Future X Communications

FXC3126A Management Guide

2010年6月 Ver.2.1

FXC株式会社

本マニュアルについて

- 本マニュアルでは、FXC3126A の各種設定およびシステムの監視手順について説明します。本製品の設定および監視は、RS-232C シリアルポートまたは、イーサネットポートに設定、監視用の端末接続して、CLI （コマンドラインインタフェース）または Web ブラウザで行います。
- 本マニュアルに記載している機能は、ファームウェアバージョン 1.1.0.27 以降の製品に対応しています。

製品取り扱い時のご注意

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

・下記事項は、安全のために必ずお守りください。

● 安全のための注意事項を守る

注意事項をよくお読みください。製品全般の注意事項が記載されています。

● 故障したら使わない

すぐに販売店まで修理をご依頼ください。

● 万一異常が起きたら

・煙が出たら
・異常な音、においがしたら
・内部に水・異物が入ったら
・製品を高所から落としたり、破損したとき

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

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

● 電源ケーブルや接続ケーブルを傷つけない

・電源ケーブルを傷つけると火災や感電の原因となります。
・重いものをのせたり、引っ張ったりしない。
・加工したり、傷つけたりしない。
・熱器具の近くに配線したり、加熱したりしない。
・電源ケーブルを抜くときは、必ずプラグを持って抜く。

● 内部に水や異物を入れない

・火災や感電の原因となります。
・万一、水や異物が入ったときは、すぐに電源を切り（電源ケーブルを抜き）、販売店に点検・修理をご依頼ください。

● 内部をむやみに開けない

本体及び付属の機器（ケーブル含む）をむやみに開けたり改造したりすると、火災や感電の原因となります。

● 落雷が発生したらさわらない

感電の原因となります。また、落雷の恐れがあるときは、電源ケーブルや接続ケーブルを事前に抜いてください。本機が破壊される原因となります。

● 油煙、湯気、湿気、ほこりの多い場所には設置しない

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

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

● ぬれた手で電源プラグやコネクタに触らない

感電の原因となります。

● 指定された電源コードや接続ケーブルを使う

マニュアルに記載されている電源ケーブルや接続ケーブルを使わないと、火災や感電の原因となります。

● 指定の電圧で使う

マニュアルに記されている電圧の範囲で使わないと、火災や感電の原因となります。

● コンセントや配線器具の定格を超えるような接続はしない

発熱による火災の原因となります。

● 通風孔をふさがない

・通風孔をふさいでしまうと、内部に熱がこもり、火災や故障の原因となります。また、風通しをよくするために次の事項をお守りください。

・毛足の長いジュウタンなどの上に直接設置しない。

・布などでくるまない。

● 移動させるときは、電源ケーブルや接続ケーブルを抜く

接続したまま移動させると、電源ケーブルが傷つき、火災や感電の原因となります。

目次

目次

1. イントロダクション

1.1 主な機能

本機はレイヤ 2 **スイッチとして豊富な機能を搭載しています。**

本機は管理エージェントを搭載し、各種設定を行うことができます。
ネットワーク環境に応じた適切な設定を行うことや、各種機能を有効に設定することで、機能を最大限に活用できます。

機能	**解説**
Configuration Backup and Restore	TFTP **サーバによるバックアップ可能**
Authentication	Console, Telnet, web －**ユーザ名** / **パスワード** , RADIUS,TACACS+ Web － HTTPS Telnet － SSH SNMPv1/2c －**コミュニティ名** SNMPv3 － MD5 、SHA **パスワード** Port － IEEE802.1x **認証**、MAC **アドレスフィルタリング**
Access Control Lists	**最大** 32 **の** IP ACL、MAC **ルールをサポート**
DHCP Client	**サポート**
DHCP Snooping	**サポート**（Option 82 relay **情報**）
Port Configuration	**スピード、通信方式、フローコントロール**
Rate Limiting	**ポートごとの入力・出力帯域制御**
Port Mirroring	1 **つの分析ポートに対する、１つまたは複数ポートのミラーリング**
Port Trunking	Static **及び** LACP **による最大** 12 **トランク**
Broadcast Storm Control	**サポート**
Static Address	**最大登録可能** MAC **アドレス数**　8k
IEEE802.1D Bridge	**動的スイッチング及び** MAC **アドレス学習**
Store-and-Forward Switching	**ワイヤスピードスイッチング**
Spanning Tree Protocol	STP、Rapid STP（RSTP）、Multiple STP (MSTP)
Virtual LANs	IEEE802.1Q **タグ付** VLAN/ **ポートベース** VLAN/ **プロトコルベース** VLAN/ **プライベート** VLAN（**最大** 255 **グループ**）
Traffic Prioritization	**ポートプライオリティ、トラフィッククラスマッピング、キュースケジューリング、**DSCP、IP Precedence,、IP TOS、TCP/UDP **ポート**
Quality of Service	DiffServ **サポート**
Multicast Filtering	IGMP Snooping、Query、MVR
Switch Clustering	**最大** 36 **スイッチ**

1.2 ソフトウェア機能

本機はレイヤ 2 イーサネットスイッチとして多くの機能を有し、それにより、効果的なネットワークの運用を実現します。

ここでは、本機の主要機能を紹介します。

設定のバックアップ及び復元

TFTP サーバを利用して現在の設定情報を保存することができます。
また、保存した設定情報を本機に復元することも可能です。

認証 /Authentication

本機はコンソール、Telnet、Web ブラウザ経由の管理アクセスに対する本機内又はリモート認証サーバ (RADIUS/TACACS+) によるユーザ名とパスワードベースでの認証を行います。また、Web ブラウザ経由では HTTPS を、Telnet 経由では SSH を利用した認証オプションも提供しています。

SNMP、Telnet、Web ブラウザでの管理アクセスに対しては IP アドレスフィルタリング機能も有しています。

各ポートに対しては IEEE802.1x 準拠のポートベース認証をサポートしています。本機能では、EAPOL(Extensible Authentication Protocol over LANs) を利用し、IEEE802.1x クライアントに対してユーザ名とパスワードを要求します。その後、認証サーバにおいてクライアントのネットワークへのアクセス権を確認します。

その他に、HTTPS によるセキュアなマネージメントアクセスや、Telnet アクセスを安全に行う SSH もサポートしています。また、各ポートへのアクセスには MAC アドレスフィルタリング機能も搭載しています。

ACL/Access Control Lists

ACL では IP アドレス、プロトコル、TCP/UDP ポート番号による IP フレームのフィルタリングもしくは、MAC アドレス、イーサネットタイプによるフレームのフィルタリングを提供します。ACL を使用することで、不要なネットワークトラフィックを抑制し、パフォーマンスを向上させることができます。

また、ネットワークリソースやプロトコルによるアクセスの制限を行うことでセキュリティのコントロールが行えます。

ポート設定 /Port Configuration

本機ではオートネゴシエーション機能により対向機器に応じて各ポートの設定を自動的に行える他、手動で各ポートの通信速度、通信方式及びフローコントロールの設定を行うことができます。

通信方式を Full-Duplex にすることによりスイッチ間の通信速度を 2 倍にすることができます。IEEE802.3x に準拠したフローコントロール機能では通信のコントロールを行い、パケットバッファを越えるパケットの損失を防ぎます。

帯域制御 /Rate Limiting

各インタフェースにおいて、受信トラフィックの最大帯域の設定を行うことができます。設定範囲内のパケットは転送されますが、設定した値を超えたパケットは転送されずにパケットが落とされます。

ポートミラーリング /Port Mirroring

本機は任意のポートからモニターポートに対して通信のミラーリングを行うことができます。ターゲットポートにネットワーク解析装置（Sniffer 等）又は RMON プローブを接続し、トラフィックを解析することができます。

ポートトランク /Port Trunking

複数のポートをバンド幅の拡大によるボトルネックの解消や、障害時の冗長化を行うことができます。本機で手動及び IEEE802.3ad 準拠の LACP を使用した動的設定で行うことができます。

本機では最大 12 グループのトランクをサポートしています。

ブロードキャストストームコントロール /Broadcast Storm Control

ブロードキャストストームコントロール機能は、ブロードキャスト通信によりネットワークの帯域が占有されることを防ぎます。ポート上で本機能を有効にした場合、ポートを通過するブロードキャストパケットを制限することができます。ブロードキャストパケットが設定しているしきい値を超えた場合、しきい値以下となるよう制限を行います。

静的アドレス /Static Addresses

特定のポートに対して静的な MAC アドレスの設定を行うことができます。設定された MAC アドレスはポートに対して固定され、他のポートに移動することはできません。設定された MAC アドレスの機器が他のポートに接続された場合、MAC アドレスは無視され、アドレステーブル上に学習されません。

静的 MAC アドレスの設定を行うことにより、指定のポートに接続される機器を制限し、ネットワークのセキュリティを提供します。

IEEE802.1D ブリッジ /IEEE 802.1D Bridge

本機では IEEE802.1D ブリッジ機能をサポートします。

MAC アドレステーブル上で MAC アドレスの学習を行い、その情報に基づきパケットの転送を行います。本機では最大 8K 個の MAC アドレスの登録を行うことが可能です。

ストア & フォワード スイッチング /Store-and Forward Switching

本機ではスイッチング方式としてストア＆フォワードをサポートします。

本機では 2Mbit のバッファを有し、フレームをバッファにコピーをした後、他のポートに対して転送します。これによりフレームがイーサネット規格に準拠しているかを確認し、規格外のフレームによる帯域の占有を回避します。また、バッファにより通信が集中した場合のパケットのキューイングも行います。

スパニングツリープロトコル /Spanning Tree Protocol

本機は 3 種類のスパニングツリープロトコルをサポートしています。

Spanning Tree Protocol (STP, IEEE 802.1D) ―

本機能では、LAN 上の通信に対して複数の通信経路を確保することにより冗長化を行うことができます。

複数の通信経路を設定した場合、1 つの通信経路のみを有効とし、他の通信経路はネットワークのループを防ぐため無効にします。但し、使用している通信経路が何らかの理由によりダウンした場合には、他の無効とされている通信経路を有効にして通信を継続して行うことを可能とします。

Rapid Spanning Tree Protocol (RSTP, IEEE 802.1w) ―

既存の IEEE802.1D 準拠の STP に比べ約 10 分の 1 の時間でネットワークの再構築を行うことができます。

RSTP は STP の完全な後継とされていますが、既存の STP のみをサポートしている製品と接続され STP に準拠したメッセージを受信した場合には、STP 互換モードとして動作することができます。

Multiple Spanning Tree Protocol (MSTP, IEEE 802.1s) ―

本機能は RSTP の拡張機能です。本機能により各 VLAN 単位での STP 機能を提供することが可能となります。VLAN 単位にすることにより、各 VLAN 単位でネットワークの冗長化を行えるほか、ネットワーク構成が単純化され RSTP よりさらに早いネットワークの再構築を行うことが可能となります。

VLAN/Virtual LANs

本機は最大 255 グループの VLAN をサポートしています。VLAN は物理的な接続に関わらず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となります。

本機では IEEE802.1Q 準拠のタグ付 VLAN をサポートしています。VLAN グループメンバーは GVRP を利用した動的な設定及び手動での VLAN 設定を行うことができます。VLAN の設定を行うことにより指定した通信の制限を行うことができます。

VLAN によりセグメントを分ける事で以下のようなメリットがあります。

- 細かいネットワークセグメントにすることによりブロードキャストストームによるパフォーマンスの悪化を回避します。
- 物理的なネットワーク構成に関わりなく、VLAN の設定を変更することでネットワークの構成を簡単に変更することが可能です。
- 通信を VLAN 内に制限することでセキュリティが向上します。
- プライベート VLAN を利用することにより設定可能な VLAN 数に制限がある中で、同一 VLAN 内の各ポート間の通信を制限し、アップリンクポートとの通信のみを行うことが可能となります。
- プロトコルベース VLAN により、プロトコルタイプに基づいたトラフィックの制限を行うことが可能です。

プライオリティ /Traffic Prioritization

本機では 4 段階のキューと Strict 又は WRR キューイング機能によりサービスレベルに応じた各パケットに優先順位を設定することができます。これらは、入力されるデータの IEEE802.1p 及び 802.1Q タグにより優先順位付けが行われます。

本機能により、アプリケーション毎に要求される優先度を個別に設定することができます。

また、本機では IP フレーム上の ToS オクテット内のプライオリティビットを利用した優先順位の設定など、いくつかの方法により L3/L4 レベルでの優先順位の設定も行うことができます。

マルチキャストフィルタリング /Multicast Filtering

正常なネットワークの通信に影響させず、リアルタイムでの通信を確保するために、VLAN のプライオリティレベルを設定し、マルチキャスト通信を特定し各 VLAN に対して割り当てることができます。

本機では IGMP Snooping 及び Query を利用し、マルチキャストグループの登録を管理します。

また、本機は Multicast VLAN Registration (MVR) もサポートしています。

2. 本機の管理

2.1 本機への接続

2.1.1 設定方法

FXC3126A は、ネットワーク管理エージェントを搭載し SNMP、RMON、及び Web インタフェースによるネットワーク経由での管理を行うことができます。また、PC から本機に直接接続しコマンドラインインタフェース (Command Line Interface/CLI) を利用した設定及び監視を行うことも可能です。

[注意]　初期設定状態では、DHCP サーバーよる IP アドレスの取得を行うよう設定されています。この設定の変更を行うには 2.2.3 項「IP アドレスの設定」を参照して下さい。

本機には管理用の Web サーバが搭載されています。Web ブラウザから設定を行ったり、ネットワークの状態を監視するための統計情報を確認したりすることができます。
ネットワークに接続された PC 上で動作する、Internet Explorer 5.0 以上から、Web インタフェースにアクセスすることができます。

本機の CLI へは本体のコンソールポートへの接続及びネットワーク経由での Telnet による接続によりアクセスすることができます。

本機には SNMP (Simple Network Management Protocol) に対応した管理エージェントが搭載されています。ネットワークに接続されたシステムで動作する、SNMP に対応した管理ソフトから、本機の SNMP エージェントにアクセスし設定などを行うことが可能です。

本機の CLI、Web インタフェース及び SNMP エージェントからは以下の設定を行うことが可能です。

- ユーザ名、パスワードの設定
- 管理 VLAN の IP インタフェースの設定
- SNMP パラメータの設定
- 各ポートの有効 / 無効
- 各ポートの通信速度及び Full/Half Duplex の設定
- 帯域制御による各ポートの入力及び出力帯域の設定
- IEEE802.1Q 準拠のタグ付 VLAN (最大 255 グループ)
- GVRP 有効
- IGMP マルチキャストフィルタリング設定
- TFTP 経由のファームウェアのアップロード及びダウンロード
- TFTP 経由の設定情報のアップロード及びダウンロード

- スパニングツリーの設定
- Class of Service (CoS) の設定
- 静的トランク及び LACP 設定 (最大 12)
- 各ポートのブロードキャストストームコントロールの設定
- システム情報及び統計情報の表示

2.1.2 接続手順

本機のシリアルポートと PC を RS-232C ケーブルを用いて接続し、本機の設定及び監視を行うことができます。

PC 側では VT100 準拠のターミナルソフトウェアを利用して下さい。PC を接続するための RS-232C ケーブルは、本機に同梱されているケーブルを使用して下さい。

手順 :

（1）RS-232C ケーブルの一方を PC のシリアルポートに接続し、コネクタ部分のねじを外れないように止めます。

（2）RS-232C ケーブルのもう一方を本機のコンソールポートに接続します。

（3）パソコンのターミナルソフトウェアの設定を以下の通り行ってください。

通信ポート ---------- RS-232C ケーブルが接続されているポート
（COM ポート 1 又は COM ポート 2）

通信速度 ---------- 9600 ボー (baud)

データビット -------- 8bit

ストップビット ----- 1bit

パリティ ---------- なし

フロー制御 ---------- なし

エミュレーション -- VT100

（4）上記の手順が正しく完了すると、コンソールログイン画面が表示されます。

[注意] コンソール接続に関する設定の詳細は P229 「Line （ラインコマンド)」を参照して下さい。
CLI の使い方は P219 「コマンドラインインタフェース」を参照して下さい。
また、CLI の全コマンドと各コマンドの使い方は P227 「コマンドグループ」を参照して下さい。

2.1.3 リモート接続

ネットワークを経由して本機にアクセスする場合は、事前にコンソール接続又は DHCP、BOOTP により本機の IP アドレス、サブネットマスク、デフォルトゲートウェイを設定する必要があります。

初期設定では本機は DHCP、BOOTP を用いて自動的に IP アドレスを取得します。手動で IP アドレスの設定を行う場合の設定方法は P10 「IP アドレスの設定」を参照して下さい。

[注意] 本機は同時に最大 4 セッションまでの Telnet 接続が行えます。IP アドレスの設定が完了すると、ネットワーク上のどの PC からも本機にアクセスすることができます。PC 上からは Telnet、Web ブラウザ、ネットワーク管理ソフトを使うことにより本機にアクセスすることができます(対応Webブラウザは Internet Explorer 5.0、又は Netscape Navigator 6.2 以上です)。

[注意] 本機に搭載された管理エージェントでは SNMP 管理機能の設定項目に制限があります。すべての SNMP 管理機能を利用する場合は SNMP に対応したネットワーク管理ソフトウェアを使用して下さい。

2.2 基本設定

2.2.1 コンソール接続

CLI ではゲストモード (normal access level/Normal Exec) と管理者モード (privileged access level/ Privileged Exec) の 2 つの異なるコマンドレベルがあります。ゲストモード (Normal Exec) を利用した場合、利用できる機能は本機の設定情報などの表示と一部の設定のみに制限されます。本機のすべての設定を行うためには管理者モード (Privileged Exec) を利用し CLI にアクセスする必要があります。

2 つの異なるコマンドレベルは、ユーザ名とパスワードによって区別されています。初期設定ではそれぞれに異なるユーザ名とパスワードが設定されています。

管理者モード (Privileged Exec) の初期設定のユーザ名とパスワードを利用した接続方法は以下の通りです。

（1）コンソール接続を初期化し、<Enter> キーを押します。ユーザ認証が開始されます。

（2）ユーザ名入力画面で "admin" と入力します。

（3）パスワード入力画面で "admin" と入力します。
(入力したパスワードは画面に表示されません)

（4）管理者モード (Privileged Exec) でのアクセスが許可され、画面上に "Console#" と表示が行われます。

2.2.2 パスワードの設定

[注意] 安全のため、最初に CLI にログインした際に "username" コマンドを用いて両方のアクセスレベルのパスワードを変更するようにしてください。

パスワードは最大 8 文字の英数字です。大文字と小文字は区別されます。

パスワードの設定方法は以下の通りです。

（1）コンソールにアクセスし、初期設定のユーザ名とパスワード "admin" を入力して管理者モード (Privileged Exec) でログインします。

（2）"configure" と入力し <Enter> キーを押します。

（3）"username guest password 0 password" と入力し、<Enter> キーを押します。Password 部分には新しいパスワードを入力します。

（4）"username admin password 0 password" と入力し、<Enter> キーを押します。Password 部分には新しいパスワードを入力します。

[注意] "0" は平文パスワード、"7" は暗号化されたパスワードを入力します。

```
Username: admin
Password:

      CLI session with the FXC3126A 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)#
```

2.2.3 IP アドレスの設定

本機の管理機能にネットワーク経由でアクセスするためには、IP アドレスを設定する必要があります。

IP アドレスの設定は下記のどちらかの方法で行うことができます。

手動設定

IP アドレスとサブネットマスクを手動で入力し、設定を行います。本機に接続する PC が同じサブネット上にない場合には、デフォルトゲートウェイの設定も行う必要があります。

動的設定

ネットワーク上の BOOTP 又は DHCP サーバに対し、IP アドレスのリクエストを行い自動的に IP アドレスを取得します。

手動設定

IP アドレスを手動で設定します。セグメントの異なる PC から本機にアクセスするためにはデフォルトゲートウェイの設定も必要となります。

[注意] IP アドレスの設定を行う前に、必要な下記の情報をネットワーク管理者から取得して下さい

- **（本機に設定する）IP アドレス**
- **デフォルトゲートウェイ**
- **サブネットマスク**

IP アドレスを設定するための手順は以下の通りです。

（1）interface モードにアクセスするために、管理者モード (Privileged Exec) で "interface vlan 1" と入力し、<Enter> キーを押します。

（2）"ip address ip-address netmask" と入力し、<Enter> キーを押します。
"ip-address" には本機の IP アドレスを、"netmask" にはネットワークのサブネットマスクを入力します。

（3）Global Configuration モードに戻るために、"exit" と入力し、<Enter> キーを押します。

（4）本機の所属するネットワークのデフォルトゲートウェイの IP アドレスを設定するために、"ip default-gateway gateway" と入力し、<Enter> キーを押します。
"gateway" にはデフォルトゲートウェイの IP アドレスを入力します。

```
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)#
```

動的設定

"bootp" 又は "dhcp" を選択した場合、BOOTP 又は DHCP からの応答を受け取るまで IP アドレスは有効になりません。IP アドレスを取得するためには "ip dhcp restart client" コマンドを使用してブロードキャストサービスリクエストを行う必要があります。リクエストは IP アドレスを取得するために周期的に送信されます（BOOTP と DHCP から取得する値には 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 アドレスの取得方法として "bootp" 又は "dhcp" が起動ファイルに設定されている場合、本機は電源投入時に自動的にブロードキャストリクエストを送信します。

"BOOTP" 又は "DHCP" サーバを用いて動的に IP アドレスの取得を行う場合は、下記の手順で設定を行います。

（1）interface configuration モードにアクセスするために、global configuration モードで "interface vlan 1" と入力し <Enter> キーを押します。

（2）interface configuration モードで、下記のコマンドを入力します。

- DHCP で IP アドレスを取得する場合 : "ip address dhcp" と入力し <Enter> キーを押します。
- BOOTP で IP アドレスを取得する場合 : "ip address bootp" と入力し <Enter> キーを押します。

（3）Privileged Exec モードに戻るために、"end" と入力し、<Enter> キーを押します。

（4）ブロードキャストサービスのリクエストを送信するために、"ip dhcp restart " と入力し、<Enter> キーを押します。

（5）数分待った後、IP 設定を確認するために、"show ip interface" と入力し、<Enter> キーを押します。

（6）設定を保存するために、"copy running-config startup-config" と入力し、<Enter> キーを押します。起動ファイル名を入力し、<Enter> キーを押します。

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

\Write to FLASH finish.
Success.
```

2.2.4 SNMP 管理アクセスを有効にする

本機は、SNMP(Simple Network Management Protocol) ソフトウェア経由での管理コマンドによる設定が行えます。

本機では (1)SNMP リクエストへの応答、及び (2)SNMP トラップの生成、が可能です。

SNMP ソフトウェアが本機に対し情報の取得や設定のリクエストを出した場合、本機はリクエストに応じて情報の提供や設定を行います。また、あらかじめ設定することによりリクエストがなくても決められた出来事が発生した場合にトラップ情報を SNMP ソフトウェアに送ることが可能です。

コミュニティ名（Community Strings）

コミュニティ名 (Community Strings) は、本機からトラップ情報を受け取る SNMP ソフトウェアの認証と、SNMP ソフトウェアからのアクセスをコントロールするために使用されます。指定されたユーザもしくはユーザグループにコミュニティ名を設定し、アクセスレベルを決定することができます。

初期設定でのコミュニティ名は以下のとおりです。

- public ― 読み取り専用のアクセスが可能です。public に設定された SNMP 管理ソフトウェアからは MIB オブジェクトの閲覧のみが行えます。
- private ― 読み書き可能なアクセスができます。private に設定された SNMP 管理ソフトウェアからは MIB オブジェクトの閲覧及び変更をすることが可能です。

[注意] SNMP を利用しない場合には、初期設定のコミュニティ名を削除して下さい。コミュニティ名が設定されていない場合には、SNMP 管理アクセス機能は無効となります。

SNMP 経由での不正なアクセスを防ぐため、コミュニティ名は初期設定から変更して下さい。コミュニティ名の変更は以下の手順で行います。

（1）管理者モード (Privileged Exec) の global configuration モードから "snmp-server community string mode" と入力し <Enter> キーを押します。
"string" にはコミュニティ名 "mode" には rw（read/wirte、読み書き可能）、ro（read only、読み取り専用）のいずれかを入力します（初期設定では read only となります）

（2）（初期設定などの）登録済みのコミュニティ名を削除するために、"no snmp-server community string" と入力し <Enter> キーを押します。
"string" には削除するコミュニティ名を入力します。

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

トラップ・レシーバ（Trap Receivers）

本機からのトラップを受ける SNMP ステーション（トラップ・レシーバ）を設定することができます。

トラップ・レシーバの設定は以下の手順で行います

（1）管理者モード (Privileged Exec) の global configuration モードから "snmp-server host host-address community-string" と入力し <Enter> キーを押します。"host-address" にはトラップ・レシーバの IP アドレスを、"community-string" にはホストのコミュニティ名を入力します。

（2）SNMP に情報を送信するためには 1 つ以上のトラップコマンドを設定する必要があります。"snmp-server enable traps type" と入力し、<Enter> キーを押します。"type" には "authentication" か "link-up-down" のどちらかを入力します。

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

2.2.5 設定情報の保存

configuration command を使用しての設定変更は、実行中の設定ファイルが変更されるだけとなります。本機の再起動を行った場合には設定情報が保存されません。

変更した設定を保存するためには "copy" コマンドを使い、実行中の設定ファイルを起動設定ファイルにコピーする必要があります。

設定ファイルの保存は以下の手順で行います :

（1）管理者モード (Privileged Exec) で "copy running-config startup-config" と入力し、<Enter> キーを押します。

（2）起動設定ファイル名前を入力し、<Enter> キーを押します。

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

\Write to FLASH finish.
Success.

Console#
```

2.3 システムファイルの管理

本機のフラッシュメモリ上に CLI、Web インタフェース、SNMP から管理可能な 3 種類のシステムファイルがあります。これらのファイルはファイルのアップロード、ダウンロード、コピー、削除、及び起動ファイルへの設定を行うことができます。

3 種類のファイルは以下の通りです。

- **Configuration(設定ファイル)** ― このファイルはシステムの設定情報が保存されており、設定情報を保存した際に生成されます。保存されたシステム起動ファイルに設定することができる他、サーバに TFTP 経由でアップロードしバックアップを取ることができます。
  "Factory_Default_Config.cfg" というファイルはシステムの初期設定が含まれており、削除することはできません。
  詳細に関しては 28 ページの「設定情報ファイルの保存・復元」を参照して下さい。

- **Operation Code(オペレーションコード)** ― 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。オペレーションコードは本機のオペレーションを行なう他、CLI、Web インタフェースを提供します。
  詳細に関しては 26 ページの「ファームウェアの管理」を参照して下さい。

- **Diagnostic Code(診断コード)** ― POST(パワー・オン・セルフテスト) として知られているソフトウェア (システム・ブートアップ時の実行プログラム)。

本機はオペレーションコードを 2 つまで保存することができます。診断コードと設定ファイルに関しては、フラッシュメモリの容量の範囲内で無制限に保存することができます。

フラッシュメモリでは、各種類のそれぞれ 1 つのファイルが起動ファイルとなります。

システム起動時には診断コードファイルとオペレーションコードファイルが実行されます。その後設定ファイルがロードされます。設定ファイルは、ファイル名を指定してダウンロードされます。

実行中の設定ファイルをダウンロードした場合、本機は再起動されます。実行中の設定ファイルを保存用ファイルに保存しておく必要があります。

3. Web インタフェース

3.1 Web インタフェースへの接続

本機には管理用の Web サーバが搭載されています。Web ブラウザから設定を行ったり、ネットワークの状態を監視するための統計情報を確認したりすることができます。

ネットワークに接続された PC 上で動作する、Internet Explorer 5.0、又は Netscape Navigator 6.2 以上から、Web インタフェースにアクセスすることができます。

[注意] Web インタフェース以外に、ネットワーク経由での Telnet 及びシリアルポート経由のコンソール接続でコマンドラインインタフェース (CLI) を使用し本機の設定を行うことができます。
CLI の使用に関する詳細は 4 章コマンドラインインタフェースを参照して下さい。

[注意] 一部、Web インタフェースでは設定できず、CLI 経由でのみ設定できる項目があります。Web インタフェースで設定できない内容に関しては CLI を利用し、設定を行って下さい。

Web インタフェースを使用する場合は、事前に下記の設定を行って下さい。

（1）コンソール接続、BOOTP 又は DHCP プロトコルを使用して本機に IP アドレス、サブネットマスク、デフォルトゲートウェイを設定します（詳細は P22 ページの「IP アドレスの設定」を参照して下さい）

（2）コンソール接続で、ユーザ名とパスワードを設定します。Web インタフェースへの接続はコンソール接続の場合と同じユーザ名とパスワード使用します。

（3）Web ブラウザからユーザ名とパスワードを入力すると、アクセスが許可され、本機のホームページが表示されます。

[注意] パスワードは 3 回まで再入力することができます。3 回失敗すると接続は切断されます。

[注意] ゲストモード (Normal Exec) で Web インタフェースにログインする場合、ページ情報の閲覧と、ゲストモードのパスワードの変更のみ行えます。管理者モード (Privileged Exec) でログインする場合は全ての設定変更が行えます。

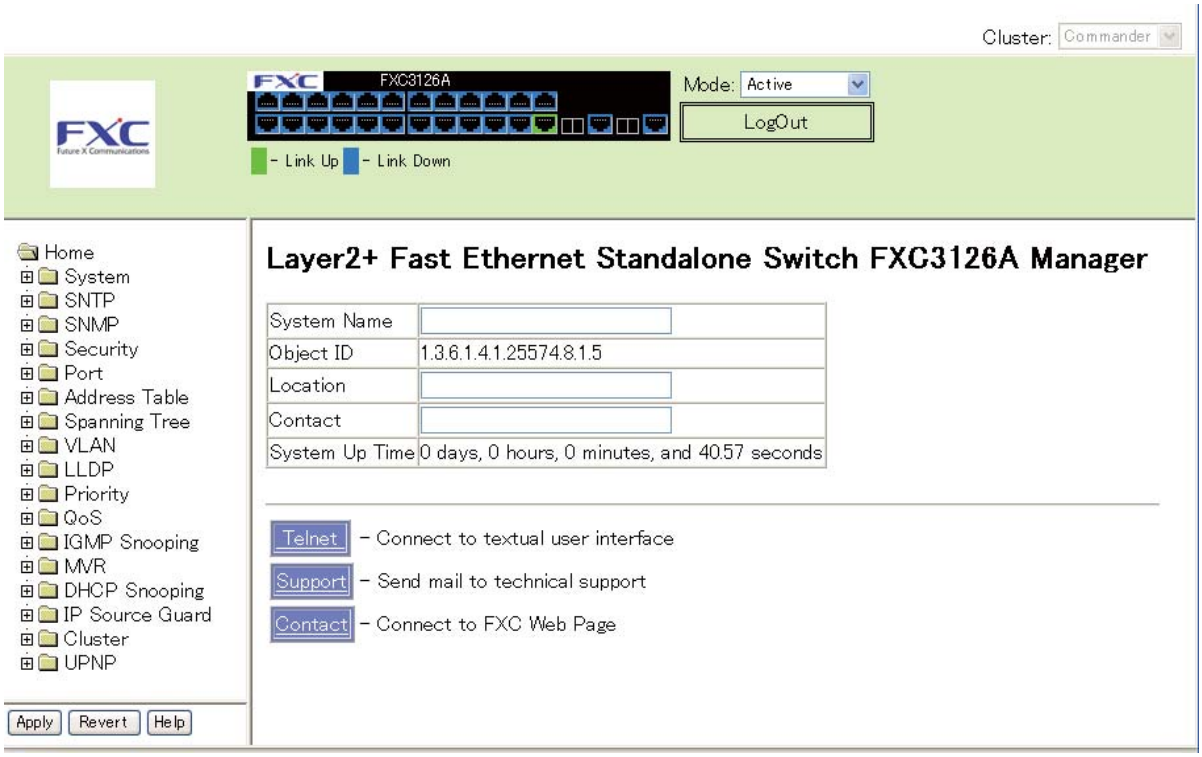
[注意] 管理用 PC と本機の間でスパニングツリーアルゴリズム (STA) が使用されていない場合、管理用 PC に接続されたポートをファストフォワーディングにする（Admin Edge Port の有効化）ことにより、Web インタフェースからの設定に対する本機の応答速度を向上させることができます（詳細は P130 「インタフェース設定」を参照して下さい）

3.2 Web インタフェースの操作方法

Web インタフェースへアクセスする際は、初めにユーザ名とパスワードを入力する必要があります。管理者モード (Privileged Exec) では全ての設定パラメータの表示 / 変更と統計情報の表示が可能です。管理者モード (Privileged Exec) の初期設定のユーザ名とパスワードは "admin" です

3.2.1 ホームページ

Web インタフェースにアクセスした際の本機の管理画面のホームページは以下の通り表示されます。画面の左側にメインメニュー、右側にはシステム情報が表示されます。メインメニューからは、他のメニューや設定パラメータ、統計情報の表示されたページへリンクしています。



3.2.2 設定オプション

設定パラメータにはダイアログボックスとドロップダウンリストがあります。

ページ上で設定変更を行った際は、必ず新しい設定を反映させるために、[Apply] ボタンをクリックしてください。

次の表は Web ページに表示される設定ボタンの内容を解説しています。

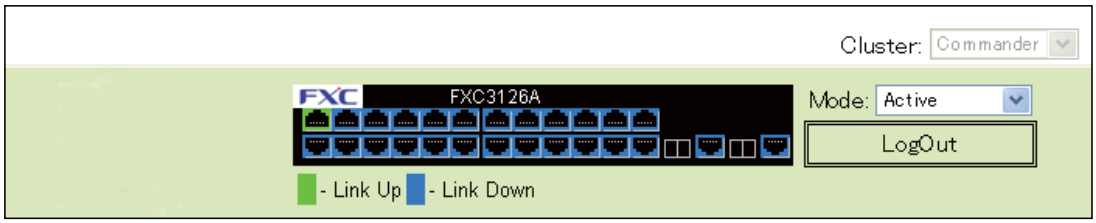
ボタン	操作
Revert	入力した値をキャンセルし、[Apply] 又は [Apply Changes] をクリックする前に表示されていた元の値に戻す
Apply	入力した値を本機に反映させる
Help	Web ヘルプにリンクしています

[注意]　ページ内容の更新を確実に行うため Internet Explorer 5.x では、メニューから [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] を選択し、[設定で保存しているページの新しいバージョンの確認] の [ページを表示するごとに確認する] をチェックして下さい。

[注意]　Internet Explorer5.0 を使用する場合は、設定の変更後にブラウザの更新ボタンを使用し、画面上に表示されている情報の更新を手動で行う必要があります。

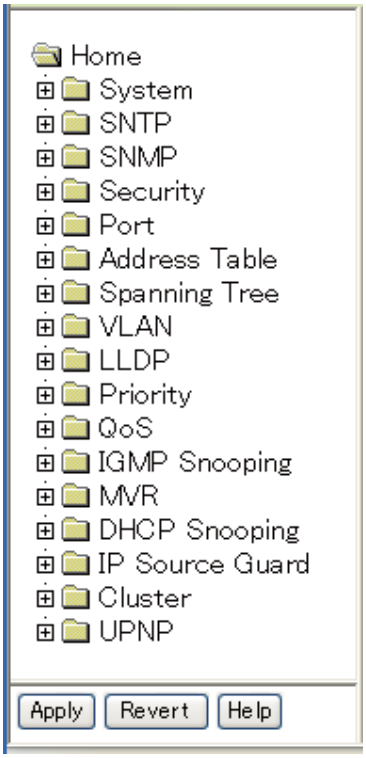
3.2.3 パネルの表示

Web インタフェースではポートの状態が画像で表示されます。各ポートのリンク状態、Duplex、フローコントロールなどの状態を確認することができます。また、各ポートをクリックすることで P102 「インタフェース接続の設定」で解説している各ポートの設定ページが表示されます。



3.2.4 メインメニュー

Web インタフェースを使用することで、システムパラメータの設定、本機全体や各ポートの管理、又はネットワーク状況の監視を行うことができます。



3.3 基本設定

3.3.1 システム情報の表示

本機に名前、設置場所及びコンタクト情報を設定することにより、管理する際に本機の識別を容易に行うことができます。

設定・表示項目

System Name

本機に設定した名前

Object ID

本機のネットワーク管理サブシステムの MIBII **オブジェクト** ID

Location

本機の設置場所

Contact

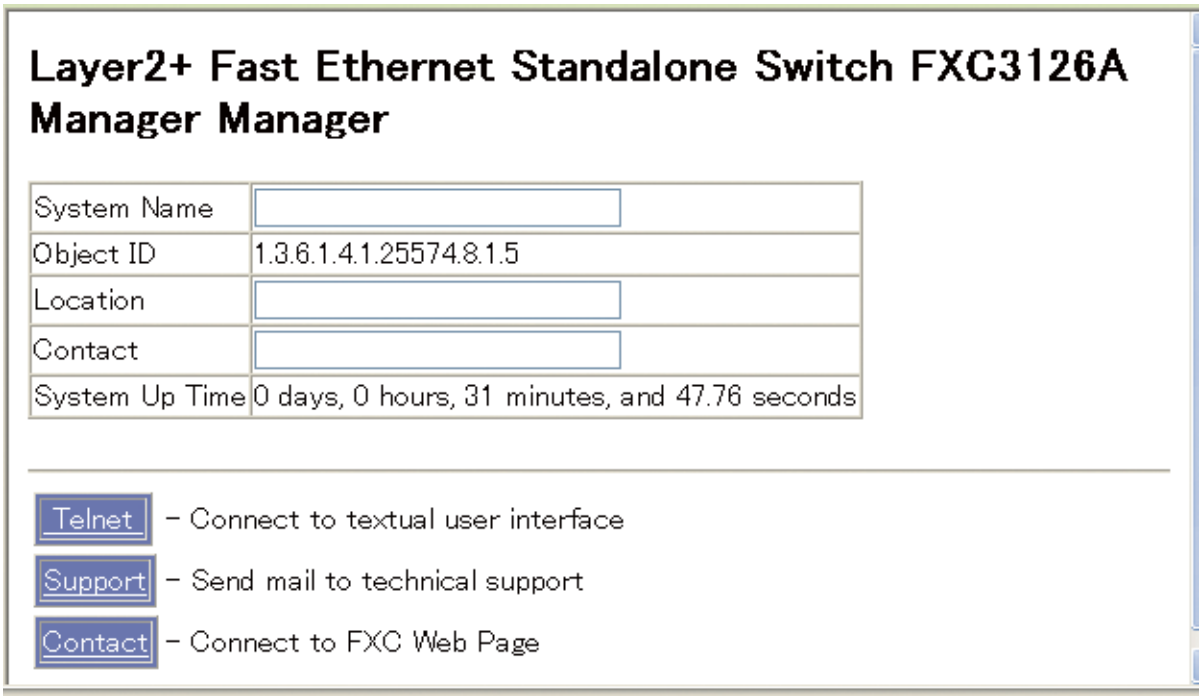
管理者のコンタクト情報

System Up Time

管理システムを起動してからの時間

設定方法

[System] → [System Information] **をクリックします。**system name**（システム名）、**location**（設置場所）及び** Contact**（管理者のコンタクト情報）を入力し、**[Apply] **ボタンをクリックします。**
（このページは Telnet **を利用し** CLI **にアクセスするための** [Telnet] **ボタンがあります）**



3.3.2 ハードウェア及びソフトウェアバージョンの表示

設定・表示項目

[Main Board](ハードウェア本体)

Serial Number

本機のシリアルナンバー

Number of Ports

搭載された RJ-45 **ポートの数**

Hardware Version

ハードウェアのバージョン

[Management Software](管理ソフトウェア)

Loader Version

Loader Code **のバージョン**

Boot-ROM Version

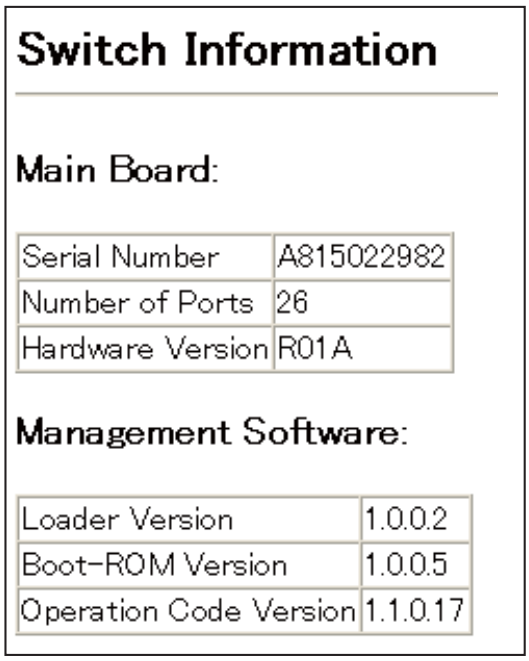
Power-On Self-Test (POST) **及び** boot code **のバージョン数**

Operation Code Version

runtime code **のバージョン**

設定方法

[System] → [Switch Information] **をクリックすると表示されます。**



3.3.3 ブリッジ拡張機能の表示

ブリッジ MIB **には、トラフィッククラス、マルチキャストフィルタリング、**VLAN **に対応した管理装置用の拡張情報が含まれます。**
変数の表示を行うために、ブリッジ MIB **拡張設定にアクセスすることができます。**

設定・表示項目

Extended Multicast Filtering Services

GARP Multicast Registration Protocol(GMRP) **を使用した個々のマルチキャストアドレスのフィルタリングが行われないことを表します（現在のファームウェアでは使用できません）**

Traffic Classes

ユーザプライオリティが複数のトラフィッククラスにマッピングされていることを表します。(詳細は、P166 **「**Class of Service（CoS)**」を参照して下さい**)

Static Entry Individual Port

ユニキャスト及びマルチキャストアドレスの静的フィルタリングが行なわれていることを表します。

VLAN Learning

本機は各ポートが独自のフィルタリングデータベースを保有する Independent VLAN Learning(IVL) **を使用していることを表しています。**

Configurable PVID Tagging

本機は各ポートに対して初期ポート VLAN ID**（フレームタグで使用される** PVID**）と、その出力形式（タグ付又はタグなし** VLAN**）が設定可能であることを表しています（**P137 **「**VLAN**」を参照して下さい)**

Local VLAN Capable

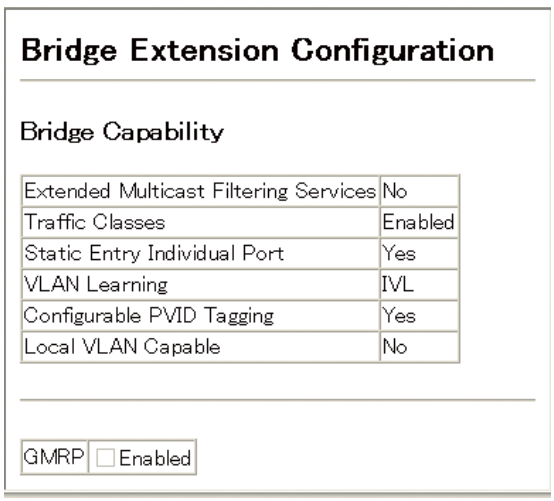
本機は複数のローカルブリッジ(マルチプルスパニングツリー)をサポートしていることを表しています

GMRP

GMRP **を使用することで、マルチキャストグループ内の終端端末をネットワーク機器に登録することができます。本機では** GMRP **に対応していません。本機は自動的なマルチキャストフィルタリングを行う** Internet Group Management Protocol (IGMP) **を使用しています。**

設定方法

[System] → [Bridge Extension Configuration] **をクリックすると表示されます。**



3.3.4 IP アドレスの設定

ネットワーク経由での管理アクセスを行うために IP アドレスが必要となります。初期設定では、IP アドレスは設定されていません。

手動で IP アドレスの設定を行う際は、使用するネットワークで利用可能な IP アドレスを設定して下さい。（手動設定時の初期設定は、IP アドレス :192.168.1.1、サブネットマスク 255.0.0.0）また、他のネットワークセグメント上の管理用 PC からアクセスする場合にはデフォルトゲートウェイの設定を行う必要があります。

本機では、手動での IP アドレスの設定及び BOOTP 又は DHCP サーバを用いて IP アドレスの取得を行うことができます。

設定・表示項目

Management VLAN

VLAN の ID(1-4094)。初期設定ではすべてのポートが VLAN 1 に所属しています。しかし、IP アドレスを割り当てる VLAN を設定することにより、管理端末を IP アドレスを割り当てた任意のポートに接続することができます。

IP Address Mode

IP アドレスを設定する方法を Static（手動設定）、DHCP、BOOTP から選択します。DHCP 又は BOOTP を選択した場合、サーバからの応答があるまで IP アドレスの取得ができません。IP アドレスを取得するためのサーバへのリクエストは周期的に送信されます（DHCP 又は BOOTP から取得する情報には IP アドレス、サブネットマスク及びデフォルトゲートウェイの情報を含みます）

IP Address

管理アクセスを行うことができる VLAN インタフェースの IP アドレスを設定します。
有効な IP アドレスは、0-255 までの十進数 4 桁によって表現され、それぞれピリオドで区切られます
（初期設定：0.0.0.0）

Subnet Mask

サブネットマスクを設定します。ルーティングに使用されるホストアドレスのビット数の識別に利用されます（初期設定：255.0.0.0）

Gateway IP Address

管理端末へのゲートウェイの IP アドレスを設定します。
管理端末が異なったセグメントにある場合には、設定が必要となります
（初期設定：0.0.0.0）

MAC Address

本機の MAC アドレスを表示しています。

DHCP Relay Option 82

リレーエージェント情報オプションの有効 / 無効。

DHCP Relay Option 82 Policy

リレーエージェント情報オプション付きクライアントパケットを転送するときの動作。

- **Replace** ― Option-82 情報が存在する場合、リプレースをおこないます。
- **Drop** ― 既にリレー情報があった場合、そのメッセージを削除します。
- **Keep** ― 既存のリレー情報をそのまま保持します。

DHCP Relay Server

スイッチの DHCP リレーエージェントに使用される DHCP サーバのアドレス。

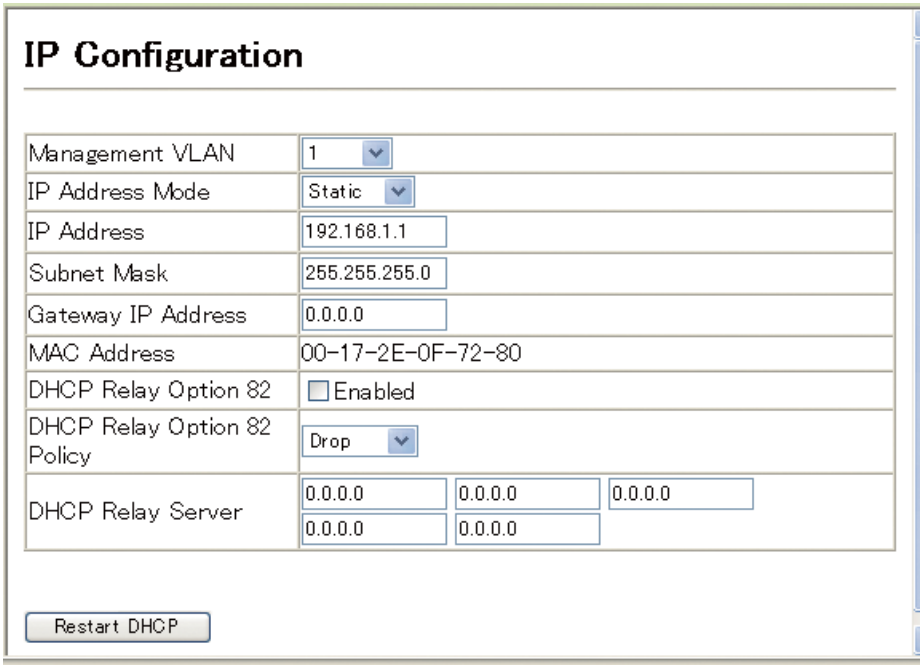
Restart DHCP

DHCP サーバへ新しい IP アドレスを要求します。

手動での IP アドレスの設定

設定方法

[System] → [IP Configuration] をクリックします。管理端末を接続する VLAN を選択し、"IP Address Mode" を Static にします。IP Address、Subnet Mask、Gateway IP Address を入力し、[Apply] をクリックします。

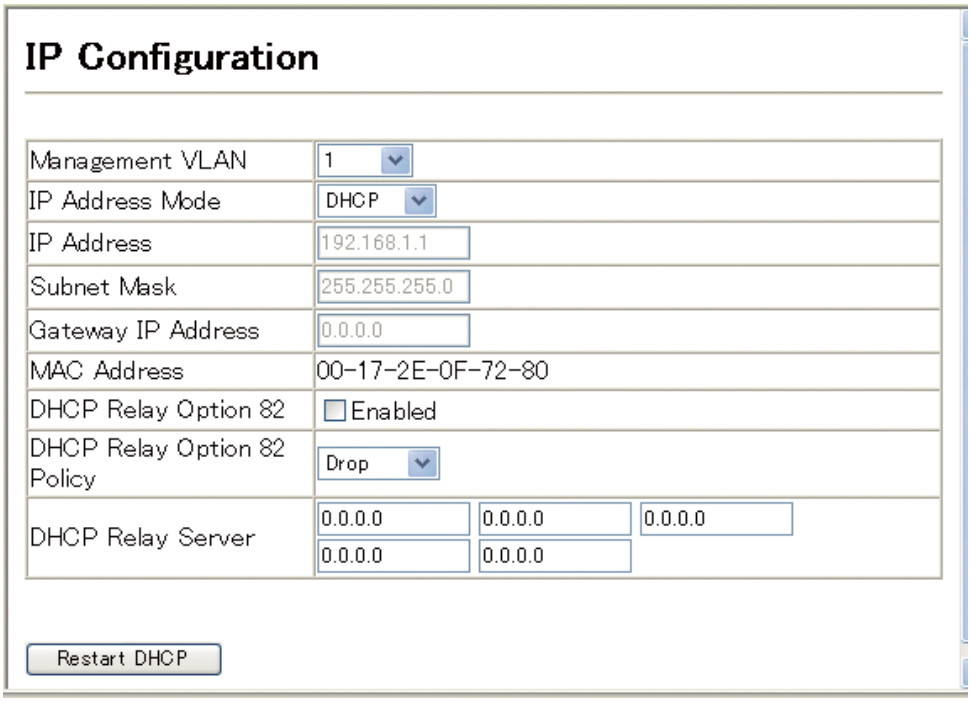


DHCP 又は BOOTP による IP アドレスの設定

DHCP 又は BOOTP サービスが利用可能な環境では、それらのサービスを利用し動的に IP アドレスの設定を行うことができます。

設定方法

[System] → [IP Configuration] をクリックします。管理端末を接続する VLAN を選択し、"IP Address Mode" を DHCP 又は BOOTP にし [Apply] をクリックします。その後 [Restart DHCP] ボタンをクリックすることで、直ちに新しい IP アドレスのリクエストを送信します。また次回以降、本機を再起動した際に IP アドレスのリクエストを送信します。



[注意]　IP アドレスの設定が変更され管理アクセスが切断された場合には、コンソール接続を行ない "show ip interface" コマンドを使用することで、新しい IP アドレスを確認することができます。

DHCP の更新

DHCP は、永久又は一定期間クライアントに IP アドレスを貸し出します。指定された期間が過ぎた場合や、本機を他のネットワークセグメントへ移動した場合、本機への管理アクセスが行えなくなります。その場合には、本機の再起動を行うか、コンソール経由で IP アドレスの再取得を行うリクエストを送信して下さい。

設定方法

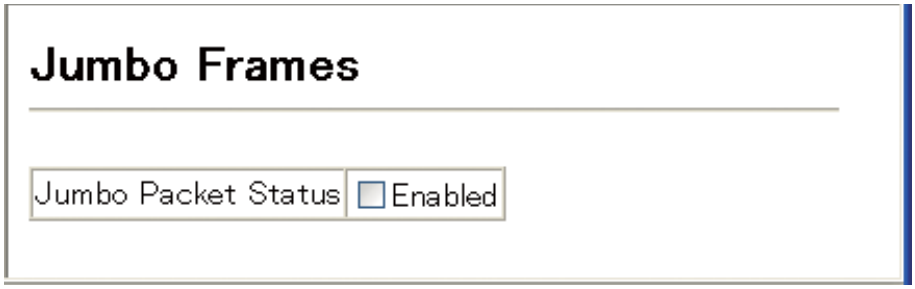
DHCP サービスを利用して IP アドレスが割り当てられ、すでに IP アドレスが利用できなくなっている場合には、Web インタフェースからの IP アドレスの更新はできません。以前の IP アドレスが利用可能な場合は、Web インタフェースを使い [Restart DHCP] ボタンから IP アドレスのリクエストを行うことができます。

3.3.5 Jumbo フレームの有効化

Jumbo フレームを有効を有効化することにより、最大 9000 バイトの Jumbo フレームパケットをサポートできます。

設定方法

[System] → [Jumbo Frames] をクリックします。



3.3.6 ファームウェアの管理

TFTP サーバを使用したファームウェアのダウンロード及びアップロードを行うことができます。TFTP サーバ上に runtime code を保存することにより、後で本機の復元を行う際にダウンロードすることができます。また、以前のバージョン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ことができます。

設定・表示項目

File Transfer Method

ファームウェアコピーの操作方法。下記のオプションがあります。

- **file to file** ― 本機のディレクトリに新たなファイル名を付けて、ファームウェアをコピーします。
- **file to tftp** ― 本機から TFTP サーバへファイルをコピーします。
- **tftp to file** ― TFTP サーバから本機へファイルをコピーします。

TFTP Server IP Address

TFTP サーバの IP アドレス

File Type

ファームウェアコピーのための opcode (オペレーションコード) または config（設定ファイル）

File Name

ファイル名は大文字と小文字が区別され、スラッシュ及びバックスラッシュを使用することはできません。また、ファイル名の頭文字にはピリオド (.) は使用できません。TFTP サーバ上のファイル名は最長 127 文字、本機内では最長 31 文字です（利用できる文字 :A-Z, a-z,0-9, ".", "-", "_"）

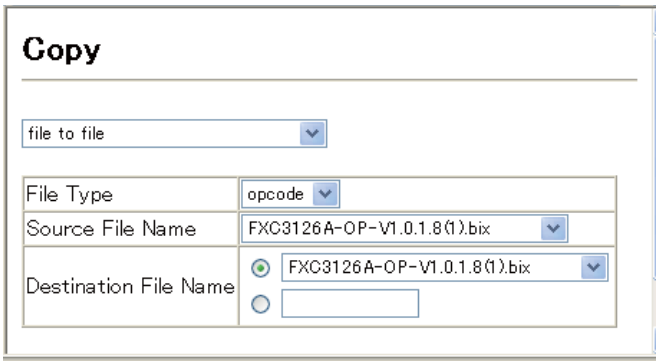
[注意] システムソフトウェアファイルは最大 2 つまでしか保存できません。起動ファイルに指定されているファイルは削除することができません。

システムソフトウェアのダウンロード

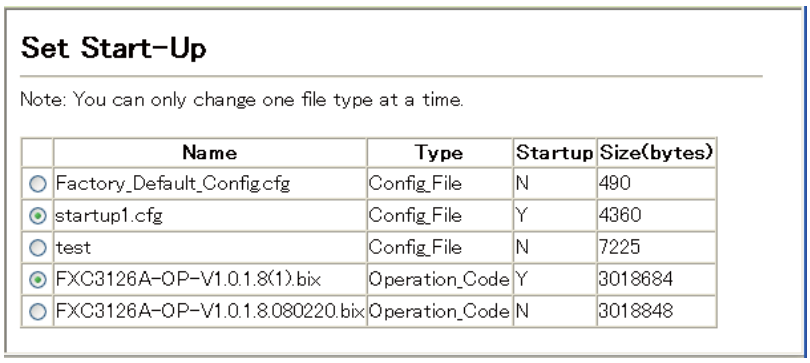
runtime code をダウンロードする場合、現在のイメージと置き換えるために現在のファイルを Destination File Name として指定することができます。また、現在の runtime code ファイルと異なるファイル名を使用し本体にダウンロードし、その後ダウンロードしたファイルを起動ファイルに設定することもできます。

設定方法

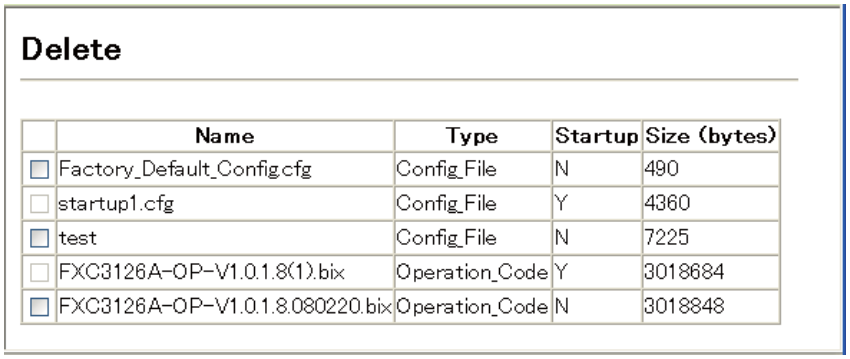
[System] → [File Management] → [Copy Operation] をクリックします。



現在のファイルと異なる名前でダウンロードを行った場合には、新しくダウンロードしたファイルを、起動ファイルに設定する必要があります。ドロップダウンボックスから新しいファイル名を選択します。その後、[Apply Changes] をクリックします。新しいファームウェアを使用するためには本機の再起動を行います。



ファイルを削除するには、[System] → [File] → [Delete] をクリックします。チェックボックスをクリックして削除するファイル名をリストから選択し、[Apply] をクリックします。起動ファイルとして指定されているファイルは削除できないことに注意して下さい。



3.3.7 設定情報ファイルの保存・復元

TFTP サーバを使用し、設定情報ファイルをダウンロード又はアップロードする事ができます。アップロードした設定情報ファイルは後からダウンロードし、本機の設定を復元するために使用することができます。

設定・表示項目

File Transfer Method

設定情報ファイルコピーの操作方法。下記のオプションがあります。

- **file to file** ― 新たなファイル名を付けて本機のディレクトリへコピーします。
- **file to running-config** ― 本機のファイルを実行中の設定ファイルへコピーします。
- **file to startup-config** ― 本機のファイルを起動設定ファイルへコピーします。
- **file to tftp** ― 本機から TFTP サーバへファイルをコピーします。
- **running-config to file** ― 実行中の設定ファイルをコピーします。
- **running-config to startup-config** ― 実行中の設定ファイルを起動設定ファイルへコピーします。
- **running-config to tftp** ― 実行中の設定ファイルを TFTP サーバへコピーします。
- **startup-config to file** ― 起動設定ファイルを本機のファイルへコピーします。
- **startup-config to running-config** ― 起動設定ファイルを実行中の設定ファイルへコピーします。
- **startup-config to tftp** ― 起動設定ファイルを TFTP サーバへコピーします。
- **tftp to file** ― TFTP サーバから本機へファイルをコピーします。
- **tftp to running-config** ― TFTP サーバから実行中の設定ファイルへコピーします。
- **tftp to startup-config** ― TFTP サーバから起動設定ファイルへコピーします。

TFTP Server IP Address

TFTP サーバの IP アドレス

File Type

設定情報をコピーするための config (設定ファイル)

File Name

ファイル名は大文字と小文字が区別され、スラッシュ及びバックスラッシュを使用することはできません。また、ファイル名の頭文字にはピリオド (.) は使用できません。TFTP サーバ上のファイル名は最長 127 文字、本機内では最長 31 文字です（利用できる文字 :A-Z, a-z,0-9, ".", "-", "_")

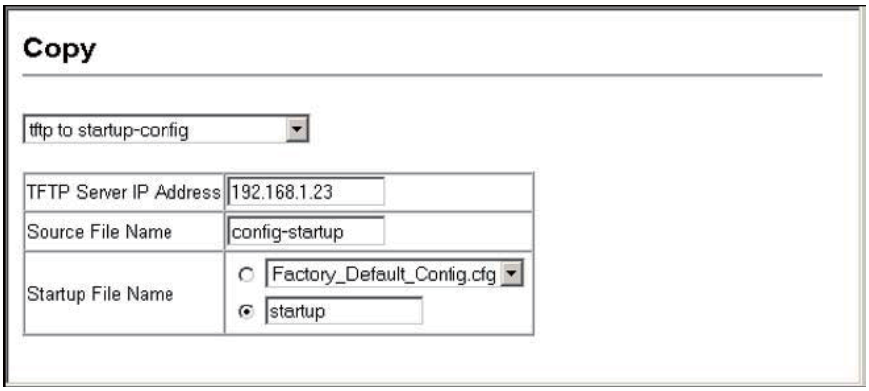
[注意] 本機内に保存可能な設定ファイルの最大数はフラッシュメモリの容量に依存します。

設定情報ファイルのダウンロード

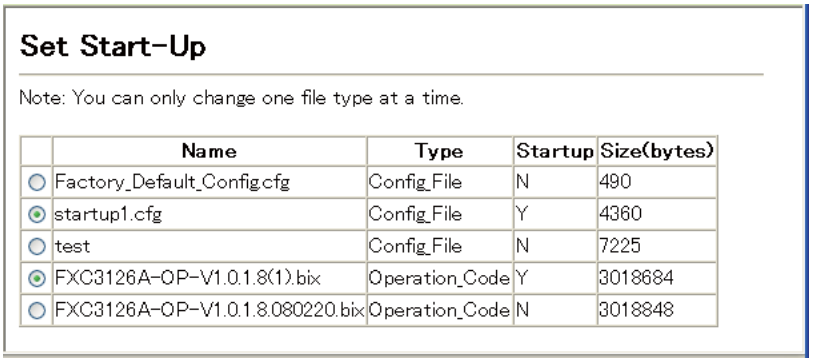
設定ファイルは新しいファイル名で保存し、起動ファイルとして設定できる他に、現在の起動設定ファイルを保存先に指定することで直接起動設定ファイルを置き換えることができます。但し、"Factory_Default_Config.cfg" ファイルは TFTP サーバへコピーすることはできますが、設定ファイルをダウンロードする際に、ダウンロード先のファイル名として指定し、新しいファイルに置き換えることはできません。

設定方法

[System] → [File] → [Copy Operation] をクリックします。



現在の起動設定ファイルと異なる名前でダウンロードを行った場合には、新しくダウンロードしたファイルを、起動ファイルとして使用される設定ファイルにする必要があります。ドロップダウンボックスから新しいファイル名を選択します。その後、[Apply] をクリックします。新しい設定を使用するためには本機の再起動を行います。



[注意]　工場出荷時の状態に戻すには「startup1.cfg」を起動ファイルに設定し、再起動を行って下さい。

3.3.8 コンソールポートの設定

VT100 端末を本機のシリアル（コンソール）ポートに接続し、本機の設定を行うことができます。コンソール経由での管理機能の利用は、パスワード、タイムアウト、その他の基本的な通信条件など、数々のパラメータにより可能となります。CLI または Web インタフェースからパラメータ値の設定を行うことができます。

設定・表示項目

Login Timeout

CLI でのログインタイムアウト時間。設定時間内にログインが行われない場合、その接続は切断されます（範囲：0-300 秒、初期設定：0 秒）

Exec Timeout

ユーザ入力のタイムアウト時間。設定時間内に入力が行われない場合、その接続は切断されます（範囲：0-65535 秒、初期設定：600 秒）

Password Threshold

ログイン時のパスワード入力のリトライ回数。リトライ数が設定値を超えた場合、本機は一定時間（Silent Time パラメータで指定した時間）、ログインのリクエストに応答しなくなります（範囲：0-120 回、初期設定：3 回）

Silent Time

パスワード入力のリトライ数を超えた場合に、コンソールへのアクセスができなくなる時間（範囲：0-65535 秒、初期設定：0 秒）

Data Bits

コンソールポートで生成される各文字あたりのデータビットの値。パリティが生成されている場合は 7 データビットを、パリティが生成されていない場合 (no parity) は 8 データビットを指定して下さい（初期設定：8 ビット）

Parity

パリティビット。接続するターミナルによっては個々のパリティビットの設定を要求する場合があります。Even(偶数)、Odd(奇数)、None(なし) から設定します（初期設定：None）

Speed

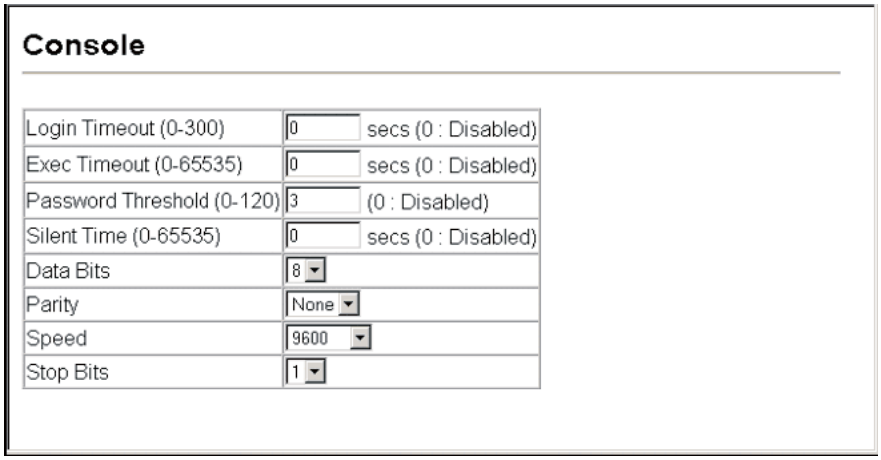
ターミナル接続の送信 (ターミナルへの)/ 受信 (ターミナルからの) ボーレート。シリアルポートに接続された機器でサポートされているボーレートを指定して下さい。
（初期設定：9600 bps)

Stop Bits

送信するストップビットの値（範囲：1-2、初期設定：1 ストップビット)

設定方法

[System] → [Line] → [Console] **をクリックします。コンソールポート接続パラメータを設定します。その後、**[Apply] **をクリックします。**



3.3.9 Telnet の設定

ネットワーク経由、Telnet (仮想ターミナル) で本機の設定を行うことができます。Telnet 経由での管理機能利用の可 / 不可、又は TCP ポート番号、タイムアウト、パスワードなど数々のパラメータの設定が可能です。CLI または Web インタフェースからパラメータ値の設定を行うことができます。

設定・表示項目

Telnet Status

本機への Telnet 接続の有効 / 無効（初期設定：有効）

Telnet Port Number

本機へ Telnet 接続する場合の TCP ポート番号（初期設定：23）

Login Timeout

CLI でのログインタイムアウト時間。設定時間内にログインが行われない場合、その接続は切断されます（範囲：0-300 秒、初期設定：300 秒）

Exec Timeout

ユーザ入力のタイムアウト時間。設定時間内に入力が行われない場合、その接続は切断されます（範囲：0-65535 秒、初期設定：600 秒）

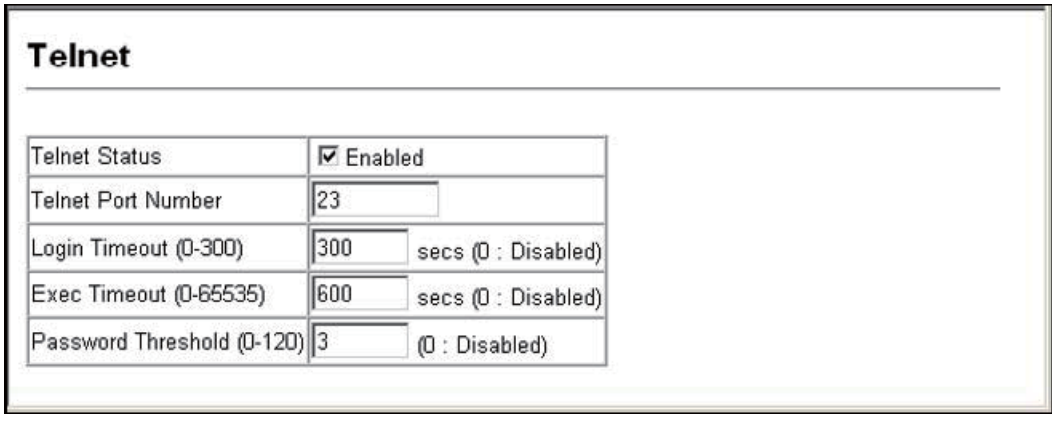
Password Threshold

ログイン時のパスワード入力のリトライ回数。

（範囲：0-120 回、初期設定：3 回）

設定方法

[System] → [Line] → [Telnet] をクリックします。Telnet 接続のためのパラメータを設定します。その後、[Apply] をクリックします。



3.3.10 Event Logging の設定

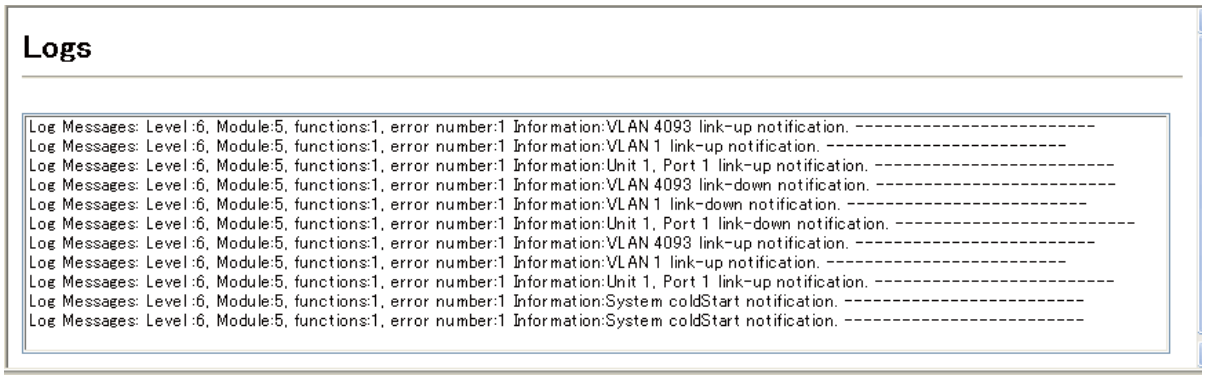
エラーメッセージのログに関する設定を行うことができます。スイッチ本体へ保存するイベントメッセージの種類、syslog サーバへのログの保存、及び最新のイベントメッセージの一覧表示などが可能です。

ログメッセージの表示

Logs 画面では、保存されているシステム / イベントメッセージを表示できます。本体の RAM (電源投入時には消去されます) に一時的に保存されるメッセージは 2048 エントリです。フラッシュメモリに永久的に保存されるメッセージは 4096 エントリです。

設定方法

[System] → [Log] → [Logs] をクリックします。



syslog の設定

本機は、イベントメッセージの保存 / 非保存、RAM/ フラッシュメモリに保存するメッセージレベルの指定が可能です。

フラッシュメモリのメッセージは本機に永久的に保存され、ネットワークで障害が起こった際のトラブル解決に役立ちます。フラッシュメモリには 4096 件まで保存することができ、保存可能なログメモリ (256KB) を超えた場合は最も古いエントリから上書きされます。

System Logs 画面では、フラッシュメモリ /RAM に保存するシステムメッセージの制限を設定できます。初期設定では、フラッシュメモリには 0-3 のレベル、又 RAM には 0-6 のレベルのイベントに関してそれぞれ保存されます。

設定・表示項目

System Log Status

デバッグ又はエラーメッセージのログ保存の有効 / 無効（初期設定：有効）

Flash Level

スイッチ本体のフラッシュメモリに永久的に保存するログメッセージ。指定したレベルより上のレベルのメッセージをすべて保存します。例えば "3" を指定すると、0-3 のレベルのメッセージがすべてフラッシュメモリに保存されます（範囲：0-7、初期設定：3）

レベル	名前	解説
7	Debug	デバッグメッセージ
6	Informational	情報メッセージ
5	Notice	重要なメッセージ
4	Warning	警告メッセージ
3	Error	エラー状態を示すメッセージ
2	Critical	重大な状態を示すエラーメッセージ
1	Alert	迅速な対応が必要なメッセージ
0	Emergency	システム不安定状態を示すメッセージ

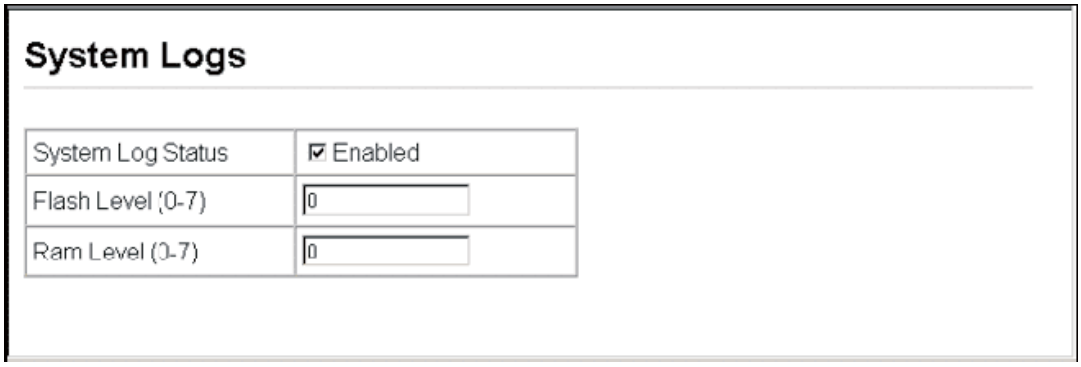
RAM Level

スイッチ本体の RAM **に一時的に保存するログメッセージ。指定したレベルより上のレベルのメッセージをすべて保存します。例えば** "7" **を指定すると、**0-7 **のレベルのメッセージがすべてフラッシュメモリに保存されます（範囲：**0-7**、初期設定：**7**）**

[注意] フラッシュメモリのレベルは RAM レベルと同じか、これより下のレベルにして下さい。

設定方法

[System] → [Log] → [System Logs] **をクリックします。**"System Log Status" **にチェックを入れ、**RAM/ **フラッシュメモリに保存するイベントメッセージを設定します。その後、**[Apply] **をクリックします。**



リモートログの設定

Remote Logs 画面では、他の管理ステーションから syslog サーバへ送信するイベントメッセージのログに関する設定を行います。指定したレベルより下のエラーメッセージだけ送信するよう制限することができます。

設定・表示項目

Remote Log Status

デバッグ又はエラーメッセージのリモートログ保存の有効 / 無効（初期設定：有効）

Logging Facility

送信する syslog メッセージのファシリティタイプ。8 つのファシリティタイプを 16-23 の値で指定します。syslog サーバはイベントメッセージを適切なサービスへ送信するためにファシリティタイプを使用します。

本属性では syslog メッセージとして送信するファシリティタイプタグを指定します (詳細：RFC3164)。タイプの設定は、本機により報告するメッセージの種類に影響しません。syslog サーバにおいてソートやデータベースへの保存の際に使用されます（範囲：16-23、初期設定：23）

Logging Trap

syslog サーバに送信するメッセージの種類。指定したレベルより上のレベルのメッセージをすべて保存します。例えば "3" を指定すると、0-3 のレベルのメッセージがすべてリモートサーバに保存されます（範囲：0-7、初期設定：6）

Host IP List

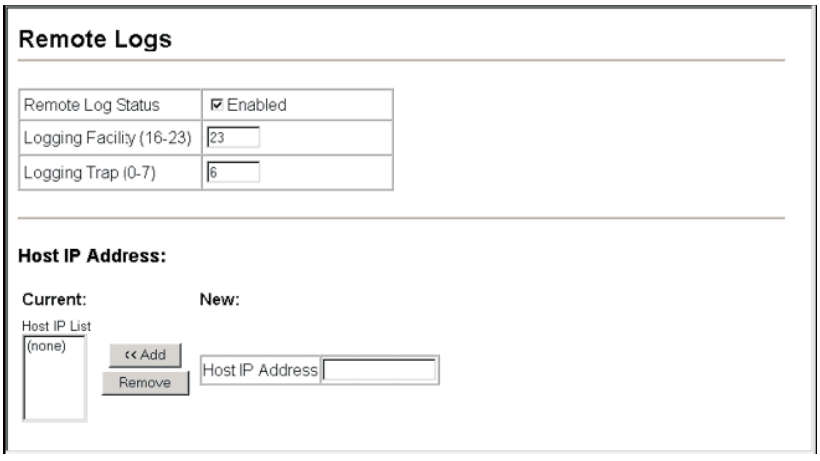
syslog メッセージを受け取るリモート syslog サーバの IP アドレスのリストを表示します。Host IP アドレスの上限は 5 つです。

Host IP Address

Host IP List に追加するリモート syslog サーバの IP アドレス。

設定方法

[System] → [Log] → [Remote Logs] をクリックします。"Host IP List" に IP アドレスを指定するには、"Host IP Address" に追加する IP アドレスを入力し、[Add] をクリックします。IP アドレスを削除するには、"Host IP List" から削除する IP アドレスをクリックし、その後 [Remove] をクリックします。



SMTP（Simple Transfer Protocol）

指定したレベルのイベントが発生した際、システム管理者にトラブルの発生を知らせるために、本機は SMTP (Simple Mail Transfer Protocol) を使用したメール送信を行うことができます。メールはネットワークに接続している指定した SMTP サーバに送信され、POP 又は IMAP クライアントから受信できます。

設定・表示項目

Admin Status

SMTP 機能の有効 / 無効（初期設定：有効）

Email Source Address

アラートメッセージの "From" に入力されるメール送信者名を設定します。本機を識別するためのアドレス（文字列）や本機の管理者のアドレスなどを使用します。

Severity

アラートメッセージのしきい値。指定したレベルより上のレベルのイベント発生時には、設定したメール受信者あてに送信されます。例えば "7" を指定すると、0-7 のレベルのメッセージがすべて通知されます。レベルについては P34 を参照してください。

SMTP Server List

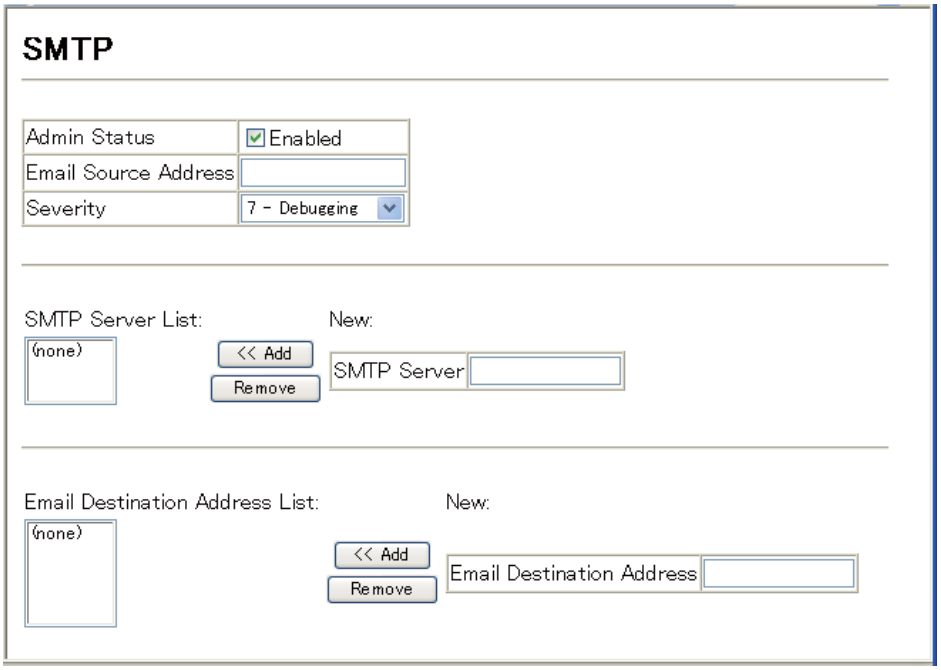
本機からのアラートメッセージを受信する SMTP サーバを指定できます。

Email Destination Address Liet

アラートメッセージを受信するアドレス。

設定方法

[System] → [Log] → [SMTP] をクリックします。"Server IP address" に新しい IP アドレスを入力し、[Add] をクリックします。IP アドレスを削除する場合には、エントリからアドレスを選択し [Remove] をクリックします。



3.3.11 再起動

設定方法

[System] → [Reset] をクリックします。[Reset] ボタンを押して、本機の再起動を行います。再起動の確認を促すプロンプトが表示されたら、確認して実行します。

[注意]　再起動時には Power-On Self-Test が実行されます。

3.3.12 システムクロック設定

SNTP(Simple Network Time Protocol) 機能は、タイムサーバ (SNTP/NTP) からの周期的なアップデートにより本機内部の時刻設定を行うことができます。本機の内部時刻の設定を正確に保つことにより、システムログの保存の際に日時を正確に記録することができます。

また、CLI から手動で時刻の設定を行うこともできます（詳細は 303 ページの「calendar set」を参照）

時刻の設定がされていない場合、初期設定の時刻が記録され本機起動時からの時間となります。

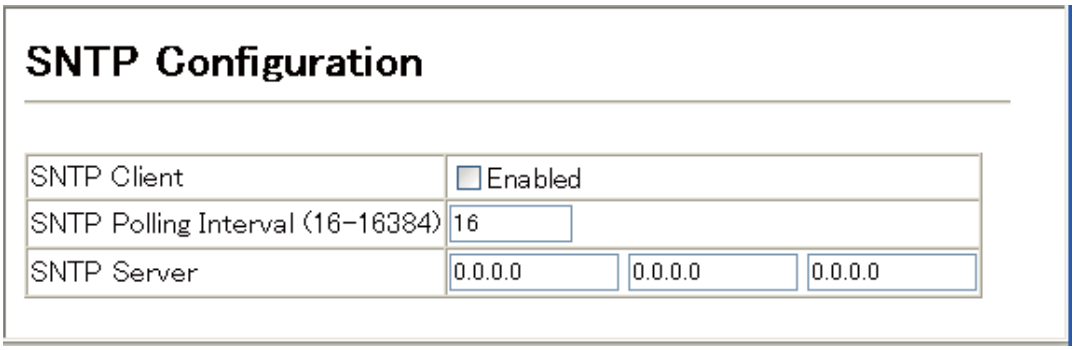
本機は SNTP クライアントとして有効な場合、設定してあるタイムサーバに対して時刻の取得を要求します。最大 3 つのタイムサーバの IP アドレスを設定することができます。各サーバに対して時刻の取得を要求します。

SNTP 設定

本機では、特定のタイムサーバに対して時間の同期リクエストを送信します。

設定方法

[SNTP] → [Configuration] をクリックします。各項目を入力し、[Apply] をクリックします。



タイムゾーンの設定

SNTP では UTC(Coordinated Universal Time: 協定世界時間。別名：GMT/Greenwich Mean Time) を使用します。

本機を設置している現地時間に対応するために UTC からの時差（タイムゾーン）の設定を行う必要があります。

設定・表示項目

Current Time

現在時刻の表示

Name

タイムゾーンに対する名称を設定します。（設定範囲：1-29 文字）

Hours (0-12)

UTC からの時間の差を設定します。

Minutes (0-59)

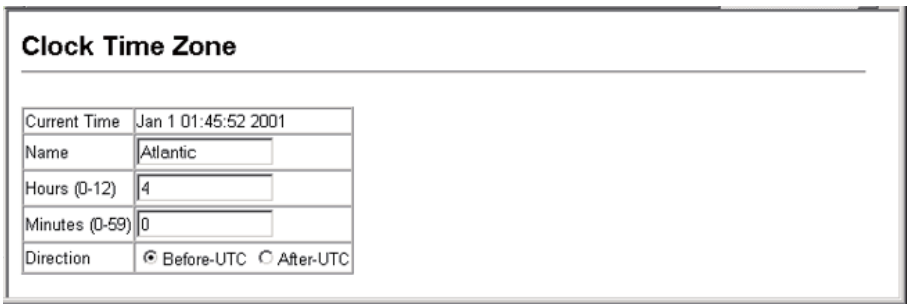
UTC からの時間（分数）の差を設定します。

Direction

UTC からのタイムゾーンの差がプラスかマイナスかを設定します。

設定方法

[SNTP] → [Clock Time Zone] をクリックします。UTC との時差を設定し [Apply] をクリックします。



3.4 SNMP

Simple Network Management Protocol (SNMP) はネットワーク上の機器の管理用の通信プロトコルです。SNMP は一般的にネットワーク機器やコンピュータなどの監視や設定をネットワーク経由で行う際に使用されます。

本機は SNMP エージェントを搭載し、ポートの通信やハードウェアの状態を監視することができます。SNMP 対応のネットワーク管理ソフトウェアを使用することで、これらの情報にアクセスすることが可能です。本機の内蔵エージェントへのアクセス権はコミュニティ名 (Community Strings) により設定されます。そのため、本機にアクセスするためには、事前に管理ソフトウェアのコミュニティ名を適切な値に設定する必要があります。

本機は、SNMP バージョン 1,2c,3 をサポートするエージェントを搭載し、ポートの通信やハードウェアの状態を監視することができます。ネットワーク上のマネージメントステーションは、ネットワーク管理ソフトウェアを使用し、これらの情報にアクセスすることが可能です。

SNMPv1,v2c を使用時のアクセス認証はコミュニティ名によってのみ行われますが、SNMPv3 ではマネージャとエージェント間が交換するメッセージを認証、暗号化することによって、機器へのセキュアなアクセスを提供しています。

SNMPv3 では、セキュリティモデルおよびセキュリティレベルが定義されます。セキュリティモデルは、ユーザーおよび、ユーザーが属するグループを設定するプロセスです。セキュリティレベルは、セキュリティモデルで許可されるセキュリティのレベルです。セキュリティモデルとセキュリティレベルの組み合わせによって、SNMP パケットの取り扱いに際して使用されるプロセスが決定されます。セキュリティモデルには SNMPv1、SNMPv2c および SNMPv3 の 3 種類が定義されています。

3.4.1 コミュニティ名の設定

管理アクセスの認証のためのコミュニティ名を最大 5 つ設定することができます。IP トラップマネージャで使用されるコミュニティ名もすべてここにリストされています。

セキュリティのため、初期設定のコミュニティ名を削除することを推奨します。

設定・表示項目

SNMP Community Capability

本機が最大 5 つのコミュニティ名をサポートしていることを表しています

Current

現在設定されているコミュニティ名のリスト

Community String

SNMP でのアクセスを行う際にパスワードの役割を果たすコミュニティ名

（初期設定："public"（Read-Only アクセス）, "private"（Read/Write アクセス）、設定範囲：1-32 文字 , 大文字小文字は区別されます）

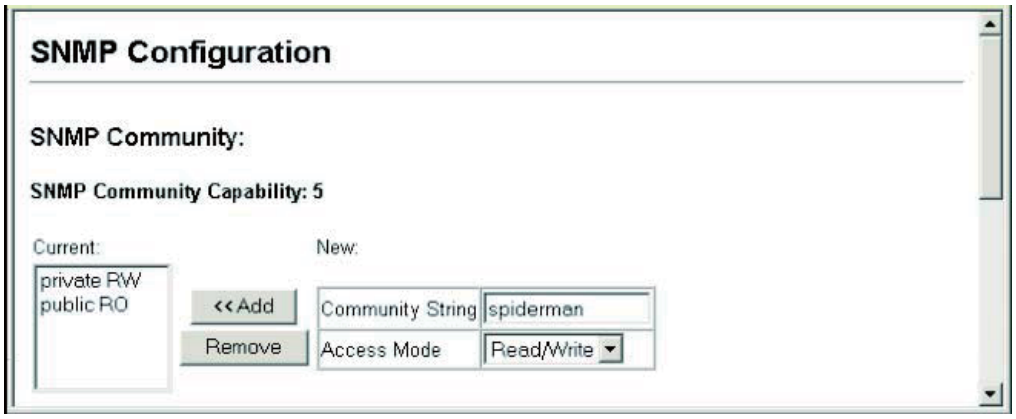
Access Mode

コミュニティ名へのアクセス権を設定します :

- **Read-Only** ― 読み取り専用アクセスとなります。管理ソフトウェアからは MIB オブジェクトの取得のみができます。
- **Read/Write** ― 読み書き可能なアクセスとなります。認可された管理ステーションは MIB オブジェクトの取得と変更の両方が可能です。

設定方法

[SNMP] → [Configuration] をクリックします。コミュニティ名の追加を行う場合は [Community String] 欄に新しいコミュニティ名を入力し、Access Mode ダウンリストからアクセス権を選択し、[Add] をクリックします。



3.4.2 トラップマネージャ・トラップタイプの指定

本機の状態に変更があった場合に本機からトラップマネージャに対してトラップが出されます。トラップを有効にするためにはトラップを受け取るトラップマネージャを指定する必要があります。

認証失敗メッセージ及び他のトラップメッセージを受信する管理端末を最大 5 つまで指定することができます。

設定・表示項目

Trap Manager Capability

本機が最大 5 つのトラップマネージャをサポートしていることを表しています

Current

登録されているトラップマネージャのリスト

Trap Manager IP Address

トラップを受信するホストの IP アドレス

Trap Manager Community String

トラップ送信時のコミュニティ名（設定範囲：1-32 文字、大文字小文字は区別されます）

Trap UDP Port

トラプマネージャが使用する UDP ポートを指定します（初期設定：162）

Trap Version

送信するトラップのバージョン（SNMP v1 又は SNMP v2、v3　初期設定：SNMP v1）

Trap Security Level

トラップセキュリティレベルを指定します

Enable Authentication Traps

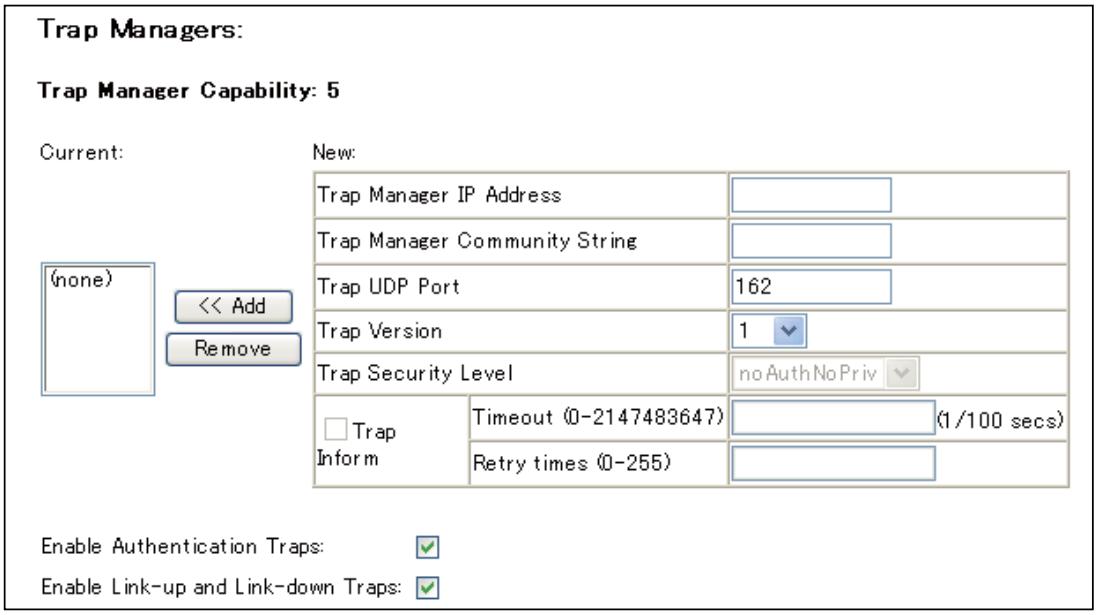
認証時に不正なパスワードが送信された場合にトラップが発行されます（初期設定：有効）

Enable Link-up and Link-down Traps

Link-up **又は** Link-down **時にトラップが発行されます（初期設定：有効）**

設定方法

[SNMP] → [Configuration] **をクリックします。**[Trap Managers] **で、トラップを受信するトラップマネージャの** IP **アドレス** (Trap Manager IP Address)**、コミュニティ名** (Trap Manager Community String) **を入力します。**
SNMP **バージョン** (SNMP Version) **を指定します。**
[Add] **をクリックすると、左側の（**Current**）リストに新しいマネージャが追加されます。トラップの種類 (認証時、**Link-up/down) **の変更を行う場合はチェックボックスで選択します。設定完了後、**[Apply] **をクリックします。**
トラップマネージャを削除する場合は、リストからマネージャを選択し [Remove] **をクリックします。**



3.4.3 SNMP エージェントを有効にする

SNMPv3 サービスを有効にします

設定・表示項目

SNMP Agent Status

チェックを入れることで、SNMP エージェントが有効になります

設定方法

[SNMP] → [Agent Status] をクリックします。[Enable] チェックボックスにチェックを入れ、[Apply] をクリックします。

3.4.4 SNMPv3 マネージメントアクセスの設定

スイッチへ SNMPv3 マネージメントアクセスを行う際には以下の手順で設定します。

(1) エンジン ID の設定を行います。エンジン ID の設定は必ず一番最初に行ってください。

(2) ビューの設定を行います。ビューを基に、読み込み専用・書き込み許可などのアクセス制御が行われます。

(3) グループを設定します。セキュリティモデルの選択および (2) で設定したビューを使用し、グループに所属する全ユーザーのアクセス制限を定義します。

(4) ユーザーを作成し、所属するグループを決定します。

ローカルエンジン ID の設定

SNMP エンジンは、スイッチ上の独立した SNMP エージェントです。このエンジンはメッセージの再送、遅延およびリダイレクションを防止します。エンジン ID は、ユーザーパスワードと組み合わせて、SNMPv3 パケットの認証と暗号化を行うためのセキュリティキーを生成します。

ローカルエンジン ID はスイッチにたいして固有になるように自動的に生成されます。これをデフォルトエンジン ID とよびます。

ローカルエンジン ID が削除または変更された場合、全ての SNMP ユーザーはクリアされます。そのため既存のユーザーの再構成を行う必要があります。

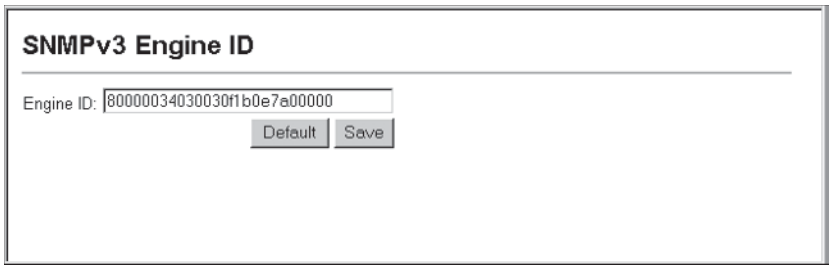
設定・表示項目

Engine ID

エンジン ID を設定します。

設定方法

[SNMP] → [SNMPv3 Engine ID] をクリックします。Engine ID を入力し、[Save] をクリックします。デフォルト値を使用する場合には [Default] ボタンをクリックします。



リモートエンジン ID の設定

リモートデバイス上の SNMPv3 ユーザーへインフォームメッセージを送る場合、最初にリモートエンジン ID を設定します。リモートエンジン ID は、リモートホストで認証と暗号化パケットのセキュリティダイジェストを計算するために使用されます。
SNMP パスワードは、信頼できるエージェントのエンジン ID を使用してローカライズされます。インフォームの信頼できる SNMP エージェントはリモートエージェントです。そのため、プロキシリクエストまたはインフォームを送信する前にリモートエージェントの SNMP エンジン ID を設定する必要があります。（詳しくは P41 「トラップマネージャ・トラップタイプの指定」および P48 「SNMPv3 リモートユーザーの設定」を参照してください）

設定・表示項目

Remote Engine ID

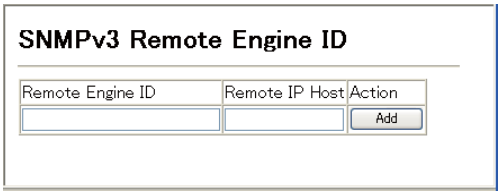
リモートエンジン ID を設定します。

Remote IP Host

リモートデバイスの IP アドレスを設定します。

設定方法

[SNMP] → [SNMPv3 Remote Engine ID] をクリックします。Engine ID、Remote IP Host を入力し、[Add] をクリックします。ID を削除する場合には [Remove] をクリックします。



SNMPv3 ユーザーの設定

それぞれの SNMPv3 **ユーザーは固有の名前を持ちます。**

ここでは、各ユーザーの所属グループ、セキュリティレベル等を設定します。SNMP v3 **では、ユーザーが所属するグループによってアクセス制限が定義されます。**

設定・表示項目

User Name

SNMPv3 **ユーザー名（**1-32 **文字）**

Group Name

既存のグループから選択または新規グループを作成します（1-32 **文字）**

Model

セキュリティモデルを選択します（v1,v2c,v3　**初期設定：**v1）

Level

セキュリティレベル

- noAuthNoPriv － **認証も暗号化も行いません（**v3 **セキュリティモデルの初期設定値）**
- AuthNoPriv － **認証を行いますが暗号化は行いません（**v3 **セキュリティモデルでのみ設定可）**
- AuthPriv － **認証と暗号化を行います（**v3 **セキュリティモデルでのみ設定可）**

Authentication

認証用プロトコルの選択。MD5 **または** SHA**（初期設定：**MD5）

Authentication Password

認証用パスワード（最小 8 **文字）**

Privacy

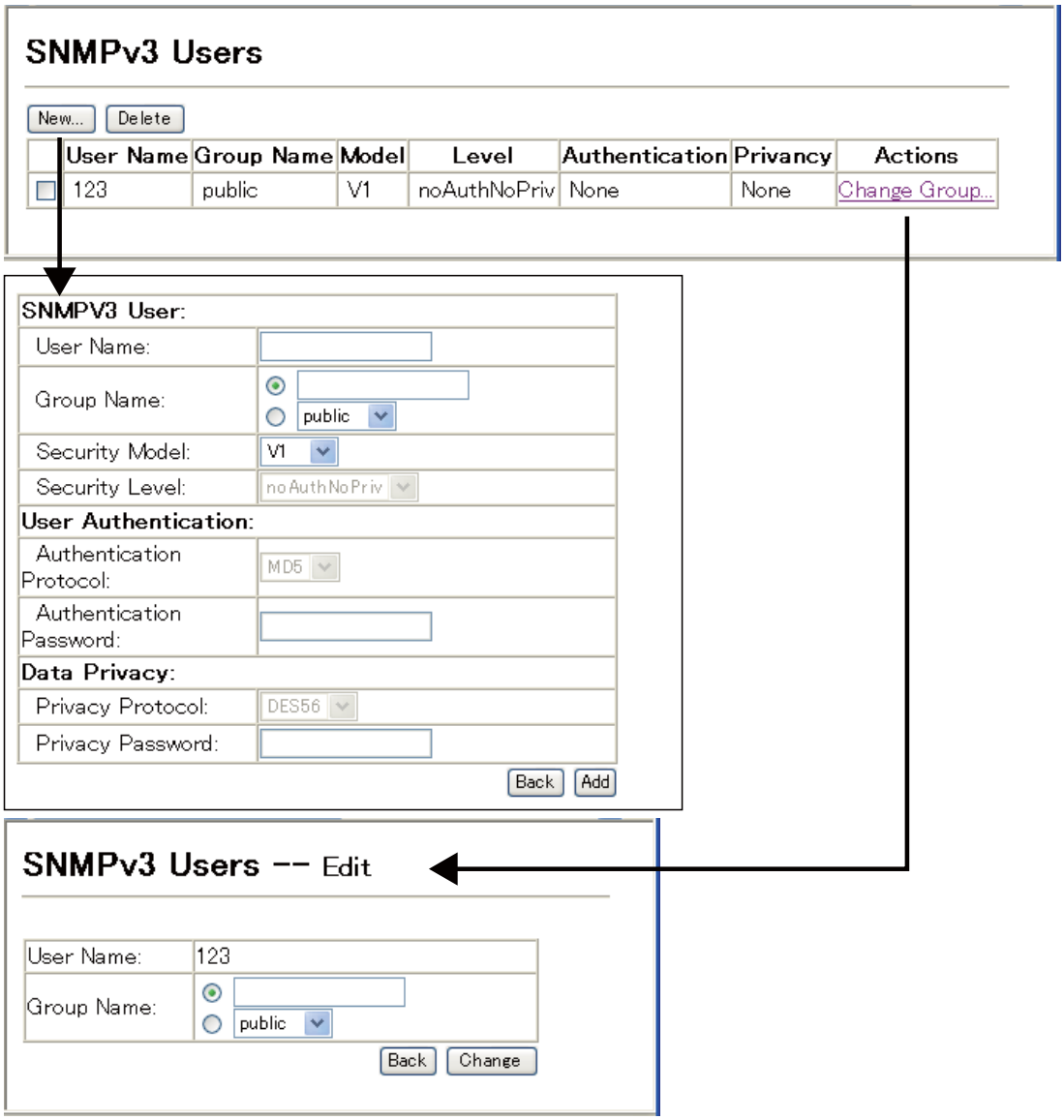
暗号化プロトコル。DES56bit **のみ使用可。**

Actions

ユーザを別の SNMPv3 **グループへアサインすることができます。**

設定方法

[SNMP] → [SNMPv3 Users] をクリックします。新しいユーザーを登録する場合、[New...] をクリックします。[SNMPv3 Users--New] のページが表示されます。(User Name)(Group Name)(Security Model)(Security Lebel)(User Authentication)(Data Privacy) の設定を行い、[Add] をクリックします。[SNMPv3 Users] のページに戻り、登録したユーザーがリストに追加されます。変更を行う場合には [Change Group] をクリックすると [SNMPv3 Users--Edit] のページへ移動します。ユーザーを削除する場合には、削除したいユーザー名のチェックボックスへチェックを入れ、[Delete] をクリックします。



SNMPv3 リモートユーザーの設定

それぞれの SNMPv3 ユーザーは固有の名前を持ちます。

SNMP v3 では、ユーザーが所属するグループによってアクセス制限が定義されます。

リモートデバイス上の SNMP ユーザーへインフォームメッセージを送るために、最初に、ユーザーが属するリモートデバイス上の SNMP エージェントへ ID を設定します。

リモートエンジン ID は、リモートホストで認証と暗号化パケットのセキュリティダイジェストを計算するために使用されます。（詳細は P41 「トラップマネージャ・トラップタイプの指定」および P45 「リモートエンジン ID の設定」を参照してください）

設定・表示項目

User Name

SNMPv3 ユーザー名（1-32 文字）

Group Name

グループ名を選択します（1-32 文字）

Engine ID

リモートデバイス上に設定されているエンジン ID を表示します（P45 参照）

Model

セキュリティモデル（v1,v2c,v3　初期設定：v1）

Lebel

セキュリティレベル

- noAuthNoPriv ー 認証も暗号化も行いません（v3 セキュリティモデルの初期設定値）
- AuthNoPriv ー 認証を行いますが暗号化は行いません（v3 セキュリティモデルでのみ設定可）
- AuthPriv ー 認証と暗号化を行います（v3 セキュリティモデルでのみ設定可）

Authentication

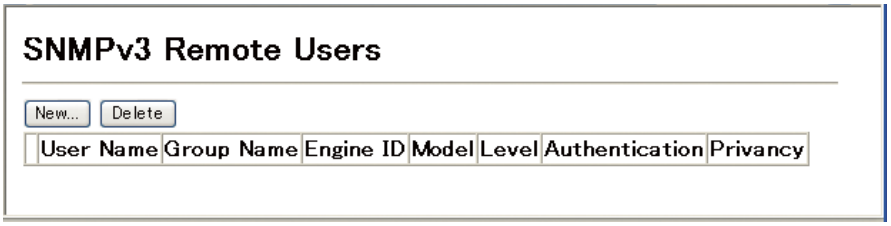
認証用プロトコルの選択。MD5 または SHA（初期設定：MD5）

Privacy

暗号化プロトコル。DES56bit のみ使用可。

設定方法

[SNMP] → [SNMPv3 Remote Users] をクリックします。新しいユーザーを登録する場合、[New...] をクリックします。[SNMPv3 Remote Users--New] のページが表示されます。(User Name)(Group Name)(Security Model)(Security Lebel)(User Authentication)(Data Privacy) の設定を行い、[Add] をクリックします。[SNMPv3 Remote Users] のページに戻り、登録したユーザーがリストに追加されます。ユーザーを削除する場合には、削除したいユーザー名のチェックボックスへチェックを入れ、[Delete] をクリックします。



SNMPv3 グループの設定

SNMPv3 グループは、特定のセキュリティモデルに属するユーザーの集合です。グループはそのグループに属する全ユーザーのアクセスポリシーを定義します。アクセスポリシーによって、読み取り、書き込み、または受信できるトラップ通知の制限が行われます。

設定・表示項目

Group Name

グループ名（1-32 文字）

Model

セキュリティモデル（1,v2c,v3）

Lebel

- noAuthNoPriv ー 認証も暗号化も行いません
- AuthNoPriv ー 認証を行いますが暗号化は行いません（v3 セキュリティモデルでのみ設定可）
- AuthPriv ー 認証と暗号化を行います（v3 セキュリティモデルでのみ設定可）

Read View

Read アクセスのビューを設定します

Write View

Wite アクセスのビューを設定します

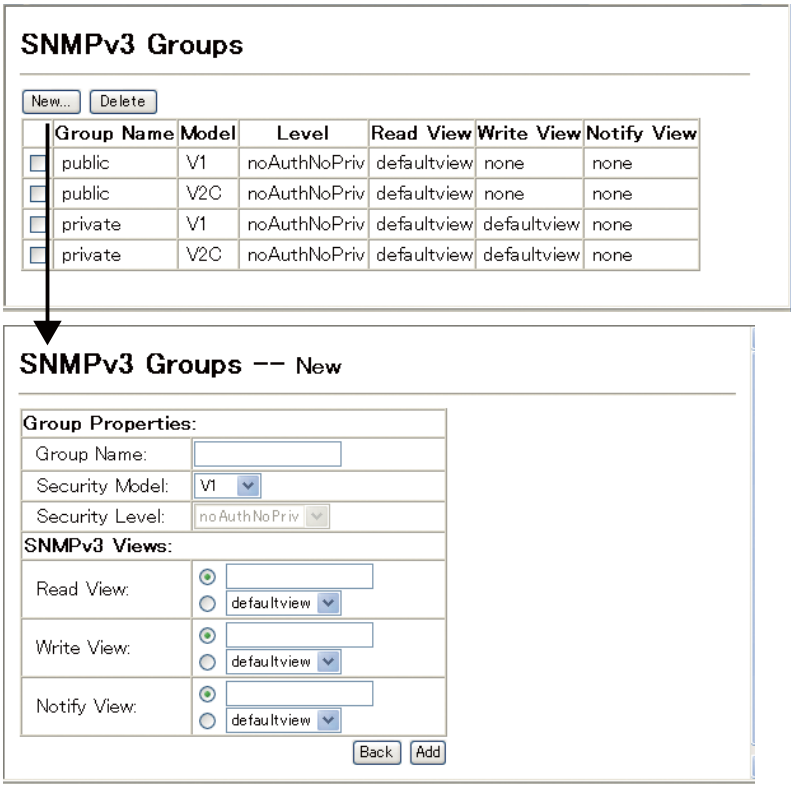
Notify View

通知ビューを設定します。下表にてサポートする通知メッセージを示します。

Object Label	Object ID
RFC1493Traps	
newRoot	1.3.6.1.2.1.17.0.1
topologyChange	1.3.6.1.2.1.17.0.2
SNMPv2 Traps	
coldStart	1.3.6.1.6.3.1.1.5.1
warmStart	1.3.6.1.6.3.1.1.5.2
linkDown	1.3.6.1.6.3.1.1.5.3
linkUp	1.3.6.1.6.3.1.1.5.4
authentication Failure	1.3.6.1.6.3.1.1.5.5
RMON Events(V2)	
risingAlarm	1.3.6.1.2.1.16.0.1
fallingAlarm	1.3.6.1.2.1.16.0.2
Private Traps	
swPowerStatus Change Trap	1.3.6.1.4.1.202.20.56.63.2.1.0.1
swIpFilter RejectTrap	1.3.6.1.4.1.202.20.56.63.2.1.0.40

設定方法

[SNMP] → [SNMPv3 Groups] **をクリックします。新しいグループを登録する場合、**[New...] **をクリックします。**(Group Name)(Security Model)(Security Lebel)(Read View)(Write View)(Notify View) **の設定を行い、**[Add] **をクリックします。**[SNMPv3 Groups] **のページに戻り、登録したグループがリストに追加されます。グループを削除する場合には、削除したいグループ名のチェックボックスへチェックを入れ、**[Delete] **をクリックします。**



SNMPv3 ビューの設定

SNMP ビューとは、SNMP オブジェクトと、それらのオブジェクトについて使用可能なアクセス権限と対応関係を示した物です。

事前に定義されているビュー（デフォルトビュー）には全体の MIB ツリーへのアクセスが含まれます。

設定・表示項目

View Name

SNMP ビュー名（1-64 文字）

View OID Subtrees

ビューの内容が表示されます

Edit OID Subtrees

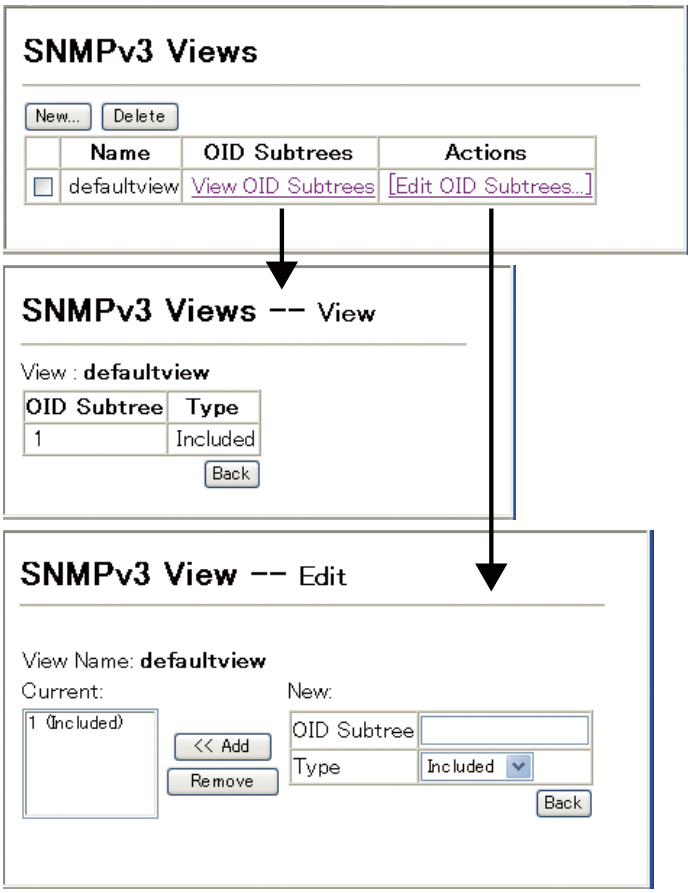
既存のビューの編集ができます

Type

[OID Subtrees] で指定した OID を、参照可能な範囲に含む（included）か含まない（excluded）かを選択します

設定方法

[SNMP] → [SNMPv3 Views] をクリックします。新しいビューを登録する場合、[New...] をクリックします。(View Name)(OID Subtree)(Type) の設定を行い、[Add] をクリックします。
設定後は [Back] で [SNMPv3 Views] のページに戻ります。
グループを削除する場合には、削除したいグループ名のチェックボックスへチェックを入れ、[Delete] をクリックします。
(OID Subtree) をクリックすると View の情報が表示されます。
編集を行う場合には (Edit OID Subtree) をクリックします。



3.5 ユーザ認証

本機の管理アクセスへは以下の方法により制限を行えます。

- **パスワード** - 本機内部において各ユーザのアクセス権の設定を行うことができます。
- **認証設定** - リモート認証サーバを利用しユーザのアクセス権の設定を行います。
- **HTTPS** - HTTPS を利用したセキュリティを確保した Web アクセスを行えます。
- **SSH** - secure shell を利用したセキュリティを確保した Telnet アクセスを行えます。
- **ポートセキュリティ** - 各ポートに MAC アドレスによるセキュリティを提供します。
- **IEEE802.1x** - IEEE802.1x ポート認証により各ポートのアクセスをコントロールします。
- **IP フィルタ** - Web、SNMP、Telnet への管理アクセスをフィルタリングします。

3.5.1 ユーザアカウントの設定

ゲストモードではほとんどの設定パラメータにおいて、表示しか行うことができません。管理者モードでは設定パラメータの変更も行うことができます。

安全のため、管理者用パスワードは初期設定からの変更を行ない、パスワードは安全な場所に保管して下さい。

初期設定では、ゲストモードのユーザ名・パスワードは共に「guest」、管理者モードのユーザ名・パスワードは「admin」です。

ユーザ名は CLI を使用した場合のみ利用、変更可能です。

設定・表示項目

Accout List

登録されているユーザアカウントと、各アカウントに関連付けられているアクセスレベルのリスト（初期設定：admin 及び guest)

New Account

新たに追加するユーザアカウント情報

- **User Name** ― ユーザ名 (最大文字数：8 文字、最大ユーザ数：16 人)
- **Access Level** ― ユーザのアクセスレベル (オプション：Normal, Privileged)
- **Password** ― ユーザのパスワード（範囲：0-8 文字、大文字と小文字は区別されます）

Change Password

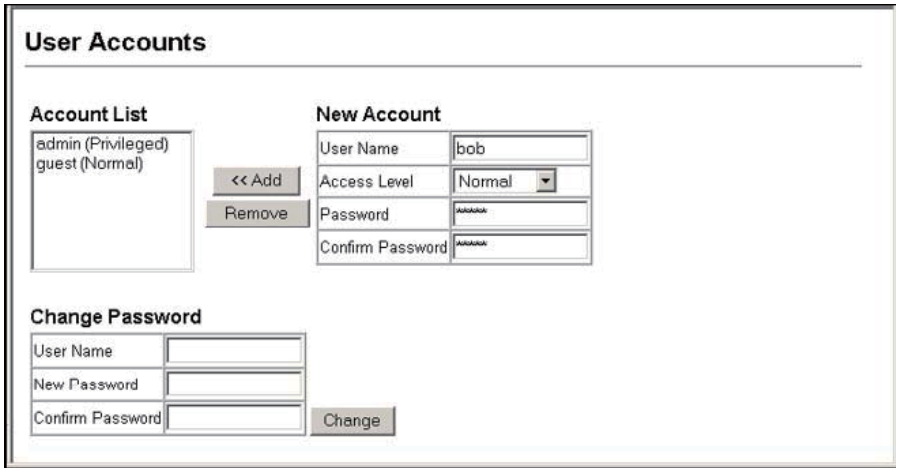
既存ユーザアカウントのパスワードを変更します。

Add/Remove

ユーザアカウントのリストへの追加、又はリストからの削除を行います。

設定方法

[Security] → [User Accounts] **をクリックします。新規のユーザアカウントを設定するには、ユーザ名** (User Name)**、ユーザのアクセスレベル** (Access Level) **を設定します。パスワード** (Password) **を入力し、再確認のためにパスワード** (Confirm Password) **を再度入力します。** [Add] **をクリックすると、新規のユーザアカウントは保存され** [Account List] **欄に追加されます。既存ユーザアカウントのパスワードを変更する場合は、**[Change Password] **欄にユーザ名** (User Name) **及び新たなパスワード** (New Password) **を入力し、再確認のためにパスワード** (Confirm Password) **を再度入力して** [Change] **をクリックします。**

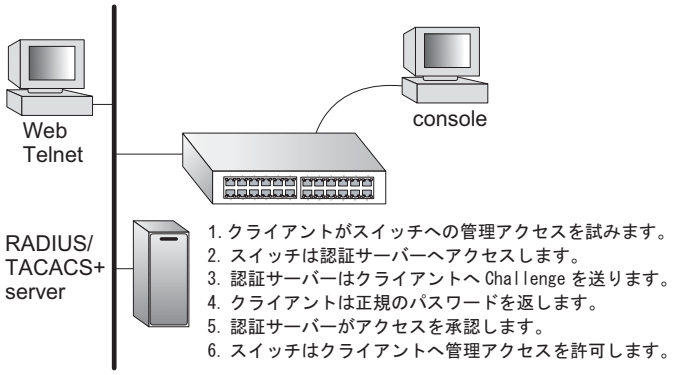


3.5.2 ローカル / リモート認証ログオン設定

本機ではユーザ名とパスワードベースによる管理アクセスの制限を行うことができます。本機内部でのアクセス権の設定が行える他、RADIUS **及び** TACACS+ **によるリモート認証サーバでの認証も行うことができます。**

RADIUS **及び** TACACS+ **は、ネットワーク上の** RADIUS **対応及び** TACACS+ **対応のデバイスのアクセスコントロールを認証サーバにより集中的に行うことができます。認証サーバは複数のユーザ名 / パスワードと各ユーザの本機へのアクセスレベルを管理するデータベースを保有しています。**

RADIUS **ではベストエフォート型の** UDP **を使用しますが、**TACACS+ **では接続確立型通信の** TCP **を使用します。また、**RADIUS **ではサーバへのアクセス要求パケットのパスワードのみが暗号化されますが、**TACACS+ **は全てのパケットが暗号化されます。**



機能解説

- 初期設定では、管理アクセスは本機内部の認証データベースを使用します。外部の認証サーバを使用する場合、認証手順とリモート認証プロトコルの対応したパラメータの設定を行う必要があります。ローカル、RADIUS 及び TACACS+ 認証では、コンソール接続、Web インタフェース及び Telnet 経由のアクセス管理を行います。
- RADIUS 及び TACACS+ 認証では、各ユーザ名とパスワードに対し、アクセスレベル (Pribilege Level) を設定します。ユーザ名、パスワード及びアクセスレベル (Pribilege Level) は認証サーバ側で設定を行います。
- 最大 3 つの認証方法を利用することができます。例えば (1) RADIUS、(2) TACACS、(3) Local と設定した場合、初めに RADIUS サーバでユーザ名とパスワードの認証を行います。RADIUS サーバが使用できない場合には、次に TACACS+ サーバを使用し、その後本体内部のユーザ名とパスワードによる認証を行います。

設定・表示項目

Authentication

認証方式を選択します。

ー **Local** ― 本機内部においてユーザ認証を行います。

ー **RADIUS** ― RADIUS サーバによるユーザ認証を行います。

ー **TACACS** ― TACACS+ サーバによるユーザ認証を行います。

RADIUS 設定

Global

RADIUS サーバの設定をグローバルに適用します。

ServerIndex

設定する RADIUS サーバを、5 つのうち 1 つ指定します。本機は、表示されたサーバの順に認証プロセスを実行します。認証プロセスは、サーバがそのユーザのアクセスを許可または拒否した時点で終了します。

Authentication Port Number

認証メッセージに使用される、UDP ポート番号（1-65535、初期設定 :1812）

Accounting Port Number

アカウンティングメッセージに使用される UDP ポート番号（1-65535、初期設定 :1813）

Secret Text String

ログインアクセス認証に使用される暗号キー。間にスペースを入れないで下さい（最大文字数 :20 文字）

Number of Server Transmits

RADIUS サーバに対し認証リクエストを送信する回数（範囲 :1-30、初期設定 :2）

Timeout for a reply

認証リクエストを再送信する前に RADIUS サーバからの応答を待つ待機時間（秒）（範囲 :1-65535、初期設定 :5）

TACACS+ 設定

Server IP Address

TACACS+ サーバの IP アドレス（初期設定 : 10.11.12.13）

Server Port Number

TACACS+ サーバで使用される TCP ポート番号（1-65535、初期設定 :49）

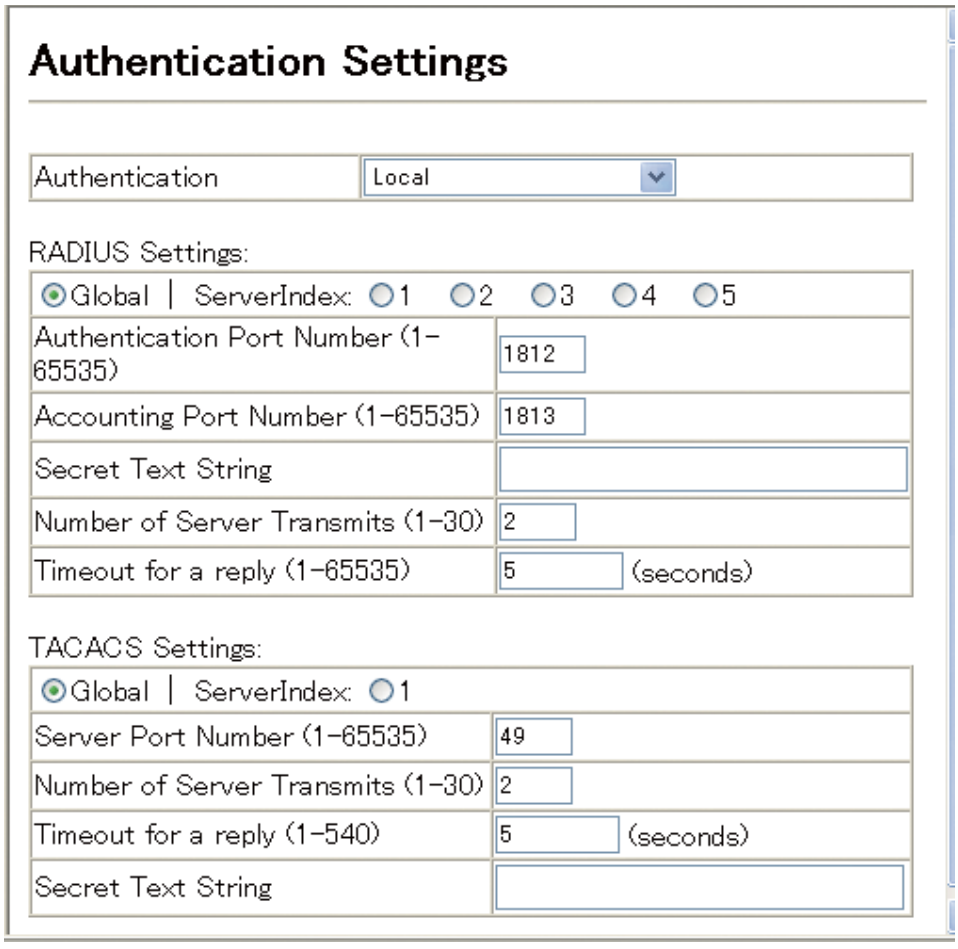
Secret Text String

ログインアクセス認証に使用される暗号キー。間にスペースを入れないで下さい。

[注意]　本機内部の認証データベースは CLI を使用し、ユーザ名とパスワードを入力することで設定が行えます。

設定方法

[Security] → [Authentication Settings] をクリックします。Authentication（認証方式）を選択し、RADIUS 及び TACACS+ を選択した場合には、それぞれの認証に必要なパラメータを入力し、[Apply] をクリックします。



3.5.3 AAA 許可とアカウンティング

オーセンティケーション、オーソライゼーション、アカウンティング（AAA）機能はスイッチ上でアクセス制御を行うための主要なフレームワークを規定します。この 3 つのセキュリティ機能は下のようにまとめることができます。

- オーセンティケーション：ネットワークへのアクセスを要求するユーザーを認証します。
- オーソライゼーション：ユーザーが特定のサービスにアクセスできるかどうかを決定します。
- アカウンティング：ネットワーク上のサービスにアクセスしたユーザーに関する報告、監査、請求を行います。

AAA 機能を使用するにはネットワーク上で RADIUS サーバー、もしくは TACACS+ サーバーを構成することが必要です。セキュリティサーバーはシーケンシャルグループとして定義され、特定のサービスへのユーザーアクセスを制御するために適用されます。例えば、スイッチがユーザーを認証しようと試みた場合、最初にリクエストが定義されたグループ内のサーバーに送信されます。応答がない場合、第 2 のサーバーにリクエストが送信され、さらに応答がない場合、次のサーバーにリクエストが送信されます。どこかの時点で認証が成功するか失敗した場合、プロセスは停止します。

スイッチは下記のような AAA 機能をサポートしています。

- スイッチを通してネットワークにアクセスした IEEE802.1x で認証されたユーザーをアカウンティングします。
- コンソールと Telnet を通してスイッチ上の管理インターフェースにアクセスするユーザーをアカウンティングします。
- 特定の CLI 特権レベルに入ったユーザーにコマンドをアカウンティングします。
- コンソールと Telnet を通してスイッチ上の管理インターフェースにアクセスするユーザーのオーソライゼーションを行います。

スイッチ上の AAA 機能の設定を行うために、下の手順を実行する必要があります。

（1）RADIUS サーバー、TACACS+ サーバーへアクセスするための値を設定します。

（2）サービスのアカウンティング、オーソライゼーション機能をサポートするため、RADIUS サーバーと TACACS+ サーバーのグループを定義します。

（3）適用したいそれぞれのサービスのアカウンティング、オーソライゼーションのメソッド名を定義し、使用する RADIUS サーバー、もしくは TACACS+ サーバーのグループを指定します。

（4）ポートもしくはラインインターフェースにメソッド名を適用します。

[注意] 上の説明は RADIUS サーバーと TACACS+ サーバーが既に AAA 機能をサポートしていることを前提にしています。RADIUS サーバーと TACACS+ サーバーの設定については、各サーバー、ソフトウェアのマニュアルを参照してください。

AAA RADIUS グループ設定

この画面ではアカウンティング、オーソライゼーションに使用する RADIUS サーバーについて設定します。

設定・表示項目

Group Name

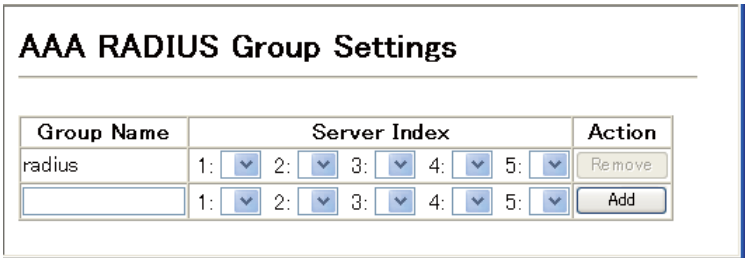
RADIUS サーバーのグループ名を指定します（範囲：1 ～ 255 文字）

Server Index

RADIUS サーバーと、グループ内で使用する順序を指定します（範囲：1 ～ 5）。
RADIUS サーバーのインデックスを指定したとき、サーバーのインデックスは事前に設定されていなくてはいけません。

設定方法

[Security] → [AAA] → [Radius Group Settings] をクリックします。



AAA TACACS+ グループ設定

この画面ではアカウンティング、オーソライゼーションに使用する TACACS+ サーバーについて設定します。

設定・表示項目

Group Name

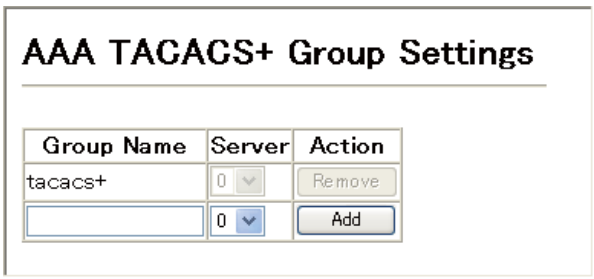
TACACS+ サーバーのグループ名を指定します（範囲：1 ～ 255 文字）

Server Index

グループに使用する TACACS+ サーバーを指定します（範囲：1）
TACACS+ サーバーのインデックスを指定したとき、サーバーのインデックスは事前に設定されていなくてはいけません。

設定方法

[Security] → [AAA] → [TACACS+ Group Settings] をクリックします。



AAA アカウンティングの設定

この画面では課金やセキュリティ目的でリクエストされたサービスのアカウンティングを有効にするかどうかを設定します。

設定・表示項目

Method Name

サービス要求のアカウンティングメソッドを設定します。"default" メソッドは他に定義されたメソッドがない場合、リクエストされたサービスに使用されます。（範囲：1 ～ 255 文字）

Service Request

サービスを 802.1x（ユーザーアカウンティング）か Exec（ローカルコンソール、Telnet、SSH 接続）のどちらかを指定します。

Accounting Notice

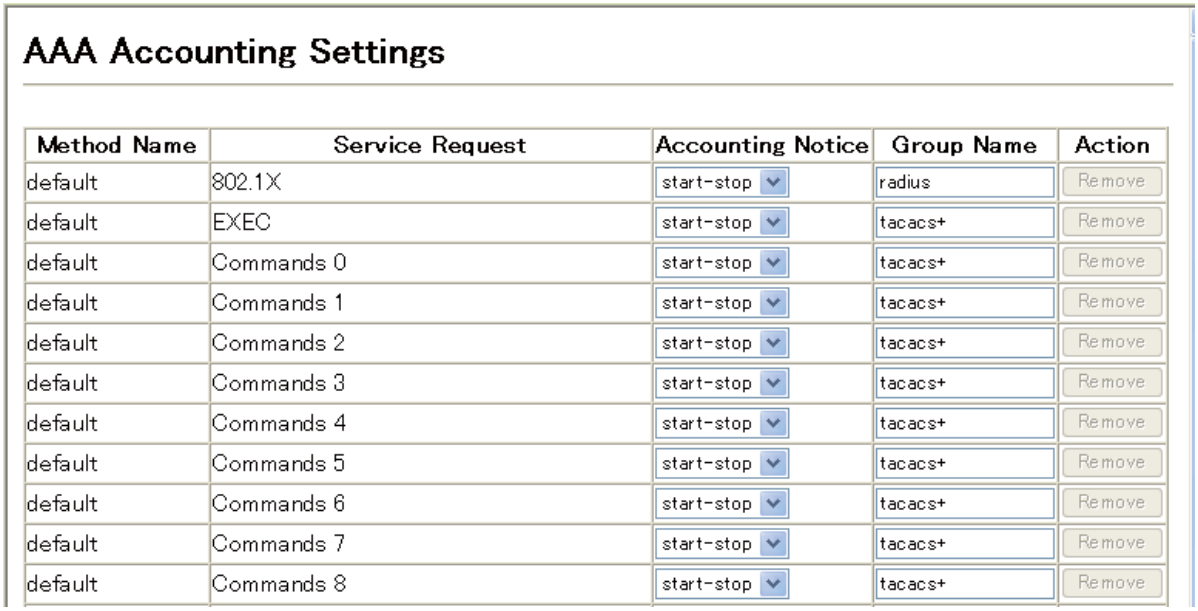
ログインした時点からログアウトした時点までのユーザーの活動を記録します。

Group Name

アカウンティングサーバーのグループを設定します（範囲：1 ～ 255 文字）。グループ名 "radius" と "tacacs+" は設定されたすべての RADIUS ホスト、TACACS ホストに指定されます。どの名前のグループも RADIUS、TACACS+ グループ設定画面で設定されたサーバーグループを参照します。

設定方法

[Security] → [AAA] → [Accounting] → [Settings] をクリックします。



AAA アカウンティングアップデート

この画面ではアカウンティングアップデートをアカウンティングサーバーに送信する間隔を設定します。

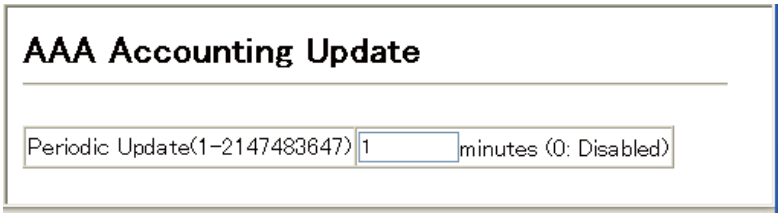
設定・表示項目

Periodic Update

ローカルアカウンティングサービスが情報をアカウンティングサーバーにアップデートする間隔を指定します（範囲：1 ～ 2147483647 分、デフォルトでは無効）

設定方法

[Security] → [AAA] → [Accounting] → [Periodic Update] をクリックします。



AAA アカウンティング 802.1x ポート設定

この画面ではインターフェースに特定のアカウンティング方法を割り当てます。

設定・表示項目

Port/Trunk

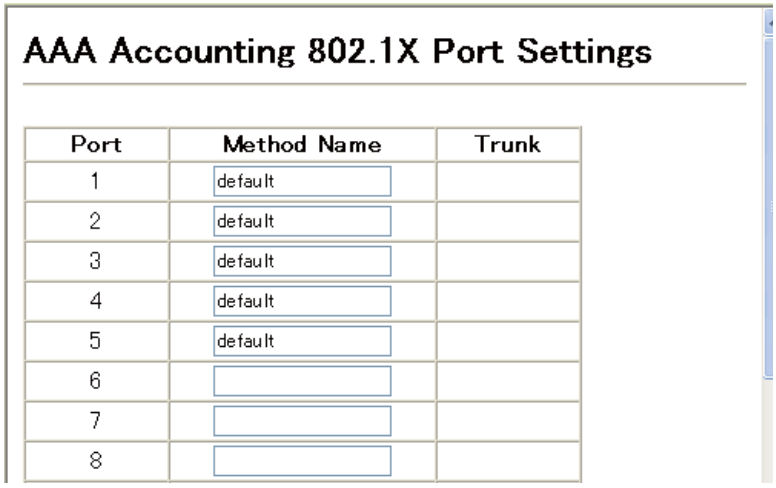
ポート、トランクポートの番号を表示します。

Method Name

インターフェースに割り当てるユーザー定義のメソッド名を指定します（範囲：1 ～ 255 文字）

設定方法

[Security] → [AAA] → [Accounting] → [802.1X Port Settings] をクリックします。



AAA アカウンティング Exec コマンド

この画面では CLI 特権モードに入るコマンドを割り当てるメソッド名を設定します。

設定・表示項目

Commands Privilege Level

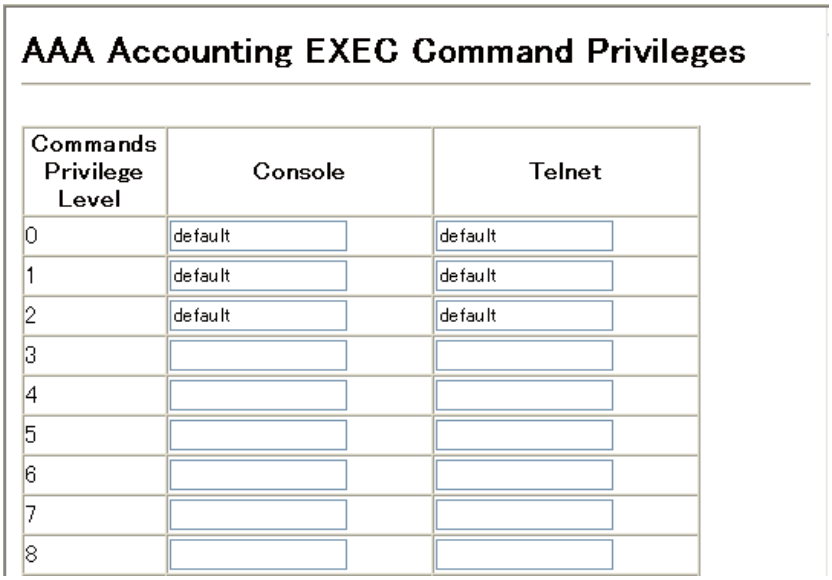
CLI の特権レベルです（範囲：0 ～ 15）

Console/Telnet

CLI 特権モードに入るコマンドを割り当てるユーザー定義のメソッド名を指定します（範囲：1 ～ 255 文字）

設定方法

[Security] → [AAA] → [Accounting] → [Command Privilges] をクリックします。



AAA アカウンティング Exec 設定

この画面はコンソール接続と Telnet 接続に割り当てるメソッド名を設定します。

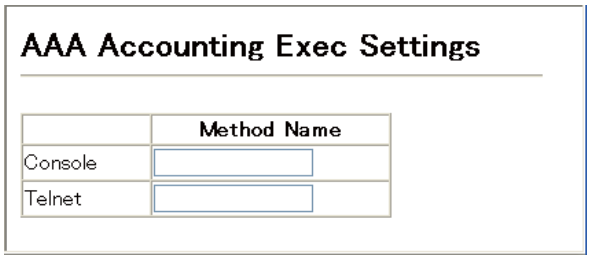
設定・表示項目

Method Name

コンソール接続と Telnet 接続に割り当てるユーザー定義のメソッド名を指定します。

設定方法

[Security] → [AAA] → [Accounting] → [Exec Settings] をクリックします。



AAA アカウンティングサマリ

設定・表示項目

AAA Accounting Summary

Accounting Type

アカウンティングサービスを表示します。

Method List

ユーザー定義、もしくはデフォルトのアカウンティングメソッドを表示します。

Group List

アカウンティングサーバーのグループを表示します。

Interface

ルールを適用するポート、トランクポートを表示します (この欄はアカウンティング方法、関連付けられたサーバーグループがインターフェースに割り当てられていないとき空欄になります)

AAA Accounting Statistics Summary

User Name

登録されたユーザー名を表示します。

Interface

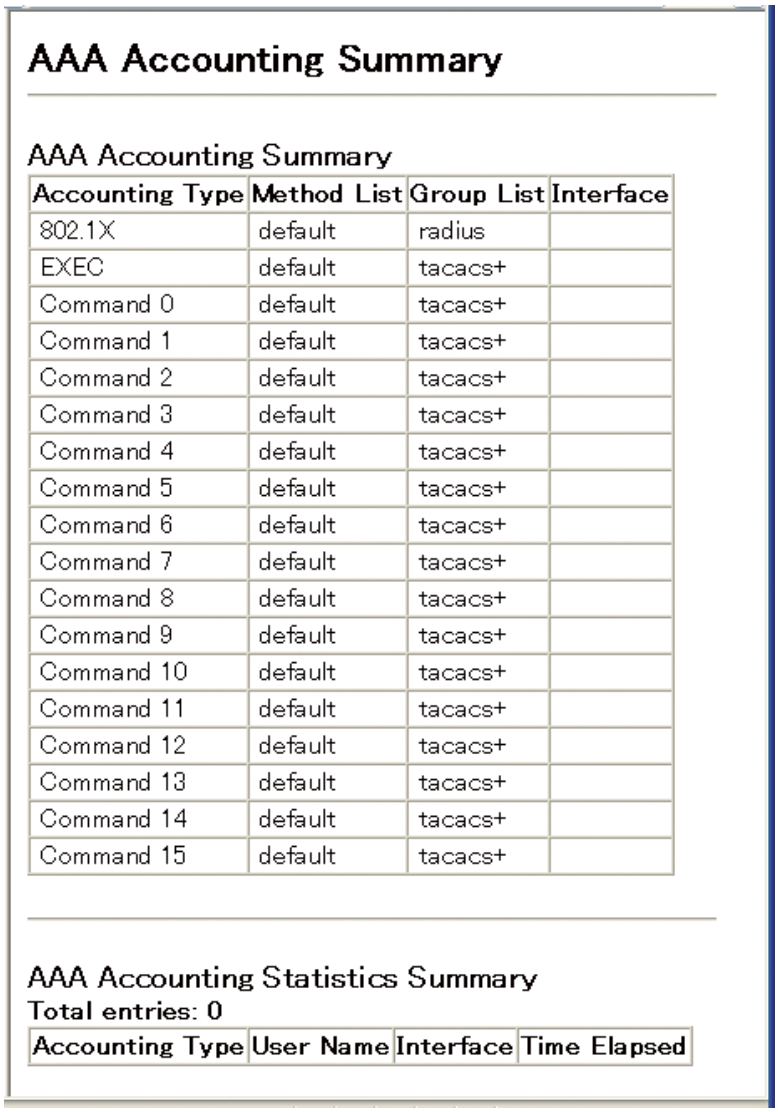
このユーザーがスイッチにアクセスする受信ポートの番号を表示します。

Time Elapsed

このエントリが有効になった時間の長さを表示します。

設定方法

[Security] → [AAA] → [Summary] **をクリックします。**



認可設定

この画面では、ユーザーが特定のサービスにアクセスしたことを証明する機能の設定を行います。

設定・表示項目

Method Name

サービス要求のオーソライゼーション方法を指定します。"default" メソッドは他のメソッドが定義されていない場合、リクエストされたサービスに使用されます（範囲：1 ～ 255 文字）

Service Request

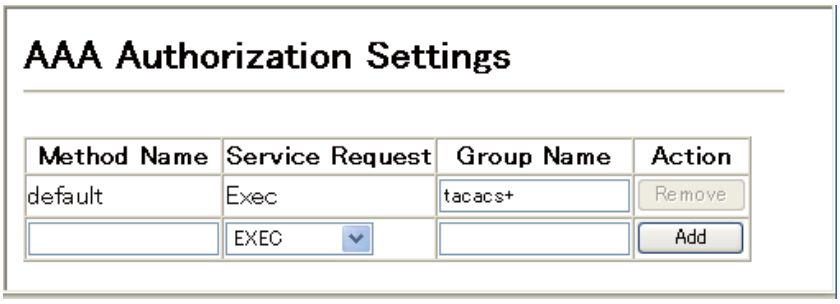
ローカルコンソール接続、Telnet 接続へのオーソライゼーションを設定します。

Group Name

オーソライゼージョンサービスグループを指定します（範囲：1 ～ 255 文字）。グループ名 "tacacs+" はすべての TACACS+ ホストに設定されます。他のグループ名は TACACS+ グループの設定ページで指定したサーバーグループを参照します。オーソライゼーションは TACACS+ サーバーのみサポートします。

設定方法

[Security] → [AAA] → [Authorization] → [Settings] をクリックします。



認可 EXEC 設定

この画面では、コンソール接続と Telnet 接続に適用するオーソライゼーションメソッド名を設定します。

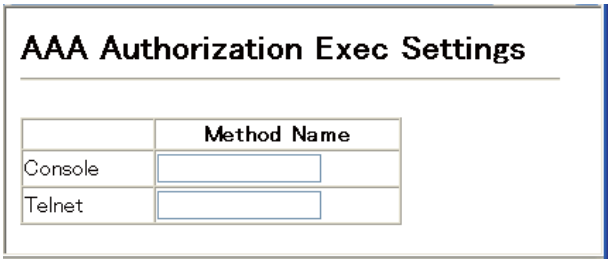
設定・表示項目

Method Name

コンソール接続と Telnet 接続にユーザー定義のメソッド名を割り当てます。

設定方法

[Security] → [AAA] → [Authorization] → [Exec Settings] をクリックします。



認可サマリ

この画面では、設定したオーソライゼーションメソッドとメソッドを割り当てたインターフェースについて表示します。

設定・表示項目

Authorization Type

オーソライゼーションサービスの種類を表示します。

Method List

ユーザー定義、もしくはデフォルトのオーソライゼーションメソッドを表示します。

Group List

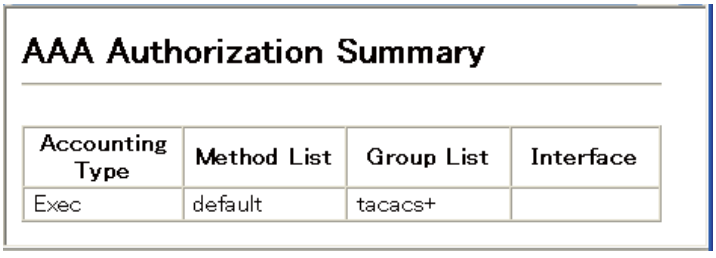
オーソライゼーションサービスグループを表示します。

Interface

オーソライゼーションメソッドを適用したコンソール、もしくは Telnet のインターフェースを表示します（この欄はオーソライゼーションメソッド、または関連付けられたサーバーグループが割り当てられていない場合、空欄になります）

設定方法

[Security] → [AAA] → [Authorization] → [Summary] をクリックします。



3.5.4 HTTPS 設定

Secure Socket Layer(SSL) を使った Secure Hypertext Transfer Protocol(HTTPS) によって本機の Web インタフェースに暗号化された安全な接続を行うことができます。

機能解説

- HTTP 及び HTTPS サービスは共に使用することはできます。但し、HTTP 及び HTTPS サービスで同じ UDP ポート番号を設定することはできません。
- HTTPS を使用する場合、URL は HTTPS: から始まる表示がされます。
  例 :[https://device: ポート番号]
- HTTPS のセッションが開始されると以下の手順で接続が確立されます。
  －クライアントはサーバのデジタル証明書を使用し、サーバを確認します。
  －クライアントとサーバが接続用のセキュリティプロトコルの調整を行います。
  －クライアントとサーバは、データを暗号化し解読するためのセッション・キーを生成します。
- HTTPS を使用した場合、クライアントとサーバは安全な暗号化された接続を行います。Internet Explorer 5.x 又は NetscapeNavigator 4.x のステータスバーには鍵マークが表示されます。
- "HTTP をサポートしている Web ブラウザ及び OS は以下の通りです。

Web ブラウザ	OS
Internet Explorer 5.0 以上	Windows 98、Windows NT (サービスパック 6A)、Windows 2000、Windows XP
Netscape Navigator 4.76 以上	Windows 98、Windows NT (サービスパック 6A)、Windows 2000、Windows XP、Solaris 2.6

※ 安全なサイトの証明を指定するためには、P68 「サイト証明書の設定変更」を参照して下さい。

設定・表示項目

HTTPS Status

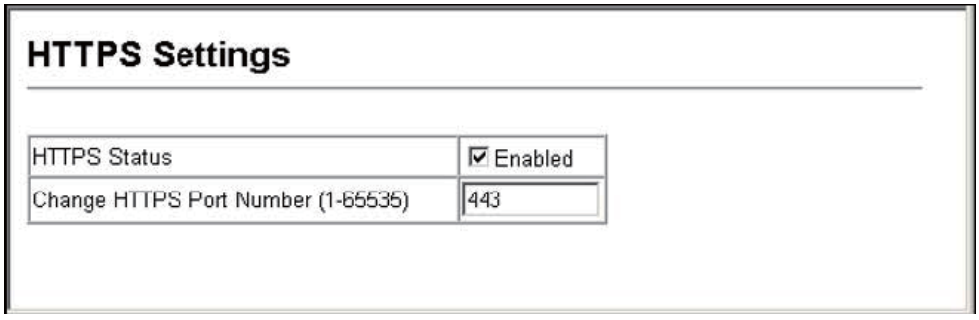
HTTPS サーバ機能を有効または無効に設定します（初期設定 : 有効 (Enabled)）

Change HTTPS Port Number

HTTPS 接続に使用される UDP ポートを指定します（初期設定：443）

設定方法

[Security] → [HTTPS Settings] をクリックします。HTTPS を有効にするためには、HTTPS Status で Enabled を選択します。ポート番号を指定し、[Apply] をクリックします。



サイト証明書の設定変更

HTTPS を使用して Web インタフェースにログインする際に、SSL を使用します。初期設定では認証機関による認証を受けていないため、Netscape 及び Internet Explorer 画面で安全なサイトとして認証されていないという警告が表示されます。この警告を表示させないようにするためには、認証機関から個別の証明書を入手し、設定を行う必要があります。

[注意] 初期設定の証明書は個々のハードウェアで固有の認証キーではありません。より高度なセキュリティ環境を実現するためには、できるだけ早くで独自の SSL 証明書を取得し設定を行う事を推奨します。

個別の証明書を取得した場合には、TFTP サーバを使用してコンソール接続の CLI により既存の証明書と置き換えます。証明書の設定を行う CLI の手順は以下の通りです。

```
Console#copy tftp https-certificate 3-21
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] 証明書の変更を行った後に本機の再起動を行わないと、新しい証明書は有効になりません。再起動は CLI を使用し以下の手順で行います。

```
Console#reload
```

3.5.5 Secure Shell 設定

Secure Shell (SSH) は、それ以前からあったバークレーリモートアクセスツールのセキュリティ面を確保した代替としてサーバ / クライアントアプリケーションを含んでいます。また、SSH は Telnet に代わる本機へのセキュア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 プロトコルによって本機と接続する場合、本機はアクセス認証のためにローカルのユーザ名およびパスワードと共にクライアントが使用する公開暗号キーを生成します。さらに、SSH では本機と SSH を利用する管理端末の間の通信をすべて暗号化し、ネットワーク上のデータの保護を行ないます。

[注意] SSH 経由での管理アクセスを行なうためには、クライアントに 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] 本機では SSH Version1.5 と 2.0 をサポートしています。

機能解説

本機の SSH サーバはパスワード及びパブリックキー認証をサポートしています。SSH クライアントによりパスワード認証を選択した場合、認証設定ページで設定したパスワードにより本機内、RADIUS、TACACS+ のいずれかの認証方式を用います。クライアントがパブリックキー認証を選択した場合には、クライアント及び本機に対して認証キーの設定を行なう必要があります。

公開暗号キー又はパスワード認証のどちらかを使用するに関わらず、本機上の認証キー（SSH ホストキー）を生成し、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で設定を行ないます。

（1）**ホストキーペアの生成** ― SSH ホストキー設定ページでホスト パブリック / プライベートキーのペアを生成します。

(2) **ホスト公開キーのクライアントへの提供** ― 多くの SSH クライアントは、本機との自動的に初期接続設定中に自動的にホストキーを受け取ります。そうでない場合には、手動で管理端末のホストファイルを作成し、ホスト公開キーを置く必要があります。ホストファイル中の公開暗号キーは以下の例のように表示されます。

10.1.0.54 1024 35
156849954018676692593339467750546173253136748908365472541502024559319986854435836165199992332978176606583095610825913212890233765468017262725714134287629413011961955667825956641048695742788814620651941746772984865468615717739390164779355942303577413098022737087794545240839717526463580581767167095748047761170

(3) **クライアント公開キーの本機への取り込み** ― 313 ページの「copy」を参照コマンドを使用し、SSH クライアントの本機の管理アクセスに提供される公開キーを含むファイルをコピーします。クライアントへはこれらのキーを使用し、認証が行なわれます。現在のファームウェアでは以下のような UNIX 標準フォーマットのファイルのみ受け入れることが可能です。

1024 35134108168560989392104094492015542534763164192187295892114317388005553616163105177594083868631109291232226828519254374603100937187721199696317813662774141689851320491172048303392543241016379975923714490119380060902539484084827178194372288402533115952134861022902978982721353267131629432532818915045306393916643 steve@192.168.1.19

(4) **オプションパラメータの設定** ― SSH 設定ページで、認証タイムアウト、リトライ回数、サーバキーサイズなどの設定を行なってください。

(5) **SSH の有効化** ― SSH 設定ページで本機の SSH サーバを有効にして下さい。

(6) **Challenge/Response 認証** ― SSH クライアントが本機と接続しようとした場合、SSH サーバはセッションキーと暗号化方式を調整するためにホストキーペアを使用します。本機上に保存された公開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アクセスすることができます。

以下のような手順で認証プロセスが行なわれます。

a. クライアントが公開キーを本機に送ります。

b. 本機はクライアントの公開キーとメモリに保存されている情報を比較します。

c. 一致した場合、公開キーを利用し本機はバイトの任意のシーケンスを暗号化し、その値をクライアントに送信します。

d. クライアントはプライベートキーを使用してバイトを解読し、解読したバイトを本機に送信します。

e. 本機は、元のバイトと解読されたバイトを比較します。2 つのバイトが一致した場合、クライアントのプライベートキーが許可された公開キーに対応していることを意味し、クライアントが認証されます。

[注意] **パスワード認証と共に SSH を使用する場合にも、ホスト公開キーは初期接続時又は手動によりクライアントのホストファイルに与えられます。但し、クライアントキーの設定を行なう必要はありません。**

[注意] **SSH サーバは Telnet とあわせて最大 4 クライアントの同時セッションをサポートします。**

SSH サーバ設定

認証用の SSH **サーバの設定**

設定・表示項目

SSH Server Status

SSH **サーバ機能を有効または無効にします（初期設定** : **無効** (Disabled)**）**

Version

Secure Shell **のバージョンナンバー。**Version 2.0 **と表示されていますが、**Version1.5 **と** 2.0 **の両方をサポートしています。**

SSH authentication timeout

SSH **サーバの認証時に認証端末からの応答を待つ待機時間（**1-120**（秒）、初期設定** :120**（秒））**

SSH authentication Retries

認証に失敗した場合に、認証プロセスを再度行うことができる回数。設定した回数を超えると認証エラーとなり、認証端末の再起動を行う必要があります（1-5**、初期設定** :3 **回）**

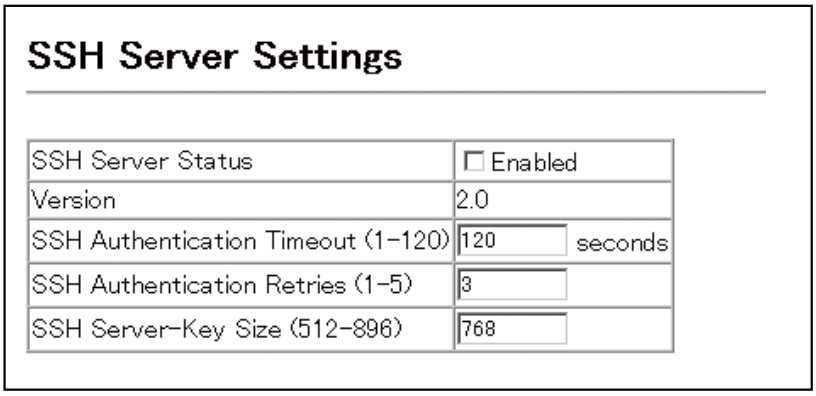
SSH Server-Key Size

SSH **サーバのキーサイズ（設定範囲：**512-896 **ビット、初期設定** :768 **ビット）**

- **サーバキーはプライベートキーで、本機以外とは共有しません。**
- SSH **クライアントと共有されるホストキーは、**1024 **ビット固定です。**

設定方法

[Security] → [SSH Settings] **をクリックします。**SSH **を有効にし、必要に応じて各項目の設定を行い、**[Apply] **をクリックします。**SSH **サーバを有効にする際は、事前に** SSH Host-Key Settings page **で** host key pair **を生成する必要があります。**



ホストキーペアの生成

ホスト公開 / プライベートキーペアは本機と SSH クライアント間のセキュアな接続のために使用されます。
キーペアが生成された後、ホスト公開キーを SSH クライアントに提供し、上記の機能解説の通りにクライアントの公開キーを本機に取り込む必要があります。

設定・表示項目

Public-Key of Host-Key

ホストへのパブリックキー

- **RSA**: 最初のフィールドはホストキーのサイズ (1024) を表しています。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 (65537)、最後の値はエンコードされた係数を表しています。
- **DSA**: 最初のフィールドはデジタル署名標準(DSS)に基づく SSHによって私用される暗号化方法を表示します。最後の値はエンコードされた係数を表します。

Host-Key Type

キータイプは（公開キー、プライベートキーの）ホストキーペアを生成するために使用されます（設定範囲：RSA, DSA, Both、初期設定：RSA）
クライアントが本機と最初に接続を確立する場合、SSH サーバはキー交換のために RSA 又は DSA を使用します。その後、データ暗号化に DES(56-bit) 又は 3DES(168 -bit) のいずれかを用いるためクライアントと調整を行ないます。

Save Host-Key from Memory to Flash

ホストキーを RAM からフラッシュメモリに保存します。ホストキーペアは初期設定では RAM に保存されています。ホストキーペアを生成するには、事前にこのアイテムを選択する必要があります。

Generate

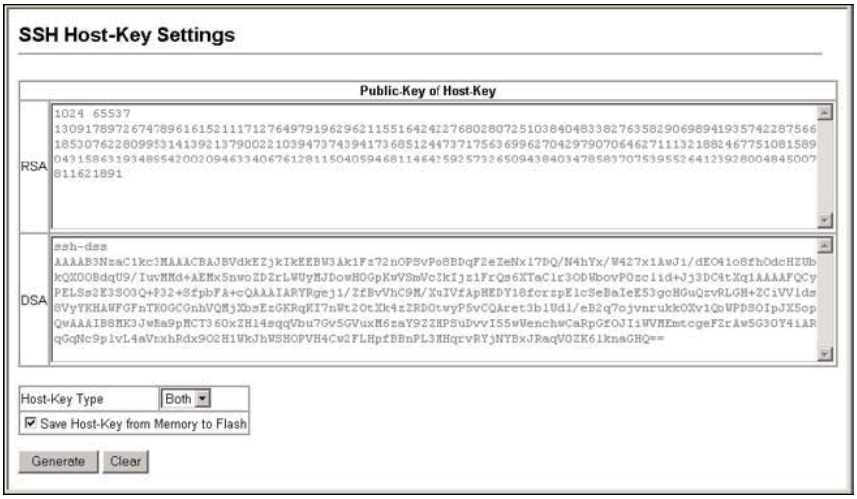
ホストキーペアを生成します。SSH サーバ設定ページで SSH サーバを有効にする前に、ホストキーペアを生成する必要があります。

Clear

RAM 及びフラッシュメモリの両方に保存されているホストキーを削除します。

設定方法

[Security] → [SSH Host-Key Settings] をクリックします。ドロップダウンボックスからホストキータイプ (host-key type) を選択し、必要に応じて save the host key from memory to flash にチェックを入れます。その後、[Generate] をクリックし、キーの生成を行ないます。



3.5.6 ポートセキュリティの設定

ポートセキュリティは、ポートに対しそのポートを使用しネットワークにアクセスする事ができるデバイスの MAC アドレスを設定し、その他の MAC アドレスのデバイスではネットワークへのアクセスを行えなくする機能です。

ポートセキュリティを有効にした場合、本機は有効にしたポートにおいて MAC アドレスの学習を停止します。本機に入って来た通信のうち、ソースアドレスが動的・静的なアドレステーブルに登録済みの MAC アドレスの場合にのみ、そのポートを利用したネットワークへのアクセスを行うことができます。登録されていない不正な MAC アドレスのデバイスがポートを使用した場合、侵入は検知され、自動的にポートを無効にし、トラップメッセージの送信を行います。

ポートセキュリティを使用する場合、ポートに許可する MAC アドレスの最大数を設定し、動的に < ソース MAC アドレス、VLAN> のペアをポートで受信したフレームから学習します。P119 「動的アドレステーブルの設定」を使用し、入力により MAC アドレスを設定することもできます。ポートに設定された最大 MAC アドレス数に達すると、ポートは学習を終了します。アドレステーブルに保存された MAC アドレスは保持され、時間の経過により消去されることはありません。これ以外のデバイスがポートを利用しようとしても、スイッチにアクセスすることはできません。

機能解説

- セキュリティポートに設定できるポートは、以下の制限があります。

  －ポートモニタリングに使用できません。
  －マルチ VLAN ポートにはできません。
  － LACP 又は静的トランクポートに設定できません。
  － HUB などネットワーク接続デバイスは接続しないで下さい。

- 初期設定では、セキュリティポートへのアクセスを許可している最大 MAC アドレス数は "0" です。セキュリティポートへのアクセスを許可するためには、最大 MAC アドレス数を 1-1024 のいずれかに設定する必要があります。

- セキュリティ違反によりポートが Disabled となった（シャットダウンした）場合、P100 「ポート設定」からポートの有効化を行なってください。

設定・表示項目

Port

ポート番号

Name

ポート説明

Action

- **None** ― **動作が行なわれません** (**初期設定ではこの設定になっています**)
- **Trap** ― SNMP **トラップメッセージを送信します。**
- **Shutdown** ― **ポートを無効にします。**
- **Trap and Shutdown** ― **ポートを無効にし、**SNMP **トラップメッセージを送信します。**

Security Status

ポートセキュリティの有効 / 無効

初期設定：無効 (Disabled)

Max MAC Count

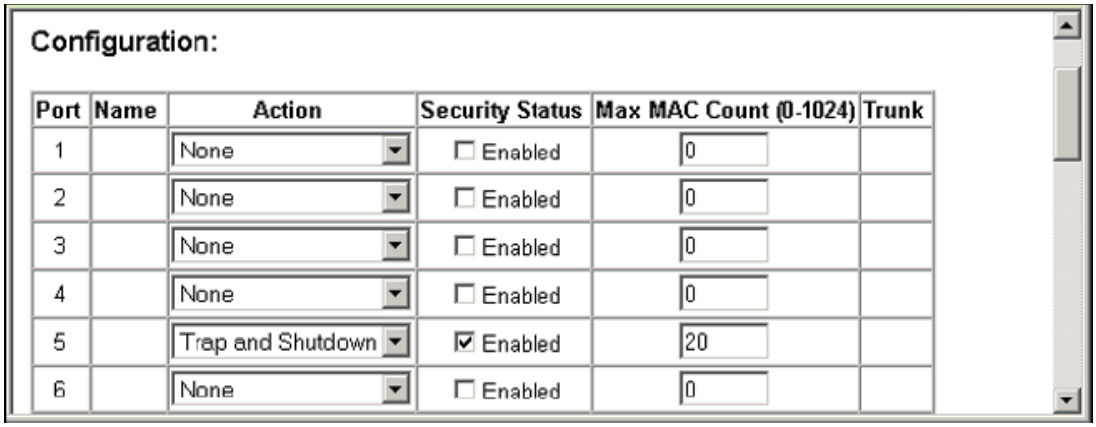
ポートが学習可能な MAC **アドレス数（設定範囲：**0-1024、0 **は学習の無効）**

Trunk

ポートがトランクされている場合のトランク番号

設定方法

[Security] → [Port Security] **をクリックします。ポートのセキュリティを有効にするには、設定を行うポート番号の** Action **を選択し、**Security Status **チェックボックスをオンにし、最大** MAC **アドレス数を設定し、**[Apply] **をクリックします。**

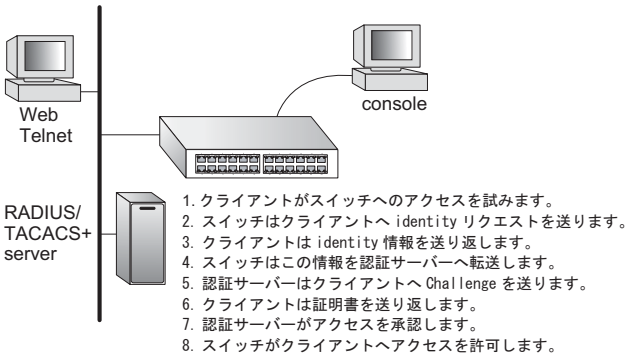


3.5.7 802.1x ポート認証

スイッチは、クライアント PC **から容易にネットワークリソースにアクセスすることができます。しかし、それによりは好ましくないアクセスを許容し、ネットワーク上の機密のデータへのアクセスが行える可能性もあります。**

IEEE802.1x(dot1x) **規格では、ユーザ** ID **及びパスワードにより認証を行うことにより無許可のアクセスを防ぐポートベースのアクセスコントロールを提供します。**

ネットワーク中のすべてのポートへのアクセスはセントラルサーバによる認証を行うことで、どのポートからでも 1 **つの認証用のユーザ** ID **及びパスワードによりユーザの認証が行えます。**



本機では Extensible Authentication Protocol over LAN (EAPOL) **によりクライアントの認証プロトコルメッセージの交換を行います。**RADIUS **サーバによりユーザ** ID **とアクセス権の確認を行います。**

クライアント（サプリカント）がポートに接続されると、本機では EAPOL **の** ID **のリクエストを返します。クライアントは** ID **をスイッチに送信し、**RADIUS **サーバに転送されます。**

RADIUS **サーバはクライアントの** ID **を確認し、クライアントに対して** access challenge back **を送ります。**

RADIUS **サーバからの** EAP **パケットには** Challenge **及び認証モードが含まれます。クライアントソフト及び** RADIUS **サーバの設定によっては、クライアントは認証モードを拒否し、他の認証モードを要求することができます。認証モードには、**MD5, TLS (Transport Layer Security),TTLS (Tunneled Transport Layer Security) **等があります。**

クライアントは、パスワードや証明書などと共に、適切な方法により応答します。

RADIUS **サーバはクライアントの証明書を確認し、許可または不許可のパケットを返します。認証が成功した場合、クライアントに対してネットワークへのアクセスを許可します。そうでない場合は、アクセスは否定され、ポートはブロックされます。**

IEEE802.1x **認証を使用するには本機に以下の設定を行います。**

- **スイッチの** IP **アドレスの設定を行います。**
- RADIUS **認証を有効にし、**RADIUS **サーバの** IP **アドレスを設定します。**
- **認証を行う各ポートで** dot1x"Auto" **モードに設定します。**
- **接続されるクライアント側に** dot1x **クライアントソフトがインストールされ、適切な設定を行います。**
- RADIUS **サーバ及び** IEEE802.1x **クライアントは** EAP **をサポートする必要があります（本機では** EAP **パケットをサーバからクライアントにパスするための** EAPOL **のみをサポートしています）**
- RADIUS **サーバとクライアントは** MD5、TLS、TTLS、PEAP **等の同じ** EAP **認証タイプをサポートしている必要があります（一部は** Windows **でサポートされていますが、それ以外に関しては** IEEE802.1x **クライアントによりサポートされている必要があります）**

802.1x グローバルセッティングの表示

802.1X プロトコルはクライアントの認証を可能にします。

設定・表示項目

802.1X System Authentication Control

スイッチに対する 802.1X の設定

設定方法

[Security] → [802.1x Information] をクリックします。

802.1x グローバルセッティング

dot1X プロトコルはポート認証を可能にします。ポートをアクティブに設定する前に、スイッチに対し 802.1X プロトコルを有効に設定する必要があります。

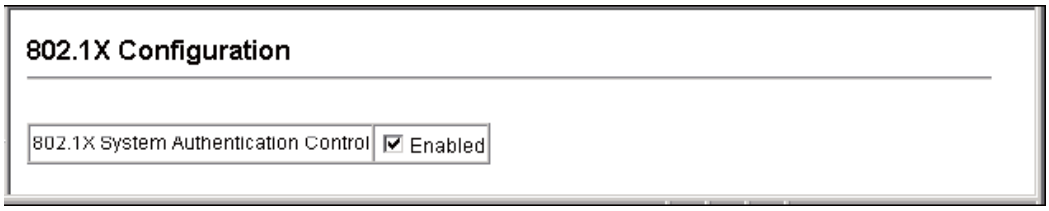
設定・表示項目

802.1X System Authentication Control

802.1X の設定（初期設定：無効)

設定方法

[Security] → [802.1X] → [Configuration] をクリックします。スイッチに対する 802.1X を有効に設定し、[Apply] をクリックします。



802.1X 認証ポート設定

802.1X を有効にした場合、クライアントとスイッチ間及びスイッチと認証サーバ間のクライアント認証プロセスに関するパラメータを設定する必要があります。これらのパラメータについて解説します。

設定・表示項目

Port

ポート番号

Status

ポートの認証の有効 / 無効

Operation Mode

1 台又は複数のクライアントが IEEE802.1x 認証ポートにアクセスすることを設定します（設定範囲：Single-Host、Multi-Host、初期設定：Single-Host）

Max Count

Multi-Host 設定時の最大接続可能クライアント数（設定範囲：1-1024、初期設定：5）

Mode

認証モードを以下のオプションの中から設定します。

- **Auto** ― dot1x 対応クライアントに対して RADIUS サーバによる認証を要求します。dot1x 非対応クライアントからのアクセスは許可しません。

- **Force-Authorized** ― dot1x **対応クライアントを含めたすべてのクライアントのアクセスを許可します。**
- **Force-Unauthorized** ― dot1x**対応クライアントを含めたすべてのクライアントのアクセスを禁止します。**

Re-authen

Re-authentication Period **で設定した期間経過後にクライアントを再認証するかどうか。再認証により、新たな機器がスイッチポートに接続されていないかを検出できます（初期設定：無効**)

Max-Req

認証セッションがタイムアウトになる前に、EAP **リクエストパケットをスイッチポートからクライアントへ再送信する場合の最大回数（範囲：**1-10 **回、初期設定：**2 **回）**

Quiet Period

EAP **リクエストパケットの最大送信回数を過ぎた後、新しいクライアントの接続待機状態に移行するまでの時間（範囲：**1-65535 **秒、初期設定：**60 **秒）**

Re-authen Period

接続済みのクライアントの再認証を行う間隔（範囲：1-65535 **秒、初期設定：**3600 **秒）**

TX Period

認証時に EAP **パケットの再送信を行う間隔（範囲：**1-65535 **秒、初期設定：**30 **秒）**

Authorized

- **Yes** ― **接続されたクライアントは認証されています。**
- **No** ―**接続されたクライアントは認証されていません。**
- *Blank* ― IEEE802.1x **がポートで無効化されている場合は空欄となります。**

Supplicant

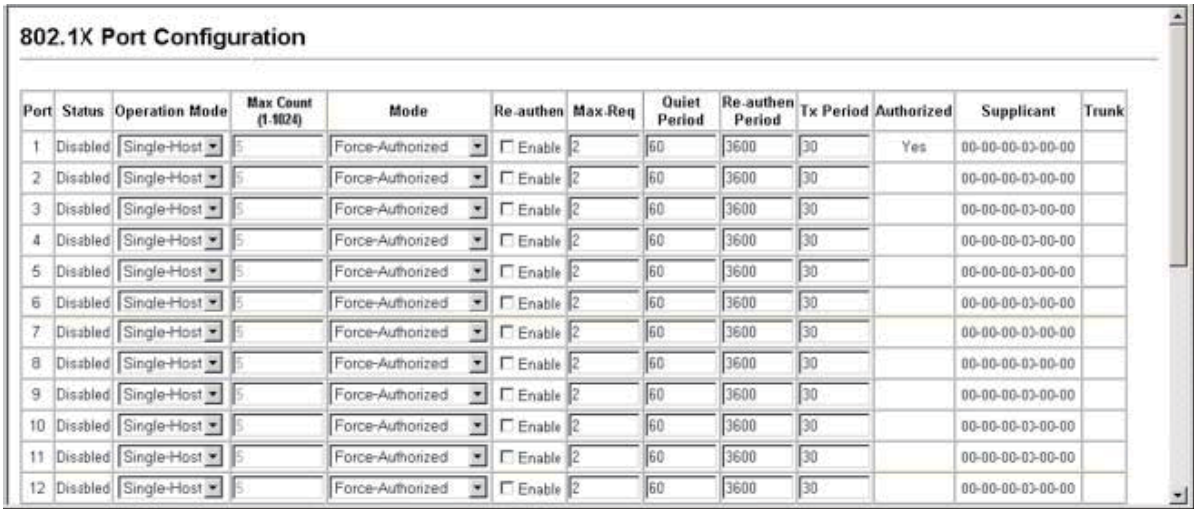
接続されたクライアントの MAC **アドレス**

Trunk

トランク設定がされている場合に表示

設定方法

[Security] → [802.1x] → [Port Configuration] をクリックします。必要に応じてパラメータを変更し、[Apply] をクリックします。



802.1X Port Configuration

Port	Status	Operation Mode	Max Count (1-1024)	Mode	Re-authen	Max-Req	Quiet Period	Re-authen Period	Tx Period	Authorized	Supplicant	Trunk
1	Disabled	Single-Host	5	Force-Authorized	Enable	2	60	3600	30	Yes	00-00-00-00-00-00	
2	Disabled	Single-Host	5	Force-Authorized	Enable	2	60	3600	30		00-00-00-00-00-00	
3	Disabled	Single-Host	5	Force-Authorized	Enable	2	60	3600	30		00-00-00-00-00-00	
4	Disabled	Single-Host	5	Force-Authorized	Enable	2	60	3600	30		00-00-00-00-00-00	
5	Disabled	Single-Host	5	Force-Authorized	Enable	2	60	3600	30		00-00-00-00-00-00	
6	Disabled	Single-Host	5	Force-Authorized	Enable	2	60	3600	30		00-00-00-00-00-00	
7	Disabled	Single-Host	5	Force-Authorized	Enable	2	60	3600	30		00-00-00-00-00-00	
8	Disabled	Single-Host	5	Force-Authorized	Enable	2	60	3600	30		00-00-00-00-00-00	
9	Disabled	Single-Host	5	Force-Authorized	Enable	2	60	3600	30		00-00-00-00-00-00	
10	Disabled	Single-Host	5	Force-Authorized	Enable	2	60	3600	30		00-00-00-00-00-00	
11	Disabled	Single-Host	5	Force-Authorized	Enable	2	60	3600	30		00-00-00-00-00-00	
12	Disabled	Single-Host	5	Force-Authorized	Enable	2	60	3600	30		00-00-00-00-00-00	

IEEE802.1x 統計情報の表示

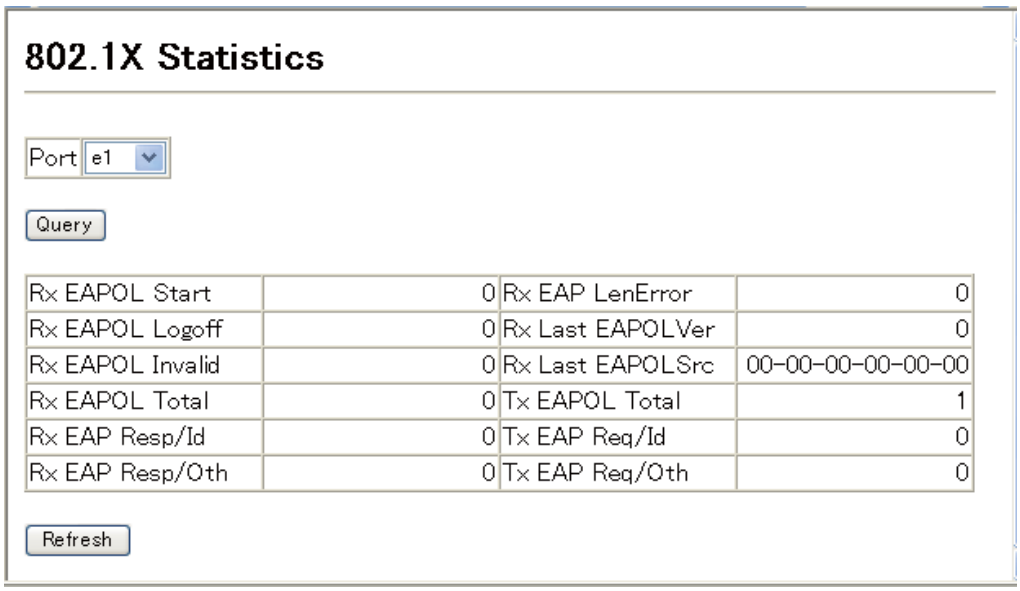
dot1x プロトコルの各ポートの統計情報を表示します。

機能解説

パラメータ	解説
Rx EXPOL Start	EAPOL スタートフレームの受信数
Rx EAPOL Logoff	EAPOL ログオフフレームの受信数
Rx EAPOL Invalid	全 EAPOL フレームの受信数
Rx EAPOL Total	有効な EAPOL フレームの受信数
Rx EAP Resp/Id	EAP Resp/Id フレームの受信数
Rx EAP Resp/Oth	Resp/Id frames 以外の有効な EAP 応答フレームの受信数
Rx EAP LenError	パケット長が不正な無効 EAPOL フレームの受信数
Rx Last EAPOLVer	直近の受信 EAPOL フレームのプロトコルバージョン
Rx Last EAPOLSrc	直近の受信 EAPOL フレームのソース MAC アドレス
Tx EAPOL Total	全 EAPOL フレームの送信数
Tx EAP Req/Id	EAP Resp/Id フレームの送信数
Tx EAP Req/Oth	Resp/Id frames 以外の有効な EAP 応答フレームの送信数

設定方法

[Security] → [802.1X] → [Statistics] をクリックします。



3.5.8 Web 認証

Web Authentication は、802.1x やネットワークアクセス認証は実行不可能であり実用的でない状況で、ネットワークへの認証とアクセスを行うことを端末に許可します。Web Authentication 機能は IP アドレスを割り当てる DHCP のリクエストと受信、DNS クエリの実行を、認証されていないホストに許可します。HTTP を除いたほかのすべてのトラフィックはブロックされます。スイッチは HTTP トラフィックを傍受し、RADIUS を通してユーザーネームとパスワードを入力する、スイッチが生成した Web ページにリダイレクトします。一度認証に成功すると、Web ブラウザは元のリクエストされた Web ページに転送されます。認証が成功したポートに接続されたすべてのホストについて、認証が有効になります。

[注意] MAC アドレス認証、Web Authentication、802.1x、ポートセキュリティは同じポート上で同時に使用することができません。1 つのセキュリティ機能のみ適用できます。

[注意] RADIUS 認証は適切に機能させるために、アクティベートし Web Authentication のために適切に構成しなくてはいけません。

[注意] Web Authentication はトランクポート上で設定することはできません。

Web 認証の設定

Web Authentication はポートごとに設定しますが、スイッチのすべてのポートに適用されるパラメータが 4 つあります。

設定・表示項目

System Authentication Control

スイッチ上で Web Authentication 機能を有効にします（初期設定：無効）

Session Timeout

ホストの再認証をする前に認証セッションをどのくらいの時間維持するかを設定します
（範囲：300 － 3600 秒　初期設定：3600 秒）

Quiet Period

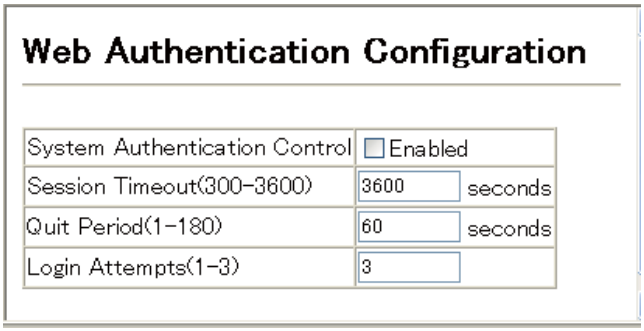
ホストがログインの試行回数の上限を超えた後、再び認証ができるまでに待機する時間を設定します（範囲：1 － 180 秒　初期設定：60 秒）

Login Attempts

ログインの試行回数の上限を設定します。（範囲：1 － 3 回　初期設定：3 回）

設定方法

[Security] → [Web Authentication] → [Configuration] をクリックします。



Web 認証の設定（ポート）

Web Authentication はポートごとに設定されます。下記のパラメータはそれぞれのポートに結び付けられています。

設定・表示項目

Port

設定されるポート

Status

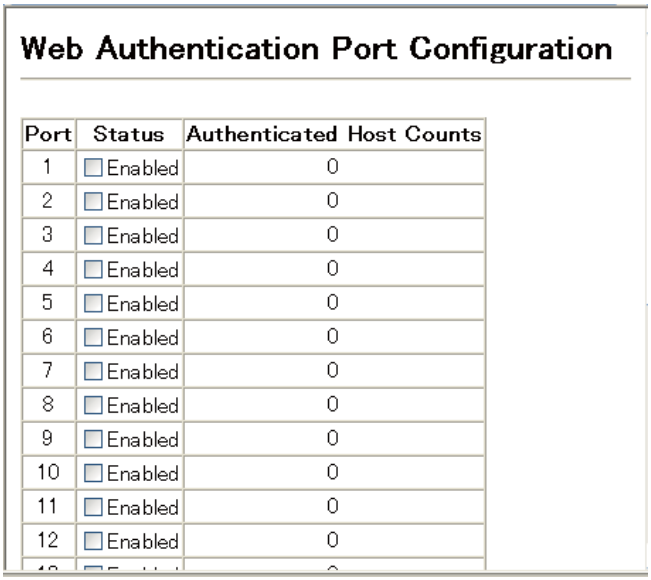
ポートの Web Authentication の状態を設定します。

Authentication Host Counts

ポートに接続されている認証済みのホストの数を表示します。

設定方法

[Security] → [Web Authentication] → [Port Configuration] をクリックします。



Web 認証・ポート情報の表示

すべてのポートと接続されたホストの認証情報を表示します。

設定・表示項目

Interfacde

問い合わせるイーサネットのポートを表示します。

IP Address

接続されたホストの IP アドレスを表示します。

Status

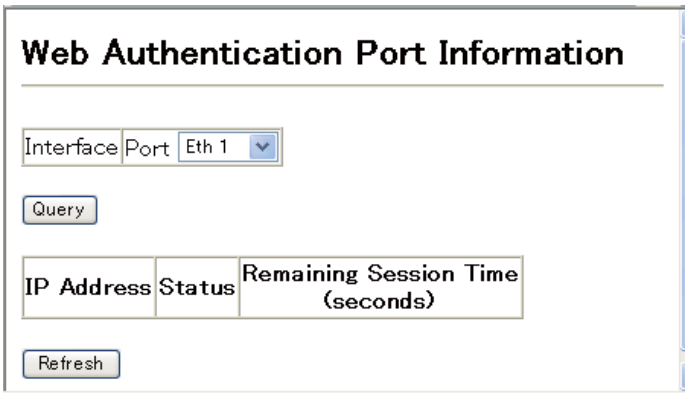
接続されたホストの認証状態を表示します。

Remaining Session Time(seconds)

ホストの現在の認証セッションの期限が切れるまでの残り時間を表示します。

設定方法

[Security] → [Web Authentication] → [Port Information] をクリックします。



Web 認証ポートの再認証

スイッチは手動でどれかのポートに接続された認証済みのホストの再認証を行うことができます。

設定・表示項目

Interfacde

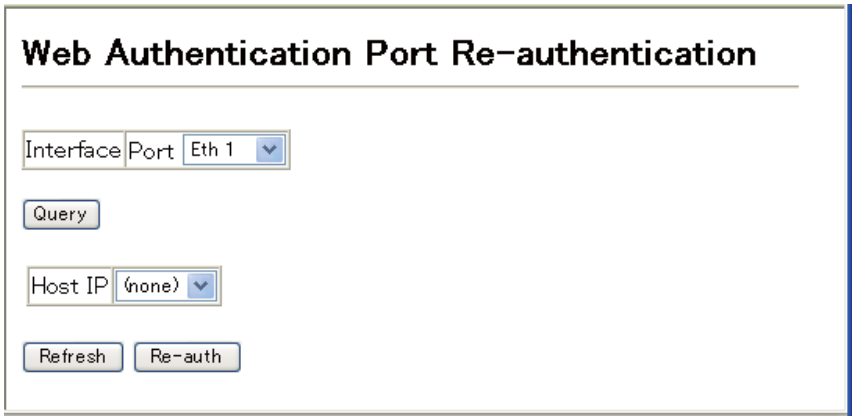
問い合わせるイーサネットのポートを表示します。

Host IP

再認証するホストの IP アドレスを表示します。

設定方法

[Security] → [Web Authentication] → [Re-authentication] をクリックします。



3.5.9 ネットワークアクセス（MAC アドレス認証）

スイッチポートに接続するいくつかのデバイスはハードウェアやソフトウェアの制限により 802.1x 認証をサポートできないかもしれません。これはネットワークプリンタ、IP 電話、ワイヤレスアクセスポイントのようなデバイスでしばしば遭遇します。スイッチは、RADIUS サーバーでデバイスの MAC アドレスを認証し管理することで、これらのデバイスからのネットワークアクセスを可能にします。

[注意] MAC Authentication、Web Authentication、802.1x、ポートセキュリティは同じポートに一緒に設定することはできません。1 つのセキュリティ機能のみ適用できます。

ネットワークアクセス機能は、ホストが接続されたスイッチポート上で MAC アドレスを認証することで、ホストのネットワークへのアクセスを管理しています。特定の MAC アドレスから受信したトラフィックは、送信元 MAC アドレスが RADIUS サーバーで認証された場合のみスイッチにより転送されます。MAC アドレスによる認証が進行しているとき、すべてのトラフィックは認証が完了するまでブロックされます。認証が成功した場合、RADIUS サーバーはスイッチポートに VLAN 設定を任意に割り当てる可能性があります。

ポート上で有効にしたとき、認証プロセスは設定された RADIUS サーバーに Password Authentication Protocol（PAP）リクエストを送信します。ユーザーネームとパスワードは両方とも認証する予定の MAC アドレスと同じです。RADIUS サーバー上で PAP のユーザーネームとパスワードは MAC アドレスのフォーマット（xx-xx-xx-xx-xx-xx）で設定しなくてはいけません。

認証された MAC アドレスは、スイッチの保護された MAC アドレステーブルにダイナミックエントリとして保存され、エージングタイムが過ぎたときに取り除かれます。スイッチでサポートする保護された MAC アドレスの最大数は 1024 個です。

[注意] MAC Authentication はトランクポート上で設定することはできません。

RADIUS サーバーはスイッチポートに適用するために VLAN ID のリストを任意に返すかもしれません。下記の設定は RADIUS サーバー上で設定するために必要です。

- Tunnel-Type ＝ VLAN
- Tunnel-Medium-Type ＝ 802
- Tunnel-Private-Group-ID ＝ 1u、2t（VLAN ID リスト）

VLAN ID リストは RADIUS の "Tunnel-Private-Group-ID" の中で維持されています。VLAN ID のリストは、"1u、2t、3u" といったフォーマットの複数の VLAN ID を含むことができます。"u" が付いているのはタグなしの VLAN ID で、"t" が付いているのはタグありの VLAN ID となります。

MAC 認証・再認証時間の設定

MAC アドレス認証は基本的にポートごとに設定しますが、スイッチすべてのポートに適用する設定が 2 つあります。

設定・表示項目

Authenticated Age

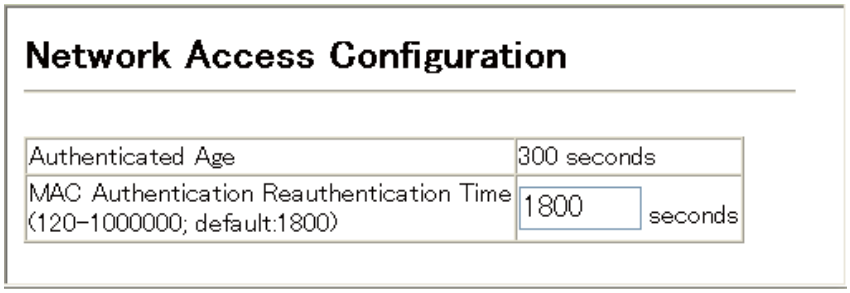
保護された MAC アドレステーブルのエージングタイムです。このパラメータはスイッチの MAC アドレステーブルの値と同じで、エージングタイム設定の画面で設定できます（初期設定：300 秒）

MAC Authentication Reauthentication Time

MAC アドレスが認証された後、再認証されるまでの期間を設定します
（範囲：120 秒ー 1,000,000 秒　初期設定：1800 秒）

設定方法

[Security] → [Network Access] → [Configuration] をクリックします。



MAC 認証の設定（ポート）

スイッチポートに MAC アドレス認証の設定を行います。

設定・表示項目

Mode

ポート上で MAC アドレス認証を有効にします（デフォルトでは無効）

Maximum MAC Count

ポート上で認証できる MAC アドレスの最大数を設定します。ポートごとの MAC アドレスの最大数は 1024 です。制限に達したとき、すべての新しい MAC アドレスは認証が失敗したものと取り扱われます（範囲：1 － 1024　初期設定：1024）

Guest VLAN

802.1x の認証が失敗したとき、ポートに割り当てる VLAN を指定します。VLAN は事前に作成して、有効にする必要があります。

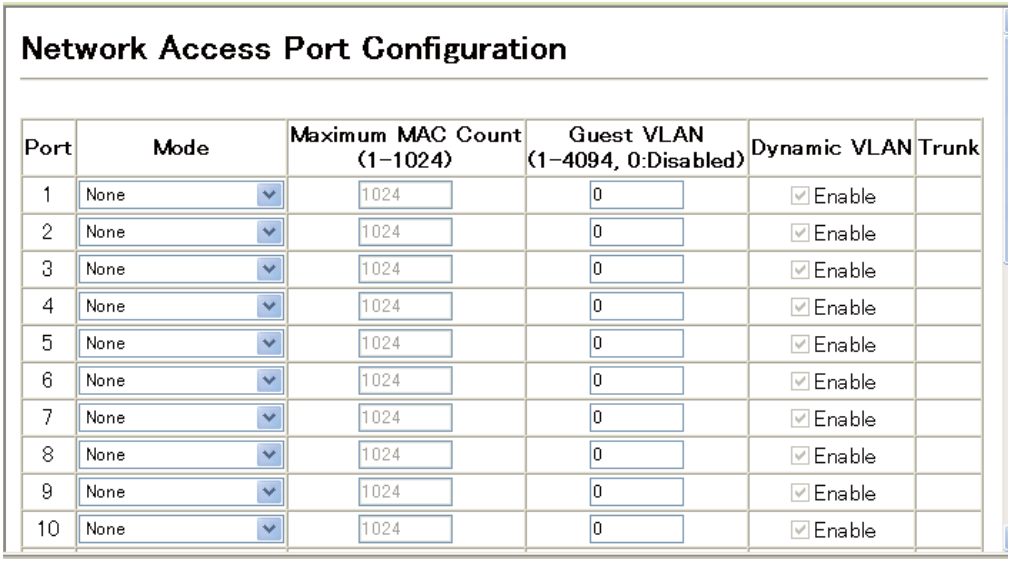
Dynamic VLAN

認証されたポートへのダイナミック VLAN の割り当てを有効にします。有効にしたとき、RADIUS サーバーより返ってきた VLAN ID がポートに割り当てられ、スイッチ上で事前に作成した VLAN が規定されます（VLAN 作成に GVRP は使用できません）。VLAN の設定は最初に行ってください（初期設定：有効）

[注意]　MAC アドレス認証はトランクポート上で有効にすることはできません。トランクメンバーとして構成されたポートは Network Access Port Configuration 画面の "Trunk" 列でその設定の有無が表示されます。

設定方法

[Security] → [Network Access] → [Port Configuration] をクリックします。



送信元 MAC アドレス情報の表示

認証された MAC アドレスは、保護された MAC アドレステーブルに保存されます。ここでは保護された MAC エントリの情報を表示し、選択したエントリをテーブルから削除することができます。

設定・表示項目

Network Access MAC Address Count

現在、保護された MAC アドレステーブルにある MAC アドレスの数です。

Query By

MAC アドレスの検索に使用する値を指定します。

- **Port**― ポートを指定します。
- **MAC Address** ― MAC アドレスを 1 つ指定します。
- **Attribute** ―スタティックアドレスかダイナミックアドレスかを指定します。
- **Address Table Sort Key** ― 表示される情報のソートを MAC アドレスとポートのどちらで行うかを指定します。

Unit/Port

保護された MAC アドレスの属するポート

MAC Address

認証された MAC アドレス

RADIUS Server

MAC アドレスを認証した RADIUS サーバーの IP アドレス

Time

MAC アドレスが最後に認証された時刻

Attribute

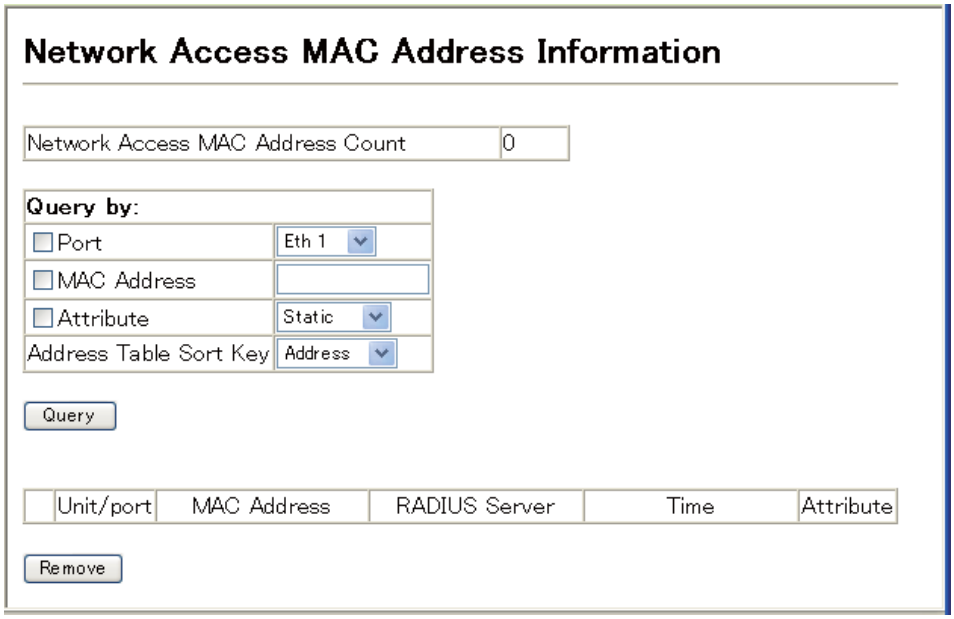
MAC アドレスがスタティックかダイナミックかを表示

Remove

クリックすると保護された MAC アドレステーブルから選択した MAC アドレスを削除します。

設定方法

[Security] → [Network Access] → [MAC Address Information] **をクリックします。**



3.6 ACL （Access Control Lists）

Access Control Lists (ACL) は IP アドレス、プロトコル、TCP/UDP ポート番号によるパケットフィルタリングを提供します。

入力されるパケットのフィルタリングを行うには、初めにアクセスリストを作成し、必要なルールを追加します。その後、リストに特定のポートをバインドします。

3.6.1 ACL の設定

ACL は IP アドレス、又は他の条件と一致するパケットに対して許可 (Permit) 又は拒否 (Deny) するためのリストです。

本機では入力及び出力パケットに対して ACL と一致するかどうか１個ずつ確認を行ないます。パケットが許可ルールと一致した場合には直ちに通信を許可し、拒否ルールと一致した場合にはパケットを落とします。リスト上の許可ルールに一致しない場合、パケットは落とされ、リスト上の拒否ルールに一致しない場合、パケットは通信を許可されます。

機能解説

ACL は以下の制限があります。

- 各 ACL は最大 32 ルールまで設定可能です。
- 最大 ACL 設定数は 32 個です。
- ACL が出力フィルタとしてインタフェースに設定された場合、ACL ルールは拒否ルール (deny) にする必要があります。そうでない場合には設定がエラーとなります。
- 本機では出力 IP ACL において "deny any any" ルールをサポートしていません。そのような設定が ACL に含まれていて、ポートの出力フィルタに設定をした場合にはエラーとなります。

有効な ACL は以下の順番で実行されます。

（1）出力ポートの出力 IP ACL のユーザに定義されたルール

（2）入力ポートの入力 IP ACL のユーザに定義されたルール

（3）入力ポートの入力 IP ACL のデフォルトルール (permit any any)

（4）明確なルールに一致しない場合、暗黙のデフォルトルール (permit all)

ACL 名およびタイプの設定

ACL Configuration ページでは、ACL の名前及びタイプを設定することができます。

設定・表示項目

Name

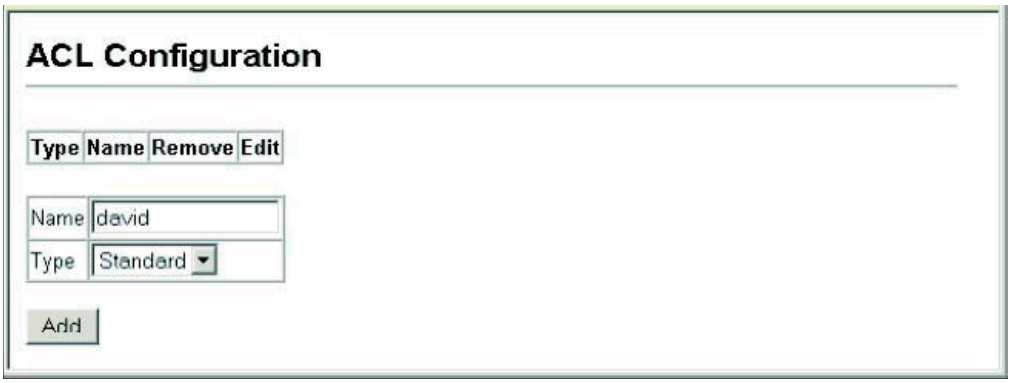
ACL 名（15 文字以内）

Type

- **Standard** ― ソース IP アドレスに基づくフィルタリングを行なう IP ACL モード
- **Extended** ― ソース又はディスティネーション IP アドレス、プロトコルタイプ、TCP/UDP ポート番号、TCP コントロールコードに基づくフィルタリングを行なう IP ACL モード
- **MAC** ― ソース又はディスティネーション MAC アドレス、イーサネットフレームタイプ (RFC 1060) に基づくフィルタリングを行なう MAC ACL モード

設定方法

[Security] → [ACL] → [Configuration] をクリックします。[Neme] に ACL 名を入力し、[Type] をリストから選択します (IP Standard, IP Extended, MAC)。その後、[Add] をクリックし、新規リストの設定ページを開きます。



Standard IP ACL の設定

設定・表示項目

Action

ACL のルールが「permit（許可）」か「deny(拒否)」を選択します（初期設定：Permit ルール）

Address Type

ソース IP アドレスの指定を行ないます。"any" ではすべての IP アドレスが対象となります。"host" ではアドレスフィールドのホストが対象となります。"IP" では、IP アドレスとサブネットマスクにより設定した IP アドレスの範囲が対象となります。

（オプション：Any, Host, IP、初期設定：Any）

IP Address

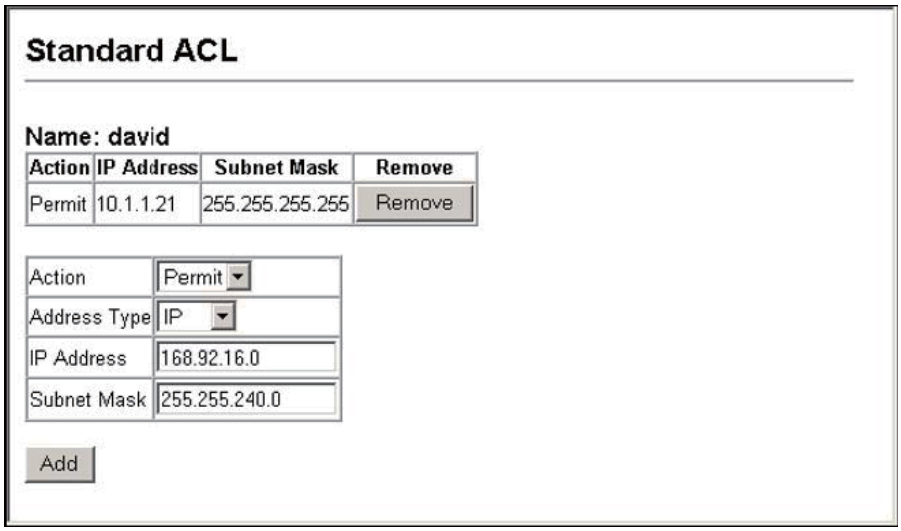
ソース IP アドレス

SubnetMask

サブネットマスク

設定方法

「許可」又は「拒否」の動作を設定し、その後アドレスタイプを Any, Host, IP から選択します。"Host" を選択した場合には特定の IP アドレスを指定します。"IP" を選択した場合には IP アドレスの範囲を指定するためにサブネットアドレスとマスクを設定します。その後 [Add] をクリックします。



Extended IP ACL の設定

設定・表示項目

Action

ACL のルールが「permit（許可）」か「deny(拒否)」を選択します（初期設定：Permit ルー

Source/Destination Address Type

ソース又はディスティネーション IP アドレスの設定を行います。"any" ではすべての IP アドレスが対象となります。"host" ではアドレスフィールドのホストが対象となります。"IP" では、IP アドレスとサブネットマスクにより設定した IP アドレスの範囲が対象となります（オプション：Any, Host, IP、初期設定：Any）

Source/Destination IP Address

ソース又はディスティネーション IP アドレス

Source/Destination Subnet Mask

ソース又はディスティネーション IP アドレスのサブネットマスク

Service Type

- **Precedence** ― IP precedence レベル（範囲：0-7）
- **DSCP** ― DSCP プライオリティレベル（範囲：0-63）

Protocol

TCP、UDP のプロトコルタイプの指定又はポート番号 (0-255)

（オプション：TCP, UDP, Others;、初期設定：TCP）

Source Port Start /End

ソースポート番号の開始値と終了値（範囲：0-65535）

Destination Port Start /End

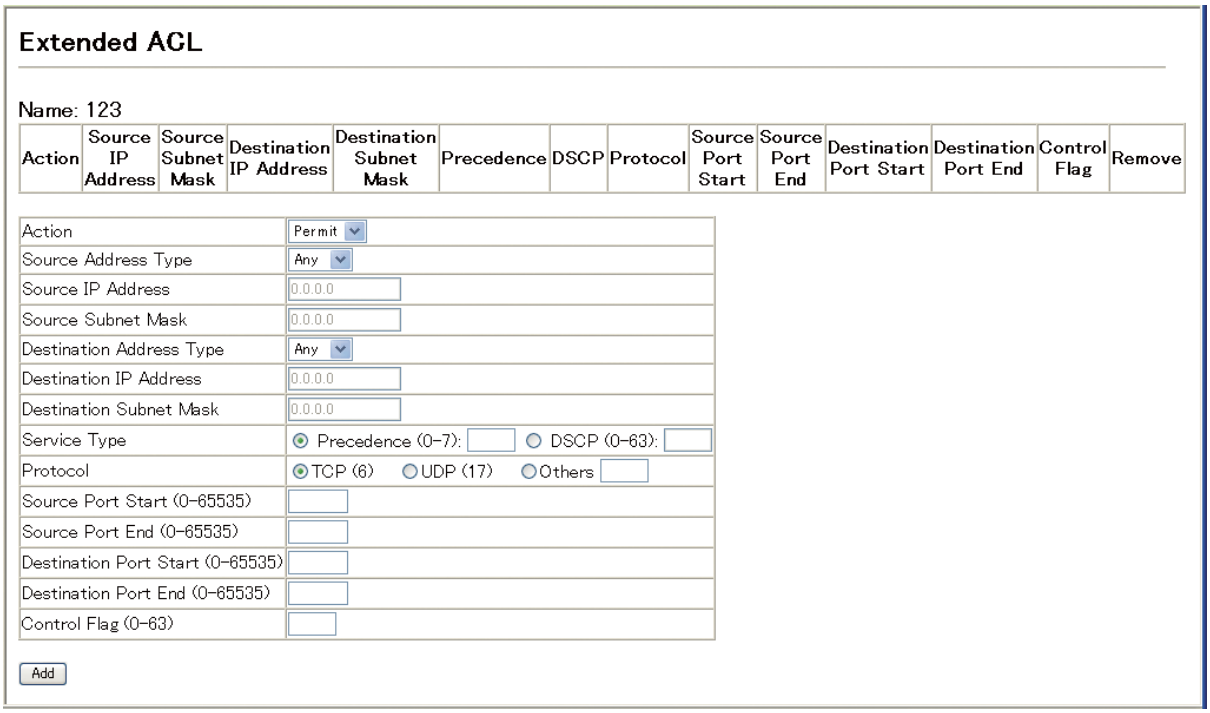
ディスティネーションポート番号の開始値と終了値（範囲：0-65535）

Control Flag

TCP ヘッダのバイト 14 内のフラグ・ビットを指定（範囲 :0-63）

設定方法

（permit/deny の）動作を指定します。ソース及び / 又はディスティネーションアドレスを指定し、アドレスタイプ ((Any, Host, IP) を選択します。"Host" を選択した場合、特定のアドレスを入力します。"IP" を選択した場合、アドレス範囲を指定するためにサブネットアドレスとマスクを指定します。プロトコルタイプ等のその他の必要項目を設定し、[Add] をクリックします。



MAC ACL の設定

設定・表示項目

Action

ACL のルールが「permit（許可）」か「deny(拒否)」を選択します（初期設定：Permit ルール）

Source/Destination MAC

"any" ではすべての IP アドレスが対象となります。"host" ではアドレスフィールドのホストが対象となります。"MAC" では、MAC アドレスとビットマスクにより設定した MAC アドレスの範囲が対象となります（オプション：Any, Host, MAC、初期設定：Any）

Source/Destination MAC Address

ソース又はディスティネーション MAC アドレス

Source/Destination MAC Bitmask

ソース又はディスティネーション MAC アドレスの 16 進数のマスク

VID

VLAN ID（範囲：1-4094）

Ethernet Type

この項目はイーサネット II フォーマットのパケットのフィルタリングに使用します（範囲：600-fff hex）
イーサネットプロトコルタイプのリストは RFC 1060 で定義されていますが、一般的なタイプとしては、0800(IP)、0806(ARP)、8137(IPX) 等があります。

Packet Format

本属性は次のパケット・タイプから選択できます。

- Any ― すべてのイーサネットパケットタイプ
- eth2 ― イーサネット II パケット
- 802.3 ― IEEE802.3 パケット

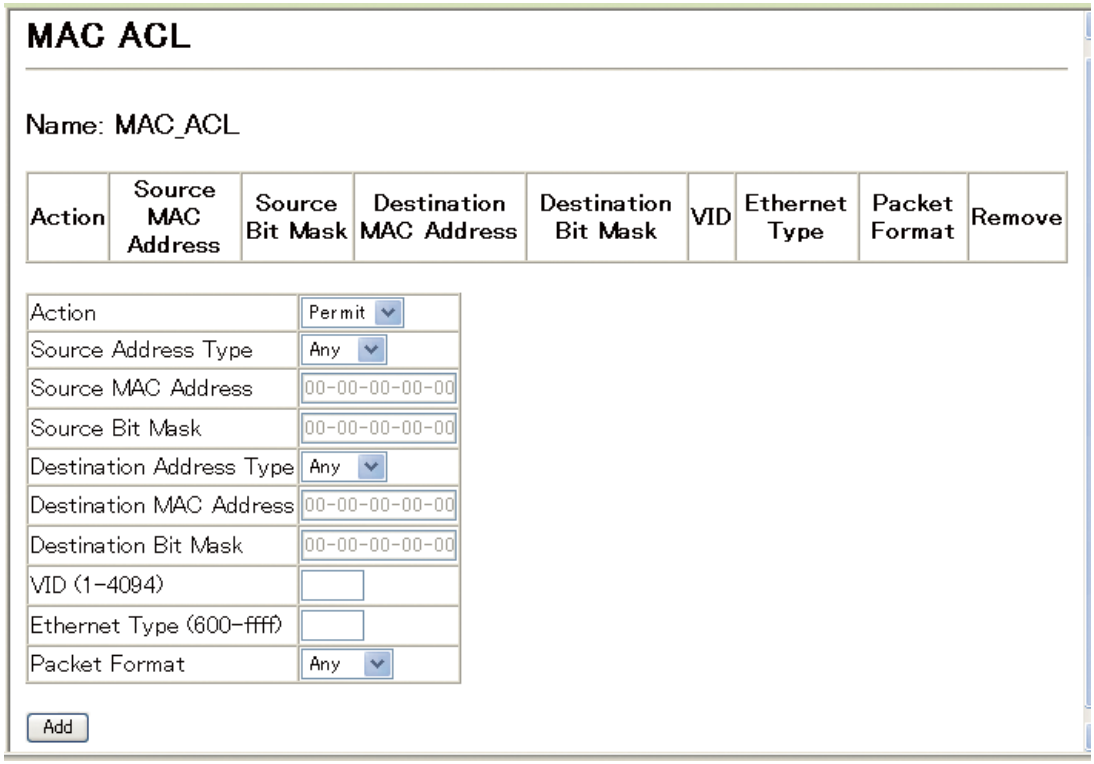
機能解説

ACL は以下の制限があります。

- 出力 MAC ACL は destination-mac-known パケットのみに機能し、マルチキャストパケット、ブロードキャストパケット及び destination-mac-unknown パケットには機能しません。

設定方法

（permit/deny **の）動作を指定します。ソース及び / 又はディスティネーションアドレスを指定し、アドレスタイプ** ((Any, Host, MAC) **を選択します。**"Host" **を選択した場合、特定のアドレスを入力します。**"MAC" **を選択した場合、アドレス範囲を指定するためにベースアドレスとビットマスクを指定します。その他の必要項目を設定し、**[Add] **をクリックします。**



3.6.2 ACL へのポートのバインド

ACL の設定が完了後、フィルタリングを機能させるためにはポートをバインドする必要があります。ACL は 1 つを任意のポートに指定できます。

機能解説

本機では ingress（入力）ACL をサポートします。

設定・表示項目

Port

ポート又は拡張モジュールスロット（範囲：1-26）

IP

ポートにバインドする IP ACL ルール

MAC

ポートにバインドする MAC ACL ルール

IN

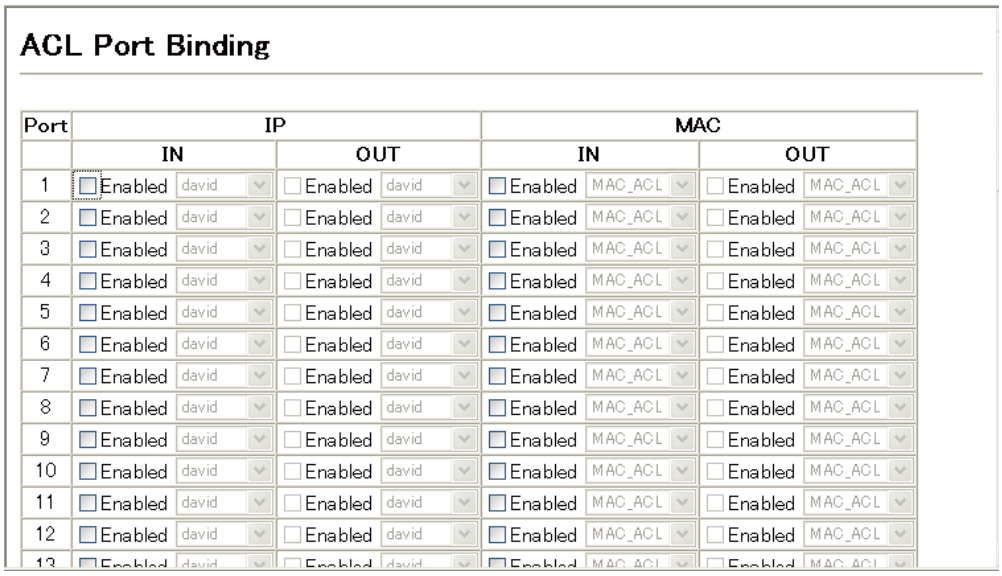
入力 (ingress) パケットに対する ACL

OUT

出力 (egress) パケットに対する ACL

設定方法

[Security] → [ACL] → [Port Binding] をクリックします。ACL をバインドするポートに対して "Enable" フィールドにチェックを入れ、ドロップダウンリストから ACL を選択します。その後、[Apply] をクリックします。



3.6.3 管理アドレスのフィルタリング

Web インタフェース、SNMP、Telnet による管理アクセスが可能な IP アドレス又は IP アドレスグループを最大 16 個作成できます。

機能解説

- 管理インタフェースは、初期設定ではすべての IP アドレスに対して接続可能な状態になっています。フィルタリストに 1 つでも IP アドレスを指定すると、そのインタフェースは指定したアドレスからの接続のみを許可します。
- 設定以外の無効な IP アドレスから管理アクセスに接続された場合、本機は接続を拒否し、イベントメッセージをシステムログに保存し、トラップメッセージの送信を行います。
- SNMP、Web、Telnet アクセスへの IP アドレス又は IP アドレス範囲の設定は合計で最大 5 つまで設定可能です。
- SNMP、Web、Telnet の同一グループに対して IP アドレス範囲を重複して設定することはできません。異なるグループの場合には IP アドレス範囲を重複して設定することは可能です。
- 設定した IP アドレス範囲から特定の IP アドレスのみを削除することはできません。IP アドレス範囲をすべて削除し、その後設定をし直して下さい。
- IP アドレス範囲の削除は IP アドレス範囲の最初のアドレスだけを入力しても削除することができます。また、最初のアドレスと最後のアドレスの両方を入力して削除することも可能です。

設定・表示項目

Web IP Filter

Web グループの IP アドレス

SNMP IP Filter

SNMP グループの IP アドレス

Telnet IP Filter

Telnet グループの IP アドレス

IP Filter List

そのインタフェースに接続が許可されている IP アドレス

Start IP Address

IP アドレス、又は IP アドレスを範囲で指定している場合の最初の IP アドレス

End IP Address

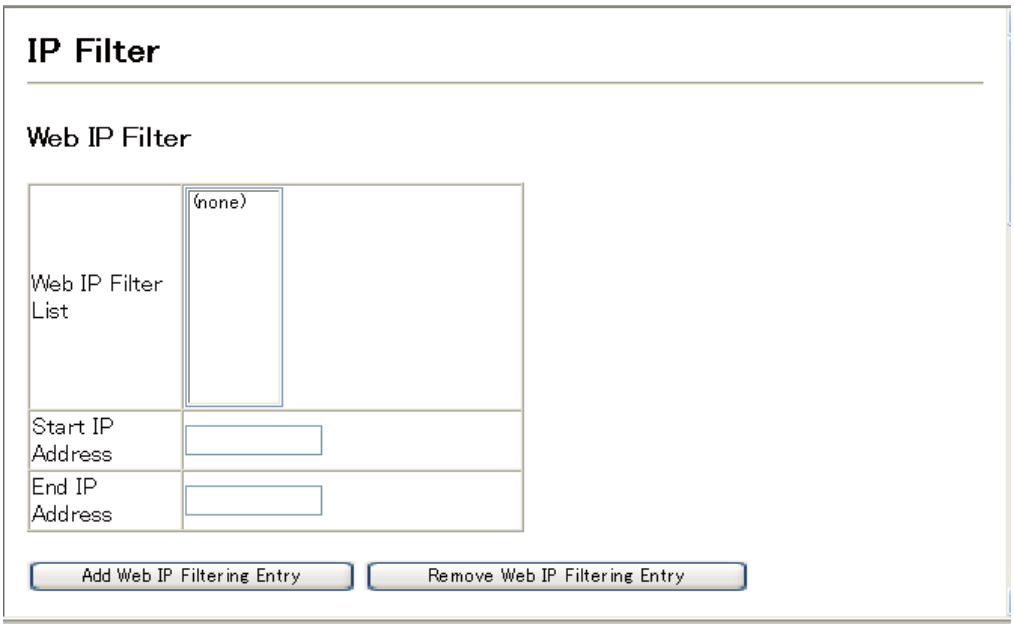
IP アドレスを範囲で指定している場合の最後の IP アドレス

Add/Remove Filtering Entry

IP アドレスをリストへ追加または削除

設定方法

[Security] → [IP Filter] **をクリックします。マネージメントアクセスを許可する** IP **アドレスを入力し、**[Add Web IP Filtering Entry] **をクリックします。**



3.7 ポート設定

3.7.1 接続状況の表示

接続状態の情報・速度及び通信方式・フロー制御そして、オートネゴシエーションを含む現在の接続情報を表示するために Port Information **及び** Trunk Information **画面を使用することができます。**

設定・表示項目

Name

インタフェースラベルの表示

Type

ポートの種類 (100Base-TX **又は** 1000BASE-T, SFP) **の表示**

Admin Status

インタフェースの有効 / 無効の表示

Oper Status

リンクアップ / リンクダウンの表示

Speed/Duplex Status

通信速度及び通信方式の表示 (Auto, Fixed)

Flow Control Status

使用中のフロー制御の種類の表示 (IEEE 802.3x, Back-Pressure, None)

Autonegotiation

オートネゴシエーションの有効 / 無効の表示

Media Type（Port Information **ページのみ**）

メディアタイプ

Trunk Member

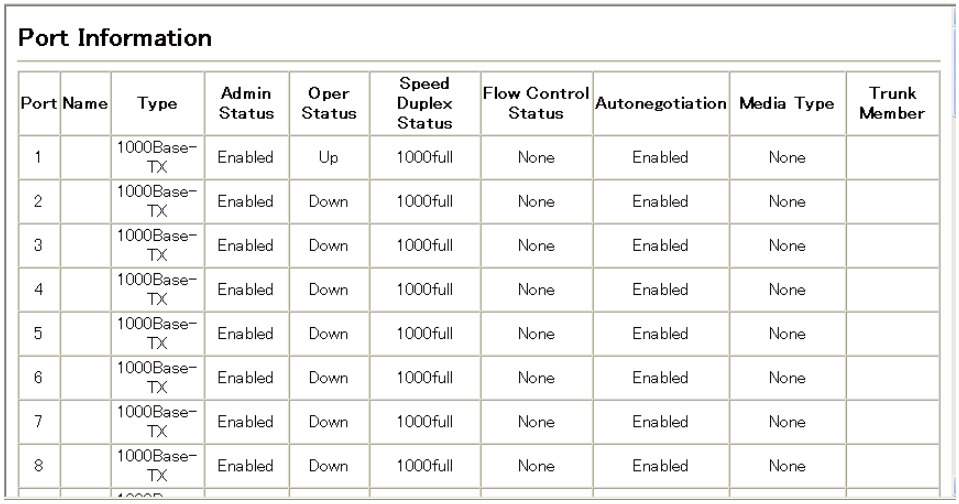
ポートのトランク状態の表示（Port Information **ページのみ**）

Creation

トランクが LACP **を使用して動的に設定されているか、手動で設定されているかの表示**（Trunk Information **ページのみ**）

設定方法

[Port] → [Port Information] 又は [Trunk Information] をクリックします。必要なインタフェースの設定の変更し、[Apply] をクリックします。



Port Information

Port	Name	Type	Admin Status	Oper Status	Speed Duplex Status	Flow Control Status	Autonegotiation	Media Type	Trunk Member
1		1000Base-TX	Enabled	Up	1000full	None	Enabled	None	
2		1000Base-TX	Enabled	Down	1000full	None	Enabled	None	
3		1000Base-TX	Enabled	Down	1000full	None	Enabled	None	
4		1000Base-TX	Enabled	Down	1000full	None	Enabled	None	
5		1000Base-TX	Enabled	Down	1000full	None	Enabled	None	
6		1000Base-TX	Enabled	Down	1000full	None	Enabled	None	
7		1000Base-TX	Enabled	Down	1000full	None	Enabled	None	
8		1000Base-TX	Enabled	Down	1000full	None	Enabled	None	

3.7.2 インタフェース接続の設定

Trunk Configuration（トランク設定）ページ及び Port Configuration（ポート設定）ページから、インタフェースの有効 / 無効、手動での通信速度及び通信方式、フローコントロール、オートネゴシエーションの設定及びインタフェースの対応機能を設定することができます。

設定・表示項目

Name

各インタフェースに管理識別用に名前をつけることができます (1-64 文字)

Admin

コリジョンの多発などの場合にインタフェースを手動で無効にすることができます。問題が解決した後に、再度インタフェースを有効にすることができます。また、セキュリティのためにインタフェースを無効にすることもできます。

Speed/Duplex

オートネゴシエーションを無効にした場合に、ポートの通信速度及び通信方式を手動で設定できます。

Flow Control

フローコントロールを自動設定又は手動設定で行うことができます。

Autonegotiation(Port Capabilities)

オートネゴシエーションを有効又は無効にします。また、オートネゴシエーション時のポートの対応機能を通知する設定を行います。

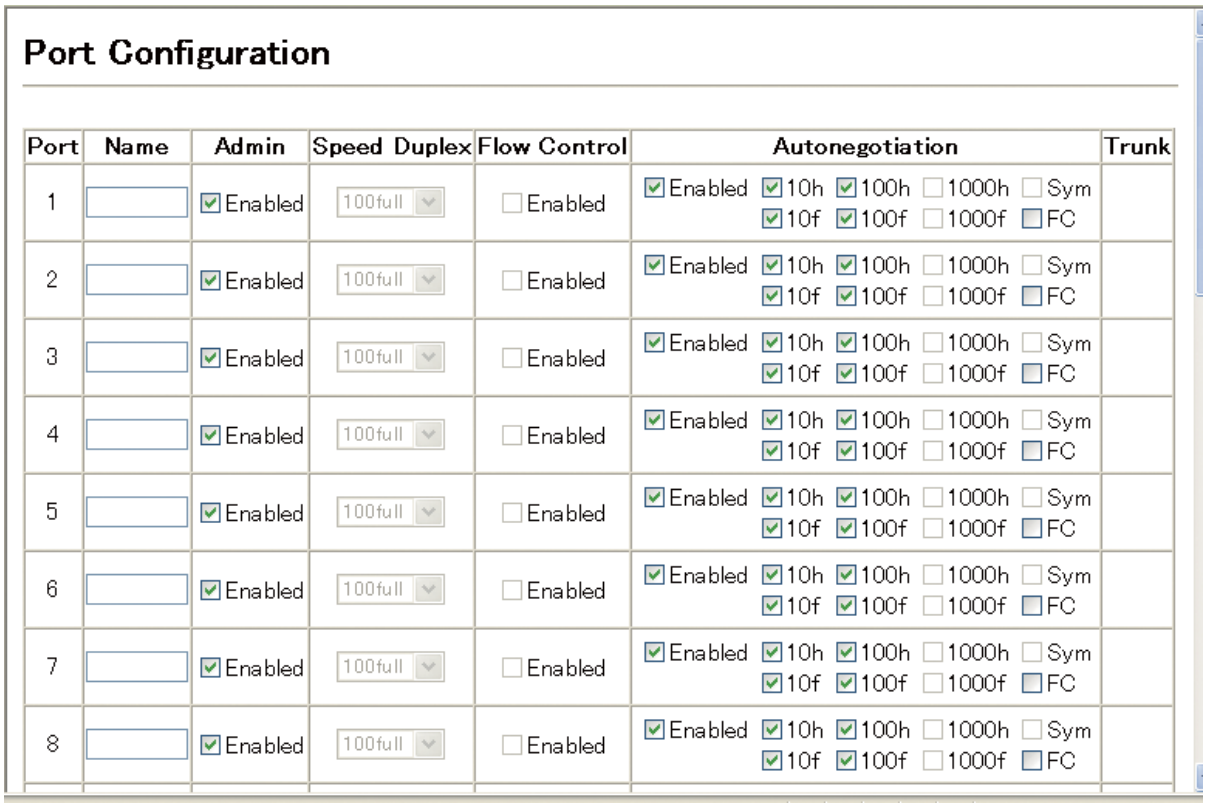
Trunk

ポートがトランクメンバーの場合に表示されます。トランクの設定及びポートメンバーの選択は、P104 「トランクグループの設定」を参照して下さい。

[注意] ポートの設定を手動で行ない、Speed/Duplex Mode 及び Flow Control の設定を反映させるためには、Autonegotiation（オートネゴシエーション）は Disabled（無効）にする必要があります。

設定方法

[Port] → [Port Configuration] 又は [Trunk Configuration] をクリックします。必要なインタフェースの設定を変更し [Apply] をクリックします。



3.7.3 トランクグループの設定

ネットワーク接続におけるバンド幅の拡大によるボトルネックの解消や障害の回避のために複数のポートは束ねるトランク機能を利用することができます。最大 12 のトランクを同時に設定することができます。

本機は、静的トランク及び動的な Link Aggregation Control Protocol (LACP) の両方をサポートしています。静的トランクでは、接続の両端において手動で設定する必要があり、また Cisco EtherChannel に準拠している必要があります。一方 LACP では LACP に設定したポートが、対向の LACP 設定ポートと連携し、自動的にトランクの設定を行ないます。静的トランクポートとして設定していない場合には、すべてのポートが LACP ポートに設定することができます。もし、8 つ以上のポートにより LACP トランクを形成している場合、8 つのポート以外はスタンバイモードとなります。トランクしている 1 つのポートに障害が発生した場合には、スタンバイモードのポートの 1 つが自動的に障害ポートと置き換わります。

機能解説

トランク内の各ポートで通信を分散すること及び、トランク内のポートで障害が発生した場合に他のポートを使用し通信を継続させる機能を提供します。

なお、設定を行なう場合には、デバイス間のケーブル接続を行なう前に両端のデバイスにおいてトランクの設定を行なって下さい。

トランクの設定を行なう場合には以下の点に注意して下さい :

- ループを回避するため、スイッチ間のネットワークケーブルを接続する前にポートトランクの設定を行なって下さい。
- 1 トランク最大 8 ポート、最大 12 トランクを作成することができます。
- 両端のデバイス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。
- 異なる機器同士で静的トランクを行なう場合には、Cisco EtherChannel と互換性がなければなりません。
- トランクの両端のポートは通信速度、通信方式、及びフロー制御の通信モード、VLAN 設定、及び CoS 設定等に関して同じ設定を行なう必要があります。
- トランクの全てのポートは VLAN の移動、追加及び削除を行なう際に 1 つのインタフェースとして設定する必要があります。
- STP、VLAN 及び IGMP の設定はトランク全体への設定のみが可能です。

静的トランクの設定

機能解説

- メーカー独自の機能の実装により、異なる機種間ではトランク接続ができない可能性があります。本機の静的トランクは Cisco EtherChannel に対応しています。
- ネットワークのループを回避するため、ポート接続前静的トランクを設定し、静的トランクを解除する前にポートの切断を行なって下さい。

設定・表示項目

Member List (Current)

既存のトランク情報（トランク ID、ユニット番号、ポート番号）

New

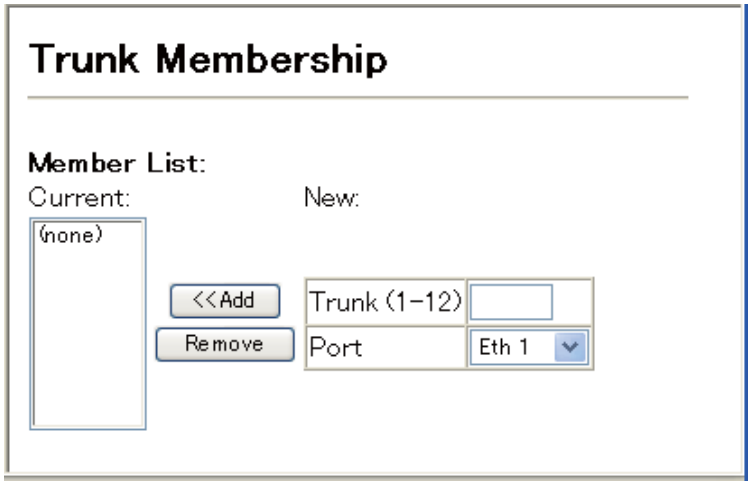
新規にトランクを作成するための入力欄

ー **Trunk** ― トランク識別子（範囲：1-12）

ー **Port** ― ポート識別子（範囲：1-26）

設定方法

[Port] → [Trunk Membership] をクリックします。1 から 25 のトランク ID を Trunk に入力し、スクロールダウンリストからポート番号を選択し [Add] をクリックします。Member List へのポートの追加が完了した後、[Apply] をクリックします。



LACP 設定

機能解説

- ネットワークのループを回避するため、ポート接続前に LACP を有効にし、LACP を無効にする前にポートの切断を行って下さい。
- 対向のスイッチのポートが LACP を有効に設定している場合、トランクは自動的にアクティブになります。
- LACP により対向のスイッチと構成されたトランクには、自動的に次の番号のトランク ID が割り当てられます。
- 8 つ以上のポートにより LACP トランクを有効にした場合、8 つのポート以外はスタンバイモードとなります。トランクしている 1 つのポートに障害が発生した場合には、スタンバイモードのポートの 1 つが自動的に障害ポートと置き換わります。
- LACP トランクの両端のポートは固定又はオートネゴシエーションにより full duplex に設定する必要があります。
- LACP により動的なトランクグループに設定されたトランク情報は、Member List 画面又は Trunk Membership 画面でも確認できます (P104)

設定・表示項目

Member List (Current)

既存のトランク情報（ユニット番号、ポート番号）

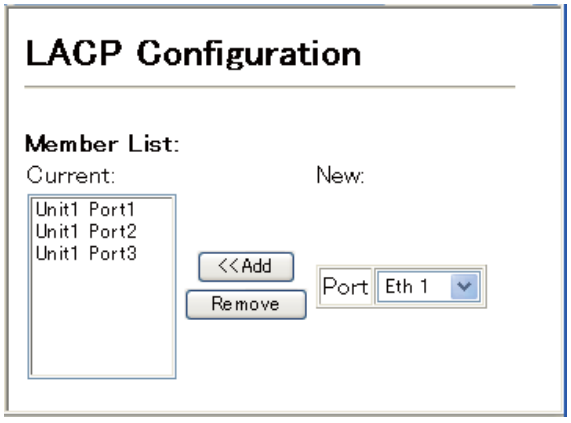
New

新規にトランクを作成するための入力欄

ー **Port** ― ポート識別子（範囲：1-26）

設定方法

[Port] → [LACP] → [Configuration] をクリックします。スクロールダウンリストからポートを選択し、[Add] をクリックします。Member List へのポートの追加が完了した後、[Apply] をクリックします。



LACP パラメータ設定

ポートチャンネルの動的設定 ― 同一のポートチャンネルに指定されたポートは以下の条件を満たす必要があります。

- ポートは同一の LACP システムプライオリティです。
- ポートは同一の LACP ポートアドミンキーです。
- 「ポートチャンネル」アドミンキーを設定する場合には、ポートアドミンキーはチャンネルグループへの参加が可能な同じ値を設定する必要があります。

[注意] チャンネルグループが形成され、port channel admin key が設定されていない場合、このキーはグループに参加しているインタフェースのポートアドミンキーと同じ値に設定されます。

設定・表示項目

Set Port Actor ― 本メニューは LACP のローカル側（本機上）の設定を行ないます。

Port

ポート番号（範囲：1-26）

System Priority

LACP システムプライオリティは、リンク集合グループ (LAG) メンバーを決定し、且つ LAG 間での設定の際に、他のスイッチが本機を識別するために使用されます（範囲：0-65535、初期設定：32768）

－同じ LAG に参加するポートは同じシステムプライオリティを設定する必要があります。
－システムプライオリティはスイッチの MAC アドレスと結合し、LAG の ID となります。この ID は LACP が他のシステムとネゴシエーションをする際に特定の LAG を示す ID となります。

Admin Key

LACP 管理キーは、同じ LAG に属するポートと同じ価に設定する必要があります（範囲：0-65535、初期設定：1）

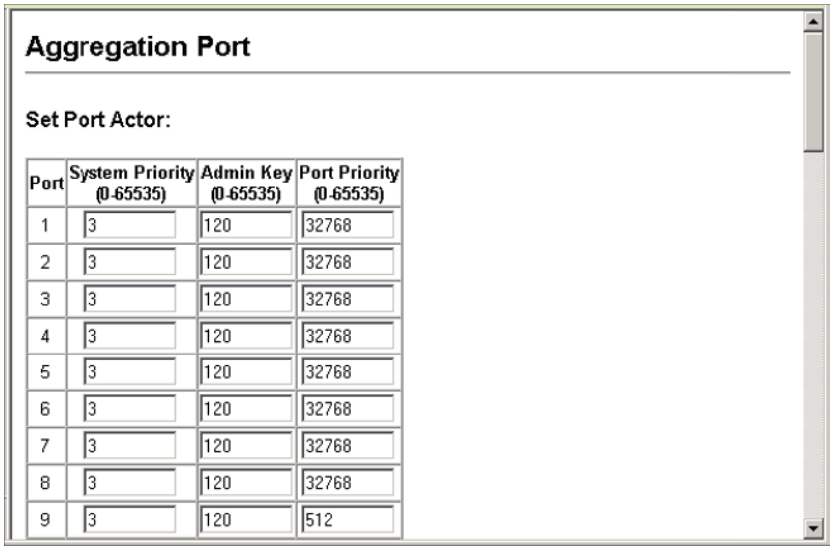
Port Priority

リンクが落ちた場合、LACP ポートプライオリティはバックアップリンクを選択するために使用されます（範囲：0-65535、初期設定：32768）

Set Port Partner ― 本メニューは LACP のリモート側（接続された機器上のポート）の設定を行ないます。コマンドの意味は *Port Actor* と同様です。パートナーの LACP 設定は運用状態ではなく管理状態を表し、今後 LACP がパートナーと確立される際に使用されます。

設定方法

[Port] → [LACP] → [Aggregation Port] をクリックします。Port Actor のための System Priority, Admin Key, Port Priority の設定を行ないます。その他に Port Partner の設定を行なうこともできます (これらの設定は Port Partner の管理状態に対応し、次回の本機に対する LACP まで有効となりません)。すべての設定が完了後、[Apply] をクリックします。



LACP ポートカウンタの表示

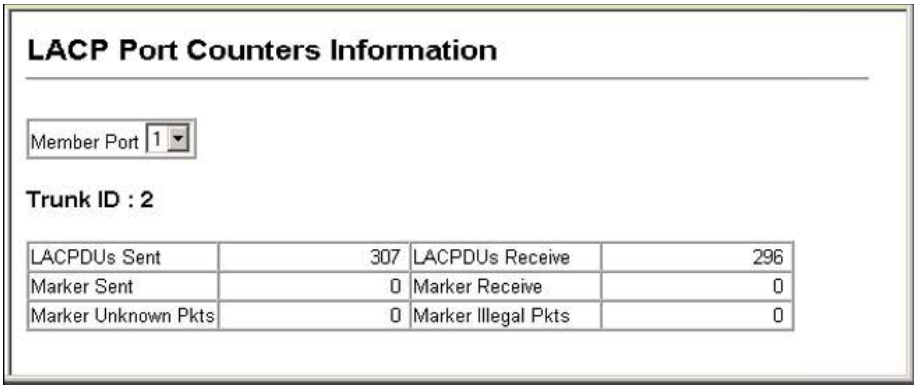
LACP プロトコルメッセージの統計情報の表示を行ないます。

カウンター情報

項目	解説
LACPDUs Sent	チャンネルグループから送信された有効な LACPDU の数
LACPDUs Received	チャンネルグループが受信した有効な LACPDU の数
Marker Sent	本チャンネルグループから送信された有効な Marker PDU の数
Marker Received	本チャンネルグループが受信した有効な Marker PDU の数
LACPDUs Unknown Pkts	以下のフレームの受信数 (1) スロープロトコル・イーサネット・タイプ値を運び、未知の PDU を含んでいるフレーム (2) スロープロトコルグループ MAC アドレスに属し、スロープロトコル・イーサネット・タイプ値を運んでいないフレーム
LACPDUs Illegal Pkts	不正な PDU 又はプロトコルサブタイプが不正な値を含むスロープロトコルイーサネットパケットを運ぶフレーム数

設定方法

[Port] → [LACP] → [Port Counters Information] をクリックします。メンバーポートを選択すると関連する情報が表示されます。



ローカル側の LACP 設定及びステータスの表示

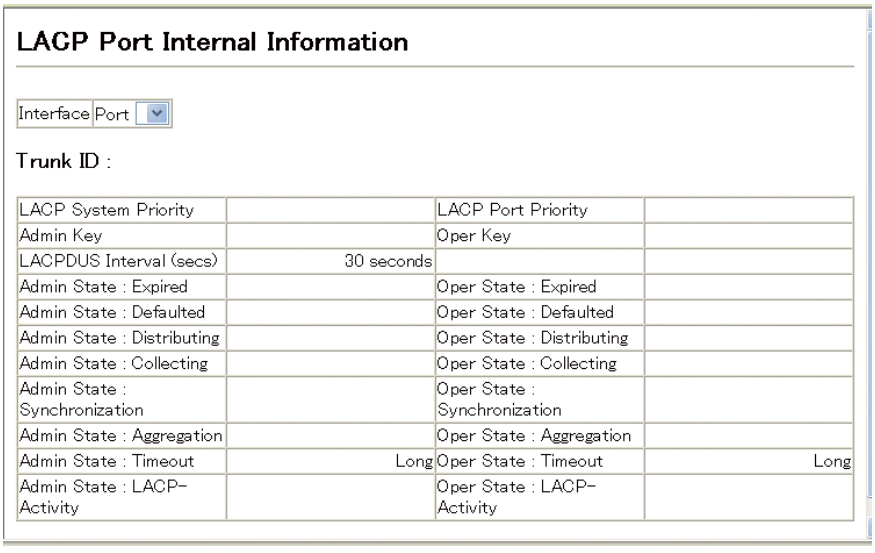
LACP のローカル側の設定及びステータスの表示を行なうことができます。

内部設定情報

項目	解説
Oper Key	現在のアグリゲーションポートのキーの運用値
Admin Key	現在のアグリゲーションポートのキーの管理値
LACPDUs Internal	受信した LACPDU 情報を無効にするまでの秒数
LACP System Priority	本ポートチャンネルグループに割り当てられた LACP システムプライオリティ
LACP Port Priority	本ポートチャンネルグループに割り当てられた LACP ポートプライオリティ
Admin State, Oper State	Actor の管理値又は運用値の状態のパラメータ。 ♦Expired — Actor の受信機器は失効状態です ♦Defaulted — Actorの受信機器は初期設定の運用partnerの情報を使用しています ♦Distributing — 誤りの場合、このリンク上の出力フレームの配信は無効になります。配信は現在無効状態で、受信プロトコル情報の管理上の変更、又は変更がない状態で有効にはなりません。 ♦Collecting — このリンク上の入力フレームの収集は可能な状態です。収集は現在可能な状態で、受信プロトコル情報の管理上の変化、又は変化がない状態で無効にはなりません。 ♦Synchronization — システムはリンクを IN_SYNC と認識します。それにより正しいリンクアグリゲーショングループに属すことができます。グループは互換性のある Aggregator に関係します。リンクアグリゲーショングループの ID はシステム ID と送信されたオペレーショナルキー情報から形成されます。 ♦Aggregation — システムは、アグリゲーション可能なリンクと認識しています。アグリゲーションの存在的な候補です。 ♦Long timeout — LACPDU の周期的な送信にスロー転送レートを使用します。 ♦LACP-Activity — 本リンクに関するアクティブコントロール値（0：Passive、1：Active）

設定方法

[Port] → [LACP] → [Port Internal Information] をクリックします。port channel を選択すると関連する情報が表示されます。



リモート側の LACP 設定及びステータスの表示

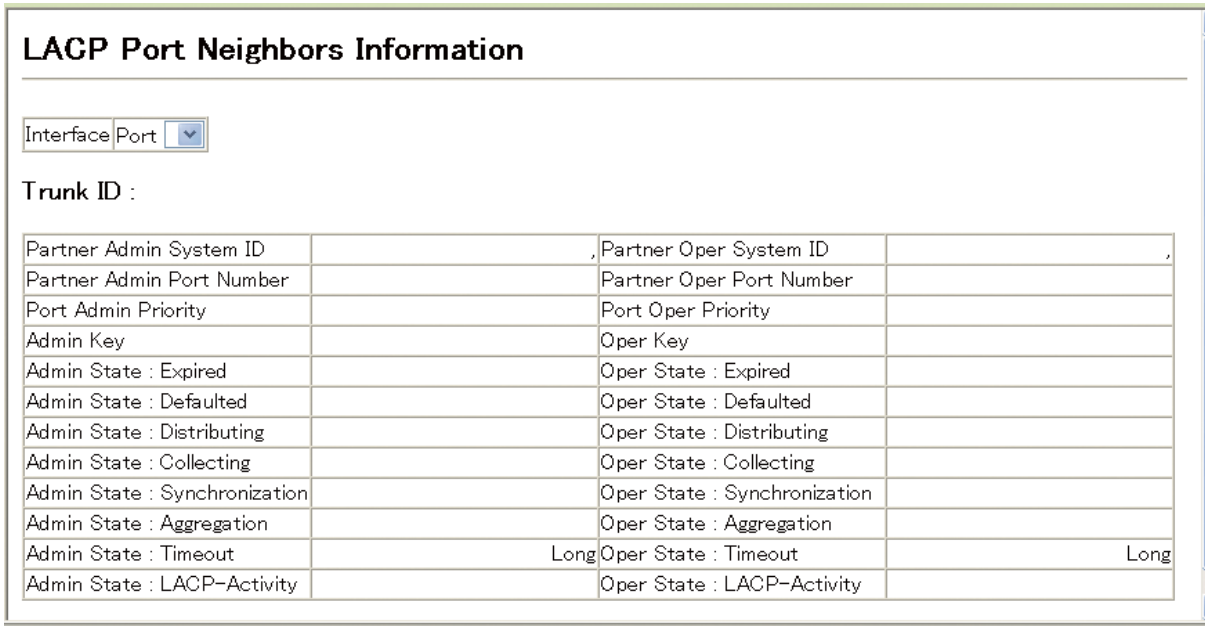
LACP のリモート側の設定及びステータスの表示を行なうことができます。

隣接設定情報

項目	解説
Partner Admin System ID	ユーザにより指定された LAG partner のシステム ID
Partner Oper System ID	LACP プロトコルにより指定された LAG partner のシステム ID
Partner Admin Port Number	プロトコル partner 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 partner によりアグリゲーションポートに指定された運用ポート番号
Port Admin Priority	プロトコル partner のポートプライオリティの現在の管理値
Port Oper Priority	partner により指定された本アグリゲーションポートのプライオリティ
Admin Key	プロトコル partner のキーの現在の管理値
Oper Key	プロトコル partner のキーの現在の運用値
Admin State	partner のパラメータの管理値（前の表を参照）
Oper State	partner のパラメータの運用値（前の表を参照）

設定方法

[Port] → [LACP] → [Port Neighbors Information] をクリックします。表示する port channel を選択すると関連情報が表示されます。



3.7.4 ストームしきい値の設定

ブロードキャスト、マルチキャスト、アンノウンユニキャストストームは、ネットワーク上のデバイスが誤作動した場合や、アプリケーションプログラムの設計が正しくない、適切に構成されていない時に起こります。ネットワーク上でこれらのトラフィックが過度に発生した場合、ネットワークの性能は大幅に低下し、通信が完全に中断されることがあります。

各ポートのブロードキャスト、マルチキャスト、アンノウンユニキャストトラフィックのしきい値を設定することにより各種ストームからネットワークを保護することができます。
指定されたしきい値を超えたパケットはドロップされます。

機能解説

- **各種ストームコントロールは初期設定で有効になっています。**

設定・表示項目

Port/Trunk Broadcast Control

Threshold

ポートを通過するブロードキャストパケットの閾値を設定できます
(Scale **範囲：**8Kbits、80Kbits、800Kbits、8Mbits **初期設定：**8Mbit
Level **範囲：**1-127 **初期設定：**5)

Port

ポート番号

Type

ポートの種類を表示

Protect Status

ブロードキャストストームコントロールの有効 / 無効（初期設定：有効）

Trunk

トランクメンバーのポートの場合表示（Port **設定時のみ表示）**

Port/Trunk Multicast Control

Threshold

(Scale **範囲：**8Kbits、80Kbits、800Kbits、8Mbits **初期設定：**8Mbit
Level **範囲：**1-127 **初期設定：**5)

Port

ポート番号

Type

ポートの種類を表示

Protect Status

マルチキャストストームコントロールの有効 / 無効（初期設定：有効）

Trunk

トランクメンバーのポートの場合表示（Port **設定時のみ表示）**

Port/Trunk Unknown Unicast Control

Threshold

(Scale　**範囲：**8Kbits、80Kbits、800Kbits、8Mbits　**初期設定：**8Mbit
Level　**範囲：**1-127　**初期設定：**5)

Port

ポート番号

Type

ポートの種類を表示

Protect Status

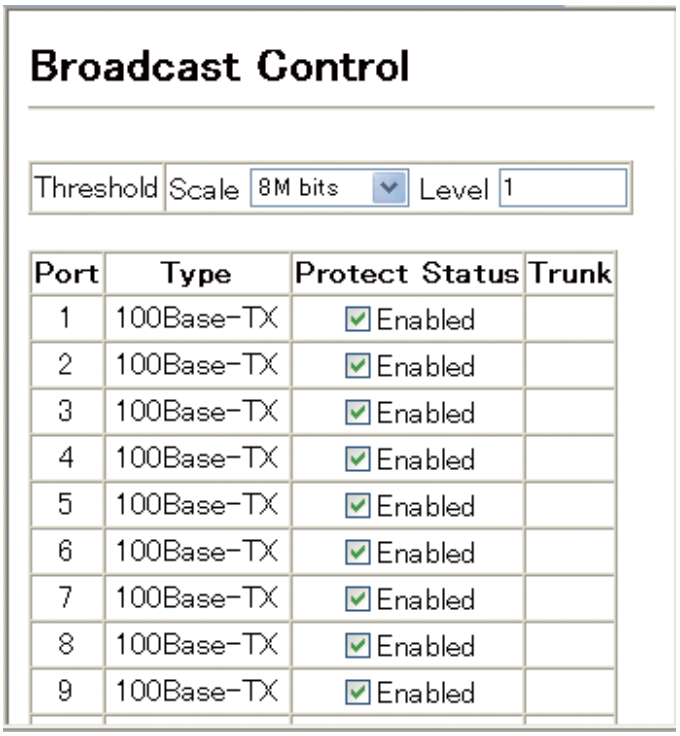
アンノウンユニキャストストームコントロールの有効 / 無効（初期設定：有効）

Trunk

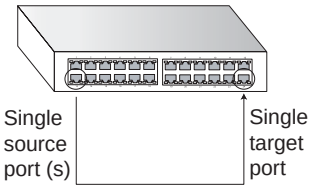
トランクメンバーのポートの場合表示（Port **設定時のみ表示）**

設定方法

[Port] → [Port Broadcast Control] **をクリックします。**Threshold**（しきい値）を設定し、**[Apply] **をクリックします。**



3.7.5 ポートミラーリングの設定



リアルタイムで通信の解析を行うために、ソースポートからターゲットポートへ通信のミラーリングをする事ができます。それにより、ターゲットポートにネットワーク解析装置（Sniffer 等）又は RMON プローブを接続し、通信に影響を与えずにソースポートのトラフィックを解析することができます。

機能解説

- ソースポートとターゲットポートの通信速度は同じでなければいけません。通信速度が異なる場合には、通信がターゲットポート側で落とされます。
- 全てのミラーセッションは、同じポートターゲットポートを共有します。
- ソースポートとターゲットポートは同じ VLAN 内に所属する必要があります。

設定・表示項目

Mirror Sessions

現在のミラーセッションの一覧を表示します。

Source Port

通信がモニターされるソースポート

Type

モニターを行う通信の種類。

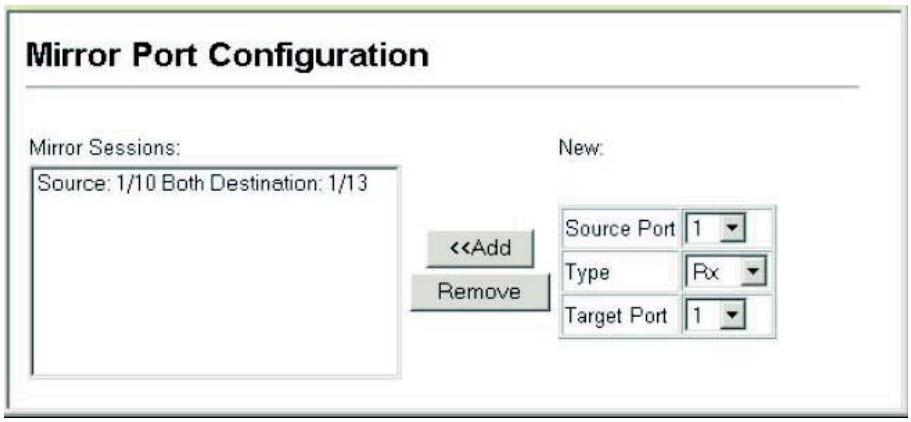
Rx（受信）、Tx（送信）、Both（送・受信）（初期設定：Rx）

Target Port

ソースポートの通信のミラーリングがされるターゲットポート

設定方法

[Port] → [Mirror] をクリックします。Source Port（ソースポート）及び Type（ミラーリングするトラフィックタイプ）そして Target Port（ターゲットポート）を指定し、[Add] をクリックします。



3.7.6 帯域制御

帯域制御機能では各インタフェースの送信及び受信の最大速度を設定することができます。帯域制御を有効にすると、通信はハードウェアにより監視され、設定を超える通信はドロップされます。設定範囲内の通信はそのまま転送されます。

機能解説

- **各インタフェースに対し、入力及び出力の帯域制御の有効 / 無効を設定できます。**

設定・表示項目（Input/Output Rate Limit Port Configuration 共通）

Port

ポート番号

Input/Output Rate Limit Status

帯域制御の有効 / 無効（初期設定：無効）

Input/Output Rate Limit Scale

帯域制御のスケールを設定（範囲：8Mbits、80Kbits **初期設定：**8Mbits）

Input/Output Rate Limit Level

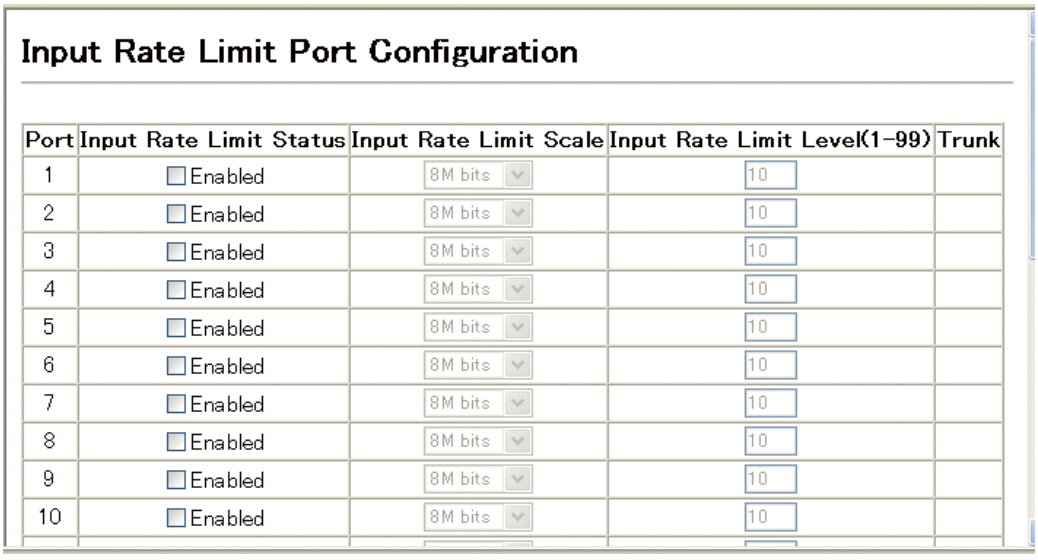
帯域制御のレベルを設定（範囲：1-99 **初期設定：**10）

Trunk

トランクメンバーのポートの場合表示

設定方法

[Port] → [Rate Limit] → [Input Port/Output Port Configuration] **をクリックします。各インタフェースに対して** [Rate Limit Status] **を選択し、**[Rate Limit Scale]、[Rate Limit Level] **を設定し、**[Apply] **をクリックします。**



[注意] TCP における入力に対しての帯域制御（Ingress Rate-Limit）はサポートしておりません。

3.7.7 ポート統計情報表示

RMON MIB をベースとした通信の詳細情報の他、Ethernet-like MIB やインタフェースグループからのネットワーク通信の標準的な統計情報の表示を行うことができます。

インタフェース及び Ethernet-like 統計情報は各ポートの通信エラー情報を表示します。これらの情報はポート不良や、重負荷などの問題点を明確にすることができます。

RMON 統計情報は各ポートのフレームタイプ毎の通信量を含む幅広い統計情報を提供します。すべての値はシステムが再起動された時からの累積数となり、毎秒単位 (per second) で表示されます。初期設定では統計情報は 60 秒ごとに更新されます。

[注意] RMONグループ2、3、9は、SNMP管理ソフトウェアを使用しないと利用できません。

統計値

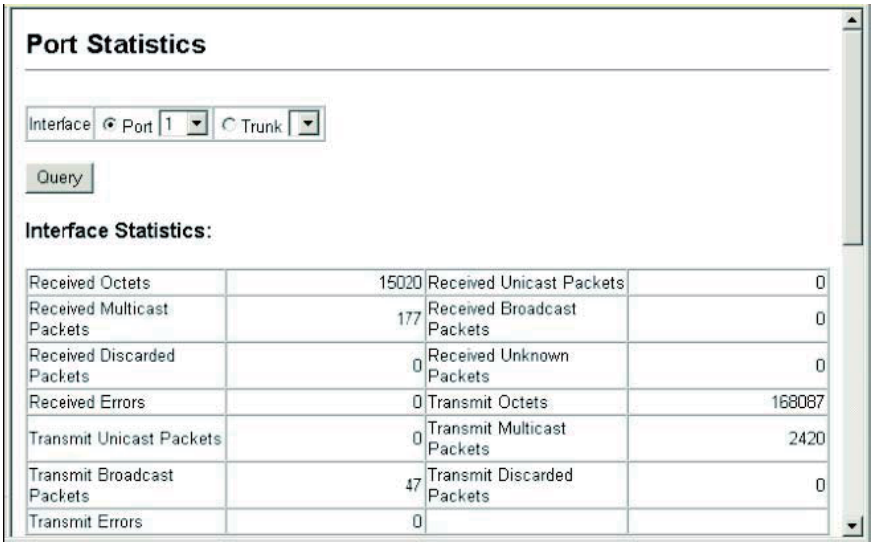
パラメータ	解説
Interface Statistics	
Received Octets	フレーム文字を含むインタフェースで受信されたオクテットの数
Received Unicast Packets	層位プロトコルで受信したサブネットワークユニキャストパケットの数
Received Multicast Packets	このサブレイヤから送信され、高層のレイヤで受信されたパケットで、このサブレイヤのマルチキャストアドレス宛てのパケットの数
Received Broadcast Packets	このサブレイヤから送信され、高層のレイヤで受信されたパケットで、このサブレイヤのブロードキャストアドレス宛てのパケットの数
Received Discarded Packets	ラー以外の理由で削除された受信パケットの数。パケットが削除された理由は、バッファスペースを空けるためです
Received Unknown Packets	インタフェースから受信したパケットで、未知又は未対応プロトコルのために削除されたパケットの数。
Received Errors	受信パケットで、上層位プロトコルへ届けることを妨げるエラーを含んでいたパケットの数。
Transmit Octets	フレーム文字列を含むインタフェースから送信されたオクテットの数。
Transmit Unicast Packet	上層位プロトコルがサブネットワークユニキャストアドレスに送信するよう要求したパケットの数。(削除されたパケット及び送信されなかったパケットを含む)
Transmit Multicast Packets	上層位プロトコルが要求したパケットで、このサブレイヤのマルチキャストアドレスに宛てられたパケットの数。(削除されたパケット及び送信されなかったパケットを含む)
Transmit Broadcast Packets	上層位プロトコルが要求したパケットで、このサブレイヤのブロードキャストアドレスに宛てられたパケットの数。(削除されたパケット及び送信されなかったパケットを含む)
Transmit Discarded Packets	エラー以外の理由で削除されたアウトバウンドパケットの数。パケットが削除された理由は、バッファスペースを空けるためです。
Transmit Errors	エラーにより送信されなかったアウトバウンドパケットの数
Etherlike Statistics	
Alignment Errors	整合性エラー数 (同期ミスデータパケット)
Late Collisions	512 ビットタイムより後にコリジョンが検出された回数
FCS Errors	特定のインタフェースで受信したフレームで、完全なオクテットの長さで、FCS チェックにパスしなかったフレームの数。frame-too-long frame-too-short エラーと共に受信したフレームは除きます。

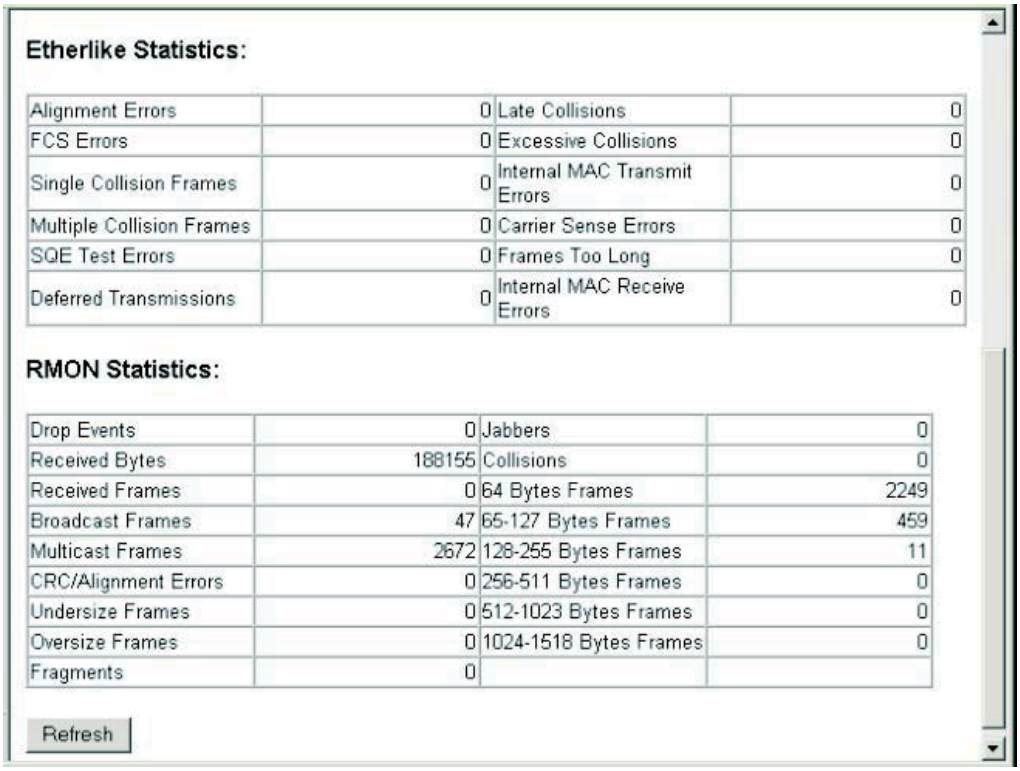
Excessive Collisions	特定のインタフェースでコリジョンの多発によりエラーを起こしたパケット数。full-duplex モードでは動作しません。
Single Collision	1 つのコリジョンで転送が妨げられたフレームで、送信に成功したフレーム数
Internal MAC Transmit Errors	内部の MAC サブレイヤーエラーにより特定のインタフェースへの送信に失敗したフレーム数
Multiple Collision Frames	2 つ以上のコリジョンで転送が妨げられたフレームで、送信に成功したフレーム数
Carrier Sense Errors	レームを送信しようとした際、キャリアセンスの状況が失われたり、機能しなかった回数
SQE Test Errors	特定のインタフェースの PLS サブレイヤで SQE TEST ERROR メッセージが生成された回数
Frames Too Long	特定のインタフェースで受信したフレームで許容最大フレームサイズを超えたフレームの数
Deferred Transmissions	メディアが使用中のため、特定のインタフェース上で最初の送信試みが遅延したフレーム数
Internal MAC Receive Errors	内部の MAC サブレイヤーエラーにより特定のインタフェースへの受信に失敗したフレーム数
RMON Statistics	
Drop Events	ソースの不足によりパケットがドロップした数
Jabbers	フレーミングビットを除き、FCS オクテットは含む)1518 オクテットより長いフレームで、FCS 又は配列エラーを含む受信フレーム数で
Received Bytes	ネットワークから受信した総バイト数。本統計情報は容易なイーサネット利用状況の目安となります。
Collisions	本 Ethernet セグメント上のコリジョンの総数の最良推定数
Received Frames	受信したすべてのフレーム数 (不良フレーム、ブロードキャストフレーム、マルチキャストフレーム)
Broadcast Frames	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転送したフレーム数。マルチキャストパケットは含まない。
Multicast Frames	信した正常なフレームのうち、このマルチキャストアドレスに転送したフレーム数
CRC/Alignment Errors	CRC/ 配列エラー数 (FCS 又は配列エラー)
Undersize Frames	フレーミングビットを除き、FCS オクテットは含む)64 オクテットより短い長さの受信フレーム数で、その他の点では正常な受信フレーム数
Oversize Frames	フレーミングビットを除き、FCS オクテットは含む)1518 オクテットよりも長い受信フレームで、その他の点では正常な受信フレーム数
Fragments	フレーミングビットを除き、FCS オクテットは含む)64 オクテットよりも小さい長さで FCS もしくは配列エラーがあった受信フレーム数
64 Bytes Frames	不良パケットを含む送受信トータルフレーム数 (フレーミングビットを除き、FCS オクテットは含みます。)
65-127 Byte Frames 128-255 Byte Frames 256-511 Byte Frames 512-1023 Byte Frames 1024-1518 Byte Frames 1519-1536 Byte Frames	不良パケットを含む送受信トータルフレーム数で、各オクテット数の範囲に含まれるもの (フレーミングビットを除き、FCS オクテットは含みます。)

設定方法

[Port] → [Port Statistics] をクリックします。表示するインタフェースを選択し [Query] をクリックします。

ページ下部の Refresh ボタンを使用することで、表示されている内容を最新の情報に更新することができます。





3.8 アドレステーブル

本機には認知されたデバイスの MAC アドレスが保存されています。この情報は受送信ポート間での通信の送信に使用されます。通信の監視により学習された全ての MAC アドレスは動的アドレステーブルに保存されます。また、手動で特定のポートに送信する静的なアドレスを設定することができます。

3.8.1 動的アドレステーブルの設定

静的アドレスは本機の指定されたインタフェースに割り当てることができます。静的アドレスは指定したインタフェースに送信され、他へは送られません。静的アドレスが他のインタフェースで見つかった場合は、アドレスは無視されアドレステーブルには登録されません。

設定・表示項目

Static Address Counts

手動設定した静的アドレス数　*Web のみ

Current Static Address Table

静的アドレスの一覧

Interface

静的アドレスと関連したポート又はトランク

MAC Address

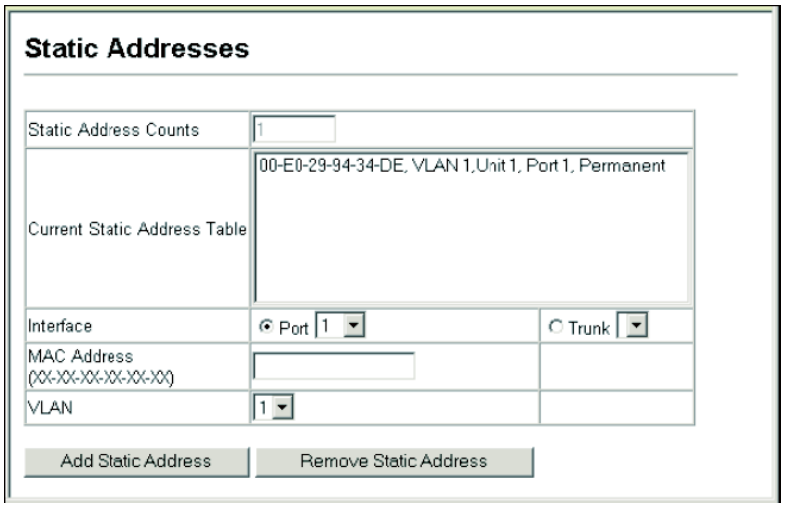
インタフェースの MAC アドレス

VLAN

VLAN ID(1-4094)

設定方法

[Address Table] → [Static Addresses] をクリックします。インタフェース、MAC アドレス及び VLAN を設定し、[Add Static Address] をクリックします。



3.8.2 アドレステーブルの表示

動的アドレステーブルには、入力された通信の送信元アドレスの監視により学習した MAC **アドレスが保存されています。入力された通信の送信先アドレスがアドレステーブル内で発見された場合、パケットはアドレステーブルに登録された関連するポートへ直接転送されます。アドレステーブルに見つからなかった場合には全てのポートに送信されます。**

設定・表示項目

Interface

ポート又はトランク

MAC Address

インタフェースの MAC **アドレス**

VLAN

VLAN ID (1-4094)

Address Table Sort Key

リストの並びを MAC **アドレス、**VLAN**、インタフェースから選択**

Dynamic Address Counts

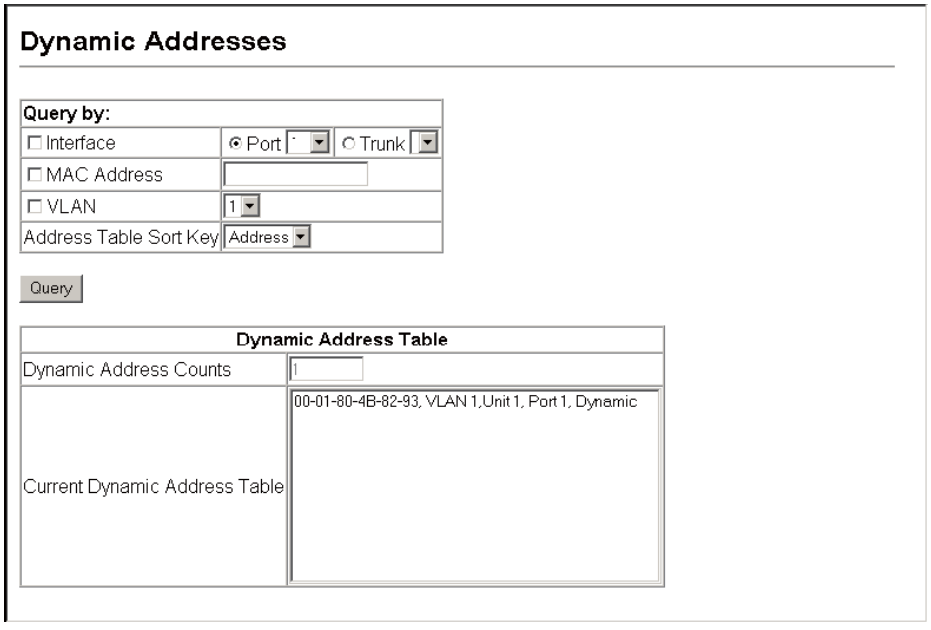
動的に学習する MAC **アドレス数**

Current Dynamic Address Table

動的に学習された MAC **アドレスのリスト**

設定方法

[Address Table] → [Dynamic Addresses] **をクリックします。**Query By**（検索を行う種類）を** Interface**、**MAC Address **又は** VLAN **から選択し、**Address Table Sort Key**（表示するアドレスの分類方法）を指定し、**[Query] **をクリックします。**



3.8.3 エージングタイムの変更

動的アドレステーブルに学習されたアドレスが削除されるまでの時間（エージングタイム）を設定することができます。

設定・表示項目

Aging Status

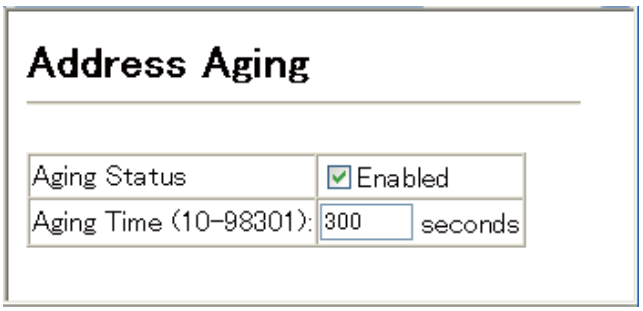
エージングタイムの機能の有効 / 無効

Aging Time

MAC **アドレスエージングタイム（範囲：**10-98301 **秒、初期設定：**300 **秒）**

設定方法

[Address Table] → [Address Aging] **をクリックします。新しい** Aging Time **（エージングタイム）を設定し、**[Apply] **をクリックします。**



3.9 スパニングツリーアルゴリズム

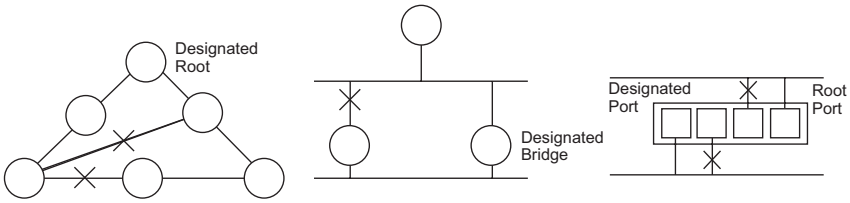
スパニングツリープロトコル STP はネットワークのループを防ぎ、また、スイッチ、ブリッジ及びルータ間のバックアップリンクを確保するために使用します。

STP 機能を有するスイッチ、ブリッジ及びルータ間で互いに連携し、各機器間のリンクで 1 つのルートがアクティブになるようにします。また、別途バックアップ用のリンクを提供し、メインのリンクがダウンした場合には自動的にバックアップを行います。

本機は、以下の規格に準拠した STP に対応しています。

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

STP はスパニングツリーネットワークの経路となる STP 対応スイッチ・ブリッジ又はルータを選択するために分散アルゴリズムを使用します。それにより、デバイスからルートデバイスにパケットを送信する際に最小のパスコストとなるようにルートデバイスを除く各デバイスのルートポートの設定を行います。これにより、ルートデバイスから LAN に対し最小のパスコストにより各 LAN の指定されたデバイスに対してパケットが転送されます。その後、指定のポートとして各関連する LAN 又はホストデバイスと通信する指定ブリッジ上のポートを選択します。



最小コストのスパニングツリーが決定した後、すべてのルートポートと指定ポートが有効となり、他のポートは無効となります。それによりパケットはルートポートから指定ポートにのみ送信され、ネットワークのループが回避されます。

安定したネットワークトポロジーが確立された後、ルートブリッジから送信される Hello BPDU(Bridge Protocol Data Units) をすべてのブリッジが受信します。定められた間隔（最大値）以内にブリッジが Hello BPDU を確認できない場合、ルートブリッジへの接続を行っているリンクを切断します。そして、このブリッジはネットワークの再設定を行ない有効なネットワークトポロジーを回復するために、他のブリッジとネゴシエーションを開始します。

RSTP は既存の遅い STP に代わる機能とされています。RSTP は MSTP にも組み込まれています。RSTP はあらかじめ障害時の代替ルートを定め、ツリー構造に関連のない転送情報を区別することにより、STP に比べ約 10 分の 1 の速さでネットワークの再構築が行えます。

STP 又は RSTP を利用した場合、すべての VLAN メンバー間での安定的なパスの提供が難しくなります。ツリー構造の頻繁な変更により一部のグループメンバーが孤立してしまうことがあります。（RSTP の拡張である）MSTP では、VLAN グループ毎に独立したスパニングツリーを提供することができます。特定の VLAN を Multiple Spanning Tree インスタンス (MSTI) に含むように指定すると、MSTI ツリーが自動的に構成され、各 VLAN の接続状況が維持されます。

各インスタンスは、Common Spanning Tree (CST) 内の RSTP ノードとして扱われるので、MSTP は、ネットワーク全体との接続を行なうことができます。

3.9.1 グローバル設定の表示

STP 情報ページから現在の STP の情報を確認することができます。

設定・表示項目

Spanning Tree State

STP が有効で STP ネットワークに参加しているかを表示します。

Bridge ID

STP で本機を認識するための一意の ID を表示します。ID は本機の STP プライオリティと MAC アドレスから算出されます。

Max Age

本機が再設定される前に設定メッセージを待ち受ける最大の時間（秒）が表示されます。

指定ポートを除く全機器のポートで、通常のインターバル内に設定メッセージが受信される必要があります。STP 情報がエージアウトしたすべてのポートは接続されている LAN の指定ポートに変更されます。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のポートから新たなルートポートが選択されます。

Hello Time

ルートデバイスが設定メッセージを送信する間隔（秒）が表示されます。

Forward Delay

機器状態の遷移に対してルート機器が待機する最大の時間（秒）で表示されます。フレームの転送が開始される前に、トポロジの変更を機器に認識させるため、遅延を設定する必要があります。さらに各ポートでは、一時的なデータのループを防ぐため、ポートをブロック状態に戻す競合情報のリスニングを行う時間が必要になります。

Designated Root

ルートデバイスに設定された、スパニングツリー内の機器のプライオリティ及び MAC アドレスが表示されます。

- Root Port ― ルートに最も近いポートの番号が表示されます。ルートデバイスとの通信は、このポートを介して行われます。ルートポートが存在しない場合は、本機がスパニングツリーネットワーク上のルートデバイスとして設定されたことを表します。
- Root Path Cost ― 本機のルートポートからルートデバイスまでのパスコストが表示されます。

Configuration Changes

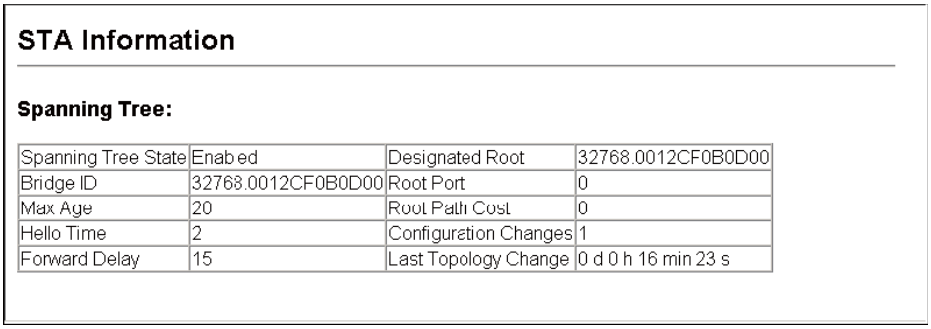
スパニングツリーが再設定された回数が表示されます。

Last Topology Change

最後にスパニングツリーが再設定されてから経過した時間が表示されます。

設定方法

[Spanning Tree] → [STA Information] をクリックします。現在の STP 情報が表示されます。



STA Information

Spanning Tree:

Spanning Tree State	Enabled	Designated Root	32768.0012CF0B0D00
Bridge ID	32768.0012CF0B0D00	Root Port	0
Max Age	20	Root Path Cost	0
Hello Time	2	Configuration Changes	1
Forward Delay	15	Last Topology Change	0 d 0 h 16 min 23 s

3.9.2 グローバル設定

ここでの設定は本機全体に適用されます。

機能解説

- Spanning Tree Protocol
  本機の初期設定では RSTP **に指定されていますが、**STP **に設定し** IEEE802.1D **に準拠した** BPDU **のみを送信することができます。この場合、ネットワーク全体に対して** 1 **つの** SpanningTree **のみの設定が行なえます。もしネットワーク上に複数の** VLAN **を設定する場合、一部の** VLAN **メンバー間はネットワークのループを回避するため無効となる場合があります。複数の** VLAN **を構成する場合には** MSTP **を使用することを推奨します。**

- Rapid Spanning Tree Protocol
  RSTP **は、以下のそれぞれの着信プロトコルメッセージを監視し動的に各プロトコルメッセージに適合させることにより、**STP **と** RSTP **ノードのどちらへの接続もサポートします。**

  - **STP Mode** ― **ポートの移動遅延タイマーが切れた後に** IEEE802.1D BPDU **を受け取ると、本機は** IEEE802.1D **ブリッジと接続していると判断し、**IEEE802.1D BPDU **のみを使用します。**
  - **RSTP Mode** ― RSTP **において、ポートで** IEEE802.1D BPDU **を使用しポート移動遅延タイマーが切れた後に** RSTP BPDU **を受け取ると、**RSTP **は移動遅延タイマーを再スタートさせそのポートに対し** RSTP BPDU **を使用します。**

- Multiple Spanning Tree Protocol

  - **ネットワーク上で** MSTP **を有効にするには、接続された関連するブリッジにおいても同様の** MSTP **の設定を行ない、スパニングツリーインスタンスに参加することを許可する必要があります。**
  - **スパニングツリーモードを変更する場合、変更前のモードのスパニングツリーインスタンスをすべて止め、その後新しいモードにおいて通信を再開します。スパニングツリーのモード変更時には通信が一時的に遮断されるので注意して下さい。**

設定・表示項目

グローバル設定の基本設定

Spanning Tree State

スパニングツリーを有効又は無効にします。(初期設定 : **有効**)

Spanning Tree Type

使用されるスパニングツリープロトコルの種類を指定します。(初期設定 :RSTP)

- **STP** ― Spanning Tree Protocol **(**IEEE 802.1D**。**STP **を選択すると、本機は** RSTP **の** STP **互換モードとなります)**
- **RSTP** ― Rapid Spanning Stree Protocol(IEEE 802.1w)
- **MSTP** ―Multiple Spanning Stree Protocol(IEEE 802.1s)

Spanning Tree BPDU Flooding

BPUD **のフラッディングを設定します。(**To VLAN **または** To All**)**

Priority

ルートデバイス、ルートポート、指定ポートの識別に使用される、デバイスプライオリティを設定できます。最上位のプライオリティを持つ機器が STP **ルート機器になります(値が小さいほどプライオリティが高くなります)。すべての機器のプライオリティが同じ場合は、最小の** MAC **アドレスを持つ機器がルート機器になります。(初期設定** :32768**、範囲** : 0-61440 **の値で** 4096 **ずつ** (0**、**4096**、**8192**、**12288**、**16384**、**20480**、**24576**、**28672**、**32768**、**36864**、**40960**、**45056**、**49152**、**53248**、**57344**、**61440))**

ルート機器設定

Hello Time

ルートデバイスが設定メッセージを送信する間隔(秒)を設定できます(初期設定 :2(**秒**)**、最小値** :1**、最大値** :10 **又は** [(Maximum Age/2)-1] **の小さい方の値)**

Maximum Age

機器が再設定される前に設定メッセージを待ち受ける、最大の時間を秒で設定できます。指定ポートを除く全機器のポートで、通常のインターバル内に設定メッセージが受信される必要があります。STP **情報がエージアウトしたポートは接続されている** LAN **の指定ポートに変更されます。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のポートから新たなルートポートが選択されます。(初期設定** :20**(秒)、最小値** :6 **又は** [2 × (Hello Time+1)] **の大きい方の値、最大値** :40 **もしくは** [2 × (Forward Delay-1)] **小さい方の値)**

Forward Delay

機器状態の遷移に対してルート機器が待機する最大の時間(秒)が設定できます。フレームの転送が開始される前に、トポロジの変更を機器に認識させるため、遅延を設定する必要があります。さらに各ポートでは、一時的なデータのループを防ぐため、ポートをブロック状態に戻す競合情報のリスニングを行う時間が必要になります(初期設定 :15**(秒)、最小値** :4 **又は** [(Maximum Age/2)+1] **の大きい方の値、最大値** :30**)**

RSTP 設定

Path Cost Method

パスコストはデバイス間の最適なパスを決定するために使用されます。パスコスト方式は各インタフェースに割り当てることのできる値の範囲を決定するのに使用されます。

- Long ― 32 **ビットの** 1-200,000,000 **の値 (初期値)**
- Short ― 16 **ビットの** 1-65535 **の値**

Transmission Limit

継続的なプロトコルメッセージの最小送信間隔の設定による BPDU **の最大転送レートの設定を行います（範囲** :1-10**（秒）、初期設定** :3**）**

*MSTP **設定***

Max Instance Numbers

本機で設定可能な MST **インスタンスの最大数（初期設定：**65**）**

Region Revision*

MST **インスタンスのリビジョン（設定範囲：**0-65535**、初期設定：**0**）**

Region Name*

MST **インスタンス名（最大値：**32 **文字）**

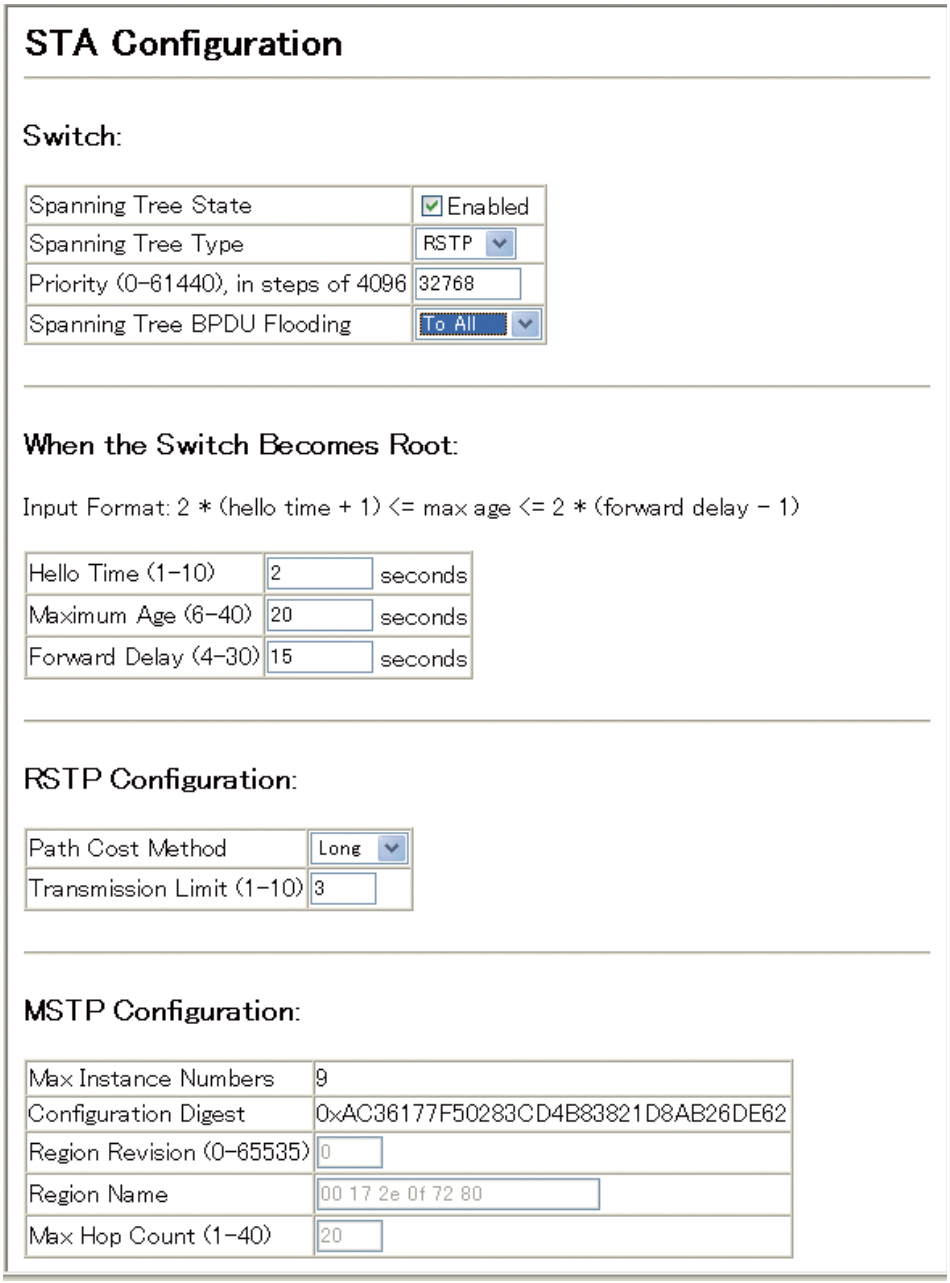
Maximum Hop Count

BPDU **が破棄される前の** MST **内での最大ホップ数（設定範囲：**1-40**、初期設定：**20**）**

* MST name **及び** revision number **は** MST **の特定を行なうため、どちらも必要となります。**

設定方法

[Spanning Tree] → [STA Configuration] をクリックします。必要な設定項目を変更し、[Apply] をクリックします。



3.9.3 インタフェース設定の表示

STA Port Information 及び STA Trunk Information 画面では STA ポート及び STA トランクの現在の状態を表示します。

設定・表示項目

Spanning Tree

STA の有効 / 無効が表示されます。

STA Status

スパニングツリー内での各ポートの現在の状態を表示します :

- Discarding — STP 設定メッセージを受信しますが、パケットの送信は行っていません。
- Learning — 矛盾した情報を受信することなく、Forward Delay で設定した間隔で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はクリアされ、アドレスの学習が開始されています。
- Forwarding — パケットの転送が行われ、アドレスの学習が継続されています。

ポート状態のルール :

- STP 準拠のブリッジデバイスが接続されていないネットワークセグメント上のポートは、常に転送状態 (Forwarding) にあります。
- 他の STP 準拠のブリッジデバイスが接続されていないセグメント上に、2 個のポートが存在する場合は、ID の小さい方でパケットの転送が行われ (Forwarding)、他方ではパケットが破棄されます (Discarding)。
- 起動時にはすべてのポートでパケットが破棄されます (Discarding)。その後学習状態 (Learning)、フォワーディング (Forwarding) へと遷移します。

Forward Transitions

ポートが転送状態 (Forwarding) に遷移した回数が表示されます。

Designated Cost

スパニングツリー設定における、本ポートからルートへのコストが表示されます。媒体が遅い場合、コストは増加します。

Designated Bridge

スパニングツリーのルートに到達する際に、本ポートから通信を行うデバイスのプライオリティと MAC アドレスが表示されます。

Designated Port

スパニングツリーのルートに到達する際に、本機と通信を行う指定ブリッジデバイスのポートのプライオリティと番号が表示されます。

Oper Link Type

インタフェースの属する LAN セグメントの使用中の 2 点間の状況。この項目は STP Port/Trunk Configuration ページの Admin Link Type に記載されているように手動設定又は自動検出により決定されます。

Oper Edge Port

この項目は STP Port/Trunk Configuration ページの Admin Eddge Port の設定により設定のために初期化されます。しかし、このポートへの接続された他のブリッジを含め、BPDU を受信した場合は false に設定されます。

Port Role

実行中のスパニングツリートポロジの一部であるかないかに従って役割が割り当てられています。

- Root **ポート — ルートブリッジへのブリッジに接続します。**
- Designated **ポート — ルートブリッジへのブリッジを通じて** LAN **に接続します。**
- Master **ポート** — MSTI regional **ルート**
- Alternate **又は** Backup **ポート — 他のブリッジ、ブリッジポート又は** LAN **が切断または削除された場合に、接続を提供します。**
- Disabled **ポート — スパニングツリー内での役割がない場合には無効** (Disabled) **となります。**

Trunk Member

トランクメンバーに設定されているかどうかを表示します。(STA Port Information **ページのみ)**

設定方法

[Spanning Tree] → [STA] → [Port Information] **又は** [Trunk Information] **をクリックします。**

STA Port Information

Port	Spanning Tree	STA Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port	Oper Path Cost	Oper Link Type	Oper Edge Port	Port Role	Trunk Member
1	Enabled	Forwarding	1	0	32768.0013F7CFAFAC	128.1	10000	Point-to-Point	Disabled	Designated	
2	Enabled	Discarding	0	0	32768.0013F7CFAFAC	128.2	10000	Point-to-Point	Disabled	Disabled	
3	Enabled	Discarding	0	0	32768.0013F7CFAFAC	128.3	10000	Point-to-Point	Disabled	Disabled	
4	Enabled	Discarding	0	0	32768.0013F7CFAFAC	128.4	10000	Point-to-Point	Disabled	Disabled	
5	Enabled	Discarding	0	0	32768.0013F7CFAFAC	128.5	10000	Point-to-Point	Disabled	Disabled	
6	Enabled	Discarding	0	0	32768.0013F7CFAFAC	128.6	10000	Point-to-Point	Disabled	Disabled	

3.9.4 インタフェース設定

ポートプライオリティ、パスコスト、リンクタイプ及びエッジポートを含む各インタフェースの RSTP 及び MSTP 属性を設定することができます。
ネットワークのパスを指定するために同じメディアタイプのポートに対し異なるプライオリティ又はパスコストを設定し、二点間接続または共有メディア接続を示すためリンクタイプを設定します。また、ファストフォワーディングをサポートした機器を接続した場合にはエッジポートの指定を行います。(本項での " ポート " とは " インタフェース " を意味するため、ポートとトランクの両方を示します)

設定・表示項目

以下の設定は変更することはできません。

STA Status

スパニングツリー内での各ポートの現在の状態を表示します :

(詳細は P128 「インタフェース設定の表示」を参照して下さい)

- **Discarding** ― STP 設定メッセージを受信しますが、パケットの送信は行っていません。
- **Learning** ― 矛盾した情報を受信することなく、Forward Delay で設定した間隔で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はクリアされ、アドレスの学習が開始されています。
- **Forwarding** ― パケットの転送が行われ、アドレスの学習が継続されています。

Trunk

トランクメンバーに設定されているかどうかを表示します。

(STA Port Configuration ページのみ)

以下の設定は変更することができます。

Spanning Tree

インタフェースの STA の有効 / 無効を設定します (初期設定 : 有効)

Priority

STP での各ポートのプライオリティを設定します。
本機の全てのポートのパスコストが同じ場合には、最も高いプライオリティ (最も低い設定値) がスパニングツリーのアクティブなリンクとなります。これにより、STP においてネットワークのループを回避する場合に、高いプライオリティのポートが使用されるようになります。2 つ以上のポートが最も高いプライオリティの場合には、ポート番号が小さいポートが有効になります (初期設定 : 128、範囲 : 0-240 の 16 ずつ)

Path Cost

このパラメータは STP においてデバイス間での最適なパスを決定するために設定します。低い値がスピードの早いメディアのポートに割り当てられ、より高い値がより遅いメディアに割り当てられる必要があります (パスコストはポートプライオリティより優先されます)

- **設定範囲** :
  Ethernet: 200,000-20,000,000
  Fast Ethernet: 20,000-2,000,000
  Gigabit Ethernet: 2,000-200,000
- **初期設定** :
  Ethernet ― half duplex: 2,000,000、full duplex: 1,000,000、 trunk: 500,000
  Fast Ethernet ― half duplex: 200,000、full duplex: 100,000、 trunk: 50,000
  Gigabit Ethernet ― full duplex: 10,000、trunk: 5,000

[注意]　パスコスト方式が short に設定された場合、最大パスコストは 65,535 となります。

Admin Link Type

インタフェースへ接続する接続方式（初期設定 :Auto）

- Point-to-Point ― **他の** 1 **台のブリッジへの接続**
- Shared ― 2 **台以上のブリッジへの接続**
- Auto ― Point-to-Point **か** Shared **のどちらかを自動的に判断します。**

Admin Edge Port (Fast Forwarding)

ブリッジ型 LAN **の終端、もしくはノードの終端にインタフェースが接続されている場合、本機能を有効にすることができます。**

ノードの終端ではループが起きないため、直接、転送状態にすることができます。Edge Port **を指定することにより、ワークステーションやサーバなどのデバイスへの迅速な転送を提供し、以前の転送アドレステーブルを保持することにより、スパニングツリー再構築時のタイムアウト時間を削減します。**

但し、必ずノードの終端デバイスに接続されているポートのみで Edge Port **を有効にして下さい（初期設定：有効）**

Migration

設定及びトポロジ変更通知 BPDU **を含む** STP BPDU **を検知することにより、自動的に** STP **互換モードに変更することができます。**

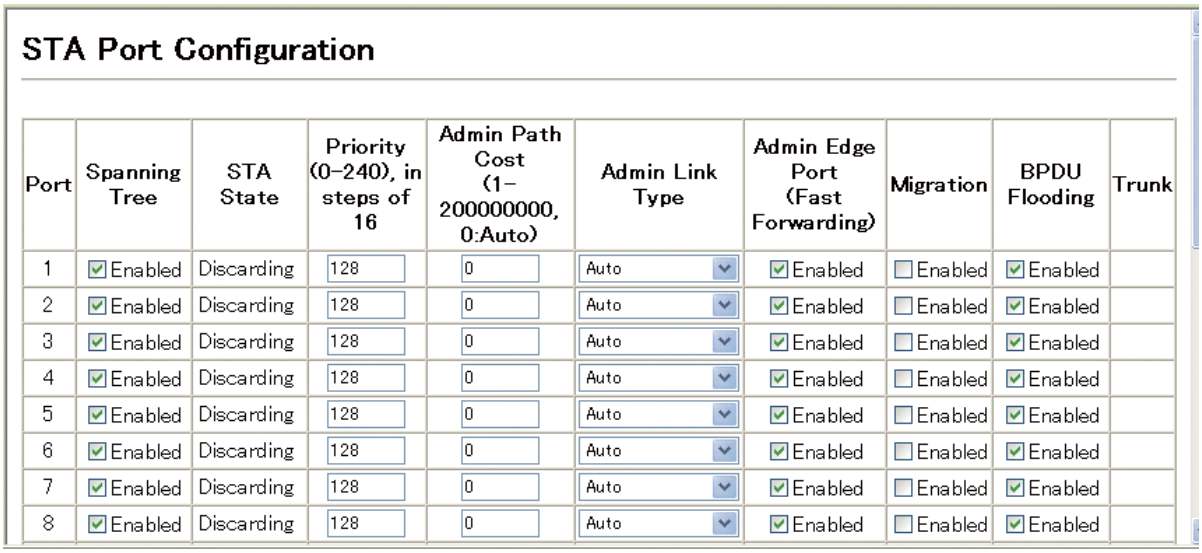
また、本機能のチェックボックスをチェックし機能を有効にすることにより、手動で適切な BPDU **フォーマット（**RSTP **又は** STP **互換）の再確認を行うことができます。**

BPDU Flooding

BPUD **フラッティングの有効 / 無効を設定します。（初期設定：有効）**

設定方法

[Spanning Tree] → [STA] → [Port Configuration] **又は** [Trunk Configuration] **をクリックします。必要な設定項目を変更し、**[Apply] **をクリックします。**



STA Port Configuration

Port	Spanning Tree	STA State	Priority (0-240), in steps of 16	Admin Path Cost (1-200000000, 0:Auto)	Admin Link Type	Admin Edge Port (Fast Forwarding)	Migration	BPDU Flooding	Trunk
1	Enabled	Discarding	128	0	Auto	Enabled	Enabled	Enabled	
2	Enabled	Discarding	128	0	Auto	Enabled	Enabled	Enabled	
3	Enabled	Discarding	128	0	Auto	Enabled	Enabled	Enabled	
4	Enabled	Discarding	128	0	Auto	Enabled	Enabled	Enabled	
5	Enabled	Discarding	128	0	Auto	Enabled	Enabled	Enabled	
6	Enabled	Discarding	128	0	Auto	Enabled	Enabled	Enabled	
7	Enabled	Discarding	128	0	Auto	Enabled	Enabled	Enabled	
8	Enabled	Discarding	128	0	Auto	Enabled	Enabled	Enabled	

3.9.5 MSTP 設定

MSTP は各インスタンスに対し特定のスパニングツリーを生成します。これによりネットワーク上に複数のパスを構築し、通信のロードバランスを行い、単一のインスタンスに不具合が発生した場合に大規模なネットワークの障害が発生することを回避すると共に、不具合の発生したインスタンスの新しいトポロジーへの変更を迅速に行ないます。

初期設定ではすべての VLAN は、MST 内に接続されたブリッジおよび LAN はすべて内部スパニング・ツリー (MST インスタンス 0) に割り当てられます。

本機では最大 65 のインスタンスをサポートしています。ネットワークの同一エリアをカバーする VLAN をグループ化するように設定して下さい。

但し、同一インスタンスのセットにより同一 MSTI 内のすべてのブリッジ、及び同一 VLAN のセットにより同一インスタンスを形成する必要があります。RSTP は単一ノードとして各 MSTI を扱い、すべての MSTI を Common Spanning Tree として接続する点に注意して下さい。

MSTP を使用するには以下の手順で設定を行なってください。

（1）スパニングツリータイプを MSTP に設定します (P124 「グローバル設定」参照)

（2）選択した MST インスタンスにスパニングツリープライオリティを入力します。

（3）MSTI を共有する VLAN を追加します。

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

MSTI をネットワーク上で有効にし、接続を継続するためには、同様の設定を関連するブリッジにおいて行なう必要があります。

設定・表示項目

MST Instance

スパニングツリーのインスタンス ID（初期設定：0）

Priority

スパニングツリーインスタンスのプライオリティ（範囲：4096 飛ばしの値で 0-61440、選択肢：0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440、初期設定：32768）

VLANs in MST Instance

インスタンスに指定された VLAN

MST ID

設定のためのインスタンス ID（設定範囲：0-57、初期設定：0）

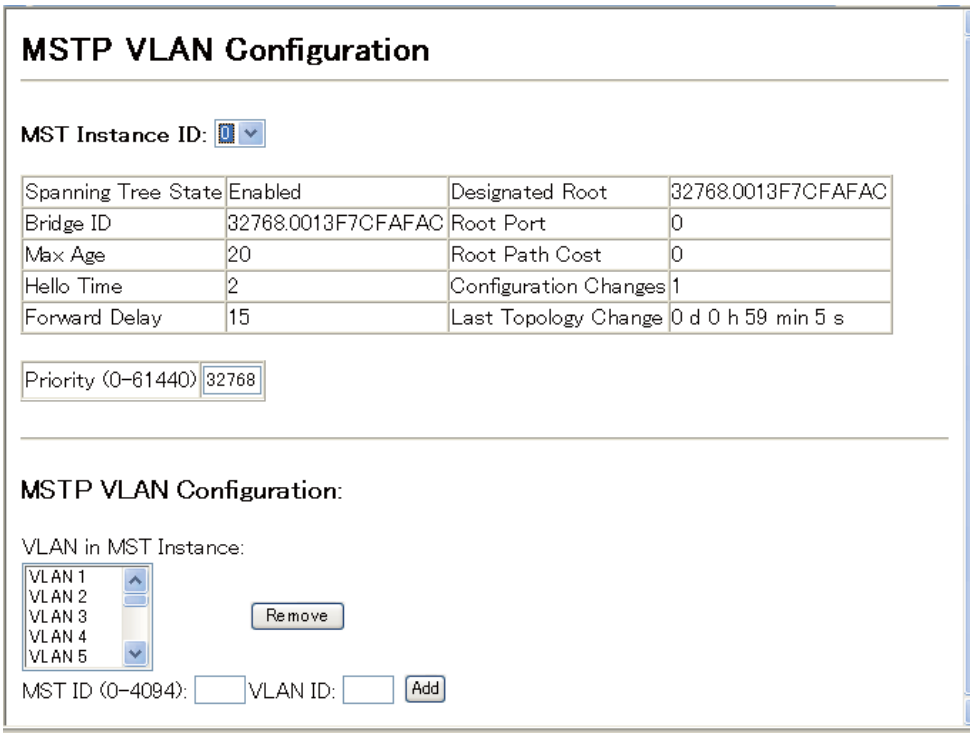
VLAN ID

MST インスタンスに指定する VLAN ID（設定範囲：1-4093）

他の項目は、P128 「インタフェース設定の表示」を参照して下さい。

設定方法

[Spanning Tree] → [MSTP] → [VLAN Configuration] をクリックします。リストから MST インスタンス ID を選択し、インスタンスプライオリティを設定し、[Add] をクリックします。MST インスタンスに VLAN を加えるには、インスタンス ID と VLAN ID を入力し、[Add] をクリックします。



3.9.6 MSTP インタフェース設定の表示

MSTP ポート / トランク情報ページでは、選択した MST インスタンスの現在のステータスを表示することができます。

設定・表示項目

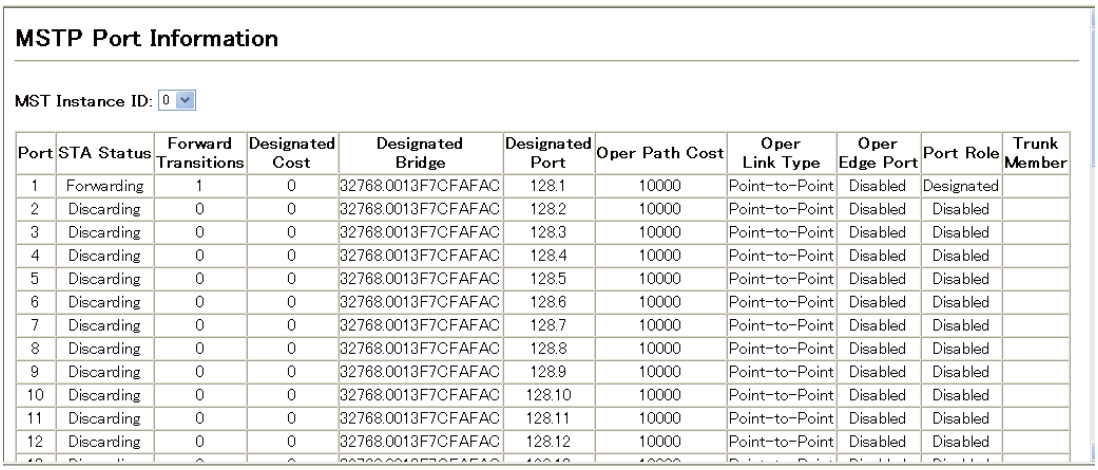
MST Instance ID

インスタンス ID（初期設定：0）

[注意] 他の項目に関しては P128 「インタフェース設定の表示」を参照して下さい。

設定方法

[Spanning Tree] → [MSTP] → [Port Information] 又は [Trunk Information] をクリックします。
MST インスタンスを選択し、現在の Spanning Tree の値を表示します。



MSTP Port Information

MST Instance ID: 0

Port	STA Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port	Oper Path Cost	Oper Link Type	Oper Edge Port	Port Role	Trunk Member
1	Forwarding	1	0	32768.0013F7CFAFAC	128.1	10000	Point-to-Point	Disabled	Designated	
2	Discarding	0	0	32768.0013F7CFAFAC	128.2	10000	Point-to-Point	Disabled	Disabled	
3	Discarding	0	0	32768.0013F7CFAFAC	128.3	10000	Point-to-Point	Disabled	Disabled	
4	Discarding	0	0	32768.0013F7CFAFAC	128.4	10000	Point-to-Point	Disabled	Disabled	
5	Discarding	0	0	32768.0013F7CFAFAC	128.5	10000	Point-to-Point	Disabled	Disabled	
6	Discarding	0	0	32768.0013F7CFAFAC	128.6	10000	Point-to-Point	Disabled	Disabled	
7	Discarding	0	0	32768.0013F7CFAFAC	128.7	10000	Point-to-Point	Disabled	Disabled	
8	Discarding	0	0	32768.0013F7CFAFAC	128.8	10000	Point-to-Point	Disabled	Disabled	
9	Discarding	0	0	32768.0013F7CFAFAC	128.9	10000	Point-to-Point	Disabled	Disabled	
10	Discarding	0	0	32768.0013F7CFAFAC	128.10	10000	Point-to-Point	Disabled	Disabled	
11	Discarding	0	0	32768.0013F7CFAFAC	128.11	10000	Point-to-Point	Disabled	Disabled	
12	Discarding	0	0	32768.0013F7CFAFAC	128.12	10000	Point-to-Point	Disabled	Disabled	

3.9.7 MSTP インタフェースの設定

MSTP ポート / トランク設定により MST インスタンスへの STA インタフェースの設定を行なうことができます。

設定・表示項目

以下の項目は設定を変更できません。

STA Status

スパニングツリー内での各ポートの現在の状態を表示します :

（詳細は 128 ページの「インタフェース設定の表示」を参照して下さい）

- Discarding ― STP 設定メッセージを受信しますが、パケットの送信は行っていません。
- Learning ― 矛盾した情報を受信することなく、Forward Delay で設定した間隔で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はクリアされ、アドレスの学習が開始されています。
- Forwarding ― パケットの転送が行われ、アドレスの学習が継続されています。

Trunk Member

トランクメンバーに設定されているかどうかを表示します。

（STA Port Configuration ページのみ）

以下の項目は設定を変更できます。

MST Instance ID

設定のインスタンス ID（初期設定：0）

Priority

STP での各ポートのプライオリティを設定します。

本機の全てのポートのパスコストが同じ場合には、最も高いプライオリティ（最も低い設定値）がスパニングツリーのアクティブなリンクとなります。これにより、STP においてネットワークのループを回避する場合に、高いプライオリティのポートが使用されるようになります。2 つ以上のポートが最も高いプライオリティの場合には、ポート番号が小さいポートが有効印なります（初期設定 : 128、範囲 : 0-240 の 16 ずつ）

MST Path Cost

このパラメータは MSTP においてデバイス間での最適なパスを決定するために設定します。低い値がスピードの早いメディアのポートに割り当てられ、より高い値がより遅いメディアに割り当てられる必要があります（パスコストはポートプライオリティより優先されます）

－設定範囲 :

Ethernet: 200,000-20,000,000

Fast Ethernet: 20,000-2,000,000

Gigabit Ethernet: 2,000-200,000

－初期設定 :

Ethernet ― half duplex: 2,000,000、full duplex: 1,000,000、 trunk: 500,000

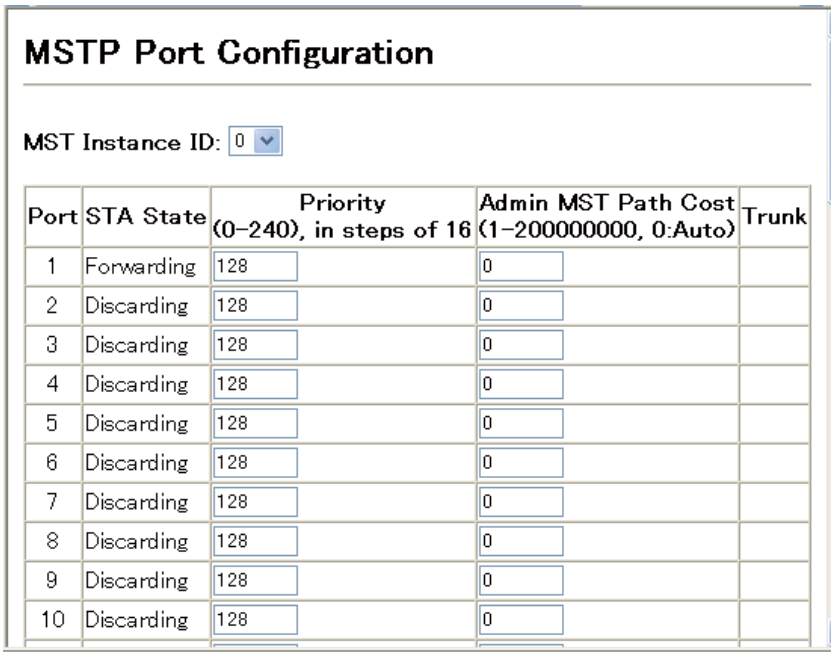
Fast Ethernet ― half duplex: 200,000、full duplex: 100,000、 trunk: 50,000

Gigabit Ethernet ― full duplex: 10,000、trunk: 5,000

[注意]　パスコスト方式が short に設定された場合、最大パスコストは 65,535 となります。

設定方法

[Spanning Tree] → [MSTP] → [Port Configuration] **又は** [Trunk Configuration] **をクリックします。インタフェースのプライオリティ及びパスコストを設定し、**[Apply] **をクリックします。**



MSTP Port Configuration

MST Instance ID: 0

Port	STA State	Priority (0-240), in steps of 16	Admin MST Path Cost (1-200000000, 0:Auto)	Trunk
1	Forwarding	128	0	
2	Discarding	128	0	
3	Discarding	128	0	
4	Discarding	128	0	
5	Discarding	128	0	
6	Discarding	128	0	
7	Discarding	128	0	
8	Discarding	128	0	
9	Discarding	128	0	
10	Discarding	128	0	

3.10 VLAN

大規模なネットワークでは、ブロードキャストトラフィックを分散させるためにルータにより各サブネットを異なるドメインに分割します。本機では同様のサービスをレイヤ 2 の VLAN 機能によりブロードキャストドメインを分割させたネットワークのグループを作成させることができます。VLAN は各グループでブロードキャストトラフィックを制限し、大規模ネットワークにおけるブロードキャストストームを回避します。

また、VLAN により安全で快適なネットワーク環境の構築も行なうことができます。

IEEE 802.1Q VLAN は、ネットワーク上どこにでも配置することができ、物理的に離れていても同じ物理的なセグメントに属するように通信を行うことができます。

VLAN は物理的な接続を変更することなく新しい VLAN へデバイスを追加することよりネットワーク管理を簡単に行うことができます。VLAN はマーケティング、R&D 等の部門別のグループ、e-mail やマルチメディアアプリケーションなどの使用方法ごとにグループ分けを行うことができます。

VLAN はブロードキャスト通信を軽減することにより巨大なネットワーク能力効率を実現し、IP アドレス又は IP サブネットを変更することなくネットワーク構成の変更を可能にします。VLAN は本質的に異なる VLAN への通信に、設定されたレイヤ 3 による転送が必要となるため、高水準のネットワークセキュリティを提供します。

本機では以下の VLAN 機能をサポートしています。

- EEE802.1Q 準拠の最大 255VLAN グループ
- GVRP プロトコルを利用した、複数のスイッチ間での動的な VLAN ネットワーク構築
- 複数の VLAN に参加できるオーバラップポートの設定が可能なマルチプル VLAN
- エンドステーションは複数の VLAN へ所属可能
- VLAN 対応と VLAN 非対応デバイス間での通信が可能
- プライオリティタギング

[注意] 本機の、ユーザー設定可能 VLAN は 255 個です。その他１つの VLAN（VLAN ID4093）は、スイッチクラスタリングのために確保されています。

VLAN へポートの割り当て

VLAN を有効にする前に、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。初期設定では全てのポートが VLAN 1 にタグなしポートとして割り当てられています。1 つ又は複数の VLAN で通信を行う場合や、VLAN に対応したネットワーク機器、ホストと通信を行う場合には、タグ付ポートとして設定を行います。その後、手動又は GVRP による動的な設定により、同じ VLAN 上で通信が行われる他の VLAN 対応デバイス上でポートを割り当てます。

しかし、1 つ又は複数の VLAN にポートが参加する際に、対向のネットワーク機器、ホストが VLAN に対応してない場合には、このポートをタグなしポートとして設定を行う必要があります。

[注意]　タグ付 VLAN フレームは VLAN 対応及び VLAN 非対応のネットワーク機器を通ることができますが、VLAN タグに対応していない終端デバイスに到達する前にタグを外す必要があります。

VLAN の分類 ― フレームを受信した際、スイッチは 2 種類のうち 1 種類のフレームとして認識します。タグなしフレームの場合、受信したポートの PVID に基づいた VLAN にフレームを割り当てます。タグ付フレームの場合、VLAN ID タグを使用してフレームのポートブロードキャストドメインを割り当てます。

ポートのオーバラップ ― ポートのオーバラップは、ファイルサーバ又はプリンタのように異なった VLAN グループ間で共有されるネットワークリソースへのアクセスを許可するために使用します。

オーバラップを行わない VLAN を設定し、VLAN 間での通信を行う必要がある場合にはレイヤ 3 ルータ又はスイッチを使用することにより通信が行えます。

タグなし VLAN ― タグなし又は静的 VLAN はブロードキャストトラフィックの軽減及びセキュリティのため、使用されます。

VLAN に割り当てられたユーザグループが、他の VLAN と分けられたブロードキャストドメインとなります。パケットは同じ VLAN 内の指定されたポート間でのみ送信されます。タグなし VLAN は手動でのユーザグループ又はサブネットの分割が行えます。また、GVRP を使用した IEEE802.3 タグ VLAN により、完全に自動化した VLAN 登録を行うことも可能となります。

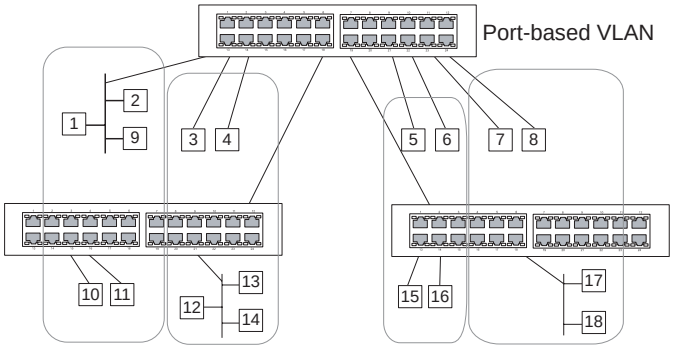
自動 VLAN 登録 ― GVRP (GARP VLAN Registration Protocol) は各終端装置が VLAN を割り当てられる必要がある場合に、VLAN を自動的に学習し設定を行います。終端装置（又はそのネットワークアダプタ）が IEEE802.1Q VLAN プロトコルに対応している場合、参加したい VLAN グループを提示するメッセージをネットワークに送信するための設定を行うことができます。本機がこれらのメッセージを受信した際、指定された VLAN の受信ポートへ自動的に追加し、メッセージを他の全てのポートへ転送します。

メッセージが他の GVRP 対応のスイッチに届いたときにも、同様に指定された VLAN の受信ポートへ追加され、他の全てのポートへメッセージが送られます。VLAN の要求はネットワークを通じて送られます。GVRP 対応デバイスは、終端装置の要求に基づき自動的に VLAN グループの構成を行うことが可能となります。

ネットワークで GVRP を使用するために、最初に要求された VLAN へ（OS 又はアプリケーションを使用して）ホストデバイスを追加します。その後、この VLAN 情報がネットワーク上へ伝達されます。ホストに直接接続されたエッジスイッチおよびネットワークのコアスイッチにおいて GVRP を有効にします。また、ネットワークのセキュリティ境界線を

決め、通知の伝送を防ぐためポートの GVRP を無効にするか、ポートの VLAN への参加を禁止する必要があります。

[注意] GVRP に対応していないホストデバイスでは、デバイスへ接続するポートで静的 VLAN を設定する必要があります。また、コアスイッチとエッジスイッチにおいて GVRP を有効にする必要があります。



タグ付・タグなしフレームの送信

1 台のスイッチでポートベースの VLAN を構成する場合、同じタグなし VLAN にポートを割り当てることで構成できます。しかし、複数のスイッチ間での VLAN グループに参加するためには、全てのポートをタグ付ポートとする VLAN を作成する必要があります。

各ポートは複数のタグ付又はタグなし VLAN に割り当てることができます。また、各ポートはタグ付及びタグなしフレームを通過させることができます。

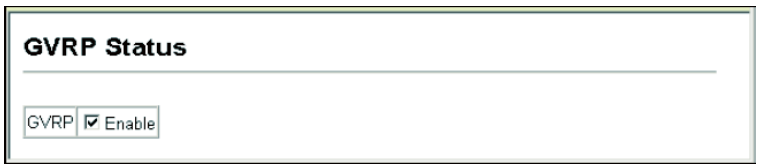
VLAN 対応機器に送られるフレームは、VLAN タグを付けて送信されます。VLAN 未対応機器（目的ホストを含む）に送られるフレームは、送信前にタグを取り除かなければなりません。タグ付フレームを受信した場合は、このフレームをフレームタグにより指示された VLAN へ送ります。VLAN 非対応機器からタグなしフレームを受信した場合は、フレームの転送先を決め、進入ポートのデフォルト VID を表示する VLAN タグを挿入します。

3.10.1 GVRP の有効・無効（Global Setting）

GARP VLAN Registration Protocol (GVRP) は、VLAN 情報の交換を行いネットワーク上の VLAN メンバーポートの登録を行なう方法を定義します。VLAN はネットワーク上のホストデバイスにより発行された join メッセージにより、自動的に設定されます。自動的な VLAN の登録を許可するためには、GVRP を有効にする必要があります（初期設定：Disabled）

設定方法

[VLAN] → [802.1Q VLAN] → [GVRP Status] をクリックします。GVRP を有効 (Enable) 又は無効 (Disable) に設定し、[Apply] をクリックします。



3.10.2 VLAN 基本情報の表示

VLAN 基本情報ページでは本機でサポートしている VLAN の種類などの基本的な情報を表示します。

設定・表示項目

VLAN Version Number

本機で使用している IEEE 802.1Q 標準の VLAN のバージョン

Maximum VLAN ID

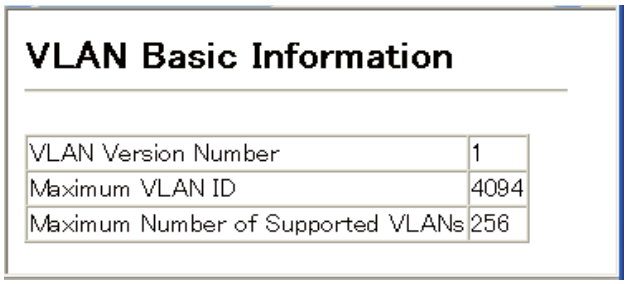
本機で認識可能な VLAN ID の最大値

Maximum Number of Supported VLANs

本機で設定することのできる最大 VLAN 数

設定方法

[VLAN] → [802.1Q VLAN] → [Basic Information] をクリックします。



3.10.3 現在の VLAN 表示

VLAN Current Table は、現在の各 VLAN のポートメンバー及びポートが VLAN タギングに対応しているかを表示します。複数のスイッチ間の大きな VLAN グループに参加するポートは VLAN タギングを使う必要があります。しかし、1 台又は 2 台程度のスイッチによる VLAN を作成する場合には、VLAN タギングを無効にすることができます。

設定・表示項目

VLAN ID

設定されている VLAN の ID (1-4094)

Up Time at Creation

VLAN が作成されてからの経過時間

Status

VLAN の設定方法 :

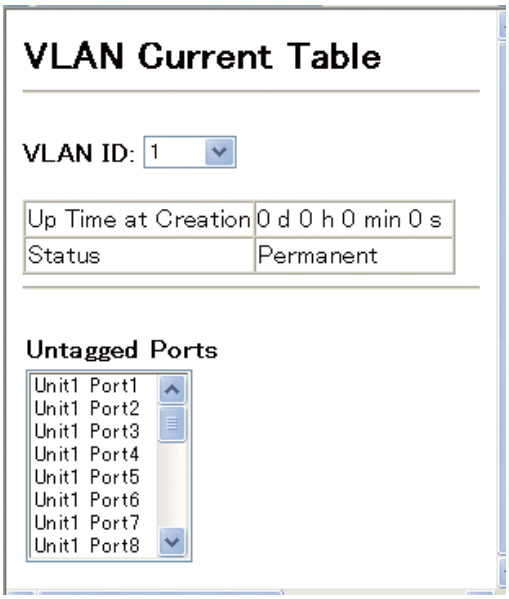
- Dynamic GVRP ― GVRP を使用しての自動学習
- Permanent ― 静的な手動設定

Untagged Ports

タグなし VLAN ポートメンバー

設定方法

[VLAN] → [802.1Q VLAN] → [Current Table] をクリックします。スクロールダウンリストから VLAN ID を選択します。



3.10.4 VLAN の作成

VLAN Static List を使用し、VLAN グループの作成及び削除が行えます。外部のネットワーク機器へ本機で使用されている VLAN グループに関する情報を伝えるため、これらの VLAN グループそれぞれに VLAN ID を設定する必要があります。

設定・表示項目

Current

このシステムを作成する全ての現在の VLAN グループを表示します。最大 256 個の VLAN グループを設定することができます。VLAN 1 はデフォルトタグなし VLAN です。

New

新しい VLAN グループの名前及び ID を設定します。（VLAN 名は本機で管理用に利用され、VLAN タグには記載されません）

VLAN ID

設定した VLAN の ID（1 から 4094）

VLAN Name

VLAN 名 (1 から 32 文字)

Status (Web)

この VLAN を有効にします。

- **Enable**: VLAN は使用することができます。
- **Disable**: VLAN は停止されます。

Status (CLI)

この VLAN を有効にします。

- **Active**: VLAN は使用することができます。
- **Suspend**: VLAN は停止されます。

Add

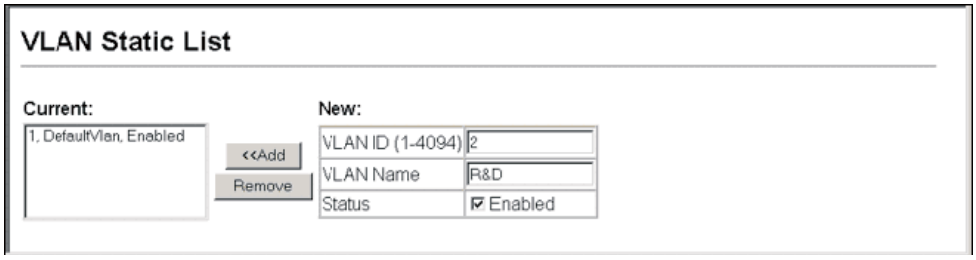
リストに新しい VLAN グループを追加します。

Remove

リストから VLAN グループを削除します。ポートがタグなしポートとしてこのグループに割り当てられている場合、タグなしポートとして VLAN 1 に割り当てられます。

設定方法

[VLAN] → [802.1Q VLAN] → [Static List] をクリックします。VLAN ID と VLAN Name を入力し VLAN をアクティブにするために Enable チェックボックスをチェックし、[Add] をクリックします。



3.10.5 VLAN への静的メンバーの追加（VLAN Index）

ポートメニューをを使用し、選択した VLAN のポートメンバーの設定を行ないます。

IEEE802.1Q VLAN 準拠の機器と接続する場合にはポートはタグ付として設定し、VLAN 非対応機器と接続する場合にはタグなしとして設定します。また、GVRP による自動 VLAN 登録から回避するためポートの設定を行ないます。

[注意] P146 「VLAN への静的メンバーの追加（Port Index）」でも、ポートインデックスを元に VLAN グループの設定を行なうことができますが、タグ付としてしかポートの追加はできません。

[注意] VLAN 1 は本機のすべてのポートが参加するデフォルトタグなし VLAN です。P147 「インタフェースの VLAN 動作の設定」にあるデフォルトポート VLAN ID を変更することができます。

設定・表示項目

VLAN

設定された VLAN ID（1 から 4094）

Name

VLAN 名（1 から 32 文字）

Status

この VLAN が有効か無効かを表示します。

- **Enable**: VLAN は使用することができます。
- **Disable**: VLAN は停止されます。

Port

ポート番号

Membership Type

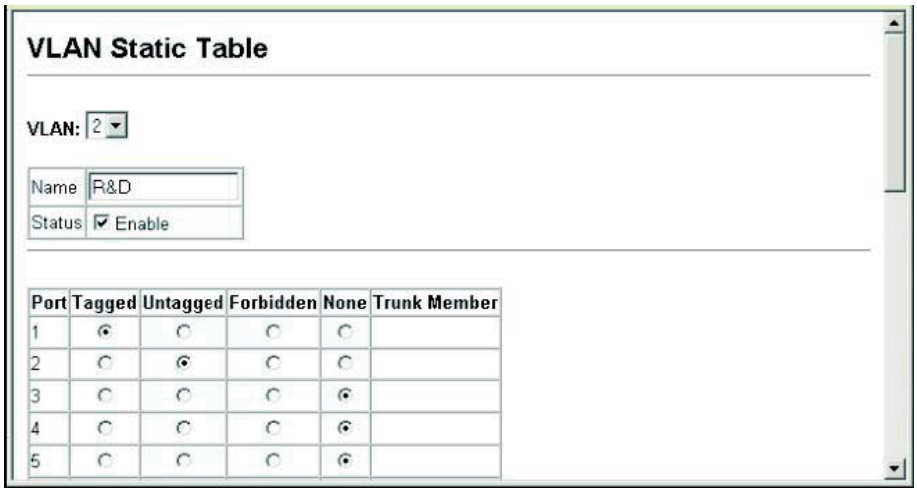
ラジオボタンをマークすることにより、各インタフェースへの VLAN メンバーシップを選択します。

- **Tagged** ―インタフェースは VLAN のメンバーとなります。ポートから送信される全てのパケットにタグがつけられます。タグにより VLAN 及び CoS 情報が運ばれます。
- **Untagged** ―インタフェースは VLAN のメンバーとなります。ポートから転送された全てのパケットからタグがはずされます。タグによる VLAN 及び CoS 情報は運ばれません。各インタフェースはタグなしポートとして最低 1 つのグループに割り当てなければいけません。
- **Forbidden** ―GVRP を使用した VLAN への自動的な参加を禁止します。詳細は P2-97 「GVRP」を参照して下さい。
- **None** ―インタフェースは VLAN のメンバーではありません。この VLAN に関連したパケットは、インタフェースから送信されません。
- **Trunk Member**

ポートがトランクメンバーの場合に表示されます。VLAN でのトランクを追加するためには、ページ下部のテーブルを使用します。

設定方法

[VLAN] → [802.1QVLAN] → [Static Table] をクリックします。スクロールダウンリストから VLAN ID を選択します。VLAN の Name と Status を必要に応じて変更します。各ポート又はトランクの適切なラジオボタンをマークしメンバーシップの種類を選択して、[Apply] をクリックします。



3.10.6 VLAN への静的メンバーの追加（Port Index）

静的 VLAN メンバーシップを使用し、VLAN グループを選択したインタフェースにタグ付メンバーとして追加します。

設定・表示項目

Interface

ポート又はトランク番号

Member

選択されたインタフェースがタグ付メンバーとして登録されている VLAN

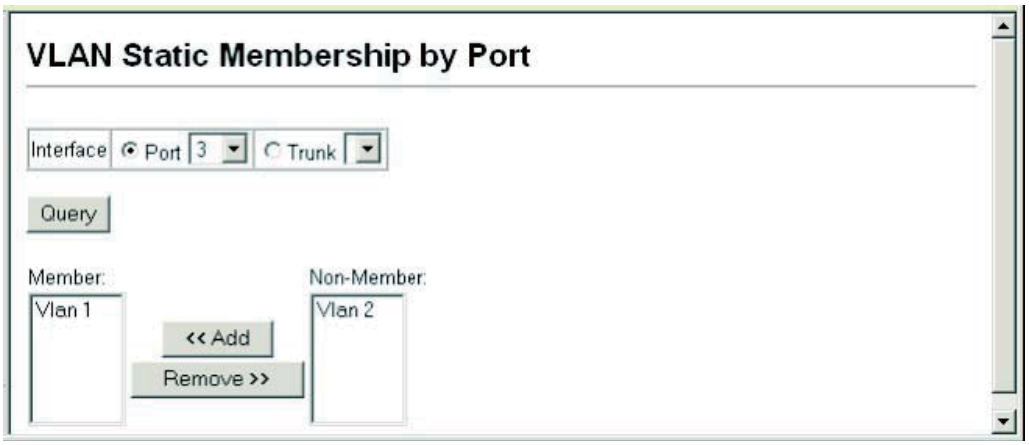
Non-Member

選択されたインタフェースがタグ付メンバーとして登録されていない VLAN

設定方法

[VLAN] → [802.1Q VLAN] → [Static Membership] をクリックします。スクロールダウンリストからインタフェースを選択します。[Query] をクリックし、インタフェースのメンバーシップインフォメーションを表示します。VLAN ID を選択し、インタフェースをタグ付メンバーとして追加するために [Add] をクリックします。インタフェース削除する場合には [Remove] をクリックします。

各インタフェースの VLAN メンバーシップの設定後、[Apply] をクリックします。



3.10.7 インタフェースの VLAN 動作の設定

デフォルト VLAN ID、利用可能なフレームの種類、イングレスフィルタリング、GVRP ステータス及び GARP タイマーを含む各インタフェースの VLAN に関する動作の設定を行うことができます。

機能解説

- GVRP ― GARP VLAN 登録プロトコルはネットワークを通るインタフェースの VLAN メンバーを自動的に登録するために VLAN 情報を交換するためのスイッチへの方法を決定します。
- GARP ― グループアドレス登録プロトコルはブリッジ LAN 内のクライアントサービスのためにクライアント属性を登録または登録の取り消しのための GVRP により使用されます。GARP タイマーの初期値はメディアアクセス方法又はデータ転送速度の独立したものです。これらの値は GVRP 登録又は登録の取り消しの問題に直面しない限り変更されません。

設定・表示項目

PVID

タグなしフレームを受信した際に付ける VLAN ID（初期設定 : 1）

－インタフェースが VLAN 1 のメンバーでない場合に、この VLAN へ PVID ”1” を割り当てた場合、インタフェースは自動的にタグなしメンバーとして VLAN 1 に参加します。その他の VLAN に関しては、まず「Static table」（144 ページの「VLAN への静的メンバーの追加（VLAN Index）」を参照）にて、各 VLAN に所属しているポートごとに Tag 付き、Tag なしの設定を行う必要があります。

例 ）Port1 の PVID を "30" に設定する場合

- Static Table にて、Port1 を VLAN30 の Tag なしメンバーの設定する。
- Port Configuration にて、Port1 の PVID を "30" に設定する。

* あらかじめ、Static List にて VLAN30 を作成しておいてください。

Acceptable Frame Type(受け入れ可能なフレームの種類)

全てのフレーム又はタグ付フレームのみのどちらか受け入れ可能なフレームの種類を設定します。全てのフレームを選択した場合には、受信したタグなしフレームはデフォルト VLAN に割り当てられます。(選択肢 : 全て又はタグ付き、初期設定 : 全て (all))

Ingress Filtering

入力ポートがメンバーでない VLAN のタグ付フレームを受信した場合の処理を設定します（初期設定：有効 (Enabled)）

－イングレスフィルタリングはタグ付フレームでのみ機能します。

－イングレスフィルタリングが有効で、ポートがメンバーでない VLAN のタグ付フレームを受信した場合、受信フレームを破棄します。

－イングレスフィルタリングはGVRP又はSTP等のVLANと関連しないBPDUフレームに機能しません。しかし、GMRP のような VLAN に関連する BPDU フレームには機能します。

Mode

ポートの VLAN メンバーシップモードを表示します：(初期設定 :Hybrid)

－ 1Q Trunk ― VLAN トランクの終端となっているポートを指定します。トランクは 2 台のスイッチの直接接続となり、ポートは発信元 VLAN のタグ付フレームを送信します。しかし、ポートのデフォルト VLAN に属したフレームはタグなしフレームが送信されます。

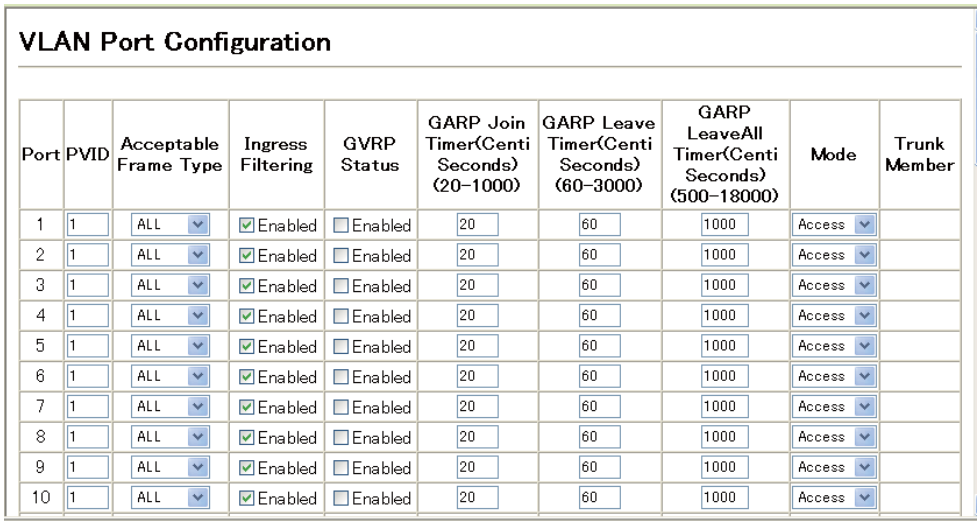
－ Hybrid ― ハイブリッド VLAN インタフェースを指定します。ポートはタグ付又はタグなしフレームを送受信します。

Trunk Member

ポートがトランクメンバーの場合に表示されます。VLAN **でのトランクを追加するためには、ページ下部のテーブルを使用します。**

設定方法

[VLAN] → [802.1Q VLAN] → [Port Configuration] **又は** [VLAN Trunk Configuration] **をクリックします。各インタフェースで必要な項目を設定し** [Apply] **をクリックします。**



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	Access	
2	1	ALL	Enabled	Enabled	20	60	1000	Access	
3	1	ALL	Enabled	Enabled	20	60	1000	Access	
4	1	ALL	Enabled	Enabled	20	60	1000	Access	
5	1	ALL	Enabled	Enabled	20	60	1000	Access	
6	1	ALL	Enabled	Enabled	20	60	1000	Access	
7	1	ALL	Enabled	Enabled	20	60	1000	Access	
8	1	ALL	Enabled	Enabled	20	60	1000	Access	
9	1	ALL	Enabled	Enabled	20	60	1000	Access	
10	1	ALL	Enabled	Enabled	20	60	1000	Access	

3.10.8 802.1Q トンネリングの設定

本機は通常 VLAN モードまたは、サービスプロバイダのメトロポリタンネットワークを通過するレイヤ 2 トラフィックに使用される、IEEE 802.1Q(QinQ) トンネリングモードでに設定することができます。

QinQ トンネルの設定を行うため、前セクションのガイドラインに補足を行います。
VLAN ポート設定または VLAN トランク設定画面にて、エッジスイッチのアクセスポートを 802.1Q トンネルモードに設定します。

機能解説

- トンネルポートの設定を行う前に 802.1Q Tunnel Status 画面でスイッチを QinQ モードに設定します。（P149 を参照）
- TPID field を選択されたインタフェースで、カスタム 802.1Q ethertype の値を設定するために使います。この機能は、サードパーティ製の s、tandard 0x8100 ethertype を 802.1Q-tagged frames の識別に使用しないスイッチとの相互運用を可能にします。例えば、トランクポートのカスタム 802.1Q ethertype として 0x1234 がセットされ、標準 802.1Q trunk になるように、ethertype を持つ入力フレームは、ethertype フィールドの後のタグに含まれて、VLAN に割り当てられます。
- 他の ethertype を含んでポートに到達したフレームはタグ無しフレームと見なされ。ポートのネイティブ VLAN に割り当てられます。

QinQ トンネリングの有効

スイッチは通常の VLAN か、サービスプロバイダのメトロポリタンエリアネットワーク上のレイヤ 2 トラフィックを通過させるために IEEE802.1Q（QinQ）トンネリングで動作するよう構成することができます。

設定・表示項目

802.1Q Tunnel

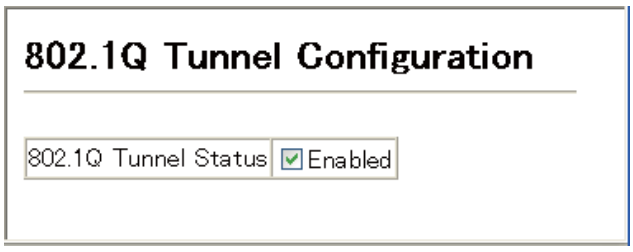
スイッチを QinQ モードに設定し、802.1Q の TPID を適用し、ポートを QinQ のトンネルポートとして構成できるよう許可します。デフォルトではスイッチはノーマルモードとして機能します。

802.1Q Ethernet Type

タグプロトコル識別子（TPID）（範囲；16 進 0800-FFFF　初期設定：8100）

設定方法

[VLAN] → [802.1Q VLAN] → [802.1Q Tunnel Configuration] をクリックします。



インタフェースを QinQ トンネリングへ追加

前のセクションに従い、QinQ トンネルの準備を行ってください。
VLAN ポートコンフィグレーションまたは VLAN トランクコンフィグレーション画面で、
エッジポート上のアクセスポートを 802.1Q トンネルモードへ設定してください。

Mode

ポートの VLAN モードを設定します（初期設定 : 無効）

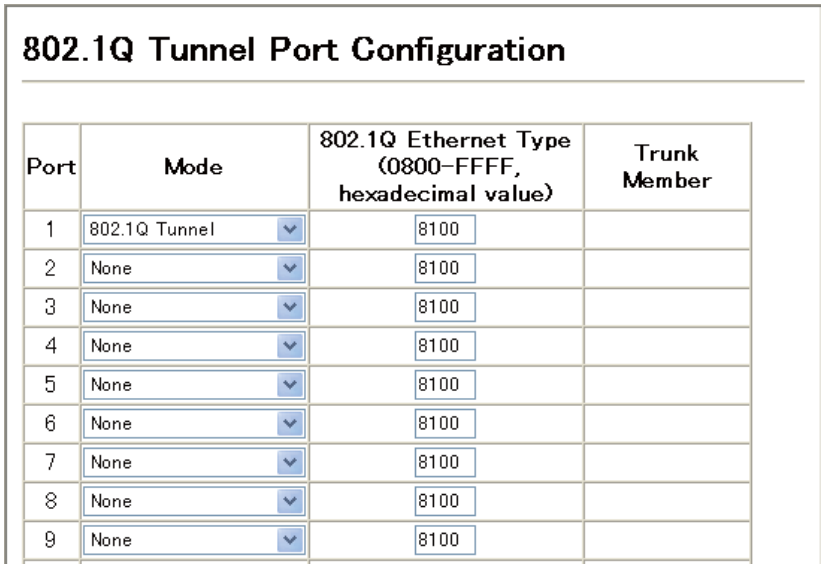
- None －通常 VLAN モードで動作
- 802.1Q Tunnel －サービスプロバイダのネットワークを横断するカスタマーの VLAN ID を分離し、保つためにクライアントのアクセスポートに IEEE802.1Q トンネリング（QinQ）を設定します。
- 802.1Q Tunnel Uplink －サービスプロバイダのネットワーク内のもう 1 つのデバイスに向けたアップリンクポートとして IEEE802.1Q トンネリング（QinQ）を設定します。

l802.1Q Ethernet Type

トンネルポートに入ってきたパケットのタグプロトコル識別子（TPID）
（範囲；16 進 0800-FFFF　初期設定：8100）

設定方法

[VLAN] → [802.1Q VLAN] → [802.1Q Tunnel Configuration] または [Tunnel Trunk Configuration] をクリックします。



3.10.9 プライベート VLAN の設定

プライベート VLAN は、ポートベースでのセキュリティの確保と VLAN 内のポート間の分離を行うことができます。本機はプライマリ VLAN と、セカンダリ VLAN の 2 種類をサポートしています。プライマリ VLAN には無差別ポートがあり、このポートは同じプライベート VLAN に所属する他のポートと通信が可能です。セカンダリ (コミュニティ) VLAN にはコミュニティポートがあり、このポートは同じセカンダリ VLAN 内の他のホスト、又は関連付けを行ったプライマリ VLAN の任意の無差別ポートとのみ通信が可能です。独立 VLAN は、1 つの無差別ポートと 1 つ以上の独立 (又はホスト) ポートから構成される、単一のスタンドアロンの VLAN です。いずれの VLAN も無差別ポートはインターネットなど外部ネットワークからのアクセスが可能ですが、コミュニティ / 独立ポートはローカルユーザからのアクセスのみに制限されます。

本機には複数のプライマリ VLAN を設定でき、又複数のコミュニティ VLAN を各プライマリ VLAN と関連付けできます。独立 VLAN も 1 つ以上設定できます (プライベート VLAN と通常の VLAN は同一スイッチ内に同時に構成することができることに注意して下さい)

プライマリグループ、セカンダリグループに設定するには、次の方法で行います。

（1）Private VLAN Configuration 画面 (P151) で 1 つ以上のコミュニティ VLAN と、VLAN グループ以外のトラフィックのやり取りをするプライマリ VLAN を 1 つ指定します。

（2）Private VLAN Association 画面 (P154) で、セカンダリ (コミュニティ) VLAN とプライマリ VLAN とのマッピングを行ないます。

（3）Private VLAN Port Configuration 画面 (P153) でポートの種類を Promiscuous (プライマリ VLAN のすべてのポートへアクセス可能な無差別ポート) 又は Host (コミュニティ VLAN から、又コミュニティ VLAN 以外の場合は無差別ポートへのアクセスのみ可能) から指定します。その後、任意の無差別ポートをプライマリ VLAN とコミュニティ VLAN のホストポートに指定します。

独立 VLAN に設定するには、次の方法で行います。

（1）Private VLAN Configuration 画面 (P153) ですべてのトラフィックが経由する無差別ポートを 1 つ設定します。

（2）Private VLAN Port Configuration 画面 (P156) でポートの種類を Promiscuous (外部ネットワークとの単一の経路となる) 又は Isolated (同一 VLAN の無差別ポートへのアクセスのみ可能) から指定します。その後、設定した無差別ポートと独立 (ホスト) ポートを独立 VLAN に指定します。

現在のプライベート VLAN の表示

Private VLAN Information 画面に、プライマリ VLAN、コミュニティ VLAN、独立 VLAN、各 VLAN に関連付けられたインタフェースなど、本機に設定したプライベート VLAN 情報を表示します。

設定・表示項目

VLAN ID

表示する VLAN ID（1-4094）と VLAN の種類

Primary VLAN

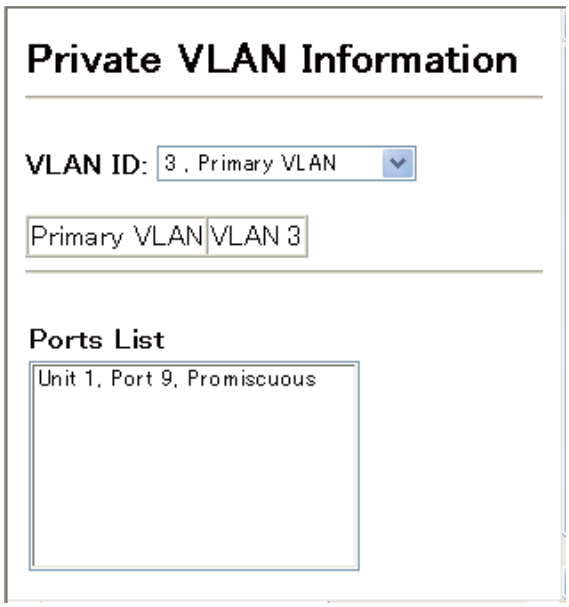
表示している VLAN ID に関連付けされている VLAN。プライマリ VLAN の場合は自身の VLAN ID を、コミュニティ VLAN の場合は関連付けされているプライマリ VLAN ID を、又独立 VLAN はスタンドアロンの VLAN を表示します。

Ports List

表示しているプライベート VLAN に所属するポート (ポートの種類)

設定方法

[VLAN] → [Private VLAN] → [Information] をクリックします。ドロップダウンリストから表示させたいポートを選択します。



プライベート VLAN の設定

Private VLAN Configuration 画面で、プライマリ VLAN、コミュニティ VLAN、独立 VLAN の作成、削除を行います。

設定・表示項目

VLAN ID

設定する VLAN ID（1-4094）

Type

プライベート VLAN には次の 3 つの種類があります。

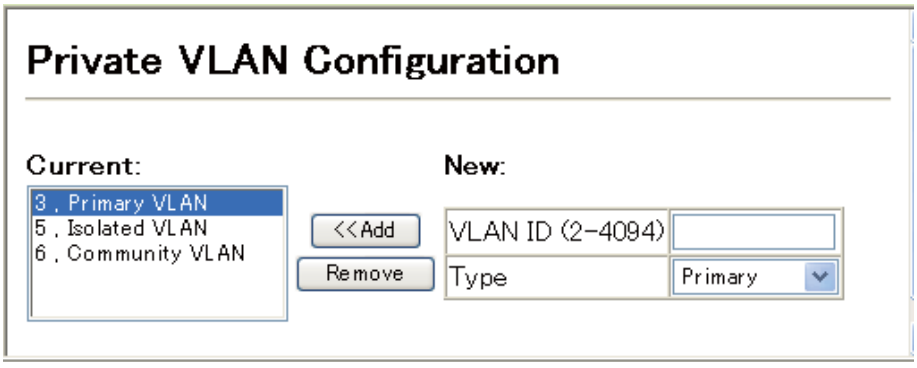
- Primary ― セカンダリ (コミュニティ) VLAN 内で、無差別ポートとコミュニティポート間でデータをやり取りします。
- Community ― 関連付けたプライマリ VLAN 内で、無差別ポートとコミュニティポート間でデータをやり取りします。

Current

設定済みの VLAN のリスト

設定方法

[VLAN] → [Private VLAN] → [Configuration] をクリックします。VLAN ID に VLAN ID 番号を入力し、Type から Primary、Isolated、Community を選択し、その後 [Add] をクリックします。本機に設定したプライベート VLAN を削除するには、削除する項目を Current リストから選択して反転表示させ、[Remove] をクリックします。VLAN を削除する前にその VLAN に所属するポートをすべて削除しておかなくてはなりません。



VLAN の関連付け

コミュニティ VLAN とプライマリ VLAN は関連付けを行う必要があります。

設定・表示項目

Primary VLAN ID

プライマリ VLAN ID（1-4094）

Association

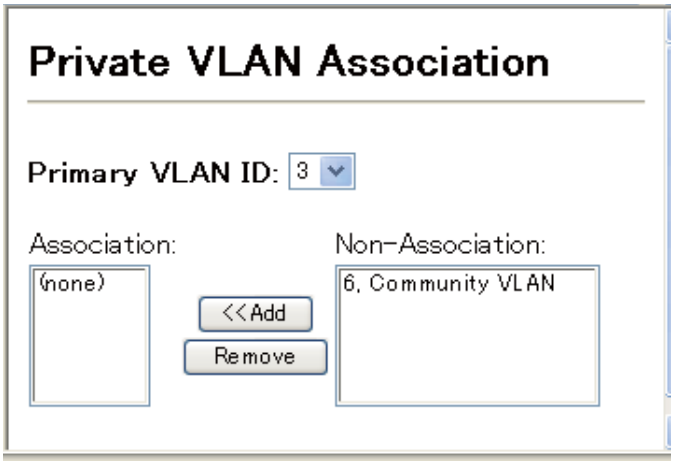
選択したプライマリ VLAN と既に関連付けられているコミュニティ VLAN

Non-Association

選択したプライマリ VLAN と関連付けられていないコミュニティ VLAN

設定方法

[VLAN] → [Private VLAN] → [Association] をクリックします。Primary VLAN ID ドロップダウンボックスから設定するプライマリ VLAN を選択します。Non-Association リストボックスの 1 つまたは複数のコミュニティ VLAN を選択して反転表示させ、[Add] をクリックします。コミュニティ VLAN が選択したプライマリ VLAN に関連付けられます（コミュニティ VLAN は 1 つのプライマリ VLAN にしか所属できません）。



プライベート VLAN インタフェース情報の表示

Private VLAN Port Information 及び Private VLAN Trunk Information 画面で、プライベート VLAN に関連付けられているインタフェース情報を表示します。

設定・表示項目

Port 又は Trunk

本機のインタフェース

PVLAN Port Type

プライベート VLAN のポートの種類を表示します。

- Normal ― このポートはプライベート VLAN での設定はありません。
- Host ― コミュニティポートに設定されており、同一コミュニティ VLAN に所属するポートと、又は指定された無差別ポートとのみ通信が可能です。あるいは、独立ポートに設定されており、同一の独立 VLAN に所属する無差別ポートとのみ通信が可能です。
- Promiscuous ― 無差別ポートに設定されており、プライベート VLAN 内のすべてのポートと通信が可能です。

Primary VLAN

セカンダリ (コミュニティ) VLAN 内で、無差別ポート同士、又は無差別ポートとコミュニティポート間でデータをやり取りします。

Community VLAN

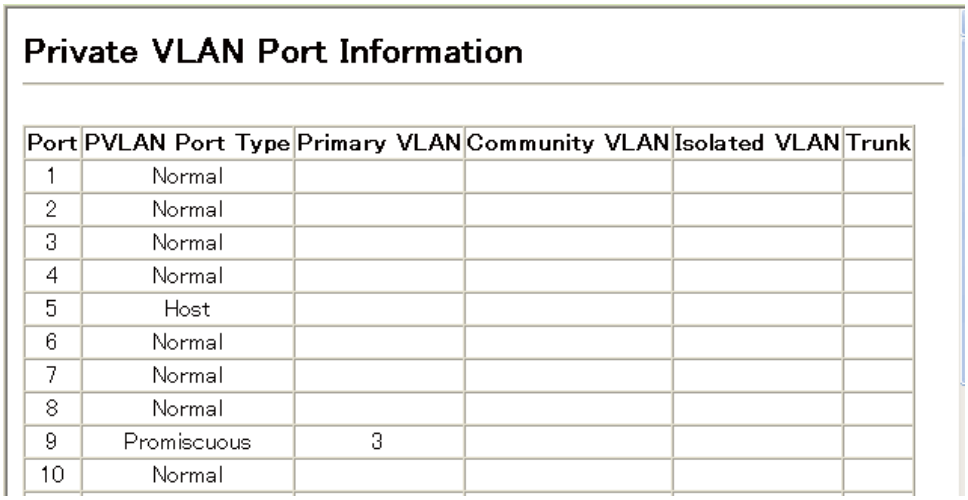
コミュニティ VLAN。コミュニティポート間、又はコミュニティポートと指定した無差別ポート間でデータをやり取りします。

Trunk

トランク識別子（Port Information 画面のみ）

設定方法

[VLAN] → [Private VLAN] → [Port Information] 又は [Trunk Information] をクリックします。



Private VLAN Port Information

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

プライベート VLAN インタフェースの設定

Private VLAN Port Configuration 及び Private VLAN Trunk Configuration 画面で、プライベート VLAN のインタフェース種類の設定と、インタフェースのプライベート VLAN への割り当てを行います。

設定・表示項目

Port

本機のインタフェース

PVLAN Port Type

プライベート VLAN のポートの種類を設定します。

- **Normal** ― このポートはプライベート VLAN に割り当てません。
- **Host** ― コミュニティポート又は独立ポートに設定します。コミュニティポートは、同一コミュニティ VLAN に所属するポートと、又は指定された無差別ポートとのみ通信が可能です。独立ポートは、同一の独立 VLAN に所属する無差別ポートとのみ通信が可能で、他の Host ポートとは通信できません。
- **Promiscuous** ― 無差別ポートに設定します。プライベート VLAN 内のすべてのポートと通信が可能です。

Primary VLAN

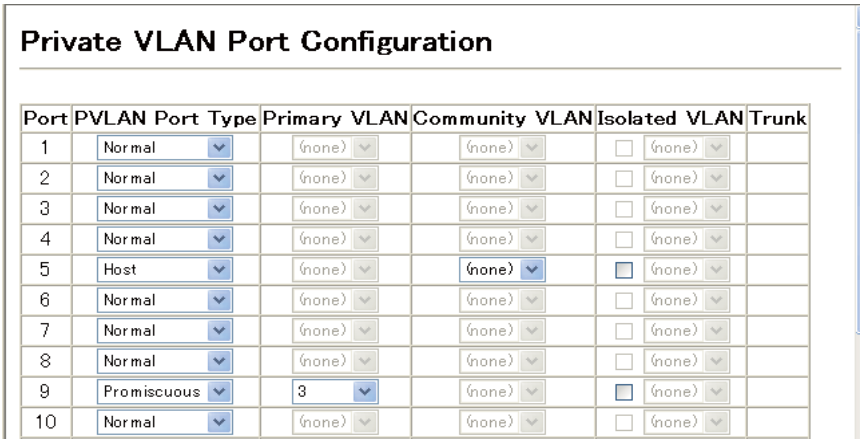
関連付けたセカンダリ (コミュニティ) VLAN 内で、無差別ポート同士、又は無差別ポートとコミュニティポート間でデータをやり取りします。

Community VLAN

コミュニティ VLAN。コミュニティポート間、又はコミュニティポートと指定した無差別ポート間でデータをやり取りします。PVLAN Port Type を "Host" に設定し、関連付けたコミュニティ VLAN を設定します。

設定方法

[VLAN] → [Private VLAN] → [Port Configuration] 又は [Trunk Configuration] をクリックします。プライベート VLAN に所属させるポートを PVLAN Port Type で設定します。無差別ポートをプライマリ VLAN または独立 VLAN に割り当てます。ホストポートをコミュニティ VLAN または独立 VLAN に割り当てます。すべてのポートを設定したら、[Apply] をクリックします。



3.10.10 プロトコル VLAN

複数のプロトコルのトラフィックが、異なった VLAN を通過することを可能にします。ポートでパケットが受け取られる際、そのパケットのプロトコルタイプにより VLAN メンバーシップを決定します。

プロトコル VLAN グループ設定

設定・表示項目

Protocol Group ID

プロトコル VLAN グループに割り当てられる、プロトコルグループ ID（範囲：1-2147483647）

Special protocol

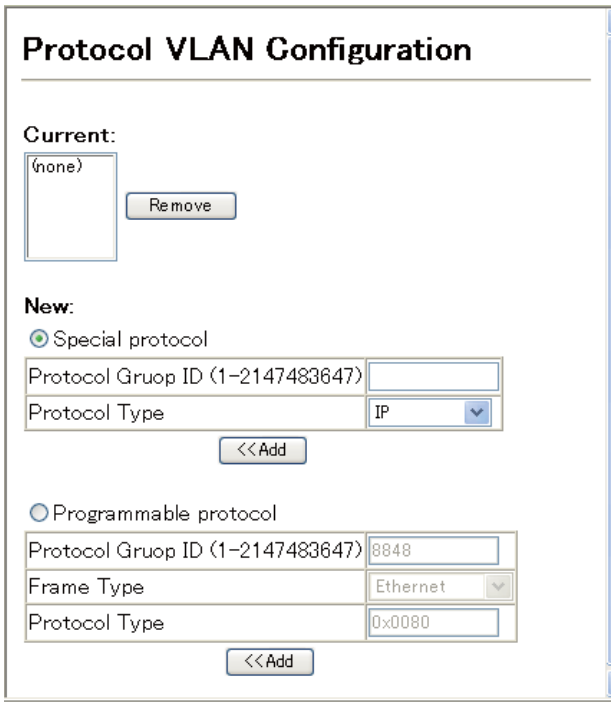
- **IP** (0x0800)
- **IPX** (0x8137)
- **Apple-talk** (0x809B)

Programmable protocol

- **Frame Type**
  - Ethernet
  - LLC_other
  - RFC_1042
  - SNAP_8021H
- **Protocol Type**

設定方法

[VLAN] → [Protocol VLAN] → [Configuration] **をクリックします。**



プロトコル VLAN インタフェース設定

ポートごとのプロトコル VLAN 設定を行います。

設定・表示項目

Interface

ポートまたはトランクを指定

Protocol Group ID

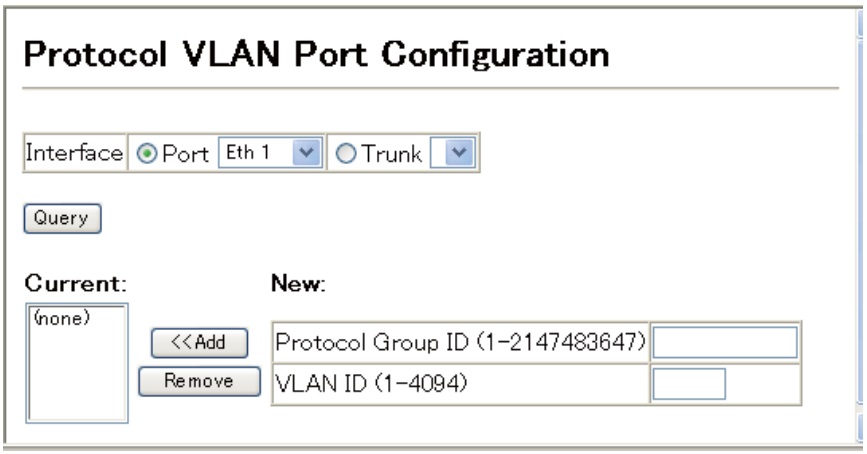
プロトコル VLAN グループに割り当てられたプロトコルグループ ID（範囲：1-2147483647）

VLAN ID

一致したプロトコルトラフィックがフォワードされる VLAN（範囲：1-4094）

設定方法

[VLAN] → [Protocol VLAN] → [Port Configuration] をクリックします。



3.11 LLDP

Link Layer Discovery Protocol（LLDP）はローカルブロードキャストドメインの中の接続デバイスについての基本的な情報を発見するために使用します。LLDP はレイヤ 2 のプロトコルであり、デバイスについての情報を周期的なブロードキャストで伝達します。伝達された情報は IEEE802.1ab に従って Type Length Value（TLV）で表され、そこにはデバイス自身の識別情報、能力、設定情報の詳細が含まれています。また LLDP は発見した近隣のネットワークノードについて集められた情報の保存方法と管理方法を定義します。

Link Layer Discovery Protocol - Media Endpoint Discovery（LLDP-MED）は VoIP やスイッチのようなエンドポイントのデバイスを管理するための拡張された LLDP です。LLDP-MED の TLV はネットワークポリシー、電力、インベントリ、デバイスのロケーションの詳細情報を伝達します。LLDP と LLDP-MED の情報は、トラブルシューティングの簡易化、ネットワーク管理の改善、間違いのないネットワークトポロジーを維持するため、SNMP アプリケーションによって使用することができます。

3.11.1 LLDP タイム属性の設定

LLDP の有効化、メッセージのエージアウトタイム、通常の情報伝達をブロードキャストする間隔、LLDP MIB の変更についての伝達といった、一般的な設定は LLDP 設定画面で行います。

設定・表示項目

LLDP

ポートまたはトラックを指定

Transmission Interval

LLDP の情報伝達のため周期的に送信する間隔を設定します

（範囲：5 － 32768 秒初期設定：30 秒）

この値は下の数式に従って設定しなくてはいけません。

Transmission Interval × Hold Time Multiplier ≦ 65536

Hold Time Multiplier

下の式で示されているように、LLDP のアドバタイズメントで送信された Time-To-Live（TTL）値を設定します（範囲：2 － 10　初期設定：4）

TTL は、タイムリーな方法でアップデートが送信されない場合、送信した LLDP エージェントに関係のあるすべての情報をどのくらいの期間維持するかを受信した LLDP エージェントに伝達します。TTL は秒で表され、下の数式で計算します。

Transmission Interval × Hold Time Multiplier ≦ 65536

つまり上の式からデフォルトの TTL は下のようになります。

30 × 4 ＝ 120

Delay Interval

ローカル LLDP MIB の変数に変化が起こった後に引き続き、アドバタイズメントを送信するまでの時間を設定します（範囲：1 ～ 8192 秒　初期設定：2 秒）

Reinitialization Delay

LLDP ポートが無効になるかリンクダウンした後、再初期化を試みるまでの時間を設定します（範囲：1 － 10 秒　初期設定：2 秒）

Notification Interval

LLDP MIB の変更を行い、SNMP 通知が送信されるまでの時間を設定します

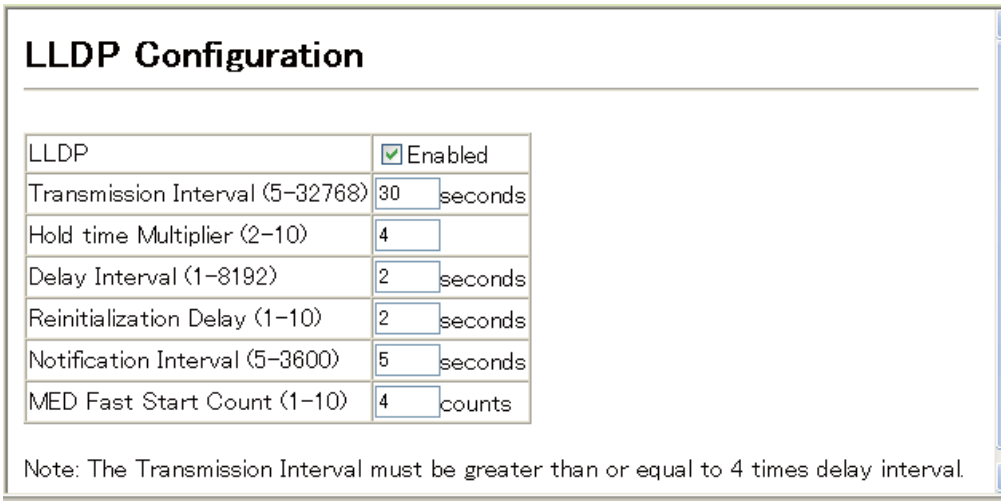
（範囲：5 ー 3600 秒　初期設定：5 秒）

MED Fast Start Count

LLDP-MED Fast Start メカニズムのアクティベーションプロセスの間に送信する LLDP MED Fast Start LLDPDU の数を設定します（範囲：1 ～ 10 パケット　初期設定：4 パケット）

設定方法

[LLDP] → [Configuration] →をクリックします。



3.11.2 LLDP インタフェースの設定

個別のインターフェースに対し、メッセージの内容を指定するために LLDP ポート・トランクの設定を行います。

設定・表示項目

Admin Status

LLDP メッセージの送信・受信のモードを有効にします

（設定項目：Tx only, Rx only, TxRx, Disabled　**初期設定：**TxRx**）**

SNMP Notification

LLDP と LLDP-MED **の変更について** SNMP **トラップ通知の送信を有効にします**

（初期設定：有効）

TLV Type

アドバタイズするメッセージの TLV **フィールドの情報について設定します。**

- **Port Description** ― RFC2863 **の** ifDescr **オブジェクトで規定されています。これには製造者、スイッチの製品名、インターフェースのハードウェアとソフトウェアのバージョンが含まれます。**
- **System Description** ― RFC3418 **の** sysDescr **オブジェクトで規定されています。システムのハードウェア、オペレーティングソフト、ネットワーキングソフトのフルネームとバージョンが含まれています。**
- **Management Address** ― **スイッチの** IPv4 **アドレスが含まれます。スイッチに管理用のアドレスがない場合、アドレスはスイッチの** CPU **の** MAC **アドレスが、このアドバタイズメントを送信するポートの** MAC **アドレスになります。**
- **System Name** ― RFC3418 **の** sysName **オブジェクトで規定されています。システムの管理用に割り当てられた名前が含まれます。**
- **System Capabilities** ―**システムの主な機能が含まれます。この情報には機能自体が有効かどうかは関係ありません。この** TLV **によってアドバタイズされる情報は** IEEE802.1AB **規格に記述されています。**

MED TLV Type

アドバタイズするメッセージの MED TLV **フィールドの情報について設定します。**

- **Port Capabilities** ― **このオプションは** LLDP-MED TLV **の能力をアドバタイズします。スイッチでサポートする** LLDP-MED TLV **に関係のある項目を効率的に発見するために、メディアのエンドポイントと接続されたデバイスをアドバタイズします。**
- **Network Policy** ―**このオプションはネットワークポリシー設定の情報をアドバタイズします。この情報はポートの** VLAN **設定ミスの発見や分析の役に立ちます。妥当でないネットワークポリシーは音声品質の低下やサービスの破綻に頻繁につながります。**
- **Location** ―**このオプションは設置場所の詳細をアドバタイズします。**
- **Extended Power** ―**このオプションは拡張された** PoE（Power over Ethernet）**についての詳細情報をアドバタイズします。この情報にはスイッチから利用できる電力供給源、スイッチの電力状態、スイッチが主電源もしくはバックアップ電源のどちらで動作しているかが含まれます。**
- **Inventory** ―**このオプションは製造者、モデル、ソフトウェアのバージョン、その他適切な情報などデバイスの詳細情報をアドバタイズします。**

MED Notification

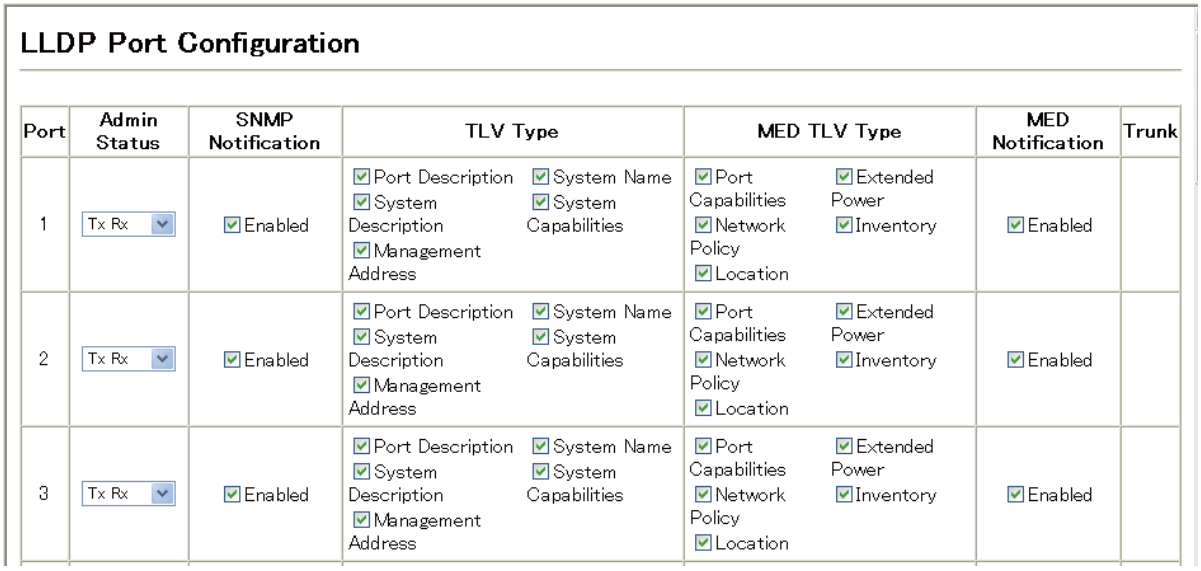
LLDP-MED の変更について SNMP トラップ通知の送信を有効にします（初期設定：有効）

Trunk

ポートがトランクポートであるかどうかを表示します（ポート設定画面のみ）

設定方法

[LLDP] → [Port/Trunk Configuration] →をクリックします。



LLDP Port Configuration

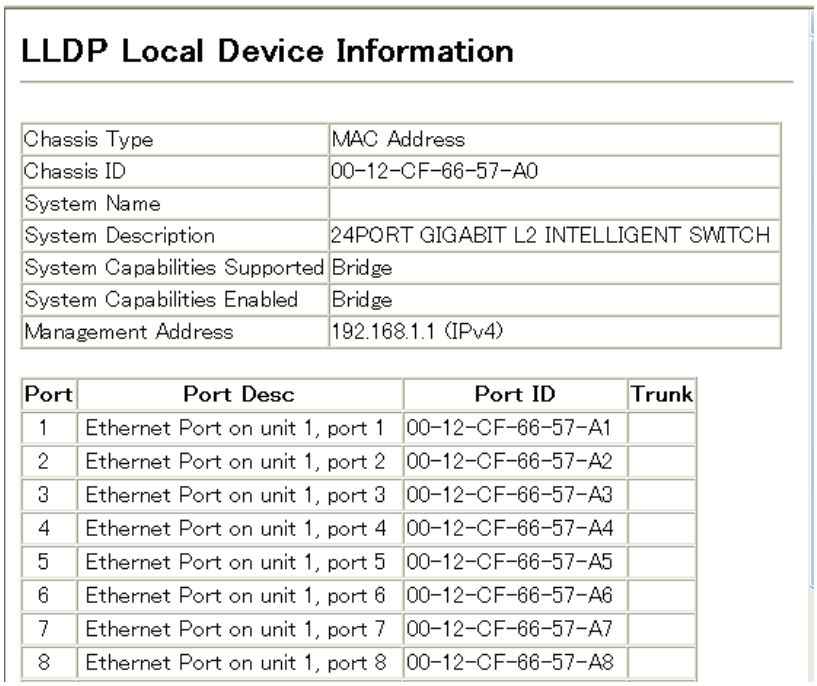
Port	Admin Status	SNMP Notification	TLV Type	MED TLV Type	MED Notification	Trunk
1	Tx Rx	Enabled	Port Description, System Name, System Description, System Capabilities, Management Address	Port Capabilities, Extended Power, Network Policy, Inventory, Location	Enabled	
2	Tx Rx	Enabled	Port Description, System Name, System Description, System Capabilities, Management Address	Port Capabilities, Extended Power, Network Policy, Inventory, Location	Enabled	
3	Tx Rx	Enabled	Port Description, System Name, System Description, System Capabilities, Management Address	Port Capabilities, Extended Power, Network Policy, Inventory, Location	Enabled	

3.11.3 LLDP ローカルデバイス情報の表示

LLDP Local Device Information 画面は、スイッチについての情報を表示します。表示される情報は MAC アドレス、シャーシ ID、管理用 IP アドレス、ポート情報等です。

設定方法

[LLDP] → [Local Information] →をクリックします。



LLDP Local Device Information

Chassis Type	MAC Address
Chassis ID	00-12-CF-66-57-A0
System Name	
System Description	24PORT GIGABIT L2 INTELLIGENT SWITCH
System Capabilities Supported	Bridge
System Capabilities Enabled	Bridge
Management Address	192.168.1.1 (IPv4)

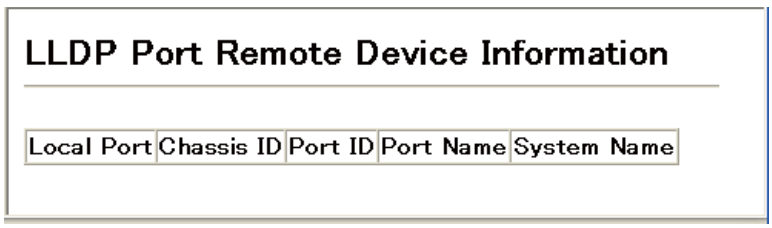
Port	Port Desc	Port ID	Trunk
1	Ethernet Port on unit 1, port 1	00-12-CF-66-57-A1	
2	Ethernet Port on unit 1, port 2	00-12-CF-66-57-A2	
3	Ethernet Port on unit 1, port 3	00-12-CF-66-57-A3	
4	Ethernet Port on unit 1, port 4	00-12-CF-66-57-A4	
5	Ethernet Port on unit 1, port 5	00-12-CF-66-57-A5	
6	Ethernet Port on unit 1, port 6	00-12-CF-66-57-A6	
7	Ethernet Port on unit 1, port 7	00-12-CF-66-57-A7	
8	Ethernet Port on unit 1, port 8	00-12-CF-66-57-A8	

3.11.4 LLDP リモートポート情報の表示

LLDP Remote Port/Trunk Information 画面は、スイッチのポートに直接接続されたデバイスについての情報を表示します。これらの情報は LLDP を通してアドバタイズされています。

設定方法

[LLDP] → [Remote Port/Trunk Information] →をクリックします。



LLDP Port Remote Device Information

Local Port	Chassis ID	Port ID	Port Name	System Name

3.11.5 LLDP リモート詳細情報の表示

LLDP Remote Information Details 画面は、ローカルスイッチの指定されたポートに接続された、LLDP が有効のデバイスについての詳細情報を表示します。

設定方法

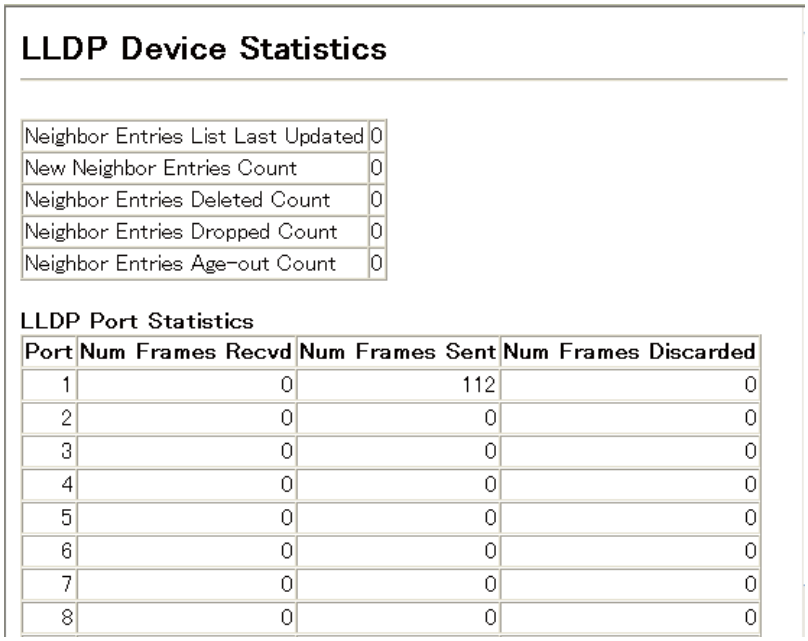
[LLDP] → [Remote Information Details] →をクリックします。

3.11.6 デバイス統計値の表示

LLDP Device Statistics 画面は、このスイッチに接続されている LLDP が有効なすべてのデバイスの統計を表示します。

設定方法

[LLDP] → [Device Statistics] →をクリックします。

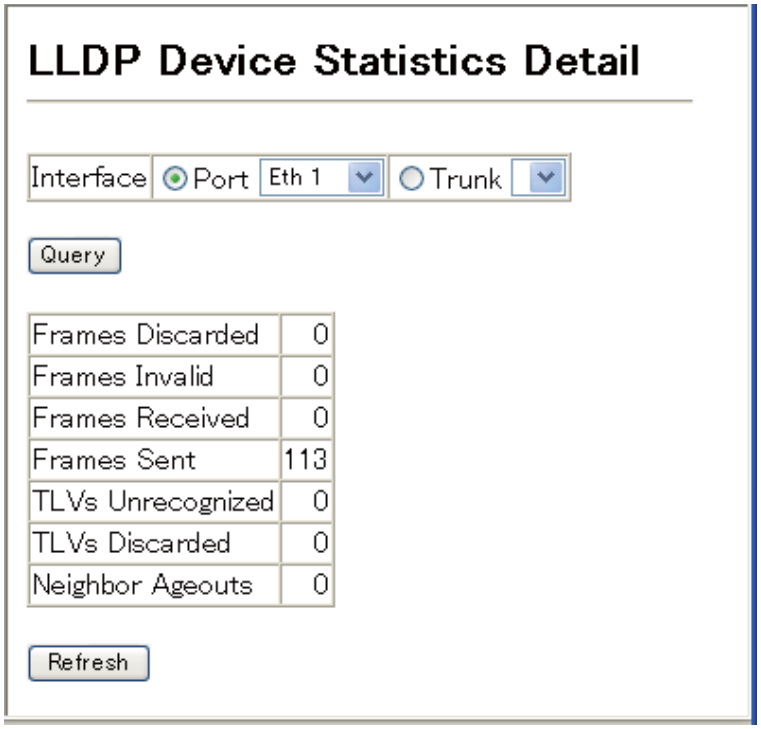


3.11.7 デバイス統計値詳細の表示

LLDP Device Statistics Details **画面は、**LLDP **が有効のインターフェースを通して受信したトラフィックをベースにした統計を表示します。**

設定方法

[LLDP] → [Device Statistics Details] **→をクリックします。**



3.12 Class of Service（CoS）

Class of Service(CoS) は、ネットワークの混雑状態のために通信がバッファされる場合に、優先するデータパケットを指定することができます。本機では各ポートで 4 段階のキューの CoS をサポートしています。高いプライオリティのキューを持ったデータパケットを、より低いプライオリティのキューを持ったデータパケットよりも先に転送します。各インタフェースにデフォルトプライオリティを設定することができ、又本機のプライオリティキューに対し、フレームプライオリティタグのマッピングを行うことができます。

3.12.1 レイヤ 2 キュー設定

インタフェースへのデフォルトプライオリティの設定

各インタフェースのデフォルトポートプライオリティを指定することが出来ます。スイッチへ入る全てのタグなしパケットは指定されたデフォルトポートプライオリティによりタグが付けられ、出力ポートでの適切なプライオリティキューが設定されます。

機能解説

- 本機は各ポートで 4 つのプライオリティキューを提供します。head-of-queue blockage を防止するために重み付けラウンドロビン (WRR) を使用します。
- デフォルトプライオリティは、"accept all frame type" に設定されたポートで受信したタグなしフレームの場合に適用されます。このプライオリティは IEEE 802.1Q VLAN タグ付フレームに対応していません。受信フレームが IEEE 802.1Q VLAN タグ付フレームの場合、IEEE 802.1Q VLAN User Priority ビットが使用されます。
- 出力ポートが関連 VLAN のタグなしメンバーの場合、これらのフレームは送信前に全ての VLAN タグを外します。

設定・表示項目

Default Priority

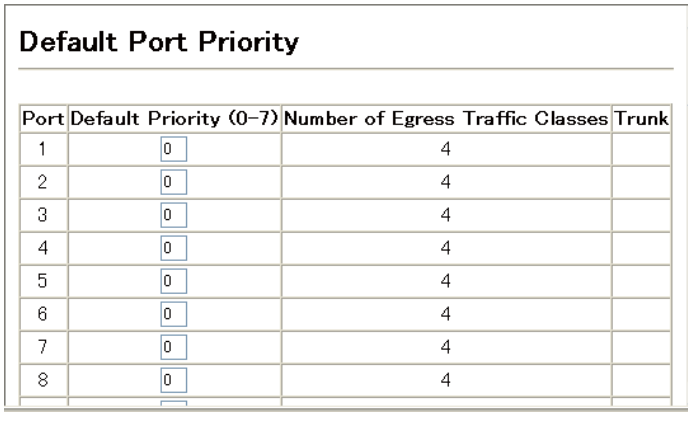
各インタフェースの受信されたタグなしフレームに割り当てられるプライオリティ
（範囲 :0 - 7、初期設定 :0）

Number of Egress Traffic Classes

各ポートに割り当てられたキューバッファの値

設定方法

[Priority] → [Default Port Priority] 又は [Default Trunk Priority] をクリックします。インタフェースのデフォルトプライオリティを変更し、[Apply] をクリックします。



Egress キューへの CoS 値のマッピング

本機は各ポートの 8 つのプライオリティキューを使用することによる CoS プライオリティタグ付通信の処理を、重み付けラウンドロビン (Weighted Round Robin/WRR) に基づいたサービススケジュールにより行います。
最大 8 つに分けられた通信プライオリティは IEEE802.1p で定められます。デフォルトプライオリティレベルは次の表に記載されている IEEE802.1p の勧告に基づいて割り当てられています。

キュー	0	1	2	3
プライオリティ	1、2	0、3	4、5	6、7

様々なネットワークアプリケーションの IEEE 802.1p 標準で推奨されたプライオリティレベルが以下の表に記載されています。しかし、アプリケーションの通信に対して、自由にアウトプットキューのプライオリティレベルを設定することが可能です。

プライオリティレベル	トラフィックタイプ
1	Background
2	(Spare)
0（初期設定）	Best Effort
3	Excellent Effort
4	Controlled Load
5	Video, less than 100 milliseconds latency and jitter
6	Voice, less than 10 milliseconds latency and jitter
7	Network Control

設定・表示項目

Interface

ポートまたはトランクを選択します。

Priority

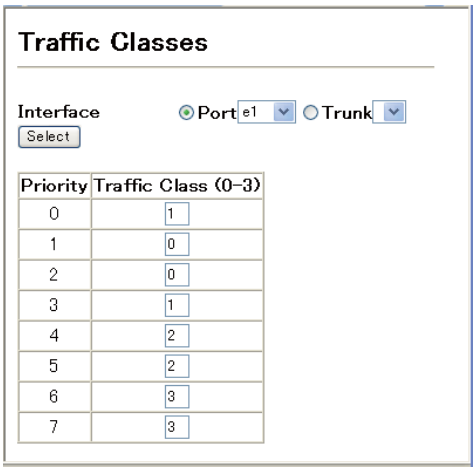
CoS 値（範囲 :0 から 7、7 が最高プライオリティ）

Traffic Class

アウトプットキューバッファ (範囲 :0 から 3、3 が最高 CoS プライオリティキュー)

設定方法

[Priority] → [Traffic Classes] をクリックします。各インタフェースのアウトプットキューへプライオリティ (Traffic Class) を割り当て、[Apply] をクリックします。



キューモードの選択

本機では、すべての高プライオリティキューが低プライオリティキューに優先される strict ルール、又は各キューの重み付けを行う Weighted Round-Robin (WRR) を用いてキューイングを行います。WRR では、あらかじめ設定した重みに応じて各キューの転送時間の割合を決定します。それにより、Strict ルールにより生じる HOL Blocking を防ぐことができます（初期設定では WRR に設定されています）

設定・表示項目

WRR

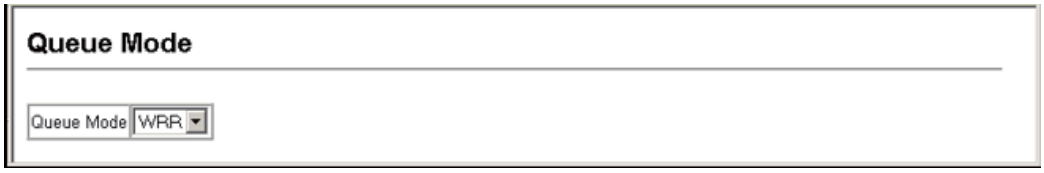
Weighted Round-Robin ではイングレスポートの帯域を それぞれの 0-3 のキューに対して 1, 2, 4, , 8 のスケジューリングウェイトを設定し共有します。

Strict

イングレスキューを順次処理します。すべての高プライオリティキューのトラフィックが低プライオリティキューのトラフィックより優先的に処理されます

設定方法

[Priority] → [Queue Mode] をクリックします。Strict 又は WRR を選択し、[Apply] をクリックします。



トラフッククラスのサービスウェイト設定

本機は各プライオリティキューの提供をする時に重み付けラウンドロビン (WRR) アルゴリズムを使用しています。P167 「Egress キューへの CoS 値のマッピング」に記載されているように、トラフィッククラスは各ポートに供給された 8 つの Egress キューのうちの一つにマッピングされます。これらのキューと対応しているトラフィックプライオリティのそれぞれへのウェイトを割り当てることができます。このウェイトは、各キューがサービスに登録され、それにより、特定のプライオリティ値に応じたソフトウェア・アプリケーション毎のレスポンス時間に影響する頻度が設定されます。

設定・表示項目

WRR Setting Table

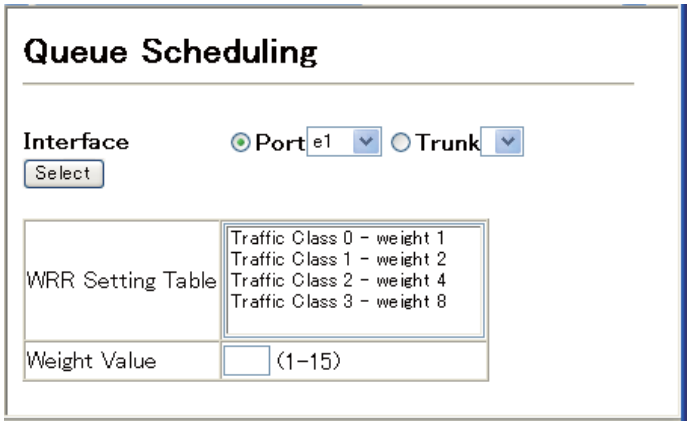
各トラフィッククラス（キュー）のウェイトの値を表します。

Weight Value

選択されたトラフィッククラスの新しいウェイトを設定します。(範囲 :1-15)

設定方法

[Priority] → [Queue Scheduling] をクリックします。インタフェースを選択し、トラフィッククラスを選択します。ウェイト値を入力後、[Apply] をクリックします。



3.12.2 レイヤ 3/4 プライオリティの設定

CoS 値へのレイヤ 3/4 プライオリティのマッピング

本機はアプリケーションの要求を満たすため、レイヤ 3/4 プライオリティをサポートしています。通信プライオリティは Type of Service (ToS) オクテットのプライオリティビットや TCP ポート番号を使用しフレームの IP ヘッダで指定します。プライオリティビットを使用する場合、ToS オクテットは Differentiated Services Code Point(DSCP) サービスの 6 ビットを使用します。これらのサービスが有効な時、プライオリティは CoS 値へマッピングされ、該当する出力キューへ送られます。

異なったプライオリティ情報が通信に含まれている可能性があるため、本機は次の方法で出力キューへプライオリティ値をマッピングしています :

- プライオリティマッピングの優先順位は IP ポートプライオリティ、IP Precedence または DSCP プライオリティ、デフォルトポートプライオリティの順番となります。
- IP Precedence と DSCP プライオリティを両方共有効にすることはできません。どちらか一方を有効にすると、もう一方は自動的に無効になります。

IP DSCP プライオリティの有効

DSCP プライオリティの有効 / 無効を設定します。

設定・表示項目

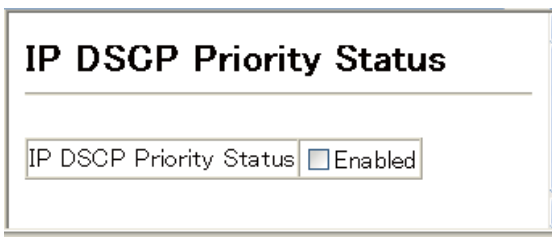
IP DSCP Priority Status

－ Disabled －プライオリティサービスを無効にします（初期設定：無効）

－ IP DSCP － DSCP を使用し、レイヤ 3/4 プライオリティをマッピングします

設定方法

[Priority] → [IP DSCP Priority Status] をクリックします。DSCP Priority Status メニューから Enabled にチェックを入れます。その後［Apply］をクリックします。



DSCP プライオリティのマッピング

DSCP は 6 ビットで最大 64 個の異なった転送動作が可能です。DSCP は ToS ビットと置き換えることができ先行 3 ビットを使用して下位互換性を維持するので、DSCP 非対応で ToS 対応のデバイスは DSCP マッピングを使用することができます。DSCP では、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を異なる種類の転送とすることができます。DSCP 初期設定値は次の表で定められます。指定されていない全ての DSCP 値は CoS 値 0 にマッピングされます：

IP DSCP 値	CoS 値
0,8	0
10, 12, 14, 16,18, 20, 22, 24	1
26, 28, 30, 32, 34, 36,38, 40, 42	2
48,46, 56	3

設定・表示項目

DSCP Priority Table

CoS 値と各 DSCP プライオリティの相関マップを表示します。

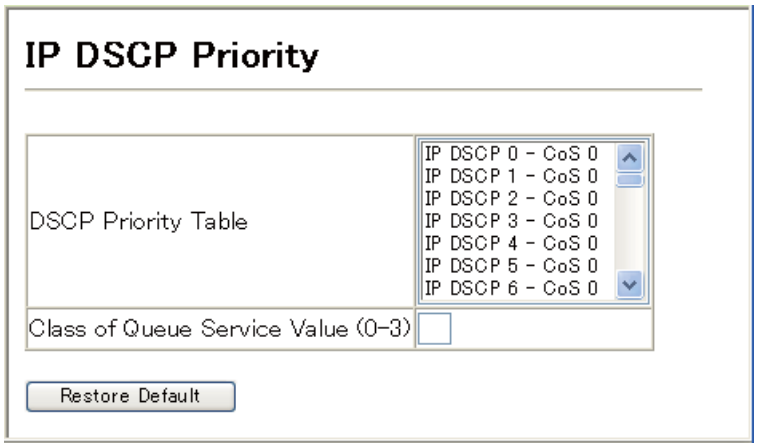
Class of Service Value

選択された DSCP プライオリティ値へ CoS 値をマッピングします。"0" が低いプライオリティ、"3" が高いプライオリティを示します。

[注意]　IP DSCP 設定はすべてのインタフェースに対して有効となります。

設定方法

[Priority] → [IP DSCP Priority] をクリックします。DSCP Priority Table から DSCP Priority 値を選択し、Class of Service Value 値を入力し［Apply］をクリックします。



IP ポートプライオリティのマッピング

フレームヘッダの IP ポート番号 (TCP/UDP ポート番号) に基づき、ネットワークアプリケーションと CoS のマッピングが可能です。よく知られている TCP/UDP ウェルノウンポート番号には、HTTP：80、FTP：21、Telnet：23、POP3：110 などがあります。

設定・表示項目

IP Port Priority Status

IP ポートプライオリティの有効 / 無効

IP Port Priority Table

CoS 値と各 IP ポート番号との相関マップを表示します

IP Port Number (TCP/UDP)

IP ポート番号を設定します。

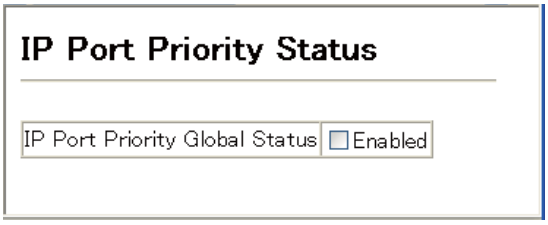
Class of Service Value

選択された IP ポートプライオリティへ CoS 値をマッピングします。“ 0 ” が低いプライオリティ、“ 7 ” が高いプライオリティを示します。

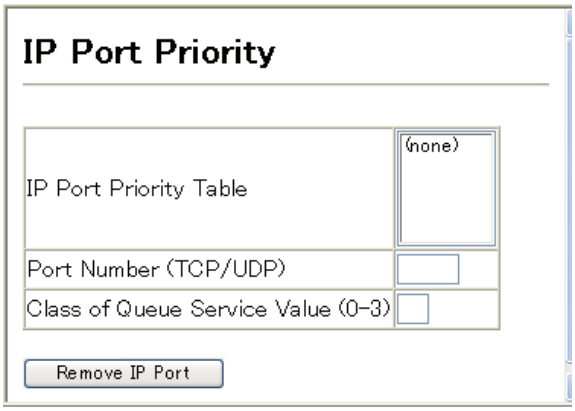
[注意]　IP ポートプライオリティ設定はすべてのインタフェースに対して有効となります。

設定方法

[Priority] → [IP Port Priority Status] をクリックします。



[Priority] → [IP Port Priority] をクリックします。



IP Precedence プライオリティのマッピング

IPv4 ヘッダ中の ToS オクテットは、先行 3 ビットにより、8 段階のプライオリティレベルを定義します。初期設定の IP Precedence 値は Class of Service 値に 1 対 1 でマッピングされています（Precedence 値 0 は CoS 値 0 にマッピング）。プライオリティレベル 6 及び 7 は、ネットワーク制御に使用され、他のレベルは様々なアプリケーション形式に使用されます。ToS ビットは以下の表で定められます

IP Precedence 値	トラフィックタイプ	デフォルト CoS 出力キュー
0	Routine	0
1	Priority	0
2	Immediate	1
3	Flash	1
4	Flash Override	2
5	Critical	2
6	Internetwork Control	3
7	Network Control	3

設定・表示項目

IP Precedence Priority Status

IP Precedence プライオリティの有効 / 無効

IP Precedence Priority Table

CoS 値と各 IP Precedence 値 の相関マップを表示します。

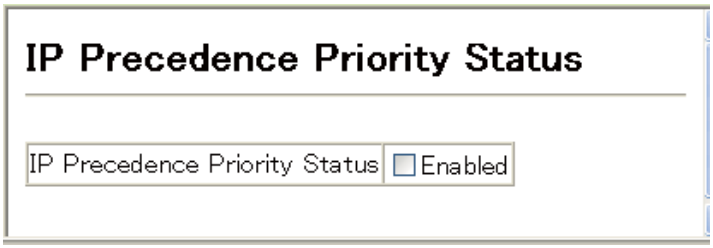
Class of Service Value

選択された IP Precedence 値へ CoS 値をマッピングします。"0" が低いプライオリティ、"3" が高いプライオリティを示します。

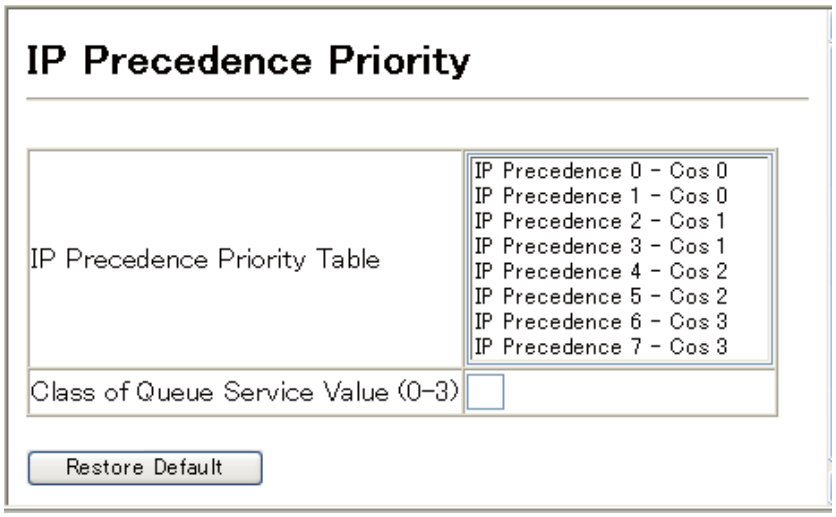
[注意] IP Precedence プライオリティ設定はすべてのインタフェースに対して有効となります。

設定方法

[Priority] → [IP Precedence Priority Status] をクリックします。IP Precedence Priority Status を Enable にします。



[Priority] → [IP Precedence Priority] をクリックします。



ToS プライオリティのマッピング

IP v 4 ヘッダーのサービスタイプ（ToS）は 3 つの部分；優先（3 ビット）、ToS （4 ビット）と MBZ （1 ビット）に分けられます。優先の部分はパケットの重要性を示すのに対して、ToS はスループット、遅延、信頼性、コスト（RFC 1394 に定義）を示します。MBZ （0）は現在は未使用です。

4 つの ToS は 15 の異なった優先順位の値を提供しますが、5 つの値のみ意味を定義されています。ToS 値は以下の表で定められます。

IP ToS 値	リクエストサービス	デフォルト CoS 出力キュー
0	Normal service	0
1	Minimize monetary cost	0
2	Maximize reliability	1
4	Maximize throughput	2
8	Minimize delay	3

設定・表示項目

IP TOS Priority Status

IP ToS プライオリティの有効 / 無効

IP TOS Priority Table

CoS 値と各 IP ToS 値 の相関マップを表示します。

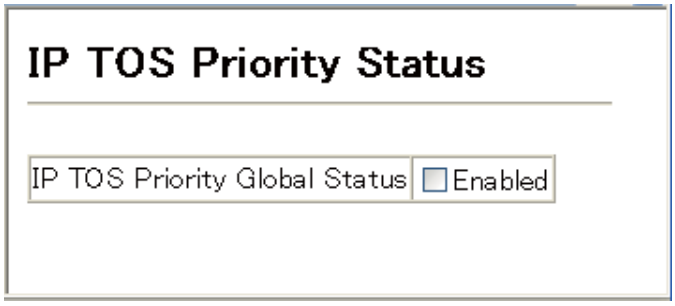
Class of Queue Service Value

選択された ToS 値へ CoS 値をマッピングします。"0" が低いプライオリティ、"3" が高いプライオリティを示します。

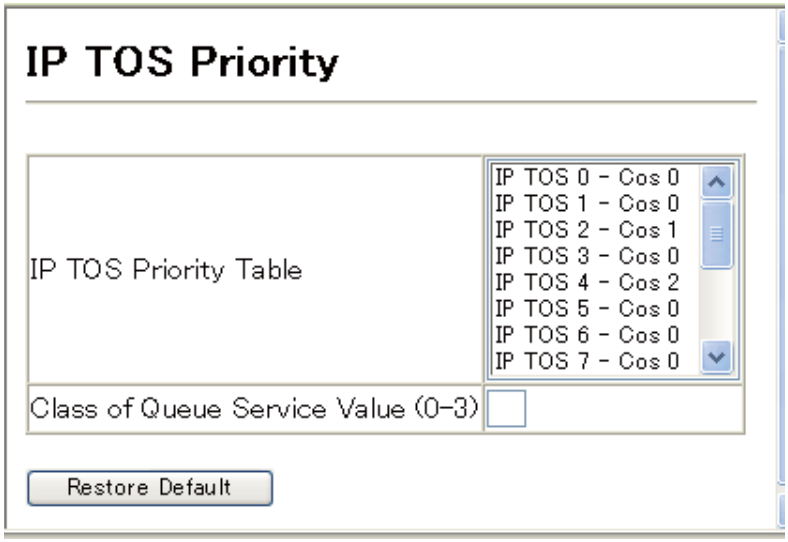
[注意]　IP ToS プライオリティ設定はすべてのインタフェースに対して有効となります。

設定方法

[Priority] → [IP TOS Priority Status] **をクリックします。**



[Priority] → [IP TOS Priority] **をクリックします。**



ACL への CoS 値のマッピング

ACL CoS マッピングページでは、ACL ルールに一致したパケットに対する出力キューの設定が以下の表に基づき設定を行うことができます。

ACL の詳細は 90 ページの「ACL （Access Control Lists)」を参照して下さい。

設定・表示項目

Port

ポート番号

Name

ACL 名

Type

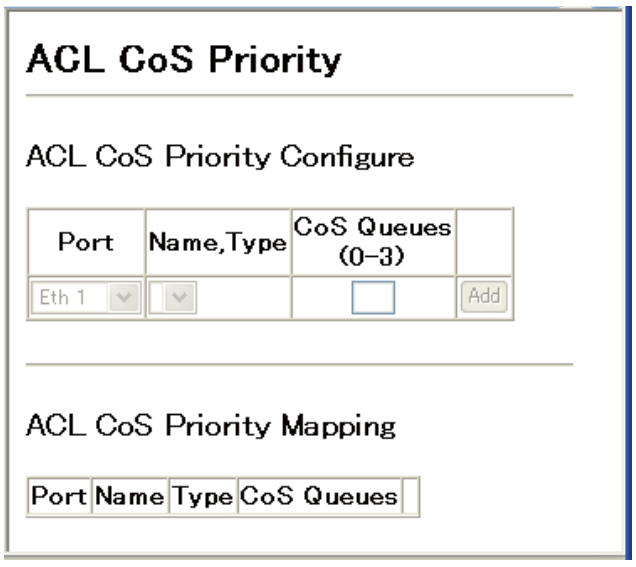
ACL タイプ（IP、MAC）

CoS Priority

ACL ルールにマッチしたパケットに割り当てる CoS キュー

設定方法

[Priority] → [ACL CoS Priority] をクリックします。



3.13 Quality of Service

3.13.1 Quality of Service の設定

この章で記載されているコマンドは QoS(Quality of Service) 機能の基準とサービスポリシーを構成するために使用されます。DiffServ(Differentiated Services) 機能は、ネットワーク上を流れるフレームの 1 つの単位を特定のトラフィックの要件に合致させるため、ネットワークリソースを優先する管理機能を提供します。それぞれのパケットはアクセスリスト、IP Precedence、DSCP、VLAN リストをベースにしたネットワークの中のエントリによって分類されます。アクセスリストを使用することにより、それぞれのパケットが含んでいるレイヤ 2 ～ 4 の情報を元にトラフィックの選別を許可します。設定されたネットワークポリシーをベースにして、異なる種類のトラフィックに対し、異なる種類の転送のためにマークを付けることができます。

インターネットにアクセスするすべてのスイッチとルーターは、同じクラスのパケットには同じ方向への転送を行うためにクラス情報を使用します。クラス情報は、経路の終端のホスト、スイッチ、ルーターのいずれかから割り当てられます。そして、優先度は一般的なポリシー、もしくはパケット詳細調査によって割り当てられます。しかし、パケットの詳細調査はコアスイッチとルーターに負荷がかかり過ぎないようにするため、ネットワークのエッジ側に近いところで行われる必要があります。

経路に属するスイッチとルーターは、異なるクラスにリソースの割り当ての優先順位をつけるため、クラス情報を使用することができます。個々のデバイスが DiffServ 機能に基づいてトラフィックを扱う方法は、Per-Hop Behavior と呼ばれます。経路に属するすべてのデバイスは、エンド・トゥ・エンドの QoS ソリューションを構成するために矛盾のない方法で設定されます。

[注意] クラスマップごとに最大 16 個のルールを設定することができます。ポリシーマップには複数のクラスを設定することもできます。

[注意] ポリシーマップを作成する前にクラスマップを作成してください。作成しない場合、ポリシールールの設定画面からクラスマップを選択することはできません。

[注意] チップの制限により、IP ソースガードと QoS（IP 関連のみ）機能を同時に有効にすることはできません。したがって、もしユーザーが既に IP ソースガード機能を有効にしている場合、QoS 機能の設定を行う前に、IP ソースガードの設定を消去し、無効にする必要があります。

クラスマップの設定

特定のカテゴリや入力トラフィックのためのサービスポリシーを作成するには、下のステップを実施してください。

（1）アクセスリストを作成します。作成方法は 90 ページの「ACL （Access Control Lists)」を参照してください。

（2）Class Map を使用して、トラフィックの特定のカテゴリにクラスの名前を設定します。

（3）アクセスリスト、DSCP、IP Precedence の値、VLAN に基づいてトラフィックの種類を指定するために、それぞれのクラスのルールを編集します。

（4）Policy Map を使用して、入力トラフィックを取り扱う特定の方法のポリシーの名前を設定します。

（5）ポリシーマップに 1 つ、もしくはそれ以上のクラスを追加します。トラフィックに合致するクラスに QoS の値を割り当てるため、setting 画面でそれぞれのクラスにルールを割り当てます。ポリシールールはフローレートとバーストレートの平均の監視、特定のレートを超えたトラフィックの破棄、特定のレートを超えたトラフィックの DSCP サービスレベルを減らすよう構成できます。

（6）Service Policy を使用して、特定のインターフェースにポリシーマップを割り当てます。

設定・表示項目

Class Map

Modify Name and Description

クラスマップの名前と簡単な説明を設定（範囲：name-1-16 文字、Description-1-64 文字）

Edit Rules

Match Class Settings ページを開きます。

Add Class

Class Configurationn ページを開きます。

Remove Class

選択したクラスを削除します。

Class Configuration

Class Name

クラスマップ名（範囲：1-16 文字、）

Type

タイプを指定します。

Description

クラスマップの簡単な説明（範囲：1-64 文字）

Add

指定したクラスを追加します。

Back

前のページに戻ります。

Match Class Settings

Class Name

クラスマップ名（範囲：1-16 文字）

ACL List

ACL リスト名（範囲：1-16 文字）

Add

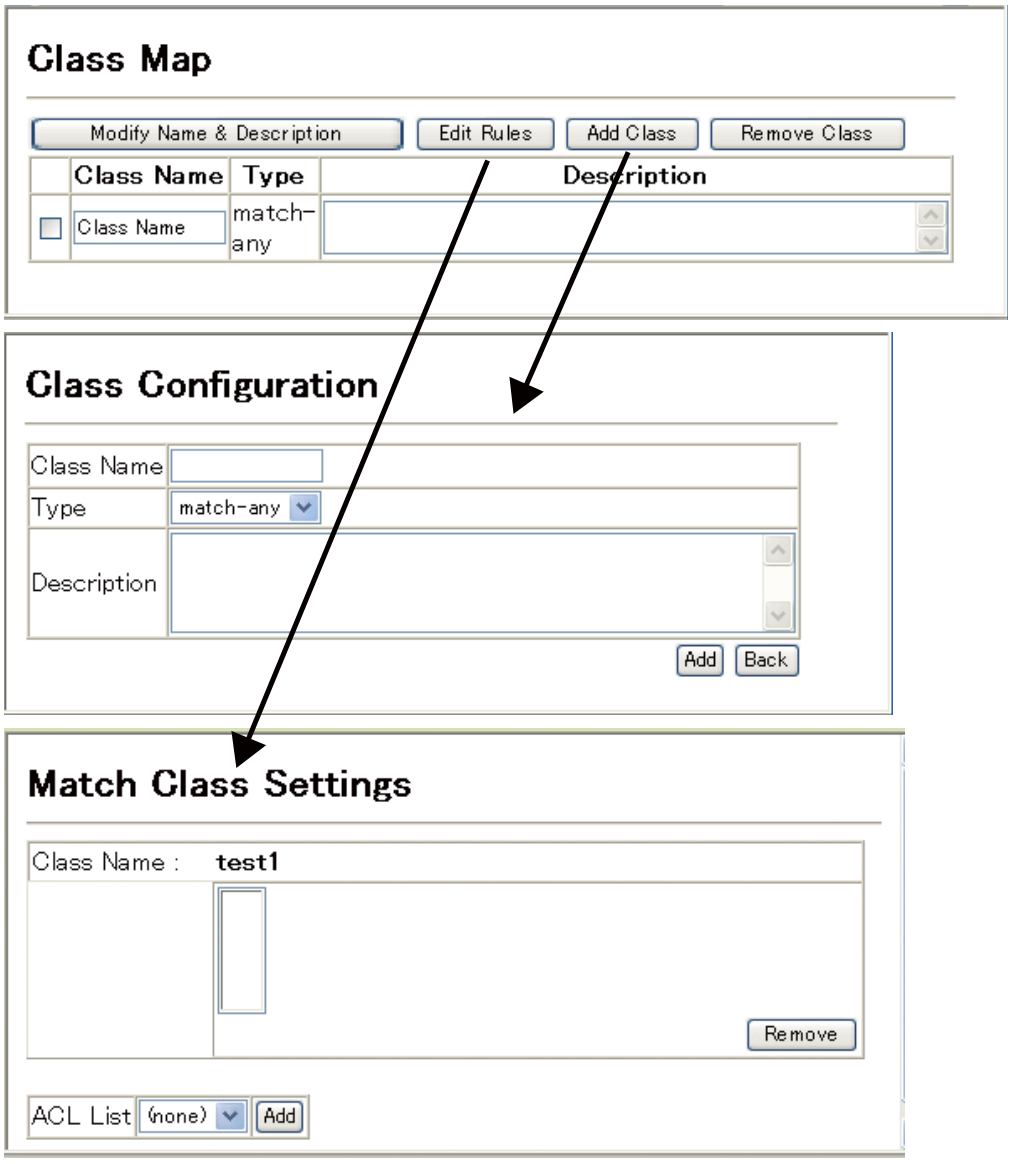
クラスマップに追加します。１つのクラスにつき、最大 16 個まで登録できます。

Remove

選択した基準をクラスから削除します。

設定方法

[QoS] → [DiffServ] → [Class Map] **をクリックします。**[Add Class] **をクリックし、新しいクラスを作成するか、**[Edit Rules] **をクリックし、既存のクラスのルールを編集します。**



QoS ポリシーの作成

この機能は複数のインターフェースに結び付けられたポリシーマップを作成します。
ポリシーマップの設定手順

（1）クラスマップを作成します（P177 「クラスマップの設定」参照）

（2）Policy Map ページを開き、「Add Policy」をクリックします。

（3）「Policy Configuration」ページで「Policy Name」を入力し「Add」をクリックしてください。

（4）「Policy Rule Settings」ページが開きます。スクロールダウンリスト（Class Name の下）からクラス名を選択します。受信した IP パケットの QoS の設定（Action 欄）、最大スループットとバーストレートの設定（Meter 欄）、ポリシーに反するパケットの取り扱い設定（Exceed 欄）で、このクラスの条件に合致したトラフィックのポリシーを構成します。最後に Add をクリックして新しいポリシーを登録します。

- ポリシーマップには複数のクラス設定が含まれています。インターフェースへのポリシーの設定は Service Policy Settings 画面で行います（P166 参照）。それぞれのアクセスリスト（MAC ACL、Standard ACL、Extend ACL）に最大 64 個のポリシーを構成することができます。また、ポリシーマップに適用できるクラスの最大数は 16 個です。
- ポリシングはトークンバケットを基にしています。バケットの深さ（バケットがオーバーフローする前の最大バーストレート）は Burst 欄で指定します。またバケットから移動するトークンの平均レートは Rate 欄で指定します。
- パケットのクラス分け、サービスタグ、帯域幅のポリシーを定義してポリシーマップを作成した後、設定を反映させるため Service Policy 画面で特定のインターフェースにポリシーマップを割り当ててください。

設定・表示項目

Policy Map

Modify Name and Description

ポリシーマップの名前と簡単な説明を設定（範囲：name-1-16 文字、Description-1-64 文字）

Edit Classes

選択したクラスの Policy Rule Settings 画面を開きます。この画面で入力トラフィックへの条件を設定します。

Add Policy

Policy Configuration 画面を開きます。この画面でポリシーの名前と概要を入力し、Add をクリックして Policy Rule Settings 画面を開きます。ここで入力されるトラフィックへの条件を設定します。

Remove Policy

選択したポリシーを削除します。

Policy Configurataion

Policy Name

ポリシー名（範囲：1-16 **文字、）**

Description

ポリシーマップの簡単な説明（範囲：1-64 **文字）**

Add

指定したポリシーを追加します。

Back

ポリシーを追加せず前のページに戻る。

Policy Rule Settings

- Class Settings -

Class Name

クラスマップ名

Action

条件に合致するパケットに適用する CoS、DSCP、IP Precedence **の値。**

Meter

最大スループットとバーストレート

- Rate(kb**p**s) - 1 **秒あたりの転送レート**
- Burst(byte) - **バーストレート**

Exceed Action

特定のレートを超えたトラフィックの破棄、または DSCP **サービスレベルを減らすかを指定します。**

Remove Class

クラスを削除します。

- Policy Options -

Class Name

クラスマップ名

Action

条件に合致するパケットに CoS、IP DSCP **を設定。**

（範囲：CoS-0-7、DSCP-0-63）

Meter

最大スループット / バーストレート

- Rate(kb**p**s) - 1 **秒あたりの転送レート（範囲：**1-100000kbps **または最大ポート速度）**
- Burst(byte) - **バーストレート（範囲：**64-1522）

Exceed

指定したレート / バースト値を超えたトラフィックの処理

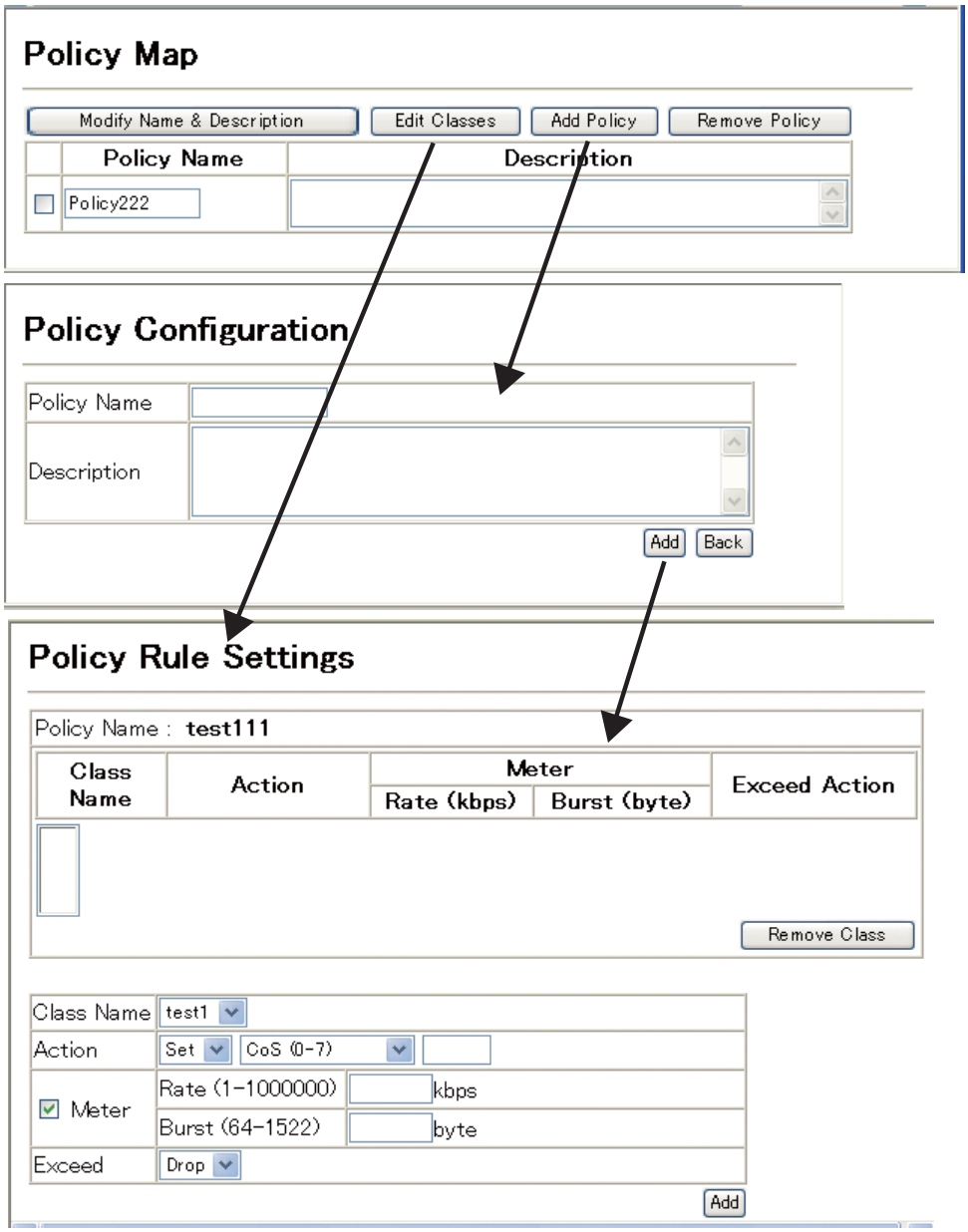
- Drop - **条件に一致しないトラフィックを破棄する**

Add

ポリシーマップに設定した条件を追加。

設定方法

[QoS] → [DiffServ] → [Policy Map] をクリックます。



イングレスキューへのポリシーマップ適用

ポリシーマップをインタフェースの入力キューへ適用します。

設定方法

- 始めにクラスマップの定義を行ってください。その後、ポリシーマップの定義を行い、最後にサービスポリシーをインタフェースへ適用します。
- 一つのインタフェースに一つのポリシーをバインド可能です。
- 現在のファームウェアは、ポリシーマップの出力キューへの適用をサポートしていません。

設定・表示項目

Port

ポートを指定。

Ingress

入力トラフィックへルールを適用します。

Enabled

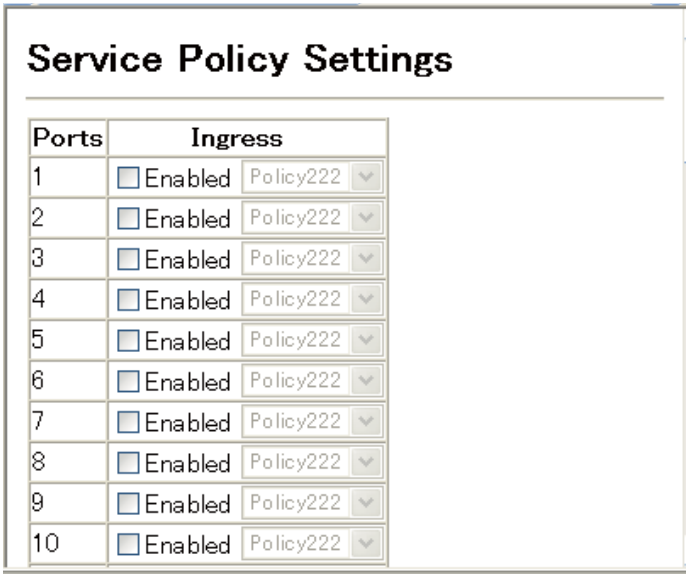
指定したポートでポリシーマップを有効にします。

Policy Map

スクロールダウンボックスからポリシーマップを選択。

設定方法

[QoS] → [DiffServ] → [Service Policy Settings] をクリックします。



3.14 VoIP 設定

IP 電話がエンタープライズネットワークに配置される場合、他のデータトラフィックから VoIP ネットワークを分離することを推奨します。トラフィックの分離は極端なパケット到達遅延、パケットロス、ジッターを防ぎ、より高い音声品質を得ることにつながります。これは 1 つの Voice VLAN にすべての VoIP トラフィックを割り当てることで実現できます。

Voice VLAN を使用することにはいくつかの利点があります。他のデータトラフィックから VoIP トラフィックを分離することでセキュリティが保たれます。エンドトゥーエンドの QoS ポリシーと高い優先度の設定により、ネットワークを横断して VoIP VLAN トラフィックに必要な帯域幅を保証することができます。また、VLAN 分割は音声品質に重大な影響を及ぼすブロードキャストやマルチキャストからトラフィックを保護することができます。

スイッチはネットワーク間で Voice VLAN を設定し、VoIP トラフィックに CoS 値を設定することができます。VoIP トラフィックはパケットの送信先 MAC アドレス、もしくは接続された VoIP デバイスを発見するために LLDP（IEEE802.1AB）を使うことで、スイッチポート上において検出されます。VoIP トラフィックが設定されたポート上で検出されたとき、スイッチは自動的に Voice VLAN のタグメンバーとしてポートを割り当てます。

スイッチポートを手動で設定することもできます。

VoIP トラフィックの設定

VoIP 向けにスイッチを構成するため、最初にスイッチポートに接続された VoIP デバイスの Automatic Detection を有効にし、次にネットワーク中の Voice VLAN の ID を設定します。また Voice VLAN Aging Time は、VoIP トラフィックがポート上で受信されていないとき、Voice VLAN からポートを取り外すために設定します。

設定・表示項目

Auto Detection Status

スイッチポート上で VoIP トラフィックの自動検出を有効にします（初期設定：無効）

Voice VLAN ID

ネットワーク中の Voice VLAN ID を設定します。1 つの Voice VLAN ID のみサポートします。またその VLAN ID は事前にスイッチ上で作成されていなければ行けません（範囲：1 ～ 4096）

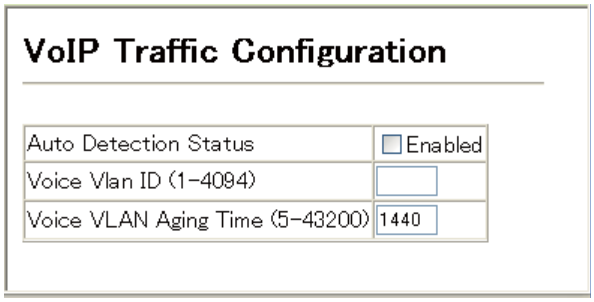
Vioce VLAN Aging Time

Voice VLAN Aging Time…ポート上で VoIP トラフィックが受信されていないとき、ポートが Voice VLAN から取り外されるまでの時間。

[注意]　Auto Detection Status が有効のとき、Voice VLAN ID を設定することができません。

設定方法

[QoS] → [VoIP Traffic Setting] → [Configuration] をクリックします。



VoIP トラフィックポートの設定

VoIP トラフィックのためにポートを構成するため、モード（Auto か Manual）、VoIP デバイスを発見する方法、トラフィックの優先度を設定する必要があります。また VoIP トラフィックのみ Voice VLAN 上を転送できることを保証するため、セキュリティフィルタを有効にすることができます。

設定・表示項目

Mode

ポートが Voice VLAN に加わった場合、VoIP トラフィックをどの時点で検出するかを設定します（初期設定：None）

- None －ポート上で Voice VLAN 機能は無効になります。ポートは VoIP トラフィックを検出せず、Voice VLAN にも追加されません。
- Auto －ポートが VoIP トラフィックを検出したとき、ポートは Voice VLAN のタグメンバーとして追加されます。VoIP トラフィックを検出する方法を、OUI か 802.1AB のどちらかから選択しなくてはいけません。OUI を選択した場合、Telephony OUI List で MAC アドレスの範囲を確認してください。
- Manual － Voice VLAN 機能はポート上で有効になりますが、ポートは手動で Voice VLAN に追加されます。

Security

ポート上で受信した Voice VLAN ID のタグの付いた非 VoIP パケットを破棄するために、セキュリティフィルタを有効にします。VoIP トラフィックは Telephony OUI List で構成された送信元 MAC アドレス、もしくはスイッチ上で接続された VoIP デバイスを発見する LLDP を通して認証されます。VoIP デバイスではない送信元から受信したパケットは破棄されます
（初期設定：無効）

Discovery Protocol

ポート上で VoIP トラフィックを検出するために使う方式を選択します。

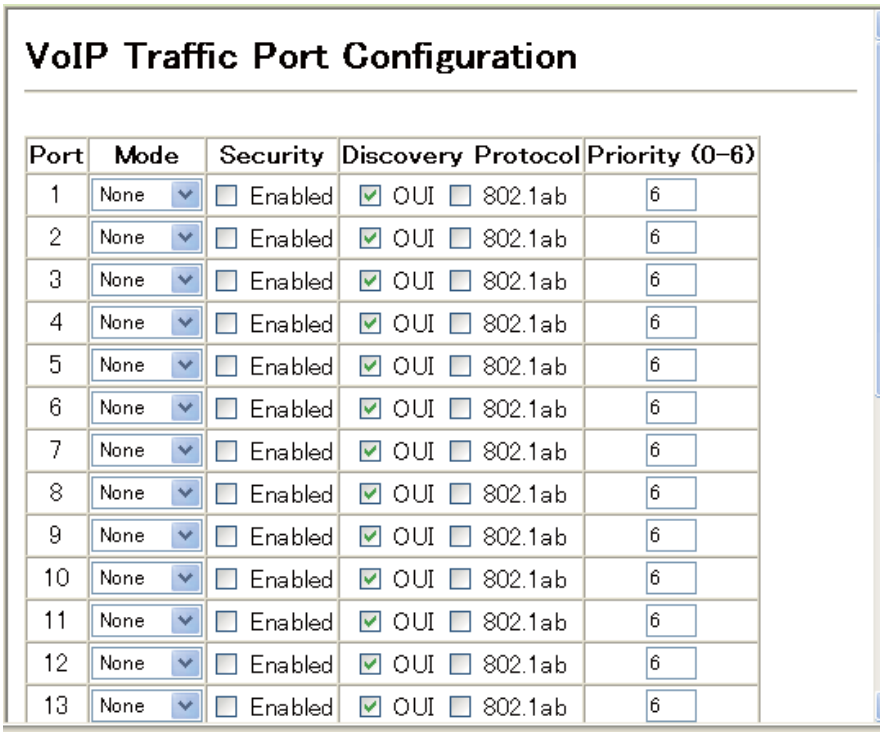
- OUI － VoIP デバイスからのトラフィックは送信元 MAC アドレスの Organizationally Unique Identifier（OUI）によって検出されます。OUI 番号は製造者によって割り当てられ、デバイスの MAC アドレスの最初の 3 オクテットを構成します。スイッチが VoIP デバイスからのトラフィックを認識するには、MAC アドレスの OUI 番号を Telephony OUI List で構成しなくてはいけません。
- 802.1ab －ポートに接続された VoIP デバイス発見するために LLDP を使用します。LLDP は System Capability TLV の中の Telephone Bit が有効であるかどうかをチェックします。LLDP（Link Layer Discovery Protocol）については本マニュアルの LLDP の項目を参照してください。

Priority

Voice VLAN 上のポートとトラフィックの CoS 優先度を定義します。Voice VLAN 機能がポート上で有効であるとき、受信したすべての VoIP パケットの優先度が新しい優先度で上書きされます。

設定方法

[QoS] → [VoIP Traffic Setting] → [Port Configuration] をクリックします。



VoIP Traffic Port Configuration

Port	Mode	Security	Discovery Protocol	Priority (0-6)
1	None	Enabled	OUI 802.1ab	6
2	None	Enabled	OUI 802.1ab	6
3	None	Enabled	OUI 802.1ab	6
4	None	Enabled	OUI 802.1ab	6
5	None	Enabled	OUI 802.1ab	6
6	None	Enabled	OUI 802.1ab	6
7	None	Enabled	OUI 802.1ab	6
8	None	Enabled	OUI 802.1ab	6
9	None	Enabled	OUI 802.1ab	6
10	None	Enabled	OUI 802.1ab	6
11	None	Enabled	OUI 802.1ab	6
12	None	Enabled	OUI 802.1ab	6
13	None	Enabled	OUI 802.1ab	6

テレフォニー OUI の設定

スイッチに接続された VoIP デバイスは、受信したパケットの送信元 MAC アドレスの中の VoIP デバイス製造者の Organizational Unique Identifier（OUI）によって認識されます。OUI 番号は製造者によって割り当てられ、デバイスの MAC アドレスの最初の 3 オクテットを構成します。VoIP デバイスからのトラフィックを VoIP と認識するために、VoIP 機器の MAC アドレスの OUI 番号をスイッチ上で設定することができます。

設定・表示項目

Telephony OUI

リストに追加する MAC アドレスの範囲を指定します。「01-23-45-67-89-AB」というフォーマットで MAC アドレスを入力します。

Mask

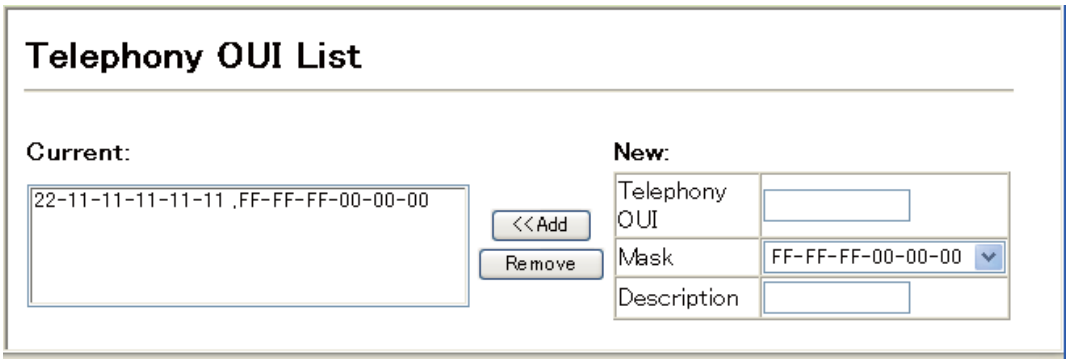
VoIP デバイスの MAC アドレスの範囲を確定します。ここで「FF-FF-FF-00-00-00」を設定すると同じ OUI 番号（最初の 3 オクテットが同一）であるすべてのデバイスを VoIP デバイスとして認識します。他の値を指定することで MAC アドレスの範囲を制限することができます。ここで「FF-FF-FF-FF-FF-FF」を選択すると 1 つの MAC アドレスのみ VoIP デバイスとして設定します（デフォルトでは FF-FF-FF-00-00-00）

Description

VoIP デバイスの内容を説明するテキストを入力します。

設定方法

[QoS] → [VoIP Traffic Setting] → [OUI Configuration] をクリックします。



3.15 マルチキャストフィルタリング

マルチキャストはビデオカンファレンスやストリーミングなどのリアルタイムアプリケーションの動作をサポートします。マルチキャストサーバは各クライアントに対し異なるコネクションを確立することができません。ネットワークにブロードキャストを行うサービスとなり、マルチキャストを必要とするホストは接続されているマルチキャストサーバ / ルータと共に登録されます。また、この方法はマルチキャストサーバによりネットワークのオーバヘッドを削減します。ブロードキャストトラフィックは各マルチキャストスイッチ / ルータによって本サービスに加入しているホストにのみ転送されるよう処理されます。

本機では接続されるホストがマルチキャストサービスを必要とするか IGMP (Internet Group Management Protocol) のクエリを使用します。サービスに参加を要求しているホストを含むポートを特定し、そのポートにのみデータを送ります。また、マルチキャストサービスを受信しつづけるためにサービスリクエストを隣接するマルチキャストスイッチ / ルータに広めます。この機能をマルチキャストフィルタリングと呼びます。

IP マルチキャストフィルタリングの目的は、スイッチのネットワークパフォーマンスを最適化し、マルチキャストパケットをマルチキャストグループホスト又はマルチキャストルータ / スイッチに接続されたポートのみに転送し、サブネット内の全てのポートにフラッディングするのを防ぎます。

3.15.1 レイヤ 2 IGMP（Snooping and Query）

IGMP Snooping and Query －マルチキャストルーティングがネットワーク上の他の機器でサポートされていない場合、IGMP Snooping 及び Query を利用し、マルチキャストクライアントとサーバ間での IGMP サービスリクエストの通過を監視し、動的にマルチキャストトラフィックを転送するポートの設定を行なうことができます。

静的 IGMP ルータインタフェース－ IGMP Snooping が IGMP クエリアを検索できない場合、手動で IGMP クエリア（マルチキャストルータ / スイッチ）に接続された本機のインタフェースの指定を行なうことができます。その後、指定したインタフェースは接続されたルータ / スイッチのすべてのマルチキャストグループに参加し、マルチキャストトラフィックは本機内の適切なインタフェースに転送されます。

静的 IGMP ホストインタフェース－確実にコントロールする必要のあるマルチキャストアプリケーションに対しては、特定のポートに対して手動でマルチキャストサービスを指定することができます。（P195 参照）

IGMP Snooping Query パラメータの設定

マルチキャストトラフィックの転送設定を行います。

IGMP クエリ及びリポートメッセージに基づき、マルチキャストトラフィックを必要とするポートにのみ通信します。すべてのポートに通信をブロードキャストし、ネットワークパフォーマンスの低下を招くことを防ぎます。

機能解説

- IGMP Snooping ― 本機は、IGMP クエリの snoop を受け、リポートパケットを IP マルチキャストルータ / スイッチ間で転送し、IP マルチキャストホストグループを IP マルチキャストグループメンバーに設定します。IGMP パケットの通過を監視し、グループ登録情報を検知し、それに従ってマルチキャストフィルタの設定を行います。
- IGMP Query ― ルータ又はマルチキャスト対応スイッチは、定期的にホストに対しマルチキャストトラフィックが必要かどうかを質問します。もしその LAN 上に 2 つ以上の IP マルチキャストルータ / スイッチが存在した場合、1 つのデバイスが " クエリア " となります。その後、マルチキャストサービスを受け続けるために接続されたマルチキャストスイッチ / ルータに対しサービスリクエストを広げます。

[注意] マルチキャストルータはこれらの情報を、DVMRP や PIM などのマルチキャストルーティングプロトコルと共に、インターネットの IP マルチキャストをサポートするために使用します。

設定・表示項目

IGMP Status

有効にした場合、本機はネットワークの通信を監視し、マルチキャストトラフィックを必要とするホストを特定します。これは IGMP Snooping と呼ばれます。

（初期設定 : 有効 (Enabled)）

Act as IGMP Querier

有効にした場合、本機はクエリアとして機能し、ホストに対しマルチキャストトラフィックが必要かを聞きます。

（初期設定 : 有効 (Enabled)）

IGMP Query Count

応答を受けて、レポートの要求を開始するまで送信するクエリの最大数を入力します。

（2-10、初期設定 :2）

IGMP Query Interval

IGMP クエリメッセージを送信する間隔 (秒) を指定します（60-125、初期設定 :125）

IGMP Report Delay

IP マルチキャストアドレスのレポートをポートで受信してから、IGMP クエリがそのポートから送信され、リストからエントリーが削除されるまでの時間（秒）を設定します（5-25、初期設定 : 10）

IGMP Query Timeout

前のクエリアが停止した後、クエリパケットを受信していたルータポートが無効と判断されるまでの時間（秒）を設定します（300-500、初期設定 :300）

IGMP Version

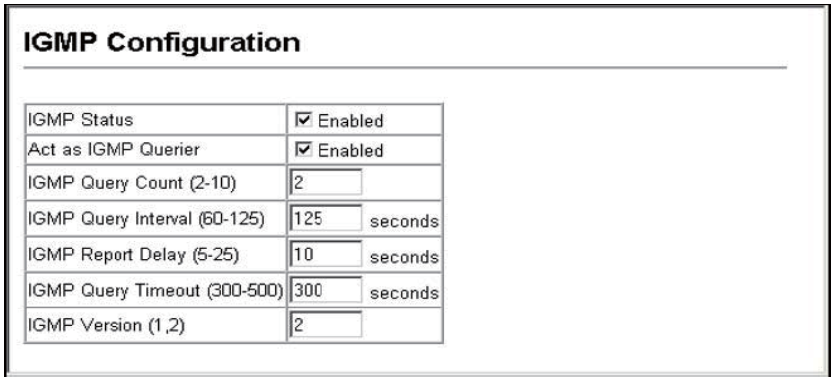
ネットワーク上の他のデバイスと互換性のある IGMP バージョンの設定を行います
（1-2、初期設定 :2）

[注意] サブネット上のすべてのデバイスが同じバージョンをサポートしている必要があります。

[注意] IGMP Report Delay 及び IGMP Query Timeout は IGMP v2 でのみサポートされます。

設定方法

[IGMP Snooping] → [IGMP Configuration] をクリックします。必要な IGMP の設定を行い、[Apply] をクリックします。（以下の画面では初期設定を表示しています。）



3.15.2 IGMP フィルタリング / スロットリング

特定の定期購読契約に基づいた IP/TV サービス等の環境において、管理者が、エンドユーザーの入手できるマルチキャストサービスの制御を希望するケースがあります。

IGMP フィルタリングは、指定されたスイッチポート上のマルチキャストサービスへのアクセス制限したり、同時にアクセスできるマルチキャストグループの数を調整することによって、この条件を満たすことが可能です。

IGMP フィルタリング機能を使用することにより、プロファイルを特定のマルチキャストグループのスイッチ ポートに割り当て、ポート単位でマルチキャスト加入をフィルタリングできます。

IGMP フィルタプロファイルは、一つまたは複数のアドレスを含む範囲を指定することが可能です。ただし、ポートに割り当てられるプロファイルは１つのみです。

アクセスを拒否する IGMP プロファイルがスイッチ ポートに適用された場合、IP マルチキャストトラフィックのストリームを要求する IGMP Join レポートは廃棄され、ポートはそのグループからの IP マルチキャスト トラフィックを受信できなくなります。マルチキャスト グループへのアクセスが許可されている場合は、ポートからのレポート転送はされ、通常の処理が行われます。

IGMP スロットリングは、同時に加入が可能なマルチキャストグループポートの最大値を設定します。グループ数が、設定した最大値に達した時、スイッチは「どちらも拒否する」「置き換え」の内どちらかの処理を行うことができます。

「拒否する」設定になっている場合、全ての新規 IGMPjoin レポートは破棄されます。

「置き換え」設定になっている場合、スイッチはランダムに既存のグループを取り去り、新しいマルチキャストグループに置き換えます。

[注意] IGMP フィルタリングおよびスロットリングは、動的学習を行うマルチキャストグループにのみ適用可能です。静的に構成されたグループでは使用できません。

IGMP フィルタリング / スロットリングの有効

IGMP フィルタリングおよび IGMP スロットリングをスイッチ上で実行するため、
まず最初に、設定を有効にし、IGMP プロファイル番号を作成します。

設定・表示項目

IGMP Filter

IGMP フィルタリングおよびスロットリングを、スイッチ上で有効にします。

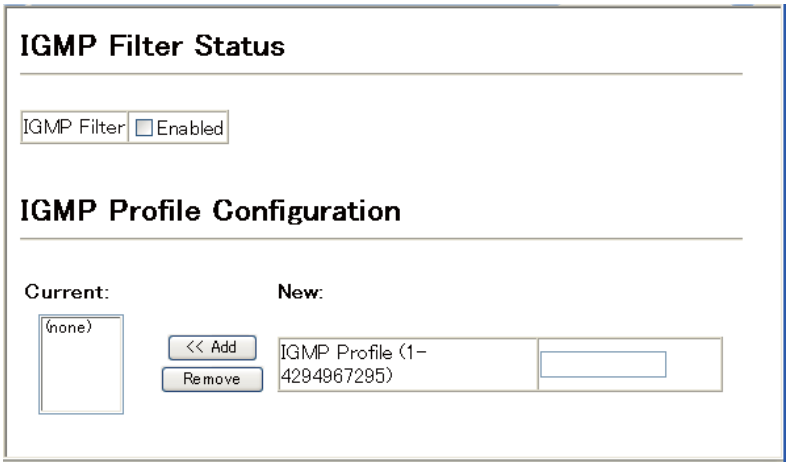
（初期設定 : 無効 (Disabled)）

IGMP Profile

IGMP プロファイル番号を作成します。（範囲 :1-4294967295）

設定方法

[IGMP Snooping] → [IGMP Filter Configuration] をクリックします。必要な設定を行い、[Add] をクリックします。[IGMP Filter Status] → Enabled にチェックを入れ、[Apply] をクリックします。



IGMP Immediate Leave（即時脱退機能）の有効

IGMP スヌーピング immediate-leave（即時脱退機能）の有効 / 無効を設定します。

immediate-leave を有効にすることによって、複数のマルチキャスト グループを同時に使用する環境でも、スイッチド ネットワーク上のすべてのホストに対して最適な帯域幅管理を行うことができます。

設定・表示項目

VLAN ID

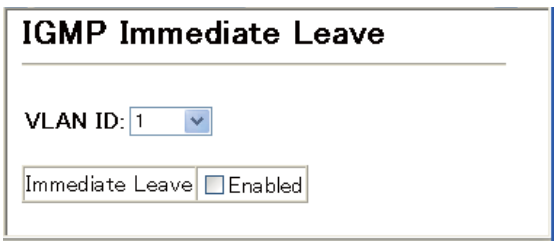
VLAN ID（1-4094）

Immediate Leave

選択した VLAN で、IGMP immediate leave を有効 / 無効

設定方法

[IGMP Snooping] → [IGMP Immediate Leave] をクリックします。



マルチキャストルータに接続されたインタフェースの表示

マルチキャストルータは、IGMP からの情報に加え、インターネットでの IP マルチキャスティングを行うため DVMRP、PIM 等のマルチキャスト・ルーティング・プロトコルを使用します。ルータは、本機により動的に設定されるか、静的にインタフェースの追加を行うことができます。
Multicast Router Port Information ページでは、各 VLAN ID で隣接するマルチキャストルータ / スイッチの接続されたポートを表示します。

設定・表示項目

VLAN ID

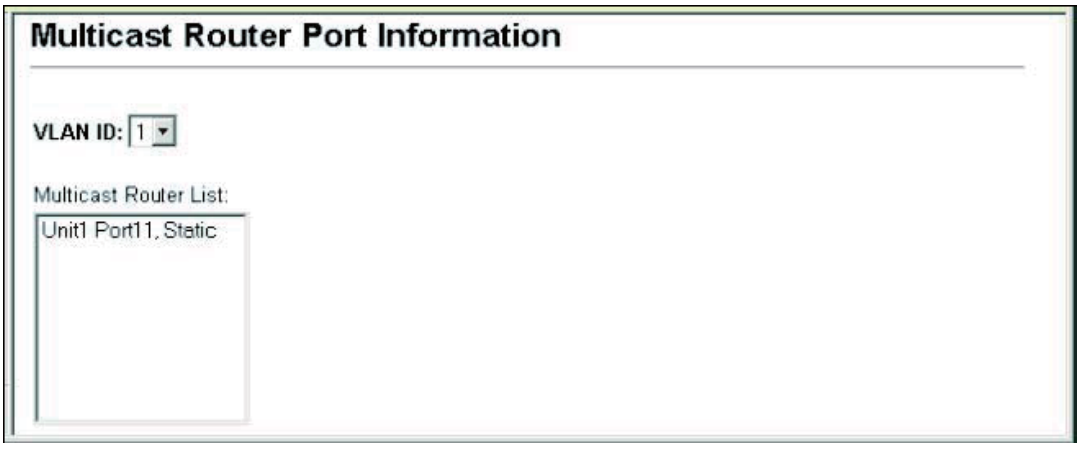
リストを表示させる VLAN ID（1-4094）

Multicast Router List

動的及び静的に設定されたマルチキャストルータの設定情報

設定方法

[IGMP Snooping] → [Multicast Router Port Information] をクリックします。スクロールダウンリストから VLAN ID を選択すると、関連するマルチキャストルータの情報を表示されます。



マルチキャストルータに接続するインタフェースの設定

ネットワーク接続状況により、IGMP snooping による IGMP クエリアが配置されない場合があります。IGMP クエリアとなるマルチキャストルータ / スイッチが接続されているインタフェース（ポート又はトランク）が判明している場合、ルータがサポートするマルチキャストグループへのインタフェース（及び VLAN）の参加設定を手動で行えます。これにより、本機のすべての適切なインタフェースへマルチキャストトラフィックが渡すことができます。

設定・表示項目

Interface

ポート (Port) 又はトランク (Trunk) をスクロールダウンリストから選択します。

VLAN ID

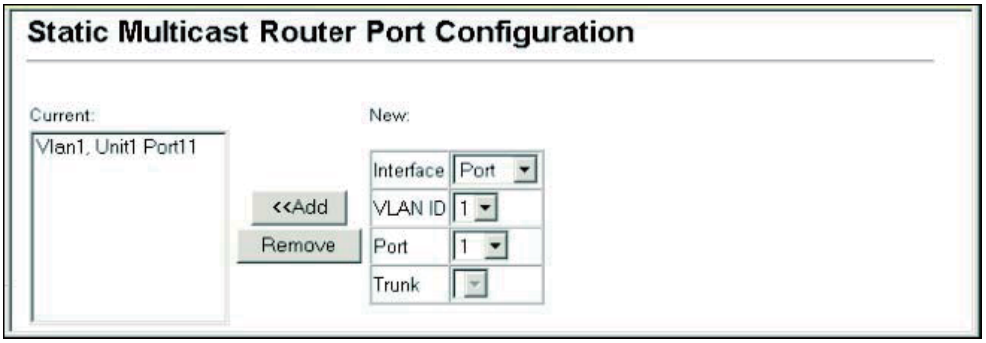
マルチキャストルータ / スイッチから送られるマルチキャストトラフィックを受信し、転送する VLAN を選択します。

PortñîÇÕTrunk

マルチキャストルータに接続されたインタフェースを指定します。

設定方法

[IGMP Snooping] → [Static Multicast Router Port Configuration] をクリックします。マルチキャストルータに接続されたインタフェースとマルチキャストトラフィックを送受信する VLAN を指定し、[Add] をクリックします。すべての設定が完了後、[Apply] をクリックします。



マルチキャストサービスのポートメンバー表示

マルチキャスト IP アドレス及び VLAN を指定し、関連するポートメンバーを表示します。

設定・表示項目

VLAN ID

ポートメンバーを表示する VLAN を選択します。

Multicast IP Address

マルチキャストサービスを行う IP アドレスを選択します。

Multicast Group Port List

VLAN グループに所属し、マルチキャストサービスが送信されるポートが表示されます。

設定方法

[IGMP Snooping] → [IP Multicast Registration Table] をクリックします。VLAN ID とマルチキャスト IP アドレスを選択すると、マルチキャストサービスが送信されるすべてのポートが表示されます。

マルチキャストサービスへのポートの指定

マルチキャストフィルタリングは、P188 「IGMP Snooping Query パラメータの設定」の通り、IGMP snooping と IGMP クエリメッセージを使用し、動的に設定することができます。一部のアプリケーションではさらに細かい設定が必要なため、静的にマルチキャストサービスの設定を行う必要があります。同じ VLAN に参加するホストの接続されたすべてのポートを加え、その後 VLAN グループにマルチキャストサービスの設定を行います。

機能解説

- 静的マルチキャストアドレスはタイムアウトを起こしません。
- マルチキャストアドレスが特定の VLAN に設定された場合、関連するトラフィックは VLAN 内のポートにのみ転送されます。

設定・表示項目

Interface

ポート (Port) 又はトランク (Trunk) をスクロールダウンリストで選択します。

VLAN ID

マルチキャストルータ / スイッチからのマルチキャストトラフィックを受信し、転送する VLAN を選択します。

Multicast IP

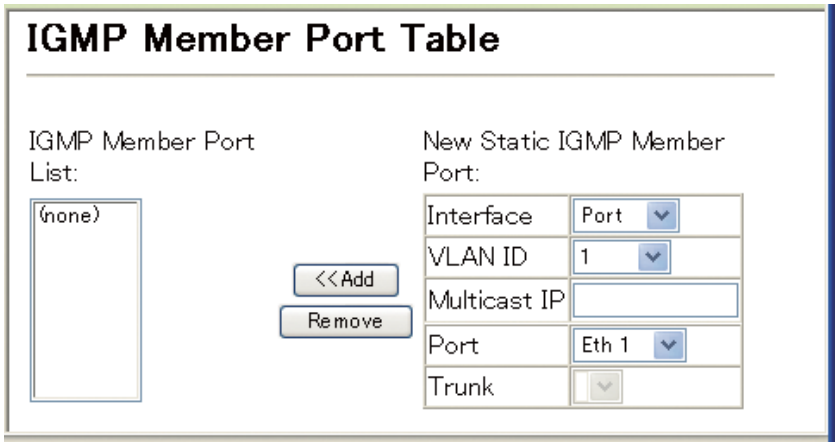
マルチキャストサービスを行う IP アドレスを入力します。

Port 又は Trunk

マルチキャストルータに接続されたインタフェースの番号を指定します。

設定方法

[IGMP Snooping] → [IGMP Member Port Table] をクリックします。マルチキャストサービスに参加させるインタフェース、マルチキャストサービスを転送する VLAN、マルチキャスト IP アドレスを指定し、[Add] をクリックします。すべての設定が終了後、[Apply] をクリックします。



IGMP フィルタプロファイルの設定

IGMP プロファイル番号を作成後、マルチキャストグループのフィルタへの設定、およびアクセスモードの設定を行うことができます。

機能解説

- それぞれのプロフィールはひとつのアクセスモードが設定されます。（許可もしくは拒否）
- アクセスモードが許可に設定時、マルチキャストグループが制御されたコントロール範囲に一致した場合、IGMP join レポートが処理されます。
  拒否に設定時、マルチキャストグループが制御されたコントロール範囲に一致しない場合のみ、IGMP join レポートが処理されます。

設定・表示項目

Profile ID

既存のプロファイル番号から、設定を行う番号を選択します。ID ナンバーを選択した後、「Query」ボタンをクリックすると、現在の設定が表示されます。

Access Mode

プロファイルのアクセスモードを設定します。Permit（許可）または deny（拒否）を指定してください。（初期設定：Deny（拒否）

New Multicast Address Range List

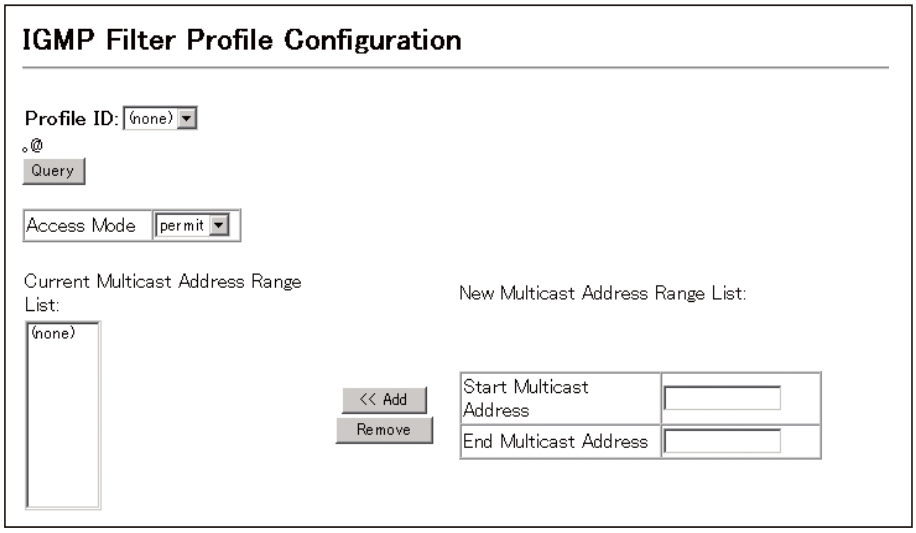
Start と End の IP アドレスを入力し、プロファイルに含めるマルチキャストグループ範囲を指定してください。単独のマルチキャストグループを指定する場合には、Start と End に同一のアドレスを入力してください。「Add」ボタンをクリックすると、範囲が現在のリストに追加されます。

Current Multicast Address Range List

現在、プロファイルに含まれているマルチキャストグループのリスト。
エントリを選択し、「Remove」ボタンをクリックすることで、リストから削除が行えます。

設定方法

[IGMP Snooping] → [IGMP Filter Profile Configuration] をクリックします。設定を行うプロファイル番号を選択し、[Query] をクリックすると現在の設定が表示されます。アクセスモードを指定し、マルチキャストグループをリストへ追加し、[Apply] をクリックします。



IGMP フィルタリング / スロットリングの設定（ポート）

IGMP プロファイルの設定を行うと、それらをインタフェースに適用することができます。また、IGMP スロットリングの設定を行うことで、インターフェイスが加入できる IGMP グループの最大数を設定することもできます。

機能解説

- インタフェースにアサインできるプロファイルは１つのみです。
- ポートがトランクのメンバーである場合、トランクは、最初にポートメンバーへ適用された設定を使用します。
- IGMP スロットリングは、同時に加入が可能なマルチキャストグループポートの最大値を設定します。グループ数が、設定した最大値に達した時、スイッチは「どちらも拒否する」「置き換え」の内どちらかの処理を行うことができます。
  「拒否する」設定になっている場合、全ての新規 IGMP join レポートは破棄されます。
  「置き換え」設定になっている場合、スイッチはランダムに既存のグループを取り去り、新しいマルチキャストグループに置き換えます。

設定・表示項目

Profile

既存のプロファイル、インタフェースに適用するプロファイル番号を選択します。

Max Multicast Groups

同時に加入が可能なマルチキャストグループの最大値を設定します。
（範囲：0 － 1024　初期設定：1024）

Current Multicast Groups

現在加入しているマルチキャストグループを表示します。

Throttling Action Mode

グループ数が、設定した最大値に達した時の処理を選択。（初期設定：deny）

－ deny
　新規のレポートは破棄されます。
－ replace
　既存のマルチキャストグループは、新しいグループへ置き換えられます。

Throttling Status

インタフェース上で、スロットリングの動作が実行されたかどうかを表示します。（オプション：ture または False）

Trunk

ポートがトランクメンバーである場合に表示

設定方法

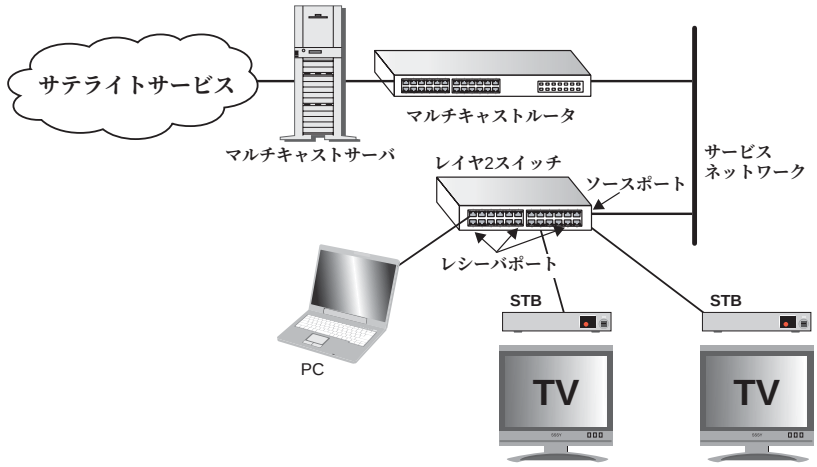
[IGMP Snooping] → [IGMP Filter/Throttling Port Configuration] **または** [IGMP Filter/Throttling Trunk Configuration] **をクリックします。インタフェースに適用するプロファイルを選択し、スロットリング番号および動作を設定後** [Apply] **をクリックします。**

IGMP Filter and Throttling Port Configuration

Port	Profile	Max Multicast Groups (0-256)	Current Multicast Groups	Throttling Action Mode	Throttling Status	Trunk
1	(none)	256	0	deny	False	
2	(none)	256	0	deny	False	
3	(none)	256	0	deny	False	
4	(none)	256	0	deny	False	
5	(none)	256	0	deny	False	
6	(none)	256	0	deny	False	
7	(none)	256	0	deny	False	
8	(none)	256	0	deny	False	
9	(none)	256	0	deny	False	
10	(none)	256	0	deny	False	

3.16 MVR（Multicast VLAN Registration）

Multicast VLAN Registration(MVR) はサービスプロバイダのネットワーク上の、VLAN にマルチキャストのトラフィック（例：テレビチャンネル、ビデオ・オン・デマンド）を送信するために使用されるシングルネットワークへの通信を管理するプロトコルです。MVR ネットワークに入るどのマルチキャストトラフィックも、接続されたすべての Subscribers に送信されます。このプロトコルは動的な監視に必要なオーバーヘッドのプロセスを著しく減少させ、正常なマルチキャスト VLAN のため配送ツリーを設立することができます。これはマルチキャストルーティングプロトコルを使用せずに、広大なネットワークの上に共通のマルチキャストサービスのサポートを可能にします。



MVR の一般的な設定手順

（1）スイッチ全体に MVR を有効にして、MVR に使用する VLAN ID を選択します。次にトラフィックを流すマルチキャストグループを追加します。

（2）ソースポート、レシーバーポートとして MVR に参加するインタフェースを設定します。

（3）Subscribers に MVR グループに動的に参加、離脱することを可能にするため、IGMP Snooping を有効にします（IGMP バージョン 2,3 のホストのみマルチキャスト参加、離脱のメッセージを発行することができます）。

（4）長時間送信し、安定してホストに関連付けられるマルチキャストストリームのため、マルチキャストグループを参加するインタフェースに固定的に結びつけることができます。(206 ページの「静的マルチキャストグループをインタフェースへ追加」を参照)

3.16.1 グローバル MVR 設定

グローバル MVR の設定画面は、下記の項目を設定できます。

設定・表示項目

MVR Status

l スイッチの MVR 機能の有効・無効（初期設定：無効）

MVR Running Status

MVR 環境において、全ての必要条件が満たされているか否かを表示します。

MVR VLAN

ストリーミングのチャンネルとして動作する VLAN ID を指定。

MVR Group IP

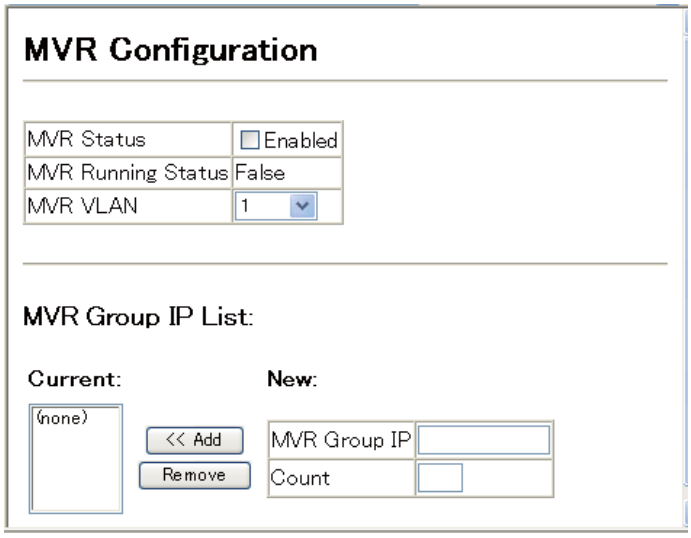
MVR マルチキャストグループの IP アドレス。

Count

連続する MVR グループアドレスの数

設定方法

[MVR] → [Configuration] をクリックします。MVR を有効にし、MVR VLAN を選択します。マルチキャストグループを追加し [Apply] をクリックします。



3.16.2 MVR インタフェース情報の表示

MVR として設定されたインタフェースの情報を表示することができます。

設定・表示項目

Type

MVR ポートタイプを表示します。

Oper Status

リンクステータスを表示します。

MVR Status

MVR ステータスを表示します。MVR がスイッチで有効の場合、ソースポートの MVR ステータスが ” Active ” になります。

Immediate Leave

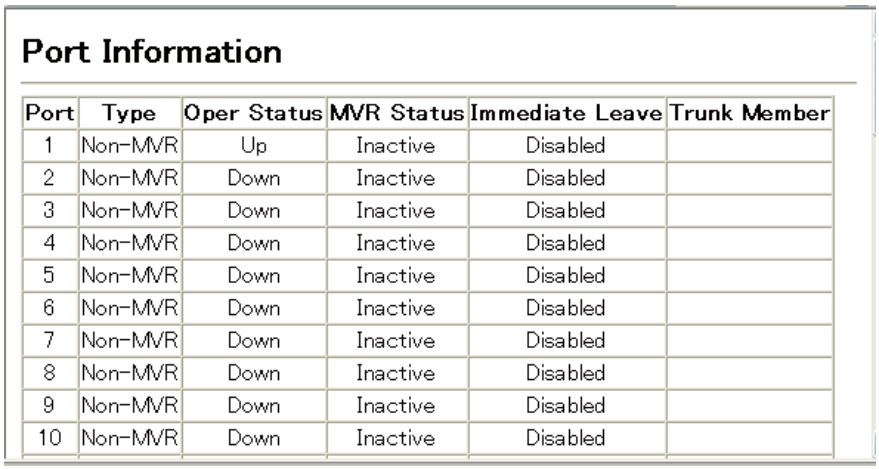
即時脱退の有効 / 無効を表示します。

Trunk Member

ポートがトランクのメンバーであることを表示します。

設定方法

[MVR] → [Port Information] または [Trunk Information] をクリックします。



Port Information

Port	Type	Oper Status	MVR Status	Immediate Leave	Trunk Member
1	Non-MVR	Up	Inactive	Disabled	
2	Non-MVR	Down	Inactive	Disabled	
3	Non-MVR	Down	Inactive	Disabled	
4	Non-MVR	Down	Inactive	Disabled	
5	Non-MVR	Down	Inactive	Disabled	
6	Non-MVR	Down	Inactive	Disabled	
7	Non-MVR	Down	Inactive	Disabled	
8	Non-MVR	Down	Inactive	Disabled	
9	Non-MVR	Down	Inactive	Disabled	
10	Non-MVR	Down	Inactive	Disabled	

3.16.3 マルチキャストグループのポートメンバー表示

MVRV LAN に割り当てられたインタフェースの情報を表示することができます。

設定・表示項目

Group IP

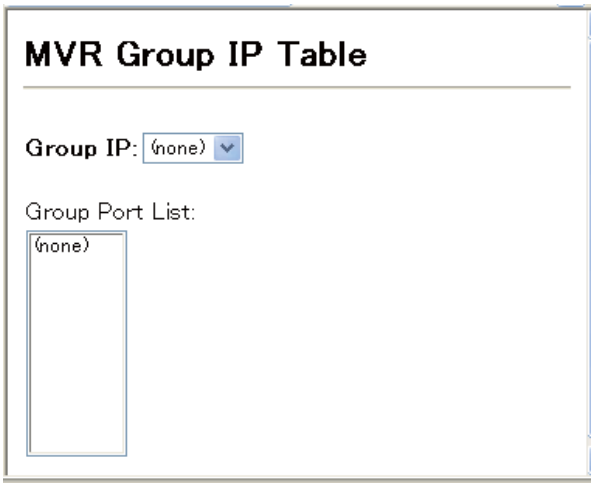
MVR VLAN に割り当てられたマルチキャストグループ

Group Port List

グループに属するインタフェースを表示します。

設定方法

[MVR] → [Group IP Informaation] をクリックします。



3.16.4 MVR インタフェースの設定

MVR に参加したそれぞれのインタフェースは、MVR のソースポートかレシーバーポートとして設定しなくてはいけません。マルチキャストを受信している、インタフェースに接続されている Subscriber が 1 つだけの場合、即時脱退機能を有効にすることができます。

機能解説

- 1 つ、もしくはそれ以上のインタフェースを MVR ソースポートとして設定することができます。
- MVR レシーバーポートはトランクのメンバーにすることができない。レシーバーポートは複数の VLAN に属することができるが、MVR のメンバーにとして設定するべきではありません。
- IGMP Snooping は、マルチキャストフィルタリングの標準ルールを使用して MVR のマルチキャストグループに動的に参加、離脱するソースポートやレシーバーポートを割当てることができます。マルチキャストグループはソースポートやレシーバーポートに固定的に割り当てることもできます。
- Immediate Leave 機能はレシーバーポートのみに適用される。有効にしたとき、レシーバーポートは離脱メッセージに記録されたマルチキャストグループから即座に取り除かれます。Immediate Leave を無効にしたとき、スイッチはグループリストからポートを取り除く前にマルチキャストグループの Subscriber が残っている場合、レシーバーポートに特定のグループのクエリを送信し決定するための返事を待つという、標準のルールに従います。Immediate Leave 機能で離脱するまでの時間を短くすることができますが、同じインタフェースに接続されているグループメンバーへのサービスを混乱させることを避けるため、1 つのマルチキャストの Subscriber がポートに接続されている場合のみ有効にしてください。Immediate Leave 機能はポートに固定的に割り当てられたマルチキャストグループには適用されません。

設定・表示項目

MVR Type

本気では以下にインタフェースタイプをサポートしています。

- Source
- Receiver
- Non-MVR

Immediate Leave

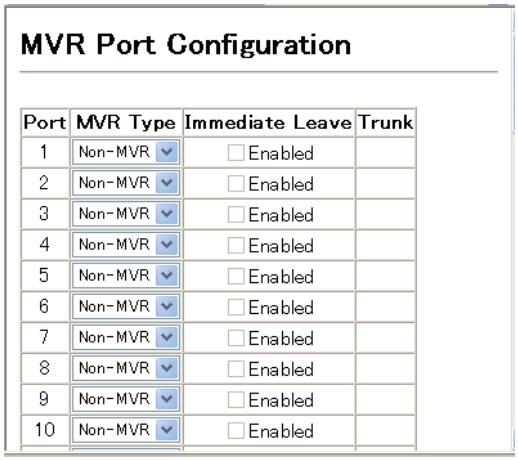
即時脱退処理。Leave メッセージを受け取るとすぐにインターフェイスを転送テーブルから削除できるようにします。

Trunk

トランクのメンバーである場合に表示します。

設定方法

[MVR] → [Port Configuration] **または** [Trunk Configuration] **をクリックします。**



3.16.5 静的マルチキャストグループをインタフェースへ追加

長時間送信し、安定してホストに関連付けられるマルチキャストストリームのため、マルチキャストグループを参加するインタフェースに固定的に結びつけることができます。

機能解説

- MVR で使用するどのマルチキャストグループも Configuration メニューの下で固定的に割り当てられる必要があります。
- マルチキャスト送信に使用される IP アドレスの範囲は 224.0.0.0 から 239.255.255.255 です。MVR グループアドレスは 224.0.0.x の範囲の予約された IP マルチキャストアドレスは使用することができません

設定・表示項目

Interface

ポートまたはトランクを指定します。

Member

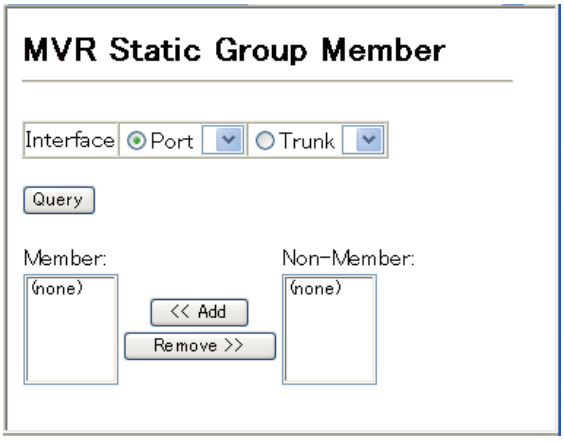
選択したインタフェースへ静的に割り当てられた MVR **マルチキャストの** IP **アドレス。**

Non-Member

選択したインタフェースへ静的に割り当てられていない MVR **マルチキャストの** IP **アドレス。**

設定方法

[MVR] → [Group Member Configuration] **をクリックします。**
[Interface] **フィールドからポートまたはトランクを選択し、**[Query] **をクリックします。**
リストからマルチキャストアドレスを選択し [Add] **または** [Remove] **ボタンをクリックし、メンバーリストを変更します。**



3.17 DHCP Snooping

DHCP Snooping は悪意のある DHCP サーバーや DHCP サーバーに関連のある情報を送信する他のデバイスからネットワークを守ります。この情報は物理ポートへ IP アドレスを戻す際への追跡に役立つ場合があります。

ネットワークの外側から悪意のある DHCP メッセージが受信されたとき、ネットワークトラフィックが混乱する可能性があります。DHCP Snooping はネットワークやファイアウォールの外側からの安全でないインタフェースで受信した DHCP メッセージをフィルタするために使用されます。DHCP Snooping を有効にして VLAN インタフェースに設定したとき、DHCP Snooping テーブル上に載っていないデバイスから untrust のインタフェースで DHCP メッセージを受信するとそれを破棄します。

有効にしたとき、untrust のインタフェースに入った DHCP メッセージには、DHCP Snooping で学習したダイナミックエントリをベースにしたフィルタが行われます。

フィルタのルールは下記の通りです。

- lDHCP Snooping が無効の場合、DHCP パケットは転送される。
- lDHCP Snooping が有効で DHCP パケットを受信する VLAN 上でも有効の場合、すべての DHCP パケットは trust 状態のポートに向けて転送されます。受信したパケットが DHCP ACK メッセージの場合、このエントリはバインドテーブルに追加されます。
- lDHCP Snooping が有効で DHCP パケットを受信する VLAN 上でも有効だが、ポートが trust でない場合は下記の動作を行います。

（1）DHCP パケットが DHCP サーバーからの返答パケット（OFFER,ACK,NAK メッセージを含む）の場合、そのパケットは破棄されます。

（2）DHCP パケットがクライアントからのものである場合、DECLINE や RELEASE メッセージのようなパケットは、一致するエントリがバインドテーブルで見つかった場合のみ、スイッチはパケットを転送します。

（3）DHCP パケットがクライアントからのものである場合、DISCOVER、REQUEST、INFORM、DECLINE、RELEASE メッセージのようなパケットは、MAC アドレスによる照合が無効である場合にはパケットは転送されます。しかし、MAC アドレスの照合が有効の場合、DHCP パケットに記録されているクライアントのハードウェアアドレスが Ehternet ヘッダの Source MAC アドレスと同じ場合にパケットは転送されます。

（4）DHCP パケットが認識できないタイプの場合は破棄されます。

- クライアントからの DHCP パケットが上記のフィルタ基準を通過した場合、同じ VLAN の trust ポートに転送されます。
- サーバーからの DHCP パケットが trust ポートで受信された場合、同じ VLAN の trust ポートと untrust ポートに転送されます。

DHCP Snooping が無効の場合、すべてのダイナミックエントリはバインドテーブルから取り除かれます。

- スイッチ自身が DHCP クライアントの場合の動作
  スイッチが DHCP サーバーにクライアントの Request パケットを送信するポートは trust として設定しなくてはいけません。スイッチは DHCP サーバーから ACK メッセージを受信したとき、自身の情報をバインドテーブルのダイナミックエントリとして追加しません。また、スイッチが DHCP クライアントのパケットを自身に送信したとき、フィルタの動作は発生しません。しかし、スイッチが DHCP サーバーからメッセージを受信したとき、untrust ポートで受信したパケットはすべて破棄されます。

3.17.1 DHCP スヌーピング設定

設定・表示項目

DHCP Snooping Status

スイッチで DHCP スヌーピングを有効 / 無効にします。

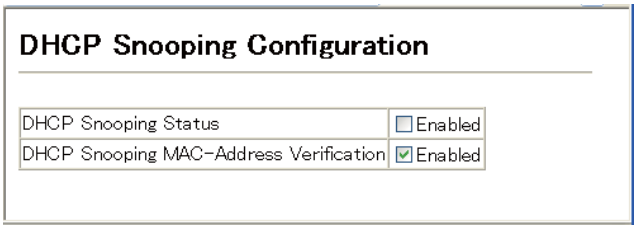
DHCP Snooping MAC-Address Verification

MAC address 検証の有効 / 無効 .

もしパケットの Ethernet ヘッダー で送信元 MAC アドレスが DHCP パケットでクライアントのハードウェアアドレスと同じではないなら、DHCP パケットは破棄されます。

設定方法

[DHCP Snooping] → [Configuration] をクリックします。



3.17.2 DHCP スヌーピング VLAN 設定

特定の VLAN 上で DHCP Snooping を有効にします。

設定・表示項目

VLAN ID

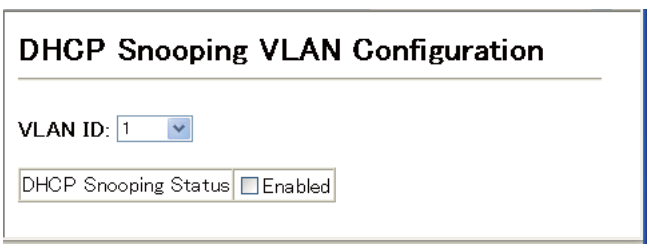
設定を行う VLAN（範囲：1-4094）

DHCP Snooping Status

選択した VLAN での DHCP スヌーピングの有効 / 無効

設定方法

[DHCP Snooping] → [VLAN Configuration] をクリックします。



3.17.3 DHCP スヌーピングオプション設定

DHCP はスイッチと DHCP クライアントについての情報を DHCP サーバーに送信するリレーメカニズムを提供します。これは DHCP Option 82 として知られており、IP アドレスを割り当てたときの情報を使うため、もしくはクライアントに他のサービスやポリシーを設定するために DHCP サーバーに互換性を提供します。

DHCP Snooping Information Option が有効のとき、クライアントは自身の MAC アドレスよりもそれらと接続されているスイッチによって同一であると認証されます。次に、メッセージを交換する DHCP クライアント・サーバーは VLAN 全体にメッセージをフラッディングすることなしで、サーバーとクライアントとの間を直接転送します。

同じケースで、スイッチは DHCP Option 82 Information を既に含むクライアントから DHCP パケットを受信する可能性があります。スイッチはこれらのパケットのためのポリシーを設定することができます。スイッチはその DHCP パケットを破棄するか、パケット内の情報をそのままにするか、スイッチ自身のリレー情報に置き換えるかを設定することができます。

[注意]　パケットの中に DHCP Option 82 Information を埋め込むため、DHCP Snooping 機能を有効にしなくてはいけません。

設定・表示項目

DHCP Snooping Information Option Status

DHCP Option 82 Indormation Relay 有効 / 無効

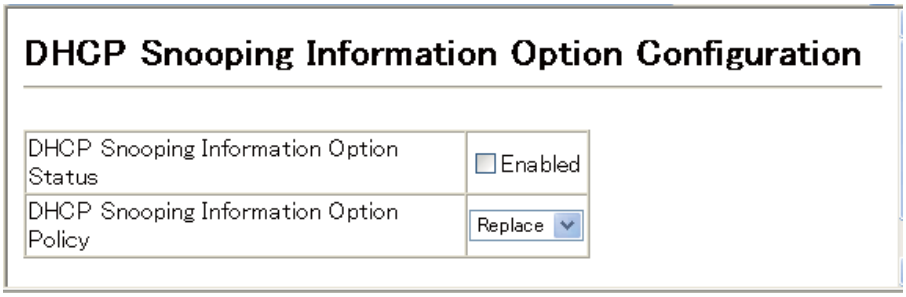
DHCP Snooping Information Option Policy

Option 82 を含む DHCP クライアントからのパケットのため、DHCP Snooping Information オプションを設定 .

- Replace －スイッチのリレー情報で、DHVP クライアントパケットのインフォメーションを上書きします。
- Keep －既存のリレー情報をそのまま保持します。
- Drop －既にリレー情報があった場合そのメッセージを破棄し、全ての VLAN にフラッティングします。

設定方法

[DHCP Snooping] → [Information Option Configuration] をクリックします。



3.17.4 DHCP スヌーピングポート設定

スイッチのポートを trust か untrust に設定することができます。untrust に設定したインタフェースはネットワークやファイアウォールの外側からメッセージを受信するように構成されます。trust に設定したインタフェースはネットワーク内部からのメッセージのみ受信するよう構成されます。

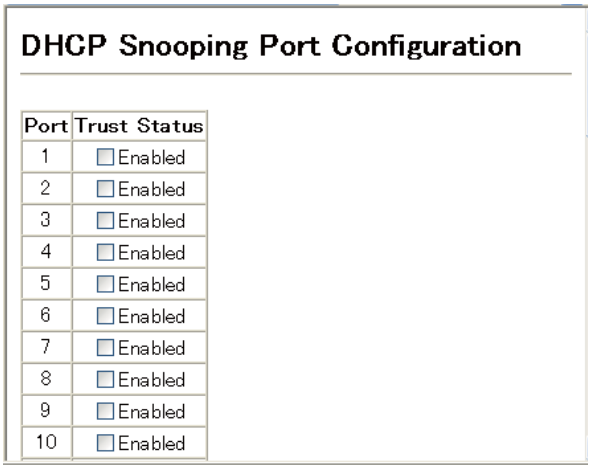
設定・表示項目

Trust Status

ポート Trust ポートとして有効 / 無効に設定します。

設定方法

[DHCP Snooping] → [Information Option Configuration] をクリックします。.



3.18 IP ソースガード

IP ソースガードは、IP ソースガードテーブルに手動で構成されたエントリか、DHCP スヌーピングを有効にしたときの固定・動的エントリを基にして、ネットワークインタフェース上の IP トラフィックをフィルタするセキュリティ機能です。IP ソースガードはあるホストがネットワークにアクセスしてネットワーク内の IP アドレスを使用しようという試みがあったとき、引き起こされる攻撃から守るために使用されます。この章は IP ソースガードで使用するコマンドについて解説します。

[注意] チップの制限により、IP ソースガードと QoS（IP 関連のみ）機能を同時に有効にすることはできません。したがって、もしユーザーが既に IP ソースガード機能を有効にしている場合、QoS 機能の設定を行う前に、IP ソースガードの設定を消去し、無効にする必要があります。

3.18.1 IP ソースガードポート設定

IP ソースガードはネットワークやファイアウォールの外側からメッセージを受信した、保護されていないポート上のトラフィックをフィルタするために使用されます。
有効にしたとき、トラフィックは DHCP スヌーピングを通して学習したダイナミックエントリや IP ソースガードのバインドテーブルで構成された固定アドレスを基にフィルタが行われます。フィルタはスイッチのインバウンドパケットに対して行われ、IP アドレスのみ（SIP）、もしくは IP アドレスと MAC アドレスの両方（SIP-MAC）がバインドテーブル上のエントリと比較されます。パケットがバインドテーブル上のエントリと違う場合、パケットは破棄されます。

設定・表示項目

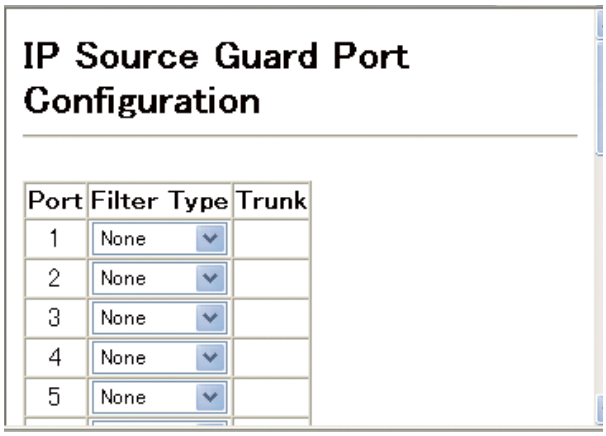
Filter Type

送信元 IP アドレスまたは対応する MAC アドレスを元にした入力トラフィックのフィルタリングを設定

- None － ポートで IP ソースガードフィルタリングを無効
- SIP －バインディングテーブルに保存された IP アドレスによるトラフィックフィルタリングを有効
- SIP-MAC － バインディングテーブルに保存された IP アドレスにおよび対応する MAC アドレスよるトラフィックフィルタリングを有効

設定方法

[IP Source Gard] → [Port Configuration] をクリックします。



3.18.2 バインディング設定（静的 IP）

IP ソースガードのバインドテーブルに固定アドレスを追加します。エントリは MAC アドレス、IP アドレス、リースタイム、エントリの種類（Static、Dynamic）、VLAN ID、Port ID を含んでいます。すべての固定エントリはリースタイムが無限で構成されます。リースタイムはテーブル上では 0 で表示されます。

設定・表示項目

Static Binding Table Counts

テーブル内の静的エントリ合計数

Port

ポート番号（範囲：1-26/50）.

VLAN ID

設定を行う VLAN ID**（範囲：**1-4094）

MAC Address

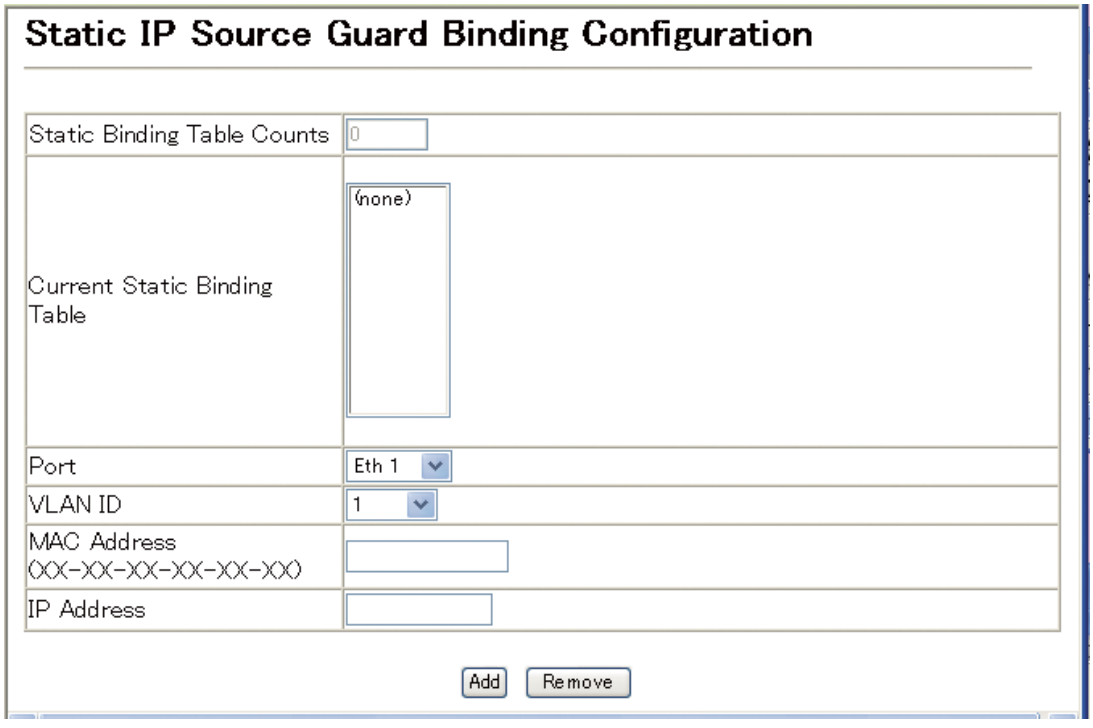
有効なユニキャスト MAC **アドレス**

IP Address

有効なユニキャスト IP **アドレス**

設定方法

[IP Source Gard] → [Static Configuration] **をクリックします。**



3.18.3 バインディング設定（動的 IP）

選択したインタフェースの IP ソースガードの動的に取得した分のバインドテーブルを表示します。

設定・表示項目

Query by

ソースガードバインディングを表示するインタフェースを選択

Dynamic Binding Table Counts

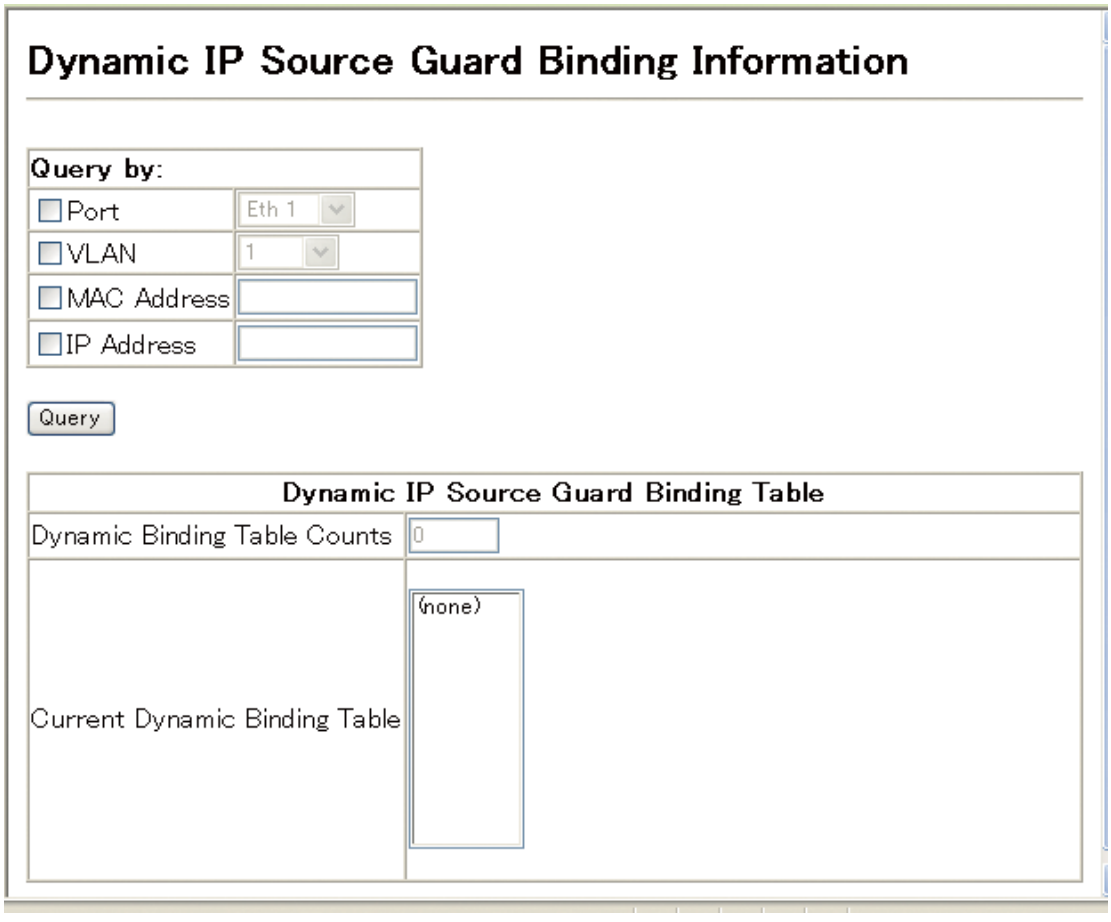
ソースガードバインディングテーブルに登録されている IP アドレス数

Current Dynamic Binding Table

現在の動的バインディングテーブル

設定方法

[IP Source Gard] → [Dynamic Information] **をクリックします。**



3.19 スイッチクラスタリング

スイッチクラスタリングは 1 つのスイッチを通した中央管理を有効にするため、スイッチをグループ化する機能です。クラスタリングをサポートするスイッチは、それらが同じローカルネットワーク内に接続されている限り、物理的な場所やスイッチの種類に関係なくグループ化することができます。

スイッチクラスタは、クラスタの他のすべてのメンバーを管理するために使用するコマンダユニットを持ちます。管理端末は IP アドレスを通してコマンダと直接通信するために Telnet と Web インタフェースの両方を使用することができます。またコマンダはクラスタの内部 IP アドレスを使用してメンバースイッチを管理します。1 つのクラスタに 36 個のメンバーを追加することができます。クラスタに追加するスイッチは同じ IP サブネットに所属しなければいけません。

スイッチをクラスタのコマンダーとして構成した直後、コマンダーはネットワーク上のクラスタを有効にしたスイッチを自動的に発見します。発見されたスイッチは Candidate（候補）と呼ばれ、管理端末を通して手動でクラスタのメンバーに設定することができます。

コマンダとメンバーを構成した後、Web エージェントの右上のドロップダウンメニューからクラスタの ID を選択することで、クラスタに参加したスイッチの管理を行うことができます。コマンダの CLI 画面からは、rcommand コマンドを使用することでメンバースイッチに接続することができます。

3.19.1 クラスタ設定

スイッチのクラスタを作成するためには、最初にスイッチ上でクラスタリングが有効であることを確認し（出荷時設定で有効）、次にクラスタのコマンダとしてスイッチを設定します。ネットワークの IP サブネットと干渉しないようにクラスタの IP Pool を設定します。クラスタ用の IP アドレスは、スイッチがメンバーになりメンバースイッチとコマンダ間の通信で使用されるときにスイッチに割り当てられます。

設定・表示項目

Cluster Status

スイッチクラスタリングの有効 / 無効

Cluster Commander

スイッチをクラスタコマンダーとして有効 / 無効

Role

クラスタスイッチの現在の役割を表示（Commander、Member または Candidate）

Cluster IP Pool

IIP アドレスプールの設定がメンバースイッチに割り当てられる IP アドレスとして内部的に使用されます。クラスタの IP アドレスの形式は「10.x.x. メンバースイッチの id」という構成になります。メンバーに設定する必要のある IP アドレスの数は 1 個から 16 個です。

Number of Members

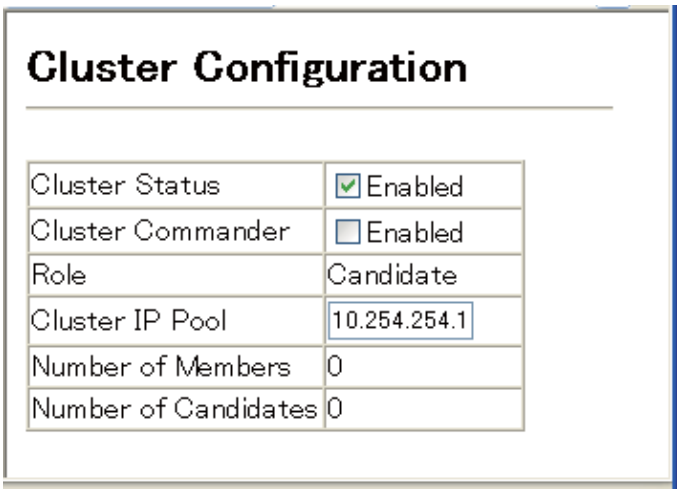
現在のクラスタメンバー数

Number of Candidates

現在、ネットワーク内で検索された候補スイッチ

設定方法

[Cluster] → [Configuration] をクリックします。



3.19.2 クラスタメンバー設定

候補スイッチをクラスタのメンバースイッチとして追加します。

設定・表示項目

Member ID

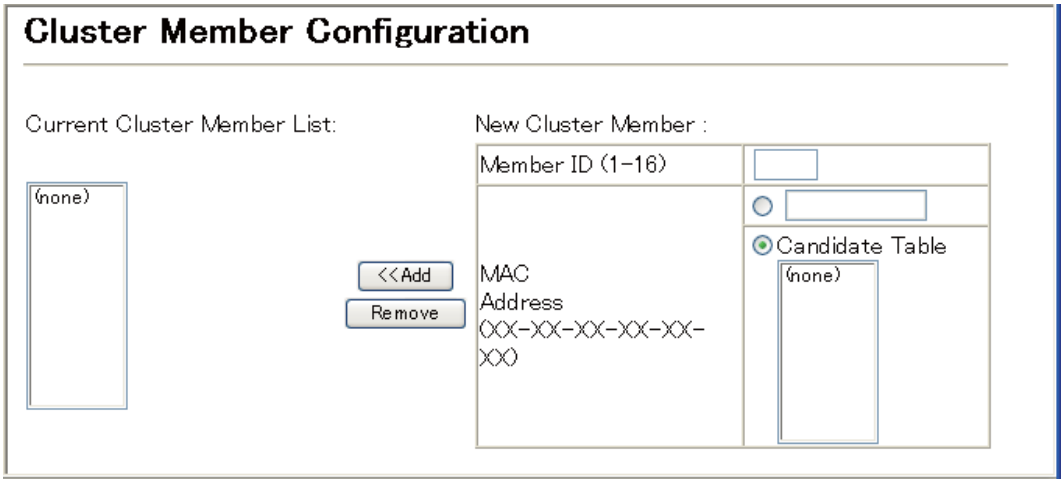
選択した候補スイッチにメンバー ID **を設定します。**

MAC Address

候補テーブルから、スイッチの MAC **アドレスを選択します。あるいは、既知のスイッチ** MAC **アドレスを指定します。**

設定方法

[Cluster] → [Member Configuration] をクリックします。



3.19.3 クラスタメンバー情報

現在のクラスタのメンバースイッチの情報を表示します。

設定・表示項目

Member ID

メンバースイッチの ID **番号（範囲：**1-16）

Role

現在のスイッチクラスタステータス

IP Address

メンバスイッチに割り当てられた、内部クラスタ IP **アドレス**

MAC Address

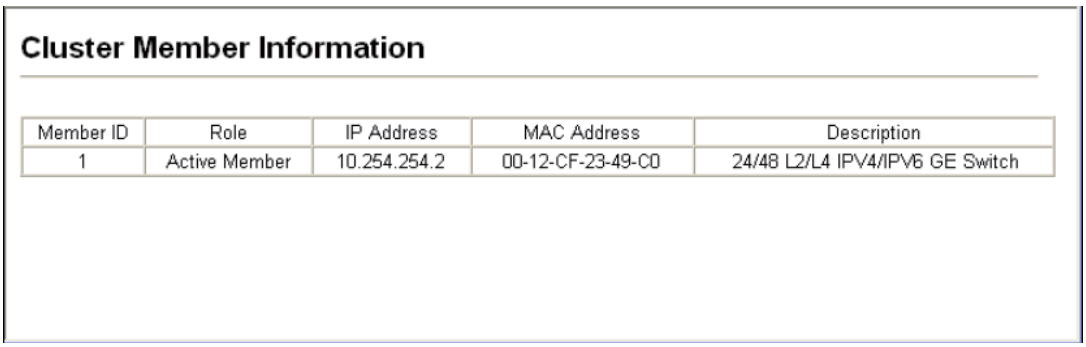
メンバースイッチの MAC **アドレス** .

Description

メンバースイッチの説明

設定方法

[Cluster] → [Member Information] **をクリックします。**



3.19.4 クラスタ候補スイッチ情報

ネットワーク上で発見されたクラスタのメンバーとして利用できるスイッチ（候補スイッチ）、既にクラスタのメンバー（Active Member**）であるスイッチの情報を表示します。**

設定・表示項目

Role

現在のネットワーク内に存在する候補スイッチのステータス

MAC Address

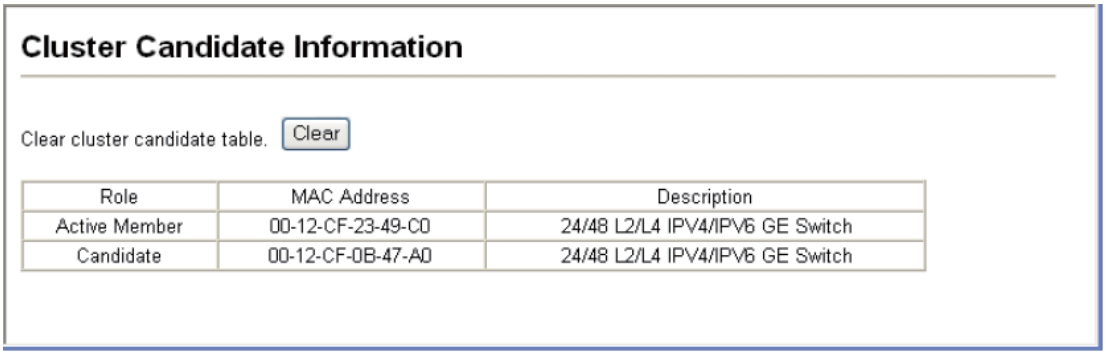
候補スイッチの MAC **アドレス** .

Description

候補スイッチの説明

設定方法

[Cluster] → [Cluster Candidate Information] **をクリックします。**



3.20 UPnP

Universal Plug and Play(UPnP) はデバイスをシームレスに接続し、家庭と企業のネットワークの配置を容易にするプロトコルです。UPnP はインターネットで使用されるオープンなコミュニケーション方式の規格の上で UPnP Device Control Protocol を動作させることでこれを実現します。

UPnP の設定

UPnP の有効 / 無効を設定します。また、タイムアウト値の設定を行います。

チ)、既にクラスタのメンバー（Active Member）であるスイッチの情報を表示します。

設定・表示項目

UPNP Status

UPnP デバイスの有効 / 無効

Advertising Duration

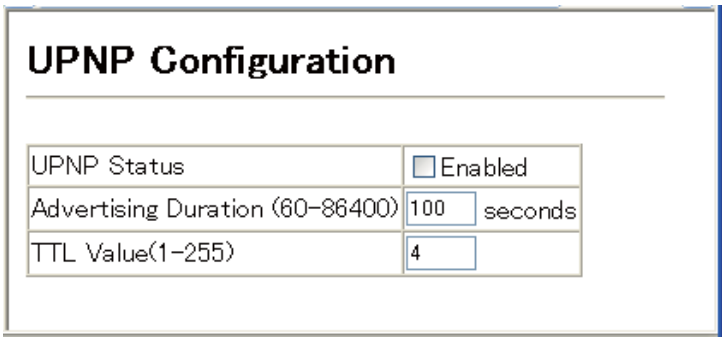
デバイスがステータスをアドバタイズする継続時間を設定します
（範囲：60-86400 秒　初期設定：100 秒）

TTL Value

TTL 値を設定（範囲：1-255　初期設定：4）

設定方法

[UPNP] → [Configuration] をクリックします。



4. コマンドラインインタフェース

4.1 コマンドラインインタフェースの利用

4.1.1 コマンドラインインタフェースへのアクセス

コンソールポート、又はネットワークから Telnet 経由で管理インタフェースにアクセスする場合、Unix のコマンドに似たコマンドキーとパラメータのプロンプト（コマンドラインインタフェース /CLI）により本機の設定を行います。

4.1.2 コンソール接続

コンソールポートへの接続は以下の手順で行います。

（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。初期設定のユーザ名は "admin" と "guest"、パスワードも同じく "admin" と "guest" となっています。管理者ユーザ名とパスワード（初期設定ではどちらも "admin"）を入力した場合、CLI には "Console#" と表示され Privileged Exec モードとなります。一方ゲストユーザ名とパスワード（初期設定ではどちらも "guest"）を入力した場合、CLI には "Console>" と表示され Normal Exec モードとなります。

（2）ユーザ名とパスワードを入力後は、必要に応じたコマンドを入力し、本機の設定、及び統計情報の閲覧を行います。

（3）終了時には "quit" 又は "exit" コマンドを使用しセッションを終了します。

コンソールポートから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 FXC 10/100/1000 is opened.
      To end the CLI session, enter [Exit].

Console#
```

4.1.3 Telnet 接続

Telnet を利用するとネットワーク経由での管理が可能となります。Telnet を行うには管理端末側と本機側のどちらにも IP アドレスを事前に設定する必要があります。また、異なるサブネットからアクセスする場合にはデフォルトゲートウェイもあわせて設定する必要があります。

[注意]　工場出荷時には、本機は DHCP サーバー経由で IP アドレスが割り振られる設定になっています。

IP アドレスとデフォルトゲートウェイの設定例は以下の通りです。

```
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
```

本機を外部と接続されたネットワークに接続する場合には、登録された IP アドレスを設定する必要があります。独立したネットワークの場合には内部で自由に IP アドレスを割り当てることができます。

本機の IP アドレスを設定した後、以下の手順で Telnet セッションを開始することができます。

（1）リモートホストから Telnet コマンドと本機の IP アドレスを入力します。

（2）プロンプト上でユーザ名とパスワードを入力します。Privileged Exec モードの場合には "Vty-0#" と表示されます。Normal Exec モードの場合には "Vty-0>" と表示されます。

（3）ユーザ名とパスワードを入力後は、必要に応じたコマンドを入力し、本機の設定、及び統計情報の閲覧を行います。

（4）終了時には "quit" 又は "exit" コマンドを使用しセッションを終了します。

```
Username: admin
Password:

   CLI session with TigerSwitch 10/100/1000 is opened.
   To end the CLI session, enter [Exit].

Vty-0#
```

[注意]　同時に最大 4 セッションまでの Telnet 接続が可能です。

4.2 コマンド入力

4.2.1 キーワードと引数

CLI コマンドはキーワードと引数のグループから構成されます。キーワードによりコマンドを決定し、引数により設定パラメータを入力します。

例えば、"show interfaces status ethernet 1/5" というコマンドの場合、"show interfaces" と "status" というキーワードがコマンドなり、"ethernet" と "1/5" がそれぞれインタフェースとユニット / ポートを指定する引数となります。

以下の手順でコマンドの入力を行います。

- 簡単なコマンドを入力する場合は、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場合は、各コマンドを必要とされる順番で入力します。例えば Privileged Exec コマンドモードを有効にして、起動設定を表示するためには、以下のようにコマンドを入力します。

```
Console>enable
password:
Console#show startup-config
```

- パラメータを必要とするコマンドを入力する場合は、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。例えば、管理者パスワードを設定する場合には、以下のようにコマンドを入力します。

```
Console(config)#username admin password 0 smith
```

4.2.2 コマンドの省略

CLI ではコマンドの省略を行うことができます。例えば "configuration" というコマンドを "con" と入力するだけでもコマンドとして認識されます。但し、省略したものが複数のコマンドとなり得る場合には、システムから再度コマンドの入力を要求されます。

4.2.3 コマンドの補完

コマンドを入力している途中で Tab キーを押すと、CLI が自動的にコマンドの残りを補完し、キーワードが入力されます。例えば "logging history" コマンドを入力する際に、"log" と入力して Tab キーを押すと "logging" とキーワードがすべて入力されます。

4.2.4 コマンド上でのヘルプの表示

コマンド上で "help" コマンドを入力することで、簡単なヘルプが表示されます。また "?" と入力するとキーワードやパラメータのコマンド文法が表示されます。

コマンドの表示

コマンド上で "?" と入力すると、現在のコマンドクラスの第一階層にあるすべてのキーワードが表示されます。また特定のコマンドのキーワードを表示することもできます。例えば "show ?" と入力すると、"show" コマンド内で使用できるコマンド一覧が表示されます。

```
Console#show ?
  access-group       Access groups
  access-list        Access lists
  accounting         Uses an accounting list with this name
  banner             Banner info
  bridge-ext         Bridge extension information
  calendar           Date and time information
  class-map          Displays class maps
  cluster            Display cluster
  dot1q-tunnel       dot1q-tunnel
  dot1x              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
  lldp               LLDP
  log                System Log records
  logging            Logging setting
  mac                MAC access list
  mac-address-table  Shows the MAC address table
  management         Show management information
  map                Maps priority
  mvr                Show mvr interface information
  network-access     Shows the entries of the secure port.
  policy-map         Displays policy maps
  port               Port characteristics
  private-vlan       Private VLAN
  privilege          Shows current privilege level
  process            Device process
  protocol-vlan      Protocol-VLAN information
  public-key         Public key information
  queue              Priority queue information
  radius-server      RADIUS server information
  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
  upnp               UPnP settings
  users              Information about terminal lines
  version            System hardware and software versions
  vlan               Virtual LAN settings
  voice              Shows the voice VLAN information
  web-auth           Shows web authentication configuration
Console#show
```

"show interfaces ?" と入力した場合には、以下のような情報が表示されます。

```
Console#show interfaces ?
  counters       Interface counters information
  protocol-vlan  Protocol-VLAN information
  status         Interface status information
  switchport     Interface switchport information
Console#show interfaces
```

4.2.5 キーワードの検索

キーワードの一部と共に "?" **を入力すると、入力した文字列から始まるすべてのキーワードが表示されます（入力する際に文字列と** "?" **の間にスペースを空けないで下さい）例えば、** "s?" **と入力すると、以下のように** "s" **から始まるすべてのキーワードが表示されます。**

```
Console#show s?
snmp sntp     spanning-tree   ssh   startup-config
system
Console#show s
```

4.2.6 コマンドのキャンセル

多くのコマンドにおいて、コマンドの前に "no" と入力することでコマンド実行の取り消し、又は初期設定へのリセットを行うことができます。例えば、"logging" コマンドではホストサーバにシステムメッセージを保存します。"no logging" コマンドを使用するとシステムメッセージの保存が無効となります。

本マニュアルでは、各コマンドの解説で "no" を利用してコマンドのキャンセルができる場合にはその旨の記載がしてあります。

4.2.7 コマンド入力履歴の利用

CLI **では入力されたコマンドの履歴が保存されています。「↑」キーを押すことで、以前入力した履歴が表示されます。表示された履歴は、再びコマンドとして利用することができる他、履歴に表示されたコマンドの一部を修正して利用することもできます。**

また、"show history" コマンドを使用すると最近利用したコマンドの一覧が表示されます。

4.2.8 コマンドモード

コマンドセットは Exec と Configuration クラスによって分割されます。Exec コマンドは情報の表示と統計情報のリセットを主に行います。一方の Configuration コマンドでは、設定パラメータの変更や、スイッチの各種機能の有効化などを行えます。

これらのクラスは複数のモードに分けら、使用できるコマンドはそれぞれのモード毎に異なります。"?" コマンドを入力すると、現在のモードで使用できるすべてのコマンドの一覧が表示されます。コマンドのクラスとモードは以下の表の通りです。

クラス	モード	
Exec	Normal Privileged	
Configuration	Global(※)	Access Control List Class Map Interface Line Multiple Spanning Tree Policy Map Server Group VLAN Database

※ Global Configuration モードへは、Privileged Exec モードの場合のみアクセス可能です。他の Configuration モードを使用する場合は、Global Configuration モードになる必要があります。

4.2.9 Exec コマンド

コンソールへの接続にユーザ名 "guest" でログインした場合、Normal Exec モード（ゲストモード）となります。この場合、一部のコマンドしか使用できず、コマンドの使用に制限があります。すべてのコマンドを使用するためには、再度ユーザ名 "admin" でセッションを開始するか、"enable" コマンドを使用して Privileged Exec モード（管理者モード）へ移行します（管理者モード用のパスワードを設定している場合には別途パスワードの入力が必要です）

Normal Exec モードの場合にはコマンドプロンプトの表示が "Console>" と表示されます。
Privileged Exec モードの場合には "Console#" と表示されます。

Privileged Exec モードにアクセスするためには、以下のコマンドとパスワードを入力します。

```
Username: admin
Password: [admin login password]

   CLI session with the FXC 10/100/1000 is opened.
   To end the CLI session, enter [Exit].

Console#
```

```
Username: guest
Password: [guest login password]

   CLI session with the FXC 10/100/1000 is opened.
   To end the CLI session, enter [Exit].

Console#enable
Password: [privileged level password]
Console#
```

4.2.10 Configuration コマンド

Configuration コマンドは Privileged Exec（管理者）モード内のコマンドで、本機の設定変更を行う際に使用します。これらのコマンドはランニングコンフィグレーションのみが変更され、再起動時には保存されません。

電源を切った場合にもランニングコンフィグレーションを保存するためには、"copy running-config startup-config" コマンドを使用します。

Configuration コマンドは複数の異なるモードがあります。

- **Global Configuration** ― "hostname"、"snmp-server community" コマンドなどシステム関連の設定変更を行うためのモードです。
- **Access Control List Configuration** ― パケットフィルタリングを行なうためのモードです。
- **Interface Configuration** ― "speed-duplex" や "negotiation" コマンドなどポート設定を行うためのモードです。
- **Line Configuration** ― "parity" や "databits" などコンソールポート関連の設定を行うためのモードです。
- **VLAN Configuration** ― VLAN グループを設定するためのモードです。

Global Configuration モードにアクセスするためには、Privileged Exec モードで "configure" コマンドを入力します。画面上のプロンプトが "Console(config)#" と変更になり、Global Configuration のすべてのコマンドを使用することができるようになります。

```
Console#configure
Console(config)#
```

他のモードへは、以下の表のコマンドを入力することにより入ることができます。又、それぞれのモードからは "exit" 又は "end" コマンドを使用して Privileged Exec モードに戻ることもできます。

モード	コマンド	プロンプト	ページ
Line	Line {console | vty}	Console(config-line)#	P229
Access Control List	access-list ip standard access-list ip extended access-list ip mac	Console(config-std-acl) Console(config-ext-acl) Console(config-mac-acl)	P373 P373 P379
Class Map	class map	Console(config-cmap)	P542
Interface	Iinterface {ethernet *port* | port-channel *id* | vlan *id*}	Console(config-if)#	P401
MSTP	spanning-tree mst-configuration	Console(config-mstp)#	P470
Policy Map	policy map	Console(config-pmap)	P544
Server Group	aaa group server radius aaa group server tacacs+	Console(config-sg-radius) Console(config-sg-tacacs+)	P320
VLAN	vlan database	Console(config-vlan)	P487

以下の例では、Interface Configuration モードにアクセスし、その後 Privileged Exec モードに戻る動作を行っています。

```
Console(config)#interface ethernet 1/5
Console(config-if)#exit
Console(config)#
```

4.2.11 コマンドラインプロセス

CLI のコマンドでは大文字と小文字の区別はありません。他のコマンドとパラメータの区別ができればコマンドとパラメータの省略をすることができます。また、コマンドの補完をするためにタブ・キーを使用することや、コマンドの一部と "?" コマンドを利用して関連するコマンドを表示させることもできます。

その他に、以下の表のキー入力を使用することもできます。

キー操作	機能
Ctrl-A	カーソルをコマンドラインの一番前に移動します。
Ctrl-B	カーソルを 1 文字左に移動します。
Ctrl-C	現在のタスクを終了し、コマンドプロンプトを表示します。
Ctrl-E	カーソルをコマンドラインの最後に移動します。
Ctrl-F	カーソルを 1 文字右に移動します。
Ctrl-K	カーソルから行の最後までの文字を削除します。
Ctrl-L	現在のコマンド行を新しい行で繰り返します。
Ctrl-N	コマンド入力履歴の次のコマンドを表示します。
Ctrl-P	最後に入力したコマンドを表示します。
Ctrl-R	現在のコマンド行を新しい行で繰り返します。
Ctrl-U	入力した行を削除します。
Ctrl-W	入力した最後のワードを削除します。
Esc-B	カーソルを 1 文字戻します。
Esc-D	カーソルから文字の最後までを削除します。
Esc-F	文字カーソルを進めます。
Delete 又は backspace	コマンド入力を間違えた際に削除します。

4.3 コマンドグループ

システムコマンドは機能別に以下の表の通り分類されます :

コマンド グループ	内容	ページ
Line	**ボーレートやタイムアウト時間などシリアルポート及び** Telnet **を使用した本機への接続に関する設定**	P229
General	Privileged Exec **モードへのアクセスやシステムの再起動、**CLI **からのログアウトなど基本的なコマンド**	P242
System Management	**システムログ、システムパスワード、ユーザ名、ジャンボフレームサポート、**Web **管理オプション、**HTTPS、SSH **などシステム情報に関連したコマンド**	P249
Flash/File	**ファームウェアコードやスイッチの設定ファイルに関連したコマンド**	P312
Authentication	AAA **セキュリティおよびその他ネットワークアクセスコントロール**	P320
Access Control List	IP **アドレス、プロトコル、**TCP/UDP **ポート番号、**TCP **コントロールコード、**MAC **アドレス及びイーサネットタイプによるフィルタリングの提供**	P371
SNMP	**認証エラートラップ** : **コミュニティ名及びトラップマネージャの設定**	P385
Interface	Trunk、LACP **や** VLAN **などを各ポートの設定**	P401
Mirror Port	**通信監視のため、ポートを通るデータを他のポートにミラーリングを行う設定**	P417
Rate Limiting	**通信の最大送受信帯域のコントロール**	P419
Link Aggregation	**複数ポートをグループ化するポートトランク及び** Link Aggregation Control Protocol (LACP) **の設定**	P420
Address Table	**アドレスフィルタの設定やアドレステーブル情報の表示とクリア、エージングタイムの設定**	P432
Spanning Tree	STA **設定**	P462
VLAN	**各ポートの** VLAN **グループの設定及びプライベート** VLAN**、プロトコル** VLAN **の設定**	P487
LLDP	LLDP **設定**	P436
Class of Service	**タグなしフレームの各ポートのプライオリティの設定。各プライオリティキューのウェイトの確認。** IP precedence、DSCP、TCP **トラフィックタイプのプライオリティの設定**	P523
Quality of Service	Diff Serv **の設定**	P541
Voice VLAN	VoIP **トラフィック検出および** Voice VLAN **の設定**	P552
Multicast Filtering	IGMP **マルチキャストフィルタ、クエリア、クエリ及び、各ポートに関連するマルチキャストルータの設定**	P559
IP Interface	**管理アクセス用** IP **アドレスの設定**	P589
DHCP Snooping	DHCP **スヌーピングの設定**	P595
IP Source Guard	IP **ソースガードセキュリティの設定**	P606
IP Cluster	**スイッチクラスタリングの設定**	P611
UPnP	UPnP **の設定**	P618

本章内の表で用いられるコマンドモードは以下の括弧内のモードを省略したものです。

ACL (Access Control List Configuration)
GM (Class Map Configuration)
GC (Global Configuration)
IC (Interface Configuration)
LC (Line Configuration)
SG (Server Group)
MST (Multiple Spanning Tree)
NE (Normal Exec)
PE (Privileged Exec)
PM (Policy Map Configuration)
VC (VLAN Database Configuration)

4.4 Line （ラインコマンド）

VT100 互換のデバイスを使用し、シリアルポート経由で本機の管理プログラムにアクセスすることができます。本コマンドはシリアルポート接続及び Telnet 端末との接続の設定を行うために使用されます。

コマンド	機能	モード	ページ
line	コンソール接続の設定及び line configuration モードの開始	GC	P230
login	コンソール接続時のパスワードの有効化	LC	P231
password	コンソール接続時のパスワードの設定	LC	P232
timeout login response	CLI のログイン入力待ち時間の設定	LC	P233
exec-timeout	接続時のタイムアウトまでのインターバル時間の設定	LC	P234
password-thresh	パスワード入力時のリトライ数の設定	LC	P235
silent-time*	ログインに失敗した後のコンソール無効時間の設定	LC	P236
databits*	各文字あたりのデータビットの設定	LC	P237
parity*	パリティビット生成の設定	LC	P237
speed*	ボーレートの設定	LC	P239
stopbits*	1byte あたりのストップビット値の設定	LC	P240
disconnect	Line 接続を終了	PE	P240
show line	ターミナル接続の設定情報を表示	NE,PE	P241

* コンソール接続にのみ反映されます。

Line

Line の設定を行うために使用します。また、本コマンドを使用した後、詳細な設定が行えます。

文法

line <console | vty >

- **console** ― コンソール接続
- **vty** ― 仮想ターミナルのためのリモートコンソール接続

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

Telnet は仮想ターミナルの一部となり "show users" コマンドを使用した場合などは "vty" と表示されます。但し、"databits" などのシリアル接続のパラメータは Telnet 接続に影響しません。

例

本例ではコンソールラインモードに入るための例を示しています。

```
Console(config)#line console
Console(config-line)#
```

関連するコマンド

show line (P241)

show users (P309)

login

ログイン時のパスワードを有効にします。"no" を前に置くことでパスワードの確認を無効にし、パスワードなしでアクセスすることが可能になります。

文法

login { local }

no login

- **local ― ローカル接続時のパスワードが有効となっています。認証は "username" コマンドで設定したユーザ名を元に行います。**

初期設定

login local

コマンドモード

Line Configuration

コマンド解説

- **本機へのログインには** 3 **種類の認証モードがあります。**
  － login を選択した場合、コンソール接続用のコマンドは 1 **つだけになります。この場合管理インタフェースは** Normal Exec (NE) **モードとなります。**
  － login local を選択した場合、"usaname" **コマンドを使用して指定したユーザ名とパスワードを使用してユーザ認証が行なわれます。この場合、管理インタフェースは入力したユーザのユーザレベルに応じて** Normal Exec (NE) **モード又は** Privileged Exec (PE) **モードのどちらかになります。**
  － no login を選択すると認証はなくなります。この場合、管理インタフェースは Normal Exec(NE) **モードとなります。**

- **本コマンドはユーザ認証を本体で行う場合のものです。認証サーバを使用してユーザ名とパスワードの設定を行う場合には** RADIUS **又は** TACACS+ **ソフトウェアをサーバにインストールする必要があります。**

例

```
Console(config-line)#login local
Console(config-line)#
```

関連するコマンド

username (P265)

password (P232)

password

コンソール接続のためのパスワードの設定を行います。"no" **を前に置くことでパスワードを削除します。**

文法

password < 0 | 7> *password*

no *password*

- {0 | 7} ― "0" **は平文パスワードを、**"7" **は暗号化されたパスワードとなります。**
- password ― **コンソール接続用のパスワード（最大** 8 **文字（平文時）、**32 **文字（暗号化時）。大文字と小文字は区別されます）。**

初期設定

パスワードは設定されていません

コマンドモード

Line Configuration

コマンド解説

- **パスワードの設定を行うと、接続時にパスワードを要求するプロンプトが表示されます。正しいパスワードを入力するとログインできます。"password-thresh" コマンドを使用し、パスワード入力時のリトライ数を設定することができます。**
- **暗号化されたパスワードはシステム起動時に設定ファイルを読み込む場合や** TFTP **サーバにダウロードする場合のためにテキスト（平文）パスワードとの互換性があります。暗号化されたパスワードを手動で生成する必要はありません。**

例

```
Console(config-line)#password 0 secret
Console(config-line)#
```

関連するコマンド

login (P231)

password-thresh (P235)

timeout login response

CLI からのログイン入力のタイムアウト時間を設定します。"no" を前に置くことで初期設定に戻します。

文法

timeout login response { *seconds* }

no timeout login response

- *seconds* — タイムアウト時間（秒）（範囲：0-300 秒、0：タイムアウト設定なし）

初期設定

- CLI：無効（0 秒）
- Telnet：300 秒

コマンドモード

Line Configuration

コマンド解説

- 設定時間内にログインが検知されなかった場合、接続は切断されます。
- 本コマンドはコンソール接続と Telnet 接続の両方に有効となります。
- 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コマンドを実行した場合、初期設定に戻します。

例

本例ではタイムアウト時間を 120 秒（2 分）に設定しています。

```
Console(config-line)#timeout login response 120
Console(config-line)#
```

関連するコマンド

silent-time (P236)

exec-timeout (P234)

exec-timeout

ユーザ入力のタイムアウト時間の設定を行います。"no" **を前に置くことでタイムアウト時間の設定を削除します。**

文法

exec-timeout *seconds*

no exec-timeout

- seconds ― **タイムアウト時間（秒）**（0 - 65535**（秒）**、0**：タイムアウト設定なし）**

初期設定

CLI**：タイムアウト設定なし**

Telnet**：**600 **秒（**10 **分）**

コマンドモード

Line Configuration

コマンド解説

- **設定時間内に入力が行なわれた場合、接続は維持されます。設定時間内に入力がなかった場合には接続は切断され、ターミナルは待機状態となります。**
- **本コマンドはコンソール接続と** Telnet **接続の両方に有効となります。**
- Telnet **のタイムアウトを無効にすることはできません。**

例

本例ではタイムアウト時間を 120 **秒（**2 **分）に設定しています。**

```
Console(config-line)#exec-timeout 120
Console(config-line)#
```

password-thresh

ログイン時のパスワード入力のリトライ回数の設定に使用するコマンドです。"no" を前に置くことで指定したリトライ回数は削除されます。

文法

password-thresh *threshold*

no password-thresh

- *threshold* ― **リトライ可能なパスワード入力回数（設定範囲：**0-120**、**0**：回数の制限をなくします）**

初期設定

3

コマンドモード

Line Configuration

コマンド解説

- **リトライ数が設定値を超えた場合、本機は一定時間、ログインのリクエストに応答しなくなります（応答をしなくなる時間に関しては "silent-time" コマンドでその長さを指定できます）。**Telnet **時にリトライ数が制限値を超えた場合には** Telnet **インタフェースが終了となります。**
- **本コマンドはコンソール接続と** Telnet **接続の両方に有効です。**

例

本例ではパスワードのリトライ回数を 5 **回に設定しています。**

```
Console(config-line)#password-thresh 5
Console(config-line)#
```

関連するコマンド

silent-time (P236)

silent-time

ログインに失敗し、"password-thresh" コマンドで指定したパスワード入力のリトライ数を超えた場合にログイン要求に反応をしない時間を設定するためのコマンドです。"no" **を前に置くことで設定されている値を削除します。**

文法

silent-time *seconds*

no silent-time

- *seconds* ― **コンソールの無効時間（秒）（設定範囲：**0-65535**、**0**：コンソールを無効にしない）**

初期設定

コンソールの応答無効時間は設定されていません。

コマンドモード

Line Configuration

例

本例ではコンソール無効時間を 60 **秒に設定しています。**

```
Console(config-line)#silent-time 60
Console(config-line)#
```

関連するコマンド

password-thresh (P235)

databits

コンソールポートで生成される各文字あたりのデータビットの値を設定するためのコマンドです。"no" を前に置くことで初期設定に戻します。

文法

databits < 7 | 8 >

no databits

- 7 ― 7 **データビット**
- 8 ― 8 **データビット**

初期設定

8 **データビット**

コマンドモード

Line Configuration

コマンド解説

パリティが生成されている場合は 7 **データビットを、パリティが生成されていない場合** (no parity) **は** 8 **データビットを指定して下さい。**

例

本例では 7 **データビットに設定しています。**

```
Console(config-line)#databits 7
Console(config-line)#
```

関連するコマンド

parity (P237)

parity

パリティビットの設定のためのコマンドです。"no" **を前に置くことで初期設定に戻します。**

文法

parity < none | even | odd >

no parity

- none ― **パリティ無し**
- even ― **偶数パリティ**
- odd ― **奇数パリティ**

初期設定

パリティ無し

コマンドモード

Line Configuration

コマンド解説

接続するターミナルやモデムなどの機器によっては個々のパリティビットの設定を要求する場合があります。

例

本例では no parity **を設定しています。**

```
Console(config-line)#parity none
Console(config-line)#
```

speed

ターミナル接続のボーレートを指定するためのコマンドです。本設定では送受信両方の値を指定します。"no" **を前に置くことで初期設定に戻します。**

文法

speed *bps*

no speed

- *bps* ― **ボーレートを** bps **で指定（**9600bps **のみ選択可）**

初期設定

9600bps

コマンドモード

Line Configuration

コマンド解説

シリアルポートに接続された機器でサポートされているボーレートを指定してください。一部のボーレートは本機ではサポートしていない場合があります。サポートされていない値を指定した場合にはメッセージが表示されます。

例

```
Console(config-line)#speed 9600
Console(config-line)#
```

stopbits

送信するストップビットの値を指定します。"no" を前に置くことで初期設定に戻します。

文法

stopbits < 1 | 2 >

- 1 ― **ストップビット** "1"
- 2 ― **ストップビット** "2"

初期設定

ストップビット 1

コマンドモード

Line Configuration

例

本例ではストップビット "2" **に設定しています。**

```
Console(config-line)#stopbits 2
Console(config-line)#
```

disconnect

本コマンドを使用し SSH、Telnet、**コンソール接続を終了することができます。**

文法

disconnect *session-id*

- *session-id* ― SSH、Telnet、**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

コマンド解説

セッション ID"0" **を指定するとコンソール接続を終了させます。その他のセッション** ID **を指定した場合には** SSH **又は** Telnet **接続を終了させます。**

例

```
Console#disconnect 1
Console#
```

関連するコマンド

show ssh (P283)

show users (P309)

show line

ターミナル接続の設定を表示します。

文法

show line { console | vty }

- console ― **コンソール接続設定**
- vty ― **リモート接続用の仮想ターミナル設定**

初期設定

すべてを表示

コマンドモード

Normal Exec, Privileged Exec

例

本例ではすべての接続の設定を表示しています。

```
Console#show line
 Console Configuration:
  Password Threshold:  3 times
  Interactive Timeout: 600 sec
  Login Timeout: Disabled
  Silent Time:         Disabled
  Baudrate:            9600
  Databits:            8
  Parity:              None
  Stopbits:            1

 VTY Configuration:
  Password Threshold:  Disabled
  Interactive Timeout: 600 sec
  Login Timeout: 300 sec
Console#
```

4.5 General（一般コマンド）

コマンド	機能	モード	ページ
enable	Privileged モードの有効化	NE	P242
disable	Privileged モードから Normal モードへの変更	PE	P244
configure	Global Configuration モードの有効化	PE	P245
show history	コマンド履歴バッファの表示	NE,PE	P246
reload	本機の再起動	PE	P247
end	Privileged Exec モードへの変更	GC,IC, LC,VC	P247
exit	前の設定モードに戻る。 又は CLI セッションを終了	すべて	P248
quit	CLI セッションを終了	NE,PE	P248

enable

Privileged Exec モードを有効にする際に使用します。Privileged Exec モードでは他のコマンドを使用することができ、スイッチの情報を表示することができます。詳しくは P224 「コマンドモード」を参照して下さい。

文法

enable { *level* }

- *level* ― Privilege Level の設定

本機では 2 つの異なるモードが存在します。

0: Normal Exec、15: Privileged Exec

Privileged Exec モードにアクセスするためには level「15」を入力して下さい。

初期設定

Level 15

コマンドモード

Normal Exec

コマンド解説

- "super" が Normal Exec から Privileged Exec モードに変更するための初期設定パスワードになります（パスワードの設定・変更を行う場合は、P266 「enable password」を参照して下さい）
- プロンプトの最後に "#" が表示されている場合は、Privileged Exec モードを表します。

例

```
Console>enable
Password: [privileged level password]
Console#
```

関連するコマンド

disable (P244)

enable password (P266)

disable

Privileged Exec から Normal Exec に変更する際に使用します。

Normal Exec モードでは、本機の設定及び統計情報の基本的な情報の表示しか行えません。すべてのコマンドを使用するためには Privileged Exec モードにする必要があります。

詳細は P224 「コマンドモード」を参照して下さい。

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

プロンプトの最後に ">" が表示されている場合は Normal Exec モードを表します。

例

```
Console#disable
Console>
```

関連するコマンド

enable (P243)

configure

Global Configuration モードを有効にする場合に使用します。スイッチの設定を行うためには Global Configuration モードにする必要があります。さらに Interface Configuration, Line Configuration, VLAN Database Configuration などを行うためには、その先のモードにアクセスします。詳細は P224 「コマンドモード」を参照して下さい。

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#configure
Console(config)#
```

関連するコマンド

end (P247)

show history

保存されているコマンドの履歴を表示する際に利用します。

初期設定

なし

コマンドモード

Normal Exec, Privileged Exec

コマンド解説

本機に保存できるコマンド履歴は Execution コマンドと Configuration コマンドがそれぞれ最大 10 コマンドです。

例

本例では、コマンド履歴として保存されているコマンドを表示しています。

```
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#
```

"!" コマンドを用いると、履歴のコマンドを実行することが可能です。Normal 又は Privileged Exec モード時には Execution コマンドを、Configuration モード時には Configuration コマンドの実行が行えます。

本例では、"!2" コマンドを入力することで、Execution コマンド履歴内の 2 番目のコマンド（"config" コマンド）を実行しています。

```
Console#!2
Console#config
Console(config)#
```

reload

システムの再起動を行う際に利用します。

[注意]　再起動時には Power-On Self-test が実行されます。

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

システム全体の再起動を行います。

例

本機の再起動方法を示しています。

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

end

Privileged モードに戻る際に利用します。

初期設定

なし

コマンドモード

Global Configuration
Interface Configuration
Line Configuration
VLAN Database Configuration
Access Control List Configuration
Class Map Configuration
Policy Map Configuration
MSTP Configuration
Server Group Configuration

例

本例は、Interface Configuration から Privileged Exec モードへの変更を示しています。

```
Console(config-if)#end
Console#
```

exit

Privileged Exec モードに戻る場合や、CLI を終了する場合に使用します。

初期設定

なし

コマンドモード

すべて

例

Global Configuration モードから Privileged Exec モードへの変更と、CLI の終了を示しています。

```
Console(config)#exit
Console#exit

Press ENTER to start session
User Access Verification

Username:
```

quit

CLI を終了する際に利用します。

初期設定

なし

コマンドモード

Normal Exec

Privileged Exec

例

本例は、CLI セッションの終了を示しています。

```
Console#quit

Press ENTER to start session

User Access Verification

Username:
```

4.6 システム管理

このコマンドはシステムログ、ユーザ名、パスワード、Web インタフェースの設定に使用されます。また、他のシステム情報の表示や設定を行えます。

コマンド	機能	ページ
Device Designation	**本機を特定する情報設定**	P249
Banner	**管理上のコンタクト、デバイス識別、位置情報を設定**	P251
User Access	**管理アクセスユーザ名及びパスワード設定**	P264
IP Filter	**管理アクセスを許可する** IP **アドレスの設定**	P267
Web Server	Web **ブラウザ経由での管理アクセスの有効化**	P269
Telnet Server	Telnet **経由での管理アクセスの有効化**	P273
Secure Shell	**セキュリティを確保した** SSH **接続**	P275
Event Logging	**エラーメッセージログ設定**	P285
Time（System Clock）	NTP/SNTP **サーバによる自動時刻設定及び手動時刻設定**	P297
System Status	**管理者やシステムバージョン、システム情報の表示**	P304
Frame Size	**ジャンボフレームサポートの有効化**	P311

4.6.1 Device Designation コマンド

コマンド	機能	モード	ページ
prompt	PE/NE **モードで使用するプロンプトのカスタマイズ**	GC	P250
hostname	**ホスト名の設定**	GC	P250
snmp-server contact	**システムコンタクト者の設定**	GC	P388
snmp-server location	**システムロケーションの設定**	GC	P388

prompt

CLI プロンプトのカスタマイズを行なうことができます。"no" を前に置くことで初期設定に戻ります。

文法

prompt *string*

no prompt

- *string* — CLI プロンプトに表示される名称（最大 255 文字）

初期設定

Console

コマンドモード

Global Configuration

例

```
Console(config)#prompt RD2
RD2(config)#
```

hostname

本機のホスト名の設定及び変更を行うことができます。"no" を前に置くことで設定を削除します。

文法

hostname *name*

no hostname

- *name* — ホスト名（最大 255 文字）

初期設定

なし

コマンドモード

Global Configuration

例

```
Console(config)#hostname RD#1
Console(config)#
```

4.6.2 Banner

スイッチのアドミニストレーション情報の設定を行います。

以下のコマンドにより、データセンターの所在地、電気・ネットワーク回線の詳細、管理者およびコンタクト情報を設定することができます。

これからの情報は、CLI **経由での接続時にのみ利用可能で、コンソールまたは** Telnet **の接続が確立した後すぐに、自動的に表示されます。**

コマンド	機能	モード	ページ
banner configure	**ログイン前に表示されるバナー情報の設定**	GC	P252
banner configure company	**会社情報の設定**	GC	P253
banner configure dc-power-info	DC **電力情報の設定**	GC	P254
banner configure department	**部門情報の設定**	GC	P255
banner configure equipment-info	**装置情報の設定**	GC	P256
banner configure equipment-location	**装置設置場所情報の設定**	GC	P257
banner configure ip-lan	IP/LAN **情報の設定**	GC	P258
banner configure lp-number	LP **番号情報の設定**	GC	P259
banner configure manager-info	**マネージャコンタクト情報の設定**	GC	P260
banner configure mux	MUX **情報の設定**	GC	P261
banner configure note	**その他情報の設定**	GC	P262
show banner	**全てのバナー情報の表示**	NE, PE	P263

banner configure

本コマンドにより、インタラクティブに管理情報を指定することができます。

文法

banner configure

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

入力するデータに、スペースは使用できません。

例

```
Console(config)#banner configure

Company: Acme Corporation
Responsible department: R&D Dept
Name and telephone to Contact the management people
Manager1 name: Sr. Network Admin
phone number: 123-555-1212
Manager2 name: Wile E. Coyote
phone number: 123-555-1213
Manager3 name: Night-shift Net Admin / Janitor
phone number: 123-555-1214
The physical location of the equipment.
City and street address: 12 Straight St. Motown, Zimbabwe
Information about this equipment:
Manufacturer: Acme Corporation
ID: 123_unique_id_number
Floor: 2
Row: 7
Rack: 29
Shelf in this rack: 8
Information about DC power supply.
Floor: 2
Row: 7
Rack: 25
Electrical circuit: : ec-177743209-xb
Number of LP:12
Position of the equipment in the MUX:1/23
IP LAN:192.168.1.1
Note: This is a random note about this managed switch and can contain
miscellaneous information.
Console(config)#
```

banner configure company

バナーに表示される、会社情報の設定を行うことができます。"no" を前に置くことで設定した情報を削除します。

文法

banner configure company *name*

no banner configure company

- *name* — 会社名（最大 32 文字）

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

入力するデータに、スペースは使用できません。

例

```
Console(config)#banner configure company Acme_Corporation
Console(config)#
```

banner configure dc-power-info

バナーに表示される、DC 電力情報の設定を行うことができます。"no" を前に置くことで設定した情報を削除します。

文法

banner configure dc-power-info floor *floor-id* **row** *row-id* **rack** *rack-id* **electrical-circuit** *ec-id*

no banner configure dc-power-info { floor | row | rack | electrical-circuit }

- *floor-id* — フロア番号（最大 32 文字）
- *row-id* — ロー番号（最大 32 文字）
- *rack-id* — ラック番号（最大 32 文字）
- *ec-id* — 電気回線 ID（最大 32 文字）

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

入力するデータに、スペースは使用できません。

例

```
Console(config)#banner configure floor 3 row 15 rack 24
 electrical-circuit 48v-id_3.15.24.2
Console(config)#
```

banner configure department

バナーに表示される、部門情報の設定を行うことができます。"no" を前に置くことで設定した情報を削除します。

文法

banner configure department *dept-name*

no banner configure company

- *dept-name* ― 部署名（最大 32 文字）

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

入力するデータに、スペースは使用できません。

例

```
Console(config)#banner configure department R&D
Console(config)#
```

banner configure equipment-info

バナーに表示される、機器情報の設定を行うことができます。"no" **を前に置くことで設定した情報を削除します。**

文法

banner configure equipment-info manufacturer-id *mfr-id* **floor** *floor-id* **row** *row-id* **rack** *rack-id* **shelf-rack** *sr-id* **manufacturer** *mfr-name*

no banner configure equipment-info { floor | manufacturer |

manufacturer-id | rack | row | shelf-rack}

- *mfr-id* ― **デバイスモデル番号（最大** 32 **文字）**
- *floor-id* ― **フロア番号（最大** 32 **文字）**
- *row-id* ― **ロー番号（最大** 32 **文字）**
- *rack-id* ― **ラック番号（最大** 32 **文字）**
- *sr-id* ― **ラック棚番号（最大** 32 **文字）**
- *mfr-name* ― **装置製造元名（最大** 32 **文字）**

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

入力するデータに、スペースは使用できません。

例

```
Console(config)#banner configure equipment-info manufacturer-id switch35
 floor 3 row 10 rack 15 shelf-rack 12 manufacturer Acme_Corporation
Console(config)#
```

banner configure equipment-location

バナーに表示される、デバイス所在地情報の設定を行うことができます。"no" **を前に置くことで設定した情報を削除します。**

文法

banner configure equipment-location *location*

no banner configure equipment-location

- *location* ― **デバイスの所在地（最大** 32 **文字）**

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

入力するデータに、スペースは使用できません。

例

```
Console(config)#banner configure equipment-location
 710_Network_Path,_Indianapolis
Console(config)#
```

banner configure ip-lan

バナーに表示される、デバイス IP アドレスおよびサブネットマスクの設定を行うことができます。"no" を前に置くことで設定した情報を削除します。

文法

banner configure ip-lan *ip-mask*

no banner configure ip-lan

- *ip-mask* — デバイスの IP アドレスおよびサブネットマスク（最大 32 文字）

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

入力するデータに、スペースは使用できません。

例

```
Console(config)#banner configure ip-lan 192.168.1.1/255.255.255.0
Console(config)#
```

banner configure lp-number

バナーに表示される、LP 番号情報の設定を行うことができます。"no" を前に置くことで設定した情報を削除します。

文法

banner configure lp-number *lp-num*

no banner configure lp-number

- *lp-num* ― LP **番号（最大** 32 **文字）**

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

入力するデータに、スペースは使用できません。

例

```
Console(config)#banner configure lp-number 12
Console(config)#
```

banner configure manager-info

バナーに表示される、マネージャコンタクト情報の設定を行うことができます。"no" **を前に置くことで設定した情報を削除します。**

文法

banner configure manager-info name *mgr1-name* **phone-number** *mgr1-number* **{ name2** *mgr2-name* **phone-number** *mgr2-number* **| name3** *mgr3-name* **phone-number** *mgr3-number* **}**

no banner configure manager-info { name1 | name2 | name3 }

- *mgr1-name* ― **マネージャ** 1 **の名前（最大** 32 **文字）**
- *mgr1-number* ― **マネージャ** 1 **の電話番号（最大** 32 **文字）**
- *mgr2-name* ― **マネージャ** 2 **の名前（最大** 32 **文字）**
- *mgr2-number* ― **マネージャ** 2 **の電話番号（最大** 32 **文字）**
- *mgr3-name* ― **マネージャ** 3 **の名前（最大** 32 **文字）**
- *mgr3-number* ― **マネージャ** 3 **の電話番号（最大** 32 **文字）**

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

入力するデータに、スペースは使用できません。

例

```
Console(config)#banner configure manager-info name Albert_Einstein
 phone-number 123-555-1212 name2 Lamar phone-number 123-555-1219
Console(config)#
```

banner configure mux

バナーに表示される、MUX 情報の設定を行うことができます。"no" を前に置くことで設定した情報を削除します。

文法

banner configure mux *muxinfo*
no banner configure mux

- *muxinfo* — **スイッチが接続されている、回線および** PVC **情報（最大** 32 **文字）**

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

入力するデータに、スペースは使用できません。

例

```
Console(config)#banner configure mux telco-8734212kx_PVC-1/23
Console(config)#
```

banner configure note

バナーに表示される、メモ情報の設定を行うことができます。"no" を前に置くことで設定した情報を削除します。

文法

banner configure note *note-info*

no banner configure note

- *note-info* — 他のバナーカテゴリに適していないその他の情報。（最大 150 文字）

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

入力するデータに、スペースは使用できません。

例

```
Console(config)#banner configure note !!!ROUTINE_MAINTENANCE_firmware
  upgrade_0100-0500_GMT-0500_20071022!!!!!_20min_network_impact_expected
Console(config)#
```

show banner

全てのバナー情報を表示します。

文法

show banner

初期設定

なし

コマンドモード

Normal Exec, Privileged Exec

例

```
Console#show banner
Acme_Corporation
WARNING - MONITORED ACTIONS AND ACCESSES
R&D_Dept

Albert_Einstein - 123-555-1212
Wile_E._Coyote - 123-555-9876
Lamar - 123-555-3322

Station's information:
710_Network_Path,Indianapolis

Acme_Corporation - switch35
Floor / Row / Rack / Sub-Rack
7 / 10 / 15 / 6
DC power supply:
Power Source A: Floor / Row / Rack / Electrical circuit
3 / 15 / 24 / 48V-id_3.15.24.2

Number of LP: 4
Position MUX: telco-9734212kx_PVC-1/23
IP LAN: 216.241.132.3/255.255.255.0
Note:
!!!!!ROUTINE_MAINTENANCE_firmware-upgrade_0100--0500_GMT-
0500_20071022!!!
!!_20min_network_impact_expected
Console#
```

4.6.3 ユーザーアクセスコマンド

管理アクセスのための基本的なコマンドです。管理アクセスに関するその他の設定に関しては、P232 **「**password**」や** P321 **「認証コマンド」、**P347 **「**802.1x **ポート認証コマンド」があります。**

コマンド	機能	モード	ページ
username	**ログインするためのユーザ名の設定**	GC	P265
enable password	**各アクセスレベルのパスワードの設定**	GC	P266

username

ログインする際のユーザ名及びパスワードの設定を行います。"no" **を前に置くことでユーザ名を削除します。**

文法

username *name* **[access-level** *level* **| nopassword | password** <0 | 7> *password*]

no username *name*

- *name* — **ユーザ名（最大** 8 **文字。大文字と小文字は区別されます）。最大ユーザ数** : 16 **ユーザ**
- **access-level** *level* — **ユーザレベルの設定**
  本機には 2 **種類のアクセスレベルがあります：**0: Normal Exec**、**15: Privileged Exec
- **nopassword** — **ログインパスワードが必要ない場合**
- <0 | 7> — "0" **は平文パスワードを、**"7" **は暗号化されたパスワードとなります。**
- **password** *password* — **ユーザ用のパスワード（最大** 32 **文字。大文字と小文字は区別されます）**

初期設定

- **初期設定のアクセスレベルは** Normal Exec **レベルです。**
- **初期設定のユーザ名とパスワードは以下の通りです。**

ユーザ名	アクセスレベル	パスワード
guest admin	0 15	guest admin

コマンドモード

Global Configuration

コマンド解説

暗号化されたパスワードはシステム起動時に設定ファイルを読み込む場合や TFTP **サーバにダウロードする場合のためにテキスト（平文）パスワードとの互換性があります。暗号化されたパスワードを手動で生成する必要はありません。**

例

本例は、ユーザへのアクセスレベルとパスワードの設定を示しています。

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

enable password

Normal Exec レベルから Privileged Exec レベルに移行する際に使用します。"no" を前に置くことで初期設定に戻ります。

安全のためパスワードは初期設定から変更してください。変更したパスワードは忘れないようにして下さい。

文法

enable password [**level** *level* **|** 0 | 7] *password*

no enable password [level *level***]**

- level *level* — Privileged Exec へは Level 15 を入力します。
  （Level0-14 は使用しません）
- 0 | 7 — "0" は平文パスワードを、"7" は暗号化されたパスワードとなります。
- *password* — privileged Exec レベルへのパスワード
  （最大 8 文字、大文字小文字は区別されます）

初期設定

初期設定レベル 15

初期設定パスワード "super"

コマンドモード

Global Configuration

コマンド解説

- パスワードを空欄にすることはできません。P243 「enable」コマンドを使用し Normal Exec から Privileged Exec へのコマンドモードの変更パスワードを入力して下さい。
- 暗号化されたパスワードはシステム起動時に設定ファイルを読み込む場合や TFTP サーバにダウンロードする場合のためにテキスト（平文）パスワードとの互換性があります。暗号化されたパスワードを手動で生成する必要はありません。

例

```
Console(config)#enable password level 15 0 admin
Console(config)#
```

関連するコマンド

enable (P243)

authentication enabled (P322)

4.6.4 IP フィルターコマンド

コマンド	機能	モード	ページ
management	管理アクセスを許可する IP アドレスを設定	GC	P267
show management	本機の管理アクセスに接続されているクライアントの表示	PE	P268

management

本機では管理アクセスに接続を許可するクライアントの IP アドレスの設定を行なうことができます。"no" を前に置くことで設定を削除します。

文法

management [all-client | http-client | snmp-client | telnet-client] *start-address* { *end-address* }

no management [all-client | http-client | snmp-client | telnet-client] *start-address* { *end-address* }

- **all-client** — SNMP/Web ブラウザ /Telnet クライアントの IP アドレス
- **http-client** — Web ブラウザクライアントの IP アドレス
- **snmp-client** — SNMP クライアントの IP アドレス .
- **telnet-client** — Telnet クライアントの IP アドレス
- *start-address* — IP アドレス又は IP アドレスグループの最初の IP アドレス
- *end-address* — IP アドレスグループの最後の IP アドレス

初期設定

全アドレス

コマンドモード

Global Configuration

コマンド解説

- 設定以外の無効な IP アドレスから管理アクセスに接続された場合、本機は接続を拒否し、イベントメッセージをシステムログに保存し、トラップメッセージの送信を行ないます。
- SNMP、Web ブラウザ、Telnet アクセスへの IP アドレス又は IP アドレス範囲の設定は合計で最大 5 つまで設定可能です。
- SNMP、Web ブラウザ、Telnet の同一グループに対して IP アドレス範囲を重複して設定することはできません。異なるグループの場合には IP アドレス範囲を重複して設定することは可能です。
- 設定した IP アドレス範囲から特定の IP アドレスのみを削除することはできません。IP アドレス範囲をすべて削除し、その後設定をし直して下さい。
- IP アドレス範囲の削除は IP アドレス範囲の最初のアドレスだけを入力しても削除することができます。また、最初のアドレスと最後のアドレスの両方を入力して削除することも可能です。

例

```
Console(config)#management all-client 192.168.1.19
Console(config)#management all-client 192.168.1.25 192.168.1.30
Console#
```

show management

管理アクセスへの接続が許可されている IP **アドレスを表示します。**

文法

show management < all-client | http-client | snmp-client |telnet-client >

- **all-client** ― SNMP/Web **ブラウザ** /Telnet **クライアントの** IP **アドレス**
- **http-client** ― Web **ブラウザクライアントの** IP **アドレス**
- **snmp-client** ― SNMP **クライアントの** IP **アドレス** .
- **telnet-client** ― Telnet **クライアントの** IP **アドレス**

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#
```

4.6.5 Web サーバーコマンド

コマンド	機能	モード	ページ
ip http port	Web インタフェースに使用するポートの設定	GC	P269
ip http server	管理用 Web インタフェースの使用	GC	P270
ip http secure-server	セキュア HTTP（HTTPS）サーバの使用	GC	P271
ip http secure-port	HTTPS 接続に使用するポートの設定	GC	P272

ip http port

Web インタフェースでアクセスする場合の TCP ポート番号を指定します。"no" を前に置くことで初期設定に戻ります。

文法

ip http port *port-number*

no ip http port

- *port-number* — Web インタフェースに使用する TCP ポート (1-65535)

初期設定

80

コマンドモード

Global Configuration

例

```
Console(config)#ip http port 769
Console(config)#
```

関連するコマンド

ip http server (P270)

ip http server

Web ブラウザから本機の設定、及び設定情報の閲覧を可能にします。

"no" を前に置くことで本機能は無効となります。

文法

ip http server

no ip http server

初期設定

有効

コマンドモード

Global Configuration

例

```
Console(config)#ip http server
Console(config)#
```

関連するコマンド

ip http port (P269)

ip http secure-server

Web インタフェースを使用し本機への暗号化された安全な接続を行うために、Secure Socket Layer (SSL) を使用した Secure hypertext transfer protocol (HTTPS) を使用するためのコマンドです。"no" を前に置くことで本機能を無効にします。

文法

ip http secure-server

no ip http secure-server

初期設定

有効

コマンドモード

Global Configuration

コマンド解説

- HTTP 及び HTTPS サービスはそれぞれのサービスを個別に有効にすることが可能です。
- HTTPS を有効にした場合は Web ブラウザのアドレスバーに https://device[: ポート番号] と入力します。
- HTTPS を有効にした場合、以下の手順で接続が確立されます：
  - ―クライアントはサーバのデジタル証明書を使用し、サーバを確証します。
  - ―クライアントおよびサーバは、接続のために使用する 1 セットのセキュリティ・プロトコルを協定します。
  - ―クライアントおよびサーバは、データを暗号化し解読するためのセッション・キーを生成します。
- クライアントとサーバ間の暗号化されたアクセスが確立した場合、Internet Explorer 5.x 及び Netscape Navigator 4.x のステータスバーに鍵マークが表示されます。
- 以下の Web ブラウザ、OS 環境で HTTPS をサポートしています。

Web ブラウザ	OS
Internet Explorer 5.0 以上	Windows 98、Windows NT（サービスパック 6a）、Windows 2000、Windows XP
Netscape Navigator 4.7 以上	Windows 98、Windows NT （サービスパック 6a）、Windows 2000、Windows XP、Solaris 2.6

※セキュアサイト証明の詳細は P68 「サイト証明書の設定変更」を参照して下さい。

例

```
Console(config)#ip http secure-server
Console(config)#
```

関連するコマンド

ip http secure-port (P272)

copy tftp https-certificate (P312)

ip http secure-port

Web インタフェースからの HTTPS/SSL 接続で使用する UDP ポートを設定することができます。"no" を前に置くことで初期設定に戻ります。

文法

ip http secure-port *port_number*

no ip http secure-port

- *port_number* ― HTTPS/SSL に使用する UDP ポート番号 (1-65535)

初期設定

443

コマンドモード

Global Configuration

コマンド解説

- HTTP と HTTPS で同じポートは設定できません。
- HTTPS ポート番号を設定した場合、HTTPS サーバにアクセスするためには URL にポート番号を指定する必要があります。(https://device:[ポート番号])

例

```
Console(config)#ip http secure-port 1000
Console(config)#
```

関連するコマンド

ip http secure-server (P271)

copy tftp https-certificate (P312)

4.6.6 Telnet サーバーコマンド

コマンド	機能	モード	ページ
ip telnet port	Telnet インタフェースに使用するポートの設定	GC	P273
ip telnet server	管理用 Telnet インタフェースの使用	GC	P274

ip telnet port

Telnet インタフェースでアクセスする場合の TCP ポート番号を指定します。"no" を前に置くことで初期設定に戻ります。

文法

ip telnet port *port-number*

no ip telnet port

- *port-number* — Telnet インタフェースに使用する TCP ポート (範囲：1-65535)

初期設定

23

コマンドモード

Global Configuration

例

```
Console(config)#ip telnet port 123
Console(config)#
```

関連するコマンド

ip telnet server (P274)

ip telnet server

Telnet から本機の設定、及び設定情報の閲覧を可能にします。

"no" を前に置くことで本機能は無効となります。

文法

ip http server

no ip http server

初期設定

有効

コマンドモード

Global Configuration

例

```
Console(config)#ip telnet server
Console(config)#
```

関連するコマンド

ip telnet port (P273)

4.6.7 Secure Shell コマンド

Secure Shell (SSH) は、それ以前からあったバークレーリモートアクセスツールのセキュリティ面を確保した代替としてサーバ / クライアントアプリケーションを含んでいます。また、SSH は Telnet に代わる本機へのセキュア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 プロトコルによって本機と接続する場合、本機はアクセス認証のためにローカルのユーザ名およびパスワードと共にクライアントが使用する公開暗号キーを生成します。さらに、SSH では本機と SSH を利用する管理端末の間の通信をすべて暗号化し、ネットワーク上のデータの保護を行ないます。

ここでは、SSH サーバを設定するためのコマンドを解説します。

なお、SSH 経由での管理アクセスを行なうためには、クライアントに 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]　本機では SSH Version1.5 と 2.0 をサポートしています。

コマンド	機能	モード	ページ
ip ssh server	SSH サーバの使用	GC	P277
ip ssh timeout	SSH サーバの認証タイムアウト設定	GC	P278
ip ssh authentication -retries	クライアントに許可するリトライ数の設定	GC	P279
ip ssh server-key size	SSH サーバキーサイズの設定	GC	P279
copy tftp public-key	ユーザ公開キーの TFTP サーバから本機へコピー	PE	P312
delete public-key	特定ユーザの公開キーの削除	PE	P280
ip ssh crypto host-key generate	ホストキーの生成	PE	P281
ip ssh crypto zeroize	RAM からのホストキーの削除	PE	P282
ip ssh save host-key	RAM からフラッシュメモリへのホストキーの保存	PE	P282
disconnect	ライン接続の終了	PE	P240
show ip ssh	SSH サーバの状態の表示及び SSH 認証タイムアウト時間とリトライ回数の設定	PE	P283
show ssh	SSH セッション状態の表示	PE	P283
show public-key	特定のユーザ又はホストの公開キーの表示	PE	P284
show users	SSH ユーザ、アクセスレベル、公開キータイプの表示	PE	P309

本機の SSH サーバはパスワード及びパブリックキー認証をサポートしています。SSH クライアントによりパスワード認証を選択した場合、認証設定ページで設定したパスワードにより本機内、RADIUS、TACACS+ のいずれかの認証方式を用います。クライアントがパブリックキー認証を選択した場合には、クライアント及び本機に対して認証キーの設定を行なう必要があります。公開暗号キー又はパスワード認証のどちらかを使用するに関わらず、本機上の認証キー（SSH ホストキー）を生成し、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で設定を行ないます。

(1) **ホストキーペアの生成** — "ip ssh crypto host-key generate" **コマンドによりホスト パブリック / プライベートキーのペアを生成します。**

(2) **ホスト公開キーのクライアントへの提供** — **多くの** SSH **クライアントは、本機との自動的に初期接続設定中に自動的にホストキーを受け取ります。そうでない場合には、手動で管理端末のホストファイルを作成し、ホスト公開キーを置く必要があります。ホストファイル中の公開暗号キーは以下の例のように表示されます。**

10.1.0.54 1024 35
156849954018676692593339467750546173253136748908365472541502024559319986854435836165199992332978176606583095610825913212890233765468017262725714134287629413011961955667825956641048695742788814620651941746772984865468615717739390164779355942303577413098022737087794545240839717526463580581767167095748047761170

(3) **クライアント公開キーの本機への取り込み** — P313 **「**copy**」コマンドを使用し、**SSH **クライアントの本機の管理アクセスに提供される公開キーを含むファイルをコピーします。クライアントへはこれらのキーを使用し、認証が行なわれます。現在のファームウェアでは以下のような** UNIX **標準フォーマットのファイルのみ受け入れることが可能です。**

1024 35
134108168560989392104094492015542534763164192187295892114317388005553616163105177594083868631109291232226828519254374603100937187721199696317813662774141689851320491172048303392543241016379975923714490119380060902539484084827178194372288402533115952134861022902978982721353267131629432532818915045306393916643 steve@192.168.1.19

(4) **オプションパラメータの設定** — SSH **設定ページで、認証タイムアウト、リトライ回数、サーバキーサイズなどの設定を行なってください。**

(5) **SSH の有効化** — "ip ssh server" **コマンドを使用し、本機の** SSH **サーバを有効にして下さい。**

(6) **Challenge/Response 認証** — SSH **クライアントが本機と接続しようとした場合、**SSH **サーバはセッションキーと暗号化方式を調整するためにホストキーペアを使用します。本機上に保存された公開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アクセスすることができます。**

以下のような手順で認証プロセスが行なわれます。

a. **クライアントが公開キーを本機に送ります。**

b. **本機はクライアントの公開キーとメモリに保存されている情報を比較します。**

c. **一致した場合、公開キーを利用し本機はバイトの任意のシーケンスを暗号化し、その値をクライアントに送信します。**

d. **クライアントはプライベートキーを使用してバイトを解読し、解読したバイトを本機に送信します。**

e. **本機は、元のバイトと解読されたバイトを比較します。**2 **つのバイトが一致した場合、クライアントのプライベートキーが許可された公開キーに対応していることを意味し、クライアントが認証されます。**

[注意] パスワード認証と共に SSH を使用する場合にも、ホスト公開キーは初期接続時又は手動によりクライアントのホストファイルに与えられます。但し、クライアントキーの設定を行なう必要はありません。

ip ssh server

SSH サーバの使用を有効にします。"no" を前に置くことで設定を無効にします。

文法

ip ssh server

no ip ssh server

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

- 最大 4 セッションの同時接続をサポートします。最大セッション数は Telnet 及び SSH の合計数です。
- SSH サーバはクライアントとの接続を確立する際に DAS 又は RAS を使ったキー交換を行います。その後、DES (56-bit) または 3DES (168-bit) を用いてデータの暗号化を行います。
- SSH サーバを有効にする前に、ホストキーを生成する必要があります。

例

```
Console#ip ssh crypto host-key generate dsa
Console#ip ssh crypto host-key generate rsa
Console#configure
Console(config)#ip ssh server
Console(config)#
```

関連するコマンド

ip ssh crypto host-key generate (P281)

show ssh (P283)

ip ssh timeout

SSH サーバのタイムアウト時間を設定します。"no" を前に置くことで初期設定に戻ります。

文法

ip ssh timeout *seconds*

no ip ssh timeout

- *seconds* — SSH 接続調整時のクライアント応答のタイムアウト時間（設定範囲：1-120）

初期設定

120 秒

コマンドモード

Global Configuration

コマンド解説

タイムアウトは SSH 情報交換時のクライアントからの応答を本機が待つ時間の指定を行ないます。SSH セッションが確立した後のユーザ入力のタイムアウトは vty セッションへの "exec-timeout" コマンドを使用します。

例

```
Console(config)#ip ssh timeout 60
Console(config)#
```

関連するコマンド

exec-timeout (P234)

show ip ssh (P283)

ip ssh authentication-retries

SSH サーバがユーザの再認証を行なう回数を設定します。"no" を前に置くことで初期設定に戻ります。

文法

ip ssh authentication-retries *count*

no ip ssh authentication-retries

- *count* ― インタフェースがリセット後、認証を行なうことができる回数（設定範囲：1-5）

初期設定

3

コマンドモード

Global Configuration

例

```
Console(config)#ip ssh authentication-retries 2
Console(config)#
```

関連するコマンド

show ip ssh (P283)

ip ssh server-key size

SSH サーバキーサイズを設定します。"no" を前に置くことで初期設定に戻ります。

文法

ip ssh server-key size *key-size*

no ip ssh server-key size

- *key-size* ― サーバキーのサイズ（設定範囲：512-896bits）

初期設定

768 bits

コマンドモード

Global Configuration

コマンド解説

- サーバキーはプライベートキーとなり本機以外との共有はしません。
- SSH クライアントと共有するホストキーサイズは 1024bit に固定されています。

例

```
Console(config)#ip ssh server-key size 512
Console(config)#
```

delete public-key

特定のユーザパブリックキーを削除します。

文法

delete public-key *username* { dsa | rsa }

- *username* ― SSH **サーバ名（設定範囲：**1-8 **文字）**
- dsa ― DSA **公開キータイプ**
- rsa ― RSA **公開キータイプ**

初期設定

DSA **及び** RSA **キーの両方の削除**

コマンドモード

Privileged Exec

例

```
Console#delete public-key admin dsa
Console#
```

ip ssh crypto host-key generate

パブリック及びプライベートのホストキーペアの生成を行ないます。

文法

ip ssh crypto host-key generate < dsa | rsa >

- dsa ― DSA（Version2）キータイプ
- rsa ― RSA（Version1）キータイプ

初期設定

DSA 及び RSA キーペア両方の生成

コマンドモード

Privileged Exec

コマンド解説

- 本コマンドはホストキーペアをメモリ (RAM) に保存します。" ip ssh save host-key" コマンドを使用してホストキーペアをフラッシュメモリに保存できます。
- 多くの SSH クライアントは接続設定時に自動的にパブリックキーをホストファイルとして保存します。そうでない場合には、手動で管理端末のホストファイルを作成し、ホスト公開キーを置く必要があります。
- SSH サーバは、接続しようとするクライアントとセッションキー及び暗号化方法を取り決めるためにホストキーを使用します。

例

```
Console#ip ssh crypto host-key generate dsa
Console#
```

関連するコマンド

ip ssh crypto zeroize (P282)

ip ssh save host-key (P282)

ip ssh crypto zeroize

ホストキーをメモリ (RAM) **から削除します。**

文法

ip ssh crypto zeroize < dsa | rsa >

- dsa ― DSA **キータイプ**
- rsa ― RSA **キータイプ**

初期設定

DSA **及び** RSA **キーの両方を削除**

コマンドモード

Privileged Exec

コマンド解説

- RAM **からホストキーを削除します。**" no ip ssh save host-key" **コマンドを使用することでフラッシュメモリからホストキーを削除できます。**
- **本コマンドを使用する際は事前に** SSH **サーバを無効にして下さい。**

例

```
Console#ip ssh crypto zeroize dsa
Console#
```

ip ssh save host-key

ホストキーを RAM **からフラッシュメモリに保存します。**

文法

ip ssh save host-key

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#ip ssh save host-key
Console#
```

関連するコマンド

ip ssh crypto host-key generate (P281)

show ip ssh

このコマンドを使用することで SSH サーバの設定状況を閲覧することができます。

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 サーバへの接続状況を表示します。

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#
```

項目	解説
Session	セッション番号 (0-3)
Version	SSH バージョン番号
State	認証接続状態（値：Negotiation-Started, Authentication-Started,Session-Started）
Username	クライアントのユーザ名
Encryption	暗号化方式はクライアントとサーバの間で自動的に情報交換を行ない設定します。 SSH v1.5 の選択肢：DES, 3DES SSH v2.0 の選択肢は client-to-server (ctos) 及び server-to-client (stoc) の 2 種類の方式をサポートします： aes128-cbc-hmac-sha1、aes192-cbc-hmac-sha1 aes256-cbc-hmac-sha1、3des-cbc-hmac-sha1 blowfish-cbc-hmac-sha1、aes128-cbc-hmac-md5 aes192-cbc-hmac-md5、aes256-cbc-hmac-md5 3des-cbc-hmac-md5、blowfish-cbc-hmac-md5 用語集： DES ― Data Encryption Standard (56-bit key) 3DES ― Triple-DES (Uses three iterations of DES, 112-bit key) aes ― Advanced Encryption Standard (160 or 224-bit key) blowfish ― Blowfish (32-448 bit key) cbc ― cypher-block chaining sha1 ― Secure Hash Algorithm 1 (160-bit hashes) md5 ― Message Digest algorithm number 5 (128-bit hashes)

show public-key

特定のユーザ又はホストの公開キーを表示します。

文法

show public-key { user { *username* } **|** host **}**

- *username* — SSH ユーザ名（範囲：1-32 文字）

初期設定

すべての公開キーの表示

コマンドモード

Privileged Exec

コマンド解説

- パラメータを設定しない場合には、すべてのキーが表示されます。キーワードを入力し、ユーザ名を指定しない場合、すべてのユーザの公開キーが表示されます。
- RSA キーが表示された場合、最初のフィールドはホストキーサイズ (1024) となり、次のフィールドはエンコードされた公開指数 (35)、その後の値がエンコードされたモジュールとなります。DSA キーが表示された場合、最初のフィールドは SSH で使用される暗号化方式の DSS となり、その後の値がエンコードされたモジュールとなります。

例

```
Console#show public-key host
Host:
RSA:
1024 35
156849954018676692593339467750546173253136748908365472541502024559319
986854435836165199992332978176606583095861082591321289023376546801726
272571413428762941301196195566782595664104869574278881462065194174677
298486546861571773939016477935594230357741309802273708779454524083971
752646358058176716709574804776117
DSA:
ssh-dss AAAB3NzaC1kc3MAAACBAPWKZTPbsRIB8ydEXcxM3dyV/yrDbKStIlnzD/
Dg0h2HxcYV44sXZ2JXhamLK6P8bvuiyacWbUW/
a4PAtp1KMSdqsKeh3hKoA3vRRSy1N2XFfAKxl5fwFfvJlPdOkFgzLGMinvSNYQwiQXbKT
BH0Z4mUZpE85PWxDZMaCNBPjBrRAAAAFQChb4vsdfQGNIjwbvwrNLaQ77isiwAAAIEAsy
5YWDC99ebYHNRj5kh47wY4i8cZvH+/
p9cnrfwFTMU01VFDly3IR2G395NLy5Qd7ZDxfA9mCOfT/
yyEfbobMJZi8oGCstSNOxrZZVnMqWrTYfdrKX7YKBw/
Kjw6BmiFq7O+jAhf1Dg45loAc27s6TLdtny1wRq/
ow2eTCD5nekAAACBAJ8rMccXTxHLFAczWS7EjOyDbsloBfPuSAb4oAsyjKXKVYNLQkTLZ
fcFRu41bS2KV5LAwecsigF/+DjKGWtPNIQqabKgYCw2 o/
dVzX4Gg+yqdTlYmGA7fHGm8ARGeiG4ssFKy4Z6DmYPXFum1Yg0fhLwuHpOSKdxT3kk475
S7 w0W
Console#
```

4.6.8 Event Logging コマンド

コマンド	機能	モード	ページ
logging on	エラーメッセージログの設定	GC	P285
logging history	重要度に基づいた SNMP 管理端末に送信する syslog の設定	GC	P286
logging host	syslog を送信するホストの IP アドレスの設定	GC	P287
logging facility	リモートで syslog を保存する際のファシリティタイプの競って尾	GC	P287
logging trap	リモートサーバへの重要度にもとづいてた syslog メッセージの保存	GC	P288
clear log	ログバッファのクリア	PE	P288
show logging	ログ関連情報の表示	PE	P290
show log	ログメッセージの表示	PE	P292

logging on

エラーメッセージのログを取るためのコマンドです。デバッグ又はエラーメッセージをログとして保存します。"no" を前に置くことで設定を無効にします。

文法

logging on

no logging on

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

ログとして保存されるエラーメッセージは本体のメモリ又はリモートの syslog サーバに保存されます。"logging history" コマンドを使用してメモリに保存するログの種類を選択することができます。

例

```
Console(config)#logging on
Console(config)#
```

関連するコマンド

logging history (P286)

clear logging (P288)

logging history

本体のメモリに保存するメッセージの種類を指定することができます。"no" **を前に置くことで初期設定に戻します。**

文法

logging history < flash | ram > *level*

no logging history < flash | ram >

- flash ― **フラッシュメモリに保存されたイベント履歴**
- ram ― RAM **に保存されたイベント履歴**
- *level* ― **レベルは以下の表の通りです。選択した** Level **から** Level0 **までのメッセージが保存されます（選択した** Level **は含まれます）**

レベル引数	**レベル**	**解説**	syslog **定義**
debugging	7	**デバッグメッセージ**	LOG_DEBUG
Informational	6	**情報メッセージ**	LOG_INFO
notifications	5	**重要なメッセージ**	LOG_NOTICE
warnings	4	**警告メッセージ**	LOG_WARNING
Errors	3	**エラー状態を示すメッセージ**	LOG_ERR
Critical	2	**重大な状態を示すエラーメッセージ**	LOG_CRIT
alerts	1	**迅速な対応が必要なメッセージ**	LOG_ALERT
emergencies	0	**システム不安定状態を示すメッセージ**	LOG_EMERG

初期設定

Flash: errors (level 3 - 0)

RAM: debugging (level 7 - 0)

コマンドモード

Global Configuration

コマンド解説

フラッシュメモリには、RAM **に設定する** Level **より高い** Level **を設定して下さい。**

例

```
Console(config)#logging history ram 0
Console(config)#
```

logging host

ログメッセージを受け取る syslog **サーバの** IP **アドレスを設定します。**"no" **を前に置くことで** syslog **サーバを削除します。**

文法

logging host *host_ip_address*

no logging host *host_ip_address*

- *host_ip_address* ― syslog **サーバの** IP **アドレス**

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- **異なる** IP **アドレスのホストを指定したコマンドを入力し、最大** 5 **つの** syslog **サーバを設定できます。**

例

```
Console(config)#logging host 10.1.0.3
Console(config)#
```

logging facility

syslog **メッセージを送る際の** facility **タイプを設定します。**"no" **を前に置くことで初期設定に戻します。**

文法

logging facility *type*

no logging facility

type ― syslog **サーバで使用する** facility **タイプの値を指定します。**(16-23)

初期設定

23

コマンドモード

Global Configuration

コマンド解説

syslog **メッセージとして送信するファシリティタイプタグの設定を行ないます** (**詳細：**RFC3164)**。タイプの設定は、本機により報告するメッセージの種類に影響しません。**syslog **サーバにおいてソートやデータベースへの保存の際に使用されます。**

例

```
Console(config)#logging facility 19
Console(config)#
```

logging trap

syslog サーバに送信するメッセージの種類を指定することができます。"no" を前に置くことで初期設定に戻します。

文法

logging trap *level*

no logging trap

level ― レベルは以下の表の通りです。選択したLevelからLevel0までのメッセージが送信されます（選択した Level は含まれます）

レベル引数	レベル	解説	syslog 定義
debugging	7	デバッグメッセージ	LOG_DEBUG
Informational	6	情報メッセージ	LOG_INFO
notifications	5	重要なメッセージ	LOG_NOTICE
warnings	4	警告メッセージ	LOG_WARNING
Errors	3	エラー状態を示すメッセージ	LOG_ERR
Critical	2	重大な状態を示すエラーメッセージ	LOG_CRIT
alerts	1	迅速な対応が必要なメッセージ	LOG_ALERT
emergencies	0	システム不安定状態を示すメッセージ	LOG_EMERG

初期設定

有効（レベル：7-0）

コマンドモード

Global Configuration

コマンド解説

- レベルを指定することによって、syslog サーバへの送信を有効に設定し、選択した Level から Level0 までのメッセージが保存されます（選択した Level は含まれます）
- レベルを指定しない場合、syslog サーバへの送信を有効に設定し、保存されるメッセージレベルを初期設定に戻します。

例

```
Console(config)#logging trap 4
Console(config)#
```

clear log

ログをバッファから削除するコマンドです。

文法

clear log < flash | ram >

- flash ― **フラッシュメモリに保存されたイベント履歴**
- ram ― RAM **に保存されたイベント履歴**

初期設定

Flash and RAM

コマンドモード

Privileged Exec

例

```
Console#clear log
Console#
```

関連するコマンド

show logging (P290)

show logging

システム、イベントメッセージに関するログを表示します。

文法

show logging < flash | ram | sendmail | trap >

- flash ― フラッシュメモリに保存されたイベント履歴
- ram ― RAM に保存されたイベント履歴
- sendmail ― SMTP イベントハンドラの設定を表示 (P295)
- trap ― syslog サーバに送信されたメッセージ

初期設定

なし

コマンドモード

Privileged Exec

例

本例では、syslog が有効で、フラッシュメモリのメッセージレベルは "errors"（初期値 3-0）、RAM へのメッセージレベルは "debugging"（初期値 7-0）と設定してあり、1 つのサンプルエラーが表示されています。

```
Console#show logging flash
Syslog logging:          Enable
History logging in FLASH: level errors
Console#show logging ram
Syslog logging: Enable
History logging in RAM: level debugging
Console#
```

項目	解説
Syslog logging	logging on コマンドによりシステムログが有効化されているかを表示
History logging in FLASH	logging history コマンドによるリポートされるメッセージレベル
History logging in RAM	logging history コマンドによるリポートされるメッセージレベル

本例では、トラップ機能の設定を表示しています。

```
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#
```

項目	解説
Syslog logging	logging on **コマンドによりシステムログが有効化されているかを表示**
REMOTELOG status	logging trap **コマンドによりリモートロギングが有効化されているかを表示**
REMOTELOG facility type	logging facility **コマンドによるリモートサーバに送信される** syslog **メッセージのファシリティタイプ**
REMOTELOG level type	logging trap **コマンドによるリモートサーバに送信される** syslog **メッセージのしきい値**
REMOTELOG server IP address	logging host **コマンドによる** syslog **サーバの** IP **アドレス**

関連するコマンド

show logging sendmail (P296)

show log

スイッチのメモリに送信された、システム / イベントメッセージを表示します。

文法

show log < flash | ram > { login }

flash ― フラッシュメモリ (恒久的) に保存されたイベント履歴

ram ― RAM(電源投入時に消去される) に保存されたイベント履歴

login ― ログインに関する履歴のみ表示

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

メモリに保存されたシステム / イベントメッセージを表示します。タイムスタンプ、メッセージレベル、プログラムモジュール、機能、及びイベント番号を表示します。

例

本例では、RAM に保存しているサンプルメッセージを表示しています。

```
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#
```

4.6.9 SMTP アラートコマンド

SMTP イベントハンドル及びアラートメッセージの SMTP サーバ及びメール受信者への送信の設定を行います。

コマンド	機能	モード	ページ
logging sendmail host	アラートメッセージを受信する SMTP サーバ	GC	P293
logging sendmail level	アラートメッセージのしきい値設定	GC	P294
logging sendmail source-email	メールの ”From” 行に入力されるアドレスの設定	GC	P294
logging sendmail destination-email	メール受信者の設定	GC	P295
logging sendmail	SMTP イベントハンドリングの有効化	GC	P295
show logging sendmail	SMTP イベントハンドラ設定の表示	NE,PE	P296

logging sendmail host

アラートメッセージを送信する SMTP サーバを指定します。

"no" を前に置くことで SMTP サーバの設定を削除します。

文法

logging sendmail host *ip_address*

no logging sendmail host *ip_address*

- *ip_address* — アラートが送られる SMTP サーバの IP アドレス

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- 最大 3 つの SMTP サーバを指定できます。複数のサーバを指定する場合は、サーバ毎にコマンドを入力して下さい。
- e-mail アラートを送信する場合、本機はまず接続を行ない、すべての e-mail アラートを順番に 1 通ずつ送信した後、接続を閉じます。
- 接続を行なう場合、本機は前回の接続時にメールの送信が成功したサーバへの接続を試みます。そのサーバでの接続に失敗した場合、本機はリストの次のサーバでのメールの送信を試みます。その接続も失敗した場合には、本機は周期的に接続を試みます（接続が行なえなかった場合には、トラップが発行されます）

例

```
Console(config)#logging sendmail host 192.168.1.19
Console(config)#
```

logging sendmail level

アラートメッセージのしきい値の設定を行ないます。

文法

logging sendmail level *level*

- *level* — システムメッセージレベル (P288)。設定した値からレベル 0 までのメッセージが送信されます（設定範囲：0-7、初期設定：7）

初期設定

Level 7

コマンドモード

Global Configuration

コマンド解説

イベントしきい値のレベルを指定します。設定したレベルとそれ以上のレベルのイベントが指定したメール受信者に送信されます（例：レベル 7 にした場合はレベル 7 から 0 のイベントが送信されます）

例

本例ではレベル 3 からレベル 0 のシステムエラーがメールで送信されます。

```
Console(config)#logging sendmail level 3
Console(config)#
```

logging sendmail source-email

メールの "From" 行に入力されるメール送信者名を設定します。

文法

logging sendmail source-email *email-address*

- *email-address* — アラートメッセージの送信元アドレス（設定範囲：0-41 文字）

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

本機を識別するためのアドレス（文字列）や本機の管理者のアドレスなどを使用します。

例

```
Console(config)#logging sendmail source-email bill@hoge.com
Console(config)#
```

logging sendmail destination-email

アラートメッセージのメール受信者を指定します。
"no" **を前に置くことで受信者を削除します。**

文法

logging sendmail destination-email *email-address*

no logging sendmail destination-email *email-address*

- *email-address* ― **アラートメッセージの送信先アドレス（設定範囲：**1-41 **文字）**

初期設定

None

コマンドモード

Global Configuration

コマンド解説

最大 5 **つのアドレスを指定することができます。複数のアドレスを設定する際はアドレス毎にコマンドを入力して下さい。**

例

```
Console(config)#logging sendmail destination-email
ted@this-company.com
Console(config)#
```

logging sendmail

SMTP **イベントハンドラを有効にします。**"no" **を前に置くことで機能を無効にします。**

文法

logging sendmail

no logging sendmail

初期設定

無効

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
-----------------------------------------------
192.168.1.19
SMTP minimum severity level: 7

SMTP destination email addresses
-----------------------------------------------
ted@this-company.com

SMTP source email address: bill@this-company.com

SMTP status: Enable

Console#
```

4.6.10 Time コマンド

NTP 又は SNTP タイムサーバを指定することによりシステム時刻の動的な設定を行なうことができます。

コマンド	機能	モード	ページ
sntp client	特定のタイムサーバからの時刻の取得	GC	P298
sntp server	タイムサーバの指定	GC	P299
sntp poll	リクエスト送信間隔の設定	GC	P300
show sntp	SNTP 設定の表示	NE,PE	P301
clock timezone	本機内部時刻のタイムゾーンの設定	GC	P302
calendar set	システム日時の設定	PE	P303
show calendar	現在の時刻及び設定の表示	NE,PE	P303

sntp client

"sntp client" コマンドにより指定した NTP 又は SNTP タイムサーバへの SNTP クライアントリクエストを有効にします。"no" を前に置くことで SNTP クライアントリクエストを無効にします。

文法

sntp client

no sntp client

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

- 本機の内部時刻の設定を正確に保つことにより、システムログの保存の際に日時を正確に記録することができます。時刻の設定がされていない場合、起動時の時刻（00:00:00, Jan. 1, 2001）が初期設定の時刻となり、そこからの時間経過となります。
- 本コマンドによりクライアント時刻リクエストが有効となり "sntp poll" コマンドにより設定した間隔で、"sntp servers" コマンドにより指定されたサーバにリクエストを行ないます。

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#
```

関連するコマンド

sntp server (P299)

sntp poll (P300)

show sntp (P301)

sntp server

SNTP タイムリクエストを受け付ける IP アドレスを指定します。"no" を引数とすることによりすべてのタイムサーバを削除します。

文法

sntp server { *ip*} *[ip2*} *[ip3*}

- *ip* — NTP/SNTP タイムサーバの IP アドレス（設定可能数：1-3）

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

SNTP クライアントモード時の時刻同期リクエストを送信するタイムサーバの指定を行ないます。本機はタイムサーバに対して応答を受信するまで要求を送信します。"sntp poll" コマンドに基づいた間隔でリクエストを送信します。

例

```
Console(config)#sntp server 10.1.0.19
Console#
```

sntp poll

SNTP クライアントモード時に時刻同期要求の送信間隔を設定します。"no" を前に置くことで初期設定に戻します。

文法

sntp poll *seconds*

no sntp poll

- *seconds* — リクエスト間隔（設定範囲：6-16384 秒）

初期設定

16 秒

コマンドモード

Global Configuration

コマンド解説

SNTP クライアントモード時にのみ有効となります。

例

```
Console(config)#sntp poll 60
Console#
```

関連するコマンド

sntp client (P298)

show sntp

SNTP クライアントの設定及び現在の時間を表示し、現地時間が適切に更新されているか確認します。

コマンドモード

Normal Exec, Privileged Exec

コマンド解説

現在時刻、SNTP クライアントモード時の時刻更新リクエスト送信間隔、現在の SNTP モードを表示します。

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

本機内部時刻のタイムゾーンの設定を行ないます。

文法

clock timezone *name* **hour** *hours* **minute** *minutes* < before-utc | after-utc >

- *name* ― **タイムゾーン名（範囲：**1-30 **文字）**
- *hours* ― UTC **との時間差（時間）（範囲：**0-12 **時間）**
- *minutes* ― UTC **との時間差（分）（範囲：**0-59 **分）**
- *before-utc* ― UTC **からのタイムゾーンの時差がマイナスの（**UTC **より早い）場合**
- *after-utc* ― UTC **からのタイムゾーンの時差がプラスの（**UTC **より遅い）場合**

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

SNTP **では** UTC(Coordinated Universal Time: **協定世界時間。別名：**GMT/Greenwich Mean Time) **を使用します。**

本機を設置している現地時間に対応させて表示するために UTC **からの時差（タイムゾーン）の設定を行う必要があります。**

例

```
Console(config)#clock timezone Japan hours 8 minute 0 after-UTC
Console(config)#
```

関連するコマンド

show sntp (P301)

calendar set

システム時刻の設定を行ないます。

文法

calendar set *hour min sec* < *day month year* | *month day year* >

- *hour* — 時間（範囲：0 - 23）
- *min* — 分（範囲 0 - 59）
- *sec* — 秒（範囲 0 - 59）
- *day* — 日付（範囲：1-31）
- *month* — 月：**january | february | march | april | may | june | july | august | september | october | november | december**
- *year* — 年（西暦 4 桁、設定範囲：2001-2100）

初期設定

なし

コマンドモード

Privileged Exec

例

本例ではシステム時刻を 2009 年 2 月 1 日 15 時 12 分 34 秒に設定しています。

```
Console#calendar set 15 12 34 february 1 2009
Console#
```

show calendar

システム時刻を表示します。

初期設定

なし

コマンドモード

Normal Exec, Privileged Exec

例

```
Console#show calendar
15:12:34 February 1 2002
Console#
```

4.6.11 システム情報の表示

コマンド	機能	モード	ページ
show startup-config	フラッシュメモリ内のスタートアップ設定ファイルの内容の表示	PE	P304
show running-config	実行中の設定ファイルの表示	PE	P306
show system	システム情報の表示	NE,PE	P308
show users	現在コンソール及び Telnet で接続されているユーザのユーザ名、接続時間、及び Telnet クライアントの IP アドレスの表示	NE,PE	P309
show version	システムバージョン情報の表示	NE,PE	P310

show startup-config

システム起動用に保存されている設定ファイルを表示するためのコマンドです。

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

- 実行中の設定ファイルと、起動用ファイルの内容を比較する場合には "show running-config" コマンドを一緒に使用して下さい。
- キーコマンドモードの設定が表示されます。各モードのグループは "!" によって分けられて configuration モードと対応するモードが表示されます。このコマンドでは以下の情報が表示されます：
  - SNMP コミュニティ名
  - ユーザ（ユーザ名及びアクセスレベル）
  - VLAN データベース（VLAN ID, VLAN 名及び状態）
  - 各インタフェースの VLAN 設定状態
  - VLAN の IP アドレス設定
  - スパニングツリー設定
  - コンソール及び Telnet に関する設定

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#
```

関連するコマンド

show running-config (P306)

show running-config

現在実行中の設定ファイルを表示するためのコマンドです。

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

- 起動用ファイルと、実行中の設定ファイルの内容を比較する場合には "show startup-config" コマンドを一緒に使用して下さい。
- キーコマンドモードの設定が表示されます。各モードのグループは "!" によって分けられて configuration モードと対応するモードが表示されます。このコマンドでは以下の情報が表示されます。
  - 本機の MAC アドレス
  - SNTP サーバの設定
  - タイムゾーンの設定
  - SNMP コミュニティ名
  - ユーザ（ユーザ名及びアクセスレベル）
  - イベントログの設定
  - VLAN データベース（VLAN ID, VLAN 名及び状態）
  - 各インタフェースの VLAN 設定状態
  - 本機の IP アドレス設定
  - IP DSCP の設定
  - コンソール及び Telnet に関する設定

例

```
Console#show running-config
building startup-config, please wait.....
!
phymap 00-12-cf-ce-2a-20 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
!
clock timezone hours 0 minute 0 after-UTC
!
!
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 DSCP
!
!
line console
!
line vty
!
end
Console#
```

関連するコマンド

show startup-config (P304)

show system

システム情報を表示するためのコマンドです。

初期設定

なし

コマンドモード

Normal Exec, Privileged Exec

コマンド解説

- **コマンドを使用して表示された内容に関しての詳細は** P19 **「システム情報の表示」を参照して下さい。**
- "POST result" **は正常時にはすべて** "PASS" **と表示されます。**"POST result" **に** "FAIL" **があった場合には販売店、又はサポートまで連絡して下さい。**

例

```
Console#show system
System Description: 24PORT GIGABIT L2 INTELLIGENT SWITCH
System OID String: 1.3.6.1.4.1.25574.8.1.5
System Information
 System Up Time:          0 days, 2 hours, 38 minutes, and 53.48
seconds
 System Name:             [NONE]
 System Location:         [NONE]
 System Contact:          [NONE]
 MAC Address (Unit1):     00-12-CF-66-57-A0
 Web Server:              Enabled
 Web Server Port:         80
 Web Secure Server:       Enabled
 Web Secure Server Port:  443
 Telnet Server:           Enable
 Telnet Server Port:      23
 Jumbo Frame:             Disabled

 POST Result:
²KMMY Test 1 ................. PASS
UART Loopback Test ........... PASS
DRAM Test .................... PASS
Switch Int Loopback Test ..... PASS

Done All Pass.
Console#
```

show users

コンソール及び Telnet **で接続されているユーザの情報を表示するためのコマンドです。**
ユーザ名、接続時間及び Telnet **接続時の** IP **アドレスを表示します。**

初期設定

なし

コマンドモード

Normal Exec, Privileged Exec

コマンド解説

コマンドを実行したユーザは行の先頭に "*" が表示されています。

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

ハードウェアとソフトウェアのバージョン情報を表示するためのコマンドです。

初期設定

なし

コマンドモード

Normal Exec, Privileged Exec

コマンド解説

表示される情報に関する詳細は P19 **「システム情報の表示」を参照して下さい。**

例

```
Console#show version
 Serial Number:           A815022982
 Service Tag:
 Hardware Version:        R01A
 EPLD Version:            0.00
 Number of Ports:         26
 Main Power Status:       Up
 Loader Version:          1.0.0.2
 Boot ROM Version:        1.0.0.5
 Operation Code Version:  1.1.0.17

Console#
```

4.6.12 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利用	GC	P311

jumbo frame

ジャンボフレームの使用を有効にします。"no" **を前に置くことで無効となります。**

文法

[no] jumbo frame

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

- **本機で最大** 9216byte **までのジャンボフレームに対応することで効率的なデータ転送を実現します。通常** 1500byte **までのイーサネットフレームに比べジャンボフレームを使用することで各パケットのオーバヘッドが縮小されます。**
- **ジャンボフレームを使用する場合は、送信側及び受信側（サーバや** PC **等）がどちらも本機能をサポートしている必要があります。また** Full-Duplex **時には** 2 **つのエンドノード間のスイッチのすべてが本機能に対応している必要があります。**Half-Duplex **時にはコリジョンドメイン内の全てのデバイスが本機能に対応している必要があります。**
- **ジャンボフレームを使用すると、ブロードキャスト制御の最大しきい値が制限されます。（詳細は、**P409 **「**broadcast bit-rate**」コマンドを参照して下さい）**
- **ジャンボフレームの現在の設定内容は** ”show system” **コマンドで確認ができます。**

例

```
Console(config)#jumbo frame
Console(config)#
```

4.7 ファイル管理（ Flash/File ）

ここで解説するコマンドはシステムコードや設定ファイルの管理を行うためのコマンドです。

コマンド	機能	モード	ページ
copy	**コードイメージや設定ファイルのフラッシュメモリへのコピーや** TFTP **サーバ間のコピー**	PE	P312
delete	**ファイルやコードイメージの削除**	PE	P316
dir	**フラッシュメモリ内のファイルの一覧の表示**	PE	P317
whichboot	**ブートファイルの表示**	PE	P318
boot system	**システム起動ファイル、イメージの設定**	GC	P319

copy

コードイメージのアップロード、ダウンロードや設定ファイルの本機、TFTP **サーバ間のアップロード、ダウンロードを行います。**

コードイメージや設定ファイルを TFTP **サーバに置いてある場合には、それらのファイルを本機にダウンロードしシステム設定等を置き換えることができます。ファイル転送は** TFTP **サーバの設定やネットワーク環境によっては失敗する場合があります。**

文法

copy *file* **< file | running-config | startup-config | tftp >**

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 >

- *file* ― **ファイルのコピーを可能にするキーワード**
- **running-config** ― **実行中の設定をコピーするキーワード**
- **startup-config** ― **システムの初期化に使用する設定**
- **tftp** ― **TFTP サーバからのコピーを行うキーワード**
- **https-certificate** ― TFTP **サーバ間の** HTTPS **認証をコピー**
- **public-key** ― TFTP **サーバから** SSH **キーをコピー（詳細は、**275 **ページの「**Secure Shell **コマンド」を参照）**

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

- **データをコピーするために完全なコマンドの入力が必要です。**
- **ファイル名は大文字と小文字が区別されます。ファイル名にはスラッシュ及びバックスラッシュは使用できません。ファイル名の最初の文字にピリオド (.) は使用できません。ファイル名の長さは** TFTP **サーバ上では** 137 **文字以下、本機上は** 31 **文字以下となります（ファイル名に使用できる文字は** A-Z, a-z, 0-9, "." , "-", "_" **です）**
- **フラッシュメモリ容量の制限により、オペレーションコードは** 2 **つのみ保存可能です。**
- **ユーザ設定ファイル数はフラッシュメモリの容量に依存します。**
- "Factory_Default_Config.cfg" **を使用し、工場出荷時設定をコピー元にすることはできますが、**" Factory_Default_Config.cfg" **をコピー先に指定することはできません。**
- **起動時の設定を変更するためには** "startup-config" **をコピー先にする必要があります。**

- **ブート** ROM **イメージは** TFTP **サーバからのアップロード及びダウンロードはできません。ブート** ROM **または診断用イメージのダウンロードを行うためには新規のファームウェアに関するリリースノートの解説か、又は代理店の指示に従う必要があります。**
- "http-certificate" **の設定については、**68 **ページの「サイト証明書の設定変更」を参照して下さい。**HTTPs **を用い、高セキュリティを確保した接続を行うための本機の設定については、**271 **ページの「**ip http secure-server**」を参照して下さい。**

例

本例では、TFTP **サーバを利用した設定ファイルのアップロードを示しています。**

```
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#
```

本例では実行ファイルのスタートアップファイルへのコピーを示しています。

```
Console#copy running-config file
destination file name: startup
Write to FLASH Programming.
\Write to FLASH finish.
Success.

Console#
```

本例では、設定ファイルのダウンロード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#
```

本例では、TFTP サーバのセキュアサイト承認を示しています。承認を完了するため、再起動を行っています。

```
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
```

本例では、TFTP サーバから SSH で使用するための公開キーをコピーしています。SSH による公開キー認証は、本機に対して設定済みのユーザに対してのみ可能であることに注意して下さい。

```
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

ファイルやイメージを削除する際に利用します。

文法

delete [public-key *username* { dsa | rsa } **|** *filename* **]**

- **public-key** *username* —**ユーザ名を指定して、公開キーを削除**
  - dsa — DSA **公開キータイプ**
  - rsa — RSA **公開キータイプ**
- *filename* —**ファイル又はイメージ名**

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

- **スタートアップファイルは削除することができません。**
- "Factory_Default_Config.cfg" **は削除することができません。**

例

本例ではフラッシュメモリからの設定ファイル "test2.cfg" **の削除を示しています。**

```
Console#delete test2.cfg
Console#
```

関連するコマンド

dir (P317)

delete public-key (P280)

dir

フラッシュメモリ内のファイルの一覧を表示させる際に利用します。

文法

dir { boot-rom | config | opcode *:filename* **}**

表示するファイル、イメージタイプは以下のとおりです :

- **boot-rom** ― ブート ROM 又は、診断イメージファイル
- **config** ― 設定ファイル
- **opcode** ― Run-time operation code イメージファイル
- *filename* ― ファイル又はイメージ名。ファイルが存在してもファイル内にエラーがある場合には表示できません。

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

- パラメータを入力せずに "dir" コマンドのみを入力した場合にはすべてのファイルが表示されます。
- 表示されるファイルの情報は以下の表の通りです

項目	内容
file name	ファイル名
file type	ファイルタイプ：Boot-Rom、Operation Code、Config file
startup	起動時に使用されているかどうか
size	ファイルサイズ (byte)

例

本例は、すべてのファイル情報の表示を示しています。

```
Console#dir
        File name                         File type       Startup Size (byte)
 ----------------------------------     --------------  ------- -----------
 Unit1:
         FXC3126A-DIAG-V1.0.0.5.bix       Boot-Rom Image  Y           305512
         FXC3126A-OP-V1.1.0.16.bix        Operation Code  Y          3043524
         Factory_Default_Config.cfg       Config File     N              489
         startup1.cfg                     Config File     Y             4512
-------------------------------------------------------------------------------
                                                  Total free space:   3407872
Console#
```

whichboot

現在、本機がどのファイルから起動されているかを表示します。

文法

whichboot

初期設定

なし

コマンドモード

Privileged Exec

例

本例は、すべてのファイル情報の表示を示しています。

```
Console#whichboot
   file name                           file type    startup size (byte)
------------------------------------ -------------- ------- -----------
   Unit1:
   D2218                               Boot-Rom image   Y   214124
   V2271                               Operation Code   Y   1761944
   Factory_Default_Config.cfg          Config File      Y   5197
Console#
```

boot system

システム起動に使用するファイル又はイメージを指定する際に利用します。

文法

boot system < boot-rom | config | opcode > : *filename*

設定するファイルタイプは以下の通りです。

- **boot-rom** ― **ブート** ROM
- **config** ― **設定ファイル**
- **opcode** ― **ランタイムオペレーションコード**
- *filename* ― **ファイル又はイメージ名**

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- **ファイルにエラーがある場合には、起動ファイルに設定できません。**

例

```
Console(config)#boot system config: startup
Console(config)#
```

関連するコマンド

dir (P317)

4.8 ユーザ認証

システム管理のためのユーザログインはローカル及び認証サーバを用いたユーザ認証が利用可能です。

また、IEEE802.1X **を利用したポートベース認証によるユーザのネットワークへのアクセス管理も可能です。**

コマンドグループ	機能	ページ
Authentication Sequence	**ログイン認証方式と優先順位の設定**	P321
RADIUS Client	RADIUS **サーバ認証の設定**	P323
TACACS+ Client	TACACS+ **サーバ認証の設定**	P329
AAA	**認証** , **認可** , **アカウンティング** (AAA) **の設定**	P333
Port Security	**ポートへのセキュアアドレスの設定**	P344
Port Authentication	EEE802.1X **によるポート認証の設定**	P347
Network Access	MAC **認証および動的** VLAN **割り当てを設定**	P356
Web Authentication	Web **認証を設定**	P363

4.8.1 認証コマンド

コマンド	機能	モード	ページ
Authentication login	認証方法と優先順位の設定	GC	P321
authentication enable	コマンドモード変更時の認証方式と優先順位の設定	GC	P321

Authentication login

ログイン認証方法及び優先順位を設定します。"no" を前に置くことで初期設定に戻します。

文法

authentication login <local | radius | tacacs>

no authentication login

- **local** ― ローカル認証を使用します
- **radius** ― RADIUS サーバ認証を使用します
- **tacacs** ― TACACS+ サーバ認証を使用します

初期設定

Local のみ

コマンドモード

Global Configuration

コマンド解説

- RADIUS では UDP、TACACS+ では TCP を使用します。UDP はベストエフォート型の接続ですが、TCP は接続確立型の接続となります。また、RADIUS 暗号化はクライアントからサーバへのアクセス要求パケットのパスワードのみが暗号化されます。
- RADIUS 及び TACACS+ ログイン認証は各ユーザ名とパスワードに対しアクセスレベルを設定することができます。ユーザ名とパスワード、アクセスレベルは認証サーバ側で設定することができます。
- 3 つの認証方式を 1 つのコマンドで設定することができます。例えば、"authentication login radius tacacs local" とした場合、ユーザ名とパスワードを RADIUS サーバに対し最初に確認します。RADIUS サーバが利用できない場合、TACACS+ サーバにアクセスします。TACACS+ サーバが利用できない場合はローカルのユーザ名とパスワードを利用します。

例

```
Console(config)#authentication login radius
Console(config)#
```

関連するコマンド

username (P265)

authentication enable

"enable" コマンド（P243）で Exec モードから Privileged Exec モードへ変更する場合の、ログイン認証方法及び優先順位を設定します。"no" を前に置くことで初期設定に戻します。

文法

authentication enable <local | radius | tacacs >

no authentication enable

- **local** ― ローカル認証を使用します
- **radius** ― RADIUS サーバ認証を使用します
- **tacacs** ― TACACS+ サーバ認証を使用します

初期設定

Local のみ

コマンドモード

Global Configuration

コマンド解説

- RADIUS では UDP、TACACS+ では TCP を使用します。UDP はベストエフォート型の接続ですが、TCP は接続確立型の接続となります。また、RADIUS 暗号化はクライアントからサーバへのアクセス要求パケットのパスワードのみが暗号化されます。
- RADIUS 及び TACACS+ ログイン認証は各ユーザ名とパスワードに対しアクセスレベルを設定することができます。ユーザ名とパスワード、アクセスレベルは認証サーバ側で設定することができます。
- 3 つの認証方式を 1 つのコマンドで設定することができます。例えば、"authentication enable radius tacacs local" とした場合、ユーザ名とパスワードを RADIUS サーバに対し最初に確認します。RADIUS サーバが利用できない場合、TACACS+ サーバにアクセスします。TACACS+ サーバが利用できない場合はローカルのユーザ名とパスワードを利用します。

例

```
Console(config)#authentication enable radius
Console(config)#
```

関連するコマンド

enable password (P243) ― コマンドモード変更のためのパスワードの設定

4.8.2 Radius クライアントコマンド

RADIUS(Remote Authentication Dial-in User Service) は、ネットワーク上の RADIUS 対応デバイスのアクセスコントロールを認証サーバにより集中的に管理することができます。認証サーバは複数のユーザ名 / パスワードと各ユーザの本機へのアクセスレベルを管理するデータベースを保有しています。

コマンド	機能	モード	ページ
radius-server host	RADIUS サーバの設定	GC	P324
radius-server auth-port	RADIUS サーバ認証ポートの設定	GC	P325
radius-server acct-port	RADIUS サーバアカウンティングポートの設定	GC	P326
radius-server key	RADIUS 暗号キーの設定	GC	P326
radius-server retransmit	リトライ回数の設定	GC	P327
radius-server timeout	認証リクエストの間隔の設定	GC	P327
show radius-server	RADIUS 関連設定情報の表示	PE	P328

radius-server host

プライマリ / バックアップ RADIUS **サーバ、及び各サーバの認証パラメータの設定を行います。**"no" **を前に置くことで初期設定に戻します。**

文法

radius-server *index* **host** *host_ip_address* **{ auth-port** *auth_port* **| acct-port** *acct_port* **| timeout** *timeout* **| retransmit** *retransmit* **| key** *key* **}**

no radius-server *index*

- *index* — **サーバを** 5 **つまで設定できます。指定したサーバの順に、サーバが応答するかタイムアウトがくるまでリクエストを送信します。**
- *host_ip_address* — RADIUS **サーバの** IP **アドレス**
- *auth_port* — **認証メッセージに使用される** UDP **ポート（範囲：**1-65535**）**
- *acct_port* — **アカウンティングメッセージに使用される** UDP **ポート（範囲：**1-65535**）**
- *timeout* — **サーバからの応答を待ち、再送信を行うまでの時間（秒）（範囲：**1-1000 **秒）**
- *retransmit* — RADIUS **サーバに対するログインアクセスをリトライできる回数（範囲：**0-30**）**
- *key* — **クライアントへの認証ログインアクセスのための暗号キー。間にスペースは入れられません（最大** 48 **文字）**

初期設定

- auth-port：1812
- acct-port：1813
- timeout：5 **秒**
- retransmit：2

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 auth-port

RADIUS サーバ認証用ポートの設定を行います。"no" を前に置くことで初期設定に戻します。

文法

radius-server auth-port *port_number*

no radius-server auth-port

- *port_number* ― RADIUS サーバ認証用 UDP ポート番号 (範囲：1-65535)

初期設定

1812

コマンドモード

Global Configuration

例

```
Console(config)#radius-server auth-port 181
Console(config)#
```

radius-server acct-port

RADIUS サーバアカウンティング用ポートの設定を行います。"no" を前に置くことで初期設定に戻します。

文法

radius-server acct-port *port_number*

no radius-server acct-port

- *port_number* — RADIUS サーバアカウンティング用 UDP ポート番号 (範囲：1-65535)

初期設定

1813

コマンドモード

Global Configuration

例

```
Console(config)#radius-server acct-port 8181
Console(config)#
```

radius-server key

RADIUS 暗号キーを設定します。"no" を前に置くことで初期設定に戻します。

文法

radius-server key *key_string*

no radius-server key

• *key_string* — クライアントへの認証ログインアクセスのための暗号キー。間にスペースは入れられません（最大 48 文字）

初期設定

なし

コマンドモード

Global Configuration

例

```
Console(config)#radius-server key green
Console(config)#
```

radius-server retransmit

リトライ数を設定します。"no" **を前に置くことで初期設定に戻します。**

文法

radius-server retransmit *number_of_retries*

no radius-server retransmit

- *number_of_retries* ― RADIUS **サーバに対するログインアクセスをリトライできる回数（範囲：**1-30**）**

初期設定

2

コマンドモード

Global Configuration

例

```
Console(config)#radius-server retransmit 5
Console(config)#
```

radius-server timeout

RADIUS **サーバへの認証要求を送信する間隔を設定します。**"no" **を前に置くことで初期設定に戻します。**

文法

radius-server timeout *number_of_seconds*

no radius-server timeout

- *number_of_seconds* ― **サーバからの応答を待ち、再送信を行うまでの時間（秒）(** 範囲：1-65535)

初期設定

5

コマンドモード

Global Configuration

例

```
Console(config)#radius-server timeout 10
Console(config)#
```

show radius-server

現在の RADIUS **サーバ関連の設定を表示します。**

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#show radius-server
Global Settings:
  Communication Key with RADIUS Server:
  Auth-Port:                              1812
  Acct-port:                              1813
  Retransmit Times:                        2
  Request Timeout:                         5

Server 1:
  Server IP Address:                     10.1.2.3
  Communication Key with RADIUS Server: ******
  Auth-Port:                              1812
  Acct-port:                              1813
  Retransmit Times:                        2
  Request Timeout:                         5

Radius server group:
Group                   Name Member Index
---------------------- -------------
radius                           1
Console#
```

4.8.3 TACACS+ クライアントコマンド

TACACS+(Terminal Access Controller Access Control System) は、ネットワーク上の TACACS+ 対応のデバイスのアクセスコントロールを認証サーバにより集中的に行うことができます。認証サーバは複数のユーザ名 / パスワードと各ユーザの本機へのアクセスレベルを管理するデータベースを保有しています。

コマンド	機能	モード	ページ
tacacs-server host	TACACS+ サーバの設定	GC	P329
tacacs-server port	TACACS+ サーバのポートの設定	GC	P330
tacacs-server key	TACACS+ 暗号キーの設定	GC	P330
tacacs-server retransmit	リトライ回数の設定	GC	P331
tacacs-server timeout	認証リクエストの間隔の設定	GC	P330
show tacacs-server	TACACS+ 関連設定情報の表示	GC	P332

tacacs-server host

TACACS+ サーバの設定を行います。"no" を前に置くことで初期設定に戻します。

文法

tacacs-server *index* **host** *host_ip_address* **{ port** *port_number* **| timeout** *timeout* **| retransmit** *retransmit* **| key** *key* **}**

no tacacs-server *index*

- *index* —サーバのインデックス番号を指定（範囲：1）
- *host_ip_address* — TACACS+ サーバの IP アドレス
- *port_number* — 認証メッセージに使用される TCP ポート（範囲：1-65535）
- *timeout* — サーバからの応答を待ち、再送信を行うまでの時間（秒）（範囲：1-540 秒）
- *retransmit* — サーバに対するログインアクセスをリトライできる回数（範囲：1-30）
- *key* — クライアントへの認証ログインアクセスのための暗号キー。スペースは入れられません。（範囲：48 文字）

初期設定

. port - 49

. timeout - 5 秒

. retransmit - 2

コマンドモード

Global Configuration

例

```
Console(config)#tacacs-server 1 host 192.168.1.25
Console(config)#
```

tacacs-server port

TACACS+ サーバのポートの設定を行います。"no" を前に置くことで初期設定に戻します。

文法

tacacs-server port *port_number*

no tacacs-server port

- *port_number* — TACACS+ サーバの認証用 TCP ポート番号 (範囲：1-65535)

初期設定

49

コマンドモード

Global Configuration

例

```
Console(config)#tacacs-server port 181
Console(config)#
```

tacacs-server key

TACACS+ 暗号キーを設定します。"no" を前に置くことで初期設定に戻します。

文法

tacacs-server key *key_string*

no tacacs-server key

- *key_string* — クライアントへの認証ログインアクセスのための暗号キー。間にスペースは入れられません（最大 48 文字）

初期設定

なし

コマンドモード

Global Configuration

例

```
Console(config)#tacacs-server key green
Console(config)#
```

tacacs-server retransmit

リトライ数を設定します。"no" **を前に置くことで初期設定に戻します。**

文法

tacacs-server retransmit *number_of_retries*

no tacacs-server retransmit

- *number_of_retries* — TACACS+ **サーバに対するログインアクセスをリトライできる回数（範囲：**1-30**）**

初期設定

2

コマンドモード

Global Configuration

例

```
Console(config)#tacacs-server retransmit 5
Console(config)#
```

tacacs-server timeout

TACACS+ **への認証要求を送信する間隔を設定します。**"no" **を前に置くことで初期設定に戻します。**

文法

tacacs-server timeout *number_of_seconds*

no tacacs-server timeout

- *number_of_seconds* — **サーバからの応答を待ち、再送信を行うまでの時間（秒）(** 範囲：1-540)

初期設定

5 秒

コマンドモード

Global Configuration

例

```
Console(config)#tacacs-server timeout 10
Console(config)#
```

show tacacs-server

現在の TACACS+ **サーバ関連の設定を表示します。**

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#show tacacs-server

Remote TACACS+ server configuration:

Global Settings:
  Communication Key with TACACS+ Server:
  Server Port Number:                    49
  Retransmit Times :                      2
  Request Times :                         5

Server 1:
  Server IP address:                   1.2.3.4
  Communication key with TACACS+ server: *****
  Server port number:                    49
  Retransmit Times :                      2
  Request Times :                         5

Tacacs server group:
Group Name             Member Index
---------------------- -------------
tacacs+                       1
Console#
```

4.8.4 AAA（認証・許可・アカウンティング）コマンド

オーセンティケーション、オーソライゼーション、アカウンティング（AAA）機能はスイッチ上でアクセス制御を行うための主要なフレームワークを規定します。この 3 つのセキュリティ機能は下のようにまとめることができます。

- **オーセンティケーション：ネットワークへのアクセスを要求するユーザーを認証します。**
- **オーソライゼーション：ユーザーが特定のサービスにアクセスできるかどうかを決定します。**
- **アカウンティング：ネットワーク上のサービスにアクセスしたユーザーに関する報告、監査、請求を行います。**

AAA 機能を使用するにはネットワーク上で RADIUS サーバー、もしくは TACACS+ サーバーを構成することが必要です。セキュリティサーバーはシーケンシャルグループとして定義され、特定のサービスへのユーザーアクセスを制御するために適用されます。例えば、スイッチがユーザーを認証しようと試みた場合、最初にリクエストが定義されたグループ内のサーバーに送信されます。応答がない場合、第 2 のサーバーにリクエストが送信され、さらに応答がない場合、次のサーバーにリクエストが送信されます。どこかの時点で認証が成功するか失敗した場合、プロセスは停止します。

コマンド	機能	モード	ページ
aaa group server	**グループサーバ名の設定**	GC	P334
server	**グループリスト内サーバの IP アドレスを設定**	SG	P334
aaa accounting dot1x	802.1X **サービスのアカウンティングを有効**	GC	P335
aaa accounting exec	Exec **サービスのアカウンティングを有効**	GC	P336
aaa accounting commands	Exec **モードコマンドのアカウンティングを有効**	GC	P337
aaa accounting update	**定期的なアップデートをアカウンティングサーバへ送信**	GC	P338
accounting dot1x	**アカウンティングメソッドをインタフェースへ適用**	IC	P338
accounting exec	**アカウンティングメソッドをローカルコンソール、**Telnet**、**SSH **接続へ適用**	Line	P339
accounting commands	**アカウンティングメソッドをユーザ入力** CLI **コマンドへ適用**	Line	P340
aaa authorization exec	Exec **セッションの許可を有効**	GC	P341
authorization exec	**許可メソッドをローカルコンソール、**Telnet**、**SSH **接続へ適用**	Line	P342
show accounting	**アカウンティング情報の表示**	PE	P343

aaa group server

セキュリティサーバホストのグループ名を設定します。"no" **を前に置くことで初期設定に戻します。**

文法

aaa group server < radius | tacacs+ > *group-name*

no aaa group server < radius | tacacs+ > *group-name*

- **radius** ― RADIUS **サーバグループ**
- **tacacs+** ― TACACS+ **サーバグループ**
- *group-name* ― **セキュリティサーバグループ名**

初期設定

なし

コマンドモード

Global Configuration

例

```
Console(config)#aaa group server radius tps
Console(config-sg-radius)#
```

server

セキュリティサーバを AAA **サーバグループに追加します。**"no" **を前に置くことで、グループからサーバを削除します。**

文法

server < *index* **|** *ip-address* **>**

no server < *index* **|** *ip-address* **>**

- *index* ― **サーバインデックスを指定します（範囲：**RADIUS 1-5　TACACS+ 1）
- *ip-address* ―**サーバ** IP **アドレスを指定します**

初期設定

なし

コマンドモード

Server Group Configuration

例

```
Console(config)#aaa group server radius tps
Console(config-sg-radius)#server 10.2.68.120
Console(config-sg-radius)#
```

aaa accounting dot1x

ネットワークアクセスのために要求された 802.1X **アカウンティングサービスを有効にします。**"no" **を前に置くことで、機能を無効にします。**

文法

aaa accounting dot1x < default | *method-name* > start-stop group <radius | tacacs+ |*server-group*>

no aaa accounting dot1x <default | *method-name*>

- **default** —**サービスリクエストの、デフォルトアカウンティングメソッドを指定します**
- *method-name* — **サービスリクエストのアカウンティングメソッドを指定します。（範囲：**1-255 **文字）**
- **start-stop** — **開始から停止時までのアカウンティングを記録します。**
- **group** —**使用するサーバグループを指定します**
  - **radius** — RADIUS **サーバに設定された全ての** RADIUS **ホスト（**P323 **参照）**
  - **tacacs+** — TACACS+ **サーバに設定された全ての** TACACS+ **ホスト（**P329 **参照）**
  - *server-group* — aaa **グループサーバに設定されたサーバグループの名前を指定（**P334 **参照）**

初期設定

アカウンティング：無効

コマンドモード

Global Configuration

例

```
Console(config)#aaa accounting dot1x default start-stop group radius
Console(config)#
```

aaa accounting exec

ネットワークアクセスのために要求された Exec **サービスのアカウンティングを有効にします。**"no" **を前に置くことで、機能を無効にします。**

文法

aaa accounting exec < default | method-name > start-stop *group*
<radius | tacacs+ |*server-group***>**

no aaa accounting exec <default | *method-name***>**

- **default** ―**サービスリクエストの、デフォルトアカウンティングメソッドを指定します**
- *method-name* ― **サービスリクエストのアカウンティングメソッドを指定します。（範囲：**1-255 **文字）**
- **start-stop** ― **開始から停止時までのアカウンティングを記録します。**
- **group** ―**使用するサーバグループを指定します**
  - **radius** ― RADIUS **サーバに設定された全ての** RADIUS **ホスト（**P323 **参照）**
  - **tacacs+** ― TACACS+ **サーバに設定された全ての** TACACS+ **ホスト（**P329 **参照）**
  - *server-group* ― aaa **グループサーバに設定されたサーバグループの名前を指定（**P334 **参照）**

初期設定

アカウンティング：無効

コマンドモード

Global Configuration

例

```
Console(config)#aaa accounting exec default start-stop group tacacs+
Console(config)#
```

aaa accounting commands

Exec モードコマンドのアカウンティングを有効にします。"no" を前に置くことで、機能を無効にします。

文法

aaaa accounting commands *level* **<default |** *method-name***> start-stop** *group*

<tacacs+ |*server-group***>**

no aaa accounting commands *level* **<default |** *method-name***>**

- *level* ― コマンド実行の privilege レベル
- **default** ―サービスリクエストの、デフォルトアカウンティングメソッドを指定します
- *method-name* ― サービスリクエストのアカウンティングメソッドを指定します。（範囲：1-255 文字）
- **start-stop** ― 開始から停止時までのアカウンティングを記録します。
- **group** ―使用するサーバグループを指定します
  - ー **tacacs+** ― TACACS+ サーバに設定された全ての TACACS+ ホスト（P329 参照）
  - ー *server-group* ― aaa グループサーバに設定されたサーバグループの名前を指定（P334 参照）

初期設定

アカウンティング：無効

コマンドモード

Global Configuration

例

```
Console(config)#aaa accounting commands 15 default start-stop group
tacacs+
Console(config)#
```

aaa accounting update

アカウンティングサーバへの定期的な更新を有効にします。"no" **を前に置くことで、機能を無効にします。**

文法

aaa accounting update { periodic *interval* **}**

no aaa accounting update

- *interval*— **サーバーへアカウンティングレコードを送信うする間隔を指定します (範囲：**1-2147483647 **分)**

初期設定

1 **分**

コマンドモード

Global Configuration

例

```
Console(config)#aaa accounting update periodic 30
Console(config)#
```

accounting dot1x

インタフェースに、802.1x **サービスリクエストのアカウンティングメソッドを適用します。**no" **を前に置くことで、機能を無効にします。**

文法

accounting dot1x < default | *list-name* **>**

no accounting dot1x

- **default**— "aaa accounting dot1x" **コマンドで作成された、デフォルトメソッドリストを指定します（**P335 **参照）**
- *list-name*— "aaa accounting dot1x" **コマンドで作成された、メソッドリストを指定します。**

初期設定

なし

コマンドモード

Interface Configuration

例

```
Console(config)#interface ethernet 1/2
Console(config-if)#accounting dot1x tps
Console(config-if)#
```

accounting exec

ローカルコンソールまたは Telnet **接続にアカウンティングメソッドを適用します。**no" **を前に置くことで、機能を無効にします。**

文法

accounting exec < default | *list-name* **>**

no accounting exec

- **default**— "aaa accounting dot1x" **コマンドで作成された、デフォルトメソッドリストを指定します（**P335 **参照）**
- *list-name*— "aaa accounting dot1x" **コマンドで作成された、メソッドリストを指定します。**

初期設定

なし

コマンドモード

Line Configuration

例

```
Console(config)#line console
Console(config-line)#accounting exec tps
Console(config-line)#exit
Console(config)#line vty
Console(config-line)#accounting exec default
Console(config-line)#
```

accounting commands

入力される CLI **コマンドにアカウンティングメソッドを適用します。**no" **を前に置くことで、機能を無効にします。**

文法

accounting commands *level* **< default |** *list-name* **>**

no accounting commands *level*

- *level*—**実行コマンドの特権レベル（範囲：**0-15**）**
- **default**— "aaa accounting dot1x" **コマンドで作成された、デフォルトメソッドリストを指定します（**P335 **参照）**
- *list-name*— "aaa accounting dot1x" **コマンドで作成された、メソッドリストを指定します。**

初期設定

なし

コマンドモード

Line Configuration

例

```
Console(config)#line console
Console(config-line)#accounting commands 15 default
Console(config-line)#
```

aaa authorization exec

Exec アクセスの認可を有効にします。no" を前に置くことで、機能を無効にします。

文法

aaa authorization exec <default | *method-name***> group <tacacs+ |** *server-group***>**
no aaa authorization exec < default | *method-name* **>**

- **default**—Exec アクセスの、デフォルト認可メソッドを指定します
- *method-name*—メソッド名を指定します
- **group** —使用するサーバグループを指定します
  - **tacacs+** — TACACS+ サーバに設定された全ての TACACS+ ホスト（P329 参照）
  - *server-group* — aaa グループサーバに設定されたサーバグループの名前を指定（P334 参照）

初期設定

Authorization：有効

コマンドモード

Global Configuration

例

```
Console(config)#aaa authorization exec default group tacacs+
Console(config)#
```

authorization exec

ローカルコンソールまたは Telnet **接続に認可メソッドを適用します。**no" **を前に置くことで、機能を無効にします。**

文法

authorization exec < default | *list-name* **>**

no authorization exec

- **default**—"aaa authorization exec" **で作成されたデフォルトメソッドリスト**(P341 **参照**)
- *list-name*— "aaa accounting dot1x" **コマンドで作成された、メソッドリストを指定します。**

初期設定

なし

コマンドモード

Line Configuration

例

```
Console(config)#line console
Console(config-line)#authorization exec tps
Console(config-line)#exit
Console(config)#line vty
Console(config-line)#authorization exec default
Console(config-line)#
```

show accounting

機能ごと、またはポートごとに、現在のアカウンティング設定情報を表示します。

文法

show accounting {commands { *level* **} | dot1x {statistics { username** *user-name* **|** *interface* **} } | exec {statistics} }**

- **commands**—**特権レベルコマンドアカウンティング情報の表示**
- *level*—CLI **コマンドの特権レベル（範囲：**0-15）
- **dot1x**—dod1x **アカウンティング情報の表示**
- **exec**—exec **アカウンティング情報の表示**
- **statistics**—**アカウンティング記録の表示**
- *user-name*—**指定したユーザーのアカウンティング記録の表示**
- *interface*

  − **ethernet** *unit/port*

  − *unit* — **ユニット番号** "1"

  − *port* — **ポート番号（範囲：**1-26）

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#show accounting
Accounting Type : dot1x
  Method List   : default
  Group List    : radius
  Interface     :

Accounting Type : Exec
  Method List   : default
  Group List    : radius
  Interface     :
```

4.8.5 ポートセキュリティコマンド

ポートへのポートセキュリティ機能を使用できるようにします。ポートセキュリティ機能を使用すると、ポートにおける最大学習数に達した際に MAC **アドレスの学習を止めます。そして、そのポートの動的 / 静的なアドレステーブルに既に登録されているソース** MAC **アドレスの受信フレームのみネットワークへのアクセスを許可します。そのポートでも他のポートからも学習されていない不明なソース** MAC **アドレスの受信フレームは破棄します。学習されていない** MAC **アドレスを送信するデバイスがあった場合、この動作はスイッチで検知され、自動的にそのポートを無効にし、**SNMP **トラップメッセージを送信します。**

コマンド	機能	モード	ページ
port security	**ポートセキュリティの設定**	IC	P345
mac-address-table static	VLAN **内のポートへの静的アドレスのマッピング**	GC	P432
show mac-address-table	**フォワーディングデータベースのエントリ表示**	PE	P434

port security

ポートへのポートセキュリティを有効に設定します。キーワードを使用せず "no" **を前に置くことでポートセキュリティを無効にします。キーワードと共に** "no" **を前に置くことで侵入動作及び最大** MAC **アドレス登録数を初期設定に戻します。**

文法

port security { action < shutdown | trap | trap-and-shutdown **>**

| max-mac-count *address-count* **}**

no port security {action | *max-mac-count* **}**

- **action** ― **ポートセキュリティが破られた場合のアクション**
  - shutdown ― **ポートを無効**
  - 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ポートを無効**
- max-mac-count
  - *address-count* ― **ポートにおいて学習する** MAC **アドレスの最大値（範囲：**0-1024）

初期設定

- Status：**無効** (Disabled)
- Action：**なし**
- Maximum Addresses：0

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- **ポートセキュリティを有効にした場合、本機は設定した最大学習数に達すると、有効にしたポートで** MAC **アドレスの学習を行わなくなります。すでにアドレステーブルに登録済みの** MAC **アドレスのデータのみがアクセスすることができます。**
- **まず** "port security max-mac-count" **コマンドを使用して学習するアドレス数を設定し、**"port security" **コマンドでポートのセキュリティを有効に設定します。**
- **ポートセキュリティを無効に設定し、最大アドレス学習数を初期設定値に戻すには、**"no port security max-mac-count" **コマンドを使用します。**
- **新しい** VLAN **メンバーを追加する場合には、**MAC **アドレスを** "mac-address-table static" **コマンドを使用します。**
- **セキュアポートには以下の制限があります：**
  - ― **ポートミラーリングは使用できません。**
  - ― **複数の** VLAN **に所属できません。**
  - ― **ネットワークを相互接続するデバイスには接続できません。**
  - ― **トランクグループに加えることはできません。**
- **ポートセキュリティが機能しポートを無効にした場合、**"no shutdown" **コマンドを使用し、手動で再度有効にする必要があります。**

例

本例では、5 番ポートにポートセキュリティとポートセキュリティ動作を設定しています。

```
Console(config)#interface ethernet 1/5
Console(config-if)#port security action trap
```

関連するコマンド

shutdown (P408)

mac-address-table static (P432)

show mac-address-table (P434)

4.8.6 802.1x ポート認証コマンド

本機では IEEE802.1X (dot1x) のポートベースアクセスコントロールをサポートし、ID とパスワードによる認証により許可されないネットワークへのアクセスを防ぐことができます。クライアントの認証は RADIUS サーバにより EAP(Extensible Authentication Protocol) を用いて行われます。

コマンド	機能	モード	ページ
dot1x system-auth-control	dot1x をスイッチ全体に有効に設定	GC	P347
dot1x default	dot1x の設定値をすべて初期設定に戻します。	GC	P348
dot1x max-req	認証プロセスを初めからやり直す前に認証プロセスを繰り返す最大回数	GC	P348
dot1x port-control	ポートへの dot1x モードの設定	IC	P349
dot1x operation-mode	dot1x ポートへの接続可能ホスト数の設定	IC	P350
dot1x re-authenticate	特定ポートへの再認証の強制	PE	P351
dot1x re-authentication	全ポートへの再認証の強制	GC	P351
dot1x timeout quiet-period	max-req を超えた後、クライアントの応答を待つ時間	GC	P352
dot1x timeout re-autheperiod	接続済みクライアントの再認証間隔の設定	GC	P352
dot1x timeout tx-period	認証中の EAP パケットの再送信間隔の設定	GC	P353
dot1x intrusion-action	認証失敗時の、侵入にたいするポート返答	IC	P353
show dot1x	dot1x 関連情報の表示	PE	P354

dot1x system-auth-control

スイッチが、802.1X ポート認証を使用できるよう設定します。"no" を前に置くことで初期設定に戻します。

文法

dot1x system-auth-control

no dot1x system-auth-control

初期設定

無効（Disabled）

コマンドモード

Global Configuration

例

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

dot1x default

すべての dot1x **の設定を初期設定に戻します。**

文法

dot1x default

コマンドモード

Global Configuration

例

```
Console(config)#dot1x default
Console(config)#
```

dot1x max-req

ユーザ認証のタイムアウトまでのクライアントへの EAP **リクエストパケットの最大送信回数の設定を行います。**"no" **を前に置くことで初期設定に戻します。**

文法

dot1x max-req *count*

no dot1x max-req

- *count* ― **最大送信回数（範囲：**1-10）

初期設定

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

ポートに対して dot1x **モードの設定を行います。**

文法

dot1x port-control < auto | force-authorized | force-unauthorized >

no dot1x port-control

- **auto** ― dot1x **対応クライアントに対して** RADIUS **サーバによる認証を要求します。** dot1x **非対応クライアントからのアクセスは許可しません。**
- **force-authorized** ― dot1x **対応クライアントを含めたすべてのクライアントのアクセスを許可します。**
- **force-unauthorized** ― dot1x **対応クライアントを含めたすべてのクライアントのアクセスを禁止します。**

初期設定

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

IEEE802.1x 認証ポートに対して 1 台もしくは複数のホスト（クライアント）の接続を許可する設定を行います。キーワードなしで "no" を前に置くことで初期設定に戻ります。" multi-host max-count" キーワードと共に "no" を前に置くことで複数ホスト時の初期値 5 となります。

文法

dot1x operation-mode [single-host | multi-host {max-count *count* **}]**

no dot1x operation-mode { multi-host max-count }

- **single-host** ― ポートへの 1 台のホストの接続のみを許可
- **multi-host** ― ポートへの複数のホストの接続を許可
- **max-count** ― 最大ホスト数
  - *count* ― ポートに接続可能な最大ホスト数（設定範囲：1-1024、初期設定：5）

初期設定

Single-host

コマンドモード

Interface Configuration

コマンド解説

- "max-count" パラメータは P349 「dot1x port-control」で "auto" に設定されている場合にのみ有効です。
- "multi-host" を設定すると、ポートに接続するホストのうちの 1 台のみが認証の許可を得られれば、他の複数のホストもネットワークへのアクセスが可能になります。逆に、接続するホスト再認証に失敗したり、EAPOL ログオフメッセージを送信した場合、他のホストも認証に失敗したことになります。

例

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x operation-mode multi-host max-count 10
Console(config-if)#
```

dot1x re-authenticate

全ポート又は特定のポートでの再認証を強制的に行います。

文法

dot1x re-authenticate { *interface* }

- i*nterface*
  - **ethernet** *unit/port*
    - *unit* — **ユニット番号** "1"
    - *port* — **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

全ポートでの周期的な再認証を有効にします。"no" **を前に置くことで再認証を無効にします。**

文法

dot1x re-authentication

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

EAP リクエストパケットの最大送信回数を過ぎた後、新しいクライアントの接続待機状態に移行するまでの時間を設定します。"no" を前に置くことで初期設定に戻します。

文法

dot1x timeout quiet-period *seconds*

no dot1x timeout quiet-period

- *seconds* — 秒数（範囲：1-65535 秒）

初期設定

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

接続されたクライアントに再認証を要求する間隔を設定します。

文法

dot1x timeout re-authperiod *seconds*

no dot1x timeout re-authperiod

- *seconds* — 秒数（範囲：1-65535 秒）

初期設定

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

認証時に EAP **パケットの再送信を行う間隔を設定します。**"no" **を前に置くことで初期設定に戻します。**

文法

dot1x timeout tx-period *seconds*

no dot1x timeout tx-period

- *seconds* — **秒数（範囲：**1-65535 **秒）**

初期設定

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)#
```

dot1x intrusion-action

認証失敗時、全てのトラフィックをブロックするか、ポートのトラフィックをゲスト VLAN **に割り当てるかを設定します。**"no" **を前に置くことで初期設定に戻します。**

文法

dot1x intrusion-action < block-traffic | guest-vlan >

no dot1x intrusion-action

初期設定

block-traffic

コマンドモード

Interface Configuration

コマンド解説

- **ゲスト** VLAN **割り当てを行うには、あらかじめ** VLAN **の設定を行い、**"Active" **にしてください。（**P487 **「**VLAN**」を参照）またゲスト** VLAN **として割り当てを行ってください。（**P359 **「**network-access guest-vlan**」を参照）**

例

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x intrusion-action guest-vlan
Console(config-if)#
```

show dot1x

本機または特定のインタフェースのポート認証に関連した設定状態の表示を行います。

文法

show dot1x { statistics | interface *interface* **}**

- *interface*

  ー **ethernet** *unit/port*

  unit ― ユニット番号 “1”

  port ― ポート番号（範囲：1-26）

コマンドモード

Privileged Exec

コマンド解説

本コマンドで表示されるのは以下の情報です。

- *Global 802.1X Parameters* ― 本機全体に対する、802.1X ポート認証の有効 / 無効
- *802.1X Port Summary* ― 各インタフェースのアクセスコントロールの設定値
  - Status ― ポートアクセスコントロールの管理状態
  - Operation Mode ― P350 「dot1x operation-mode」の設定値
  - Mode ― dot1x port-control で設定する dot1x モード (P349)
  - Authorized ― 認証状態 (yes 又は n/a - not authorized)
- *802.1X Port Details* ― 各インタフェースでのポートアクセスコントロール設定の詳細を表示します。以下の値が表示されます。
  - reauth-enabled - 周期的な再認証 (P351)
  - reauth-period - 接続されたクライアントに再認証を要求する間隔 (P352)
  - quiet-period - 最大送信回数超過後、新しいクライアントの接続待機状態に移行するまでの時間 (P352)
  - tx-period - 認証時に EAP パケットの再送信を行う間隔 (P353)
  - supplicant-timeout - クライアントのタイムアウト
  - server-timeout - サーバのタイムアウト
  - reauth-max - 再認証の最大回数
  - max-req - ユーザ認証のタイムアウトまでの、ポートからクライアントへの EAP リクエストパケットの最大送信回数 (P348)
  - Status - 認証ステータス (許可又は禁止)
  - Operation Mode - 802.1X認証ポートに1台もしくは複数のホスト(クライアント)の接続が許可されているか
  - Max Count - ポートに接続可能な最大ホスト数 (P350)
  - Port-control - ポートの dot1x モードが "auto"、"force-authorized" 又は "force-unauthorized のいずれになっているか (P349)
  - Supplicant - 認証されたクライアントの MAC アドレス

- Current Identifier - **認証機能により、現行の認証接続を識別するために使用された整数値** (0-255)

- *Authenticator State Machine* —
  - State — **現在の状態** (initialize, disconnected, connecting, authenticating, authenticated, aborting, held, force_authorized, force_unauthorized)
  - Reauth Count — **再認証回数**

- *Backend State Machine* —
  - State — **現在の状態** (request, response, success, fail, timeout, idle, initialize)
  - Request Count — **クライアントからの応答がない場合に送信される** EAP **リクエストパケットの送信回数**
  - Identifier(Server) — **直近の** EAP**の成功/失敗又は認証サーバから受信したパケット**

- *Reauthentication State Machine* —
  - State — **現在の状態** (initialize, reauthenticate)

例

```
Console#show dot1x interface ethernet 1/1

802.1X is enabled on port 1/1
 Reauth-enabled:       Enabled
 Reauth-period:        3600
 Quiet-period:         60
 TX-period:            30
 Supplicant-timeout:   30
 Server-timeout:       10
 Reauth-max:           2
 Max-req:              2
Status                 Unauthorized
Operation Mode         Single-Host
Max Count              5
Port-control           Auto
Supplicant             00-00-00-00-00-00
Current Identifier     0
Intrusion action       Block traffic

Authenticator State Machine
State               Initialize
Reauth Count        0

Backend State Machine
State               Initialize
Request Count       0
Identifier(Server)  0

Reauthentication State Machine
State               Initialize
Console#
```

4.8.7 ネットワークアクセス（MAC アドレス認証）

スイッチポートに接続するいくつかのデバイスはハードウェアやソフトウェアの制限により 802.1x 認証をサポートできないかもしれません。これはネットワークプリンタ、IP 電話、ワイヤレスアクセスポイントのようなデバイスでしばしば遭遇します。スイッチは、RADIUS サーバーでデバイスの MAC アドレスを認証し管理することで、これらのデバイスからのネットワークアクセスを可能にします。

コマンド	機能	モード	ページ
network-access mode	インタフェースで MAC 認証を有効	IC	P356
network-access max-mac-count	全ての認証方式によって、ポートで認証可能な MAC アドレスの最大数を設定	IC	P357
mac-authentication intrusion-action	MAC 認証失敗時に、ポートがホストへ行う行動を設定	IC	P357
mac-authentication max-mac-count	802.1X 認証あるいは Mac 認証によって、ポートに認証可能な MAC アドレスの最大数を設定	IC	P358
network-access dynamic-vlan	認証ポートの、動的 VLAN 割り当てを有効	IC	P358
network-access guest-vlan	ネットワークアクセス（Mac 認証）あるいは 802.1x 認証が拒否時、全てのトラフィックをゲスト VLAN ポートへ割り当て	IC	P359
mac-authentication reauth-time	認証された MAC アドレスが再認証を行うまでの時間を設定	GC	P359
clear network-access	セキュア MAC アドレステーブルから、エントリを削除	PE	P360
show network-access	ポートインタフェースの MAC 認証設定を表示	PE	P361
show network-access mac-address-table	セキュア MAC アドレステーブルエントリを表示	PE	P362

network-access mode

ネットワークアクセス認証をポートで有効にします。"no" **を前に置くことで無効に設定します。**

文法

network-access mode mac-authentication

no network-access mode mac-authentication

初期設定

無効

コマンドモード

Interface Configuration

例

```
Console(config-if)#network-access mode mac-authentication
Console(config-if)#
```

network-access max-mac-count

全ての認証方式によって、ポートで認証可能な MAC **アドレスの最大数を設定します。**"no" **を前に置くことで設定を初期状態に戻します。**

ネットワークアクセス認証をポートで有効にします。"no" **を前に置くことで無効に設定します。**

文法

network-access max-mac-count *count*

no network-access max-mac-count

- *count* ― **認証できる** MAC **アドレスの最大数を設定します。(範囲：**1-1024)

初期設定

1024

コマンドモード

Interface Configuration

例

```
Console(config-if)#network-access max-mac-count 5
Console(config-if)#
```

mac-authentication intrusion-action

MAC **認証失敗時に、ポートがホストへ行う行動を設定します。**"no" **を前に置くことで設定を初期状態に戻します。**

文法

mac-authentication intrusion-action < block traffic | pass traffic >

no mac-authentication intrusion-action

初期設定

Block Traffic

コマンドモード

Interface Configuration

例

```
Console(config-if)#mac-authentication intrusion-action block-traffic
Console(config-if)#
```

mac-authentication max-mac-count

802.1X 認証あるいは Mac 認証によって、ポートに認証可能な MAC アドレスの最大数を設定します。"no" を前に置くことで設定を初期状態に戻します。

文法

mac-authentication max-mac-count *count*

no mac-authentication max-mac-count

- *count* ― 認証できる MAC アドレスの最大数を設定します。（範囲：1-1024）

初期設定

1024

コマンドモード

Interface Configuration

例

```
Console(config-if)#mac-authentication max-mac-count 32
Console(config-if)#
```

network-access dynamic-vlan

認証ポートの、動的 VLAN 割り当てを有効にします。"no" を前に置くことで無効に設定します。

文法

network-access dynamic-vlan

no network-access dynamic-vlan

初期設定

有効

コマンドモード

Interface Configuration

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access dynamic-vlan
Console(config-if)#
```

network-access guest-vlan

ネットワークアクセス（Mac 認証）あるいは 802.1x 認証が拒否時、全てのトラフィックをゲスト VLAN ポートへ割り当てます。"no" を前に置くことでゲスト VLAN アサイメントを無効にします。

文法

network-access guest-vlan *vlan-id*

no network-access guest-vlan

- *vlan-id* — VLAN ID **を指定（範囲：**1-4094**）**

初期設定

無効

コマンドモード

Interface Configuration

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access guest-vlan 25
Console(config-if)#
```

mac-authentication reauth-time

認証された MAC アドレスが再認証を行うまでの時間を設定します。"no" を前に置くことで設定を初期状態に戻します。

文法

mac-authentication reauth-time *seconds*

no mac-authentication reauth-time

- *seconds* — **再認証時間（範囲：**120-1000000 **秒）**

初期設定

1800 **秒**

コマンドモード

Global Configuration

例

```
Console(config)#mac-authentication reauth-time 300
Console(config)#
```

clear network-access

セキュア MAC **アドレステーブルから、エントリを削除します。**

文法

clear network-access mac-address-table { static | dynamic| address *mac-address*| **interface** *interface* **}**

- **static** ― **静的アドレスエントリを指定**
- **dynamic** ― **動的アドレスエントリを指定**
- *mac-address* ― MAC **アドレスエントリを指定（フォーマット：**xx-xx-xx-xx-xx-xx**）**
- *interface*
  - **ethernet** *unit/port*
    - *unit* ― **ユニット番号** "1"
    - *port* ― **ポート番号（範囲：**1-26**）**

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#clear network-access mac-address-table interface ethernet 1/1
Console#
```

show network-access

ポートインタフェースの、MAC 認証設定を表示します。

文法

show network-access { interface *interface* **| mac-address-table }**

- *interface*
  - **ethernet** *unit/port*
    - *unit* ― **ユニット番号** "1"
    - *port* ― **ポート番号（範囲：**1-26）
- **mac-address-table** ― MAC **アドレステーブルを指定。**

初期設定

全てのインタフェースで無効

コマンドモード

Privileged Exec

例

```
Console#show network-access interface ethernet 1/1
Global secure port information
Reauthentication Time : 1800
-------------------------------------------------
-------------------------------------------------
Port : 1/1
MAC Authentication : Disabled
MAC Authentication Intrusion action : Block traffic
MAC Authentication Maximum MAC Counts : 1024
Maximum MAC Counts : 2048
Dynamic VLAN Assignment : Enabled
Guest VLAN : Disabled
Console#
```

show network-access mac-address-table

セキュア MAC **アドレステーブルエントリを表示します。**

文法

show network-access mac-address-table { static | dynamic |
address *mac-address mask* **| interface** *interface* **| sort < address | interface> }**

- **static** ― **静的アドレスエントリを指定**
- **dynamic** ― **動的アドレスエントリを指定**
- *mac-address* ― MAC **アドレスエントリを指定（フォーマット：**xx-xx-xx-xx-xx-xx**）**
- *mask* ― MAC **アドレスビットマスクを指定**
- *interface*
  - **ethernet** *unit/port*
    - *unit* ― **ユニット番号** "1"
    - *port* ― **ポート番号（範囲：**1-26**）**
- **sort** ― **表示されたエントリを** MAC **アドレスまたはインタフェースでソートします。**

初期設定

全てのフィルタを表示

コマンドモード

Privileged Exec

例

```
Console#show network-access mac-address-table
---- ----------------- -------------- --------- -------------------------
Port MAC-Address RADIUS-Server Attribute Time
---- ----------------- -------------- --------- -------------------------
1/1 00-00-01-02-03-04 172.155.120.17 Static 00d06h32m50s
1/1 00-00-01-02-03-05 172.155.120.17 Dynamic 00d06h33m20s
1/1 00-00-01-02-03-06 172.155.120.17 Static 00d06h35m10s
1/3 00-00-01-02-03-07 172.155.120.17 Dynamic 00d06h34m20s
Console#
```

4.8.8 Web 認証

Web Authentication は、802.1x やネットワークアクセス認証は実行不可能であり実用的でない状況で、ネットワークへの認証とアクセスを行うことを端末に許可します。Web Authentication 機能は IP アドレスを割り当てる DHCP のリクエストと受信、DNS クエリの実行を、認証されていないホストに許可します。HTTP を除いたほかのすべてのトラフィックはブロックされます。スイッチは HTTP トラフィックを傍受し、RADIUS を通してユーザーネームとパスワードを入力する、スイッチが生成した Web ページにリダイレクトします。一度認証に成功すると、Web ブラウザは元のリクエストされた Web ページに転送されます。認証が成功したポートに接続されたすべてのホストについて、認証が有効になります。

[注意] MAC アドレス認証、Web Authentication、802.1x、ポートセキュリティは同じポート上で同時に使用することができません。1 つのセキュリティ機能のみ適用できます。

[注意] RADIUS 認証は適切に機能させるために、アクティベートし Web Authentication のために適切に構成しなくてはいけません。

[注意] Web Authentication はトランクポート上で設定することはできません。

コマンド	機能	モード	ページ
web-auth login-attempts	Web 認証ログイン失敗時の再認証回数を設定	GC	P364
web-auth quiet-period	Web 認証ログインの最大回数を過ぎた後、接続待機状態に移行するまでの時間を設定	GC	P364
web-auth session-timeout	セッションタイムアウト時間を設定	GC	P365
web-auth system-auth-control	Web 認証をグローバルで有効	GC	P365
web-auth	Web 認証をインタフェースで有効	IC	P366
show web-auth	グローバル Web 認証パラメータを表示	PE	P366
show web-auth interface	指定したインタフェースの Web 認証パラメータおよび統計値を表示	PE	P367
web-auth re-authenticate(Port)	ポートに確立されている全ての Web 認証セッションを終了	PE	P368
web-auth re-authenticate (IP)	ートに確立されている全ての Web 認証セッションを終了	PE	P369
show web-auth summary	指定した IP アドレスで確立されている Web 認証セッションを終了	PE	P370
authorization exec	許可メソッドをローカルコンソール、Telnet、SSH 接続へ適用	Line	P342
show accounting	Web 認証ポートパラメータおよび統計値の概要を表示	PE	P343

web-auth login-attempts

認証ログイン失敗時に、再認証を行う制限を設定します。設定した最大回数を過ぎた後は、"web-authquiet-period" **を設定した期限が切れるまで、スイッチはそれ以上のログインを拒否します。**"no" **を前に置くことで設定を初期状態に戻します。**

文法

web-auth login-attempts *count*

no web-auth login-attempts

- *count* ― **ログインの試行回数の上限を設定します（範囲：**1-3 **回）**

初期設定

3 **回**

コマンドモード

Global Configuration

例

```
Console(config)#web-auth login-attempts 2
Console(config)#
```

web-auth quiet-period

Web **認証ログインの、最大試行回数を過ぎた後、ログイン待機状態に移行するまでの時間を設定します。**"no" **を前に置くことで設定を初期状態に戻します。**

文法

web-auth quiet-period *time*

no web-auth quiet period

- *time*― **ホストがログインの試行回数の上限を超えた後、再び認証ができるまでに待機する時間を設定します（範囲：**1 ー 180 **秒）**

初期設定

60 **秒**

コマンドモード

Global Configuration

例

```
Console(config)#web-auth quiet-period 120
Console(config)#
```

web-auth session-timeout

セッションタイムアウト時間を設定します。設定したタイムアウト時間に達した時、ホストは強制的にログオフされ、再度認証を行う必要があります。"no" **を前に置くことで設定を初期状態に戻します。**

文法

web-auth session-timeout *timeout*

no web-auth session timeout

- *timeout*— **ホストの再認証をする前に認証セッションをどのくらいの時間維持するかを設定します（範囲：**300 ～ 3600 **秒）**

初期設定

3600 **秒**

コマンドモード

Global Configuration

例

```
Console(config)#web-auth session-timeout 1800
Console(config)#
```

web-auth system-auth-control

Web **認証をグローバルで有効にします。**"no" **を前に置くことで設定を初期状態に戻します。**

文法

web-auth system-auth-control

no web-auth system-auth-control

初期設定

無効

コマンドモード

Global Configuration

例

```
Console(config)#web-auth system-auth-control
Console(config)#
```

web-auth

Web 認証をインタフェースで有効にします。"no" を前に置くことで設定を初期状態に戻します。

文法

web-auth

no web-auth

初期設定

無効

コマンドモード

Interface Configuration

例

```
Console(config-if)#web-auth
Console(config-if)#
```

show web-auth

グローバル Web 認証パラメータを表示します。

文法

show web-auth

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#sh web-auth

Global Web-Auth Parameters

  System Auth Control : Enabled
  Login Page URL :
  Login Fail Page URL :
  Login Success Page URL :
  Session Timeout : 3600
  Quiet Period : 60
  Max Login Attempts : 3
Console#
```

show web-auth interface

指定したインタフェースの Web **認証パラメータおよび統計値を表示します。**

文法

show web-auth interface *interface*

- *interface*

  − **ethernet** *unit/port*

    − *unit* ― **ユニット番号** "1"

    − *port* ― **ポート番号（範囲：**1-26）

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#show web-auth interface eth 1/2
Web Auth Status : Enabled

Host Summary

IP address Web-Auth-State Remaining-Session-Time
---------------- -------------- ----------------------
Console#
```

web-auth re-authenticate (Port)

ポートに確立されている全ての Web **認証セッションを終了します。ユーザは再認証を行う必要があります。**

文法

web-auth re-authenticate interface *interface*

- *interface*

  − **ethernet** *unit/port*

  − *unit* ― **ユニット番号** "1"

  − *port* ― **ポート番号（範囲：**1-26）

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#web-auth re-authenticate interface ethernet 1/2
Console#
```

web-auth re-authenticate (IP)

指定した IP **アドレスで確立されている** Web **認証セッションを終了します。ユーザは再認証を行う必要があります。**

文法

sweb-auth re-authenticate interface *interface IP Address*

- *interface*
  - **ethernet** *unit/port*
    - *unit* ― **ユニット番号** "1"
    - *port* ― **ポート番号（範囲：**1-26）
- *IP Address*― IPv4 **フォーマット** IP **アドレス**

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#web-auth re-authenticate interface ethernet 1/2 192.168.1.5
Console#
```

show web-auth summary

Web 認証ポートパラメータおよび統計値の概要を表示します。

文法

show web-auth summary

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#show web-auth summary
Global Web-Auth Parameters
System Auth Control : Enabled
Port Status Authenticated Host Count
---- ------ ------------------------
1/ 1 Disabled 0
1/ 2 Enabled 0
1/ 3 Disabled 0
1/ 4 Disabled 0
1/ 5 Disabled 0
1/ 6 Disabled 0
1/ 7 Disabled 0
1/ 8 Disabled 0
1/ 9 Disabled 0
1/10 Disabled 0
Console#
```

4.9 ACL（Access Control Lists）

Access Control Lists (ACL) は IP アドレス、プロトコル、TCP/UDP ポート番号よる IP パケットへのパケットフィルタリングを提供します。

入力されるパケットのフィルタリングを行うには、初めにアクセスリストを作成し、必要なルールを追加します。その後、リストに特定のポートをバインドします。

Access Control Lists

ACL は IP アドレス、又は他の条件と一致するパケットに対して許可 (Permit) 又は拒否 (Deny) するためのリストです。

本機では入力パケットに対して ACL と一致するかどうか１個ずつ確認を行います。パケットが許可ルールと一致した場合には直ちに通信を許可し、拒否ルールと一致した場合にはパケットを落とします。リスト上の許可ルールに一致しない場合、パケットは落とされ、リスト上の拒否ルールに一致しない場合、パケットは通信を許可されます。

本機には 2 つのフィルタリングモードがあります。

- Standard IP ACL mode (STD-ACL) ― ソース IP アドレスに基づくフィルタリングを行う IP ACL モード
- Extended IP ACL mode (EXT-ACL) ― ソース又はディスティネーション IP アドレス、プロトコルタイプ、TCP/UDP ポート番号に基づくフィルタリングを行う IP ACL モード

ACL は以下の制限があります。

- 各 ACL は最大 32 ルールまで設定可能です。
- 但し、リソースの制限により、ポートに結び付けられた規則の数の平均は 20 を超えないようにして下さい。
- 本機は ingress（入力）ACL のみをサポートしています。1 個の IP ACL を任意の ingress（入力）ポートにバインドできます。

有効な ACL は以下の順番で実行されます。

（1）入力ポートの入力 IP ACL のユーザに定義されたルール

（2）入力ポートの入力 IP ACL のデフォルトルール (permit any any)

（3）明確なルールに一致しない場合、暗黙のデフォルトルール (permit all)

コマンド	機能	ページ
IP ACLs	IP アドレス、TCP/UDP ポート番号、TCP コントロールコードに基づく ACL の設定	P372
MAC ACLs	ハードウェアアドレス、パケットフォーマット、イーサネットタイプに基づく ACL の設定	P379
ACL Information	ACL 及び関連するルールの表示。各ポートの ACL の表示	P384

4.9.1 IP ACL コマンド

コマンド	機能	モード	ページ
access-list IP	IP ACL の作成と configuration mode への移行	GC	P373
permit,deny	ソース IP アドレスが一致するパケットのフィルタリング	STD-ACL	P374
permit,deny	ソース又はディスティネーション IP アドレス、プロトコルタイプ、TCP/UDP ポート番号に基づくフィルタリング	EXT-ACL	P375
show ip access-list	設定済み IP ACL のルールの表示	PE	P376
ip access-group	IP ACL へのポートの追加	IC	P377
show ip access-group	IP ACL に指定したポートの表示	PE	P378

access-list ip

IP ACL を追加し、スタンダード又は拡張 IP ACL の設定モードに移行します。"no" を前に置くことで特定の ACL を削除します。

文法

access-list ip < standard | extended > *acl_name*

no access-list ip < standard | extended > *acl_name*

- **standard** ― ソース IP アドレスに基づくフィルタリングを行う ACL
- **extended** ― ソース又はディスティネーション IP アドレス、プロトコルタイプ、TCP/UDP ポート番号に基づくフィルタリングを行う ACL
- *acl_name* ― ACL 名（最大 15 文字）

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- 新しい ACL を作成した場合や、既存の ACL の設定モードに移行した場合、"permit" 又は "deny" コマンドを使用し、新しいルールを追加します。ACL を作成するには、最低 1 つのルールを設定する必要があります。
- ルールを削除するには "no permit" 又は "no deny" コマンドに続けて設定済みのルールを入力します。
- 1 つの ACL には最大 100 個のルールが設定可能です。

例

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

関連するコマンド

permit, deny (P374)

ip access-group (P377)

show ip access-list (P376)

permit,deny（Standard ACL）

スタンダード IP ACL ルールを追加します。本ルールでは特定のソース IP アドレスからのパケットへのフィルタリングが行えます。"no" を前に置くことでルールを削除します。

文法

[permit | deny] [any | *source bitmask* **| host** *source*]

no [permit | deny] [any | *source bitmask* **| host** *source*]

- **any** ― すべての IP アドレス
- *source* ― ソース IP アドレス
- *bitmask* ― 一致するアドレスビットを表す 10 進数値
- **host** ― 特定の IP アドレスを指定

初期設定

なし

コマンドモード

Standard ACL

コマンド解説

- 新しい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似ており、4 つの 0-255 の値で表示され、それぞれがピリオド (.) により分割されています。2 進数のビットが "1" の場合、一致するビットであり、"0" の場合、拒否するビットとなります。ビットマスクはビット毎に特定の IP アドレスと共に使用し、ACL が指定した入力 IP パケットのアドレスと比較されます。

例

本例では、10.1.1.21 のソースアドレスへの許可 (permit) ルールとビットマスクを使用した 168.92.16.x-168.92.31.x までのソースアドレスへの許可 (permit) ルールを設定しています。

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

関連するコマンド

access-list ip (P373)

permit,deny（Extended ACL）

拡張 IP ACL **へのルールの追加を行います。ソース又はディスティネーション** IP **アドレス、プロトコルタイプ、**TCP/UDP **ポート番号、**TCP **コントロールコードに基づくフィルタリングを行います。**"no" **を前に置くことでルールの削除を行います。**

文法

[**no**] {**permit | deny**} *[protocol-number* **| udp**]

{**any |** *source address-bitmask* **| host** *source*}

{**any |** *destination address-bitmask* | **host** destination}

[**source-port sport** [*end*]] [**destination-port** *dport* [*end*]]

[**no**] {**permit** | **deny**} **tcp**

{**any** | *source address-bitmask* | **host** *source*}

{**any** | *destination address-bitmask* | **host** *destination*}

[**source-port sport** [*end*]] [**destination-port** *dport* [*end*]]

- *protocol-number* ― **特定のプロトコル番号（範囲：**0-255）
- *source* ― **ソース** IP **アドレス**
- *destination* ― **ディスティネーション** IP **アドレス**
- *address-bitmask* ― **アドレスビットマスク**
- **host** ― **特定の** IP **アドレスの指定**
- *sport* ― **プロトコル** * **ソースポート番号（範囲：**0-65535）
- *dscp* ― DSCP **プライオリティレベル（範囲：**0-63）
- *end* ― **プロトコルポート範囲の上限（範囲：**0-65535）

初期設定

なし

コマンドモード

Extended ACL

コマンド解説

- **新しい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似ており、**4 **つの** 0-255 **の値で表示され、それぞれがピリオド** (.) **により分割されています。**2 **進数のビットが** "1" **の場合、一致するビットであり、**"0" **の場合、拒否するビットとなります。ビットマスクはビット毎に特定の** IP **アドレスと共に使用し、**ACL **が指定した入力** IP **パケットのアドレスと比較されます。**

例

本例では、ソースアドレスがサブネット 10.7.1.x **内の場合、すべての入力パケットを許可します。**

```
Console(config-ext-acl)#permit 10.7.1.1 255.255.255.0 any
Console(config-ext-acl)#
```

本例では、ディスティネーション TCP **ポート番号** 80 **のクラス** C **アドレス** 192.168.1.0 **からすべてのディスティネーションアドレスへの** TCP **パケットを許可します。**

```
Console(config-ext-acl)#permit 192.168.1.0 255.255.255.0 any
destination-port 80
Console(config-ext-acl)##
```

関連するコマンド

access-list ip (P373)

show ip access-list

設定済みの IP ACL **のルールを表示します。**

文法

show ip access-list < standard | extended > *acl_name*

- **standard** ― **スタンダード** IP ACL
- **extended** ― **拡張** IP ACL
- *acl_name* ― ACL **名（最大** 16 **文字、スペースは不可）**

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 168.92.16.0 255.255.240.0
Console#
```

ip access-group

IP ACL へのポートのバインドを行います。"no" を前に置くことでポートを外します。

文法

ip access-group *acl_name* **< in | out >**

no ip access-group *acl_name* **< in | out >**

- *acl_name* ― （最大 16 文字、スペースは不可）
- **in** ― 入力パケットへのリスト
- **out** ― 出力パケットへのリスト

初期設定

なし

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- 1 つのポートは 1 つの ACL のみ設定可能です。
- ポートがすでに ACL を設定済みで、他の ACL をバインドした場合、新しくバインドした ACL が有効となります。

例

```
Console(config)#int eth 1/25
Console(config-if)#ip access-group david in
Console(config-if)#
```

関連するコマンド

show ip access-list (P376)

show ip access-group

IP ACL のポートの設定を表示します。

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#
```

関連するコマンド

ip access-group (P377)

4.9.2 MAC ACL コマンド

コマンド	機能	モード	ページ
access-list mac	MAC ACL の作成と configuration mode への移行	GC	P379
permit,deny	ソース又はディスティネーションアドレス、パケットフォーマット、イーサネットタイプに基づくフィルタリング	MAC-ACL	P380
show mac access-list	設定済み MAC ACL のルールの表示	PE	P382
mac access-group	MAC ACL へのポートの追加	IC	P382
show mac access-group	MAC ACL に指定したポートの表示	PE	P383

access-list mac

MAC アドレスリストを追加し、MAC ACL 設定モードに移行します。"no" を前に置くことで指定した ACL を削除します。

文法

access-list mac *acl_name*

no access-list mac *acl_name*

- *acl_name* — ACL 名（最大 15 文字）

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- 新しい ACL を作成した場合や、既存の ACL の設定モードに移行した場合、"permit" 又は "deny" コマンドを使用し、新しいルールを追加します。ACL を作成するには、最低 1 つのルールを設定する必要があります。
- ルールを削除するには "no permit" 又は "no deny" コマンドに続けて設定済みのルールを入力します。
- 1 つの ACL には最大 32 個のルールが設定可能です。

例

```
Console(config)#access-list mac jerry
Console(config-mac-acl)#
```

関連するコマンド

permit, deny (MAC ACL) (P374)

mac access-group (P377)

show mac access-list (P376)

permit,deny（MAC ACL）

MAC ACL へのルールの追加を行います。MAC ソース / ディスティネーションアドレス、イーサネットプロトコルタイプによりフィルタリングを行います。"no" を前に置くことでルールを削除します。

文法

[**no**] {**permit | deny**}
{**any |host** *source*|*source address-bitmask*}
{**any | host** *destination* | *destination address-bitmask*}
[**vid** *vid vid-bitmask*] [**ethertype** *protocol* [*protocol-bitmask*]]
※初期設定は Ethernet2 パケットです。

[**no**] {**permit | deny**} **tagged-eth2**
{**any |host** *source*|*source address-bitmask*}
{**any | host** *destination* | *destination address-bitmask*}
[**vid** *vid vid-bitmask*] [**ethertype** *protocol* [*protocol-bitmask*]

[**no**] {**permit | deny**} **untagged-eth2**
{**any |host** *source*|*source address-bitmask*}
{**any | host** *destination* | *destination address-bitmask*}
[**ethertype** *protocol* [*protocol-bitmask*]

[**no**] {**permit | deny**} **tagged-802.3**
{**any |host** *source*|*source address-bitmask*}
{**any | host** *destination* | *destination address-bitmask*}
[**vid** *vid vid-bitmask*]

[**no**] {**permit | deny**} **untagged-802.3**
{**any |host** *source*|*source address-bitmask*}
{**any | host** *destination* | *destination address-bitmask*}

protocol-number — 特定のプロトコル番号（範囲：0-255）

- **tagged-eth2** — タグ付きイーサネット 2 パケット
- **untagged-eth2** — タグ無しイーサネット 2 パケット定
- **tagged-802.3** — タグ付きイーサネット 802.3 パケット
- **untagged-802.3** — タグ無しイーサネット 802.3 パケット
- **any** — すべての MAC ソース / ディスティネーションアドレス
- **host** — 特定の MAC アドレス
- *source* — ソース MAC アドレス
- *destination* — ビットマスクを含むディスティネーション MAC アドレス範囲
- *address-bitmask* — MAC アドレスのビットマスク（16 進数）

- *vid* ― VLAN ID（範囲：1-4093）
- *vid* ― VLAN ビットマスク（範囲：1-4093）
- *protocol* ― イーサネットプロトコル番号（範囲：600-fff 16 進数）
- *protocol -bitmask*― プロトコルビットマスク（範囲：600-fff 16 進数）

初期設定

なし

コマンドモード

MAC ACL

コマンド解説

- 新しいルールはリストの最後に追加されます。
- イーサネットタイプオプションは Ethernet II のフィルタにのみ使用します。
- イーサネットプロトコルタイプのリストは RFC 1060 で定義されていますが、一般的なタイプは以下の通りです。
  - ― 0800(IP)
  - ― 0806(ARP)
  - ― 8137(IPX)

例

```
Console(config-mac-acl)#permit any host 00-e0-29-94-34-de ethertype 0800
Console(config-mac-acl)#
```

関連するコマンド

access-list mac (P379)

show mac access-list

MAC ACL のルールを表示します。

文法

show mac access-list { *acl_name* }

- *acl_name* ― ACL 名（最大 16 文字）

コマンドモード

Privileged Exec

例

```
Console#show mac access-list
MAC access-list jerry:
   permit any 00-e0-29-94-34-de ethertype 0800
Console#
```

関連するコマンド

permit, deny (P380)
mac access-group (P382)

mac access-group

MAC ACL へのポートのバインドを行います。"no" を前に置くことでポートを外します。

文法

mac access-group *acl_name* **< in | out >**

no mac access-group *acl_name* **< in | out >**

- *acl_name*― ACL 名（最大 15 文字）
- **in** ― 入力パケットへのリスト
- **out** ― 出力パケットへのリスト

コマンドモード

Interface Configuration (Ethernet)

例

```
Console(config)#interface ethernet 1/2
Console(config-if)#mac access-group jerry in
Console(config-if)#
```

関連するコマンド

show mac access-list (P382)

show mac access-group

MAC ACL に指定された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 1/5
 MAC access-list M5 in
Console#
```

関連するコマンド

mac access-group (P382)

4.9.3 ACL 情報の表示

コマンド	機能	モード	ページ
show access-list	全ての ACL と関連するルールの表示	PE	P384
show access-group	ソース IP アドレスが一致するパケットのフィルタリング	PE	P384

show access-list

すべての ACL とユーザ定義マスクを含む関連するルールを表示します。

コマンドモード

Privileged Exec

コマンド解説

- ACL がインタフェースに結合されると、ルールが表示される順序は関連するマスクによって決定されます。

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
IP access-list jerry:
 permit any host 00-30-29-94-34-de ethertype 800 800
IP extended access-list A6:
 permit any any
Console#
```

show access-group

ACL のポートの指定を表示します。

コマンドモード

Privileged Executive

例

```
Console#show access-group
Interface ethernet 1/1
 IP access-list jerry in
.
.
.
Interface ethernet 1/26
 IP access-list jerry in
Console#
```

4.10 SNMP

トラップマネージャで送信するエラータイプなどの SNMP **管理端末を使用した本機へのアクセスに関する設定を行います。**

コマンド	機能	モード	ページ
snmp-server	SNMP **サーバーを有効化**	GC	P385
show snmp	SNMP **の設定情報を表示**	NE,PE	P386
snmp-server community	SNMP **コマンドでアクセスするためのコミュニティ名の設定**	GC	P387
snmp-server contact	**システムコンタクト情報の設定**	GC	P388
snmp-server location	**システム設置情報の設定**	GC	P388
snmp-server host	SNMP **メッセージを受信するホストの設定**	GC	P389
snmp-server enable traps	SNMP **メッセージを受信するホストの有効化**	GC	P391
snmp-server engine-id	**エンジン** ID **の設定**	GC	P392
show snmp engine-id	**エンジン** ID **の表示**	PE	P393
snmp-server view	**ビューの設定**	GC	P394
show snmp view	**ビューの表示**	PE	P395
snmp-server group	**グループの追加と、ユーザーをビューへマッピング**	GC	P396
show snmp group	**グループの表示**	PE	P397
snmp-server user	SNMP v3 **グループへユーザーの追加**	GC	P399
show snmp user	SNMP v3 **ユーザーの表示**	PE	P400

snmp-server

SNMPv3 **エンジンおよび、その他全ての管理クライアントサービスを有効にします。**

"no" **を前に置くことでサービスを無効にします。**

+ 初期設定

有効

コマンドモード

Global Configuration

例

```
Console(config)#snmp-server
Console(config)#
```

show snmp

SNMP のステータスを表示します。

文法

show snmp

初期設定

なし

コマンドモード

Normal Exec, Privileged Exec

コマンド解説

本コマンドを使用することで、コミュニティ名に関する情報、及び SNMP の入出力データの数が "snmp-server enable traps" コマンドが有効になっていなくても表示されます。

例

```
Console#show snmp

SNMP Agent: enabled

SNMP traps:
  Authentication: enable
    Link-up-down: enable

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#
```

snmp-server community

SNMP 使用時のコミュニティ名を設定します。"no" を前に置くことで個々のコミュニティ名の削除を行います。

文法

snmp-server community *string* **{ ro | rw }**

no snmp-server community *string*

- *string* — SNMP プロトコルにアクセスするためのパスワードとなるコミュニティ名（最大 32 文字、大文字小文字は区別されます。最大 5 つのコミュニティ名を設定できます）
- **ro** — 読み取りのみ可能なアクセス。ro に指定された管理端末は MIB オブジェクトの取得のみが行えます
- **rw** — 読み書きが可能なアクセス。rw に指定された管理端末は MIB オブジェクトの取得及び変更が行えます

初期設定

- public — 読み取り専用アクセス (ro)。MIB オブジェクトの取得のみが行えます
- private — 読み書き可能なアクセス (rw)。管理端末は MIB オブジェクトの取得及び変更が行えます

コマンドモード

Global Configuration

コマンド解説

"snmp-server community" コマンドは SNMP **を有効にします。"no snmp-server community" コマンドは** SNMP **を無効にします。**

例

```
Console(config)#snmp-server community alpha rw
Console(config)#
```

snmp-server contact

システムコンタクト情報の設定を行います。"no" **を前に置くことでシステムコンタクト情報を削除します。**

文法

snmp-server contact *text*

no snmp-server contact

- *text* — **システムコンタクト情報の解説（最大** 255 **文字）**

初期設定

なし

コマンドモード

Global Configuration

例

```
Console(config)#snmp-server contact Joe
Console(config)#
```

snmp-server location

システム設置場所情報の設定を行います。"no" **を前に置くことでシステム設置場所情報を削除します。**

文法

snmp-server location *text*

no snmp-server location

- *text* — **システム設置場所の解説（最大** 255 **文字）**

初期設定

なし

コマンドモード

Global Configuration

例

```
Console(config)#snmp-server location Room 23
Console(config)#
```

snmp-server host

SNMP メッセージを受け取るホストの指定を行います。"no" を前に置くことでホストを削除します。

文法

snmp-server host *host-addr* **inform** [**retry** *retries* **| timeout** *seconds* *community-string*] **version < 2c | 3 < auth | noauth | priv > >** { **udp-port** *port* }

no snmp-server host *host-addr*

- *host-addr* ― SNMP メッセージを受け取るホストのアドレス（最大 5 つのホストを設定できます）
- **inform** ― インフォームを使用（version2c と 3 でのみ使用可）
  - ー **retry** *retries* ー 再送を行う最大回数（0-255 回　初期設定：3 回）
  - ー **timeout** *seconds* ー 再送までの待ち時間（0-2147483647 センチセカンド　初期設定：1500 センチセカンド）
- *community-string* ― メッセージとともに送られるコミュニティ名。本コマンドでもコミュニティ名の設定が行えますが、"snmp-server community" コマンドを利用して設定することを推奨します（最大 32 文字）
- **version** ― トラップバージョンを指定します（範囲：v1,v2c,v3）

ー **auth | noauth |priv** ー v3 使用時に設定します。これらの認証 \ 暗号化オプションの詳細については P40 「SNMP」を参照してください。

- *port* ― トラップマネージャが使用する UDP ポートを指定（1-65535　初期設定：162）

初期設定

Host Address：なし

通知：トラップ

コマンドモード

Global Configuration

コマンド解説

- "snmp-server host" コマンドを使用しない場合は、SNMP メッセージは送信されません。SNMP メッセージの送信を行うためには必ず "snmp-server host" コマンドを使用し最低 1 つのホストを指定して下さい。複数のホストを設定する場合にはそれぞれに "snmp-server host" コマンドを使用してホストの設定を行って下さい。
- "snmp-server host" コマンドは "snmp-server enable traps" コマンドとともに使用されます。"snmp-server enable traps" コマンドではどのような SNMP メッセージを送信するか指定します。ホストが SNMP メッセージを受信するためには最低 1 つ以上の "snmp-server enable traps" コマンドと "snmp-server host" コマンドが指定されホストが有効になっている必要があります。
- 一部のメッセージタイプは "snmp-server enable traps" コマンドで指定することができず、メッセージは常に有効になります。

- スイッチは初期設定でトラップメッセージの通知を行いますが、トラップメッセージの受け取り側はスイッチへ応答を送りません。その為、十分な信頼性は確保できません。インフォームを使用することにより、重要情報がホストに受け取られるのを保証することが可能です。

[注意] インフォームを使用した場合、スイッチは応答を受け取るまでの間、情報をメモリ内に保持しなくてはならないため多くのシステムリソースを使用します。またインフォームはネットワークトラフィックにも影響を与えます。これらの影響を考慮した上で、トラップまたはトラップ通知の使用を決定してください。

- SNMPv3 ホストを指定している場合、トラップマネージャのコミュニティ名は、SNMP ユーザー名として解釈されます。SNMPv3 認証または暗号化オプションを使用している際には（authNoPriv または authPriv）、最初に P399 「snmp-server user」でユーザー名を定義してください。ユーザー名が定義されていない場合、認証パスワードおよびプライバシーパスワードが存在せず、スイッチはホストからのアクセスを許可しません。
尚、SNMPv3 ホストを no authentication（noAuth）として設定している場合には、SNMP ユーザーアカウントは自動的に生成されますので、スイッチはホストからのアクセスを許可します。

例

```
Console(config)#snmp-server host 10.1.19.23 batman
Console(config)#
```

関連するコマンド

snmp-server enable traps (P391)

snmp-server enable traps

SNMP のトラップメッセージの送信を有効化します。"no" を前に置くことで機能を無効にします。

文法

[no] snmp-server enable traps {authentication | link-up-down}

- **authentication** ― 認証時に不正なパスワードが送信された場合にトラップが発行されます
- **link-up-down** ― Link-up 又は Link-down 時にトラップが発行されます

初期設定

authentication 及び link-up-down トラップを通知

コマンドモード

Global Configuration

コマンド解説

- snmp-server enable traps" コマンドを使用しない場合、一切のメッセージは送信されません。SNMP メッセージを送信するためには最低 1 つの "snmp-server enable traps" コマンドを入力する必要があります。キーワードを入力せずにコマンドを入力した場合にはすべてのメッセージが有効となります。キーワードを入力した場合には、キーワードに関連するメッセージのみが有効となります。
- "snmp-server host" コマンドは "snmp-server enable traps" コマンドとともに使用されます。"snmp-server host" コマンドでは SNMP メッセージを受け取るホストを指定します。ホストが SNMP メッセージを受信するためには最低 1 つ以上の "snmp-server host" コマンドが指定されホストが有効になっている必要があります。

例

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

関連するコマンド

snmp-server host (P389)

snmp-server engine-id

エンジン ID の設定を行います。
エンジン ID はデバイス内のエージェントを固有に識別するためのものです。
"no" を前に置くことでエンジン ID を初期設定値に戻します。

文法

snmp-server engine-id < local | remote *IP Address* **>** *engine-id*
no snmp-server engine-id < local | remote *IP Address* **>**

- **local** ― スイッチ上の SNMP エンジンを指定
- **remote** ― リモートデバイス上の SNMP エンジンを指定
- *IP Address* ― リモートデバイスの IP アドレス
- *engine-id* ― エンジン ID

初期設定

スイッチの MAC アドレスを基に自動的に生成されます

コマンドモード

Global Configuration

コマンド解説

- SNMP エンジンはメッセージ再送、遅延およびダイレクションを防止します。エンジン ID はユーザパスワードと組み合わせて、SNMPv3 パケットの認証と暗号化を行うためのセキュリティキーを生成します。
- リモートエンジン ID は SNMPv3 インフォームを使用する際に必要です。（詳しくは P389 「snmp-server host」を参照してください）リモートエンジン ID は、リモートホストでユーザに送られた認証と暗号化パケットのセキュリティダイジェストを計算するために使用されます。SNMP パスワードは信頼できるエージェントのエンジン ID を使用してローカライズされます。インフォームの信頼できるエージェントはリモートエージェントです。したがってプロキシリクエストまたはインフォームを送信する前に、リモートエージェントの SNMP エンジン ID を変更を行う必要があります。
- ローカルエンジン ID はスイッチにたいして固有になるように自動的に生成されます。これをデフォルトエンジン ID とよびます。ローカルエンジン ID が削除または変更された場合、全ての SNMP ユーザーはクリアされます。そのため既存のユーザーの再構成を行う必要があります。

例

```
Console(config)#snmp-server engine-id local 123456789
onsole(config)#snmp-server engine-id remote 192.168.1.19 987654321
Console(config)#
```

show snmp engine-id

設定中の SNMP **エンジン** ID **を表示します**

文法

show snmp engine-id

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

Field	Description
Local SNMP engineID	**ローカルエンジン** ID **を表示**
Local SNMP engineBoots	**前回エンジン** ID **の設定が行われてから、エンジンの（再）初期化が行われた回数を表示**
Remote SNMP engineID	**リモートデバイスのエンジン** ID **を表示**
IP address	**リモートエンジンの** IP **アドレスを表示**

例

```
Console#show snmp engine-id
Local SNMP engineID: 8000002a8000000000e8666672
Local SNMP engineBoots: 1
Remote SNMP engineID                                IP address
80000000030004e2b316c54321                        192.168.1.19
Console#
```

関連するコマンド

snmp-server engine-ID (P392)

snmp-server view

このコマンドでは、ビューの追加を行います。"no" を前に置くことでビューを削除します。

文法

snmp-server view *view-name* {oid-tree}

no snmp-server view *view-name oid-tree*

- *view-name* — ビューの名前（1-32 文字）
- *oid-tree* — 参照可能にする MIB ツリーの OID。ストリングの特定の部分に、ワイルドカードを使用してマスクをかけることができます

初期設定

デフォルトビュー

コマンドモード

Global Configuration

コマンド解説

- 作成されたビューは、MIB ツリーの指定された範囲へのユーザアクセスを制限するために使用されます。
- デフォルトビューは全体の MIB ツリーへのアクセスを含みます。

例

MIB-2 を含む View を設定

```
Console(config)#snmp-server view mib-2 1.3.6.1.2.1 included
Console(config)#
```

MIB-2 インタフェーステーブル、ifDescr を含む View を設定。ワイルドカードは、このテーブル内のすべてのインデックス値を選択するのに使用されます。

```
Console(config)#snmp-server view ifEntry.2 1.3.6.1.2.1.2.2.1.*.2
  included
Console(config)#
```

MIB-2 インタフェーステーブルを含む View を設定。マスクはすべてのインデックスエントリーを選択します。

```
Console(config)#snmp-server view ifEntry.a 1.3.6.1.2.1.2.2.1.1.*
  included
Console(config)#
```

show snmp view

ビューを表示します。

文法

show snmp view

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

Field	Description
View Name	ビュー名
Subtree OID	参照可能な MIB ツリーの OID
View Type	OID で表示される MIB ノードがビューに含まれてるか（included）、含まれていないか（excluded）
Storage Type	このエントリーのストレージタイプ
Row Status	ビューの状態

例

```
Console#show snmp view
View Name: mib-2
Subtree OID: 1.2.2.3.6.2.1
View Type: included
Storage Type: nonvolatile
Row Status: active
View Name: defaultview
Subtree OID: 1
View Type: included
Storage Type: nonvolatile
Row Status: active
Console#
```

snmp-server group

SNMP グループ追加と、SNMP ユーザーのビューへのマッピングを行います。
"no" を前に置くことでグループを削除します。

文法

[no] snmp-server group *groupname* **< v1 | v2c | v3 < auth | noauth |priv> >**
{read *readview* | **write** *writeview* **| notify** *notify view* }

- *groupname* — SNMP グループ名（1-32 文字）
- **v1 | v2c | v3** — 使用する SNMP バージョンを選択します
- **ー auth | noauth |priv ー** v3 使用時に設定します。これらの認証 \ 暗号化オプションの詳細については P40 「SNMP」を参照してください。
- *readview* — Read アクセスのビューを設定します（1-32 文字）
- *writeview* — write アクセスのビューを設定します（1-32 文字）
- *notify view* — 通知ビューを設定します（1-32 文字）

初期設定

Default groups: public5 (read only), private6 (read/write)

readview - 全てのオブジェクトは Internet OID space (1.3.6.1) に属します

writeview - なし

notifyview - なし

コマンドモード

Global Configuration

コマンド解説

- SNMP グループは、所属するユーザーのアクセスポリシーを定義します。
- authentication が有効時は、「snmp-server user」で、MD5 または SHA どちらかの認証方式を選択してください。
- privacy が有効時は、DES56bit 暗号化方式が使用されます。
- 本機がサポートする通知メッセージの詳しい情報については P49 「SNMPv3 グループの設定」を参照してください。また、authentication, link-up および link-down のレガシートラップについては P391 「snmp-server enable traps」を参照してください。

例

```
Console(config)#snmp-server group r&d v3 auth write daily
Console(config)#
```

show snmp group

本機は 4 つのデフォルトグループを提供します。

- SNMPv1 read-only access
- read/write access
- SNMPv2c read-only access
- read/write access

文法

show snmp group

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

Field	Description
groupname	**グループ名**
security model	**セキュリティモデル**
readview	read **ビュー**
writeview	write **ビュー**
notifyview	**通知ビュー**
storage-type	**このエントリーのストレージタイプ**
Row Status	**ビューの状態**

例

```
Console#show snmp group
Group Name: public
Security Model: v1
Read View: defaultview
Write View: none
Notify View: none
Storage Type: volatile
Row Status: active

Group Name: public
Security Model: v2c
Read View: defaultview
Write View: none
Notify View: none
Storage Type: volatile
Row Status: active

Group Name: private
Security Model: v1
Read View: defaultview
Write View: defaultview
Notify View: none
Storage Type: volatile
Row Status: active

Group Name: private
Security Model: v2c
Read View: defaultview
Write View: defaultview
Notify View: none
Storage Type: volatile
Row Status: active

Console#
```

snmp-server user

SNMP ユーザーをグループへ追加します。"no" を前に置くことでユーザーをグループから除きます。

文法

snmp-server user *username groupname*
[remote *ip-address* **| v1 | v2c | v3 {auth <md5 | sha > |encrypted {auth < md5 | sha >}]**

no snmp-server user *username* **{ v1 | v2c | v3 | remote** *IP Address***s }**

- *username* — **ユーザー名**（1-32 **文字**）
- *groupname* — **グループ名**（1-32 **文字**）
- **remote** — **リモートデバイス上の** SNMP **エンジンを選択します**
- *ip-address* — **リモートデバイスの** IP **アドレス**
- **v1 | v2c | v3** — SNMP **バージョンの選択します**
- **auth** — **認証を使用します**
- **md5 | sha** — MD5 **または** SHA **認証を選択します**
- **encrypted** — **暗号化パスワード**

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- **リモートユーザーの設定を行う前に、「**snmp-server engine-id**」コマンドで、リモートエンジン** ID **の設定を行ってください。その後に「**snmp-server user**」を使用しユーザーと、ユーザーが所属するリモートデバイスの** IP **アドレスを設定してください。リモートエージェントのエンジン** ID **はユーザーのパスワードから認証 / プライバシーのダイジェストを計算するのに使用されます。**
- SNMP **パスワードは、信頼できるエージェントのエンジン** ID **を使用してローカライズされます。トラップ通知の信頼できる** SNMP **エージェントはリモートエージェントです。そのため、プロキシリクエストまたはトラップ通知を送信する前にリモートエージェントの** SNMP **エンジン** ID **を設定する必要があります。（詳しくは** P41 **「トラップマネージャ・トラップタイプの指定」および** P48 **「**SNMPv3 **リモートユーザーの設定」を参照してください）**

例

```
Console(config)#snmp-server user steve group r&d v3 auth md5 greenpeace
priv des56 einstien
Console(config)#snmp-server user mark group r&d remote 192.168.1.19 v3
auth md5 greenpeace priv des56 einstien
Console(config)#
```

show snmp user

SNMP ユーザー情報を表示します。

文法

show snmp user

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

Field	Description
EngineId	エンジン ID
User Name	ユーザー名
Authentication Protocol	認証プロトコル
Privacy Protocol	暗号化方式
storage-type	このエントリーのストレージタイプ
Row Status	ビューの状態
SNMP remote user	リモートデバイス上の SNMP エンジンに所属するユーザー

例

```
Console#show snmp user
EngineId: 0100000000000000000000000
User Name: steve
Authentication Protocol: md5
Privacy Protocol: des56
Storage Type: nonvolatile
Row Status: active
SNMP remote user
EngineId: 80000000030004e2b316c54321
User Name: mark
Authentication Protocol: mdt
Privacy Protocol: des56
Storage Type: nonvolatile
Row Status: active
Console#
```

4.11 インタフェース

コマンド	機能	モード	ページ
interface	本機の DHCP クライアント ID の指定	GC	P402
description	インタフェースタイプの設定及び interface configuration モードへの変更	IC	P403
speed-duplex	インタフェースの解説	IC	P404
negotiation	インタフェースへのオートネゴシエーションの設定	IC	P405
capabilities	オートネゴシエーション無効時の通信速度、通信方式の設定	IC	P406
flowcontrol	インタフェースへのフローコントロール設定	IC	P407
shutdown	インタフェースの無効	IC	P408
broadcast bit-rate	ブロードキャストストームコントロール閾値の設定	GC	P409
switchport broadcast	インタフェースでブロードキャストストームコントロールを有効	IC	P409
multicast bit-rate	マルチキャストストームコントロール閾値の設定	GC	P410
switchport multicast	インタフェースでマルチキャストストームコントロールを有効	IC	P410
unicast bit-rate	ユニキャストストームコントロール閾値の設定	GC	P411
switchport unicast	インタフェースでユニキャストストームコントロールを有効	IC	P411
clear counters	インタフェースの統計情報のクリア	PE	P412
show interfaces status	インタフェースの設定状況を表示	NE,PE	P413
show interfaces counters	インタフェースの統計情報の表示	NE,PE	P414
show interfaces switchport	インタフェースの管理、運用状況の表示	NE,PE	P415

interface

インタフェースの設定及び interface configuration **モードへの変更が行えます。**"no" **を前に置くことでトランクを解除することができます。**

文法

interface *interface*

no interface port-channel *channel-id*

- *interface*
  - **ethernet** *unit/port*
    - *unit* — **ユニット番号** "1"
    - *port* — **ポート番号（範囲：**1-26）
  - **port-channel** *channel-id* — Channel ID (1-12)
  - **vlan** *vlan-id* — VLAN ID (1-4094)

初期設定

なし

コマンドモード

Global Configuration

例

本例では 24 **番ポートの指定を行っています。**

```
Console(config)#interface ethernet 1/24
Console(config-if)#
```

description

各インタフェースの解説を行います。"no" **を前に置くことで解説を削除します。**

文法

description *string*

no description

- *string* ― **設定や監視作業を行いやすくするための各ポートの接続先などのコメントや解説（範囲：**1-31 **文字）**

初期設定

なし

コマンドモード

Interface Configuration (Ethernet, Port Channel)

例

本例は、24 **番ポートに解説を加えている設定です。**

```
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を無効にした場合の通信速度及び通信方式の設定が行えます。"no" **を前に置くことで初期設定に戻します。**

文法

speed-duplex　< 1000full | 100full | 100half | 10full 10half >

no speed-duplex

- **1000full** ― 1000 Mbps full-duplex **固定**
- **100full** ― 100 Mbps full-duplex **固定**
- **100half** ― 100 Mbps half-duplex **固定**
- **10full** ― 10 Mbps full-duplex **固定**
- **10half** ― 10 Mbps half-duplex **固定**

初期設定

- **初期設定ではオートネゴシエーションが有効になっています。**

コマンドモード

Interface Configuration (Ethernet、Port Channel)

コマンド解説

- **通信速度と** Duplex **を固定設定にするためには** "speed-duplex" **コマンドを使用します。又、**"no negotiation" **コマンドを使用しオートネゴシエーションを無効にして下さい。**
- "negotiation" **コマンドを使用しオートネゴシエーションが有効になっている場合は** "capabilities" **コマンドを使用することで最適な接続を行うことができます。オートネゴシエーション時の通信速度、通信方式の設定を行うためには** "capabilities" **コマンドを使用する必要があります。**

例

本例では 5 **番ポートに** 100Mbps half-duplex **固定の設定を行っています。**

```
Console(config)#interface ethernet 1/5
Console(config-if)#speed-duplex 100half
Console(config-if)#no negotiation
Console(config-if)#
```

関連するコマンド

negotiation (P405)

capabilities (P406)

negotiation

各ポートのオートネゴシエーションを有効にします。"no" **を前に置くことでオートネゴシエーションを無効にします。**

文法

negotiation

no negotiation

初期設定

有効 (Enabled)

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- **オートネゴシエーションが有効になっている場合、**"capabilities" **コマンドに指定された内容に基づき、最適な通信方法を選択します。オートネゴシエーションが無効の場合には** "speed-duplex" **コマンドと** "flowcontrol" **コマンドを使用して手動で通信方式を設定する必要があります。**

例

本例では 11 **番ポートをオートネゴシエーションの設定にしています。**

```
Console(config)#interface ethernet 1/11
Console(config-if)#negotiation
Console(config-if)#
```

関連するコマンド

capabilities (P406)

speed-duplex (P404)

capabilities

オートネゴシエーション時のポートの通信方式を設定します。

"no" **を前に置きパラメータを設定することで指定したパラメータの値を削除します。パラメータを設定せず** "no" **を前に置いた場合には初期設定に戻ります。**

文法

capabilities <1000full | 100full | 100half | 10full | 10half | flowcontrol | symmetric>

no port-capabilities <1000full | 100full | 100half |10full |10half | flowcontrol | symmetric>

- **1000full** ― 1000Mbps full-duplex **通信**
- **100full** ― 100Mbps full-duplex **通信**
- **100half** ― 100Mbps half-duplex **通信**
- **10full** ― 10Mbps full-duplex **通信**
- **10half** ― 10Mbps half-duplex **通信**
- **flowcontrol ― f**low control **サポート**
- **symmetric ― フローコントロールからポーズフレームを送受信（本機では**symmetric **ポーズフレームのみがサポートされています）。（ギガビット環境のみ）**

初期設定

- 100BASE-TX：10half, 10full, 100half, 100full
- 1000BASE-T：10half, 10full, 100half, 100full, 1000full
- SFP：1000full

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

"negotiation" **コマンドを使用しオートネゴシエーションが有効になっている場合、**"capabilites" **コマンドで指定された内容に基づき最適な通信方式でリンクを行います。オートネゴシエーションが無効の場合には** "speed-duplex" **コマンドと** "flowcontrol" **コマンドを使用して手動で通信方式を設定する必要があります。**

例

本例では 5 **番ポートに** 100half, 100full **及びフローコントロールを設定しています。**

```
Console(config)#interface ethernet 1/5
Console(config-if)#capabilities 100half
Console(config-if)#capabilities 100full
Console(config-if)#capabilities flowcontrol
Console(config-if)#
```

flow control

フローコントロールを有効にします。"no" を前に置くことでフローコントロールを無効にします。

文法

flowcontrol

no flowcontrol

初期設定

無効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- フローコントロールを使用するとスイッチのバッファ容量がいっぱいになった場合に通信のロスが発生するのを防ぐことができます。フローコントロールを有効にした場合、full-duplex では IEEE802.3x 準拠、half-duplex ではバックプレッシャを用いてフローコントロールを行います。"negotiation" コマンドを使用しオートネゴシエーションを有効にした場合、"capabilities" コマンドによりフローコントロールを使用するか決定されます。オートネゴシエーション時にフローコントロールを有効にするためには各ポートの機能 (Capabilities) に "flowcontrol" を含める必要があります。
- flowcontrol" コマンド又は "no flowcontrol" コマンドを使用してフローコントロールを固定設定する場合には、"no negotiation" コマンドを使用してオートネゴシエーションを無効にする必要があります。
- HUB と接続されたポートではフローコントロールを使用することは避けて下さい。使用した場合にはバックプレッシャのジャム信号が全体のネットワークパフォーマンスを低下させる可能性があります。

例

本例では 5 番ポートでフローコントロールを有効にしています。

```
Console(config)#interface ethernet 1/5
Console(config-if)#flowcontrol
Console(config-if)#no negotiation
Console(config-if)#
```

関連するコマンド

negotiation (P405)

capabilities (flowcontrol, symmetric) (P406)

shutdown

インタフェースを無効にします。"no" **を前に置くことでインタフェースを有効にします。**

文法

shutdown

no shutdown

初期設定

すべてのインタフェースが有効になっています。

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

コリジョンの発生などによる異常な動作を回避するなどの目的や、セキュリティの目的でポートを無効にすることができます。問題が解決した場合や、ポートを使用する場合には再度ポートを有効にすることができます。

例

本例では 5 **番ポートを無効にしています。**

```
Console(config)#interface ethernet 1/5
Console(config-if)#shutdown
Console(config-if)#
```

broadcast bit-rate

ブロードキャストストームコントロールの閾値を設定します。

文法

broadcast bit-rate *scale* **level** *level*

- *scale* — **閾値のスケール** (**範囲：**8 (8Kbits) 80 (80Kbits) 800 (800Kbits)800 (800Kbits))
- *level* — **しきい値のスケール** (**範囲：**1-127)

初期設定

Scale：8000 K
Level:：5

コマンドモード

Global Configuration

コマンド解説

- **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た場合、超えたパケットに関しては破棄されます。**
- **指定した閾値は、スイッチの全てのポートに適用されます。**

例

```
Console(config)#broadcast bit-rate 80 level 120
Console(config)#
```

switchport broadcast

指定したインタフェースで、ブロードキャストストームコントロールを有効にします。"no" **を前に置くことで無効にします。**

文法

switchport broadcast

no switchport broadcast

初期設定

全てのポートで有効

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- **選択したインタフェースで、ブロードキャストストームコントロールを有効または無効にしますが、**"broadcast bit-rate" **コマンドを使用して指定された閾値は、スイッチの全てのポートに適用されます。**

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#switchport broadcast
Console(config-if)#
```

multicast bit-rate

マルチキャストストームコントロールの閾値を設定します。

文法

multicast bit-rate *scale* **level** *level*

- *scale* — **閾値のスケール** (**範囲：**8 (8Kbits) 80 (80Kbits) 800 (800Kbits)800 (800Kbits))
- *level* — **しきい値のスケール** (**範囲：**1-127)

初期設定

Scale：8000 K
Level:：5

コマンドモード

Global Configuration

コマンド解説

- **マルチキャストトラフィックが指定したしきい値を超えた場合、超えたパケットに関しては破棄されます。**
- **指定した閾値は、スイッチの全てのポートに適用されます。**

例

```
Console(config)#multicast bit-rate 80 level 120
Console(config)#
```

switchport multicast

指定したインタフェースで、マルチキャストストームコントロールを有効にします。"no" **を前に置くことで無効にします。**

文法

switchport multicast

no switchport multicast

初期設定

全てのポートで有効

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- **選択したインタフェースで、マルチキャストストームコントロールを有効または無効にしますが、**"multicast bit-rate " **コマンドを使用して指定された閾値は、スイッチの全てのポートに適用されます。**

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#switchport multicast
Console(config-if)#
```

unicast bit-rate

ユニキャストストームコントロールの閾値を設定します。

文法

unicast bit-rate *scale* **level** *level*

- *scale* — **閾値のスケール** (**範囲：**8 (8Kbits) 80 (80Kbits) 800 (800Kbits)800 (800Kbits))
- *level* — **しきい値のスケール** (**範囲：**1-127)

初期設定

Scale：8000 K
Level:：5

コマンドモード

Global Configuration

コマンド解説

- **ユニキャストトラフィックが指定したしきい値を超えた場合、超えたパケットに関しては破棄されます。**
- **指定した閾値は、スイッチの全てのポートに適用されます。**

例

```
Console(config)#unicast bit-rate 80 level 120
Console(config)#
```

switchport unicast

指定したインタフェースで、ユニキャストストームコントロールを有効にします。"no" **を前に置くことで無効にします。**

文法

switchport unicast

no switchport unicast

初期設定

全てのポートで有効

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- **選択したインタフェースで、ブロードキャストストームコントロールを有効または無効にしますが、**"unicast bit-rate" **コマンドを使用して指定された閾値は、スイッチの全てのポートに適用されます。**

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#switchport unicast
Console(config-if)#
```

clear counters

インタフェースの統計情報をクリアします。

文法

clear counters *interface*

- *Interface*
  - **ethernet** *unit/port*
    - *unit* — **ユニット番号** ”1”
    - *port* — **ポート番号（範囲：**1-26）
  - **port-channel** channel-id (**範囲：**1-12)

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

統計情報は電源をリセットした場合のみ初期化されます。本機能を使用した場合、現在の管理セッションで表示されている統計情報はリセットされます。但し、一度ログアウトし再度管理画面にログインした場合には統計情報は最後に電源をリセットした時からの値となります。

例

本例では 5 **番ポートの統計情報をクリアしています。**

```
Console#clear counters ethernet 1/5
Console#
```

show interfaces status

インタフェースの状態を表示します。

文法

show interfaces status *interface*

- *interface*
  - **ethernet** *unit/port*
    - *unit* — **ユニット番号** "1"
    - *port* — **ポート番号（範囲：**1-26）
  - **port-channel** *channel-id*（**範囲：**1-12）

初期設定

すべてのインタフェースの状況が表示されます。

コマンドモード

Normal Exec, Privileged Exec

コマンド解説

- ポートを指定しない場合は、すべてのポートの状況が表示されます。
- 本コマンドを使用した際に表示される情報の詳細は P100 「接続状況の表示」を参照して下さい。

例

```
onsole#show interfaces status ethernet 1/10
Information of Eth 1/10
 Basic Information:
  Port Type:              100TX
  Mac Address:            00-17-2E-0F-72-8A
 Configuration:
  Name:
  Port Admin:             Up
  Speed-duplex:           Auto
  Capabilities:           10half, 10full, 100half, 100full
  Broadcast Storm:        Enabled
  Broadcast Storm Limit:  scale:80K level:120 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#
```

show interfaces counters

インタフェースの統計情報を表示します。

文法

show interfaces counters { *interface* }

- *interface*
  - **ethernet** *unit/port*
    - *unit* — **ユニット番号** ”1”
    - *port* — **ポート番号 （範囲：**1-26）
  - **port-channel** *channel-id*（**範囲：**1-12）

初期設定

すべてのポートのカウンタを表示します。

コマンドモード

Normal Exec, Privileged Exec

コマンド解説

- **ポートを指定しない場合は、すべてのポートの状況が表示されます。**
- **本コマンドを使用した際に表示される情報の詳細は** P2-75**「ポート統計情報の表示」を参照して下さい。**

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: 4, Packet size 256 to 511 octets:0
  Packet size 512 to 1023ctets:0,Packet size 1024 to 1518 octets: 0
Console#
```

show interfaces switchport

指定したポートの管理、運用状況を表示します。

文法

show interfaces switchport { *interface* }

- *interface*

  − **ethernet** *unit/port*
    − *unit* — **ユニット番号** "1"
    − *port* — **ポート番号（範囲：**1-26）
  − **port-channel** *channel-id*（**範囲：**1-12）

初期設定

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

例

本例は 10 **番ポートの情報を表示しています。**

```
Console#show interfaces switchport ethernet 1/10
Information of Eth 1/10
 Broadcast Threshold:           Enabled, scale:80K level:120 bits/second
 Multicast Threshold:           Enabled, scale:8K level:10 bits/second
 Unicast Threshold:            Enabled, scale:8000K level:1 bits/second
 LACP Status:                   Disabled
 Ingress Rate Limit:            Disabled, scale:8M level:10
  Egress Rate Limit:            Disabled, scale:8M level:10
 VLAN Membership Mode:          Hybrid
 Ingress Rule:                  Enabled
 Acceptable Frame Type:         All frames
 Native VLAN:                   1
 Priority for Untagged Traffic: 0
 GVRP Status:                   Disabled
 Allowed VLAN:                    1(u),4093(t),
 Forbidden VLAN:
 Private-VLAN Mode:             NONE
 Private-VLAN Mapping:          NONE
 802.1Q-tunnel Status:          Disable
 802.1Q-tunnel Mode:            NORMAL
 802.1Q-tunnel TPID:            8100(Hex)
Console#
```

コマンド解説

項目	解説
Broadcast threshold	ブロードキャストストーム制御機能の有効 / 無効の表示。有効時にはしきい値を表示（P409 参照）
multicast threshold	マルチキャストストーム制御機能の有効 / 無効の表示。有効時にはしきい値を表示（P410 参照）
unicast threshold	ユニキャストストーム制御機能の有効 / 無効の表示。有効時にはしきい値を表示（P411 参照）
Lacp status	LACP の有効 / 無効（P422 参照）
Ingress rate limit	入力帯域制御の有効 / 無効。現在の設定（P419 参照）
Egress rate limit	出力帯域制御の有効 / 無効。現在の設定（P419 参照）
VLAN membership mode	トランク又は Hybrid のメンバーモードを表示（P496 参照）
Ingress rule	イングレスフィルタの有効 / 無効の表示（P498 参照）
Acceptable frame type	VLAN フレームは、全てのフレームタイプか、タグフレームのみ受け取り可能か（P497 参照）
Native VLAN	デフォルトポート VLAN ID の表示（P499 参照）
Priority for untagged traffic	タグなしフレームへの初期設定のプライオリティの表示（P523 参照）
Gvrp status	GVRP の有効 / 無効（P488 参照）
Allowed Vlan	参加している VLAN の表示。"(u)" はタグなし、"(t)" はタグ（P500 参照）
Forbidden Vlan	GVRP によって動的に参加できない VLAN の表示（P502 参照）
Private VLAN mode	プライベート VLAN モードがホスト、無差別、なしのいずれなのか（P511 参照）
Private VLANhost-association	ポートが関連付けられているセカンダリ（コミュニティ）VLAN（P514 参照）
Private VLAN mapping	Private VLAN mapping 無差別ポートにマッピングされているプライマリ VLAN（P516 参照）

4.12 ポートミラーリング

ミラーセッションの設定方法を解説しています。

コマンド	機能	モード	ページ
port monitor	ミラーセッションの設定	IC	P417
show port monitor	ミラーポートの設定の表示	PE	P418

port monitor

ミラーセッションの設定を行います。"no" を前に置くことでミラーセッションをクリアします。

文法

port monitor *interface* { both | rx | tx }

no port monitor *interface*

- *interface* ー **ethernet** *unit/port* (source port)
  - ー *unit* ― ユニット番号　"1"
  - ー *port* ― ポート番号（範囲：1-26）
- both ― 送・受信両方のパケットをミラー
- rx ― 受信パケットのミラー
- tx ― 送信パケットのミラー

初期設定

なし

コマンドモード

Interface Configuration (Ethernet, destination port)

コマンド解説

- ソースポートからディスティネーションポートに通信をミラーし、リアルタイムでの通信分析を行えます。ディスティネイションポートにネットワーク解析装置（Sniffer 等) 又は RMON プローブを接続し、通信に影響を与えずにソースポートのトラフィックを解析することができます。
- ディスティネーションポートは Ethernet インタフェースに設定します。
- ソース及びディスティネーションポートの通信速度は同じ必要があります。同じ通信速度でない場合には通信がソースポートから落とされます。
- 単一のミラーセッションのみを作成することができます。
- ディスティネーションポートとソースポートは同一の VLAN に所属している必要があります。

例

本例では 6 番から 11 番ポートへのミラーを行います。

```
Console(config)#interface ethernet 1/11
Console(config-if)#port monitor ethernet 1/6 rx
Console(config-if)#
```

show port monitor

ミラー情報の表示を行います。

文法

show port monitor { *interface* }

- *interface*

  − **ethernet** *unit/port*

    − *unit* ― **ユニット番号** "1"

    − *port* ― **ポート番号（範囲：**1-26）

初期設定

すべてのセッションを表示

コマンドモード

Privileged Exec

コマンド解説

本コマンドを使用することで現在設定されているソースポート、ディスティネーションポート、ミラーモード (Both,RX, TX) **の表示を行います。**

例

本例では 6 **番から** 11 **番ポートへのミラーの設定が表示されています。**

```
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#
```

4.13 帯域制御

帯域制御機能では各インタフェースの送信及び受信の最大速度を設定することができます。帯域制御は各ポート / トランク毎に設定可能です。

帯域制御を有効にすると、通信はハードウェアにより監視され、設定を超える通信は破棄されます。設定範囲内の通信はそのまま転送されます。

コマンド	機能	モード	ページ
rate-limit	**ポートの入出力の最大帯域の設定**	IC	P419

rate-limit

特定のインタフェースの帯域制御レベルを設定します。帯域を設定せずに本コマンドを使用すると初期値が適用されます。"no" **を前に置くことで本機能を無効とします。**

文法

rate-limit < input | output > scale < 80K | 8M > level *level*

no rate-limit <input | output>

- **input** ― **入力帯域（レート）**
- **output** ― **出力帯域（レート）**
- **scale** ― **トラフィックレートリミットスケール（**80Kbits **または** 8Mbits**）**
- *level* ― **トラフィックレートリミットレベル（範囲：**1-99**）**

初期設定

入力 / 出力レートリミットステータス：無効

レートスケール：8M

レートレベル：10

コマンドモード

Interface Configuration (Ethernet)

例

```
Console(config-if)#rate-limit input scale 80K level 99
Console(config-if)#
```

[注意] TCP における入力に対しての帯域制御（Ingress Rate-Limit）はサポートしておりません。

4.14 リンクアグリゲーション

バンド幅拡張のため、又ネットワーク障害時の回避のため、ポートを束ねた静的グループを設定することができます。又、IEEE802.1ad 準拠の Link Aggregation Control Protocol (LACP) を使用し、本機と他のデバイス間のトランクを自動的に行うこともできます。静的トランクでは、本機は Cisco EtherChannel 標準との互換性があります。動的トランクに関しては IEEE802.1ad 準拠の LACP となります。

本機では最大 25 トランクグループをサポートします。

2 つの 1000Mbps ポートをトランクした場合、full duplex 時には最大 4Gpbs のバンド幅となります。

コマンド	機能	モード	ページ
Manual Configuration Commands			
interface port-channel	interface configuration モードへの移動とトランク設定	GC	P402
channel-group	トランクへのポートの追加	IC	P421
Dynamic Configuration Command			
lacp	現在のインタフェースでの LACP の設定	IC	P422
lacp system-priority	ポート LACP システムプライオリティの設定	IC (Ethernet)	P424
lacp admin-key	ポートアドミンキーの設定	IC (Ethernet)	P425
lacp admin-key	ポートチャンネルアドミンキーの設定	IC(Port Channel)	P426
lacp port-priority	LACP ポートプライオリティの設定	IC (Ethernet)	P427
Trunk Status Display Command			
show interfaces status port-channel	トランク情報の表示	NE,PE	P413
show lacp	LACP 関連情報の表示	PE	P428

トランク設定ガイドライン

- ループを防ぐため、ネットワークケーブルを接続する前にトランクの設定を完了させて下さい。
- 各トランクは最大 8 ポートまでトランク可能です。
- トランクの両端のポートはトランクポートとして設定される必要があります。
- トランクに参加するすべてのポートは、通信速度、duplex モード、フローコントロール、VLAN、CoS などすべて同一の設定である必要があります。
- port-channel を使用し VLAN からの移動、追加、削除する場合、トランクされたすべてのポートは１つのものとして扱われます。
- STP、VLAN および IGMP の設定は、指定したポートチャンネルを使用しすべてのトランクに設定することができます。

LACP 設定ガイドライン

ポートを同一ポートチャンネルに設定するには以下の条件に一致する必要があります。

- ポートは同一の LACP システムプライオリティの必要があります
- ポートは同一のポートアドミンキーの必要があります (Ethernet Interface)
- チャンネルグループが形成される場合に、ポートチャンネルアドミンキーをセットしなければ、このキーは、グループのインタフェースのポートアドミンキーと同一の値に設定されます。
- ポートチャンネルアドミンキーを設定する場合には、ポートアドミンキーはチャンネルグループへの参加が可能な同じ値を設定する必要があります。
- リンクが落ちた場合、LACP ポートプライオリティはバックアップリンクを選択します。

channel-group

トランクにポートを追加します。"no" を前に置くことでポートをトランクからはずします。

文法

channel-group *channel-id*

no channel-group

- *channel-id* — トランク ID（範囲：1-12）

初期設定

現在のポートがそのトランクに追加されます。

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- 静的トランクの設定を行う場合、対向のスイッチは Cisco EtherChannel 標準と互換性がなくてはいけません。
- " no channel-group" コマンドを使うことでポートグループをトランクからはずします。
- " no interfaces port-channel" コマンドを使うことでスイッチからトランクを削除します。

例

本例では、trunk 1 を生成し、11 番ポートをメンバーに加えています。

```
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

IEEE802.3ad 準拠の LACP を現在のインタフェースに対して設定します。"no" を前に置くことで本機能を無効にします。

文法

lacp

no lacp

初期設定

無効 (Disabled)

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- LACP トランクの両端は固定設定もしくはオートネゴシエーションにより full duplex に設定されている必要があります。
- LACP を使用したトランクは自動的に使用可能なポートチャンネル ID を割り当てられます。
- 対向のスイッチも接続するポートで LACP を有効にしている場合、トランクは自動的に有効になります。
- 8 つ以上のポートが同じ対向のスイッチに接続されて、LACP が有効になっている場合、追加されるポートはスタンバイモードとなり、他のアクティブなリンクが落ちた場合にのみ有効となります。

例

本例では、11 から 13 番ポートの LACP を有効にしています。"show interfaces status port-channel 1" コマンドを使用し、Trunk1 が対向の機器と確立されていることを確認することができます。

```
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:               00-00-e8-00-00-0b
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 **システムプライオリティの設定を行います。**"no" **を前に置くことで初期設定に戻します。**

文法

lacp {actor | partner} system-priority *priority*

no lacp {actor | partner} system-priority

- **actor** ― **リンクアグリゲーションのローカル側**
- **partner** ― **リンクアグリゲーションのリモート側**
- *priority* ― **プライオリティは、リンクアグリゲーショングループ** (LAG) **メンバーシップを決定し、又** LAG **接続時に他のスイッチが本機を識別するために使用します（範囲：**0-65535）

初期設定

32768

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- **同一** LAG **に参加するポートは同一システムプライオリティに設定する必要があります。**
- **システムプライオリティは本機の** MAC **アドレスと結合し** LAG ID **となります。**ID **は他のシステムとの** LACP **接続時の特定の** LAG **を表すために使用されます。**
- **リモート側のリンクが確立されると、**LACP **運用設定は使用されている状態です。パートナーの** LACP **設定は運用状態ではなく管理状態を表し、今後** LACP **がパートナーと確立される際に使用されます。**

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor system-priority 3
Console(config-if)#
```

lacp admin-key（Ethernet Interface）

ポートの LACP **アドミニストレーションキーの設定を行います。**"no" **を前に置くことで初期設定に戻します。**

文法

lacp {actor | partner} admin-key *key*

no lacp {actor | partner} admin-key

- **actor** ― **リンクアグリゲーションのローカル側**
- **partner** ― **リンクアグリゲーションのリモート側**
- *key* ― **ポートアドミンキーは同じ** LAG **のポートが同一の値を設定する必要があります（範囲：**0-65535）

初期設定

0

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- **同じ** LAG **に参加するには、**LACP **システムプライオリティが一致し、**LACP **ポートアドミンキーが一致し、**LACP **ポートチャンネルキーが一致した場合となります。**
- **ポートチャンネルアドミンキーを設定する場合には、ポートアドミンキーはチャンネルグループへの参加が可能な同じ値を設定する必要があります。**
- **リモート側のリンクが確立されると、**LACP **運用設定は使用されている状態です。パートナーの** LACP **設定は運用状態ではなく管理状態を表し、今後** LACP **がパートナーと確立される際に使用されます。**

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor admin-key 120
Console(config-if)#
```

lacp admin-key（Port Channel）

ポートチャンネル LACP アドミニストレーションキーの設定を行います。"no" を前に置くことで初期設定に戻します。

文法

lacp admin-key *key*

no lacp admin-key

- *key* ― ポートアドミンキーは同じ LAG のポートが同一の値を設定する必要があります（範囲：0-65535）

初期設定

0

コマンドモード

Interface Configuration (Port Channel)

コマンド解説

- 同じ LAG に参加するには、LACP システムプライオリティが一致し、LACP ポートアドミンキーが一致し、LACP ポートチャンネルアドミンキーが一致した場合となります。
- チャンネルグループが形成され、ポートチャンネルアドミンキーが設定されていない場合、ポートアドミンキーと同一の値に設定されます。LAG がポートチャンネルアドミンキーを使用しない場合には 0 にリセットされます。

例

```
Console(config)#interface port-channel 1
Console(config-if)#lacp admin-key 3
Console(config-if)#
```

lacp port-priority

LACP ポートプライオリティの設定を行います。"no" を前に置くことで初期設定に戻します。

文法

lacp {actor | partner} port-priority *priority*

no lacp {actor | partner} port-priority

- **actor** — リンクアグリゲーションのローカル側
- **partner** — リンクアグリゲーションのリモート側
- *priority* — バックアップリンクに使用する LACP ポートプライオリティ（範囲：0-65535）

初期設定

32768

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- 低い値が高いプライオリティを示します。
- アクティブなポートがダウンした場合、高いプライオリティを持ったポートがバックアップとなります。複数のポートが同じプライオリティの場合には低いポート番号のポートがバックアップリンクとなります。
- リモート側のリンクが確立されると、LACP 運用設定は使用されている状態です。パートナーの LACP 設定は運用状態ではなく管理状態を表し、今後 LACP がパートナーと確立される際に使用されます。

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor port-priority 128
```

show lacp

LACP 情報の表示を行います。

文法

show lacp [*port-channel* **| counters | internal | neighbors | sysid]**

- *port-channel* ― **リンクアグリゲーショングループ** ID（**範囲：**1-8）
- **counters** ― LACP **プロトコルメッセージの統計情報**
- **internal** ― **ローカルサイドの運用状況と設定情報**
- **neighbors** ― **リモートサイドの運用状況と設定情報**
- **sysid** ― **すべてのチャンネルグループの** MAC **アドレスとシステムプライオリティのサマリ**

初期設定

Port Channel：**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
```

項目	解説
LACPDUs Sent	チャンネルグループから送信された有効な LACPDU の数
LACPDUs Received	チャンネルグループが受信した有効な LACPDU の数
Marker Sent	本チャンネルグループから送信された有効な Marker PDU の数
Marker Received	本チャンネルグループが受信した有効な Marker PDU の数
LACPDUs Unknown Pkts	以下のフレームの受信数 (1) スロープロトコル・イーサネット・タイプ値を運び、未知の PDU を含んでいるフレーム (2) スロープロトコルグループ MAC アドレスに属し、スロープロトコル・イーサネット・タイプ値を運んでいないフレーム
LACPDUs Illegal Pkts	不正な PDU 又はプロトコルサブタイプが不正な値を含むスロープロトコルイーサネットパケットを運ぶフレーム数

例

```
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
```

項目	解説
Oper Key	現在のアグリゲーションポートのキーの運用値
Admin Key	現在のアグリゲーションポートのキーの管理値
LACPDUs Internal	受信した LACPDU 情報を無効にするまでの秒数
LACP System Priority	本ポートチャンネルに割り当てられた LACP システムプライオリティ
LACP Port Priority	本ポートチャンネルグループに割り当てられた LACP ポートプライオリティ

Admin State, Oper State	Actor の管理値又は運用値の状態のパラメータ。 •Expired ― Actor の受信機器は失効状態です •Defaulted ― Actor の受信機器は初期設定の運用 partner の情報を使用しています •Distributing ― 誤りの場合、このリンク上の出力フレームの配信は無効になります。配信は現在無効状態で、受信プロトコル情報の管理上の変更、又は変更がない状態で有効にはなりません。 •Collecting ― このリンク上の入力フレームの収集は可能な状態です。収集は現在可能な状態で、受信プロトコル情報の管理上の変化、又は変化がない状態で無効にはなりません。 •Synchronization ― システムはリンクを IN_SYNC と認識します。それにより正しいリンクアグリゲーショングループに属すことができます。グループは互換性のある Aggregator に関係します。リンクアグリゲーショングループの ID はシステム ID と送信されたオペレーショナルキー情報から形成されます。 •Aggregation ― システムは、アグリゲーション可能なリンクと認識しています。アグリゲーションの存在的な候補です。 •Long timeout ― LACPDU の周期的な送信にスロー転送レートを使用します。 •LACP-Activity ― 本リンクに関するアクティブコントロール値（0：Passive、1：Active）

例

```
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, 00-00-00-00-00-01
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
```

項目	解説
Partner Admin System ID	ユーザにより指定された LAG partner のシステム ID
Partner Oper System ID	LACP プロトコルにより指定された LAG partner のシステム ID
Partner Admin Port Number	プロトコル partner 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 partner によりアグリゲーションポートに指定された運用ポート番号
Port Admin Priority	プロトコル partner のポートプライオリティの現在の管理値
Port Oper Priority	partner により指定された本アグリゲーションポートのプライオリティ
Admin Key	プロトコル partner のキーの現在の管理値
Oper Key	プロトコル partner のキーの現在の運用値
Admin State	partner のパラメータの管理値（前の表を参照）
Oper State	partner のパラメータの運用値（前の表を参照）

例

```
Console#show lacp sysid
Port Channel     System Priority     System MAC Address
-------------------------------------------------------------------
             1                  32768      00-30-F1-D3-26-00
             2                  32768      00-30-F1-D3-26-00
             3                  32768      00-30-F1-D3-26-00
             4                  32768      00-30-F1-D3-26-00
Console#
```

項目	解説
Channel group	本機のリンクアグリゲーショングループ設定
System Priority*	本チャンネルグループの LACP システムプライオリティ
System MAC Address*	システム MAC アドレス

*LACP system priority 及び system MAC address は LAG システム ID 形成します。

4.15 アドレステーブル

MAC アドレステーブルに対するアドレスフィルタリング、現在エントリーされているアドレスの表示、テーブルのクリア、エージングタイムの設定を行います。

コマンド	機能	モード	ページ
mac-address-table static	VLAN ポートへの MAC アドレスの静的なマッピング	GC	P432
clear mac-address-table dynamic	転送データベースに学習された情報の削除	PE	P433
show mac-address-table	転送データベースに登録された情報の表示	PE	P434
mac-address-table aging-time	アドレステーブルのエージングタイムの設定	GC	P435
show mac-address-table aging-time	アドレステーブルのエージングタイムの表示	PE	P435

mac-address-table static

VLAN のポートに静的に MAC アドレスをマッピングします。"no" を前に置くことで MAC アドレスを削除します。

文法

mac-address-table static *mac-address* **interface** *interface* **vlan** *vlan-id* [*action*]

no mac-address-table static *mac-address* **vlan** *vlan-id*

- *mac-address* — MAC アドレス
- *interface*
  - **ethernet** *unit/port*
    - *unit* — ユニット番号　"1"
    - *port* — ポート番号（範囲：1-26）
- **port-channel** *channel-id*（範囲：1-12）
- **vlan** *vlan-id* — VLAN ID (1-4094)
- *action*
  - **delete-on-reset** — 本機が再起動されるまで登録されます。
  - **permanent** — 永久に登録されます。

初期設定

mac-address：なし

action：permanent

コマンドモード

Global Configuration

コマンド解説

静的アドレスは特定の VLAN の特定のポートに割り当てることができます。本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することができます。静的アドレスは以下の特性を持っています。

- インタフェースのリンクがダウンしても、静的アドレスはアドレステーブルから削除されません。
- 静的アドレスは指定したインタフェースに固定され、他のインタフェースに移動することはありません。静的アドレスが他のインタフェースに現れた場合、アドレスは拒否されアドレステーブルに記録されません。
- 静的アドレスは "no" コマンドを使って削除するまで、他のポートで学習されません。

例

```
Console(config)#mac-address-table static 00-e0-29-94-34-de
 interface ethernet 1/1 vlan 1 delete-on-reset
Console(config)#
```

clear mac-address-table dynamic

転送データベース上に登録してあるすべての MAC アドレスを削除します。また、すべての送受信情報を削除します。

初期設定

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に登録されている情報を表示します。

文法

show mac-address-table count

show mac-address-table multicast {igmp-snooping | user | vlan [*vlan-id*] }

show mac-address-table address *mac-address* { **interface** *interface* | **vlan** *vlan-id* } {**sort** < **address** | **vlan | interface** >}

- **count** ― MAC **アドレスのカウントを表示**
- **multicast** ― **認知のマルチキャストアドレス**
  - igmp-snooping ― IGMP **スヌーピングで学習されたエントリ**
  - user ― **ユーザによって設定されたマルチキャストエントリ**
  - vlan ― VLAN ID
- *mac-address* ― MAC **アドレス**
- *mask* ― **アドレス内のビット数**
- *interface*
  - **ethernet** *unit/port*
    - *unit* ― **ユニット番号** ”1”
    - *port* ― **ポート番号（範囲：**1-26）
- **port-channel** *channel-id*（**範囲：**1-12）
- *vlan-id* ― VLAN ID (1-4094)
- **sort** ― **アドレス、**VLAN**、インタフェースによる並び替え**

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

例

```
Console#show mac-address-table
  Interface    Mac Address           Vlan  Type
  ---------    -----------------    ----  -----------------
   Eth 1/1      00-00-E8-49-5E-DC     1   Delete-on-reset
   Trunk 2      00-E0-29-8F-AA-1B     1   Learned
Console#
```

mac-address-table aging-time

アドレステーブルのエージングタイムを設定します。"no" を前に置くことで初期設定に戻します。

文法

mac-address-table aging-time *seconds*

no mac-address-table aging-time

- *seconds* - 秒数を設定します (10-98301 の値。0 に設定した場合はエージングを無効にします)

初期設定

300（秒）

コマンドモード

Global Configuration

コマンド解説

エージングタイムは動的転送情報を本機に保持する時間を表します。

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ージングタイムを表示します。

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#show mac-address-table aging-time
 Aging time: 100 sec.
Console#
```

4.16 LLDP コマンド

Link Layer Discovery Protocol（LLDP）はローカルブロードキャストドメインの中の接続デバイスについての基本的な情報を発見するために使用します。LLDP はレイヤ 2 のプロトコルであり、デバイスについての情報を周期的なブロードキャストで伝達します。伝達された情報は IEEE802.1ab に従って Type Length Value（TLV）で表され、そこにはデバイス自身の識別情報、能力、設定情報の詳細が含まれています。また LLDP は発見した近隣のネットワークノードについて集められた情報の保存方法と管理方法を定義します。

Link Layer Discovery Protocol - Media Endpoint Discovery（LLDP-MED）は VoIP やスイッチのようなエンドポイントのデバイスを管理するための拡張された LLDP です。LLDP-MED の TLV はネットワークポリシー、電力、インベントリ、デバイスのロケーションの詳細情報を伝達します。LLDP と LLDP-MED の情報は、トラブルシューティングの簡易化、ネットワーク管理の改善、間違いのないネットワークトポロジーを維持するため、SNMP アプリケーションによって使用することができます。

コマンド	機能	モード	ページ
lldp	スイッチで LLDP を有効	GC	P437
lldp holdtime-multiplier	TTL(time-to-live) 値の設定	GC	P438
lldp med-fast-start-count	medFastStart の数を設定	GC	P439
lldp notification-interval	LLDP の変更に関する SNMP 通知送信の間隔を設定	GC	P439
lldp refresh-interval	LLDP 配信の転送間隔を設定	GC	P440
lldp reinit-delay	LLDP ポートが無効またはリンクダウン時の再初期化までの待ち時間を設定	GC	P440
lldp tx-delay	ローカル LLDP MIB の変数に変化が起こった後に、アドバタイズメントを送信するまでの時間を設定します	GC	P441
lldp admin-status	LLDP メッセージの送信・受信のモードを有効	IC	P441
lldp notification	LLDP と LLDP-MED の変更について SNMP トラップ通知の送信を有効	IC	P442
lldp med-notification	LLDP-MED の変更について SNMP トラップ通知の送信を有効	IC	P442
lldp basic-tlv management-ip-address	TLV Type “management-ip-address“ を設定	IC	P443
lldp basic-tlv port-description	TLV Type “port-description“ を設定	IC	P443
lldp basic-tlv system-capabilities	TLV Type “system-capabilities“ を設定	IC	P444
lldp basic-tlv system-description	TLV Type “system-description“ を設定	IC	P445
lldp basic-tlv system-name	TLV Type “system-name“ を設定	IC	P446
lldp dot1-tlv proto-ident	lldp dot1-TLV“ proto-ident“ を設定	IC	P447
lldp dot1-tlv proto-vid	lldp dot1-TLV“ proto-vid“ を設定	IC	P447
lldp dot1-tlv pvid	lldp dot1-TLV“pvid“ を設定	IC	P448
lldp dot1-tlv vlan-name	lldp dot1-TLV“vlan-name“ を設定	IC	P449
lldp dot3-tlv link-agg	lldp dot3-TLV“link-agg“ を設定	IC	P450
lldp dot3-tlv mac-phy	lldp dot3-TLV“mac-phy“ を設定	IC	P451

lldp dot3-tlv max-frame	lldp dot3-TLV“max-frame“ を設定	IC	P452
lldp dot3-tlv poe	lldp dot3-TLV“poe“ を設定	IC	P453
lldp med-tlv extPoe	MED TLV Type“extpoe“ を設定	IC	P454
lldp med-tlv inventory	MED TLV Type“ inventory“ を設定	IC	P455
lldp med-tlv location	MED TLV Type“location“ を設定	IC	P455
lldp med-tlv med-cap	MED TLV Type“med-cap“ を設定	IC	P456
lldp med-tlv network-policy	MED TLV Type“network-policy“ を設定	IC	P456
show lldp config	LLDP 設定の表示	PE	P457
show lldp info local-device	LLDP ローカルデバイス情報を表示	PE	P459
show lldp info remote-device	LLDP リモートデバイス情報を表示	PE	P460
show lldp info statistics	LLDP 統計情報を表示	PE	P461

lldp

スイッチで LLDP を有効にします。"no" を前に置くことで機能を無効にします。

文法

lldp

no lldp

初期設定

有効

コマンドモード

Global Configuration

例

```
Console(config)#lldp
Console(config)#
```

lldp holdtime-multiplier

LLDP のアドバタイズメントで送信された Time-To-Live（TTL）値を設定します。"no" を前に置くことで設定を初期状態に戻します。

文法

lldp holdtime-multiplier *value*

no lldp holdtime-multiplier

- *value* - TTL 値を設定します。TTL は秒で表され、下の数式で計算します。
  Transmission Interval × Hold Time Multiplier ≦ 65536
  （範囲：2 － 10　初期設定：4）

初期設定

Holdtime multiplier：4

TTL：4 × 30 = 120 秒

コマンドモード

Global Configuration

コマンド解説

TTL は、タイムリーな方法でアップデートが送信されない場合、送信した LLDP エージェントに関係のあるすべての情報をどのくらいの期間維持するかを受信した LLDP エージェントに伝達します。TTL は秒で表され、下の数式で計算します。

Transmission Interval × Hold Time Multiplier ≦ 65536

つまり上の式からデフォルトの TTL は下のようになります。

30 × 4 ＝ 120

例

```
Console(config)#lldp holdtime-multiplier 10
Console(config)#
```

medFastStartCount

LLDP-MED Fast Start メカニズムのアクティベーションプロセスの間に送信する LLDP MED Fast Start LLDPDU の数を設定します。

文法

lldp medfaststartcount *packets*

- *packets* - パケット数（範囲：1-10 パケット　初期設定：4 パケット）

初期設定

4 パケット

コマンドモード

Global Configuration

例

```
Console(config)#lldp medfaststartcount 6
Console(config)#
```

lldp notification-interval

LLDP MIB の変更を行い、SNMP 通知が送信されるまでの時間を設定します。"no" を前に置くことで設定を初期状態に戻します。

文法

lldp notification-interval *seconds*

no lldp notification-interval

- *seconds* - SNMP 通知が送られる周期的な間隔を指定します
  （範囲：5 ～ 3600 秒　初期設定 5 秒）

初期設定

5 秒

コマンドモード

Global Configuration

例

```
Console(config)#lldp notification-interval 30
Console(config)#
```

lldp refresh-interval

LLDP アドバタイズが送信されるまでの間隔を設定します。"no" を前に置くことで設定を初期状態に戻します。

文法

lldp refresh-interval *seconds*

no lldp refresh-delay

- *seconds* - LLDP アドバタイズが送信されるまでの間隔を指定します（範囲：5 ～ 32768 秒　初期設定 5 秒）

初期設定

30 秒

コマンドモード

Global Configuration

コマンド解説

refresh-interval × Hold Time Multiplier ≦ 65536

例

```
Console(config)#lldp refresh-interval 60
Console(config)#
```

lldp reinit-delay

LLDP ポートが無効になるかリンクダウンした後、再初期化を試みるまでの時間を設定します。"no" を前に置くことで設定を初期状態に戻します。

文法

lldp reinit-delay *seconds*

no lldp reinit-delay

- *seconds* - 再初期化を試みるまでの時間を指定します（範囲：1-10 秒　初期設定 2 秒）

初期設定

2 秒

コマンドモード

Global Configuration

例

```
Console(config)#lldp reinit-delay 10
Console(config)#
```

lldp tx-delay

ローカル LLDP MIB **の変数に変化が起こった後に引き続き、アドバタイズメントを送信するまでの時間を設定します。**"no" **を前に置くことで設定を初期状態に戻します。**

文法

lldp tx-delay *seconds*

no lldp tx-delay

- *seconds* - **アドバタイズメントを送信するまでの時間を設定を指定します（範囲：**1-8192 **秒）**

初期設定

2 **秒**

コマンドモード

Global Configuration

例

```
Console(config)#lldp tx-delay 10
Console(config)#
```

lldp admin-status

個別のインターフェースに対し、メッセージの内容を指定するために LLDP **ポート・トランクの設定を行います。**"no" **を前に置くことでこの機能を無効にします。**

文法

lldp admin-status < rx-only | tx-only | tx-rx >

no lldp admin-status

- **rx-only** - LLDP PDUs. **受信のみ**
- **tx-only** - LLDP PDUs. **送信のみ**
- **tx-rx** - LLDP PDUs. **送受信**

初期設定

tx-rx

コマンドモード

Interface Configuration (Ethernet, Port Channel)

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp admin-status rx-only
Console(config-if)#
```

lldp notification

LLDP 変更について SNMP トラップ通知の送信を可能にします。"no" を前に置くことでこの機能を無効にします。

文法

lldp notification

no lldp notification

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp notification
Console(config-if)#
```

lldp med-notification

LLDP -MED 変更について SNMP トラップ通知の送信を可能にします。"no" を前に置くことでこの機能を無効にします。

文法

lldp med-notification

no lldp med-notification

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp med-notification
Console(config-if)#
```

lldp basic-tlv management-ip-address

LLDP 有効ポートで "management-ip-address ” のアドバタイズを行います。"no" を前に置くことで機能を無効にします。

文法

lldp basic-tlv management-ip-address

no lldp basic-tlv management-ip-address

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

management-ip-address には、スイッチの IPv4 アドレスが含まれます。スイッチに管理用のアドレスがない場合、アドレスはスイッチの CPU の MAC アドレスが、このアドバタイズメントを送信するポートの MAC アドレスになります。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv management-ip-address
Console(config-if)#
```

lldp basic-tlv port-description

LLDP 有効ポートで "port-description ” のアドバタイズを行います。"no" を前に置くことで機能を無効にします。

文法

lldp basic-tlv port-description

no lldp basic-tlv port-description

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

port-description には、RFC2863 の ifDescr オブジェクトで規定されています。これには製造者、スイッチの製品名、インターフェースのハードウェアとソフトウェアのバージョンが含まれます。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv port-description
Console(config-if)#
```

lldp basic-tlv system-capabilities

LLDP 有効ポートで "system-capabilities ” のアドバタイズを行います。"no" を前に置くことで機能を無効にします。

文法

lldp basic-tlv system-capabilities

no lldp basic-tlv system-capabilities

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

system-capabilities には、システムの主な機能が含まれます。この情報には機能自体が有効かどうかは関係ありません。この TLV によってアドバタイズされる情報は IEEE802.1AB 規格に記述されています。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv system-capabilities
Console(config-if)#
```

lldp basic-tlv system-description

LLDP 有効ポートで "system-description ” のアドバタイズを行います。"no" を前に置くことで機能を無効にします。

文法

lldp basic-tlv system-description

no lldp basic-tlv system-description

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

system-description は RFC3418 の sysDescr オブジェクトで規定されています。システムのハードウェア、オペレーティングソフト、ネットワーキングソフトのフルネームとバージョンが含まれています。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv system-description
Console(config-if)#
```

lldp basic-tlv system-name

LLDP 有効ポートで "system-name ” のアドバタイズを行います。"no" を前に置くことで機能を無効にします。

文法

lldp basic-tlv system-name

no lldp basic-tlv system-name

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

System-name は RFC3418 の sysName オブジェクトで規定されています。システムの管理用に割り当てられた名前が含まれます。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv system-name
Console(config-if)#
```

lldp dot1-tlv proto-ident

LLDP 有効ポートで "proto-ident ” のアドバタイズを行います。"no" を前に置くことで機能を無効にします。

文法

lldp dot1-tlv proto-ident

no lldp dot1-tlv proto-ident

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

このインタフェースを通して、アクセス可能なプロトコルの情報をアドバタイズします。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot1-tlv proto-ident
Console(config-if)#
```

lldp dot1-tlv proto-vid

LLDP 有効ポートで "proto-vid ” のアドバタイズを行います。"no" を前に置くことで機能を無効にします。

文法

lldp dot1-tlv proto-vid

no lldp dot1-tlv proto-vid

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

ポートベースおよびプロトコルベース VLAN 情報をアドバタイズします。
詳細については P495 「VLAN インタフェースの設定」および P518 「プロトコル VLAN の設定」を参照してください。

例

```
Console(config)#inter ethernet 1/1
Console(config-if)#no lldp dot1-tlv proto-vid
Console(config-if)#
```

lldp dot1-tlv pvid

LLDP 有効ポートで "pvid ” のアドバタイズを行います。"no" を前に置くことで機能を無効にします。

文法

lldp dot1-tlv pvid

no lldp dot1-tlv pvid

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

PVID 情報をアドバタイズします。
詳細については P499 「switchport native vlan」を参照してください。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot1-tlv pvid
Console(config-if)#
```

lldp dot1-tlv vlan-name

LLDP 有効ポートで "vlan-name ” のアドバタイズを行います。"no" を前に置くことで機能を無効にします。

文法

lldp dot1-tlv vlan-name

no lldp dot1-tlv vlan-name

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

指定したインタフェースが割り当てられた、全ての VLAN **名をアドバタイズします。**
VLAN **については** P500 **「**switchport allowed vlan**」および** P519 **「**protocol-vlan protocol-group (Configuring Groups)**」を参照してください。**

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot1-tlv vlan-name
Console(config-if)#
```

lldp dot3-tlv link-agg

LLDP 有効ポートで "link-agg" のアドバタイズを行います。"no" を前に置くことで機能を無効にします。

文法

lldp dot3-tlv link-agg

no lldp dot3-tlv link-agg

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

リンクのアグリゲーションステータスをアドバタイズします。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot3-tlv link-agg
Console(config-if)#
```

lldp dot3-tlv mac-phy

LLDP 有効ポートで "mac-phy" のアドバタイズを行います。"no" を前に置くことで機能を無効にします。

文法

lldp dot3-tlv mac-phy

no lldp dot3-tlv mac-phy

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

MAC/PHY 設定およびステータスをアドバタイズします。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot3-tlv mac-phy
Console(config-if)#
```

lldp dot3-tlv max-frame

LLDP 有効ポートで "max-frame ” のアドバタイズを行います。"no" を前に置くことで機能を無効にします。

文法

lldp dot3-tlv max-frame

no lldp dot3-tlv max-frame

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

最大フレームサイズ情報をアドバタイズします。フレームサイズについての詳細は P311 **「フレームサイズコマンド」を参照してください。**

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp dot3-tlv max-frame
Console(config-if)#
```

lldp dot3-tlv poe

LLDP 有効ポートで "poe ” のアドバタイズを行います。"no" を前に置くことで機能を無効にします。

文法

lldp dot3-tlv poe

no lldp dot3-tlv poe

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

デバイスが PoE **機能をサポートしているか否か、サポートしている場合には、**PoE **に関する情報をアドバタイズします。**

[注意] 本機は PoE 機能をサポートしていません。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp dot3-tlv poe
Console(config-if)#
```

lldp med-tlv extPoe

LLDP 有効ポートで "extpoe ” のアドバタイズを行います。"no" を前に置くことで機能を無効にします。

文法

lldp med-tlv extPoe

no lldp med-tlv extPoe

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

拡張された PoE（Power over Ethernet）**についての詳細情報をアドバタイズします。この情報にはスイッチから利用できる電力供給源、スイッチの電力状態、スイッチが主電源もしくはバックアップ電源のどちらで動作しているかが含まれます。**

[注意] 本機は PoE 機能をサポートしていません。

例

```
Console(config)#interface ethernet 1/10
Console(config-if)#lldp med-tlv extPoe
Console(config-if)#
```

lldp med-tlv inventory

LLDP 有効ポートで "inventory ” のアドバタイズを行います。"no" を前に置くことで機能を無効にします。

文法

lldp med-tlv inventory

no lldp med-tlv inventory

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

製造者、モデル、ソフトウェアのバージョン、その他適切な情報などデバイスの詳細情報をアドバタイズします。

例

```
Console(config)#interface ethernet 1/10
Console(config-if)#lldp med-tlv inventory
Console(config-if)#
```

lldp med-tlv location

LLDP 有効ポートで " location ” のアドバタイズを行います。"no" を前に置くことで機能を無効にします。

文法

lldp med-tlv location

no lldp med-tlv location

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

所在地情報をアドバタイズします。

例

```
Console(config)#interface ethernet 1/10
Console(config-if)#lldp med-tlv location
Console(config-if)#
```

lldp med-tlv med-cap

LLDP 有効ポートで "med-cap ” のアドバタイズを行います。"no" を前に置くことで機能を無効にします。

文法

lldp med-tlv med-cap

no lldp med-tlv med-cap

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

LLDP-MED TVL キャパビリティのアドバタイズを行います。

例

```
Console(config)#interface ethernet 1/10
Console(config-if)#lldp med-tlv med-cap
Console(config-if)#
```

lldp med-tlv network-policy

LLDP 有効ポートで "network-policy ” のアドバタイズを行います。"no" を前に置くことで機能を無効にします。

文法

lldp med-tlv network-policy

no lldp med-tlv network-policy

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

ネットワークポリシー設定情報のアドバタイズを行います。
この情報はポートの VLAN 設定ミスの発見や分析の役に立ちます。妥当でないネットワークポリシーは音声品質の低下やサービスの破綻に頻繁につながります。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp med-tlv network-policy
Console(config-if)#
```

show lldp config

全てのポートの LLDP **設定を表示します。**

文法

show lldp config [detail *interface***]**

- **detail** ― **設定サマリを表示**
- *interface*
  - **ethernet** *unit/port*
    - *unit* ― **ユニット番号** ”1”
    - *port* ― **ポート番号（範囲：**1-26）
  - **port-channel** *channel-id*（**範囲：**1-12）

コマンドモード

Privileged Exec

例

```
Console#show lldp config

LLDP Global Configuation
 LLDP Enable                 : Yes
 LLDP Transmit interval      : 32768
 LLDP Hold Time Multiplier   : 4
 LLDP Delay Interval         : 2
 LLDP Reinit Delay           : 2
 LLDP Notification Interval  : 5
 LLDP MED fast start counts  : 4
LLDP Port Configuration
 Port       AdminStatus NotificationEnabled
 -------- + ----------- -------------------
 Eth 1/1  | Tx-Rx       True
 Eth 1/2  | Tx-Rx       True
 Eth 1/3  | Tx-Rx       True
 Eth 1/4  | Tx-Rx       True
 Eth 1/5  | Tx-Rx       True...
Console#show lldp config detail ethernet 1/10
LLDP Port Configuration Detail
 Port : Eth 1/10
 Admin Status : Tx-Rx
 Notification Enabled : True
 Basic TLVs Advertised:
   port-description
   system-name
   system-description
   system-capabilities
   management-ip-address
 802.1 specific TLVs Advertised:
  *port-vid
  *vlan-name
  *proto-vlan
  *proto-ident
 802.3 specific TLVs Advertised:
  *mac-phy
  *poe
  *link-agg
  *max-frame
 MED Configuration:
 MED Notification Enabled : True
 MED Enabled TLVs Advertised:
  *med-cap
 *network-policy
 *location
 *extPoe
 *inventory

Console#
```

show lldp info local-device

スイッチについての情報を表示します。

文法

show lldp info local-device [detail *interface***]**

- **detail** ― **詳細情報を表示**
- *interface*
  - **ethernet** *unit/port*
    - *unit* ― **ユニット番号** ”1”
    - *port* ― **ポート番号（範囲：**1-26）
  - **port-channel** *channel-id*（**範囲：**1-12）

コマンドモード

Privileged Exec

例

```
Console#show lldp info local-device
LLDP Local System Information
Chassis Type : MAC Address
Chassis ID : 00-01-02-03-04-05
System Name :
System Description : 24PORT GIGABIT L2 INTELLIGENT SWITCH
System Capabilities Support : Bridge
System Capabilities Enable : Bridge
Management Address : 192.168.0.101 (IPv4)
LLDP Port Information
Interface |PortID Type PortID PortDesc
--------- + ---------------- ----------------- -------------------------
--
Eth 1/1 |MAC Address 00-01-02-03-04-06 Ethernet Port on unit 1, port 1
Eth 1/2 |MAC Address 00-01-02-03-04-07 Ethernet Port on unit 1, port 2
Eth 1/3 |MAC Address 00-01-02-03-04-08 Ethernet Port on unit 1, port 3
Eth 1/4 |MAC Address 00-01-02-2-03-04-09 Ethernet Port on unit 1, port 4
...
Console#show lldp info local-device detail ethernet 1/1
LLDP Port Information Detail
Port : Eth 1/1
Port Type : MAC Address
Port ID : 00-01-02-03-04-06
Port Desc : Ethernet Port on unit 1, port 1
Console#
```

show lldp info remote-device

ローカルスイッチの指定されたポートに接続された、LLDP が有効のデバイスについての詳細情報を表示します。

文法

show lldp info remote-device [detail *interface***]**

- **detail** ― **詳細情報を表示**
- *interface*
  - **ethernet** *unit/port*
    - *unit* ― **ユニット番号** ”1”
    - *port* ― **ポート番号（範囲：**1-26）
  - **port-channel** *channel-id*（**範囲：**1-12）

コマンドモード

Privileged Exec

例

```
Console#show lldp info remote-device
LLDP Remote Devices Information
Interface | ChassisId PortId SysName
--------- + ----------------- ----------------- ---------------------
Eth 1/1 | 00-01-02-03-04-05 00-01-02-03-04-06
Console#show lldp info remote-device detail ethernet 1/1
LLDP Remote Devices Information Detail
---------------------------------------------------------------
Local PortName : Eth 1/1
Chassis Type : MAC Address
Chassis Id : 00-01-02-03-04-05
PortID Type : MAC Address
PortID : 00-01-02-03-04-06
SysName :
SysDescr : 24PORT GIGABIT L2 INTELLIGENT SWITCH
PortDescr : Ethernet Port on unit 1, port 1
SystemCapSupported : Bridge
SystemCapEnabled : Bridge
Remote Management Address :
00-01-02-03-04-05 (MAC Address)
Console#
```

show lldp info statistics

このスイッチに接続されている LLDP **が有効なすべてのデバイスの統計を表示します。**

文法

show lldp info statistics [detail *interface***]**

- **detail** ― **詳細情報を表示**
- *interface*
  - **ethernet** *unit/port*
    - *unit* ― **ユニット番号** ”1”
    - *port* ― **ポート番号（範囲：**1-26）
  - **port-channel** *channel-id*（**範囲：**1-12）

コマンドモード

Privileged Exec

例

```
Console#show lldp info statistics

 LLDP Device Statistics

  Neighbor Entries List Last Updated : 0 seconds
  New Neighbor Entries Count         : 0
  Neighbor Entries Deleted Count     : 0
  Neighbor Entries Dropped Count     : 0
  Neighbor Entries Ageout Count      : 0

  Port   | NumFramesRecvd NumFramesSent NumFramesDiscarded
  ------ + -------------- ------------- ------------------
  1      | 0              0             0
  2      | 0              0             0
  3      | 0              0             0
  4      | 0              0             0
  5      | 0              0             0 ...

Console#show lldp info statistics detail ethernet 1/10
 LLDP Port Statistics Detail
  PortName           : Eth 1/10
  Frames Discarded   : 0
  Frames Invalid     : 0
  Frames Received    : 0
  Frames Sent        : 0
  TLVs Unrecognized  : 0
  TLVs Discarded     : 0
  Neighbor Ageouts   : 0

Console#
```

4.17 スパニングツリー

本機へのスパニングツリーアルゴリズム (Spanning Tree Algorithm/STA) **の設定と、選択したインタフェースへの** STA **の設定を行うコマンドです。**

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の有効化**	GC	P463
spanning-tree mode	STP/RSTP/MSTP **モードの選択**	GC	P464
spanning-tree forward-time	**スパニングツリーブリッジ転送時間の設定**	GC	P465
spanning-tree hello-time	**スパニングツリーブリッジハロー時間の設定**	GC	P466
spanning-tree max-age	**スパニングツリーブリッジ最長時間の設定**	GC	P467
spanning-tree priority	**スパニングツリーブリッジプライオリティの設定**	GC	P468
spanning-tree path-cost method	RSTP/MSTP **のパスコスト方法の設定**	GC	P469
spanning-tree transmission-limit	RSTP/MSTP **の送信リミットの設定**	GC	P470
spanning-tree-mst-configuration	MSTP **設定モードの変更**	GC	P470
mst vlan	**スパニングツリーインスタンスへの** VLAN **の追加**	MST	P471
mst priority	**スパニングツリーインスタンスのプライオリティの設定**	MST	P472
name	MST **名の設定**	MST	P473
revision	MST **リビジョンナンバーの設定**	MST	P474
max-hops	BPDU **が破棄される前最大ホップ数の設定**	MST	P475
spanning-tree spanning-disabled	**インタフェースのスパニングツリーの無効化**	IC	P475
spanning-tree cost	**各インタフェースのスパニングツリーのパスコスト設定**	IC	P476
spanning-tree port-priority	**各インタフェースのスパニングツリーのプライオリティ設定**	IC	P477
spanning-tree edge-port	**エッジポートへのポートファストの有効化**	IC	P478
spanning-tree portfast	**インタフェースのポートファストの設定**	IC	P479
spanning-tree link-type	RSTP/MSTP **のリンクタイプを設定**	IC	P480
spanning-tree mst cost	MST **インスタンスのパスコストの設定**	IC	P481
spanning-tree mst port-priority	MST **インスタンスプライオリティの設定**	IC	P482
spanning-tree protocol-migration	**適切な** BPDU **フォーマットの再確認**	PE	P483
show spanning-tree	**スパニングツリーの設定を表示**	PE	P484
show spanning-tree mst configuration	MST **設定の表示**	PE	P486

spanning-tree

本機に対して STA を有効に設定します。"no" を前に置くことで機能を無効にします。

文法

spanning-tree

no spanning-tree

初期設定

STA 有効

コマンドモード

Global Configuration

コマンド解説

STA はネットワークのループを防ぎつつブリッジ、スイッチ及びルータ間のバックアップリンクを提供します。STA 機能を有するスイッチ、ブリッジ及びルータ間で互いに連携し、各機器間のリンクで 1 つのルートがアクティブになるようにします。また、別途バックアップ用のリンクを提供し、メインのリンクがダウンした場合には自動的にバックアップを行います。

例

本例では STA を有効にしています。

```
Console(config)#spanning-tree
Console(config)#
```

spanning-tree mode

STP のモードを設定します。"no" を前に置くことで初期設定に戻します。

文法

spanning-tree mode < stp | rstp | mstp >

no spanning-tree mode

- **stp** ― Spanning Tree Protocol（IEEE 802.1D 準拠）
- **rstp** ― Rapid Spanning Tree Protocol（IEEE 802.1w 準拠）
- **mstp**― mstp - Multiple Spanning Tree（IEEE 802.1s 準拠）

初期設定

rstp

コマンドモード

Global Configuration

コマンド解説

- Spanning Tree Protocol(STP)
  スイッチ内部では RSTP を用いますが、外部へは IEEE802.1D 準拠の BPDU の送信のみを行います。
- Rapid Spanning Tree Protocol(RSTP)
  RSTP は以下の入ってくるメッセージの種類を判断し STP 及び RSTP のいずれにも自動的に対応することができます。
  - STP Mode ― ポートの移行遅延タイマーが切れた後に IEEE802.1D BPDU を受け取ると、本機は IEEE802.1D ブリッジと接続していると判断し、IEEE802.1D BPDU のみを使用します。
  - RSTP Mode ― IEEE802.1D BPDU を使用し、ポートの移行遅延タイマーが切れた後に RSTP BPDU を受け取ると、RSTP は移行遅延タイマーを再スタートさせ、そのポートに対し RSTP BPDU を使用します。
- Multiple Spanning Tree Protocol(MSTP)
  - ネットワーク上で MSTP を有効にするには、接続された関連するブリッジにおいても同様の MSTP の設定を行ない、スパニングツリーインスタンスに参加することを許可する必要があります。
  - スパニングツリーインスタンスは、互換性を持つ VLAN インスタンスを持つブリッジにのみ設定可能です。
  - スパニングツリーモードを変更する場合、変更前のモードのスパニングツリーインスタンスをすべて止め、その後新しいモードにおいて通信を再開します。スパニングツリーのモード変更時には通信が一時的に遮断されるので注意して下さい。

例

本例では RSTP を使用する設定をしています。

```
Console(config)#spanning-tree mode rstp
Console(config)#
```

spanning-tree forward-time

スパニングツリー転送遅延時間を本機すべてのインタフェースに設定します。"no" **を前に置くことで初期設定に戻します。**

文法

spanning-tree forward-time *seconds*

no spanning-tree forward-time

- *seconds* ― **秒数（範囲：**4-30 **秒）**
  最小値は 4 **又は** [(max-age / 2) + 1] **のどちらか小さい方となります。**

初期設定

15**（秒）**

コマンドモード

Global Configuration

コマンド解説

ルートデバイスがステータスを変更するまでの最大時間を設定することができます。各デバイスがフレームの転送をはじめる前にトポロジー変更を受け取るために遅延時間が必要です。また、各ポートの競合する情報を受信し、廃棄するためにも時間が必要となります。そうしなければ一時的にでも、データのループが発生します。

例

```
Console(config)#spanning-tree forward-time 20
Console(config)#
```

spanning-tree hello-time

スパニングツリー Hello **タイムを設定します。**"no" **を前に置くことで初期設定に戻します。**

文法

spanning-tree hello-time *time*

no spanning-tree hello-time

- *time* ― **秒数（範囲：**1-10 **秒）**
  最大値は 10 **または** [(max-age / 2) -1] **の小さい方となります。**

初期設定

2**（秒）**

コマンドモード

Global Configuration

コマンド解説

設定情報の送信を行う間隔を設定するためのコマンドです。

例

```
Console(config)#spanning-tree hello-time 5
Console(config)#
```

spanning-tree max-age

スパニングツリーの最大エージングタイムを設定します。"no" **を前に置くことで初期設定に戻します。**

文法

spanning-tree max-age *seconds*

no spanning-tree max-age

- *seconds* ― **秒（範囲：**6-40 **秒）**
  最小値は 6 **又は** [2 x (hello-time + 1)] **のどちらか大きい値です。**
  最大値は 40 **又は** [2 x (forward-time - 1)] **のどちらか小さい値です。**

初期設定

20**（秒）**

コマンドモード

Global Configuration

コマンド解説

設定変更を行う前に設定情報を受け取るまでの最大待ち時間（秒）。

指定ポートを除くすべてのポートが設定情報を一定の間隔で受け取ります。タイムアウトした STP **ポートは付属する** LAN **のための指定ポートになります。そのポートがルートポートの場合、ネットワークに接続された他のポートがルートポートとして選択されます。**

例

```
Console(config)#spanning-tree max-age 40
Console(config)#
```

spanning-tree priority

本機全体に対してスパニングツリーのプライオリティの設定を行います。"no" **を前に置くことで初期設定に戻します。**

文法

spanning-tree priority *priority*

no spanning-tree priority

- *priority* — **ブリッジの優先順位**
  (0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440)

初期設定

32768

コマンドモード

Global Configuration

コマンド解説

プライオリティはルートデバイス、ルートポート、指定ポートを決定する際に使用されます。一番高いプライオリティを持ったデバイスが STA **ルートデバイスとなります。すべてのデバイスが同じプライオリティの場合、**MAC **アドレスが一番小さいデバイスがルートデバイスとなります。**

例

```
Console(config)#spanning-tree priority 40960
Console(config)#
```

spanning-tree pathcost method

RSTP のパスコストを設定します。"no" を前に置くことで初期設定に戻します。

文法

spanning-tree pathcost method < long | short >

no spanning-tree pathcost method

- **long** — 0-200,000,000 までの 32 ビットの値
- **short** — 0-65535 までの 16 ビットの値

初期設定

long

コマンドモード

Global Configuration

コマンド解説

パスコストはデバイス間の最適なパスを決定するために使用されます。速度の速いポートに対し小さい値を設定し、速度の遅いポートに対し大きな値を設定します。pathcost は port priority よりも優先されます。

例

```
Console(config)#spanning-tree pathcost method long
Console(config)#
```

spanning-tree transmission-limit

RSTP BPDU の最小送信間隔を設定します。"no" を前に置くことで初期設定に戻します。

文法

spanning-tree transmission-limit *count*

no spanning-tree transmission-limit

- *count* ― 転送リミットの秒数（範囲：1-10 秒）

初期設定

3

コマンドモード

Global Configuration

コマンド解説

本コマンドでは BPDU の最大転送レートを制限します。

例

```
Console(config)#spanning-tree transmission-limit 4
Console(config)#
```

spanning-tree mst configuration

MST 設定モードに移行します。

初期設定

- MST インスタンスに VLAN がマッピングされていません
- リジョン名は本機の MAC アドレスです

コマンドモード

Global Configuration

例

```
Console(config)#spanning-tree mst configuration
Console(config-mstp)#
```

関連するコマンド

mst vlan (P471)
mst priority (P472)
name (P473)
revision (P474)
max-hops (P475)

mst vlan

スパニングツリーインスタンスに VLAN を追加します。"no" を前に置くことで特定の VLAN を削除します。VLAN を指定しない場合にはすべての VLAN を削除します。

文法

mst *instance_id* **vlan** *vlan-range*

no mst *instance_id* **vlan** *vlan-range*

- *instance_id* ― MST インスタンス ID（範囲：0-4094）
- *vlan-range* ― VLAN 範囲（範囲：1-4094）

初期設定

なし

コマンドモード

MST Configuration

コマンド解説

- 本コマンドによりスパニングツリーに VLAN をグループ化します。MSTP は各インスタンスに対し特定のスパニングツリーを生成します。これによりネットワーク上に複数のパスを構築し、通信のロードバランスを行い、単一のインスタンスに不具合が発生した場合に大規模なネットワークの障害が発生することを回避すると共に、不具合の発生したインスタンスの新しいトポロジーへの変更を迅速に行ないます。
- 初期設定では、MST リジョン内のすべてのブリッジと LAN に接続されたすべての VLAN が内部スパニングツリー (MSTI 0) に割り当てられています。本機では最大 58 のインスタンスをサポートしています。但し、同一インスタンスのセットにより同一 MSTI 内のすべてのブリッジ、及び同一 VLAN のセットにより同一インスタンスを形成する必要があります。RSTP は単一ノードとして各 MSTI を扱い、すべての MSTI を Common Spanning Tree として接続する点に注意して下さい。

[注意] MST の設定を行う際には、事前に spanning-tree mode を mstp に選択してください。（P464 「spanning-tree mode」を参照）

例

```
Console(config-mstp)#mst 1 vlan 2-5
Console(config-mstp)#
```

mst priority

スパニングツリーインスタンスのプライオリティを設定します。"no" **を前に置くことで初期設定に戻します。**

文法

mst *instance_id* **priority** *priority*

no mst *instance_id* **priority**

- *instance_id* ― MST **インスタンス** ID**（範囲：**0-4094**）**
- *priority* ― MST **インスタンスのプライオリティ**
  (0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440)

初期設定

32768

コマンドモード

MST Configuration

コマンド解説

- MST **プライオリティはルートデバイス、特定のインスタンスの代理ブリッジの決定に使用されます。一番高いプライオリティを持ったデバイスが** MSTI **ルートデバイスとなります。すべてのデバイスが同じプライオリティの場合、**MAC **アドレスが一番小さいデバイスがルートデバイスとなります。**
- **プライオリティを** 0 **に設定することにより本機を** MSTI **のルートデバイスに、**16384 **に設定することにより代理デバイスに設定できます。**

例

```
Console(config-mstp)#mst 1 priority 4096
Console(config-mstp)#
```

name

本機の設置されている MST リジョン名の設定を行ないます。"no" を前に置くことで名前を削除します。

文法

name *name*

- *name* — スパニングツリー名 (31 文字以内)

初期設定

本機の MAC アドレス

コマンドモード

MST Configuration

コマンド解説

MST リジョン名とリビジョンナンバーは唯一の MST リジョンを指定するために使用されます。(本機のようなスパニングツリー対応機器である) ブリッジは 1 つの MST リジョンにのみ属すことができます。同じリジョン内のすべてのブリッジはすべて同じ MST インスタンスの設定をする必要があります。

例

```
Console(config-mstp)#name R&D
Console(config-mstp)#
```

関連するコマンド

revision (P474)

revision

本機の MST 設定のリビジョンナンバーの設定を行ないます。"no" を前に置くことで初期設定に戻ります。

文法

revision *number*

- *number* — スパニングツリーのリビジョンナンバー（範囲：0-65535）

初期設定

0

コマンドモード

MST Configuration

コマンド解説

MST リジョン名とリビジョンナンバーは唯一の MST リジョンを指定するために使用されます。（本機のようなスパニングツリー対応機器である）ブリッジは 1 つの MST リジョンにのみ属すことができます。同じリジョン内のすべてのブリッジはすべて同じ MST インスタンスの設定をする必要があります。

例

```
Console(config-mstp)#revision 1
Console(config-mstp)#
```

関連するコマンド

name (P473)

max-hops

BPDU が破棄される前の MST 内での最大ホップ数を設定します。"no" を前に置くことで初期設定に戻ります。

文法

max-hops *hop-number*

- *hop-number* — MST の最大ホップ数（設定範囲：1-40）

初期設定

20

コマンドモード

MST Configuration

コマンド解説

MSTI リジョンは STP と RSTP プロトコルでは単一のノードとして扱われます。従って MSTI リジョン内の BPDU のメッセージエイジは変更されません。しかし、リジョン内の各スパニングツリーインスタンス及びインスタンスを接続する内部スパニングツリー (IST) は、BPDU を広げるためブリッジの最大数を指定するために hop カウントを使用します。各ブリッジは BPDU を渡す前に hop カウントを 1 つ減らします。hop カウントが 0 になった場合にはメッセージは破棄されます。

例

```
Console(config-mstp)#max-hops 30
Console(config-mstp)#
```

spanning-tree spanning-disabled

特定のポートの STA を無効にします。"no" を前に置くことで再び STA を有効にします。

文法

spanning-tree spanning-disabled

no spanning-tree spanning-disabled

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

例

5 番ポートの STA を無効にしています。

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree spanning-disabled
Console(config-if)#
```

spanning-tree cost

各ポートの STA **パスコストを設定します。**"no" **を前に置くことで初期設定に戻します。**

文法

spanning-tree cost *cost*

no spanning-tree cost

- *cost* ― **インタフェースへのパスコストの値（範囲：**1-200,000,000)

推奨する値は以下の通りです。

- Ethernet (10Mbps): 200,000-20,000,000
- Fast Ethernet (100Mbps): 20,000-2,000,000
- Gigabit Ethernet (1Gbps): 2,000-200,000

初期設定

- Ethernet ― half duplex: 2,000,000、full duplex: 1,000,000、**トランク** : 500,000
- Fast Ethernet ― half duplex: 200,000、full duplex: 100,000、**トランク** : 50,000
- Gigabit Ethernet ― full duplex: 10,000、**トランク** : 5,000

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- **本コマンドはデバイス間の** STA **のパスを最適に決定するためのコマンドです。従って、速度の速いポートに対し小さい値を設定し、速度の遅いポートに対し大きな値を設定します。**
- **パスコストはポートプライオリティより優先されます。**
- STP **パスコストが** "short" **に設定されている場合には最大値が** 65,535 **となります。**

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree cost 5000
Console(config-if)#
```

spanning-tree port-priority

指定ポートのプライオリティを設定します。"no" **を前に置くことで初期設定に戻します。**

文法

spanning-tree port-priority *priority*

no spanning-tree port-priority

- *priority* — **ポートの優先順位（範囲：**16 **間隔で** 0-240 **の値）**

初期設定

128

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- STP **に使用するポートの優先順位を指定するためのコマンドです。もし、すべてのポートのパスコストが同じ場合には、高い優先順位（低い設定値）のポートが** STP **のアクティブリンクとなります。**
- 1 **つ以上のポートに最優先順位が割り当てられる場合、ポート番号の低いポートが有効となります。**

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree port-priority 128
Console(config-if)#
```

関連するコマンド

spanning-tree cost (P476)

spanning-tree edge-port

エッジに対するポートを指定します。"no" **を前に置くことで初期設定に戻します。**

文法

spanning-tree edge-port

no spanning-tree edge-port

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- **本コマンドは選択したポートに対しファストスパニングツリーモードの設定を行います。このモードでは、ポートは学習ステートをパスして、フォワーディングを行います。エンドノードではループを発生しないため、スパニングツリーステートの変更を通常よりも早く行うことができます。ファストフォワーディングは、エンドノードのサーバ、ワークステーションに対し** STP **によるタイムアウトを軽減します。(ファストフォワーディングは** LAN **のエンドノードのデバイス又は** LAN **のエンドのブリッジに接続されたポートにのみ有効にして下さい。)**
- **本コマンドは** "spanning-tree portfast" **コマンドと同一の機能です。**

例

```
Console(config)#interface ethernet ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#
```

関連するコマンド

spanning-tree portfast (P479)

spanning-tree portfast

ポートをポートファストに指定します。"no" **を前に置くことで本機能を無効にします。**

文法

spanning-tree portfast

no spanning-tree portfast

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- **本コマンドは選択したポートに対しファストスパニングツリーモードの設定を行います。このモードでは、ポートは学習ステートをパスして、フォワーディングを行います。**
- **エンドノードではループを発生しないため、スパニングツリーステートの変更を通常よりも早く行うことができます。ファストフォワーディングは、エンドノードのサーバ、ワークステーションに対し** STP **によるタイムアウトを軽減します（ファストフォワーディングは** LAN **のエンドノードのデバイス又は** LAN **のエンドのブリッジに接続されたポートにのみ有効にして下さい）**
- **本コマンドは** "spanning-tree edge-port" **コマンドと同じ機能を有します。本コマンドは旧製品との互換性を保つために用意されており、将来のファームウェアでは使用できなくなる可能性があります。**

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree portfast
Console(config-if)#
```

関連するコマンド

spanning-tree edge-port (P478)

spanning-tree link-type

RSTP のリンクタイプを設定します。"no" を前に置くことで初期設定に戻します。

文法

spanning-tree link-type < auto | point-to-point | shared >

no spanning-tree link-type

- **auto** — duplex モードの設定から自動的に設定
- **point-to-point** — point to point リンク
- **shared** — シェアードミディアム

初期設定

auto

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- ポートが対向のブリッジにのみ接続されている場合は point-to-point リンクを、複数のブリッジに接続されている場合には shared を選択します。
- 自動検知が選択されている場合、リンクタイプは duplex モードから選択されます。Full-duplex のポートでは point-to-point リンクが、half-duplex ポートでは、shared リンクが自動的に選択されます。
- RSTP は 2 つのブリッジ間の point-to-point リンクでのみ機能します。指定されたポートが shared リンクの場合には RSTP は許可されません。

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree link-type point-to-point
```

spanning-tree mst cost

MST インスタンスのパスコストの設定を行ないます。"no" を前に置くことで初期設定に戻します。

文法

spanning-tree mst *instance_id* **cost** *cost*

no spanning-tree mst *instance_id* **cost**

- *instance_id* — MST インスタンス ID（範囲：0-4094）
- *cost* — インタフェースへのパスコストの値 (1-200,000,000)
  推奨する値は以下の通りです。
  - Ethernet (10Mbps): 200,000-20,000,000
  - Fast Ethernet (100Mbps): 20,000-2,000,000
  - Gigabit Ethernet (1Gbps): 2,000-200,000

初期設定

- Ethernet — half duplex: 2,000,000、full duplex: 1,000,000、トランク : 500,000
- Fast Ethernet — half duplex: 200,000、full duplex: 100,000、トランク : 50,000
- Gigabit Ethernet — full duplex: 10,000、トランク : 5,000

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- 各スパニングツリーインスタンスは VLAN ID に関連付けられます。
- 本コマンドはデバイス間の MSTA のパスを最適に決定するためのコマンドです。従って、速度の速いポートに対し小さい値を設定し、速度の遅いポートに対し大きな値を設定します。
- パスコストはインタフェースプライオリティより優先されます。

例

```
Console(config)#interface ethernet ethernet 1/5
Console(config-if)#spanning-tree mst 1 cost 50
Console(config-if)#
```

関連するコマンド

spanning-tree mst port-priority (P482)

spanning-tree mst port-priority

MST インスタンスのインタフェースプライオリティの設定を行ないます。"no" を前に置くことで初期設定に戻ります。

文法

spanning-tree mst *instance_id* **port-priority** *priority*

no spanning-tree mst *instance_id port-priority*

- *instance_id* — MST インスタンス ID（範囲：0-4094）
- *priority* — ポートの優先順位（16 間隔で 0-240 の値）

初期設定

128

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- MST に使用するインタフェースの優先順位を指定するためのコマンドです。もし、すべてのポートのパスコストが同じ場合には、高い優先順位（低い設定値）のポートが STP のアクティブリンクとなります。
- 複数のポートに最優先順位が割り当てられる場合、ポート番号の低いポートが有効となります。

例

```
Console(config)#interface ethernet ethernet 1/5
Console(config-if)#spanning-tree mst 1 port-priority 0
Console(config-if)#
```

関連するコマンド

spanning-tree mst cost (P481)

spanning-tree protocol-migration

選択したポートに送信する適切な BPDU **フォーマットを再確認します。**

文法

spanning-tree protocol-migration *interface*

- *interface*
  - **ethernet** *unit/port*
    - *unit* ― **ユニット番号** ”1”
    - *port* ― **ポート番号（範囲：**1-26）
  - **port-channel** *channel-id*（**範囲：**1-12）

コマンドモード

Privileged Exec

コマンド解説

本機が設定、トポロジーチェンジ BPDU **を含む** STP BPDU **を検知した場合、該当するポートは自動的に** STP **互換モードにセットされます。**"spanning-tree protocol-migration" **コマンドを使用し、手動で選択したポートに対して最適な** BPDU **フォーマット（**RSTP **又は** STP **互換）の再確認を行うことができます。**

例

```
Console#spanning-tree protocol-migration ethernet 1/5
Console#
```

show spanning-tree

STP の設定内容を表示します。

文法

show spanning-tree

show spanning-tree ethernet *unit / port*

show spanning-tree port-channel *channel-id*

show spanning-tree mst *instance-id*

- **ethernet** *unit / port*
  - *unit* ― **ユニット番号** ”1”
  - *port* ― **ポート番号（範囲：**1-26）
- **port-channel** *channel-id*（**範囲：**1-12）
- **mst** *instance-id* （**範囲：**0-4094）

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

- **パラメータを使わず** "show spanning-tree" **コマンドを使用した場合、ツリー内の各インタフェースのための本機のスパニングツリー設定が表示されます。**
- "show spanning-tree interface" **コマンドを使用した場合、指定したインタフェースのスパニングツリー設定のみ表示されます。**
- **「**Spanning-tree information**」で表示される情報の詳細は** P124 **「グローバル設定」を参照して下さい。各インタフェースで表示される内容は** P128 **「インタフェース設定の表示」を参照して下さい。**

例

```
Console#show spanning-tree
Spanning Tree Information
---------------------------------------------------------------------
 Spanning Tree Mode:                RSTP
 Spanning Tree Enabled/Disabled:    Enabled
 Instance:                          0
 VLANs Configuration:               1-4094
 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
 Max Hops:                          20
 Remaining Hops:                    20
 Designated Root:                   32768.00172E0F7280
 Current Root Port:                 0
 Current Root Cost:                 0
 Number of Topology Changes:        0
 Last Topology Change Time (sec.): 44
 Transmission Limit:                3
 Path Cost Method:                  Long
 Flooding Behavior:                 To VLAN
---------------------------------------------------------------------
Eth  1/ 1 Information
---------------------------------------------------------------------
 Admin Status:              Enabled
 Role:                      Disabled
 State:                     Discarding
 Admin Path Cost:           100000
 Oper Path Cost:            100000
 Priority:                  128
 Designated Cost:           0
 Designated Port:           128.1
 Designated Root:           32768.00172E0F7280
 Designated Bridge:         32768.00172E0F7280
 Fast Forwarding:           Enabled
 Forward Transitions:       0
 Admin Edge Port:           Enabled
 Oper Edge Port:            Enabled
 Admin Link Type:           Auto
 Oper Link Type:            Point-to-point
 Flooding Behavior:         Enabled
 Spanning Tree Status:      Enabled.
.
.
.
Console#
```

show spanning-tree mst configuration

MST の設定を表示します。

文法

show spanning-tree mst configuration

コマンドモード

Privileged Exec

例

```
Console#show spanning-tree mst configuration
MSTP Configuration Information
-------------------------------------------------------------
 Configuration Name: 00 17 2e 0f 72 80
 Revision Level:     0

 Instance VLANs
-------------------------------------------------------------
     0    1-4094
Console#
```

4.18 VLAN

VLAN はネットワーク上のどこにでも位置することができますが、あたかもそれらが物理的な同一セグメントに属するかのように動作し、通信を行うポートのグループです。
ここでは VLAN 関連コマンドを使用し、指定するポートの VLAN グループの生成、メンバーポートの追加、VLAN タグ使用法の設定、自動 VLAN 登録の有効化を行います。

コマンドグループ	機能	ページ
GVRP and Bridge Extension	GVRP の設定	P487
Editing VLAN Groups	VLAN 名、VID、状態を含む VLAN の設定	P493
Configuring VLAN Interfaces	入力フィルタ、入力 / 出力タグモード、PVID、GVRP を含む VLAN インタフェースパラメータの設定	P495
Displaying VLAN Information	状態、ポートメンバー、MAC アドレスを含む VLAN グループの表示	P503
Configuring 802.1Q Tunneling	802.1Q トンネリング（QinQ トンネリング）の設定	
Configuring Private VLANs	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 の設定	P504
Configuring Protocol VLANs	フレームタイプおよびプロトコルを基にした Protocol-based VLAN の設定	P518

4.18.1 GVRP の設定

GARP VLAN Registration Protocol(GVRP) はスイッチが自動的にネットワークを介してインタフェースを VLAN メンバーとして登録するために VLAN 情報を交換する方法を定義します。各インタフェース又は本機全体への GVRP の有効化の方法と、Bridge Extension MIB の設定の表示方法を説明しています。

コマンド	機能	モード	ページ
bridge-ext gvrp	本機全体に対し GVRP を有効化	GC	P488
show bridge-ext	bridge extension 情報の表示	PE	P489
switchport gvrp	インタフェースへの GVRP の有効化	IC	P489
switchport forbidden vlan	インタフェースへの登録禁止 VLAN の設定	IC	P502
show gvrp configuration	選択したインタフェースへの GVRP の設定の表示	NE,PE	P490
garp timer	選択した機能への GARP タイマーの設定	IC	P491
show garp timer	選択した機能への GARP タイマーの表示	NE,PE	P492

bridge-ext gvrp

GVRP を有効に設定します。"no" を前に置くことで機能を無効にします。

文法

bridge-ext gvrp

no bridge-ext gvrp

初期設定

無効 (Disabled)

コマンドモード

Global Configuration

コマンド解説

GVRP は、スイッチがネットワークを介してポートを VLAN メンバーとして登録するために VLAN 情報を交換する方法を定義します。この機能によって自動的に VLAN 登録を行うことができ、ローカルのスイッチを越えた VLAN の設定をサポートします。

例

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

show bridge-ext

bridge extension コマンドの設定を表示します。

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

表示される内容は P141 「VLAN 基本情報の表示」及び P21 「ブリッジ拡張機能の表示」を参照して下さい。

例

```
Console#show bridge-ext
Max support vlan numbers:                256
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

ポートの GVRP を有効に設定します。"no" を前に置くことで機能を無効にします。

文法

switchport gvrp

no switchport gvrp

初期設定

無効 (Disabled)

コマンドモード

Interface Configuration (Ethernet, Port Channel)

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。

文法

show gvrp configuration { interface }

- *interface*

  − ***ethernet*** *unit/port*

  unit — **ユニット番号** ”1”

  port — **ポート番号（範囲：**1-26）

  − **port-channel** *channel-id*（**範囲：**1-12）

初期設定

全体と各インタフェース両方の設定を表示します。

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

leave、leaveall、join タイマーに値を設定します。"no" を前に置くことで初期設定の値に戻します。

文法

garp timer < join | leave | leaveall > *timer_value*

no garp timer < join | leave | leaveall >

- **< join | leave | leaveall >** ― 設定するタイマーの種類
- *timer_value* ― タイマーの値

範囲：

join：20-1000 センチセカンド

leave：60-3000 センチセカンド

leaveall：500-18000 センチセカンド

初期設定

- join：20 センチセカンド
- leave：60 センチセカンド
- leaveall：1000 センチセカンド

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- ブリッジされた LAN 内でのクライアントサービスのクライアント属性の登録、削除を行うために、Group Address Registration Protocol(GARP) は GVRP 及び GMRP で使用されます。GARP タイマーの初期設定の値は、メディアアクセス方法又はデータレートと独立しています。GMRP 又は GVRP 登録 / 削除に関する問題がない場合には、これらの値は変更しないで下さい。
- タイマーの値はすべての VLAN の GVRP に設定されます。
- タイマーの値は以下の式に適応した値である必要があります :
  leave >= (2 x join)
  leaveall > leave

[注意]　GVRP タイマーの値は同一ネットワーク内のすべての L2 スイッチで同じに設定して下さい。同じ値に設定されない場合は GVRP が正常に機能しません。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#garp timer join 100
Console(config-if)#
```

関連するコマンド

show garp timer (P492)

show garp timer

選択したポートの GARP **タイマーを表示します。**

文法

show garp timer { *interface* **}**

- *interface*

  − **ethernet** *unit/port*

  unit ― **ユニット番号** ”1”

  port ― **ポート番号（範囲：**1-26）

  − **port-channel** *channel-id*（**範囲：**1-12）

初期設定

すべての GARP **タイマーを表示します。**

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#
```

関連するコマンド

garp timer (P491)

4.18.2 VLAN グループの設定

コマンド	機能	モード	ページ
vlan database	VLAN database モードに入り、VLAN の設定を行う	GC	P493
VLAN	VID,VLAN 名、ステートなど VLAN の設定	VC	P494

vlan database

VLAN データベースモードに入ります。このモードのコマンドは設定後直ちに有効となります。

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- VLAN データベースコマンドを使用し VLAN の追加、変更、削除が行えます。VLAN の設定終了後は " show vlan" コマンドを使用しエントリー毎に VLAN 設定を表示することができます。
- "interface vlan" コマンドモードを使用し、ポートメンバーの指定や、VLAN からのポートの追加、削除が行えます。コマンドを使用した結果は、実行中の設定ファイルに書き込まれ "show running-config" コマンドを使用することでファイルの内容を表示させることができます。

例

```
Console(config)#vlan database
Console(config-vlan)#
```

関連するコマンド

show vlan (P503)

vlan

VLAN を設定します。"no" を前に置くことで VLAN の削除、もしくは初期設定に戻します。

文法

vlan *vlan-id* [**name** *vlan-name*] [**media ethernet** { **state** < active | suspend >]

no vlan *vlan-id* { **name** | **state** }

- *vlan-id* — 設定する VLAN ID（範囲：1-4094）
- **name** — 識別するための VLAN 名
- *vlan-name* — 1-32 文字
- **media ethernet** — イーサネットメディアの種類
- **state** — VLAN のステートの識別
  - active — VLAN の実行
  - suspend — VLAN の中断。中断中の VLAN はパケットの転送を行いません。

初期設定

初期設定では VLAN 1 が存在し、active 状態です。

コマンドモード

VLAN Database Configuration

コマンド解説

- "**no vlan** *vlan-id*" を使用した場合、VLAN が削除されます。
- "**no vlan** *vlan-id* **name**" を使用した場合、VLAN 名が削除されます。
- " **no vlan** *vlan-id* **state**" を使用した場合、VLAN は初期設定の状態 (active) に戻ります。
- 最大 255VLAN の設定が可能です。

例

VLAN ID：105、VLAN name：RD5 で新しい VLAN を追加しています。VLAN は初期設定で active になっています。

```
Console(config)#vlan database
Console(config-vlan)#vlan 105 name RD5 media ethernet
Console(config-vlan)#
```

関連するコマンド

show vlan (P503)

4.18.3 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	VLAN を設定するための Interface 設定モードへの参加	IC	P495
switchport mode	インタフェースの VLAN メンバーモードの設定	IC	P496
switchport acceptable frame types	インタフェースで受け入れ可能なフレームタイプの設定	IC	P497
switchport ingress-filtering	インタフェースへの入力フィルタの有効化	IC	P498
switchport native vlan	インタフェースの PVID(native VLAN) の設定	IC	P499
switchport allowed vlan	インタフェースに関連した VLAN の設定	IC	P500
switchport gvrp	インタフェースへの GVRP の有効化	IC	P489
switchport forbidden vlan	インタフェースの登録を禁止する VLAN の設定	IC	P502
switchport priority default	タグなし受信フレームのポートプライオリティの設定	IC	P525

interface vlan

VLAN の設定のために interface 設定モードに入り、各インタフェースの設定を行います。

文法

interface vlan *vlan-id*

- *vlan-id* — 設定する VLAN ID（範囲：1-4094）

初期設定

なし

コマンドモード

Global Configuration

例

本例では、VLAN 1 の interface configuration モードに参加し、VLAN に対し IP アドレスを設定しています。

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.254 255.255.255.0
Console(config-if)#
```

関連するコマンド

show vlan (P503)

switchport mode

ポートの VLAN **メンバーシップモードの設定を行います。**"no" **を前に置くことで初期設定に戻します。**

文法

switchport mode < private-vlan | access | hybrid | trunk >

no switchport mode { private-vlan }

- **private-vlan** ― **詳細については、**513 **ページの「**switchport mode private-vlan**」を参照して下さい。**
- **access** ― VLAN **のアクセスリンクを設定します。**
- **hybrid** ― **ハイブリッド** VLAN **インタフェースを指定。ポートはタグ付及びタグなしフレームを送信します。**
- **trunk** ― VLAN **トランクに使用されるポートを指定します。トランクは** 2 **つのスイッチ間の直接接続で、ポートはソース** VLAN **を示すタグ付フレームを送信します。デフォルト** VLAN **に所属するフレームもタグ付フレームを送信します。**

初期設定

すべてのポートは hybrid **に指定され、**VLAN 1 **が** PVID **に設定されています。**

コマンドモード

Interface Configuration (Ethernet, Port Channel)

例

本例では、1 **番ポートの** configuration **モードの設定を行い、**switchport **モードを** hybrid **に指定しています。**

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport mode hybrid
Console(config-if)#
```

switchport acceptable-frame-types

ポートの受け入れ可能なフレームの種類を指定します。"no" **を前に置くことで初期設定に戻します。**

文法

switchport acceptable-frame-types < all | tagged >

no switchport acceptable-frame-types

- **all ― タグ付、タグなしのすべてのフレームを受け入れます。**
- **tagged ― タグ付フレームのみを受け入れます。**

初期設定

すべてのフレームタイプ

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

すべてのフレームを許可する設定にした場合、タグなし受信フレームはデフォルト VLAN **に指定されます。**

例

本例では 1 **番ポートにタグ付フレームのみを許可する設定にしています。**

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#
```

関連するコマンド

switchport mode (P496)

switchport ingress-filtering

ポートに対してイングレスフィルタリングを有効にします。"no" を前に置くことで初期設定に戻します。

[注意] 本機の Ingress filtering は常に有効です。無効に設定することはできませんが、Ingress filtring コマンドは常に利用可能になっており、"no switchport ingress-filtring" コマンドも入力が可能です。使用時には "Note:Failed to ingress-filtring on ethernet interface!" のエラーが出て、設定変更不可能となります。

文法

switch port ingress-filtering

no switchport ingress-filtering

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- イングレスフィルタリングはタグ付フレームにのみ有効です。
- イングレスフィルタリングが有効の場合、メンバーでない VLAN へのタグがついたフレームを受信すると、そのフレームは捨てられます。
- イングレスフィルタリングは GVRP や STP などの VLAN と関連のない BPDU フレームには影響を与えません。但し、VLAN に関連した GMRP などの BPDU フレームには影響を与えます。

例

本例では、1 番ポートを指定し、イングレスフィルタリングを有効にしています。

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport ingress-filtering
Console(config-if)#
```

switchport native vlan

ポートへのデフォルト VLAN ID **である** PVID **の設定を行います。**"no" **を前に置くことで初期設定に戻します。**

文法

switchport native vlan *vlan-id*

no switchport native vlan

- *vlan-id* — **ポートへのデフォルト** VLAN ID**（範囲：**1-4094**）**

初期設定

VLAN 1

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- PVID **を設定するためには、対象のポートが指定する** PVID **と同じ** VLAN **に所属しており、またその** VLAN **がタグなしである必要があります。**
- **受け入れ可能なフレームタイプを** "all" **にしている場合か、**switchport **モードを** "hybrid" **にしている場合、入力ポートに入るすべてのタグなしフレームには** PVID **が挿入されます。**

例

本例では PVID **を** VLAN3 **として** 1 **番ポートに設定しています。**

```
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の VLAN グループの設定を行います。"no" を前に置くことで初期設定に戻します。

[注意] 各ポートは、1つのタグなし VLAN にのみ所属することができ、この VLAN がポートの PVID となります。2 つ目のタグなし VLAN に所属させた場合、最初に Tag なしとして所属していた VLAN は、自動的に Tag 付きへ変わり、2 つ目の VLAN がポートの PVID に設定されます。また、”no switchport allowed vlan” コマンドを使用し、VLAN の所属から外れた場合は、ポートの PVID はタグなしの VLAN1 に変更されます。

文法

switchport allowed vlan [add *vlan-list* **{tagged | untagged } | remove** *vlan-list***}**

no switchport allowed vlan

- **add** *vlan-list* ― 追加する VLAN の ID のリスト
- **remove** *vlan-list* ― 解除する VLAN の ID のリスト
- *vlan-list* ― 連続しない VLAN ID をカンマで分けて入力（スペースは入れない）。連続する ID はハイフンで範囲を指定（範囲：1-4094）

初期設定

すべてのポートが VLAN 1 に参加

フレームタイプはタグなし

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- switchport モードが " trunk" に設定されている場合、インタフェースをタグ付メンバーとしてしか VLAN に設定できません。
- インタフェースの switchport mode が "hybrid" に設定されている場合、インタフェースを最低 1 つの VLAN にタグなしメンバーとして設定する必要があります。
- スイッチ内では常にフレームはタグ付となっています。タグ付及びタグなしパラメータはインタフェースへ VLAN を加えるとき使われ、出力ポートでフレームのタグをはずすか保持するかを決定します。
- ネットワークの途中や対向のデバイスが VLAN をサポートしていない場合、インタフェースはこれらの VLAN をタグなしメンバーとして加えます。1 つの VLAN にタグなしとして加え、その VLAN がネイティブ VLAN となります。
- インタフェースの禁止リスト上の VLAN が手動でインタフェースに加えられた場合、VLAN は自動的にインタフェースの禁止リストから削除されます。
- ポートへの接続装置にかかわらず、タグなし VLAN へメンバーを追加することができます。初期設定では VLAN1 となります。
  各ポートは 1 つのタグ無し VLAN にしか所属ができないので、もし 2 つ目の VLAN がタグなしと定義された場合、もう一方の VLAN は自動的にタグつきに変更されます。またポートの PVID もこの VLAN ID へ変更されます。

例

本例では、1 番ポートのタグ付 VLAN 許可リストに VLAN1,2,5,6 を加えています。

```
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 の設定を行います。"no" を前に置くことで禁止 VLAN リストから削除します。

文法

switchport forbidden vlan [add *vlan-list* **| remove** *vlan-list* **]**

no switchport forbidden vlan

- **add** *vlan-list* ― 追加する VLAN の ID のリスト
- **remove** *vlan-list* ― 解除する VLAN の ID のリスト
- *vlan-list* ― 連続しない VLAN ID をカンマで分けて入力（スペースは入れない）。連続する ID はハイフンで範囲を指定（範囲：1-4094)

初期設定

なし

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- GVRP で自動的に VLAN に加えられることを防ぐためのコマンドです。
- インタフェース上で VLAN が許可 VLAN にセットされている場合、同じインタフェースの禁止 VLAN リストに加えることはできません。

例

本例では 1 番ポートを VLAN 3 に加えることを防いでいます。

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport forbidden vlan add 3
Console(config-if)#
```

4.18.4 VLAN 情報の表示

コマンド	機能	モード	ページ
show vlan	VLAN 情報の表示	NE,PE	P503
show interfaces status vlan	特定 VLAN インタフェースの状態の表示	NE,PE	P413
show interfaces switchport	インタフェースの管理、運用状態の表示	NE,PE	P415

show vlan

VLAN 情報の表示を行います。

文法

show vlan { id *vlan-id* **| name** *vlan-name* **}**

- **id** ― VLAN ID が続くキーワード

  vlan-id ― 表示する VLAN ID（範囲：1-4094）

- **name** ― VLAN 名が続くキーワード

  vlan-name ― 1-32 文字の VLAN 名

初期設定

すべての VLAN を表示

コマンドモード

Normal Exec, Privileged Exec

例

本例では VLAN 1 の情報を表示しています。

```
Console#show vlan id 1
Default VLAN ID : 1

VLAN ID: 1
Type: Static
Name: DefaultVlan
Status: Active
Ports/Port Channels: 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) Eth1/19(S)
Eth1/20(S) Eth1/21(S) Eth1/22(S) Eth1/23(S) Eth1/24(S)
Eth1/25(S) Eth1/26(S)
Trunk 1(S)
Console#
```

4.18.5 IEEE802.1Q トンネリングの設定

本機は通常 VLAN **モードまたは、サービスプロバイダのメトロポリタンネットワークを通過するレイヤ** 2 **トラフィックに使用される、**IEEE 802.1Q(QinQ) **トンネリングモードでに設定することができます。**

QinQ **トンネルの設定を行うため、前セクションのガイドラインに補足を行います。**
VLAN **ポート設定または** VLAN **トランク設定画面にて、エッジスイッチのアクセスポートを** 802.1Q **トンネルモードに設定します。**

コマンド	機能	モード	ページ
dot1q-tunnel system-tunnel-control	**スイッチをノーマルモードまたは** QinQ **モードに設定**	GC	P505
switchport dot1q-tunnel mode	**インタフェースを** QinQ **トンネルポートに設定**	IC	P506
switchport dot1q-tunnel tpid	**トンネルポートの** TPID（Tag Protocol Identifier）**値を設定**	IC	P507
show dot1q-tunnel	QinQ **トンネル設定の表示**	PE	P508
show interfaces switchport	QinQ **操作ステータス**	PE	P415

dot1q-tunnel system-tunnel-control

スイッチを QinQ **モードに設定します。**"no" **を前に置くことで、機能を無効にします。**

文法

dot1q-tunnel system-tunnel-control

no dot1q-tunnel system-tunnel-control

初期設定

無効

コマンドモード

Global Configuration

例

```
Console(config)#dot1q-tunnel system-tunnel-control
Console(config)#
```

関連するコマンド

show dot1q-tunnel (P508)

show interfaces switchport (P415)

switchport dot1q-tunnel mode

インタフェースを QinQ **トンネルポートに設定します。**"no" **を前に置くことで、設定を初期状態に戻します。**

文法

switchport dot1q-tunnel mode <access | uplink>

no switchport dot1q-tunnel mode

- **access** ― **ポートを** 802.1Q **トンネルアクセスポートに設定**
- **uplink** ― **ポートを** 802.1Q **トンネルアップリンクポートに設定**

初期設定

無効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport dot1q-tunnel mode access
Console(config-if)#
```

関連するコマンド

show dot1q-tunnel (P508)

show interfaces switchport (P415)

switchport dot1q-tunnel tpid

トンネルポートのタグプロトコル識別子（TPID）を設定します。"no" を前に置くことで、設定を初期状態に戻します。

文法

switchport dot1q-tunnel tpid *tpid*

no switchport dot1q-tunnel tpid

- *tpid* ― **トンネルポートに入ってきたパケットのタグプロトコル識別子（TPID）（範囲；16 進 0800-FFFF　初期設定：8100）**

初期設定

0x8100

コマンドモード

Interface Configuration (Ethernet, Port Channel)

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport dot1q-tunnel tpid 9100
Console(config-if)#
```

関連するコマンド

show interfaces switchport (P415)

show dot1q-tunnel

QinQ トンネルポート情報を表示します。

コマンドモード

Privileged Exec

例

```
Console(config)#dot1q-tunnel system-tunnel-control
Console(config)#interface ethernet 1/1
Console(config-if)#switchport dot1q-tunnel mode access
Console(config-if)#interface ethernet 1/2
Console(config-if)#switchport dot1q-tunnel mode uplink
Console(config-if)#end
Console#show dot1q-tunnel

Current double-tagged status of the system is Enabled

The dot1q-tunnel mode of the set interface 1/1 is Access mode, TPID is 0x8100.
The dot1q-tunnel mode of the set interface 1/2 is Uplink mode, TPID is 0x8100.
The dot1q-tunnel mode of the set interface 1/3 is Normal mode, TPID is 0x8100.
The dot1q-tunnel mode of the set interface 1/4 is Normal mode, TPID is 0x8100.
The dot1q-tunnel mode of the set interface 1/5 is Normal mode, TPID is 0x8100.
The dot1q-tunnel mode of the set interface 1/6 is Normal mode, TPID is 0x8100.
The dot1q-tunnel mode of the set interface 1/7 is Normal mode, TPID is 0x8100.
.
.
.
The dot1q-tunnel mode of the set interface 1/24 is Normal mode, TPID is 0x8100.
Console#
```

関連するコマンド

switchport dot1q-tunnel mode (P506)

4.18.6 プライベート VLAN の設定

プライベート VLAN **は、ポートベースでのセキュリティの確保と** VLAN **内のポート間の分離を行うことができます。本機はプライマリ** VLAN **と、セカンダリ** VLAN **の** 2 **種類をサポートしています。プライマリ** VLAN **には無差別ポートがあり、このポートは同じプライベート** VLAN **に所属する他のポートと通信が可能です。セカンダリ (コミュニティ)** VLAN **にはコミュニティポートがあり、このポートは同じセカンダリ** VLAN **内の他のホスト、又は関連付けを行ったプライマリ** VLAN **の任意の無差別ポートとのみ通信が可能です。独立** VLAN **は、**1 **つの無差別ポートと** 1 **つ以上の独立 (又はホスト) ポートから構成される、単一のスタンドアロンの** VLAN **です。いずれの** VLAN **も無差別ポートはインターネットなど外部ネットワークからのアクセスが可能ですが、コミュニティ / 独立ポートはローカルユーザからのアクセスのみに制限されます。**

本機には複数のプライマリ VLAN **を設定でき、又複数のコミュニティ** VLAN **を各プライマリ** VLAN **と関連付けできます。独立** VLAN **も** 1 **つ以上設定できます (プライベート** VLAN **と通常の** VLAN **は同一スイッチ内に同時に構成することができることに注意して下さい)**

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、コミュニティ、独立** VLAN **の追加と削除**	VC	P511
private-vlan association	**コミュニティ** VLAN **とプライマリ** VLAN **の関連付け**	VC	P512
プライベート** VLAN Interface **の設定			
switchport mode private-vlan	**インタフェースへのホストモード / 無差別モードの指定**	IC	P513
switchport private-vlan host-association	**インタフェースのセカンダリ** VLAN **への関連付け**	IC	P514
switchport private-vlan isolated	**インタフェースの独立** VLAN **への関連付け**	IC	P515
switchport private-vlan mapping	**インタフェースのプライマリ** VLAN **へのマッピング**	IC	P516
プライベート** VLAN **の表示			
show vlan private-vlan	**プライベート** VLAN **の情報を表示**	NE,PE	P517

プライマリ / セカンダリに関連付けられたグループに設定するには、以下の手順で行います。

（1）"private-vlan" コマンドを使用し、1 つ以上のコミュニティ VLAN と、コミュニティグループ以外のトラフィックのやり取りをお行うプライマリ VLAN を 1 つ指定します。

（2）"private-vlan association" コマンドを使用し、コミュニティ VLAN とプライマリ VLAN とのマッピングを行います。

（3）"switchport mode private-vlan" コマンドを使用し、ポートを無差別（プライマリ VLAN のすべてのポートと通信が可能）又はホスト（コミュニティポートなど）に指定します。

（4）"switchport private-vlan host-association" コマンドを使用し、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、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、設定内容を確認します。

独立 VLAN を設定するには、以下の手順で行います。

（1）"private-vlan" コマンドを使用し、独立 VLAN を指定します。独立 VLAN には、1 つの無差別ポートと 1 つ以上の独立ポートが所属しています。

（2）"switchport mode private-vlan" コマンドを使用し、ポートを無差別（プライマリ VLAN のすべてのポートと通信が可能）又はホスト（コミュニティポートなど）に指定します。

（3）"switchport private-vlan isolated" コマンドを使用し、ポートを独立 VLAN に指定します。

（4）"show vlan private-vlan" コマンドを使用し、設定内容を確認します。

Private vlan

プライベート VLAN（**プライマリ、コミュニティ、独立**）**を作成します。**"no" **を前に置くことで、プライベート** VLAN **を削除します。**

文法

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：**2-4094）
- **community** ― **同一の** VLAN **に所属するホストか、又は関連付けられたプライマリ** VLAN **に所属する無差別ポートのみに通信が制限される** VLAN
- **primary** ― 1 **つ以上のコミュニティ** VLAN **を所有し、コミュニティ** VLAN **と他との通信のやり取りを行う** VLAN
- **isolated** ― **独立** VLAN**。独立ポートに関連付けられたポートは、同じ** VLAN **に所属する無差別ポートとのみ通信が可能**

初期設定

なし

コマンドモード

VLAN Configuration

コマンド解説

- **プライベート** VLAN **は、同一のコミュニティ** VLAN **又は同一の独立** VLAN **に所属するポート宛に、或いは** VLAN **外の場合は無差別ポート宛に、通信先を制限する場合に使用します。コミュニティ** VLAN **を使用する場合、無差別ポートを所有する** " **プライマリ** "VLAN **とマッピングされなくてはなりません。独立** VLAN **を使用する場合、単一の無差別ポートを所有するように設定しなくてはなりません。**
- **プライベート** VLAN **におけるポートの所属方法は静的な設定で行います。一度ポートがプライベート** VLAN **に所属すると、**GVRP **で他の** VLAN **に動的に移動できなくなります。**
- **プライベート** VLAN **をトランクモードに設定することはできません** P496 「switchport mode」**コマンドを参照して下さい）**

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。**"no" **を前に置くことで、指定したプライマリ** VLAN **に関連付けられていたものがすべて削除されます。**

文法

private vlan *primary-vlan-id* **association**
[**add** *secondary-vlan-id* | **remove** *secondary-vlan-id*} | *VLAN ID*]

no private vlan *primary-vlan-id* **association**

- *primary-vlan-id* ― **プライマリ** VLAN **の** ID**（範囲：**2-4094**）**
- *secondary-vlan-id* ― **セカンダリ（コミュニティ）**VLAN**（範囲：**2-4094**）**

初期設定

なし

コマンドモード

VLAN Configuration

コマンド解説

- **セカンダリ** VLAN **は所属メンバーのセキュリティを確保します。関連付けられたプライマリ** VLAN **はプライマリ** VLAN **内で他のネットワークとの、又は（無差別ポートを介した）プライマリ** VLAN **の外の宛先との、共通のインタフェース（無差別ポート）となります。**

例

```
Console(config-vlan)#private-vlan 2 association 3
Console(config)#
```

switchport mode private-vlan

インタフェースにプライベート VLAN **モードを設定します。**"no" **を前に置くことで、初期設定に戻します。**

文法

switchport mode private-vlan < host | promiscuous>

no switchport mode private-vlan

- **host ― コミュニティ** VLAN **または独立** VLAN **に割り当て可能なポートに設定します。**
- **promiscuous ― 関連付けられたセカンダリ** VLAN **に所属するすべてのポートと、又同じプライマリ** VLAN **に所属する他のすべての無差別ポートと通信可能なポートに設定します。**

初期設定

Normal VLAN

コマンドモード

Interface Configuration（Ethernet、Port Channel）

コマンド解説

- **プライマリ** VLAN **に無差別ポートを割り当てるには、**"switch port private-vlan mapping" **コマンドを使用します。ホストポートをコミュニティ** VLAN **に割り付けるには、**"private-vlan host association" **コマンドを使用します。**
- **無差別ポート又はホストポートを独立** VLAN **に割り当てるには、**"switch port private-vlan isolated" **コマンドを使用します。**

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)#
```

関連するコマンド

Private-vlan host association (P514)

switchport private-vlan host-association

インタフェースにセカンダリ VLAN **を関連付けます。**"no" **を前に置くことで、関連付けを削除します。**

文法

switchport private-vlan host-association *secondary-vlan-id*

no switchport private-vlan host-association

- *secondary-vlan-id* ― **セカンダリ（コミュニティ）**VLAN **の** ID**（範囲：**2-4094**）**

初期設定

なし

コマンドモード

Interface Configuration（Ethernet、Port Channel）

コマンド解説

- **セカンダリ** VLAN **に割り当てたすべてのポートはグループメンバ間で通信できますが、グループ外との通信は関連付けたプライマリ** VLAN **の無差別ポート経由で行わなくてはなりません。**

例

```
Console(config)#interface ethernet 1/3
Console(config-if)#switchport private-vlan host-association 3
Console(config-if)#
```

switchport private-vlan isolated

インタフェースを独立 VLAN **に割り当てます。**"no" **を前に置くことで、割り当てを解除します。**

文法

switchport private-vlan isolated *isolated-vlan-id*

no switchport private-vlan isolated

- *isolated-vlan-id* - **独立** VLAN **の** ID**（範囲：**2-4094**）**

初期設定

なし

コマンドモード

Interface Configuration（Ethernet、Port Channel）

コマンド解説

独立 VLAN **に割り当てたホストポートはグループメンバ間で通信できないため、グループ外との通信は無差別ポート経由で行わなくてはなりません。**

例

```
Console(config)#interface ethernet 1/3
Console(config-if)#switchport private-vlan isolated 3
Console(config-if)#
```

switchport private-vlan mapping

インタフェースをプライマリ VLAN **にマッピングします。**"no" **を前に置くことで、マッピングを削除します。**

文法

switchport private-vlan mapping *primary-vlan-id*

no switchport private-vlan mapping

- *primary-vlan-id* - **プライマリ** VLAN **の** ID**（範囲：**2-4094**）**

初期設定

なし

コマンドモード

Interface Configuration（Ethernet、Port Channel）

コマンド解説

- **セカンダリ** VLAN **に割り当てた無差別ポートは同一** VLAN **内の他の無差別ポートと、又関連付けたセカンダリ** 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

本機におけるプライベート VLAN **の設定情報を表示します。**

文法

show vlan private-vlan {community | isolated | primary}

- **community - コミュニティ** VLAN **をすべて表示します。関連付けられたプライベート** VLAN**、割り当てられたホストポート情報も一緒に表示します。**
- **isolated - 独立** VLAN **を表示します。割り当てられた無差別ポートとホストポート情報も一緒に表示します。**"Primary" **又は** "Secondary" **フィールドに表示しているのは、独立** VLAN **の** ID **番号です。**
- **primary - プライマリ** VLAN **をすべて表示します。割り当てられた無差別ポート情報も一緒に表示します。**

初期設定

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#
```

4.18.7 プロトコル VLAN の設定

通常の VLAN では、プロトコル毎の VLAN グループの形成を容易に行なうことはできません。そのため、特定のプロトコルに関連するすべての機器が通信を行えるよう、特殊なネットワーク機器を使用して異なる VLAN 間の通信をサポートする必要があります。
しかし、このような方法では、セキュリティと容易な設定が可能な VLAN のメリットを失ってしまいます。

そのような問題を回避するため、本機では物理的なネットワークの構成を、プロトコルを基にした論理的 VLAN のネットワーク構成とすることが可能なプロトコルベース VLAN 機能を提供します。ポートがフレームを受信した際、受信フレームのプロトコルタイプに応じて VLAN メンバーシップが決定されます。

コマンド	機能	モード	ページ
protocol-vlan protocol-group	プロトコルグループの作成及びサポートプロトコルの指定	GC	P519
protocol-vlan protocol-group	プロトコルグループの VLAN へのマッピング	IC	P520
show protocol-vlan protocol-group	プロトコルグループの設定の表示	PE	P521

プロトコル VLAN の設定は以下の手順で行ないます。

（1）使用するプロトコルのための VLAN グループを作成します。主要なプロトコル毎に VLAN の作成を行なうこと推奨します。また、この時点ではポートメンバーの追加を行なわないで下さい。

（2）VLAN に設定するプロトコル毎のグループを "protocol-vlan protocol-group" コマンド (General Configuration mode) を利用して生成します。

（3）適切な VLAN に各インタフェースのプロトコルを "protocol-vlan protocol-group" コマンド (Interface Configuration mode) を利用してマッピングします。

protocol-vlan protocol-group (Configuring Groups)

プロトコルグループの作成及び特定のプロトコルのグループへの追加を行ないます。"no" **を前に置くことでプロトコルグループを削除します。**

文法

protocol-vlan protocol-group *group-id* **{ add | remove } protocol-type <apple_talk | ip | ipx |** *0-ffff* **frame-type <ethernet | llc-other | rfc-1042 |snap_8021h>>**

no protocol-vlan protocol-group *group-id*

- *group-id* ― **プロトコルグループ** ID**（設定範囲：**1-2147483647**）**
- **protocol-type** ― **プロトコルタイプ**
  （選択肢：Options: apple_talk, ip, ipx,user-defined (0-ffff)**）**
- **frame-type** ― **フレームタイプ（選択肢：**ethernet, llc-other,rfc-1042, snap_8021h**）**

初期設定

プロトコルグループ未設定

コマンドモード

Global Configuration

例

プロトコルグループ "1" **を作成し、フレームタイプを** "Ethernet"**、プロトコルタイプを** "IP" **及び** "ARP" **に設定しています。**

```
Console(config)#protocol-vlan protocol-group 1  add protocol-type ip
Console(config)#protocol-vlan protocol-group 1  add protocol-type 0806
frame-type ethernet
Console(config)#
```

protocol-vlan protocol-group (Configuring Interfaces)

インタフェースにおいてプロトコルグループを VLAN **にマッピングします。**"no" **を前におくことでインタフェースのプロトコルのマッピングを解除します。**

文法

protocol-vlan protocol-group *group-id* **vlan** *vlan-id*

no protocol-vlan protocol-group *group-id* **vlan**

- *group-id* ― **プロトコルグループ** ID**（設定範囲：**1-2147483647**）**
- *vlan-id* ― **致したプロトコルの通信が転送される** VLAN**（設定範囲：**1-4094**）**

初期設定

プロトコルグループはインタフェースにマッピングされていません。

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- **インタフェースの設定を行なって下さい。他の** VLAN **コマンドを使用した場合、設定したインタフェースはすべてのプロトコルタイプの通信を関連した** VLAN **に対して行います。**
- **フレームがプロトコル** VLAN **に割り当てられたポートに入力する場合、以下の方法で処理されます。**
  - **フレームにタグ付フレームの場合、タグの情報に基づき処理されます。**
  - **フレームがタグなしフレームで、プロトコルタイプが一致した場合、フレームは適切な** VLAN **に転送されます。**
  - **フレームがタグなしフレームで、プロトコルタイプが一致しない場合、フレームはインタフェースのデフォルト** VLAN **に転送されます。**

例

本例では、1 **番ポートに入ってきた通信でプロトコルグループ** 1 **と一致する通信が** VLAN2 **にマッピングしています。**

```
Console(config)#interface ethernet 1/1
Console(config-if)#protocol-vlan protocol-group 1 vlan 2
Console(config-if)#
```

show protocol-vlan protocol-group

プロトコルグループに関連したフレーム及びプロトコルタイプの表示

文法

show protocol-vlan protocol-group { *group-id* **}**

- *group-id* ― **プロトコルグループ** ID（**設定範囲：**1-2147483647）

初期設定

すべてのプロトコルグループを表示

コマンドモード

Privileged Exec

例

プロトコルグループ 1 **が** Ethernet、IP **に設定されていることを表示しています。**

```
Console#show protocol-vlan protocol-group

ProtocolGroup ID Frame Type Protocol Type
---------------- ------------ ---------------
4 Ethernet 0B AD
8 Ethernet 80 2E
5000 Ethernet 81 37
12 Ethernet 81 46
5000 Ethernet 86 DD
6 RFC 1042 43 21
10 RFC 1042 80 49
7 SNAP 802.1h 80 3C
11 SNAP 802.1h 80 A3
50 SNAP 802.1h 81 2B
5000 SNAP 802.1h 86 DD
1 08 00
3 80 9B
2 81 37
```

show interfaces protocol-group

選択したインタフェースのプロトコルグループと VLAN **のマッピング情報を表示します。**

文法

show interfaces protocol-group { *interface* }

- *interface*
  - ethernet unit/port
    - unit — **ユニット番号** "1"
    - port — **ポート番号**（1-26）
  - port-channel channel-id (1-12)

初期設定

すべてのプロトコルグループを表示

コマンドモード

Privileged Exec

例

1 **番ポートに入ってきた通信でプロトコルグループ** 1 **と一致する通信が** VLAN2 **にマッピングされています。**

```
Console#show interfaces protocol-group
Port ProtocolGroup ID Vlan ID
---------- ------------------ -----------
Eth 1/1 1                  vlan2
Console#
```

4.19 プライオリティ

通信の過密によりパケットがスイッチにバッファされた場合、通信の優先権を持つデータパケットを明確にすることができます。本機は各ポートに 4 段階のプライオリティキューを持つ CoS をサポートします。

ポートの最高プライオリティキューの付いたデータパケットは、より低いプライオリティのキューのパケットよりも先に送信されます。各ポートに対しデフォルトプライオリティ、各キューの重みの関連、フレームプライオリティタグのマッピングをスイッチのキューに付けることができます。

コマンドグループ	機能	ページ
Priority（Layer 2）	タグなしフレームへのデフォルトプライオリティの設定、キューウエイトの設定、CoS タグのハードウェアキューへのマッピング	P523
Priority（Layer 3 and 4 ）	TCP ポート、IP DSCP タグの CoS 値への設定	P530

4.19.1 プライオリティコマンド（Layer 2）

コマンド	機能	モード	ページ
queue mode	キューモードを "strict" 又は " Weighted Round-Robin (WRR)" に設定	GC	P524
switchport priority default	入力タグなしフレームにポートプライオリティを設定	IC	P525
queue bandwidth	プライオリティキューに重み付けラウンドロビンを指定	GC	P526
queue cos map	プライオリティキューに Class of Service(CoS) を指定	IC	P527
show queue mode	現在のキューモードを表示	PE	P528
show queue bandwidth	プライオリティキューの重み付けラウンドロビンを表示	PE	P528
show queue cos-map	CoS マップの表示	PE	P529
show interfaces switchport	インタフェースの管理、運用ステータスの表示	PE	P415

queue mode

キューモードの設定を行います。CoS のプライオリティキューを strict 又は Weighted Round-Robin (WRR) のどちらのモードで行うかを設定します。"no" を前に置くことで初期設定に戻します。

文法

queue mode < strict | wrr | hybrid >

no queue mode

- **strict** ― 出力キューの高いプライオリティのキューが優先され、低いプライオリティのキューは高いプライオリティのキューがすべてなくなった後に送信されます。
- **wrr** ― WRR はキュー 0-3 にそれぞれスケジューリングウエイト 1、2、4、6 を設定し、その値に応じて帯域を共有します。
- **hybrid** ― 最高値のプライオリティ（3）のみ strict プライオリティキューイングにより処理を行い、3 よりも低いプライオリティ（0,1,2）は WRR キューイングで処理します。

初期設定

WRR(Weighted Round Robin)

コマンドモード

Global Configuration

コマンド解説

プライオリティモードを "strict" に設定した場合、出力キューの高いプライオリティのキューが優先され、低いプライオリティのキューは高いプライオリティのキューがすべてなくなった後に送信されます。

プライオリティモードを "wrr" に設定した場合、WRR はキュー 0-3 にそれぞれスケジューリングウエイト 1、2、4、6 を設定し、その値に応じて各キューの使用する時間の割合を設定し帯域を共有します。これにより "strict" モード時に発生する HOL Blocking を回避することが可能となります。

例

本例ではキューモードを Strict に設定しています。

```
Console(config)#queue mode strict
Console(config)#
```

switchport priority default

入力されるタグなしフレームに対してプライオリティを設定します。"no" を前に置くことで初期設定に戻します。

文法

switchport priority default *default-priority-id*

no switchport priority default

- *default-priority-id* — 入力されるタグなしフレームへのプライオリティ番号（0-7、7 が最高のプライオリティ）

初期設定

プライオリティ未設定。タグなしフレームへの初期設定値は 0。

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- プライオリティマッピングの優先順位は IP DSCP、デフォルトプライオリティの順番です。
- デフォルトプライオリティは、タグなしフレームを受信した際に設定されます。
  入力されたフレームが IEEE8021Q タグ付フレームの場合、IEEE802.1p のプライオリティ bit が使用されます。このプライオリティは IEEE802.1Q VLAN tagging フレームには適用されません。
- 本機では 8 段階のプライオリティキューを各ポートに提供します。それらは重み付けラウンドロビンを使用し、"show queue bandwidth" コマンドを使用し確認することが可能です。タグ VLAN ではない入力フレームは入力ポートでタグによりデフォルトプライオリティを付けられ、適切なプライオリティキューにより出力ポートに送られます。
  すべてのポートのデフォルトプライオリティは "0" に設定されています。したがって、初期設定ではプライオリティタグを持たないすべての入力フレームは出力ポートの "0" キューとなります（出力ポートがタグなしに設定されている場合、送信されるフレームは送信前にタグが取り外されます）

例

本例では 3 番ポートのデフォルトプライオリティを 5 に設定しています。

```
Console(config)#interface ethernet 1/3
Console(config-if)#switchport priority default 5
```

queue bandwidth

4 つの CoS に対し重み付けラウンドロビン (Weighted Round-Robin / WRR) による重み付けを行います。"no" を前に置くことで初期設定に戻します。

文法

queue bandwidth *weight1...weight8*

no queue bandwidth

- *weight1...weight4* - キュー 0 ～ 3 の WRR スケジューラで使用される重みの比率（範囲：1-15)

初期設定

1、2、4、8 がそれぞれキュー 0-3 に対応しています。キュー 0 は設定できません。

コマンドモード

Global Configuration

コマンド解説

WRR はスケジューリングされた重さでの出力ポートでのバンド幅の共用を許可します。

例

本例では WRR の重み付けを行っています。

```
Console(config)#queue bandwidth 6 9 12 12
Console(config)#
```

関連するコマンド

show queue bandwidth (P528)

queue cos-map

CoS 値をハードウェア出力キューのプライオリティキュー 0-3 に対応させます。"no" を前に置くことで初期設定に戻します。

文法

queue cos-map *queue_id* **[***cos1 ... cosn***]**

no queue cos-map

- *queue_id* - CoS プライオリティキュー ID

  ー 0-3 の値で 3 が最高の CoS プライオリティキュー

- *cos1 .. cosn* — キュー ID にマッピングする CoS 値。スペースでわけられた数字のリスト。CoS 値は 0-7 までの値で、7 が最高のプライオリティ

初期設定

各ポートに対し重み付けラウンドロビンと共に 4 段階のプライオリティキューの CoS をサポートします。8 つにわけられたトラフィッククラスが IEEE802.1p で定義されています。定義されたプライオリティレベルは IEEE802.1p 標準の推奨された以下のテーブルにより設定されます。

キュー	0	1	2	3
プライオリティ	1,2	0,3	4,5	6,7

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- 入力ポートで指定した CoS 値は出力ポートで使用されます。
- 本コマンドでは全インタフェースの CoS プライオリティを設定します。

例

本例では、CoS 値 0、1、2 を出力キュー 0 に、CoS 値 3 を出力キュー 1 に、CoS 値 4、5 を出力キュー 2 に、CoS 値 6、7 を出力キュー 3 に設定しています。

```
Console(config)#interface ethernet 1/1
Console(config-if)#queue cos-map 0 0
Console(config-if)#queue cos-map 1 1
Console(config-if)#queue cos-map 2 2
Console(config-if)#exit
Console#show queue cos-map ethernet 1/1
Information of Eth 1/1
Traffic Class : 0 1 2 3 4 5 6 7
Priority Queue: 0 1 2 1 2 2 3 3
Console#
```

show queue mode

現在のキューモードを表示します。

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#show queue mode

Queue mode: wrr
Console#
```

show queue bandwidth

ラウンドロビン (WRR) **バンド幅を表示します。**

初期設定

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 プライオリティマップを表示します。

文法

show queue cos-map { *interface* }

- *interface*

  ー **ethernet** *unit/port*

  unit ― **ユニット番号** ”1”

  port ― **ポート番号（範囲：**1-26）

  ー **port-channel** *channel-id*（**範囲：**1-12）

初期設定

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#
```

4.19.2 プライオリティコマンド（Layer 3 and 4）

コマンド	機能	モード	ページ
map ip dscp	IP DSCP の CoS キューへのマッピング	GC	P531
map ip port	TCP ポートの CoS キューへのマッピング	GC	P532
map ip precedence	IP precedence の CoS キューへのマッピング	GC	P533
map ip tos	IP ToS の CoS キューへのマッピング	GC	P534
map access-list ip	IP ACL ルールにマッチしたパケットの出力キュー設定	IC	P535
map access-list mac	MAC ACL ルールにマッチしたパケットの出力キュー設定	IC	P536
show map ip dscp	IP DSCP マップの表示	PE	P537
show map ip port	IP ポートマップの表示	PE	P537
show map ip precedence	IP Precedence マップの表示	PE	P538
show map ip tos	IP ToS マップの表示	PE	P539
show map access-list	インタフェースのアクセスリストにマッピングされた Cos 値を表示	PE	P540

map ip dscp

IP DSCP (Differentiated Services Code Point mapping) マッピングを有効にします。"no" を前に置くことで機能を無効にします。

文法

map ip dscp { *dscp-value* **cos** *cos-queue* }

no map ip dscp { *dscp-value* }

- *dscp-value* ― 8-bit DSCP 値（範囲：0-63）
- *cos-value* ― CoS 値（範囲：0-3）

初期設定

無効 (Disabled)

DSCP の初期値は以下の通りです。
下記の表は初期設定のマッピングです。マッピングされない DSCP 値はすべて CoS 値 0 に設定されます。

IP DSCP 値	CoS 値
0,8	0
10, 12, 14, 16, 18, 20, 22, 24	1
26, 28, 30, 32, 34, 36, 38, 40, 42	2
46, 48, 56	3

コマンドモード

Global Configuration

コマンド解説

- プライオリティマッピングの優先順位は IP ポート、IP Precedence/DSCP/ToS、デフォルトポートプライオリティです。
- 本コマンドで設定した IP DSCP プライオリティは全てのインタフェースに適用されます。

例

本例では本機に IP DSCP マッピングを有効にしています。

```
Console(config)#map ip dscp 1 cos 0
Console(config)#map ip dscp
Console(config)#
```

map ip port

IP ポートプライオリティマッピングを有効にします。"no" を前に置くことで機能も無効にします。

文法

map ip port { *port-number* **cos** *cos-queue* }

no map ip port { *port-number* }

- *port-number* ― 16-bit TCP/UDP ポート番号（範囲：1-65535）
- *cos-queue* ― CoS 値（範囲：0-3）

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

- プライオリティマッピングの優先順位は IP ポート、IP Precedence/DSCP/ToS、デフォルトポートプライオリティです。
- 本コマンドで設定した IP ポートプライオリティは全てのインタフェースに適用されます。

例

```
Console(config)#map ip port 80 cos 0
Console(config)#map ip port
Console(config)#
```

map ip precedence

IP precedence プライオリティマッピングを有効にします。"no" を前に置くことで機能も無効にします。

文法

map ip precedence { *precedence-value* **cos** *cos-queue*}

no map ip precedence { *precedence-value*}

- *precedence-value* — 3-bit precedence 値（範囲：0-7）
- *cos-queue* — CoS 値（範囲：0-3）

初期設定

なし

以下はデフォルトプライオリティマッピング値になります。

IP Precedence 値	0	1	2	3	4	5	6	7
CoS Queue	0	0	1	1	2	2	3	3

コマンドモード

Global Configuration

コマンド解説

- プライオリティマッピングの優先順位は IP ポート、IP Precedence/DSCP/ToS、デフォルトポートプライオリティです。
- 本コマンドで設定した IP Precedence プライオリティは全てのインタフェースに適用されます。

例

```
Console(config)#map ip precedence 1 cos 0
Console(config)#map ip precedence
```

map ip tos

IP ToS プライオリティマッピングを有効にします。"no" を前に置くことで機能も無効にします。

文法

map ip tos { *tos-value* **cos** *cos-queue* }

no map ip tos { *tos-value* }

- *tos-value* — 4-bit ToS 値（範囲：0-15）
- *cos-queue* — CoS 値（範囲：0-3）

初期設定

なし

以下はデフォルト CoS 値になります。
マッピングされない ToS 値はすべて CoS 値 0 に設定されます。

IP ToS 値	サービス	Default CoS Output Queue
0	Normal service	0
1	Minimize monetary cost	0
2	Maximize reliability	1
4	Maximize throughput	2
8	Minimize delay	3

コマンドモード

Global Configuration

コマンド解説

- プライオリティマッピングの優先順位は IP ポート、IP Precedence/DSCP/ToS、デフォルトポートプライオリティです。
- 本コマンドで設定した IP ToS プライオリティは全てのインタフェースに適用されます。

例

```
Console(config)#map ip tos 0 cos 1
Console(config)#map ip tos
```

map access-list ip

IP ACL ルールにマッチしたパケットの、出力キューを設定します。IP ToS プライオリティマッピングを有効にします。"no" を前に置くことで設定を削除します。

文法

map access-list ip *acl_name* **cos** *cos-queue*

no map access-list ip *acl_name*

- *acl_name* — IP ACL 名を指定（範囲：15 文字）
- *cos-queue* — CoS 値（範囲：0-3）

初期設定

なし

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- CoS キューのルールへのマップを行う前に ACL 設定を行ってください。

例

```
Console(config)#interface ethernet 1/2
Console(config-if)#map access-list ip bill cos 0
Console(config-if)#
```

map access-list mac

MAC ACL ルールにマッチしたパケットの、出力キューを設定します。IP ToS プライオリティマッピングを有効にします。"no" を前に置くことで設定を削除します。

文法

map access-list mac *acl_name* **cos** *cos-queue*

no map access-list mac *acl_name*

- *acl_name* — MAC ACL 名を指定（範囲：15 文字）
- *cos-queue* — CoS 値（範囲：0-3）

初期設定

なし

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- CoS キューのルールへのマップを行う前に ACL 設定を行ってください。

例

```
Console(config)#interface ethernet 1/2
Console(config-if)#map access-list mac steve cos 0
Console(config-if)#
```

show map ip dscp

IP DSCP プライオリティマップを表示します。

文法

show map ip dscp

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#show map ip dscp
dscp Mapping Status: Disabled
DSCP COS
---- ---
0 1
1 0
2 0
3 0
...
61 0
62 0
63 0
Console#
```

関連するコマンド

map ip dscp (P531)

show map ip port

IP ポートプライオリティマップを表示します。

文法

show map ip port

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#show map ip port
TCP Port Mapping Status: Disabled
Port no. COS
-------- ---
21 2
Console#
```

show map ip precedence

IP ポートプライオリティマップを表示します。

文法

show map ip precedence

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#show map ip precedence
Precedence Mapping Status: Enabled
Precedence COS
---------- ---
0 0
1 0
2 1
3 1
4 2
5 2
6 3
7 3
Console#
```

関連するコマンド

map ip precedence (P533)

show map ip tos

IP ToS プライオリティマップを表示します。

文法

show map ip tos

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#show map ip tos
tos Mapping Status: Disabled
TOS COS
--- ---
0  0
1  0
2  1
3  0
4  2
5  0
6  0
7  0
8  3
9  0
10  0
11  0
12  0
13  0
14  0
15  0
Console#
```

関連するコマンド

map ip tos (P534)

show map access-list

インタフェースの ACL **にマッピングされた** CoS **キューを表示します。**

文法

show map access-list <ip | mac> [*interface***]**

- **ip** ― IP ACL **を指定**
- **mac** ― MAC ACL **を指定**
- *interface*

― **ethernet** *unit/port*

unit ― **ユニット番号** ”1”

port ― **ポート番号（範囲：**1-26）

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#show map access-list ip
Eth 1/1
access-list ip aclname cos 3
Console#
```

4.20 Quality of Service

この章で記載されているコマンドは QoS(Quality of Service) 機能の基準とサービスポリシーを構成するために使用されます。DiffServ(Differentiated Services) 機能は、ネットワーク上を流れるフレームの 1 つの単位を特定のトラフィックの要件に合致させるため、ネットワークリソースを優先する管理機能を提供します。それぞれのパケットはアクセスリスト、IP Precedence、DSCP、VLAN リストをベースにしたネットワークの中のエントリによって分類されます。アクセスリストを使用することにより、それぞれのパケットが含んでいるレイヤ 2 ～ 4 の情報を元にトラフィックの選別を許可します。設定されたネットワークポリシーをベースにして、異なる種類のトラフィックに対し、異なる種類の転送のために印を付けることができます

コマンド	機能	モード	ページ
class-map	クラスマップを作成	GC	P542
match	クラス分類のためトラフィックに使う条件を定義	CM	P543
policy-map	ポリシーマップを作成	GC	P544
class	ポリシー上で実行するクラスを設定	PM	P545
set	IP パケットに適用する CoS、DSCP、IP Precedence の値を設定	PM-C	P546
police	クラス分けされたトラフィックに制限を設定	PM-C	P547
service-policy	ポリシーマップをインターフェースに適用	IC	P548
show class-map	クラスマップの情報を表示	PE	P549
show policy-map	ポリシーマップの情報を表示	PE	P550
show policy-map interface	インターフェースに設定されたポリシーマップの情報を表示	PE	P551

class-map

このコマンドはクラスマップを作成し、クラスマップコンフィグレーションモードに移行します。no を付けるとクラスマップを削除し、グローバルコンフィグレーションモードに戻ります。

文法

class-map *class-map-name* **{ match-any }**

no class-map *class-map-name*

- **match-any** ― クラスマップの条件のうちいずれか 1 つに一致するトラフィックを対象
- *class-map-name* ― クラスマップ名（1-16 文字）

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- 最初にこのコマンドを実行してクラスマップを作成し、クラスマップコンフィグレーションモードに入ります。次に入力トラフィックの分類条件を match コマンドで指定します。
- 1 つのクラスマップあたり最大 16 個、match コマンドを実行することができます。
- クラスマップは、パケットの分類、タグの付与、帯域幅の制限をインターフェースに対して行うため、ポリシーマップと同時に使用されます。

例

```
Console(config)#class-map rd_class match-any
Console(config-cmap)#match access-list sun
Console(config-cmap)#
```

関連するコマンド

show class map (P549)

match

このコマンドはトラフィックを分類するために使用する条件を設定します。

文法

match access-list *acl-name*

no match access-list *acl-name*

- *acl-name* — アクセスコントロールリスト名（1-16 文字）

初期設定

なし

コマンドモード

Class Map Configuration

コマンド解説

- 最初に class-map コマンドを実行してクラスマップを作成し、クラスマップコンフィグレーションモードに入ります。次にこのクラスマップ上で合致させたい入力パケット中の値を match コマンドで指定します。
- 1 つのクラスマップあたり 1 つの match コマンドのみ入力することができま

例

```
Console(config)#class-map rd_class#1 match-any
Console(config-cmap)#match access-list fxctest
Console(config-cmap)#
```

policy-map

このコマンドはポリシーマップを作成し、ポリシーマップコンフィグレーションモードに入ります。no を付けるとポリシーマップは削除され、グローバルコンフィグレーションモードに戻ります。

文法

policy-map *policy-map-name*

no policy-map *policy-map-name*

- *policy-map-name* — ポリシーマップ名（1-16 文字）

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- ポリシーマップの名前を設定するために policy-map コマンドを使用します。次にクラスマップで指定された条件に合致するトラフィックにポリシーを設定するため、class コマンドを使用します。
- ポリシーマップに複数のクラス設定を含めることができます。
- ポリシーマップを作成する前にクラスマップを作成する必要があります。

例

```
Console(config)#policy-map rd_policy
Console(config-pmap)#class rd_class
Console(config-pmap-c)#set ip dscp 3
Console(config-pmap-c)#police 100000 1522 exceed-action drop
Console(config-pmap-c)#
```

class

このコマンドはポリシーマップが実行するクラスマップを指定し、ポリシーマップ・クラスコンフィグレーションモードに入ります。no を付けるとクラスマップを削除し、ポリシーマップコンフィグレーションモードに戻ります。

文法

class *class-map-name*

no class *class-map-name*

- *class-map-name* ― クラスマップ名（1-16 文字）

初期設定

なし

コマンドモード

Policy Map Configuration

コマンド解説

- ポリシーマップの設定を行うために policy-map コマンドを使用し、ポリシーマップコンフィグレーションモードに入ります。次にポリシーマップ・クラスコンフィグレーションモードに入るために class コマンドを使用します。そして最後に、set コマンドと police コマンドを使用して設定を行います。
  - set ーコマンドは受信した IP パケットをクラス分けします。
  - police ーコマンドは最大スループット、バーストレート、ポリシーに反した場合の動作を定義します。
- 1 つのクラスマップあたり最大 16 個のルールを設定できます。また、ポリシーマップには複数のクラスを所属させることができます。

例

この例では "rd_policy" という名前のポリシーを作成し、class コマンドを使って前もって設定されたクラス "rd_class" を設定しています。次に set コマンドを使用して受信された入力パケットのクラス分けを行い、police コマンドで平均帯域幅を 100,000kbps、バーストレートを 1522bytes に制限し、それに反したパケットを破棄するよう設定しています。

```
Console(config)#policy-map rd_policy
Console(config-pmap)#class rd_class
Console(config-pmap-c)#set ip dscp 3
Console(config-pmap-c)#police 100000 1522 exceed-action drop
Console(config-pmap-c)#
```

set

このコマンドは match **コマンドで設定した条件に合致したパケットに** CoS、DSCP、IP Precedence **の値を** IP **パケットに付加します。**no **を付けるとトラフィックのクラス分けを取り止めます。**

文法

set [cos *new-cos* **| ip dscp** *new-dscp* **]**

no set [cos *new-cos* **| ip dscp** *new-dscp* **]**

- *new-cos* ― **新しく付加する** CoS **の値**（0-7）
- *new-dscp* ― **新しく付加する** DSCP **の値**（0-63）

初期設定

なし

コマンドモード

Policy Map Class Configuration

例

```
Console(config)#policy-map rd_policy
Console(config-pmap)#class rd_class
Console(config-pmap-c)#set ip dscp 3
Console(config-pmap-c)#police 100000 1522 exceed-action drop
Console(config-pmap-c)#
```

police

このコマンドはクラス分けされたトラフィックにポリサを設定します。no **を付けるとポリサの適用を取り止めます。**

文法

police *rate-kbps burst-byte* **{ exceed-action drop }**

no police *rate-kbps burst-byte* **{ exceed-action drop }**

- *rate-kbps* ― 1 **秒あたりの転送レート（単位：**kbps　**範囲：**1 ～ 100,000kbps）
- *burst-byte* ― **バーストレート** (**範囲：**64-1522 bytes)
- **exceed-action drop ― 設定した帯域幅とバーストレートを超えたパケットは破棄する。**

初期設定

drop

コマンドモード

Policy Map Class Configuration

コマンド解説

- **各アクセスリスト（**Standard ACL、Extended ACL、MAC ACL**）のそれぞれに最大** 64 **個のポリサを構成できます。**
- **ポリシングはトークンバケットを基にしています。バケットの深さ（バケットがオーバーフローする前の最大バーストレート）は** burst-byte **オプションで指定します。またバケットから移動するトークンの平均レートは** rate-kbps **オプションで指定します。**

例

```
Console(config)#policy-map rd_policy
Console(config-pmap)#class rd_class
Console(config-pmap-c)#set ip dscp 3
Console(config-pmap-c)#police 100000 1522 exceed-action drop
Console(config-pmap-c)#
```

service-policy

このコマンドはインターフェースの入力キューに policy-map **コマンドで定義されたポリシーマップを割り当てます。**no **を付けるとこのインターフェースからポリシーマップの割り当てを外します。**

文法

service-policy input *policy-map-name*

no service-policy input *policy-map-name*

- **input** ― **入力トラフィックにインタフェースを適用**
- *policy-map-name* ― **ポリシーマップ名（**1-16 **文字）**

初期設定

インタフェースにポリシーマップは未適用

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- **インターフェースには** 1 **つのポリシーマップのみ割り当てることができます。**
- **最初にクラスマップを定義し、次にポリシーマップを設定し、最後に** service-policy **コマンドを使用して必要なインターフェースにポリシーマップを関連付けてください。**

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#service-policy input rd_policy
Console(config-if)#
```

show class-map

このコマンドは match **コマンドで設定した** QoS **のクラスマップを表示します。**

文法

show class-map { *class-map-name* }

- *class-map-name* — **クラスマップ名（**1-16 **文字）**

初期設定

全てのクラスマップを表示

コマンドモード

Privileged Exec

例

```
Console#show class-map
Class Map match-any rd_class#1
Match ip dscp 3
Class Map match-any rd_class#2
Match ip precedence 5
Class Map match-any rd_class#3
Match vlan 1
Console#
```

show policy-map

このコマンドは QoS **のポリシーマップを表示します。**

文法

show policy-map { *interface* **input |** *policy-map-name* **class** *class-map-name***}**

- *interface*
  - *unit/port*
    unit — **ユニット番号** "1"
    port — **ポート番号（範囲：**1-26**）**
- **input** — **入力トラフィック**
- *policy-map-name* — **ポリシーマップ名（**1-16 **文字）**
- *class-map-name* — **クラスマップ名（**1-16 **文字）**

初期設定

全てのポリシーマップおよびクラスマップを表示

コマンドモード

Privileged Exec

例

```
Console#show policy-map
Policy Map rd_policy
class rd_class
set ip dscp 3
Console#show policy-map rd_policy class rd_class
Policy Map rd_policy
class rd_class
set ip dscp 3
Console#
```

show policy-map interface

このコマンドはインターフェースに割り当てられたサービスポリシーを表示します。.

文法

show policy-map interface *interface* **input**

- *interface*
  - **ethernet** *unit/port*
    unit — **ユニット番号** ”1”
    port — **ポート番号（範囲：**1-26）
  - port-channel *channel-id*（**範囲：**1-12）

コマンドモード

Privileged Exec

例

```
Console#show policy-map interface ethernet 1/5
Service-policy rd_policy input
Console#
```

4.21 Voice VLAN

IP 電話がエンタープライズネットワークに配置される場合、他のデータトラフィックから VoIP ネットワークを分離することを推奨します。トラフィックの分離は極端なパケット到達遅延、パケットロス、ジッターを防ぎ、より高い音声品質を得ることにつながります。これは 1 つの Voice VLAN にすべての VoIP トラフィックを割り当てることで実現できます。

Voice VLAN を使用することにはいくつかの利点があります。他のデータトラフィックから VoIP トラフィックを分離することでセキュリティが保たれます。エンドトゥーエンドの QoS ポリシーと高い優先度の設定により、ネットワークを横断して VoIP VLAN トラフィックに必要な帯域幅を保証することができます。また、VLAN 分割は音声品質に重大な影響を及ぼすブロードキャストやマルチキャストからトラフィックを保護することができます。

スイッチはネットワーク間で Voice VLAN を設定し、VoIP トラフィックに CoS 値を設定することができます。VoIP トラフィックはパケットの送信先 MAC アドレス、もしくは接続された VoIP デバイスを発見するために LLDP（IEEE802.1AB）を使うことで、スイッチポート上において検出されます。VoIP トラフィックが設定されたポート上で検出されたとき、スイッチは自動的に Voice VLAN のタグメンバーとしてポートを割り当てます。スイッチポートを手動で設定することもできます。

コマンド	機能	モード	ページ
voice vlan	Voice VLAN ID を設定	GC	P553
voice vlan aging	Voice VLAN ポートのエージングタイムを設定	GC	P553
voice vlan mac-address	VoIP デバイスの MAC アドレスを設定	GC	P554
switchport voice vlan	Voice VLAN ポートモードを設定	IC	P555
switchport voice vlan rule	自動 VoIP トラフィック検出メソッドをポートに設定	IC	P556
switchport voice vlan security	ポートの Voice VLAN セキュリティを有効	IC	P557
switchport voice vlan priority	ポートの VoIP トラフィックプライオリティを設定	IC	P557
show voice vlan	Voice VLAN 設定を表示	PE	P558

voice vlan

VoIP トラフィックの検出を有効にし、Voice VLAN ID を定義します。"no" を前に置くことで機能を無効にします。

文法

voice vlan *voice-vlan-id*

no voice vlan

- *voice-vlan-id* — Voice VLAN ID を指定します（範囲：1-4094）

初期設定

無効

コマンドモード

Global Configuration

例

```
Console(config)#voice vlan 1234
Console(config)#
```

voice vlan aging

Voice VLAN ID タイムアウトを設定します。"no" を前に置くことで設定を初期状態に戻します。

文法

voice vlan aging *minutes*

no voice vlan

- *minutes* — タイムアウトを指定します（範囲：5-43200 分）

初期設定

1440 分

コマンドモード

Global Configuration

例

```
Console(config)#voice vlan aging 3000
Console(config)#
```

voice vlan mac-address

OUI テレフォニーリストに追加する MAC アドレスの範囲を指定します。"no" を前に置くことでリストからエントリを削除します。

文法

voice vlan mac-address *mac-address* **mask** *mask-address* **{ description** *description* **}**

no voice vlan mac-address *mac-address* **mask** *mask-address*

- *mac-address* — ネットワーク上の VoIP デバイスを識別する MAC アドレス OUI を指定します。(例：01-23-45-00-00-00)
- *mask-address* — VoIP デバイスの MAC アドレスの範囲を確定します。
（範囲：80-00-00-00-00-00 to FF-FF-FF-FF-FF-FF　初期設定：FF-FF-FF-00-00-00）
- **description** — VoIP デバイスを識別するためのユーザー定義テキスト

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- Mask の設定－「FF-FF-FF-00-00-00」を設定すると同じ OUI 番号（最初の 3 オクテットが同一）であるすべてのデバイスを VoIP デバイスとして認識します。他の値を指定することで MAC アドレスの範囲を制限することができます。ここで「FF-FF-FF-FF-FF-FF」を選択すると 1 つの MAC アドレスのみ VoIP デバイスとして設定します

例

```
Console(config)#voice vlan mac-address 00-12-34-56-78-90 mask
ff-ff-ff-00-00-00 description A new phone
Console(config)#
```

switchport voice vlan

ポートの Voice VLAN **モードを指定します。**"no" **を前に置くことで、ポートの** Voice VLAN **機能を無効にします。**

文法

switchport voice vlan < manual | auto >

no switchport voice vlan

- **manual** ― Voice VLAN **機能はポート上で有効になりますが、ポートは手動で** Voice VLAN **に追加されます。**
- **auto** ― **ポートが** VoIP **トラフィックを検出したとき、ポートは** Voice VLAN **のタグメンバーとして追加されます。**VoIP **トラフィックを検出する方法を、**OUI **か** 802.1AB **のどちらかから選択しなくてはいけません。**OUI **を選択した場合、**Telephony OUI List **で** MAC **アドレスの範囲を確認してください。**

初期設定

無効

コマンドモード

Interface Configuration

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport voice vlan auto
Console(config-if)#
```

switchport voice vlan rule

ポートで VoIP **トラフィックを検出する方法を選択します。**"no" **を前に置くことで、選択した検出メソッドを無効にします。**

文法

switchport voice vlan rule <oui | lldp>

no switchport voice vlan rule <oui | lldp>

- **oui** — VoIP **デバイスからのトラフィックは送信元** MAC **アドレスの** Organizationally Unique Identifier（OUI）**によって検出されます。**OUI **番号は製造者によって割り当てられ、デバイスの** MAC **アドレスの最初の** 3 **オクテットを構成します。スイッチが** VoIP **デバイスからのトラフィックを認識するには、**MAC **アドレスの** OUI **番号を** Telephony OUI List **で構成しなくてはいけません。**
- **lldp** — **ポートに接続された** VoIP **デバイス発見するために** LLDP **を使用します。**LLDP **は** System Capability TLV **の中の** Telephone Bit **が有効であるかどうかをチェックします。**LLDP（Link Layer Discovery Protocol）**については** 436 **ページの「**LLDP **コマンド」を参照してください。**

初期設定

OUI：**有効**

LLDP：**無効**

コマンドモード

Interface Configuration

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport voice vlan rule oui
Console(config-if)#
```

switchport voice vlan security

ポートの、VoIP **トラフィックのセキュリティフィルタリングを有効にします。**"no" **を前に置くことで、フィルタリングを無効にします。**

文法

switchport voice vlan security

no switchport voice vlan security

初期設定

無効

コマンドモード

Interface Configuration

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport voice vlan security
Console(config-if)#
```

switchport voice vlan priority

ポートの VoIP **トラフィックに、**CoS **プライオリティを指定します。**"no" **を前に置くことで、設定を初期状態に戻します。**

文法

switchport voice vlan priority *priority-value*

no switchport voice vlan priority

priority-value ― CoS **プライオリティ値（範囲：**0-6）

初期設定

6

コマンドモード

Interface Configuration

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport voice vlan priority 5
Console(config-if)#
```

show voice vlan

Voice VLAN 設定情報および OUI テレフォニーリストを表示します。

文法

show voice vlan <oui | status>

oui ― OUI テレフォニーリストの表示します。

status ― グローバルおよびポートの Voice VLAN 設定を表示します。

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#show voice vlan status
Global Voice VLAN Status
Voice VLAN Status : Enabled
Voice VLAN ID : 1234
Voice VLAN aging time : 1440 minutes

Voice VLAN Port Summary
Port Mode Security Rule Priority
-------- -------- -------- --------- --------
Eth 1/ 1 Auto Enabled OUI 6
Eth 1/ 2 Disabled Disabled OUI 6
Eth 1/ 3 Manual Enabled OUI 5
Eth 1/ 4 Auto Enabled OUI 6
Eth 1/ 5 Disabled Disabled OUI 6
Eth 1/ 6 Disabled Disabled OUI 6
Eth 1/ 7 Disabled Disabled OUI 6
Eth 1/ 8 Disabled Disabled OUI 6
Eth 1/ 9 Disabled Disabled OUI 6
Eth 1/10 Disabled Disabled OUI 6

Console#show voice vlan oui
OUIAddress Mask Description
00-12-34-56-78-9A FF-FF-FF-00-00-00 old phones
00-11-22-33-44-55 FF-FF-FF-00-00-00 new phones
00-98-76-54-32-10 FF-FF-FF-FF-FF-FF Chris' phone

Console#
```

4.22 マルチキャストフィルタリング

IGMP (Internet Group Management Protocol) を使用し、特定のマルチキャストサービスを受けたいホストに対してクエリを実行します。リクエストしているホストが所属するポートを特定し、それらのポートにのみデータを送ります。マルチキャストサービスを受け取り続けるために、隣接するマルチキャストスイッチ / ルータにサービスリクエストを伝搬します。

コマンドグループ	機能	ページ
IGMP Snooping	IGMP snooping 又は静的設定によるマルチキャストグループの設定。IGMP バージョンの設定、設定状態、マルチキャストサービスグループやメンバーの表示	P559
IGMP Query	レイヤ 2 でのマルチキャストフィルタリングの IGMP query パラメータの設定	P566
Static Multicast Routing	静的マルチキャストルータポートの設定	P571
IGMP Filtering and Throttling	IGMP フィルタリングおよびスロットリングの設定	P573
Multicast VLAN Registration	MVR の設定	P583

4.22.1 IGMP Snooping コマンド

コマンド	機能	モード	ページ
ip igmp snooping	IGMP snooping の有効化	GC	P560
ip igmp snooping vlan static	インタフェースのマルチキャストグループへの追加	GC	P561
ip igmp snooping version	Snooping の IGMP バージョンの設定	GC	P562
ip igmp snooping leave-proxy	leave-proxy の有効化	GC	P563
ip igmp snooping immediate-leave	immediate-leave の有効化	IC	P563
show ip igmp snooping	IGMP snooping の設定の表示	PE	P564
show mac-address-table multicast	IGMP snooping の MAC アドレスマルチキャストリストの表示	PE	P565

ip igmp snooping

IGMP snooping を有効にします。"no" を前に置くことで機能を無効にします。

文法

ip igmp snooping

no ip igmp snooping

初期設定

有効 (Enabled)

コマンドモード

Global Configuration

例

本例では IGMP snooping **を有効にしています。**

```
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。"no" **を前に置くことでグループからポートを削除します。**

文法

ip igmp snooping vlan *vlan-id* **static** *ip-address interface*

no ip igmp snooping vlan *vlan-id* **static** *ip-address interface*

- *vlan-id* ― VLAN ID（**範囲：**1-4094）
- *ip-address* ― **マルチキャストグループの** IP **アドレス**
- *interface*

  ― **ethernet** *unit/port*

  unit ― **ユニット番号** ”1”

  port ― **ポート番号（範囲：**1-26）

  ― port-channel *channel-id*（**範囲：**1-12）

初期設定

なし

コマンドモード

Global Configuration

例

本例ではポートにマルチキャストグループを静的に設定しています。

```
Console(config)#ip igmp snooping vlan 1 static 224.0.0.12
ethernet 1/5
Console(config)#
```

ip igmp snooping version

IGMP snooping のバージョンを設定します。"no" を前に置くことで初期設定に戻します。

文法

ip igmp snooping version < 1 | 2 | 3 >

no ip igmp snooping version

- **1** ― IGMP Version 1
- **2** ― IGMP Version 2
- **3** ― IGMP Version 3

初期設定

IGMP Version 2

コマンドモード

Global Configuration

コマンド解説

- サブネット上のすべてのシステムが同じバージョンをサポートする必要があります。もし既存のデバイスが Version 1 しかサポートしていない場合、本機に対しても Version 1 を設定します。
- **"ip igmp query-max-response-time" コマンド及び "ip igmp router-port-expire-time" コマンドは** Version 2 **でしか使えません。**

例

本例では IGMP Version 1 **に設定しています。**

```
Console(config)#ip igmp snooping version 1
Console(config)#
```

ip igmp snooping leave-proxy

スイッチで IGMP Leave プロキシ を有効にします。"no" を前に置くことで無効にします。

文法

ip igmp snooping leave-proxy

no ip igmp snooping leave-proxy

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

- スイッチがクエリアとしてセットされている場合、leave プロキシは機能しません。

例

```
Console(config)#ip igmp snooping leave-proxy
Console(config)#
```

ip igmp snooping immediate-leave

指定した VLAN にて、IGMP の即時脱退を有効にします。
"no" を前に置くことで無効にします。

文法

ip igmp snooping immediate-leave

no ip igmp snooping immediate-leave

初期設定

無効

コマンドモード

Interface Configuration(VLAN)

例

```
Console(config)#interface vlan 1
Console(config-if)#ip igmp snooping immediate-leave
Console(config-if)#
```

show ip igmp snooping

IGMP snooping の設定情報を表示します。

文法

show ip igmp snooping { mrouter { vlan *vlan-id* **} }**

- **mrouter** ― マルチキャストルータポートの情報を表示
- *vlan-id* ― VLAN ID（範囲：1-4094）

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

表示される内容に関しては、P188 「IGMP Snooping Query パラメータの設定」を参照して下さい。

例

本例では現在の IGMP snooping の設定を表示しています。

```
Console#show ip igmp snooping
Service status: Enabled
Querier status: Enabled
Leave proxy status: Disabled
Query count: 10
Query interval: 100 sec
Query max response time: 20 sec
Router port expire time: 300 sec
Immediate Leave Processing: Disabled on all VLAN
IGMP snooping version: Version 2
Console#
```

show mac-address-table multicast

マルチキャストアドレスとして認識されているリストを表示します。

文法

show mac-address-table multicast { vlan *vlan-id* | **user | igmp-snooping }**

- *vlan-id* ― VLAN ID（**範囲：**1-4094)
- **user** ― **ユーザ設定のマルチキャストエントリのみ表示**
- **igmp-snooping** ― IGMP snooping **によって学習されたアドレスのみ表示**

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

メンバーの種類は選択したオプションにより IGMP **又は** USER **を含む表示がされます。**

例

本例では VLAN 1 **で** IGMP snooping **により登録されたマルチキャストエントリを表示しています。**

```
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#
```

4.22.2 IGMP Query コマンド（Layer2）

コマンド	機能	モード	ページ
ip igmp snooping querier	IGMP snooping クエリアとしての動作の有効化	GC	P566
ip igmp snooping query-count	クエリーカウントの設定	GC	P567
ip igmp snooping query-interval	クエリー間隔の設定	GC	P568
ip igmp snooping query-maxrsponse-time	レポート遅延の設定	GC	P569
ip igmp snooping rouoter-port-expire-time	クエリータイムアウトの設定	GC	P570

ip igmp snooping querier

IGMP snooping クエリアとしての機能を有効にします。"no" を前に置くことで機能を無効にします。

文法

ip igmp snooping querier

no ip igmp snooping querier

初期設定

有効 (Enabled)

コマンドモード

Global Configuration

コマンド解説

有効にした場合、本機はクエリアとして機能します。クエリアはマルチキャストトラフィックを受け取る必要があるかどうか、ホストに質問します。

例

```
Console(config)#ip igmp snooping querier
Console(config)#
```

ip igmp snooping query-coount

クエリーカウントの設定を行います。"no" を前に置くことで初期設定に戻します。

文法

ip igmp snooping query-count *count*

no ip igmp snooping query-count

- *count* ― マルチキャストグループからクライアントを除外する前に、スイッチからクエリ送信する最大回数（範囲：2-10）

初期設定

2 回

コマンドモード

Global Configuration

コマンド解説

クエリーカウントではマルチキャストクライアントからの応答をクエリアが待つ回数を定めます。クエリアが本コマンドで定義された数のクエリーを送り、クライアントからの応答がなかった場合、" ip igmp snooping query-max-response-time" コマンドで指定したカウントダウンタイマーがスタートします。

カウントダウンが終わり、クライアントからの応答がない場合、クライアントがマルチキャストグループからはずれたと判断されます。

例

本例では、クエリーカウントを 10 に設定しています。

```
Console(config)#ip igmp snooping query-count 10
Console(config)#
```

関連するコマンド

ip igmp snooping query-max-response-time (P569)

ip igmp snooping query-interval

クエリの送信間隔を設定します。"no" **を前に置くことで初期設定に戻します。**

文法

ip igmp snooping query-interval *seconds*

no ip igmp snooping query-interval

- *seconds* — IGMP **クエリを送信する間隔（範囲：**60-125)

初期設定

125**（秒）**

コマンドモード

Global Configuration

例

本例ではクエリ間隔を 100 **秒に設定しています。**

```
Console(config)#ip igmp snooping query-interval 100
Console(config)#
```

ip igmp snooping query-max-response-time

クエリの送信間隔を設定します。"no" **を前に置くことで初期設定に戻します。**

文法

ip igmp snooping query-max-response-time *seconds*

no ip igmp snooping query-max-response-time

- *seconds* — IGMP **クエリを送信する間隔（範囲：**5-25)

初期設定

10**（秒）**

コマンドモード

Global Configuration

コマンド解説

- **本機能を有効にするには** IGMP v2 **を使用する必要があります。**
- **クエリ後のマルチキャストクライアントからの正式な回答があるまでの待ち時間を設定します。クエリアが送信するクエリ数を** " ip igmp snooping query-count" **コマンドを使用して設定している場合、クライアントからの応答がないとカウントダウンタイマーが本コマンドで設定した値でスタートします。カウントダウンが終わり、クライアントからの応答がない場合、クライアントがマルチキャストグループからはずれたと判断されます。**

例

本例では、最大返答時間を 20 **秒に設定しています。**

```
Console(config)#ip igmp snooping query-max-response-time 20
Console(config)#
```

ip igmp snooping router-port-expiretime

クエリータイムアウト時間の設定を行います。"no" を前に置くことで初期設定に戻します。

文法

ip igmp snooping router-port-expire-time *seconds*

no ip igmp snooping router-port-expire-time

- *seconds* — クエリーパケットを受信していたルータポートが無効になると判断される前の待機時間（範囲：300-500（秒））

初期設定

300（秒）

コマンドモード

Global Configuration

コマンド解説

本機能を有効にするには IGMP v2 を使用する必要があります。

例

本例では、タイムアウト時間を 300（秒）に設定しています。

```
Console(config)#ip igmp snooping router-port-expire-time 300
Console(config)#
```

関連するコマンド

ip igmp snooping version (P562)

4.22.3 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の追加	GC	P571
show ip igmp snooping mrouter	マルチキャストルータポートの表示	PE	P572

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。"no" **を前に置くことで設定を削除します。**

文法

ip igmp snooping vlan *vlan-id* **mrouter** *interface*

no ip igmp snooping vlan *vlan-id* **mrouter** *interface*

- *vlan-id* - VLAN ID（**範囲：**1-4094）
- *interface*
  - **ethernet** *unit/port*
    unit — **ユニット番号** ”1”
    port — **ポート番号（範囲：**1-26）
  - port-channel *channel-id*（**範囲：**1-12）

初期設定

静的マルチキャストルータポートは設定されていません。

コマンドモード

Global Configuration

コマンド解説

ネットワーク接続状況により、IGMP snooping **では常に** IGMP **クエリアが配置されません。したがって、**IGMP **クエリアがスイッチに接続された既知のマルチキャストルータ / スイッチである場合、インタフェースをすべてのマルチキャストグループに参加させる設定を手動で行えます。**

例

本例では 11 **番ポートを** VLAN 1 **のマルチキャストルータポートに設定しています。**

```
Console(config)#ip igmp snooping vlan 1 mrouter ethernet 1/11
Console(config)#
```

show ip igmp snooping mrouter

静的設定及び動的学習によるマルチキャストルータポートの情報の表示を行います。

文法

show ip igmp snooping mrouter { vlan *vlan-id* **}**

- *vlan-id* ― VLAN ID（範囲：1-4094）

初期設定

VLAN に設定されたすべてのマルチキャストルータポートを表示します。

コマンドモード

Privileged Exec

コマンド解説

マルチキャストルータポートとして表示されるタイプには静的及び動的の両方が含まれます。

例

本例では、VLAN 1 のマルチキャストルータに接続されたポートを表示します。

```
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#
```

4.22.4 IGMP Filtering/Throttling コマンド

特定の定期購読契約に基づいた IP/TV サービス等の環境において、管理者が、エンドユーザーの入手できるマルチキャストサービスの制御を希望するケースがあります。

IGMP フィルタリングは、指定されたスイッチポート上のマルチキャストサービスへのアクセス制限したり、同時にアクセスできるマルチキャストグループの数を調整することによって、この条件を満たすことが可能です。

IGMP フィルタリング機能を使用することにより、プロファイルを特定のマルチキャストグループのスイッチ ポートに割り当て、ポート単位でマルチキャスト加入をフィルタリングできます。

コマンド	機能	モード	ページ
ip igmp filter	スイッチで IGMP フィルタリング / スロットリングを有効	GC	P573
ip igmp profile	プロファイル番号の設定及び IGMP profile 設定モードへ移行	GC	P574
permit, deny	プロファイルアクセスモードを設定	IPC	P575
range	プロファイルのマルチキャストアドレスを設定	IPC	P576
ip igmp filter	IGMP フィルタプロファイルをインタフェースへアサイン	IC	P577
ip igmp max-groups	IGMP スロットリング番号を指定	IC	P578
ip igmp max-groups action	インタフェースのスロットリングアクションを設定	IC	P579
show ip igmp filter	IGMP フィルタリングステータスを表示	PE	P580
show ip igmp profile	IGMP プロファイルおよび設定の表示	PE	P581
show ip igmp throttle interface	インタフェースの IGMP スロットリング設定を表示	PE	P582

ip igmp filter (Global Configuration)

本コマンドは IGMP フィルタリングおよびスロットリングを、スイッチで有効にします。"no" を前に置くことで機能を無効にします。

文法

ip igmp filter

no ip igmp filter

初期設定

無効

コマンドモード

Global Configuration

例

```
Console(config)#ip igmp filter
Console(config)#
```

ip igmp profile

本コマンドを実行することで、IGMP **フィルタプロファイル番号の作成を行うと共に、**
IGMP **プロファイル設定モード（**IPC **モード）へ移行します。**
"no" **を前に置くことでプロファイル番号を削除します。**

文法

ip igmp profile *profile-number*

no ip igmp profile *profile-number*

- *profile-number*― IGMP **フィルタプロファイル番号（範囲：**1-4294967295）

初期設定

無効

コマンドモード

Global Configuration

例

```
Console(config)#ip igmp profile 19
Console(config-igmp-profile)#
```

permit, deny

IGMP フィルタプロファイルにアクセスモードを設定します。

文法

permit | deny

初期設定

Deny

コマンドモード

IGMP Profile Configuration

コマンド解説

- それぞれのプロフィールはひとつのアクセスモードが設定されます。（許可もしくは拒否）
- アクセスモードが許可に設定時、マルチキャストグループが制御されたコントロール範囲に一致した場合、IGMP join レポートが処理されます。拒否に設定時、マルチキャストグループが制御されたコントロール範囲に一致しない場合のみ、IGMP join レポートが処理されます。

例

```
Console(config)#ip igmp profile 19
Console(config-igmp-profile)#permit
Console(config-igmp-profile)#
```

range

プロファイルの、マルチキャストグループアドレスを設定します。

"no" **を前に置くことでプロファイルからアドレスを削除します。**

文法

range *low-ip-address* { *high-ip-address* }

no range *low-ip-address* { *high-ip-address* }

- *low-ip-address*— **マルチキャストグループ** IP **アドレス、または指定する範囲の最初の** IP **アドレス**
- *high-ip-address*— **指定する範囲の最後の** IP **アドレス**

初期設定

なし

コマンドモード

IGMP Profile Configuration

例

```
Console(config)#ip igmp profile 19
Console(config-igmp-profile)#range 239.1.1.1
Console(config-igmp-profile)#range 239.2.3.1 239.2.3.100
Console(config-igmp-profile)#
```

ip igmp filter (Interface Configuration)

IGMP フィルタリングプロファイルを、スイッチ上のインタフェースに割り当てます。

"no" を前に置くことでインタフェースからプロファイルを取り除きます。

文法

ip igmp filter *profile-number*

no ip igmp filter { *profile-number* }

- *profile-number*— IGMP フィルタプロファイル番号（範囲：1-4294967295）

初期設定

なし

コマンドモード

Interface Configuration

コマンド解説

- インタフェースにアサインできるプロファイルは１つのみです。
- ポートがトランクのメンバーである場合、トランクは、最初にポートメンバーへ適用された設定を使用します。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip igmp filter 19
Console(config-if)#
```

ip igmp max-groups

スイッチ上のインタフェースに、IGMP **スロットリング番号を設定します。**"no" **を前に置くことで初期設定へ戻します。**

文法

ip igmp max-groups *number*

no ip igmp max-groups

- *number*—**インターフェイスが加入できる** IGMP **グループの最大数（範囲：**0-1024）

初期設定

1024

コマンドモード

Interface Configuration

コマンド解説

- **ポートがトランクのメンバーである場合、トランクは、最初にポートメンバーへ適用された設定を使用します。**

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip igmp max-groups 10
Console(config-if)#
```

ip igmp max-groups action

スイッチ上のインタフェースに、IGMP スロットリングアクションを設定します。

文法

ip igmp max-groups action < replace | deny >

- replace―既存のマルチキャストグループは、新しいグループへ置き換えられます。
- deny―新規のレポートは破棄されます。

初期設定

Deny

コマンドモード

Interface Configuration

コマンド解説

- IGMP スロットリングは、同時に加入が可能なマルチキャストグループポートの最大値を設定します。グループ数が、設定した最大値に達した時、スイッチは「どちらも拒否する」「置き換え」の内どちらかの処理を行うことができます。
「拒否する」設定になっている場合、全ての新規 IGMP join レポートは破棄されます。
「置き換え」設定になっている場合、スイッチはランダムに既存のグループを取り去り、新しいマルチキャストグループに置き換えます。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip igmp max-groups action replace
Console(config-if)#
```

show ip igmp filter

グローバルおよび、インタフェースの IGMP **フィルタリング設定を表示します。**

文法

show ip igmp filter { interface *interface* **}**

- *interface*
  - **ethernet** *unit/port*
    unit ― **ユニット番号** ”1”
    port ― **ポート番号（範囲：**1-26）
  - port-channel *channel-id*（**範囲：**1-12）

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#show ip igmp filter
IGMP filter enabled
Console#show ip igmp filter interface ethernet 1/1
Ethernet 1/1 information
---------------------------------
IGMP Profile 19
Deny
range 239.1.1.1 239.1.1.1
range 239.2.3.1 239.2.3.100
Console#
```

show ip igmp profile

スイッチ上の IGMP **フィルタリングプロファイルを表示します。**

文法

show ip igmp profile [*profile-number***]**

- *profile-number*―**既存の** IGMP **フィルタプロファイル番号（範囲：**1-4294967295**）**

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#show ip igmp profile
IGMP Profile 19
IGMP Profile 50
Console#show ip igmp profile 19
IGMP Profile 19
Deny
range 239.1.1.1 239.1.1.1
range 239.2.3.1 239.2.3.100
Console#
```

show ip igmp throttle interface

IGMP スロットリングのインタフェース設定を表示します。

文法

show ip igmp throttle interface [*interface***]**

- *interface*

  − **ethernet** *unit/port*

  unit ― ユニット番号 ”1”

  port ― ポート番号（範囲：1-26）

  − port-channel *channel-id*（範囲：1-12）

初期設定

なし

コマンドモード

Privileged Exec

例

本例では、VLAN 1 のマルチキャストルータに接続されたポートを表示します。

```
Console#show ip igmp throttle interface ethernet 1/1
Eth 1/1 Information
Status : TRUE
Action : Deny
Max Multicast Groups : 32
Current Multicast Groups : 0
Console##
```

4.23 MVR の設定

この章は Multicast VLAN Registration(MVR) を設定するために使用されるコマンドを記載しています。

サービスプロバイダーのネットワークを通して広いシングルネットワークの VLAN にマルチキャストトラフィック（例：テレビのチャンネル）を送信することができます。

MVR VLAN に入ったどのマルチキャストトラフィックもすべての Subscribers に送信することができます。これは動的な監視に必要なオーバーヘッドのプロセスを著しく減少させ、正常なマルチキャスト VLAN の配信ツリーを確立します。

また、MVR は他の VLAN から Subscribers が属する VLAN にマルチキャストトラフィックだけを通過させることによって、VLAN を分割することによるユーザーの分離とデータ保護機能を維持します。

コマンド	機能	モード	ページ
mvr	MVR の有効、および MVR グループアドレスや MVR VLAN ID を静的に構成	GC	P584
mvr	インタフェースを MVR レシーバーポート・ソースポートに設定、Immediate Leave 機能の有効、インターフェースの MVR VLAN への登録	IC	P585
show mvr	MVR 設定、MVR VLAN 関連のインタフェース、MVR VLAN に割り当てられたマルチキャストグループアドレスを表示	PE	P587

mvr (Global Configuration)

このコマンドはスイッチ上で Multicast VLAN Registration(MVR) を有効にします。group オプションで MVR マルチキャストグループの IP アドレスを静的に構成します。VLAN オプションで MVR VLAN の ID を設定します。オプションなしでこのコマンドに no を付けると MVR 機能を無効にします。group オプションと同時に no を付けると特定のアドレス、もしくは複数のアドレスを消去します。vlan キーワードに no を付けると MVR VLAN ID の設定はデフォルトに戻ります。

文法

mvr { group *ip-address* { count } **| vlan** *vlan-id* **}**

no mvr { group *ip-address* { count } **| vlan }**

- *ip-address* — MVR マルチキャストグループの IP アドレス（範囲：224.0.1.0-239.255.255.255）
- *count* — 連続する MVR グループアドレスの番号（範囲：1-255）
- *vlan-id* — MVR VLAN ID（範囲：1-4097）

初期設定

MVR は無効、グループアドレスは指定されていません。

コマンドモード

Global Configuration

コマンド解説

- mvr group コマンドを使用して MVR VLAN に参加するすべてのマルチキャストグループアドレスを静的に構成することができます。MVR グループに関連付けられたどのマルチキャストデータもすべてのソースポートから、マルチキャストのデータを受信するよう登録されたすべてのレシーバーポートに送信されます。
- 224.0.0.0 ～ 239.255.255.255 の範囲の IP アドレスはマルチキャストストリームとして使用されます。予約された IP マルチキャストアドレス（224.0.0.0 ～ 224.0.0.255）は MVR グループアドレスとして使用することができません。
- Subscriber を MVR グループに動的に参加・離脱するために IGMP Snooping を有効にしなくてはいけません。IGMP のバージョンが 2 か 3 のホストのみマルチキャストへの参加・離脱メッセージを発することができます。

例

本例では、VLAN 1 のマルチキャストルータに接続されたポートを表示します。

```
Console(config)#mvr
Console(config)#mvr group 228.1.23.1 10
Console(config)#
```

mvr (Interface Configuration)

type オプションを使用することでインターフェースを MVR レシーバーポート、もしくはソースポートに設定することができます。immediate オプションを使用することで Immediate Leave 機能を有効にすることができます。group オプションを使用することでインターフェースを MVR VLAN の固定メンバーに設定することができます。no を付けると設定が初期状態に戻ります。

文法

mvr [type <receiver | source> | immediate | group *ip-address*]

no mvr [type | immediate | group *ip-address*]

- **receiver** ― インタフェースをマルチキャストデータを受信可能な加入者ポートに設定
- **source** ― インタフェースを送受信可能なアップリンクポートに設定
- **immediate** ― 即刻脱退機能を使用
- *ip-address*― IP アドレスを静的に設定（範囲：224.0.1.0-239.255.255.255）

初期設定

ポートタイプ：未設定

immediate leave：無効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- MVR のレシーバーポートもしくはソースポートとして構成されていないポートは、マルチキャストフィルタリングの標準ルールを使用するマルチキャストグループへ参加・離脱するために IGMP Snooping を使うことができます。
- MVR レシーバーポートはトランクのメンバーになることができません。レシーバーポート同士は複数の VLAN に所属することができますが、これを MVR VLAN のメンバーとして構成すべきではありません。IGMP Snooping はレシーバーポートが MVR VLAN のマルチキャストグループに、動的に参加・離脱を許可するために使用されます。group オプションを使用してレシーバーポートにマルチキャストグループを静的に割り当てることもできます。
- 1 つ、もしくはそれ以上の数のインターフェースは MVR ソースポートとして構成することができます。ソースポートは IGMP Snooping 機能を通してグループに参加するか、group オプションを使用して静的に割り当てたマルチキャストグループの間で受信と送信の両方ができます。
- 224.0.0.0 ～ 239.255.255.255 の範囲の IP アドレスはマルチキャストストリームとして使用されます。予約された IP マルチキャストアドレス（224.0.0.0 ～ 224.0.0.255）は MVR グループアドレスとして使用することができません。
- Immediate Leave 機能はレシーバーポートのみに適用されます。有効にしたとき、レシーバーポートは離脱メッセージに記録されたマルチキャストグループから即座に取

り除かれます。Immediate Leave を無効にしたとき、スイッチはグループリストからポートを取り除く前にマルチキャストグループの Subscriber が残っている場合、レシーバーポートに特定のグループのクエリを送信し決定するための返事を待つという、標準のルールに従います。

- Immediate Leave 機能で離脱するまでの時間を短くすることができますが、同じインターフェースに接続されているグループメンバーへのサービスを混乱させることを避けるため、1 つのマルチキャストの Subscriber がポートに接続されている場合のみ有効にしてください。
- Immediate Leave 機能はポートに固定的に割り当てられたマルチキャストグループには適用されません。
- Subscriber を MVR グループに動的に参加・離脱するために IGMP Snooping を有効にしなくてはいけません。IGMP のバージョンが 2 か 3 のホストのみマルチキャストへの参加・離脱メッセージを発することができます。

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#mvr type source
Console(config-if)#exit
Console(config)#interface ethernet 1/6
Console(config-if)#mvr type receiver
Console(config-if)#mvr immediate
Console(config-if)#exit
Console(config)#interface ethernet 1/7
Console(config-if)#mvr type receiver
Console(config-if)#mvr group 225.0.0.5
Console(config-if)#
```

show mvr

MVR の情報を表示します。

文法

show mvr { interface *interface* **| members {** *ip-address***} }**

- *interface*
  - **ethernet** *unit/port*
    unit — **ユニット番号** ”1”
    port — **ポート番号（範囲：**1-26）
  - port-channel *channel-id*（**範囲：**1-12）
- *ip-address* — MVR **マルチキャストグループの** IP **アドレス**
  （範囲：224.0.1.0-239.255.255.255）

初期設定

なし

コマンド解説

MVR **のレシーバーポートもしくはソースポートとして構成されていないポートは、マルチキャストフィルタリングの標準ルールを使用するマルチキャストグループへ参加・離脱するために** IGMP Snooping **を使うことができます。**

例

グローバル MVR **設定を表示します。**

```
Console#show mvr
MVR Status:enable
MVR running status:TRUE
MVR multicast vlan:1
MVR Max Multicast Groups:255
MVR Current multicast groups:10
Console#
```

Field	解説
MVR Status	MVR **がスイッチ上で有効であるかを表示**
MVR Running Status	MVR **環境の中のすべての必要条件が満たさているかを表示**
MVR Multicast VLAN	**全ての** MVR **マルチキャストトラフィックを転送される** VLAN
MVR Max Multicast Group	MVR VLAN **にアサイン可能なマルチキャストグループの最大数**
MVR Current multiccast Group	**現在** MVR VLAN **にアサインされているマルチキャストグループの最大数**

例

インタフェース情報を表示します。:

```
Console#show mvr interface
Port Type Status Immediate Leave
------- -------- ------------ --------------
eth1/1 SOURCE ACTIVE/UP Disable
eth1/2 RECEIVER ACTIVE/UP Disable
eth1/5 RECEIVER INACTIVE/DOWN Disable
eth1/6 RECEIVER INACTIVE/DOWN Disable
eth1/7 RECEIVER INACTIVE/DOWN Disable
Console#
```

Field	解説
Port	MVR VLAN に付加されているインタフェース
Type	MVR ポートタイプ
Status	MVR がスイッチで有効の場合 “ ACTIVE ” レシーバポートの MVR が “ ACTIVE ” の場合、加入者が MVR グループの内ひとつからマルチキャストトラフィックを受信中、またはマルチキャストグループはインタフェースに静的にアサイン
Immediate Leave	即時脱退の有効 / 無効

例

```
Console#show mvr members
MVR Group IP Status Members
---------------- -------- -------
225.0.0.1 ACTIVE eth1/1(d), eth1/2(s)
225.0.0.2 INACTIVE None
225.0.0.3 INACTIVE None
225.0.0.4 INACTIVE None
225.0.0.5 INACTIVE None
225.0.0.6 INACTIVE None
225.0.0.7 INACTIVE None
225.0.0.8 INACTIVE None
225.0.0.9 INACTIVE None
225.0.0.10 INACTIVE None
Console#
```

Field	解説
MVR Group IP	MVR VLAN にアサインしているマルチキャストグループ
Status	マルチキャストグループにアクティブな加入者が存在するかどうかを表示。 MVR がグローバルで無効の場合、“ INACTIVE ”が表示。
Members	マルチキャストサービスの加入インタフェースを表示。

4.24 IP インタフェース

IP アドレスは本機へのネットワーク経由での管理用アクセスの際に使用されます。初期設定では DHCP を使用して IP アドレスの取得を行う設定になっています。IP アドレスは手動で設定することも、又 BOOTP/DHCP サーバから電源投入時に自動的に取得することもできます。また、他のセグメントから本機へのアクセスを行うためにはデフォルトゲートウェイの設定も必要となります。

4.24.1 基本 IP 設定

コマンド	機能	モード	ページ
ip address	本機への IP アドレスの設定	IC	P589
ip default-gateway	本機と管理端末を接続するためのゲートウェイ設定の表示	GC	P591
ip dhcp restart	BOOTP/DHCP クライアントリクエストの送信	PE	P592
show ip interface	本機の IP 設定の表示	PE	P593
show ip redirects	本機のデフォルトゲートウェイ設定の表示	PE	P593
ping	ネットワーク上の他のノードへの ICMP echo リクエストパケットの送信	NE,PE	P594

ip address

本機への IP アドレスの設定を行います。"no" を前に置くことで初期設定に戻します。

文法

ip address [*ip-address netmask* **| bootp | dhcp]**

no ip address

- *ip-address* — IP アドレス
- *netmask* — サブネットマスク
- **bootp** — IP アドレスを BOOTP から取得します。
- **dhcp** — IP アドレスを DHCP から取得します。

初期設定

DHCP

コマンドモード

Interface Configuration (VLAN)

コマンド解説

- 管理用にネットワーク経由で本機へアクセスする場合、IP アドレスの設定が必須となります。手動で IP アドレスを入力する方法と、BOOTP、DHCP を使用して自動で IP アドレスを取得する方法があります。
- bootp 又は dhcp を選択した場合、BOOTP 又は DHCP からの応答があるまで IP アドレスは設定されません。IP アドレスを取得するためのリクエストは周期的にブロードキャストで送信されます（BOOTP 及び DHCP によって取得できるのは IP アドレス、サブネットマスク及びデフォルトゲートウェイの値です）
- BOOTP 又は DHCP に対するブロードキャストリクエストは "ip dhcp restart" コマンドを使用するか、本機を再起動させた場合に行われます。

[注意] IP アドレスは VLAN インタフェース 1 つのみに割り当てできます（初期設定では VLAN1 に割り当てるようになっています）ここで設定した VLAN が管理用の VLAN となり、この VLAN を介してのみ本機への管理アクセスが可能になります。IP アドレスを他の VLAN に割り当てると、新たに割り当てた IP アドレスが既存の IP アドレスを上書きし、新たな管理 VLAN として機能します。

例

本例では、VLAN 1 に対して IP アドレスを設定しています。

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.5 255.255.255.0
Console(config-if)#
```

関連するコマンド

ip dhcp restart (P592)

ip default-gateway

セグメントがわかれたスイッチと管理端末を接続するためのデフォルトゲートウェイの設定を行います。"no" **を前に置くことでデフォルトゲートウェイを削除します。**

文法

ip default-gateway *gateway*

no ip default-gateway

- *gateway* ― **デフォルトゲートウェイの** IP **アドレス**

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

異なるセグメントに管理端末が設置されている場合には必ず設定する必要があります。

例

本例ではデフォルトゲートウェイの設定を行っています。

```
Console(config)#ip default-gateway 10.1.1.254
Console(config)#
```

関連するコマンド

show ip redirects (P593)

ip dhcp restart

BOOTP/DHCP クライアントリクエストを送信します。

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

- "ip address" コマンドで BOOTP 又は DHCP に設定済みの IP インタフェースに対し、BOOTP/DHCP クライアントリクエストを送信します。
- DHCP は、有効な場合、サーバにクライアントの最後の IP アドレスを再付与するよう要求します。
- DHCP/BOOTP サーバが別のドメインに移動した場合、クライアントに付与されていた IP アドレスのネットワーク部は新たなドメインの IP アドレスとなります。

例

本例ではデフォルトゲートウェイの設定を行っています。

```
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#
```

関連するコマンド

ip address (P589)

show ip interface

IP インタフェースの設定を表示します。

初期設定

すべてのインタフェース

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#
```

関連するコマンド

show ip redirects (P593)

show ip redirects

デフォルトゲートウェイの設定を表示します。

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#show ip redirects
ip default gateway 10.1.0.254
Console#
```

関連するコマンド

ip default-gateway (P591)

ping

ネットワーク上の他のノードに対し ICMP echo **リクエストパケットを送信します。**

文法

ping *host* **{ count** *count* **} {size** *size* **}**

- *host* ― **ホストの** IP **アドレス / エイリアス**
- *size* ― **パケットのサイズ** (bytes)**（範囲** 32-512**、初期設定：**32**）**
  ヘッダ情報が付加されるため、実際のパケットサイズは設定した値より 8bytes **大きくなります。**
- *count* ― **送信するパケット数（範囲：**1-16**、初期設定：**5**）**

初期設定

設定されたホストはありません。

コマンドモード

Normal Exec, Privileged Exec

コマンド解説

- ping **コマンドを使用することでネットワークの他の場所（端末など）に接続されているか確認することができます。**
- ping **コマンドの結果は以下のような内容となります：**
  - Normal response ― **正常なレスポンスは、ネットワークの状態に依存して、**1 ～ 10 **秒で生じます**
  - Destination does not respond ― **ホストが応答しない場合、**"timeout" **が** 10 **秒以内に表示されます**
  - Destination unreachable ― **目的のホストに対するゲートウェイが見つからない場合**
  - Network or host unreachable ― **ゲートウェイが目的となるルートテーブルを見つけられない場合**
- <ESC> **キーを押すと** Ping **が中断されます。**

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#
```

関連するコマンド

interface (P402)

4.25 DHCP

4.25.1 DHCP スヌーピング

DHCP スヌーピングは悪意のある DHCP サーバーや DHCP サーバーに関連のある情報を送信する他のデバイスからネットワークを守ります。この情報は物理ポートへ IP アドレスを戻す際への追跡に役立つ場合があります。この章は DHCP スヌーピング機能を構成するために使用するコマンドについて記載しています。

コマンド	機能	モード	ページ
ip dhcp snooping	DHCP スヌーピングをスイッチで有効化	GC	P596
ip dhcp snooping vlan	DHCP スヌーピングを指定の VLAN で有効化	GC	P598
ip dhcp snooping trust	指定したインタフェースを trusted ポートに設定	IC	P599
ip dhcp snooping verify mac-address	イーサネットヘッダ中の MAC アドレスに対して DHCP パケットにストアされたクライアントのハードウェアアドレスを確認。	GC	P600
ip dhcp snooping information option	DHCP Option 82 情報リレーを有効 / 無効化	GC	P601
ip dhcp snooping information policy	DHCP Option 82 情報を含む、DHCP クライアントパケット Information option policy を設定	GC	P602
show ip dhcp snooping	DHCP スヌーピング設定を表示	PE	P603
show ip dhcp snooping binding	DHCP スヌーピングバインディングテーブルエントリを表示	PE	P603

ip dhcp snooping

このコマンドは DHCP スヌーピング機能を有効にします。no を付けると設定を初期状態に戻します。

文法

ip dhcp snooping

no ip dhcp snooping

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

- ネットワークの外側から悪意のある DHCP メッセージが受信されたとき、ネットワークトラフィックが混乱する可能性があります。DHCP スヌーピングはネットワークやファイアウォールの外側からの安全でないインターフェースで受信した DHCP メッセージをフィルタするために使用されます。DHCP スヌーピングをこのコマンドで有効にして ip dhcp snooping vlan コマンドで VLAN インターフェース上の DHCP スヌーピングを有効にしたとき、DHCP スヌーピングテーブルのリストに載っていないデバイスから、スイッチの untrust インターフェースで DHCP メッセージを受信すると、それを破棄します。
- 有効にしたとき、untrust のインターフェースに入った DHCP メッセージには、DHCP スヌーピングで学習したダイナミックエントリをベースにしたフィルタが行われます。
- DHCP スヌーピングテーブルのエントリは、untrust インターフェースからのパケットのみ学習されます。それぞれのエントリには MAC アドレス、IP アドレス、リースタイム、エントリタイプ（Dynamic DHCP Binding、Static DHCP Binding）、VLAN ID、Port ID が含まれています。
- DHCP スヌーピングを有効にしたとき、スイッチが処理することのできる DHCP メッセージの数の制限が設定され、1 秒当たり 100 パケットとなります。この制限を越える DHCP パケットは破棄されます。
- フィルタのルールは下記の通りです。
  - DHCP スヌーピングが無効の場合、DHCP パケットは転送される。
  - DHCP スヌーピングが有効で DHCP パケットを受信する VLAN 上でも有効の場合、すべての DHCP パケットは trust 状態のポートに向けて転送されます。受信したパケットが DHCP ACK メッセージの場合、このエントリはバインドテーブルに追加されます。
  - DHCP スヌーピングが有効で DHCP パケットを受信する VLAN 上でも有効だが、ポートが trust でない場合は下記の動作を行います。

（1）DHCP パケットが DHCP サーバーからの返答パケット（OFFER,ACK,NAK メッセージを含む）の場合、そのパケットは破棄されます。

（2）DHCP パケットがクライアントからのものである場合、DECLINE や RELEASE メッセージのようなパケットは、一致するエントリがバインドテーブルで見つかった場合のみ、スイッチはパケットを転送します。

（3）DHCP パケットがクライアントからのものである場合、DISCOVER、REQUEST、INFORM、DECLINE、RELEASE メッセージのようなパケットは、MAC アドレスによる照合が無効である場合にはパケットは転送されます。しかし、MAC アドレスの照合が有効の場合、DHCP パケットに記録されているクライアントのハードウェアアドレスが Ehternet ヘッダの Source MAC アドレスと同じ場合にパケットは転送されます。

（4）DHCP パケットが認識できないタイプの場合は破棄されます。

－クライアントからの DHCP パケットが上記のフィルタ基準を通過した場合、同じ VLAN の trust ポートに転送されます。

－サーバーからの DHCP パケットが trust ポートで受信された場合、同じ VLAN の trust ポートと untrust ポートに転送されます。

- DHCP スヌーピングが無効の場合、すべてのダイナミックエントリはバインドテーブルから取り除かれます。
- スイッチ自身が DHCP クライアントの場合の動作：スイッチが DHCP サーバーにクライアントの Request パケットを送信するポートは trust として設定しなくてはいけません。スイッチは DHCP サーバーから ACK メッセージを受信したとき、自身の情報をバインドテーブルのダイナミックエントリとして追加しません。また、スイッチが DHCP クライアントのパケットを自身に送信したとき、フィルタの動作は発生しません。しかし、スイッチが DHCP サーバーからメッセージを受信したとき、untrust ポートで受信したパケットはすべて破棄されます。

例

```
Console(config)#ip dhcp snooping
Console(config)#
```

関連するコマンド

ip dhcp snooping vlan (P598)

ip dhcp snooping trust (P599)

ip dhcp snooping vlan

このコマンドは指定した VLAN **上で** DHCP **スヌーピング機能を有効にします。**no **を付けると設定を初期状態に戻します。**

文法

ip dhcp snooping vlan *vlan-id*

no ip dhcp snooping vlan *vlan-id* { tagged | untagged }

- *vlan-id* ― **設定を行う** VLAN ID**（範囲：**1-4094**）**

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

- ip dhcp snooping **コマンドを使用して** DHCP **スヌーピングを有効にした後にこのコマンドで** DHCP Snooping **を** VLAN **上で有効にしたとき、**ip dhcp snooping trust **コマンドで指定した** VLAN **内の** untrust **ポートで** DHCP **パケットのフィルタが実行されます。**
- DHCP **スヌーピングの全体の設定を無効にした（**no ip dhcp snooping **を実行）とき、**VLAN **上での** DHCP **スヌーピング設定はまだ可能ですが、この変更は** DHCP Snooping **全体の設定が再度有効になるまで反映されません。**
- DHCP **スヌーピングが有効のとき、**VLAN **の** DHCP **スヌーピング設定を変更すると下のような結果になります。**
  - VLAN **上で** DHCP **スヌーピング設定を無効にした場合、この** VLAN **で学習したすべてのダイナミックエントリはバインドテーブルから削除されます。**

例

```
Console(config)#ip dhcp snooping vlan 1
Console(config)#
```

関連するコマンド

ip dhcp snooping (P596)

ip dhcp snooping trust (P599)

ip dhcp snooping trust

このコマンドは特定のインターフェースを trust として設定します。no を付けると設定を初期状態に戻します。

文法

ip dhcp snooping trust

no ip dhcp snooping trust

初期設定

全てのインタフェースは Untrust に設定

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- untrust インターフェースはネットワークやファイアウォールの外側からメッセージを受信するよう設定されたインターフェースです。trust インターフェースはネットワークの内側からメッセージのみ受信するよう設定されたインターフェースです。
- ip dhcp snooping を使用して DHCP スヌーピング機能を有効にし、次に VLAN 上で DHCP スヌーピングを有効にしたとき、DHCP パケットのフィルタリングが VLAN 内の untrust ポートで実行されます。
- untrust ポートが trust ポートに変更されたとき、このポートに関連付けられたすべての DHCP スヌーピングのダイナミックエントリは削除されます。
- スイッチ自身が DHCP クライアントの場合の動作：DHCP クライアントとしてのリクエストを DHCP サーバーに出力するポートを trust に設定してください。

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#no ip dhcp snooping trust
Console(config-if)#
```

関連するコマンド

ip dhcp snooping (P596)

ip dhcp snooping vlan (P598)

ip dhcp snooping verify mac-address

DHCP パケットにストアされたクライアントハードウェアアドレスに対し、イーサネットヘッダの送信元 MAC アドレスを検査します、

文法

ip dhcp snooping verify mac-address

no ip dhcp snooping verify mac-address

初期設定

有効

コマンドモード

Global Configuration

コマンド解説

- MAC アドレス検査が有効であり、パケットのイーサネットヘッダ内の送信元 MAC アドレスが、クライアントの DHCP パケットのハードウェアアドレスと一致しない場合、パケットは破棄されます。.

例

```
Console(config)#ip dhcp snooping verify mac-address
Console(config)#
```

関連するコマンド

ip dhcp snooping (P596)

ip dhcp snooping vlan (P598)

ip dhcp snooping trust (P599)

ip dhcp snooping information option

このコマンドはスイッチの DHCP Option 82 Information Relay **機能を有効にします。**no **を付けるとこの機能は無効になります。**

文法

ip dhcp snooping information option

no ip dhcp snooping information option

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

- DHCP **機能はスイッチと** DHCP **クライアントについての情報を** DHCP **サーバーに送信するため、リレー機能を装備しています。**DHCP Option 82 **として知られる機能で、**IP **アドレスを割り当てるときの情報を使用するため、もしくはクライアントに他のサービスやポリシーを設定するために** DHCP **サーバーを共用できる状態にします。**
- DHCP Snooping Information Option **が有効のとき、クライアントは** MAC **アドレスよりむしろクライアントが接続されているスイッチのポートによって同一のものであると識別されます。それにより、**DHCP **クライアントとサーバー間のメッセージ交換は、**VLAN **全体にメッセージをフラッディングすることなしでクライアントとサーバー間を直接転送します。**
- **スイッチ上で** DHCP Option 82 **の情報をパケットの中に入れるためには** DHCP Snooping **機能を有効にしなくてはいけません。**

例

```
Console(config)#ip dhcp snooping information option
Console(config)#
```

関連するコマンド

ip dhcp snooping vlan (P598)

ip dhcp snooping trust (P599)

ip dhcp snooping information policy

このコマンドは Option 82 **を含む** DHCP **クライアントからのパケットのため、**DHCP **スヌーピング** Information Option **を設定します。**

文法

ip dhcp snooping information policy <drop | keep | replace>

- **drop** ― **パケット中の** Option82 **情報を破棄し、全ての** VLAN **にフラッティングします。**
- **keep** ―DHCP **クライアント情報を残します。**
- **replace** ― DHCP **クライアントパケット情報をスイッチ自身のリレー情報で置き換えます。**

初期設定

replace

コマンドモード

Global Configuration

コマンド解説

スイッチが DHCP Option 82 **を既に含んでいるクライアントから** DHCP **パケットを受信したとき、スイッチはこれらのパケットのためアクションポリシーの設定を構成します。** DHCP **パケットを破棄するかどうか、**Option 82 **の情報をそのままにするか、**Option 82 **をスイッチ自身のリレー情報に置き換えるかを選択することができます。**

例

```
Console(config)#ip dhcp snooping information policy drop
Console(config)#
```

関連するコマンド

ip dhcp snooping vlan (P598)

ip dhcp snooping trust (P599)

show ip dhcp snooping

DHCP スヌーピング設定を表示します。

コマンドモード

Privileged Exec

例

```
Console#show ip dhcp snooping
Global DHCP Snooping status: disable
DHCP Snooping Information Option Status: disable
DHCP Snooping Information Policy: replace
DHCP Snooping is configured on the following VLANs:
   1,
Verify Source Mac-Address: disable
Interface           Trusted
----------          ----------
Eth 1/1             No
Eth 1/2             No
Eth 1/3             No
Eth 1/4             No
Eth 1/5             No
.
.
.
```

show ip dhcp snooping binding

DHCP スヌーピング・バインディングテーブルのエントリを表示します。

コマンドモード

Privileged Exec

例

```
Console#show ip dhcp snooping binding
MacAddress IpAddress Lease(sec) Type VLAN Interface
------------------ --------------- ---------- ------------------- ---
------
11-22-33-44-55-66 192.168.0.99 0 Static 1 Eth 1/5
Console#
```

4.25.2 DHCP リレー

本機は、接続されたホストデバイスのため、DHCP リレーサービスをサポートしています。

DHCP リレーが有効であり、本機が DHCP ブロードキャストリクエストを閲覧できる場合、スイッチ自身の IP アドレスをリクエストに挿入することで、DHCP サーバはクライアントが位置するサブネットを認識します。

スイッチはパケットを DHCP サーバに転送し、サーバは DHCP リクエストを受け取ると、定義された範囲からフリー IP アドレスを DHCP クライアントに割り当てます。

コマンド	機能	モード	ページ
ip dhcp relay information	指定した VLAN で DHCP リレーを有効化	GC	P604
ip dhcp relay server	DHCP サーバを指定	GC	P605
ip dhcp relay server	DHCP リレーサービスの情報を表示	PE	P605

ip dhcp relay information

このコマンドは指定した VLAN の DHCP リレーを有効にします。no を付けるとこの機能は無効になります。

文法

ip dhcp relay information [option | policy < drop | keep | replace >]

- **option** — relay 情報（Option-82 フィールド）を有効にします。
- **policy** — Option-82 情報が存在する場合の処理方法を選択します。
  - **drop** — Option-82 情報が存在する場合、リプレースをおこないます。
  - **keep** —既にリレー情報があった場合、そのメッセージを削除します。
  - **replace** —既存のリレー情報をそのまま保持します。

初期設定

無効

コマンドモード

Grobal Configuration

例

```
Console(config)#ip dhcp relay information policy replace
Console(config)#
```

ip dhcp relay server

このコマンドは DHCP リレーエージェントが使用する、DHCP サーバの IP アドレスを指定します。no を付けると設定したアドレスを削除します。

文法

ip dhcp relay server *IP Address*

- *IP Address* — DHCP サーバの IP アドレスを指定します。
  アドレスは 5 つまで設定することができます。

初期設定

アドレス未設定

コマンドモード

Grobal Configuration

例

```
Console#(config)#ip dhcp relay server 192.168.1.105 192.168.1.205
Console#
```

show ip dhcp-relay

DHCP リレーサービスの情報を表示します。

文法

show ip dhcp-relay

コマンドモード

Privileged Exec

例

```
Console#show ip dhcp-relay
Status of DHCP relay option82:
Insertion of option82 is Enabled.
DHCP option policy :drop.
DHCP relay-server address 192.168.1.105 192.168.1.205 0.0.0.0
0.0.0.0 0.0.0.0
Console#
```

4.26 IP ソースガード

IP ソースガードは、IP ソースガードテーブル上の手動で設定されたエントリ、もしくは DHCP スヌーピング機能を有効にしたときに DHCP スヌーピングテーブル上のダイナミックエントリを基にしたネットワークインターフェース上の IP トラフィックをフィルタするセキュリティ機能です。IP ソースガードは、あるホストがネットワークにアクセスする別のホストの IP アドレスを使用する試みがあったとき、そのホストが行う攻撃からネットワークを守るために使用されます。

この章は IP ソースガードの設定を行うために使用するコマンドを記載しています。

コマンド	機能	モード	ページ
ip source-guard	送信元 IP アドレス、もしくは送信元 IP アドレスと対応する MAC アドレスを基に入力トラフィックをフィルタするようスイッチを設定します。	IC	P607
ip source-guard binding	IP Source Guard のバインドテーブルに固定 IP アドレスを追加します。	GC	P608
show ip source-guard	それぞれのインターフェースで IP Source Guard 機能が有効か無効かどうかを表示します。	PE	P610
show ip source-guard binding	IP Source Guard のバインドテーブルを表示します。	PE	P608

ip source-guard

このコマンドは送信元 IP アドレス、もしくは送信元 IP アドレスと対応する MAC アドレスを基に入力トラフィックをフィルタするようスイッチを設定します。no を付けると設定を無効にすることができます。

文法

ip source-guard {sip | sip-mac}

no ip source-guard

- **sip** ― バインディングテーブルにストアされた IP アドレスによる、トラフィックのフィルタリング
- **sip-mac** ― バインディングテーブルにストアされた IP アドレスおよび、関連した MAC アドレスによる、トラフィックのフィルタリング

初期設定

無効

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- IP ソースガードはネットワークやファイアウォールの外側からメッセージを受信した、保護されていないポート上のトラフィックをフィルタするために使用されます。
- "sip" や "sip-mac" にソースガードのモードを設定することにより、選択したポート上でこの機能を有効にします。バインドテーブルのすべてのエントリに対して VLAN ID、送信元 IP アドレスポート番号をチェックするには "sip" オプションを使用してください。"sip-mac" オプションを使用すると、上に加えて送信元 MAC アドレスもチェックします。選択したポートでこの機能を無効にするには no source guard コマンドを使用します。
- 有効にしたとき、トラフィックは DHCP スヌーピングを通して学習したダイナミックエントリや IP ソースガードのバインドテーブルで構成された固定アドレスを基にフィルタが行われます。
- テーブルエントリには MAC アドレス、IP アドレス、リースタイム、エントリの種類 (Static IP SG Binding、Dynamic DHCP Binding、Static DHCP Binding)、VLAN ID、ポート ID が含まれます。
- ip source-guard binding コマンドを実行して表示されるソースガードバインドテーブル上に入力されたスタティックアドレスは、リースタイムが無限として自動的に設定されます。DHCP スヌーピングを通して学習されたダイナミックエントリは DHCP サーバー自身によって構成されます。スタティックエントリには手動で設定されたリースタイムが含まれます。
- IP ソースガードを有効にした場合、入力パケットの IP アドレス（sip オプションが有効の場合)、もしくは入力パケットの IP アドレスと MAC アドレス（sip-mac オプションが有効の場合）はバインドテーブルと比較されます。エントリが合致していないことが分かった場合、パケットは破棄されます。

- フィルタのルールは下のように実行されます。

- DHCP スヌーピングが無効の場合、IP ソースガードは VLAN ID、送信元 IP アドレス、ポート番号、送信元 MAC アドレス（sip-mac オプションが有効の場合）をチェックします。バインドテーブルに合致するエントリがありエントリの種類が Static（IP ソースガードバインドテーブルに記載）の場合、パケットは転送されます。
- DHCP スヌーピングが有効の場合、IP ソースガードは VLAN ID、送信元 IP アドレス、ポート番号、送信元 MAC アドレス（sip-mac オプションが有効の場合）をチェックします。バインドテーブルに合致するエントリがありエントリの種類が Static（IP ソースガードバインドテーブルに記載）、Static（DHCP スヌーピングバインドテーブルに記載）、Dynamic（DHCP スヌーピングバインドテーブルに記載）のいずれかの場合にパケットは転送されます。
- IP ソースガードが Static、Dynamic のエントリのどちらもまだ存在しない状態においてインターフェース上で有効になった場合、スイッチはそのポート上のすべての IP トラフィックを破棄します。ただし DHCP パケットは除きます。

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#ip source-guard sip
Console(config-if)#
```

関連するコマンド

ip source-guard binding (P610)

ip dhcp snooping (P596)

ip dhcp snooping vlan (P598)

ip source-guard binding

このコマンドはソースガードのバインドテーブルにスタティックアドレスを追加します。no を付けるとスタティックエントリを削除します。

文法

ip source-guard binding *mac-address* **vlan** *vlan-id ip-address*

interface ethernet *unit/port*

no ip source-guard binding mac-address vlan vlan-id

- *mac-address* — 有効なユニキャスト ＭＡＣ アドレス
- *vlan-id* — 設定を行う VLAN ID（範囲 1-4094）
- *ip-address* — 有効なユニキャスト IP アドレス
- *unit* — スタックユニット（常に 1）
- *port* — ポート番号（範囲 1-26）

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- テーブルエントリには MAC アドレス、IP アドレス、リースタイム、エントリの種類 (Static IP SG Binding、Dynamic DHCP Binding、Static DHCP Binding)、VLAN ID、ポート ID が含まれます。
- すべてのスタティックエントリはリースタイムが無限で設定されます。show ip source-guard コマンドを実行すると、そのスタティックエントリのリースタイムには 0 が表示されます。
- ソースガードを有効にしたとき、DHCP スヌーピングを通して学習されたダイナミックエントリ、DHCP スヌーピングを通して設定されたスタティックエントリ、このコマンドで設定されたスタティックアドレスに基づいてトラフィックのフィルタが行われます。
- スタティックバインドテーブルは下のような処理を行います。

  −同じ VLAN ID と MAC アドレスのエントリがない場合、新しいエントリが Static IP Source Guard Binding としてバインドテーブルに追加されます。

  −同じ VLAN ID と MAC アドレスのエントリがありエントリの種類が Static IP Source Guard Binding である場合、新しいエントリは古いエントリを上書きします。

  −同じ VLAN ID と MAC アドレスのエントリがありエントリの種類が Dynamic DHCP Snooping Binding である場合、新しいエントリは古いエントリを上書きし、エントリの種類は Static IP Source Guard Binding に変更されます。

例

```
Console(config)#ip source-guard binding 11-22-33-44-55-66 vlan 1
192.168.0.99 interface ethernet 1/5
Console(config-if)#
```

関連するコマンド

ip source-guard (P607)

ip dhcp snooping (P596)

ip dhcp snooping vlan (P598)

show ip source-guard

このコマンドは、それぞれのインタフェースでソースガードが有効か無効かを表示します。

文法

show ip source-guard

コマンドモード

Privileged Exec

例

```
Console#show ip source-guard
Interface Filter-type
--------- -----------
Eth 1/1 DISABLED
Eth 1/2 DISABLED
Eth 1/3 DISABLED
Eth 1/4 DISABLED
Eth 1/5 SIP
Eth 1/6 DISABLED
```

show ip source-guard binding

ソースガードバインディングテーブルを表示します。

文法

show ip source-guard { binding { dhcp-snooping | static } **}**

- **binding** ― **バインディング情報を表示します。**
- dhcp-snooping ― DHCP **スヌーピングバインディングエントリ。**
- static ― **静的バインディング情エントリ。**

コマンドモード

Privileged Exec

例

```
Console#show ip source-guard binding
MacAddress IpAddress Lease(sec) Type VLAN Interface
------------------ --------------- ---------- -------------------- --
-- ----
11-22-33-44-55-66 192.168.0.99 0 Static 1 Eth 1/5
Console#
```

4.27 スイッチクラスタ

スイッチクラスタリングは 1 つのスイッチを通した中央管理を有効にするため、スイッチをグループ化する機能です。スイッチクラスタは、クラスタの他のすべてのメンバーを管理するために使用するコマンダユニットを持ちます。管理端末は IP アドレスを通してコマンダと直接通信するために Telnet と Web インターフェースの両方を使用することができます。またコマンダはクラスタの内部 IP アドレスを使用してメンバースイッチを管理します。1 つのクラスタに 36 個のメンバーを追加することができます。クラスタのスイッチは 1 つの IP サブネット内に制限されます。

コマンド	機能	モード	ページ
cluster	スイッチクラスタの設定	GC	P612
cluster ip-pool	クラスタ IP アドレスプールを設定	GC	P613
cluster commander	スイッチをクラスタコマンダに設定	GC	P614
cluster member	候補スイッチをクラスタメンバーに設定	GC	P615
rcommand	メンバースイッチへのコンフィギュレーションアクセスを提供	GC	P616
show cluster	スイッチクラスタリング設定を表示	PE	P617
show cluster members	現在のクラスタメンバーを表示	PE	P617
show cluster candidates	ネットワーク上の、クラスタ候補スイッチを表示	PE	P617

cluster

このコマンドはスイッチのクラスタリングを有効にします。no を付けるとクラスタリングを無効にします。

文法

cluster

no cluster

初期設定

有効

コマンドモード

Global Configuration

コマンド解説

- スイッチのクラスタを作成するためには、最初にスイッチ上でクラスタリングが有効であることを確認し（出荷時設定で有効）、次にクラスタのコマンダとしてスイッチを設定します。ネットワークの他の IP サブネットと干渉しないようにクラスタの IP プールを設定します。クラスタ用の IP アドレスは、スイッチがメンバーになりメンバースイッチとコマンダの間の通信で使用されるときにスイッチに割り当てられます。
- スイッチクラスタは 1 つのサブネットに制限されます。
- スイッチは 1 つのクラスタのメンバーにだけ所属することができます。
- 構成されたスイッチクラスタはリセット、ネットワークの変更を行っても維持されます。

例

```
Console(config)#cluster
Console(config)#
```

cluster ip-pool

このコマンドはクラスタの IP **アドレスプールを設定します。**no **を付けるとアドレスを初期状態に戻すことができます。**

文法

cluster ip-pool < *ip-addres s***>**

no cluster ip-pool

- *ip-address* ― **クラスタメンバーにアサインされた** IP **アドレス（**10.x.x.x.）

初期設定

10.254.254.1

コマンドモード

Global Configuration

コマンド解説

- IP **アドレスプールの設定が** Member **スイッチに割り当てられる** IP **アドレスとして内部的に使用されます。クラスタの** IP **アドレスの形式は「**10.x.x.Member **スイッチの** id**」という構成になります。**Member **に設定する必要のある** IP **アドレスの数は** 1 **個から** 36 **個です。**
- **ネットワークの** IP **サブネットと矛盾しないようクラスタの** IP **プールを設定してください。クラスタの** IP **アドレスはスイッチが** Member **になり、**Member **スイッチと** Commander **スイッチが相互に通信するときにスイッチに割り当てられます。**
- **スイッチが現在** Commander **モードの場合、クラスタの** IP **プールの変更ができません。最初に** Commander **モードを無効にしてください。**

例

```
Console(config)#cluster ip-pool 10.2.3.4
Console(config)#
```

cluster commander

このコマンドはクラスタのコマンダとしてスイッチを設定します。no を付けるとスイッチのコマンダ設定が無効になります。

文法

cluster commander

no cluster commander

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

- スイッチをコマンダとして設定した直後に、スイッチは自動的にネットワーク上のクラスタ機能が有効になっているスイッチを発見しようとします。これらの候補状態のスイッチは、管理端末を通して管理者が手動で選択したときクラスタのメンバーになることができます。
- クラスタのメンバーは Telnet でコマンダに接続することで管理することができます。コマンダから CLI でメンバースイッチに接続するには rcommand id コマンドを使います。

例

```
Console(config)#cluster commander
Console(config)#
```

cluster member

このコマンドは候補スイッチをクラスタメンバーとして設定します。.

文法

cluster member mac-address *mac-address* **id** *member-id*

no cluster member id *member-id*

- *mac-address* ―**候補スイッチの** MAC **アドレス**
- *member-id* ―**メンバースイッチに割り振られた** ID **番号（範囲：**1-36）

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- **クラスタメンバーの最大数は** 36 **です。**
- **候補スイッチの最大数は** 100 **です。**

例

```
Console(config)#cluster member mac-address 00-12-34-56-78-9a id 5
Console(config)#
```

rcommand

このコマンドを使用するとクラスタのメンバーに CLI でアクセスできます。

文法

rcommand id *member-id*

- *member-id* ―メンバースイッチの ID（範囲：1-36）

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

- このコマンドはコマンダスイッチへの Telnet 接続を通してのみ実行できます。コマンダ上にローカルコンソール接続をした上でのクラスタのメンバーの管理はサポートしていません。
- メンバースイッチの CLI にアクセスするためにユーザーネームとパスワードを入力する必要はありません。

例

```
Vty-0#rcommand id 1
     CLI session with the TigerSwitch 10/100/1000 is opened.
     To end the CLI session, enter [Exit].
Vty-0#
```

show cluster

スイッチクラスタリング設定を表示します。

コマンドモード

Privileged Exec

例

```
Console#show cluster
Role: commander
Interval heartbeat: 30
Heartbeat loss count: 3
Number of Members: 1
Number of Candidates: 2
Console#
```

show cluster members

現在のスイッチクラスタメンバーを表示します。

コマンドモード

Privileged Exec

例

```
Console#show cluster members
Cluster Members:
ID: 1
Role: Active member
IP Address: 10.254.254.2
MAC Address: 00-12-cf-23-49-c0
Description: TigerSwitch 10/100/1000 SPORT MANAGE
Console#
```

show cluster candidates

ネットワーク上の候補スイッチを検索します。

コマンドモード

Privileged Exec

例

```
Console#show cluster candidates
Cluster Candidates:
Role Mac Description
-------------- ------------------------------------------------------
--
ACTIVE MEMBER 00-12-cf-23-49-c0 TigerSwitch 10/100/1000 SPORT MANAGE
CANDIDATE 00-12-cf-0b-47-a0 TigerSwitch 10/100/1000 SPORT MANAGE
Console#
```

4.28 UPnP

Universal Plug and Play(UPnP) はデバイスをシームレスに接続し、家庭と企業のネットワークの配置を容易にするプロトコルです。UPnP はインターネットで使用されるオープンなコミュニケーション方式の規格の上で UPnP Device Control Protocol を動作させることでこれを実現します。

コマンド	機能	モード	ページ
upnp device	ネットワークの UPnP の有効 / 無効	GC	P618
upnp device ttl	TTL 値を設定	GC	P619
upnp device advertise duration	アドバタイズメント継続時間を設定	GC	P619
show upnp	UPnP ステータスおよびパラメータの表示	PE	P620

upnp device

UPnP を有効にします。"no" を前に置くことで機能を無効にします。

文法

upnp device

no upnp device

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

- UPnP を有効にする前に、UPnP メッセージのタイムアウト設定を行ってください。

例

```
Console(config)#upnp device
Console(config)#
```

関連するコマンド

upnp device ttl (P619)

upnp device advertise duration (P619)

upnp device ttl

デバイスからの UPnP **メッセージ送信のために、**TTL **値を設定します。**

文法

upnp device ttl *value*

- *value* —**ルータホップ数（範囲：**1-255**）**

初期設定

4

コマンドモード

Global Configuration

例

```
Console(config)#upnp device ttl 6
Console(config)#
```

upnp device advertise duration

アドバタイズメント継続時間を設定します。

文法

upnp device advertise duration *value*

value —**タイムアウト値（範囲：**60-86400 **秒）**

初期設定

100 **秒**

コマンドモード

Global Configuration

例

```
Console(config)#upnp device advertise duration 200
Console(config)#
```

関連するコマンド

upnp device ttl（P619）

show upnp

UPnP 管理ステータスおよびタイムアウト設定を表示します。

コマンドモード

Privileged Exec

例

```
Console#show upnp
UPnP global settings:
  Status: Enabled
  Advertise duration: 200
  TTL: 20
Console#
```

付録 A. トラブルシューティング

Telnet 又は Web ブラウザ、SNMP ソフトウェアから接続できない。

- スイッチに電源が投入されていることを確認して下さい。
- 管理端末とスイッチを接続するネットワークケーブルが、正しく接続されていることを確認して下さい。
- スイッチとの接続と接続先のポートが、無効になっていないか確認して下さい。
- 有効な IP アドレス、サブネットマスク、及びデフォルトゲートウェイが設定されたエージェントであることを確認して下さい。
- 管理端末が管理 VLAN（初期設定では VLAN 1）に接続していることを確認して下さい。
- 管理端末の IP アドレスが、スイッチが接続している IP インタフェースと同じサブネットの IP アドレスであることを確認して下さい。
- タグ付VLANグループに所属するIPアドレスを使用してスイッチへの接続を行おうとしている場合は、管理端末、及びネットワークへの接続を中継するスイッチに接続しているポートの設定が正しいタグになっていることを確認して下さい。
- Telnet で接続できない場合は、同時に接続できる Telnet セッション数の最大値を超過している可能性があります。
- 時間を置いて再度接続してみて下さい。

セキュアシェルを使用した接続ができない。

- SSH での接続ができない場合は、同時に接続できる Telnet/SSH セッション数の最大値を超過している可能性があります。
- 時間を置いて再度接続してみて下さい。
- SSH サーバの制御パラメータがスイッチに対して正しく設定されており、SSH クライアントソフトウェアが管理端末に対して正しく設定されていることを確認して下さい。
- スイッチの公開キーを生成し、このキーを SSH クライアントに提供していることを確認して下さい。
- 各 SSH ユーザアカウント（ユーザ名、認証レベル、パスワードを含む）を設定していることを確認して下さい。
- （公開キーによる認証機能を使用している場合）クライアントの公開キーをスイッチに取り込んでいることを確認して下さい。

シリアルポート接続から内蔵の設定プログラムに接続できない。

- ターミナルエミュレーションプログラムが、以下の通り設定されていることを確認して下さい。

  ターミナル：VT100 互換
  データビット：8 ビット
  ストップビット：1 ビット
  パリティ：なし
  通信速度：9600 bps

- 同梱のシリアルケーブルを使用していることを確認して下さい。

パスワードを無くしてしまった、又は忘れてしまった。

- お買い上げの販売店または、当社指定のサービス窓口にご連絡下さい。

FXC3126A Management Guide (FXC08-DC-200009-R2.1)

初版	2008 **年** 3 **月**
第 2 **版**	2009 **年** 6 **月**
第 3 **版**	2010 **年** 6 **月**

Management Guide
FXC3126A
Management Guide
FXC3126A
Management Guide
FXC3126A
Management Guide
FXC3126A
Management Guide
FXC3126A
Management Guide
FXC3126A
Management Guide
FXC3126A
Management Guide
FXC3126A
Management Guide
FXC3126A
Management Guide
FXC3126A
Management Guide
FXC3126A
Management Guide
FXC3126A
Management Guide
FXC3126A
Management Guide

FXC株式会社