのように通信できるようになっています。

VLANでは物理的な接続を一切変更することなく機器を新規VLANに移動させるといったことが可能なため、ネットワークの管理もより簡単に行えるようになります。VLANは簡単に再編成できるようになっているため、部署グループ（例：マーケティング部、技術開発部など）、利用目的別グループ（例：e-mailなど）およびマルチキャストグループ（例：ビデオ会議などのマルチメディアアプリケーションなど）もすべて反映させることが可能です。

VLANはブロードキャストトラフィックを縮減させることによりネットワーク上の通信効率を改善することが可能なほか、ネットワーク上で何か変更を加える場合においても、IPアドレスやIPサブネットといったパラメータを更新する手動を手間を完全に省きます。VLANでは、他のVLANに到達（通信）する際においてトラフィックが設定済みのレイヤ3リンクを通過する必要が発生するため、VLAN自身がすでに高度なネットワークセキュリティを提供していると言えます。

本製品で対応しているVLAN機能は以下のとおりです。

- IEEE802.1Q標準準拠のVLANグループを最大255グループまでサポート
- GVRPプロトコルおよび明示的ないし暗示的なタギングを使用した、複数スイッチ間における分散型VLAN学習機能
- ポートオーバラーラッピング（重複）に対応するため、一つのポートで複数のVLANに参加することが可能
- 末端ステーションは複数のVLANに所属可能
- VLAN対応機器とVLAN未対応機器との間でトラフィックの転送が可能
- 優先度タギング機能

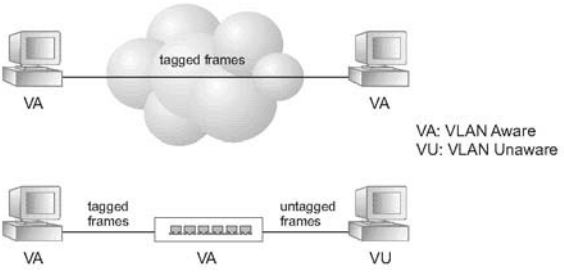
### 3-18-1-1 VLANへのポートの割当

本製品上でVLANを有効にする前に、まず各ポートを参加するVLANグループに割り当てる必要があります。初期設定では、ポートはすべてタグ無しポートとしてVLAN1に割り当てられています。一つ以上のVLANに対しトラフィックを運ぶ形でポートを利用する場合で、

かつ中間のネットワーク機器ならびに接続の反対側のホストがVLANに対応している場合は、同ポートをタグ付きポートとして追加してください。次に手動ないしGVRPを使った自動設定にて、トラフィックを運ぶ経路上に存在する他のVLAN対応ネットワーク機器上のポートを同VLANに割り当ててください。ただし本製品上のポートを複数のVLANに参加させたい場合で、中間ネットワーク機器および接続の反対側のホストのどちらもVLANに対応していない場合は、同ポートはタグ無しポートとして追加する必要があります。

注意:

VLANタグの付いているフレームはVLAN対応/VLAN非対応のネットワーク相互接続機器を通過できますが、VLANタギングに対応していない末端ノードホストに到達する前の時点でVLANタグを取り外す必要があります。




tagged frames :タグ付きフレーム

VA: VLAN対応

VU:VLAN未対応

untagged frames:タグ無しフレーム

■VLANの区分

本製品はフレームを受信すると、同フレームを以下の二通りの区分いずれかに分類します。フレームがタグ無しのものであった場合、本製品は同フレームを(受信ポートの初期設定VLAN IDに基づき)関連付けられているVLANに割り当てます。逆にフレームがタグ付きであった場合、本製品はタグ付きVLAN IDを使って同フレームのポートブロードキャストドメインを識別します。

■ポート重複(Port Overlapping)

ポート重複機能を使用することにより、ファイルサーバやプリンタといったよく利用される共有ネットワーク資源を異なるVLANグループ間でアクセスすることが可能となります。なお、重複しないVLANを導入しかつVLAN間で通信を行わせる場合は、該当するVLANを本製品経由で接続し、本製品上でルーティングを有効とすることで通信が可能となります。

■タグ無しVLAN

タグ無し(固定)VLANは通常、ブロードキャストトラフィックを減らしセキュリティを向上させる目的で利用されています。同一のVLANに割り当てられたネットワーク上のユーザは、本製品上で設定されている他のVLANとは隔離されたブロードキャストドメインを構成するかたちになります。パケットも、同じVLANが指定されているポート間でのみ転送されます。タグ無しVLANを使用することにより、ユーザグループやサブネットを手動で隔離することが可能です。ただし利用可能な場合においては、なるべくIEEE802.3タグ付きVLANをGVRPと併用し、VLAN登録が完全に自動で行われるようにしてください。

■自動VLAN登録

GVRP(GARP VLAN登録プロトコル)は、各末端ステーション(端末)を割り当てるVLANを本製品が自動的に学習できるよう、システムの定義(設定)を行います。末端ステーション(ないしそのネットワークアダプタ)がIEEE802.1Q VLANプロトコルに対応している場合は、同ステーションからご使用ネットワークに対し、自身が参加を希望するVLANグループを示すようメッセージをブロードキャストさせることが可能です。本製品はこれらのメッセージを受信すると、受信ポートを自動的に指定VLANに割り当て、同メッセージを他のすべてのポートに転送します。メッセージがGVRPに対応した他のスイッチに到達すると、同スイッチもまた受信ポートを指定VLANに割り当て、同メッセージを他のすべてのポートに渡します。
VLANの必須条件(要求条件)は、このようにしてネットワーク全体に伝播します。この結果、末端ステーション側の要求にのみ基づきGVRP対応機器を自動的に設定することが可能となります。

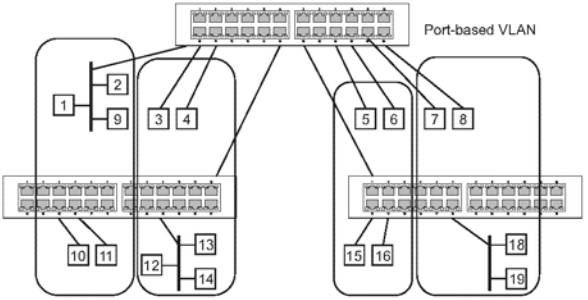
GVRPをネットワークで導入する場合は、まずホスト機器を必要なVLANに追加し(OSないし他のアプリケーションソフトウェアを使用)、これらのVLANがネットワーク上で増殖できるようにしておく必要があります。

1)これらのホストに直接接続されているエッジスイッチ

2)ネットワーク内のコアスイッチ

両者において、同機器間のリンクではGVRPを有効に設定してください。またネットワーク上におけるセキュリティ境界も決定し、該当する境界ポートにおいてはGVRPを無効にして宣伝内容などが伝播しないようにするか、該当ポートの制限(付)VLANへの参加を禁止してください。

**注意**:ご使用のホスト機器の中にGVRPに対応していないものがある場合は、該当機器に接続されているスイッチポート用として固定ないしタグ無しのVLANを設定する必要があります(p.189の「Adding Static Members to VLANs (VLAN Index):VLAN/VLANインデックスに固定メンバーを追加する」を参照)。ただしこれらのエッジ(末端)スイッチでも、またネットワーク内のコアスイッチ上においても、GVRPは有効に設定することが可能です。




Port-based VLAN (ポートベースVLAN)〉

### 3-18-1-2 タグ付き/タグ無しフレームの転送

スイッチ一台に直接接続されている機器用として小規模のポートベースVLANを作成する場合は、ポートを同一のタグ無しVLANに割り当ててください。ただし複数のスイッチにまたがっているVLANに参加させる場合は、同グループ用のVLANを作成した上で全ポート上でタギングを有効とする必要があります。

ポートは、複数のタグ付きないしタグ無しVLANに対し割り当てることが可能です。このため、当スイッチ上のポートはいずれも、タグ付きおよびタグ無しフレーム両者に対応していることになります。VLAN対応機器を含む経路に沿ってフレームを本製品から転送する場合、本製品側でVLANタグを付与する必要があります。送信先ホストも含め、VLAN対応機器を一切含まない経路に沿ってフレームを本製品から転送する場合、同フレームを転送する前に本製品上でVLANタグを取り外す必要があります。タグ付きフレームを受信した場合、本製品は同フレームを、フレームタグにて示されるVLANに対し転送します。ただしVLAN未対応機器からタグ無しフレームを受信した場合、本製品はフレームの転送先を決定した上で、着信ポートの初期設定VIDを反映するVLANタグを挿入します。

### 3-18-1-3 GVRPの有効/無効設定(グローバル設定)

GVRP (GARP VLAN登録プロトコル)を使用することにより、スイッチ間でVLAN情報を交換しネットワーク全般に渡ってVLANメンバーポートを登録することが可能となります。VLANは、ホスト機器により発行される参加(join)メッセージに基づき自動的に設定され、またネットワーク上で伝播するようになっています。VLANの自動登録を許可するためにはGVRPを有効にしておく必要があるほか、ローカルスイッチを越えて拡がっているVLANもサポートしていなければなりません。(初期設定:Disabled (無効))

WEB:

VLAN→802.1Q VLAN→GVRP Status (GVRPステータス)と選択します。

GVRPを必要に応じて有効/無効に設定し、Apply(適用)をクリックしてください。


CLI:

以下の例では、本製品上でGVRPを有効に設定しています。

```
Console(config)#bridge-ext gvrp                                    4-164
Console(config)#
```

### 3-18-1-4 基本VLAN情報の表示

VLAN Basic Information (VLAN基本情報)ページでは、本製品で対応しているVLANの種別に関する基本的な情報を表示します。

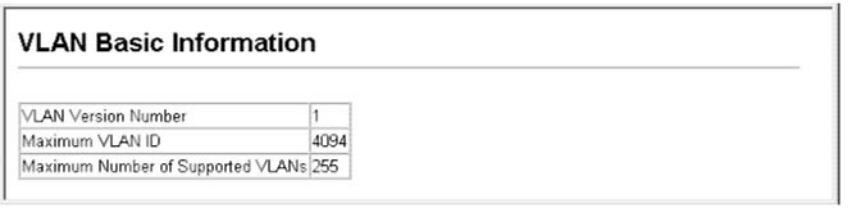
フィールド解説:

- VLAN Version Number (*1) (VLANバージョン)
  IEEE802.1Q標準で定義されているもののうち、本製品上で対応しているVLANのバージョン番号となります。
- Maximum VLAN ID(最大VLAN ID)
  本製品上で認識可能なVLAN IDの最大値です。

(*1) WEBのみ

WEB:

VLAN→802.1Q VLAN→Basic Information(基本情報)と選択します。




CLI:

以下のコマンドを入力してください。

```
Console#show bridge-ext                                          4-165
 Max support vlan numbers:              255
 Max support vlan ID:                   4094
 Extended multicast filtering services: No
 Static entry individual port:          Yes
 VLAN learning:                         IVL
 Configurable PVID tagging:             Yes
 Local VLAN capable:                    No
 Traffic classes:                       Enabled
 Global GVRP status:                    Enabled
 GMRP:                                  Disabled
Console#
```

### 3-18-1-5 現在のVLAN情報の表示

VLAN Current Table (現在のVLAN状態テーブル(表))は、各VLANの現時点におけるポートメンバーおよび各ポート上でVLANタギングに対応しているかどうかを表示します。複数のスイッチを経由するような大規模なVLANグループに割り当てられているポートは、VLANタギングを使用する必要があります。ただし、1～2台のスイッチのみを利用する小規模のポートベースVLANを作成する場合はタギングを無効にすることが可能です。

コマンド解説(WEB):

- VLAN ID
  設定されているVLANのIDです。(範囲:1～4094)
- Up Time at Creation(作成時間)
  当VLANが作成された時間です(例:System Up Time)。
- Status (ステータス)
  当VLANがどのようにして本製品に追加されているかを示します。
  - Dynamic GVRP (自動GVRP)
    GVRP経由で自動的に学習しています。
  - Permanent (固定)
    固定(static)エントリとして追加されています。
- Egress Ports (発信ポート)
  すべてのVLANポートメンバーを表示します。
- Untagged Ports (タグ無しポート)
  タグ無しVLANポートメンバーを表示します。

WEB：

VLAN→802.1Q VLAN→Current Table (現在の状況(テーブル))と選択します。

スクロールダウンリストから該当するIDを選んでください。


コマンド解説(CLI)：

- VLAN
  設定されているVLANのIDです。(範囲：1～4094、番号の先頭でゼロは使えません)
- Type (種別)
  当VLANがどのようにして本製品に追加されているかを示します。
  - Dynamic (自動)
    GVRP経由で自動的に学習しています。
  - Static (固定)
    固定(static)エントリとして追加されています。
- Name (名称)
  当VLANの名称を1～32文字の範囲で設定します。
- Status (ステータス)
  当VLANが有効/無効のどちらの状態であるかを表示します。
  - Active (有効)
    VLANは稼動可能状態にあります。

- Suspend (一時停止)

  VLANは一時停止状態となっています(例:パケットが通過できない状態です)。

・ Ports/Channel groups (ポート/チャネルグループ)

  VLANインタフェースメンバーを表示します。

CLI:

現在のVLAN情報を表示する場合は以下のコマンドを入力してください。

```
Console#show vlan id 1                                              4-157
Vlan ID:               1
Type:                  Static
Name:                  DefaultVlan
Status:                Active
Ports/Port Channel:    Eth1/ 1(S) Eth1/ 2(S) Eth1/ 3(S) Eth1/ 4(S) Eth1/ 5(S)
                       Eth1/ 6(S) Eth1/ 7(S) Eth1/ 8(S) Eth1/ 9(S) Eth1/10(S)
                       Eth1/11(S) Eth1/12(S) Eth1/13(S) Eth1/14(S) Eth1/15(S)
                       Eth1/16(S) Eth1/17(S) Eth1/18(S) Eth1/19(S) Eth1/20(S)
                       Eth1/21(S) Eth1/22(S) Eth1/23(S) Eth1/24(S) Eth1/25(S)
                       Eth1/26(S)
Console#
```

### 3-18-1-6 VLANの作成

VLANグループの作成ないし削除を行う場合は、VLAN Static List (VLAN固定リスト)を使用します。本製品上で使用されているVLANグループの情報を外部ネットワーク機器に対し広げる場合は、これらのグループのVLAN IDをそれぞれ指定する必要があります。

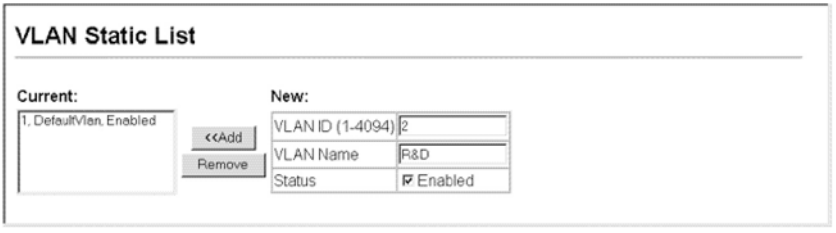
コマンド解説:

- Current (現在の状況)
  当システム用に現時点で作成されているVLANグループをすべて一覧表示します。VLANは最大255グループまで定義することが可能です。デフォルトのタグ無しVLANはVLAN 1となります。
- New (新規)
  新規VLANグループの名称およびID番号を指定することが可能です。(VLAN名は当システム上での管理目的でのみ使用します。同情報はVLANタグには追加されません。)
- VLAN ID
  設定されているVLANのIDです。(範囲:1～4094、先頭でゼロは使えません)
- VLAN Name (VLAN名)
  VLAN名を1～32文字の範囲で設定します。
- Status (ステータス)(WEB)
  指定VLANを有効/無効に設定します。
  - Enabled (有効)
    VLANは稼動可能状態となっています。
  - Disabled (無効)
    VLANは一時停止状態となっています(パケットが通過できない状態です)。
- State(ステート)(CLI)
  指定VLANを有効/無効に設定します。
  - Active (有効)
    VLANは稼動可能状態となっています。
  - Suspend (一時停止)
    VLANは一時停止状態となっています(パケットが通過できない状態です)
- Add (追加)
  現在の一覧に対しVLANグループを新規に追加します。
- Remove (削除)
  VLANグループを現在の一覧から削除します。同グループに割り当てられているポートいずれかがタグ無し状態であった場合、同ポートはVLANグループ1にタグ無しポートとして割り当てられます。

WEB：

VLAN→802.1Q VLAN→Static List (固定リスト)と選択します。

新規にVLANを作成する場合はVLAN IDおよびVLAN名を入力し、Enable (有効)チェックボックスにマークを入れVLANを有効とした上でAdd(追加)をクリックしてください。




CLI：

以下の例では新規にVLANを作成しています。

```
Console(config)#vlan database                                          4-149
Console(config-vlan)#vlan 2 name R&D media ethernet state active       4-150
Console(config-vlan)#end
Console#show vlan                                                      4-157
Vlan ID:               1
Type:                  Static
Name:                  DefaultVlan
Status:                Active
Ports/Port Channel:    Eth1/ 1(S) Eth1/ 2(S) Eth1/ 3(S) Eth1/ 4(S) Eth1/ 5(S)
                       Eth1/ 6(S) Eth1/ 7(S) Eth1/ 8(S) Eth1/ 9(S) Eth1/10(S)
                       Eth1/11(S) Eth1/12(S) Eth1/13(S) Eth1/14(S) Eth1/15(S)
                       Eth1/16(S) Eth1/17(S) Eth1/18(S) Eth1/19(S) Eth1/20(S)
                       Eth1/21(S) Eth1/22(S) Eth1/23(S) Eth1/24(S) Eth1/25(S)
                       Eth1/26(S)


Vlan ID:               2
Type:                  Static
Name:                  R&D
Status:                Active
Ports/Port Channel:

Console#
```

## 3-18-1-7 VLANに固定メンバーを追加する(VLANインデックス)

VLAN Static Table (VLAN固定テーブル)を使用することにより、選択されているVLANインデックス上でポートメンバーの設定を行うことが可能となります。ポートが802.1Q VLAN対応機器と接続している場合はタグ付きとして設定してください。逆に、VLAN対応機器に接続していない場合はタグ無しとしてポートを設定してください。また本製品はGVRPプロトコルによりポートを自動的にVLANに追加することが可能となっていますが、この機能にてVLANにポートを追加させたくない場合は、該当ポートをforbidden (禁止)に設定してください。

**注意:** 1. VLAN Static Membership by Port (ポート別VLAN固定メンバーシップ)ページにて、ポートインデックスに基づきVLANグループを設定することも可能です。ただし当設定ページでは、VLANにポートを追加する際該当ポートはタグ付きメンバーとしてしか追加できませんのでご注意ください。

2. VLAN 1は本製品上のすべてのポートを含むデフォルトのタグ無しVLANとなっており、デフォルト(初期設定)ポートVLAN IDを「Configuring VLAN Behavior for Interfaces(インタフェース上でのVLANの行動を設定する)(p.193)」にて解説されている方法にて再度割り当てる以外に、変更する手段はありません。

コマンド解説:

- VLAN
  設定されているVLANのIDです(範囲:1～4094)。
- Name (名称)
  VLANの名称です。(範囲:1～32文字)
- Status (ステータス)
  指定VLANを有効ないし無効に設定します。
  - Enable (有効)
    VLANは稼動可能状態にあります。
  - Disable(無効)
    VLANは一時停止状態となっています(パケットが通過できない状態です)。
- Port (ポート)
  ポートIDです。
- Membership Type (メンバー種別)
  該当するポートないしトランクのラジオボタンにマークを入れ、同インタフェースのVLANメンバー属性を選択してください。
  - Tagged (タグ付き)
    該当インタフェースはVLANのメンバーとなっています。同ポートから送信されるパケットはすべてタグ付きとなります。このため、該当パケットはVLANないしCoS情報を備えるかたちになります。

- Untagged (タグ無し)

  該当インタフェースはVLANのメンバーとなっています。同ポートから送信されるパケットはすべてタグ無しとなります。このため、該当パケットはVLANないしCoS情報を一切備えません。なお、インタフェースは少なくとも1つのグループに対しタグ無しポートとして割り当てる必要がありますのでご注意ください。

- Forbidden (禁止)

  インタフェースは、GVRP経由でVLANに自動的に参加することを禁止されています。詳細についてはp.180の「自動VLAN登録」をご覧ください。

- None (無し)

  該当インタフェースはVLANのメンバーではありません。当VLANと関連付けられているパケットは同インタフェースからは送信されません。

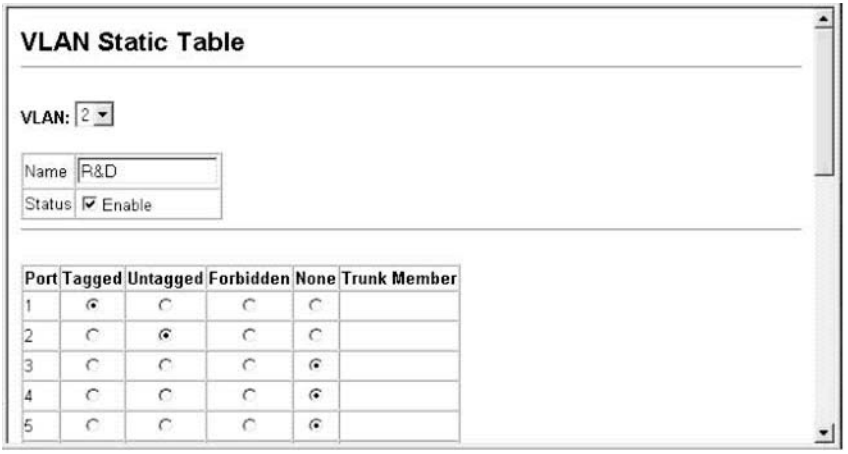
・ Trunk Member(トランクメンバー)

ポートがトランクのメンバーであるかどうかを示します。選択されているVLANにトランクを追加する場合は、VLAN Static Table (VLAN固定テーブル)ページの最後のテーブルをお使いください。

WEB:

VLAN→802.1Q VLAN→Static Table (固定テーブル)と選択します。

スクロールダウンリストからVLAN IDを選択し、必要に応じてVLAN名およびステータスを変更してください。次にポートないしトランク一覧の中の該当するラジオボタンにチェックマークを入れ、メンバー種別を選択してください。最後にApply(適用)をクリックしてください。



CLI:

以下の例では、VLAN2に対しタグ付きおよびタグ無しポートを追加しています。

```
Console(config)#interface ethernet 1/1                                  4-108
Console(config-if)#switchport allowed vlan add 2 tagged                 4-155
Console(config-if)#exit
Console(config)#interface ethernet 1/2
Console(config-if)#switchport allowed vlan add 2 untagged
Console(config-if)#exit
Console(config)#interface ethernet 1/13
Console(config-if)#switchport allowed vlan add 2 tagged
```

## 3-18-1-8 固定メンバーをVLANに追加する(ポートインデックス)

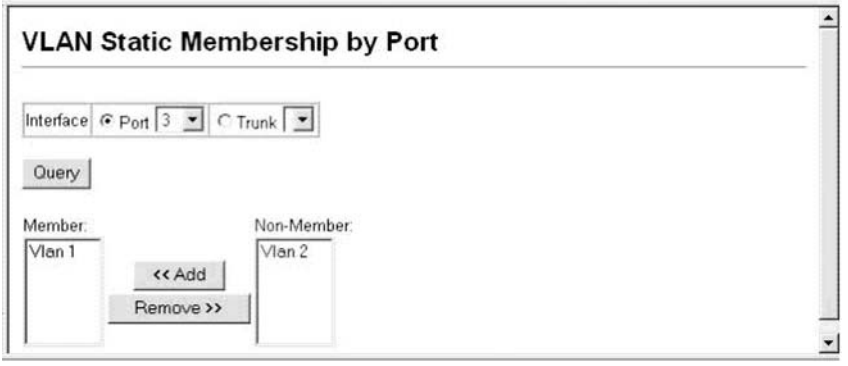
VLAN Static Membership by Port (ポート別VLAN固定メンバーシップ)メニューを使用することにより、VLANグループを選択されているインタフェースに対し、タグ付きメンバーとして割り当てることが可能となります。(訳注:上記文の後半は「～選択されているインタフェースをVLANに対しタグ付きメンバーとして割り当てることが可能となります」のことかと思いますが、念のため原文のまま訳してあります)

コマンド属性:

- Interface (インタフェース)
  ポート/トランクIDです。
- Member(メンバー)
  選択されているインタフェースがタグ付きメンバーとして所属しているVLANです。
- Non-Member(非メンバー)
  選択されているインタフェースがタグ付きメンバーとして所属していないVLANです。

WEB:

VLAN→802.1Q VLAN→Static Membership by Port(ポート別固定メンバーシップ)と選択します。スクロールダウンボックスからポートないしトランク(インタフェース)を選び、その上でQuery(クエリ)をクリックして同インタフェースのメンバーシップ情報を表示してください。次にVLAN IDを選択し、Add(追加)をクリックして同インタフェースをタグ付きメンバーとして追加するか、Remove (削除)をクリックして同インタフェースを削除してください。各インタフェースのVLANメンバーシップ設定が完了した時点でApply(適用)をクリックしてください。




CLI:

以下の例では、VLAN1に対しポート3をタグ付きポートとして追加し、さらにVLAN2からポート3を削除しています。

```
Console(config)#interface ethernet 1/3                          4-108
Console(config-if)#switchport allowed vlan add 1 tagged         4-155
Console(config-if)#switchport allowed vlan remove 2
```

## 3-18-1-9 インタフェース上でのVLAN動作を設定する

指定インタフェース上において、初期VLAN ID(PVID)、許容フレーム種別、着信フィルタリング、GVRPステータスならびにGARPタイマなどを含む、VLANの動作に関するパラメータを設定することが可能です。

コマンド利用：

- GVRP

  GVRP (GARP VLAN登録プロトコル)を使用することにより、スイッチ間でVLAN情報を交換し、ネットワーク全般に渡ってインタフェースをVLANメンバーとして自動的に登録することが可能となります。
- GARP

  GVRPは、GARP(グループアドレス登録プロトコル)を使用することにより、ブリッジ接続されているLAN内におけるクライアントサービスのクライアント属性の登録および登録解除を行います。GARPタイマの初期値は、メディアアクセス方式やデータ速度には依存しません。GVRPでの登録および登録解除がうまくいかない場合などを除き、通常の場合はこれらの値は変更しないようにしてください。

コマンド解説：

- PVID

  インタフェース上で受信されたタグ無しフレームに割り当てられるVLAN IDです。(初期設定：1)
  - インタフェースがVLAN 1のメンバーでない状態でそのPVIDを当VLANに割り当てる場合、同インタフェースは自動的にVLAN 1にタグ無しメンバーとして追加されます。他のすべてのVLANの場合、インタフェースは、そのPVIDをグループに割り当てる前に必ずタグ無しメンバーとして設定しておかなくてはなりません。
- Acceptable Frame Type (許容フレーム種別)

  インタフェースがタグ付きフレームとタグ無しフレームを含むすべての種類のフレームを受け付けるようにするか、もしくはタグ付きフレームのみ受け付けるように設定します。すべての種類のフレームを受け付けるよう設定した場合、受信されるすべてのタグ無しフレームはデフォルト(初期)VLANに割り当てられます。(選択項目：All(すべて)、Tagged (タグ付き)　初期設定：すべて)
- Ingress Filtering (着信フィルタリング)

  着信ポートがメンバーとなっていないVLAN用としてタギングの行われているフレームをどのように処理するかを決定します。(初期設定：Disabled(無効))
  - 着信フィルタリングは、タグ付きフレームにのみ影響を与えます。
  - 着信フィルタリングが無効となっている状態で、ポートがメンバーとなっていないVLANに宛てられたタグ付きフレームを同ポート上で受信した場合、同フレームは他のすべてのポートに対しフラッド送信されます(ただし当ポート上で明示的に禁止されているVLANは除く)。

- 着信フィルタリングが有効となっている状態で、ポートがメンバーとなっていないVLANに宛てられたタグ付きフレームを同ポート上で受信した場合、同フレームは破棄されます。
- 着信フィルタリングは、GVRPやSTPなどのVLANに依存しないBPDUフレームには影響を与えません。ただし、GMRPなどのVLANに依存するBPDUフレームには影響を与えます。

・ GVRP Status (GVRPステータス)

当インタフェース上でGVRPを有効/無効に設定します。当設定を行う場合は、事前にGVRPを本製品全体で(グローバルに)有効にしておく必要があります。(p.37の「ブリッジ拡張機能の表示」をご覧ください。) 無効と設定されている場合、当ポート上で受信されるGVRPパケットはすべて破棄され、またGVRP登録が他ポートから広まることもありません。(初期設定:Disabled(無効))

・ GARP Join Timer (*1) (GARP参加タイマ)

VLANグループ内に参加するための要求/クエリを発信する時間間隔です。(範囲:20～1000センチ秒(1/100秒)、初期設定:20)

・ GARP Leave Timer (GARP離脱タイマ)(*2)

VLANグループから離脱する前にポートが待機する時間間隔です。同タイマは、join(参加)時間の2倍を上回るよう設定する必要があります。このようにすることで、Leave(離脱)ないしLeaveAll(すべて離脱)メッセージが発行された後で、候補者(意訳:参加希望中の他ポートなど)は上記ポートが実際にグループから離脱する前に再び参加できるようになります。(範囲:60～3000×1/100秒、初期設定:60)

・ GARP LeaveAll Timer (*3) (GARPすべて離脱タイマ)

VLANグループ参加者(ポート)に対しLeaveAllクエリメッセージを送ってからポートがグループを離脱するまでの時間間隔です。ノードが再びグループに参加する際に発生するトラフィックの量を最小限にとどめるためにも、当時間間隔はLeave Time (離脱時間)よりきわめて大きくなるよう設定する必要があります。

(範囲:500～18000×1/100秒、初期設定:1000)

・ Mode (モード)

インタフェースのVLANメンバーシップモードを表示します。(初期設定:Hybrid(ハイブリッド))

- 1Q Trunk (1Qトランク)

  ポートをVLANトランクの末端ポイントとして指定します。トランクは2機のスイッチ間における直接的なリンクとなるため、ポートは送信元(ソース)VLANを識別するタグ付きフレームを送信します。なお、ポートのデフォルトVLAN(例:PVIDと関連付けられているものなど)に所属するポートもまたタグ付きフレームとして送信されます。

- Hybrid (ハイブリッド)

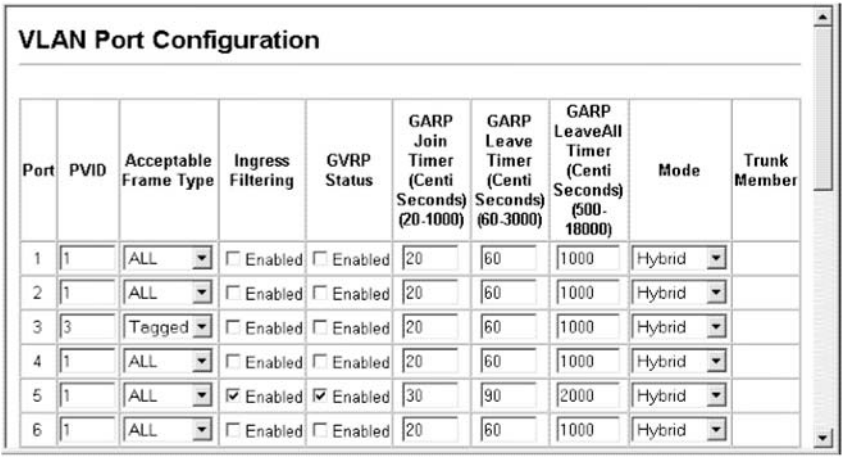
ハイブリッドVLANインタフェースを指定します。該当ポートは、タグ付きフレームとタグ無しフレームのどちらも送信することが可能です。

・ Trunk Member (トランクメンバー)

ポートがトランクのメンバーであるかどうかを示します。選択されているVLANにトランクを追加する場合は、VLAN Static Table (VLAN固定テーブル)上の最後のテーブルをお使いください。

WEB:

VLAN→802.1Q VLAN→Port Configuration(ポート設定)ないしVLAN Trunk Configuration(VLANトランク設定)と選択します。必要に応じて各インタフェースの設定内容を入力し、Apply(適用)をクリックしてください。



VLAN Port Configuration

| Port | PVID | Acceptable Frame Type | Ingress Filtering | GVRP Status | GARP Join Timer (Centi Seconds) (20-1000) | GARP Leave Timer (Centi Seconds) (60-3000) | GARP LeaveAll Timer (Centi Seconds) (500-18000) | Mode | Trunk Member |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | ALL | Enabled | Enabled | 20 | 60 | 1000 | Hybrid | |
| 2 | 1 | ALL | Enabled | Enabled | 20 | 60 | 1000 | Hybrid | |
| 3 | 3 | Tagged | Enabled | Enabled | 20 | 60 | 1000 | Hybrid | |
| 4 | 1 | ALL | Enabled | Enabled | 20 | 60 | 1000 | Hybrid | |
| 5 | 1 | ALL | Enabled | Enabled | 30 | 90 | 2000 | Hybrid | |
| 6 | 1 | ALL | Enabled | Enabled | 20 | 60 | 1000 | Hybrid | |

*1 タイマ設定は必ず以下の条件を満たさなくてはなりません。

2 x (join timer) < leave timer < LeaveAll timer

(2 x (参加タイマ)<離脱タイマ<すべて離脱タイマ)

*2 タイマ設定は以下の条件を満たす必要があります。

2 x (join timer)< leave timer < LeaveAll timer

2 x (参加タイマ)< 離脱タイマ < すべて離脱タイマ

*3 タイマ設定は以下の条件を満たす必要があります。

2 x (join timer)< leave timer < LeaveAll timer

2 x (参加タイマ)< 離脱タイマ < すべて離脱タイマ

CLI:

以下の例では、次の設定を行っています。

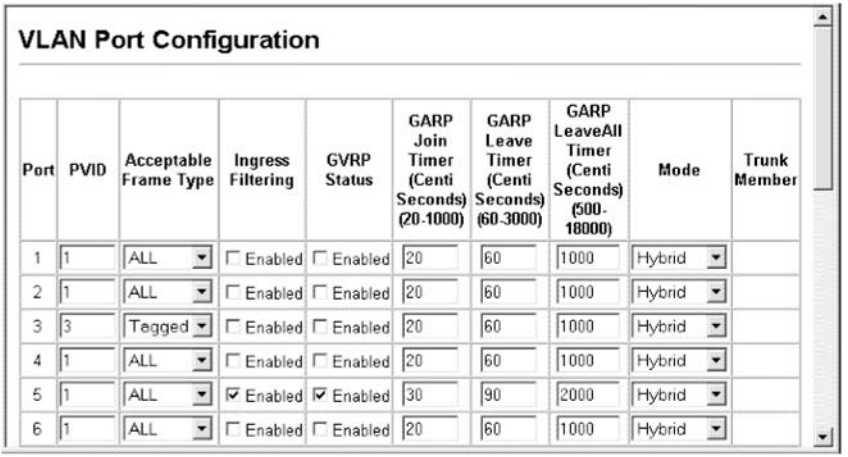
1)ポート3でタグ付きフレームのみを受信するように設定

2)PVID 3をネイティブVLAN IDとして割当

3)GVRPを有効に設定

4)GARPタイマを設定

5)スイッチポートモードをハイブリッドに設定



**VLAN Port Configuration**

| Port | PVID | Acceptable Frame Type | Ingress Filtering | GVRP Status | GARP Join Timer (Centi Seconds) (20-1000) | GARP Leave Timer (Centi Seconds) (60-3000) | GARP LeaveAll Timer (Centi Seconds) (500-18000) | Mode | Trunk Member |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | ALL | Enabled | Enabled | 20 | 60 | 1000 | Hybrid | |
| 2 | 1 | ALL | Enabled | Enabled | 20 | 60 | 1000 | Hybrid | |
| 3 | 3 | Tagged | Enabled | Enabled | 20 | 60 | 1000 | Hybrid | |
| 4 | 1 | ALL | Enabled | Enabled | 20 | 60 | 1000 | Hybrid | |
| 5 | 1 | ALL | Enabled | Enabled | 30 | 90 | 2000 | Hybrid | |
| 6 | 1 | ALL | Enabled | Enabled | 20 | 60 | 1000 | Hybrid | |

## 3-18-2 プライベートVLAN

ポートVLANは、割り当てられているVLAN内においてポートベースでのセキュリティを提供するほか、ポート間において通信を隔離することが可能です。

本製品は

1)プライマリ/セカンダリの関連付けのなされているプライベートVLANグループ

2)スタンドアロンタイプの隔離VLANの2種類のプライベートVLAN

に対応しています。プライマリVLANはプライベートVLANグループ内のすべてのポートと通信が行える無差別(promiscuous)ポートを備えています。またセカンダリ(ないしコミュニティ)VLANは、セカンダリVLAN内の他のホストおよび関連付けられているプライマリVLAN内の無差別ポートとのみ通信が行えるコミュニティポートを備えます。一方隔離VLANは、無差別ポート1ポートならびに1ポート以上の隔離(ないしホスト)ポートを備えるスタンドアロンVLAN一つのみで構成されています。いずれの場合も、無差別ポートはインターネットを含む外部ネットワークに対し自由にアクセスできますが、コミュニティないし隔離ポートはローカルユーザに対し制限されたアクセスを提供します。

本製品ではプライマリVLANを複数設定できるようになっているほか、各プライマリVLANは複数のコミュニティVLANと関連付けることが可能です。1つないしそれ以上の隔離VLANを設定することも可能です。(なお、プライベートVLANと通常のVLANは、同一のスイッチ内で同時に存続させることが可能です。)

プライマリ/セカンダリ関連付けグループを設定する場合は以下の操作を行ってください。

1. p.201のPrivate VLAN Configuration (プライベートVLAN設定)メニューを使用し、1つないしそれ以上のコミュニティVLANを指定してください。次に、VLANグループの外部のトラフィックを経由させるプライマリVLANを指定してください。

2. p.201のPrivate VLAN Association (プライベートVLAN関連付け)メニューを使用し、セカンダリ(コミュニティ)VLANをプライマリVLANに対し関連付けてください。

3. p.206のPrivate VLAN Port Configuration (プライベートVLANポート設定)メニューを使用し、ポートの種別を1)無差別(promiscuous)(プライマリVLAN内のすべてのポートに対しアクセス)か2)ホスト(host)(コミュニティVLANメンバーにのみ限定してアクセス可能とし、他のすべてのトラフィックを無差別ポートにて経由させる)のいずれかに設定してください。次に、無差別ポートをプライマリVLANに割り当て、同様にホストポートをコミュニティVLANに割り当ててください。

隔離VLANを設定する場合は以下の操作を行ってください。

1. p.201のPrivate VLAN Configuration (プライベートVLAN設定)メニューを使用し、すべてのトラフィックを単一の無差別ポートで経由させる隔離(isolated)VLANを設定してください。

2. p.206のPrivate VLAN Port Configuration(プライベートVLANポート設定)メニューを使用し、ポート種別を1)無差別(promiscuous)(外部ネットワークに接続する唯一のチャネル)か、2)隔離(isolated)(自身のVLAN内の無差別ポートにのみアクセス可能)のいずれかに設定してください。次に、同無差別ポートならびにすべてのホストポートを隔離VLANに割り当ててください。

### 3-18-2-1 現在のプライベートVLANを表示する

Private VLAN Information(プライベートVLAN情報)ページでは、本製品上で設定されているプライベートVLANの情報を確認することが可能です。表示される情報にはプライマリVLAN、コミュニティVLAN、隔離VLANならびにこれらのVLANが割り当てられているインタフェースなどが含まれます。

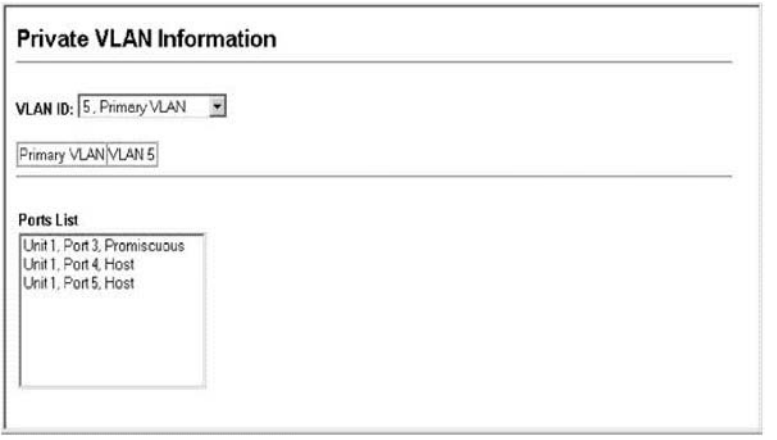
コマンド解説:

- VLAN ID
  設定されているVLANのID(1～4094)およびVLANの種別です。
- Primary VLAN (プライマリVLAN)
  選択されているVLAN IDが関連付けられているVLANです。プライマリVLANは自身のIDを表示するほか、コミュニティVLANは関連付けられているVLANを、また隔離VLANはスタンドアロンVLANを表示します。
- Port List (ポートリスト)
  選択されているプライベートVLAN内におけるポート(および割り当てられているポートの種別)の一覧です。

WEB:

VLAN→Private VLAN(プライベートVLAN)→Information(情報)と選択します。

VLAN IDドロップダウンメニューから該当するポートを選んでください。



CLI:

以下の例は、本製品にプライマリVLAN 5およびセカンダリVLAN 6が設定されている様子を示しています。ポート3は無差別ポートとして設定されかつVLAN 5にマッピングされているほか、ポート4ならびに5はホストポートとして設定され、VLAN 6に関連付けられています。このため、ポート4および5宛てのトラフィックはポート3のみ通過できるかたちになります。

```
Console#show vlan private-vlan                                    4-153
Primary   Secondary       Type        Interfaces
--------  -----------  ----------  ---------------------------------------
     5                 primary     Eth1/ 3
     5         6       community   Eth1/ 4 Eth1/ 5
```

## 3-18-2-2 プライベートVLANの設定

Private VLAN Configuration (プライベートVLAN設定)画面では、プライマリVLAN、コミュニティVLANおよび隔離VLANの作成および削除が行えます。

コマンド解説:

・VLAN ID

設定されているVLANのIDです(範囲:1～4094)。

・Type (種別)

プライベートVLANには以下の3種類が存在します。

- Primary VLANs (プライマリVLAN)
  無差別ポート間のトラフィックならびに、セカンダリ(ないしコミュニティ)VLAN内でのコミュニティポート間の通信を担います。
- Community VLANs(コミュニティVLAN)
  コミュニティポート間のトラフィックならびに、関連付けられているプライマリVLAN内の無差別ポートとの通信を担います。
- Isolated VLANs(隔離VLAN)
  VLANの隔離ポートと無差別ポートとの間でのみ通信を行います。VLAN内の隔離ポート同士のトラフィックは遮断されます。

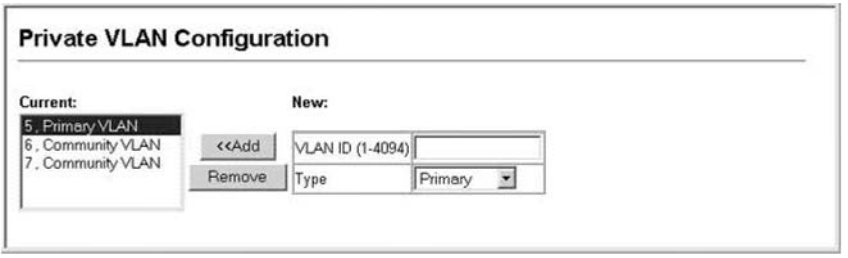
・Current (現在の設定)

現時点で設定されているVLANの一覧を表示します。

WEB:

VLAN→Private VLAN(プライベートVLAN)→Configuration(設定)と選択します。

VLAN IDを入力し、Primary(プライマリ)、Isolated(隔離)ないしCommunity(コミュニティ)のいずれかの種別を選択してAdd(追加)をクリックしてください。本製品からプライベートVLANを削除する場合は、Current (現在の設定)リストボックス内のエントリを選択し反転表示させた状態でRemove (削除)をクリックしてください。なおVLANを削除する場合は、そのメンバーポートすべてをあらかじめ削除しておく必要がありますのでご注意ください。



CLI:

以下の例ではVLAN 5をプライマリVLANとして設定しているほか、VLAN 6をコミュニティVLANに、またVLAN 7を隔離VLANとして設定しています。

```
Console(config)#vlan database                                    4-149
Console(config-vlan)#private-vlan 5 primary                      4-159
Console(config-vlan)#private-vlan 6 community
Console(config-vlan)#private-vlan 7 isolated
Console(config-vlan)#
```

### 3-18-2-3 VLANの関連付け

コミュニティVLANはいずれも、プライマリVLANと関連付ける必要があります。

コマンド解説：

- Primary VLAN ID(プライマリVLAN ID)
  プライマリVLANのIDです（範囲：1～4094）。
- Association(関連付け)
  選択されているプライマリVLANに関連付けられているコミュニティVLANです。
- Non-Association（関連なし）
  選択されているVLANと関連付けられていないコミュニティVLANです。

WEB：

VLAN→Private VLAN(プライベートVLAN)→Association（関連付け)と選択します。

スクロールダウンボックスから該当するプライマリVLANを選び、Non-Association(関連なし)リストボックス内でコミュニティVLANを1つ以上選択してください。この状態でAdd(追加)をクリックし、これらのエントリを選択されているプライマリVLANと関連付けてください。（なお、各コミュニティVLANとも、関連付けが行えるプライマリVLANは1つのみとなります。）


CLI：

以下の例では、コミュニティVLAN6および7をプライマリVLAN 5に関連付けています。

```
Console(config)#vlan database                                    4-149
Console(config-vlan)#private-vlan 5 association 6                4-160
Console(config-vlan)#private-vlan 5 association 7                4-160
Console(config)#
```

### 3-18-2-4 プライベートVLANインタフェース情報の表示

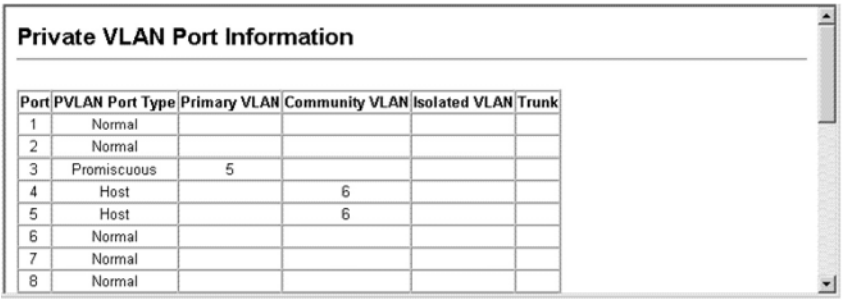
Private VLAN Port Information(プライベートVLANポート情報)およびPrivate VLAN Trunk Information(プライベートVLANトランク情報)メニューを使用することにより、プライベートVLANと関連付けられているインタフェースを表示させることが可能です。

コマンド解説：

- Port/Trunk (ポート/トランク)
  本製品上のインタフェースです。
- PVLAN Port Type (プライベートVLANポート種別)
  プライベートVLANのポートの種類を示します。
  - Normal(通常)
    ポートはいずれのプライベートVLAN内にも含まれていません(設定されていません)。
  - Host (ホスト)
    ポートはコミュニティポートとなっているため、自身のコミュニティVLANの中にある他のポートおよび指定無差別(promiscuous)ポートとのみ通信が行えます。もしくは、ポートは隔離ポートとなっているため自身の隔離VLAN内にある単一の無差別ポートとのみ通信が行えます。
  - Promiscuous(無差別)
    無差別ポートは、プライベートLVAN内のすべてのインタフェースと通信が行えます。
- Primary VLAN(プライマリVLAN)
  無差別ポート間のトラフィックならびに、関連付けられているセカンダリVLAN内部のコミュニティポートと無差別ポートとの間のトラフィックを通します。
- Community VLAN (コミュニティVLAN)
  コミュニティポート間のトラフィックならびに、コミュニティポートから同ポートの指定無差別ポートまでのトラフィックを通します。
- Isolated VLAN(隔離VLAN)
  VLANの隔離ポートと無差別ポートとの間のトラフィックのみ通します。VLAN内の、隔離ポート間のトラフィックは遮断されます。
- Trunk (トランク)
  トランクIDです(Port Information(ポート情報)のみ)

WEB：

VLAN→Private VLAN(プライベートVLAN)→Port Information(ポート情報)ないしTrunk Information (トランク情報)と選択します。



**Private VLAN Port Information**

| Port | PVLAN Port Type | Primary VLAN | Community VLAN | Isolated VLAN | Trunk |
|---|---|---|---|---|---|
| 1 | Normal | | | | |
| 2 | Normal | | | | |
| 3 | Promiscuous | 5 | | | |
| 4 | Host | | 6 | | |
| 5 | Host | | 6 | | |
| 6 | Normal | | | | |
| 7 | Normal | | | | |
| 8 | Normal | | | | |

CLI：

以下の例では、本製品にプライマリVLAN 5ならびにコミュニティVLAN 6を設定しています。ポート3は無差別ポートとして設定されVLAN 5にマッピングされているほか、ポート4および5はホストポートとして設定されVLAN 6と関連付けられています。この結果、ポート4および5宛てのトラフィックはポート3のみ通過するかたちになります。

```
Console#show vlan private-vlan                                    4-163
Primary   Secondary       Type        Interfaces
--------  -----------  ----------  ------------------------------
     5                 primary     Eth1/ 3
     5          6      community   Eth1/ 4 Eth1/ 5
Console#
```

### 3-18-2-5 プライベートVLANインタフェースの設定

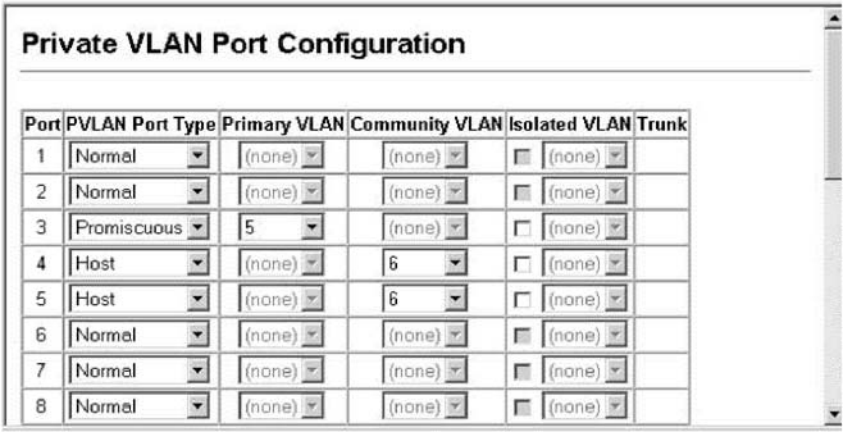
Private VLAN Port Configuration(プライベートVLANポート設定)メニューおよびPrivate VLAN Trunk Configuration(プライベートVLANトランク設定)メニューでは、プライベートVLANインタフェースの種類を設定しインタフェースをプライベートに割り当てることが可能です。

コマンド解説：

- Port/Trunk (ポート/トランク)
  本製品上のインタフェースです。
- PVLAN Port Type (プライベートVLANポート種別)
  プライベートVLANのポートの種類を示します。
  - Normal(通常)
    ポートはプライベートVLANに割り当てられていません。
  - Host (ホスト)
    ポートはコミュニティポートか隔離ポートとなっています。コミュニティポートは、自身のコミュニティVLANの中にある他のポートおよび指定無差別(promiscuous)ポートと通信が行えます。隔離ポートは自身の隔離VLAN内にある単一の指定無差別ポートとのみ通信が行えます(他のホストポートとは通信できません)。
  - Promiscuous(無差別)
    無差別ポートは、プライベートLVAN内のすべてのインタフェースと通信が行えます。
- Primary VLAN(プライマリVLAN)
  無差別ポート間のトラフィックならびに、関連付けられているセカンダリVLAN内部のコミュニティポートと無差別ポートとの間のトラフィックを通します。PVLAN種別がPromiscuous(無差別)となっている場合は、関連付けられているプライマリVLANを指定してください。
- Community VLAN (コミュニティVLAN)
  コミュニティポート間のトラフィックならびに、コミュニティポートから同ポートの指定無差別ポートまでのトラフィックを通します。PVLAN Port Type (PVLANポート種別)をHost(ホスト)に設定し、関連付けられているコミュニティVLANを指定してください。
- Isolated VLAN(隔離VLAN)
  VLANの隔離ポートと無差別ポートとの間のトラフィックのみ通します。VLAN内の、隔離ポート間のトラフィックは遮断されます。PVLAN Port Type (PVLANポート種別)をHost(ホスト)に設定し、Isolated VLAN(隔離VLAN)にチェックマークを入れて隔離VLANを指定してください。最後に、該当するVLANをドロップダウンボックスから選んでください。

WEB：

VLAN→Private VLAN(プライベートVLAN)→Port Configuration(ポート設定)またはTrunk Configuration(トランク設定)と選択します。プライベートVLANに参加させる各ポートにつきそのPVLAN Port Type(PVLANポート種別)を設定してください。プライマリVLANないし隔離VLANには、無差別(promiscuous)ポートを割り当ててください。またコミュニティVLANないし隔離VLANにはホストポートを割り当ててください。ポートの設定が完了した時点でApply(適用)をクリックしてください。




CLI：

以下の例では、本製品にプライマリVLAN 5およびセカンダリVLAN 6が設定されていることを表しています。ポート3は無差別ポートとし設定されVLAN 5にマッピングされているほか、ポート4および5はホストポートとして設定されVLAN 6に関連付けられています。このため、ポート4および5宛てのトラフィックはポート3のみ通過可能となります。

```
Console(config)#interface ethernet 1/3
Console(config-if)#switchport mode private-vlan promiscuous          4-161
Console(config-if)#switchport private-vlan mapping 5                 4-163
Console(config-if)#exit
Console(config)#interface ethernet 1/4
Console(config-if)#switchport mode private-vlan host                 4-161
Console(config-if)#switchport private-vlan host-association 6        4-161
Console(config-if)#exit
Console(config)#interface ethernet 1/5
Console(config-if)#switchport mode private-vlan host
Console(config-if)#switchport private-vlan host-association 6
Console(config-if)#
```

# 3-19 CoS設定

CoS(クラス・オブ・サービス)を使用することにより、通信が混雑し本製品内でトラフィックがバッファ(格納)された際に、どのデータパケットを優先的に扱うかを指定することが可能となります。

本製品では各ポートとも、4本の優先度キューを使用するCoSをサポートしています。ポートの高優先度キュー内のデータパケットは、より優先度の低いキュー内にあるデータパケットより先に送信されるかたちになります。各インタフェース上で初期(デフォルト)優先度を設定し、さらに本製品の優先度キューに対するフレーム優先度タグのマッピング(関連付け)も変更することが可能となっています。

## 3-19-1 レイヤ2キュー設定

### 3-19-1-1 インタフェースの初期優先度を設定する

本製品上の各インタフェースの初期ポート優先度を指定することが可能です。本製品に到着するすべてのタグ無しパケットは、指定された初期ポート優先度情報を追加した上で(タグを付与した上で)、出力ポートにて適切な優先度キューへと並び替えられるかたちになります。

コマンド利用:

- 本製品は各ポートにて4本の優先度キューを提供します。またウェイトラウンドロビン方式を使用することにより、キュー先頭が混雑(詰まり)状態となるのを防ぎます。
- 初期優先度は、すべての種類のフレームを受け付けるよう設定されているポート(タグ無し、タグ付きの両者を受信)で受信されるタグ無しフレームすべてに対し適用されます。当優先度は、IEEE802.1Q 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IEEE802.1Q VLANタグ付きフレームであった場合は、IEEE802.1p User Priority (ユーザ優先度)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のタグ無しメンバーである場合、これらのフレームは送信前にVLANタグをすべて取り外されるかたちになります。

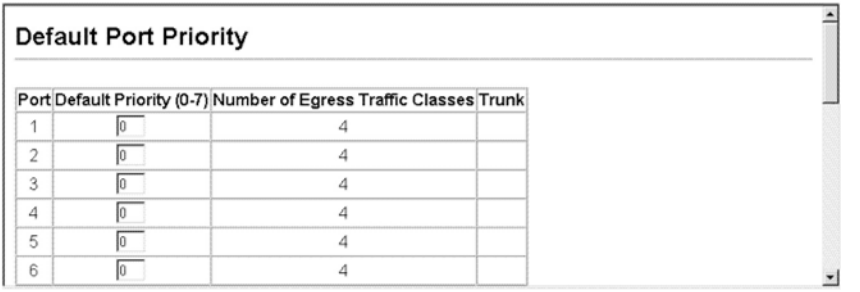
コマンド解説:

- Default Priority (初期優先度)(*1)
  指定インタフェース上で受信されるタグ無しフレームに割り当てられる優先度です。(範囲:0～7、初期設定:0)
- Number of Egress Traffic Classes (送信トラフィッククラスの数)
  各ポート上で提供されているキューバッファの数です。

*1 CLIでは、当情報はPriority for untagged traffic (タグ無しトラフィックの優先度)として表示されます。

WEB：

Priority(優先度)→Default Port Priority (初期ポート優先度)ないしDefault Trunk Priority (初期トランク優先度)と選択します。該当するインタフェースの初期優先度を変更して Apply(適用)をクリックしてください。




CLI：

以下の例では、ポート3に対し初期優先度5を割り当てています。

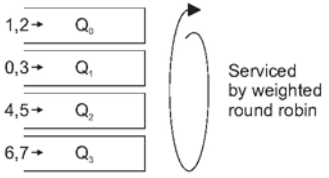
```
Console(config)#interface ethernet 1/3                          4-108
Console(config-if)#switchport priority default 5                4-169
Console(config-if)#end
Console#show interfaces switchport ethernet 1/3                 4-117
Information of Eth 1/3
 Broadcast threshold:           Disabled
 LACP status:                   Disabled
 Ingress rate limit: disable, Level: 30
 Egress rate limit: disable, Level: 30
 VLAN membership mode:          Hybrid
 Ingress rule:                  Enabled
 Acceptable frame type:         Tagged frames only
 Native VLAN:                   1
 Priority for untagged traffic: 5
 GVRP status:                   Disabled
 Allowed VLAN:                  1(u),
 Forbidden VLAN:
 Private-VLAN mode:             NONE
 Private-VLAN host-association: NONE
 Private-VLAN mapping:          NONE
Console#
```

## 3-19-1-2 CoS値をEgress(送信)キューに割り当てる

本製品は、各ポート上にて4本の優先度キューを使用することによりCoS優先度のタギングされているトラフィックを処理します。サービススケジュールは、ストリクトおよびウェイトラウンドロビン(Weighted Round Robin = WRR)に基づいています。IEEE802.1pでは、最大8個までの個別のトラフィック優先度を定義することが可能です。初期優先度レベルは、以下の表が示すようにIEEE802.1p標準の推奨内容に従って割り当てられています。

表3-10 CoS値の送信キューへのマッピング

| キュー | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 優先度 | 1,2 | 0,3 | 4,5 | 6,7 |




Serviced by…:ウェイトラウンドロビンに基づきサービスを実行

以下の表は、様々なネットワークアプリケーション用としてIEEE802.1p標準が推奨している優先度レベルを示しています。ただし優先度レベルは、ご使用ネットワーク上のアプリケーショントラフィックにとり最適となるよう、お客様の希望に合わせて本製品の出力キューへとマッピング(割り当て)できるようになっています。

表3-11 CoS優先度レベル

| 優先度レベル | トラフィック種別 |
|---|---|
| 1 | バックグラウンド |
| 2 | (予備) |
| 0 (初期設定) | ベストエフォート |
| 3 | エクセレントエフォート(最上エフォート) |
| 4 | 制限負荷 |
| 5 | 動画:レイテンシ、ジッターともに100ミリ秒以下 |
| 6 | 音声:レイテンシ、ジッターともに10ミリ秒以下 |
| 7 | ネットワーク制御 |

コマンド解説：

- Priority（優先度）
  CoS値（範囲：0～7、7が最も高い優先度となります）
- Traffic Class (*1)（トラフィッククラス）
  出力キューバッファ（範囲：0～3、3が最も高いCoS優先度キューとなります）
  *1 CLIではQueue ID(キューID)が表示されます。

WEB：

Priority（優先度）→Traffic Classes（トラフィッククラス）と選択します。

現時点での、CoS値の出力キューへの割当状況が表示されます。トラフィッククラス（例：出力キューなど）に対し優先度を割り当て、Apply(適用)をクリックしてください。


CLI：

以下の例では、CoS割当を1対1マッピングに変更する方法を示しています。

```
Console(config)#interface ethernet 1/1                          4-108
Console(config-if)#queue cos-map 0 0                            4-171
Console(config-if)#queue cos-map 1 1
Console(config-if)#queue cos-map 2 2
Console(config-if)#end
Console#show queue cos-map ethernet 1/1                         4-173
Information of Eth 1/1
 CoS Value     : 0 1 2 3 4 5 6 7
 Priority Queue: 0 1 2 1 2 2 3 3
Console#
```

＊ 特定の値のCoS優先度への割り当てはインタフェース設定コマンドにて行っていますが、変更内容は本製品上のすべてのインタフェースに対して適用されます。

### 3-19-1-3 キューモードの選択

本製品のキューの処理方法には、

1）優先度のより高いキュー上のトラフィックはすべて、より優先度の低いキュー上のものより必ず先に処理を行う、厳密なルールに基づいて行う方法

2）各キューの相対的なウェイト（比重）を指定するWRR(ウェイトラウンドロビン)キュー方式

の2種類があります。WRRは各キュー上において、あらかじめ定義されている相対ウェイトを使用します。同ウェイトは、本製品が次のキューに移行する前にキュー上で実行するサービスの時間のパーセント比率を決定します。この処理を行うことにより、厳密な優先度に基づくキュー方式で発生するヘッドオブライン（ライン先頭）遮断の問題を回避することが可能となります。

コマンド解説：

- WRR：ウェイトラウンドロビン方式では、すべての送信ポートにてキュー0～3にウェイト1、2、4、6をこの順番で設定することで帯域幅を共有します。（これが初期選択設定となります。）
- Strict（厳密方式）：送信キューを順番に実行します。より高い優先度キュー内のトラフィックはすべて、より優先度の低いキュー内のそれより前の時点で送信します。

WEB：

Priority（優先度）→Queue Mode（キューモード）と選択します。

Strict(厳密方式)かWRRのいずれかを選択してApply（適用）をクリックしてください。


CLI：

以下の例では、キューモードをStrict（厳密）優先サービスモードに設定しています。

```
Console(config)#queue mode wrr                                    4-169
Console(config)#exit
Console#show queue mode                                           4-172
Queue mode: wrr
Console#
```

### 3-19-1-4 トラフィッククラスにサービスウェイトを設定する

本製品はWRR(ウェイトラウンドロビン)アルゴリズムを使用することにより各優先度キューの処理を行う頻度を決定します。P.210の「CoS値を送信キューに割り当てる」にて解説されているように、トラフィッククラスは、各ポートに提供されている4本の送信キューのうちいずれか1本に割り当てられる（マッピングされる）ようになっています。これらのキュー一つ一つ

(ならびに対応するトラフィック優先度に)ウェイトを割り当てることが可能です。同ウェイトは、各キューを処理する際に行うポーリングの頻度を設定するほか、特定の優先度値を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(レスポンス)にも影響を与えます。

コマンド解説:

- WRR Setting Table (*1) (WRR設定テーブル)

  各トラフィッククラス(キュー)用のウェイトの一覧を表示します。

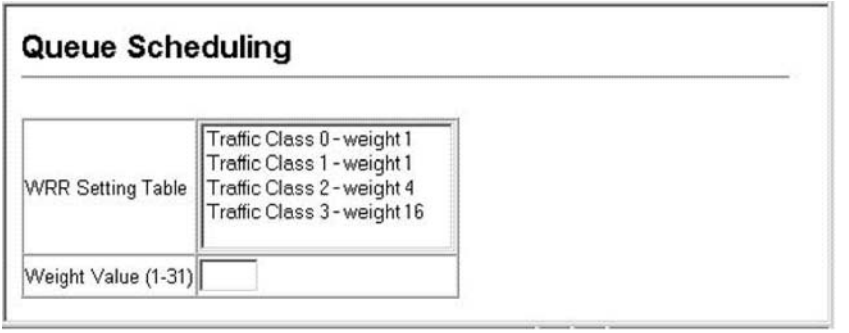
- Weight Value (ウェイト値)

  選択されているトラフィッククラスに対し新規にウェイトを設定します。ただし、キュー0のウェイトは1で固定されており変更することはできませんのでご注意ください。(範囲:1～31)

  *1 CLIではQueue ID(キューID)が表示されます。

WEB:

Priority (優先度)→Queue Scheduling(キュースケジュール)と選択します。トラフィッククラス(例:出力キューなど)を反転表示させ、ウェイトを入力した上でApply(適用)をクリックしてください。




CLI:

以下の例は、WRRウェイトを各優先度キューに割り当てる方法を示しています。

```
Console(config)#queue bandwidth 6 9 12                          4-170
Console(config)#exit
Console#show queue bandwidth                                    4-172
Queue ID  Weight
 --------  ------
    0         1
    1         6
    2         9
    3         12
Console
```

## 3-19-2 レイヤ3/4優先度設定

### 3-19-2-1 レイヤ3/4優先度をCoS値に割り当てる

本製品は、レイヤ3/4トラフィックの優先順位付けを行うための一般的な方式を複数サポートしており、これらの方式を使用することによりアプリケーションの要求を満たすことが可能となります。トラフィックの優先度は、フレームのIPヘッダ内にて、ToS(サービスの種別)オクテット内の優先度ビットもしくはTCPポートの番号を使って指定することが可能です。優先度ビットを使用した場合、ToSオクテットはIP優先度(precedence)用の3ビットか、DSCP(分化サービスコードポイント)サービス用の6ビットを備えます。これらのサービスが有効となっている場合、本製品は優先度をCoS値に割り当て、その後トラフィックは対応する出力キューに送信されるかたちになります。

トラフィック内には異なる優先度情報が含まれている可能性があるため、本製品は優先度値を以下の方法にて出力キューに割り当てます。

- 優先度割り当て(マッピング)の優先度は、IP Port Priority(IPポート優先度)、IP Precedence (IP優先度)ないしDSCP Priority (DSCP優先度)、Default Port Priority (初期ポート優先度)の順となります。
- IP Precedence (IP優先度)およびDSCP Priority (DSCP優先度)は、同時に有効に設定できないようになっています。いずれか一方を有効にした時点で、他方が自動的に無効に設定されます。

### 3-19-2-2 IP優先度/DSCP優先度の選択

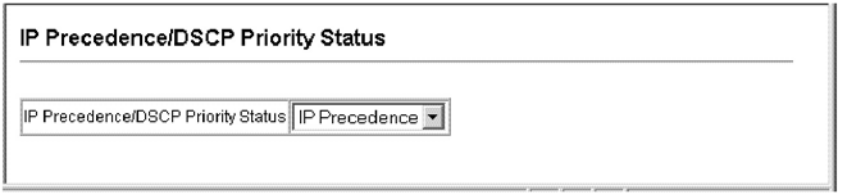
本製品では、IP Precedence(IP優先度)とDSCP Priority(DSCP優先度)のうちどちらを使用するか選択できるようになっています。いずれか一方を選択するか、当機能を無効に設定してください。

コマンド解説:

- Disabled (無効設定済)
  どちらの優先度サービスも無効とします。(初期設定)
- IP Precedence (IP優先度)
  IP優先度を使用し、レイヤ3/4優先度のマッピングを行います。
- IP DSCP
  DSCPを使ってレイヤ3/4優先度のマッピングを行います。

WEB：

Priority（優先度）→ IP Precedence/DSCP Priority Status（IP優先度/DSCP優先度ステータス）と選択します。スクロールダウンメニュー上でDisabled（無効化済）、IP Precedence（IP優先度）およびIP DSCPのいずれかを選択してApply（適用）をクリックしてください。




CLI：

以下の例では、本製品上でIP優先度サービスを有効に設定しています。

```
Console(config)#map ip precedence                                    4-174
Console(config)#
```

### 3-19-2-3 IP優先度のマッピング

IPv4ヘッダ内のToS(サービス種別)オクテットには3つの優先度ビットが含まれています。

同ビットを使用することにより、ネットワーク制御パケット用の最も高い優先度から、定期的にやりとりするトラフィック用の最も低い優先度までを含めた8種類の異なる優先度レベルを決定することが可能となります。初期設定では、IP優先度値はCoS値と一対一の関係となるよう設定されています(例:優先度値0はCoS値0にマッピングし他も同様に、など)。ビット6および7はネットワーク制御の目的で使用されており、他のビットは様々なアプリケーションの種別用となっています。以下にToSビットの定義内容を示します。

表3-12　IP優先度のマッピング内容

| 優先度レベル | トラフィック種別 | 優先度レベル | トラフィック種別 |
|---|---|---|---|
| 7 | ネットワーク制御 | 3 | フラッシュ |
| 6 | ネットワーク間制御 | 2 | 中間 |
| 5 | 重要 | 1 | 優先度 |
| 4 | フラッシュ上書き | 0 | ルーチン(通常) |

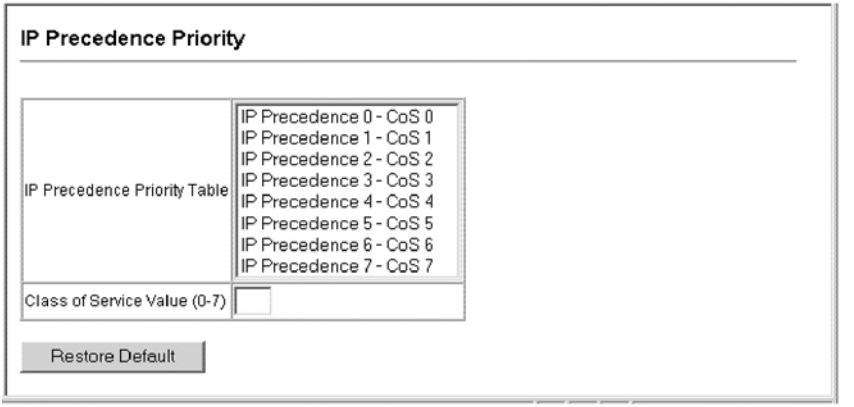
コマンド解説:

- IP Precedence Priority Table (IP優先度設定テーブル)
  IP優先度のCoS値への割当内容(表)を示します。
- Class of Service Value (CoS値)
  選択されているIP優先度値に対し、CoS値を割り当てます。なお、0が最も低い優先度となり7が最も高い優先度を示します。

WEB：

Priority (優先度)→Ip Precedence Priority (IP優先度設定)と選択します。

IP Precedence Priority Table (IP優先度設定テーブル)からエントリを選択し、Class of Service Value (CoS値)フィールドに値を入力してください。最後にApply (適用)をクリックしてください。




CLI：

以下の例では、IP Precedence (IP優先度)サービスを本製品全体で有効とし、IP優先度値1をCoS値0(ポート1上)に割り当てた上でIP優先度設定を表示しています。

```
Console(config)#map ip precedence                                    4-174
Console(config)#interface ethernet 1/1                               4-108
Console(config-if)#map ip precedence 1 cos 0                         4-176
Console(config-if)#end
Console#show map ip precedence ethernet 1/1                          4-179
Precedence mapping status: enabled

 Port      Precedence COS
 --------- ---------- ---
  Eth 1/ 1          0   0
  Eth 1/ 1          1   0
  Eth 1/ 1          2   2
  Eth 1/ 1          3   3
  Eth 1/ 1          4   4
  Eth 1/ 1          5   5
  Eth 1/ 1          6   6
  Eth 1/ 1          7   7
Console#
```

＊ 特定の値のIP優先度への割当はインタフェース設定コマンドにて実行しますが、変更は本製品上のすべてのインタフェースに対し適用されます。

### 3-19-2-4 DSCP優先度の割当

DSCPは6ビット幅となっているため、最大64種の異なる転送動作のコーディングが可能です。DSCPはToSビットを置き換えますが、優先度(precedence)3ビットとも下位互換性があるためToS対応機器がDSCPマッピングで問題となることはありません。ネットワークポリシーに基づき、異なる種類のトラフィックに対し異なる種類での転送を印し付ける(設定する)ことが可能です。以下の表はDSCP初期値を示しています。なお、指定のないDSCP値はすべてCoS値0にマッピングされています。

表3-13 DSCP優先度値の割当内容

| 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 |

コマンド解説:

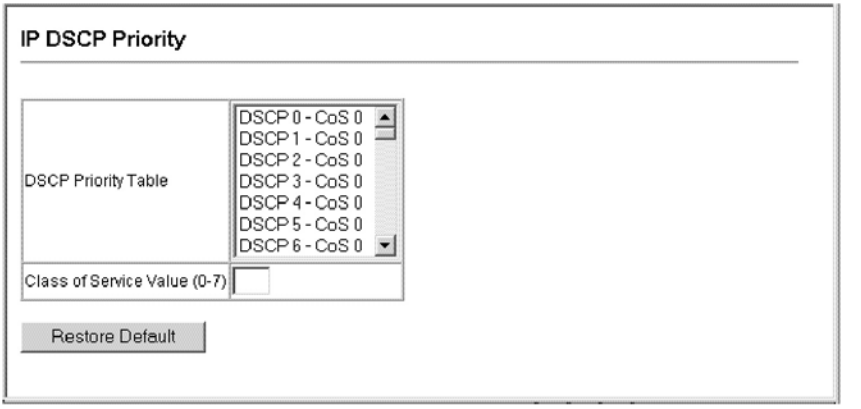
- DSCP Priority Table (DSCP優先度テーブル)
  DSCP優先度のCoS値への割当(マッピング)内容を表示します。
- Class of Service Value (CoS値)
  CoS値を選択されているDSCP優先度値へとマッピング(割当)します。なお0は優先度が低く、7は優先度が高いことを示します。

**注意**: IP DSCP設定はすべてのインタフェースに対し適用されます。

WEB:

Priority (優先度)→DSCP Priority (DSCP優先度)と選択します。

DSCPテーブル上でエントリを選択し、Class of Service Value (CoS値)フィールド内に値を入力してApply (適用)をクリックしてください1




CLI:

以下の例では、本製品全体でDSCP優先度サービスを有効に設定し、DSCP値0をCoS値1(ポート1上)に割り当てた上でDSCP優先度設定を表示しています。

```
Console(config)#map ip dscp                                    4-177
Console(config)#interface ethernet 1/1                         4-108
Console(config-if)#map ip dscp 1 cos 0                         4-177
Console(config-if)#end
Console#show map ip dscp ethernet 1/1                          4-180
DSCP mapping status: disabled

 Port      DSCP COS
 --------- ---- ---
  Eth 1/ 1    0   0
  Eth 1/ 1    1   0
  Eth 1/ 1    2   0
  Eth 1/ 1    3   0
:
  Eth 1/ 1   61   0
  Eth 1/ 1   62   0
  Eth 1/ 1   63   0
Console#
```

*特定の IP DSCP値の割当はインタフェース設定コマンドを使って行いますが、変更内容は本製品上のインタフェースすべてに対し適用されます。

### 3-18-2-5 IPポート優先度の割当

フレームヘッダ内のIPポート番号(TCP/UDPポート番号など)に基づき、ネットワークアプリケーションをCoS値に割り当てる(マッピングする)ことも可能です。一般的によく利用されているTCPサービスポートには、HTTP:80、FTP:21、Telnet:23およびPOP3:110などがあります。

コマンド解説:

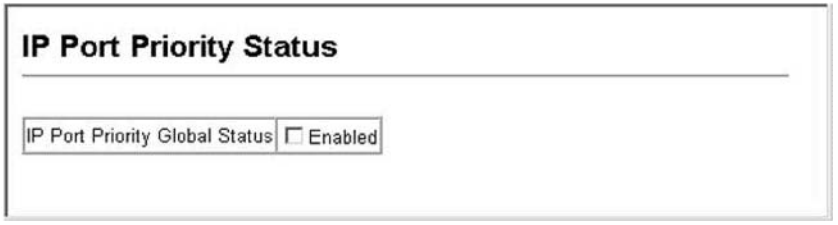
- IP Port Priority Status (IPポート優先度ステータス)
  IPポート優先度の有効/無効を決定します。
- IP Port Priority Table (IPポート優先度テーブル)
  IPポートのCoS値への割当内容を表示します。
- IP Port Number (TCP/UDP)(IPポート番号(TCP/UDP)
  新規にIPポート番号を設定します。
- Class of Service Value (CoS値)
  CoS値を新規IPポートに設定します。なお0は低優先度、7は高優先度を示します。

**注意**: IP Port Priority (IPポート優先度)設定は全インタフェースに対し適用されます。

WEB:

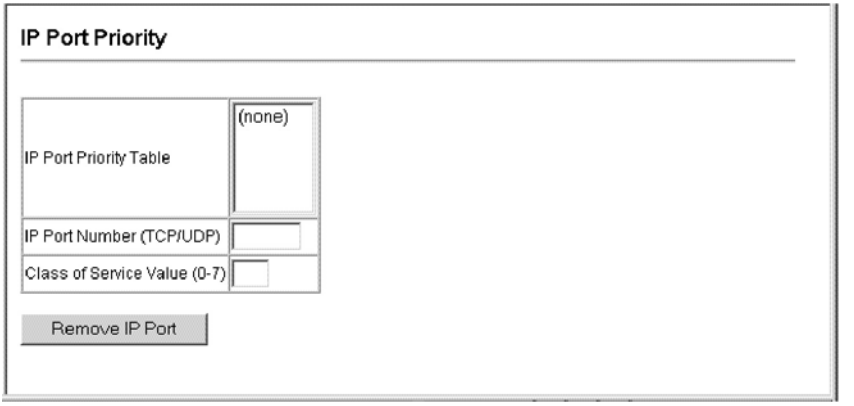
Priority (優先度)→IP Port Priority Status(IPポート優先度ステータス)と選択します。

IPポート優先度ステータスを有効(Enabled)に設定してください。



Priority (優先度)→IP Port Priority (IPポート優先度)と選択します。

IP Port Number (IPポート番号)ボックス内でネットワークアプリケーション用のポート番号を入力し、続いてClass of Service (CoS)ボックス内で新規CoS値を入力してください。最後にApply(適用)をクリックしてください。




CLI:

以下の例では、本製品全体でIP Port Priority (IPポート優先度)を有効にし、ポート5上のHTTPトラフィックをCoS値0に割り当てた上で、同ポート上のすべてのIPポート優先度設定を表示しています。

```
Console(config)#map ip port                                    4-174
Console(config)#interface ethernet 1/5
Console(config-if)#map ip port 80 cos 0                        4-175
Console(config-if)#end
Console#show map ip port ethernet 1/5                          4-175
TCP port mapping status: disabled

 Port      Port no. COS
 --------- -------- ---
  Eth 1/ 5       80   0
Console#
```

＊IP Port Priority(IPポート優先度)への特定値の割り当てはインタフェース設定コマンドにて実行しますが、変更は本製品上のすべてのインタフェースに対し適用されます。

## 3-18-2-6 CoS値のACLへの割当

ACL CoS Mapping(ACL CoS割当)ページにて、出力キューを以下に示すACLルールと合致するパケットに設定することが可能です。なお指定されたCoS値は、合致するパケットを出力キューに割り当てる(マッピングする)目的でのみ使用されます。パケット自体に書き込まれるわけではありませんのでご注意ください。CoS値の出力キューへの割り当てに関する情報についてはp.210をご覧ください。

表3-14 送信キュー優先度割当

| キュー | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 優先度 | 1,2 | 0,3 | 4,5 | 6,7 |

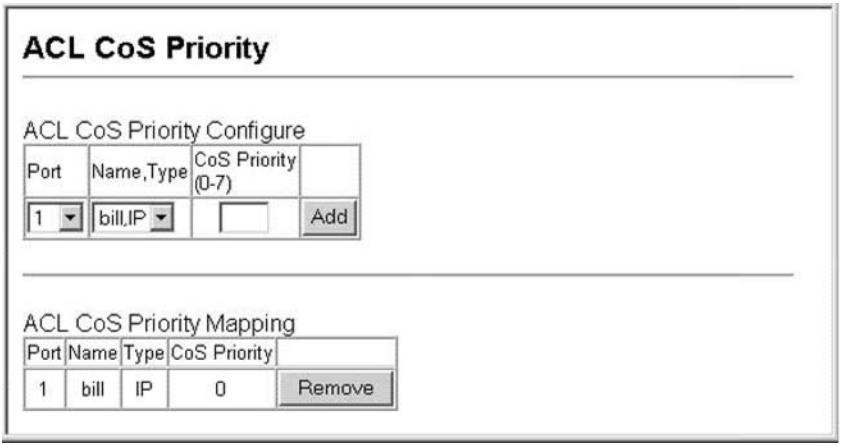
コマンド解説:

- Port (ポート)
  ポートIDです。
- Name (名称)(*1)
  ACL名です。
- Type (種別)
  ACLの種類(IPまたはMAC)です。
- CoS Priority (CoS値)
  IP ACLルールに合致するパケットに使用されるCoS値です(範囲:0～7)。
- ACL CoS Priority Mapping (ACL CoS優先度割当)
  設定されている情報を表示します。

WEB：

Priority（優先度）→ACL CoS Priority（ACL CoS優先度）と選択します。

いずれかのポート上で割当（マッピング）を有効にし、スクロールダウンリストからACLを選択してAdd（追加）をクリックしてください。




CLI：

以下の例では、ポート24上の指定ACL内パケットの内ルールに合致するものに対しCoS値0(ゼロ)を割り当てています。

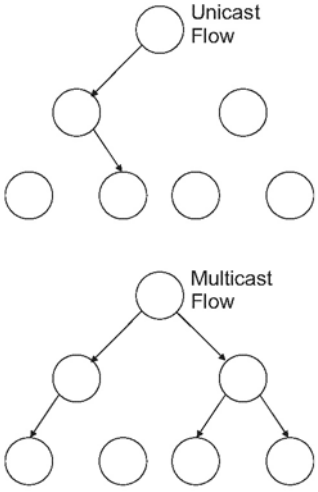
```
Console(config)#interface ethernet 1/24                    4-108
Console(config-if)#map access-list ip bill cos 0           4-95
Console(config-if)#
```

＊1　ACLの設定に関する情報についてはp.105をご覧ください。

# 3-20 マルチキャストフィルタリング

マルチキャストは、テレビ会議や音声ストリーミングといったリアルタイム性が重視されるアプリケーションを使用する際に用いられます。マルチキャストサーバは、各クライアントとそれぞれ個別に接続を行う必要はありません。代わりに同サーバはサービス内容をそのままネットワークにブロードキャスト送信し、同マルチキャスト内容の受信が必要となるホスト側がローカルマルチキャストスイッチないしルータに対し登録を行うかたちになります。この方式ではマルチキャストサーバ側で要求されるオーバーヘッド(間接コスト)が軽減されますが、ブロードキャストトラフィックが通過する各マルチキャストスイッチ/ルータでは、同トラフィックを慎重に取り扱い、同サービスを申し込んだホストにのみ確実に同トラフィックが届くようにしなければなりません。

本製品はIGMP(インターネットグループ管理プロトコル)を使用し、特定のマルチキャストサービスの受信を希望する接続済みホストすべてに対しクエリ(問い合わせ)を実行します。本製品はサービスへの参加を要求しているホストを含むポートを識別し、同ポートに対してのみデータを送信します。本製品は次に、隣接しているすべてのマルチキャストスイッチないしルータに対し同サービス要求を拡大送信し、マルチキャストサービスを継続して受信できるようにします。この一連の流れをマルチキャストフィルタリングと呼びます。




Unicast Flow ：ユニキャストでのデータの流れ

Multicast Flow：マルチキャストでのデータの流れ

IPマルチキャストフィルタリングを利用する目的は、スイッチ接続されているネットワークの性能を最適化することにあります。本製品はマルチキャストパケットをサブネット(VLAN)内

のポートすべてにフラッド送信される代わりに、マルチキャストグループホストないしマルチキャストルータ/スイッチを含むポートにのみ同トラフィックを転送します。

## 3-20-1 レイヤ2IGMP (スヌーピングおよびクエリ)

■IGMP Snooping and Query(IGMPスヌーピングおよりクエリ)

マルチキャストルーティングがご使用ネットワーク内の太のスイッチでサポートされていない場合は、IGMP Snooping and Query (IGMPスヌーピングおよびクエリ)を使用することにより、1)マルチキャストクライアントとサーバとの間で交わされるIGMPサービス要求を監視しまた2)マルチキャストトラフィックを転送する必要がある本製品上のスイッチポートを自動的(動的)に設定することが可能となります。

■Static IGMP Router Interface (固定IGMPルータインタフェース)

IGMPスヌーピングがIGMPクエリア(クエリ発行者)を見つけられない場合は、ネットワーク経由で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/スイッチなど)を本製品上のインタフェースに対して手動で指定することが可能です(p.230)。同インタフェースは次に、接続されているすべてのルータ/スイッチ上で対応している現時点でのマルチキャストグループすべてに参加し、同マルチキャストトラフィックを必要とする本製品内部のインタフェースすべてにトラフィックが届くようにします。

■Static IGMP Host Interface (固定IGMPホストインタフェース)

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をご利用の場合は、マルチキャストサービスを本製品上の特定のインタフェースに手動で割り当てることが可能です(p.233)。

### 3-20-1-1 IGMPスヌーピングおよびクエリパラメータの設定

マルチキャストトラフィックを、インテリジェントに(無駄なく)転送するよう、本製品を設定することが可能です。IGMPクエリおよび報告メッセージに基づき、本製品は、マルチキャストトラフィックを要求したポートにのみトラフィックを転送します。この結果、本製品からすべてのポートに対しトラフィックをブロードキャスト送信しネットワーク上の通信性能を低下させてしまう、といった事態を回避することが可能となります。

コマンド利用:

- IGMPスヌーピング

  本製品は、IPマルチキャストルータ/スイッチとIPマルチキャストホストグループとの間で送信されるIGMPクエリおよび報告(Report)パケットを受動的に監視することにより、IPマルチキャストグループメンバーを識別します。

  本製品は自身を通過するIGMPパケットを監視し、グループ登録情報を読み取り、これに見合うようマルチキャストフィルタを適切に設定します。
- IGMP Querier (IGMPクエリア)

  ルータおよびマルチキャスト対応スイッチは、各ホストに対し、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確認することが可能です。IPマルチキャストを実行するLAN上にルータないしスイッチが複数存在する場合は、これらの機器のうち一台が「クエリア」として選ばれます。

クエリアは、グループメンバーについてLANに対しクエリを実行する役目を持ちます。クエリアは次に、より上流に存在する各マルチキャストスイッチ/ルータに対しサービス要求を送信し、同機器が継続してマルチキャストサービスを受けられるようにします。

**注意**: マルチキャストルータは、当情報ならびにDVMRPやPIMといったマルチキャストルーティングプロトコルを使用することで、インターネット経由でのIPマルチキャスト通信に対応します。

コマンド解説:

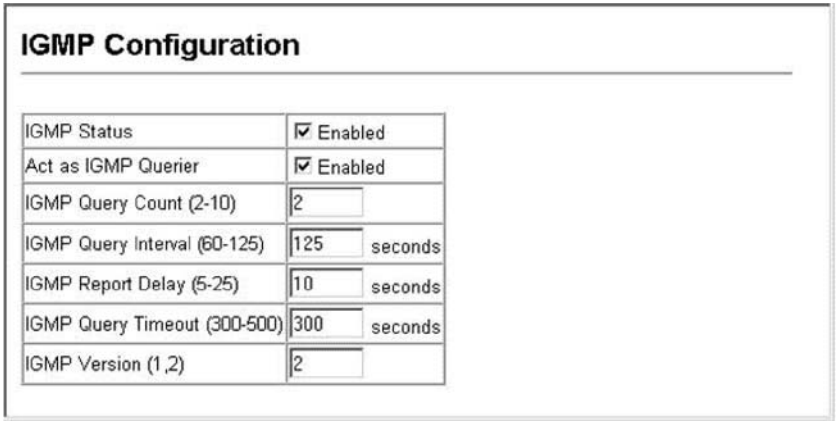
- IGMP Status (IGMPステータス)
  有効となっている場合、本製品はネットワークトラフィックを監視し、どのホストがマルチやストトラフィックの受信を希望しているのかを確認します。IGMP Snooping(IGMPスヌーピング)とも呼ばれています。(初期設定:Enabled (有効))
- Act as IGMP Querier (IGMPクエリアとして動作)
  有効となっている場合、本製品はクエリアとして動作します。クエリアは、ホストに対しマルチキャストトラフィックの受信を希望するかどうかを問い合わせる役目を持ちます。(初期設定:Enabled(有効))
- IGMP Query Count (IGMPクエリカウント)
  応答のないクライアントをマルチキャストグループから削除する前に、本製品がクエリを発行する回数を設定します。(範囲:2～10、初期設定:2)
- IGMP Query Interval (IGMPクエリ間隔)
  本製品がIGMPホストークエリメッセージを送信する頻度(時間間隔)を設定します。(範囲:60～125秒、初期設定:125)
- IGMP Report Delay (IGMP報告遅延)
  ポート上のIPマルチキャストアドレス用のIGMP報告(Report)を受信してから本製品が同ポートからIGMPクエリを送信しエントリをリストから削除するまでの時間を設定します。(範囲:5～25秒、初期設定:10)
- IGMP Query Timeout(IGMPクエリタイムアウト)
  前回のクエリアが停止してから本製品がルータポート(クエリパケットを以前受信していたインタフェースなど)を期限切れと見なすまでの時間です。(範囲:300～500秒、初期設定:300)
- IGMP Version (IGMPバージョン)
  ネットワーク上の他機器との互換性を保つため使用するプロトコルのバージョンを設定します。(範囲:1～2、初期設定:2)

**注意**: 1. サブネット上のどのシステムも、同一のバージョンをサポートする必要があります。

2. IGMP Report Delay (IGMP遅延報告)およびIGMP Query Timeout (IGMPクエリタイムアウト)などを含むいくつかの属性は、IGMPv2でのみ有効にすることが可能です。

WEB:

IGMP Snooping (IGMPスヌーピング)→IGMP Configuration (IGMP設定)と選択します。必要に応じてIGMP設定を調整し、Apply (適用)をクリックしてください。(以下に、初期設定の内容を示します。)




CLI:

以下の例では、マルチキャストフィルタリング用として設定を変更したあとで現在の状態を表示しています。

```
Console(config)#ip igmp snooping                                    4-182
Console(config)#ip igmp snooping querier                            4-185
Console(config)#ip igmp snooping query-count 10                     4-185
Console(config)#ip igmp snooping query-interval 100                 4-186
Console(config)#ip igmp snooping query-max-response-time 20         4-187
Console(config)#ip igmp snooping router-port-expire-time 300        4-187
Console(config)#ip igmp snooping version 2                          4-183
Console(config)#exit
Console#show ip igmp snooping                                       4-183
 Service status:           Enabled
 Querier status:           Enabled
 Query count:              10
 Query interval:           100 sec
 Query max response time:  20 sec
 Router port expire time:  300 sec
 IGMP snooping version:    Version 2
Console#
```

### 3-20-1-2 マルチキャストルータに接続されているインタフェースを表示する

本製品上のポートに接続されているマルチキャストルータは、IGMPにより取得した情報ならびにDVMRPやPIMといったマルチキャストルーティングプロトコルを使用することで、インターネット上でのIPマルチキャストを実現しています。これらのルータは本製品により自動的に検出することが可能なほか、本製品上のインタフェースに固定で割り当てられるようにもなっています。

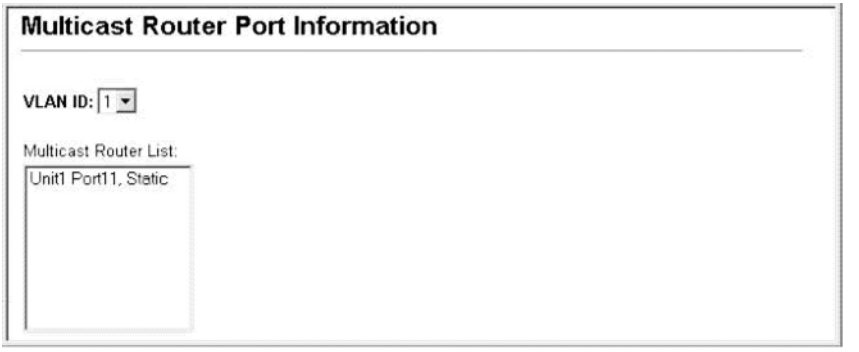
Multicast Router Port Information (マルチキャストルータポート情報)ページは、隣接するマルチキャストルータ/スイッチと接続されている本製品上のポートをVLAN IDごとに表示します。

コマンド解説:

- VLAN ID
  設定されているVLANのIDです(範囲:1～4094)。
- Multicast Router List(マルチキャストルーター一覧)
  本製品により自動的に検出されたマルチキャスタルータならびに、本製品上のインタフェースに固定で割り当てられているマルチキャストルータです。

WEB:

IGMP Snooping (IGMPスヌーピング)→Multicast Router Port Information (マルチキャストルータポート情報)と選択します。スクロールダウンリスト上でVLAN IDを選ぶと、関連付けられているマルチキャストルータの情報が表示されます。



CLI:

以下の例では、マルチキャストルータに接続しているポートとしてポート11を固定で設定しています。

```
Console#show ip igmp snooping mrouter vlan 1                    4-189
 VLAN M'cast Router Port Type
 ---- ------------------ -------
    1           Eth 1/11 Static
Console#
```

### 3-20-1-3 マルチキャストルータ用に固定インタフェースを指定する

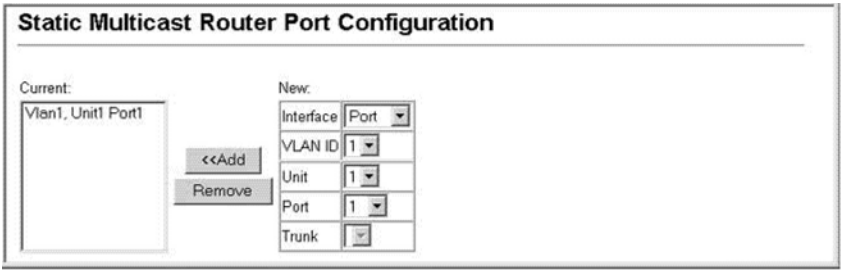
ご使用ネットワーク上の接続にもよりますが、稀にIGMPスヌーピングでIGMPクエリアを見つけられない場合があります。このため、IGMPクエリアがネットワーク経由で本製品上のインタフェース(ポートないしトランク)に接続されている既知のマルチキャストルータ/スイッチである場合は、インタフェース(ならびに指定されているVLAN)を手動で設定し、接続されているルータでサポートされている現時点におけるマルチキャストグループすべてに参加させられるようになっています。この操作を行うことで、本製品内のすべての適切なインタフェースに対しマルチキャストトラフィックを確実に送ることが可能となります。

コマンド解説:

- Interface (インタフェース)
  Port (ポート)ないしTrunk(トランク)スクロールダウンリストを起動します。
- VLAN ID
  接続されているマルチキャストルータから届くマルチキャストトラフィックすべてを広めるためのVLANを選択します。
- Unit (ユニット)
  スタックユニットです(範囲:1～8)。
- Port(ポート)/Trunk (トランク)
  マルチキャストルータに接続されているインタフェースを指定します。

WEB:

IGMP Snooping (IGMPスヌーピング)→Static Multicast Router Port Configuration (固定マルチキャストルータポート設定)と選択します。マルチキャストルータに接続されているインタフェースを指定し、該当するマルチキャストトラフィックを転送するためのVLANを示した(選んだ)上でAdd(追加)をクリックしてください。インタフェースの追加が終わりましたらApply(適用)をクリックしてください。




CLI:

以下の例では、ポート11をVLAN 1内におけるマルチキャストルータポートとして設定しています。

```
Console(config)#ip igmp snooping vlan 1 mrouter ethernet 1/11        4-188
Console(config)#exit
Console#show ip igmp snooping mrouter vlan 1                          4-189
 VLAN M'cast Router Port Type
 ---- ----------------- -------
    1           Eth 1/11  Static
Console#
```

### 3-20-1-4 マルチキャストサービスのポートメンバーを表示する

指定されているVLANおよびマルチキャストサービスに関連付けられているポートメンバーを表示することが可能です。

コマンド解説:

- VLAN ID
  ポートメンバーを表示するVLANを選択します。
- Multicast IP Address (マルチキャストIPアドレス)
  特定のマルチキャストサービス用のIPアドレスです。
- Multicast Group Port List(マルチキャストグループポート一覧)
  選択されているVLANにすでに割り当てられているインタフェースを表示します。同インタフェースは、特定のマルチキャストサービスを広める目的で使用します。

WEB：

IGMP Snooping(IGMPスヌーピング)→IP Multicast Registration Table (IPマルチキャスト登録テーブル)と選択します。VLAN IDおよび、マルチキャストサービス用のIPアドレスをスクロールダウンリストから選んでください。本製品は、同マルチキャストサービスを広めるインタフェースをすべて表示します。


CLI：

以下の例では、VLAN 1上でサポートされている既知のマルチキャストサービスすべてと、該当するサービスを広めているポートを表示しています。Type (種別)フィールドは、エントリが自動的に学習されたのか、もしくは固定で設定されたのかを示します。

```
Console#show bridge 1 multicast vlan 1                              4-184
 VLAN M'cast IP addr. Member ports Type
 ---- --------------- ------------ -------
    1      224.1.1.12      Eth1/12    USER
    1       224.1.2.3      Eth1/12    IGMP
Console#
```

## 3-20-1-5 ポートをマルチキャストサービスに割り当てる

p.226の「IGMPスヌーピングおよびクエリパラメータの設定」の説明にあるように、IGMPスヌーピングおよびIGMPクエリメッセージを使ってマルチキャストフィルタリングを自動的に設定することが可能です。より厳重な制御を必要とするアプリケーションにすいては、本製品上でマルチキャストサービスを固定で設定する必要があります。参加中のホストに接続されているすべてのポートを共通（一般）VLANに追加し、マルチキャストサービスを同VLANグループに割り当ててください。

コマンド利用：

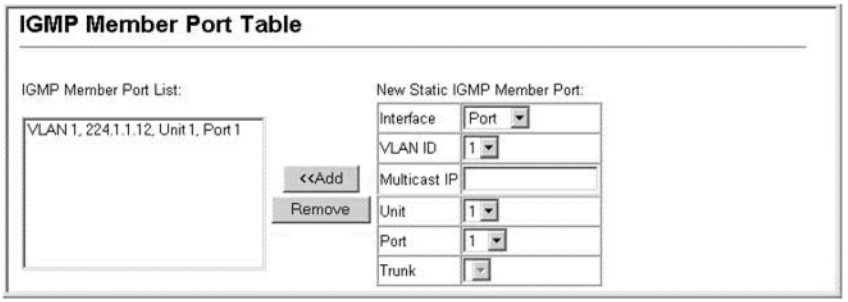
- 固定マルチキャストアドレスはエージアウトしません。
- 特定VLAN内のインタフェースに対しマルチキャストアドレスを割り当てる場合、該当トラフィックは同VLAN内のポートに対してのみ転送することが可能です。

コマンド解説：

- Interface（インタフェース）
  Port(ポート)ないしTrunk(トランク)スクロールダウンリストを起動します。
- VLAN ID
  接続されているマルチキャストルータないしスイッチから届くすべてのマルチキャストトラフィックを広めるVLANを選択します。
- Multicast IP（マルチキャストIP）
  特定のマルチキャストサービス用のIPアドレスです。
- Unit（ユニット）
  スタックユニットです（範囲：1～8）。
- Port（ポート)ないしTrunk（トランク）
  マルチキャストルータないしスイッチに接続されているインタフェースを指定します。

WEB：

IGMP Snooping (IGMPスヌーピング)→IGMP Member Port Table (IGMPメンバーポートテーブル)と選択します。IGMP対応スイッチないしマルチキャストルータ経由でマルチキャストサービスに接続されているインタフェースを指定してください。同マルチキャストサービスを広めるVLANを選び、マルチキャストIPアドレスを指定してAdd (追加)をクリックしてください。該当ポートをすべてメンバーリストに追加し終えた時点でApply(適用)をクリックしてください。




CLI：

以下の例では、マルチキャストアドレスをVLAN 1に割り当ててた上で、VLAN1上でサポートされているすべての既知のマルチキャストサービスを表示しています。

```
Console(config)#ip igmp snooping vlan 1 static 224.1.1.12
  ethernet 1/12                                                    4-182
Console(config)#exit
Console#show mac-address-table multicast vlan 1                    4-184
 VLAN M'cast IP addr. Member ports Type
 ---- --------------- ------------ -------
    1      224.1.1.12       Eth1/12    USER
    1       224.1.2.3       Eth1/12    IGMP
Console#
```

# 第4章：コマンドラインインタフェース

本章では、コマンドラインインタフェース(CLI)の使用方法について解説します。

## コマンドラインインタフェースの使用

### CLIへのアクセス

サーバのコンソールポートへの直接接続を介して、またはTelnet接続経由で、本製品の管理インタフェースにアクセスする場合、プロンプトにコマンドキーワードおよびパラメータを入力することで本製品を管理できます。 本製品のコマンドラインインタフェース(CLI)の使用方法は、UNIXシステムでのコマンド入力とよく似ています。

### コンソール接続

コンソールポートを使用して本製品にアクセスするには、以下の手順を実行してください。

1. コンソールプロンプトで、ユーザ名とパスワードを入力します（デフォルトのユーザ名は「admin」と「guest」で、対応するパスワードはそれぞれ「admin」と「guest」)。 管理者のユーザ名とパスワード(admin)を入力すると、CLIに「Console#」というプロンプトが表示され、優先アクセスモード(Privileged Exec)になります。 ゲストのユーザ名とパスワード(guest)を入力すると、CLIには「Console>」というプロンプトが表示され、通常アクセスモード(Normal Exec)になります。
2. 必要なコマンドを入力して目的の作業を完了します。
3. 完了したら、quitコマンドまたはexitコマンドを使用してセッションを終了します。

コンソールポートを介してシステムに接続すると、以下のログイン画面が表示されます。

```
User Access Verification

Username: admin
Password:

      CLI session with the 24PORT STACKABLE SWITCH is opened.
      To end the CLI session, enter [Exit].
Console#
```

### Telnet接続

TelnetはIPトランスポートプロトコルを介して動作します。 この環境では、使用する管理ステーションとネットワーク経由で管理するネットワーク機器に、有効なIPアドレスが必要です。有効なIPアドレスは、0から255までの4つの数値をピリオドで区切った形式です。 各アドレスは、ネットワーク部分とホスト部分で構成されます。 たとえば、本製品に割り当てられているIPアドレス10.1.0.1 (サブネットマスク255.255.255.0)は、ネットワーク部分が10.1.0、ホ

スト部分が1です。

**注意：** 本製品のIPアドレスは、デフォルト設定によりDHCP経由で取得されます。

Telnetセッション経由で本製品にアクセスするには、まずマスタユニットのIPアドレスを設定する必要があります。また、別のIPサブネットから本製品を管理する場合は、デフォルトゲートウェイを設定する必要があります。 以下に例を示します。

```
Console(config)#interface vlan 1
Console(config-if)#ip address 10.1.0.254 255.255.255.0
Console(config-if)#exit
Console(config)#ip default-gateway 10.1.0.254
```

会社のネットワークが社外の別のネットワークまたはインターネットに接続している場合は、登録済みのIPアドレスを申請する必要があります。 ただし、外部と分離されたネットワークに接続している場合は、接続先のネットワークセグメントに一致する任意のIPアドレスを使用できます。

本製品のIPアドレスを設定後、以下の手順を実行するとTelnetセッションを開くことができます。

1. リモートホストから、Telnetコマンドとアクセス先の機器のIPアドレスを入力します。
2. プロンプトで、ユーザ名とシステムパスワードを入力します 管理者の場合は優先アクセスモード(Privileged Exec)を使用していることを示す「Vty-*n*#」プロンプトが、ゲストの場合は通常アクセスモード(Normal Exec)を使用していることを示す「Vty-*n*>」プロンプトがCLIに表示されます(*n*は現在のTelnetセッションの数)。
3. 必要なコマンドを入力して目的の作業を完了します。
4. 完了したら、「quit」コマンドまたは「exit」コマンドを使用してセッションを終了します。

Telnetコマンドを入力後、以下のログイン画面が表示されます。

```
Username: admin
Password:


      CLI session with the 24PORT STACKABLE SWITCH is opened.
      To end the CLI session, enter [Exit].


Vty-0#
```

**注意：** Telnet経由では、本製品へのセッションを最大4つ開くことができます。

# コマンドの入力

本セクションでは、CLIコマンドの入力方法について解説します。

## キーワードおよび引数

CLIコマンドは、一連のキーワードと引数で構成されます。 キーワードでコマンドを特定し、引数で設定パラメータを指定します。 たとえば、show interfaces status ethernet 1/5コマンドでは、**show interfaces**と**status**がキーワードであり、**ethernet**はインタフェースのタイプを指定する引数、**1/5**はユニット/ポートを示します。

コマンドは以下のように入力できます。

- 単純なコマンドを1つ入力するには、コマンドキーワードを入力します。
- 複数のコマンドを入力するには、各コマンドを必要な順序で入力します。 たとえば、Privileged Execコマンドモードを有効にし、起動設定(startup configuration)を表示するには、以下のように入力します。

  Console>**enable**
  Console#**show startup-config**

- パラメータが必要なコマンドを入力するには、コマンドキーワードの後に必要なパラメータを入力します。 たとえば、管理者のパスワードを設定するには、以下のように入力します。

  Console(config)#**username admin password 0 smith**

## 最小省略形

CLIには、コマンドを一意に識別できる最小限の文字数で入力できます。 たとえば、configureコマンドは、**con**と入力できます。 入力があいまいな場合は、再度入力するように指示があります。

## コマンドのオートコンプリート

Tabキーを押して入力を終了すると、途中まで入力したキーワードの残りの文字がCLIに表示されます。「logging history」の例では、**log**と入力してTabキーを押すと、**logging**コマンドまでが表示されます。

## コマンドに関するヘルプ

**help**コマンドを入力すると、ヘルプシステムの簡単な説明を表示できます。「?」を使用してキーワードまたはパラメータのリストを表示することにより、コマンドの構文を表示することもできます。

## コマンドの表示

コマンドプロンプトで「?」を入力すると、現在のコマンドクラス(Normal ExecまたはPrivileged Exec)あるいは設定クラス(Global、ACL、Interface、Line、VLAN Databaseのいずれか)に関して、第1レベルのキーワードが表示されます。 特定のコマンドに関して有効なキーワードのリストを表示することもできます。 たとえば、**show ?**コマンドを実行すると、使用可能なshowコマンドのリストが以下のように表示されます。

```
Console#show ?
  access-group          Access groups
  access-list           Access lists
  bridge-ext            Bridge extension information
  calendar              Date  and time information
  dot1x                 Show 802.1X content
  garp                  GARP properties
  gvrp                  GVRP interface information
  history               History information
  interfaces            Interface information
  ip                    IP information
  lacp                  LACP statistics
  line                  TTY line information
  log                   Login records
  logging               Login setting
  mac                   MAC access lists
  mac-address-table     Configuration of the address table
  management            Management IP filter
  map                   Maps priority
  port                  Port Characteristics
  public-key            Public Key information
  queue                 Priority queue information
  radius-server         RADIUS server information
  rate-limit            Configures rate-limits
  running-config        Information on the running configuration
  snmp                  Simple Network Management Protocol statistics
  sntp                  Simple Network Time Protocol configuration
  spanning-tree         Spanning-tree configuration
  ssh                   Secure shell server connections
  startup-config        Startup system configuration
  system                System Information
  tacacs-server         TACACS server settings
  users                 Information about terminal lines
  version               System hardware and software versions
  vlan                  Virtual LAN settings
Console#show
```

**show interfaces ?**コマンドを実行すると、以下の情報が表示されます。

```
Console#show interfaces ?
  counters          Interface counters information
  status            Interface status information
  switchport        Interface switchport information
Console#show interfaces
```

## キーワード部分検索

キーワードの一部を入力し、末尾に疑問符を付けて実行すると、頭文字が一致する選択肢が表示されます（コマンドと疑問符の間にスペースを入れないでください）。 たとえば、「**s?**」を実行すると、「s」で始まるキーワードがすべて表示されます。

```
Console#show s?
snmp            sntp            spanning-tree   ssh             startup-config
system
Console#show s
```

## コマンドの機能の否定

多数の設定コマンドに関して、接頭辞として「**no**」というキーワードを入力すると、コマンドの機能を取り消す、または設定をデフォルト値にリセットすることができます。 たとえば、**logging**コマンドを実行すると、システムメッセージがホストサーバに記録されます。 ログを無効にするには、**no logging**コマンドを指定します。 本書では、該当するすべてのコマンドの否定機能について解説します。

## コマンド履歴の使用

CLIでは、以前に入力されたコマンドの履歴が維持されます。 上向き矢印キーを押すと、コマンドの履歴をさかのぼることができます。 履歴リストに表示されるコマンドはすべて再実行できます。また、変更してから実行することもできます。

**show history**コマンドを使用すると、最近実行したコマンドがさらに多数表示されます。

## コマンドモードについて

コマンドセットは、Execクラスと設定(Configuration)クラスに分けられます。 Execコマンドでは通常、システムのステータスを表示、または統計カウンタをクリアします。 一方、設定コマンドでは、インタフェースのパラメータを変更、または一定のスイッチ機能を有効にします。これらのクラスは、さらに複数のモードに分けられます。 使用可能なコマンドは、選択したモードによって異なります。 プロンプトで疑問符「**?**」を入力すると、現在のモードで使用可能なコマンドの一覧を表示できます。 コマンドクラスおよび関連するモードを、以下の表に示します。

表 4-1　コマンドモード

| クラス | モード | |
|---|---|---|
| Exec (実行) | Normal (通常)<br>Privileged (優先) | |
| Configuration (設定) | Global (グローバル)* | Access Control List (アクセス制御リスト)<br>Interface (インタフェース)<br>Line (回線)<br>VLAN Database (VLANデータベース) |

＊ グローバル設定モードへは、Privileged Execモードからアクセスする必要があります。
その他の設定モードへは、グローバル設定モードからアクセスする必要があります。

## Execコマンド

本製品で、「guest」のユーザ名とパスワードを使用して新しいコンソールセッションを開くと、システムはNormal Execコマンドモード(またはゲストモード)になり、「Console>」コマンドプロンプトが表示されます。 このモードで使用できるコマンドの数は限られています。
Privileged Execコマンドモード(または管理者モード)からのみ、すべてのコマンドにアクセスできます。 Privilege Execモードにアクセスするには、「admin」のユーザ名とパスワードを使用して新しいコンソールセッションを開きます。 そうすると、「Console#」コマンドプロンプトが表示されます。 また、**enable**コマンドに続けて優先レベルのパスワード「super」を入力し、Normal Execモード内からPrivileged Execモードに移行することもできます(266ページ)。

Privileged Execモードにするには、以下のユーザ名とパスワードを入力します。

```
Username: admin
Password: [admin login password]


        CLI session with the 24PORT STACKABLE SWITCH is opened.
        To end the CLI session, enter [Exit].
Console#
```

```
 Username: guest
 Password: [guest login password]


         CLI session with the 24PORT STACKABLE SWITCH is opened.
         To end the CLI session, enter [Exit].
 Console>enable
 Password: [privileged level password]
 Console#
```

## 設定コマンド

設定コマンドは、優先レベルのコマンドであり、スイッチの設定の変更に使用します。 設定コマンドでは、実行中の設定のみが変更され、本製品を再起動した場合は保存されません。 実行中の設定を不揮発性ストレージに保存するには、**copy running-config startup-config**コマンドを使用します。

設定コマンドは、以下のモードに分けられます。

- Global Configuration (グローバル設定) - システムレベルの設定を変更します。 **hostname**や**snmp-server community**などのコマンドが含まれます。
- Access Control List Configuration (アクセス制御リスト設定) - パケットフィルタリングに使用します。
- Interface Configuration (インタフェース設定) - **speed-duplex**や**negotiation**などのポート設定を変更します。
- Line Configuration (回線設定) - コンソールポートおよびTelnetの設定を変更します。 **parity**や**databits**などのコマンドが含まれます。
- VLAN Configuration (VLAN設定) - VLANグループを作成するコマンドが含まれます。

グローバル設定モードに移行するには、Privileged Execモードで**configure**コマンドを入力します。 システムプロンプトが「Console(config)#」に変わり、すべてのグローバル設定コマンドにアクセス可能になります。

```
Console#configure
Console(config)#
```

その他のモードに移行するには、設定プロンプトで以下のいずれかのコマンドを入力します。 **exit**コマンドまたは**end**コマンドを使用すると、Privileged Execモードに戻ります。

表 4-2 設定モード

| モード | コマンド | プロンプト | ページ |
|---|---|---|---|
| Line (回線) | line {console \| vty} | Console(config-line)# | 245 |
| Access Control List (アクセス制御リスト) | access-list ip standard<br>access-list ip extended<br>access-list mac | Console(config-std-acl)#<br>Console(config-ext-acl)#<br>Console(config-mac-acl)# | 341 |
| Interface (インタフェース) | interface {ethernet *port* \| port-channel *id*\| vlan *id*} | Console(config-if)# | 365 |
| VLAN | vlan database | Console(config-vlan)# | 413 |

たとえば、以下のコマンドを使用すると、インタフェース設定モードに移行してから、
Privileged Execモードに戻ります。

```
Console(config)#interface ethernet 1/5
.
.
.
Console(config-if)#exit
Console(config)#
```

## コマンドライン処理

コマンドでは大文字小文字は区別されません。 現在使用可能な他のコマンドまたはパラメータと区別できるだけの文字数があれば、コマンドやパラメータを省略できます。 コマンドの一部を入力してTabキーを押す、またはコマンドの一部を入力して末尾に「?」を付けると、入力した文字列に一致する候補の一覧が表示されます。 また、以下の編集用キー操作をコマンドライン処理に使用することもできます。

**表 4-3　コマンドライン処理**

| キー操作 | 機能 |
|---|---|
| Ctrl + A | カーソルをコマンドラインの先頭に移動 |
| Ctrl + B | カーソルを左に1文字分移動 |
| Ctrl + C | 現在の作業を終了してコマンドプロンプトを表示 |
| Ctrl + E | カーソルをコマンドラインの末尾に移動 |
| Ctrl + F | カーソルを右に1文字分移動 |
| Ctrl + K | カーソルの位置から行末までのすべての文字を削除 |
| Ctrl + L | 現在のコマンドラインを新規の行で繰り返し |
| Ctrl + N | 履歴バッファの次のコマンドラインを入力 |
| Ctrl + P | 直前のコマンドを入力 |
| Ctrl + R | 現在のコマンドラインを新規の行で繰り返し |
| Ctrl + U | カーソルの位置から行頭までを削除 |
| Ctrl + W | 最後に入力したワードを削除 |
| Esc + B | カーソルを1ワード前に移動 |
| Esc + D | カーソルの位置からワードの末尾までを削除 |
| Esc + F | カーソルを1ワード後に移動 |
| DeleteキーまたはBackspaceキー | コマンド入力時の誤りを消去 |

# コマンドグループ

システムコマンドは、以下に示す機能グループに分けられます。

表 4-4　コマンドグループ

| コマンドグループ | 説明 | ページ |
|---|---|---|
| 回線 | ボーレートやコンソールタイムアウトを含む、シリアルポートおよびTelnetの通信パラメータを設定 | 245 |
| 一般 | 優先アクセスモードへの移行、システムの再起動、CLIの終了のための基本コマンド | 256 |
| システム管理 | システムログ、システムパスワード、ユーザ名、ブラウザ管理オプション、その他様々なシステム情報を制御 | 258 |
| フラッシュ/ファイル | コードイメージファイルまたはスイッチ設定ファイルを管理 | 313 |
| 認証 | ローカルまたはリモートの認証を使用したログオンアクセスの設定、ポートセキュリティおよびIEEE 802.1Xポートアクセス制御の設定 | 321 |
| アクセス制御リスト | IPフレーム(アドレス、プロトコル、TCP/UDPポート番号、TCP制御コードのいずれかに基づく)または非IPフレーム(MACアドレスまたはイーサネットタイプに基づく)のフィルタリング | 341 |
| SNMP | 認証障害トラップのアクティブ化、コミュニティアクセス文字列とトラップマネージャの設定、およびIPアドレスフィルタリングの設定 | 358 |
| インタフェース | すべてのイーサネットポート、集合リンク、VLANの接続パラメータを設定 | 365 |
| ミラーポート | 通過するデータや監視対象のポートに影響を与えずに、データを分析用に別のポートへミラーリング | 379 |
| 速度制限 | 任意のポートで送受信されるトラフィックの最高速度を制御 | 381 |
| リンクアグリゲーション | 複数のポートを1つの論理トランクに統計的にグループ化、LACP (Link Aggregation Control Protocol)をポートトランク用に設定 | 383 |
| アドレステーブル | 指定したアドレスのフィルタリング用にアドレステーブルを設定、現在のエントリを表示、テーブルをクリア、またはエージング期間を設定 | 395 |
| スパニングツリー | 本製品のスパニングツリーを設定 | 400 |

| | | |
|---|---|---|
| VLAN | VLANを設定してVLANグループのポートメンバシップを定義、プライベートVLANを有効化または設定 | 413 |
| GVRPおよびブリッジ拡張 | 自動VLAN学習を可能にするGVRPを設定、ブリッジ拡張MIBの設定を表示 | 430 |
| 優先度 | タグ無しフレームのポート優先度の設定、優先度キューごとにストリクトまたはウェイトラウンドロビン（相対的ウェイト）の選択、TCPトラフィックタイプ、IP優先度、DSCPの優先度を設定 | 434 |
| マルチキャストフィルタリング | IGMPマルチキャストフィルタリング、クエリパラメータを設定してマルチキャストルータに接続されているポートを指定 | 451 |
| IPインタフェース | スイッチのIPアドレスを設定 | 462 |

これ以降の表では、アクセスモードを以下の略語で示します。

**NE** (Normal Exec)
**PE** (Privileged Exec)
**GC** (Global Configuration)
**ACL** (Access Control List Configuration)
**IC** (Interface Configuration)
**LC** (Line Configuration)
**VC** (VLAN Database Configuration)

# 回線コマンド

オンボード設定プログラムにアクセスするには、VT100互換機器をサーバのシリアルポートに接続します。 以下のコマンドを使用して、シリアルポートまたはTelnet (仮想端末)の通信パラメータを設定します。

表 4-5　回線コマンド

| コマンド | 機能 | モード | ページ |
|---|---|---|---|
| line | 設定する回線を特定して回線設定モードを開始 | GC | 246 |
| login | ログイン時のパスワードチェックを有効化 | LC | 247 |
| password | 任意の回線のパスワードを指定 | LC | 248 |
| timeout login response | ユーザがCLIにログインするまでのシステムの待機時間を設定 | LC | 249 |
| exec-timeout | ユーザの入力が検出されるまでのコマンドインタプリタの待機時間を設定 | LC | 249 |
| password-thresh | 不正なパスワード入力のしきい値を設定してログオン試行の失敗回数を制限 | LC | 250 |

| | | | |
|---|---|---|---|
| silent-time* | ログオン試行の失敗回数が**password-thresh**コマンドで設定したしきい値を超えた後に、管理コンソールがアクセス不能になる期間を設定 | LC | 251 |
| databits* | ハードウェアで解釈および生成された、文字ごとのデータビット数を設定 | LC | 252 |
| parity* | パリティビットの生成を定義 | LC | 252 |
| speed* | 端末のボーレートを設定 | LC | 253 |
| stopbits* | 1バイトごとに送信されるストップビットの数を設定 | LC | 254 |
| disconnect | 回線接続を停止 | PE | 254 |
| show line | 端末回線のパラメータを表示 | NE、PE | 255 |

** これらのコマンドは、シリアルポートのみで使用できます。*

### line

設定を行い、後続の回線設定コマンドを処理する回線を特定します。

#### 構文

**line** {**console** | **vty**}

- **console** – コンソール端末回線
- **vty** – リモートコンソールアクセス(Telnet)用の仮想端末

#### デフォルト設定

デフォルトの回線なし

#### コマンドモード

Global Configuration

#### コマンドの使用方法

Telnetは仮想端末接続とみなされ、**show users**などの画面表示では「Vty」と表示されます。 ただし、シリアル通信パラメータ(データビットなど)はTelnet接続に影響しません。

#### 例

コンソール回線モードに移行するには、以下のコマンドを入力します。

```
Console(config)#line console
Console(config-line)#
```

### 関連コマンド

show line (p.255)
show users (p.311)

## login

ログイン時のパスワードチェックを有効にします。 パスワードチェックを無効にしてパスワードなしの接続を許可するには、**no**形式を使用します。

### 構文

**login** [**local**]
**no login**

**local** – ローカルのパスワードチェックを選択。 認証は、**username**コマンドで指定したユーザ名に基づいて行われます。

### デフォルト設定

login local

### コマンドモード

Line Configuration

### コマンドの使用方法

- 本製品では、ログイン時に以下の3つの認証モードを使用できます。
  - **login** – **password**回線設定コマンドで指定されている単一のグローバルパスワードによる認証を選択します。 この方法を使用している場合、管理インタフェースはNormal Exec (NE)モードで起動します。
  - **login local** – **username**コマンドで指定されているユーザ名とパスワード(デフォルト設定)による認証を選択します。 この方法を使用している場合、管理インタフェースは、ユーザの優先レベルが0のときはNormal Exec (NE)モード、ユーザの優先レベルが15のときはPrivileged Exec (PE)モードで起動します。
  - **no login** – 認証を選択しません。 この方法を使用している場合、管理インタフェースはNormal Exec (NE)モードで起動します。
- このコマンドは、本製品自体でのログイン認証を制御します。 リモートの認証サーバのユーザ名およびパスワードを設定するには、該当するサーバにインストールされているRADIUSソフトウェアまたはTACACSソフトウェアを使用する必要があります。

### 例

```
Console(config-line)#login local
Console(config-line)#
```

**関連コマンド**

username (p.265)
password (p.248)

**password**

任意の回線のパスワードを指定します。 パスワードを削除するにはno形式を使用します。

**構文**

**password** {**0** | **7**} *パスワード*
**no password**

- {**0** | **7**} – 0は通常のパスワード、7は暗号化パスワード
- *パスワード* – 回線パスワードを指定する文字列 (最大設定:通常テキストは8文字、暗号化は32文字、大文字小文字を区別)

**デフォルト設定**

パスワード指定なし

**コマンドモード**

Line Configuration

**コマンドの使用方法**

- パスワード保護されている回線で接続が開始されると、パスワードが要求されます。正しいパスワードを入力すると、プロンプトが表示されます。 **password-thresh**コマンドを使用すると、誤ったパスワードを何回入力したら回線接続が切断され、端末がアイドル状態に戻るかを設定できます。
- 暗号化パスワードは、システムの起動中に設定ファイルを読み込む場合や、TFTPサーバから設定ファイルをダウンロードする場合に、従来のパスワード設定(通常テキストまたは暗号化)と互換性を持たせるために必要です。 暗号化パスワードをユーザが手動で設定する必要はありません。

**例**

```
Console(config-line)#password 0 secret
Console(config-line)#
```

**関連コマンド**

login (p.247)
password-thresh (p.250)

### timeout login response

ユーザがCLIにログインするまでのシステムの待機時間を設定します。 デフォルトを復元するにはno形式を使用します。

#### 構文

**timeout login response** [*秒*]
**no timeout login response**

*秒* - タイムアウト時間を指定する整数
(範囲:0～300秒、0:無効)

#### デフォルト設定

- CLI: 無効(0秒)
- Telnet: 600秒

#### コマンドモード

Line Configuration

#### コマンドの使用方法

- タイムアウト時間内にログイン試行が検出されない場合、そのセッションの接続は停止されます。
- このコマンドは、ローカルコンソール接続とTelnet接続の両方に該当します。
- Telnetのタイムアウトを無効にすることはできません。
- タイムアウトを指定せずにこのコマンドを使用した場合、デフォルトの設定が復元されます。

#### 例

タイムアウトを2分に設定するには、以下のコマンドを入力します。

```
Console(config-line)#timeout login response 120
Console(config-line)#
```

#### 関連コマンド

silent-time (p.251)
exec-timeout (p.249)

### exec-timeout

ユーザの入力が検出されるまでのシステムの待機時間を設定します。 デフォルトを復元するにはno形式を使用します。

#### 構文

**exec-timeout** [*秒*]
**no exec-timeout**

*秒* - 秒数を指定する整数（範囲:0～65535秒、0:タイムアウトなし）

**デフォルト設定**

CLI: タイムアウトなし
Telnet: 10分

**コマンドモード**

Line Configuration

**コマンドの使用方法**

- タイムアウト時間内にユーザの入力が検出された場合、セッションは開いたままになり、検出されない場合、セッションは停止されます。
- このコマンドは、ローカルコンソール接続とTelnet接続の両方に該当します。
- Telnetのタイムアウトを無効にすることはできません。
- タイムアウトを指定せずにこのコマンドを使用した場合、デフォルトの設定が復元されます。

**例**

タイムアウトを2分に設定するには、以下のコマンドを入力します。

```
Console(config-line)#exec-timeout 120
Console(config-line)#
```

**関連コマンド**

silent-time (p.251)
timeout login response (p.249)

### password-thresh

不正なパスワード入力のしきい値を設定してログオン試行の失敗回数を制限します。 しきい値を削除するには**no**形式を使用します。

**構文**

**password-thresh** [*しきい値*]
**no password-thresh**

*しきい値* - パスワード入力試行が可能な回数（範囲:1～120回、0:しきい値なし）

**デフォルト設定**

デフォルト値は3回

**コマンドモード**

Line Configuration

**コマンドの使用方法**

- ログオン試行のしきい値に達すると、システムインタフェースは指定された期間アクセス不能になり、その後次のログオン試行が可能になります（**silent-time**コマンドでこの期間を設定)。 Telnetでこのしきい値に達すると、Telnetログオンインタフェースがシャットダウンします。
- このコマンドは、ローカルコンソール接続とTelnet接続の両方に該当します。

**例**

パスワードのしきい値を5回に設定するには、以下のコマンドを入力します。

```
Console(config-line)#password-thresh 5
Console(config-line)#
```

**関連コマンド**

silent-time (p.251)
timeout login response (p.249)

### silent-time

ログオン試行の失敗回数が**password-thresh**コマンドで設定したしきい値を超えた後に、管理コンソールがアクセス不能になる期間を設定します。 沈黙期間の値を削除するには**no**形式を使用します。

**構文**

**silent-time** [*秒*]
**no silent-time**

*秒* - コンソールを無反応にする秒数（範囲:0～65535秒、0:沈黙期間なし）

**デフォルト設定**

デフォルト値は沈黙期間なし

**コマンドモード**

Line Configuration

**例**

沈黙期間を60秒に設定するには、以下のコマンドを入力します。

```
Console(config-line)#silent-time 60
Console(config-line)#
```

**関連コマンド**

password-thresh (p.250)

### databits
コンソールポートで解釈および生成された、文字ごとのデータビット数を設定します。 デフォルト値を復元するには**no**形式を使用します。

#### 構文
**databits** {**7** | **8**}
**no databits**

- 7 – 1文字につき7データビット
- 8 – 1文字につき8データビット

#### デフォルト設定
1文字につき8データビット

#### コマンドモード
Line Configuration

#### コマンドの使用方法
**databits**コマンドを使用すると、パリティを含む7データビットを生成する機器からの入力時に高いビットをマスクできます。 パリティが生成されている場合、1文字ごとのデータビットを7に指定します。 パリティが不要な場合、1文字ごとのデータビットを8に指定します。

#### 例
7データビットを指定するには、以下のコマンドを入力します。

```
Console(config-line)#databits 7
Console(config-line)#
```

#### 関連コマンド
parity (p.252)

### parity
パリティビットの生成を定義します。 デフォルト設定を復元するには**no**形式を使用します。

#### 構文
**parity** {**none** | **even** | **odd**}
**no parity**

- **none** – パリティなし
- **even** – 偶数のパリティ
- **odd** – 奇数のパリティ

**デフォルト設定**

パリティなし

**コマンドモード**

Line Configuration

**コマンドの使用方法**

端末やモデムなどの機器で使用する通信プロトコルには、多くの場合、特定のパリティビット設定が必要です。

**例**

パリティなしを指定するには、以下のコマンドを入力します。

```
Console(config-line)#parity none
Console(config-line)#
```

**speed**

端末回線のボーレートを設定します。 (端末への)送信および(端末からの)受信の両方の速度を設定します。 デフォルト設定を復元するには**no**形式を使用します。

**構文**

**speed** *bps*
**no speed**

*bps* - ボーレート(ビット/秒)
(オプション:9600、19200、38400、57600、115200bps)

**デフォルト設定**

9600

**コマンドモード**

Line Configuration

**コマンドの使用方法**

シリアルポートに接続されている機器のボーレートに一致する速度を設定します。 ポートに接続されている機器のボーレートによっては、サポートされない場合があります。選択した速度がサポートされていない場合、それを示すメッセージが表示されます。

**例**

57600bpsを指定するには、以下のコマンドを入力します。

```
Console(config-line)#speed 57600
Console(config-line)#
```

### stopbits

1バイトごとに送信されるストップビットの数を設定します。 デフォルト設定を復元するには no形式を使用します。

#### 構文

**stopbits** {**1** | **2**}

- 1 – 1ストップビット
- 2 – 2ストップビット

#### デフォルト設定

1ストップビット

#### コマンドモード

Line Configuration

#### 例

2ストップビットを指定するには、以下のコマンドを入力します。

```
Console(config-line)#stopbits 2
Console(config-line)#
```

### disconnect

SSH、Telnet、またはコンソールの接続を停止します。

#### 構文

**disconnect** *セッションID*

*セッションID* – SSH、Telnet、またはコンソール接続のセッションID (範囲:0～4)

#### コマンドモード

Privileged Exec

#### コマンドの使用方法

セッションID「0」を指定すると、コンソール接続が切断されます。 その他のアクティブセッションのIDを指定すると、SSH接続またはTelnet接続が切断されます。

#### 例

```
Console#disconnect 1
Console#
```

**関連コマンド**

show ssh (p.282)
show users (p.311)

### show line

端末回線のパラメータを表示します。

**構文**

**show line** [**console** | **vty**]

- **console** – コンソール端末回線
- **vty** – リモートコンソールアクセス(Telnet)用の仮想端末

**デフォルト設定**

すべての回線を表示

**コマンドモード**

Normal Exec、Privileged Exec

**例**

すべての回線を指定するには、以下のコマンドを入力します。

```
Console#show line
  Console configuration:
    Password threshold:   3 times
    Interactive timeout: Disabled
    Login timeout: Disabled
    Silent time:              Disabled
    Baudrate:                   9600
    Databits:                   8
    Parity:                     none
    Stopbits:                   1


  VTY configuration:
    Password threshold:   3 times
    Interactive timeout: 600 sec
    Login timeout: 300 sec
console#
```

# 一般コマンド

表 4-6 一般コマンド

| コマンド | 機能 | モード | ページ |
|---|---|---|---|
| enable | 優先モードをアクティブ化 | NE | 256 |
| disable | 優先モードから通常モードに戻る | PE | 257 |
| configure | グローバル設定モードをアクティブ化 | PE | 258 |
| show history | コマンド履歴バッファを表示 | NE、PE | 258 |
| reload | システムを再起動 | PE | 259 |
| end | Privileged Execモードに戻る | 任意の設定モード | 260 |
| exit | 前の設定モードに戻る、またはCLIを終了 | 任意 | 260 |
| quit | CLIセッションを終了 | NE、PE | 261 |
| help | ヘルプの使用方法を表示 | 任意 | 該当なし |
| ? | コマンドのオートコンプリートのオプションを表示(コンテキストに依存) | 任意 | 該当なし |

### enable

Privileged Execモードをアクティブにします。 優先モードでは、追加のコマンドを使用でき、一定のコマンドを使用すると追加情報が表示されます。 239ページの「コマンドモードについて」を参照してください。

#### 構文

**enable** [*レベル*]

*レベル* – 本製品にログインする優先レベル

本製品には、事前に定義されている優先レベルが2つあります(0:Normal Exec、15:Privileged Exec)。 Privileged Execモードにアクセスするには、レベル15を入力します。

#### デフォルト設定

レベル15

**コマンドモード**

Normal Exec

**コマンドの使用方法**

- 「super」は、コマンドモードをNormal ExecからPrivileged Execに変更する場合に必要なデフォルトのパスワードです (このパスワードを設定するには、266ページの **enable password**コマンドを参照)。
- 「#」記号がプロンプトの末尾に表示されている場合、システムは優先アクセスモードになっています。

**例**

```
Console>enable
Password: [privileged level password]
Console#
```

**関連コマンド**

disable (4-21)
enable password (p.266)

**disable**

優先モードからNormal Execモードに戻ります。 通常アクセスモードでは、スイッチの設定やイーサネットの統計に関する基本情報のみを表示できます。 すべてのコマンドにアクセスするには、優先モードを使用する必要があります。 239ページの「コマンドモードについて」を参照してください。

**デフォルト設定**

なし

**コマンドモード**

Privileged Exec

**コマンドの使用方法**

「>」記号がプロンプトの末尾に表示されている場合、システムは通常アクセスモードになっています。

**例**

```
Console#disable
Console>
```

**関連コマンド**

enable (p.256)

### configure
グローバル設定モードをアクティブにします。 スイッチの設定を変更するには、このモードに移行する必要があります。 また、インタフェース設定、回線設定、VLANデータベース設定など、他の一部の設定モードを有効にする前にも、グローバル設定モードに移行する必要があります。 239ページの「コマンドモードについて」を参照してください。

#### デフォルト設定
なし

#### コマンドモード
Privileged Exec

#### 例
```
Console#configure
Console(config)#
```

#### 関連コマンド
end (p.260)

### show history
コマンド履歴バッファの内容を表示します。

#### デフォルト設定
なし

#### コマンドモード
Normal Exec、Privileged Exec

#### コマンドの使用方法
履歴バッファのサイズは、Execution (実行)コマンド10個とConfiguration (設定)コマンド10個に固定されています。

#### 例
以下の例では、show historyコマンドでコマンド履歴バッファの内容が表示されています。

```
Console#show history
Execution command history:
 2 config
 1 show history

Configuration command history:
 4 interface vlan 1
 3 exit
 2 interface vlan 1
 1 end

Console#
```

**!**コマンドを使用すると、Normal ExecモードまたはPrivileged Execモードの場合はExecutionコマンド履歴バッファのコマンドが、設定モードの場合はConfigurationコマンド履歴バッファのコマンドが繰り返されます。 以下の例では、**!2**コマンドにより、Execution履歴バッファの2番目のコマンド(**config**)が繰り返されます。

```
Console#!2
Console#config
Console(config)#
```

### reload

システムを再起動します。

**注意:** このコマンドでシステムを再起動すると、Power-On Self-Testが常に実行されます。 また、**copy running-config startup-config**コマンドにより、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。

#### デフォルト設定

なし

#### コマンドモード

Privileged Exec

#### コマンドの使用方法

システム全体をリセットします。

#### 例

以下の例は、スイッチのリセット方法を示しています。

```
Console#reload
System will be restarted, continue <y/n>? y
```

**end**
Privileged Execモードに戻ります。

**デフォルト設定**

なし

**コマンドモード**

Global Configuration、Interface Configuration、Line Configuration、VLAN Database Configuration

**例**
以下の例は、インタフェース設定モードからPrivileged Execモードに戻る方法を示しています。

```
Console(config-if)#end
Console#
```

**exit**
前の設定モードに戻るか、または設定プログラムを終了します。

**デフォルト設定**

なし

**コマンドモード**

任意

**例**
以下の例は、グローバル設定モードからPrivileged Execモードに戻り、CLIセッションを終了する方法を示しています。

```
Console(config)#exit
Console#exit

Press ENTER to start session
User Access Verification

Username:
```

**quit**
設定プログラムを終了します。

**デフォルト設定**

なし

**コマンドモード**

Normal Exec、Privileged Exec

**コマンドの使用方法**

**quit**コマンドと**exit**コマンドのどちらを使用しても、設定プログラムを終了できます。

**例**
以下の例は、CLIセッションの終了方法を示しています。

```
Console#quit

Press ENTER to start session

User Access Verification

Username:
```

# システム管理コマンド

これらのコマンドでは、システムログ、パスワード、ユーザ名、ブラウザ設定オプションを制御し、その他様々なシステム情報を表示または設定します。

表 4-7　システム管理コマンド

| コマンドグループ | 機能 | ページ |
|---|---|---|
| 機器指定 | 本製品を一意に識別する情報を設定 | 263 |
| ユーザアクセス | 管理アクセス用の基本のユーザ名およびパスワードを設定 | 264 |
| IPフィルタ | 管理アクセスが可能なIPアドレスを設定 | 267 |
| Webサーバ | Webブラウザ経由での管理アクセスを有効化 | 269 |
| Telnetサーバ | Telnet経由での管理アクセスを有効化 | 273 |
| セキュアシェル | Telnet用のセキュアな再配置を提供 | 274 |
| イベントログ | エラーメッセージのログを制御 | 285 |

| | | |
|---|---|---|
| 時間(システムクロック) | 自動(NTP/SNTPサーバ経由)または手動でシステムクロックを設定 | 299 |
| Time Commands | Sets the system clock using SNTP and time zone commands | 4-32 |
| システムステータス | システム設定、アクティブマネージャ、およびバージョン情報を表示 | 304 |
| フレームサイズ | 巨大フレームのサポートを有効化 | 312 |

# 機器指定コマンド

表 4-8　機器指定コマンド

| コマンド | 機能 | モード | ページ |
|---|---|---|---|
| prompt | PEモードおよびNEモードで使用するプロンプトをカスタマイズ | GC | 263 |
| hostname | スイッチのホスト名を指定 | GC | 263 |
| snmp-server contact | システムの連絡先の文字列を設定 | GC | 359 |
| snmp-server location | システムの場所の文字列を設定 | GC | 359 |

### prompt

CLIプロンプトをカスタマイズします。 デフォルトのプロンプトを復元するにはno形式を使用します。

#### 構文

**prompt** *文字列*
**no prompt**

*文字列* - CLIプロンプトに使用する任意の英数字の文字列（最大設定：255文字）

#### デフォルト設定

Console

#### コマンドモード

Global Configuration

#### 例

```
Console(config)#prompt RD2
RD2(config)#
```

### hostname

本製品のホスト名を指定または変更します。 デフォルトのホスト名を復元するにはno形式を使用します。

**構文**

**hostname** *名前*
**no hostname**

*名前* - このホストの名前（最大設定:255文字）

**デフォルト設定**

なし

**コマンドモード**

Global Configuration

**例**

```
Console(config)#hostname RD#1
Console(config)#
```

## ユーザアクセスコマンド

本セクションでは、管理アクセスに必要な基本コマンドについて解説します。 本製品には、コンソールまたはTelnet接続経由でのパスワードチェック(245ページ)、リモート認証サーバ経由でのユーザ認証(321ページ)、特定のポートのホストアクセス認証(332ページ)などのオプションも含まれています。

表 4-9　ユーザアクセスコマンド

| コマンド | 機能 | モード | ページ |
|---|---|---|---|
| username | ログイン時にユーザ名ベースの認証システムを確立 | GC | 265 |
| enable password | Privileged Execレベルへのアクセスを制御するパスワードを設定 | GC | 266 |

**username**

名前付きユーザの追加、ログイン時の認証要求、ユーザのパスワードの指定または変更(またはパスワード不要と指定)、ユーザのアクセスレベルの指定または変更を行います。ユーザ名を削除するには**no**形式を使用します。

**構文**

**username** *名前* {**access-level** *レベル* | **nopassword** | **password** {**0** | **7**} *パスワード*}
**no username** *名前*

- *名前* – ユーザの名前
  (最大設定:8文字、大文字小文字を区別。 最大ユーザ数:16)
- **access-level** *レベル* – ユーザレベルを指定
  本製品には、事前に定義されている優先レベルが2つあります(**0**:Normal Exec、**15**:Privileged Exec)。
- **nopassword** – このユーザのログインにパスワードは不要
- {**0** | **7**} – 0は通常のパスワード、7は暗号化パスワード
- **password** *パスワード* – ユーザの認証パスワード (最大設定:通常テキストは8文字、暗号化は32文字、大文字小文字を区別)

**デフォルト設定**

- デフォルトのアクセスレベルはNormal Exec
- ユーザ名とパスワードの出荷時のデフォルトは以下のとおり

**表 4-10 デフォルトのログイン設定**

| username | access-level | password |
|---|---|---|
| guest | 0 | guest |
| admin | 15 | admin |

**コマンドモード**

Global Configuration

**コマンドの使用方法**

暗号化パスワードは、システムの起動中に設定ファイルを読み込む場合や、TFTPサーバから設定ファイルをダウンロードする場合に、従来のパスワード設定(通常テキストまたは暗号化)と互換性を持たせるために必要です。 暗号化パスワードをユーザが手動で設定する必要はありません。

**例**

以下の例は、任意のユーザのアクセスレベルとパスワードの設定方法を示しています。

```
Console(config)#username bob access-level 15
Console(config)#username bob password 0 smith
Console(config)#
```

### enable password

システムに最初にログオンした後に、Privileged Execパスワードを設定する必要があります。パスワードは安全な場所に記録してください。 このコマンドは、Normal Execレベルから Privileged Execレベルへのアクセスを制御します。 デフォルトのパスワードにリセットするには**no**形式を使用します。

#### 構文

**enable password** [**level** *レベル*] {**0** | **7**} *パスワード*
**no enable password** [**level** *レベル*]

- **level** *レベル* – Privileged Execの場合はレベル15 (レベル0～14は不使用)
- {**0** | **7**} – 0は通常のパスワード、7は暗号化パスワード
- *パスワード* – この優先レベルのパスワード
  (最大設定:通常テキストは8文字、暗号化は32文字、大文字小文字を区別)

#### デフォルト設定

- デフォルトはレベル15
- デフォルトのパスワードは「super」

#### コマンドモード

Global Configuration

#### コマンドの使用方法

- ヌルパスワードを設定できません。 **enable**コマンド(p.256)を使用してコマンドモードをNormal ExecからPrivileged Execに変更するには、パスワードを入力する必要があります。
- 暗号化パスワードは、システムの起動中に設定ファイルを読み込む場合や、TFTPサーバから設定ファイルをダウンロードする場合に、従来のパスワード設定(通常テキストまたは暗号化)と互換性を持たせるために必要です。 暗号化パスワードをユーザが手動で設定する必要はありません。

#### 例

```
Console(config)#enable password level 15 0 admin
Console(config)#
```

#### 関連コマンド

enable (p.256)
authentication enable (p.322)

## IPフィルタコマンド

表 4-11　IPフィルタコマンド

| コマンド | 機能 | モード | ページ |
|---|---|---|---|
| management | 管理アクセスが可能なIPアドレスを設定 | GC | 267 |
| show management | ブラウザから監視または設定するスイッチを表示 | PE | 268 |

### management

様々なプロトコル経由で本製品への管理アクセスが許可されているクライアントIPアドレスを指定します。 デフォルト設定を復元するには**no**形式を使用します。

#### 構文

[**no**] **management** {**all-client** | **http-client** | **snmp-client** | **telnet-client**} *開始アドレス* [*終了アドレス*]

- **all-client** －IPアドレスをSNMP、WebおよびTelnetグループに追加
- **http-client** －IPアドレスをWebグループに追加
- **snmp-client** －IPアドレスをSNMPグループに追加
- **telnet-client** －IPアドレスをTelnetグループに追加
- *開始アドレス* － 単一のIPアドレス、または任意の範囲の開始アドレス
- *終了アドレス* － 任意の範囲の終了アドレス

#### デフォルト設定

全アドレス

#### コマンドモード

Global Configuration

#### コマンドの使用方法

- ・何者かが無効なアドレスから本製品の管理インタフェースにアクセスしようとすると、本製品は接続を拒否し、システムログにイベントメッセージを入力して、トラップマネージャにトラップメッセージを送信します。
- IPアドレスは、SNMP、Web、Telnetアクセス用にそれぞれ設定できます。 これらのグループにはそれぞれ、個々のアドレスまたはアドレスの範囲を5セットまで含めることができます。
- 同じグループ(SNMP、Web、Telnetのいずれか)のアドレスを入力する場合、本製品では、重複するアドレス範囲を受け入れられません。 異なる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。
- 指定した範囲から個々のアドレスを削除することはできません。 該当する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。
- 開始アドレスのみを指定、または開始アドレスと終了アドレスの両方を指定すると、

アドレス範囲を削除できます。

**例**

以下の例では、管理アクセスを指定したアドレスに制限します。

```
Console(config)#management all-client 192.168.1.19
Console(config)#management all-client 192.168.1.25 192.168.1.30
Console(config)#
```

### show management

様々なプロトコル経由での本製品への管理アクセスが許可されているクライアントIPアドレスを表示します。

**構文**

**show management** {**all-client** | **http-client** | **snmp-client** | **telnet-client**}

- **all-client** – IPアドレスをSNMP、WebおよびTelnetグループに追加
- **http-client** – IPアドレスをWebグループに追加
- **snmp-client** – IPアドレスをSNMPグループに追加
- **telnet-client** – IPアドレスをTelnetグループに追加

**コマンドモード**

Privileged Exec

**例**

```
Console#show management all-client
Management IP Filter
 HTTP-Client:
    Start IP address         End IP address
-------------------------------------------------
1. 192.168.1.19              192.168.1.19
2. 192.168.1.25              192.168.1.30

 SNMP-Client:
    Start IP address         End IP address
-------------------------------------------------
1. 192.168.1.19              192.168.1.19
2. 192.168.1.25              192.168.1.30

 TELNET-Client:
    Start IP address         End IP address
-------------------------------------------------
1. 192.168.1.19              192.168.1.19
2. 192.168.1.25              192.168.1.30

Console#
```

## Webサーバコマンド

表 4-12　Webサーバコマンド

| コマンド | 機能 | モード | ページ |
|---|---|---|---|
| ip http port | Webブラウザインタフェースで使用するポートを指定 | GC | 269 |
| ip http server | ブラウザからのスイッチの監視または設定を許可 | GC | 269 |
| ip http secure-server | 暗号化通信用にHTTPS/SSLを有効化 | GC | 270 |
| ip http secure-port | HTTPS/SSL用のUDPポート番号を指定 | GC | 271 |

### ip http port

Webブラウザインタフェースで使用するTCPポート番号を指定します。 デフォルトのポートを使用するにはno形式を使用します。

#### 構文

**ip http port** *ポート番号*
**no ip http port**

*ポート番号* - ブラウザインタフェースで使用するTCPポート（範囲：1～65535）

#### デフォルト設定

80

#### コマンドモード

Global Configuration

#### 例

```
Console(config)#ip http port 769
Console(config)#
```

#### 関連コマンド

ip http server (p.269)

### ip http server

本製品をブラウザから監視または設定できるようにします。 この機能を無効にするにはno形式を使用します。

**構文**

[no] ip http server

**デフォルト設定**

有効

**コマンドモード**

Global Configuration

**例**

```
Console(config)#ip http server
Console(config)#
```

**関連コマンド**

ip http port (p.269)

### ip http secure-server

Secure Socket Layer (SSL)経由のハイパーテキスト転送プロトコル(HTTPS)を有効にし、本製品のWebインタフェースにセキュアアクセス(暗号化接続)できます。 この機能を無効にするにはno形式を使用します。

**構文**

[no] ip http secure-server

**デフォルト設定**

有効

**コマンドモード**

Global Configuration

**コマンドの使用方法**

- 本製品では、HTTPサービスとHTTPSサービスの両方を個別に有効にできます。ただし、HTTPサーバとHTTPSサーバを、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。
- HTTPSを有効にする場合、ブラウザで指定するURLで以下のように示す必要があります。 https://*機器*[:*ポート番号*]
- HTTPSを起動すると、接続は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のネゴシエーションを行います。
  - クライアントとサーバが、データの暗号化および復号化に使用するセッションキ

ーを生成します。

- クライアントとサーバは、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Netscape Navigator 4.x以降のバージョンでは、ステータスバーに南京錠型のアイコンが表示されます。
- 現在、以下のWebブラウザおよびオペレーティングシステムがHTTPSに対応しています。

表 4-13　HTTPSのシステムサポート

| Webブラウザ | オペレーティングシステム |
|---|---|
| Internet Explorer 5.0以降 | Windows 98、Windows NT (サービスパック 6aを適用)、Windows 2000、Windows XP |
| Netscape Navigator 6.2以降 | Windows 98、Windows NT (サービスパック 6aを適用)、Windows 2000、Windows XP、Solaris 2.6 |

- セキュアサイト証明書を指定するには、82ページの「セキュアサイトの初期証明を置き換える」を参照してください。 また、314ページのcopyコマンドも参照してください。

**例**

```
Console(config)#ip http secure-server
Console(config)#
```

**関連コマンド**

ip http secure-port (p.271)
copy tftp https-certificate (p.314)

### ip http secure-port

本製品のWebインタフェースへのHTTPS/SSL接続に使用するUDPポート番号を指定します。 デフォルトのポートを復元するにはno形式を使用します。

**構文**

**ip http secure-port** *ポート番号*
**no ip http secure-port**

*ポート番号* - HTTPS/SSLに使用するUDPポート番号
(範囲:1～65535)

**デフォルト設定**

443

**コマンドモード**

Global Configuration

**コマンドの使用方法**

- HTTPサーバとHTTPSサーバを、同じポートを使用するように設定することはできません。
- HTTPSポート番号を変更する場合、HTTPSサーバに接続しようとするクライアントは、以下の形式でURL内にポート番号を指定する必要があります。
  **https://***機器*:*ポート番号*

**例**

```
Console(config)#ip http secure-port 1000
Console(config)#
```

**関連コマンド**

ip http secure-server (p.270)

## Telnetサーバコマンド

表 4-14　Telnetサーバコマンド

| コマンド | 機能 | モード | ページ |
|---|---|---|---|
| ip telnet port | Telnetインタフェースで使用するポートを指定 | GC | 273 |
| ip telnet server | Telnetからのスイッチの監視または設定を許可 | GC | 273 |

### ip telnet port

Telnetインタフェースで使用するTCPポート番号を指定します。 デフォルトのポートを使用するには**no**形式を使用します。

#### 構文

**ip telnet port** *ポート番号*
**no ip telnet port**

*ポート番号* - ブラウザインタフェースで使用するTCPポート (範囲:1～65535)

#### デフォルト設定

23

#### コマンドモード

Global Configuration

#### 例

```
Console(config)#ip telnet port 123
Console(config)#
```

#### 関連コマンド

ip telnet server (p.273)

### ip telnet server

本製品をTelnetから監視または設定できるようにします。 この機能を無効にするには**no**形式を使用します。

#### 構文

[no] ip telnet server

**デフォルト設定**

有効

**コマンドモード**

Global Configuration

**例**

```
Console(config)#ip telnet server
Console(config)#
```

**関連コマンド**

ip telnet port (p.273)

## セキュアシェルコマンド

バークレ標準には、本来はUnixシステム用に設計されたリモートアクセスツールが含まれます。 これらのツールの一部は、Microsoft Windowsおよびその他の環境用にも実装されています。 これらのツールは、*rlogin* (リモートログイン)、*rsh* (リモートシェル)、*rcp* (リモートコピー)などのコマンドも含めて、悪意のある攻撃の対象となる場合があります。

セキュアシェル(SSH)には、従来のバークレリモートアクセスツールに代わるセキュアなサーバ/クライアントアプリケーションが含まれています。 SSHはまた、本製品に対してTelnetに代わる、よりセキュアなリモート管理アクセスも提供できます。 クライアントがSSHプロトコル経由で本製品に接続すると、パブリックキーが発行されます。クライアントがアクセス認証を受けるには、パブリックキーとローカルのユーザ名およびパスワードが必要です。 また、SSHは本製品とSSHが有効な管理ステーションクライアントの間でやり取りされるすべてのデータ転送を暗号化するため、ネットワーク経由で移動するデータの改ざんを防止できます。

本セクションでは、SSHサーバの設定に使用するコマンドについて解説します。 ただし、SSHプロトコルを使用して本製品を設定する場合、管理ステーションにSSHクライアントをインストールすることも必要です。

**注意:** 本製品はSSHバージョン1.5および2.0の両方に対応しています。

表 4-15　SSHコマンド

| コマンド | 機能 | モード | ページ |
|---|---|---|---|
| ip ssh server | 本製品でSSHサーバを有効化 | GC | 276 |
| ip ssh timeout | SSHサーバの認証タイムアウトを指定 | GC | 277 |
| ip ssh authentication-retries | クライアントで可能な再試行の回数を指定 | GC | 278 |

| | | | |
|---|---|---|---|
| ip ssh server-key size | SSHサーバキーサイズを設定 | GC | 278 |
| copy tftp public-key | ユーザのパブリックキーをTFTPサーバから本製品にコピー | PE | 276 |
| delete public-key | 指定したユーザのパブリックキーを削除 | PE | 279 |
| ip ssh crypto host-key generate | ホストキーを生成 | PE | 280 |
| ip ssh crypto zeroize | ホストキーをRAMから消去 | PE | 280 |
| ip ssh save host-key | ホストキーをRAMからフラッシュメモリへ保存 | PE | 281 |
| disconnect | 回線接続を停止 | PE | 254 |
| show ip ssh | SSHサーバのステータスと、認証タイムアウトおよび再試行の設定値を表示 | PE | 281 |
| show ssh | 現在のSSHセッションのステータスを表示 | PE | 282 |
| show public-key | 指定したユーザまたはホストのパブリックキーを表示 | PE | 283 |
| show users | 優先レベルおよびパブリックキーのタイプを含めてSSHユーザを表示 | PE | 311 |

本製品のSSHサーバは、パスワード認証とパブリックキー認証の両方に対応しています。SSHクライアントでパスワード認証が指定されている場合、パスワードは321ページの **authentication login**コマンドの指定に従って、ローカルで、あるいはRADIUSまたはTACACS+のリモート認証サーバ経由で認証できます。 クライアントでパブリックキー認証が指定されている場合、以降のセクションで解説するように、クライアントと本製品の両方で認証キーを設定する必要があります。 パブリックキー認証を使用するかパスワード認証を使用するかにかかわらず、本製品で認証キーを生成してSSHサーバを有効にする必要があります。

SSHサーバを使用するには、以下の手順を完了します。

1. ホストキーペアを生成する – **ip ssh crypto host-key generate**コマンドを使用して、ホストのパブリックキーとプライベートキーのペアを作成します。

2. クライアントにホストパブリックキーを提供する – 多くのSSHクライアントプログラムでは、本製品での最初の接続設定中にホストパブリックキーが自動的にインポートされます。 自動的にインポートされない場合、管理ステーションで既知のホストファイルを手動で作成して、その中にホストパブリックキーを配置する必要があります。 既知のホストファイル内のパブリックキーのエントリは、以下の例のようになります。

10.1.0.54 1024 35 156849954018676692593339467750546173253136748908365472541502024559319986854435836165199992332978176606583095610825913212890233765468017262725714134287629413011961955667821588888146206519417467729848654686157177393901647793559423035774130980227370877945452408397

17526463580581767167095748047761 17

3. クライアントのパブリックキーを本製品にインポートする – **copy tftp public-key**コマンドを使用してファイルをコピーします。ファイルは、全SSHクライアントで承認済みの、本製品への管理アクセスに使用するパブリックキーを含みます（これらのクライアントは、265ページで解説されているように、本製品の「User Accounts (ユーザアカウント)」ページを使用して、ローカルで設定する必要があります)。 その後クライアントは、これらのキーを使用して認証されます。 以下のRSAバージョン1キーの例に示すように、現在のファームウェアでは、標準のUNIX形式に基づいたパブリックキーファイルのみが受け入れられます。

1024 35 134108168560989392104094492015542534763164192187295892114317388 0555361616310517759408386863110929123222682851925437460310093718772119969631781366277414168985132049117204830339254324101637997592371449011938006090253948408482717819437228840253311595213486102290297898272135326713162943253281891504530639391664 3 steve@192.168.1.19

4. オプションのパラメータを設定する – 認証タイムアウト、再試行回数、サーバキーサイズなど、他のオプションのパラメータを設定します。

5. SSHサービスを有効にする – **ip ssh server**コマンドを使用して、本製品でSSHサーバを有効にします。

6. チャレンジレスポンス認証を設定する – SSHクライアントが本製品にアクセスしようとするとき、SSHサーバはホストキーペアを使用してセッションキーと暗号化方法のネゴシエーションを行います。 本製品に保存されているパブリックキーに対応するプライベートキーを持つクライアントのみがアクセスできます。 この処理中に、以下の情報交換が行われます。

   a. クライアントが本製品にパブリックキーを送信します。
   b. 本製品は、クライアントのパブリックキーとメモリに保存されているキーを比較します。
   c. 一致するキーが見つかった場合、本製品はそのパブリックキーを使用してランダムなバイトのシーケンスを暗号化し、この文字列をクライアントに送信します。
   d. クライアントはパブリックキーを使用してバイトを復号化し、復号化されたバイトを本製品に送信します。
   e. 本製品が、復号化されたバイトと、もともと送信したバイトを比較します。 この2つのセットが一致した場合、クライアントのプライベートキーは承認済みのパブリックキーに対応しており、クライアントは認証されます。

**注意:** SSHをパスワード認証のみで使用する場合でも、ホストパブリックキーをクライアントに提供する必要があります。これは最初の接続中に行うか、または既知のホストファイルに手動で入力します。 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。

### ip ssh server

本製品でセキュアシェル(SSH)サーバを有効にします。 このサービスを無効にするには**no**形式を使用します。

### 構文

[no] ip ssh server

### デフォルト設定

無効

### コマンドモード

Global Configuration

### コマンドの使用方法

- SSHサーバは最大4つのクライアントセッションに対応します。 クライアントセッションの最大数には、現在のTelnetセッションとSSHセッションの両方が含まれます。
- SSHは、クライアントが本製品への接続を最初に確立するときにDSAまたはRSAを使用してキー交換を行い、次にクライアントとネゴシエーション・ し、データの暗号化方法としてDES (56ビット)または3DES (168ビット)を選択します。
- ホストキーを生成してから、SSHサーバを有効にする必要があります。

### 例

```
Console#ip ssh crypto host-key generate dsa
Console#configure
Console(config)#ip ssh server
Console(config)#
```

### 関連コマンド

ip ssh crypto host-key generate (p.280)
show ssh (p.282)

## ip ssh timeout

SSHサーバのタイムアウトを設定します。 デフォルト設定を復元するにはno形式を使用します。

### 構文

**ip ssh timeout** *秒*
**no ip ssh timeout**

*秒* - SSHネゴシエーション中のクライアント応答のタイムアウト (範囲:1～120)

### デフォルト設定

10秒

### コマンドモード

Global Configuration

### コマンドの使用方法

timeoutは、SSHネゴシエーションフェーズで本製品がクライアントからの応答を待機する時間を指定します。 いったんSSHセッションが確立されると、ユーザ入力のタイムアウトは、vtyセッション用のexec-timeoutコマンドで制御されます。

### 例

```
Console(config)#ip ssh timeout 60
Console(config)#
```

### 関連コマンド

exec-timeout (p.249)
show ip ssh (4-42)

## ip ssh authentication-retries

SSHサーバがユーザの再認証を試行する回数を設定します。 デフォルト設定を復元するにはno形式を使用します。

### 構文

**ip ssh authentication-retries** *回数*
**no ip ssh authentication-retries**

*回数* - 認証試行がここで指定する回数を超えると、インタフェースをリセット（範囲：1～5）

### デフォルト設定

3

### コマンドモード

Global Configuration

### 例

```
Console(config)#ip ssh authentication-retires 2
Console(config)#
```

### 関連コマンド

show ip ssh (p.281)

## ip ssh server-key size

SSHサーバキーサイズを設定します。 デフォルト設定を復元するにはno形式を使用します。

**構文**

**ip ssh server-key size** *キーサイズ*
**no ip ssh server-key size**

*キーサイズ* - サーバキーサイズ (範囲:512～896ビット)

**デフォルト設定**

768ビット

**コマンドモード**

Global Configuration

**コマンドの使用方法**

- サーバキーは、本製品以外では共有されることのないプライベートキーです。
- ホストキーはSSHクライアントと共有され、1024ビットに固定されています。

**例**

```
Console(config)#ip ssh server-key size 512
Console(config)#
```

**delete public-key**

指定したユーザのパブリックキーを削除します。

**構文**

**delete public-key** *ユーザ名* [**dsa** | **rsa**]

- *ユーザ名* - SSHユーザの名前 (範囲:1～8文字)
- **dsa** - DSAパブリックキータイプ
- **rsa** - RSAパブリックキータイプ

**デフォルト設定**

DSAキーとRSAキーの両方を削除

**コマンドモード**

Privileged Exec

**例**

```
Console#delete public-key admin dsa
Console#
```

### ip ssh crypto host-key generate

ホストキーペア(パブリックとプライベート)を生成します。

#### 構文

ip ssh crypto host-key generate [dsa | rsa]

- **dsa** – DSA (バージョン2)キータイプ
- **rsa** – RSA (バージョン1)キータイプ

#### デフォルト設定

DSAキーとRSAキーの両方を生成

#### コマンドモード

Privileged Exec

#### コマンドの使用方法

- ホストキーペアをメモリ(RAM)に保存します。 ホストキーペアをフラッシュメモリに保存するには、**ip ssh save host-key**コマンドを使用します。
- 一部のSSHクライアントプログラムでは、設定プロセスの一環として、パブリックキーが既知のホストファイルに自動的に追加されます。 自動的に追加されない場合、既知のホストファイルを手動で作成して、その中にホストパブリックキーを配置する必要があります。
- SSHサーバは、このホストキーを使用して、接続しようとしているクライアントとの間でセッションキーと暗号化方法のネゴシエーションを行います。

#### 例

```
Console#ip ssh crypto host-key generate dsa
Console#
```

#### 関連コマンド

ip ssh crypto zeroize (p.280)
ip ssh save host-key (p.281)

### ip ssh crypto zeroize

ホストキーをメモリ(RAM)から消去します。

#### 構文

ip ssh crypto zeroize [dsa | rsa]

- **dsa** – DSAキータイプ
- **rsa** – RSAキータイプ

#### デフォルト設定

DSAキーとRSAキーの両方を消去

**コマンドモード**

Privileged Exec

**コマンドの使用方法**

- ホストキーを揮発性メモリ(RAM)から消去します。 ホストキーをフラッシュメモリから消去するには、**no ip ssh save host-key**コマンドを使用します。
- このコマンドを実行する前に、SSHサーバを無効にする必要があります。

**例**

```
Console#ip ssh crypto zeroize dsa
Console#
```

**関連コマンド**

ip ssh crypto host-key generate (p.280)
ip ssh save host-key (p.28)
no ip ssh server (p.279)

### ip ssh save host-key

ホストキーをRAMからフラッシュメモリへ保存します。

**構文**

**ip ssh save host-key** [**dsa** | **rsa**]

- **dsa** - DSAキータイプ
- **rsa** - RSAキータイプ

**デフォルト設定**

DSAキーとRSAキーの両方を保存

**コマンドモード**

Privileged Exec

**例**

```
Console#ip ssh save host-key dsa
Console#
```

**関連コマンド**

ip ssh crypto host-key generate (p.280)

### show ip ssh

SSHサーバへのクライアントアクセスを認証する際に使用する接続設定を表示します。

**コマンドモード**

Privileged Exec

**例**

```
Console#show ip ssh
SSH Enabled - version 1.99
Negotiation timeout: 120 secs; Authentication retries: 3
Server key size: 768 bits
Console#
```

### show ssh

現在のSSHサーバ接続を表示します。

**コマンドモード**

Privileged Exec

**例**

```
Console#show ssh
Connection Version State                Username   Encryption
  0          2.0     Session-Started    admin      ctos aes128-cbc-hmac-md5
                                                       stoc aes128-cbc-hmac-md5
Console#
```

表 4-16 show ssh - 表示の説明

| フィールド | 説明 |
|---|---|
| Session | セッション番号 (範囲:0～3) |
| Version | セキュアシェルのバージョン番号 |
| State | 認証ネゴシエーションの状態<br>(値:Negotiation-Started (ネゴシエーション開始)、<br>Authentication-Started (認証開始)、Session-Started (セッション開始)) |
| Username | クライアントのユーザ名 |

| | |
|---|---|
| Encryption | 暗号化方法は、クライアントとサーバの間で自動的にネゴシエーションされます。<br>SSHv1.5のオプションには、DESと3DESがあります。<br>SSHv2.0のオプションには、クライアントからサーバ(ctos)とサーバからクライアント(stoc)で、別々のアルゴリズムが含まれる場合があります。<br>aes128-cbc-hmac-sha1<br>aes192-cbc-hmac-sha1<br>aes256-cbc-hmac-sha1<br>3des-cbc-hmac-sha1<br>blowfish-cbc-hmac-sha1<br>aes128-cbc-hmac-md5<br>aes192-cbc-hmac-md5<br>aes256-cbc-hmac-md5<br>3des-cbc-hmac-md5<br>blowfish-cbc-hmac-md5<br><br>*用語:*<br>DES -データ暗号化規格(56ビットキー)<br>3DES -トリプルDES (DESを3回繰り返して使用、112ビットキー)<br>aes - Advanced Encryption Standard (160または224ビットキー)<br>blowfish - Blowfish (32～448ビットキー)<br>cbc - 暗号ブロック連鎖方式<br>sha1 - Secure Hash Algorithm 1 (160ビットハッシュ)<br>md5 - Message Digestアルゴリズム第5番(128ビットハッシュ) |

### show public-key

指定したユーザまたはホストのパブリックキーを表示します。

#### 構文

**show public-key** [**user** [*ユーザ名*]| **host**]

*ユーザ名* - SSHユーザの名前 (範囲:1～8文字)

#### デフォルト設定

すべてのパブリックキーを表示

#### コマンドモード

Privileged Exec

#### コマンドの使用方法

- パラメータをまったく入力しない場合は、すべてのキーが表示されます。 userキーワードを入力してユーザ名を指定しない場合は、すべてのユーザのパブリックキーが表示されます。

・ RSAキーが表示されているとき、最初のフィールドはホストキーのサイズ(例:1024)、2番目のフィールドはエンコードされたパブリック指数(例:35)、最後の文字列はエンコードされた係数を示します。 DSAキーが表示されているとき、最初のフィールドはSSHで使用されている暗号化方法が・ DSS (デジタル署名標準)に基づいていることを示し、最後の文字列はエンコードされた係数を示します。

**例**

```
Console#show public-key host
Host:
RSA:
1024 35
156849954018676692593339467750546173253136748908365472541502024559319986854435836165199992332978176606583095861082591321289023376546801726272571413428762941301196195566782595664104869574278881462065194174677298486546861571773939016477935594230357741309802273708779454524083971752646358058176716709574804776117
DSA:
ssh-dss AAAB3NzaC1kc3MAAACBAPWKZTPbsRlB8ydEXcxM3dyV/yrDbKStIlnzD/Dg0h2Hxc
YV44sXZ2JXhamLK6P8bvuiyacWbUW/a4PAtp1KMSdqsKeh3hKoA3vRRSy1N2XFfAKxl5fwFfv
JlPdOkFgzLGMinvSNYQwiQXbKTBH0Z4mUZpE85PWxDZMaCNBPjBrRAAAAFQChb4vsdfQGNIjwbvwrN
LaQ77isiwAAAIEAsy5YWDC99ebYHNRj5kh47wY4i8cZvH+/p9cnrfwFTMU01VFDly3IR
2G395NLy5Qd7ZDxfA9mCOfT/yyEfbobMJZi8oGCstSNOxrZZVnMqWrTYfdrKX7YKBw/Kjw6Bm
iFq7O+jAhf1Dg45loAc27s6TLdtny1wRq/ow2eTCD5nekAAACBAJ8rMccXTxHLFAczWS7EjOy
DbsloBfPuSAb4oAsyjKXKVYNLQkTLZfcFRu41bS2KV5LAwecsigF/+DjKGWtPNIQqabKgYCw2
o/dVzX4Gg+yqdTlYmGA7fHGm8ARGeiG4ssFKy4Z6DmYPXFum1Yg0fhLwuHpOSKdxT3kk475S7 w0W
Console#
```

## イベントログコマンド

表 4-17 イベントログコマンド

| コマンド | 機能 | モード | ページ |
|---|---|---|---|
| logging on | エラーメッセージのログを制御 | GC | 285 |
| logging history | スイッチメモリに保存されるsyslogメッセージを重要度に基づいて制限 | GC | 287 |
| logging host | ログメッセージを受信するsyslogサーバのホストIPアドレスを追加 | GC | 289 |
| logging facility | syslogメッセージのリモートログ用のFacilityタイプを設定 | GC | 289 |
| logging trap | リモートサーバに保存されるsyslogメッセージを重要度に基づいて制限 | GC | 290 |
| clear logging | ログバッファからメッセージを消去 | PE | 290 |
| show logging | ログの状態を表示 | PE | 291 |
| show log | ログメッセージを表示 | PE | 291 |

### logging on

エラーメッセージのログを制御して、デバッグメッセージまたはエラーメッセージをスイッチメモリに送信します。 **no**形式を使用するとログプロセスが無効になります。

#### 構文

[no] **logging on**

#### デフォルト設定

なし

#### コマンドモード

Global Configuration

#### コマンドの使用方法

ログプロセスは、スイッチメモリに保存されるエラーメッセージを制御します。 **logging history**コマンドを使用すると、保存されるエラーメッセージのタイプを制御できます。

**例**

```
Console(config)#logging on
Console(config)#
```

**関連コマンド**

logging history (p.287)
clear logging (p.290)

### logging history

スイッチメモリに保存されるsyslogメッセージを重要度に基づいて制限します。 no形式を使用すると、syslogメッセージのログがデフォルトレベルに戻ります。

### 構文

**logging history** {**flash** | **ram**} *レベル*
**no logging history** {**flash** | **ram**}

- **flash** – イベント履歴をフラッシュメモリ(固定メモリ)に保存
- **ram** – イベント履歴を一時RAM (電源リセット時に消去されるメモリ)に保存
- *レベル* – 以下のいずれかのレベル。 送信されるメッセージには、レベル0までのうち選択されたレベルが含まれます(範囲:0～7)。

表 4-18 ログレベル

| レベル | 重要度 | 説明 |
|---|---|---|
| 7 | debugging (デバッグ) | デバッグメッセージ |
| 6 | informational (情報) | 情報メッセージのみ |
| 5 | notifications (通知) | コールドスタートなど、正常であるものの注意が必要な状態 |
| 4 | warnings (警告) | 警告状態 (応答失敗、予期せぬ応答など) |
| 3 | errors (エラー) | エラー状態 (無効な入力、デフォルトの使用など) |
| 2 | critical (重大) | 重大な状況(メモリ割り当てや空きメモリのエラー、リソース不足など) |
| 1 | alerts (緊急) | ただちに対応が必要 |
| 0 | Emergencies (非常事態) | システム使用不可 |

** 現在リリースされているファームウェアでは、レベル2、5、6のエラーメッセージのみが使用されています。*

### デフォルト設定

Flash: errors (レベル3～0)
RAM: warnings (レベル6～0)

### コマンドモード

Global Configuration

**コマンドの使用方法**

フラッシュメモリ用に指定するメッセージレベルは、RAM用に指定するレベルより重要度を高く(数値を小さく)する必要があります。

**例**

```
Console(config)#logging history ram 0
Console(config)#
```

### logging host

ログメッセージを受信するsyslogサーバのホストIPアドレスを追加します。 syslogサーバホストを削除するには**no**形式を使用します。

#### 構文

[**no**] **logging host** *ホストIPアドレス*

*ホストIPアドレス* – syslogサーバのIPアドレス

#### デフォルト設定

なし

#### コマンドモード

Global Configuration

#### コマンドの使用方法

- このコマンドを複数回使用すると、ホストIPアドレスのリストを作成できます。
- 指定可能なホストIPアドレスは最大5つです。

#### 例

```
Console(config)#logging host 10.1.0.3
Console(config)#
```

### logging facility

syslogメッセージのリモートログ用のFacilityタイプを設定します。 デフォルトのタイプに戻すには**no**形式を使用します。

#### 構文

[**no**] **logging facility** *タイプ*

*タイプ* – syslogサーバでログメッセージを適切なサービスに送信するために使用するFacilityを示す数値（範囲：16～23）

#### デフォルト設定

23

#### コマンドモード

Global Configuration

#### コマンドの使用方法

syslogメッセージで送信するFacilityタイプタグを指定します（RFC 3164を参照）。このタイプは、本製品で報告されるメッセージの種類には影響しません。 ただし、

syslogサーバでのメッセージの並べ替えや、対応するデータベースでのメッセージの保存に使用される場合があります。

**例**

```
Console(config)#logging facility 19
Console(config)#
```

### logging trap

リモートサーバへのシステムメッセージのログ出力を有効にするか、リモートサーバに保存されるsyslogメッセージを重要度に基づいて制限します。 リモートログを有効にするには、レベルを指定せずにこのコマンドを使用します。 リモートログを無効にするにはno形式を使用します。

**構文**

**logging trap** [*レベル*]
**no logging trap**

*レベル* – 以下のいずれかのレベル引数。 送信されるメッセージには、レベル0までのうち選択されたレベルが含まれます(287ページの表を参照)。

**デフォルト設定**

- 有効
- レベル6～0

**コマンドモード**

Global Configuration

**コマンドの使用方法**

- レベルを指定してこのコマンドを使用すると、リモートログが有効になり、保存する最低の重要度レベルが設定されます。
- レベルを指定せずにこのコマンドを使用しても、リモートログは有効になりますが、最低の重要度レベルがデフォルトに復元されます。

**例**

```
Console(config)#logging trap 4
Console(config)#
```

### clear logging

ログバッファからメッセージを消去します。

### 構文

clear logging [flash | ram]

- flash – イベント履歴をフラッシュメモリ(固定メモリ)に保存
- ram – イベント履歴を一時RAM (電源リセット時に消去されるメモリ)に保存

### デフォルト設定

フラッシュおよびRAM

### コマンドモード

Privileged Exec

### 例

```
Console#clear logging
Console#
```

### 関連コマンド

show logging (p.291)

## show logging

ローカルスイッチメモリ、SMTPイベントハンドラ、リモートsyslogサーバのいずれかにメッセージをログ出力するための設定を表示します。

### 構文

show logging {flash | ram | sendmail | trap}

- flash – イベントメッセージをフラッシュメモリに保存するための設定を表示 (固定メモリ)
- ram – イベントメッセージを一時RAMに保存するための設定を表示 (電源リセット時に消去されるメモリ)
- sendmail – SMTPイベントハンドラの設定を表示(299ページ)
- trap – トラップ機能の設定を表示

### デフォルト設定

なし

### コマンドモード

Privileged Exec

### 例

以下の例は、システムログが有効で、フラッシュメモリのメッセージレベルが「errors」(デフォルトレベル3～0)、RAMのメッセージレベルが「debugging」(デフォルトレベル7～0)の場合を示しています。

```
Console#show logging flash
Syslog logging:                 Enabled
History logging in FLASH: level errors
Console#show logging ram
Syslog logging:                 Enabled
History logging in RAM: level debugging
Console#
```

表 4-19　show logging flash/ram – 表示の説明

| フィールド | 説明 |
|---|---|
| Syslog logging | **logging on**コマンドでシステムログが有効になっているかどうかを表示 |
| History logging in FLASH | **logging history**コマンドに基づいて報告されるメッセージレベル |
| History logging in RAM | **logging history**コマンドに基づいて報告されるメッセージレベル |

以下の例では、トラップ機能の設定が表示されます。

```
Console#show logging trap
Syslog logging: Enable
REMOTELOG status: disable
REMOTELOG facility type: local use 7
REMOTELOG level type: Debugging messages
REMOTELOG server IP address: 1.2.3.4
REMOTELOG server IP address: 0.0.0.0
REMOTELOG server IP address: 0.0.0.0
REMOTELOG server IP address: 0.0.0.0
REMOTELOG server IP address: 0.0.0.0
Console#
```

**表 4-20 show logging trap – 表示の説明**

| フィールド | 説明 |
|---|---|
| Syslog logging | **logging on**コマンドでシステムログが有効になっているかどうかを表示 |
| REMOTELOG status | **logging trap**コマンドでリモートログが有効になっているかどうかを表示 |
| REMOTELOG facility type | **logging facility**コマンドで指定されている、syslogメッセージのリモートログ用のFacilityタイプ |
| REMOTELOG level type | **logging trap**コマンドで指定されている、リモートサーバへ送信されるsyslogメッセージの重要度のしきい値 |

| | |
|---|---|
| REMOTELOG server IP address | **logging host**コマンドで指定されている、syslogサーバのアドレス |

**関連コマンド**

show logging sendmail (p.297)

### show log

メモリに保存されているシステムメッセージおよびイベントメッセージを表示します。

**構文**

**show log** {**flash** | **ram**} [**login**] [**tail**]

- **flash** - イベント履歴をフラッシュメモリ(固定メモリ)に保存
- **ram** - イベント履歴を一時RAM (電源リセット時に消去されるメモリ)に保存
- **tail** - イベント履歴を最新のエントリから順に表示
- **login** - ログインレコードのみを表示

**デフォルト設定**

なし

**コマンドモード**

Privileged Exec

**コマンドの使用方法**

メモリに保存されているシステムメッセージおよびイベントメッセージを表示します。これには、タイムスタンプ、メッセージレベル(287ページ)、プログラムモジュール、関数、イベント番号などが含まれます。

**例**

以下の例は、RAMに保存されているサンプルメッセージを示しています。

```
Console#show log ram
[5] 00:01:06 2001-01-01
    "STA root change notification."
    level: 6, module: 6, function: 1, and event no.: 1
[4] 00:01:00 2001-01-01
    "STA root change notification."
    level: 6, module: 6, function: 1, and event no.: 1
[3] 00:00:54 2001-01-01
    "STA root change notification."
    level: 6, module: 6, function: 1, and event no.: 1
[2] 00:00:50 2001-01-01
    "STA topology change notification."
    level: 6, module: 6, function: 1, and event no.: 1
[1] 00:00:48 2001-01-01
    "VLAN 1 link-up notification."
```

```
    level: 6, module: 6, function: 1, and event no.: 1
Console#
```

## SMTP警告コマンド

以下のコマンドでは、SMTPイベントの処理と、指定したSMTPサーバおよびE-mail受信者に対する警告メッセージの転送を設定します。

表 4-21 SMTP警告コマンド

| コマンド | 機能 | モード | ページ |
|---|---|---|---|
| logging sendmail host | 警告メッセージを受信するSMTPサーバ | GC | 294 |
| logging sendmail level | 警告メッセージの起動に使用する重要度のしきい値 | GC | 295 |
| logging sendmail source-email | 警告メッセージの「From (差出人)」フィールドに使用するE-mailアドレス | GC | 296 |
| logging sendmail destination-email | 警告メッセージのE-mail受信者 | GC | 296 |
| logging sendmail | SMTPイベント処理を有効化 | GC | 297 |
| show logging sendmail | SMTPイベントハンドラの設定を表示 | NE、PE | 297 |

### logging sendmail host

警告メッセージの送信先となるSMTPサーバを指定します。 SMTPサーバを削除するには**no**形式を使用します。

#### 構文

[no] logging sendmail host *IPアドレス*

*IPアドレス* - イベント処理の警告メッセージの送信先となるSMTPサーバのIPアドレス

#### デフォルト設定

なし

#### コマンドモード

Global Configuration

**コマンドの使用方法**

- イベント処理用に、SMTPサーバを3台まで指定できます。 ただし、サーバごとに別々のコマンドを入力して指定する必要があります。
- E-mail警告を送信する際、本製品はまず接続を開き、キューで待機しているすべてのE-mail警告を1つずつ送信して、最後に接続を閉じます。
- 接続を開く際、本製品はまず前回の接続で正常にメールを送信したサーバ、またはこのコマンドで最初に設定されているサーバを選択します。 メールの送信が失敗した場合は、リスト内の次のサーバを選択し、再度メール送信を試みます。 それでも失敗する場合は、この処理が一定の間隔で繰り返されます (接続を正常に開くことができない場合は、トラップが起動されます)。

**例**

```
Console(config)#logging sendmail host 192.168.1.200
Console(config)#
```

### logging sendmail level

警告メッセージの起動に使用する重要度のしきい値を設定します。

**構文**

logging sendmail level *レベル*

*レベル* - いずれかのシステムメッセージレベル(287ページ)。 送信されるメッセージには、レベル0までのうち選択されたレベルが含まれます(範囲:0～7、デフォルト:7)。

**デフォルト設定**

レベル7

**コマンドモード**

Global Configuration

**コマンドの使用方法**

指定したレベルは、イベントのしきい値を示します。 このレベル以上のイベントはすべて、設定されているE-mail受信者に送信されます (たとえば、レベル7を使用すると、レベル7からレベル0までのすべてのイベントが報告されます)。

**例**

以下の例では、レベル4～0のシステムエラーに関してE-mail警告が送信されます。

```
Console(config)#logging sendmail level 4
Console(config)#
```

### logging sendmail source-email

警告メッセージの「From (差出人)」フィールドに使用するE-mailアドレスを設定します。 送信元のE-mailアドレスを削除するには**no**形式を使用します。

#### 構文

[no] logging sendmail source-email *E-mailアドレス*

*E-mailアドレス* - 警告メッセージで使用する送信元のE-mailアドレス (範囲:0～41文字)

#### デフォルト設定

なし

#### コマンドモード

Global Configuration

#### コマンドの使用方法

装置を識別するシンボリックなE-mailアドレス、または装置の管理担当者のアドレスを使用できます。

#### 例

以下の例では、送信元のE-mailアドレスがjohn@acme.comに設定されます。

```
Console(config)#logging sendmail source-email john@acme.com
Console(config)#
```

### logging sendmail destination-email

警告メッセージのE-mail受信者を指定します。 受信者を削除するには**no**形式を使用します。

#### 構文

[no] logging sendmail destination-email *E-mailアドレス*

*E-mailアドレス* - 警告メッセージで使用する送信先のE-mailアドレス (範囲:1～41文字)

#### デフォルト設定

なし

#### コマンドモード

Global Configuration

#### コマンドの使用方法

警告メッセージ用に、受信者を5人まで指定できます。 ただし、受信者ごとに別々の

コマンドを入力して指定する必要があります。

**例**

```
Console(config)#logging sendmail destination-email ted@this-company.com
Console(config)#
```

### logging sendmail

SMTPイベント処理を有効にします。 この機能を無効にするにはno形式を使用します。

**構文**

[no] logging sendmail

**デフォルト設定**

有効

**コマンドモード**

Global Configuration

**例**

```
Console(config)#logging sendmail
Console(config)#
```

### show logging sendmail

SMTPイベントハンドラの設定を表示します。

**コマンドモード**

Normal Exec、Privileged Exec

**例**

```
Console#show logging sendmail
SMTP servers
-----------------------------------------------
   1. 192.168.1.200

SMTP minimum severity level: 4

SMTP destination email addresses
-----------------------------------------------
   1. geoff@acme.com

SMTP source email address:     john@acme.com

SMTP status:                   Enabled
Console#
```

## 時刻コマンド

一連の指定されている時刻サーバ(NTPまたはSNTP)をポーリングすることにより、システムクロックを動的に設定できます。 本製品上の時間を正確に保つと、システムログに正確な日時でイベントエントリを記録できます。 システムクロックを設定しない場合は、最後に起動したときに設定された、出荷時のデフォルトの時刻のみが記録されます。

表 4-22 時刻コマンド

| コマンド | 機能 | モード | ページ |
|---|---|---|---|
| sntp client | 指定した時刻サーバの時間を使用 | GC | 299 |
| sntp server | 1台以上の時刻サーバを指定 | GC | 300 |
| sntp poll | クライアントが時刻取得のためのポーリング間隔を設定 | GC | 301 |
| show sntp | 現在のSNTP設定を表示 | NE、PE | 301 |
| clock timezone | 本製品の内部クロックのタイムゾーンを設定 | GC | 302 |
| calendar set | システム日時を設定 | PE | 303 |
| show calendar | 現在の日時設定を表示 | NE、PE | 303 |

### sntp client

SNTPクライアントの、**sntp servers**コマンドで指定されているNTPまたはSNTPサーバとの時刻同期要求を有効にします。 SNTPクライアントの要求を無効にするには**no**形式を使用します。

#### 構文

[no] sntp client

#### デフォルト設定

無効

#### コマンドモード

Global Configuration

#### コマンドの使用方法

- 時刻サーバから取得した時間を使用すると、ログイベントの日時が正確に記録されます。 SNTPを使用しない場合、出荷時のデフォルト(2001年1月1日00:00:00)から始まる時間のみが記録されます。

・ このコマンドは、**sntp servers**コマンドで指定されている時刻サーバに対するクライアントの時刻要求を有効にします。 **sntp poll**コマンドで指定されている間隔に基づいて、時刻同期要求を発行します。

**例**

```
Console(config)#sntp server 10.1.0.19
Console(config)#sntp poll 60
Console(config)#sntp client
Console(config)#end
Console#show sntp
Current time:   Dec 23 02:52:44 2002
Poll interval: 60
Current mode: unicast
SNTP status: Enabled
SNTP server: 10.1.0.19 0.0.0.0 0.0.0.0
Current server: 10.1.0.19
Console#
```

**関連コマンド**

sntp server (p.300)
sntp poll (p.300)
show sntp (p.301)

### sntp server

SNTP時刻要求の発行対象となるサーバのIPアドレスを設定します。 このコマンドを引数なしで使用すると、すべての時刻サーバが現在のリストから消去されます。

**構文**

**sntp server** [*ip1* [*ip2* [*ip3*]]]

*ip* - 時間確認用サーバのIPアドレス(NTPまたはSNTP)
(範囲:1～3アドレス)

**デフォルト設定**

なし

**コマンドモード**

Global Configuration

**コマンドの使用方法**

SNTPクライアントモードに設定されているときに、本製品が時刻更新のためのポーリングを行う時刻サーバを指定します。 クライアントは、応答を受信するまで、指定されている順序で時刻サーバをポーリングします。 **sntp poll**コマンドで指定されている間隔に基づいて、時刻同期要求を発行します。

**例**

```
Console(config)#sntp server 10.1.0.19
```

**関連コマンド**

sntp client (p.299)
sntp poll (p.301)
show sntp (p.301)

### sntp poll

本製品がSNTPクライアントモードに設定されているときに、時間要求を送信する間隔を設定します。 デフォルトを復元するには**no**形式を使用します。

**構文**

**sntp poll** *秒*
**no sntp poll**

*秒* - 時刻要求の間隔 (範囲:16～16384秒)

**デフォルト設定**

16秒

**コマンドモード**

Global Configuration

**例**

```
Console(config)#sntp poll 60
Console(config)#
```

**関連コマンド**

sntp client (p.299)

### show sntp

SNTPクライアントの現在の時刻および設定を表示し、ローカル時刻が適切に更新されているかどうかを示します。

**コマンドモード**

Normal Exec、Privileged Exec

**コマンドの使用方法**

現在の時刻、時刻同期要求を送信するポーリング間隔、現在のSNTPモード(ユニキ

ャストなど)を表示します。

**例**

```
Console#show sntp
Current time:   Dec 23 05:13:28 2002
Poll interval: 16
Current mode:   unicast
SNTP status : Enabled
SNTP server 137.92.140.80 0.0.0.0 0.0.0.0
Current server: 137.92.140.80
Console#
```

### clock timezone

本製品の内部クロックのタイムゾーンを設定します。

**構文**

clock timezone *名前* hour *時間* minute *分* {before-utc | after-utc}

- *名前* - タイムゾーンの名前、通常は頭字語 (範囲:1～29文字)
- *時間* - UTCとの時差(時間単位) (範囲:0～12時間)
- *分* - UTCとの時差(分単位) (範囲:0～59分)
- before-utc - ローカルのタイムゾーンをUTCより前(東)に設定
- after-utc - ローカルのタイムゾーンをUTCより後(西)に設定

**デフォルト設定**

なし

**コマンドモード**

Global Configuration

**コマンドの使用方法**

ローカルのタイムゾーンを、地球の子午線、経度ゼロ度に基づいて、協定世界時(UTC、旧称はグリニッジ標準時(GMT))との相対的な時間で設定します。 ローカル時間に対応する時刻を表示するには、現在のタイムゾーンがUTCより何時間何分東(前)か西(後)かを指定する必要があります。

**例**

```
Console(config)#clock timezone Japan hours 8 minute 0 after-UTC
Console(config)#
```

### 関連コマンド

show sntp (p.303)

## calendar set

システムクロックを設定します。 ネットワーク上に時刻確認用サーバがない場合や、時刻サーバから信号を受信するように本製品を設定していない場合に使用できます。

### 構文

**calendar set** *時間 分 秒* {*日 月 年* | *月 日 年*}

- *時間* - 時間を24時間形式で指定 (範囲:0～23)
- *分* - 分 (範囲:0～59)
- *秒* - 秒 (範囲:0～59)
- *日* - 日 (範囲:1～31)
- *月* - **january** | **february** | **march** | **april** | **may** | **june** | **july** | **august** | **september** | **october** | **november** | **december**
- *年* - 年を4桁で指定 (範囲:2001～2100)

### デフォルト設定

なし

### コマンドモード

Privileged Exec

### 例

以下の例は、システムクロックを2004年4月1日15:12:34に設定する方法を示しています。

```
Console#calendar set 15 12 34 1 April 2004
Console#
```

## show calendar

システムクロックを表示します。

### デフォルト設定

なし

### コマンドモード

Normal Exec、Privileged Exec

**例**

```
Console#show calendar
  15:12:43 April 1 2004
Console#
```

## システムステータスコマンド

表 4-23 システムステータスコマンド

| コマンド | 機能 | モード | ページ |
|---|---|---|---|
| light unit | フロントパネルのLEDインジケータを使用してスイッチのユニットIDを表示 | NE、PE | 304 |
| show startup-config | システムの起動に使用する設定ファイル(フラッシュメモリに保存)の内容を表示 | PE | 305 |
| show running-config | 現在使用中の設定データを表示 | PE | 307 |
| show system | システム情報を表示 | NE、PE | 310 |
| show users | ユーザ名、アイドル時間、TelnetクライアントのIPアドレスを含め、アクティブなコンソールおよびTelnetセッションをすべて表示 | NE、PE | 311 |
| show version | システムのバージョン情報を表示 | NE、PE | 311 |

### light unit

フロントパネルのLEDインジケータを使用してスイッチのユニットIDを表示します。

**構文**

**light unit** [ユニット]

ユニット - スイッチスタック内の、パネルのLEDを点灯するユニットを指定

**デフォルト設定**

なし

**コマンドモード**

Normal Exec、Privileged Exec

### コマンドの使用方法

ユニットIDは、ポート1～8のポートステータスLEDインジケータを使用して表示されます。 **light unit**コマンドを入力すると、スイッチのIDに対応するLEDが約15秒間点滅します。

### 例

```
Console#light unit 1
Console#
```

## show startup-config

システムの起動に使用する、不揮発性メモリに保存されている設定ファイルを表示します。

### デフォルト設定

なし

### コマンドモード

Privileged Exec

### コマンドの使用方法

- このコマンドを**show running-config**コマンドと組み合わせて使用すると、実行中のメモリ内の情報と不揮発性メモリに保存されている情報を比較できます。
- このコマンドは、主なコマンドモードの設定を表示します。 各モードグループは「!」で区切られ、設定モードコマンド、および対応するコマンドが含まれます。 以下の情報が表示されます。
  - SNMPコミュニティ文字列
  - ユーザ(名前およびアクセスレベル)
  - VLANデータベース(VLAN ID、名前および状態)
  - 各インタフェース用のVLAN設定
  - スイッチに設定されているIPアドレス
  - スパニングツリーの設定
  - コンソールポートおよびTelnet用の設定

**例**

```
Console#show startup-config
building startup-config, please wait.....
!
!
username admin access-level 15
username admin password 0 admin
!
username guest access-level 0
username guest password 0 guest
!
enable password level 15 0 super
!
snmp-server community public ro
snmp-server community private rw
!
logging history ram 6
logging history flash 3
!
vlan database
 vlan 1 name DefaultVlan media ethernet state active
!
interface ethernet 1/1
 switchport allowed vlan add 1 untagged
 switchport native vlan 1
.
.
.
interface vlan 1
 ip address dhcp
!
line console
!
line vty
!
end


Console#
```

**関連コマンド**

show running-config (p.307)

### show running-config

現在使用中の設定情報を表示します。

#### デフォルト設定

なし

#### コマンドモード

Privileged Exec

#### コマンドの使用方法

- このコマンドを**show startup-config**コマンドと組み合わせて使用すると、実行中のメモリ内の情報と不揮発性メモリに保存されている情報を比較できます。
- このコマンドは、主なコマンドモードの設定を表示します。 各モードグループは「!」で区切られ、設定モードコマンド、および対応するコマンドが含まれます。 以下の情報が表示されます。
  - スタック内の各スイッチのMACアドレス
  - SNTPサーバの設定
  - SNMPコミュニティ文字列
  - ユーザ(名前、アクセスレベル、および暗号化パスワード)
  - イベントログの設定
  - VLANデータベース(VLAN ID、名前および状態)
  - 各インタフェース用のVLAN設定
  - スイッチに設定されているIPアドレス
  - レイヤ4優先度設定
  - コンソールポートおよびTelnet用の設定

**例**

```
Console#show running-config
building running-config, please wait.....
!
phymap 00-90-cc-55-44-32 00-00-00-00-00-00 00-00-00-00-00-00 00-00-00-00-00-00
00-00-00-00-00-00 00-00-00-00-00-00 00-00-00-00-00-00 00-00-00-00-00-00
!
SNTP server 0.0.0.0 0.0.0.0 0.0.0.0
!
!
!
SNMP-server community private rw
SNMP-server community public ro
!
!
username admin access-level 15
username admin password 7 21232f297a57a5a743894a0e4a801fc3
username guest access-level 0
username guest password 7 084e0343a0486ff05530df6c705c8bb4
enable password level 15 7 1b3231655cebb7a1f783eddf27d254ca
!
!
logging history ram 6
logging history flash 3
!
vlan database
 vlan 1 name DefaultVlan media ethernet state active
!
!
interface ethernet 1/1
 switchport allowed vlan add 1 untagged
 switchport native vlan 1
.
.
.
!
interface vlan 1
 ip address DHCP
!
!
no map IP precedence
no map IP DSCP
!
!
line console
!
line vty
!
end
!
Console#
```

**関連コマンド**

show startup-config (p.305)

### show system

システム情報を表示します。

### デフォルト設定

なし

### コマンドモード

Normal Exec、Privileged Exec

### コマンドの使用方法

- このコマンドで表示される項目の詳細については、32ページの「システム情報を表示する」を参照してください。
- POSTの結果(POST result)はすべて「PASS」と表示されます。 POSTテストのいずれかが「FAIL」と表示される場合は、サポートセンターに連絡してください。

### 例

```
Console#show system
System description: SF-0224FS Layer2 Stackable Intelligent Switch
System OID string: 1.3.6.1.4.1.4537.66
System information
 System Up time:            0 days, 0 hours, 0 minutes, and 7.18 seconds
 System Name:                [NONE]
 System Location:           [NONE]
 System Contact:            [NONE]
 MAC address:                00-90-CC-55-44-32
 Web server:                enabled
 Web server port:           80
 Web secure server:         enabled
 Web secure server port:   443
 Telnet server             : enable
 Telnet port               : 23
 Jumbo Frame :                Disabled
 POST result
POST result
UART LOOP BACK Test.....PASS
DRAM Test.....PASS
Timer Test.....PASS
PCI Device 1 Test.....PASS
PCI Device 2 Test.....PASS
Switch Int Loopback test.....PASS


Done All Pass.
Console#
```

### show users

ユーザ名、アイドル時間、Telnetクライアントの IPアドレスを含め、アクティブなコンソールおよびTelnetセッションをすべて表示します。

**デフォルト設定**

なし

**コマンドモード**

Normal Exec、Privileged Exec

**コマンドの使用方法**

このコマンドの実行に使用するセッションは、Line (セッションなど)のインデックス番号の隣に「*」記号を付けて指定されます。

**例**

```
Console#show users
  Username accounts:
    Username Privilege Public-Key
    -------- --------- ----------
         admin        15       None
         guest         0       None
         steve        15        RSA


  Online users:
    Line          Username Idle time (h:m:s) Remote IP addr.
    ------------ -------- ----------------- ---------------
     0    console     admin              0:14:14
* 1       VTY 0      admin               0:00:00     192.168.1.19
     2       SSH 1      steve               0:00:06     192.168.1.19


  Web online users:
    Line          Remote IP addr Username Idle time (h:m:s).
    ------------ -------------- -------- ------------------
  1         HTTP     192.168.1.19      admin                0:00:00


Console#
```

### show version

システムのハードウェアおよびソフトウェアのバージョン情報を表示します。

**デフォルト設定**

なし

**コマンドモード**

Normal Exec、Privileged Exec

**コマンドの使用方法**

このコマンドで表示される項目の詳細については、35ページの「ハードウェアおよびソフトウェアのバージョンを表示する」を参照してください。

**例**

```
Console#show version
Unit1
  Serial number:              S416000937
  Service tag:
  Hardware version:           R01
  Module A type:               1000BaseT
  Module B type:               1000BaseT
  Number of ports:            26
  Main power status:          up
  Redundant power status      :not present


Agent (master)
  Unit ID:                     1
  Loader version:             2.2.1.4
  Boot ROM version:            2.2.1.8
  Operation code version:    2.2.6.4
Console#
```

## フレームサイズコマンド

表 4-24 フレームサイズコマンド

| コマンド | 機能 | モード | ページ |
|---|---|---|---|
| jumbo frame | ジャンボフレームのサポートを有効化 | GC | 312 |

**jumbo frame**

ジャンボフレームのサポートを有効にします。 無効にするには**no**形式を使用します。

**構文**

[**no**] **jumbo frame**

**デフォルト設定**

無効

**コマンドモード**

Global Configuration

**コマンドの使用方法**

- 本製品では、最大9216バイトのジャンボフレームをサポートすることにより、大規模な順次データ転送のスループットがより効率的になっています。 最大1.5KBまでしか対応しない標準的なイーサネットフレームと比較して、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ヘッドを著しく削減できます。
- ジャンボフレームを使用するには、転送元と転送先の両方の末端ノード(コンピュータやサーバなど)がこの機能をサポートする必要があります。 また、接続が全二重で動作している場合は、2つの末端ノード間のネットワークに存在するすべてのスイッチが、拡大されたフレームサイズに対応できる必要があります。 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機器がジャンボフレームをサポートする必要があります。
- ジャンボフレームを有効にすると、ブロードキャストストーム制御の最大しきい値が64パケット/秒に制限されます (373ページのswitchport broadcastコマンドを参照)。
- ジャンボフレームの現在の設定は、show systemコマンド(373ページ)で表示できます。

**例**

```
Console(config)#jumbo frame
Console(config)#
```

# フラッシュ/ファイルコマンド

これらのコマンドでは、システムコードまたは設定ファイルを管理します。

表 4-25　フラッシュ/ファイルコマンド

| コマンド | 機能 | モード | ページ |
|---|---|---|---|
| copy | フラッシュメモリまたはTFTPサーバとの間でコードイメージまたはスイッチ設定をコピー | PE | 314 |
| delete | ファイルまたはコードイメージを削除 | PE | 317 |
| dir | フラッシュメモリ内のファイルのリストを表示 | PE | 318 |
| whichboot | ブートされたファイルを表示 | PE | 319 |
| boot system | システムの起動に使用するファイルまたはイメージを指定 | GC | 320 |

### copy

スイッチのフラッシュメモリとTFTPサーバの間で、コードイメージまたは設定ファイルを移動(アップロード/ダウンロード)します。 システムコードまたは設定をTFTPサーバ上のファイルに保存すると、後にそのファイルをスイッチにダウンロードしてシステム動作を復元することができます。 ファイル転送が成功するかどうかは、TFTPサーバへのアクセスのしやすさと、ネットワーク接続の質次第です。

### 構文

**copy file** {**file** | **running-config** | **startup-config** | **tftp** | **unit**}
**copy running-config** {**file** | **startup-config** | **tftp**}
**copy startup-config** {**file** | **running-config** | **tftp**}
**copy tftp** {**file** | **running-config** | **startup-config** | **https-certificate** | **public-key**}
**copy unit file**

- **file** – ファイルへ、またはファイルからコピーする場合のキーワード
- **running-config** – 現在実行中の設定へ、またはその設定からコピーする場合のキーワード
- **startup-config** – システムの初期化に使用する設定
- **tftp** – TFTPサーバへ、またはTFTPサーバからコピーする場合のキーワード
- **https-certificate** – TFTPサーバからスイッチへのHTTPS証明書のコピー
- **public-key** – SSHキーをTFTPサーバからコピーする場合のキーワード (274ページの「セキュアシェルコマンド」)
- **unit** – ユニットへ、またはユニットからコピーする場合のキーワード

### デフォルト設定

なし

### コマンドモード

Privileged Exec

### コマンドの使用方法

- copyコマンドを完成させるために必要なデータを入力するよう指示があります。
- コピー先のファイル名にスラッシュ(¥または/)を含めることはできません。また、ファイル名の先頭文字にピリオド(.)は使用できません。TFTPサーバ上のファイル名は最大127文字まで、スイッチ上のファイル名は最大31文字までです (有効な文字: A～Z、a～z、0～9、「.」、「-」、「_」)。
- フラッシュメモリのサイズ制限により、本製品で対応可能な実行コードファイルは2つのみです。
- ユーザ定義の設定ファイルの最大数は、使用可能なメモリによって異なります。
- 「Factory_Default_Config.cfg」をコピー元として、出荷時のデフォルト設定ファイルからコピーすることはできますが、このファイルをコピー先として使用することはできません。

- 起動設定を置き換えるには、**startup-config**をコピー先として使用する必要があります。
- ローカルファイルをスタック内の別のスイッチにコピーするには、**copy file unit**コマンドを使用します。 スタック内の別のスイッチからファイルをコピーするには、**copy unit file**コマンドを使用します。
- Boot ROMおよびローダを、TFTPサーバにアップロードしたり、TFTPサーバからダウンロードすることはできません。 新しいファームウェアのリリースノートの指示に従うか、または販売元にお問い合わせください。
- https証明書指定の詳細については、82ページの「セキュアサイトの初期証明を置き換える」を参照してください。 本製品を、セキュアな接続のためにHTTPSを使用するように設定する場合の詳細については、270ページの「ip http secure-server」を参照してください。

**例**

以下の例は、TFTPサーバに設定ファイルをアップロードする方法を示しています。

```
Console#copy file tftp
Choose file type:
  1. config:   2. opcode: <1-2>: 1
Source file name: startup
TFTP server ip address: 10.1.0.99
Destination file name: startup.01
TFTP completed.
Success.

Console#
```

以下の例は、起動ファイルに実行中の設定をコピーする方法を示しています。

```
Console#copy running-config file
destination file name: startup
Write to FLASH Programming.
¥Write to FLASH finish.
Success.

Console#
```

以下の例は、TFTPサーバから設定ファイルをダウンロードする方法を示しています。

```
Console#copy tftp startup-config
TFTP server ip address: 10.1.0.99
Source configuration file name: startup.01
Startup configuration file name [startup]:
Write to FLASH Programming.

¥Write to FLASH finish.
Success.

Console#
```

以下の例は、TFTPサーバからセキュアサイト証明書をコピーする方法を示しています。 この後本製品がリブートされ、証明書がアクティブになります。

```
Console#copy tftp https-certificate
TFTP server ip address: 10.1.0.19
Source certificate file name: SS-certificate
Source private file name: SS-private
Private password: ********


Success.
Console#reload
System will be restarted, continue <y/n>? y
```

以下の例は、SSHで使用するパブリックキーをTFTPサーバからコピーする方法を示しています。 ただし、SSH経由でのパブリックキーの認証は、本製品でローカルに設定されているユーザのみに対応していることに注意してください。

```
Console#copy tftp public-key
TFTP server IP address: 192.168.1.19
Choose public key type:
 1. RSA:   2. DSA: <1-2>: 1
Source file name: steve.pub
Username: steve
TFTP Download
Success.
Write to FLASH Programming.
Success.


Console#
```

### delete

ファイルまたはイメージを削除します。

### 構文

**delete** [*ユニット:*] *ファイル名*

*ファイル名* - 設定ファイルまたはイメージファイルの名前
*ユニット* - スタックユニット (範囲:1～8)

### デフォルト設定

なし

### コマンドモード

Privileged Exec

**コマンドの使用方法**

- システムの起動に使用するタイプのファイルは削除できません。
- 「Factory_Default_Config.cfg」は削除できません。
- 指定のユニット番号の後にはコロン(:)が必要です。

**例**

以下の例は、ユニット1のフラッシュメモリからtest2.cfg設定ファイルを削除する方法を示しています。

```
Console#delete 1:test2.cfg
Console#
```

**関連コマンド**

dir (p.318)
delete public-key (p.279)

### dir

フラッシュメモリ内のファイルのリストを表示します。

**構文**

**dir** [*ユニット:*] {{**boot-rom:** | **config:** | **opcode:**} [:*ファイル名*]}

表示するファイルまたはイメージのタイプには、以下が含まれます。

- **boot-rom** - Boot ROM (または診断)イメージファイル
- **config** - スイッチ設定ファイル
- **opcode** - ランタイム実行コードイメージファイル
- *ファイル名* - 設定ファイルまたはコードイメージの名前
- *ユニット* - スタックユニット (範囲:1～8)

**デフォルト設定**

なし

**コマンドモード**

Privileged Exec

**コマンドの使用方法**

- **dir**コマンドをパラメータなしで入力すると、すべてのファイルが表示されます。
- 指定のユニット番号の後にはコロン(:)が必要です。
- ファイル情報は以下のとおりです。

表 4-26 ファイルディレクトリ情報

| 列ヘッダ | 説明 |
|---|---|
| file name | ファイルの名前 |
| file type | ファイルタイプ： Boot-Rom、Operation Code (実行コード)、Config (設定)ファイル |
| startup | システム起動時にこのファイルを使用するかどうかを表示 |
| size | ファイルの長さ(バイト) |

**例**

以下の例は、すべてのファイル情報の表示方法を示しています。

```
Console#dir 1:
              file name                    file type          startup size (byte)
-----------------------------------    --------------   ------- -------------
Unit1:
            D2218                          Boot-Rom image    Y              214000
            V2260                          Operation Code    N             1751624
            V2264-J                        Operation Code    Y             1754316
            Factory_Default_Config.cfg     Config File       N                5013
            startup                        Config File       Y                3251
-------------------------------------------------------------------------------
                                                  Total free space:     5111808
Console#
```

**whichboot**

システム電源投入時にブートされたファイルを表示します。

**構文**

**whichboot** [*ユニット*]

*ユニット* - スタックユニット (範囲:1～8)

**デフォルト設定**

なし

**コマンドモード**

Privileged Exec

**例**

以下の例は、**whichboot**コマンドで表示される情報を示しています。 このコマンドで表示されるファイル情報の詳細については、**dir**コマンドの表を参照してください。

```
Console#whichboot
          file name                          file type          startup size (byte)
 ------------------------------------  ---------------  -------  ------------
 Unit1:
          D2218                           Boot-Rom image    Y          214000
          V2264-J                         Operation Code    Y         1754316
          startup                        Config File        Y            3251
Console#
```

### boot system

システムの起動に使用するイメージを指定します。

#### 構文

**boot system** [*ユニット*:] {**boot-rom**| **config** | **opcode**}: *ファイル名*

デフォルトとして設定するファイルまたはイメージのタイプには、以下が含まれます。

- **boot-rom*** – Boot ROM
- **config*** – 設定ファイル
- **opcode*** – ランタイム実行コード
- *ファイル名* – 設定ファイルまたはコードイメージの名前
- *ユニット** – ユニット番号を指定

* コロン(:)が必要です。

#### デフォルト設定

なし

#### コマンドモード

Global Configuration

#### コマンドの使用方法

- 指定のユニット番号およびファイルタイプの後にはコロン(:)が必要です。
- エラーが含まれているファイルは、デフォルトファイルとして設定できません。

#### 例

```
Console(config)#boot system config: startup
Console(config)#
```

#### 関連コマンド

dir (p.318)
whichboot (p.319)

# 認証コマンド

管理アクセスの目的でシステムにログインするユーザを、ローカルまたはRADIUSの認証方法を使用して認証するように、本製品を設定することができます。 また、IEEE 802.1Xを使用して、ネットワーククライアントアクセス用のポートベースの認証を有効にすることもできます。

**表 4-27　認証コマンド**

| コマンドグループ | 機能 | ページ |
|---|---|---|
| 認証順序 | ログオン認証方法および優先度を定義 | 321 |
| RADIUSクライアント | RADIUSサーバ経由の認証を設定 | 323 |
| TACACS+クライアント | TACACS+サーバ経由の認証を設定 | 327 |
| ポートセキュリティ | ポートのセキュアアドレスを設定 | 330 |
| ポート認証 | 802.1Xを使用した特定のポートのホスト認証を設定 | 332 |

## 認証順序

表 4-28　認証順序

| コマンド | 機能 | モード | ページ |
|---|---|---|---|
| authentication login | ログオン認証方法および優先度を定義 | GC | 321 |
| authentication enable | コマンドモード変更の認証方法および優先度を定義 | GC | 322 |

### authentication login

ログオン認証方法および優先度を定義します。 デフォルトを復元するにはno形式を使用します。

**構文**

**authentication login** {[**local**] [**radius**] [**tacacs**]}
**no authentication login**

- **local** – ローカルのパスワードの使用
- **radius** – RADIUSサーバのパスワードの使用
- **tacacs** – TACACSサーバのパスワードの使用

**デフォルト設定**

ローカル

**コマンドモード**

Global Configuration

**コマンドの使用方法**

- RADIUSはUDPを、TACACS+はTCPを使用します。 UDPではベストエフォート式配信のみが行われますが、TCPではコネクション型のトランスポートが行われます。また、RADIUSはクライアントからサーバへのアクセス要求パケットでパスワードのみを暗号化しますが、TACACS+はパケット全体を暗号化します。
- RADIUSおよびTACACS+のログオン認証では、ユーザ名とパスワードの各ペアに対して、特定の優先レベルが割り当てられます。 ユーザ名、パスワード、および優先レベルは、認証サーバで設定する必要があります。
- 1つのコマンドで3つの認証方法を指定して、認証順序を示すことができます。 たとえば、「**authentication login radius tacacs local**」と入力した場合、RADIUSサーバ上のユーザ名とパスワードが最初に確認されます。 RADIUSサーバが使用できない場合、認証はTACACS+サーバで行われます。 TACACS+サーバが使用できない場合、ローカルのユーザ名とパスワードがチェックされます。

**例**

```
Console(config)#authentication login radius
Console(config)#
```

**関連コマンド**

username – ローカルのユーザ名とパスワードを設定する場合(p.265)

### authentication enable

**enable**コマンド(256ページを参照)を使用してExecコマンドモードからPrivileged Execコマンドモードへ切り替えるときに使用する認証方法および優先度を定義します。 デフォルトを復元するには**no**形式を使用します。

**構文**

**authentication enable** {[**local**] [**radius**] [**tacacs**]}
**no authentication enable**

- **local** – ローカルのパスワードのみの使用
- **radius** – RADIUSサーバのパスワードのみの使用
- **tacacs** – TACACSサーバのパスワードの使用

**デフォルト設定**

ローカル

**コマンドモード**

Global Configuration

**コマンドの使用方法**

- RADIUSはUDPを、TACACS+はTCPを使用します。 UDPではベストエフォート式配信のみが行われますが、TCPではコネクション型のトランスポートが行われます。また、RADIUSはクライアントからサーバへのアクセス要求パケットでパスワードのみを暗号化しますが、TACACS+はパケット全体を暗号化します。
- RADIUSおよびTACACS+のログオン認証では、ユーザ名とパスワードの各ペアに対して、特定の優先レベルが割り当てられます。 ユーザ名、パスワード、および優先レベルは、認証サーバで設定する必要があります。
- 1つのコマンドで3つの認証方法を指定して、認証順序を示すことができます。 たとえば、「**authentication enable radius tacacs local**」と入力した場合、RADIUSサーバ上のユーザ名とパスワードが最初に確認されます。 RADIUSサーバが使用できない場合、認証はTACACS+サーバで行われます。 TACACS+サーバが使用できない場合、ローカルのユーザ名とパスワードがチェックされます。

**例**

```
Console(config)#authentication enable radius
Console(config)#
```

**関連コマンド**

enable password – コマンドモードを変更するためのパスワードを設定(p.266)

## RADIUSクライアント

Remote Authentication Dial-in User Service (RADIUS)は、中央のサーバで実行しているソフトウェアを使用してネットワーク上のRADIUS対応機器への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、複数のユーザ名/パスワードのペアと、スイッチに対して管理アクセスが必要なユーザまたはグループごとに関連付けられている優先レベルのデータベースが含まれます。

**表 4-29　RADIUSクライアントコマンド**

| コマンド | 機能 | モード | ページ |
|---|---|---|---|
| radius-server host | RADIUSサーバを指定 | GC | 324 |
| radius-server port | RADIUSサーバのネットワークポートを設定 | GC | 324 |
| radius-server key | RADIUS暗号化キーを設定 | GC | 325 |
| radius-server retransmit | 再試行回数を設定 | GC | 325 |
| radius-server timeout | 認証要求を送信する間隔を設定 | GC | 326 |

| | | | |
|---|---|---|---|
| show radius-server | RADIUSの現在の設定を表示 | PE | 326 |

### radius-server host

プライマリおよびバックアップ用のRADIUSサーバと、各サーバに該当する認証パラメータを指定します。 デフォルト値を復元するには**no**形式を使用します。

#### 構文

[**no**] **radius-server** *インデックス* **host** {*ホストIPアドレス* | *ホストエイリアス*} [**auth-port** *認証ポート*] [**timeout** *タイムアウト*] [**retransmit** *再送信*] [**key** *キー*]

- *インデックス* – サーバを5台まで指定可能。 これらのサーバは、いずれかのサーバが応答するまで、または再送信期限が切れるまで、順番にクエリされます。
- *ホストIPアドレス* – サーバのIPアドレス
- *ホストエイリアス* – サーバの記号的な名前(最大設定:20文字)
- *ポート番号* – 認証メッセージに使用するRADIUSサーバのUDPポート (範囲:1～65535)
- *タイムアウト* – リクエストを再送する前に、応答を待機する秒数 (範囲:1～65535)
- *再送信* – RADIUSサーバ経由でログオンアクセスの認証を試行する回数 (範囲:1～30)
- *キー* – クライアントのログオンアクセスの認証に使用する暗号化キー。 この文字列にはスペースを含めないでください (最大設定:20文字)。

#### デフォルト設定

- **auth-port** – 1812
- **timeout** – 5秒
- **retransmit** – 2回

#### コマンドモード

Global Configuration

#### 例

```
Console(config)#radius-server 1 host 192.168.1.20 auth-port 181 timeout 10 retransmit 5 key green
Console(config)#
```

### radius-server port

RADIUSサーバのネットワークポートを設定します。 デフォルトを復元するには**no**形式を使用します。

#### 構文

**radius-server port** *ポート番号*

**no radius-server port**

*ポート番号* - 認証メッセージに使用するRADIUSサーバのUDPポート（範囲：1～65535）

**デフォルト設定**

1812

**コマンドモード**

Global Configuration

**例**

```
Console(config)#radius-server port 181
Console(config)#
```

### radius-server key

RADIUSの暗号化キーを設定します。 デフォルトを復元するにはno形式を使用します。

**構文**

**radius-server key** *キー文字列*
**no radius-server key**

*キー文字列* - クライアントのログオンアクセスの認証に使用する暗号化キー。この文字列にはスペースを含めないでください（最大設定：20文字）。

**デフォルト設定**

なし

**コマンドモード**

Global Configuration

**例**

```
Console(config)#radius-server key green
Console(config)#
```

### radius-server retransmit

再試行回数を設定します。 デフォルトを復元するにはno形式を使用します。

**構文**

**radius-server retransmit** *再試行回数*
**no radius-server retransmit**

*再試行回数* - RADIUSサーバ経由でログオンアクセスの認証を試行する回数（範囲：1～30）

**デフォルト設定**

2

**コマンドモード**

Global Configuration

**例**

```
Console(config)#radius-server retransmit 5
Console(config)#
```

### radius-server timeout

RADIUSサーバに認証要求を送信する間隔を設定します。 デフォルトを復元するにはno形式を使用します。

**構文**

**radius-server timeout** *秒数*
**no radius-server timeout**

*秒数* - リクエストを再送する前に、応答を待機する秒数（範囲：1～65535）

**デフォルト設定**

5

**コマンドモード**

Global Configuration

**例**

```
Console(config)#radius-server timeout 10
Console(config)#
```

### show radius-server

RADIUSサーバの現在の設定を表示します。

**デフォルト設定**

なし

**コマンドモード**

Privileged Exec

**例**

```
Console#show radius-server

Remote RADIUS server configuration:

  Global settings
  Communication key with RADIUS server:
  Server port number:                    1812
  Retransmit times:                      2
  Request timeout:                       5

Sever 1:
  Server IP address: 192.168.1.1
  Communication key with RADIUS server: *****
  Server port number: 1812
  Retransmit times:   2
  Request timeout:   5

Console#
```

## TACACS+クライアント

Terminal Access Controller Access Control System (TACACS+)は、中央のサーバで実行しているソフトウェアを使用してネットワーク上のTACACS対応機器への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、複数のユーザ名/パスワードのペアと、スイッチに対して管理アクセスが必要なユーザまたはグループごとに関連付けられている優先レベルのデータベースが含まれます。

**表 4-30 TACACSコマンド**

| コマンド | 機能 | モード | ページ |
|---|---|---|---|
| tacacs-server host | TACACS+サーバを指定 | GC | 327 |
| tacacs-server port | TACACS+サーバのネットワークポートを指定 | GC | 328 |
| tacacs-server key | TACACS+暗号化キーを設定 | GC | 329 |
| show tacacs-server | TACACS+の現在の設定を表示 | GC | 329 |

### tacacs-server host

TACACS+サーバを指定します。 デフォルトを復元するには**no**形式を使用します。

**構文**

**tacacs-server host** *ホストIPアドレス*
**no tacacs-server host**

*ホストIPアドレス* - TACACS+サーバのIPアドレス

**デフォルト設定**

10.11.12.13

**コマンドモード**

Global Configuration

**例**

```
Console(config)#tacacs-server host 192.168.1.25
Console(config)#
```

**tacacs-server port**

TACACS+サーバのネットワークポートを指定します。 デフォルトを復元するには**no**形式を使用します。

**構文**

**tacacs-server port** *ポート番号*
**no tacacs-server port**

*ポート番号* - 認証メッセージに使用するTACACS+サーバのTCPポート (範囲:1～65535)

**デフォルト設定**

49

**コマンドモード**

Global Configuration

**例**

```
Console(config)#tacacs-server port 181
Console(config)#
```

### tacacs-server key

TACACS+暗号化キーを設定します。 デフォルトを復元するには**no**形式を使用します。

#### 構文

**tacacs-server key** *キー文字列*
**no tacacs-server key**

*キー文字列* - クライアントのログオンアクセスの認証に使用する暗号化キー。 この文字列にはスペースを含めないでください
(最大設定:20文字)。

#### デフォルト設定

なし

#### コマンドモード

Global Configuration

#### 例

```
Console(config)#tacacs-server key green
Console(config)#
```

### show tacacs-server

TACACS+サーバの現在の設定を表示します。

#### デフォルト設定

なし

#### コマンドモード

Privileged Exec

#### 例

```
Console#show tacacs-server
Remote TACACS server configuration:
  Server IP address:                      10.11.12.13
  Communication key with TACACS server: *****
  Server port number:                     49
Console#
```

## ポートセキュリティコマンド

これらのコマンドを使用すると、ポート上のポートセキュリティを有効にできます。 本製品でポートセキュリティを使用すると、設定されている最大数に達したときに、指定のポートでの新規MACアドレスの学習が停止します。 送信元のアドレスがこのポートの動的または静的なアドレステーブルに保存されている着信トラフィックのみに、ネットワークのアクセスが承認されます。 送信元のMACアドレスが不明もしくは以前に別のポートから学習されたものである場合、そのアドレスを含む着信フレームは削除されます。 非承認のMACアドレスを持つ機器が本製品のポートを使用しようとすると、侵入が検知され、ポートを無効にしてトラップメッセージを送信する処理が自動的に実行することができます。

表 4-31 ポートセキュリティコマンド

| コマンド | 機能 | モード | ページ |
|---|---|---|---|
| port security | セキュアポートを設定 | IC | 330 |
| mac-address-table static | VLANで任意のポートに静的アドレスをマッピング | GC | 331 |
| show mac-address-table | ブリッジ転送データベースのエントリを表示 | PE | 398 |

### port security

ポートセキュリティを有効化または設定します。 ポートセキュリティを無効にするには**no**形式をキーワードなしで使用します。 セキュリティ侵害への対応または許可できるアドレスの最大数のデフォルト設定を復元するには、**no**形式を適切なキーワードを指定して使用します。

#### 構文

**port security** [**action** {**shutdown** | **trap** | **trap-and-shutdown**} | **max-mac-count** *アドレス数*]

**no port security** [**action** | **max-mac-count**]

- **action** – ポートセキュリティが侵害された場合の対応
  - **shutdown** – ポートの無効化
  - **trap** – SNMPトラップメッセージの発行
  - **trap-and-shutdown** – SNMPトラップメッセージを発行してポートを無効化
- max-mac-count
  - *アドレス数* – ポートから学習可能なMACアドレスの最大数（範囲：0～1024）

#### デフォルト設定

- 状態：無効
- 対応：なし
- アドレスの最大数：0

**コマンドモード**

Interface Configuration (イーサネット)

**コマンドの使用方法**

・本製品でポートセキュリティを有効にすると、設定されている最大数に達したときに、指定のポートでの新規MACアドレスの学習が停止します。 送信元のアドレスが動的または静的なアドレステーブルに保存されている着信トラフィックのみが受け入れられます。

- まず**port security max-mac-count**コマンドを使用してアドレスの数を設定し、その後port securityコマンドを使用してポート上のセキュリティを有効にします。
- ポートセキュリティを無効にしてアドレスの最大数をデフォルトにリセットするには、**no port security max-mac-count**コマンドを使用します。
- **mac-address-table static**コマンドを使用して、手動でセキュアアドレスを追加することもできます。
- セキュアポートには、以下の制限があります。
  - ポート監視は使用できません。
  - マルチVLANポートは使用できません。
  - ネットワーク相互接続機器には接続できません。
  - トランクポートは使用できません。
- セキュリティ侵害によって無効になっているポートは、**no shutdown**コマンドを使用して手動で有効にする必要があります。

**例**

以下の例では、ポート5のポートセキュリティが有効になり、セキュリティ侵害への対応はトラップメッセージの発行に設定されます。

```
Console(config)#interface ethernet 1/5
Console(config-if)#port security action trap
```

**関連コマンド**

shutdown (p.371)
mac-address-table static (p.331)
show mac-address-table (p.397)

## 802.1Xポート認証

本製品は、IEEE 802.1X (dot1x)ポートベースのアクセス制御に対応しています。これを使用すると、ユーザはまず認証のための資格情報を提出する必要があるため、ネットワークへの不正アクセスを防ぐことができます。 クライアント認証は、中央のRADIUSサーバによって、EAP (Extensible Authentication Protocol)を使用して制御されます。

**表 4-32 802.1Xポート認証**

| コマンド | 機能 | モード | ページ |
|---|---|---|---|
| dot1x system-auth-control | 本製品でdot1xをグローバルに有効化 | GC | 332 |
| dot1x default | すべてのdot1xパラメータをデフォルト値にリセット | GC | 333 |
| dot1x max-req | 認証セッションがタイムアウトするまでに、EAP要求/IDパケットをクライアントに再送信する最大回数を設定 | IC | 333 |
| dot1x port-control | ポートインタフェースのdot1xモードを設定 | IC | 334 |
| dot1x operation-mode | dot1xポートで単一または複数のホストを許可 | IC | 334 |
| dot1x re-authenticate | 特定のポートで再認証を強制的に実行 | PE | 335 |
| dot1x re-authentication | すべてのポートに関して再認証を有効化 | IC | 335 |
| dot1x timeout quiet-period | 要求の最大数を超えてから、新規のクライアントを取得するまでのスイッチポートの待機時間を設定 | IC | 336 |
| dot1x timeout re-authperiod | 接続しているクライアントに再認証が必要になる期限を設定 | IC | 336 |
| dot1x timeout tx-period | 認証セッション中に、EAPパケットを再送信するまでの本製品の待機時間を設定 | IC | 337 |
| show dot1x | dot1xに関連するすべての情報を表示 | PE | 337 |

### dot1x system-auth-control

本製品で802.1Xポート認証をグローバルに有効にします。 デフォルトを復元するにはno形式を使用します。

#### 構文

[no] system-auth-control

**デフォルト設定**

無効

**コマンドモード**

Global Configuration

**例**

```
Console(config)#dot1x system-auth-control
Console(config)#
```

### dot1x default

設定可能なすべてのdot1xグローバルおよびポートの設定をデフォルト値に設定します。

**コマンドモード**

Global Configuration

**例**

```
Console(config)#dot1x default
Console(config)#
```

### dot1x max-req

認証セッションがタイムアウトするまでに、EAP要求/IDパケットをクライアントに再送信する最大回数を設定します。 デフォルトを復元するには**no**形式を使用します。

**構文**

**dot1x max-req** *回数*
**no dot1x max-req**

*回数* - 要求の最大数(範囲:1～10)

**デフォルト**

2

**コマンドモード**

Interface Configuration

**例**

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x max-req 2
Console(config-if)#
```

### dot1x port-control

ポートインタフェースのdot1xモードを設定します。 デフォルトを復元するにはno形式を使用します。

#### 構文

**dot1x port-control** {**auto** | **force-authorized** | **force-unauthorized**}
**no dot1x port-control**

- **auto** – dot1x対応の接続クライアントはRADIUSサーバの承認を受ける必要あり。dot1xに対応していないクライアントは、アクセスが拒否されます。
- **force-authorized** – dot1x対応かどうかにかかわらず、すべてのクライアントに対してアクセスを承認するようにポートを設定。
- **force-unauthorized** – dot1x対応かどうかにかかわらず、すべてのクライアントに対してアクセスを拒否するようにポートを設定。

#### デフォルト

force-authorized

#### コマンドモード

Interface Configuration

#### 例

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x port-control auto
Console(config-if)#
```

### dot1x operation-mode

単一または複数のホスト(クライアント)に、802.1X承認ポートへの接続を許可します。 デフォルトを単一ホストに復元するにはno形式をキーワードなしで使用します。 デフォルトの最大数を復元するには、no形式をmulti-host max-countキーワードを指定して使用します。

#### 構文

**dot1x operation-mode** {**single-host** | **multi-host** [**max-count** *数*]}
**no dot1x operation-mode** [**multi-host max-count**]

- **single-host** – 単一のホストのみにこのポートへの接続を許可。
- **multi-host** – 複数のホストにこのポートへの接続を許可。
- **max-count** – ホストの最大数を指定するキーワード。
  – *数* – ポートに接続できるホストの最大数 (範囲:1～1024、デフォルト:5)

**デフォルト**

Single-host

**コマンドモード**

Interface Configuration

**コマンドの使用方法**

- このコマンドで指定する「max-count」パラメータは、dot1x port-controlコマンド(334ページ)でdot1xモードが「auto」に設定されている場合にのみ有効です。
- 「multi-host」モードでは、ポートに接続されているホストのうち1台が認証されれば、その他すべてのホストにネットワークアクセスが承認されます。 同様に、接続されているホストのうち1台が再認証に失敗またはEAPOL logoffメッセージを送信した場合は、すべてのホストに対してポートが非承認になることがあります。

**例**

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x operation-mode multi-host max-count 10
Console(config-if)#
```

### dot1x re-authenticate

すべてのポートまたは特定のインタフェースで再認証を強制的に実行します。

**構文**

dot1x re-authenticate [*インタフェース*]

*インタフェース*

- ethernet *ユニット/ポート*
  - *ユニット* - スタックユニット (範囲:1～8)
  - *ポート* - ポート番号 (範囲:1～26)

**コマンドモード**

Privileged Exec

**例**

```
Console#dot1x re-authenticate
Console#
```

### dot1x re-authentication

すべてのポートに関してグローバルに定期的な再認証を有効にします。 再認証を無効に

するにはno形式を使用します。

**構文**

[no] dot1x re-authentication

**コマンドモード**

Interface Configuration

**例**

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x re-authentication
Console(config-if)#
```

### dot1x timeout quiet-period

要求の最大数を超えてから、新規のクライアントの取得を試みるまでのスイッチポートの待機時間を設定します。 デフォルトをリセットするにはno形式を使用します。

**構文**

**dot1x timeout quiet-period** *秒*
**no dot1x timeout quiet-period**

*秒* - 秒数（範囲:1～65535）

**デフォルト**

60秒

**コマンドモード**

Interface Configuration

**例**

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout quiet-period 350
Console(config-if)#
```

### dot1x timeout re-authperiod

接続しているクライアントに再認証が必要になる期限を設定します。

**構文**

**dot1x timeout re-authperiod** *秒*
**no dot1x timeout re-authperiod**

*秒* - 秒数 (範囲:1～65535)

**デフォルト**

3600秒

**コマンドモード**

Interface Configuration

**例**

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout re-authperiod 300
Console(config-if)#
```

### dot1x timeout tx-period

認証セッション中に、EAPパケットを再送信するまでの本製品のインタフェースの待機時間を設定します。 デフォルト値にリセットするには**no**形式を使用します。

**構文**

**dot1x timeout tx-period** *秒*
**no dot1x timeout tx-period**

*秒* - 秒数 (範囲:1～65535)

**デフォルト**

30秒

**コマンドモード**

Interface Configuration

**例**

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout tx-period 300
Console(config-if)#
```

### show dot1x

本製品または特定のインタフェースの一般的なポート認証関連の設定を表示します。

**構文**

**show dot1x** [**statistics**] [**interface** *インタフェース*]

- **statistics** - 各ポートのdot1xステータスの表示

- *インタフェース*
  - **ethernet** *ユニット/ポート*
    - *ユニット* - スタックユニット（範囲:1～8）
    - *ポート* - ポート番号（範囲:1～26）

**コマンドモード**

Privileged Exec

**コマンドの使用方法**

以下の情報が表示されます。

- *Global 802.1X Parameters* - 802.1Xポート認証が本製品でグローバルに有効になっているかどうかを表示します。
- *802.1X Port Summary* - 以下の項目を含む、各インタフェースのポートアクセス制御パラメータを表示します。
  - Status - ポートアクセス制御の管理状態
  - Operation Mode - Dot1xポート制御実行モード(334ページ)
  - Mode - Dot1xポート制御モード(333ページ)
  - Authorized - 承認ステータス(yesまたはn/a (非承認))

- *802.1X Port Details* – 以下の項目を含む、各インタフェースのポートアクセス制御パラメータを表示します。
  - reauth-enabled – 定期的な再認証(335ページ)
  - reauth-period – 接続しているクライアントに再認証が必要になる期限(336ページ)
  - quiet-period – 要求の最大数を超えてから、新規のクライアントを取得するまでのポートの待機時間(336ページ)
  - tx-period – 認証セッション中に、EAPパケットを再送信するまでのポートの待機時間(337ページ)
  - supplicant-timeout – サプリカントのタイムアウト
  - server-timeout – サーバのタイムアウト
  - reauth-max – 再認証の最大試行回数
  - max-req – 認証セッションがタイムアウトするまでに、EAP要求/IDパケットをポートからクライアントに再送信する最大回数(333ページ)
  - Status – 承認ステータス(承認または非承認)
  - Operation Mode – 単一または複数のホスト(クライアント)が、802.1X承認ポートに接続できるかどうかを表示
  - Max Count – このポートにアクセスできるホストの最大数(334ページ)
  - Port-control – ポート上のdot1xモードを、auto (自動)、force-authorized (強制承認)、force-unauthorized (強制非承認)のいずれかで表示(334ページ)
  - Supplicant – 承認クライアントのMACアドレス
  - Current Identifier – Authenticator (認証者)が現在の認証セッションを識別する整数(0～255)
- *Authenticator State Machine*
  - State – 現在の状態(initialize (初期化)、disconnected (切断)、connecting (接続中)、authenticating (認証中)、authenticated (認証済み)、aborting (中止中)、held (保留)、force_authorized (強制承認)、force_unauthorized (強制非承認)を含む)
  - Reauth Count – 接続状態を再入力する回数
- *Backend State Machine*
  - State – 現在の状態(request (要求)、response (応答)、success (成功)、fail (失敗)、timeout (タイムアウト)、idle (アイドル)、initialize (初期化)を含む)
  - Request Count – Supplicant (サプリカント)へ送信された応答のないEAP要求パケットの数
  - Identifier(Server) – 認証サーバから受信した最新のEAP Success (成功)、Failure (失敗)、Request (要求)パケットに含まれるID
- *Reauthentication State Machine*

- State　　- 現在の状態(initialize (初期化)、reauthenticate (再-認証)を含む)

**例**

```
Console#show dot1x
Global 802.1X Parameters
  system-auth-control: enable

802.1X Port Summary

Port Name   Status          Operation Mode    Mode                 Authorized
1/1         disabled        Single-Host       ForceAuthorized      n/a
1/2         enabled         Single-Host       auto                 yes
:
1/26        disabled        Single-Host       ForceAuthorized      n/a

802.1X Port Details

802.1X is disabled on port 1/1

802.1X is enabled on port 1/2
  reauth-enabled: Enable
  reauth-period:   1800
  quiet-period:    30
  tx-period:       40
  supplicant-timeout:    30
  server-timeout: 10
  reauth-max:      2
  max-req:         5
Status                  Authorized
Operation mode          Single-Host
Max count               5
Port-control            Auto
Supplicant              00-90-cc-49-5e-dc
Current Identifier   3


Authenticator State Machine
State                   Authenticated
Reauth Count            0


Backend State Machine
State                   Idle
Request Count           0
Identifier(Server)   2


Reauthentication State Machine
State                   Initialize
:
802.1X is disabled on port 1/26
Console#
```

# アクセス制御リストコマンド

アクセス制御リスト(ACL)では、IPフレーム(アドレス、プロトコル、レイヤ4プロトコルポート番号、TCP制御コードのいずれかに基づく)または任意のフレーム(MACアドレスまたはイーサネットタイプに基づく)のパケットフィルタリングが可能です。 パケットをフィルタリングするには、まずアクセスリストを作成し、必要なルールを追加して、リストを特定のポートにバインドします。

**アクセス制御リスト**

ACLは、許可または拒否の条件を順次示したリストであり、IPアドレス、MACアドレス、またはその他のより具体的な条件に適用されます。 本製品は、着信パケットまたは送信パケットを、ACLの条件に対して1つずつテストします。 許可ルールに該当するパケットは受け入れられ、拒否ルールに該当するパケットは削除されます。 許可ルールのリストにまったく該当しないパケットは削除され、拒否ルールのリストにまったく該当しないパケットは受け入れられます。

フィルタリングには以下の3つのモードがあります。

- Standard IP ACL (標準IP ACL)モード(STD-ACL) - 送信元のIPアドレスに基づいてパケットをフィルタリング
- Extended IP ACL (拡張IP ACL)モード(EXT-ACL) - 送信元または送信先のIPアドレスと、プロトコルのタイプおよびプロトコルのポート番号に基づいてパケットをフィルタリング。TCPプロトコルが指定されている場合は、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。
- MAC ACLモード(MAC-ACL) - 送信元または送信先のMACアドレスと、イーサネットのフレームタイプ(RFC 1060)に基づいてパケットをフィルタリング

ACLには以下の制限が適用されます。

- ACLごとに指定可能なルールは最大32個です。
- ACLの最大数は88個です。
- ただし、リソース制限のため、ポートにバインドされるルールの平均数は20を超えないようにしてください。
- 本製品では、ACLは着信フィルタリングのみに対応しています。 着信フィルタリング用には、1つのIP ACLを任意のポートに対して、また1つのMAC ACLをグローバルにバインドできるだけです。 つまり、1つのインタフェースにバインドできるACLは、着信IP ACLと着信MAC ACLの2つだけです。

有効な(アクティブとなっている)ACLは、以下の順番にて確認が行われます。

1. 着信ポート用の着信MAC ACL内のユーザ定義ルール
2. 着信ポート用の着信IP ACL内のユーザ定義ルール
3. 着信ポート用の着信IP ACL内の明示(Explicit)初期設定ルール
   (permit any any: any any)

4. 着信ポート用の着信MAC ACL内の明示(Explicit)初期設定ルール(permit any any: any any)

5. いずれの明示ルールとも合致しない場合、暗示(implicit)初期設定はpermit all (すべて許可)となります。

**表 4-33 アクセス制御リスト**

| コマンドグループ | 機能 | ページ |
|---|---|---|
| IP ACL | IPアドレス、TCP/UDPポート番号、プロトコルタイプ、TCP制御コードに基づいてACLを設定 | 342 |
| MAC ACL | ハードウェアアドレス、パケット形式、イーサネットタイプに基づいてACLを設定 | 350 |
| ACL情報 | ACLおよび関連するルール、各ポートに割り当てられているACLを表示 | 356 |

## IP ACL

表 4-34 IP ACL

| コマンド | 機能 | モード | ページ |
|---|---|---|---|
| access-list ip | IP ACLを作成して設定モードに移行 | GC | 343 |
| permit、deny | 指定した送信元IPアドレスに一致するパケットをフィルタリング | STD-ACL | 343 |
| permit、deny | 送信元と送信先のIPアドレス、TCP/UDPポート番号、プロトコルタイプ、TCP制御コードなど指定した条件を満たすパケットをフィルタリング | EXT-ACL | 343 |
| show ip access-list | 設定済みのIP ACLのルールを表示 | PE | 346 |
| ip access-group | IP ACLにポートを追加 | IC | 347 |
| show ip access-group | IP ACLのポート割り当てを表示 | PE | 348 |
| map access-list ip | ACLルールに一致するパケットのCoS値および対応する出力キューを設定 | IC | 348 |
| show map access-list ip | 任意のインタフェースのアクセスリストにマッピングされているCoS値を表示 | PE | 349 |

### access-list ip

標準または拡張IP ACLに関して、IPアクセスリストを追加して設定モードに移行します。
指定したACLを削除するには**no**形式を使用します。

#### 構文

[**no**] **access-list ip** {**standard** | **extended**} *ACL名*

- **standard** - 送信元のIPアドレスに基づいてパケットをフィルタリングするACLを指定
- **extended** - 送信元または送信先のIPアドレス、およびその他のより具体的な条件に基づいてパケットをフィルタリングするACLを指定
- *ACL名* - ACLの名前（最大設定:16文字）

#### デフォルト設定

なし

#### コマンドモード

Global Configuration

#### コマンドの使用方法

- 新規のACLを作成するとき、または既存のACLに関して設定モードに移行するときは、**permit**コマンドまたは**deny**コマンドを使用して、リストの一番下に新規のルールを追加します。 ACLを作成するには、1個以上のルールをリストに追加する必要があります。
- ルールを削除するには、**no permit**コマンドまたは**no deny**コマンドの後に、以前に設定したルールの正確なテキストを入力して使用します。
- ACLに指定可能なルールは最大32個です。

#### 例

```
Console(config)#access-list ip standard david
Console(config-std-acl)#
```

#### 関連コマンド

permit、deny (p.343)
ip access-group (p.347)
show ip access-list (p.346)

### permit、deny (標準ACL)

標準IP ACLにルールを追加します。 このルールは、指定した送信元からのパケットのフィルタ条件を設定します。 ルールを削除するには**no**形式を使用します。

### 構文

[no] {permit | deny} {any | *送信元 ビットマスク* /host *送信元*}

- any – 任意の送信元IPアドレス
- *送信元* – 送信元IPアドレス
- *ビットマスク* – 一致するアドレスビットを表す10進数
- host – 特定のIPアドレスの前に付けるキーワード

### デフォルト設定

なし

### コマンドモード

Standard ACL

### コマンドの使用方法

- 新規のルールはリストの最後に追加されます。
- アドレスビットマスクはサブネットマスクと同様で、0～255の4つの整数をピリオドで区切った形式です。 バイナリマスクでは、1ビットが「一致」を示し、0ビットが「無視」を示します。 ビットマスクは指定した送信元IPアドレスとビット単位でAND演算され、このACLの割り当て先ポートで受信する各IPパケットのアドレスと比較されます。

### 例

以下の例では、特定のアドレス10.1.1.21の許可(permit)ルールと、アドレス範囲168.92.16.x～168.92.31.xに関するビットマスクを使用するルールを設定します。

```
Console(config-std-acl)#permit host 10.1.1.21
Console(config-std-acl)#permit 168.92.16.0 255.255.240.0
```

### 関連コマンド

access-list ip (p.343)

## permit、deny (拡張ACL)

拡張IP ACLにルールを追加します。 このルールは、特定の送信元または送信先のIPアドレス、プロトコルタイプ、送信元または送信先のプロトコルポート、またはTCP制御コードを使用して、パケットのフィルタ条件を設定します。 ルールを削除するにはno形式を使用します。

### 構文

[no] {permit | deny} [*プロトコル番号* /udp]
{any | *送信元アドレスビットマスク* /host *送信元*}
{any | *送信先アドレスビットマスク* /host *送信先*}
[precedence *優先度*] [tos *tos*] [dscp *dscp*]

[**source-port** *sport* [*上限*]] [**destination-port** *dport* [*上限*]]

[**no**] {**permit** | **deny**} **tcp**
{**any** | *送信元アドレスビットマスク* /**host** *送信元*}
{**any** | *送信先アドレスビットマスク* /**host** *送信先*}
[**precedence** *優先度*] [**tos** *tos*] [**dscp** *dscp*]
[**source-port** *sport* [*上限*]] [**destination-port** *dport* [*上限*]]
[**control-flag** *制御フラグ フラグビットマスク*]

- *プロトコル番号* – 特定のプロトコル番号（範囲:0～255）
- *送信元* – 送信元IPアドレス
- *送信先* – 送信先IPアドレス
- *アドレスビットマスク* – 一致するアドレスビットを表す10進数
- **host** – 特定のIPアドレスの前に付けるキーワード
- *優先度* – IP優先度レベル（範囲:0～7）
- *tos* – サービスレベルのタイプ（範囲:0～15）
- *dscp* – DSCP優先度レベル（範囲:0～63）
- *sport* – プロトコル（※1）の送信元ポート番号（範囲:0～65535）
- *dport* – プロトコル（※1）の送信先ポート番号（範囲:0～65535）
- *上限* – プロトコルのポート範囲の上限（範囲:0～65535）
- *制御フラグ* – TCPヘッダのバイト14のフラグビットを指定する10進数(ビット文字列を表す)（範囲:0～63）
- *フラグビットマスク* – 一致するコードビットを表す10進数（範囲:0～63）

※1 TCP、UDP、その他のプロトコルタイプを含みます。

### デフォルト設定

なし

### コマンドモード

Extended ACL

### コマンドの使用方法

- 新規のルールはすべてリストの最後に追加されます。
- アドレスビットマスクはサブネットマスクと同様で、0～255の4つの整数をピリオドで区切った形式です。 バイナリマスクでは、1ビットが「一致」を示し、0ビットが「無視」を示します。 ビットマスクは指定した送信元IPアドレスとビット単位でAND演算され、このACLの割り当て先ポートで受信する各IPパケットのアドレスと比較されます。
- 優先度とToSの両方を同じルールで指定できます。 ただし、DSCPが使用されている場合は、優先度もToSも指定できません。
- 制御コードビットマスクは、制御コードに適用される10進数です(対応するビットマスクを表します)。 任意の10進数を入力します。対応するバイナリビットは、「1」がビッ

トに一致、「0」がビットを無視という意味です。 以下のビットを指定できます。

- 1 (fin) - Finish (終了)
- 2 (syn) - Synchronize (同期化)
- 4 (rst) - Reset (リセット)
- 8 (psh) - Push (プッシュ)
- 16 (ack) - Acknowledgement (承認)
- 32 (urg) - Urgent pointer (緊急ポインタ)

たとえば、以下のコード値とマスクを使用して、以下のフラグが設定されているパケットを捕らえることができます。

- SYNフラグが有効:「control-code 2 2」を使用
- SYNとACKの両方が有効:「control-code 18 18」を使用
- SYNが有効でACKが無効:「control-code 2 18」を使用

**例**

以下の例では、送信元アドレスがサブネット10.7.1.x内にある場合、すべての着信パケットが受け入れられます。 たとえば、ルールが一致している場合、つまりルール(10.7.1.0および255.255.255.0)がマスクされているアドレス(10.7.1.2および255.255.255.0)と等しい場合、パケットは通過します。

```
Console(config-ext-acl)#permit 10.7.1.1 255.255.255.0 any
Console(config-ext-acl)#
```

以下の例では、クラスCアドレス192.168.1.0からのTCPパケットを、送信先TCPポート80 (HTTP)に設定されている任意の送信先アドレスに送信できます。

```
Console(config-ext-acl)#permit 192.168.1.0 255.255.255.0 any destination-port 80
Console(config-ext-acl)#
```

以下の例では、TCP制御コードを持つクラスCアドレス192.168.1.0からのすべてのTCPパケットを「SYN」に設定できます。

```
Console(config-ext-acl)#permit tcp 192.168.1.0 255.255.255.0 any    control-flag 2 2
Console(config-ext-acl)#
```

**関連コマンド**

access-list ip (p.343)

### show ip access-list

設定済みのIP ACLのルールを表示します。

**構文**

**show ip access-list** {**standard** | **extended**} [*ACL名*]

- **standard** – 標準IP ACLの指定
- **extended** – 拡張IP ACLの指定
- *ACL名* – ACLの名前（最大設定:16文字）

**コマンドモード**

Privileged Exec

**例**

```
Console#show ip access-list standard
IP standard access-list david:
  permit host 10.1.1.21
  permit 168.92.0.0 255.255.255.0
Console#
```

**関連コマンド**

permit、deny (p.344)
ip access-group (p.347)

### ip access-group

IP ACLにポートをバインドします。 ポートを削除するには**no**形式を使用します。

**構文**

[**no**] **ip access-group** *ACL名* **in**

- *ACL名* – ACLの名前（最大設定:16文字）
- **in** – このリストが着信パケットに適用されることを表示

**デフォルト設定**

なし

**コマンドモード**

Interface Configuration（イーサネット）

**コマンドの使用方法**

- 1つのポートは、1つのACLのみにバインドできます。
- すでにACLにバインドされているポートを別のACLにバインドすると、古いバインドは新しいバインドに置き換えられます。

**例**

```
Console(config)#int eth 1/25
Console(config-if)#ip access-group david in
Console(config-if)#
```

**関連コマンド**

show ip access-list (p.346)

### show ip access-group

IP ACLに割り当てられているポートを表示します。

**コマンドモード**

Privileged Exec

**例**

```
Console#show ip access-group
Interface ethernet 1/25
  IP access-list david in
Console#
```

**関連コマンド**

ip access-group (p.347)

### map access-list ip

ACLルールに一致するパケットの出力キューを設定します。 指定したCoS値は、一致するパケットを出力キューにマッピングする目的のみに使用され、パケット自体には書き込まれません。 CoSマッピングを削除するには**no**形式を使用します。

**構文**

[**no**] **map access-list ip** *ACL名* **cos** *CoS値*

- *ACL名* - ACLの名前 (最大設定:16文字)
- *CoS値* - CoS値 (範囲:0～7)

**デフォルト設定**

なし

**コマンドモード**

Interface Configuration (イーサネット)

### コマンドの使用方法

以下の表に示すように、指定したACL内のルールに一致するパケットがいずれかの出力キューにマッピングされます。 CoS値を出力キューにマッピングする場合の詳細については、438ページの「**queue cos-map**」を参照してください。

**表 4-35 送信キュー優先度マッピング**

| キュー | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 優先度 | 1,2 | 0,3 | 4,5 | 6,7 |

### 例

```
Console(config)#interface ethernet 1/25
Console(config-if)#map access-list ip bill cos 0
Console(config-if)#
```

### 関連コマンド

queue cos-map (p.438)
show map access-list ip (p.349)

## show map access-list ip

現在のインタフェースに関してIP ACLにマッピングされているCoS値を表示します（CoS値によって、ACLルールに一致するパケットの出力キューが決定)。

### 構文

**show map access-list ip** [*インタフェース*]

*インタフェース*

- **ethernet** *ユニット/ポート*
  - *ユニット* - スタックユニット（範囲:1～8）
  - *ポート* - ポート番号

### コマンドモード

Privileged Exec

### 例

```
Console#show map access-list ip
Eth 1/25
  access-list ip bill cos 0
Console#
```

**関連コマンド**

map access-list ip (4-101)

## MAC ACL

表 4-36 MAC ACL

| コマンド | 機能 | モード | ページ |
|---|---|---|---|
| access-list mac | MAC ACLを作成して設定モードに移行 | GC | 350 |
| permit、deny | 指定した送信元および送信先アドレス、パケット形式、イーサネットタイプに一致するパケットをフィルタリング | MAC-ACL | 351 |
| show mac access-list | 設定済みのMAC ACLのルールを表示 | PE | 352 |
| mac access-group | MAC ACLにポートを追加 | IC | 353 |
| show mac access-group | MAC ACLのポート割り当てを表示 | PE | 354 |
| map access-list mac | ACLルールに一致するパケットのCoS値および対応する出力キューを設定 | IC | 354 |
| show map access-list mac | 任意のインタフェースのアクセスリストにマッピングされているCoS値を表示 | PE | 355 |

### access-list mac

MACアクセスリストを追加して、MAC ACL設定モードに移行します。 指定したACLを削除するには**no**形式を使用します。

**構文**

[**no**] **access-list mac** *ACL名*

*ACL名* - ACLの名前（最大設定:16文字）

**デフォルト設定**

なし

**コマンドモード**

Global Configuration

### コマンドの使用方法

- 新規のACLを作成するとき、または既存のACLに関して設定モードに移行するときは、**permit**コマンドまたは**deny**コマンドを使用して、リストの一番下に新規のルールを追加します。 ACLを作成するには、1個以上のルールをリストに追加する必要があります。
- ルールを削除するには、**no permit**コマンドまたは**no deny**コマンドの後に、以前に設定したルールの正確なテキストを入力して使用します。
- ACLに指定可能なルールは最大32個です。

### 例

```
Console(config)#access-list mac jerry
Console(config-mac-acl)#
```

### 関連コマンド

permit、 deny (MAC ACL) (p.351)
mac access-group (p.353)
show mac access-list (4-106)

## permit、 deny (MAC ACL)

MAC ACLにルールを追加します。 このルールは、指定したMAC送信元または送信先アドレス(物理レイヤアドレス)、またはイーサネットプロトコルタイプに一致するパケットをフィルタリングします。 ルールを削除するには**no**形式を使用します。

### 構文

[**no**] {**permit** | **deny**}
{**any** | **host** *送信元* | *送信元アドレスビットマスク*}
{**any** | **host** *送信先* | *送信先アドレスビットマスク*}
[**vid** *vid* [*VID上限*]] [**ethertype** *プロトコル* [*プロトコル上限*]]

**注意:** デフォルトはイーサネットIIパケット用です。

- **any** – 任意のMAC送信元または送信先アドレス
- **host** – 特定のMACアドレス
- *送信元* – 送信元MACアドレス
- *送信先* – 送信先MACアドレス範囲とビットマスク
- *アドレスビットマスク(※)*– MACアドレスのビットマスク(16進形式)
- *vid* – VLAN ID (範囲:1～4094)
- *VID上限* – VID範囲の上限 (範囲:1～4094)
- *プロトコル* – 特定のイーサネットプロトコル番号 (範囲:0～65535)
- *プロトコル上限* – プロトコル範囲の上限 (範囲:0～65535)

※1 すべてのビットマスクに関して、「1」は注意、「0」は無視の意味です。

**デフォルト設定**

なし

**コマンドモード**

MAC ACL

**コマンドの使用方法**

- 新規のルールはリストの最後に追加されます。
- ethertypeオプションは、イーサネットII形式のパケットのフィルタリングのみに使用できます。
- イーサネットプロトコルタイプの詳細なリストは、RFC 1060にあります。比較的一般的なタイプは、以下のとおりです。
  - 0800 - IP
  - 0806 - ARP
  - 8137 - IPX

**例**

以下のルールでは、任意の送信元MACアドレスからのパケットを、送信先アドレス 00-90-cc-94-34-de (イーサネットタイプ0800)に送信できます。

```
Console(config-mac-acl)#permit any host 00-90-cc-94-34-de ethertype 0800
Console(config-mac-acl)#
```

**関連コマンド**

access-list mac (p.350)

### show mac access-list

設定済みのMAC ACLのルールを表示します。

**構文**

show mac access-list [*ACL名*]

*ACL名* - ACLの名前 (最大設定:16文字)

**コマンドモード**

Privileged Exec

### 例

```
Console#show mac access-list
MAC access-list jerry:
   permit any host 00-90-cc-94-34-de ethertype 800 800
Console#
```

### 関連コマンド

permit、deny (p.351)
mac access-group (p.353)

## mac access-group

MAC ACLにポートをバインドします。 ポートを削除するには**no**形式を使用します。

### 構文

**mac access-group** *ACL名* **in**

- *ACL名* - ACLの名前 (最大設定:16文字)
- **in** - このリストが着信パケットに適用されることを表示

### デフォルト設定

なし

### コマンドモード

Interface Configuration (イーサネット)

**コマンドの使用方法**

- 1つのポートは、1つのACLのみにバインドできます。
- すでにACLにバインドされているポートを別のACLにバインドすると、古いバインドは新しいバインドに置き換えられます。

**例**

```
Console(config)#interface ethernet 1/25
Console(config-if)#mac access-group jerry in
Console(config-if)#
```

**関連コマンド**

show mac access-list (4-106)

### show mac access-group

MAC ACLに割り当てられているポートを表示します。

**コマンドモード**

Privileged Exec

**例**

```
Console#show mac access-group
Interface ethernet 1/1
  MAC access-list jerry in
.
.
.
Interface ethernet 1/26
  MAC access-list jerry in
Console#
```

**関連コマンド**

mac access-group (p.353)

### map access-list mac

ACLルールに一致するパケットの出力キューを設定します。 指定したCoS値は、一致するパケットを出力キューにマッピングする目的のみに使用され、パケット自体には書き込まれません。 CoSマッピングを削除するには**no**形式を使用します。

### 構文

[no] map access-list mac *ACL名* cos *CoS値*

- *ACL名* – ACLの名前 (最大設定:16文字)
- *CoS値* – CoS値 (範囲:0～7)

### デフォルト設定

なし

### コマンドモード

Interface Configuration (イーサネット)

### コマンドの使用方法

- CoS値をルールにマッピングする前に、ACLマスクを設定する必要があります。
- 以下に示すように、指定したACL内のルールに一致するパケットがいずれかの出力キューにマッピングされます。

**表 4-37 送信キュー優先度マッピング**

| キュー | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 優先度 | 1,2 | 0,3 | 4,5 | 6,7 |

### 例

```
Console(config)#int eth 1/5
Console(config-if)#map access-list mac jerry cos 0
Console(config-if)#
```

### 関連コマンド

queue cos-map (p.438)
show map access-list mac (p.355)

## show map access-list mac

現在のインタフェースに関してMAC ACLにマッピングされているCoS値を表示します (CoS値によって、ACLルールに一致するパケットの出力キューが決定)。

### 構文

show map access-list mac [*インタフェース*]

*インタフェース*

- ethernet *ユニット/ポート*
  - *ユニット* – スタックユニット (範囲:1～8)

- *ポート* - ポート番号

**コマンドモード**

Privileged Exec

**例**

```
Console#show map access-list mac
Eth 1/5
 access-list mac jerry cos 0
Console#
```

**関連コマンド**

map access-list mac (p.354)

## ACL情報

表 4-38 ACL情報

| コマンド | 機能 | モード | ページ |
|---|---|---|---|
| show access-list | すべてのACLおよび関連するルールを表示 | PE | 356 |
| show access-group | 各ポートに割り当てられているACLを表示 | PE | 357 |

### show access-list

すべてのACLおよび関連するルールと、ユーザ定義のすべてのマスクを表示します。

**コマンドモード**

Privileged Exec

**コマンドの使用方法**

ACLがインタフェースにバインドされると(ACLがアクティブな状態)、ルールの表示順序は関連するマスクによって決定します。

**例**

```
Console#show access-list
IP standard access-list david:
   permit host 10.1.1.21
   permit 168.92.16.0 255.255.240.0
IP extended access-list bob:
   permit 10.7.1.1 255.255.255.0 any
   permit 192.168.1.0 255.255.255.0 any destination-port 80 80
   permit 192.168.1.0 255.255.255.0 any protocol tcp control-code 2 2
MAC access-list jerry:
   permit any host 00-90-cc-94-34-de ethertype 800 800
IP extended access-list A6:
   deny tcp any any control-flag 2 2
   permit any any
Console#
```

### show access-group

ACLへのポート割り当てを表示します。

**コマンドモード**

Privileged Executive

**例**

```
Console#show access-group
Interface ethernet 1/1
  MAC access-list jerry in
.
.
.
Interface ethernet 1/26
  MAC access-list jerry in
Console#
```

# SNMPコマンド

Simple Network Management Protocol (SNMP)を使用した管理ステーションから本製品へのアクセスおよびトラップマネージャに送信されるエラータイプを制御します。

表 4-39 SNMPコマンド

| コマンド | 機能 | モード | ページ |
|---|---|---|---|
| snmp-server community | SNMPコマンドへのアクセスを許可するコミュニティアクセス文字列を設定 | GC | 358 |
| snmp-server contact | システムの連絡先の文字列を設定 | GC | 359 |
| snmp-server location | システムの場所の文字列を設定 | GC | 359 |
| snmp-server host | SNMP通知の受信者を指定 | GC | 360 |
| snmp-server enable traps | SNMPトラップの送信を有効化 (SNMP通知) | GC | 361 |
| show snmp | SNMP通信のステータスを表示 | NE、PE | 362 |

## snmp-server community

Simple Network Management Protocolのコミュニティアクセス文字列を定義します。 指定したコミュニティ文字列を削除するには**no**形式を使用します。

### 構文

**snmp-server community** *文字列* [**ro**|**rw**]
**no snmp-server community** *文字列*

- *文字列* – パスワードのような役割を果たし、SNMPプロトコルへのアクセスを許可するコミュニティ文字列 (最大設定:32文字、大文字小文字を区別、最大文字数:5)
- **ro** – 読み込み専用(read-only)アクセスを指定。 承認されている管理ステーションでは、MIBオブジェクトの取得のみが可能です。
- **rw** – 読み込み/書き込み(read/write)アクセスを指定。 承認されている管理ステーションでは、MIBオブジェクトの取得と変更の両方が可能です。

### デフォルト設定

- パブリック – 読み込み専用アクセス。 承認されている管理ステーションでは、MIBオブジェクトの取得のみが可能
- プライベート – 読み込み/書き込みアクセス。 承認されている管理ステーションでは、MIBオブジェクトの取得と変更の両方が可能

**コマンドモード**

Global Configuration

**コマンドの使用方法**

最初の**snmp-server community**コマンドを入力すると、SNMPが有効になります。 **no snmp-server community**コマンドを使用すると、SNMPが無効になります。

**例**

```
Console(config)#snmp-server community alpha rw
Console(config)#
```

### snmp-server contact

システムの連絡先の文字列を設定します。 システムの連絡先情報を削除するには**no**形式を使用します。

**構文**

**snmp-server contact** *文字列*
**no snmp-server contact**

*文字列* - システムの連絡先情報を説明する文字列（最大設定：255文字）

**デフォルト設定**

なし

**コマンドモード**

Global Configuration

**例**

```
Console(config)#snmp-server contact Paul
Console(config)#
```

**関連コマンド**

snmp-server location (p.359)

### snmp-server location

システムの場所の文字列を設定します。 場所の文字列を削除するには**no**形式を使用します。

**構文**

**snmp-server location** *テキスト*
**no snmp-server location**

*テキスト* - システムの場所を説明する文字列 (最大設定:255文字)

**デフォルト設定**

なし

**コマンドモード**

Global Configuration

**例**

```
Console(config)#snmp-server location WC-19
Console(config)#
```

**関連コマンド**

snmp-server contact (p.359)

### snmp-server host

Simple Network Management Protocol通知の受信者を指定します。 指定したホストを削除するには**no**形式を使用します。

**構文**

**snmp-server host** *ホストアドレス コミュニティ文字列* [**version** {**1** | **2c**}]
**no snmp-server host** *ホストアドレス*

- *ホストアドレス* - ホスト(ターゲットの受信者)のインターネットアドレス (ホストアドレスの最大数:5つのトラップ送信先IPアドレスエントリ)
- *コミュニティ文字列* - 通知と共に送信される、パスワードのようなコミュニティ文字列。 この文字列は、**snmp-server host**コマンド自体を使用して設定することもできますが、**snmp-server host**コマンドを使用する前に**snmp-server community**コマンドを使用してこの文字列を定義することをおすすめします (最大設定:32文字)。
- **version** - SNMP v1、v2cのどちらのトラップとして通知を送信するか指定 (範囲:1、2c、デフォルト:1)

**デフォルト設定**

ホストアドレス: なし
SNMPバージョン: 1

**コマンドモード**

Global Configuration

**コマンドの使用方法**

- **snmp-server host**コマンドを入力しない場合、通知は送信されません。 SNMP通

知を送信するように本製品を設定するには、**snmp-server host**コマンドを1つ以上入力する必要があります。 複数のホストを有効にするには、**snmp-server host**コマンドをホストごとに別々に発行する必要があります。

・**snmp-server host**コマンドは、**snmp-server enable traps**コマンドと共に使用します。 **snmp-server enable traps**コマンドでは、グローバルに送信するSNMP通知を指定します。 任意のホストで通知を受信するには、**snmp-server enable traps**コマンドを1つ以上と、そのホスト用の**snmp-server host**コマンドを有効にする必要があります。

・ 一部の通知タイプは、**snmp-server enable traps**コマンドでは制御できません。 たとえば、常に有効になっている通知タイプが一部あります。

・ 本製品では、管理ステーションが対応しているSNMPバージョンによって、SNMPバージョン1またはバージョン2cの通知をホストIPアドレスに送信・ できます。 snmp-server hostコマンドでSNMPバージョンを指定しない場合は、デフォルトでSNMPバージョン1の通知が送信されます。

**例**

```
Console(config)#snmp-server host 10.1.19.23 batman
Console(config)#
```

**関連コマンド**

snmp-server enable traps (p.361)

**snmp-server enable traps**

本製品から、Simple Network Management Protocol (SNMP)トラップ(SNMP通知)を送信できるようにします。 SNMP通知を無効にするには**no**形式を使用します。

**構文**

[**no**] **snmp-server enable traps** [**authentication** | **link-up-down**]

- **authentication** – 認証失敗トラップを発行するキーワード
- **link-up-down** – リンクアップまたはリンクダウンのトラップを発行するキーワード

**デフォルト設定**

認証トラップおよびリンクアップ/ダウントラップを発行

**コマンドモード**

Global Configuration

**コマンドの使用方法**

- **snmp-server enable traps**コマンドを入力しない場合、このコマンドで制御される通知は送信されません。 SNMP通知を送信するように本製品を設定するには、**snmp-server enable traps**コマンドを1つ以上入力する必要があります。 このコマンドをキーワードなしで入力すると、認証通知とリンクアップ/ダウン通知の両方が有

効になります。 キーワードを指定してこのコマンドを入力すると、そのキーワードに関連する通知タイプのみが有効になります。

・**snmp-server enable traps**コマンドは、**snmp-server host**コマンドと共に使用します。**snmp-server host**コマンドでは、SNMP通知を受信するホスト(1台または複数)を指定します。 通知を送信するには、**snmp-server host**コマンドを1つ以上設定する必要があります。

**例**

```
Console(config)#snmp-server enable traps link-up-down
Console(config)#
```

**関連コマンド**

snmp-server host (p.360)

**show snmp**

SNMP通信のステータスをチェックします。

**デフォルト設定**

なし

**コマンドモード**

Normal Exec、Privileged Exec

**コマンドの使用方法**

このコマンドを実行すると、コミュニティアクセス文字列の情報、SNMP入力出力プロトコルデータユニットのカウンタ情報、およびSNMPログが**snmp-server enable traps**コマンドで有効になっているかどうかが表示されます。

**例**

```
Console#show snmp


SNMP traps:
  Authentication: enabled
  Link-up-down:     enabled


SNMP communities:
     1. private, and the privilege is read-write
     2. public, and the privilege is read-only


0 SNMP packets input
       0 Bad SNMP version errors
       0 Unknown community name
       0 Illegal operation for community name supplied
       0 Encoding errors
       0 Number of requested variables
       0 Number of altered variables
       0 Get-request PDUs
       0 Get-next PDUs
       0 Set-request PDUs
0 SNMP packets output
       0 Too big errors
       0 No such name errors
       0 Bad values errors
       0 General errors
       0 Response PDUs
       0 Trap PDUs


SNMP logging: disabled
Console#
```

# インタフェースコマンド

以下のコマンドを使用して、イーサネットポート、トランク、VLANの通信パラメータを表示または設定します。

表 4-40 インタフェースコマンド

| コマンド | 機能 | モード | ページ |
|---|---|---|---|
| interface | インタフェースタイプを設定してインタフェース設定モードに移行 | GC | 365 |
| description | インタフェース設定に説明を追加 | IC | 366 |
| speed-duplex | オートネゴシエーション無効時に、与えられたインタフェースの速度およびデュープレックスの動作を設定 | IC | 367 |
| negotiation | 与えられたインタフェースのオートネゴシエーションを有効化 | IC | 368 |
| capabilities | オートネゴシエーションで使用できる与えられたインタフェースの機能を通知 | IC | 369 |
| flowcontrol | 与えられたインタフェースのフローコントロールを有効化 | IC | 370 |
| shutdown | インタフェースを無効化 | IC | 371 |
| switchport broadcast packet-rate | ブロードキャストストーム制御のしきい値を設定 | IC | 373 |
| clear counters | インタフェースの統計を消去 | PE | 373 |
| show interfaces status | 指定したインタフェースのステータスを表示 | NE、PE | 374 |
| show interfaces counters | 指定したインタフェースの統計を表示 | NE、PE | 375 |
| show interfaces switchport | 任意のインタフェースの管理および運用のステータスを表示 | NE、PE | 377 |

### interface

インタフェースタイプを設定してインタフェース設定モードに移行します。 トランクを削除するにはno形式を使用します。

### 構文

**interface** *インタフェース*
**no interface port-channel** *チャネルID*

*インタフェース*

- **ethernet** *ユニット/ポート*
  - *ユニット* - スタックユニット（範囲：1～8）
  - *ポート* - ポート番号（範囲：1～26）
- **port-channel** *チャネルID*（範囲：1～4）
- **vlan** *VLAN ID*（範囲：1～4094）

### デフォルト設定

なし

### コマンドモード

Global Configuration

### 例

ポート24を指定するには、以下のコマンドを入力します。

```
Console(config)#interface ethernet 1/24
Console(config-if)#
```

## description

インタフェースに説明を追加します。 説明を削除するには**no**形式を使用します。

### 構文

**description** *文字列*
**no description**

*string* - このインタフェースに何が追加されているかに関するコメントまたは説明（範囲：1～64文字）

### デフォルト設定

なし

### コマンドモード

Interface Configuration（イーサネット、ポートチャネル）

### 例

以下の例では、ポート24に説明を追加します。

```
Console(config)#interface ethernet 1/24
Console(config-if)#description RD-SW#3
Console(config-if)#
```

### speed-duplex

オートネゴシエーション無効時に、与えられたインタフェースの速度およびデュープレックスのモードを設定します。 デフォルトを復元するには**no**形式を使用します。

### 構文

**speed-duplex** {**1000full** | **100full** | **100half** | **10full** | **10half**}
**no speed-duplex**

- **1000full** - 1000Mbps全二重通信に設定
- **100full** - 100Mbps全二重通信に設定
- **100half** - 100Mbps半二重通信に設定
- **10full** - 10Mbps全二重通信に設定
- **10half** - 10Mbps半二重通信に設定

### デフォルト設定

- オートネゴシエーションはデフォルトで有効
- オートネゴシエーション無効時のspeed-duplexのデフォルトの設定は、100BASE-TXポートの場合は100half、ギガビットイーサネットポートの場合は1000full

### コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

### コマンドの使用方法

- 強制的に**speed-duplex**コマンドで指定した速度およびデュープレックスモードに設定するには、**no negotiation**コマンドを使用し、選択したインタフェースでオートネゴシエーションを無効にします。
- **negotiation**コマンドを使用してオートネゴシエーションを有効にするとき、**capabilities**コマンドによって最適な設定が決定されます。 オートネゴシエーションで速度/デュープレックスモードを設定するには、インタフェースの機能リストで必要なモードを指定する必要があります。

### 例

以下の例では、ポート5を100Mbps半二重通信に設定します。

```
Console(config)#interface ethernet 1/5
Console(config-if)#speed-duplex 100half
Console(config-if)#no negotiation
Console(config-if)#
```

### 関連コマンド

negotiation (p.368)
capabilities (p.369)

## negotiation

与えられたインタフェースのオートネゴシエーションを有効にします。 オートネゴシエーションを無効にするには**no**形式を使用します。

### 構文

[**no**] **negotiation**

### デフォルト設定

有効

### コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

### コマンドの使用方法

- オートネゴシエーションが有効な場合は、**capabilities**コマンドに基づいてリンクに最適な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が無効な場合は、**speed-duplex**コマンドおよび**flowcontrol**コマンドを使用して、リンク属性を手動で指定する必要があります。
- オートネゴシエーションが無効な場合、RJ-45ポートに関してオートMDI/MDI-Xピン信号設定も無効になります。

### 例

以下の例では、オートネゴシエーションを使用するようにポート11を設定します。

```
Console(config)#interface ethernet 1/11
Console(config-if)#negotiation
Console(config-if)#
```

### 関連コマンド

capabilities (p.369)
speed-duplex (p.367)

### capabilities

オートネゴシエーション中に与えられたインタフェースのポート機能を通知します。 通知した機能を削除するには**no**形式にパラメータを指定して使用し、デフォルト値を復元するには**no**形式をパラメータなしで使用します。

### 構文

[**no**] **capabilities** {**1000full** | **100full** | **100half** | **10full** | **10half** | **flowcontrol** | **symmetric**}

- **1000full** - 1000Mbps全二重通信に対応
- **100full** - 100Mbps全二重通信に対応
- **100half** - 100Mbps半二重通信に対応
- **10full** - 10Mbps全二重通信に対応
- **10half** - 10Mbps半二重通信に対応
- **flowcontrol** - フローコントロールに対応
- **symmetric** (ギガビットのみ) - 指定した場合、このポートがポーズフレームを送受信、指定しない場合、ポートはオートネゴシエーションを行い、非対称ポーズフレームの送信者および受信者を決定 (*現在のスイッチASICは、対称ポーズフレームのみに対応*)

### デフォルト設定

- 100BASE-TX： 10half、10full、100half、100full
- 1000BASE-T： 10half、10full、100half、100full、1000full
- SFP： 1000full

### コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

### コマンドの使用方法

**negotiation**コマンドでオートネゴシエーションが有効な場合は、**capabilities**コマンドに基づいてリンクに最適な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が無効な場合は、**speed-duplex**コマンドおよび**flowcontrol**コマンドを使用して、リンク属性を手動で指定する必要があります。

### 例

以下の例では、イーサネットポート5の機能を100half、100full、flow controlに設定します。

```
Console(config)#interface ethernet 1/5
Console(config-if)#capabilities 100half
Console(config-if)#capabilities 100full
Console(config-if)#capabilities flowcontrol
Console(config-if)#
```

### 関連コマンド

negotiation (p.368)
speed-duplex (p.367)
flowcontrol (p.370)

## flowcontrol

フローコントロールを有効にします。 フローコントロールを無効にするには**no**形式を使用します。

### 構文

[**no**] **flowcontrol**

### デフォルト設定

無効

### コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

### コマンドの使用方法

- フローコントロールを使用すると、本製品のバッファが一杯になったときに、本製品に直接接続されている末端ステーションまたはセグメントからのトラフィックをブロックすることにより、フレームの損失を防止できます。 これを有効にすると、半二重通信の場合はバックプレッシャーが、全二重通信の場合はIEEE 802.3xが使用されます。
- **flowcontrol**コマンドまたは**no flowcontrol**コマンドでフローコントロールを強制的に有効または無効にするには、**no negotiation**コマンドを使用して、選択したインタフェースでオートネゴシエーションを無効にします。
- **negotiation**コマンドを使用してオートネゴシエーションを有効にするとき、**capabilities**コマンドによって最適な設定が決定されます。 オートネゴシエーションでフローコントロールを有効にするには、任意のポートの機能リストに「flowcontrol」を含める必要があります。
- 問題解決のために必要な場合を除き、ハブに接続されているポートではフローコントロールの使用は避けてください。 使用すると、バックプレッシャー信号の混雑により、ハブに接続されているセグメントの全体的なパフォーマンスが低下する場合があります。

### 例

以下の例では、ポート5でフローコントロールを有効にします。

```
Console(config)#interface ethernet 1/5
Console(config-if)#flowcontrol
Console(config-if)#no negotiation
Console(config-if)#
```

### 関連コマンド

negotiation (p.368)
capabilities (flowcontrol、symmetric) (p.369)

## shutdown

インタフェースを無効にします。 無効にしたインタフェースを再起動するには、**no**形式を使用します。

### 構文

[**no**] **shutdown**

### デフォルト設定

すべてのインタフェースが有効

**コマンドモード**

Interface Configuration (イーサネット、ポートチャネル)

**コマンドの使用方法**

このコマンドを使用すると、動作が異常(競合が過剰など)なポートを無効にし、問題解決後に再度有効にすることができます。 また、セキュリティ上の理由でポートを無効にすることもできます。

**例**

以下の例は、ポート5を無効にします。

```
Console(config)#interface ethernet 1/5
Console(config-if)#shutdown
Console(config-if)#
```

### switchport broadcast packet-rate

ブロードキャストストーム制御を設定します。 ブロードキャストストーム制御を無効にするにはno形式を使用します。

#### 構文

**switchport broadcast octet-rate** *速度*
**no switchport broadcast**

*速度* - 速度(オクテット/秒)のしきい値レベル
(範囲:64～95232000)

#### デフォルト設定

すべてのポートに関して有効
パケット速度制限: 32000オクテット/秒

#### コマンドモード

Interface Configuration (イーサネット)

#### コマンドの使用方法

- ブロードキャストトラフィックが指定したしきい値を超えると、しきい値を超えるパケットが削除されます。
- このコマンドでは、選択したインタフェースのブロードキャストストーム制御を有効または無効にできます。 ただし、指定したしきい値は本製品のすべてのポートに適用されます。

#### 例

以下は、ブロードキャストストーム制御を600パケット/秒に設定する方法を示しています。

```
Console(config)#interface ethernet 1/5
Console(config-if)#switchport broadcast octet-rate 600
Console(config-if)#
```

### clear counters

インタフェースの統計を消去します。

#### 構文

**clear counters** *インタフェース*

*インタフェース*

- **ethernet** *ユニット/ポート*
  - *ユニット* - スタックユニット (範囲:1～8)

- *ポート* - ポート番号（範囲：1～26）
- **port-channel** *チャネルID*（範囲：1～4）

**デフォルト設定**

なし

**コマンドモード**

Privileged Exec

**コマンドの使用方法**

統計は、電源リセット時にのみ初期化されます。 このコマンドを使用すると、現在の管理セッションに関して、表示されている統計の基本値がゼロに設定されます。 ただし、管理インタフェースをいったんログアウトしてからログインしなおすと、表示される統計は、前回の電源リセット以降に累計された絶対値になります。

**例**

以下の例では、ポート5の統計を消去します。

```
Console#clear counters ethernet 1/5
Console#
```

### show interfaces status

インタフェースのステータスを表示します。

**構文**

**show interfaces status** [*インタフェース*]

*インタフェース*

- **ethernet** *ユニット/ポート*
  - *ユニット* - スタックユニット（範囲：1～8）
  - *ポート* - ポート番号（範囲：1～26）
- **port-channel** *チャネルID*（範囲：1～4）
- **vlan** *VLAN ID*（範囲：1～4094）

**デフォルト設定**

すべてのインタフェースのステータスを表示

**コマンドモード**

Normal Exec、Privileged Exec

### コマンドの使用方法

インタフェースを指定しない場合は、すべてのインタフェースの情報が表示されます。このコマンドで表示される項目の詳細については、117ページの「接続ステータスの表示」を参照してください。

### 例

```
Console#show interfaces status ethernet 1/5
Information of Eth 1/5
  Basic information:
    Port type:                  100TX
    Mac address:                00-90-CC-12-34-61
  Configuration:
    Name:
    Port admin:                 Up
    Speed-duplex:               Auto
    Capabilities:               10half, 10full, 100half, 100full,
    Broadcast storm:            Enabled
    Broadcast storm limit:  32000 octets/second
    Flow control:               Disabled
    Lacp:                       Disabled
    Port security:              Disabled
    Max MAC count:              0
    Port security action:   None
  Current status:
    Link status:                Up
    Port operation status:  Up
    Operation speed-duplex: 100full
    Flow control type:      None
Console#show interfaces status vlan 1
  Information of VLAN 1
  MAC address:                  00-90-CC-12-34-56
Console#
```

## show interfaces counters

インタフェースの統計を表示します。

### 構文

**show interfaces counters** [*インタフェース*]

*インタフェース*

- **ethernet** *ユニット/ポート*
  - *ユニット* - スタックユニット (範囲:1～8)
  - *ポート* - ポート番号 (範囲:1～26)
- **port-channel** *チャネルID* (範囲:1～4)

### デフォルト設定

すべてのインタフェースのカウンタを表示

### コマンドモード

Normal Exec、Privileged Exec

### コマンドの使用方法

インタフェースを指定しない場合は、すべてのインタフェースの情報が表示されます。このコマンドで表示される項目の詳細については149ページの「ポート統計の表示」を参照してください。

### 例

```
Console#show interfaces counters ethernet 1/7
Ethernet 1/7
  Iftable stats:
    Octets input: 30658, Octets output: 196550
    Unicast input: 6, Unicast output: 5
    Discard input: 0, Discard output: 0
    Error input: 0, Error output: 0
    Unknown protos input: 0, QLen output: 0
  Extended iftable stats:
    Multi-cast input: 0, Multi-cast output: 3064
    Broadcast input: 262, Broadcast output: 1
  Ether-like stats:
    Alignment errors: 0, FCS errors: 0
    Single Collision frames: 0, Multiple collision frames: 0
    SQE Test errors: 0, Deferred transmissions: 0
    Late collisions: 0, Excessive collisions: 0
    Internal mac transmit errors: 0, Internal mac receive errors: 0
    Frame too longs: 0, Carrier sense errors: 0
    Symbol errors: 0
  RMON stats:
    Drop events: 0, Octets: 227208, Packets: 3338
    Broadcast pkts: 263, Multi-cast pkts: 3064
    Undersize pkts: 0, Oversize pkts: 0
    Fragments: 0, Jabbers: 0
    CRC align errors: 0, Collisions: 0
    Packet size <= 64 octets: 3150, Packet size 65 to 127 octets: 139
    Packet size 128 to 255 octets: 49, Packet size 256 to 511 octets: 0
    Packet size 512 to 1023 octets: 0, Packet size 1024 to 1518 octets: 0
Console#
```

**show interfaces switchport**
指定したインタフェースの管理および運用のステータスを表示します。

**構文**

**show interfaces switchport** [*インタフェース*]

*インタフェース*

- **ethernet** *ユニット/ポート*
  - *ユニット* - スタックユニット (範囲:1～8)
  - *ポート* - ポート番号 (範囲:1～26)
- **port-channel** *チャネルID* (範囲:1～4)

**デフォルト設定**

すべてのインタフェースを表示

**コマンドモード**

Normal Exec、Privileged Exec

**コマンドの使用方法**

インタフェースを指定しない場合は、すべてのインタフェースの情報が表示されます。

**例**

以下の例は、ポート24の設定を示しています。

```
Console#show interfaces switchport ethernet 1/24
 Broadcast threshold:              Enabled, 32000 octets/second
 LACP status:                        Enabled
 Ingress rate limit: disable, Level: 30
 Egress rate limit: disable, Level: 30
 VLAN membership mode:               Hybrid
 Ingress rule:                     Disabled
 Acceptable frame type:            All frames
 Native VLAN:                        1
 Priority for untagged traffic: 0
 Gvrp status:                      Disabled
 Allowed Vlan:                     1(u),
 Forbidden Vlan:
 Private-VLAN mode:                  NONE
 Private-VLAN host-association: NONE
 Private-VLAN mapping:               NONE
Console#
```

表 4-41　　インタフェーススイッチポート統計

| フィールド | 説明 |
|---|---|
| Broadcast threshold | ブロードキャストストーム抑制が有効か無効かを表示し、有効な場合はしきい値レベルも表示(373ページ) |
| Lacp status | Link Aggregation Control Protocolが有効か無効かを表示(386ページ) |
| Ingress/Egress rate limit | 速度制限が有効かどうか、および現在の速度制限を表示( 381ページ) |
| VLAN membership mode | メンバシップモード(TrunkまたはHybrid)を表示(416ページ) |
| Ingress rule | 着信フィルタリングが有効か無効かを表示(418ページ) |
| Acceptable frame type | 受け入れ可能なVLANフレームにすべてのタイプが含まれるか、タグ付きフレームのみかを表示(417ページ) |
| Native VLAN | デフォルトのポートVLAN IDを表示(419ページ) |
| Priority for untagged traffic | タグ無しフレームのデフォルトの優先度を表示(435ページ) |
| Gvrp status | GARP VLAN登録プロトコルが有効か無効かを表示(430ページ) |
| Allowed Vlan | このインタフェースが割り当てられているVLANを表示。「(u)」はタグ無し、「(t)」はタグ付きを表す(420ページ) |
| Forbidden Vlan | このインタフェースがGVRP経由で動的に割り当てられないVLANを表示(421ページ) |
| Private VLAN mode | プライベートVLANのモード(host (ホスト)、promiscuous (無差別)、none(なし))を表示(426ページ) |
| Private VLAN host-association | このポートが関連付けられているセカンダリ(またはコミュニティ) VLANを表示(426ページ) |
| Private VLAN mapping | 無差別ポートのプライマリVLANマッピングを表示(429ページ) |

# ミラーポートコマンド

本セクションでは、ソース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方法について解説します。

**表 4-42　ミラーポートコマンド**

| コマンド | 機能 | モード | ページ |
|---|---|---|---|
| port monitor | ミラーセッションを設定 | IC | 379 |
| show port monitor | ミラーポートの設定を表示 | PE | 380 |

### port monitor

ミラーセッションを設定します。 ミラーセッションを消去するには**no**形式を使用します。

#### 構文

**port monitor** *インタフェース* [**rx** | **tx**]
**no port monitor** *インタフェース*

- *インタフェース* – **ethernet** *ユニット/ポート* (ソースポート)
  - *ユニット* – スタックユニット (範囲:1～8)
  - *ポート* – ポート番号 (範囲:1～26)
- **rx** – 受信パケットをミラーリング
- **tx** – 送信パケットをミラーリング

#### デフォルト設定

ミラーリングセッションは未定義

#### コマンドモード

Interface Configuration (イーサネット、送信先ポート)

#### コマンドの使用方法

- 任意の送信元ポートから送信先ポートへのトラフィックを、リアルタイム分析のためにミラーリングできます。 次に、ロジックアナライザまたはRMONプローブを送信先ポートに接続し、送信元ポートを通過するトラフィックを、まったく邪魔にならない方法で調査することができます。
- 送信先ポートは、イーサネットインタフェースを指定することによって設定します。
- ミラーポートとモニタポートの速度は一致させる必要があります。一致しない場合、トラフィックがモニタポートから削除されることがあります。
- ミラーセッションは複数作成できますが、すべてのセッションで同じ送信先ポートを

共有する必要があります。 ただし、複数の送信元ポートから送信先ポートへ送信するトラフィックが過剰にならないようにする必要があります。

**例**

以下の例では、ポート6で受信したパケットをポート11へミラーリングするように本製品を設定します。

```
Console(config)#interface ethernet 1/11
Console(config-if)#port monitor ethernet 1/6 rx
Console(config-if)#
```

### show port monitor

ミラー情報を表示します。

**構文**

show port monitor [*インタフェース*]

*インタフェース* - **ethernet** *ユニット/ポート* (ソースポート)

- *ユニット* - スタックユニット (範囲:1～8)
- *ポート* - ポート番号 (範囲:1～26)

**デフォルト設定**

すべてのセッションを表示

**コマンドモード**

Privileged Exec

**コマンドの使用方法**

現在設定されている送信元ポート、送信先ポート、およびミラーモード(RX、TX)を表示します。

**例**

以下は、ポート11で設定されているミラーリングを示しています。

```
Console(config)#interface ethernet 1/11
Console(config-if)#port monitor ethernet 1/6 rx
Console(config-if)#end
Console#show port monitor
Port Mirroring
-------------------------------------
 Destination port(listen port):Eth1/11
 Source port(monitored port)   :Eth1/6
 Mode                          :RX
Console#
```

# 速度制限コマンド

この機能を使用すると、ネットワーク管理者は、任意のインタフェースで送受信するトラフィックの最大速度を制御できます。 速度制限をネットワークの末端にあるインタフェースで設定すると、ネットワークへ、またはネットワークからのトラフィックを制限できます。 速度制限内のトラフィックは送信されますが、トラフィックの許容量を超えているパケットは削除されます。

速度制限は、個々のポートまたはトランクに対して適用できます。 インタフェースをこの機能で設定すると、トラフィックの速度がハードウェアで監視され、条件を満たしているかどうかの確認が行われます。 条件を満たしていないトラフィックは削除され、条件を満たしているトラフィックは変更なしで転送されます。

**注意:** 「速度制限精度」と「速度制限」( 382ページ)を掛け合わせると、インタフェースの実際の速度制限が設定されます。 この精度は、ファストイーサネットまたはギガビットイーサネットのインタフェースに適用されるグローバル設定です。

**表 4-43 速度制限コマンド**

| コマンド | 機能 | モード | ページ |
|---|---|---|---|
| rate-limit | 任意のポートの最大の入出力速度を設定 | IC | 381 |
| rate-limit granularity | ファストイーサネットおよびギガビットイーサネットの精度を設定 | IC | 382 |
| show rate-limit | 速度制限精度を表示 | PE | 383 |

### rate-limit

特定のインタフェースの速度制限レベルを定義します。 速度を指定せずにこのコマンドを使用すると、デフォルトの速度制限レベルが復元されます。 デフォルトのステータス(無効)を復元するにはno形式を使用します。

#### 構文

**rate-limit** {**input** | **output**} **level** [*速度*]
**no rate-limit** {**input** | **output**}

- **input** - 入力速度
- **output** - 出力速度
- *速度* - 最大値 (範囲:1～30)

#### デフォルト設定

30

**コマンドモード**

Interface Configuration (イーサネット、ポートチャネル)

**コマンドの使用方法**

実際の速度制限 = 速度制限レベル × 精度

**例**

```
Console(config)#interface ethernet 1/1
Console(config-if)#rate-limit input level 20
Console(config-if)#
```

### rate-limit granularity

ファストイーサネットポートおよびギガビットイーサネットポートの速度制限精度を定義します。 デフォルト設定を復元するには、このコマンドのno形式を使用します。

**構文**

**rate-limit** {**fastethernet** | **gigabitethernet**} **granularity** [*精度*]
**no rate-limit** {**fastethernet** | **gigabitethernet**} **granularity**

- **fastethernet** - ファストイーサネットの精度
- **gigabitethernet** - ギガビットイーサネットの精度
- *精度* - システムの速度制限精度を設定。 ファストイーサネットの場合は、512Kbps、1Mbps、3.3Mbpsのいずれかを選択します。 ギガビットイーサネットの場合、サポートされている制度オプションは33.3Mbpsのみとなります。

**デフォルト設定**

ファストイーサネットインタフェース - 3.3Mbps
ギガビットイーサネットインタフェース - 33.3Mbps

**コマンドモード**

Global Configuration (イーサネット、ポートチャネル)

**コマンドの使用方法**

実際の速度制限 = 速度制限レベル × 精度

**例**

以下では、ファストイーサネットの精度を1Mbpsに、ギガビットイーサネットの精度を33.3Mbpsに設定します。

```
Console(config)#rate-limit fastethernet granularity 1000
Console(config)#rate-limit gigabitethernet granularity 33300
Console(config)#
```

### show rate-limit

速度制限の精度を表示します。

**デフォルト設定**

ファストイーサネットインタフェース – 3.3Mbps
ギガビットイーサネットインタフェース – 33.3Mbps

**コマンドモード**

Privileged Exec

**コマンドの使用方法**

- ファストイーサネットインタフェースの場合、速度制限の精度は512Kbps、1Mbps、3.3Mbpsのいずれかに設定できます。
- ギガビットイーサネットインタフェースの場合、速度制限の精度は33.3Mbpsです。

**例**

```
Console#show rate-limit

Fast ethernet granularity:  1000

Gigabit ethernet granularity:  33300
Console#
```

# リンクアグリゲーション

複数のポートを1つの集合リンク(トランク)に静的にグループ化すると、ネットワーク接続の帯域幅を拡大することや、障害回復に役立てることができます。 また、Link Aggregation Control Protocol (LACP)を使用して、本製品と別のネットワーク機器の間のトランクリンクを自動的にネゴシエーションすることができます。 静的トランクの場合、すべてのスイッチがCisco EtherChannel標準に準拠している必要があります。 動的トランクの場合、すべてのスイッチがLACPに準拠している必要があります。 本製品は、最大4つのトランクに対応しています。 たとえば、1000Mbpsのポート2つで構成されているトランクを全二重で実行すると、合計4Gbpsの帯域幅に対応できます。

表 4-44 リンクアグリゲーションコマンド

| コマンド | 機能 | モード | ページ |
|---|---|---|---|
| *手動設定コマンド* | | | |
| interface port-channel | トランクを設定し、トランク用のインタフェース設定モードに移行 | GC | 365 |
| channel-group | トランクにポートを追加 | IC (イーサネット) | 385 |
| *動的設定コマンド* | | | |
| lacp | 現在のインタフェース用のLACPを設定 | IC (イーサネット) | 386 |
| lacp system-priority | ポートのLACPシステム優先度を設定 | IC (イーサネット) | 387 |
| lacp admin-key | ポートの管理キーを設定 | IC (イーサネット) | 388 |
| lacp admin-key | ポートチャネルの管理キーを設定 | IC (ポートチャネル) | 389 |
| lacp port-priority | ポートのLACPポート優先度を設定 | IC (イーサネット) | 390 |
| *トランクステータス表示コマンド* | | | |
| show interfaces status port-channel | トランク情報を表示 | NE、PE | 375 |
| show lacp | LACP情報を表示 | PE | 391 |

### トランク作成のガイドライン

*一般的なガイドライン:*

- ループの作成を防ぐために、ポートトランクの設定を完了してから、スイッチ間の対応するネットワークケーブルを接続してください。
- 1つのトランクのポート数は最大8個です。
- 接続の両端のポートを、トランクポートとして設定する必要があります。
- トランク内のすべてのポートを、通信モード(速度、デュープレックスモード、フローコントロール)、VLANの割り当て、CoSの設定を含めて、まったく同じ方法で設定する必要があります。
- 指定したポートチャネル経由でVLANとの間を移動、追加、削除を行う場合は、トランク内のすべてのポートを1つにまとめて処理する必要があります。
- STP、VLAN、およびIGMPの設定は、指定したポートチャネル経由でトランク全体に対してのみ行うことができます。

*ポートチャネルの動的作成:*

共通のポートチャネルに割り当てるポートは、以下の条件を満たす必要があります。

- LACPシステム優先度が同じである必要があります。
- ポート管理キーが同じである必要があります(イーサネットインタフェース)。
- チャネルグループ形成時にポートチャネル管理キー(ポートチャネルのlacp admin key)が設定されていない場合(ヌル値0になっている場合)、このキーは、グループに参加したインタフェースで使用されているポート管理キー(イーサネットインタフェースのlacp admin key)と同じ値に設定されます。
- ただし、ポートチャネル管理キーが設定されている場合、ポート管理キーは、チャネルグループへの参加を許可されるポートと同じ値に設定する必要があります。
- リンクがダウンした場合は、LACPポート優先度を使用してバックアップリンクが選択されます。

## channel-group

トランクにポートを追加します。 トランクからポートを削除するには**no**形式を使用します。

### 構文

**channel-group** *チャネルID*
**no channel-group**

*チャネルID* - トランクのインデックス(範囲:1～4)

### デフォルト設定

現在のポートがこのトランクを追加

### コマンドモード

Interface Configuration (イーサネット)

**コマンドの使用方法**

- 静的トランクを設定する場合は、すべてのスイッチがCisco EtherChannel標準に準拠している必要があります。
- トランクからポートグループを削除するには**no channel-group**を使用します。
- 本製品からトランクを削除するには**no interfaces port-channel**を使用します。

**例**

以下の例では、トランク1を作成してからポート11を追加します。

```
Console(config)#interface port-channel 1
Console(config-if)#exit
Console(config)#interface ethernet 1/11
Console(config-if)#channel-group 1
Console(config-if)#
```

**lacp**

現在のインタフェースに対して802.3ad Link Aggregation Control Protocol (LACP)を有効にします。 無効にするには**no**形式を使用します。

**構文**

[no] lacp

**デフォルト設定**

無効

**コマンドモード**

Interface Configuration (イーサネット)

**コマンドの使用方法**

- LACPトランクの両端にあるポートを、強制モードまたはオートネゴシエーションによって全二重用に設定する必要があります。
- 別のスイッチでLACPを使用して形成されたトランクには、次に使用可能なポートチャネルIDが自動的に割り当てられます。
- ターゲットスイッチの接続ポートでもLACPが有効になっている場合、このトランクは自動的にアクティブになります。
- 同じターゲットスイッチに接続されている8個以上のポートでLACPが有効になっている場合、それ以上のポートはスタンバイモードになり、アクティブなリンクのいずれかに障害が発生した場合にのみ有効になります。

**例**

以下は、LACPがポート11～13で有効になっている場合を示しています。LACPはリンクの

相手側のポートでも有効になっているため、**show interfaces status port-channel 1**コマンドを実行すると、Trunk 1が確立されたことが示されます。

```
Console(config)#interface ethernet 1/11
Console(config-if)#lacp
Console(config-if)#exit
Console(config)#interface ethernet 1/12
Console(config-if)#lacp
Console(config-if)#exit
Console(config)#interface ethernet 1/13
Console(config-if)#lacp
Console(config-if)#exit
Console(config)#exit
Console#show interfaces status port-channel 1
Information of Trunk 1
  Basic information:
    Port type:                  100TX
    Mac address:                00-90-CC-12-34-72
  Configuration:
    Name:
    Port admin:                 Up
    Speed-duplex:               Auto
    Capabilities:               10half, 10full, 100half, 100full
    Flow control status:        Disabled
    Port security:              Disabled
    Max MAC count:              0
  Current status:
    Created by:                 LACP
    Link status:                Up
    Operation speed-duplex: 100full
    Flow control type:          None
    Member Ports: Eth1/11, Eth1/12, Eth1/13,
Console#
```

### lacp system-priority

ポートのLACPシステム優先度を設定します。 デフォルト設定を復元するには**no**形式を使用します。

### 構文

**lacp** {**actor** | **partner**} **system-priority** *優先度*
**no lacp** {**actor** | **partner**} **system-priority**

- **actor** - 集合リンクのローカル側(アクタ)
- **partner** - 集合リンクのリモート側(パートナ)
- *優先度* - リンクアグリゲーショングループ(LAG)のメンバシップを特定し、LAGネゴシエーション中に本製品を他のスイッチに対して識別するために使用（範囲:0～65535）

### デフォルト設定

32768

### コマンドモード

Interface Configuration (イーサネット)

### コマンドの使用方法

- 同じLAGに参加するポートは、同じシステム優先度で設定する必要があります。
- システム優先度をスイッチのMACアドレスと結合して、LAGのIDが形成されます。このIDは、他のシステムとのLACPネゴシエーション中に、特定のLAGを示すために使用されます。
- リンクのリモート側が確立されれば、LACP動作設定はリモート側ですでに使用されています。 パートナに関してのみLACPを設定すると、この設定は管理状態のみに適用され、動作状態には適用されません。また、そのパートナとの集合リンクが次回確立されたときに有効になります。

### 例

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor system-priority 3
Console(config-if)#
```

## lacp admin-key (イーサネットインタフェース)

ポートのLACP管理キーを設定します。 デフォルト設定を復元するには**no**形式を使用します。

### 構文

**lacp** {**actor** | **partner**} **admin-key** キー
[**no**] **lacp** {**actor** | **partner**} **admin-key**

- **actor** - 集合リンクのローカル側(アクタ)
- **partner** - 集合リンクのリモート側(パートナ)
- キー - 同じリンクアグリゲーショングループ(LAG)に所属するポートのポート管理キーは同じ値に設定 (範囲:0～65535)

### デフォルト設定

0

### コマンドのモード

Interface Configuration (イーサネット)

### コマンドの使用方法

- 同じLAGに参加できるのは、(1) LACPシステム優先度が一致し、(2) LACPポート管理キーが一致し、(3) LACPポートチャネルキーが一致(設定されている場合)するポートのみです。
- チャネルグループ形成時にポートチャネル管理キー(ポートチャネルのlacp admin key)が設定されていない場合(ヌル値0になっている場合)、このキーは、グループに参加したインタフェースで使用されているポート管理キー(イーサネットインタフェースのlacp admin key)と同じ値に設定されます。
- リンクのリモート側が確立されれば、LACP動作設定はリモート側ですでに使用されています。 パートナに関してのみLACPを設定すると、この設定は管理状態のみに適用され、動作状態には適用されません。また、そのパートナとの集合リンクが次回確立されたときに有効になります。

### 例

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor admin-key 120
Console(config-if)#
```

## lacp admin-key (ポートチャネル)

ポートチャネルのLACP管理キー文字列を設定します。 デフォルト設定を復元するにはno形式を使用します。

### 構文

lacp {actor | partner} admin-key キー
[no] lacp {actor | partner} admin-key

キー - ポートチャネル管理キーは、本製品でローカルLACP設定中に特定のリンクアグリゲーショングループ(LAG)を識別するために使用 (範囲:0～65535)

### デフォルト設定

0

### コマンドモード

Interface Configuration (ポートチャネル)

### コマンドの使用方法

- 同じLAGに参加できるのは、(1) LACPシステム優先度が一致し、(2) LACPポート管理キーが一致し、(3) LACPポートチャネルキーが一致(設定されている場合)するポートのみです。
- チャネルグループ形成時にポートチャネル管理キー(ポートチャネルのlacp admin key)が設定されていない場合(ヌル値0になっている場合)、このキーは、グループ

に参加したインタフェースで使用されているポート管理キー(イーサネットインタフェースのlacp admin key)と同じ値に設定されます。 LAGが使用されなくなったとき、ポートチャネルの管理キーは0にリセットされます。

**例**

```
Console(config)#interface port-channel 1
Console(config-if)#lacp actor admin-key 3
Console(config-if)#
```

### lacp port-priority

LACPポート優先度を設定します。 デフォルト設定を復元するにはno形式を使用します。

**構文**

lacp {actor | partner} port-priority *優先度*
no lacp {actor | partner} port-priority

- actor – 集合リンクのローカル側(アクタ)
- partner – 集合リンクのリモート側(パートナ)
- *優先度* – LACPポート優先度をバックアップリンクの選択に使用 (範囲:0～65535)

**デフォルト設定**

32768

**コマンドモード**

Interface Configuration (イーサネット)

**コマンドの使用方法**

- 設定する値が低いほど、実際の優先度は高くなります。
- アクティブなポートリンクがダウンした場合は、優先度の最も高いバックアップポートが選択され、ダウンしたリンクの代わりとなります。 ただし、LACPポート優先度が同じポートが2つ以上ある場合は、物理的ポート番号が最も小さいポートがバックアップポートとして選択されます。
- リンクのリモート側が確立されれば、LACP動作設定はリモート側ですでに使用されています。 パートナに関してのみLACPを設定すると、この設定は管理状態のみに適用され、動作状態には適用されません。また、そのパートナとの集合リンクが次回確立されたときに有効になります。

**例**

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor port-priority 128
```

**show lacp**
LACP情報を表示します。

**構文**

**show lacp** [*ポートチャネル*] {**counters** | **internal** | **neighbors** | **sysid**}

- *ポートチャネル* – リンクアグリゲーショングループのローカルID （範囲：1～4）
- **counters** – LACPプロトコルメッセージの統計
- **internal** – ローカル側の設定および動作状態
- **neighbors** – リモート側の設定および動作状態
- **sysid** – 全チャネルグループのシステム優先度およびMACアドレスの概要

**デフォルト設定**

ポートチャネル: すべて

**コマンドモード**

Privileged Exec

**例**

```
Console#show lacp 1 counters
Port channel : 1 ------------------------------------------------------------------------
Eth 1/ 1 --------------------------------------------------------------------------
   LACPDUs Sent : 21
   LACPDUs Received : 21
   Marker Sent : 0
   Marker Received : 0
   LACPDUs Unknown Pkts : 0
   LACPDUs Illegal Pkts : 0
.
.
.
```

表 4-45 show lacp counters - 表示の説明

| フィールド | 説明 |
|---|---|
| LACPDUs Sent | このチャネルグループから送信されている、有効なLACPDUの数 |
| LACPDUs 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ている、有効なMarker PDUの数 |
| Marker Received | このチャネルグループで受信された、有効なMarker PDUの数 |
| LACPDUs Unknown Pkts | 以下のいずれかに該当する受信フレームの数。(1) Slow Protocols Ethernet Type値を持つが、不明なPDUを含むもの。(2) 宛先がSlow ProtocolsグループのMACアドレスになっているが、Slow Protocols Ethernet Typeを持たないもの。 |
| LACPDUs Illegal Pkts | Slow Protocols Ethernet Type値を持つが、正常に構成されていないPDUまたはProtocol Subtypeの不正な値を含むフレームの数 |

```
Console#show lacp 1 internal
Port channel : 1
------------------------------------------------------------------------
Oper Key : 4
Admin Key : 0
Eth 1/1
------------------------------------------------------------------------
   LACPDUs Internal : 30 sec
   LACP System Priority : 32768
   LACP Port Priority : 32768
   Admin Key : 4
   Oper Key : 4
   Admin State : defaulted, aggregation, long timeout, LACP-activity
   Oper State : distributing, collecting, synchronization, aggregation,
                long timeout, LACP-activity
.
.
.
```

表 4-46 show lacp internal - 表示の説明

| フィールド | 説明 |
|---|---|
| Oper Key | 集合ポート用のキーの現在の動作値 |
| Admin Key | 集合ポート用のキーの現在の管理値 |
| LACPDUs Internal | 受信したLACPDU情報を無効にするまでの秒数 |
| 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フェースに割り当てられているLACPポート優先度 |
| Admin State、Oper State | アクタの状態パラメータの管理値または動作値<br>・Expired - アクタの受信マシンが期限切れ状態<br>・Defaulted - アクタの受信マシンが、パートナ用に管理上設定されているデフォルトの動作パートナ情報を使用<br>・Distributing - 無効な場合、このリンクでの送信フレームの配信は無効。配布は現在無効になっており、管理者上の変更または受信プロトコル情報の変更がない限りは有効にならない<br>・Collecting - このリンクでの着信フレームの収集が有効。収集は現在有効になっており、管理者上の変更または受信プロトコル情報の変更がない限りは無効にならない<br>・Synchronization - システムはこのリンクをIN_SYNCとみなしている。このリンクは正しいリンクアグリゲーショングループに割り当てられており、そのグループが互換性のあるAggregator（集合先）に関連付けられていて、リンクアグリゲーショングループのIDが送信されたシステムIDおよび動作キー情報に一致する<br>・Aggregation - システムはこのリンクを集合可能とみなす。集合の候補<br>・Long timeout - LACPDUの定期的な送信で低速の送信速度を使用<br>・LACP-Activity - このリンクに関連する動作制御値(0:パッシブ、1:アクティブ) |

```
Console#show lacp 1 neighbors
Port channel 1 neighbors
------------------------------------------------------------------------
Eth 1/1
------------------------------------------------------------------------
   Partner Admin System ID : 32768, 00-00-00-00-00-00
   Partner Oper System ID : 32768, 00-90-CC-00-00-01
   Partner Admin Port Number : 1
   Partner Oper Port Number : 1
   Port Admin Priority : 32768
   Port Oper Priority : 32768
   Admin Key : 0
   Oper Key : 4
   Admin State : defaulted, distributing, collecting, synchronization,
                 long timeout,
   Oper State : distributing, collecting, synchronization, aggregation,
                long timeout, LACP-activity
.
.
.
```

表 4-47 show lacp neighbors - 表示の説明

| フィールド | 説明 |
|---|---|
| Partner Admin System ID | ユーザが割り当てるLAGパートナのシステムID |
| Partner Oper System ID | LACPプロトコルが割り当てるLAGパートナのシステムID |
| Partner Admin Port Number | プロトコルパートナ用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がこの集合ポートに割り当てる動作上のポート番号 |
| Port Admin Priority | プロトコルパートナ用のポート優先度の現在の管理値 |
| Port Oper Priority | パートナがこの集合ポートに割り当てる優先度の値 |
| Admin Key | プロトコルパートナ用のキーの現在の管理値 |
| Oper Key | プロトコルパートナ用のキーの現在の動作値 |
| Admin State | パートナの状態パラメータの管理値（上記の表を参照） |
| Oper State | パートナの状態パラメータの動作値（上記の表を参照） |

```
Console#show lacp sysid
Port Channel        System Priority       System MAC Address
--------------------------------------------------------------------------------
          1                32768        00-90-CC-8F-2C-A7
          2                32768        00-90-CC-8F-2C-A7
          3                32768        00-90-CC-8F-2C-A7
          4                32768        00-90-CC-8F-2C-A7
Console#
```

表 4-48 show lacp sysid - 表示の説明

| フィールド | 説明 |
|---|---|
| Channel group | 本製品で設定されているリンクアグリゲーショングループ |
| System Priority(※1) | このチャネルグループのLACPシステム優先度 |
| System MAC Address(※1) | システムMACアドレス |

※1 LACPシステム優先度とシステムMACアドレスを連結してLAGシステムIDが形成されます。

# アドレステーブルコマンド

これらのコマンドを使用してアドレステーブルを設定すると、指定したアドレスのフィルタリング、現在のエントリの表示、テーブルのクリア、エージング期間の設定を行うことができます。

**表 4-49 アドレステーブルコマンド**

| コマンド | 機能 | モード | ページ |
|---|---|---|---|
| mac-address-table static | VLANで任意のポートに静的アドレスをマッピング | GC | 396 |
| clear mac-address-table dynamic | 転送データベースから学習済みエントリを削除 | PE | 397 |
| show mac-address-table | ブリッジ転送データベースのエントリを表示 | PE | 397 |
| mac-address-table aging-time | アドレステーブルのエージング期間を設定 | GC | 398 |
| show mac-address-table aging-time | アドレステーブルのエージング期間を表示 | PE | 399 |

### mac-address-table static

VLANで任意の送信先ポートに静的アドレスをマッピングします。 アドレスを削除するには**no**形式を使用します。

#### 構文

**mac-address-table static** *MACアドレス* **interface** *インタフェース* **vlan** *VLAN ID* [*アクション*]

**no mac-address-table static** *MACアドレス* **vlan** *VLAN ID*

- *MACアドレス* – MACアドレス
- *インタフェース*
  - **ethernet** *ユニット/ポート*
    - *ユニット* – スタックユニット (範囲:1～8)
    - *ポート* – ポート番号 (範囲:1～26)
  - **port-channel** *チャネルID* (範囲:1～4)
- *VLAN ID* – VLAN ID (範囲:1～4094)
- *アクション* –
  - **delete-on-reset** – 割り当てを本製品をリセットするまで継続
  - **permanent** – 割り当てを永続

#### デフォルト設定

静的アドレスは未定義。 デフォルトのモードは**permanent**

#### コマンドモード

Global Configuration

#### コマンドの使用方法

ホスト機器の静的アドレスは、特定のVLAN内にある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、静的アドレスをMACアドレステーブルに追加してください。 静的アドレスには以下の特徴があります。

- 静的アドレスは、与えられたインタフェースリンクがダウンしても、アドレステーブルから削除されません。
- 静的アドレスは割り当てられているインタフェースにバインドされ、移動されません。別のインタフェースで確認された静的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。
- このコマンドの**no**形式を使用してアドレスを削除しない限り、静的アドレスは別のポートで学習されません。

#### 例

```
Console(config)#mac-address-table static 00-90-cc-94-34-de interface ethernet 1/1 vlan 1
  delete-on-reset
Console(config)#
```

### clear mac-address-table dynamic

転送データベースから学習済みのエントリを削除して、静的エントリまたはシステム設定エントリの送受信数をクリアします。

#### デフォルト設定

なし

#### コマンドモード

Privileged Exec

#### 例

```
Console#clear mac-address-table dynamic
Console#
```

### show mac-address-table

ブリッジ転送データベースのエントリのクラスを表示します。

#### 構文

show mac-address-table [address *MACアドレス* [*マスク*]] [interface *インタフェース*] [vlan *VLAN ID*] [sort {address | vlan | interface}]

- *MACアドレス* – MACアドレス
- *マスク* – アドレスで一致するビット
- *インタフェース*
  - ethernet *ユニット*/*ポート*
    - *ユニット* – スタックユニット (範囲:1～8)
    - *ポート* – ポート番号 (範囲:1～26)
  - port-channel *チャネルID* (範囲:1～4)
- *VLAN ID* – VLAN ID (範囲:1～4094)
- sort – アドレス、vlan、インタフェースのいずれかで並べ替え

#### デフォルト設定

なし

#### コマンドモード

Privileged Exec

### コマンドの使用方法

- MACアドレステーブルには、各インタフェースに関連付けられているMACアドレスが含まれます。「Type」フィールドには以下のいずれかのタイプが含まれます。
  - Learned - 動的アドレスエントリ
  - Permanent - 静的エントリ
  - Delete-on-reset - システムのリセット時に削除される静的エントリ
- マスクは、指定したMACアドレスに適用される、xx-xx-xx-xx-xx-xxという形式の16進数(対応するビットマスクを表す)です。 任意の16進数を入力します。対応するバイナリビットは、「0」がビットに一致、「1」がビットを無視という意味です。 たとえば、00-00-00-00-00-00というマスクは完全一致の意味で、FF-FF-FF-FF-FF-FFというマスクは「任意(any)」の意味です。
- アドレスエントリの最大数は8191個です。

### 例

```
Console#show mac-address-table
 Interface Mac Address            Vlan Type
 --------- ------------------ ---- ------------------
  Eth 1/1 00-90-cc-94-34-de       1   Delete-on-reset
  Trunk 2 00-90-cc-8f-aa-1b       1   Learned
Console#
```

## mac-address-table aging-time

アドレステーブルのエントリのエージング期間を設定します。 デフォルトのエージング期間を復元するにはno形式を使用します。

### 構文

**mac-address-table aging-time** *秒*
**no mac-address-table aging-time**

*秒* - エージング期間 (範囲:10～30000秒、0:エージング無効)

### デフォルト設定

300秒

### コマンドモード

Global Configuration

### コマンドの使用方法

エージング期間は、動的に学習した転送情報を一定の期間後に削除する場合に使用します。

**例**

```
Console(config)#mac-address-table aging-time 100
Console(config)#
```

### show mac-address-table aging-time

アドレステーブルのエントリのエージング期間を表示します。

**デフォルト設定**

なし

**コマンドモード**

Privileged Exec

**例**

```
Console#show mac-address-table aging-time
  Aging time: 100 sec.
Console#
```

# スパニングツリーコマンド

本セクションでは、本製品用にスパニングツリーアルゴリズム(STA)をグローバルに設定するコマンド、および選択したインタフェース用にSTAを設定するコマンドについて解説します。

表 4-50 スパニングツリーコマンド

| コマンド | 機能 | モード | ページ |
|---|---|---|---|
| spanning-tree | スパニングツリープロトコルを有効化 | GC | 401 |
| spanning-tree mode | STPまたはRSTPを設定 | GC | 401 |
| spanning-tree forward-time | スパニングツリーブリッジの転送時間を設定 | GC | 402 |
| spanning-tree hello-time | スパニングツリーブリッジのハロータイムを設定 | GC | 403 |
| spanning-tree max-age | スパニングツリーブリッジの最大エージング期間を設定 | GC | 404 |
| spanning-tree priority | スパニングツリーブリッジの優先度を設定 | GC | 404 |
| spanning-tree path-cost method | RSTPのパスコスト方式を設定 | GC | 405 |
| spanning-tree transmission-limit | RSTPの送信制限を設定 | GC | 406 |
| spanning-tree cost | 任意のインタフェースのスパニングツリーパスコストを設定 | IC | 406 |
| spanning-tree port-priority | 任意のインタフェースのスパニングツリー優先度を設定 | IC | 407 |
| spanning-tree edge-port | エッジポートの高速転送を有効化 | IC | 408 |
| spanning-tree portfast | 任意のインタフェースを高速転送に設定 | IC | 409 |
| spanning-tree link-type | RSTPのリンクタイプを設定 | IC | 410 |
| spanning-tree protocol-migration | 適切なBPDU形式を再確認 | PE | 410 |
| show spanning-tree | 共通のスパニングツリー(ブリッジ全体)または選択したインタフェースのスパニングツリー設定を表示 | PE | 411 |

### spanning-tree

本製品用にスパニングツリーアルゴリズムをグローバルに有効にします。 無効にするにはno形式を使用します。

#### 構文

[no] spanning-tree

#### デフォルト設定

有効

#### コマンドモード

Global Configuration

#### コマンドの使用方法

スパニングツリーアルゴリズム(STA)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の間にバックアップリンクを設定することができます。 これにより、本製品はネットワーク内の他のブリッジング機器(STA互換のスイッチ、ブリッジ、ルータ)と相互動作できるため、ネットワーク上の2つのステーション間にルートが1つだけ存在する状態が保たれ、プライマリリンクがダウンしたときに自動的に代理を務めるバックアップリンクも使用可能になります。

#### 例

以下の例は、本製品用にスパニングツリーアルゴリズムを有効にする方法を示しています。

```
Console(config)#spanning-tree
Console(config)#
```

### spanning-tree mode

本製品のスパニングツリーモードを選択します。 デフォルトを復元するにはno形式を使用します。

#### 構文

spanning-tree mode {stp | rstp}
no spanning-tree mode

- stp – スパニングツリープロトコル(IEEE 802.1D)
- rstp – ラピッドスパニングツリープロトコル(IEEE 802.1w)

#### デフォルト設定

rstp

**コマンドモード**

Global Configuration

**コマンドの使用方法**

- スパニングツリープロトコル(STP)

  802.1D BPDUを用いてスパニングツリーの作成、維持を行います。

- ラピッドスパニングツリープロトコル(RSTP)

  RSTPは、以下で説明するように、着信プロトコルメッセージを監視して、RSTPノードが送信す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、RSTPノードのいずれかへの接続に対応します。

  - STPモード – 本製品が、ポートの移行遅延タイマが期限切れになった後に802.1D BPDUを受信した場合は、802.1Dブリッジに接続しているとみなされ、802.1D BPDUのみの使用が開始されます。
  - RSTPモード – RSTPが任意のポートで802.1D BPDUを使用していて、移行遅延タイマの期限切れ後にRSTP BPDUを受信した場合、RSTPは移行遅延タイマを再起動して、そのポートでRSTP BPDUの使用を開始します。

**例**

以下の例では、ラピッドスパニングツリーを使用するように本製品を設定します。

```
Console(config)#spanning-tree mode rstp
Console(config)#
```

**spanning-tree forward-time**

本製品用にスパニングツリーブリッジの転送時間をグローバルに設定します。 デフォルトを復元するには**no**形式を使用します。

**構文**

**spanning-tree forward-time** *秒*
**no spanning-tree forward-time**

*秒* – 秒単位の時間（範囲:4～30秒）
最小値は4または[(最大エージング期間 / 2) + 1]のいずれか大きい方

**デフォルト設定**

15秒

**コマンドモード**

Global Configuration

**コマンドの使用方法**

ルート機器の状態が(discarding (破棄)→learning (学習)→forwarding (転送)の順に)変更されるまでの最大待機時間を秒単位で設定します。 どの機器でも、トポロジ変更に関する情報を受信してからフレームの転送を開始する必要があるため、この遅延が必要です。 また、ポートごとに、discarding (破棄)状態に戻るきっかけとなる競合情報の有無を確認する時間が必要です。この時間がないと、一時的にデータループが発生する場合があります。

**例**

```
Console(config)#spanning-tree forward-time 20
Console(config)#
```

### spanning-tree hello-time

本製品用にスパニングツリーブリッジのハロータイムをグローバルに設定します。 デフォルトを復元するにはno形式を使用します。

**構文**

spanning-tree hello-time *時間*
no spanning-tree hello-time

*時間* - 秒単位の時間 (範囲:1～10秒)
最大値は10または[(最大エージング期間 / 2) -1]のいずれか小さい方

**デフォルト設定**

2秒

**コマンドモード**

Global Configuration

**コマンドの使用方法**

ルート機器が設定メッセージを送信する間隔を秒単位で設定します。

**例**

```
Console(config)#spanning-tree hello-time 5
Console(config)#
```

### spanning-tree max-age

本製品用にスパニングツリーブリッジの最大エージング期間をグローバルに設定します。デフォルトを復元するにはno形式を使用します。

#### 構文

**spanning-tree max-age** *秒*
**no spanning-tree max-age**

*秒* - 秒単位の時間（範囲:6～40秒）
最小値は6または[2 ×（ハロータイム + 1)]のいずれか大きい方
最大値は40または[2 ×（転送時間 - 1)]のいずれか小さい方

#### デフォルト設定

20秒

#### コマンドモード

Global Configuration

#### コマンドの使用方法

機器が何秒間設定メッセージを受信しなかった場合に再設定を行うか、その最大時間を設定します。 機器のすべてのポート(指定ポートを除く)は、一定の間隔で設定メッセージを受信する必要があります。 STA情報(最後の設定メッセージで提供されたもの)が期限切れになったポートは、接続されているLANの指定ポートになります。これがルートポートである場合、ネットワークに接続されている機器のポートの中から新しいルートポートが選択されます。

#### 例

```
Console(config)#spanning-tree max-age 40
Console(config)#
```

### spanning-tree priority

本製品用にスパニングツリーの優先度をグローバルに設定します。 デフォルトを復元するにはno形式を使用します。

#### 構文

**spanning-tree priority** *優先度*
**no spanning-tree priority**

*優先度* - ブリッジの優先度
(範囲 - 0～61440（4096刻み)。オプション:0、4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、61440)

### デフォルト設定

32768

### コマンドモード

Global Configuration

### コマンドの使用方法

ブリッジの優先度は、ルート機器、ルートポート、指定ポートの選択に使用します。 優先度の最も高い機器がSTAルート機器になります。 ただし、すべての機器の優先度が同じ場合は、MACアドレスが最も小さい機器がルートデバイスになります。

### 例

```
Console(config)#spanning-tree priority 40960
Console(config)#
```

## spanning-tree pathcost method

ラピッドスパニングツリーに使用するパスコスト方式を設定します。 デフォルトを復元するにはno形式を使用します。

### 構文

**spanning-tree pathcost method** {**long** | **short**}
**no spanning-tree pathcost method**

- **long** - 32ビットベースの値を0～200,000,000の範囲で指定
- **short** - 16ビットベースの値を0～65535の範囲で指定

### デフォルト設定

long方式

### コマンドモード

Global Configuration

### コマンドの使用方法

パスコスト方式は、機器間の最適なパスを特定する際に使用します。 したがって、高速メディアに接続されているポートには小さい値を、低速メディアに接続されているポートには大きい値を割り当てる必要があります。 パスコスト(409ページ)は、ポート優先度(410ページ)より優先されます。

### 例

```
Console(config)#spanning-tree pathcost method long
Console(config)#
```

### spanning-tree transmission-limit

連続したRSTP BPDUを送信する最小の間隔を設定します。 デフォルトを復元するにはno形式を使用します。

### 構文

**spanning-tree transmission-limit** *数*
**no spanning-tree transmission-limit**

*数* - 秒単位の送信制限（範囲:1～10）

### デフォルト設定

3

### コマンドモード

Global Configuration

### コマンドの使用方法

BPDUの最大送信速度を制限します。

### 例

```
Console(config)#spanning-tree transmission-limit 4
Console(config)#
```

### spanning-tree cost

指定したインタフェース用にスパニングツリーパスコストを設定します。 デフォルトを復元するにはno形式を使用します。

### 構文

**spanning-tree cost** *コスト*
**no spanning-tree cost**

*コスト* - ポートのパスコスト（範囲:1～200,000,000）
推奨される範囲は以下のとおり

- イーサネット:200,000～20,000,000
- ファストイーサネット:20,000～2,000,000

・ ギガビットイーサネット:2,000～200,000

**デフォルト設定**

・ イーサネット – 半二重:2,000,000、全二重:1,000,000、トランク:500,000
・ ファストイーサネット – 半二重:200,000、全二重:100,000、トランク:50,000
・ ギガビットイーサネット – 全二重:10,000、トランク:5,000

**コマンドモード**

Interface Configuration (イーサネット、ポートチャネル)

**コマンドの使用方法**

・ このコマンドは、スパニングツリーアルゴリズムで、機器間の最適のパスを特定する際に使用します。 したがって、高速メディアに接続されているポートには小さい値を、低速メディアに接続されているポートには大きい値を割り当てる必要があります。
・ パスコストは、ポート優先度より優先されます。
・ スパニングツリーパスコスト方式( 406ページ)をshortに設定した場合のパスコストの最大値は65,535です。

**例**

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree cost 5000
Console(config-if)#
```

**spanning-tree port-priority**
指定したインタフェースの優先度を設定します。 デフォルトを復元するには**no**形式を使用します。

**構文**

**spanning-tree port-priority** *優先度*
**no spanning-tree port-priority**

*優先度* – ポートの優先度 (範囲:0～240、16刻み)

**デフォルト設定**

128

**コマンドモード**

Interface Configuration (イーサネット、ポートチャネル)

### コマンドの使用方法

- スパニングツリーアルゴリズムでのポート使用の優先度を定義します。 1つのスイッチの全ポートのパスコストが同じ場合は、優先度の最も高いポート、つまり値が最小のポートが、スパニングツリーでアクティブリンクとして設定されます。
- 優先度の最も高いポートが複数ある場合は、IDの数値が最も小さいポートが有効になります。

### 例

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree port-priority 128
Console(config-if)#
```

### 関連コマンド

spanning-tree cost (p.406)

## spanning-tree edge-port

任意のインタフェースをエッジポートとして指定します。 デフォルトを復元するにはno形式を使用します。

### 構文

[no] spanning-tree edge-port

### デフォルト設定

無効

### コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

### コマンドの使用方法

- ブリッジされているLANの末端にあるLANセグメント、または末端ノードにインタフェースが接続されている場合に、このオプションを有効にすることができます。 末端ノードでは転送ループが発生することがないため、スパニングツリーの転送状態に直接移行できます。 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機器をより短時間で収束できるほか、現在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できます。また、インタフェースの状態が変化してもスパニングツリーで再設定が開始されることはなく、STA関連のタイムアウトに関するその他の問題も克服できます。 ただし、エッジポートは、末端ノード機器に接続されているポートに関してのみ有効にしてください。
- このコマンドには、spanning-tree portfastと同じ効果があります。

**例**

```
Console(config)#interface ethernet ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#
```

**関連コマンド**

spanning-tree portfast (p.409)

### spanning-tree portfast

任意のインタフェースを高速転送に設定します。 高速転送を無効にするにはno形式を使用します。

**構文**

[no] spanning-tree portfast

**デフォルト設定**

無効

**コマンドモード**

Interface Configuration (イーサネット、ポートチャネル)

**コマンドの使用方法**

- このコマンドは、選択したポートに関して高速スパニングツリーモードを有効または無効にする際に使用します。 このモードでは、ポートはDiscarding (破棄)状態とLearning (学習)状態をスキップし、直接Forwarding (転送)状態に移行します。
- 末端ノードでは転送ループが発生することがないため、標準的な収束時間よりも早くスパニングツリーの状態変化の過程を通過することができます。 高速転送では、末端ノードのワークステーションやサーバをより短時間で収束できるほか、STA関連のタイムアウトに関するその他の問題も克服できます (高速転送は、ブリッジされているLANの末端にあるLANセグメントに接続されているポート、または末端ノード機器に関してのみ、有効にしてください)。
- このコマンドはspanning-tree edge-portと同じです。旧製品との下位互換性のために含まれています。 このコマンドは、今後のソフトウェアバージョンでは削除される場合があります。

**例**

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree portfast
Console(config-if)#
```

### 関連コマンド

spanning-tree edge-port (p.408)

## spanning-tree link-type

ラピッドスパニングツリーのリンクタイプを設定します。 デフォルトを復元するにはno形式を使用します。

### 構文

**spanning-tree link-type** {**auto** | **point-to-point** | **shared**}
**no spanning-tree link-type**

- **auto** – デュプレックスモード設定から自動的に取得
- **point-to-point** – ポイントツーポイントリンク
- **shared** – 共有メディア

### デフォルト設定

auto

### コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

### コマンドの使用方法

- インタフェースを1つのブリッジのみに接続できる場合はポイントツーポイントリンクを、2つ以上のブリッジに接続できる場合は共有リンクを指定します。
- 自動検出を選択した場合、本製品はデュプレックスモードからリンクタイプを取得します。 全二重インタフェースはポイントツーポイントリンクとみなされ、半二重インタフェースは共有リンク上にあるとみなされます。
- RSTPは、2つのブリッジ間のポイントツーポイントリンクでのみ機能します。 任意のポートを共有リンクとして指定した場合、RSTPは禁止されます。

### 例

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree link-type point-to-point
```

## spanning-tree protocol-migration

選択したインタフェースで送信する適切なBPDU形式を再確認します。

### 構文

**spanning-tree protocol-migration** *インタフェース*

*インタフェース*

- **ethernet** *ユニット/ポート*
  - *ユニット* - スタックユニット (範囲:1～8)
  - *ポート* - ポート番号 (範囲:1～26)
- **port-channel** *チャネルID* (範囲:1～6)

**コマンドモード**

Privileged Exec

**コマンドの使用方法**

設定BPDUやトポロジ変更通知BPDUなどのSTP BPDUを検出すると、本製品は、選択されているインタフェースを自動的に強制STP互換モードに設定します。 ただし、**spanning-tree protocol-migration**コマンドを使用すれば、選択したインタフェースで送信する適切なBPDU形式(RSTP互換またはSTP互換)を手動で再確認することもできます。

**例**

```
Console#spanning-tree protocol-migration ethernet 1/5
Console#
```

**show spanning-tree**
スパニングツリーの設定を表示します。

**構文**

**show spanning-tree** [*インタフェース*]

*インタフェース*

- **ethernet** *ユニット/ポート*
  - *ユニット* - スタックユニット (範囲:1～8)
  - *ポート* - ポート番号 (範囲:1～26)
- **port-channel** *チャネルID* (範囲:1～4)

**デフォルト設定**

なし

**コマンドモード**

Privileged Exec

**コマンドの使用方法**

- **show spanning-tree**コマンドをパラメータなしで使用すると、本製品およびツリー内のすべてのインタフェースのスパニングツリー設定が表示されます。

- **show spanning-tree** *インタフェース*コマンドを使用すると、指定したインタフェースのスパニングツリー設定が表示されます。
- 「Spanning-tree information」の下に表示される項目の詳細については、166ページの「Configuring Global Settings」を参照してください。 特定のインタフェースに関して表示される項目の詳細については、170ページの「インタフェース設定の表示」を参照してください。

**例**

```
Console#show spanning-tree
Spanning-tree information
---------------------------------------------------------------------
 Spanning tree mode:                RSTP
 Spanning tree enabled/disabled:    enabled
 Priority:                          40960
 Bridge Hello Time (sec.):          2
 Bridge Max Age (sec.):             20
 Bridge Forward Delay (sec.):       15
 Root Hello Time (sec.):            2
 Root Max Age (sec.):               20
 Root Forward Delay (sec.):         15
 Designated Root:                   32768.0.0000ABCD0000
 Current root port:                 1
 Current root cost:                 50000
 Number of topology changes:        5
 Last topology changes time (sec.):226
 Transmission limit:                3
 Path Cost Method:                  long
---------------------------------------------------------------------
Eth  1/ 1 information
---------------------------------------------------------------------
Admin status:              enabled
 Role:                     root
 State:                    forwarding
 Path cost:                100000
 Priority:                 128
 Designated cost:          200000
 Designated port:          128.24
 Designated root:          32768.0.0000ABCD0000
 Designated bridge:        32768.0.0030F1552000
 Fast forwarding:          enabled
 Forward transitions:   1
 Admin edge port:          enabled
 Oper edge port:           disabled
 Admin Link type:          auto
 Oper Link type:           point-to-point
 Spanning Tree Status: enabled
.
.
Console#
```

# VLANコマンド

VLANとは、ネットワークのどこにでも配置でき、同じ物理セグメントに所属するかのように通信するポートのグループのことです。 本セクションでは、VLANグループの作成、ポートメンバの追加、VLANタギングの使用方法の指定、選択したインタフェースの自動VLAN登録の有効化に使用するコマンドについて解説します。

表 4-51 VLAN

| コマンドグループ | 機能 | ページ |
|---|---|---|
| VLANグループの編集 | 名前、VID、状態を含めてVLANグループを設定 | 413 |
| VLANインタフェースの設定 | 着信/送信タギングモード、着信フィルタリング、PVID、およびGVRPを含むVLANインタフェースパラメータを設定 | 415 |
| VLAN情報の表示 | VLANグループ、ステータス、ポート番号、およびMACアドレスを表示 | 421 |
| プライベートVLANの設定 | アップリンク/ダウンリンクポートを含むプライベートVLANを設定 | 423 |

## VLANグループの編集

表 4-52 VLANグループの編集

| コマンド | 機能 | モード | ページ |
|---|---|---|---|
| vlan database | VLANデータベースモードに移行し、VLANを追加、変更、削除 | GC | 413 |
| vlan | VID、名前、状態を含めてVLANを設定 | VC | 414 |

### vlan database

VLANデータベースモードに移行します。 このモードのコマンドはすべて、ただちに有効になります。

#### デフォルト設定

なし

#### コマンドモード

Global Configuration

### コマンドの使用方法

- VLANデータベースコマンドモードを使用し、VLANを追加、変更、削除します。設定の変更を完了後、**show vlan**コマンドを入力すると、VLANの設定を表示できます。
- ポートメンバシップモードを定義してVLANのポートを追加または削除するには、**interface vlan**コマンドモードを使用します。 これらのコマンドの結果は、実行中の設定ファイルに書き込まれます。このファイルは、**show running-config**コマンドを入力すると表示できます。

### 例

```
Console(config)#vlan database
Console(config-vlan)#
```

### 関連コマンド

show vlan (p.422)

## vlan

VLANを設定します。 デフォルト設定を復元する場合やVLANを削除する場合には**no**形式を使用します。

### 構文

**vlan** *VLAN ID* [**name** *VLAN名*] **media ethernet** [**state** {**active** | **suspend**}]
**no vlan** *VLAN ID* [**name** | **state**]

- *VLAN ID* - 設定済みのVLANのID (範囲:1～4094、頭にゼロは不要)
- **name** - VLAN名の前に付けるキーワード
  - *VLAN名* - 1～32文字のASCII文字列
- **media ethernet** - イーサネットメディアタイプ
- **state** - VLANの状態の前に付けるキーワード
  - **active** - 実行中のVLAN
  - **suspend** - 一時停止状態のVLAN。 一時停止状態のVLANでは、パケットは渡されません。

### デフォルト設定

デフォルトではVLAN 1のみが存在かつアクティブ

### コマンドモード

VLAN Database Configuration (VLANデータベース設定)

**コマンドの使用方法**

- **no vlan** *VLAN ID* – VLANの削除
- **no vlan** *VLAN ID* **name** – VLAN名の削除
- **no vlan** *VLAN ID* **state** – VLANをデフォルトの状態(active)に戻す。
- 本製品で設定できるVLANは最大255個

**例**

以下の例では、VLAN ID 105とVLAN名RD5を使用してVLANを追加します。 このVLANはデフォルトでアクティブになります。

```
Console(config)#vlan database
Console(config-vlan)#vlan 105 name RD5 media ethernet
Console(config-vlan)#
```

**関連コマンド**

show vlan (p.422)

## VLANインタフェースの設定

**表 4-53 VLANインタフェースの設定**

| コマンド | 機能 | モード | ページ |
|---|---|---|---|
| interface vlan | 指定したVLANのインタフェース設定モードに移行 | IC | 416 |
| switchport mode | 任意のインタフェースのVLANメンバシップモードを設定 | IC | 416 |
| switchport acceptable-frame-types | 任意のインタフェースで受け入れられるフレームタイプを設定 | IC | 417 |
| switchport ingress-filtering | 任意のインタフェースで着信フィルタリングを有効化 | IC | 418 |
| switchport native vlan | 任意のインタフェースのPVID (ネイティブVLAN)を設定 | IC | 419 |
| switchport allowed vlan | 任意のインタフェースに関連付けられているVLANを設定 | IC | 420 |
| switchport gvrp | 任意のインタフェースのGVRPを有効化 | IC | 431 |
| switchport forbidden vlan | 任意のインタフェースの禁止VLANを設定 | IC | 421 |
| switchport priority default | 着信タグ無しフレームのポート優先度を設定 | IC | 436 |

### interface vlan

VLANのインタフェース設定モードに移行します。これは物理インタフェースのVLANパラメータを設定するモードです。

#### 構文

**interface vlan** *VLAN ID*

*VLAN ID* - 設定済みのVLANのID (範囲:1～4094、頭にゼロは不要)

#### デフォルト設定

なし

#### コマンドモード

Global Configuration

#### 例

以下の例は、インタフェース設定モードをVLAN 1に設定し、任意のIPアドレスをVLANに割り当てる方法を示しています。

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.254 255.255.255.0
Console(config-if)#
```

#### 関連コマンド

shutdown (p.371)

### switchport mode

任意のポートのVLANメンバシップモードを設定します。 デフォルトを復元するには**no**形式を使用します。

#### 構文

**switchport mode** {**trunk** | **hybrid** | **private-vlan**}
**no switchport mode**

- **trunk** - 任意のポートをVLANトランクの末端ポイントとして指定。 トランクとは2つのスイッチの間の直接リンクであるため、ポートは送信元のVLANを識別するタグ付きフレームを送信します。 ポートのデフォルトVLAN (PVIDに関連付けられているもの)に所属するフレームも、タグ付きフレームとして送信します。
- **hybrid** - ハイブリッドVLANインタフェースを指定。 このポートではタグ付き、タグ無しの両方のフレームを送信可能です。

- **private-vlan** - このコマンドの詳細については、426ページの「switchport mode private-vlan」を参照

**デフォルト設定**

すべてのポートがハイブリッドモードで、PVIDはVLAN 1に設定

**コマンドモード**

Interface Configuration (イーサネット、ポートチャネル)

**例**

以下は、設定モードをポート1に設定し、スイッチポートモードをハイブリッドに設定する方法を示しています。

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport mode hybrid
Console(config-if)#
```

**関連コマンド**

switchport acceptable-frame-types (p.417)

### switchport acceptable-frame-types

任意のポートの受け入れ可能なフレームタイプを設定します。 デフォルトを復元するには**no**形式を使用します。

**構文**

**switchport acceptable-frame-types** {**all** | **tagged**}
**no switchport acceptable-frame-types**

- **all** - タグ付き、タグ無しにかかわらず、すべてのフレームを受け入れ
- **tagged** - タグ付きフレームのみを受信

**デフォルト設定**

すべてのフレームタイプ

**コマンドモード**

Interface Configuration (イーサネット、ポートチャネル)

**コマンドの使用方法**

すべてのフレームタイプを受信する設定のときに受信したタグ無しフレームは、すべてデフォルトのVLANに割り当てられます。

### 例

以下の例は、ポート1で受信するトラフィックをタグ付きフレームに制限する方法を示しています。

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#
```

### 関連コマンド

switchport mode (p.416)

## switchport ingress-filtering

任意のインタフェースの着信フィルタリングを有効にします。 デフォルトを復元するには**no**形式を使用します。

### 構文

[no] switchport ingress-filtering

### デフォルト設定

無効

### コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

### コマンドの使用方法

- 着信フィルタリングはタグ付きフレームのみに影響します。
- 着信フィルタリングが無効なときに、あるポートが自ら所属していないVLAN宛てのタグ付きフレームを受信した場合、これらのフレームは他のすべてのポートにフラッド送信されます(このポートで明示的に禁止されているVLANを除く)。
- 着信フィルタリングが有効なときに、あるポートが自ら所属していないVLAN宛てのタグ付きフレームを受信した場合、これらのフレームは破棄されます。
- 着信フィルタリングは、GVRPやSTAなど、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VLANに依存するBPDUフレームには影響します。

### 例

以下の例は、インタフェースをポート1に設定し、着信フィルタリングを有効にする方法を示しています。

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport ingress-filtering
Console(config-if)#
```

### switchport native vlan

任意のポートのPVID (デフォルトのVLAN ID)を設定します。 デフォルトを復元するには**no**形式を使用します。

#### 構文

**switchport native vlan** *VLAN ID*
**no switchport native vlan**

*VLAN ID* - ポートのデフォルトのVLAN ID (範囲:1～4094、頭にゼロは不要)

#### デフォルト設定

VLAN 1

#### コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

#### コマンドの使用方法

- VLAN 1に所属しないインタフェースのPVIDをこのVLANに割り当てた場合、このインタフェースはタグ無しメンバとしてVLAN 1に自動的に追加されます。 その他すべてのVLANに関しては、任意のインタフェースのPVIDをグループに割り当てる前に、まずそのインタフェースをタグ無しメンバとして設定する必要があります。
- 受け入れ可能なフレームタイプが**all**に設定されているか、スイッチポートモードが**hybrid**に設定されている場合、PVIDは着信ポートに入ってくるすべてのタグ無しフレームに挿入されます。

#### 例

以下の例は、ポート1のPVIDをVLAN 3に設定する方法を示しています。

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport native vlan 3
Console(config-if)#
```

### switchport allowed vlan

選択したインタフェースでVLANグループを設定します。 デフォルトを復元するには**no**形式を使用します。

### 構文

**switchport allowed vlan** {**add** *VLANリスト* [**tagged** | **untagged**] | **remove** *VLANリスト*}
**no switchport allowed vlan**

- **add** *VLANリスト* – 追加するVLAN IDのリスト
- **remove** *VLANリスト* – 削除するVLAN IDのリスト
- *VLANリスト* – 連続しないVLAN IDはカンマ(スペースなし)区切り。IDの範囲を指定する場合はハイフンを使用し、 頭にゼロは付けません (範囲:1～4094)。

### デフォルト設定

すべてのポートはデフォルトでVLAN 1に割り当て
デフォルトのフレームタイプはタグ無し

### コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

### コマンドの使用方法

- ポート、またはスイッチポートモードが**hybrid**に設定されているトランクは、1つ以上のVLANにタグ無しとして割り当てる必要があります。
- スイッチポートモードが**trunk**に設定されているトランク(1Qトランク)がある場合、VLANグループにタグ付きメンバとして割り当てることができるインタフェースは1つだけです。
- フレームは常に本製品内でタグ付けされます。 VLANをインタフェースに追加する際に使用するtagged/untaggedのパラメータには、送信時にフレームのタグを維持するか削除するかを本製品に伝える役割があります。
- 中間ネットワーク機器や接続先のホストにVLANに対応しているものがない場合、これらのVLANにインタフェースをタグ無しメンバとして追加する必要があります。 それ以外の場合は、VLANを1つタグ無しとして追加するだけで、インタフェースのネイティブVLANに対応できます。
- あるインタフェースの禁止リストに含まれているVLANを、そのインタフェースに手動で追加した場合、このVLANは禁止リストから自動的に削除されます。

### 例

以下の例は、VLAN 1、2、5、6を、ポート1のタグ付きVLANとして許可リストに追加する方法を示しています。

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport allowed vlan add 1,2,5,6 tagged
Console(config-if)#
```

### switchport forbidden vlan

禁止VLANを設定します。 禁止VLANのリストを削除するには**no**形式を使用します。

#### 構文

**switchport forbidden vlan** {**add** *VLANリスト* | **remove** *VLANリスト*}
**no switchport forbidden vlan**

- **add** *VLANリスト* – 追加するVLAN IDのリスト
- **remove** *VLANリスト* – 削除するVLAN IDのリスト
- *VLANリスト* – 連続しないVLAN IDはカンマ(スペースなし)区切り。IDの範囲を指定する場合はハイフンを使用し、 頭にゼロは付けません (範囲:1～4094)。

#### デフォルト設定

禁止リストにVLANは含まれない

#### コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

#### コマンドの使用方法

- 任意のVLANがGVRP経由で指定したインタフェースに自動的に追加されるのを防止します。
- 任意のインタフェースの許可VLANに追加されているVLANは、同じインタフェースの禁止VLANには追加できません。

#### 例

以下の例は、ポート1がVLAN 3に追加されるのを防ぐ方法を示しています。

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport forbidden vlan add 3
Console(config-if)#
```

## VLAN情報の表示

表 4-54 VLANコマンド表示

| コマンド | 機能 | モード | ページ |
|---|---|---|---|
| show vlan | VLAN情報を表示 | NE、PE | 422 |
| show interfaces status vlan | 指定したVLANインタフェースのステータスを表示 | NE、PE | 374 |
| show interfaces switchport | 任意のインタフェースの管理および運用のステータスを表示 | NE、PE | 377 |

### show vlan

VLAN情報を表示します。

#### 構文

**show vlan** [**id** *VLAN ID* | **name** *VLAN名* | **private-vlan** *プライベートVLANタイプ*]

- **id** – VLAN IDの前に付けるキーワード
  - *VLAN ID* – 設定済みのVLANのID (範囲:1～4094、頭にゼロは不要)
- **name** – VLAN名の前に付けるキーワード
  - *VLAN名* – 1～32文字のASCII文字列
- **private-vlan** – このコマンドの詳細については、429ページの「show vlan private-vlan」を参照
  - *プライベートVLANタイプ* – プライベートVLANのタイプの表示 (オプション: Community (コミュニティ)、Isolated (隔離)、Primary (プライマリ))

#### デフォルト設定

すべてのVLANを表示

#### コマンドモード

Normal Exec、Privileged Exec

#### 例

以下の例は、VLAN 1の情報の表示方法を示しています。

```
Console#show vlan id 1


Vlan ID:                1
Type:                   Static
Name:                   DefaultVlan
Status:                 Active
Ports/Port channel:   Eth1/ 1(S) Eth1/ 2(S) Eth1/ 3(S) Eth1/ 4(S) Eth1/ 5(S)
                        Eth1/ 6(S) Eth1/ 7(S) Eth1/ 8(S) Eth1/ 9(S) Eth1/10(S)
                        Eth1/11(S) Eth1/12(S) Eth1/13(S) Eth1/14(S) Eth1/15(S)
                        Eth1/16(S) Eth1/17(S) Eth1/18(S) Eth1/19(S) Eth1/20(S)
                        Eth1/21(S) Eth1/22(S) Eth1/23(S) Eth1/24(S) Eth1/25(S)
                        Eth1/26(S)


Console#
```

## プライベートVLANの設定

プライベートVLANは、割り当てられているVLAN内でポートベースのセキュリティを提供します。また、ポート間の隔離も可能です。 本製品は、プライマリ/セカンダリが関連付けられているグループと、スタンドアロンの隔離されたVLANの、2種類のプライベートLANに対応しています。 プライマリVLANには、プライベートVLANグループの他のすべてのポートと通信できる無差別(promiscuous)ポートが含まれており、セカンダリ(またはコミュニティ)VLANには、セカンダリVLAN内の他のホストおよび関連付けられているプライマリVLANの無差別ポートとのみ通信できるコミュニティポートが含まれています。 一方、隔離VLANは、1つの無差別ポートと1つ以上の隔離(またはホスト)ポートを含む単一のスタンドアロンVLANで構成されています。 どの場合も、無差別ポートはインターネットなどの外部ネットワークへのオープンなアクセスを提供するように設計されており、コミュニティポートまたは隔離ポートはローカルユーザに制限付きのアクセスを提供します。

本製品では複数のプライマリVLANを設定でき、各プライマリVLANに複数のコミュニティVLANを関連付けることができます。 1つ以上の隔離VLANも設定できます（プライベートVLANと通常のVLANは、同じスイッチ内に同時に存在可能です)。

本セクションでは、プライベートVLANの設定に使用するコマンドについて解説します。

表 4-55 プライベートVLANコマンド

| コマンド | 機能 | モード | ページ |
|---|---|---|---|
| *プライベートVLANグループの編集* | | | |
| private-vlan | プライマリVLAN、コミュニティVLAN、隔離VLANを追加または削除 | VC | 424 |
| private-vlan association | コミュニティVLANをプライマリVLANに関連付け | VC | 425 |
| *プライベートVLANインタフェースの設定* | | | |
| switchport mode private-vlan | 任意のインタフェースをホストモードまたは無差別モードに設定 | IC | 426 |
| switchport private-vlan host-association | 任意のインタフェースをセカンダリVLANに関連付け | IC | 427 |
| switchport private-vlan isolated | 任意のインタフェースを隔離VLANに関連付け | IC | 428 |
| switchport private-vlan mapping | 任意のインタフェースをプライマリVLANにマッピング | IC | 428 |
| *プライベートVLAN情報の表示* | | | |

| | | | |
|---|---|---|---|
| show vlan private-vlan | プライベートVLAN情報を表示 | NE、PE | 429 |

プライマリ/セカンダリ関連付けグループを設定するには、以下の手順を実行してください。

1. **private-vlan**コマンドを使用して、1つ以上のコミュニティVLANと、コミュニティグループ外部にトラフィックを送信するプライマリVLANを指定します。
2. **private-vlan association**コマンドを使用して、コミュニティVLANをプライマリVLANにマッピングします。
3. **switchport mode private-vlan**コマンドを使用して、ポートを無差別(プライマリVLANの全ポートにアクセス可能)またはホスト(コミュニティポート)として設定します。
4. **switchport private-vlan host-association**コマンドを使用して、任意のポートをセカンダリVLANに割り当てます。
5. **switchport private-vlan mapping**コマンドを使用して、任意のポートをプライマリVLANに割り当てます。
6. **show vlan private-vlan**コマンドを使用して設定を確認します。

隔離VLANを設定するには、以下の手順を実行してください。

1. **private-vlan**コマンドを使用して、1つの無差別ポートと1つ以上の隔離ポートを含む隔離VLANを指定します。
2. **switchport mode private-vlan**コマンドを使用して、1つのポートを無差別(隔離VLANの全ポートにアクセス可能)として、1つ以上のポートをホスト(隔離ポート)として設定します。
3. **switchport private-vlan isolated**コマンドを使用して、任意のポートを隔離VLANに割り当てます。
4. **show vlan private-vlan**コマンドを使用して設定を確認します。

### private-vlan

プライマリ/コミュニティ/隔離プライベートVLANを作成します。 指定したプライベートVLANを削除するには**no**形式を使用します。

#### 構文

**private-vlan** *VLAN ID* {**community** | **primary** | **isolated**}
**no private-vlan** *VLAN ID*

- *VLAN ID* – プライベートVLANのID (範囲:1～4094、頭にゼロは不要)
- **community** – トラフィックが同じVLAN内のホストメンバおよび関連付けられているプライマリVLANの無差別ポートに制限されているVLAN
- **primary** – 1つ以上のコミュニティVLANを含めることができ、コミュニティVLANと

他の場所とのトラフィック送信を行う役割を持つVLAN

- **isolated** – 隔離VLANを指定。 隔離VLANに割り当てられているポートは、該当するVLAN内の無差別ポートとのみ通信が可能です。

### デフォルト設定

なし

### コマンドモード

VLAN Configuration (VLAN設定)

### コマンドの使用方法

- プライベートVLANは、トラフィックを同じコミュニティまたは隔離VLAN内のポートに制限し、コミュニティ外部へのトラフィックを無差別ポート経由で送信するために使用します。 コミュニティVLANを使用するときは、関連付けられている「プライマリ」VLAN (無差別ポートを含む)にマッピングする必要があります。 隔離VLANを使用するときは、無差別ポートを1つ含むように設定する必要があります。
- プライベートVLANのポートメンバシップは静的です。 いったんプライベートVLANに割り当てられたポートは、GVRP経由で別のVLANに動的に移動することはできません。
- プライベートVLANポートはトランクモードには設定できません (416ページの「switchport mode」を参照)。

### 例

```
Console(config)#vlan database
Console(config-vlan)#private-vlan 2 primary
Console(config-vlan)#private-vlan 3 community
Console(config)#
```

## private vlan association

プライマリVLANをセカンダリ(コミュニティ) VLANに関連付けます。 指定したプライマリVLANのすべての関連付けを削除するには**no**形式を使用します。

### 構文

**private-vlan** *プライマリVLAN ID* **association** {*セカンダリVLAN ID* | **add** *セカンダリVLAN ID* | **remove** *セカンダリVLAN ID*}

**no private-vlan** *プライマリVLAN ID* **association**

- *プライマリVLAN ID* – プライマリVLANのID
  (範囲:1～4094、頭にゼロは不要)
- *セカンダリVLAN ID* – セカンダリ(コミュニティ)VLANのID (範囲:1～4094、頭にゼロは不要)

### デフォルト設定

なし

### コマンドモード

VLAN Configuration

### コマンドの使用方法

セカンダリVLANは、グループのメンバにセキュリティを提供します。 関連付けられているプライマリVLANは、プライマリVLAN内の他のネットワークリソース(無差別ポートを含めて設定されているサーバ)、およびプライマリVLAN外部のリソース(無差別ポート経由)にアクセスする共通のインタフェースを提供します。

### 例

```
Console(config-vlan)#private-vlan 2 association 3
Console(config)#
```

## switchport mode private-vlan

任意のインタフェースのプライベートVLANモードを設定します。 デフォルト設定を復元するには**no**形式を使用します。

### 構文

**switchport mode private-vlan** {**host** | **promiscuous**}
**no switchport mode private-vlan**

- **host** - このポートタイプは、コミュニティVLANまたは隔離VLANに割り当てることが可能
- **promiscuous** - このポートタイプは、同じプライマリVLAN内の他のすべての無差別ポート、および関連付けられているセカンダリVLAN内のすべてのポートと通信可能

### デフォルト設定

Normal VLAN

### コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

### コマンドの使用方法

- **switchport private-vlan mapping**コマンドを使用して、任意の無差別ポートをプライマリVLANに割り当てます。 **private-vlan host association**コマンドを使用して、任意のホストポートをコミュニティVLANに割り当てます。

・ **switchport private-vlan isolated**コマンドを使用して、任意の無差別ポートまたはホストポートを隔離VLANに割り当てます。

**例**

```
Console(config)#interface ethernet 1/2
Console(config-if)#switchport mode private-vlan promiscuous
Console(config-if)#exit
Console(config)#interface ethernet 1/3
Console(config-if)#switchport mode private-vlan host
Console(config-if)#
```

### switchport private-vlan host-association

任意のインタフェースをセカンダリVLANに関連付けます。 この関連付けを削除するには**no**形式を使用します。

**構文**

**switchport private-vlan host-association** *セカンダリVLAN ID*
**no switchport private-vlan host-association**

*セカンダリVLAN ID* - セカンダリVLANのID (範囲:2～4094)

**デフォルト設定**

なし

**コマンドモード**

Interface Configuration (イーサネット、ポートチャネル)

**コマンドの使用方法**

セカンダリ(コミュニティ) VLANに割り当てられているポートはすべて、グループのメンバ間でトラフィックを受け渡しできますが、グループ外のリソースとは、関連付けられているプライマリVLANの無差別ポート経由で通信する必要があります。

**例**

```
Console(config)#interface ethernet 1/3
Console(config-if)#switchport private-vlan host-association 3
Console(config-if)#
```

### switchport private-vlan isolated

任意のインタフェースを隔離VLANに割り当てます。 この割り当てを削除するにはno形式を使用します。

#### 構文

**switchport private-vlan isolated** *隔離VLAN ID*
**no switchport private-vlan isolated**

*隔離VLAN ID* - セカンダリVLANのID (範囲:1～4094)

#### デフォルト設定

なし

#### コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

#### コマンドの使用方法

隔離VLANに割り当てられているホストポートは、グループのメンバ間でトラフィックを受け渡しできません。また、グループ外のリソースとは、無差別ポート経由で通信する必要があります。

#### 例

```
Console(config)#interface ethernet 1/3
Console(config-if)#switchport private-vlan isolated 3
Console(config-if)#
```

### switchport private-vlan mapping

任意のインタフェースをプライマリVLANにマッピングします。 このマッピングを削除するにはno形式を使用します。

#### 構文

**switchport private-vlan mapping** *プライマリVLAN ID*
**no switchport private-vlan mapping**

*プライマリVLAN ID* - プライマリVLANのID (範囲:1～4094、頭にゼロは不要)

#### デフォルト設定

なし

#### コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

### コマンドの使用方法

プライマリVLANに割り当てられている無差別ポートは、同じVLAN内の他のすべての無差別ポート、および関連付けられているセカンダリVLAN内のグループメンバと通信できます。

### 例

```
Console(config)#interface ethernet 1/2
Console(config-if)#switchport private-vlan mapping 2
Console(config-if)#
```

## show vlan private-vlan

本製品上のプライベートVLANの設定を表示します。

### 構文

**show vlan private-vlan** [**community** | **isolated** | **primary**]

- **community** - すべてのコミュニティVLANを、関連付けられているプライマリVLANおよび割り当てられているホストインタフェースと共に表示
- **isolated** - 任意の隔離VLANを、割り当てられている無差別インタフェースおよびホストインタフェースと共に表示。 PrimaryフィールドとSecondaryフィールドには、いずれも隔離VLAN IDが表示されます。
- **primary** - すべてのプライマリVLANを、割り当てられている無差別インタフェースと共に表示

### デフォルト設定

なし

### コマンドモード

Privileged Executive

### 例

```
Console#show vlan private-vlan
Primary    Secondary          Type          Interfaces
--------  -----------  ----------  --------------------------------
       5                  primary       Eth1/ 3
       5            6     community     Eth1/ 4 Eth1/ 5
       0            8     isolated
Console#
```

# GVRPおよびブリッジ拡張コマンド

GARP VLAN登録プロトコルは、ネットワーク全体のインタフェースでVLANメンバを自動的に登録するために、スイッチがVLAN情報を交換する方法を定義します。 本セクションでは、個々のインタフェースに対して、また本製品でグローバルにGVRPを有効にする方法、およびブリッジ拡張MIBのデフォルト設定を表示する方法について解説します。

表 4-56 GVRPおよびブリッジ拡張コマンド

| コマンド | 機能 | モード | ページ |
|---|---|---|---|
| bridge-ext gvrp | 本製品でGVRPをグローバルに有効化 | GC | 430 |
| show bridge-ext | グローバルなブリッジ拡張設定を表示 | PE | 431 |
| switchport gvrp | 任意のインタフェースのGVRPを有効化 | IC | 431 |
| switchport forbidden vlan | 任意のインタフェースの禁止VLANを設定 | IC | 421 |
| show gvrp configuration | 選択したインタフェースのGVRP設定を表示 | NE、PE | 432 |
| garp timer | 選択した機能のGARPタイマを設定 | IC | 433 |
| show garp timer | 選択した機能のGARPタイマを表示 | NE、PE | 434 |

### bridge-ext gvrp

本製品でGVRPをグローバルに有効にします。 無効にするには**no**形式を使用します。

#### 構文

[no] **bridge-ext gvrp**

#### デフォルト設定

無効

#### コマンドモード

Global Configuration

#### コマンドの使用方法

GARPは、ネットワーク全体のポートでVLANメンバを登録するために、スイッチがVLAN情報を交換する方法を定義します。 VLANの自動登録を許可する場合や、ローカルスイッチ外部に拡張するVLANに対応する場合は、この機能を有効にする必要があります。

**例**

```
Console(config)#bridge-ext gvrp
Console(config)#
```

### show bridge-ext

ブリッジ拡張コマンドの設定を表示します。

**デフォルト設定**

なし

**コマンドモード**

Privileged Exec

**コマンドの使用方法**

表示される項目の詳細については、182ページの「Enabling or Disabling GVRP (Global Setting)および 37ページの「Displaying Bridge Extension Capabilities」を参照してください。

**例**

```
Console#show bridge-ext
  Max support vlan numbers:                255
  Max support vlan ID:                     4094
  Extended multicast filtering services: No
  Static entry individual port:          Yes
  VLAN learning:                           IVL
  Configurable PVID tagging:             Yes
  Local VLAN capable:                      No
  Traffic classes:                       Enabled
  Global GVRP status:                      Enabled
  GMRP:                                        Disabled
Console#
```

### switchport gvrp

任意のポートのGVRPを有効にします。 無効にするには**no**形式を使用します。

**構文**

[no] switchport gvrp

**デフォルト設定**

無効

**コマンドモード**

Interface Configuration (イーサネット、ポートチャネル)

**例**

```
Console(config)#interface ethernet 1/6
Console(config-if)#switchport gvrp
Console(config-if)#
```

### show gvrp configuration

GVRPが有効かどうかを表示します。

**構文**

**show gvrp configuration** [*インタフェース*]

*インタフェース*

- **ethernet** *ユニット/ポート*
  - *ユニット* - スタックユニット (範囲:1～8)
  - *ポート* - ポート番号 (範囲:1～26)
- **port-channel** *チャネルID* (範囲:1～4)

**デフォルト設定**

グローバルな設定とインタフェースに固有の設定の両方を表示

**コマンドモード**

Normal Exec、Privileged Exec

**例**

```
Console#show gvrp configuration ethernet 1/6
Eth 1/ 6:
  GVRP configuration: Enabled
Console#
```

### garp timer

join (参加)タイマ、leave (離脱)タイマ、leaveall (すべて離脱)タイマの値を設定します。 タイマのデフォルト値を復元するにはno形式を使用します。

### 構文

**garp timer** {**join** | **leave** | **leaveall**} *タイマの値*
**no garp timer** {**join** | **leave** | **leaveall**}

- {**join** | **leave** | **leaveall**} - 設定するタイマを指定
- *タイマの値* - タイマの値
  範囲は以下のとおりです。
  join:20～1000センチ秒(1/100秒)
  leave:60～3000センチ秒
  leaveall:500～18000センチ秒

### デフォルト設定

- join:20センチ秒
- leave:60センチ秒
- leaveall:1000センチ秒

### コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

### コマンドの使用方法

- グループアドレス登録プロトコル(GARP)は、GVRPおよびGMRPで、ブリッジされているLANの中のクライアントサービスのクライアント属性を登録または登録解除する際に使用します。 GARPタイマのデフォルト値は、メディアのアクセス方法やデータ速度に依存しません。 これらの値は、GMRPまたはGVRPの登録や登録解除に問題が発生している場合を除き、変更しないでください。
- タイマの値は、すべてのVLANのすべてのポートのGVRPに適用されます。
- タイマの値は、以下の制限を満たす必要があります。
  - leave >= (2 × join)
  - leaveall > leave

**注意:** 同じネットワークで接続されているすべてのレイヤ2機器で、GVRPタイマを同じ値に設定してください。 そうしないと、GVRPが正常に動作しない場合があります。

### 例

```
Console(config)#interface ethernet 1/1
Console(config-if)#garp timer join 100
Console(config-if)#
```

**関連コマンド**

show garp timer (p.434)

### show garp timer

選択したインタフェースのGARPタイマを表示します。

**構文**

**show garp timer** [*インタフェース*]

*インタフェース*

- **ethernet** *ユニット/ポート*
  - *ユニット* - スタックユニット (範囲:1～8)
  - *ポート* - ポート番号 (範囲:1～26)
- **port-channel** *チャネルID* (範囲:1～4)

**デフォルト設定**

すべてのGARPタイマを表示

**コマンドモード**

Normal Exec、Privileged Exec

**例**

```
Console#show garp timer ethernet 1/1
Eth 1/ 1 GARP timer status:
  Join timer:        100 centiseconds
  Leave timer:        60 centiseconds
  Leaveall timer: 1000 centiseconds
Console#
```

**関連コマンド**

garp timer (p.433)

# 優先度コマンド

本セクションで解説するコマンドを使用すると、本製品で混雑によってトラフィックがバッファされたときに、どのデータパケットを優先するかを指定することができます。 本製品は、ポートごとに4つの優先度キューを使用するCoSに対応しています。 各ポートの優先度の高いキューにあるデータパケットが、優先度の低いキューにあるパケットより先に送信されます。 各インタフェースのデフォルトの優先度や、各キューの相対的ウェイト、本製品の優先度キューに対するフレーム優先度タグのマッピングを設定できます。

表 4-57 優先度コマンド

| コマンドグループ | 機能 | ページ |
|---|---|---|
| 優先度(レイヤ2) | タグ無しフレームのデフォルトの優先度の設定、キューのウェイトの設定、CoSタグのハードウェアキューへのマッピング | 435 |
| 優先度(レイヤ3および4) | TCPポート、IP優先度タグ、またはIP DSCPタグをCoS値にマッピング | 442 |

## 優先度コマンド(レイヤ2)

**表 4-58 優先度コマンド(レイヤ2)**

| コマンド | 機能 | モード | ページ |
|---|---|---|---|
| queue mode | キューモードをストリクトまたはウェイトラウンドロビン(WRR)に設定 | GC | 436 |
| switchport priority default | 着信タグ無しフレームのポート優先度を設定 | IC | 436 |
| queue bandwidth | ラウンドロビンウェイトを優先度キューに割り当て | GC | 437 |
| queue cos map | CoS値を優先度キューに割り当て | IC | 438 |
| show queue mode | 現在のキューモードを表示 | PE | 439 |
| show queue bandwidth | 優先度キューに割り当てられているラウンドロビンウェイトを表示 | PE | 440 |
| show queue cos-map | CoSマップを表示 | PE | 440 |
| show interfaces switchport | 任意のインタフェースの管理および運用のステータスを表示 | PE | 377 |

### queue mode

クラスオブサービス(CoS)優先度キューに関して、キューモードをストリクトまたはウェイトラウンドロビン(WRR)に設定します。 デフォルト値を復元するにはno形式を使用します。

#### 構文

queue mode {strict | wrr}
no queue mode

- strict – 送信キューを順番に処理。優先度の高いキューのトラフィックをすべて送信してから、優先度の低いキューを処理します。
- wrr – ウェイトラウンドロビンは、キュー0～3にそれぞれスケジュールウェイト1、2、4、6を使用し、送信ポートの帯域幅を共有します。

#### デフォルト設定

ウェイトラウンドロビン

#### コマンドモード

Global Configuration

#### コマンドの使用方法

本製品のキューの処理方法には、厳密なルールに基づいて優先度の高いキューのトラフィックをすべて処理してから優先度の低いキューを処理する方法と、ウェイトラウンドロビン(WRR)を使用して各キューの相対的ウェイトを指定する方法があります。WRRでは、各キューに事前に定義されている相対的ウェイトを使用します。これによって、次のキューに移動するまでの各キューでの処理時間の割合を特定できます。これにより、ストリクトのキューで発生するおそれのある行先頭のブロックを回避できます。

#### 例

以下の例では、キューモードをストリクトのサービスモードに設定します。

```
Console(config)#queue mode strict
Console(config)#
```

### switchport priority default

着信タグ無しフレームの優先度を設定します。 デフォルト値を復元するにはno形式を使用します。

#### 構文

switchport priority default *デフォルトの優先度ID*
no switchport priority default

*デフォルトの優先度ID* - タグ無し着信トラフィックの優先度を示す数値。
優先度は0～7の数値で表し、7が最も高い優先度になります。

### デフォルト設定

優先度の設定なし。インタフェースで受信するタグ無しフレームのデフォルト値はゼロ

### コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

### コマンドの使用方法

- 優先度マッピングの優先度は、IP Port (IPポート)、IP Precedence (IP優先度)またはIP DSCP、およびデフォルトのスイッチポート優先度です。
- 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ように設定されているポート(タグ無し、タグ付きの両方のフレームを受信)で受信するタグ無しフレームに適用されます。 この優先度は、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は、IEEE 802.1p User Priority (ユーザ優先度)ビットが使用されます。
- 本製品には、ポートごとに8つの優先度キューが備えられています。 ウェイトラウンドロビンを使用するように設定されており、これは**show queue bandwidth**コマンドを使用して表示できます。 VLANタグが付いていない着信フレームは、入力ポートのデフォルトの着信ユーザ優先度のタグが付けられ、出力ポートの適切な優先度キューに配置されます。 すべての着信ポートのデフォルトの優先度はゼロです。したがって、優先度タグの付いていない着信フレームはすべて、出力ポートのキュー0に配置されます (出力ポートが関連付けられているVLANのタグ無しメンバである場合、これらのフレームは、送信前にすべてのVLANタグが除去されます)。

### 例

以下の例は、ポート3のデフォルトの優先度を5に設定する方法を示しています。

```
Console(config)#interface ethernet 1/3
Console(config-if)#switchport priority default 5
```

## queue bandwidth

4つのクラスオブサービス(CoS)優先度キューにウェイトラウンドロビン(WRR)のウェイトを割り当てます。 デフォルトのウェイトを復元するには**no**形式を使用します。

### 構文

**queue bandwidth** *ウェイト1...ウェイト3*
**no queue bandwidth**

*ウェイト1...ウェイト3* - キュー0～3のウェイトの比率によって、WRRスケジューラで使用するウェイトが決定。 ただし、キュー0のウェイトは1に固定されており、変更は

できません（範囲：1～31）。

### デフォルト設定

ウェイト1、2、4、6は、それぞれキュー0～3に割り当て。
キュー0は変更不可

### コマンドモード

Global Configuration

### コマンドの使用方法

WRRは、スケジュールウェイトを定義することにより、送信ポートでの帯域幅共有を制御します。

### 例

以下の例では、優先度キュー1～3にWRRウェイトを割り当てる方法を示しています。

```
Console(config)#queue bandwidth 6 9 12
Console(config)#
```

### 関連コマンド

show queue bandwidth (p.440)

## queue cos-map

クラスオブサービス(CoS)の値を優先度キュー(ハードウェアの出力キュー0～3)に割り当てます。 CoSマップをデフォルト値に設定するには**no**形式を使用します。

### 構文

**queue cos-map** *キューID* [*cos1 ... cosn*]
**no queue cos-map**

- *キューID* - 優先度キューのID
  範囲は0～3で、3が優先度の最も高いキュー。
- *cos1 .. cosn* - キューIDにマッピングされるCoSの値。数値をスペースで区切ったリストで、 CoS値は0～7の数値で表し、7が最も高い優先度になります。

### デフォルト設定

本製品は、ポートごとに4つの優先度キューとウェイトラウンドロビンを使用して、CoSに対応しています。 IEEE 802.1pでは8つの異なるトラフィッククラスが定義されています。 デフォルトの優先度レベルは、以下に示すIEEE 802.1p標準の推奨に従って割り当てられます。

表 4-59 デフォルトのCoS優先度レベル

| キュー | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 優先度 | 1, 2 | 0, 3 | 4, 5 | 6, 7 |

**コマンドモード**

Interface Configuration (イーサネット、ポートチャネル)

**コマンドの使用方法**

- 着信ポートで割り当てられるCoS値は、出力ポートでも使用されます。
- このコマンドは、すべてのインタフェースのCoS優先度を設定します。

**例**

以下の例は、CoS値0、1および2を出力キュー0に、値3を出力キュー1に、値4および5を出力キュー2に、値6および7を出力キュー3にマッピングする方法を示しています。

```
Console(config)#interface ethernet 1/1
Console(config-if)#queue cos-map 0 0 1 2
Console(config-if)#queue cos-map 1 3
Console(config-if)#queue cos-map 2 4 5
Console(config-if)#queue cos-map 3 6 7
Console(config-if)#end
Console#show queue cos-map ethernet 1/1
Information of Eth 1/1
  CoS Value        : 0 1 2 3 4 5 6 7
  Priority Queue: 0 0 0 1 2 2 3 3
Console#
```

**関連コマンド**

show queue cos-map (p.440)

### show queue mode

現在のキューモードを表示します。

**デフォルト設定**

なし

**コマンドモード**

Privileged Exec

**例**

```
Console#show queue mode


Queue mode: wrr
Console#
```

### show queue bandwidth

4つの優先度キューへのウェイトラウンドロビン(WRR)帯域幅の割り当てを表示します。

#### デフォルト設定

なし

#### コマンドモード

Privileged Exec

#### 例

```
Console#show queue bandwidth
 Queue ID   Weight
 --------   ------
     0          1
     1          2
     2          4
     3          6
Console#
```

### show queue cos-map

CoS優先度マップを表示します。

#### 構文

**show queue cos-map** [*インタフェース*]

*インタフェース*

- **ethernet** *ユニット/ポート*
  - *ユニット* - スタックユニット (範囲:1～8)
  - *ポート* - ポート番号 (範囲:1～26)
- **port-channel** *チャネルID* (範囲:1～4)

#### デフォルト設定

なし

**コマンドモード**

Privileged Exec

**例**

```
Console#show queue cos-map ethernet 1/1
Information of Eth 1/1
  CoS Value      : 0 1 2 3 4 5 6 7
  Priority Queue: 0 0 0 1 2 2 3 3
Console#
```

## 優先度コマンド(レイヤ3および4)

表 4-60 優先度コマンド(レイヤ3および4)

| コマンド | 機能 | モード | ページ |
|---|---|---|---|
| map ip port | Enables TCP/UDP class of service mapping | GC | 443 |
| map ip port | Maps TCP/UDP socket to a class of service | IC | 444 |
| map ip port | TCPのCoSマッピングを有効化 | GC | 444 |
| map ip port | TCPソケットをCoSにマッピング | IC | 450 |
| map ip precedence | IP優先度のCoSマッピングを有効化 | GC | 443 |
| map ip precedence | IP優先度値をCoSにマッピング | IC | 445 |
| map ip dscp | IPDSCPのCoSマッピングを有効化 | GC | 447 |
| map ip dscp | IP DSCP値をCoSにマッピング | IC | 447 |
| show map ip port | Shows the IP port map | PE | 448 |
| map access-list ip | ACLルールに一致するパケットのCoS値および対応する出力キューを設定 | IC | 348 |
| map access-list mac | ACLルールに一致するパケットのCoS値および対応する出力キューを設定 | IC | 365 |
| show map ip port | IPポートマップを表示 | PE | 448 |
| show map ip precedence | IP優先度マップを表示 | PE | 449 |
| show map ip dscp | IP DSCPマップを表示 | PE | 450 |
| show map access-list ip | 任意のインタフェースのアクセスリストにマッピングされているCoS値を表示 | PE | 348 |
| show map access-list mac | 任意のインタフェースのアクセスリストにマッピングされているCoS値を表示 | PE | 355 |

**map ip port** (Global Configuration)

IPポートマッピング(TCP/UDPソケットのCoSマッピング)を有効にします。 IPポートマッピングを無効にするには**no**形式を使用します。

### 構文

[**no**] **map ip port**

### デフォルト設定

無効

### コマンドモード

Global Configuration

### コマンドの使用方法

優先度マッピングの優先度は、IP Port (IPポート)、IP Precedence (IP優先度)またはIP DSCP、およびデフォルトのスイッチポート優先度です。

### 例

以下の例は、TCP/UDPポートマッピングをグローバルに有効にする方法を示しています。

```
Console(config)#map ip port
Console(config)#
```

**map ip port** (Interface Configuration)
IPポート優先度(TCP/UDPポート優先度)を設定します。 特定の設定を削除するには**no**形式を使用します。

### 構文

**map ip port** *ポート番号* **cos** *CoS値*
**no map ip port** *ポート番号*

- *ポート番号* －16ビットのTCP/UDPポート番号(範囲:1～65535)
- *CoS値* －CoS値 (範囲:0～7)

### デフォルト設定

なし

### コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

### コマンドの使用方法

- 優先度マッピングの優先度は、IP Port (IPポート)、IP Precedence (IP優先度)またはIP DSCP、およびデフォルトのスイッチポート優先度です。
- このコマンドは、すべてのインタフェースのIPポート優先度を設定します。

### 例

以下の例は、HTTPトラフィックをCoS値0にマッピングする方法を示しています。

```
Console(config)#interface ethernet 1/5
Console(config-if)#map ip port 80 cos 0
Console(config-if)#
```

**map ip precedence** (Global Configuration)
IP優先度マッピング(IPのサービスのタイプ)を有効にします。 IP優先度マッピングを無効にするには**no**形式を使用します。

### 構文

[**no**] **map ip precedence**

### デフォルト設定

無効

**コマンドモード**

Global Configuration

**コマンドの使用方法**

- 優先度マッピングの優先度は、IP Port (IPポート)、IP Precedence (IP優先度)またはIP DSCP、およびデフォルトのスイッチポート優先度です。
- IP優先度とIP DSCPの両方を有効にすることはできません。 これらのうち一・方の優先度タイプを有効にすると、もう一方は自動的に無効になります。

**例**

以下の例は、IP優先度マッピングをグローバルに有効にする方法を示しています。

```
Console(config)#map ip precedence
Console(config)#
```

**map ip precedence** (Interface Configuration)

IP優先度(IPのサービスのタイプの優先度)を設定します。 デフォルトのテーブルを復元するには**no**形式を使用します。

**構文**

**map ip precedence** *IP優先度値* **cos** *CoS値*
**no map ip precedence**

- *優先度値* – 3ビットの優先度値 (範囲:0～7)
- *CoS値* – CoS値(範囲:0～7)

**デフォルト設定**

以下のリストは、デフォルトの優先度マッピングを表示

表 4-61 IP優先度値のマッピング

| **IP優先度値** | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| **CoS値** | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |

**コマンドモード**

Interface Configuration (イーサネット、ポートチャネル)

**コマンドの使用方法**

- 優先度マッピングの優先度は、IP Port (IPポート)、IP Precedence (IP優先度)またはIP DSCP、およびデフォルトのスイッチポート優先度です。

- IP優先度値は、IEEE 802.1p標準の推奨に従って、デフォルトのCoS値に1対1でマッピングされ、その後8つのハードウェア優先度キューにマッピングされます。
- このコマンドは、すべてのインタフェースのIP優先度を設定します。

**例**

以下の例は、IP優先度値1をCoS値0にマッピングする方法を示しています。

```
Console(config)#interface ethernet 1/5
Console(config-if)#map ip precedence 1 cos 0
Console(config-if)#
```

**map ip dscp** (Global Configuration)
IP DSCPマッピング(差別サービスコードポイントマッピング)を有効にします。 IP DSCPマッピングを無効にするには**no**形式を使用します。

### 構文

[**no**] **map ip dscp**

### デフォルト設定

無効

### コマンドモード

Global Configuration

### コマンドの使用方法

- 優先度マッピングの優先度は、IP Port (IPポート)、IP Precedence (IP優先度)またはIP DSCP、およびデフォルトのスイッチポート優先度です。
- IP優先度とIP DSCPの両方を有効にすることはできません。 これらのうち一方の優先度タイプを有効にすると、もう一方は自動的に無効になります。

### 例

以下の例は、IP DSCPマッピングをグローバルに有効にする方法を示しています。

```
Console(config)#map ip dscp
Console(config)#
```

**map ip dscp** (Interface Configuration)
IP DSCP優先度(差別サービスコードポイント優先度)を設定します。 デフォルトのテーブルを復元するには**no**形式を使用します。

### 構文

**map ip dscp** *DSCP値* **cos** *CoS値*
**no map ip dscp**

- *DSCP値* - 8ビットのDSCP値 (範囲:0～63)
- *CoS値* - CoS値(範囲:0～7)

### デフォルト設定

以下の表でDSCPのデフォルト値を定義。 指定されていないDSCPはすべてCoS値0にマッピング

表 4-62 IP DSCP値とCoS値

| 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 |

### コマンドモード

Interface Configuration (イーサネット、ポートチャネル)

### コマンドの使用方法

- 優先度マッピングの優先度は、IP Port (IPポート)、IP Precedence (IP優先度)またはIP DSCP、およびデフォルトのスイッチポート優先度です。
- DSCP優先度値は、IEEE 802.1p標準の推奨に従って、デフォルトのCoS値にマッピングされ、その後4つのハードウェア優先度キューにマッピングされます。
- このコマンドは、すべてのインタフェースのIP DSCP優先度を設定します。

### 例

以下の例は、IP DSCP値1をCoS値0にマッピングする方法を示しています。

```
Console(config)#interface ethernet 1/5
Console(config-if)#map ip dscp 1 cos 0
Console(config-if)#
```

## show map ip port

IPポート優先度マップを表示します。

### 構文

**show map ip port** [*インタフェース*]

*インタフェース*

- **ethernet** *ユニット/ポート*
  - *ユニット* - スタックユニット (範囲:1～8)
  - *ポート* - ポート番号 (範囲:1～26)
- **port-channel** *チャネルID* (範囲:1～4)

### デフォルト設定

なし

### コマンドモード

Privileged Exec

### 例

以下は、HTTPトラフィックがCoS値0にマッピングされていることを示しています。

```
Console#show map ip port
TCP port mapping status: disabled


 Port         Port no. COS
 ---------- -------- ---
   Eth 1/ 5         80     0
Console#
```

### 関連コマンド

map ip port (Global Configuration) (p.443)
map ip port (Interface Configuration) (444)

## show map ip precedence

IP優先度マップを表示します。

### 構文

**show map ip precedence** [*インタフェース*]

*インタフェース*

- **ethernet** *ユニット/ポート*
  - *ユニット* - スタックユニット (範囲:1～8)
  - *ポート* - ポート番号 (範囲:1～26)
- **port-channel** *チャネルID* (範囲:1～4)

### デフォルト設定

なし

### コマンドモード

Privileged Exec

### 例

```
Console#show map ip precedence ethernet 1/5
Precedence mapping status: disabled


 Port        Precedence COS
 --------- ---------- ---
  Eth 1/ 5           0   0
  Eth 1/ 5           1   1
  Eth 1/ 5           2   2
  Eth 1/ 5           3   3
  Eth 1/ 5           4   4
  Eth 1/ 5           5   5
  Eth 1/ 5           6   6
  Eth 1/ 5           7   7
Console#
```

### 関連コマンド

map ip port (Global Configuration) (p.443)
map ip precedence (Interface Configuration) (p.445)

## show map ip dscp

IP DSCP優先度マップを表示します。

### 構文

**show map ip dscp** [*インタフェース*]

*インタフェース*

- **ethernet** *ユニット/ポート*
  - *ユニット* - スタックユニット (範囲:1～8)
  - *ポート* - ポート番号 (範囲:1～26)
- **port-channel** *チャネルID* (範囲:1～4)

### デフォルト設定

なし

**コマンドモード**

Privileged Exec

**例**

```
Console#show map ip dscp ethernet 1/1
DSCP mapping status: disabled


 Port          DSCP COS
 ---------- ---- ---
   Eth 1/ 1      0    0
   Eth 1/ 1      1    0
   Eth 1/ 1      2    0
   Eth 1/ 1      3    0
.
.
.
   Eth 1/ 1     61    0
   Eth 1/ 1     62    0
   Eth 1/ 1     63    0
Console#
```

**関連コマンド**

map ip dscp (Global Configuration) (p.447)
map ip dscp (Interface Configuration) (p.447)

# マルチキャストフィルタリングコマンド

本製品は、IGMP (インターネットグループ管理プロトコル)を使用して、特定のマルチキャストサービスを受信する必要のある接続ホストのクエリを行います。 サービスを必要とするホストを含むポートを特定し、該当するポートのみにデータを送信します。 その後、隣接するマルチキャストスイッチまたはルータまでサービス要求を伝播し、マルチキャストサービスを継続して受信できるようにします。

表 4-63 マルチキャストフィルタリングコマンド

| コマンドグループ | 機能 | ページ |
|---|---|---|
| IGMPスヌーピング | IGMPスヌーピングまたは静的割り当てを使用したマルチキャストグループの設定、IGMPバージョンの設定、現在のスヌーピングおよびクエリの設定の表示、マルチキャストサービスおよびグループメンバの表示 | 452 |
| IGMPクエリ | レイヤ2でマルチキャストフィルタリング用のIGMPクエリパラメータを設定 | 456 |
| 静的マルチキャストルーティング | 静的マルチキャストルータポートを設定 | 460 |
| IGMP (Layer 3) | Configures the IGMP protocol used with multicast routing | 442 |

## IGMPスヌーピングコマンド

表 4-64 IGMPスヌーピングコマンド

| コマンド | 機能 | モード | ページ |
|---|---|---|---|
| ip igmp snooping | IGMPスヌーピングを有効化 | GC | 452 |
| ip igmp snooping vlan static | マルチキャストグループのメンバとしてインタフェースを追加 | GC | 453 |
| ip igmp snooping version | スヌーピングのIGMPバージョンを設定 | GC | 454 |
| show ip igmp snooping | IGMPスヌーピングおよびクエリの設定を表示 | PE | 454 |
| show mac-address-table multicast | IGMPスヌーピングMACマルチキャストリストを表示 | PE | 455 |

### ip igmp snooping

本製品でIGMPスヌーピングを有効にします。 無効にするには**no**形式を使用します。

#### 構文

[no] ip igmp snooping

#### デフォルト設定

有効

**コマンドモード**

Global Configuration

**例**

以下の例では、IGMPスヌーピングが有効になります。

```
Console(config)#ip igmp snooping
Console(config)#
```

### ip igmp snooping vlan static

マルチキャストグループにポートを追加します。 ポートを削除するには**no**形式を使用します。

**構文**

[**no**] **ip igmp snooping vlan** *VLAN ID* **static** *IPアドレス インタフェース*

- *VLAN ID* - VLAN ID (範囲:1～4094)
- *IPアドレス* - マルチキャストグループのIPアドレス
- *インタフェース*
  - **ethernet** *ユニット/ポート*
    - *ユニット* - スタックユニット (範囲:1～8)
    - *ポート* - ポート番号 (範囲:1～26)
  - **port-channel** *チャネルID* (範囲:1～4)

**デフォルト設定**

なし

**コマンドモード**

Global Configuration

**例**

以下は、任意のポートでマルチキャストグループを静的に設定する方法を示しています。

```
Console(config)#ip igmp snooping vlan 1 static 224.0.0.12 ethernet 1/5
Console(config)#
```

### ip igmp snooping version

IGMPスヌーピングのバージョンを設定します。 デフォルトを復元するにはno形式を使用します。

#### 構文

ip igmp snooping version {1 | 2}
no ip igmp snooping version

- 1 – IGMPバージョン1
- 2 – IGMPバージョン2

#### デフォルト設定

IGMPバージョン2

#### コマンドモード

Global Configuration

#### コマンドの使用方法

- サブネット上のすべてのシステムが同じバージョンに対応している必要があります。バージョン1のみに対応する旧式の機器がネットワーク内にある場合は、本製品もバージョン1を使用するように設定する必要があります。
- ip igmp query-max-response-timeやip igmp query-timeoutなど、IGMPv2のみで有効なコマンドもあります。

#### 例

以下の例では、IGMPバージョン1を使用するように本製品を設定します。

```
Console(config)#ip igmp snooping version 1
Console(config)#
```

### show ip igmp snooping

IGMPスヌーピングの設定を表示します。

#### デフォルト設定

なし

#### コマンドモード

Privileged Exec

#### コマンドの使用方法

表示される項目の詳細については、226ページの「IGMPスヌーピングおよびクエリパ

ラメータの設定」を参照してください。

**例**

以下は、現在のIGMPスヌーピングの設定を示しています。

```
Console#show ip igmp snooping
 Service status:              Enabled
 Querier status:              Enabled
 Query count:                   2
 Query interval:              125 sec
 Query max response time: 10 sec
 Router port expire time: 300 sec
 IGMP snooping version:     Version 2
Console#
```

### show mac-address-table multicast

既知のマルチキャストアドレスを表示します。

**構文**

**show mac-address-table multicast** [**vlan** *VLAN ID*] [**user** | **igmp-snooping**]

- *VLAN ID* - VLAN ID (1～4094)
- **user** - ユーザが設定したマルチキャストエントリのみを表示
- **igmp-snooping** - IGMPスヌーピングを使用して学習したエントリのみを表示

**デフォルト設定**

なし

**コマンドモード**

Privileged Exec

**コマンドの使用方法**

選択するオプションによって、IGMPやUSERなどのメンバタイプが表示されます。

**例**

以下は、VLAN 1のIGMPスヌーピングを使用して学習されたマルチキャストエントリを示しています。

```
Console#show mac-address-table multicast vlan 1 igmp-snooping
 VLAN M'cast IP addr. Member ports Type
 ---- --------------- ------------ -------
    1        224.1.2.3        Eth1/11      IGMP
Console#
```

## IGMPクエリコマンド(レイヤ2)

表 4-65 IGMPクエリコマンド(レイヤ2)

| コマンド | 機能 | モード | ページ |
|---|---|---|---|
| ip igmp snooping querier | 本製品をIGMPスヌーピング用のクエリアとして有効化 | GC | 456 |
| ip igmp snooping query-count | クエリカウントを設定 | GC | 457 |
| ip igmp snooping query-interval | クエリ間隔を設定 | GC | 457 |
| ip igmp snooping query-max-response-time | レポート遅延を設定 | GC | 458 |
| ip igmp snooping router-port-expire-time | クエリタイムアウトを設定 | GC | 459 |

### ip igmp snooping querier

本製品をIGMPクエリア(クエリ発行者)として有効にします。 無効にするにはno形式を使用します。

#### 構文

[no] ip igmp snooping querier

#### デフォルト設定

有効

#### コマンドモード

Global Configuration

#### コマンドの使用方法

有効にすると、本製品をクエリアとして使用できます。 クエリアの役割は、マルチキャストトラフィックを受信する必要があるかどうかホストに確認することです。

#### 例

```
Console(config)#ip igmp snooping querier
Console(config)#
```

### ip igmp snooping query-count

クエリカウントを設定します。 デフォルトを復元するには**no**形式を使用します。

#### 構文

**ip igmp snooping query-count** *カウント*
**no ip igmp snooping query-count**

*カウント* – 最大クエリの発行がここで指定した回数を超えても応答がない場合、本製品はマルチキャストグループからクライアントを削除する処理を実行 (範囲:2～10)

#### デフォルト設定

2回

#### コマンドモード

Global Configuration

#### コマンドの使用方法

クエリカウントは、クエリアがマルチキャストクライアントからの応答をどのくらいの期間待ってから処理を行うかを定義します。 このコマンドで定義されている数のクエリをクエリアが送信し終えてもクライアントからの応答がない場合は、**ip igmp snooping query-max- response-time**で定義されている時間を使用してカウントダウンタイマが始動します。 カウントダウンが終了してもクライアントからの応答がない場合、そのクライアントはマルチキャストグループを離脱したとみなされます。

#### 例

以下は、クエリカウントを10に設定する方法を示しています。

```
Console(config)#ip igmp snooping query-count 10
Console(config)#
```

#### 関連コマンド

ip igmp snooping query-max-response-time (p.458)

### ip igmp snooping query-interval

クエリ間隔を設定します。 デフォルトを復元するには**no**形式を使用します。

#### 構文

**ip igmp snooping query-interval** *秒*
**no ip igmp snooping query-interval**

*秒* – 本製品がIGMPホストクエリメッセージを送信する間隔 (範囲:60～125)

**デフォルト設定**

125秒

**コマンドモード**

Global Configuration

**例**

以下は、クエリ間隔を100秒に設定する方法を示しています。

```
Console(config)#ip igmp snooping query-interval 100
Console(config)#
```

**ip igmp snooping query-max-response-time**

クエリレポートの遅延を設定します。 デフォルトを復元するには**no**形式を使用します。

**構文**

**ip igmp snooping query-max-response-time** *秒*
**no ip igmp snooping query-max-response-time**

*秒* - IGMPクエリで通知されるレポートの遅延 (範囲:5～25)

**デフォルト設定**

10秒

**コマンドモード**

Global Configuration

**コマンドの使用方法**

- 本製品でIGMPv2を使用している場合にのみ、このコマンドは有効になります。
- このコマンドでは、クエリ後にマルチキャストクライアントからの応答があると予測される時間を定義します。 **ip igmp snooping query-count**で定義されている数のクエリをクエリアが送信し終えてもクライアントからの応答がない場合は、このコマンドで設定されている初期値を使用してカウントダウンタイマが始動します。 カウントダウンが終了してもクライアントからの応答がない場合、そのクライアントはマルチキャストグループを離脱したとみなされます。

**例**

以下は、最長応答時間を20秒に設定する方法を示しています。

```
Console(config)#ip igmp snooping query-max-response-time 20
```

```
Console(config)#
```

### 関連コマンド

ip igmp snooping version (p.454)
ip igmp snooping query-max-response-time (p.458)

## ip igmp snooping router-port-expire-time

クエリタイムアウトを設定します。 デフォルトを復元するにはno形式を使用します。

### 構文

**ip igmp snooping router-port-expire-time** *秒*
**no ip igmp snooping router-port-expire-time**

*秒* - 前回のクエリアが停止してから、ルータポート(クエリパケットを受信していたインタフェース)を期限切れとみなすまでの待機時間
(範囲:300～500)

### デフォルト設定

300秒

### コマンドモード

Global Configuration

### コマンドの使用方法

本製品でIGMPv2を使用している場合にのみ、このコマンドは有効になります。

### 例

以下は、デフォルトのタイムアウトを300秒に設定する方法を示しています。

```
Console(config)#ip igmp snooping router-port-expire-time 300
Console(config)#
```

### 関連コマンド

ip igmp snooping version (p.454)

## 静的マルチキャストルーティングコマンド

表 4-66 静的マルチキャストルーティングコマンド

| コマンド | 機能 | モード | ページ |
|---|---|---|---|
| ip igmp snooping vlan mrouter | マルチキャストルータポートを追加 | GC | 460 |
| show ip igmp snooping mrouter | マルチキャストルータポートを表示 | PE | 461 |

### ip igmp snooping vlan mrouter

マルチキャストルータポートを静的に設定します。 設定を削除するにはno形式を使用します。

#### 構文

[no] ip igmp snooping vlan *VLAN ID* mrouter *インタフェース*

- *VLAN ID* - VLAN ID (範囲:1～4094)
- *インタフェース*
  - ethernet *ユニット/ポート*
    - *ユニット* - スタックユニット (範囲:1～8)
    - *ポート* - ポート番号 (範囲:1～26)
  - port-channel *チャネルID* (範囲:1～4)

#### デフォルト設定

静的マルチキャストルータポートの設定

#### コマンドモード

Global Configuration

#### コマンドの使用方法

ネットワーク接続の状態によっては、IGMPスヌーピングでIGMPクエリアを検索できない場合があります。 したがって、IGMPクエリアが、使用しているルータのインタフェース(ポートまたはトランク)にネットワーク経由で接続されている既知のマルチキャストルータまたはスイッチである場合は、そのインタフェースを現在のすべてのマルチキャストグループに参加するように手動で設定することができます。

#### 例

以下は、ポート11をVLAN 1内のマルチキャストルータポートとして設定する方法を示してい

ます。

```
Console(config)#ip igmp snooping vlan 1 mrouter ethernet 1/11
Console(config)#
```

### show ip igmp snooping mrouter

静的に設定されたマルチキャストルータポートおよび動的に学習されたマルチキャストルータポートに関する情報を表示します。

#### 構文

**show ip igmp snooping mrouter** [**vlan** *VLAN ID*]

*VLAN ID* - VLAN ID (範囲:1～4094)

#### デフォルト設定

設定済みのすべてのVLANのマルチキャストルータポートを表示

#### コマンドモード

Privileged Exec

#### コマンドの使用方法

表示されるマルチキャストルータのタイプには、Static (静的)などがあります。

#### 例

以下は、VLAN 1のポート11がマルチキャストルータに接続されていることを示しています。

```
Console#show ip igmp snooping mrouter vlan 1
 VLAN M'cast Router Ports Type
 ---- ------------------- -------
    1                Eth 1/11   Static
    2                Eth 1/12   Static
Console#
```

# IPインタフェースコマンド

IPアドレスを使用して、ネットワーク経由で本製品に管理アクセスすることができます。 本製品のIPアドレスは、デフォルト設定によりDHCP経由で取得されます。 特定のIPアドレスを手動で設定できるほか、電源投入時にBOOTPサーバまたはDHCPサーバからアドレスを取得するように設定することもできます。 また、場合によっては、本製品と別のネットワークセグメントにある管理ステーションまたは他の機器との間でデフォルトのゲートウェイを確立する必要があります。

**表 4-67 IPインタフェースコマンド**

| コマンド | 機能 | モード | ページ |
|---|---|---|---|
| ip address | 現在のインタフェースのIPアドレスを設定 | IC | 462 |
| ip default-gateway | 本製品を他のサブネットワークに接続するデフォルトのゲートウェイを定義 | GC | 463 |
| ip dhcp restart | BOOTPまたはDHCPのクライアント要求を発行 | PE | 464 |
| show ip interface | 本製品のIP設定を表示 | PE | 465 |
| show ip redirects | 本製品用に設定されているデフォルトのゲートウェイを表示 | PE | 465 |
| ping | ネットワーク上の別のノードにICMPエコー要求パケットを送信 | NE、PE | 466 |

## ip address

現在選択されているVLANインタフェースのIPアドレスを設定します。 デフォルトのIPアドレスを復元するには**no**形式を使用します。

### 構文

**ip address** {*IPアドレス ネットマスク* | **bootp** | **dhcp**}
**no ip address**

- *IPアドレス* – IPアドレス
- *ネットマスク* – 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、特定のサブネットへのルーティングに使用するホストアドレスを特定します。
- **bootp** – IPアドレスをBOOTPから取得
- **dhcp** – IPアドレスをDHCPから取得

### デフォルト設定

DHCP

### コマンドモード

Interface Configuration (VLAN)

### コマンドの使用方法

- ネットワーク経由で管理アクセスできるようにするには、本製品にIPアドレスを割り当てる必要があります。 特定のIPアドレスを手動で設定できるほか、BOOTPサーバまたはDHCPサーバからアドレスを取得するように設定することもできます。 有効なIPアドレスは、0から255までの4つの数値をピリオドで区切った形式です。 この形式以外は、設定プログラムで設定できません。
- **bootp**オプションまたは**dhcp**オプションを選択すると、IPは有効になりますが、BOOTPまたはDHCPの応答を受信するまでは機能しません。 IPアドレスを学習するために、本製品から要求が定期的にブロードキャストされます (BOOTP値およびDHCP値には、IPアドレス、デフォルトのゲートウェイ、サブネットマスクを含めることができます)。
- BOOTP要求またはDHCP要求のブロードキャストは、**ip dhcp restart**コマンドを入力するか、または本製品を再起動することによって開始できます。

**注意:** IPアドレスを割り当てることができるVLANインタフェースは1つだけです(デフォルトはVLAN 1)。 これによって、管理VLAN、つまり本製品への管理アクセスが可能な唯一のVLANが定義されます。 その他のVLANにIPアドレスを割り当てると、新しいIPアドレスが元のIPアドレスより優先され、新しい管理VLANになります。

### 例

以下の例では、本製品にVLAN 1内のアドレスが割り当てられます。

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.5 255.255.255.0
Console(config-if)#
```

### 関連コマンド

ip dhcp restart (p.464)

## ip default-gateway

本製品と別のネットワークセグメントに存在する機器との間に、静的ルートを確立します。静的ルートを削除するには**no**形式を使用します。

### 構文

**ip default-gateway** *ゲートウェイ*
**no ip default-gateway**

*ゲートウェイ* – デフォルトゲートウェイのIPアドレス

**デフォルト設定**

静的ルートは未確立

**コマンドモード**

Global Configuration

**コマンドの使用方法**

管理ステーションが別のIPセグメントにある場合は、ゲートウェイを定義する必要があります。

**例**

以下の例では、本製品のデフォルトのゲートウェイを定義します。

```
Console(config)#ip default-gateway 10.1.1.254
Console(config)#
```

**関連コマンド**

show ip redirects (p.465)

**ip dhcp restart**

BOOTPまたはDHCPのクライアント要求を発行します。

**デフォルト設定**

なし

**コマンドモード**

Privileged Exec

**コマンドの使用方法**

- このコマンドは、**ip address**コマンドを使用してBOOTPモードまたはDHCPモードに設定されているIPインタフェースに関して、BOOTPまたはDHCPのクライアント要求を発行します。
- DHCPでは、クライアントの前回のアドレスが使用できれば、そのアドレスを再度割り当てる必要があります。
- BOOTPサーバまたはDHCPサーバが別のドメインに移動されている場合、クライアントに指定されているアドレスのネットワーク部分は、新しいドメインに基づいたものになります。

**例**

以下の例では、本製品に同じアドレスが再度割り当てられます。

```
Console(config)#interface vlan 1
Console(config-if)#ip address dhcp
Console(config-if)#end
Console#ip dhcp restart
Console#show ip interface
 IP address and netmask: 192.168.1.54 255.255.255.0 on VLAN 1,
 and address mode: DHCP.
Console#
```

**関連コマンド**

ip address (p.462)

### show ip interface

IPインタフェースの設定を表示します。

**デフォルト設定**

全インタフェース

**コマンドモード**

Privileged Exec

**例**

```
Console#show ip interface
 IP address and netmask: 192.168.1.54 255.255.255.0 on VLAN 1,
 and address mode:          User specified.
Console#
```

**関連コマンド**

show ip redirects (p.465)

### show ip redirects

本製品用に設定されているデフォルトのゲートウェイを表示します。

**デフォルト設定**

なし

**コマンドモード**

Privileged Exec

**例**

```
Console#show ip redirects
IP default gateway 10.1.0.254
Console#
```

**関連コマンド**

ip default-gateway (p.463)

**ping**

ネットワーク上の別のノードにICMPエコー要求パケットを送信します。

**構文**

**ping** *ホスト* [**size** *サイズ*] [**count** *カウント*]

- *ホスト* - ホストのIPアドレスまたはIPエイリアス
- *サイズ* - パケットのバイト数（範囲：32～512、デフォルト：32）。
  ヘッダ情報が追加されるため、実際のパケットサイズは指定したサイズより8バイト大きくなります。
- *カウント* - 送信するパケット数（範囲：1～16、デフォルト：5）

**デフォルト設定**

このコマンドにはホストのデフォルト設定なし

**コマンドモード**

Normal Exec、Privileged Exec

**コマンドの使用方法**

- pingコマンドを使用すると、ネットワーク上の別のサイトにアクセスできるかどうか確認できます。
- **ping**コマンドには以下のような結果があります。
  - *通常の応答* - ネットワークトラフィックの状態によって、通常の応答は1～10秒以内に発生
  - *相手先応答なし* - ホストが応答しない場合、10秒以内に「timeout」を表示
  - *相手先到達不能* - 相手先のホストのゲートウェイが、相手先に到達不能であることを表示
  - *ネットワークまたはホストに到達不能* - ルートテーブルに対応するエントリなし
- pingを停止するにはEscキーを押します。

**例**

```
Console#ping 10.1.0.9
Type ESC to abort.
PING to 10.1.0.9, by 5 32-byte payload ICMP packets, timeout is 5 seconds
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 10 ms
Ping statistics for 10.1.0.9:
  5 packets transmitted, 5 packets received (100%), 0 packets lost (0%)
Approximate round trip times:
  Minimum = 10 ms, Maximum = 20 ms, Average = 10 ms
Console#
```

**関連コマンド**

interface (p.365)

# 付録A: ソフトウェアの仕様

## ソフトウェアの機能

### 対応規格

IEEE802.3:10BASE-T
IEEE802.3u:100BASE-TX
IEEE802.3ab:1000BASE-T
IEEE802.3z:1000BASE-SX/LX
IEEE802.3x:フローコントロール
IEEE802.1Q:TagVLAN
IEEE802.1p:QoS
IEEE802.1d:STP
IEEE802.1w:Rapid Spanning Tree
IEEE802.1ad:LACP
IEEE802.1X:ユーザー認証

### ポート構成

RJ-45コネクタ×24:10BASE-T、100BASE-TX
RJ-45コネクタ×4:10BASE-T、100BASE-TX、1000BASE-T
(オートネゴシエーション、Auto-MDI/MDI-X対応)
拡張スロット(MiniGBIC用)×2

### スイッチング方式

ストア&フォワード

### パケットバッファ

512KB

### スイッチングファブリック

12.8Gbps

### MACアドレス記録数

8,000個(全ポート合計)

### スループット(64Byte)

10BASE-T：各ポート14881パケット/秒
100BASE-TX：各ポート148810パケット/秒
1000BASE-TX/SX/LX：各ポート1488095パケット/秒

フローコントロール
全二重：IEEE802.3x、半二重：バックプレッシャー

ジャンボフレーム
最大フレームサイズ：9212Bytes without CRC

VLAN
TagVLAN、PrivateVLAN
TagVLAN PVID範囲：1～4094
最大VLANグループ数：255 （IP設定可能VLAN数 1）

Trunk
最大8ポート、4グループ

QoS
4レベル
対応アルゴリズム：Strict、WRR
対応QoS方式：CoS、ToS、DiffServ

スパニングツリー
STP/MSTP

SNMP
v1/v2c
Trap v1/v2
MIB II / Interface MIB /Ether-Link MIB/Bridge MIB
Extended Bridge MIB/ Entity MIB/ RADIUS MIB/PrivateMIB

RMON
Statistics/History/Alarm/Event (1、2、3、9グループ)

ポートミラーリング
Tx、Rx

**マルチキャスト**
IGMP snooping(v1/v2)

**アクセスリスト機能**
L4(TCP、UDP、etc) 、L3(IP)、L2(MAC)
最大ACL数:88

**その他機能**
DHCP Client、NTP、RateLimit、Syslog

**ハードウェア仕様**

**LED**
Power、Diag、RPS、Stack Master、Link/ACT

**冷却ファン**
搭載

**MTBF**
81000時間

**電源**
AC100V 50/60Hz

**消費電力**
最大35W

**外形寸法**
440(W)×44(H)×230(D)mm

**重量**
2.8kg

**動作時環境**
温度:0～40℃
湿度:35～85%(結露なきこと)

**保存時環境**
温度:-40～70℃
湿度:5～95%(結露なきこと)

**取得承認規格**
CE、FCC Class A、VCCI Class A

**その他**
対応OS

**各種設定方法**
Telnet、SSH、WEBブラウザ、HTTPS、コンソール

**保証期間**
3年間(電源、ファンは1年間)

**■注意事項**
・拡張スロットはRJ-45ポート(10BASE-T、100BASE-TX、1000BASE-T)との排他利用になります。
・RJ-45ポート(10BASE-T、100BASE-TX、1000BASE-T)中の2ポートはスタック接続時にはスタック専用ポートとなり、通常の通信に利用することが出来なくなります。
・IEEE802.1XはEAP-MD5のみ対応しています。

# 付録B: トラブルシューティング

## 管理インタフェースへのアクセスに関する問題

表 B-1　トラブルシューティングチャート

| 現象 | 対応 |
| --- | --- |
| Telnet、WEBブラウザ、SNMPソフトウェアを使用して接続できない | ・本製品の電源が入っていることを確認します。<br>・管理ステーションと本製品を接続するネットワークケーブルを確認します。<br>・本製品へのネットワーク接続が有効であることと、使用しているポートが無効になっていないことを確認します。<br>・管理ステーションの接続に使用しているVLANインタフェースを、有効なIPアドレス、サブネットマスクおよびデフォルトのゲートウェイで設定していることを確認します。<br>・管理ステーションが接続されている本製品のIPインタフェースと同じサブネットに、その管理ステーションのIPアドレスがあることを確認します。<br>・タグ付きVLANグループのIPアドレスを使用して本製品に接続しようとしている場合は、管理ステーションと、ネットワーク内の中間スイッチを接続しているポートを、適切なタグを使用して設定する必要があります。<br>・Telnetを使用して接続できない場合は、Telnet/SSHの同時セッション数が最大許容数を超えているおそれがあります。 しばらくしてから再度接続を試みてください。 |
| セキュアシェルを使用して接続できない | ・SSHを使用して接続できない場合は、Telnet/SSHの同時セッション数が最大許容数を超えているおそれがあります。 しばらくしてから再度接続を試みてください。<br>・本製品でSSHサーバの制御パラメータが適切に設定されていることと、管理ステーションでSSHクライアントソフトウェアが適切に設定されていることを確認します。<br>・本製品でパブリックキーを生成し、このキーをSSHクライアントにエクスポート済みであることを確認します。<br>・本製品で、各SSHユーザのアカウント(ユーザ名、認証レベル、パスワードを含む)を設定済みであることを確認します。<br>・クライアントのパブリックキーを本製品にインポート済みであることを確認します(パブリックキー認証を使用している場合)。 |

| | |
|---|---|
| シリアルポート接続経由でオンボード設定プログラムにアクセスできない | ・端末エミュレータプログラムをVT100互換、8データビット、1ストップビット、パリティなし、9600bpsに設定済みであることを確認します。<br>・ヌルモデムシリアルケーブルが、『インストレーションガイド』に記載されているピンアウト接続に準拠していることを確認します。 |
| パスワードを忘れた、または紛失した | ・サポートセンターにお問い合わせください。 |

# システムログの使用

障害が実際に発生した場合は、『インストレーションガイド』を参照して、問題の発生原因が本製品自体にあるかどうかを確認してください。 本製品が原因と思われる場合は、以下の手順に従ってください。

1. ロギングを有効にします。
2. 報告されるエラーメッセージを、すべてのカテゴリに含めるように設定します。
3. エラーメッセージを受信するSNMPホストを指定します。
4. エラーの原因となる一連のコマンドまたはその他の処理を繰り返します。
5. 障害の原因となったコマンドまたは状況のリストを作成します。 また、表示されるエラーメッセージのリストも作成します。
6. サポートセンターに連絡します。

以下に例を示します。

```
Console(config)#logging on
Console(config)#logging history flash 7
Console(config)#snmp-server host 192.168.1.23
.
.
.
```

# 用語集

**アクセス制御リスト**(ACL)
各パケットで一定のIPまたはMAC（レイヤ2)の情報をチェックすることにより、ネットワークトラフィック、および一定のユーザまたは機器へのアクセスを制限することができます。

**ブートプロトコル**(BOOTP)
ネットワーク機器の起動情報を提供するために使用します。

この情報には、IPアドレス情報、機器のシステムファイルを含むTFTPサーバのアドレス、ブートファイルの名前などが含まれます。

**クラスオブサービス**(CoS)
必要なサービスレベルに基づいてパケットに優先順位を付け、適切な出力キューに配置することによってサポートされています。データはウェイトラウンドロビンサービスを使用してキューから送信され、優先度サービスを実施するとともに、低いレベルのキューがブロックされるのを防ぎます。 優先度は、ポートのデフォルト、パケットの優先度ビット(VLANタグ内)、TCP/UDPポート番号、IP優先度ビット、DSCP優先度ビットのいずれかに従って設定できます。

**差別サービスコードポイントサービス**(DSCP)
6ビットタグを使用して、最大64種類の異なる転送動作に対応します。

ネットワークポリシーに基づいて、様々な種類の転送を行うように、様々な種類のトラフィックをマークすることができます。 DSCPビットはCoSのカテゴリにマッピングされ、その後出力キューにマッピングされます。

**ドメインネームサービス**(DNS)
ネットワークノードのホスト名をIPアドレスに変換するシステム。

**Dynamic Host Control Protocol** (DHCP)
設定情報をTCP/IPネットワーク上のホストに渡すためのフレームワークを提供します。 DHCPは、Bootstrap Protocol (BOOTP)に基づいて、再利用可能なネットワークアドレスの自動割り当て機能およびその他の設定オプションを追加したものです。

**Extensible Authentication Protocol over LAN** (EAPOL)
本製品にプラグインされている機器のネットワークアクセス権を検証するクライア

ント認証プロトコル。 本製品からユーザ名とパスワードが要求されると、検証のために認証サーバ(RADIUSなど)に渡されます。 EAPOLは、IEEE 802.1Xポート認証規格の一環として実装されています。

### GARP VLAN Registration Protocol (GVRP)

スパニングツリーの各ポートで必要なVLANメンバを登録するための、スイッチ間でのVLAN情報の交換方法を定義して、各スイッチで定義されているVLANがスパニングツリーネットワークで自動的に機能するようにします。

### Generic Attribute Registration Protocol (GARP)

末端ステーションおよびスイッチでスイッチ環境のマルチキャストグループメンバシップ情報を登録および伝播し、登録済みの末端ステーションを含むスイッチLANのポートのみにマルチキャストデータフレームが伝播されるようにするプロトコル。

旧称はGroup Address Registration Protocolです。

### Generic Multicast Registration Protocol (GMRP)

GMRPを使用すると、ネットワーク機器が末端ステーションをマルチキャストグループに登録することができます。 GMRPを使用するには、使用するネットワーク機器や末端ステーションがIEEE 802.1p規格に準拠している必要があります。

### Group Attribute Registration Protocol (GARP)

*「Generic Attribute Registration Protocol」を参照してください。*

### IEEE 802.1D

スパニングツリープロトコルを含む、MACブリッジの一般的な操作方法を指定します。

### IEEE 802.1Q

VLANタギングは、VLAN情報を含むイーサネットフレームタグを定義します。

これを使用すると、本製品で末端ステーションを別の仮想LANに割り当て、スイッチネットワークでのVLANの標準的な通信方法を定義できます。

### IEEE 802.1p

イーサネットネットワークでサービスの質(QoS)を提供するIEEE規格。

この規格では最大8種類のトラフィッククラスを定義するパケットタグが使用され、本製品はタグ付けされた優先度値に基づいてパケットを送信できます。

### IEEE 802.1X

ユーザに対して最初にユーザIDとパスワードを要求することにより、ポート認証がスイッチポートへのアクセスを制御します。

### IEEE 802.3ac

VLANタギングのフレーム拡張を定義します。

### IEEE 802.3x

全二重リンクでフローコントロールに使用するイーサネットフレームの開始/停止要求およびタイマを定義します (現在はIEEE 802.3-2002に含まれます)。

### Internet Group Management Protocol (IGMP)

このプロトコルを使用すると、ホストをマルチキャストサービス用にローカルルータに登録することができます。与えられたサブネットワークにマルチキャストスイッチまたはルータが複数ある場合は、1つの機器が「クエリア」となり、グループメンバシップを追跡する役割を持ちます。

### IGMPクエリ

各サブネットワークでは、1台のIGMP対応機器がクエリアの役割を果たします。

クエリアとは、全ホストに対して、参加を希望する、またはすでに所属しているIPマルチキャストグループに関する報告を依頼する機器です。選択されたクエリアは、サブネットワーク内でIPアドレスの値が最も小さい機器になります。

### IGMPスヌーピング

IPマルチキャストルータとIPマルチキャストホストグループの間で転送されるIGMPクエリおよびIGMPレポートのパケットを確認し、IPマルチキャストグループのメンバを識別します。

### 帯域内管理

ネットワークに直接接続されているステーションからのネットワーク管理。

### IPマルチキャストフィルタリング

参加しているホストに対して本製品がマルチキャストトラフィックを渡すことのできるプロセス。

### IP優先度

IPv4ヘッダのサービスのタイプ(ToS)を示すオクテットには、ネットワーク制御パケット用の最も高い優先度からルーチントラフィック用の最も低い優先度まで、8つの異なる優先度レベルを定義する3ビットが含まれます。 8つの値は、デフォルトではClass of Serviceのカテゴリに1対1でマッピングされますが、特定のネットワークアプリケーションの要件に合わせて別の設定も可能です。

### レイヤ2

ISO 7-Layer Data Communications Protocolのデータリンクレイヤ。

これはネットワーク機器のハードウェアインタフェースに直接関係しており、MACアドレスに基づいてトラフィックを渡します。

### リンクアグリゲーション

*「ポートトランク」を参照してください。*

### Link Aggregation Control Protocol (LACP)

各ポートで、別の機器のLACP設定ポートとのトランクリンクを自動的にネゴシエーションできます。

### 管理情報ベース(MIB)

Management Information Baseの頭字語。

特定の機器に関する情報を含む、一連のデータベースオブジェクトです。

### MD5メッセージダイジェストアルゴリズム

デジタル署名の作成に使用するアルゴリズム。32ビットマシンでの使用を想定しており、破損しているMD4アルゴリズムより安全です。 MD5は一方向のハッシュ関数です。つまり、任意のメッセージを数字の固定文字列(メッセージダイジェストともいう)に変換します。

### マルチキャストスイッチング

着信マルチキャストフレームを、登録済みの接続ホストがないサービス用にフィルタリングするか、または指定したマルチキャストVLANグループに含まれるすべてのポートに転送するプロセス。

### Network Time Protocol (NTP)

ネットワーク全体で時間を同期化するメカニズムを提供します。

時間確認用サーバは、マスタ/スレーブ階層設定で動作し、有線または無線でサブネット内のローカルクロックと国の標準時間を同期化します。

### 帯域外管理

ネットワークに接続されていないステーションからのネットワーク管理。

### ポート認証

*「IEEE 802.1X」を参照してください。*

### ポートミラーリング

ロジックアナライザまたはRMONプローブを使用したトラブルシューティングのために、ターゲットポート上のデータをモニタポートにミラーリングする方法。 これにより、ターゲットポート上のデータを妨害されることなく調査できます。

### ポートトランク

複数の低速物理リンクを組み合わせて1つの高速論理リンクを作成する方法を指定する、ネットワークリンクアグリゲーションおよびトランキングの方法を定義します。

### プライベートVLAN

割り当てられているVLAN内でポートベースのセキュリティを提供します。

また、ポート間の隔離も可能です。 ダウンリンクポートのデータトラフィックは、アップリンクポートとの間でのみ転送できます。

### Remote Authentication Dial-in User Service (RADIUS)

中央のサーバで実行しているソフトウェアを使用してネットワーク上のRADIUS準拠の機器へのアクセスを制御するログオン認証プロトコル。

### リモート監視(RMON)

包括的なネットワーク監視機能を提供します。

標準のSNMPで必要なポーリングが不要になり、特定のエラータイプなど、様々なトラフィック条件に基づいてアラームを設定できます。

### ラピッドスパニングツリープロトコル(RSTP)

ネットワークトポロジ変更の収束時間を、古いIEEE 802.1D STP規格に比べて約10%短縮します。

### セキュアシェル(SSH)

Telnetなどのリモートアクセス機能の代わりに使用できる、セキュリティが強化された機能。 SSHでは、暗号キーでユーザを認証できるほか、管理クライアントと本製品の間のデータ接続を暗号化できます。

### Simple Network Management Protocol (SNMP)

一連のインターネットプロトコルの中のアプリケーションプロトコル。

ネットワーク管理サービスを提供します。

### Simple Network Time Protocol (SNTP)

SNTPを使用すると、Network Time Protocol (NTP)サーバからの定期的な更新に基づいて、機器の内部クロックを設定できます。 更新は、特定のNTPサーバから要求するか、またはNTPサーバによって送信されるブロードキャスト経由で受信できます。

### スパニングツリーアルゴリズム(STA)

ネットワークでループの有無をチェックするテクノロジ。

ループは、複雑な、またはバックアップリンクされたネットワークシステムで多く発生します。スパニングツリーは使用可能な最短のパスに沿ってデータを検出および送信し、ネットワークのパフォーマンスおよび効率を最大化します。

### Telnet

TCP/IP経由で端末機器にインタフェースするためのリモート通信設備を定義します。

### Terminal Access Controller Access Control System Plus (TACACS+)

中央のサーバで実行しているソフトウェアを使用して、ネットワーク上のTACACS準拠の機器へのアクセスを制御するログオン認証プロトコル。

### Transmission Control Protocol/Internet Protocol (TCP/IP)

TCPをプライマリトランスポートプロトコル、IPをネットワークレイヤプロトコルとするプロトコルスイート。

**Trivial File Transfer Protocol** (TFTP)
ソフトウェアのダウンロードに一般的に使用されるTCP/IPプロトコル。

**User Datagram Protocol** (UDP)
UDPでは、パケットスイッチ通信でデータグラムモードを使用できます。

IPを基礎のトランスポートメカニズムとして使用し、IPのようなサービスへのアクセスを提供します。 UDPパケットは、IPパケット、つまり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同様に配信されます。UDPは、TCPが複雑すぎる場合や遅すぎる場合、また単に不要な場合に便利です。

**仮想LAN** (VLAN)
物理的な場所やネットワーク内の接続ポイントにかかわらず、同じコリジョンドメインを共有するネットワークノードの集まり。 VLANは物理的障壁のない論理的ワークグループとして機能し、ユーザは情報やリソースを同じLAN内にあるかのように共有できます。

**XModem**
機器間でのファイル転送に使用するプロトコル。

データは128バイトブロックでグループ化され、エラーは修正されます。

# ユーザ登録について

このたびは弊社製品をお買い上げいただき誠にありがとうございます。弊社では、製品をお買い上げいただいたお客様にユーザ登録をお願いしております。
ユーザ登録を行っていただいたお客様には新製品情報、バージョンアップ情報、キャンペーン情報等さまざまな情報を提供させていただきます。また、製品の故障等でユーザサポートをお受けになるにはお客様のユーザ登録が必要となります。ユーザ登録の際は、ホームページ掲載の「個人情報保護方針について」をご確認後、ユーザ登録を行ってくださいますようお願いいたします。
ユーザ登録は下記弊社ホームページ上で受け付けております。

http://www.planex.co.jp/user/

# 弊社へのお問い合わせ

■　弊社製品の追加購入

弊社製品のご購入は、販売店または PLANEX DIRECT まで。
ケーブル 1 本からレイヤスイッチまで、お客様が探しているものが見つかります。

<PLANEX DIRECT>
http://direct.planex.co.jp/

■　製品に関するお問い合わせ

製品購入前のご相談や、ご質問は弊社専任アドバイザーにお任せください。
ネットワーク導入やシステム構築・拡張など、お客様のお手伝いをいたします。

<ご質問/お見積もりフォーム>
http://www.planex.co.jp/lan.shtml

■　技術的なお問い合わせ・修理に関するお問い合わせ

製品購入後のご質問は、弊社サポートセンタまでお問い合わせください。
豊富な知識をもったサポート技術者が、お客様の問題を解決いたします。

<お問い合わせフォーム>
http://www.planex.co.jp/support/techform
<電話>
フリーダイヤル：0120-415-977
受付：月～金曜日、10～12 時、13～17 時
＊　祝祭日および弊社指定の休業日を除く
<FAX>
ファクス番号：03-5766-1615
受付：24 時間

◇　お問い合わせ前のお願い

サポートを円滑に行うため、お問い合わせ前に以下のものをご用意ください。
お客様のご協力お願いいたします。

- 弊社製品の製品型番とシリアルナンバー
- ご利用のコンピュータの型番とオペレーティングシステム名（Windows XP/Me など）
- ご利用のネットワーク環境（回線の種類やインターネットサービスプロバイダ名など）
- ご質問内容（現在の状態、症状など。エラーメッセージが表示されている場合はその詳細を書きとめてください）

■　その他

その他のお問い合わせ先は、弊社ホームページからお確かめください。

プラネックスコミュニケーションズ
http://www.planex.co.jp

# 質問表

技術的なご質問は、この 2 ページをコピーして必要事項をご記入の上、下記 FAX 番号へお送りください。

プラネックスコミュニケーションズテクニカルサポート担当　行

**FAX：03-5766-1615**

送信日：＿＿＿＿＿＿＿＿

| | | | |
|---|---|---|---|
| 会社名 | | | |
| 部署名 | | | |
| 名前 | | | |
| 電話 | | FAX | |
| E-MAIL | | | |

| | |
|---|---|
| 製品名<br>Product name | 24 ポートスタッカブルスイッチ |
| 型番<br>Product No. | SF-0224FS |
| 製造番号<br>Serial No | |

**① ご使用のコンピュータについて**

| | |
|---|---|
| メーカー | |
| 型番 | |

**② OS**

| | |
|---|---|
| OS | バージョン |

③ 質問内容