Future X Communications

FXC3152A Management Guide

2010 年 1 月 Ver.1.0

FXC株式会社

本マニュアルについて

- 本マニュアルでは、FXC3152A 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 1.3.4.4 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

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	IP ACL、MAC **ルールをサポート**
DHCP	**クライアント**
DNS	**クライアントおよび** Proxy **サービス**
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** 8 **トランク**
Storm Control	**ブロードキャスト、マルチキャスト、未知のユニキャスト**
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 Algorithm	STP、Rapid STP（RSTP）、Multiple STP (MSTP)
Virtual LANs	IEEE802.1Q **タグ付** VLAN/ **ポートベース** 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、TCP/UDP **ポート**
Quality of Service	DiffServ **サポート**
Link Layer Discovery Protocol	**隣接するデバイスの基本情報を発見するために使用**
Multicast Filtering	IGMP Snooping、Query、MVR
Switch Clustering	**最大** 36 **スイッチ**
Tunneling	IEEE802.1Q **トンネリング（**QinQ**）サポート**

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。

ストームコントロール /Storm Control

ストームコントロール機能は、ブロードキャスト、マルチキャスト、未知のユニ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、マルチキャスト、未知のユニキャストパケットを制限することができます。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 4Mbit 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。

スパニングツリーアルゴリズム / Spanning Tree Algorithm

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

FXC3152A 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)
- ACL を使用したパケットのフィルタ
- 最大 255 の IEEE802.1Q VLAN 設定
- 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 8)
- ポートミラーリングの有効
- 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 P334 「Line （ラインコマンド）」を参照して下さい。
CLI の使い方は P281 「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 P289 「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 FXC3152A 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 32 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 27 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。

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 P23 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。

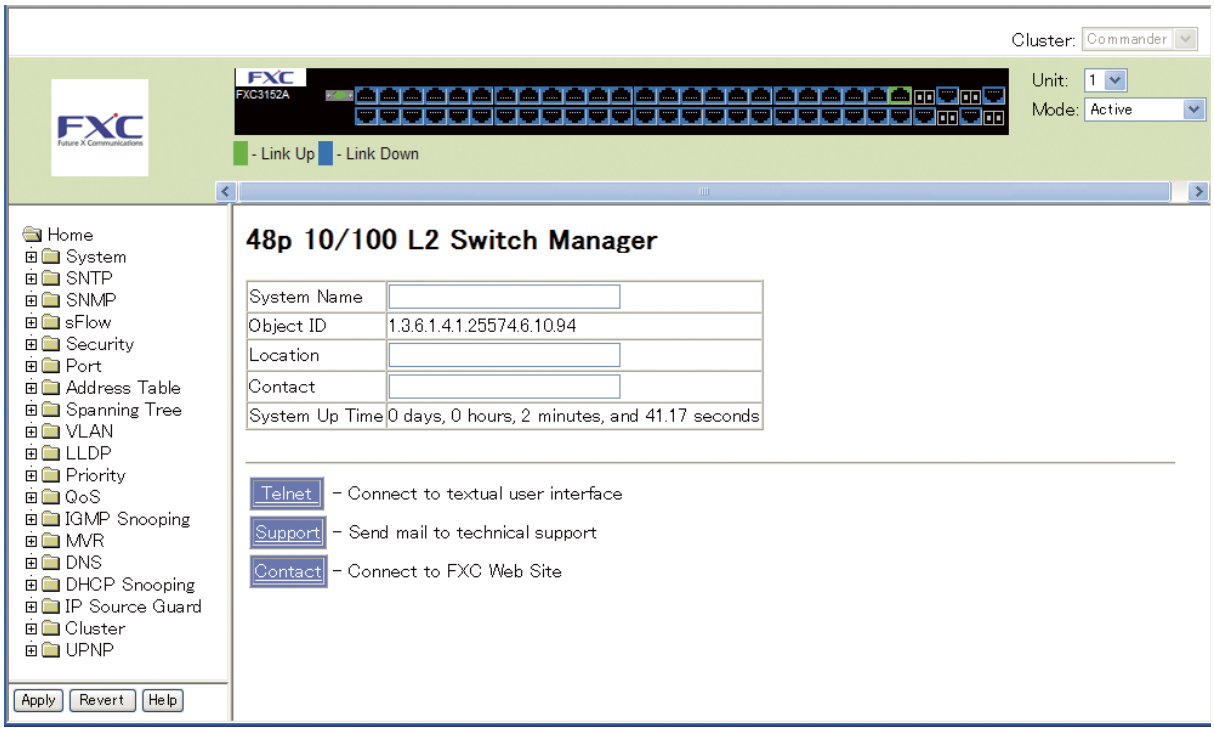
[注意] 管理用 PC と本機の間でスパニングツリーアルゴリズム （STA）が使用されていない場合、管理用 PC に接続されたポートをファストフォワーディングにする（Admin Edge Port の有効化）ことにより、Web インタフェースからの設定に対する本機の応答速度を向上させることができます（詳細は P184 「インタフェース設定」を参照して下さい）

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。

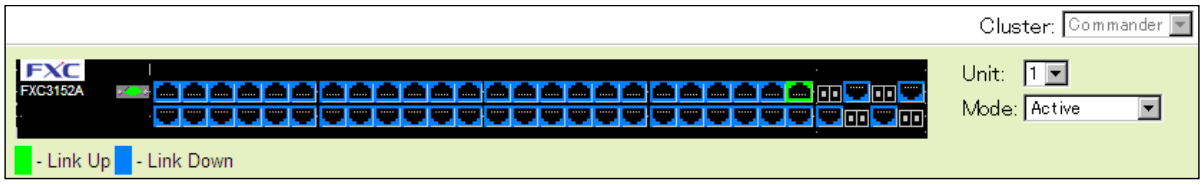
ボタン	操作
Revert	入力した値をキャンセルし、[Apply] 又は [Apply Changes] をクリックする前に表示されていた元の値に戻す
Apply	入力した値を本機に反映させる
Help	Web ヘルプにリンクしています

[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] 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って下さい。

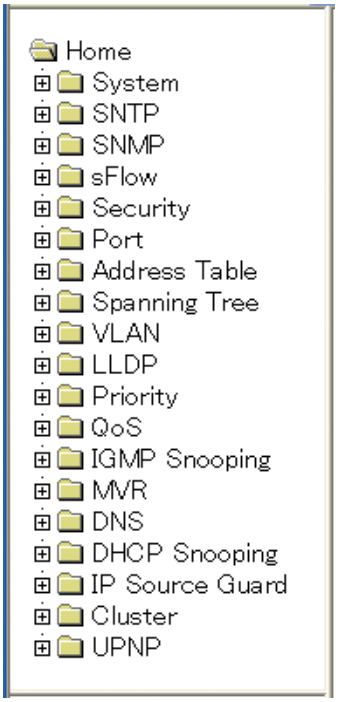
3.2.3 パネルの表示

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 P150 「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

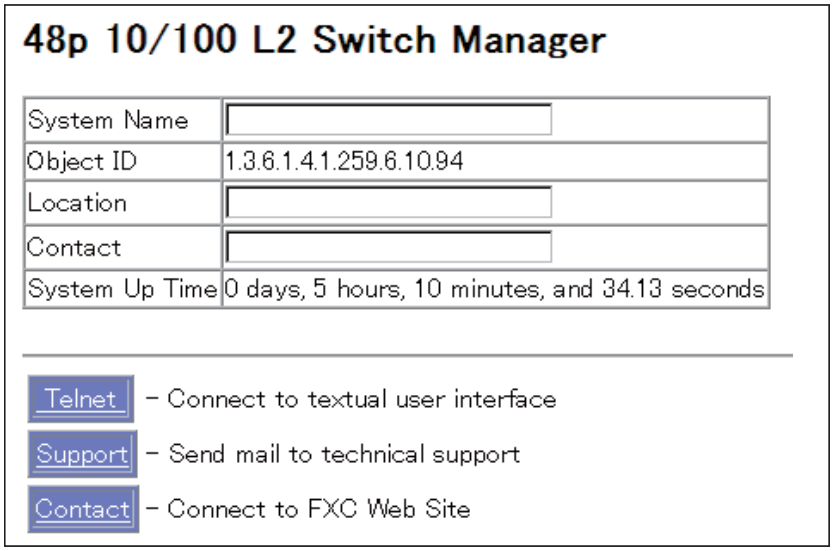
管理者のコンタクト情報

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

Chip Device ID
基本 MAC/ **物理レイヤスイッチチップ名称**

Internal Power Status
内部電源のステータスを表示

Management Software（管理ソフトウェア）

EPLD Version
EPLD（Electronically Programmable Logic Device）**コードのバージョン**

Loader Version
Loader **コードのバージョン**

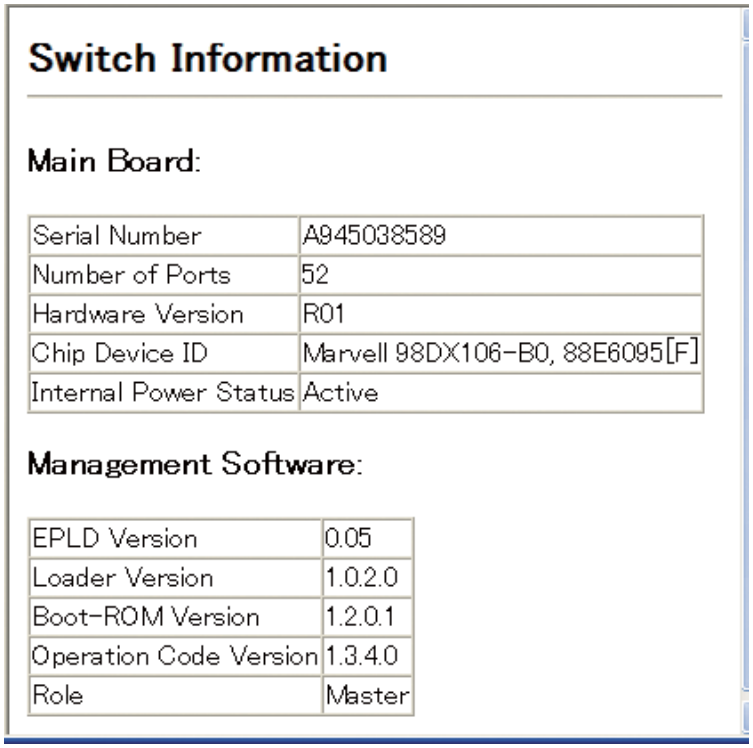
Boot-ROM Version
Power-On Self-Test (POST) **及び** boot **コードのバージョン**

Operation Code Version
runtime **コードのバージョン**

Role
本機が Master**、**Slave **どちらで動作しているかを表示**

設定方法

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



Switch Information

Main Board:

Serial Number	A945038589
Number of Ports	52
Hardware Version	R01
Chip Device ID	Marvell 98DX106-B0, 88E6095[F]
Internal Power Status	Active

Management Software:

EPLD Version	0.05
Loader Version	1.0.2.0
Boot-ROM Version	1.2.0.1
Operation Code Version	1.3.4.0
Role	Master

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、P231 「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（P193 「VLAN」を参照して下さい）

Local VLAN Capable

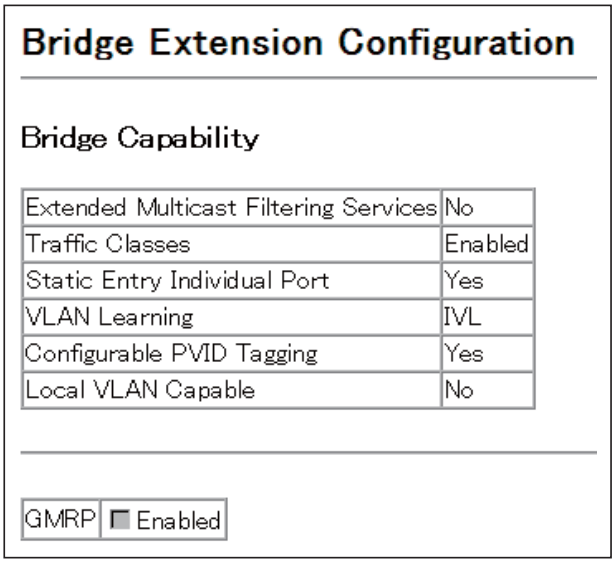
本機は複数のローカルブリッジ (マルチプルスパニングツリー) をサポートしていることを表しています。

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。**

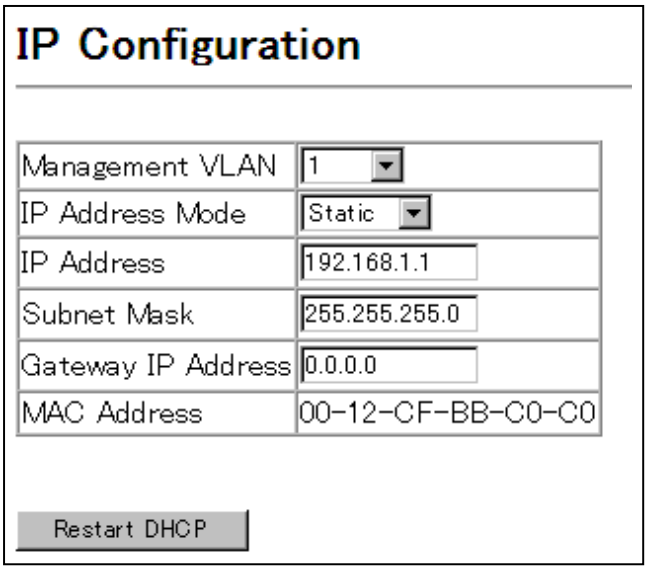
Restart DHCP

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。

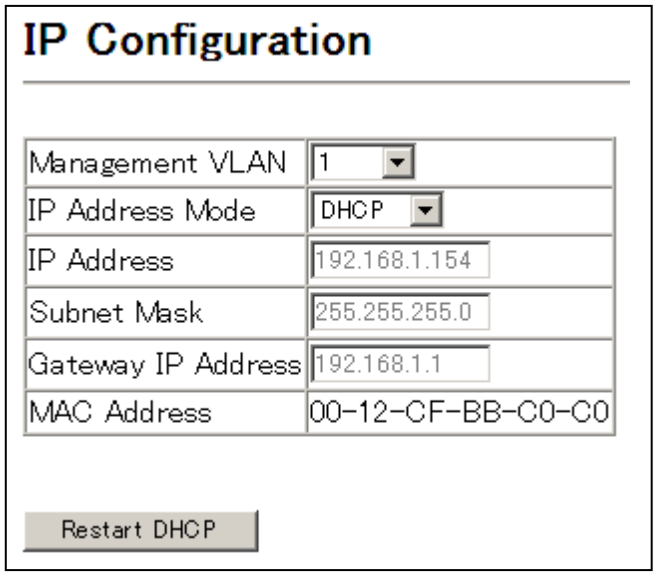


DHCP 又は BOOTP による IP アドレスの設定

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

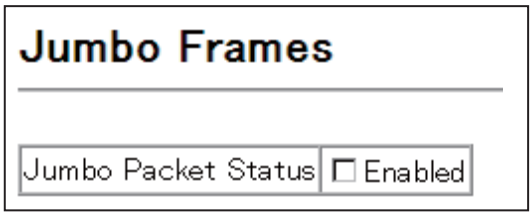
DHCP サービスを利用して IP アドレスが割り当てられ、すでに IP アドレスが利用できなくなっている場合には、Web インタフェースからの IP アドレスの更新はできません。以前の IP アドレスが利用可能な場合は、Web インタフェースを使い [Restart DHCP] ボタンから IP アドレスのリクエストを行うことができます。

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

FTP または 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。
FTP または 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。

[注意] 本機では HTTP を使用してダウンロード・アップロードファイルをスイッチへダウンロードすることも可能です。詳細は 35 ページの「HTTP を使用したファイルのアップロードとダウンロード」を参照して下さい。

本機のファイルディレクトリには、システムソフトウェア（run-time ファームウェア）の 2 つコピーのみ保存できます。
Run-time コードをダウンロードした際、保存先ファイル名は、現在の Run-time コードファイルと置き換えるように設定することが可能です。または、ファイルを現在の Run-time コードファイルと異なる名前を使用してダウンロードを行い、その後に新しいファイルをスタートアップファイルとして設定することも可能です。

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。
- file to ftp ― 本機から FTP サーバへファイルをコピーします。
- ftp to file ― FTP サーバから本機へファイルをコピーします。

TFTP Server IP Address

TFTP/FTP サーバの IP アドレス

User Name

FTP サーバアクセスのためのユーザ名

Password

FTP サーバアクセスのためのパスワード

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)

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。

オペレーションコードの自動アップグレード

本システムはオペレーションコードの自動ダウンロードを設定できます。
現在インストールされているファイルよりも、新しいバージョンのファイルがサーバーに発見された時に、オペレーションコードファイルの自動ダウンロードを行います。
ファイルがサーバーから転送され、ファイルシステムへの書き込みが成功した後、新しいファイルを自動的にスタートアップファイルとして設定し、スイッチの再起動を行います。

機能解説

- この機能が有効の際、スイッチはブートアップシーケンスの間に一度、定義された URL を検索します。
- アップグレードファイルロケーションの URL のホスト部分は、有効な IPv4 IP アドレスに設定してください。DNS ホスト名は認識されません。
  有効な IP アドレスは、ピリオドで分けられた 0-255 の 4 つの数から成ります。
- ディレクトリへのパスも同じく定義してください。
  もしファイルが TFTP/FTP サービスのルートディレクトリに保存刺されている場合、"/" を使用して指定してください。（例：ftp://192.168.0.1/）
- ファイル名は、アップグレードファイルロケーション URL に含まれなくてはなりません。リモートサーバに保存されたコードのファイル名は ES3528_52M.bix になります。
- TFTP 接続は ,PASV モードが有効時に確立されます。PASV モードは、FTP トラフィックがブロックされないとしても、ファイアウォールを横断するために必要となります。PASV モードは無効にできません。
- 大文字あるいは小文字のファイル名を受け入れるという点で（例：本機はサーバーへ "es3528_52m.bix" を要求しても、"ES3528_52M.BIX" を受け取ることができます）、スイッチベースの検索機能は大文字小文字の区別を無視します。しかしながら、Unix 等の多くの Unix ライクシステム (FreeBSD、NetBSD、OpenBSD 等) が、大文字小文字の違いを識別し、同じディレクトリの 2 つのファイル、es3528_52m.bix と ES3528_52M.BIX が別の名前であると認識するということを念頭に置いてください。もし ES3528_52M.BIX(または Es3528_52m.bix) として保存されたアップグレードファイルが大文字小文字の違いを識別するサーバに置かれている場合、スイッチ（es3528_52m.bix を要求）はアップグレードを行えません。サーバはリクエストされたファイル名と保存されているファイルが同じ物だと認識が出来ないからです。
  大文字小文字の違いを識別する Unix ライクオペレーティングシステムの顕著な例外は Mac OS X です。MAC OS X は大文字小文字の違いを無視します。
  もし、サーバのオペレーティングシステムの仕様が不確かな場合は、マニュアル等でチェックをしてください。
- もし既に 2 つのオペレーションコードイメージファイルが本機のファイルシステムに保存されている場合、アップグレードイメージが転送される前に、スタートアップイメージ以外のファイルを削除して下さい。
- 自動アップグレードプロセスは、バックグラウンドで行われ、本機の通常のオペレーションを妨げません。
- 自動検索と転送のプロセスの間、管理者は他のオペレーションコードイメージ、設定ファイル、パブリックキー、HTTPS 証明書等の転送またはアップグレードを行うことができません。
- アップグレードオペレーションコードイメージは、ファイルシステムへの書き込みが成功した後、スタートアップファイルとして設定されます。
- 全てのアップグレードの成功 / 失敗後、スイッチは SNMP トラップを送信し、ログエントリを作成します。
- アップグレードファイルのファイルシステムへの書き込みに成功し、スタートアップイメージへ設定された後、スイッチはただちに再起動を行います。

設定・表示項目

Automatic Opcode Upgrade

スイッチブートアッププロセス時に、アップグレードオペレーションコードファイルの検索を有効にします。（初期設定：無効）

Automatic Upgrade Location URL

スイッチブートアッププロセス時にスイッチがオペレーションコードアップグレードファイルを検索する場所を定義します。URL **の最後の文字は（"/"）になります。**
スイッチによって自動的に付加される為、ES3528_52M.bix **ファイル名は含みません。**
（オプション：ftp、tftp）

tftp://host[/filedir]/
tftp:// - **サーバ接続の** TFTP **プロトコルを定義します。**
host - TFTP **サーバの** IP **アドレスを定義します。有効な** IP **アドレスは、ピリオドで分けられた** 0-255 **の** 4 **つの数から成ります。**DNS **ホスト名は認識されません。**
filedir - **ディレクトリを定義します。**
/ - URL **の最後の文字であることを示します。**

ftp://[username[:password@]]host[/filedir]/
tftp:// - **サーバ接続の** FTP **プロトコルを定義します。**
Username - FTP **接続のユーザ名を定義します。入力を省略した場合、仮ユーザ名は** " anonymous" **になります。**
Password - FTP **接続のパスワードを定義します。パスワードを、**URL **のホスト部分とユーザ名から区別するために、パスワードの前にはコロン（:）を付けて下さい。また、パスワードの後にはアットマーク（@）を付けて下さい。**
host - FTP **サーバの** IP **アドレスを定義します。有効な** IP **アドレスは、ピリオドで分けられた** 0-255 **の** 4 **つの数から成ります。**DNS **ホスト名は認識されません。**
filedir - **ディレクトリを定義します。**
/ - URL **の最後の文字であることを示します。**

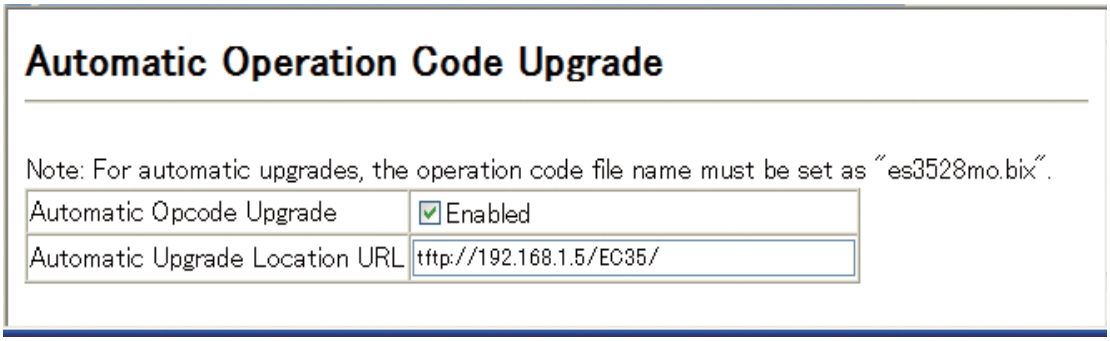
例

- **次の例は、様々な場所に保存されたオペレーションコードイメージと、**IP **アドレス** 192.168.0.1 **の** TFTP **サーバを示す** URL **構文です。**
  - tftp://192.168.0.1/
    イメージファイルは TFTP **ルートディレクトリにあります。**
  - tftp://192.168.0.1/switch-opcode/
    イメージファイルは TFTP **ルートに相対的な** "switch-opcode" **ディレクトリにあります。**
  - tftp://192.168.0.1/switches/opcode/
    イメージファイルは "opcode" **ディレクトリにあり、それは** TFTP **ルートに相対的な** "switches" **親ディレクトの中にあります。**
- **次の例は、様々なユーザ名、パスワード、ロケーションと** IP **アドレス** 192.168.0.1 **の** FTP **サーバを示す** URL **構文です。**
  - ftp://192.168.0.1/
    ユーザ名とパスワードは空です。ユーザ名は "anonymous"**、パスワードはブランクになります。イメージファイルは** FTP **ルートディレクトリにあります。**

- ftp://switches:upgrade@192.168.0.1/
  ユーザ名は "switches"**、パスワードは** "upgrade" **です。イメージファイルは** FTP **ルールにあります。**
- ftp://switches:upgrade@192.168.0.1/switches/opcode/
  ユーザ名は "switches"**、パスワードは** "upgrade" **です。イメージファイルは** "opcode" **ディレクトリにあり、それは** TFTP **ルートに相対的な** "switches" **親ディレクトの中にあります。**

設定方法

[System] → [File Management] → [Automatic Operation Code Apgrade] **をクリックします。** "Automatic Opcode Upgrade" **ボックスをチェックし、オペレーションコードのパスとディレクトリを含む** FTP **または** TFTP **サーバの** URL **を入力します。**[Apply] **をクリックして下さい。**

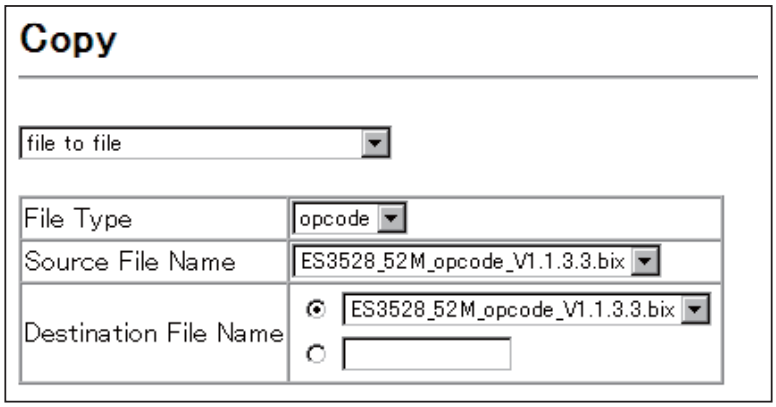


システムソフトウェアのダウンロード

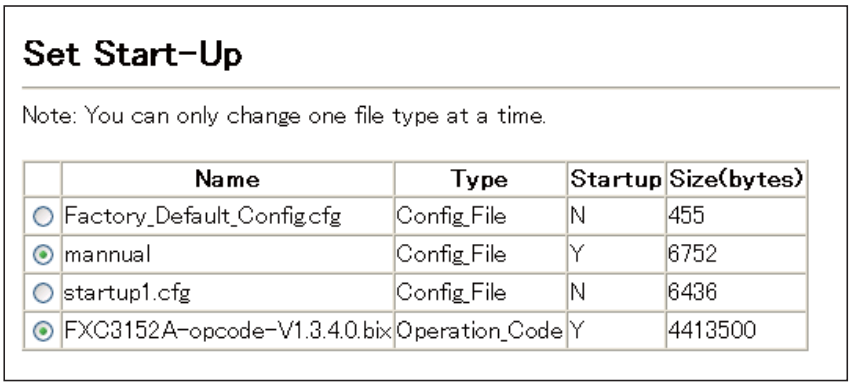
runtime **コードをダウンロードする場合、現在のイメージと置き換えるために現在のファイルを** Destination File Name **として指定することができます。また、現在の** runtime **コードファイルと異なるファイル名を使用して本体にダウンロードし、その後ダウンロードしたファイルを起動ファイルに設定することもできます。**

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。

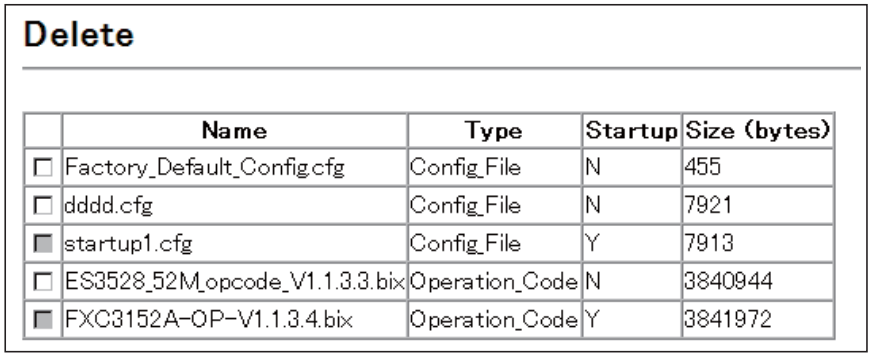


Set Start-Up

Note: You can only change one file type at a time.

	Name	Type	Startup	Size(bytes)
○	Factory_Default_Config.cfg	Config_File	N	455
◉	mannual	Config_File	Y	6752
○	startup1.cfg	Config_File	N	6436
◉	FXC3152A-opcode-V1.3.4.0.bix	Operation_Code	Y	4413500

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。



Delete

	Name	Type	Startup	Size (bytes)
☐	Factory_Default_Config.cfg	Config_File	N	455
☐	dddd.cfg	Config_File	N	7921
☑	startup1.cfg	Config_File	Y	7913
☐	ES3528_52M_opcode_V1.1.3.3.bix	Operation_Code	N	3840944
☑	FXC3152A-OP-V1.1.3.4.bix	Operation_Code	Y	3841972

設定情報ファイルの保存・復元

FTP/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 ftp ― 本機から FTP サーバへファイルをコピーします。
- 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。
- ftp to file ― FTP サーバから本機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。
- ftp to running-config ―FTP サーバから実行中の設定ファイルへコピーします。
- ftp to startup-config ― FTP サーバから起動設定ファイルへコピーします。
- running-config to file ― 実行中の設定ファイルをコピーします。
- running-config to ftp ― 実行中の設定ファイルを FTP サーバへコピーします。
- 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 ftp ― 起動設定ファイルを FTP サーバへコピーします。
- 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。

FTP/TFTP Server IP Address

FTP または TFTP サーバの IP アドレス

User Name

FTP サーバアクセスのユーザ名

Password

FTP サーバアクセスのパスワード

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。

機能解説

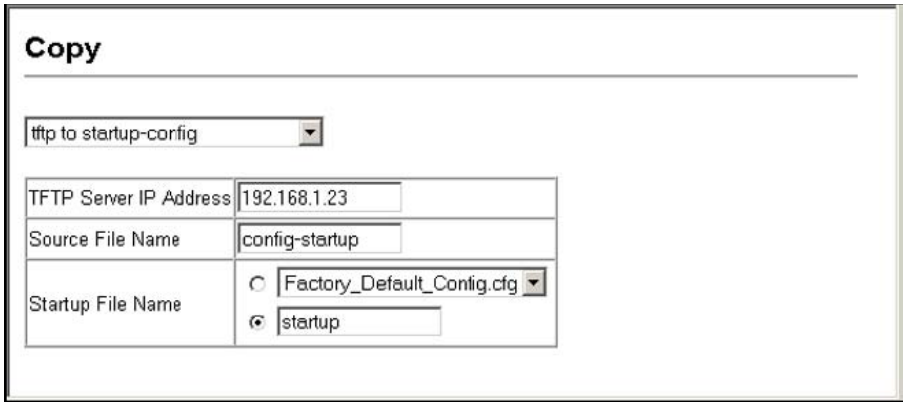
- FTP（**ポート** 21）**と** TFTP（**ポート** 69）**はどちらもサポートされます。**
- **サーバロケーションは有効な** IP **v** 4 IP **アドレスで指定してください。**DNS **ホスト名は認識されません。**
  有効な IP **アドレスは、ピリオドで分けられた** 0-255 **の** 4 **つの数から成ります。**

設定情報ファイルのダウンロード

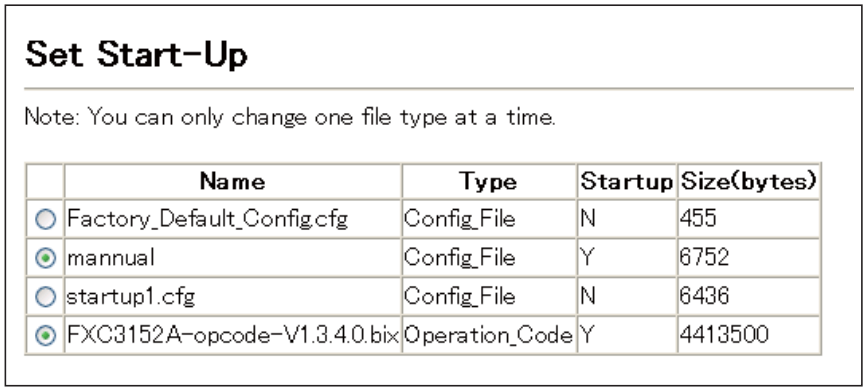
設定ファイルは新しいファイル名で保存し、起動ファイルとして設定できる他に、現在の起動設定ファイルを保存先に指定することで直接起動設定ファイルを置き換えることができます。但し、"Factory_Default_Config.cfg" **ファイルは** TFTP **サーバへコピーすることはできますが、設定ファイルをダウンロードする際に、ダウンロード先のファイル名として指定し、新しいファイルに置き換えることはできません。**

設定方法

[System] → [File Management] → [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。

HTTP を使用したファイルのアップロードとダウンロード

FTP または TFT サーバからのコピーオペレーションに加え、本機では HTTP を使用して Web マネージメントステーションにファイルをアップロード / ダウンロードをおこなうことが出来ます。
スイッチオペレーションコードファイルと設定ファイルの両方が、HTTP を使用してアップロード / ダウンロードが可能です。

設定・表示項目

File Type

ファームウェアまたはスイッチ設定ファイルをコピーする為に、opcode（オペレーションコード）または configuration（スイッチ設定ファイル）を指定してください。

Source File Name

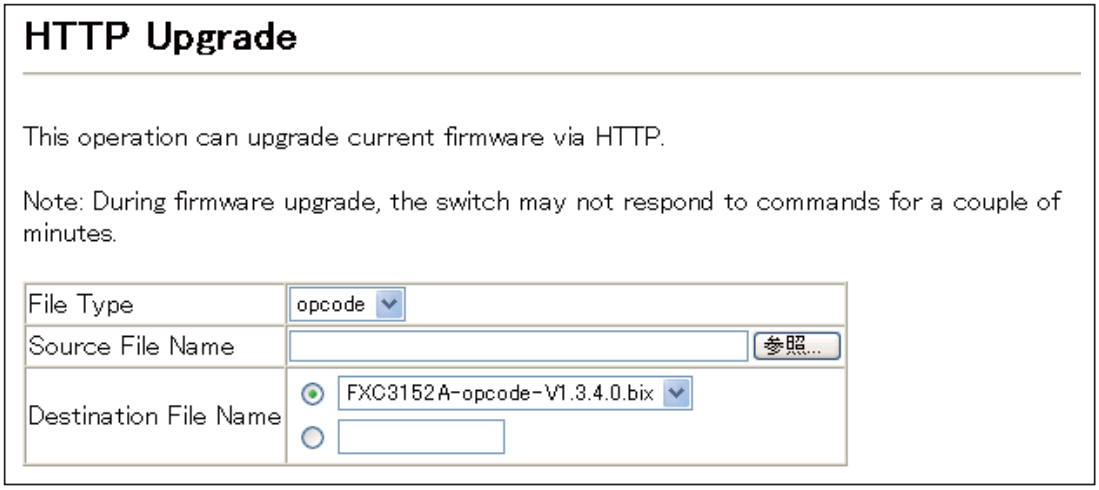
" 参照 " ボタンを使用し、ファイルを指定してください。ファイル名はスラッシュ及びバックスラッシュを使用することはできません。また、ファイル名の頭文字にはピリオド (.) は使用できません。TFTP/FTP サーバ上のファイル名は最長 127 文字、本機内では最長 31 文字です（利用できる文字 :A-Z, a-z,0-9, ".", "-", "_"）

Destination File Name

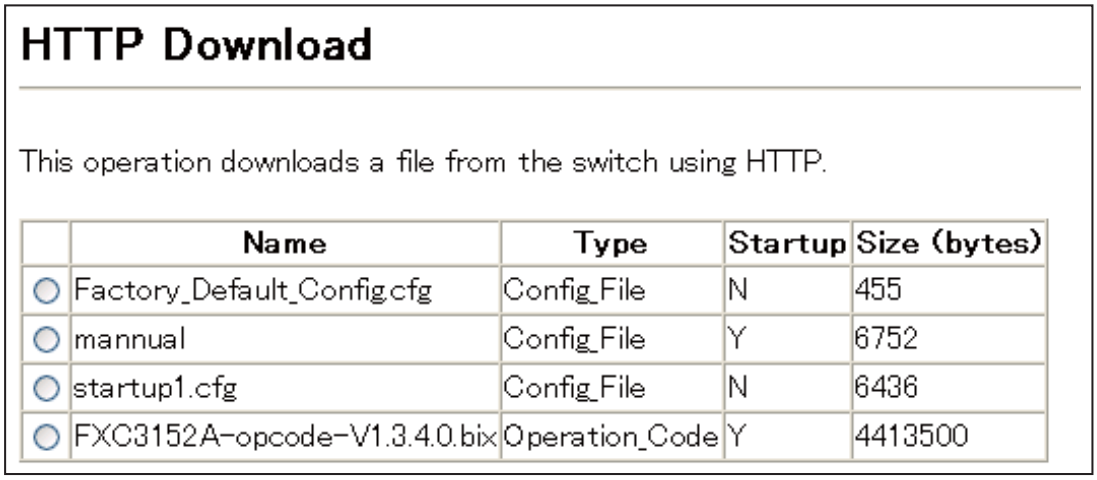
スイッチ上の既存のファイルを上書きするか、あるいは新しいファイル名を指定してください。

設定方法

[System] → [File Management] → [HTTP Upgrade] をクリックします。
"opcode" または "config" を選択し、" 参照 " ボタンを使用してファイルの場所を指定してください。
スイッチ上のファイルを上書きを選択するか、新しいファイル名を指定し [Apply] をクリックして下さい。



[System] → [File Management] → [HTTP Downgrade] をクリックします。
Web 管理ステーションへダウンロードするオペレーションコードまたは設定ファイルを選択し、[Apply] をクリックして下さい。



3.3.7 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

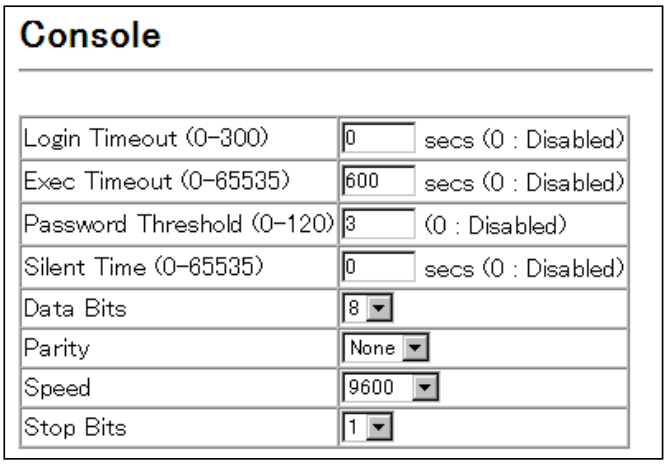
ターミナル接続の送信 (ターミナルへの)/ 受信 (ターミナルからの) ボーレート。シリアルポートに接続された機器でサポートされているボーレートを指定して下さい。
（範囲：9600、19200、38400、Auto　初期設定：Auto)

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。



3.3.8 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、または** 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）**

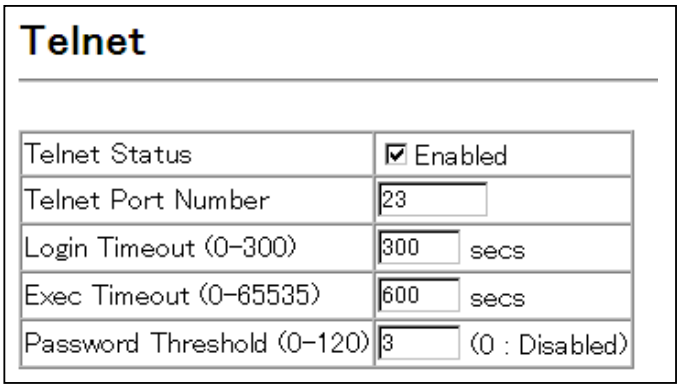
Password Threshold

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。**



3.3.9 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。

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

※現在のファームウェアではレベル 2、5、6 のエラーメッセージのみサポート

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：6）

[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

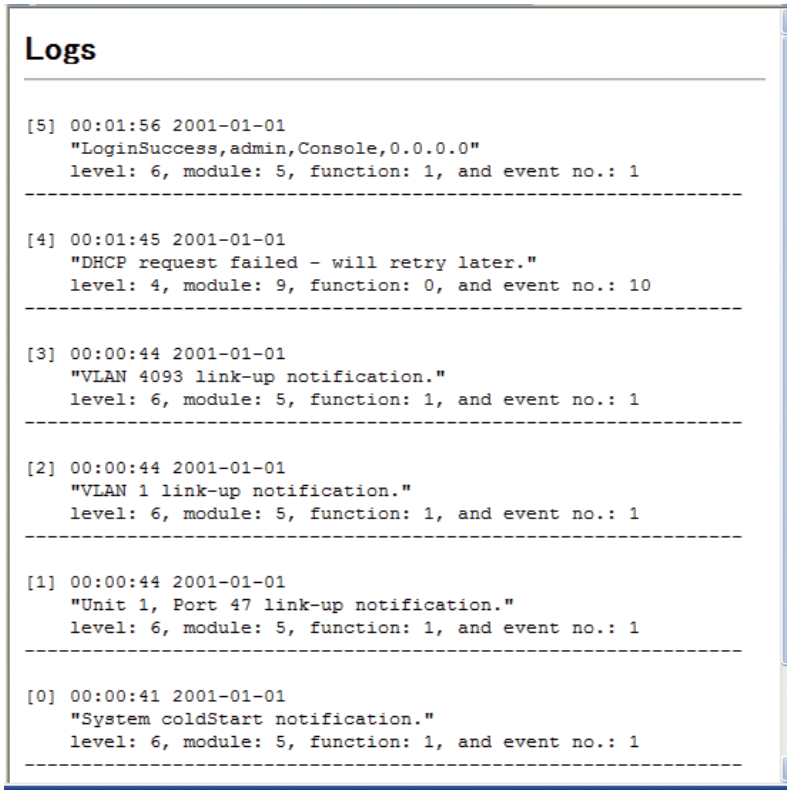
[System] → [Log] → [Remote Logs] をクリックします。"Host IP List" に IP アドレスを指定するには、"Host IP Address" に追加する IP アドレスを入力し、[Add] をクリックします。IP アドレスを削除するには、"Host IP List" から削除する IP アドレスをクリックし、その後 [Remove] をクリックします。

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。



SMTP（Simple Mail 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 P40 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 サーバのリスト。最大 3 つのアドレスを設定出来ます。

SMTP Server

本機からのアラートメッセージを受信する SMTP サーバ。アドレスをフィールドに入力し、[Add] をクリックすることでリストへの追加、[Remove] をクリックすることでリストからの削除をおこなえます。

Email Destination Address Liet

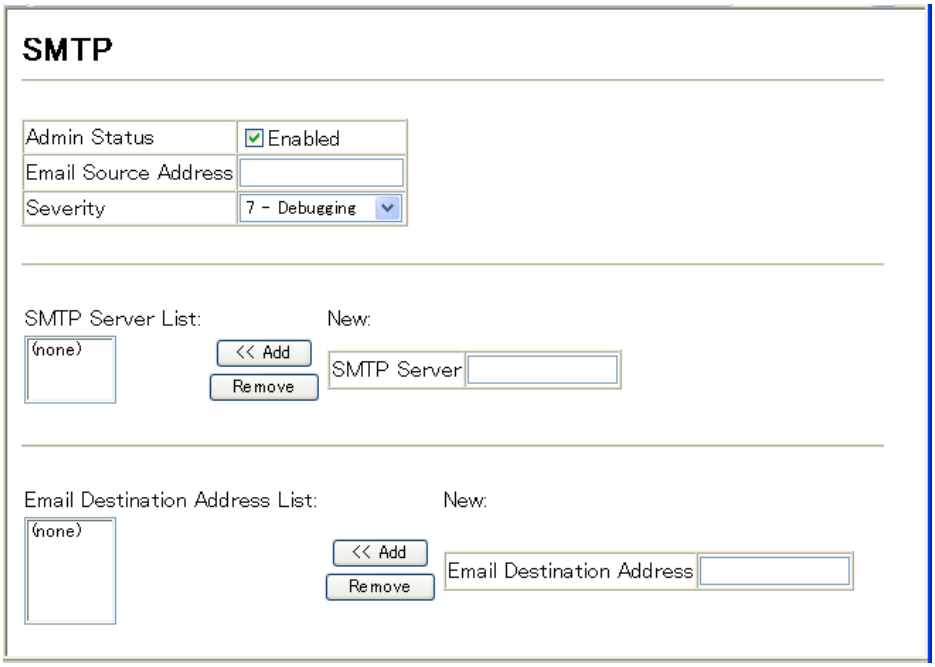
アラートメッセージを受信するアドレスのリスト。最大 5 つのアドレスを設定出来ます。

Email Destination Address

アラートメッセージを受信するアドレス。アドレスをフィールドに入力し、[Add] をクリックすることでリストへの追加、[Remove] をクリックすることでリストからの削除をおこなえます。

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。



3.3.10 再起動

システムの再起動をおこないます。直ちに再起動の実行または、指定した時間経過の後に再起動を実行するよう設定を行うことができます。

設定・表示項目

Hours

再起動までの時間（時）を設定します。(範囲：0-576; Default: 0)

Minutes

再起動までの時間（分）を設定します。(範囲：0-34560; Default: 0)

Reset

指定した時間経過後にスイッチを再起動します。

Refresh

カウントダウンタイマのリフレッシュを行います。

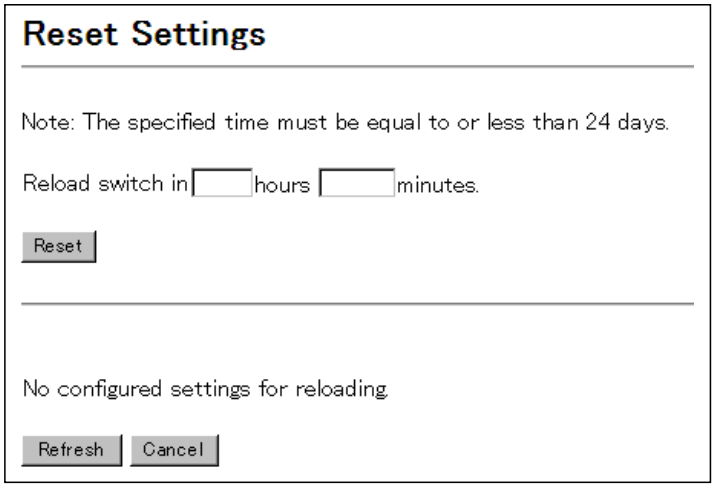
Cancel

予定されている再起動をキャンセルします。

[注意] 直ちにスイッチのリセットを実行には、"Hours"、"Minutes" フィールドに "0" を入力し、[Reset] をクリックしてください。

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。
非揮発性メモリに保存された全ての設定情報は保持されます。(設定情報の保存方法についての詳細は "P32「設定情報ファイルの保存・復元」" または "P324「copy」" を参照してください。)

3.3.11 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、手動で時刻の設定を行うこともできます。
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。

手動設定

本機では、SNTP を使用せず手動でシステムを時間を設定することも可能です。

設定・表示項目

Hours
時を設定（範囲：0-23　初期設定：0）

Minutes
分を設定（範囲：0-59　初期設定：0）

Seconds
秒を設定（範囲：0-59　初期設定：0）

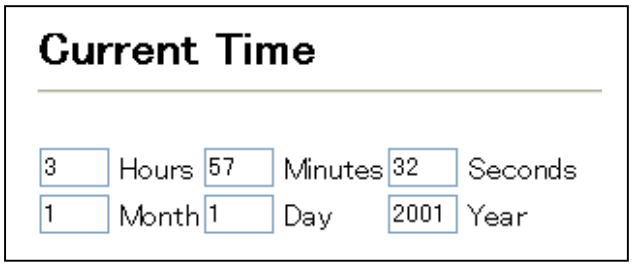
Month
月を設定（範囲：1-12　初期設定：1）

Day
日を設定（範囲：1-31　初期設定：1）

Year
年を設定（範囲：2001-2100　初期設定：2001）

設定方法

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



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・表示項目

SNTP Client

SNTP ユニキャストクライアントとして設定します。本モードを設定するには最低 1 つのタイムサーバを SNTP サーバとして設定する必要があります（初期設定：無効）

SNTP Poll Interval

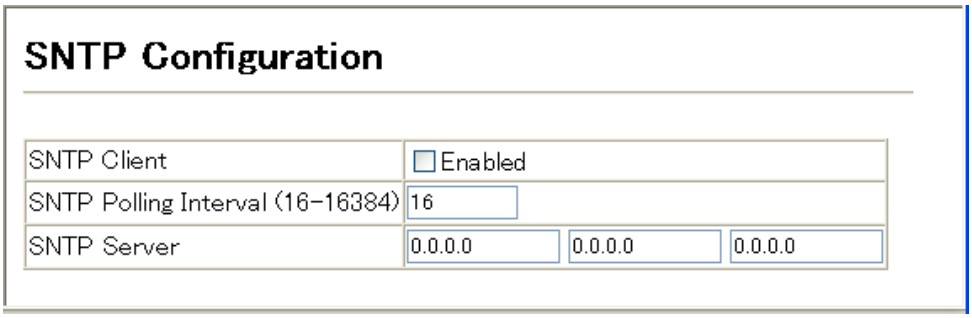
SNTP クライアントモード時のタイムサーバに対する時刻更新リクエストの送信間隔を設定します（範囲：16-16384 秒、初期設定：16 秒）

SNTP Server

最大 3 つのタイムサーバの IP アドレスの設定を行います。本機は 1 つ目のサーバを使用し時刻の更新を行いますが、更新を行えなかった場合には 2 つ目以降のサーバを使って時刻の更新を行います。

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。



NTP 設定

NTP クライアントは、時刻更新のために最大 50 の NTP サーバーの設定を可能にします。また、公認の NTP サーバのみから受信する、信頼性の高い更新を保証させる認証も可能になります。

認証キーとそれらに関連付けられたキー番号は中央で管理され、手動で NTP サーバとクライアントに配られます。キー番号とキー値は、サーバとクライアントの両方で一致しなくてはなりません。

設定・表示項目

NTP Client

スイッチを NTP クライアントとして動作するよう設定します。少なくとも１つのタイム・サーバに NTP サーバーリストで指定されるように要求します。（初期設定：Disable）

NTP Polling Interval

NTP サーバーからの時刻アップデートをリクエストする間隔。（1024 秒固定）

NTP Authenticate

スイッチと NTP サーバ間の、時刻リクエストと更新の認証を有効にします。
（初期設定：Disable）

NTP Server

NTP サーバの IP アドレスを設定します。本機は、設定した全てのサーバからの更新をリクエストでき、受け取った返答から最も正確な時刻更新を決定します。

Version

サーバでサポートされる NTP バージョンを指定します。（範囲：1-3　初期設定：3）

Authenticate Key

設定されたサーバとの認証に使用される、NTP 認証キーリストの中のキーの番号。
認証キーは、NTP サーバで設定されたキーと一致しなくてはいけません。

Key Number

NTP 認証キーリストの指定したキー値。NTP 認証キーリストには、最大 255 キーが設定できます。（範囲：1-65535）キー番号と値はサーバ、クライアントで一致しなくてはいけません。

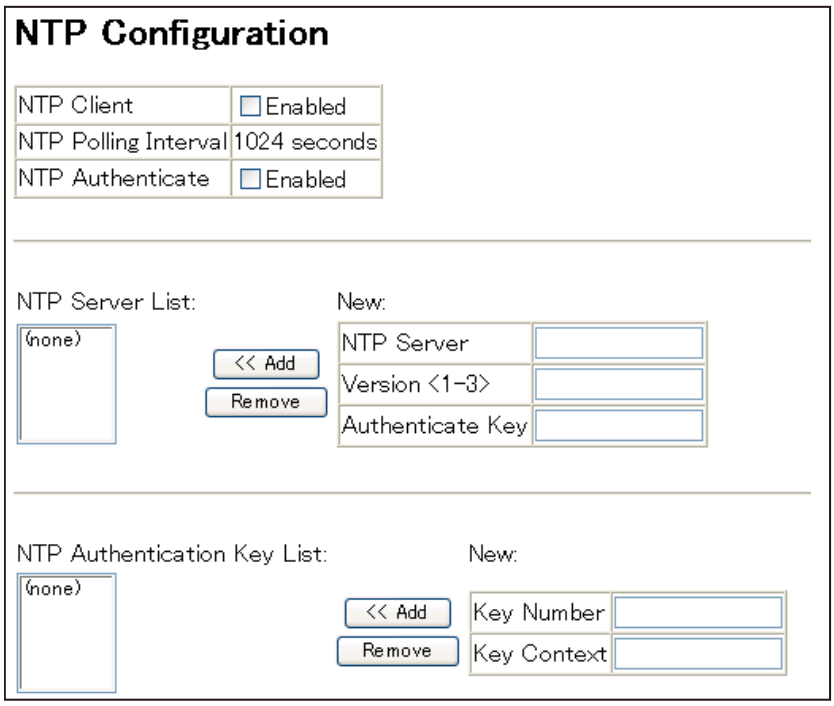
Key Context

MD5 認証キーストリングを指定します。

キーストリングは最大 32 文字の ASC II です。（大文字小文字を識別、スペースは不可）

設定方法

[NTP 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。
80 の既定義タイムゾーンから 1 つを選択、あるいは手動でローカルタイムのパラメータを設定することが出来ます。

設定・表示項目

Predefined Configuration

ドロップダウンボックスには 80 の既定義タイムゾーン設定が表示されます。

それぞれの項目は UTC からのオフセットとタイムゾーンでカバーされる最低 1 つの主要都市を示します。

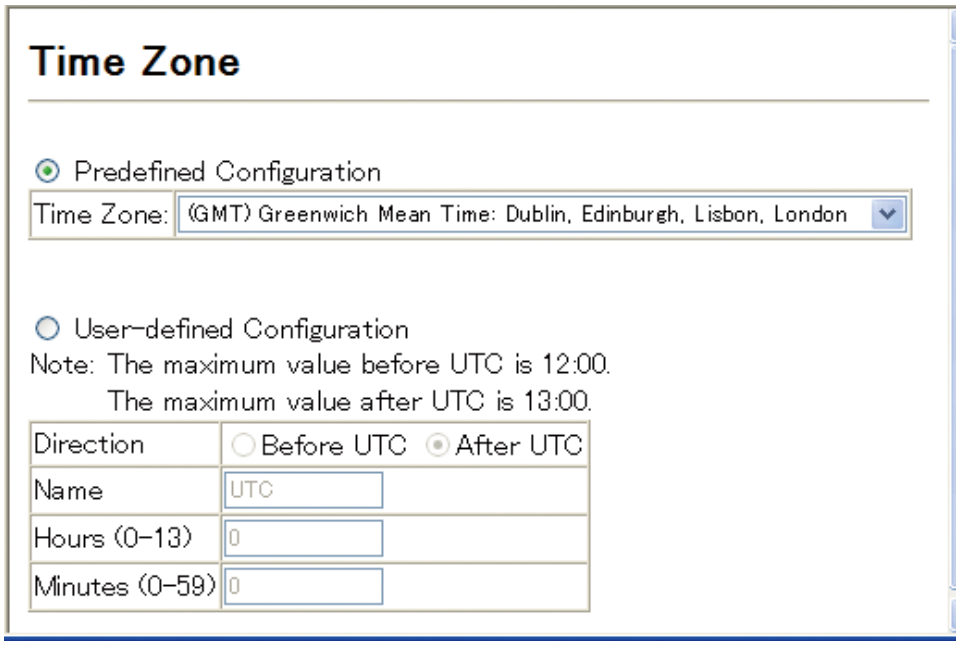
User-defined Configuration

手動でローカルタイムゾーンパラメータの設定を行います。

- Direction ー 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。
- Name ータイムゾーンに対する名称を設定します（範囲：1-29 文字）
- Hours（0-13）ー Hours (0-12) ー UTC からの時間の差を設定します。
- Minutes（0-59）ー UTC からの時間（分数）の差を設定します。

設定方法

[SNTP] → [Clock Time Zone] をクリックします。必要項目を入力し、[Apply] をクリックします。



サマータイムの設定

夏の数ヶ月間、システム時計を先に進めます（夏時間）

設定・表示項目

Summer Time in Effect

システム時計調整の有無を示します。

Status

サマータイム設定の有効化。

Name

タイムゾーン名を指定（1-30 **文字）**

Mode

設定モードを選択します。

Predefined Mode

世界のいくつかの主要地域のために前もって定義されている設定情報を使用し、サマータイムステータスおよび設定を行います。

Date Mode

1 **回ごとに、サマータイムの開始と終了およびオフセットタイムを設定します。**
このモードは現時設定されているタイムゾーンと比較して、サマータイムゾーンを設定します。

- Offset －**通常のタイムゾーンからオフセットされる時間を分で指定。（範囲：**0-99 **分）**
- From －**サマータイムオフセットの開始時間を設定。**
- To －**サマータイムオフセットの終了時間を設定。**

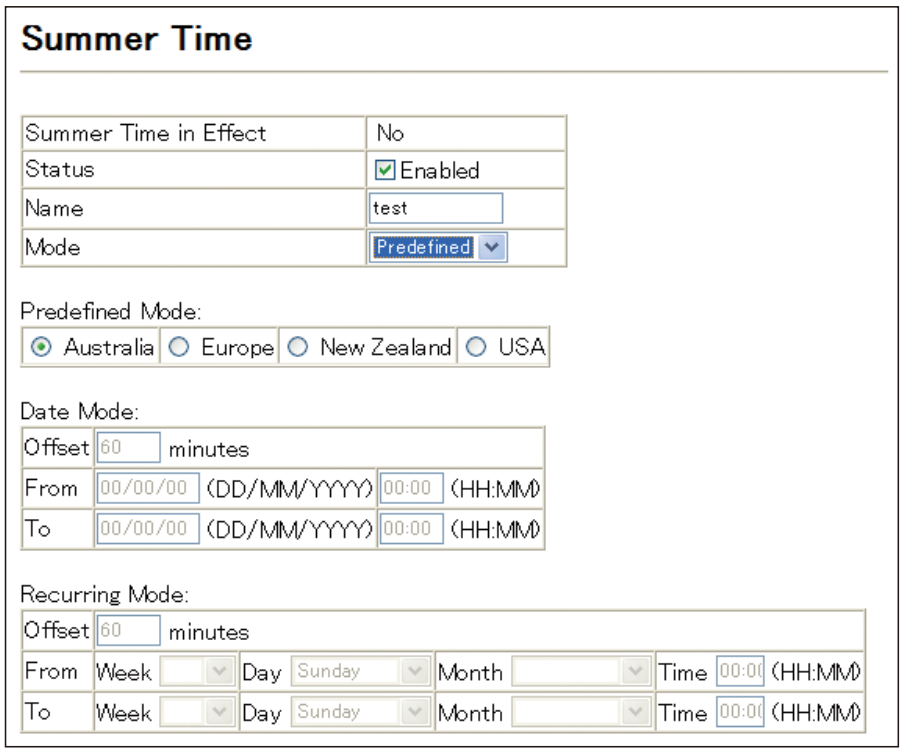
Recurring Mode

Recurring**（繰り返し）ベースで、サマータイムのオフセットタイムの開始および終了時間を設定します。**
このモードは現在設定されたタイムゾーンと比較して、サマータイムゾーンを設定します。

- Offset －**通常のタイムゾーンからオフセットされる時間を分で指定。（範囲：**0-99 **分）**
- From －**サマータイムオフセットの開始時間を設定。**
- To －**サマータイムオフセットの終了時間を設定。**

設定方法

[SNTP] → [Summer Time] をクリックします。設定モードを選択し、必要項目を入力します。
ステータスを有効にし、[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。

表 3-1 SNMPv3 セキュリティモデルとレベル

Model	Level	Group	Read View	Write View	Notify View	security
v1	noAuthNoPriv	public (read only)	defaultview	none	none	Community string only
v1	noAuthNoPriv	private (read/write)	defaultview	defaultview	none	Community string only
v1	noAuthNoPriv	user defined	user defined	user defined	user defined	Community string only
v2c	noAuthNoPriv	public (read only)	defaultview	none	none	Community string only
v2c	noAuthNoPriv	private (read/write)	defaultview	defaultview	none	Community string only
v2c	noAuthNoPriv	user defined	user defined	user defined	user defined	Community string only
v3	noAuthNoPriv	user defined	user defined	user defined	user defined	A user name match only
v3	AuthNoPriv	user defined	user defined	user defined	user defined	Provides user authentication via MD5 or SHA algorithms
v3	AuthPriv	user defined	user defined	user defined	user defined	Provides user authentication via MD5 or SHA algorithms and data privacy using DES 56-bit encryption

[注意]　既定義のデフォルトグループとビューはシステムから削除可能です。
その後にアクセスに必要な、カスタマイズグループとビューを定義することができます。

3.4.1 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

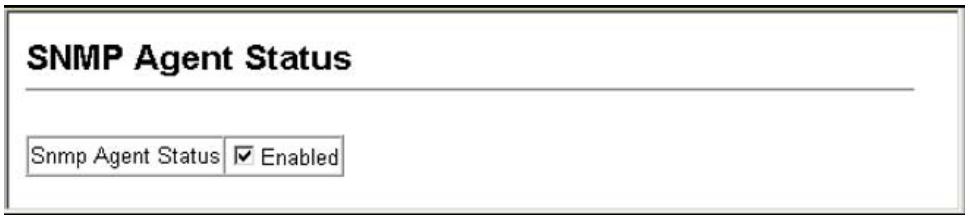
設定・表示項目

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。



3.4.2 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

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）

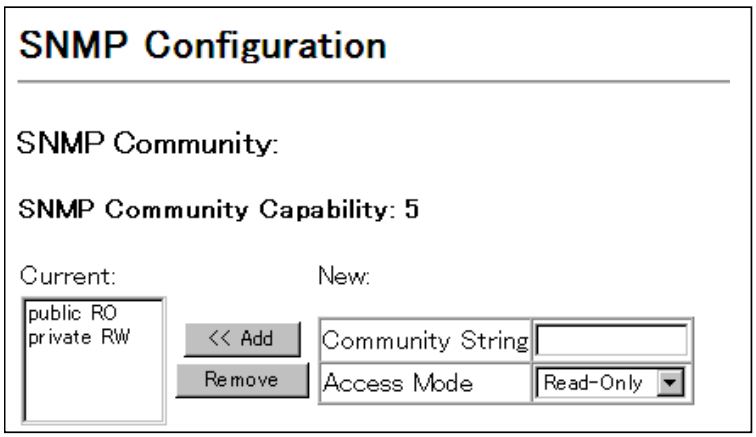
Access Mode

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。



3.4.3 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。**

機能解説

- 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する際には（**authNoPriv **または** authPriv**）、最初に** P51 **「**SNMPv3 **ユーザーの設定」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。**

- **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。**
  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インフォームの使用を決定してください。

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。

- noAuthNoPriv – **認証も暗号化も行いません**
- AuthNoPriv – **ユーザ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 – **認証と暗号化の両方を行います。（**v3 **セキュリティモデルでのみ設定可）**

Trap Inform

インフォームの有効 / 無効（v2c **または** v3 **ホスト設定時のみ使用可）**

- Timeout – **再送までの待ち時間（設定範囲：**0-2147483647 **センチセカンド）**
  （初期設定：1500 **センチセカンド）**
- Retry times – **再送を行う最大回数（設定範囲：**0-255　**初期設定：**3 **回）**

Enable Authentication Traps

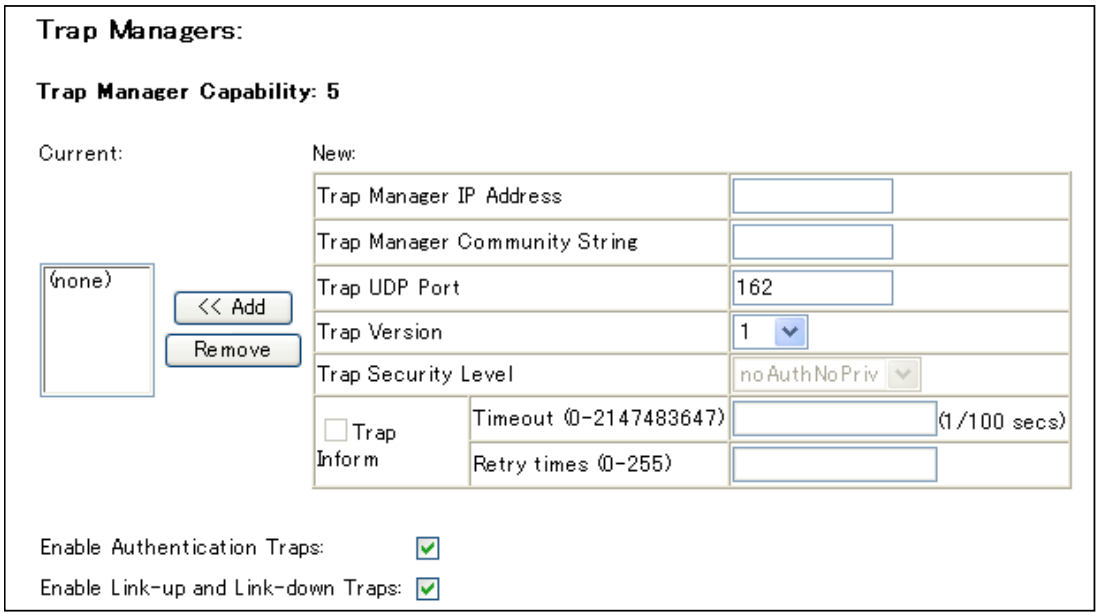
認証時に不正なパスワードが送信された場合にトラップが発行されます
（初期設定：有効）

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。**



3.4.4 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

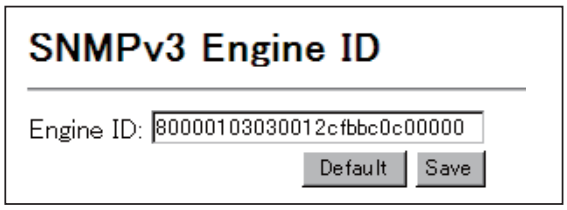
SNMPv3 **エンジンは、スイッチ上の独立した** SNMP **エージェントです。このエンジンはメッセージの再送、遅延およびリダイレクションを防止します。エンジン** ID **は、ユーザーパスワードと組み合わせて、**SNMPv3 **パケットの認証と暗号化を行うためのセキュリティキーを生成します。**

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。**

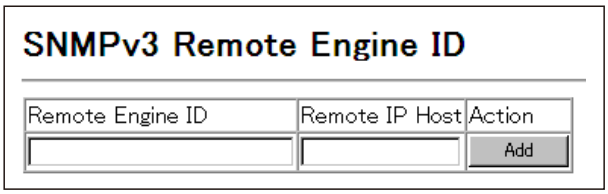


リモートエンジン ID の設定

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 P57 「トラップマネージャ・トラップタイプの指定」および P63 「SNMPv3 リモートユーザーの設定」を参照してください）

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）

Security Model

セキュリティモデルを選択します（v1,v2c,v3　初期設定：v1）

Security Level

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 Protocol

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 Protocol

暗号化プロトコル。DES56bit のみ使用可。

Privacy Password

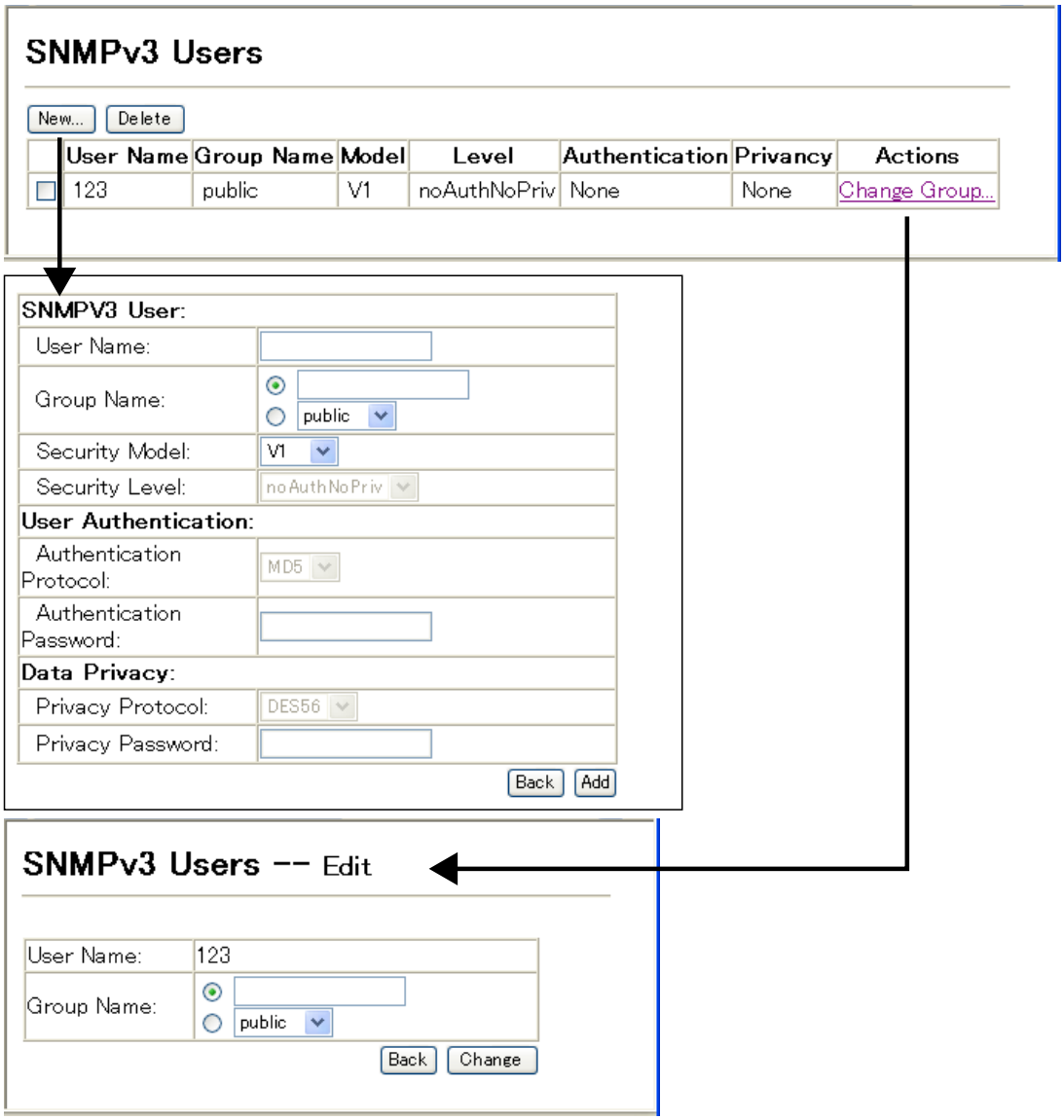
プライバシーパスワード（最小 8 文字）

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 P57 「トラップマネージャ・トラップタイプの指定」および P60 「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（P60 参照）

Security Model

セキュリティモデル（v1,v2c,v3　初期設定：v1）

Security 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 Protocol

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 Protocol

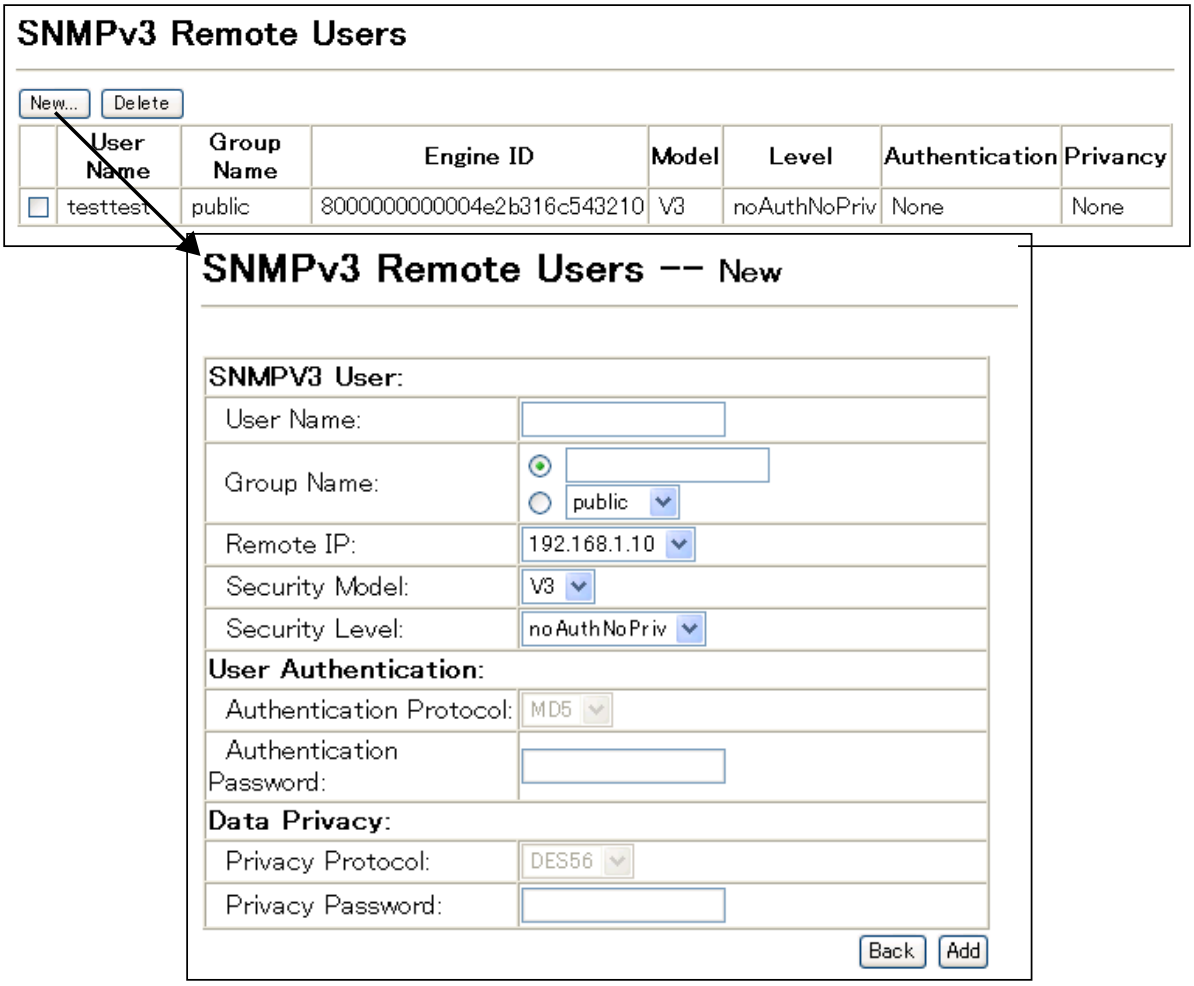
暗号化プロトコル。DES56bit のみ使用可。

Privacy Password

プライバシーパスワード（最小 8 文字）

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 – **認証も暗号化も行いません**
- 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**）

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**

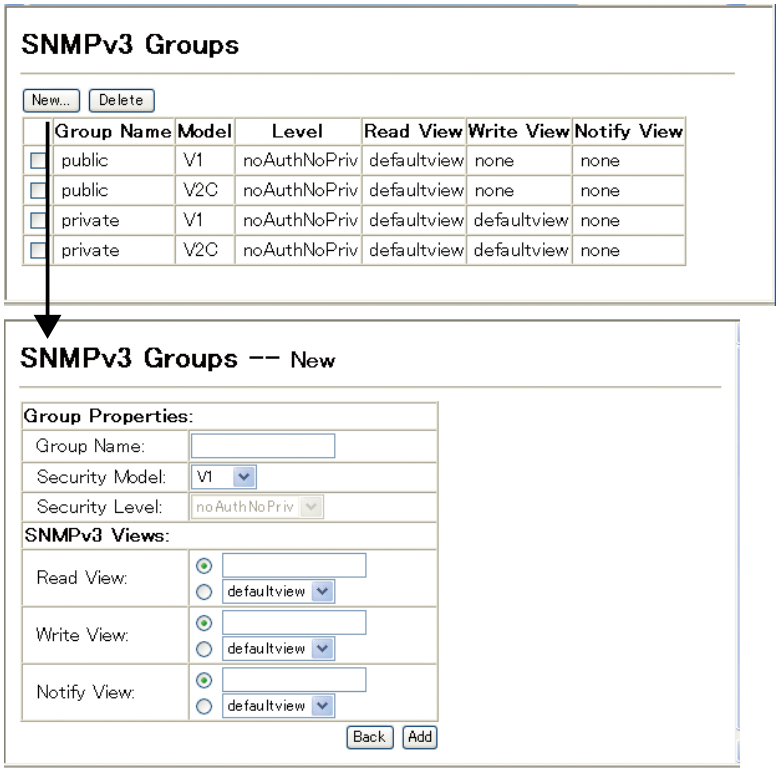
Notify View

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）

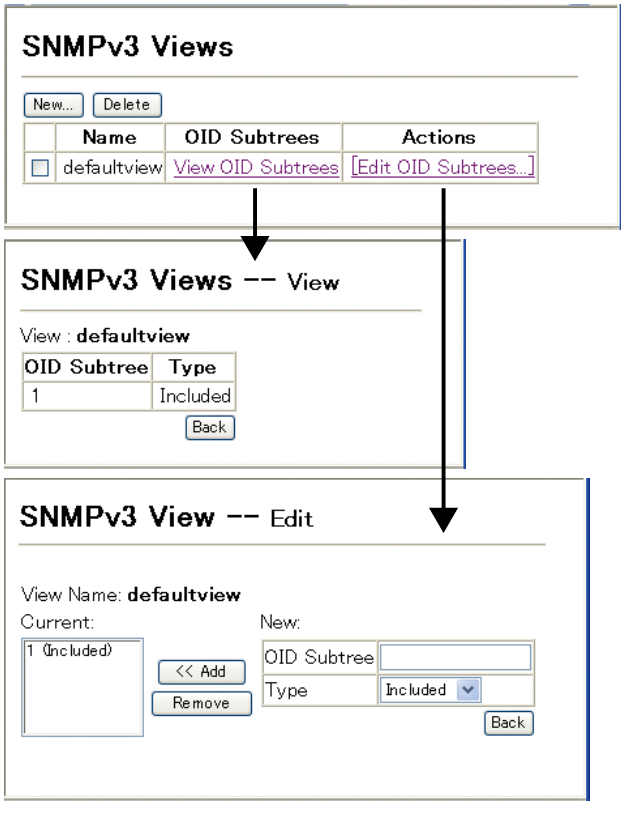
View OID Subtrees
ビューの内容が表示されます

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 トラフィックフローのサンプリング

フローサンプリング（sFlow）機能は、リモート sFlow コレクタと共に本機に装備されており、ネットワーク管理者はトラフィックのタイプとレベルのオーバービューが正確・詳細かつリアルタイムで確認できます。

SFlow エージェントは、本機を通過する全てのパケットから n の内１のパケットを採取します。sFlow データグラムとしてサンプルを再度カプセル化し、これらを sFlow コレクタに転送します。
このサンプリングは内部ハードウェアレベルで起こるのに対し、従来の調査はモニタインタフェースでサンプルされたトラフィックの部分的なビューのみの物でした。
さらに、ローカル分析は行われない為、sFlow エージェントによって課せられるプロセッサとメモリロードは最小です。
高トラフィックレベルであってもスイッチのワイヤスピード転送特性は維持されます。
コレクタはネットワーク上の様々な sFlow エージェント（他のスイッチまたはルータ）からストリームをタイムリーに受け取ります。

SFlow ストリームの解析は、様々な方法で利用可能な傾向と情報を明示します。

- ネットワークの問題を検出・診断・修復
- リアルタイム輻輳管理
- アプリケーション（P2P, Web, DNS, その他）の混在と変更を認識
- 無許可のネットワークアクティビティの身元確認と追跡
- アカウンティングの利用
- トレンディングとキャパシティプランニング

3.5.1 sFlow グローバルパラメータの設定

フローサンプリングは、設定を行うポートだけでなくスイッチでグローバルに有効化される必要があります。スイッチのハードウェアデザイン上の理由から、フローサンプリングとサンプリングレートは下のテーブルで示されるように、指定ポートグループでのみ有効にできます。ただしそれぞれのギガビットポート（49-52）は個々に制限が可能です。

設定・表示項目

Global Status
スイッチで sFlow **をグローバルに有効化**

Group/Port Members
100BASE-TX **ポートは、スイッチ** ASIC **の制限で** 8 **つのグループに組織化されます。**
4 **つのギガビットポートはそれぞれ個別のグループになります。**

表 3-2 sFlow **グループとポートメンバー**

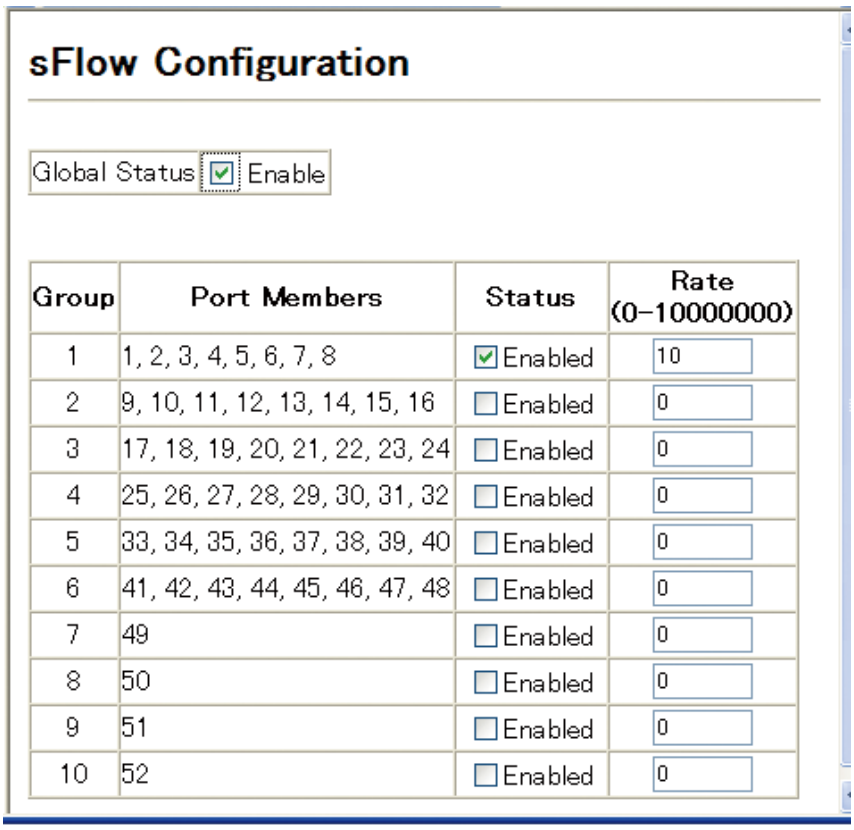
グループ	ポートメンバー
1	1,2,3,4,5,6,7,8
2	9,10,11,12,13,14,15,16
3	17,18,19,20,21,22,23,24
4	25,26,27,28,29,30,31,32
5	33,34,35,36,37,38,39,40
6	41,42,43,44,45,46,47,48
7	49
8	50
9	51
10	52

Status
SFlow **を指定されたグループのポートで有効にします。**

Rate
パケットサンプリングレートを設定します。0 **に設定するとサンプリングは無効になります。**
レートを 100 **に設定した場合、**100 **パケット毎に** 1 **つのサンプリングを設定します。**
（範囲：0-10000000　**初期設定：**0**）**

設定方法

[sFlow] → [Configuration] **をクリックします。**
フローサンプリングのグローバルステータス、サンプルされるポートまたはポートグループ、サンプリングレートを設定し、[Apply] **をクリックします。**



3.5.2 sFlow ポートパラメータの設定

サンプルデータ、ペイロードパラメータ、サンプリングインターバルのディスティネーションパラメータを設定します。

設定・表示項目

Port

設定をおこなうポートを選択します

Receiver Owner*

レシーバ名

Receiver IP Address*

SFlow **コレクタの** IP **アドレス**

Receiver Port*

sFlow **コレクタが** sFlow **リスニングをおこなう** UDP **ポート（範囲：**0-65534　**初期設定：**6343）

Time Out

全ての sFlow **ポートパラメータがリセットされる前に、**sFlow **プロセスがコレクタへ連続的にサンプルを送る時間。（レシーバオーナー、タイムアウト、最大ヘッダサイズ、最大データグラムサイズ、フローインターバル）**0 **秒に設定した場合はタイムアウトを無効にします。（範囲：**0-10000000 **秒　初期設定：**0 **秒）**
フローサンプリングが現在進行中の場合、チェックボックスはシステムによってクリアされます。
タイムアウトを変更するには、チェックボックスをマークし、タイムアウト値を入力後 Apply **をクリックして下さい。**

Max Header Size

SFlow **データグラムヘッダの最大サイズ（範囲：**64-256bytes　**初期設定：**128bytes）

Max Datagram Size

SFlow **データグラムペイロードの最大サイズ（範囲：**200-1500bytes　**初期設定：**1400bytes）

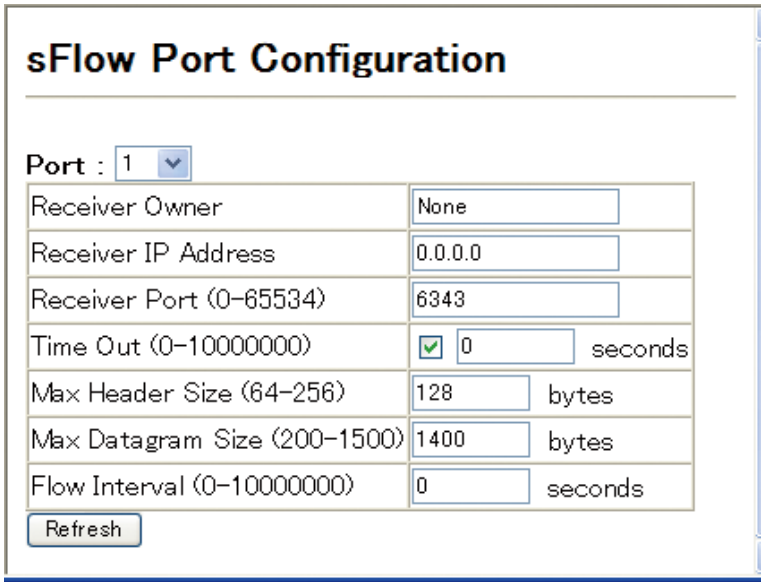
Flow Interval

sFlow **プロセスがサンプルデータグラムにカウンタ値を加える間隔。**0 **秒はこの機能を無効にします。（範囲：**0-10000000 **秒　初期設定：**0 **秒）**

* **サンプリングは、こららのフィールドの設定を行う前にタイムアウトを** 0 **にすることで無効になります。**

設定方法

[sFlow] → [Port Configuration] **をクリックします。必要な項目を入力し、**[Apply] **をクリックします。**



3.6 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。

- **ユーザアカウント** - 指定されたユーザのアクセス権を手動で設定します。
- **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。
- **暗号化キー** -RADIUS および TACACS+ の暗号化キーを設定します。
- **AAA** - アクセス権の構成を設定するためのフレームワークを提供します。
- **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。

3.6.1 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。

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

- ー **User Name** ― ユーザ名 (最大文字数：8 文字、最大ユーザ数：16 人)
- ー **Access Level** ― ユーザのアクセスレベル (オプション：Normal, Privileged)
- ー **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

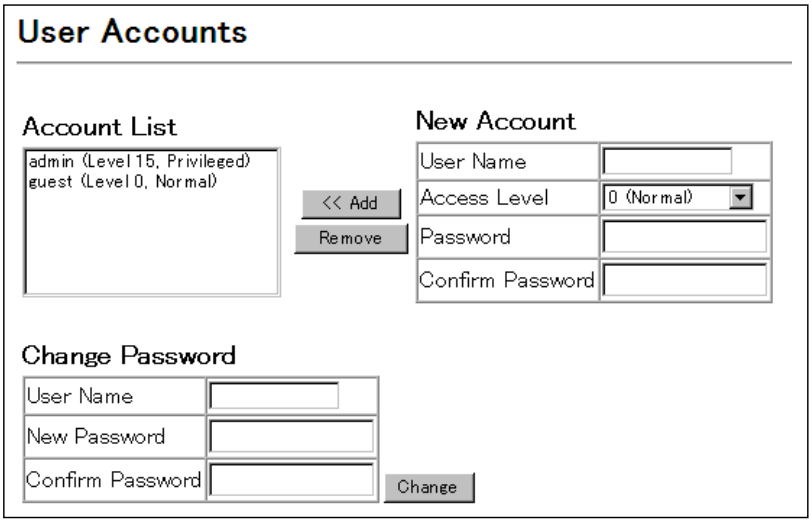
既存ユーザアカウントのパスワードを変更します。

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

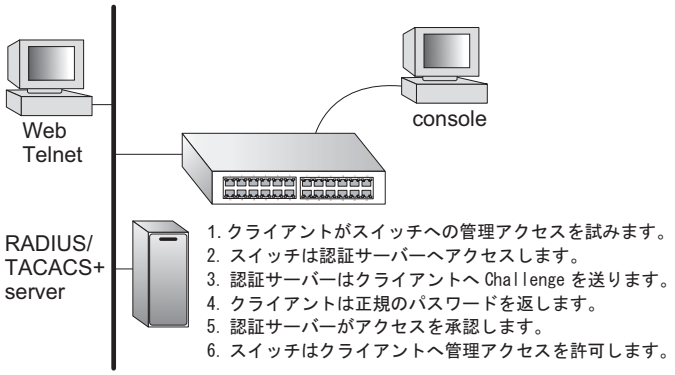
[Security] → [User Accounts] をクリックします。新規のユーザアカウントを設定するには、ユーザ名 (User Name)、ユーザのアクセスレベル (Access Level) を設定します。パスワード (Password) を入力し、再確認のためにパスワード (Confirm Password) を再度入力します。[Add] をクリックすると、新規のユーザアカウントは保存され [Account List] 欄に追加されます。既存ユーザアカウントのパスワードを変更する場合は、[Change Password] 欄にユーザ名 (User Name) 及び新たなパスワード (New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



3.6.2 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。

- **Local** ― **本機内部においてユーザ認証を行います。**
- **RADIUS** ― RADIUS **サーバによるユーザ認証を行います。**
- **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。**

Server Index

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。**

Server IP Address

RADIUS **サーバの** IP **アドレス**

Authentication Port Number

認証メッセージに使用される、認証サーバのネットワークポート（UDP**）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、認証サーバの UDP **ポート番号（**1-65535**、初期設定** :1812**）**

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

Global

TACACS+ **サーバの設定をグローバルに適用します。**

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**）**

Number of Server Transmits

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サーバからの応答を待つ待機時間（秒）（範囲 :1-540**、初期設定** :5**）**

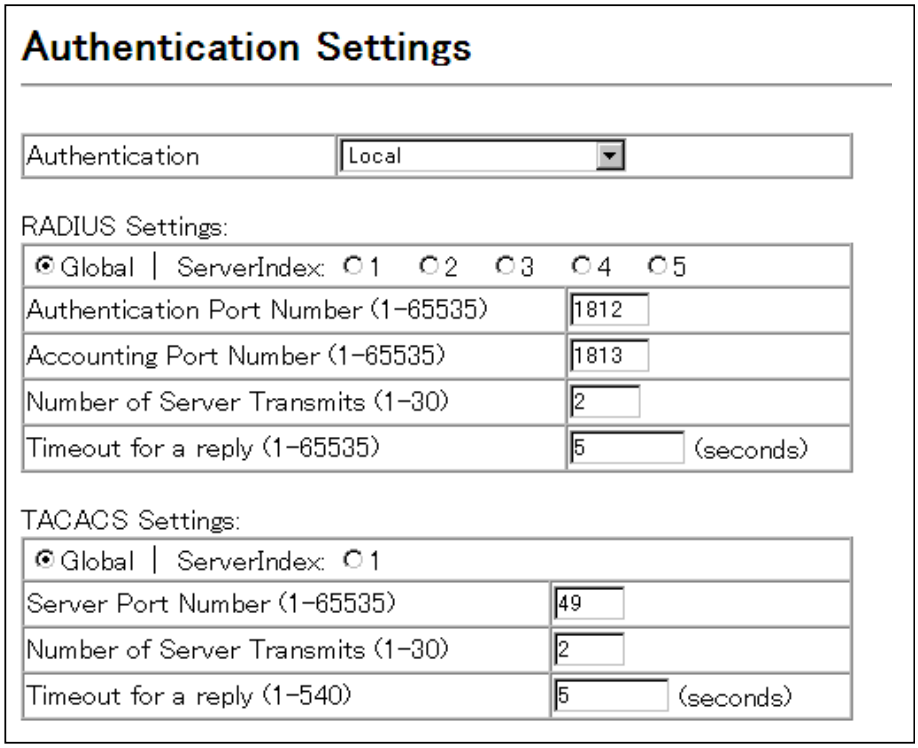
Secret Text String

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。**



3.6.3 暗号化キーの設定

暗号化キー機能は、全ての RADIUS **および** TACACS+ **サーバ暗号化キーの管理に、セントラルロケーションを提供します。**

設定・表示項目

RADIUS 設定

Global

RADIUS **暗号化キー設定をグローバルに適用します。**

Server Index

設定する RADIUS **サーバを指定します。**

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 :48 **文字）**

Confirm Secret Text String

確認のため、前のフィールドに入力したストリングを再度入力してください。

Change

選択された暗号化キーの追加、もしくは修正を行います。

TACACS+ 設定

Global

設定をグローバルに適用します。

Server Index

設定する TACACS+ **サーバを指定します。**

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（最大文字数 :48 **文字）**

Confirm Secret Text String

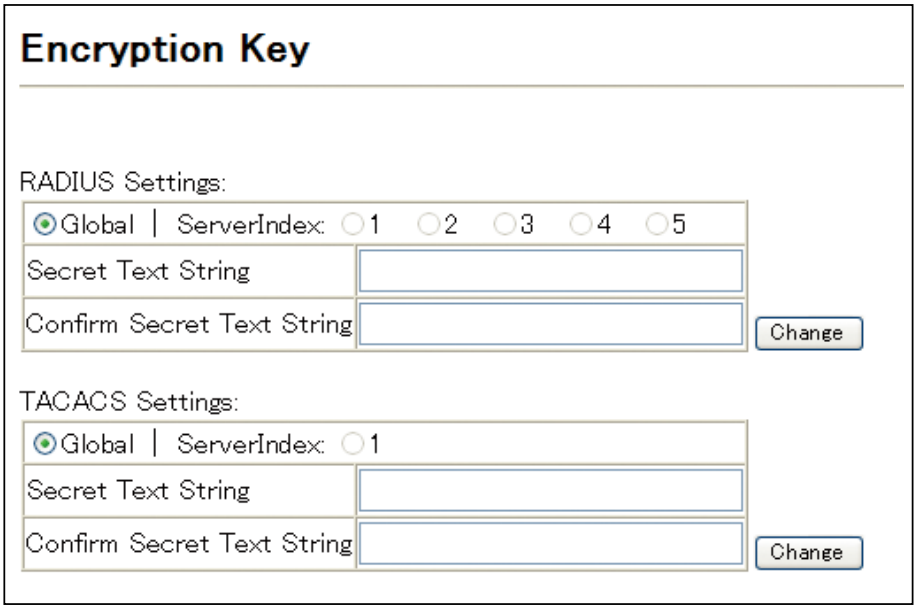
確認のため、前のフィールドに入力したストリングを再度入力してください。

Change

選択された暗号化キーの追加、もしくは修正を行います。

設定方法

[Security] → [Encryption Key] **をクリックします。適切な** RADIUS **または** TACACS+ **サーバインデックスを選択し、テキストストリングの入力と確認の為再入力を行い、**[Change] **をクリックします。**



3.6.4 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

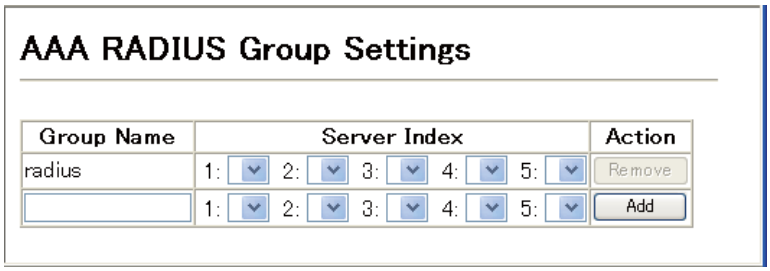
RADIUS **サーバーのグループ名を指定します（範囲：**1 ～ 255 **文字）**

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

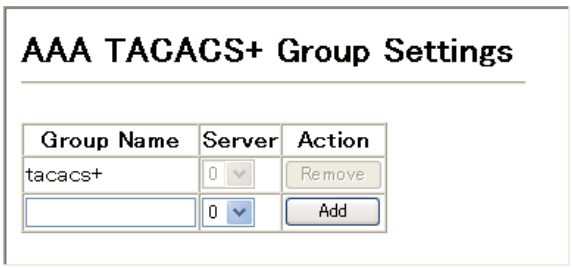
TACACS+ **サーバーのグループ名を指定します（範囲：**1 ～ 255 **文字）**

Server

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。**（P75 **「ローカル / リモート認証ログオン設定」を参照）**

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

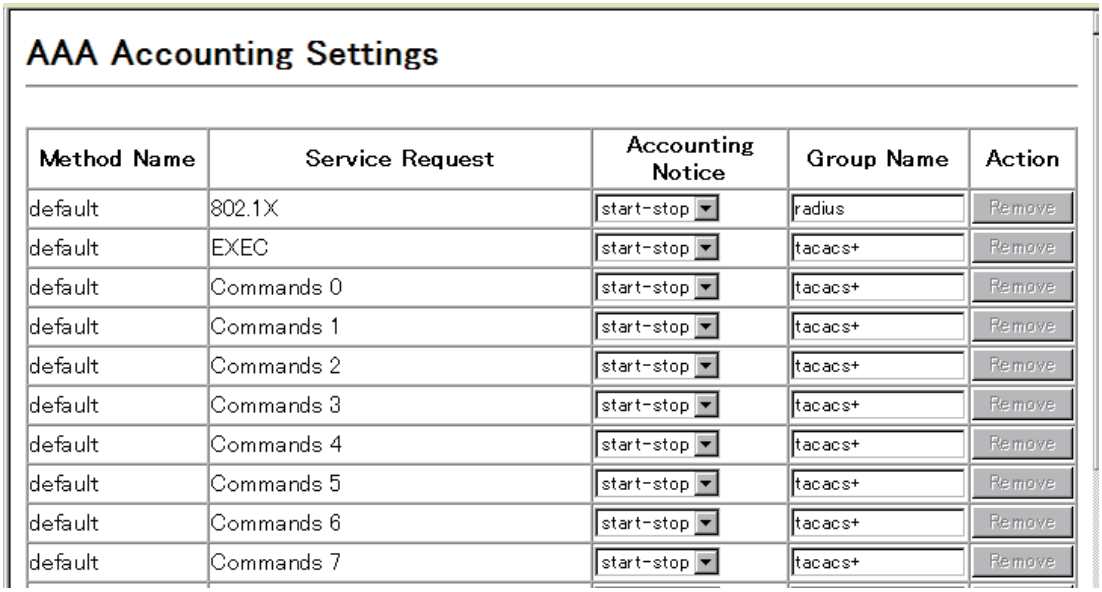
ログインした時点からログアウトした時点までのユーザーの活動を記録します。

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。

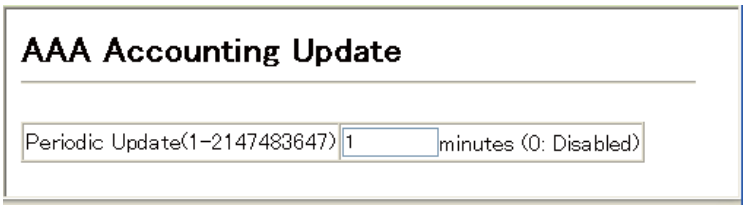
設定・表示項目

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　初期設定：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

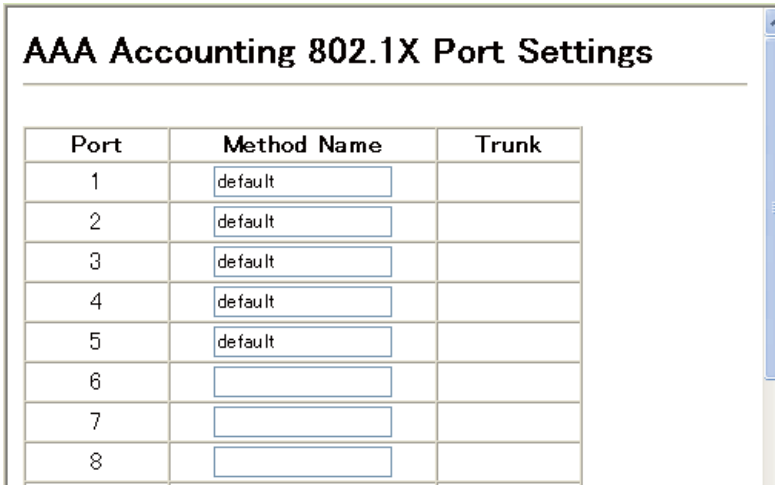
ポート、トランクポートの番号を表示します。

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

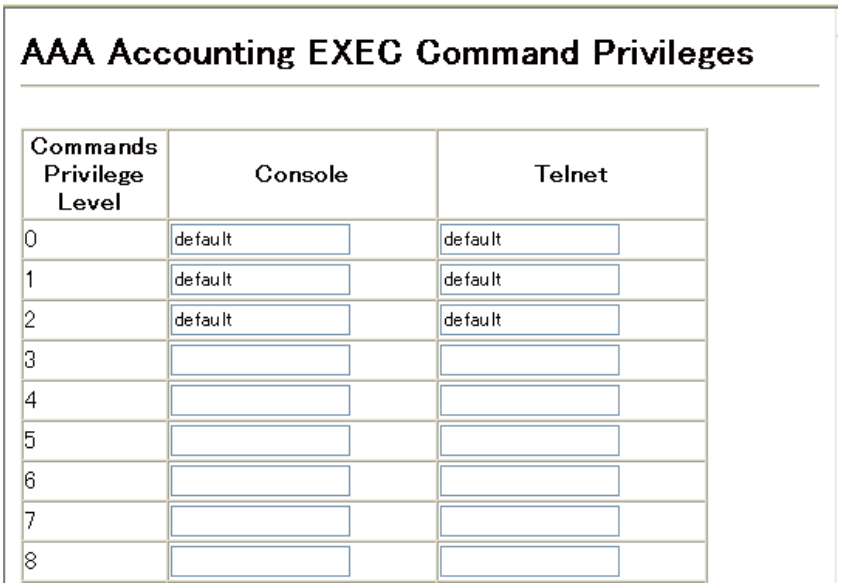
CLI の特権レベルです（範囲：0 ～ 15）

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。

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。

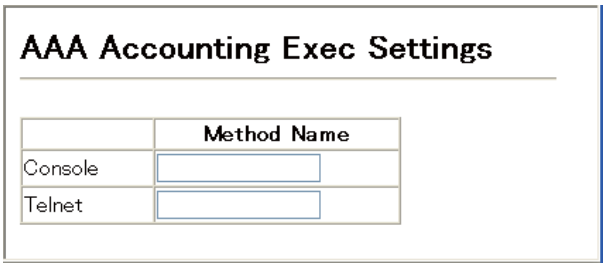
設定・表示項目

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

全てのアカウンティングを表示します。メソッドは指定したインタフェースに適用され、基本アカウンティング情報はユーザセッションの間記録されます。

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

Accounting Type

アカウンティングサービスを表示します。

User Name

登録されたユーザー名を表示します。

Interface

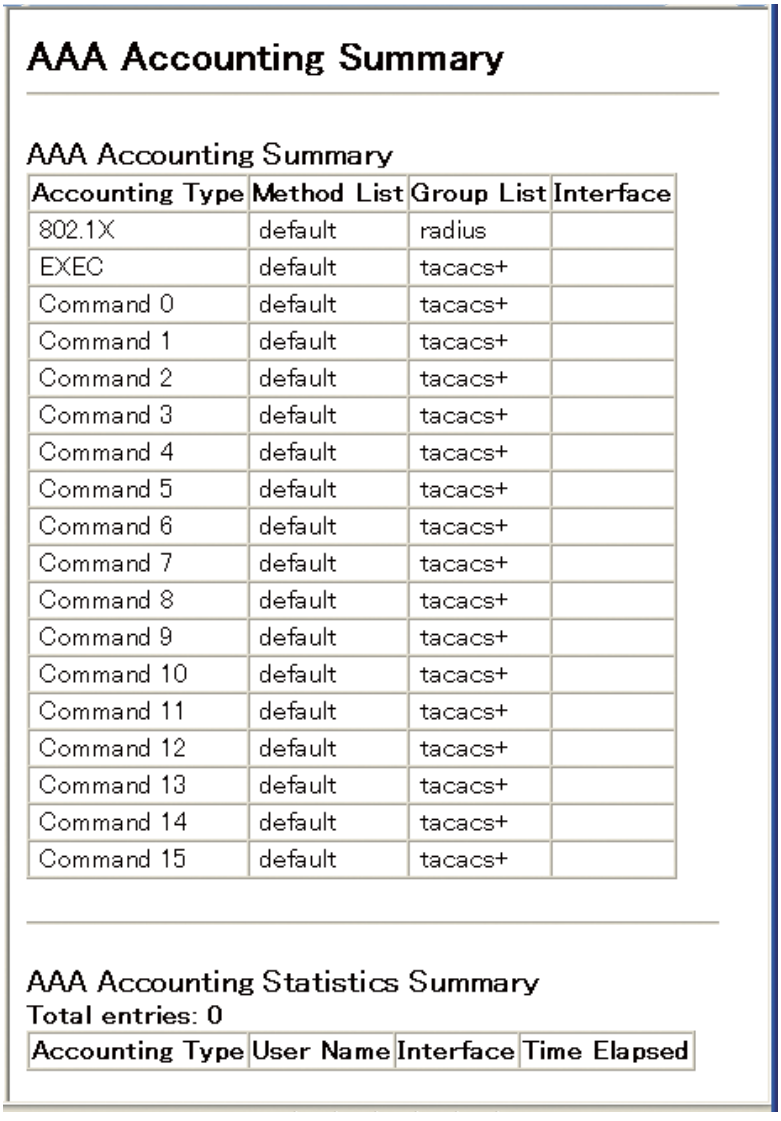
このユーザーがスイッチにアクセスする受信ポートの番号を表示します。

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] → [Accounting] → [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

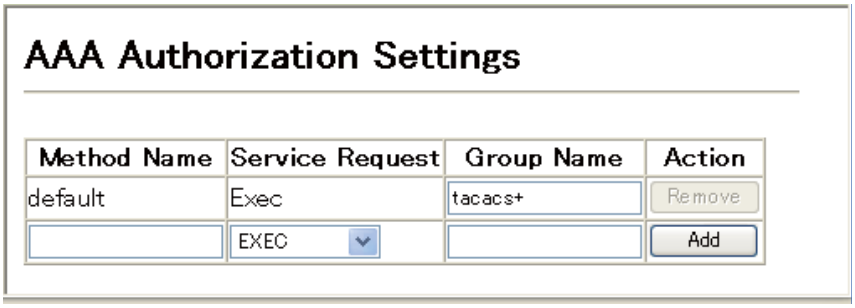
ローカルコンソール接続、Telnet 接続へのオーソライゼーションを設定します。

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。

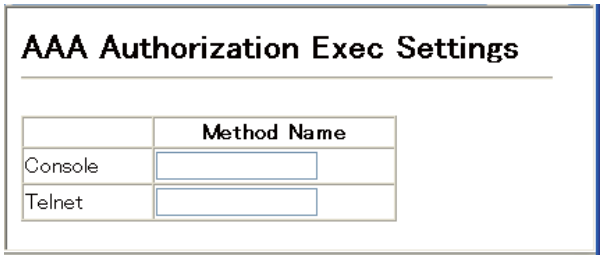
設定・表示項目

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

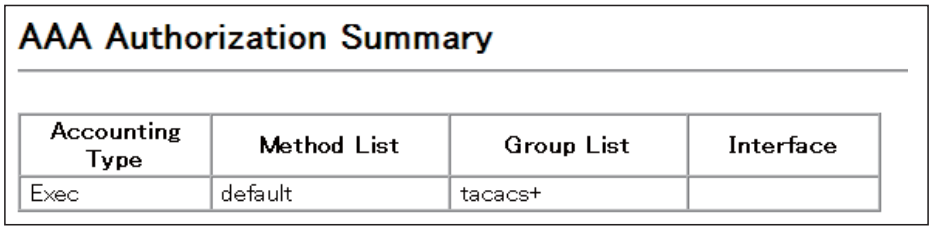
オーソライゼーションサービスグループを表示します。

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。



3.6.5 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 以上または NetscapeNavigator 6.2 以上、Mozilla Firefox 2.0.0.0 以上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 6.2 以上	Windows 98、Windows NT (サービスパック 6A)、Windows 2000、Windows XP、Solaris 2.6
Mozilla Firefox 2.0.0.0 以上	Windows 2000、Windows XP、Linux

※ 安全なサイトの証明を指定するためには、P92 「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 設定

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

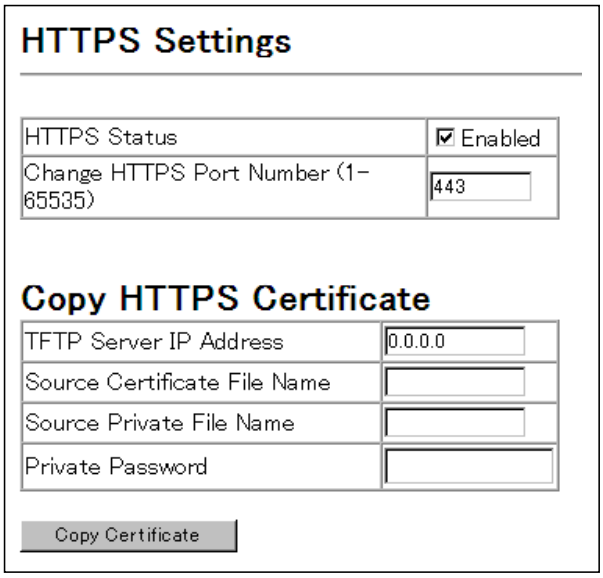
HTTPS 接続に使用される UDP ポートを指定します（初期設定：443）

HTTPS 証明書のコピー

この機能について、より詳しい情報は P92 「サイト証明書の設定変更」をご覧下さい。

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 サーバを使用して既存の証明書と置き換えます。

設定・表示項目

TFTP Server IP Address

証明書ファイルを含む、TFTP サーバの IP アドレス。

Source Certificate File Name

TFTP サーバに保存されている証明書ファイル名。

Source Private File Name

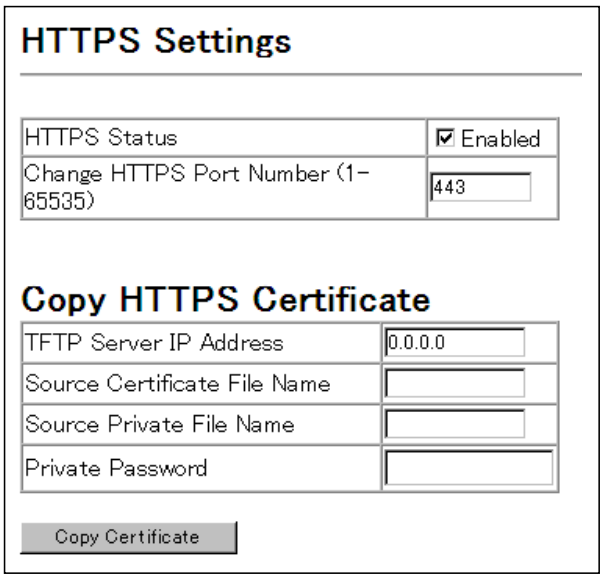
TFTP サーバに保存されているプライベートキーファイル名。

Private Password

プライベートキーファイルに保存されているパスワード。

設定方法

[Security] → [HTTPS Settings] をクリックします。必要項目を入力し、[Apply] をクリックします。



3.6.6 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
15684995401867669259333946775054617325313674890836547254150202455931998
68544358361651999923329781766065830956
10825913212890233765468017262725714134287629413011961955667 82
59566410486957427888146206519417467729848654686157177393901647793559423
03577413098022737087794545240839717526463580581767167095748047761 17

（3）**クライアント公開キーの本機への取り込み** ― 324 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 35134108168560989392104094492015542534763164192187295892114317 3
88005553616163105177594083868631109291232226828519254374603100937187721
19969631781366277414168985132049117204830339254324101637997592371449011
93800609025394840848271781943722884025331159521348610229029789827213532
671316294325328189150453063939166 43 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）**認証** － 次の認証方法の内ひとつが使用されます。

パスワード認証（SSH v1.5 **または** V2 **クライアント**）

a. **クライアントはサーバへパスワードを送信します。**

b. **スイッチはクライアントのパスワードとメモリに保存されているものを比較します。**

c. **もしマッチするならば、接続は許可されます。**

[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。

パブリックキー認証－ SSH **クライアントがスイッチへの接続を試みる時、**SSH **サーバはホストキーペアを使用し、セッションキーと暗号化方式のネゴシエートを行います。**
スイッチに保存されるパブリックキーに対応するプライベートキーを持つクライアントだけがアクセス可能です。以下のやり取りは、このプロセスの間に行われます。

SSH v1.5 **クライアント認証**

a. **クライアントはスイッチへ** RSA **パブリックキーを送信します。**

b. **スイッチはクライアントのパスワードとメモリに保存されているものを比較します。**

c. **一致した場合、スイッチはそのシークレットキーを使用してランダムな** 256-bit **ストリングを、**challenge **として生成します。このストリングをユーザパブリックキーで暗号化し、クライアントへ送信します。**

d. **クライアントはプライベートキーを使用して** challenge **ストリングを解読し、**MD5 **チェックサムを計算し、それをスイッチへチェックサムバックします。**

e. **スイッチは、クライアントから送られたチェックサムと、計算されたオリジナルストリングを比較します。**2 **つのチェックサムがマッチした場合、クライアントのプライベートキーが認証パブリックキーと一致したことを意味し、クライアントは認証されます。**

SSH v2 **クライアント認証**

a. **クライアントは最初に、**DSA **パブリックキー認証が受容出来るかどうかを決定する為、スイッチへ問い合わせます。**

a. **もし、指定されたアルゴリズムがスイッチでサポートされている場合、クライアントに認証プロセスを続けるよう知らせます。サポートされていない場合は要求は拒絶されます。**

a. **クライアントはプライベートキーを使用して生成された署名をスイッチへ送信します。**

a. **サーバがこのメッセージを受け取ると、供給されたキーが認証の為に受容できるかどうかをチェックします。可能な場合、署名が正しいかどうかをチェックします。**
両方のチェックがに成功すると、クライアントは認証されます。

[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。

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。

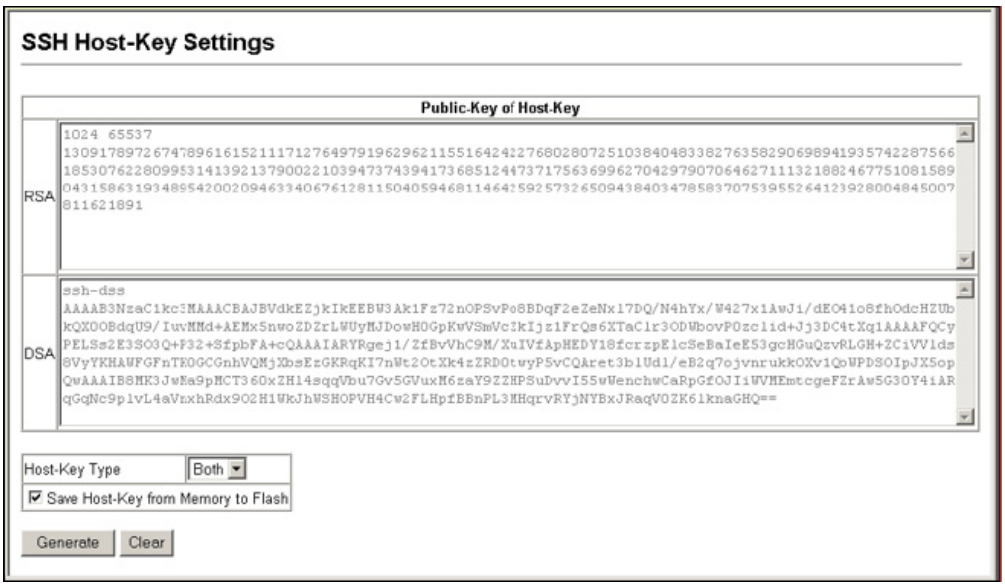
[注意] 本機は SSHv1.5 クライアントの RSA バージョン 1 と、SSHv2 の DSA バージョン 2 のみ使用します。

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。**



ユーザパブリックキーのインポート

ユーザの公開キーは、ユーザが公開キー認証メカニズムを使用してログインを行いことが可能になるために、スイッチへアップロードされる必要があります。
ユーザの公開キーがスイッチに存在しない場合、認証を完了するため、SSH は対話型のパスワード認証メカニズムに戻ります。

設定・表示項目

Public-Key of user

選択したユーザの RSA、DSA 公開キー

- 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。
- ー **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。

User Name

ドロップ - ダウンボックスで、管理したい公開キーのユーザを選択します。
（P73 「ユーザアカウントの設定」を参照してください）

Public-Key Type

ドロップ - ダウンボックスで、アップロードしたい公開キーを選択します。

- ー **RSA**: スイッチは SSH バージョン１、RSA の暗号化された公開キーを受け入れます。
- ー **DSA**: スイッチは SSH バージョン 2 の、DSA の暗号化された公開キーを受け入れます。

TFTP Server IP Address

TFTP サーバの IP アドレス（初期設定：0.0.0.0）

Source File Name

ソースファイル名

Copy Public Key

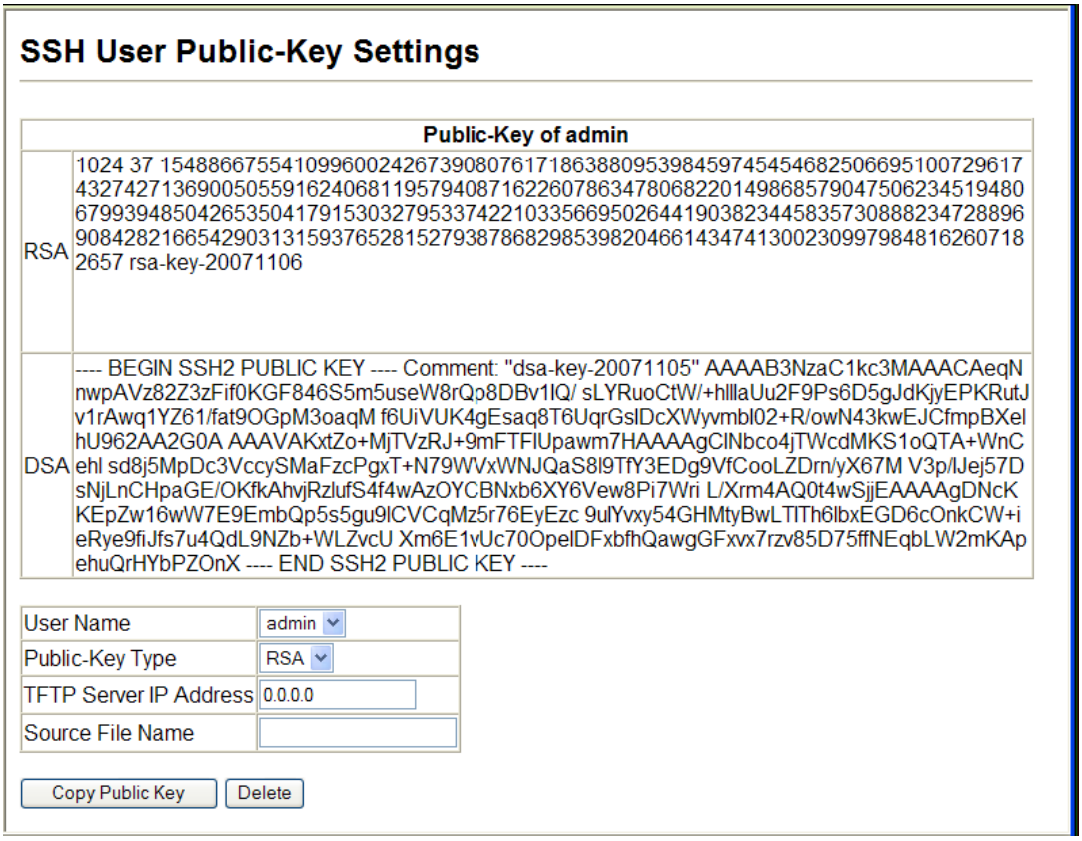
公開キーの TFTP 読み込みプロセスを開始します。
古い公開キーファイルを置き換える場合、スイッチからオリジナルキーを削除する必要はありません。

Delete

既にスイッチにインポートされている RSA または DSA 公開キーを選択し、削除します。

設定方法

[Security] → [SSH] → [SSH User Public-key Settings] をクリックします。それぞれのドロップ - ダウンボックスから、User name と公開キータイプを選択し、TFTP サーバ IP アドレスと公開キーのソースファイル名を入力します。最後に [Copy Public Key] をクリックします。



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）

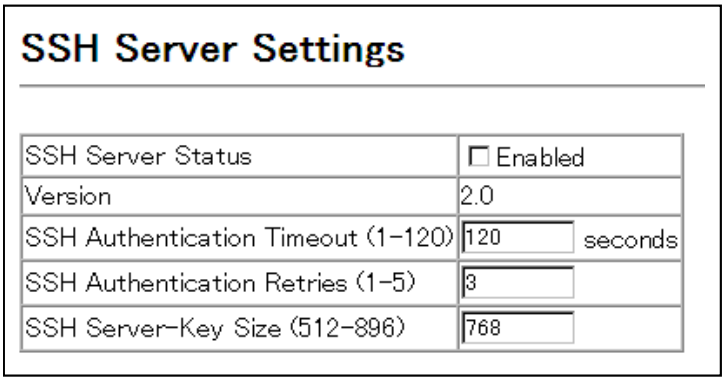
SSH Server-Key Size

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

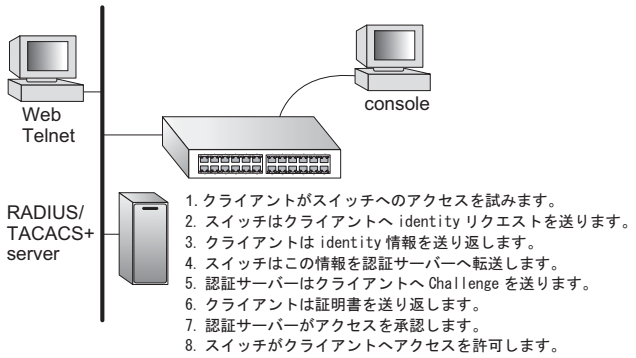
[Security] → [SSH] → [Settings] をクリックします。SSH を有効にし、必要に応じて各項目の設定を行い、[Apply] をクリックします。SSH サーバを有効にする際は、事前に SSH Host-Key Settings page で host key pair を生成する必要があります。



3.6.7 802.1x 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

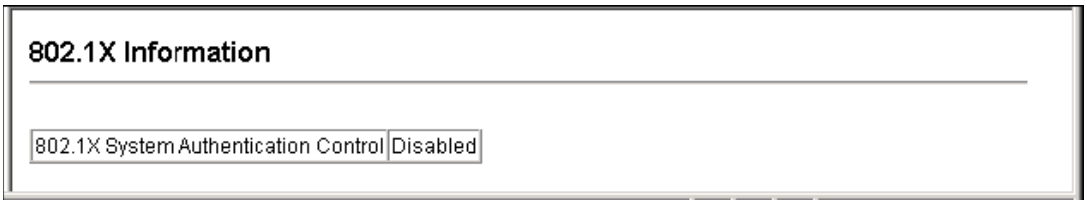
802.1X プロトコルはクライアントの認証を可能にします。

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。

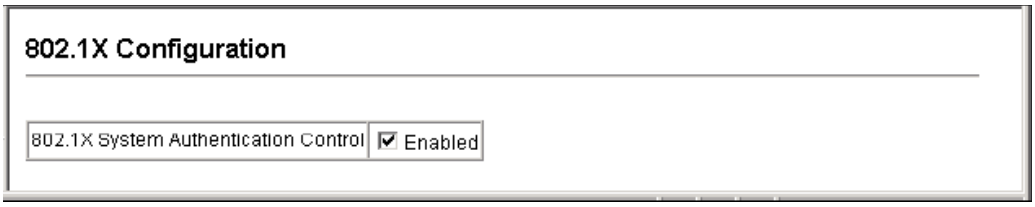
設定・表示項目

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-authentication

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-Request

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-authentication 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）**

Intrusion Action

- **Block Traffic ― 全ての非** EAP **トラフィックをブロックします（初期設定）**
- **Guest VLAN ― ポートの全トラフィックははゲスト** VLAN **にアサインされます。**
  （P198 **「**VLAN **の作成」、**P116 **「**MAC **認証の設定（ポート）」を参照してください）**

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	Instrusion Action	Authorized	Supplicant	Trunk
1	Disabled	Single-Host	5	Force-Authorized	Enable	2	60	3600	30	Block Traffic		00-00-00-00-00-00	
2	Disabled	Single-Host	5	Force-Authorized	Enable	2	60	3600	30	Block Traffic		00-00-00-00-00-00	
3	Disabled	Single-Host	5	Force-Authorized	Enable	2	60	3600	30	Block Traffic		00-00-00-00-00-00	
4	Disabled	Single-Host	5	Force-Authorized	Enable	2	60	3600	30	Block Traffic		00-00-00-00-00-00	
5	Disabled	Single-Host	5	Force-Authorized	Enable	2	60	3600	30	Block Traffic		00-00-00-00-00-00	
6	Disabled	Single-Host	5	Force-Authorized	Enable	2	60	3600	30	Block Traffic		00-00-00-00-00-00	

IEEE802.1x 統計情報の表示

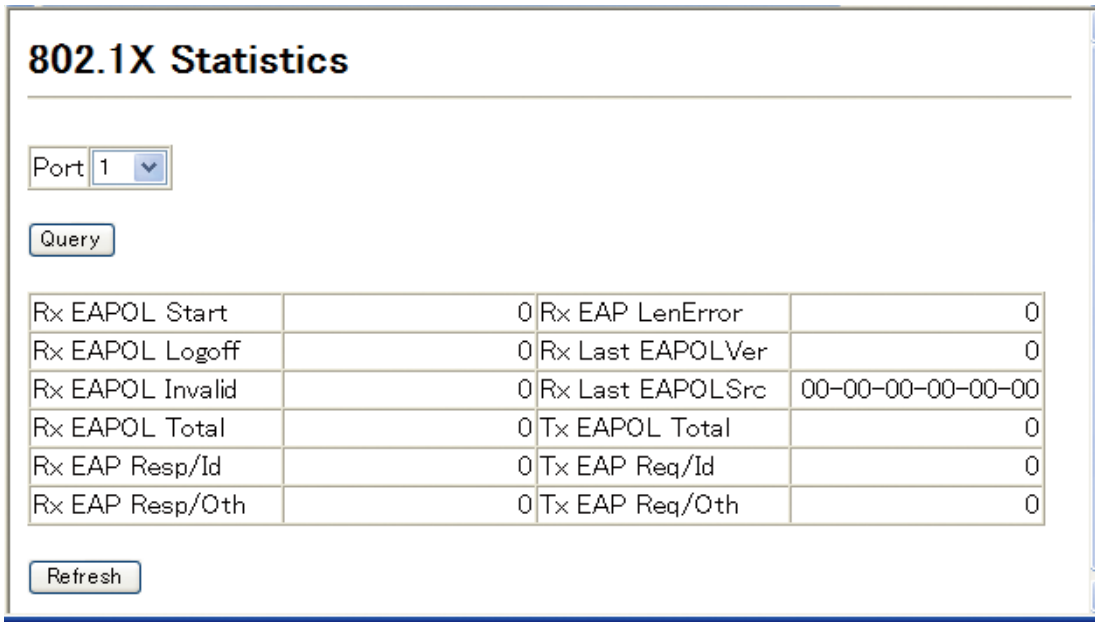
dot1x プロトコルの各ポートの統計情報を表示します。

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。



3.6.8 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 アドレスまたは 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

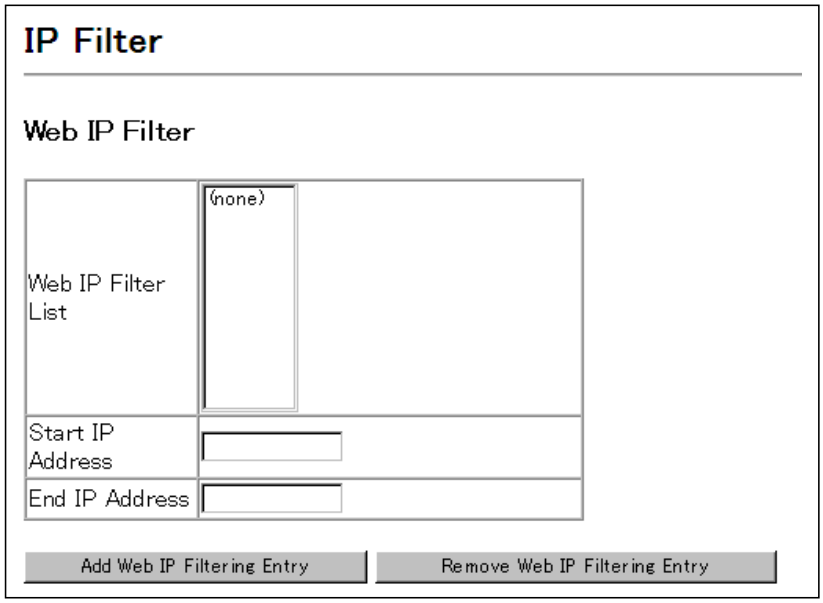
IP アドレスを範囲で指定している場合の最後の IP アドレス

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 セキュリティ

本機は、それぞれのデータポートに接続されたクライアントのトラフィックの分離および、認証されたクライアントだけがアクセスを得ることを保証するための多数のメソッドをサポートします。
プライベート VLAN と IEEE802.1x を利用したポートベース認証は、一般的にこれらの目的のために使用されます。これらのメソッドに加え、その他いくつかの提供されているセキュリティのオプションもサポートされています。

[注意] フィルタリングコマンドの実行プライオリティは、ポートセキュリティ、ポート認証、ネットワークアクセス、Web 認証、アクセスコントロールリスト、IP ソースガード、DHCP スヌーピングです。

3.7.1 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て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。P171 「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。
  － LACP または静的トランクポートに設定できません。
  －ハブ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、P149 「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

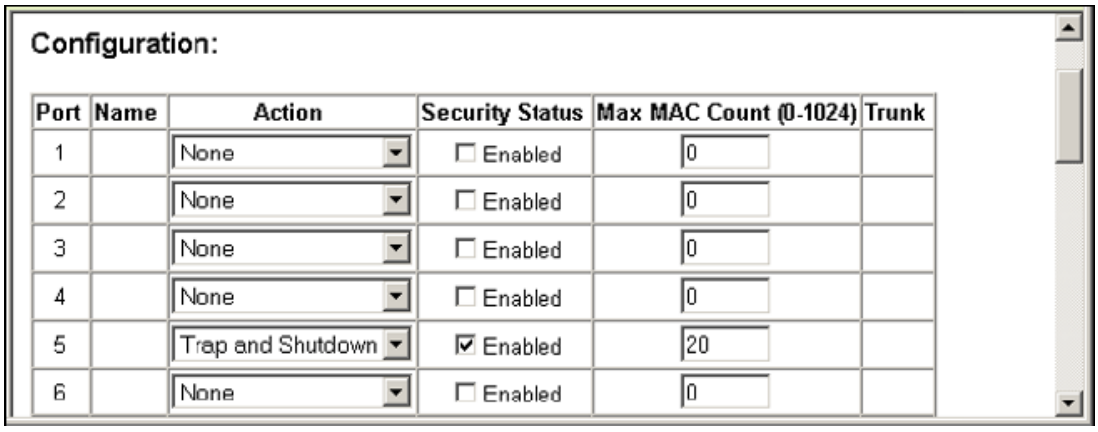
ポートが学習可能な MAC **アドレス数（設定範囲：**0-1024、0 **は無効）**

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。**



3.7.2 Web 認証

Web 認証は、802.1x やネットワークアクセス認証が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 認証機能は 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] RADIUS 認証は適切に機能させるために、アクティベートし Web 認証のために適切に構成しなくてはいけません。（P75 「ローカル / リモート認証ログオン設定」を参照）

[注意] Web 認証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 認証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 認証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

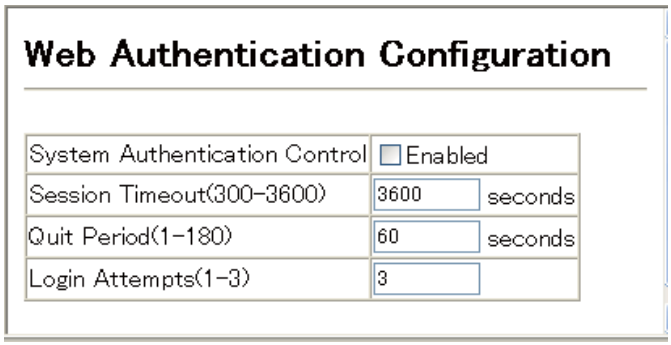
ホストがログインの試行回数の上限を超えた後、再び認証ができるまでに待機する時間を設定します（範囲：1 － 180 秒　初期設定：60 秒）

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 認証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

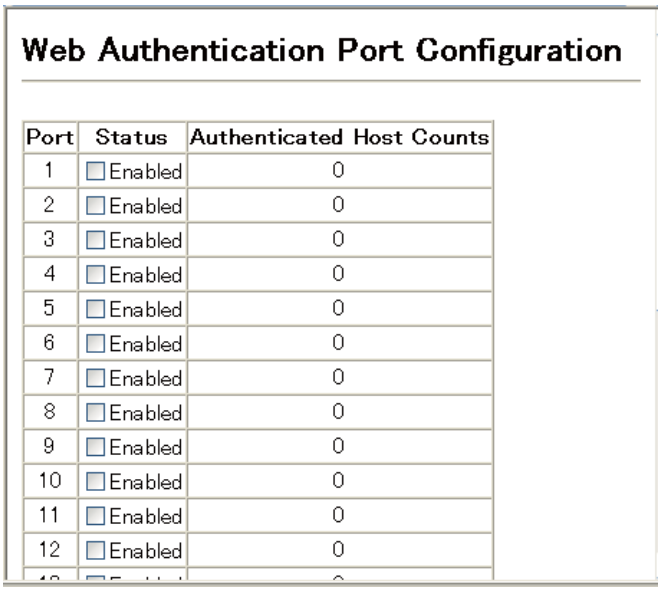
ポートの Web Authentication の状態を設定します。

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

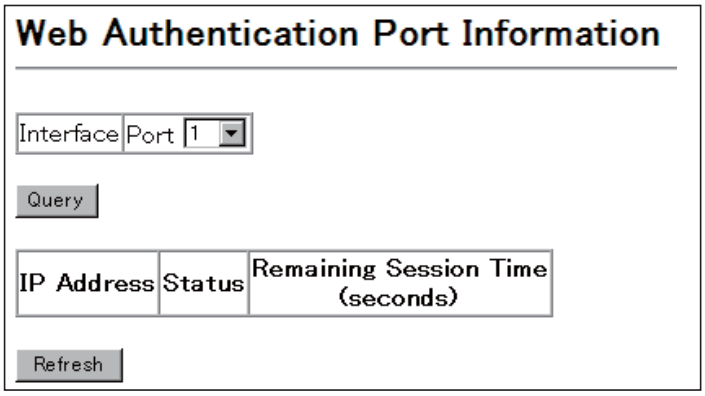
接続されたホストの認証状態を表示します。

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

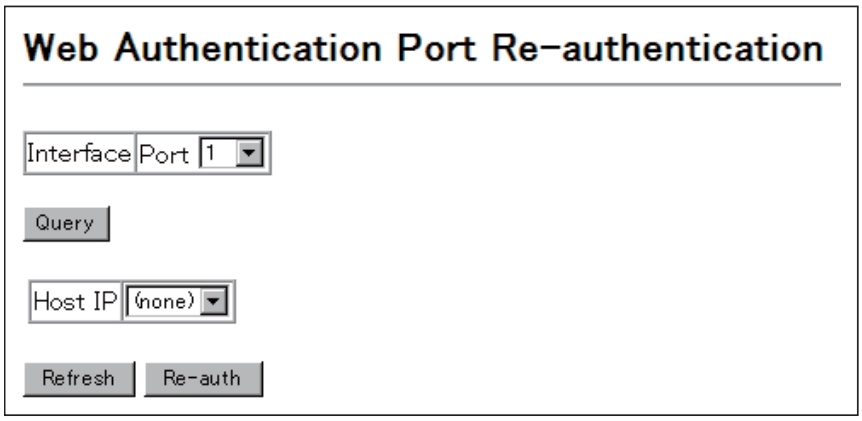
問い合わせるイーサネットのポートを表示します。

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。



3.7.3 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] RADIUS 認証は適切に機能させるために、アクティベートし Web 認証のために適切に構成しなくてはいけません。（P75 「ローカル / リモート認証ログオン設定」を参照）

[注意] Web 認証はトランクポート上で設定することはできません。

機能解説

- 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）で設定してください。

- 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。

- 設定された静的 MAC アドレスがスイッチポートで見られた時、セキュアアドレステーブルに追加されます。
  静的アドレスは RADIUS サーバへのリクエスト送信無しで認証済みとして取り扱われます。

- ポートステータスがダウンへ変更した際、全ての MAC アドレスはセキュアアドレスからクリアされます。静的 VLAN 割り当ては保存されません。

- 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。

- RADIUS サーバはオプションとして、認証されたユーザのために、スイッチポートに適用された動的 QoS 割り当てを返します。"Filter ID" 属性は、以下の QoS 情報を渡すよう RADIUS サーバに設定することができます。

表 3-1 動的 QoS プロファイル

プロファイル	属性文法	例
DiffServ	service-policy-in=policy-map-name	service-policy-in=p1
Rate Limit	rate-limit-input=rate	rate-limit-input=100 (in units of Kbps)
802.1p	switchport-priority-default=value	switchport-priority-default=2

- 複数のプロフィールはセミコロンでぞれぞれを区切ることにより、Filter-ID 属性で指定することができます。
  例えば、属性 " service-policy-in=pp1;rate-limit-input=100 "は "diffserv profile name is pp1, "と "ingress rate limit profile value is 100 kbps" を指定しています。

- 重複したプロフィールが Filter-ID 属性でパスする際、最初のプロフィールのみ使用されます。例えば、もし属性が " service-policy-in=p1;service-policy-in=p2 " の場合、スイッチは "DiffServ profile p1." のみ適用します。

- Filter-ID 属性の未サポートプロフィールは無視されます。
  例えば属性が " map-ip-dscp=2:3;service-policy-in=p1, "の場合、スイッチは " map-ip-dscp "を無視します。

- 認証成功時、動的 QoS 情報は以下のうちいずれかの状態により、RADIUS サーバからパスされないことがあります。
  - Filter-ID 属性ユーザプロフィールに見つけられない。
  - Filter-ID 属性がブランク。
  - 動的 QoS 割り当ての Filter-ID 属性フォーマットが認識不可
    （Filter-ID 属性全体を認識不可）

- 以下の状態が起きた時、動的 QoS 割り当てが失敗し認証結果が成功から失敗へ変更されます。
  - プロフィール値にイリーガル文字を発見
    （例：802.1p プロフィール値の非デジタル文字）
  - 認証ポートで受信されるプロフィール設定の失敗

- 動的 QoS にアサインする、最後のユーザがポートからログオフした時、スイッチはオリジナル QoS 設定をポートへリストアします。

- ユーザが、既に同じポートへログオンしているユーザと異なる動的 QoS プロフィールでネットワークへのログインを試みた時、このユーザはアクセスを拒否されます。

- ポートが割り当てられた QoS プロフィールを持つ間、手動 QoS 設定は、全てのユーザがポートからログオフした後にのみ効力を発します。

[注意]　動的 QoS の全ての設定変更はスイッチ設定ファイルに保存されません。

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

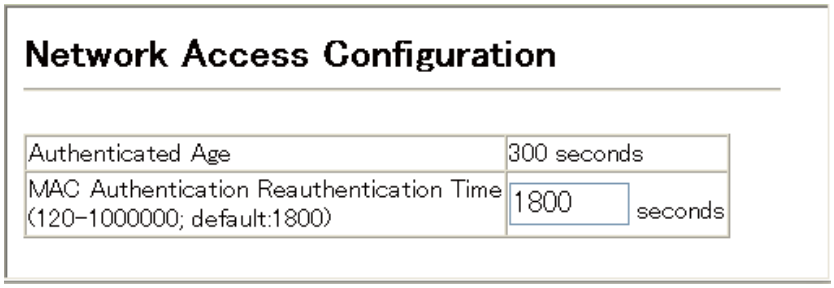
保護された MAC アドレステーブルのエージングタイムです。このパラメータはスイッチの MAC アドレステーブルの値と同じで、エージングタイム設定の画面で設定できます（初期設定：300 秒）

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。（初期設定：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）

MAC Filter ID

MAC アドレスまたは MAC アドレス範囲が、選択された MAC フィルタで指定されたポートで認証を免除されます。（詳細は P120 「MAC フィルタ」を参照してください）

（範囲：1 － 64　初期設定：なし）

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、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）

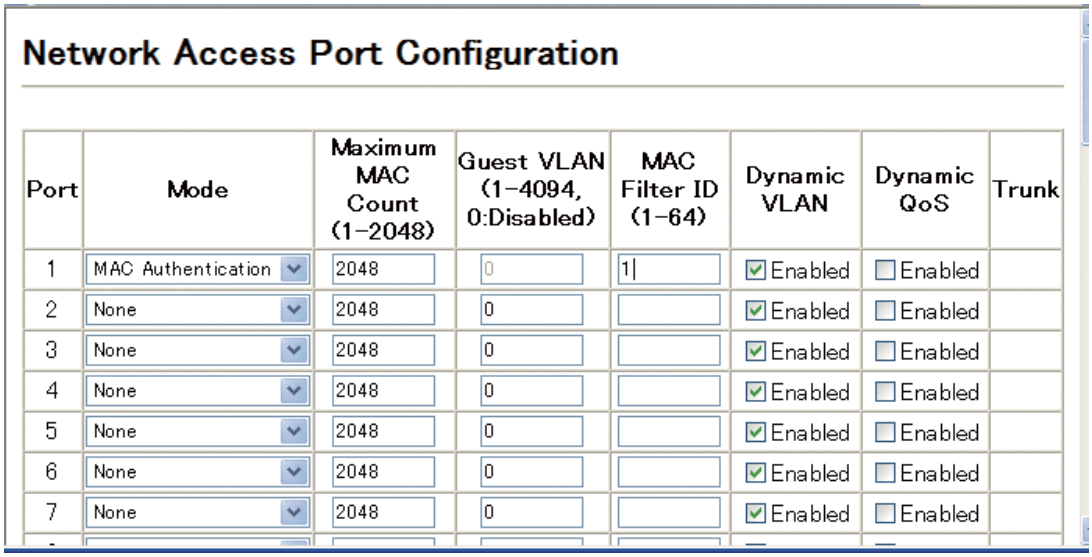
Dynamic QoS

認証ポートでの、動的 QoS 機能の有効 / 無効（初期設定：無効）

[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。



Network Access Port Configuration

Port	Mode	Maximum MAC Count (1-2048)	Guest VLAN (1-4094, 0:Disabled)	MAC Filter ID (1-64)	Dynamic VLAN	Dynamic QoS	Trunk
1	MAC Authentication	2048	0	1	Enabled	Enabled	
2	None	2048	0		Enabled	Enabled	
3	None	2048	0		Enabled	Enabled	
4	None	2048	0		Enabled	Enabled	
5	None	2048	0		Enabled	Enabled	
6	None	2048	0		Enabled	Enabled	
7	None	2048	0		Enabled	Enabled	

ポートリンク検出

ポートリンク検出機能はリンクイベント発生時に、SNMP トラップの送信とポートのシャットダウン（どちらかあるいは両方）を実行します。

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

Port

設定をおこなうポートを指定。

Status

ポートでリンク検出を有効 / 無効に設定

Condition

ポートアクションを引き起こすリンクイベントタイプ

Link Up

リンクアップイベントのみポートアクションを発生

Link Down

リンクダウンイベントのみポートアクションを発生

Link Up and Down

全てのリンクアップ・ダウンイベントでポートアクションを発生

Action

本機は以下の 3 通りの方法でリンクアップ・ダウンイベントに対応することが可能です。

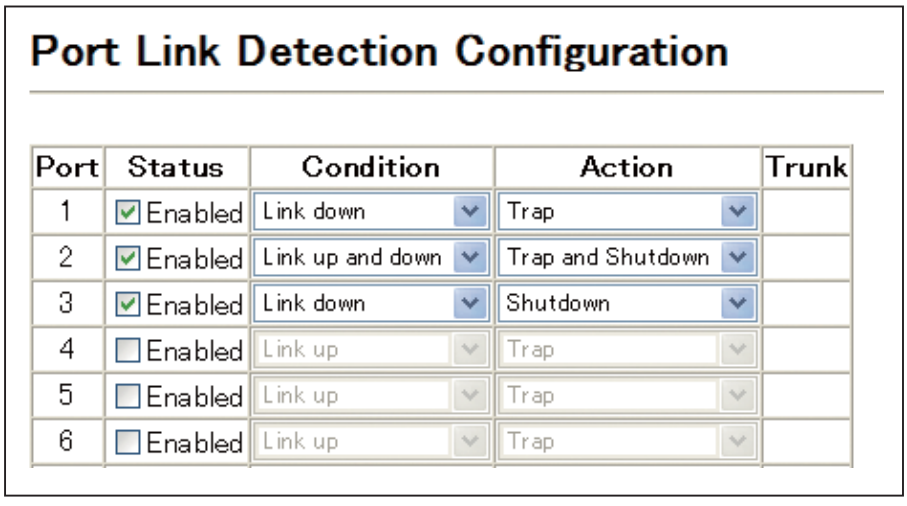
- Trap ー SNMP トラップを送信。
- Trap and Shutdown ー SNMP トラップを送信し、ポートをシャットダウンします。
- Shutdown ーポートをシャットダウン。

Trunk

ポートがトランクメンバであることを示します。

設定方法

[Security] → [Network Access] → [Port Link Detection Configuration] をクリックします。
"Status"、"Condition"、"Action" を設定し [Apply] 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

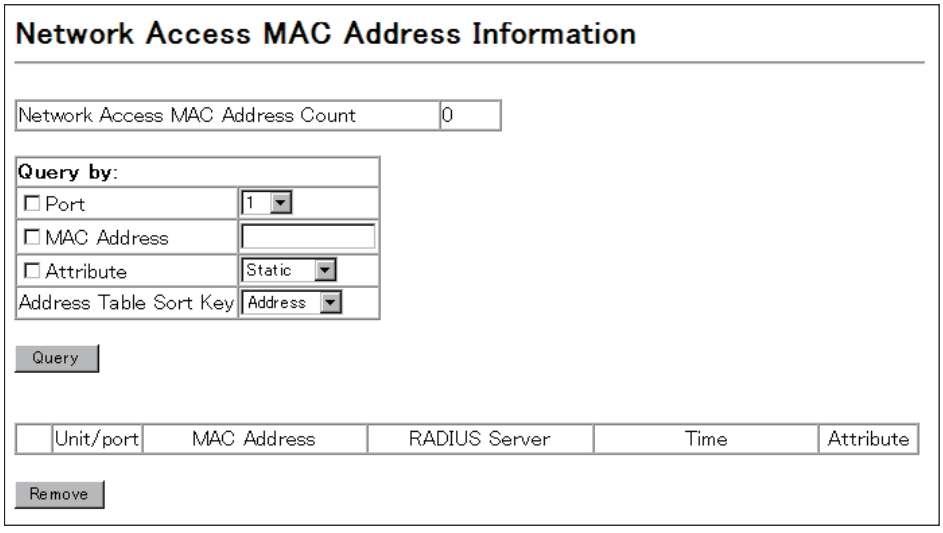
MAC アドレスがスタティックかダイナミックかを表示

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。



MAC フィルタ

それぞれのポートの MAC **認証は、独立して設定されます。**
MAC **認証ポート設定ページでは、それぞれのポートで指定する** MAC **認証の最大数と、侵入時のアクションを設定します。**

設定・表示項目

Port

設定をおこなうポートを指定します。

Status

ポートで、MAC **認証が有効か無効かを表示します。詳細は** P116 **「**MAC **認証の設定（ポート）」を参照してください。**
パラメータが無効である場合、以下のパラメータは使用できません。

Max MAC Count

認証された MAC **アドレスの合計最大数（範囲：**1-1024　**初期設定：**1024）

Intrusion Action

本機は以下の 2 **つの方法で侵入に対処が可能です。**

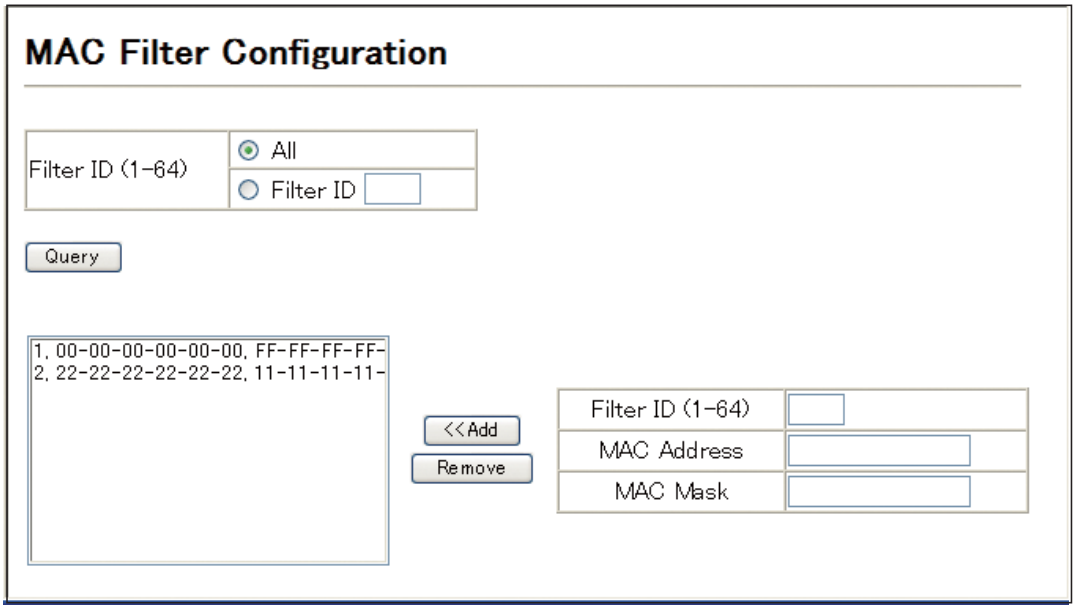
- Block Traffic― **認証されなかったホストの、全てのトラフィックをブロックします。**
- Pass Traffic ― **認証されなかったホストの、全てのトラフィックを許可します。**

Trunk

ポートがトランクのメンバーである場合表示します。

設定方法

[Security] → [MAC Authentication] **をクリックします。**



3.7.4 ACL （Access Control Lists）

Access Control Lists (ACL) は IPv4 フレーム（IP アドレス、プロトコル、レイヤ 4 プロトコルポート番号、TCP コントロールコード）およびその他のフレーム（MAC アドレス、イーサネットタイプ）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。

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、アクセスを許可 (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破棄します。リスト上の許可ルールに一致しない場合、パケットは破棄され、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。

- 最大 ACL 設定数は 64 個です。
- システムごとに設定できるルールは、混合スモードで 1024 ルールまたは拡張モードで 500 ルールです。
- 各 ACL は最大 64 ルールまで設定可能ですが、リソース制限により、ポートにバウンドされたルールの平均は 20 以上にはできません

[注意] CLI は、拡張ルールだけにアクセスリストを制限するか、標準と拡張両方のルールに許可されるコントロール機能を含みます。この機能の詳細は 519 ページの「access-list rule-mode」を参照をしてください。

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

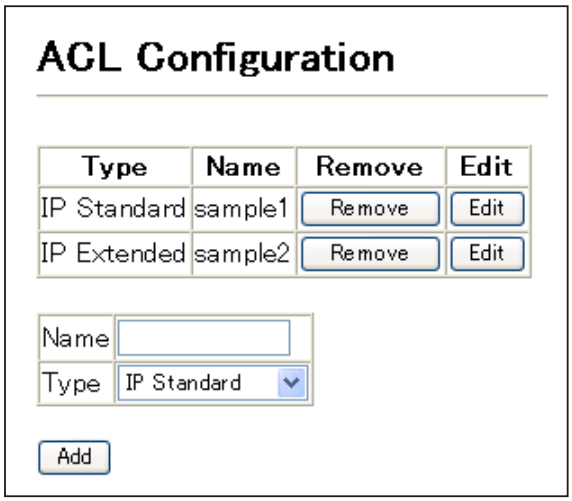
ACL 名（15 文字以内）

Type

- **IP Standard** ― ソース IPv4 アドレスに基づくパケットフィルタリングを行います。
- **IP Extended** ― ソース又はディスティネーション IPv4 アドレス、プロトコルタイプ、プロトコルポート番号、TCP コントロールコードに基づくフィルタリングを行ないます。
- **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。
- **ARP** ― ARP インスペクション（詳細は 131 ページの「ARP インスペクション」を参照）を使用した静的 IP-to-MAC アドレスバインディングを指定します。

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,ARP)。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

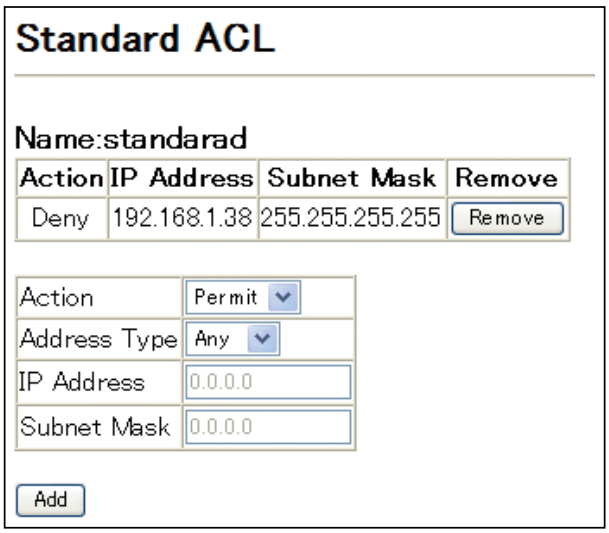
ソース IP アドレス

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）
- **TOS** ― ToS（Type of Service）レベル（範囲：0-15）
- **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 /Destination Port

プロトコルタイプに応じたソース / ディスティネーションポート番号（範囲：0-65535）

Source/Destination Port Bitmask

一致するポートビットを表す 10 進数（範囲：0-65535）

Control Code

TCP ヘッダのバイト 14 内のフラグ・ビットを指定（範囲 :0-63）

Control Code Bit Mask

一致するコードビットの値

※コントロールビットマスクは、コントロールコードに使用される 10 進数の値です。10 進数の値を入力し、等価な 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。

以下のビットが指定されます。

- 1 (fin) ― Finish
- 2 (syn) ― Synchronize
- 4 (rst) ― Reset
- 8 (psh) ― Push
- 16 (ack) ― Acknowledgement
- 32 (urg) ― Urgent pointer

例えば、コード値及びコードマスクを利用し、パケットをつかむには以下のフラグをセットします。

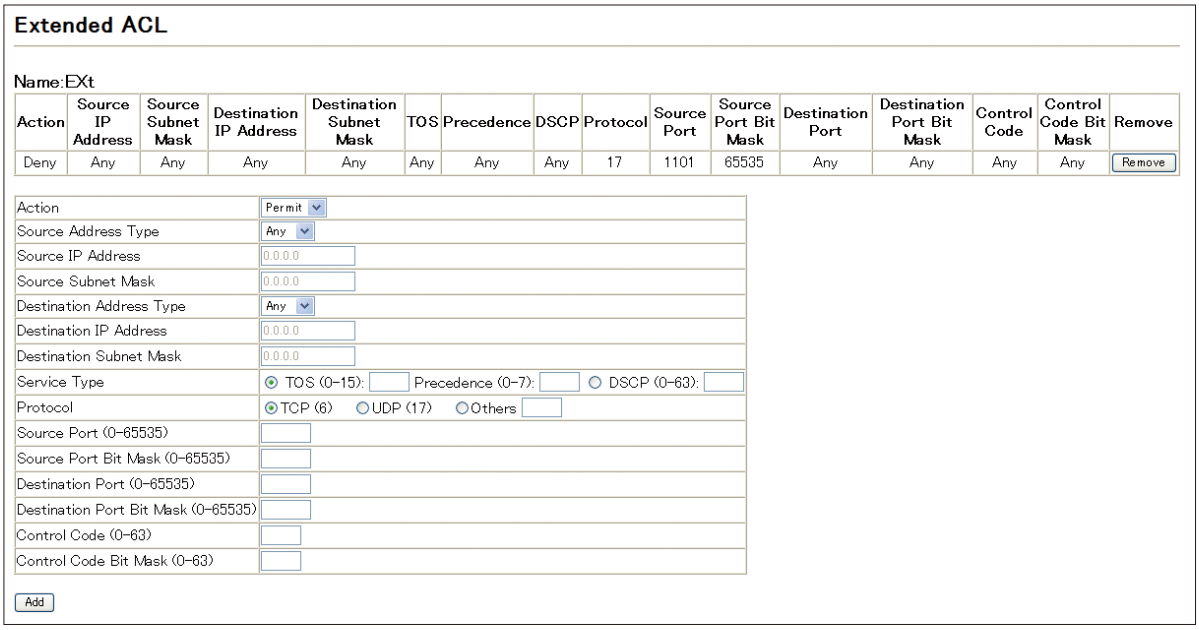
－有効な SYN flag ― コントロールコード：2、コントロールビットマスク：2

－有効な SYN 及び ACK ― コントロールコード：18、コントロールビットマスク：18

－有効な SYN 及び無効な ACK ― コントロールコード：2、コントロールビットマスク：18

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

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を基にした ACL の設定をおこないます。

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 Address Type

"Any" を使用した場合、全ての可能なアドレスを含み、"Host" を指定した場合はアドレスフィールドにホストアドレスを入れます。”MAC” を指定した場合、アドレスとビットマスクフィールドへアドレス範囲を入力します。（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 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）

VID Mask

VLAN ビットマスク（範囲：1-4095）

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。

Ethernet Type Bitmask

プロトコルビットマスク（範囲：600-fff hex）

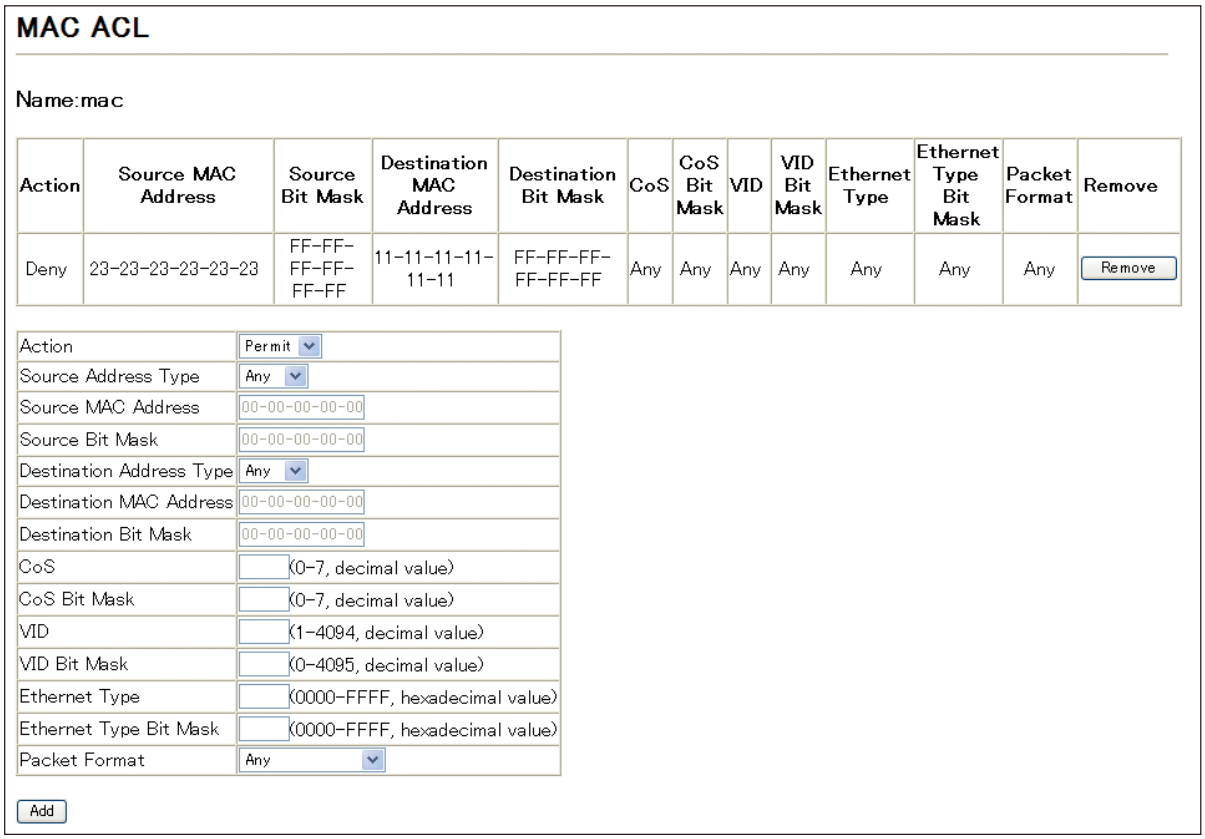
Packet Format

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
- Untagged-eth2 ― タグなしイーサネット II パケット
- Untagged-802.3 ―タグなしイーサネット IEEE802.3 パケット
- Tagged-eth2 ― タグ付イーサネット II パケット
- Tagged-802.3 ― タグ付イーサネット IEEE802.3 パケット

設定方法

（permit/deny の）動作を指定します。ソースまた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。
その他必要な項目を入力後 [Add] をクリックしてください。



ARP ACL の設定

ARP メッセージアドレスをベースにした ACL の設定をおこないます。
ARP インスペクションはこれらの ACL を、疑わしいトラフィックのフィルタを行う為に使用することが出来ます。（詳細は 131 ページの「ARP インスペクション」を参照してください）

設定・表示項目

Action

ACL はどのような許可または拒否ルールの組合せも含むことができます。

Packet Type

ARP リクエスト、ARP レスポンス、イーサタイプを指定します。（範囲：Request、Response、All　初期設定：Request）

Sender/Target IP Address Type

ソースまたはディスティネーション IP v 4 アドレスを指定します。îAnyî を使用することで、全ての可能なアドレスを含み、îHostî はアドレスフィールドに特定のホストアドレスを指定します。îIPî はアドレスとマスクフィールドへアドレスの範囲を指定します。（範囲：Any、Host、IP　初期設定：Any）

Sender/Target IP Address

ソースまたはディスティネーション IP アドレス

Sender/Target IP Address Mask

ソースまたはディスティネーションアドレスのサブネットマスク

Sender/Target MAC Address Type

ソースまたはディスティネーション IP v 4 アドレスを指定します。"Any" を使用することで、全ての可能なアドレスを含み、"Host" はアドレスフィールドに特定のホストアドレスを指定します。"MAC" はアドレスとマスクフィールドへアドレスの範囲を指定します。（範囲：Any、Host、IP　初期設定：Any）

Sender/Target MAC Address

ソースまたはディスティネーション MAC アドレス

Sender/Target MAC Address Mask

ソースまたはディスティネーション MAC アドレスの 16 進数マスク。

Log

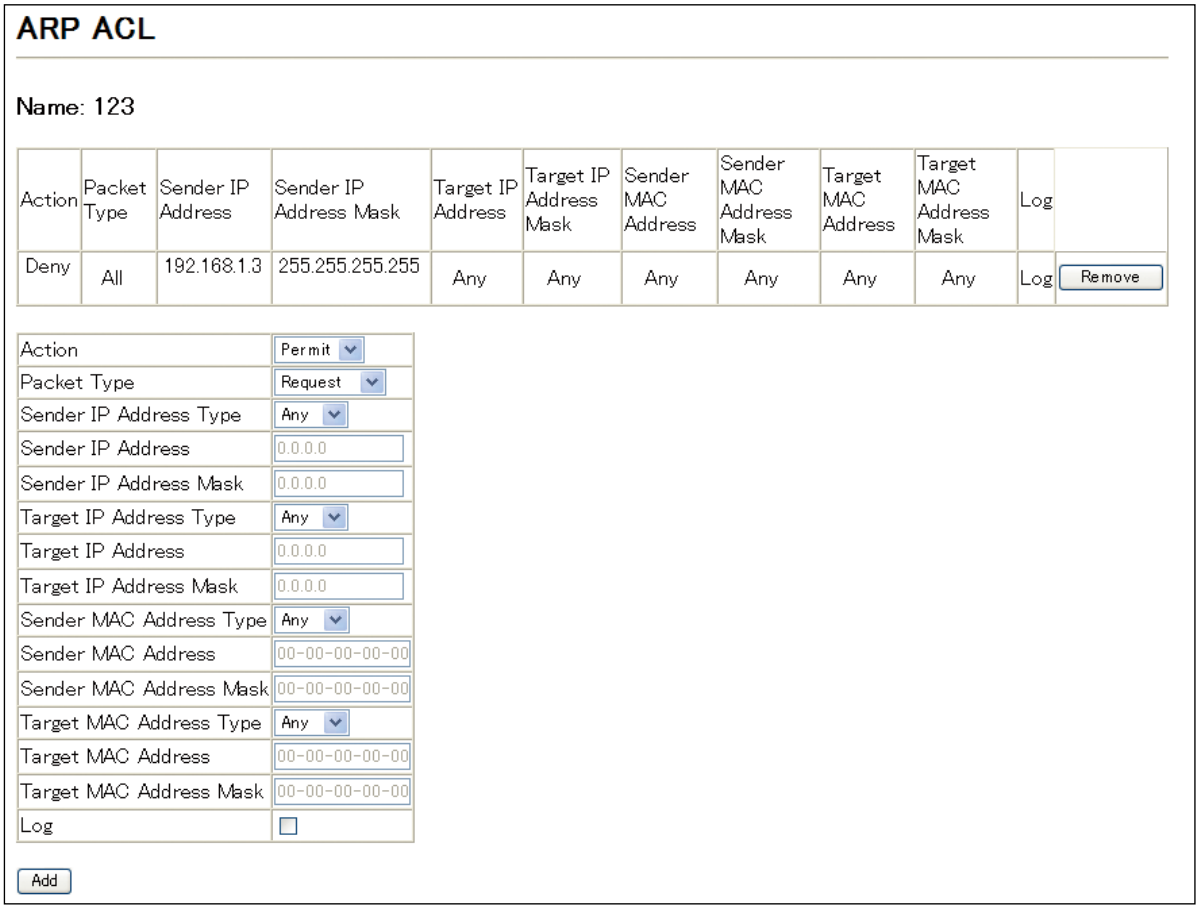
アクセスコントロールエントリに一致したパケットのログ。

機能解説

- ACL は最大 32 ルールを設定できます。
- 新しいルールはリストの最後に追加されます。

設定方法

（permit/deny の）動作を指定します。パケットタイプ、アドレスタイプ（Any、Host、MAC）、ソースまたはディスティネーションアドレスを指定します。"Host" を選択した場合、特定のアドレスを入力します。"IP" または "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。その他必要な項目を入力後 [Add] をクリックしてください。



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。1 つの IP アクセスリストと MAC アクセスリストをポートに割り当てることができます。

機能解説

- それぞれの ACL は最大 64 ルールを設定することができます。
- 本機は入力フィルタの ACL のみサポートしています。
- 入力フィルタリングを行うポートに、1 つの ACL のみをバインドすることができます。

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：1-52）

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

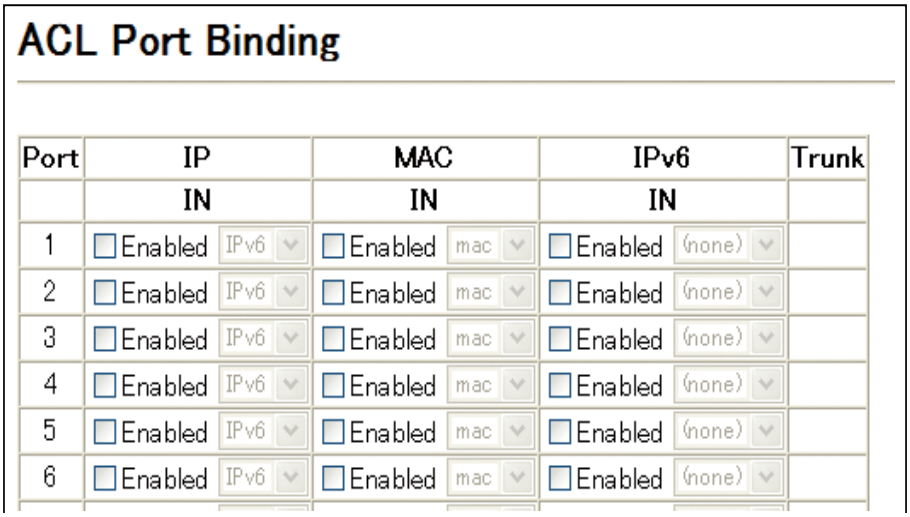
入力 (ingress) パケットに対する ACL

Trunk

ポートがトランクメンバであるか否かを示します。トランクの作成とポートメンバの選択は " トランクグループの作成 "PXX を参照してください。

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。



3.7.5 ARP インスペクション

ARP インスペクションは、Address Resolution packet（ARP）プロトコルのため、MAC アドレスバインディングの妥当性の検査を行うセキュリティ機能です。
この機能により、ある種の man-in-the-middle 攻撃等からネットワークを保護できます。
これはローカル ARP キャッシュがアップデートされるか、またはパケットが適切な目的地に転送される前に、全ての ARP リクエストを途中で捕らえ、これらのパケットのそれぞれを照合することによって達成されます。無効な ARP パケットは破棄されます。
ARP インスペクションは、信頼できるデータベースに保存された正当な IP-to-MAC アドレスバインディングに基づいて ARP パケットの正当性を決定します。（137 ページの「DHCP スヌーピング」を参照）
このデータベースは、それがスイッチと VLAN で有効になっている時に DHCP スヌーピングによって構築されます。
また、ARP インスペクションはユーザで設定された ARP アクセスコントロールリスト（ACL）に対して、ARP パケットの妥当性を確認することも可能です。（128 ページの「ARP ACL の設定」を参照）

ARP インスペクションの設定

ARP インスペクションは、スイッチ全体と VLAN ごとの両方で動作し、インスペクションパラメータはそれぞれの VLAN で設定します。
Trusted ポートの設定、Logging と同様、これらの機能は、ARP Inspection Configuration ページで提供されます。
ARP インスペクション ACL の設定は、ここで動作させる前に ARP ACL ページで行います。

機能解説

ARP インスペクションの有効・無効

- ARP インスペクションはスイッチ全体および VLAN ベースでコントロールされます。
- 初期設定では ARP インスペクションはスイッチで無効になっています。
- 初期設定では ARP インスペクションは全ての VLAN で無効になっています。
  - ー ARP インスペクションがグローバルで有効の場合、有効になっている VLAN 上でのみアクティブになります。
  - ー ARP インスペクションがグローバルで有効の場合、インスペクションが有効な VLAN の全ての ARP リクエストとリプライパケットは CPU へリダイレクトし、それらのスイッチング行為は ARP インスペクションエンジンによって処理されます。
  - ー ARP インスペクションがグローバルで無効の場合、有効になっている物も含め全ての VLAN で非アクティブになります。
  - ー ARP インスペクションが無効の場合、全ての ARP リクエストとリプライパケットは ARP インスペクションエンジンを回避し、それらのスイッチング行為はその他全てのパケットと同様になります。
  - ーグローバル ARP インスペクションの無効化とその後の再有効化は、VLAN の ARP インスペクション設定に影響を与えません。
  - ー ARP インスペクションがグローバルで無効の際、個々の VLAN の ARP インスペクション設定は可能です。グローバルで ARP インスペクションが再度有効になった時、これらの設定変更はアクティブになります。
- 現在のファームウェアバージョンの ARP インスペクションエンジンはトランクポートの ARP インスペクションをサポートしていません。

ARP インスペクション VLAN フィルタ（ACL）

- **初期設定で、**ARP **インスペクション** ACL **は設定されておらず、この機能は無効です。**
- ARP **インスペクション** ACL **は** ARP ACL Configuration **ページで設定されます。（**128 **ページの「**ARP ACL **の設定」を参照）**
- ARP **インスペクション** ACL **は設定されたどの** VLAN **にも適用することが可能です。**
- ARP **インスペクションは、正当な** IP-to-MAC **アドレスバインディングのリストのために、**DHCP **スヌーピングバインディングデータベースを使用します。**ARP ACL **は** DHCP **スヌーピングバインディングデータベースのエントリに優先されます。スイッチは最初に、指定された** ARP ACL **と** ARP **パケットを比較します。**
- "static **が指定された場合、**ARP **パケットは選択された** ACL **パケットがいずかのマッチングルールによってフィルタされることにたいしての、妥当性の検査のみ行われます。いずれのルールにもマッチングしないパケットは破棄され、**DHCP **スヌーピングバインディングデータベースチェックは回避されます。**
- "static **が指定されない場合、**ARP **パケットは最初に選択した** ACL **に対して妥当性を検査されます。**ACL **ルールとパケットが一致しない場合、**DHCP **スヌーピングバインディングデータベースはそれらの正当性を決定します。**

ARP インスペクション妥当性チェック

- **初期設定で、**ARP **インスペクション妥当性チェックは無効になっています。**
- **以下の妥当性検査の内、最低** 1 **つを指定することにより、**ARP **インスペクション妥当性チェックをグローバルで有効にすることが可能です。以下の項目のいずれも、同時にアクティブにすることができます。**

  − Destination MAC
  ARP **ボディのターゲット** MAC **アドレスにたいして、イーサネットヘッダの送信先** MAC **アドレスをチェックします。このチェックは** ARP **レスポンスのために実行されます。有効の際、異なる** MAC **アドレスを持つパケットは無効として分類され破棄されます。**

  − IP
  無効と予期せぬ IP **アドレスの** ARP **ボディをチェックします。これらのアドレスは** 0.0.0.0**、**255.255.255.255 **および全ての** IP **マルチキャストアドレスを含みます。センダー** IP **アドレスは全ての** ARP **リクエストとレスポンスでチェックされ、ターゲット** IP **アドレスは** ARP **レスポンスのみチェックされます。**

  − Source MAC
  ARP **ボディのセンダー** MAC **アドレスにたいし、イーサネットヘッダのソース** MAC **アドレスのチェックをおこないます。このチェックは** ARP **リクエストとレスポンス両方に実行されます。有効の際、異なる** MAC **アドレスを持つパケットは無効として分類され破棄されます。**

ARP インスペクションロギング

- **初期設定で、**ARP **インスペクションのロギングはアクティブになっており無効にはできません。**
- **管理者はログファシリティレートの設定をおこなえます。**
- **スイッチがパケットの破棄を行った時、スイッチはログバッファにエントリを置き、コントロールされたレートを基にシステムメッセージを生成します。システムメッセージが表示された後、エントリはログバッファからクリアされます。**
- **それぞれのログエントリは受信** VLAN**、ポート番号、ソース・ディスティネーション** IP **アドレス、ソース・ディスティネーション** MAC **アドレスの情報を含みます。**
- **複数、同一の不正な** ARP **パケットが同じ** VLAN **で連続して受信された場合、ロギングファシリティはログバッファの** 1 **つのエントリと、**1 **つの対応するシステムメッセージのみ生成します。**
- **ロギングバッファが一杯になると、最も古い項目から新しいエントリで置き換えられます。**

Trusted & Untrusted ポート

- 初期設定で全てのポートは Untrusted に設定されています。
- 指定したポートを Trusted または Untrusted に設定することができます。
- Trusted インタフェース上に到着しているパケットは全ての ARP インスペクションと ARP インスペクション妥当性の検査を回避し、常に転送が行われます。
  一方、Untrusted インタフェースは全ての設定されている ARP インスペクションテストを受けます。

・ARP パケットレート制限

- 初期設定で、全ての Untrusted ポートは ARP パケットレート制限を受けます。
- 初期設定で、全ての Trusted ポートは ARP パケットレート制限を免除されます。
- 本機は、設定された ARP-packets-per-second レート制限を越えてポートで受信された全ての ARP パケット破棄します。
- ARP インスペクションパケットレート制限を "none" に設定することは、レート制限が実施されないことを意味します。

設定・表示項目

ARP Inspection Status

ARP インスペクションをグローバルで有効にします。（初期設定：無効）

ARP Inspection VLAN

設定をおこなう VLAN を選択（初期設定：1）

ARP Inspection VLAN Status

選択した VLAN で ARP インスペクションを有効（初期設定：無効）

ARP Inspection VLAN Filter

- ー ARP ACL ー設定された ARP ACL の選択を許可
- ー Static ー ARP ACL が選択され、また static mode もまた選択されている時、本機は ARP インスペクションのみ実行し、DHCP スヌーピングバインディングデータベースの妥当性検査を回避します。ARP ACL が選択が選択され、static mode が選択されていない時、本機は最初に ARP インスペクションを実行し、次に DHCP スヌーピングバインディングデータベースにたいする妥当性検査を実行します。（初期設定：無効）

ARP Inspection Validation

以下のオプションの内いずれかが使用可能の場合、拡張 ARP インスペクション検査を有効にできます。

- ー Dst-MAC
  ARP レスポンスのボディ内のターゲット MAC アドレスに対し、イーサネットヘッダのディスティネーション MAC アドレスの妥当性検査をおこないます。
- ー IP
  不正および予期せぬ IP アドレスの ARP ボディをチェックします。
  センダー IP アドレスは全ての ARP リクエストとレスポンスをチェックされます。ターゲット IP アドレスは ARP レスポンスのみチェックされます。
- ー Src-MAC
  ARP ボディ内のセンダー MAC アドレスに対し、イーサネットヘッダのソース

MAC アドレスの妥当性検査をおこないます。このチェックは ARP リクエストとレスポンスの両方に実行されます。

ARP Inspection Log

ARP インスペクションロギングパラメータを設定します。

- Message Number
  ログメッセージに保存されるエントリの最大数 (範囲：0-256、初期設定：5)
- Interval
  ログメッセージが送信される間隔（範囲：0-86400 秒　初期設定：1 秒）

Port

ポート番号

Trust Status

ポートを Trusted または Untrusted に設定（初期設定：Untrusted）

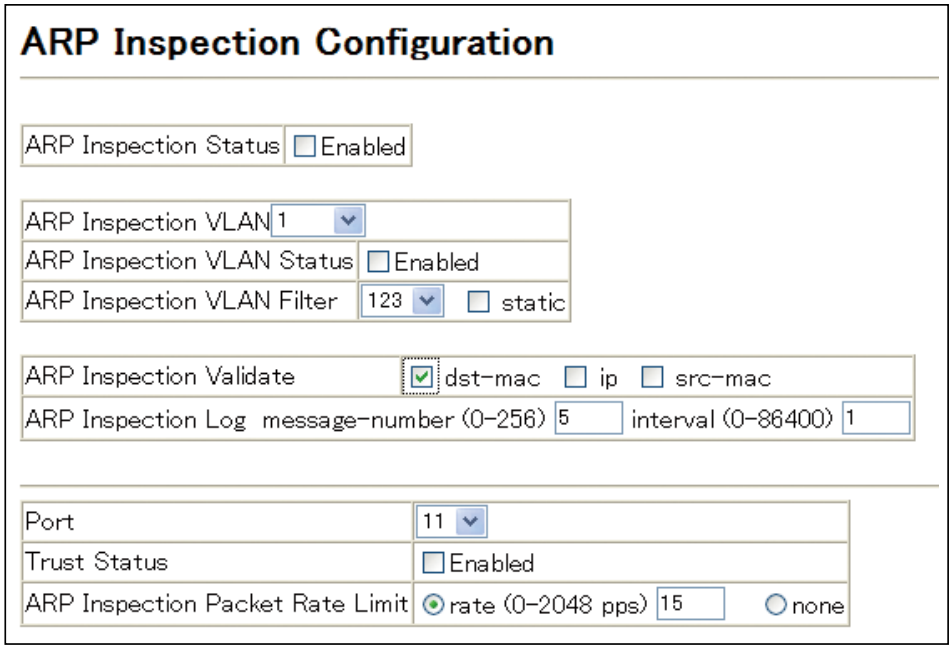
ARP Inspection Packet Rate Limit

Untrusted ポートで受信される ARP パケットのレート制限

- Rate ー毎秒 CPU によってい処理される ARP パケットの最大数(範囲:0-2048 初期設定：15)
- None ー CPU によって処理される ARP パケットの数に制限を設定しない

設定方法

[Security] → [ARP Inspection Configuration] をクリックします。
必要な項目を入力し、[Apply] をクリックします。



ARP インスペクションポート情報の表示

ARP インスペクションポート情報を表示します。
Trusted ポートのリスト、様々な理由で処理または破棄された ARP パケットの数に関する統計情報などが確認できます。

設定・表示項目

ARP Inspection Status

ARP インスペクションをグローバルで有効にします。（初期設定：無効）

Trusted Port List

Trusted に設定された全てのポートを表示します。

ARP Inspection Statistics Information

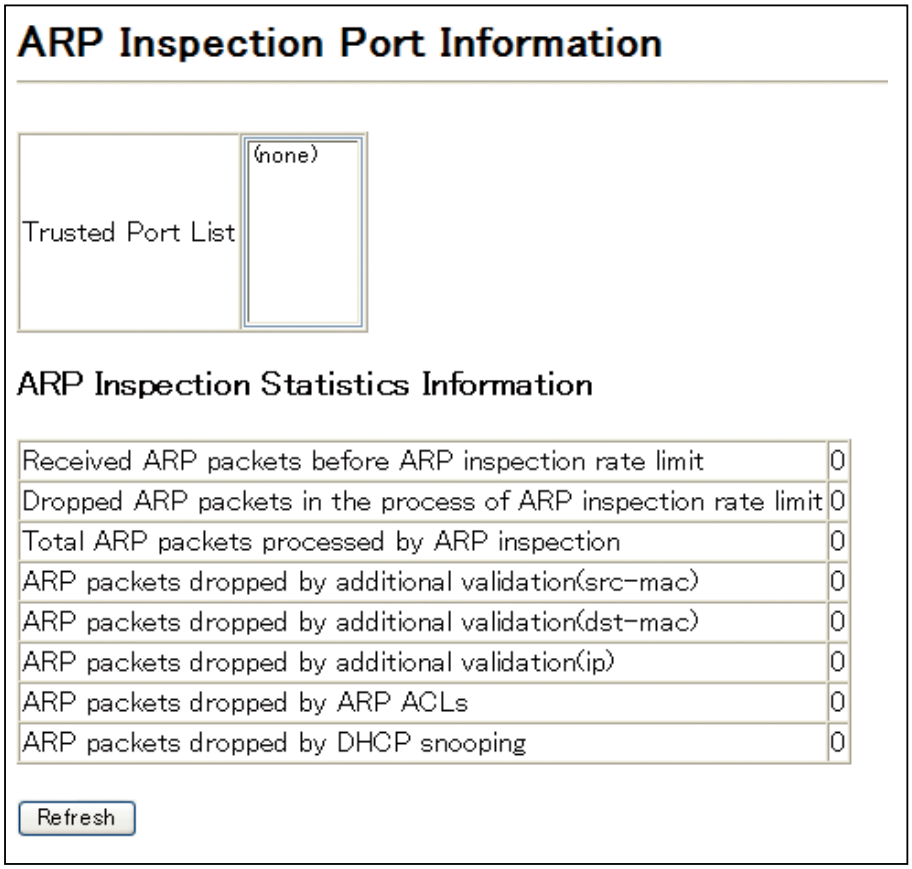
- Received ARP packets before ARP inspection rate limit
  ARP インスペクションレート制限を越えない受信 ARP パケットの数
- Dropped ARP packets in the process of ARP inspection rate limit
  ARP レート制限を越えた（破棄された）ARP パケットの数
- Total ARP packets processed by ARP inspection
  ARP インスペクションエンジンに処理された全ての ARP パケット数
- ARP packets dropped by additional validation (Src-MAC)
  ソース MAC アドレステストに落ちたパケット数
- ARP packets dropped by additional validation (Dst-MAC)
  ディスティネーション MAC アドレステストに落ちたパケット数
- ARP packets dropped by additional validation (IP)
  IP アドレステストに落ちた ARP パケット数
- ARP packets dropped by ARP ACLs
  ARP ACL ルールに対する妥当性検査に落ちた ARP パケットの数
- ARP packets dropped by DHCP snooping
  DHCP スヌーピングバインディングデータベースに対する妥当性検査に落ちたパケット数

Refresh

全てのカウンタと Trusted ポート情報をアップデート

設定方法

[Security] → [ARP Inspection Information] をクリックします。



3.7.6 DHCP スヌーピング

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。

機能解説

- 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 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。

- テーブルエントリは Trusted インタフェースのためにのみ学習されます。
  クライアントが DHCP サーバから IP アドレスを受信またはリリースした時、エントリを DHCP スヌーピングテーブルへ動的に追加または削除します。
  それぞれのエントリは MAC アドレス、IP アドレス、リースタイム、VLAN 識別情報、ポート識別情報を含みます。

- 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。

- DHCP Snooping が無効の場合、DHCP パケットは転送される。

- DHCP 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。

- DHCP 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。

  - 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。
  - 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。
  - 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。
  - 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。

DHCP スヌーピング設定

DHCP スヌーピングをグローバルで有効 / 無効、または MAC アドレス検証の設定を行います。

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。

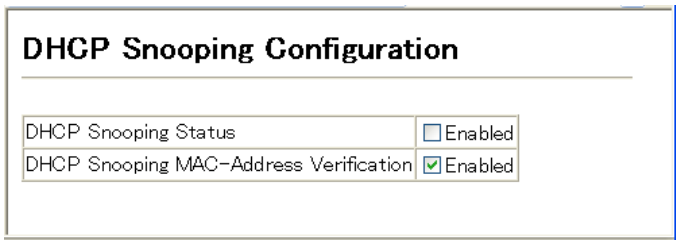
DHCP Snooping MAC-Address Verification

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。



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。

機能解説

- DHCP スヌーピングがスイッチのグローバルかつ指定された VLAN で有効の時、DHCP パケットフィルタリングは、VLAN に属する全ての Untrust ポートで実行されます。
- DHCP スヌーピングがグローバルで無効時、DHCP スヌーピングは依然指定された VLAN での設定が可能ですが、DHXP スヌーピングがグローバルで再度有効になるまで効果は反映されません。
- DHCP スヌーピングがグローバルで有効であり、VLAN で無効になった場合、この VLAN での全ての動的バインディング学習はバインディングテーブルから取り除かれます。

設定・表示項目

VLAN ID

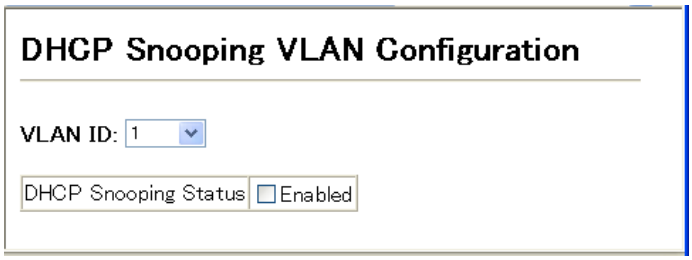
設定を行う VLAN（範囲：1-4094）

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。



DHCP スヌーピング情報オプション設定

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。

設定・表示項目

DHCP Snooping Information Option Status

DHCP Option 82 Indormation Relay 有効 / 無効

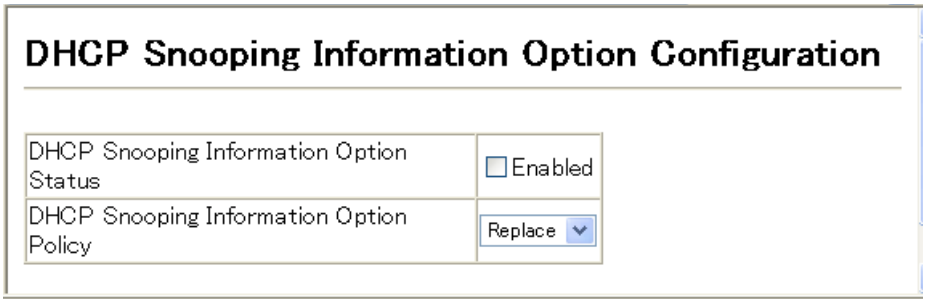
DHCP Snooping Information Option Policy

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。
- Keep －既存のリレー情報をそのまま保持します。
- 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。

設定方法

[DHCP Snooping] → [Information Option Configuration] をクリックします。



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。

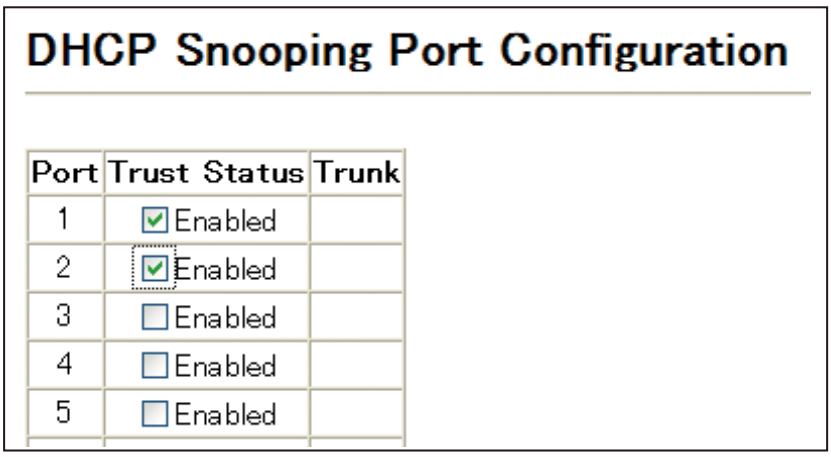
設定・表示項目

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。.



DHCP スヌーピングバインディング情報

DHCP スヌーピングバインディング情報を表示します。

設定・表示項目

Store DHCP snooping binding entries to flash

動的に学習された全てのスヌーピングエントリをフラッシュメモリへ書き込みます。

Clear DHCP snooping binding entries from flash

動的に学習された全てのスヌーピングエントリをフラッシュメモリから取り除きます。

No.

DHCP スヌーピングバインディング情報のエントリ番号

Unit

スタックユニット

Port

ポート番号

VLAN ID

設定された VLAN の ID

MAC Address

設定された VLAN の ID

IP Address

正当なユニキャスト IP アドレス

IP Address Type

IPv4 アドレスタイプ

Lease Time（Seconds）

エントリがテーブルから取り除かれてからの時間

設定方法

[DHCP Snooping] → [Information Binding Information] をクリックします。

DHCP Snooping Binding Information

Store DHCP snooping binding entry to flash. Store

Clear DHCP snooping binding entry from flash. Clear

No.	Unit	Port	VLAN ID	MAC Address	IP Address	IP Address Type	Lease Time (Seconds)

3.7.7 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。この項は 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。

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。

機能解説

- この機能は選択したポートで、ソースガードモードを SIP（Source IP）または SIP-MAC（Source IP と MAC）の有効にします。バインディングテーブルの全てのエントリにたいし、VLAN ID、ソース IP アドレス、ポート番号のチェックを行うには SIP オプションを使用してください。これらと同じパラメータに加え、ソース MAC アドレスのチェックを行うには、SIP-MAC オプションを使用して下さい。もしマッチするエントリが見つからない場合、パケットは破棄されます。
- IP ソースガードが有効の場合、トラフィックは DHCP スヌーピング経由で学習された動的エントリ（詳細は 137 ページの「DHCP スヌーピング」を参照してください）または、ソースガードバインディングテーブルで設定された静的アドレスに基づいてフィルタされます。
- IP ソースガードが有効の場合、上りのパケットの IP アドレス（SIP オプション）またはその IP アドレスと対応する MAC アドレスの両方（SIP-MAC オプション）はバインディングテーブルに照らし合わされます。もしマッチするエントリが見つからない時、パケットは破棄されます。
- フィルタリングルールは以下のように実行されます。
  - DHCP スヌーピングが無効の際（P137 参照）、IP ソースガードは VLAN ID、ソース IP アドレス、ポート番号、ソース MAC アドレス（SIP-MAC オプション）をチェックします。もしバインディングテーブルにマッチするエントリが見つからない時、パケットは破棄されます。
  - DHCP スヌーピングが有効の際、IP ソースガードは VLAN ID、ソース IP アドレス、ポート番号、ソース MAC アドレス（SIP-MAC オプション）をチェックします。もしバインディングテーブルまたは見つからず、エントリタイプが静的 IP ソースガードバインディングまたは動的 DHCP スヌーピングバインディングである場合、パケットは転送されます。
  - IP ソースガードが IP ソースバインディングが未設定のインタフェース（IP ソースガードバインディングテーブルの静的設定と DHCP スヌーピングからの動的学習のいずれか）で有効の際、スイッチはポートの DHCP パケット以外全ての IP トラフィックを破棄します。

設定・表示項目

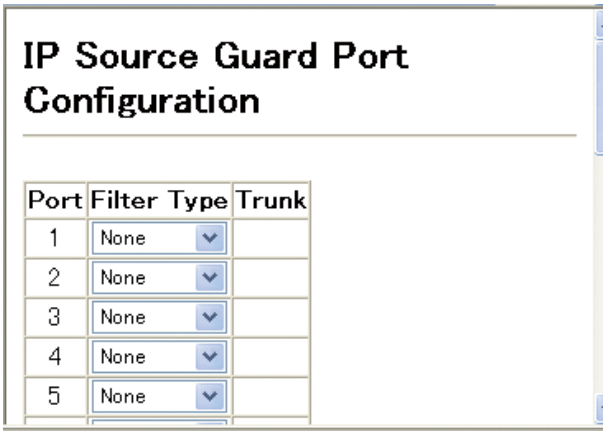
Filter Type

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。**



IP ソースガード静的バインディング設定

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。

機能解説

- ソースガードバインディングテーブルの静的アドレスエントリは、無限のリース時間で自動的に設定されます。DHCP スヌーピングで学習された動的エントリは DHCP サーバ自身で設定されます。
- 静的バインディングは以下のように処理されます。
  - －同一の VLAN ID と MAC アドレスに項目が無い場合、新しいエントリは静的 IP ソースガードバインディングタイプを使用し、バインディングテーブルに追加されます。
  - －同一の VLAN ID と MAC アドレスに項目が無く、エントリのタイプが静的 IP ソースガードバインディングである場合、新しいエントリが古い物を置き換えます。
  - －同一の VLAN ID と MAC アドレスに項目が無く、エントリのタイプが動的 DHCP スヌーピングバインディングである場合、新しいエントリが古い物を置き換え、エントリタイプは静的 IP ソースガードバインディングに変更されます。

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：1-52）.

VLAN ID

設定を行う VLAN ID（範囲：1-4094）

MAC Address

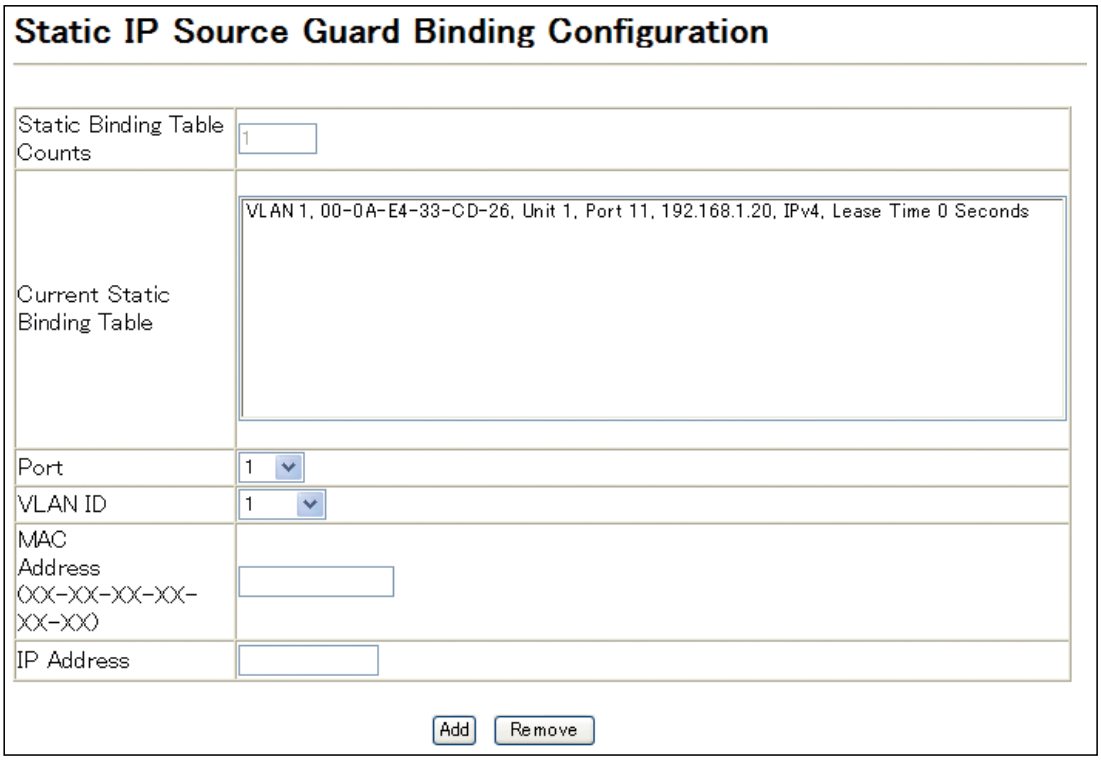
有効なユニキャスト MAC アドレス

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。**



動的 IP ソースガードバインディング情報の表示

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

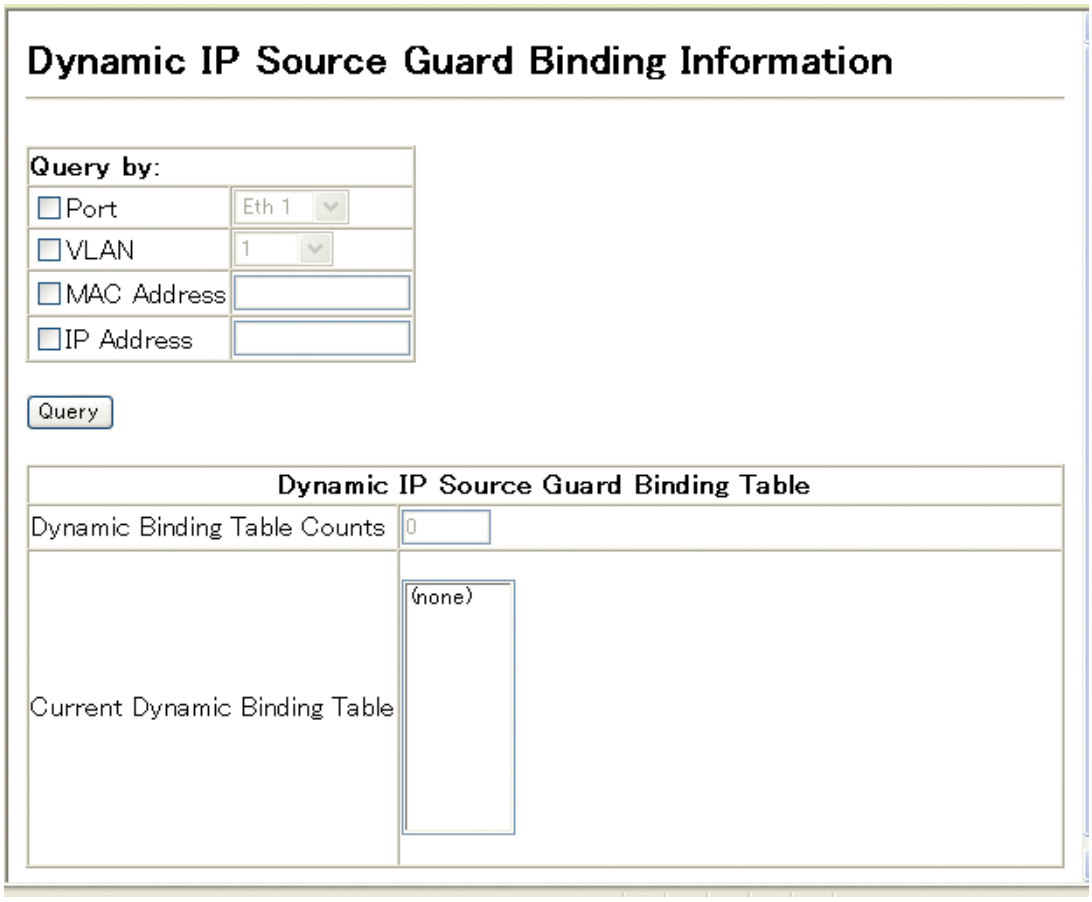
ソースガードバインディングテーブルに登録されている IP アドレス数

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。



3.8 ポート設定

3.8.1 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	

3.8.2 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。

機能解説

- ポートの設定を手動で行ない、Speed/Duplex モード 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・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。

Giga PHY Mode

Master －選択されたポートをマスターに設定します。

Slave －選択されたポートをスレーブにせってします。

Auto Prefer Master －リンクの終端で行われた他の設定にかかわらず、最初の設定としてマスターモードを使用します。

Auto Prefer Slave －リンクの終端で行われた他の設定にかかわらず、最初の設定としてスレーブモードを使用します。

固定 1000full オペレーションは、リンクの終わりの両端のポートを接続プロセスにおけるそれらの役割をマスター / スレーブとして確立することが必要です。
この機能を使用する前に、auto-negotiation は最初に無効にし、Speed/Duplex は 1000Full に設定してください。
その後に、リンクの終端の互換性のある Giga PHY モードを選択してください。

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。

Media Type

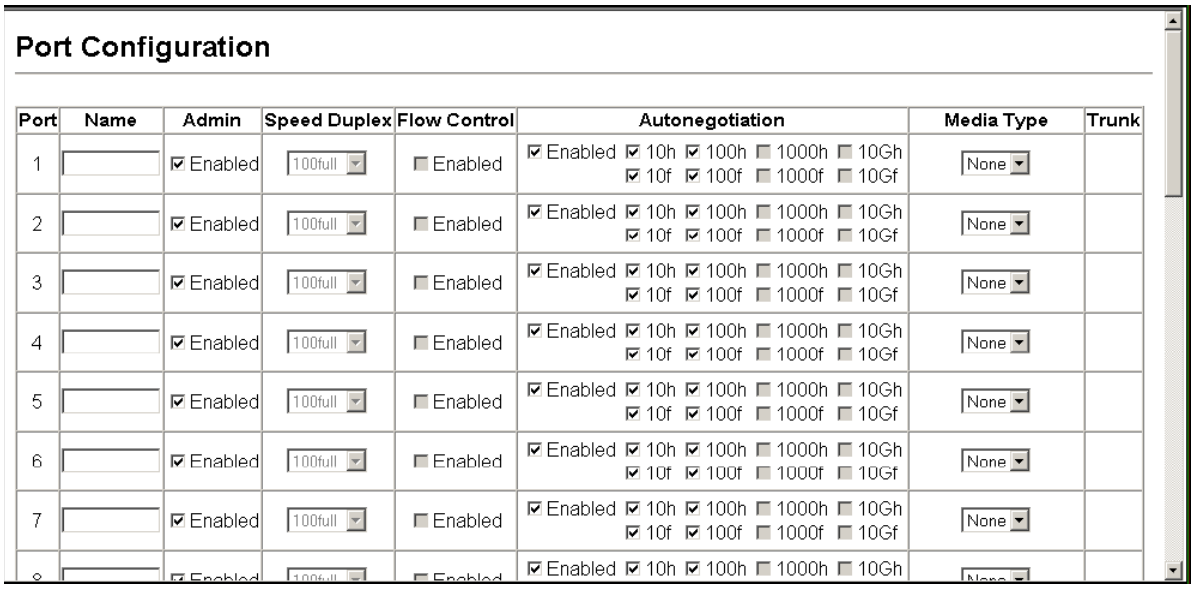
コンボポートで使用されるメディアのタイプ（オプション：Coppper-Forced、SFP-Forced、SFP-Preferred-Auto　初期設定：SFP-Preferred-Auto）

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、P152 「トランクグループの設定」を参照して下さい。

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。



3.8.3 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 8 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

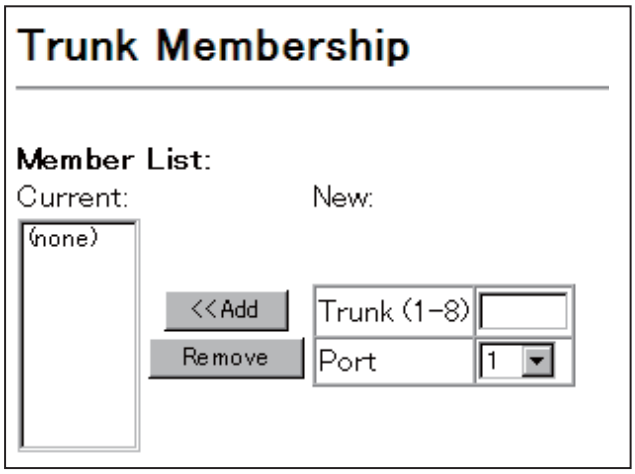
新規にトランクを作成するための入力欄

ー **Trunk** ― トランク識別子（範囲：1-8）

ー **Port** ― ポート識別子（範囲：1-52）

設定方法

[Port] → [Trunk Membership] をクリックします。1 から 8 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 (P152)

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）

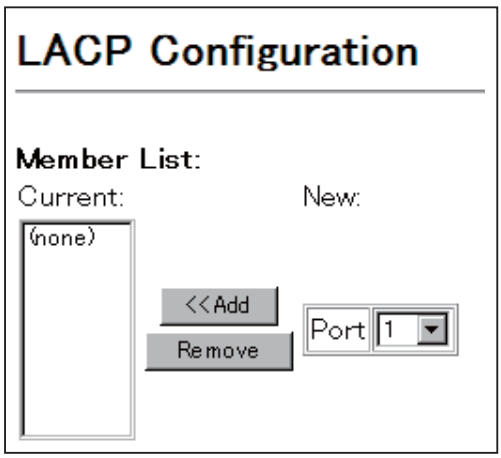
New

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：1-52）

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 グループメンバーのパラメータ設定

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：1-52）

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）

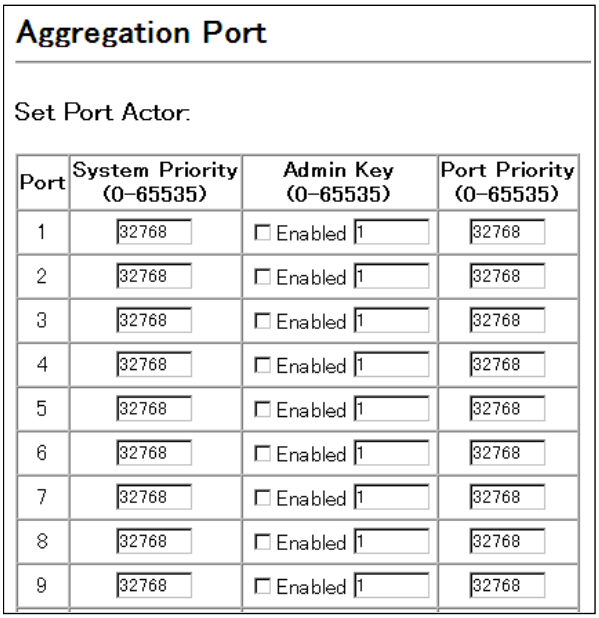
Port Priority

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 グループのパラメータ設定

指定した LACP グループに適用されるシステムパラメータの設定を行います。

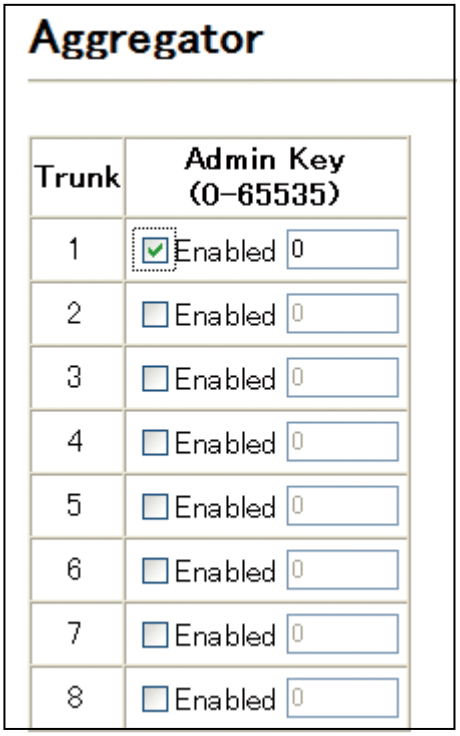
設定・表示項目

Admin Key

スイッチのローカル LACP セットアップ間のリンクアグリゲーショングループ（LAG）を識別するために使用されます。（範囲：0-65535）

設定方法

[Port] → [LACP] → [Aggregator] **をクリックします。必要とされる** LACP **グループに管理キーを設定し、**[Apply] **をクリックします。**



LACP ポートカウンタの表示

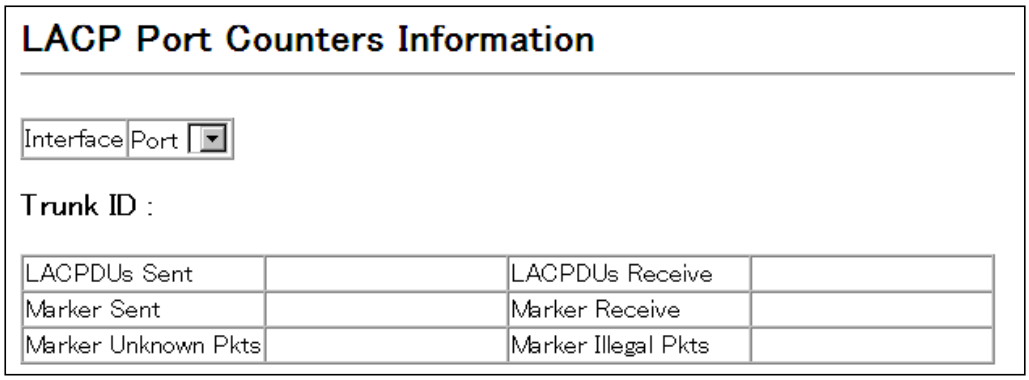
LACP プロトコルメッセージの統計情報の表示を行ないます。

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
Marker 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
Marker 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

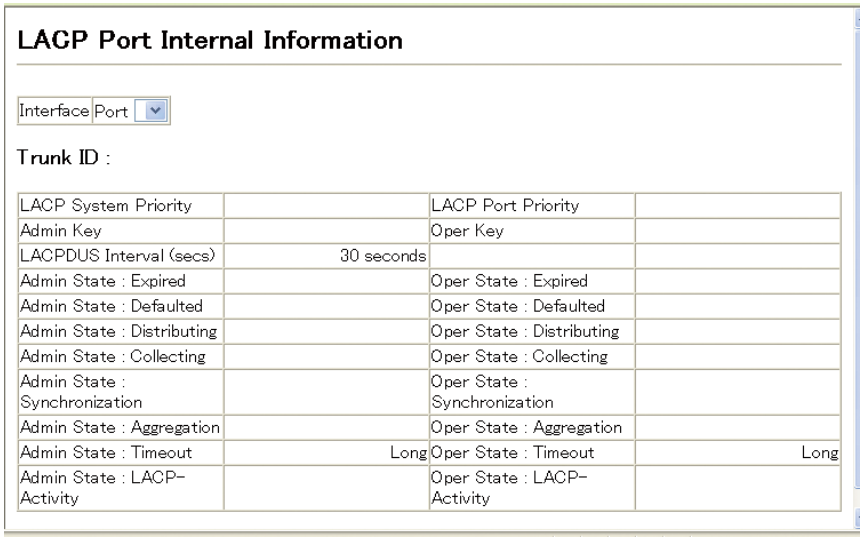
LACP のローカル側の設定及びステータスの表示を行なうことができます。

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

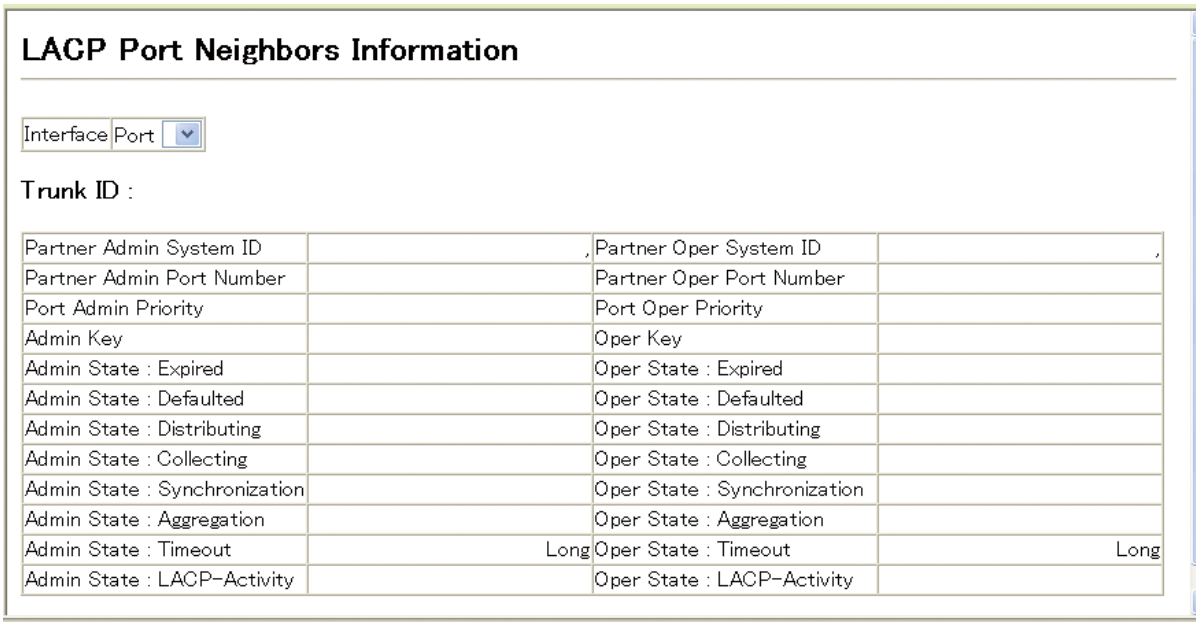
LACP のリモート側の設定及びステータスの表示を行なうことができます。

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。



3.8.4 ブロードキャストストームしきい値の設定

ブロード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ブロードキャスト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。

ブロード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

- ブロードキャスト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。
- ブロードキャストコントロールは IP マルチキャストトラフィックに影響しません。
- ASIC チップリミテーションのため、サポートされるストームコントロールモードは以下です。
  - －ブロードキャスト
  - －ブロードキャスト＋マルチキャスト
  - －ブロードキャスト＋マルチキャスト＋未知のユニキャスト

  これはマルチキャストストームコントロールが有効である時、ブロードキャストストームコントロールもまた有効になるということを意味します。（マルチキャストストームコントロールコマンドで設定されたしきい値を使用）
  また、未知のユニキャストストームコントロールが有効である時、ブロードキャスト・マルチキャストストームコントロールの両方もまた有効になります。（未知のユニキャストストームコントロールコマンドで設定されたしきい値を使用）
- このページで提供されたストームコントロール機能はハードウェアレベルコントロール機能です。トラフィックストームもまた、様々な制御反応を引き起こす自動ストームコントロールを使用することにより、ソフトウェアレベルでコントロールすることが可能です。このコントロールタイプは CLI でのみサポートされています。
  詳しくは 553 ページの「自動トラフィック制御」を参照してください。
  これらのコントロールタイプのうち、1 つだけがポートに適用されることにご注意ください。ポートでのハードウェアレベルコントロールの有効化により、自動ストームコントロールは無効になります。

設定・表示項目

Port

ポート番号

Type

ポートの種類を表示（100BASE-TX、1000BASE-T または SFP）

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）

Threshold

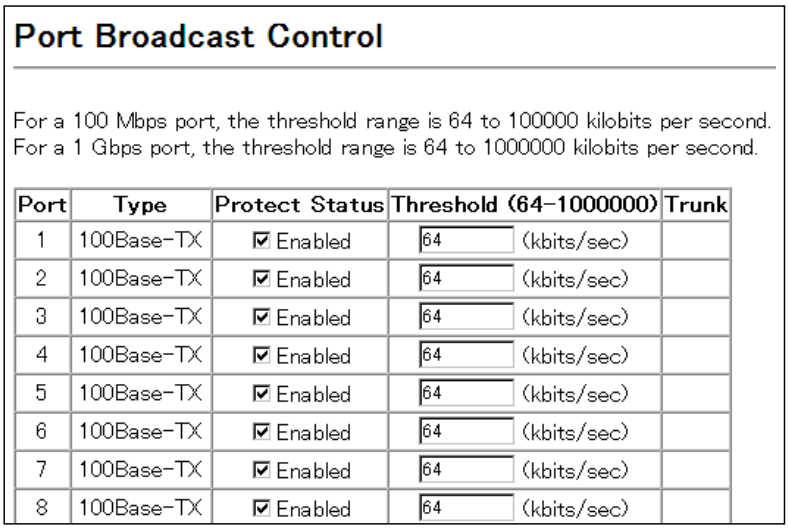
レートとしてのしきい値
範囲：Fast Ethernet ports：64-100000 Kbits/ 秒、Gigabit ports：64-1000000 Kbits/ 秒
初期設定：64 Kbits/second

Trunk

ポートがトランクメンバーの場合に表示

設定方法

[Port] → [Port/Trunk Broadcast Control] をクリックします。
しきい値を設定し、任意のポートの "Enable" フィールドへチェックを入れ、[Apply] をクリックして下さい。



3.8.5 マルチキャストストームしきい値の設定

それぞれのポートにしきい値を設定することにより、超過のマルチキャストトラフィックからネットワークを保護することが可能です。
指定されたしきい値を超える全てのマルチキャストパケットは破棄されます。

機能解説

- マルチキャストコントロールは IP マルチキャストトラフィックに影響しません。
- ASIC チップリミテーションのため、サポートされるストームコントロールモードは以下です。

－ブロードキャスト
－ブロードキャスト＋マルチキャスト
－ブロードキャスト＋マルチキャスト＋未知のユニキャスト

これはマルチキャストストームコントロールが有効である時、ブロードキャストストームコントロールもまた有効になるということを意味します。（マルチキャストストームコントロールコマンドで設定されたしきい値を使用）
また、未知のユニキャストストームコントロールが有効である時、ブロードキャスト・マルチキャストストームコントロールの両方もまた有効になります。（未知のユニキャストストームコントロールコマンドで設定されたしきい値を使用）

- このページで提供されたストームコントロール機能はハードウェアレベルコントロール機能です。トラフィックストームもまた、様々な制御反応を引き起こす自動ストームコントロールを使用することにより、ソフトウェアレベルでコントロールすることが可能です。このコントロールタイプは CLI でのみサポートされています。
詳しくは 553 ページの「自動トラフィック制御」を参照してください。
これらのコントロールタイプのうち、1 つだけがポートに適用されることにご注意ください。
ポートでのハードウェアレベルコントロールの有効化により、自動ストームコントロールは無効になります。

設定・表示項目

Port

ポート番号

Type

ポートの種類を表示（100BASE-TX、1000BASE-T **または** SFP**）**

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）

Threshold

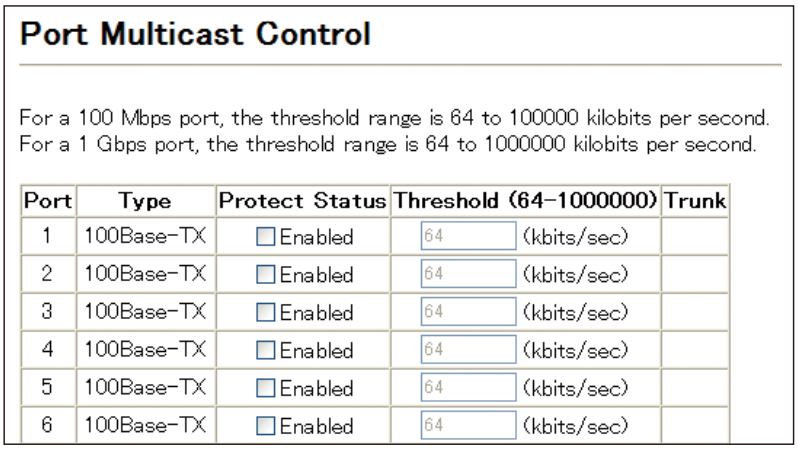
ポート帯域幅のパーセンテージ
範囲：Fast Ethernet ports：64-100000 Kbits/ **秒、**Gigabit ports：64-1000000 Kbits/ **秒**
初期設定：64 Kbits/second

Trunk

ポートがトランクメンバーの場合に表示

設定方法

[Port] → [Port/TrunkMulticast Control] **をクリックします。任意のポートの** "Enable" **フィールドへチェックを入れ、しきい値を入力し、**[Apply] **をクリックして下さい。**



3.8.6 未知のユニキャストストームしきい値の設定

それぞれのポートにしきい値を設定することにより、超過の未知のユニキャストトラフィックからネットワークを保護することが可能です。
指定されたしきい値を超える全てのマルチキャストパケットは破棄されます。

機能解説

- ASIC **チップリミテーションのため、サポートされるストームコントロールモードは以下です。**

－ブロードキャスト

－ブロードキャスト＋マルチキャスト

－ブロードキャスト＋マルチキャスト＋未知のユニキャスト

これはマルチキャストストームコントロールが有効である時、ブロードキャストストームコントロールもまた有効になるということを意味します。（マルチキャストストームコントロールコマンドで設定されたしきい値を使用）
また、未知のユニキャストストームコントロールが有効である時、ブロードキャスト・マルチ

キャストストームコントロールの両方もまた有効になります。（未知のユニキャストストームコントロールコマンドで設定されたしきい値を使用）

- このページで提供されたストームコントロール機能はハードウェアレベルコントロール機能です。トラフィックストームもまた、様々な制御反応を引き起こす自動ストームコントロールを使用することにより、ソフトウェアレベルでコントロールすることが可能です。このコントロールタイプは CLI でのみサポートされています。
  詳しくは 553 ページの「自動トラフィック制御」を参照してください。
  これらのコントロールタイプのうち、1 つだけがポートに適用されることにご注意ください。
  ポートでのハードウェアレベルコントロールの有効化により、自動ストームコントロールは無効になります。

設定・表示項目

Port

ポート番号

Type

ポートの種類を表示（100BASE-TX、1000BASE-T または SFP）

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）

Threshold

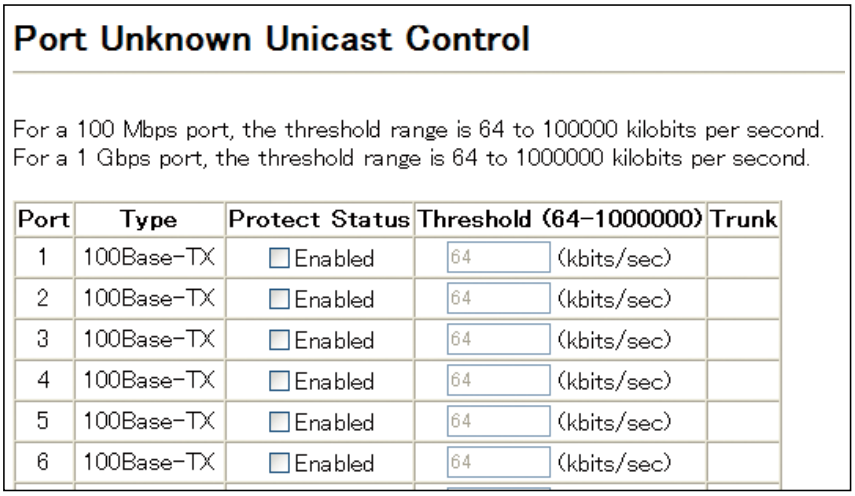
ポート帯域幅のパーセンテージ
範囲：Fast Ethernet ports：64-100000 Kbits/ 秒、Gigabit ports：64-1000000 Kbits/ 秒
初期設定：64 Kbits/second

Trunk

ポートがトランクメンバーの場合に表示

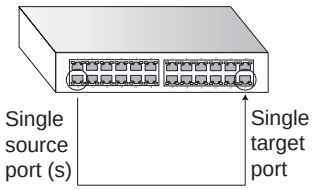
設定方法

[Port] → [Port/Trunk Unknown Unicast Control] をクリックします。
任意のポートの "Enable" フィールドへチェックを入れ、しきい値を入力し、[Apply] をクリックして下さい。



3.8.7 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。

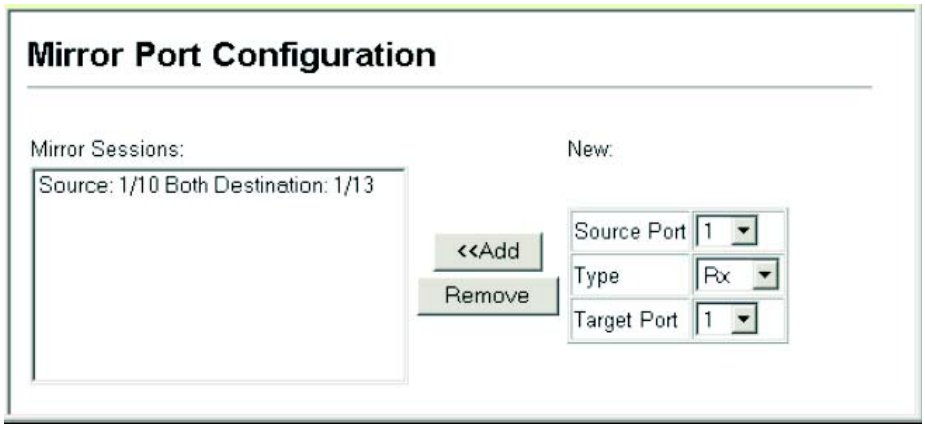
Rx**（受信）**、Tx**（送信）**、Both**（送・受信）（初期設定：**Rx**）**

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 Port Configuration] **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。**



3.8.8 MAC アドレスミラーリングの設定

本機では、リアルタイム分析の為に、スイッチのターゲットポート以外の全てのポートから、指定した特定のソースアドレスのトラフィックをターゲットポートへミラーリングすることが可能です。
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、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

- **MAC アドレスからのトラフィックのミラーリングを行う際、ターゲットポート以外のスイッチの全てのポートへ入る、指定したソースアドレスを持つ入力トラフィックはディスティネーションポートへミラーされます。**
- **全てのミラーセッションは同じディスティネーションポートを共有します。**
- **スパニングツリー BPDU パケットはターゲットポートへミラーされません。**
- **ポートトラフィックのミラーリング時に MSTP を使用する際、ターゲットポートはソースポートと同じ VLAN に含まれなくてはなりません。（詳細は P174 を参照してください）**

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 MAC Address

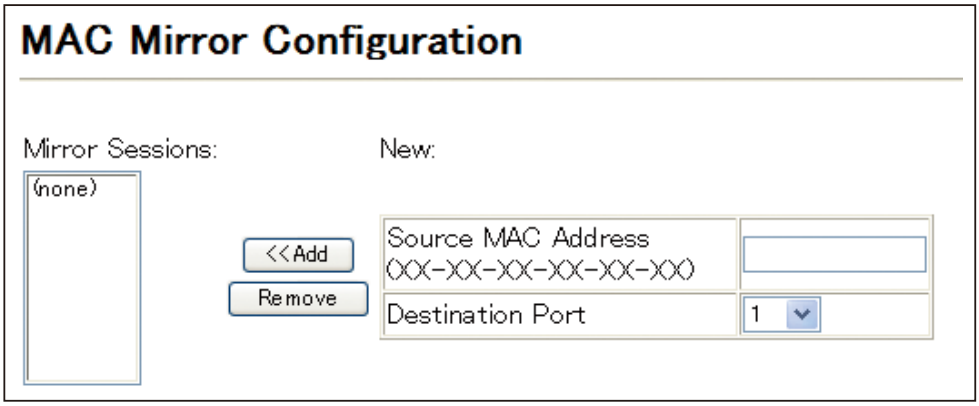
通信がモニターされる MAC アドレスを指定します。
xx-xx-xx-xx-xx-xx **または** xxxxxxxxxxxx **の形式で入力してください。**

Destination Port

ソースポートからトラフィックのミラーを行うポートを指定します。（範囲：1-52）

設定方法

[Port] → [Mirror] **をクリックします。ソース** MAC **アドレスとディスティネーションポートを指定し、**[Apply] **をクリックします。**



3.8.9 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/Trunk

ポート / トランク番号

Rate Limit Status

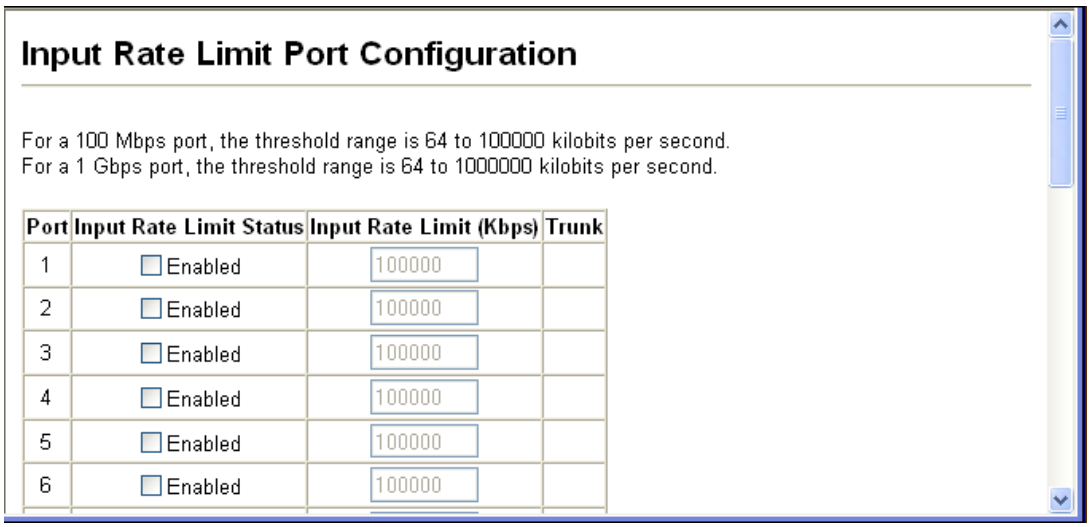
帯域制御の有効 / 無効（初期設定：有効）

Rate Limit

帯域制御のレベルを設定
（範囲：Fast Ethernet 64 - 100000 kilobits/ **秒**
Gigabit Ethernet 64-1000000 kilobits/ **秒）**

設定方法

[Port] → [Rate Limit] → [Input Port/Output Port/Trunk 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。**



3.8.10 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

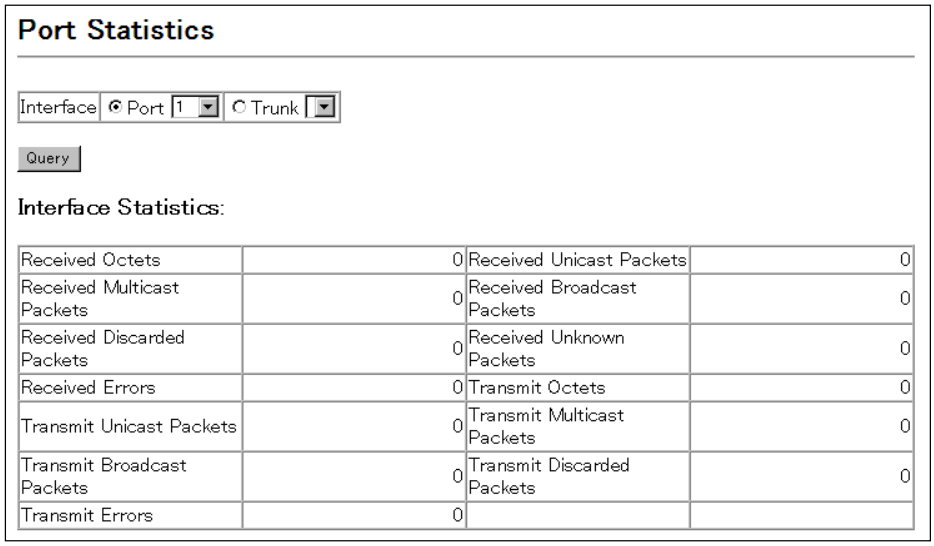
パラメータ	解説
Interface Statistics	
Received Octets	フレーム文字を含むインタフェースで受信されたオクテットの数
Received Unicast Packets	層位プロトコルで受信したサブネットワークユニキャストパケットの数
Received Multicast Packets	このサブレイヤから送信され、高層のレイヤで受信されたパケットで、このサブレイヤのマルチキャストアドレス宛てのパケットの数
Received Broadcast Packets	このサブレイヤから送信され、高層のレイヤで受信されたパケットで、このサブレイヤのブロードキャストアド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。)

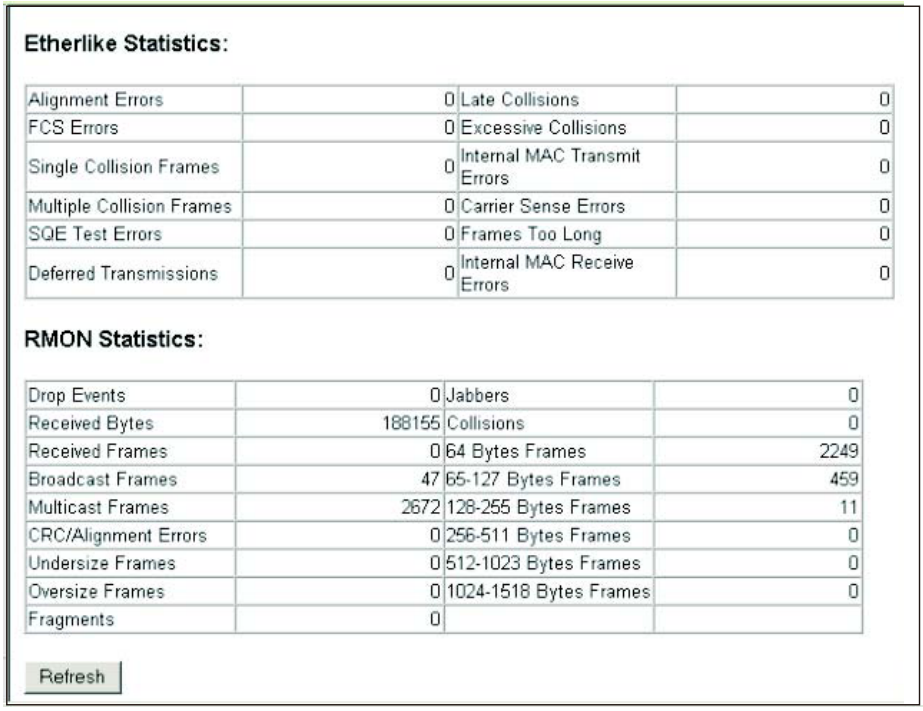
設定方法

[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。



Received Octets	0	Received Unicast Packets	0
Received Multicast Packets	0	Received Broadcast Packets	0
Received Discarded Packets	0	Received Unknown Packets	0
Received Errors	0	Transmit Octets	0
Transmit Unicast Packets	0	Transmit Multicast Packets	0
Transmit Broadcast Packets	0	Transmit Discarded Packets	0
Transmit Errors	0		



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

RMON Statistics:

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

Refresh

3.9 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。

3.9.1 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

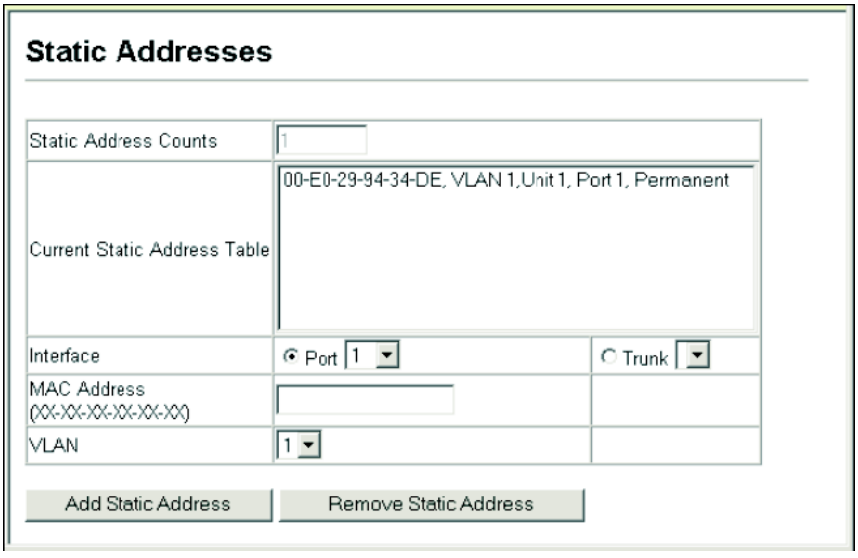
インタフェースの MAC アドレス

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。



3.9.2 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

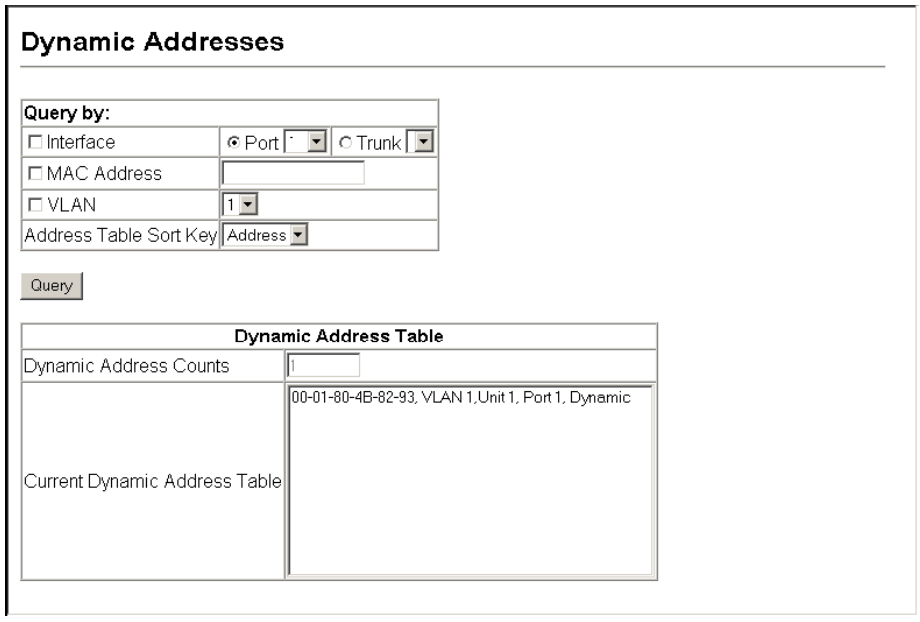
動的に学習する MAC **アドレス数**

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。**



3.9.3 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

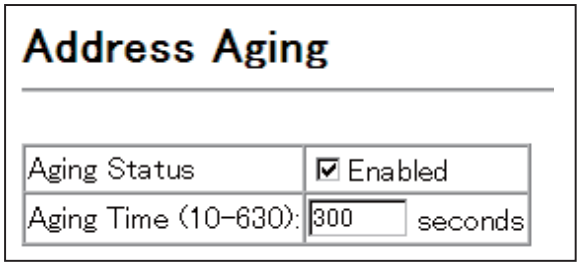
エージングタイムの機能の有効 / 無効

Aging Time

MAC **アドレスエージングタイム（範囲：**10-630 **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。**



3.10 スパニングツリーアルゴリズム

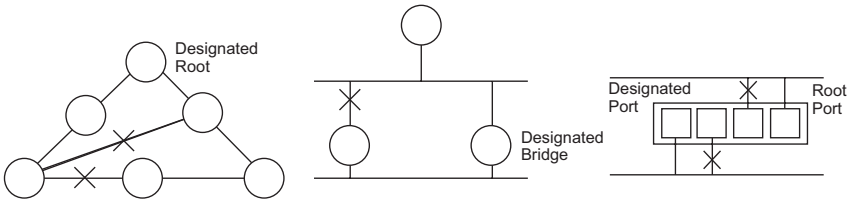
スパニングツリープロトコル STP はネットワークのループを防ぎ、また、スイッチ、ブリッジ及びルータ間のバックアップリンクを確保するために使用します。

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。

3.10.1 ループバック検出

ポートループバック検出が有効であり、ポートがそれ自身の BPUD を受信した際、ディテクションエージェントはループバック BPDU を破棄、SNMP トラップを送信し、ポートを Discard（パケット破棄）モードにします。
このループバックステーツは自動または手動でリリースすることができます。

ポートが自動ループバックリリースに設定されている場合、以下の条件の内 1 つが満たされるとポートは転送状態に戻ります。

- ポートがポート自身以外の BPUD を受信する。
- ポートのリンクステーツが一旦リンクダウンになった後、再びリンクアップになる。
- ポートがフォワード遅延インターバルでポート自身の BPUD の受信を終了。

[注意] ポートループバックディテクションが有効でなく、ポートが自身の BPUD を受信した場合、ポートは IEEE 準拠の 802.1w-2001 9.3.4 に従ってループバック BPDU を破棄します。

[注意] スパニングツリーがスイッチで無効になっている場合、ポートループバックディテクションはアクティブになりません。

[注意] 手動リリースモードに設定時、Link down/Up イベントはポートをリリースしません。

設定・表示項目

Port

設定を行うインタフェースを指定。

Status

このインタフェースでループバックディテクションを有効化。（初期設定：有効）

Trap

このインタフェースでループバックイベントの SNTP トラップ通知を有効化。（初期設定：無効）

Release Mode

ポートを自動または手動ループバックリリースに設定。

Release

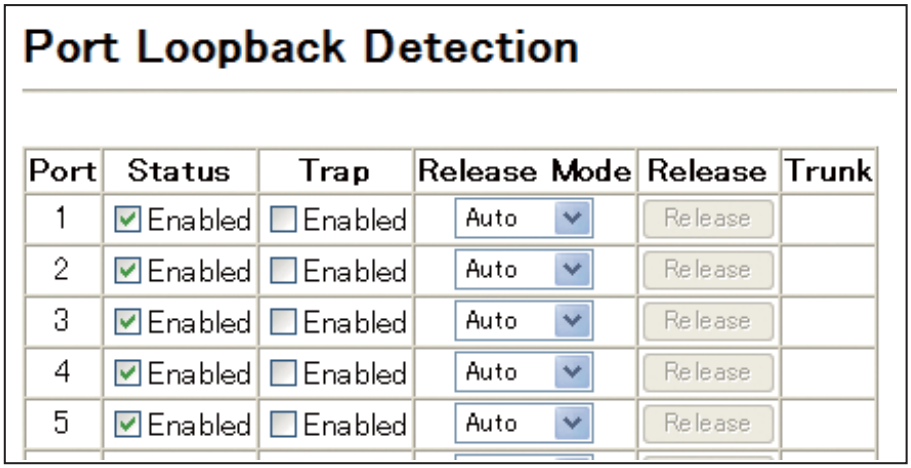
ポートが Discard モードから手動でリリースされることを許可。ポートが手動リリースモードに設定時のみ利用可能。

Trunk

このポートがトランクメンバーであることを示します。

設定方法

[Spanning Tree] → [Port Loopback Detection] **または** [Trunk Loopback Detection] **をクリックします。必要な項目を入力し、**[Apply] **をクリックします。**



3.10.2 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

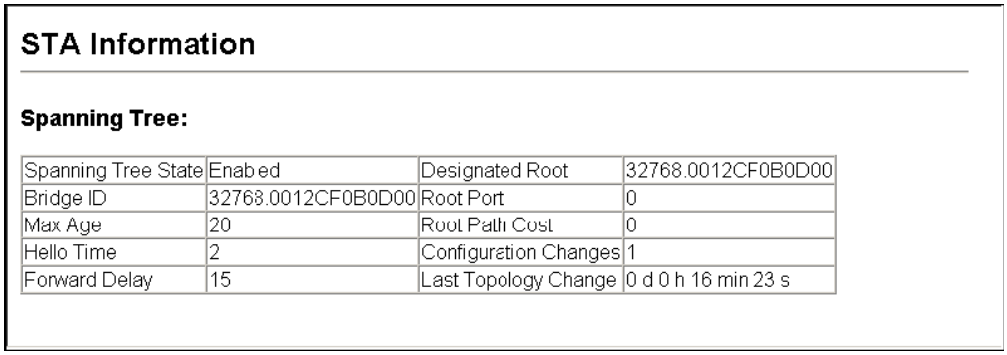
スパニングツリーが再設定された回数が表示されます。

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

3.10.3 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)

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）**

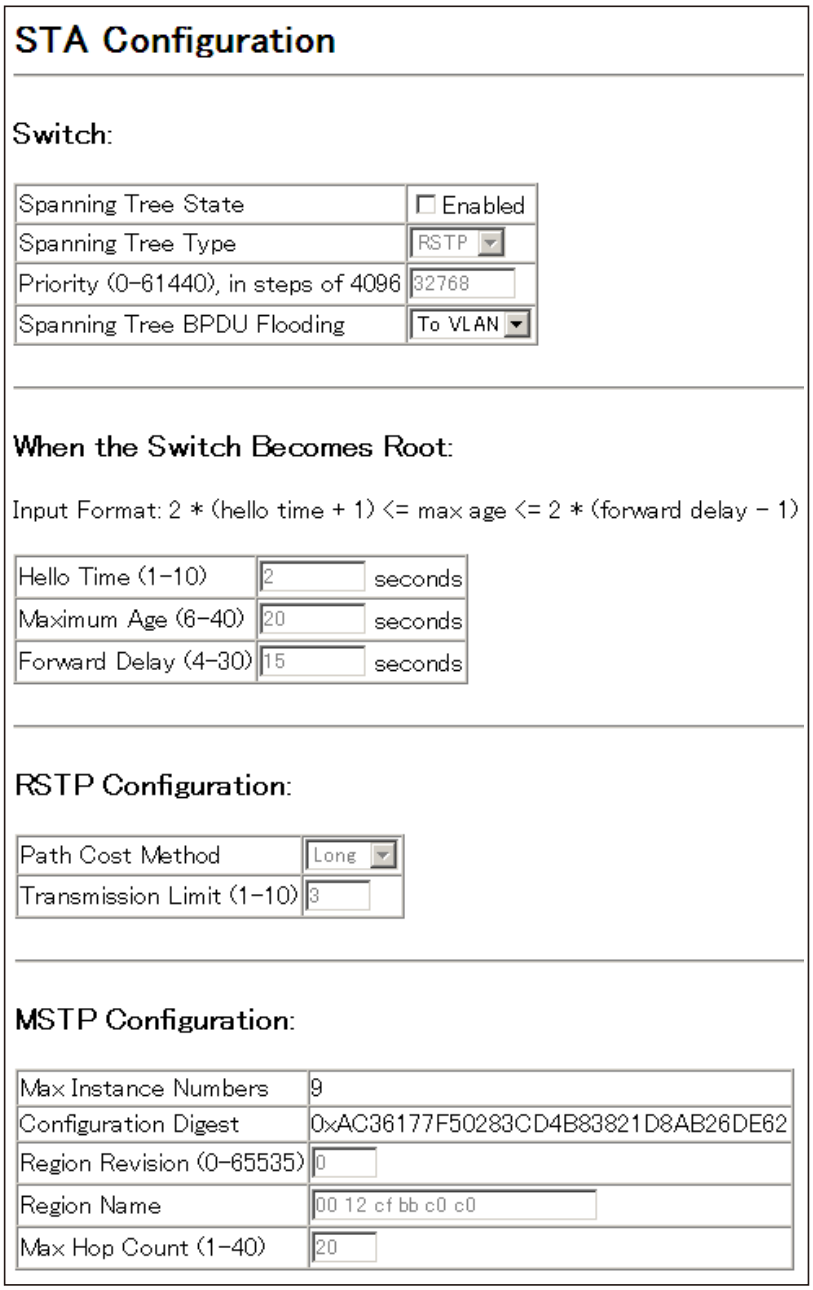
Maximum Hop Count

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。**



3.10.4 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。

BPDU Flooding

スパニングツリーがグローバルで無効時、または指定したポートで無効時、BPUD が他のポートにフラッディングされるか否かを表示します。

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	BPDU Flooding	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	Enabled	Discarding	0	0	32768.00172E119420	128.1	2000000	Shared	Enabled	Disabled	
2	Enabled	Enabled	Discarding	0	0	32768.00172E119420	128.2	2000000	Shared	Enabled	Disabled	
3	Enabled	Enabled	Discarding	0	0	32768.00172E119420	128.3	2000000	Shared	Enabled	Disabled	
4	Enabled	Enabled	Discarding	0	0	32768.00172E119420	128.4	2000000	Shared	Enabled	Disabled	
5	Enabled	Enabled	Discarding	0	0	32768.00172E119420	128.5	2000000	Shared	Enabled	Disabled	
6	Enabled	Enabled	Discarding	0	0	32768.00172E119420	128.6	2000000	Shared	Enabled	Disabled	
7	Enabled	Enabled	Discarding	0	0	32768.00172E119420	128.7	2000000	Shared	Enabled	Disabled	
8	Enabled	Enabled	Discarding	0	0	32768.00172E119420	128.8	2000000	Shared	Enabled	Disabled	
9	Enabled	Enabled	Discarding	0	0	32768.00172E119420	128.9	2000000	Shared	Enabled	Disabled	
10	Enabled	Enabled	Discarding	0	0	32768.00172E119420	128.10	2000000	Shared	Enabled	Disabled	
11	Enabled	Enabled	Forwarding	1	0	32768.00172E119420	128.11	100000	Point-to-Point	Enabled	Disabled	

3.10.5 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 P182 「インタフェース設定の表示」を参照して下さい）

- ー **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。
- ー **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。
- ー **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）

Admin 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）**

推奨 STA **パスコスト範囲**

ポートタイプ	IEEE802.1D-1998	IEEE802.1w-2001
Ethernet	50-600	200,000-20,000,000
Fast Ethernet	10-60	20,000-2,000,000
Gigabit Ethernet	3-10	2,000-200,000

推奨 STA **パスコスト**

ポートタイプ	**リンクタイプ**	IEEE802.1D-1998	IEEE802.1w-2001
Ethernet	Half Duplex Full Duplex Trunk	100 95 90	2,000,000 1,999,999 1,000,000
Fast Ethernet	Half Duplex Full Duplex Trunk	19 18 15	200,000 100,000 50,000
Gigabit Ethernet	Full Duplex Trunk	4 3	10,000 5,000

デフォルト STA **パスコスト**

ポートタイプ	**リンクタイプ**	IEEE802.1w-2001
Ethernet	Half Duplex Full Duplex Trunk	2,000,000 1,000,000 500,000
Fast Ethernet	Half Duplex Full Duplex Trunk	200,000 100,000 50,000
Gigabit Ethernet	Full Duplex Trunk	10,000 5,000

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。**

Root Guard

STA **はより低いブリッジ識別子（または同じ値と、より低い** MAC **アドレス）を持つブリッジがいつでも、ルートブリッジを引き継ぐことを許可します。**Root Guard **はルートブリッジが最適以下の場所において構成されないことを保証するために使用します。**
（初期設定：無効）

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。**

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	BPDU Flooding	STA State	Priority (0-240), in steps of 16	Admin Path Cost (1-200000000, 0:Auto)	Admin Link Type	Root Guard	Migration	Trunk
1	☑ Enabled	☑ Enabled	Discarding	128	0	Auto	☐ Enabled	☐ Enabled	
2	☑ Enabled	☑ Enabled	Discarding	128	0	Auto	☐ Enabled	☐ Enabled	
3	☑ Enabled	☑ Enabled	Discarding	128	0	Auto	☐ Enabled	☐ Enabled	
4	☑ Enabled	☑ Enabled	Discarding	128	0	Auto	☐ Enabled	☐ Enabled	
5	☑ Enabled	☑ Enabled	Discarding	128	0	Auto	☐ Enabled	☐ Enabled	
6	☑ Enabled	☑ Enabled	Discarding	128	0	Auto	☐ Enabled	☐ Enabled	
7	☑ Enabled	☑ Enabled	Discarding	128	0	Auto	☐ Enabled	☐ Enabled	

3.10.6 STA エッジポート設定

インタフェースがブリッジされた LAN の終端に接続されるか、最後のノードに接続される際、いくつかの STA オプションを有効にすることが可能です。

設定・表示項目

Admin Edge Port

- Enabled ― ポートをエッジポートとして手動で設定します。
- Disabled ― エッジポート設定を無効にします。
- Auto ― RSTP または MSTP BPDU を受信せずにエッジ遅延時間の期限が切れた際、ポートを自動でエッジポートとして設定します。

BPDU Guard

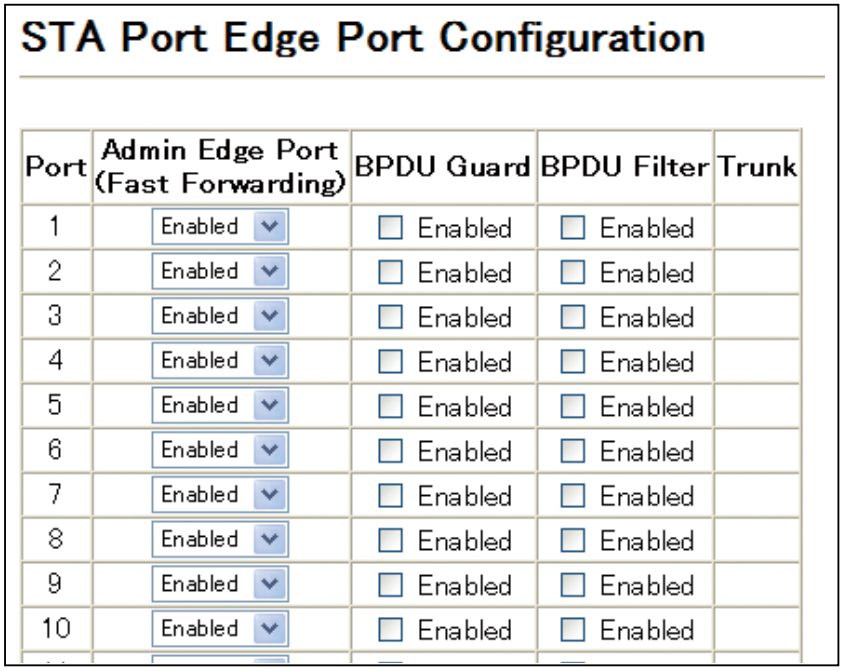
BPDU の受信からエッジポートを保護します。（初期設定：無効）

BPDU Filter

最後のノードに接続される設定をされたエッジポートで BPUD の転送を無効にします。（初期設定：無効）

設定方法

[Spanning Tree] → [STA] → [Port Edge Port Configuration] 又は [Trunk Edge Port 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。



3.10.7 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 (P179 「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）

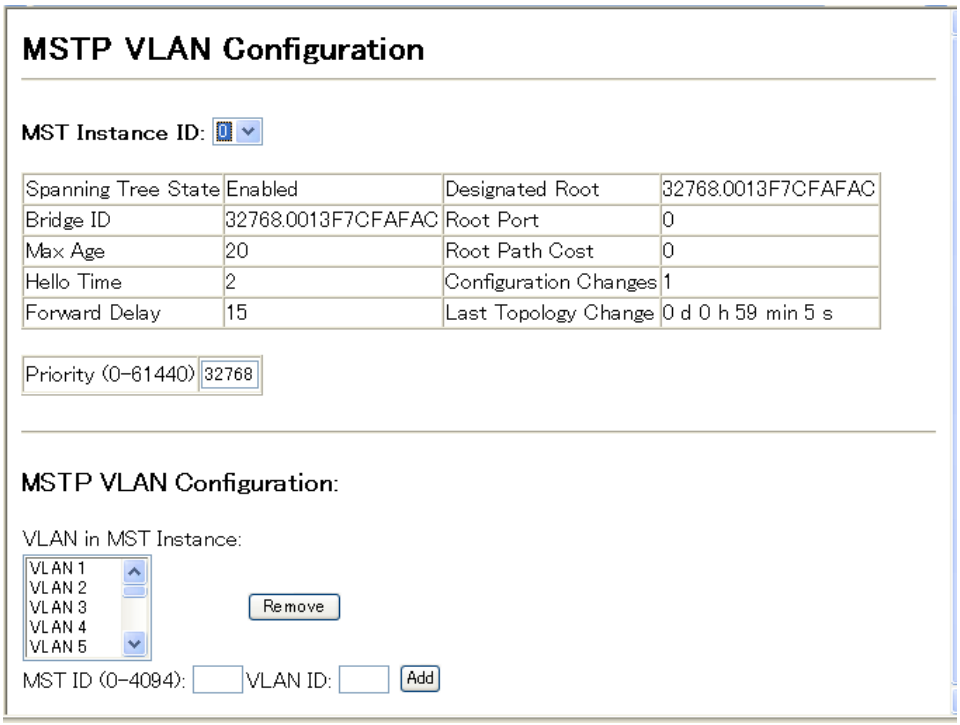
VLAN ID

MST インスタンスに指定する VLAN ID（設定範囲：1-4094）

他の項目は、P182 「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。



3.10.8 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

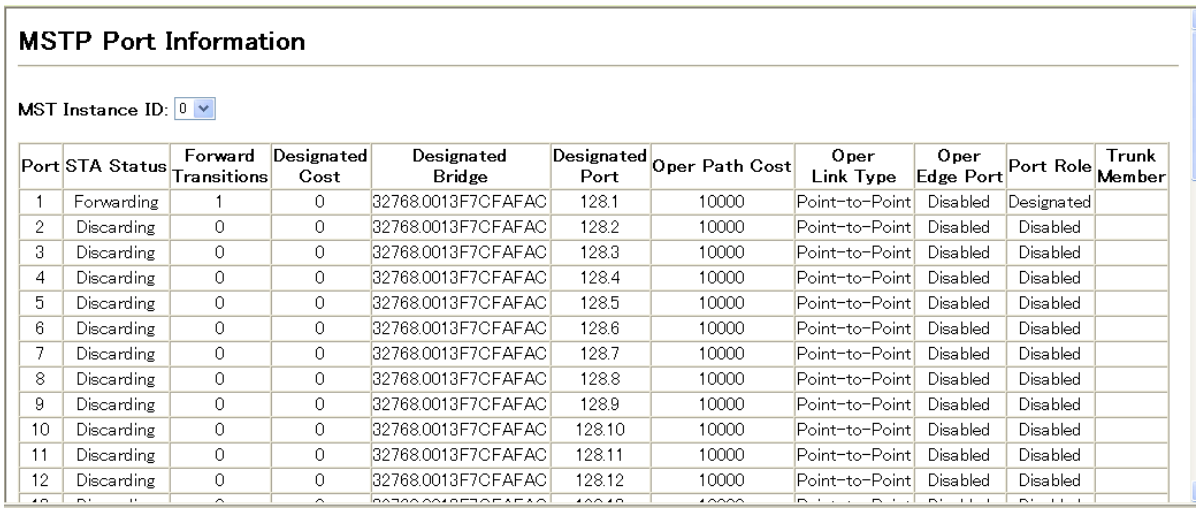
MST Instance ID

インスタンス ID（初期設定：0）

[注意] 他の項目に関しては P182 「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] または [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	

3.10.9 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 182 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

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）

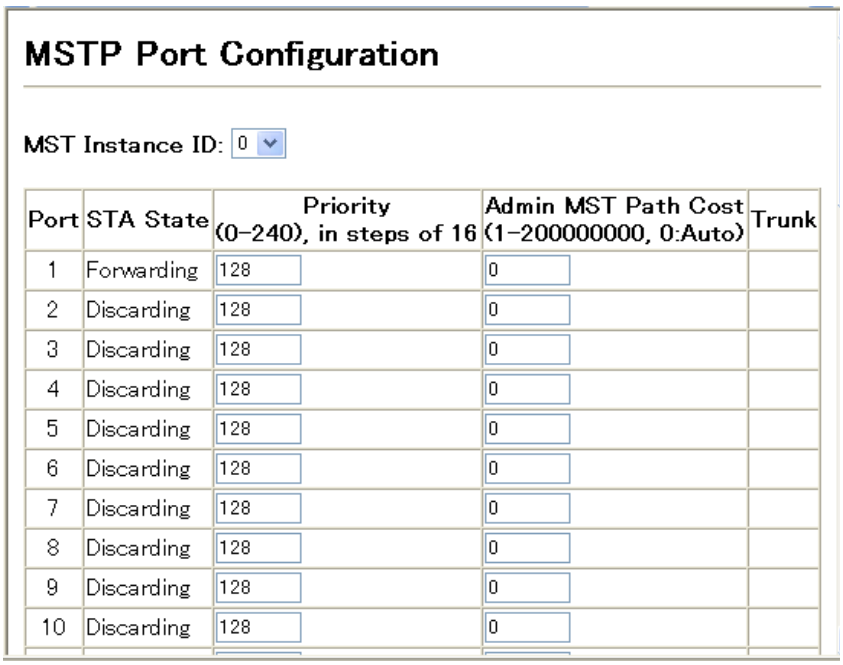
Admin MST Path Cost

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）

- 推奨設定範囲：P185 の表を参照してください。
- 推奨設定値：P185 の表を参照してください。
- 初期設定：P185 の表を参照してください。

設定方法

[Spanning Tree] → [MSTP] → [Port Configuration] **または** [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	

3.11 VLAN

3.11.1 IEEE802.1Q 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。

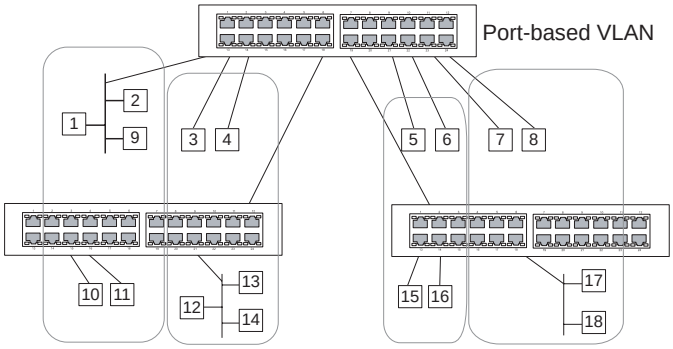
自動 VLAN 登録 ― GVRP (GARP VLAN Registration Protocol) は各終端装置が VLAN を割り当てられる必要がある場合に、VLAN を自動的に学習し設定を行います。終端装置（又はそのネットワークアダプタ）が IEEE802.1Q VLAN プロトコルに対応している場合、参加したい VLAN グループを提示するメッセージをネットワークに送信するための設定を行うことができます。本機がこれらのメッセージを受信した際、指定された VLAN の受信ポートへ自動的に追加し、メッセージを他の全てのポートへ転送します。

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。



タグ付き・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。

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。

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

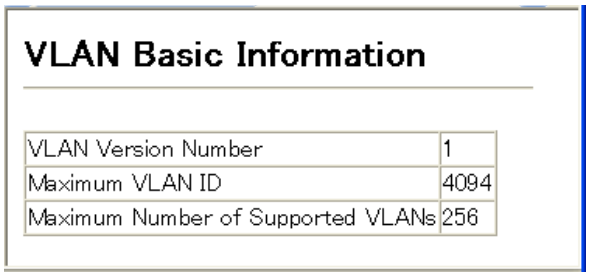
本機で認識可能な VLAN ID の最大値

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。



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

Egress Ports

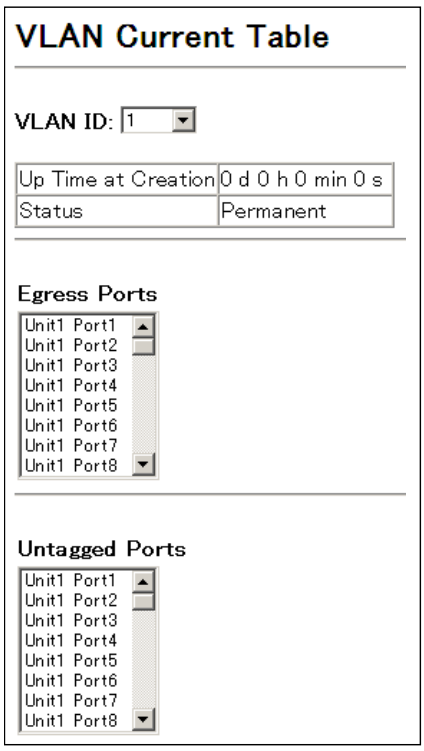
全ての VLAN ポートメンバーを表示

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。



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

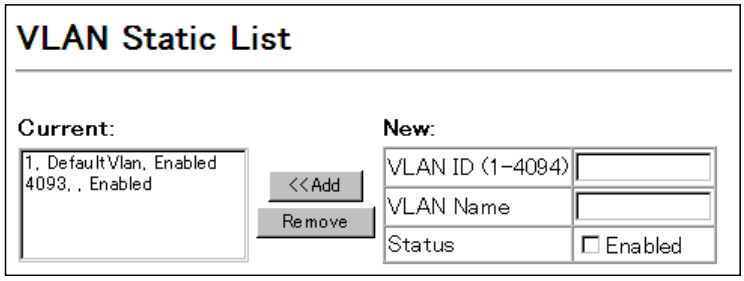
リストに新しい VLAN グループを追加します。

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。



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] P201 「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。P202 「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 100 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

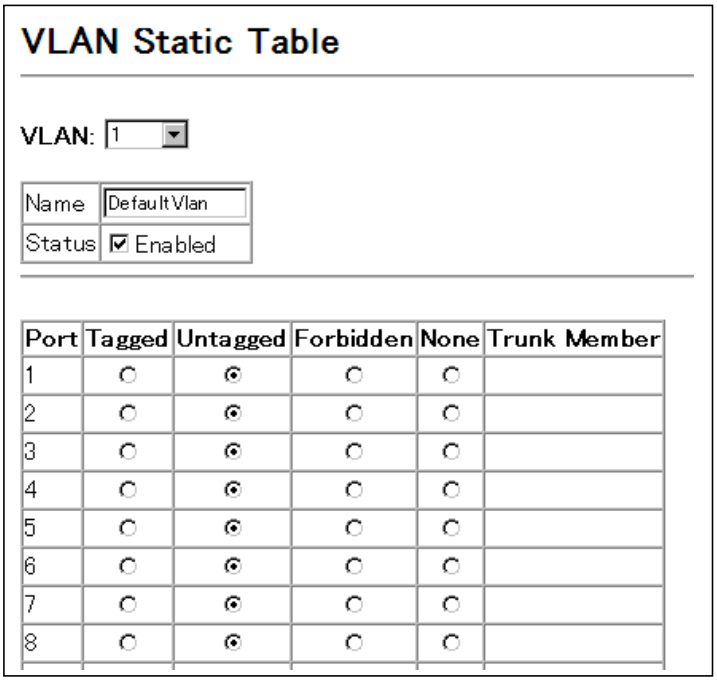
ラジオボタンをマークすることにより、各インタフェースへの VLAN メンバーシップを選択します。

- **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 P195 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。



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

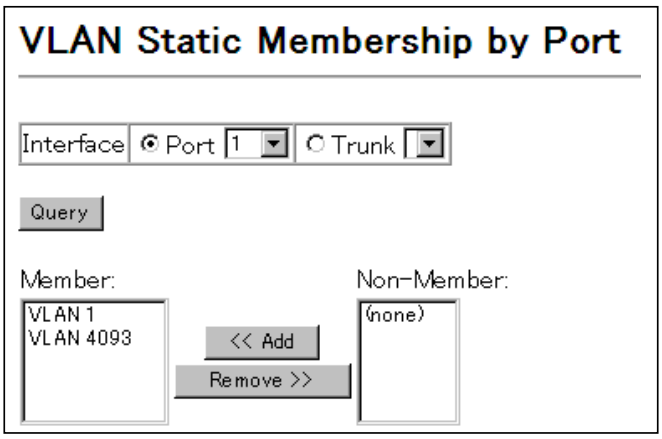
Non-Member

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。



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」（199 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。

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)

－ Access ― ポートをタグ無しインタフェースとして動作するように設定します。全てのフレームはタグ無しになります。

－ 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 (20-1000 centiseconds)	GARP Leave Timer (60-3000 centiseconds)	GARP LeaveAll Timer (500-18000 centiseconds)	Mode	Trunk Member
1	1	ALL	☑ Enabled	☐ Enabled	20	60	1000	Hybrid	
2	1	ALL	☑ Enabled	☐ Enabled	20	60	1000	Hybrid	
3	1	ALL	☑ Enabled	☐ Enabled	20	60	1000	Hybrid	
4	1	ALL	☑ Enabled	☐ Enabled	20	60	1000	Hybrid	
5	1	ALL	☑ Enabled	☐ Enabled	20	60	1000	Hybrid	
6	1	ALL	☑ Enabled	☐ Enabled	20	60	1000	Hybrid	

3.11.2 802.1Q トンネリングの設定

IEEE802.1Q トンネリング（QinQ）は、ネットワークで複数のカスタマーのトラフィックを伝送するサービスプロバイダを対象に設計された機能です。
サービスプロバイダは、他のカスタマーのトラフィックに影響を与えずに、各カスタマーの VLAN およびレイヤ 2 プロトコル設定を維持する必要があります。
QinQ トンネリングは、それらがサービスプロバイダのネットワークに入る時にサービスプロバイダ VLAN（SPVLAN）タグをカスタマーのフレームに挿入し、フレームがネットワークを去る時タグを取り去ることで実現します。

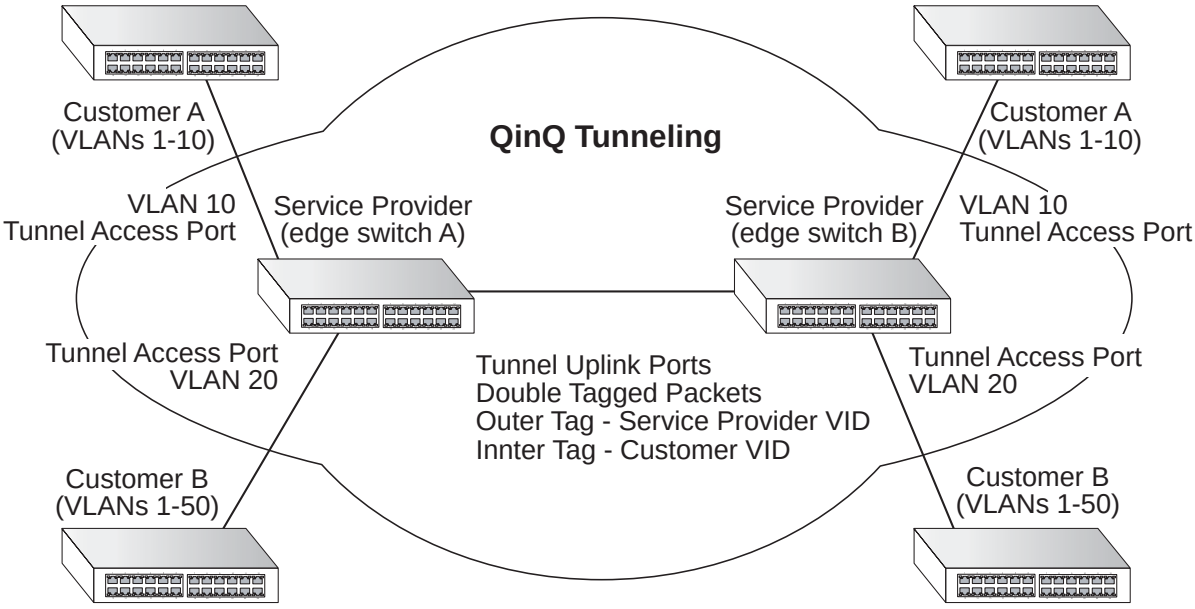
多くの場合、サービスプロバイダのカスタマーには、VLAN ID と、サポートの対象となる VLAN 数についての特定の要件があります。
同じサービスプロバイダネットワーク内の様々なカスタマーが必要とする VLAN の範囲は重複する場合があり、インフラストラクチャを介したカスタマーのトラフィックが混在する場合もあります。各カスタマーに、固有の範囲の VLAN ID を割り当てると、カスタマーの設定を制限することになり、IEEE802.1Q 仕様の 4096 という VLAN の制限を容易に超える可能性があります。

IEEE802.1Q トンネリング機能を使用することにより、サービスプロバイダは複数の VLAN を設定しているカスタマーを、1 つの VLAN を使用してサポートできます。カスタマーの VID は保持されるため、様々なカスタマーからのトラフィックは、同じ VLAN 内に存在するように見える場合でも、サービスプロバイダのインフラストラクチャ内では分離されています。
IEEE802.1Q トンネリングでは、VLAN 内 VLAN 階層を使用して、タグ付きパケットに再度タグ付けを行うことによって、VLAN スペースを拡張します。

ポートに QinQ トンネリングをサポートさせるには、トンネルポートモードに設定する必要があります。特定のカスタマーのサービスプロバイダ VLAN（SPVLAN）ID は、カスタマートラフィックがサービスプロバイダのネットワークへ入るエッジスイッチの QinQ トンネルアクセスポートにアサインします。それぞれのカスタマーは別々の SPVLAN を必要としますが、VLAN は全てのカスタマーの内部 VLAN をサポートします。
エッジスイッチからサービスプロバイダのメトロネットワークへトラフィックを渡す QinQ トンネリングアップリンクポートは、同じくこの SPVLAN へ加えられなくてはなりません。
アップリンクポートは、インバウンドトラフィックをサービスプロバイダネットワークへの異なるカスタマに運ぶ為に、複数の VLAN へ付加されることが可能です。

二重タグ付き（ダブルタキング）パケットが、サービスプロバイダの本機にあるの別のトランクポートに入ると、スイッチ内でパケットが処理される時に、外側のタグが外されます。
同じコアスイッチの別のトランクポートからパケットが送出される時には、同じ SPVLAN タグがパケットに再度追加されます。

パケットがサービスプロバイダ出力スイッチのトランクポートに入ると、スイッチでパケットが内部処理される時に、外側のタグが再度除去されます。ただし、パケットがエッジスイッチのトンネルポートからカスタマーネットワークに送信される時には、SPVLAN タグは追加されません。カスタマーネットワーク内の元の VLAN 番号を保持するために、パケットは通常の IEEE802.1Q タグ付きフレームとして送信されます。



トンネルアクセスポートへ入るパケットのレイヤ 2 フロー

QinQ トンネルポートはタグ付きまたはタグ無しパケットのいずれかを受信します。
入力パケットがいくつのタグを持つかには関わらず、タグ付きポートとして扱われます。
入力プロセスはソースとディスティネーションを検索します。
両方の検索が成功したら、入力プロセスはパケットをメモリへ書き込み、出力プロセスへパケットを伝えます。

QinQ トンネルポートへ入ったパケットは以下の方法で処理されます。

（1）既にいくつのタグを保持しているかに関わらず、新しい SPVLAN タグは全ての入力パケットに付加されます。
この入力プロセスは外のタグ（SPVLAN）を組み立て、デフォルト VLAN ID とタグ識別子に基づき挿入します。
この外側のタグはパケットの学習とスイッチングに使用されます。もしこれがタグ付きまたはプライオリティタグ付きパケットである場合、内側のタグのプライオリティは外側のタグにコピーされます。

（2）ソース、ディスティネーション検索が成功した後、入力プロセスは、2 つのタグと共にスイッチングプロセスへパケットを送ります。
もし入力パケットがタグ無しの場合、外側のタグは SPVLAN タグとなり、内側のタグはダミーとなります。(8100 0000)
もし入力パケットがタグ付きである場合、外側のタグは SPVLAN タグになり、内側のタグは CVLAN タグとなります。

（3）スイッチングプロセスを通るパケット分類の後、パケットは 1 つのタグ（外側のタグ）または 2 つのタグと共にメモリへ書き込まれます。

（4）スイッチはパケットを適切な出力ポートへ送ります。

（5）もし出力ポートが SPVLAN のタグ無しメンバーである場合、外側のタグは取り外されます。タグ付きメンバーである場合、発信パケットは 2 つのタグを持ちます。

トンネルアップリンクポートへ入るパケットのレイヤ 2 フロー

アップリンクポートは以下のパケットの 1 つを受け取ります。

- タグ無し
- 1 つのタグ付き（CVLAN または SPVLAN）
- 2 つのタグ付き（CVLAN+SPVLAN）

入力プロセスはソースとディスティネーションを検索します。
両方の検索が成功したら、入力プロセスはパケットをメモリへ書き込み、出力プロセスへパケットを伝えます。

QinQ アップリンクポートへ入ったパケットは以下の方法で処理されます。

（1）入力パケットがタグ無しである場合、PVID VLAN ネイティブタグが付加されます。

（2）入力パケット（1 つまたは 2 つのタグ付き）イーサタイプがアップリンクポートの TPID と一致しない場合、VLAN タグはカスタマ VLAN（CVLAN）タグであると決定されます。アップリンクポートの PVID VLAN ネイティブタグがパケットに付加されます。
この外側のタグは、サービスプロバイダネットワークで、パケットの学習とスイッチングに使われます。TPID はポートベースで設定され、検証は無効にすることができません。

（3）入力パケット（1 つまたは 2 つのタグつき）のイーサタイプがアップリンクポートの TPID と一致する場合、新しい VLAN タグは付加されません。
アップリンクポートが入ってきたパケットの外側の VLAN のメンバーでない場合、イングレスフィルタリング有効時であればパケットは破棄されます。
イングレスフィルタリングが有効でない場合、パケットはフォワードされます。
VLAN が VLAN テーブル上に無い場合、パケットは破棄されます。

（4）ソース、ディスティネーション探索に成功後、パケットは 2 つのタグが付けられます。スイッチは、0x8100 の TPID を、入力パケットに二重のタグが付けられていることを示す為に使用します。
二重タグ付き入力パケットの外側のタグがポートの TPID と一致し、内側のタグが 0x8100 である場合、これは二重タグ付きパケットとして取り扱われます。
シングルタグ付きパケットが、TPID として 0x8100 を持ち、ポート TPID が 0x8100 ではない場合、新しい VLAN タグが付加され、これもまた二重タグ付きパケットとして取り扱われます。

（5）ディスティネーション検索が失敗した場合、パケットは、外タグの VLAN の全てのメンバーポートへ送信されます。

（6）パケット分類の後、パケットは、シングルタグ付きまたは二重タグ付きパケットとして処理されるために、メモリへ書き込まれます。

（7）スイッチはパケットを適切な出力ポートへ送信します。

（8）出力ポートが SPVLAN のタグ無しメンバーである場合、外側のタグは取り外されます。タグ付きメンバーである場合、出て行くパケットは 2 つのタグを持ちます。

QinQ の設定制限

- アップリンクポートのネイティブ VLAN は SPVLAN としては使用できません。SPVLAN がアップリンクポートのネイティブ VLAN である場合、アップリンクポートは SPVLAN のタグ無しメンバーになります。パケットが送信される時、外側の SPVLAN タグは取り外されます。
- QinQ 設定がトランクポートグループと整合性がある限り、静的トランクポートグループは、QinQ トンネルポートと両立できます。
- ネイティブ VLAN（VLAN1）は通常、転送されたフレームに付加されません。設定不良の危険を減少する為、カスタマトラフィックの SPVLAN タグを VLAN1 にするのは避けてください。サービスプロバイダネットワークのデータ VLAN の代わりに、VLAN 1を管理 VLAN として使用してください。
- レイヤ 2 とレイヤ 3 スイッチングには若干の固有互換性があります。
  - トンネルポートは IP アドレスコントロールリストをサポートしません。
  - レイヤ 3 Quality of Service（QoS）ACL とレイヤ 3 情報に関連するその他の QoS 機能はトンネルポートでサポートされません。
  - ポートが IEEE802.1Q トランクポートとして設定されている場合、スパニングツリーの BPDU フィルタリングは、インタフェースで自動的に無効となります。

QinQ の一般的な設定ガイドライン

（1）スイッチを QinQ モードに設定します。（P208 を参照）

（2）トンネルアクセスポートの Tag Protocol Identifier （TPID）値を設定します。このステップは接続されているクライアントが 802.1Q タグ付きフレームの識別に、非標準 2 バイトイーサタイプを使用している場合に必要となります。デフォルトイーサタイプ値は 0x8100 です。（P208 を参照）

（3）SPVLAN として定義されたカスタマサービスプロバイダ VLAN を作成します。（P198 を参照）

（4）QinQ トンネルアクセスポートを 802.1Q トンネルモードに設定します。（P209 を参照）

（5）QinQ トンネルアクセスポートをタグ無しとして SPVLAN に加入させます（P199 を参照）

（6）QinQ トンネルアクセスポートに SPVLAN ID をネイティブ VID として設定します。（P202 を参照）

（7）QinQ トンネルアップリンクポートを 802.1Q トンネルアップリンクモードに設定します。（P209 を参照）

（8）QinQ トンネルアップリンクポートをタグ付きメンバーとして SPVLAN に加入させます。（P199 を参照）

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。**

機能解説

- 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。**
- **スイッチ上の全てのポートは同じイーサタイプに設定されます。**

設定・表示項目

802.1Q Tunnel Status

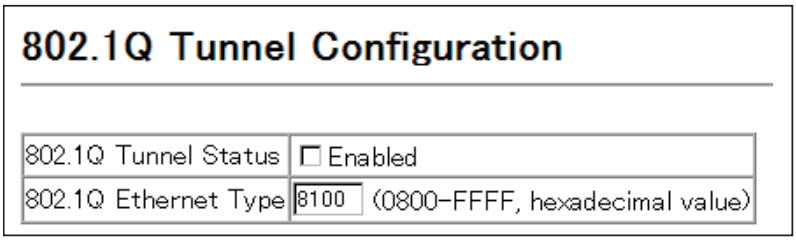
スイッチを QinQ **モードに設定し、**802.1Q **の** TPID **を適用し、ポートを** QinQ **のトンネルポートとして構成できるよう許可します。デフォルトではスイッチはノーマルモードとして機能します。**

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。**
ステータス（Enable **へチェック）とイーサタイプを入力し** [Apply] **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。

機能解説

- VLAN ポート設定または VLAN トランク設定画面を使用し、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てください。
- トンネルポートの設定を行う前に 802.1Q トンネル設定画面を使用し、スイッチを QinQ モードに設定してください。（P208 「QinQ トンネリングの有効」を参照）

設定・表示項目

Mode

ポートの VLAN モードを設定します（初期設定 : 無効）

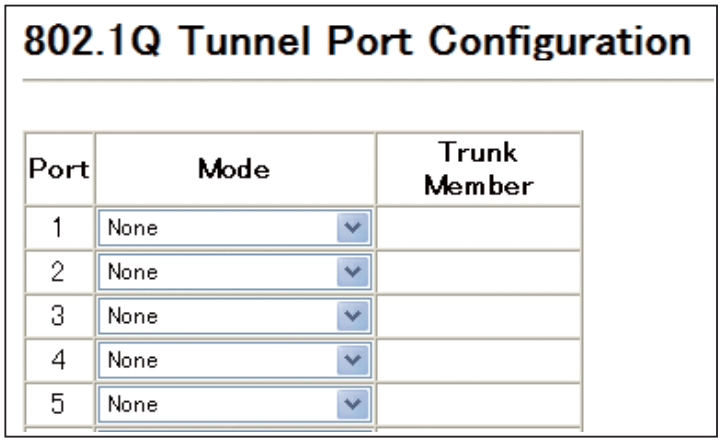
－ None －通常 VLAN モードで動作

－ 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。

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。各ポートのモードを選択し、[Apply] をクリックします。



3.11.3 トラフィックセグメンテーション

ローカルネットワークおよびサービスプロバイダへのアップリンクポート上で、異なるクライアントからダウンリンクポートを通過するトラフィックに、より厳しいセキュリティが必要とされる際、個々のクライアントセッションのトラフィックを隔離するためにポートベーストラフィックセグメンテーションを使用できます。

それぞれのクライアントに属するトラフィックは、割り当てられたダウンリンクポートに隔離されます。

スイッチは、クライアントの割り当てられたアップリンクポート全体に渡る通過を、他のクライアントにアサインされたアップリンクポートから孤立させるようにする、または異なるクライアントへセキュリティの危険が低いアップリンクポートへのアクセスの共有を許可し他のクライアントを使用してトラフィックがアップリンクポートを通過・転送可能にする、のいずれかに設定することができます。

トラフィックセグメンテーションのグローバル設定

このページでは、トラフィックセグメンテーションを有効にすることができます。
異なったクライアントセッションにアサインされたアップリンクポート間のトラフィックをブロックあるいは転送することができます。

設定・表示項目

Traffic Segmentation Status

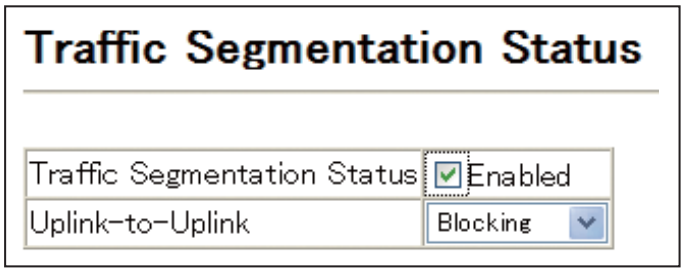
ポートベーストラフィックセグメンテーションを有効にします（初期設定：無効）

Uplink-to-Uplink

異なったクライアントセッションに割り当てられたアップリンクポート間でトラフィックの転送を行うか否かの設定をおこないます。（初期設定：Blocking）

設定方法

[VLAN] → [Traffic Segmentation] をクリックします。
"traffic segmentation status" または "Uplinnk to Uplink" を設定し [Apply] をクリックします。



トラフィックセグメンテーションセッションの設定

このページでは、クライアントセッションを作成します。
また、それぞれのセッションと関連するトラフィックにダウンリンク / アップリンクポートをアサインします。

設定・表示項目

Session ID

トラフィックセグメンテーションセッション（範囲：1-15）

Direction

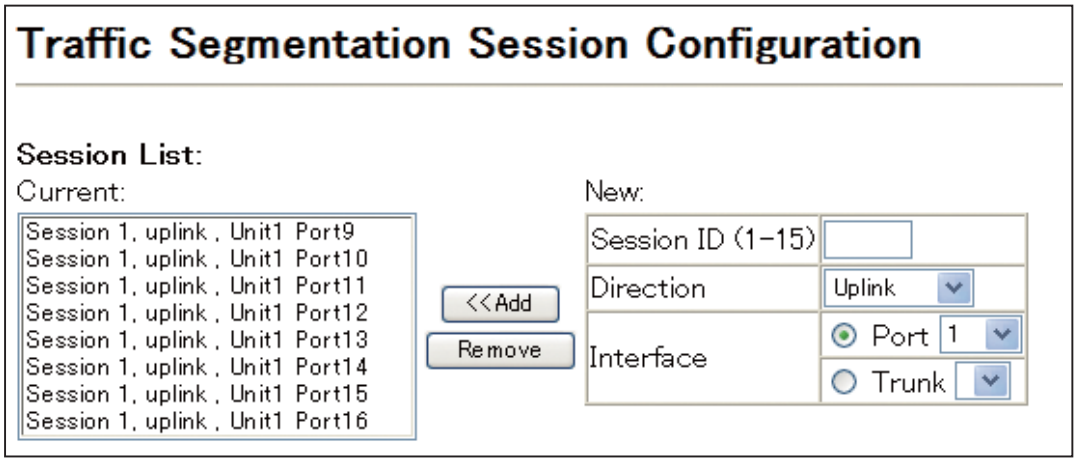
アップリンクまたはダウンリンクインタフェース

Interface

トラフィックセグメンテーションセッションにアサインされるポートまたはトランクスイッチ ASIC リミテーションにより、いずれかのグループメンバーがアップリンクまたはダウンリンクインタフェースとして設定された場合、ポート 1-8、9-16、17-24 はグループになります。

設定方法

[VLAN] → [Traffic Segmentation] → [Session Configuration] をクリックします。
セッション番号を設定し、アップリンクとダウンリンクのどちらが使われるかを指定します。



3.11.4 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。

本機には複数のプライマリ VLAN を設定でき、また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。(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 (P210) 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 (P215) 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 (P214) 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。

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

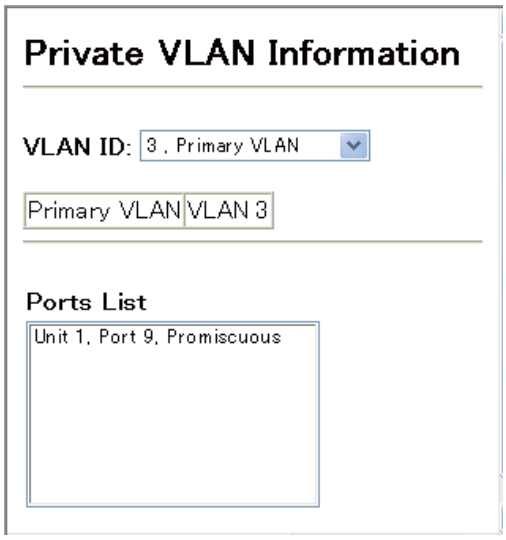
表示している VLAN ID に関連付けされている VLAN。プライマリ VLAN の場合は自身の VLAN ID を、コミュニティ VLAN の場合は関連付けされているプライマリ VLAN ID を、又独立 VLAN はスタンドアロンの VLAN を表示します。

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（2-4094）

Type

プライベート VLAN には次の 3 つの種類があります。

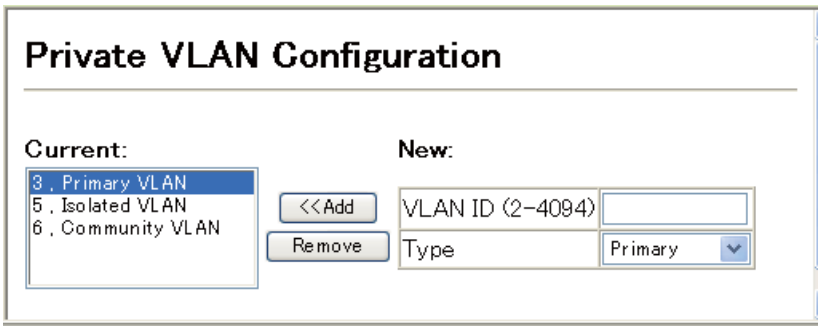
- Primary ― セカンダリ (コミュニティ) VLAN 内で、無差別ポートとコミュニティポート間でデータをやり取りします。
- Community ― 関連付けたプライマリ VLAN 内で、無差別ポートとコミュニティポート間でデータをやり取りします。

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、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（2-4094）

Association

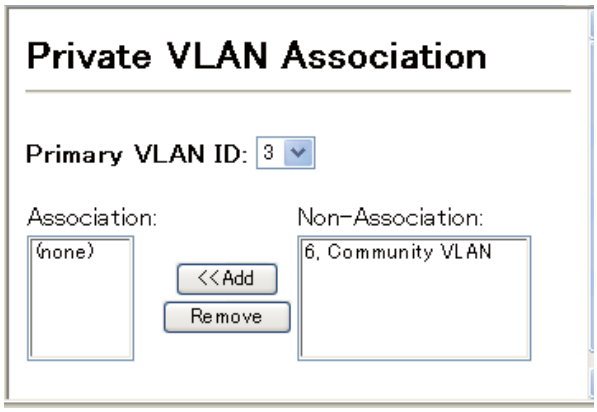
選択したプライマリ VLAN と既に関連付けられているコミュニティ VLAN

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/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

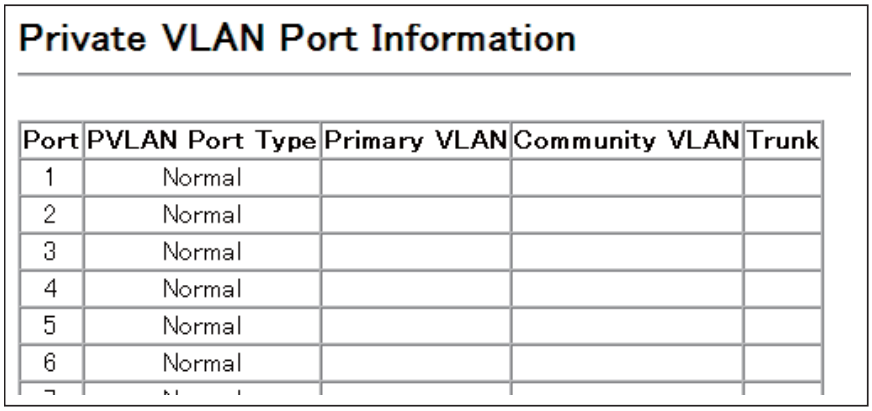
コミュニティ VLAN。コミュニティポート間、又はコミュニティポートと指定した無差別ポート間でデータをやり取りします。

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	Trunk
1	Normal			
2	Normal			
3	Normal			
4	Normal			
5	Normal			
6	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/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

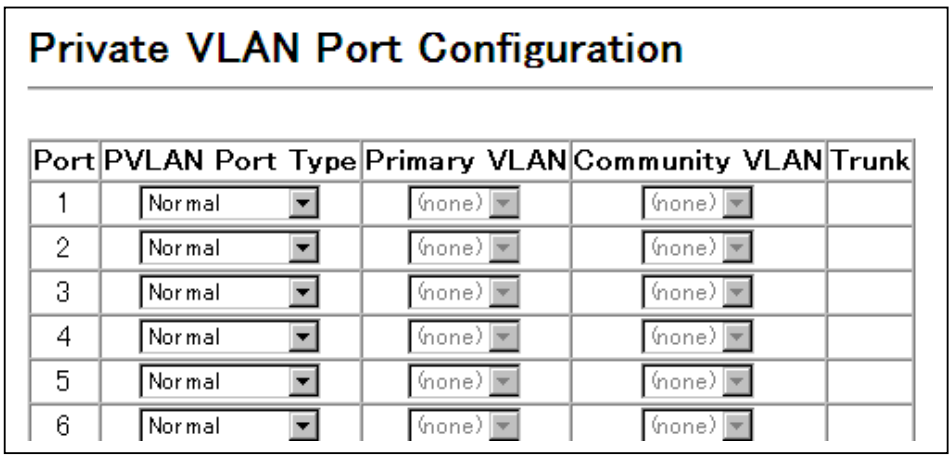
関連付けたセカンダリ (コミュニティ) VLAN 内で、無差別ポート同士、又は無差別ポートとコミュニティポート間でデータをやり取りします。

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。



3.11.5 プロトコル VLAN

多数のプロトコルをサポートすることを要求されるネットワーク装置は、通常の VLAN **では容易にグループ分けをおこなうことができません。**
これには、非標準のデバイスが特定のプロトコルに参加する全てのデバイスをカバーするように、異なった VLAN **間へトラフィックを渡すことが要求されます。**
この種類の設定はセキュリティ、アクセシビリティといった VLAN **の基本的な利益をユーザから奪います。**
これらの問題を避けるために、本機ではプロトコルベース VLAN **を設定できます。**
これにより物理的ネットワークをそれぞれ必要とされるプロトコルの論理 VLAN **グループへ分けます。ポートでフレームが受信された時、その** VLAN **メンバーシップはインバウンドパケットで使われているプロトコルタイプによって決定されます。**

機能解説

プロトコルベース VLAN **の設定は以下のステップでおこなってください。**

(1) **最初に使用したいプロトコルの** VLAN **グループを設定します。(**P198 **参照)**
それぞれの主要なプロトコルがネットワーク上で送受信される VLAN **は別個の** VLAN **設定をおこなうことを推奨します。(これは必須ではないです)**
この段階ではポートメンバーの追加を行わないで下さい。

(2) "Protocol VLAN Configuration" **ページで、**VLAN **へ割り当てたいプロトコルそれぞれのプロトコルグループを作成します。**

(3) "Protocol VLAN Port Configuration" **ページを使用し、それぞれのインタフェースのプロトコルを適切な** VLAN **へマップします。**

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)

Frame Type

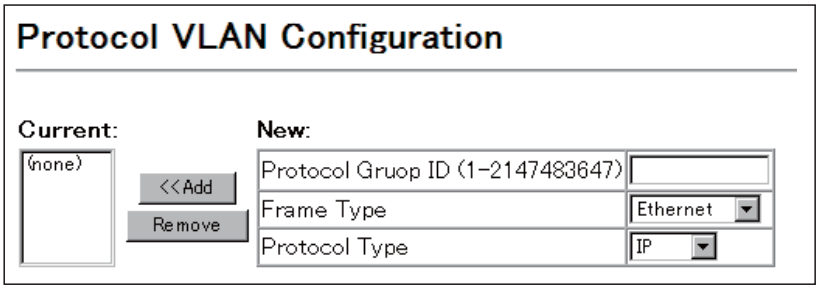
このプロトコルで使用されるフレームタイプを選択してください。
(範囲: Ethernet、RFC1042、、LLC Other)

Protocol Type

マッチするプロトコルタイプを指定します。(利用可能なオプション:IP、ARP、RARP)
フレームタイプに LLC Other **が選択される場合、利用可能なプロトコル種別は** IPX Raw **のみです。**

設定方法

[VLAN] → [Protocol VLAN] → [Configuration] **をクリックします。プロトコルグループ** ID **を入力、フレームタイプ、プロトコルタイプを選択し、**[Apply] **をクリックします。**



プロトコルを VLAN へマッピング

プロトコル VLAN グループを VLAN にマッピングします。

機能解説

- プロトコルベース VLAN を作成する際、この設定画面を使用してのみインタフェースの割り当てが行えます。もし、"VLAN Static Table"（P199 参照）や "VLAN Static Membership "(P201 参照) 等他の VLAN メニューを使用してインタフェースを割り当てた場合、これらインタフェースは関連付けられた VLAN の全てのトラフィックタイプを受け入れます。
- プロトコル VLAN へアサインされたポートへフレームが入ってくる時、次の方法で処理されます。
  - フレームがタグ付きの場合、タグフレームに適用された標準ルールに従い処理されます。
  - フレームがタグ無しで、プロトコルタイプが一致した場合、フレームは適切な VLAN へ転送されます。
  - フレームがタグ無しで、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 へ転送されます。

設定・表示項目

Protocol Group ID

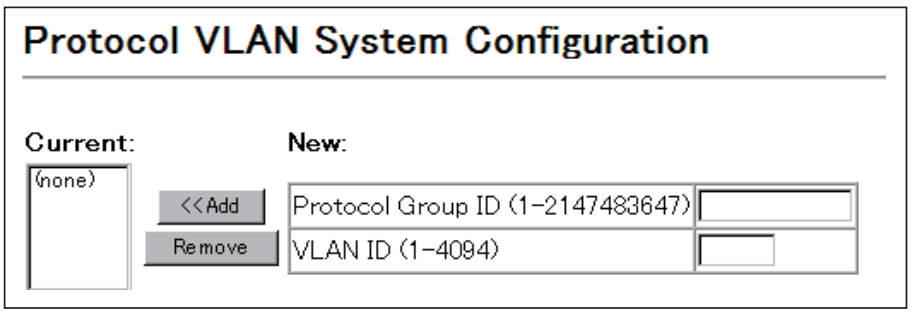
プロトコル VLAN グループに割り当てられたプロトコルグループ ID（範囲：1-2147483647）

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] → [Configuration] をクリックします。プロトコルグループ ID、フレームタイプ、プロトコルタイプを入力し、[Apply] をクリックします。



3.11.6 VLAN ミラーリング

リアルタイム解析のため、1 つまたはそれ以上のソース VLAN から、ターゲットポートへトラフィックをミラーリングをすることが出来ます。

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、ソース VLAN のトラフィックを調査することが可能です。

機能解説

- **ソース VLAN の全てのアクティブポートは入力トラフィックのみモニタされます。**
- **全ての VLAN ミラーセッションは、同一のターゲットポートをし共有します。**
- **VLAN ミラーリングとポートミラーリングの両方が有効である場合、それらは同一のターゲットポートを使用します。**
- **VLAN ミラーリングとポートミラーリングの両方が有効である場合、ターゲットポートは、2 倍のミラーされたパケットを受信します。1 つはソースミラーポートで、ソースミラー VLAN からも再度受信します。**

[注意]　スパニングツリー BPUD パケットは、ターゲットポートへミラーされません。

設定・表示項目

Mirror Sessions

現在のミラーセッションのリストを表示します。

Source VLAN

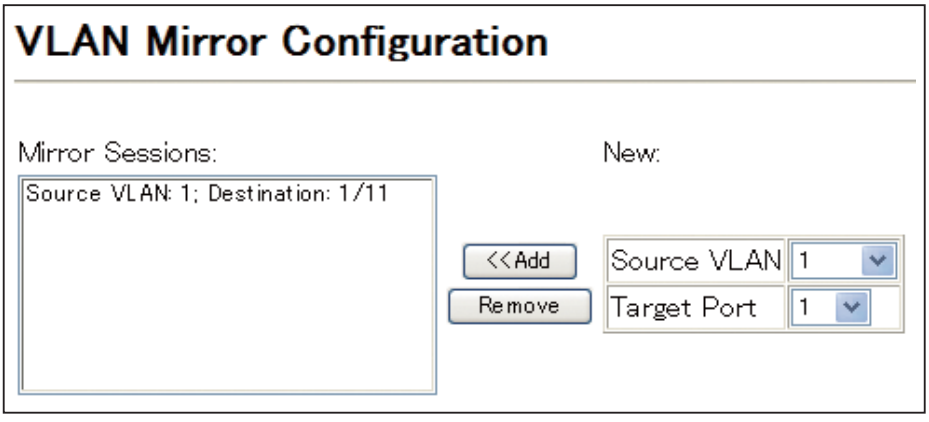
トラフィックのモニタがおこなわれる VLAN（範囲：1 － 4094）

Target Port

ソース VLAN からミラートラフィックを受信する行先ポート

設定方法

[VLAN] → [VLAN Mirror Configuration] **をクリックします。**
ソース VLAN を選択、ソース VLAN のメンバー以外のポートからターゲットポートを選択し、[Apply] **をクリックします。**



3.11.7 IP サブネット VLAN

ポートベースの分類を使用する際、ポートで受信された全てのタグ無しフレームはその VID（PVID）**がポートと結び付けられる** VLAN **に属しているとして分類されます。**
IP **サブネットベース** VLAN **分類が有効である時、タグ無し入力フレームのソースアドレスは。**IP **サブネットから** VLAN **へのマッピングテーブルと照らし合わされます。**
サブネットのエントリが発見された場合、これらのフレームはエントリで示された VLAN **に割り当てられます。**
IP **サブネットがマッチしない場合、タグ無しフレームは受信ポートの** VLAN ID（PVID）**に属すると分類されます。**

機能解説

- **それぞれのサブネットは** 1 **つの** VLAN ID **にのみマップされることが可能です。**
  IP **サブネットは** IP **アドレスとマスクから成ります。**
- **ポートでタグ無しフレームが受信された場合、ソース** IP **アドレスは** IP **サブネットから** VLAN **へのマッピングテーブルと照らし合わされ、エントリが見つかると対応する** VLAN ID **がフレームに割り当てられます。マッピングが見つからない場合、受信ポートの** PVID **がフレームに割り当てられます。**
- IP **サブネットはブロードキャストまたはマルチキャスト** IP **アドレスにはなれません。**
- MAC **ベース、**IP **サブネットベース、プロトコル** VLAN **が同時にサポートされる時、このシーケンスではプライオリティが適用され、最後にポートベース** VLAN **になります。**

設定・表示項目

IP Address

サブネットの IP **アドレス。**

Subnet Mask

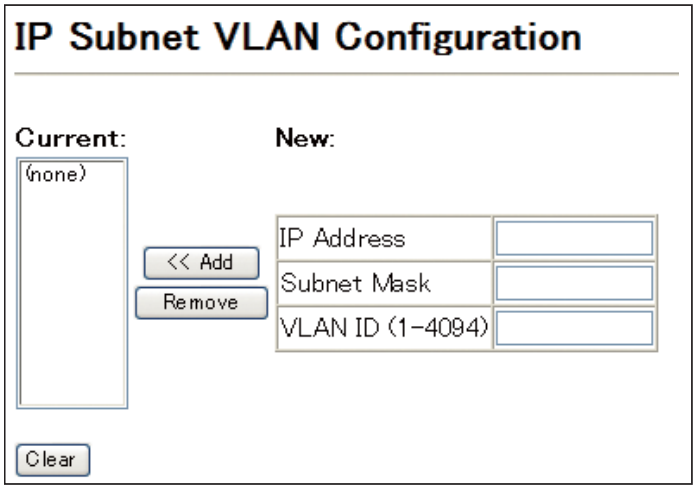
IP **サブネットのホストアドレスビットを識別します。**

VLAN ID

IP **サブネットとマッチしたトラフィックは** VLAN **は転送されます。（範囲：**1-4094）

設定方法

[VLAN] → [IP Subnet VLAN Configuration] をクリックします。
IP アドレス、サブネットマスク、VLAN ID を入力し、[Apply] をクリックします。



3.11.8 MAC ベース VLAN

MAC ベース VLAN 機能は、ソース MAC アドレスに従って VLAN ID を入力タグ無しフレームへ割り当てます。
MAC ベース VLAN 分類が有効である場合、ポートで受信されたタグ無しフレームは、フレームのソース MAC アドレスにマップされる VLAN へ割り当てられます。
MAC アドレスが一致しない時、タグ無しフレームは受信ポートのネイティブ VLAN ID（PVID）が割り当てられます。

機能解説

- MAC-to-VLAN マッピングは本機の全てのポートへ適用されます。
- ソース MAC アドレスは 1 つの VLAN ID へのみマップされることが可能です。
- 設定された MAC アドレスはブロードキャストまたはマルチキャストアドレスにはなれません。
- MAC ベース、IP サブネットベース、プロトコル VLAN が同時にサポートされる時、このシーケンスではプライオリティが適用され、最後にポートベース VLAN になります。

設定・表示項目

MAC Address

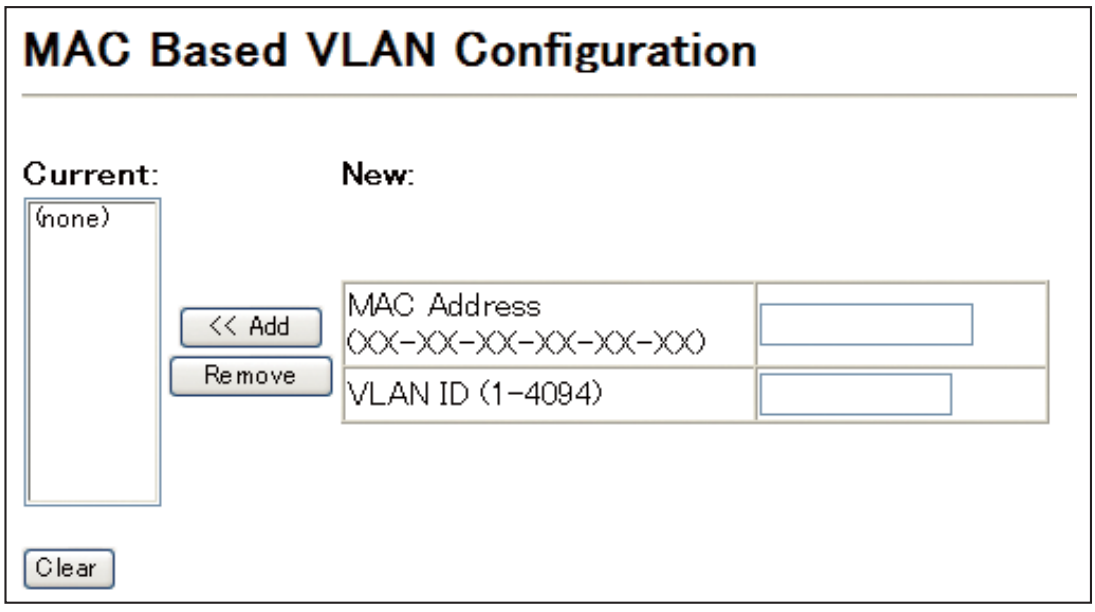
特定の VLAN にマップされるソース MAC アドレス

VLAN ID

指定されたソース MAC アドレスと一致する入力トラフィックが転送される VLAN
（範囲：1-4094）

設定方法

[VLAN] → [MAC-based VLAN Configuration] をクリックします。
MAC アドレス、VLAN ID を入力し、[Apply] をクリックします。



3.12 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。

3.12.1 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

ポートまたはトランクを指定

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

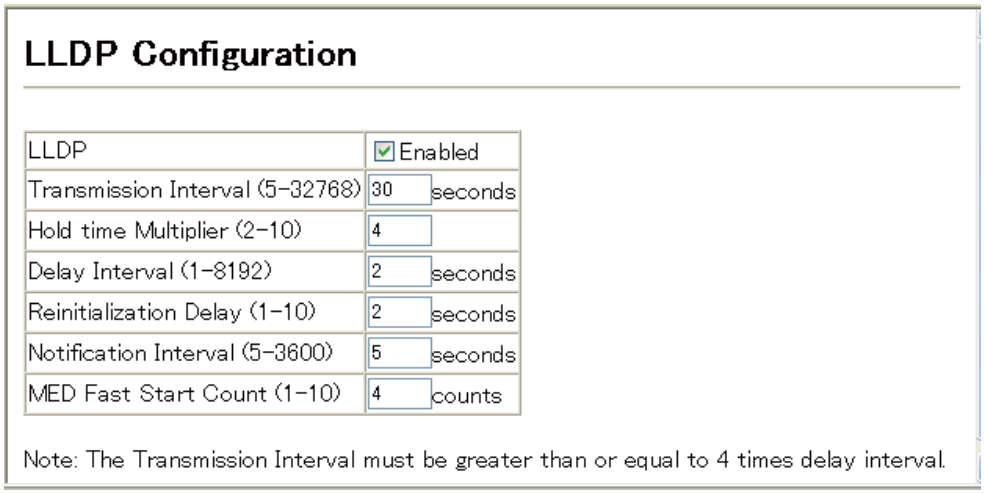
（範囲：5 ー 3600 秒　初期設定：5 秒）

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。



3.12.2 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

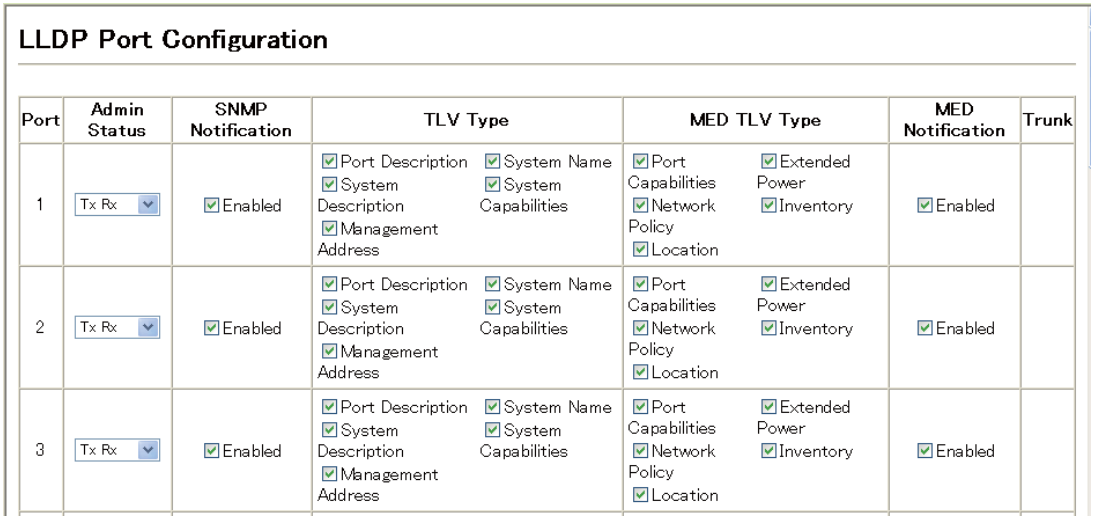
LLDP-MED の変更について SNMP トラップ通知の送信を有効にします（初期設定：有効）

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

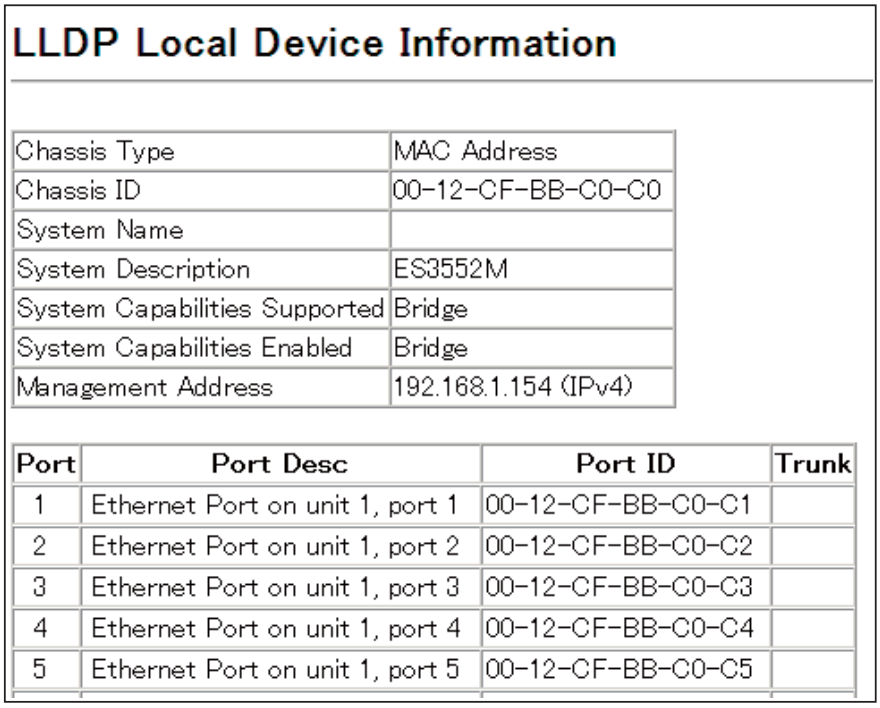
Port	Admin Status	SNMP Notification	TLV Type	MED TLV Type	MED Notification	Trunk
1	Tx Rx	☑ Enabled	☑ Port Description ☑ System Name ☑ System Description ☑ System Capabilities ☑ Management Address	☑ Port Capabilities ☑ Extended Power ☑ Network Policy ☑ Inventory ☑ Location	☑ Enabled	
2	Tx Rx	☑ Enabled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

3.12.3 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-BB-C0-C0
System Name	
System Description	ES3552M
System Capabilities Supported	Bridge
System Capabilities Enabled	Bridge
Management Address	192.168.1.154 (IPv4)

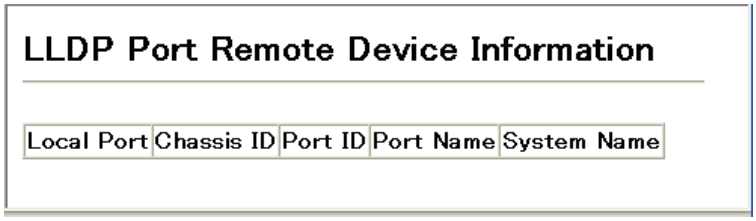
Port	Port Desc	Port ID	Trunk
1	Ethernet Port on unit 1, port 1	00-12-CF-BB-C0-C1	
2	Ethernet Port on unit 1, port 2	00-12-CF-BB-C0-C2	
3	Ethernet Port on unit 1, port 3	00-12-CF-BB-C0-C3	
4	Ethernet Port on unit 1, port 4	00-12-CF-BB-C0-C4	
5	Ethernet Port on unit 1, port 5	00-12-CF-BB-C0-C5	

3.12.4 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

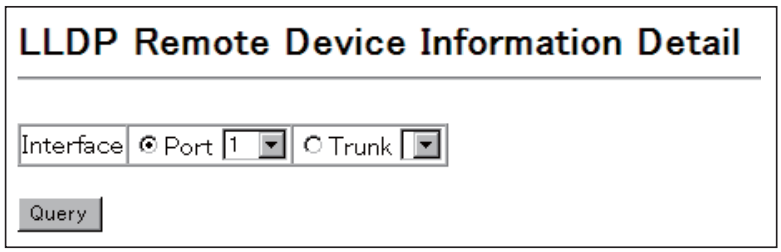
Local Port	Chassis ID	Port ID	Port Name	System Name

3.12.5 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。

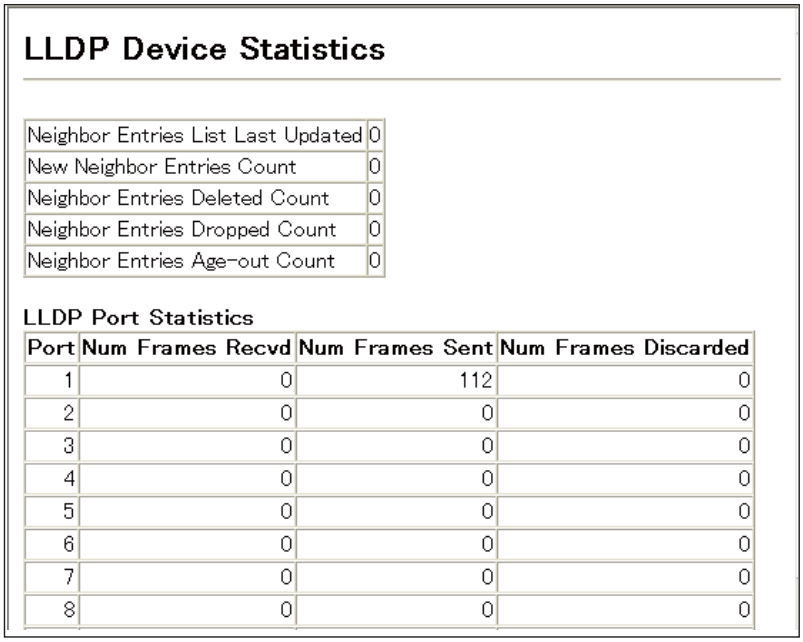


3.12.6 デバイス統計値の表示

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。

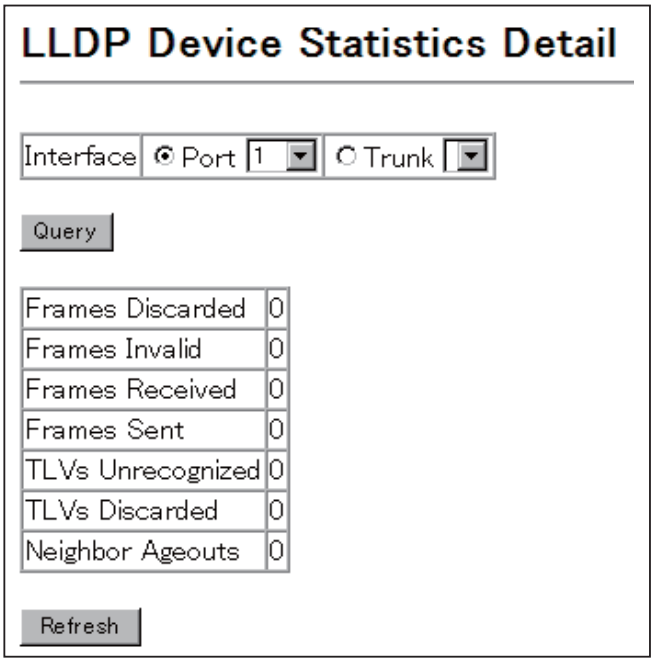


3.12.7 デバイス統計値詳細の表示

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。**



3.13 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。

3.13.1 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

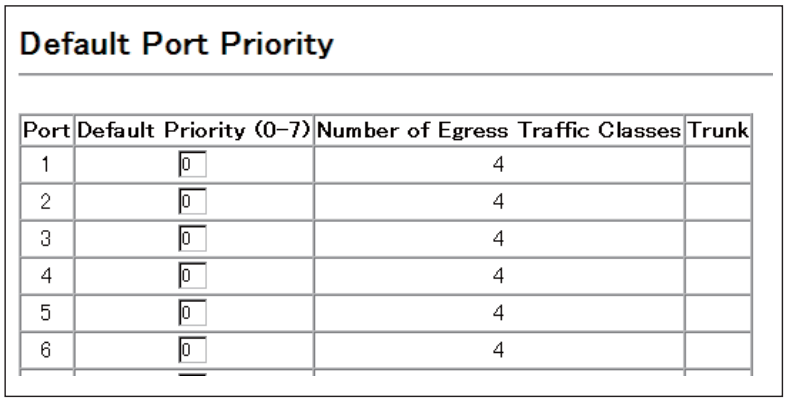
（範囲 :0 - 7、初期設定 :0）

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

Priority

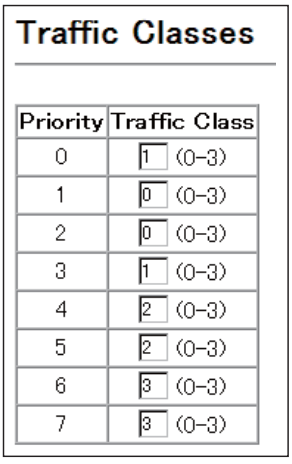
CoS 値（範囲 :0 から 7、7 が最高プライオリティ）

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

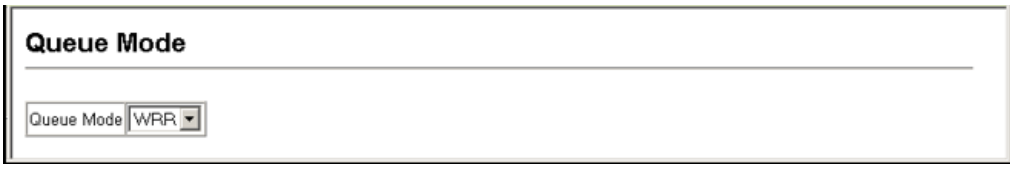
Weighted Round-Robin ではイングレスポートの帯域を それぞれの 0-3 のキューに対して 1, 2, 4, , 8 のスケジューリングウェイトを設定し共有します。

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表示

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。P232 「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。

[注意]　本機ではキューサービスウェイトの設定は出来ません。
ウェイトは 1,2,4,8 がキュー 0 から 3 へそれぞれ固定されています。

設定・表示項目

WRR Setting Table

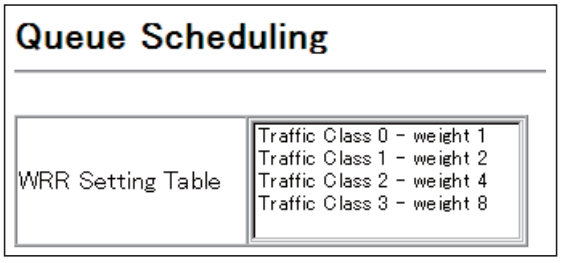
各トラフィッククラス（キュー）のウェイトの値を表します。

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。



3.13.2 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 :

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。

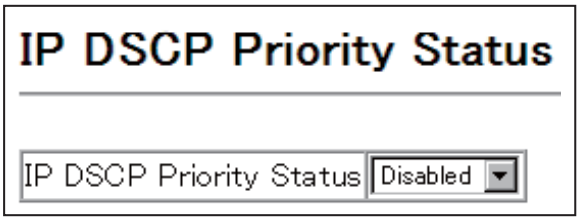
設定・表示項目

IP DSCP Priority Status

- Disabled ー 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 ー 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	0
8	1
10, 12, 14, 16	2
18, 20, 22, 24	3
26, 28, 30, 32, 34, 36	4
38, 40, 42	5
48	6
46,56	7

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。

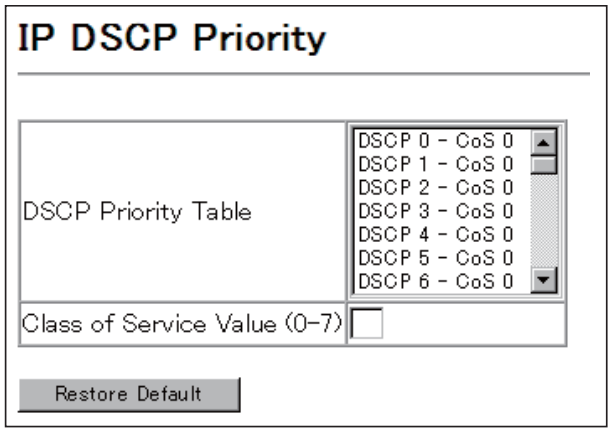
Class of Service Value

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。



3.14 Quality of Service

3.14.1 Quality of Service の設定

ここ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。

QoS パラメータの設定

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）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。

（2）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。

（3）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。

（4）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。

（5）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。

クラスマップの設定

- クラスマップは以下の手順で設定します。
  - Class Map ページを開き、[Add Class] をクリックします。
  - Class Configuration ページが開きます。“ Class Name ”フィールドへ入力し、[Add] をクリックします。
  - Match Class Settings ページが開きます。アクセスリスト、DSCP または IP Precedence 値に基づき、このクラスのトラフィックタイプを指定し、選択したトラフィック基準の隣の [Add] ボタンをクリックします。
    入力トラフィックをクラスマップに割り当てる際、最大 16 項目を指定することが可能です。
- クラスマップはポリシーマップ（P240）と共にサービスポリシー（P243）を作成する為に使用されます。
  1 つ以上のクラスマップをポリシーマップへ割り当てることが可能です。

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）

IP DSCP

IP DSCP 値（範囲：0-63 文字）

IP Precedence

IP Precedence 値（範囲：0-7 文字）

VLAN

VLAN（範囲：1-4094）

Add

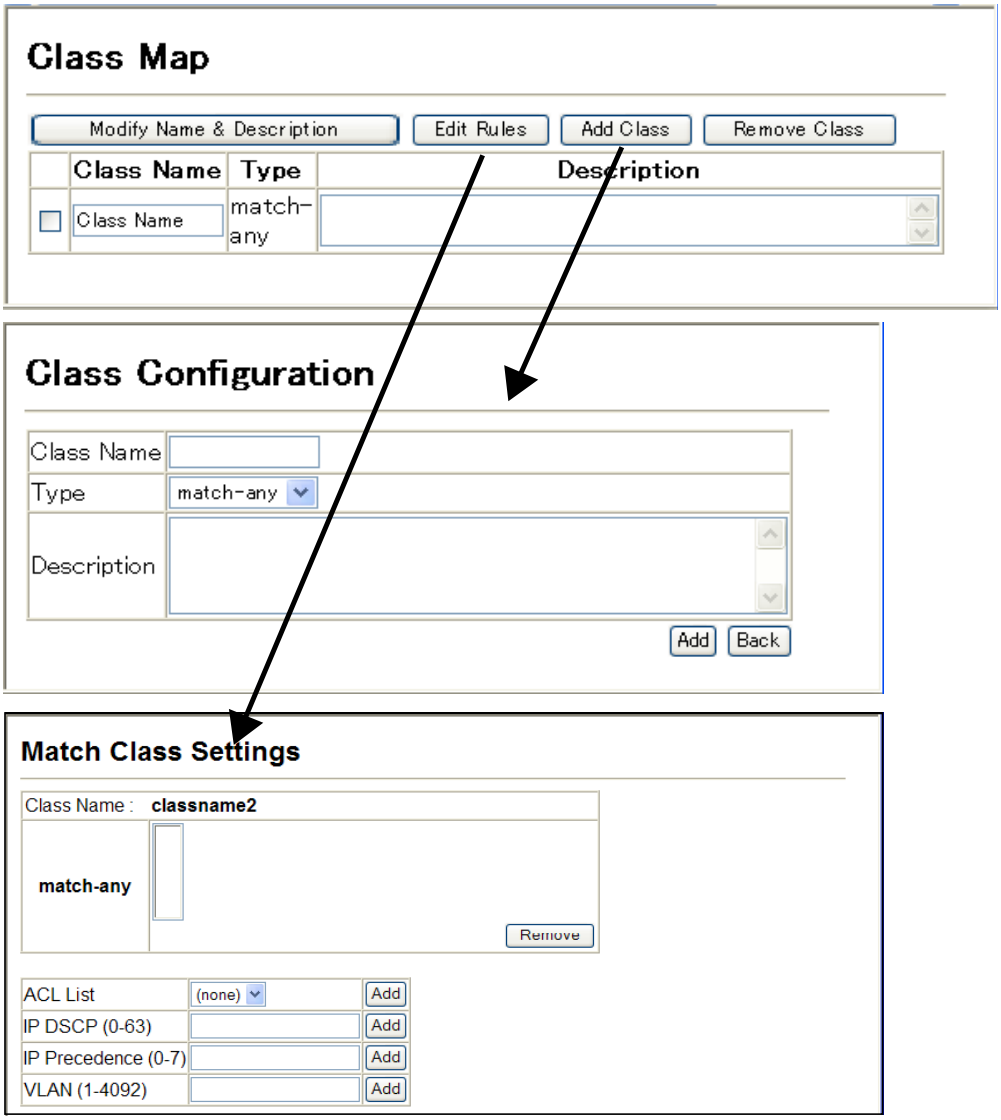
クラスマップに追加します。１つのクラスにつき、最大 16 個まで登録できます。

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（P238 「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（P231 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

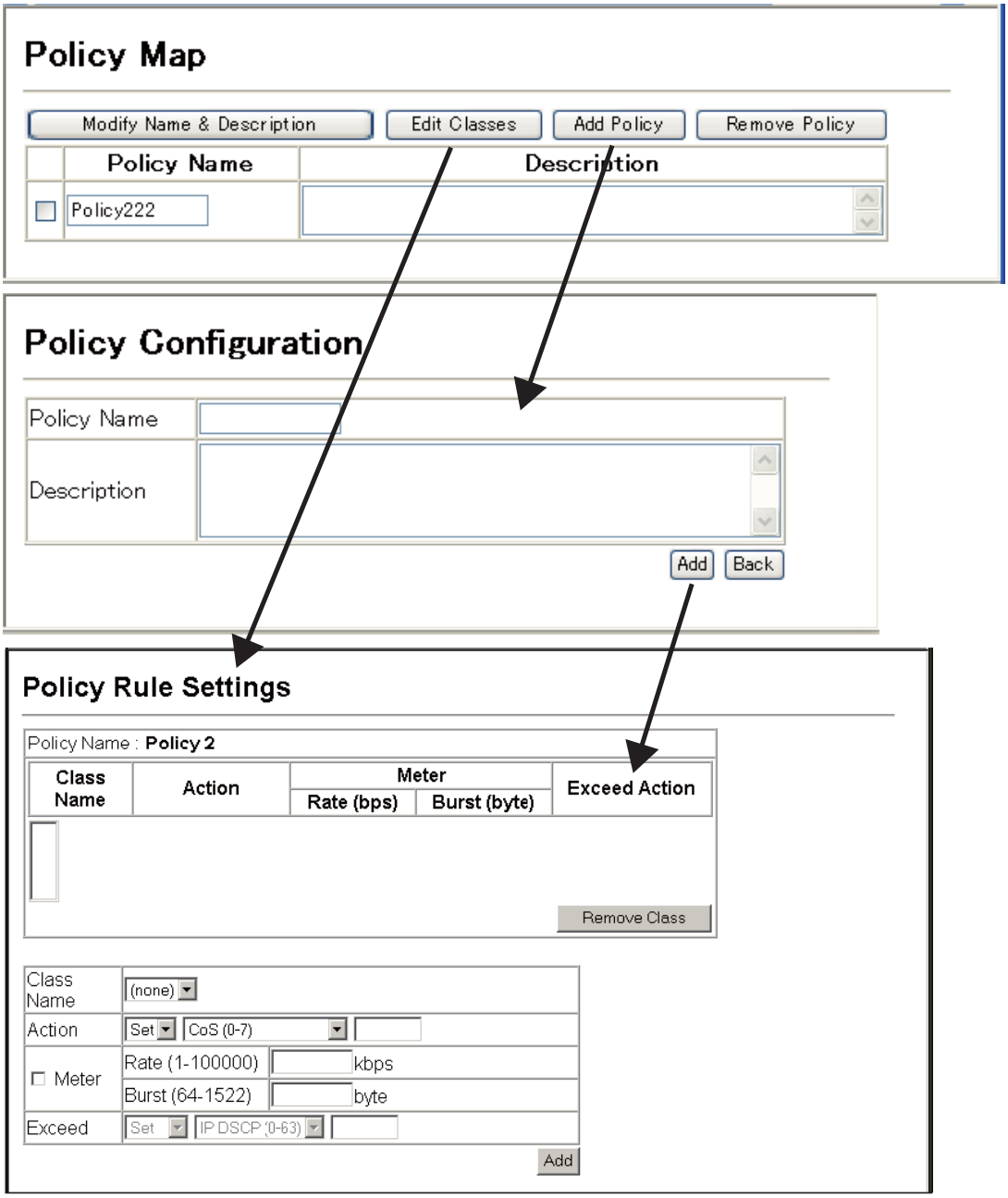
- Drop - **条件に一致しないトラフィックを破棄する**

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

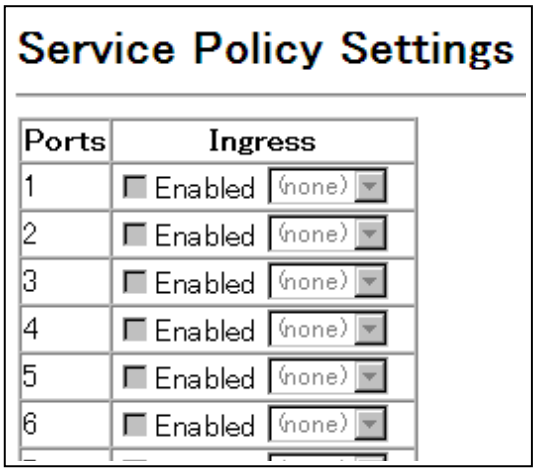
指定したポートでポリシーマップを有効にします。

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。



3.15 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 ～ 4094）

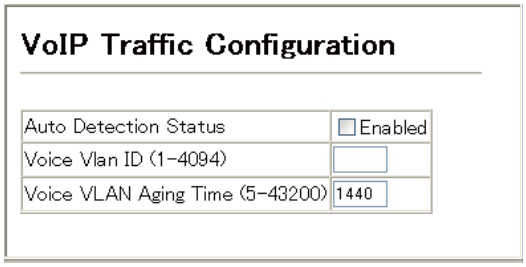
Vioce VLAN Aging Time

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。（初期設定：OUI）

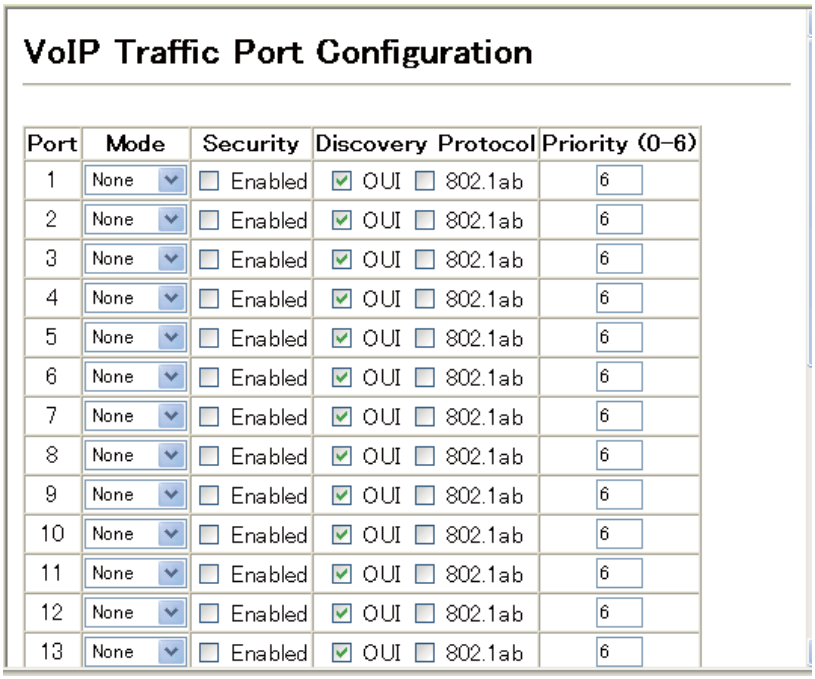
- OUI － VoIP デバイスからのトラフィックは送信元 MAC アドレスの Organizationally Unique Identifier（OUI）によって検出されます。OUI 番号は製造者によって割り当てられ、デバイスの MAC アドレスの最初の 3 オクテットを構成します。スイッチが VoIP デバイスからのトラフィックを認識するには、MAC アドレスの OUI 番号を Telephony OUI List で構成しなくてはいけません。
- 802.1ab －ポートに接続された VoIP デバイス発見するために LLDP を使用します。LLDP は System Capability 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

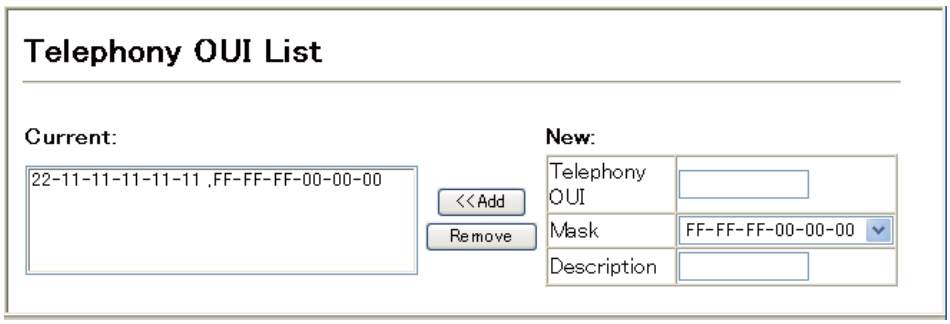
VoIP デバイスの MAC アドレスの範囲を確定します。ここで「FF-FF-FF-00-00-00」を設定すると同じ OUI 番号（最初の 3 オクテットが同一）であるすべてのデバイスを VoIP デバイスとして認識します。他の値を指定することで MAC アドレスの範囲を制限することができます。ここで「FF-FF-FF-FF-FF-FF」を選択すると 1 つの MAC アドレスのみ VoIP デバイスとして設定します（デフォルトでは FF-FF-FF-00-00-00）

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。



3.16 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。

3.16.1 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。

IGMPv3 スヌーピングを使用時、IGMP バージョン 1,2,3 ホストからのサービスリクエストは全て IGMPv3 レポートとして、上流のルータへ転送されます。

IGMPv3 スヌーピングによって提供される主な拡張は、下流の IGMPv3 ホストが要求または拒絶した特定のマルチキャストソースに関する情報の記録・追跡です。IGMPv3 ホストのみ特定のマルチキャストソースからサービスを要求出来ます。下流のホストが特定のマルチキャストサービスのソースからサービスを要求した時、これらのソースは全て Include リストに置かれ、トラフィックはこれらのソースのそれぞれからホストへ転送されます。

IGMPv3 ホストはまた、指定以外の全てのソースからのサービス転送の要求も行います。この場合、トラフィックは Exclude リストのソースからフィルタされ、その他全ての使用可能なソースから転送されます。

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。（P255 参照）

IGMP Snooping とクエリパラメータの設定

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。

[注意] 最初に受信が行われる際、数秒の間未知のマルチキャストトラフィックが VLAN 内の全てのポートにフラッディングされます。
マルチキャストルータポートが VLAN に存在している場合、IGMP スヌーピングを受けさせることで、トラフィックはフィルタされます。
ルータポートが VLAN に存在しない、またはマルチキャストフィルタリングテーブルが既に一杯の場合、スイッチは、トラフィックを VLAN 内へフラッディングし続けます。

- IGMP Querier ― 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）

IGMP Leave Proxy Status

スイッチがマルチキャストグループからクライアントをドロップするアクションを行動をとる前に、未返答を知らせるクエリの最大数を設定します。（初期設定 : 無効）

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

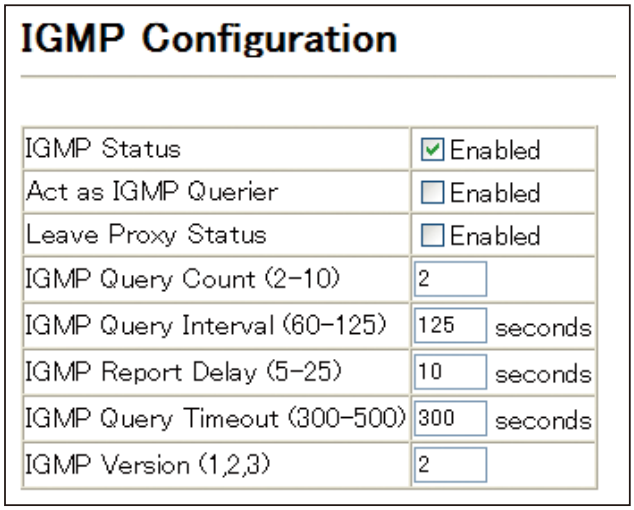
ネットワーク上の他のデバイスと互換性のある IGMP バージョンの設定を行います（1-3、初期設定 :2）

[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。）



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。

機能解説

- 即時脱退機能（Immediate leave）を使用しない場合、マルチキャストルータ（またはクエリア）は IGMPv2/v3 group leave メッセージを受信した時、group-specific クエリメッセージを送信します。
  ホストが指定されたタイムアウト時間内にクエリを返さない限り、ルータ / クエリアはこのグループのためのトラフィックの転送を停止します。
  タイムアウトピリオドは " IGMP Query Report Delay"（ "P249 「IGMP Snooping とクエリパラメータの設定」" を参照）で決定されます。
- 即時脱退機能（Immediate leave）は IGMP スヌーピングが有効の場合のみ動作し、IGMPv2 または IGMP v 3 スヌーピングが使用されます。
- スイッチがマルチキャストルータが接続されていることを学習している場合、即時脱退機能（Immediate leave）はポートに適用されません。
- 即時脱退機能（Immediate leave）はネットワークで、IGMP ホストの追加・離脱リクエストにより頻繁に発生する帯域幅使用を改善できます。

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（初期設定：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

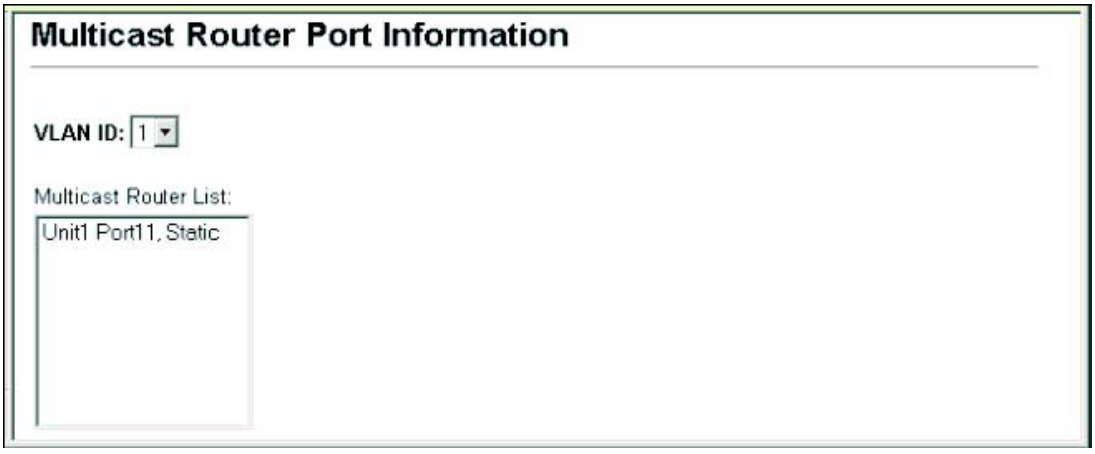
リストを表示させる VLAN ID（1-4094）

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) またはトランク (Trunk) をスクロールダウンリストから選択します。

VLAN ID

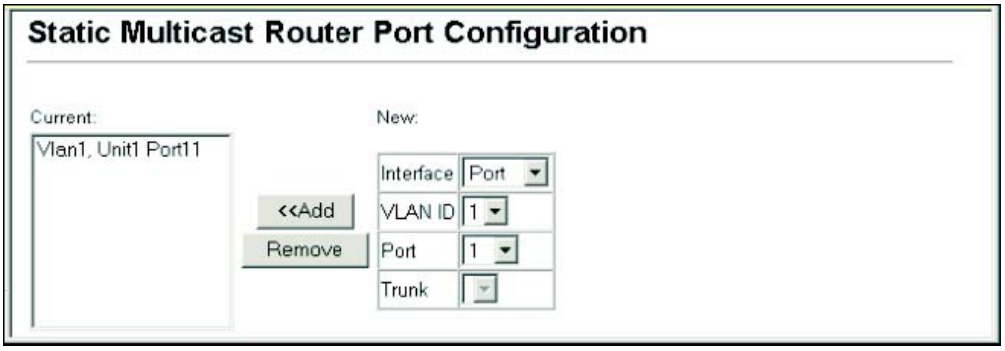
マルチキャストルータ / スイッチから送られるマルチキャストトラフィックを受信し、転送する VLAN を選択します。（1-4094）

Port/Trunk

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。（範囲：1-4094）

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、P249 「IGMP Snooping とクエリパラメータの設定」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。（範囲：1-4094）

Multicast IP

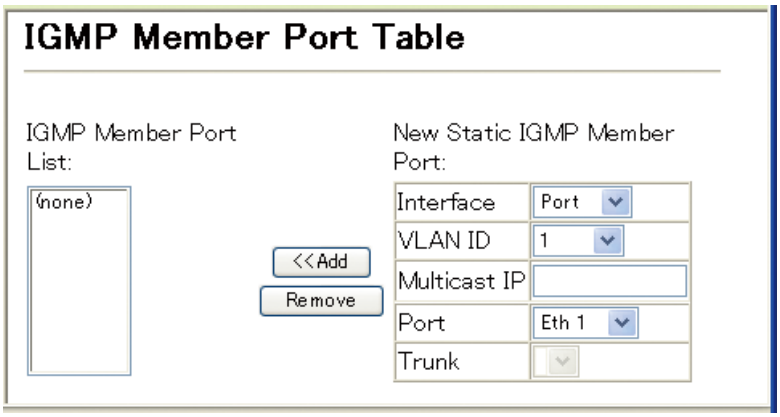
マルチキャストサービスを行う IP アドレスを入力します。

Port/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。



3.16.2 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

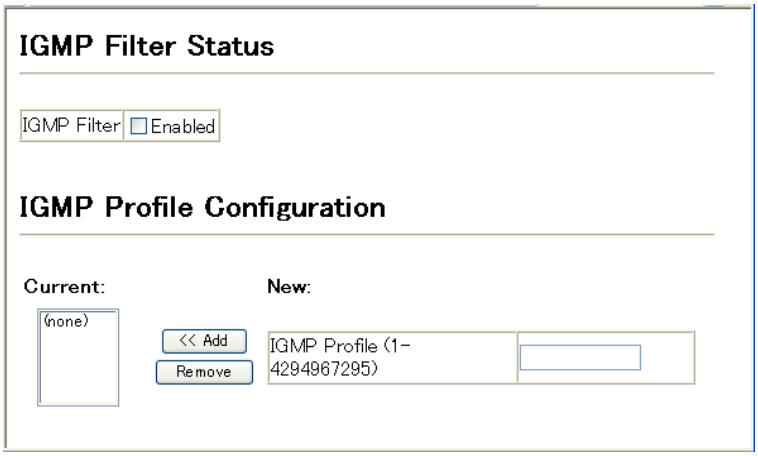
IGMP フィルタリングおよびスロットリングを、スイッチ上で有効にします。（初期設定 : 無効）

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 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

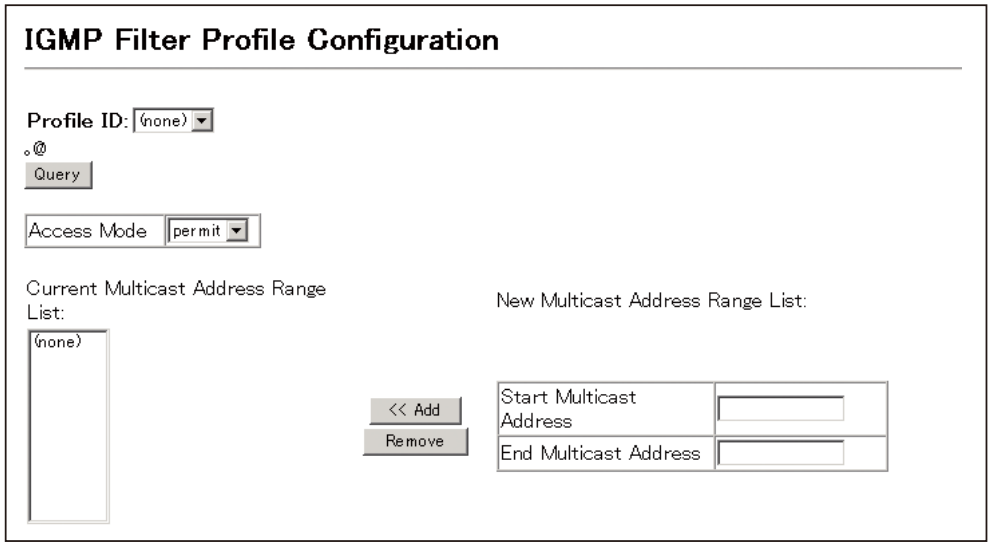
Start と End の IP アドレスを入力し、プロファイルに含めるマルチキャストグループ範囲を指定してください。単独のマルチキャストグループを指定する場合には、Start と End に同一のアドレスを入力してください。「Add」ボタンをクリックすると、範囲が現在のリストに追加されます。

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 － 255　初期設定：255）

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

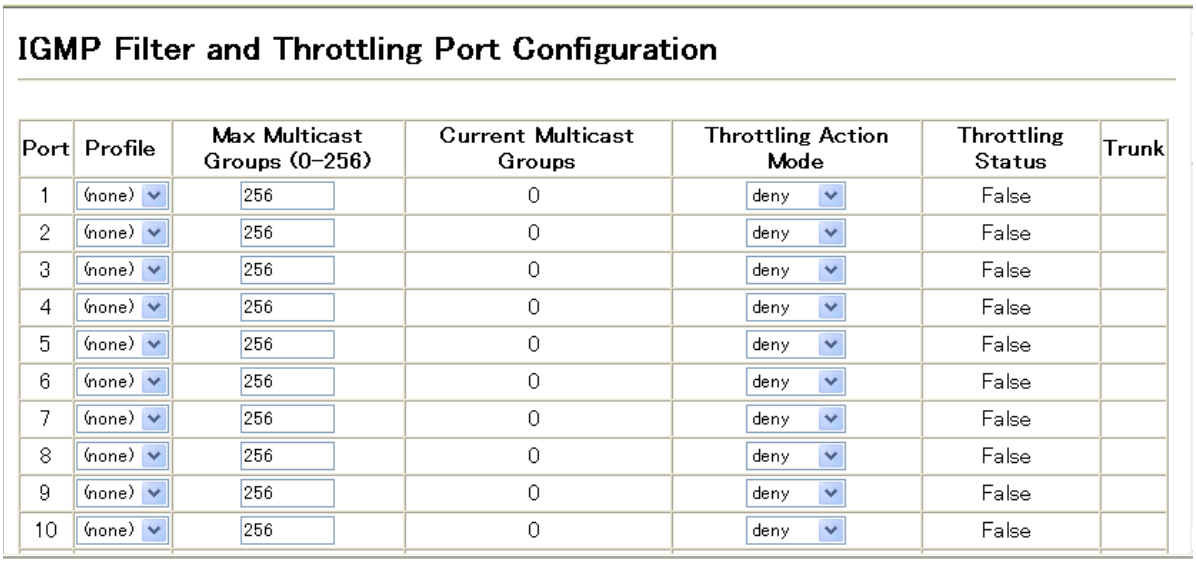
インタフェース上で、スロットリングの動作が実行されたかどうかを表示します。（オプション：true または False）

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。**

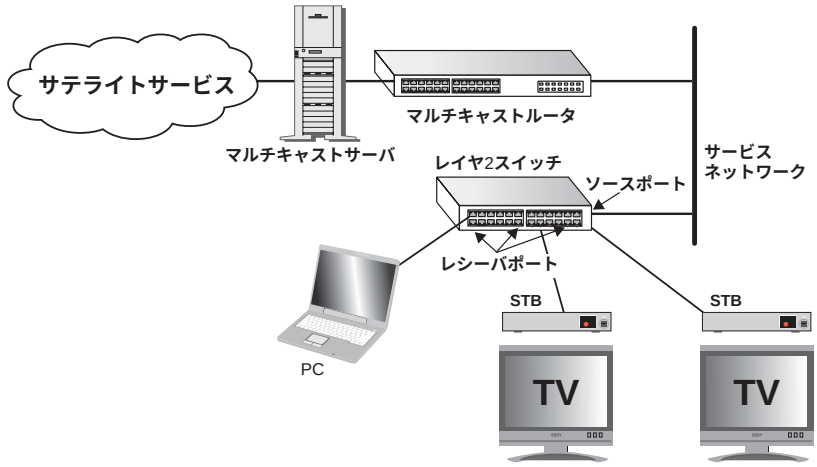


IGMP Filter and Throttling Port Configuration

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	

3.17 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。(266 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)

3.17.1 グローバル MVR 設定

MVR(Multicast VLAN Registration) のグローバル設定は、スイッチ全体での MVR の有効 / 無効、サービスプロバイダによってサポートされた通常マルチキャストストリームの単独チャンネルの役をする VLAN の選択、マルチキャストグループアドレスをそれぞれのサービスのため MVR VLAN への割り当てを含みます。

機能解説

- IGMP スヌーピングと MVR は最大 255 グループを共有します。
  この限界を超過して受信されたマルチキャストストリームは関連付けられた VLAN の全てのポートへフラッディングされます。

設定・表示項目

MVR Status

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

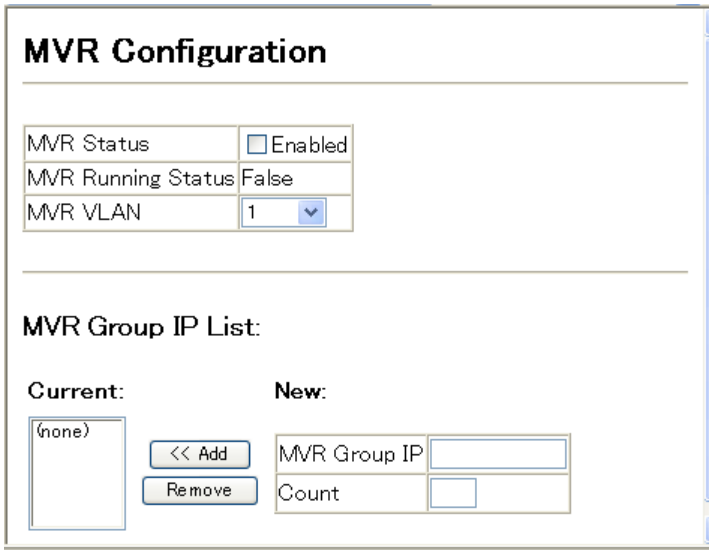
MVR マルチキャストグループの IP アドレス。

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。



3.17.2 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

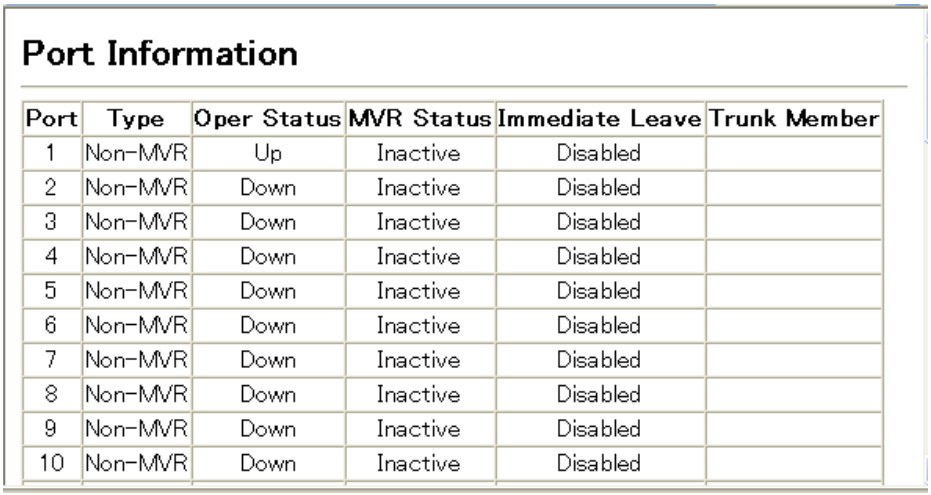
即時脱退の有効 / 無効を表示します。

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	

3.17.3 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

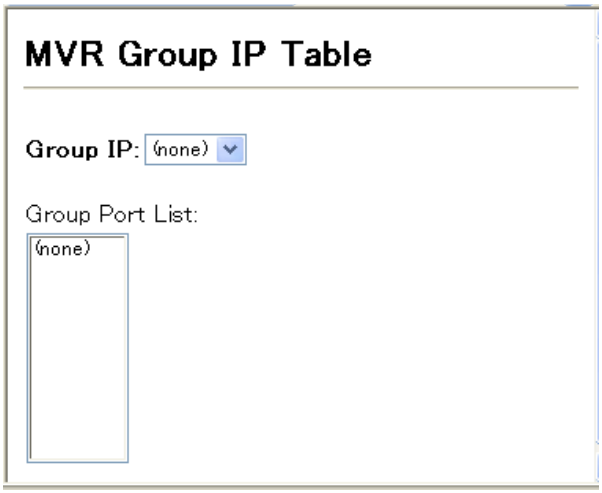
MVR VLAN に割り当てられたマルチキャストグループ

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。



3.17.4 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 － MVR VLAN にアサインされたグループへマルチキャストデータを送受信できるアップリンクポート
- Receiver － MVR VLAN を通して送信されるマルチキャストデータを受信できる加入者ポート
- Non-MVR － MVR VLAN に参加しないインタフェース（初期設定）

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フェイスを転送テーブルから削除できるようにします。

Immediate Leave

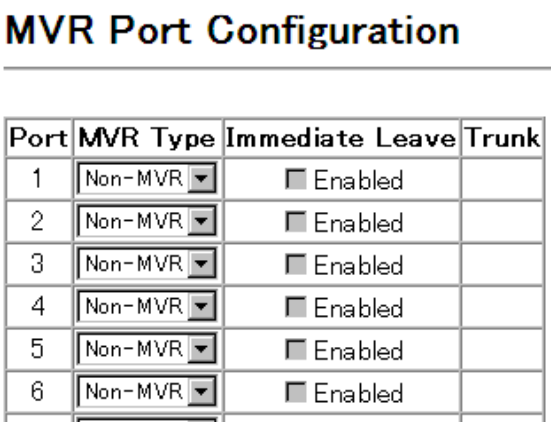
即時脱退処理。Leave メッセージを受け取るとすぐにインタフェイスを転送テーブルから削除できるようにします。

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。**



3.17.5 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

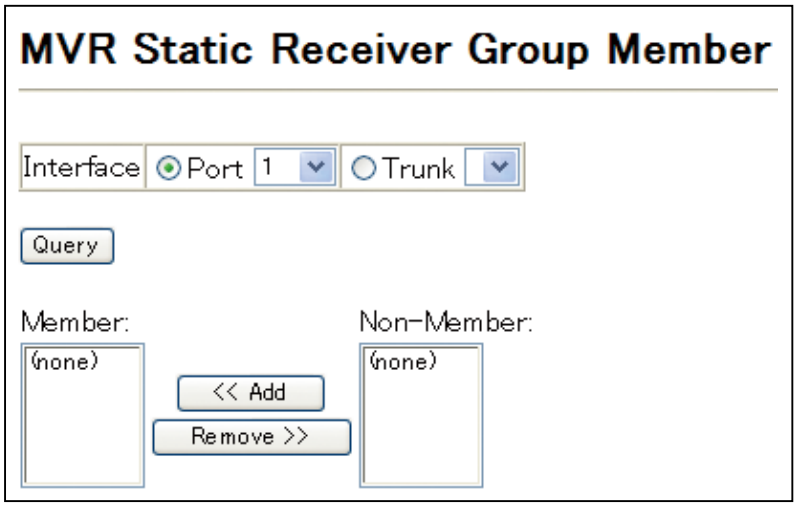
選択したインタフェースへ静的に割り当てられた MVR **マルチキャストの** IP **アドレス。**

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。**



3.17.6 MVR レシーバ VLAN とグループアドレスの設定

サブスクライバへ転送されるマルチキャストトラフィックは通常、ホストが MVR VLAN の識別情報を発見するのを阻止するためにフレームタグを取り外されます。
フレームタグの付いたマルチキャストトラフィックがサブスクライバへ転送される間、この VLAN でサポートされる MVR レシーバ VLAN とマルチキャストサービスは、MVR VLAN を隠して設定することができます。

ポートが手動でレシーバ VLAN へタグメンバーとしてアサインされている場合、サブスクライバへ転送されたマルチキャストトラフィックも、同じくタグが付きます。

設定・表示項目

MVR Receiver VLAN

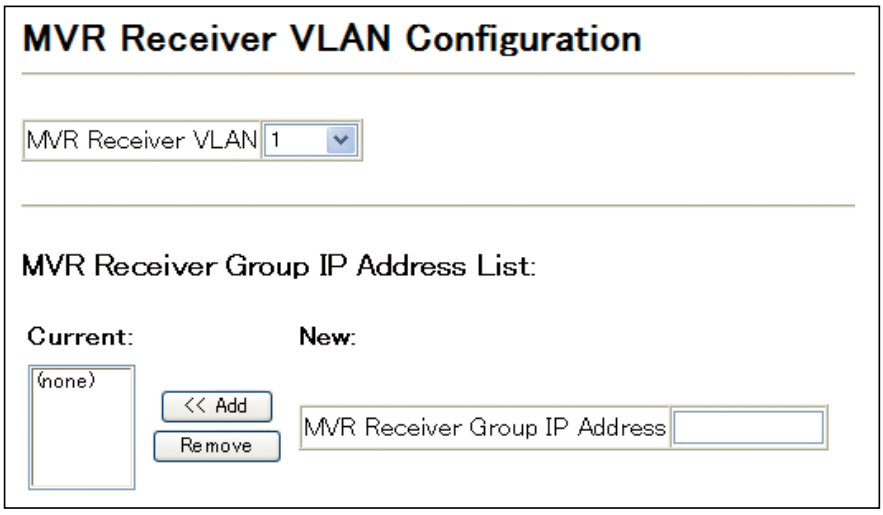
指定したレシーバ VLAN から、タグ付きフレームの MVR VLAN が識別情報を明らかにしないマルチキャストトラフィックの転送を可能にします。（範囲：1-4094）

MVR Receiver Group IP Address

レシーバ VLAN を通して管理されるグループを指定します。

設定方法

[MVR] → [Receiver Configuration] をクリックします。"
MVR Receiver VLAN" フィールドから VLAN を選択し、必要なマルチキャストグループを入力します。設定後に [Add] をクリックします。既存の設定を削除する場合は、選択後に [Remove] をクリックして下さい。



3.17.7 MVR レシーバグループの表示

MVR レシーバグループにアサインされたインタフェースは " Receiver Group IP Information" ページにて表示させることができます。

設定・表示項目

Group IP Address

MVR レシーバ VLAN にアサインされたマルチキャストグループ

Group Port List

インタフェース MVR レシーバ VLAN を通して提供されるマルチキャストサービス用サブスクライバのインタフェース

設定方法

[MVR] → [Receiver Group IP Information] をクリックします。"Group IP Address" フィールドから、合流したインタフェースを表示するレシーバグループマルチキャストアドレスを選択します。

3.17.8 静的 MVR レシーバグループメンバの設定

このページでは、マルチキャストレシーバグループを、選択したインタフェースへ静的にアサインすることができます。

設定・表示項目

Interface

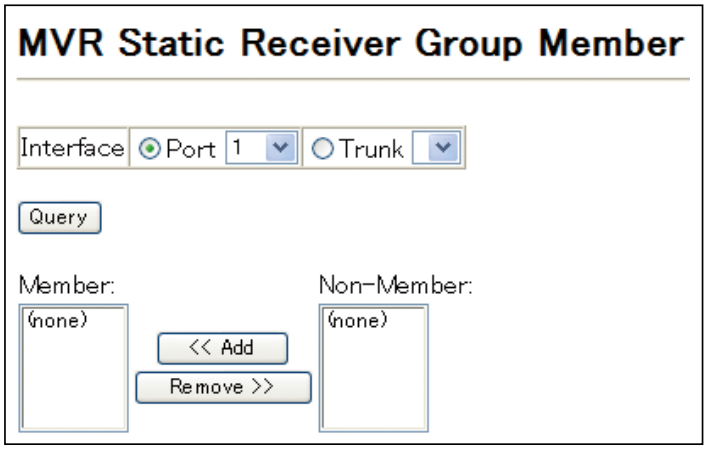
ポートまたはトランク

Group Address List

選択されたインタフェースへ割り当てられたマルチキャストレシーバグループ。

設定方法

[MVR] → [Receiver 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指定し、メンバーリストからマルチキャストグループアドレスを選択します。**
設定を追加するには [Add]**、既存の設定を削除するには** [Remove] **をクリックしてください。**



3.18 DNS（Domain Name Service）

本機の DNS(Domain Naming System) サービスは、ドメイン名と IP アドレスのマッピングを行なう DNS テーブルの手動での設定を行なえる他、デフォルトドメイン名の設定又はアドレス変換を行なうための複数のネームサーバの指定を行なうことができます。

3.18.1 DNS サービスの一般設定

機能解説

- スイッチで DNS サービスを有効にするため、まず最初に一つ以上のネームサーバーを設定後、ドメインルックアップステータスを有効にします。
- DNS クライアントから受信した不完全なホスト名に付加するデフォルトドメイン名またはドメイン名リストを指定することが可能です。
- ドメインリストが存在しない場合、デフォルトドメイン名が使われます。ドメインリストが存在する場合のはデフォルトドメイン名は使用されません。
- 本機の DNS サーバが不完全なホスト名を受信し、ドメイン名リストが指定された場合、本機は追加するリスト内の各ドメイン名をホスト名に加え、一致する特定のネームサーバを確認して、ドメインリストにより動作します。
- 一つ以上のサーバが指定されている時、サーバは応答を受信するまで、又はリストの最後に到達するまで、にリクエストを送信し続けます。
- ネームサーバが削除された場合、DNS 機能は自動で無効になります。

設定・表示項目

Domain Lookup Status

DNS ホスト名・アドレス変換を有効にします。

Default Domain Name*

不完全なホスト名に付加するデフォルトドメイン名を指定します。

Domain Name List*

不完全なホスト名に追加するドメイン名のリストを設定します。

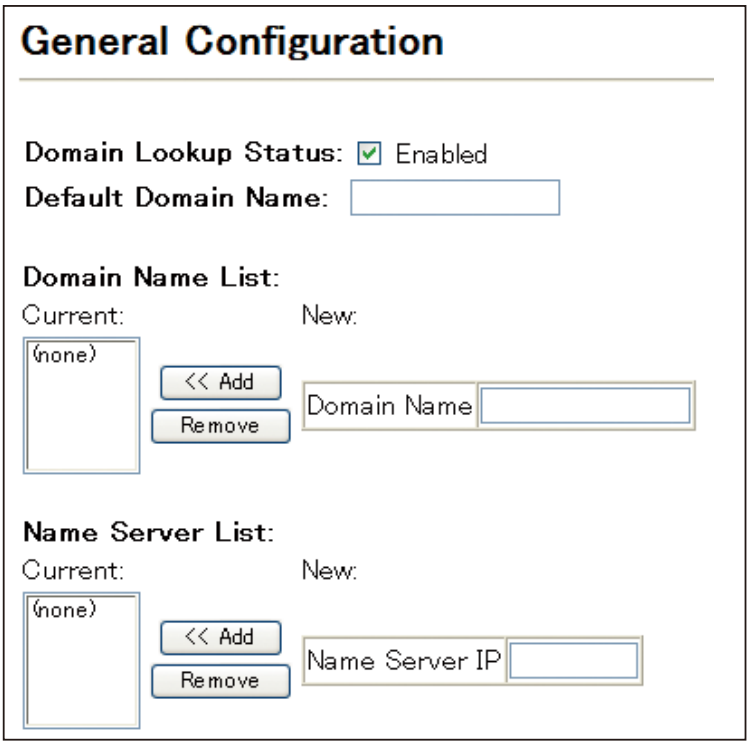
Name Server List

ドメイン名解決のために 1 つ又は複数のドメインネームサーバのアドレスを指定します。

* ホスト名をドメイン名から分離する最初のドットは含まないで下さい。

設定方法

[DNS] → [GeneralConfiguration] をクリックします。アドレスリゾルーションに使用する 1 つ以上のサーバを指定し、[Domain Lookup Status] の [Enable] にチェックを入れ、[Apply] をクリックします。



3.18.2 静的 DNS ホストのアドレスエントリ

DNS テーブルのホスト名と IP アドレスのマッピングの静的設定を行ないます。

機能解説

サーバや他のネットワーク機器は複数の IP アドレスによる複数接続をサポートしています。2 つ以上の IP アドレスを静的テーブルやネームサーバからの応答によりホスト名と関連付けする場合、DNS クライアントは接続が確立するまで各アドレスに接続を試みます。

設定・表示項目

Host Name

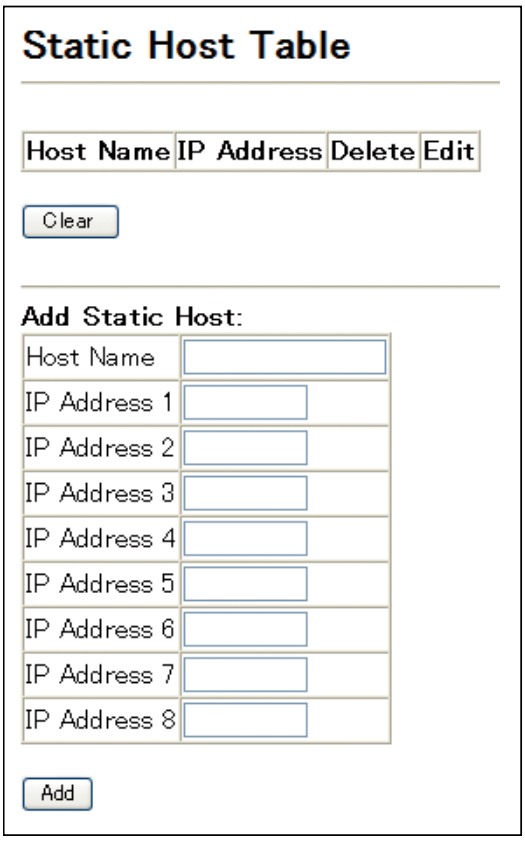
ホスト名（設定範囲：1-64 文字）

IP Address

IP アドレス（設定範囲：1-8 アドレス）

設定方法

[DNS] → [Static Host Table] をクリックします。ホスト名と一つ以上のアドレスを入力し [Apply] をクリックします。



3.18.3 DNS キャッシュの表示

DNS キャッシュの内容を表示します。

設定・表示項目

No

各リソースレコードのエントリ番号

Flag

キャッシュエントリのフラグは常に "4"

Type

標準的又はプライマリ名が指定された「CNAME」、既存のエントリと同じ IP アドレスをマッピングされている多数のドメイン名が指定された「ALIAS」

IP

レコードに関連した IP アドレス

TTL

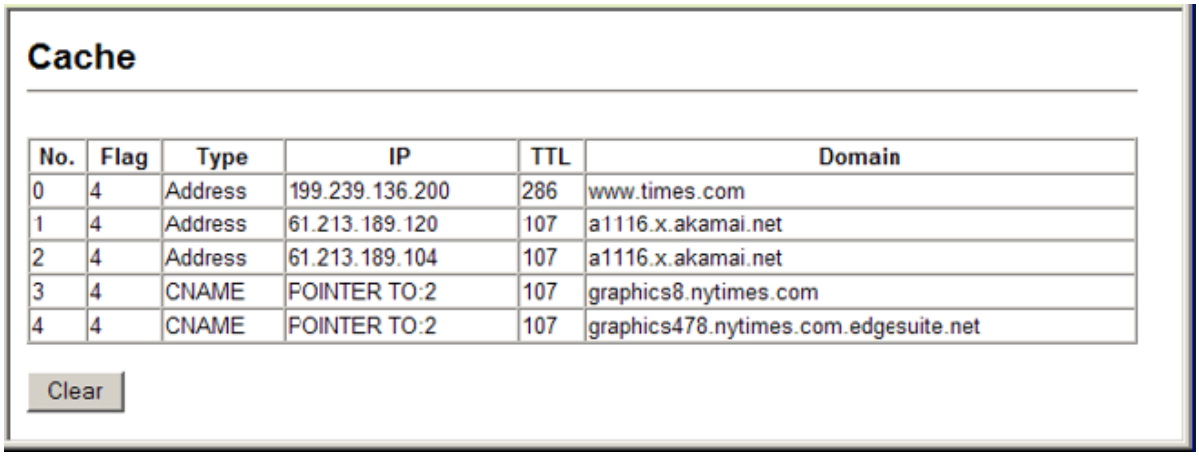
ネームサーバにより報告された生存可能時間

Domain

レコードに関連するドメイン名

設定方法

[DNS] → [Cache] 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

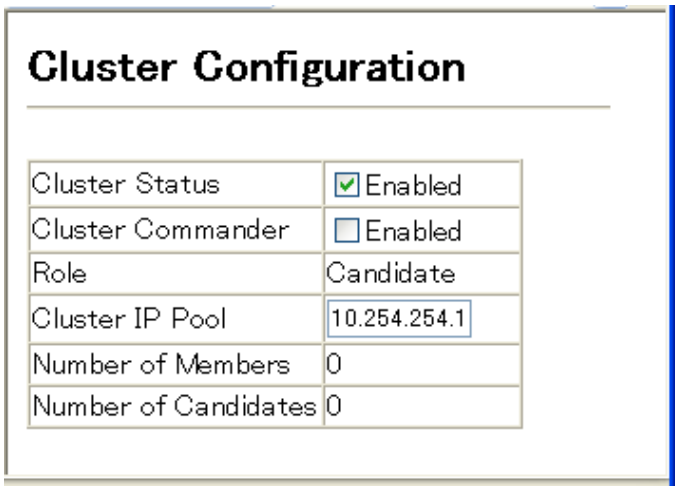
現在のクラスタメンバー数

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

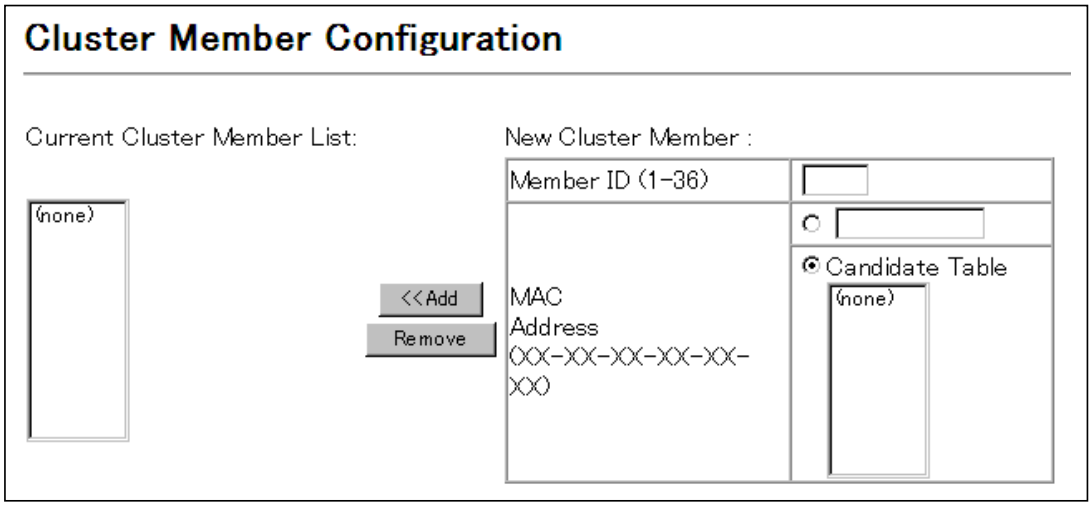
選択した候補スイッチにメンバー ID を設定します。（範囲：1-36 文字）

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の表示

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

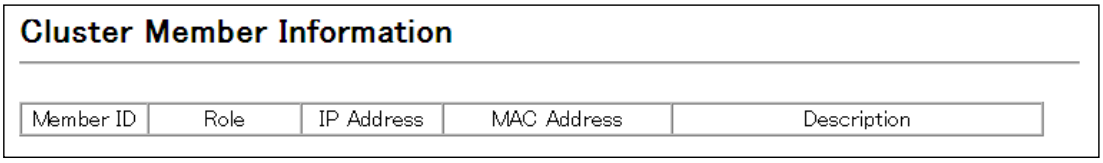
メンバースイッチの MAC **アドレス** .

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

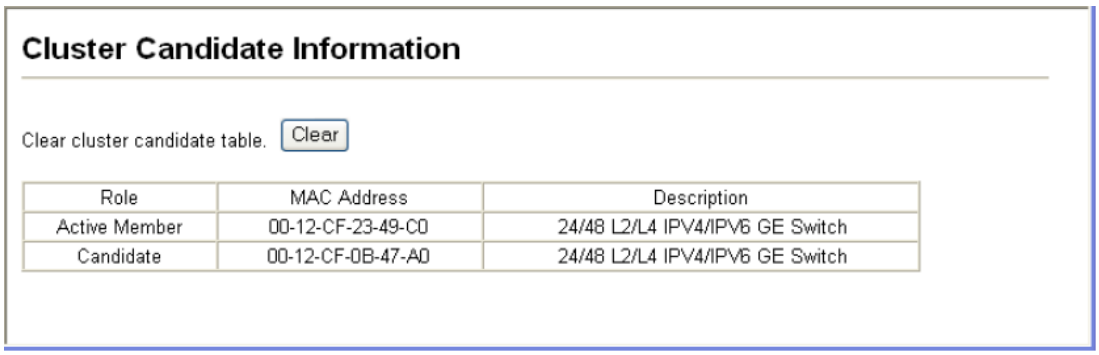
候補スイッチの MAC **アドレス** .

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

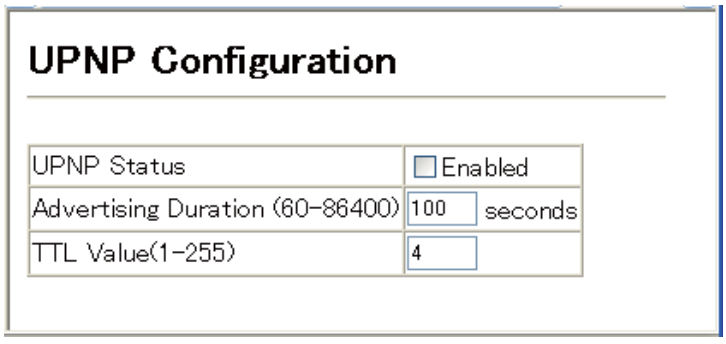
デバイスがステータスをアドバタイズする継続時間を設定します
（範囲：60-86400 秒　初期設定：100 秒）

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 FXC3152A 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 the FXC3152A 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
  arp                   Information of ARP cache
  auto-traffic-control  Auto traffic control information
  banner                Banner info
  bridge-ext            Bridge extension information
  calendar              Date and time information
  class-map             Displays class maps
  cluster               Display cluster
  debug                 State of each debugging option
  dns                   DNS information
  dot1q-tunnel          dot1q-tunnel
  dot1x                 802.1x content
  garp                  GARP properties
  gvrp                  GVRP interface information
  history               History information
  hosts                 Host information
  interfaces            Interface information
  ip                    IP information
  ipv6                  IPv6 information
  lacp                  LACP statistics
  line                  TTY line information
  lldp                  LLDP
  log                   Login records
  logging               Logging setting
  mac                   MAC access list
  mac-address-table     Shows the MAC address table
  mac-vlan              MAC-based VLAN information
  management            Show management information
  map                   Maps priority
  memory                Memory utilization
  mvr                   Shows MVR global parameters
  network-access        Shows the entries of the secure port.
  ntp                   Network Time Protocol configuration
  policy-map            Displays policy maps
  port                  Port characteristics
  privilege             Shows current privilege level
  process               Device process
  protocol-vlan         Protocol-VLAN information
  public-key            Public key information
  pvlan                 Shows the Private VLAN information
  queue                 Priority queue information
  radius-server         RADIUS server information
  reload                Shows the reload settings
  running-config        Information on the running configuration
  sflow                 Shows the sflow information
  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
  subnet-vlan           IP subnet-based VLAN information
  system                System information
  tacacs-server         TACACS server settings
  tech-support          Technical information
  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
```

"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 ?
  brief       brief interface description
  counters    Interface counters 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?
sflow           snmp            sntp        spanning-tree   ssh
startup-config  subnet-vlan     system
```

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 FXC3152A is opened.
      To end the CLI session, enter [Exit].

Console#
```

```
Username: guest
Password: [guest login password]

      CLI session with the FXC3152A 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。
電源を切った時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。
- **Class Map Configuration**― DiffServe クラスマップを作成するためのモードです。
- **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。
- **Multiple Spanning Tree Configuration** ― MST インスタンス関連の設定を行なうためのモードです。
- **Policy Map Configuration** ― パケットフィルタリングを行なうためのモードです。
- **Service Group Configuration** ― 定義されたリストにセキュリティサービスを追加します
- **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)#	P334
Access Control List	access-list arp access-list ip standard access-list ip extended access-list ip mac	Console(config-arp-acl) Console(config-std-acl) Console(config-ext-acl) Console(config-mac-acl)	P527 P520 P522 P530
Class Map	class map	Console(config-cmap)	P710
Interface	linterface {ethernet *port* | port-channel *id* | vlan *id*}	Console(config-if)#	P536
MSTP	spanning-tree mst-configuration	Console(config-mstp)#	P599
Policy Map	policy map	Console(config-pmap)	P713
VLAN	vlan database	Console(config-vlan)	P623

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
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	P291
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	P300
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	P388
Flow Sampling	トラフィックフローのサンプル	P405
Authentication	ユーザ名・パスワード、ローカルまたはリモート認証（AAA セキュリティを含む）Web サーバの管理アクセス、Telnet サーバ、SSH 等の設定	P411
General Security Measures	設定された静的または動的アドレス、Web 認証、MAC アドレス認証、DHCP リクエストとリプライのフィルタリング、無効な ARP レスポンスの廃棄によるデータポートに接続されたクライアントのトラフィックを分離および無効なアクセス防止。	P467
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	P518
Interface	Trunk、LACP や VLAN などを各ポートの設定	P536
Automatic Traffic Control	自動トラフィック制御の設定	P553
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	P570
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	P582
Rate Limiting	通信の最大送受信帯域のコントロール	P585
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	P586
Spanning Tree	STA 設定	P590
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	P623
LLDP	LLDP 設定	P674
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	P699
Quality of Service	Diff Serv の設定	P708
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	P721
Domain Name Service	DNS サーバの設定	P751
IP Interface	管理アクセス用 IP アドレスの設定	P760

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)
MST (Multiple Spanning Tree)
NE (Normal Exec)
PE (Privileged Exec)
PM (Policy Map Configuration)
SG (Server Group)
VC (VLAN Database Configuration)

4.4 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	P292
disable	Privileged モードから Normal モードへの変更	PE	P293
configure	Global Configuration モードの有効化	PE	P294
show history	コマンド履歴バッファの表示	NE,PE	P295
reload	本機の再起動	PE	P296
reload	システムリセットの時間を設定	GC	P296
show reload	現在のリロード設定を表示	PE	P297
end	Privileged Exec モードへの変更	GC,IC, LC,VC	P298
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	P299
quit	CLI セッションを終了	NE,PE	P299

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 P286「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、P413 「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 （P293）

enable password （P413）

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 P286 「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 （P292）

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 P286 「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 （P298）

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（Privileged Exec）

システムの再起動を行う際に利用します。

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

- **本コマンドは直ちに全てのシステムを再起動します。**
- Power-On **セルフテストが行われます。**"copy running-config startup-config"（P324）**コマンドで保存された全ての設定情報は保持されます。**

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
```

reload（Global Configuration）

指定した経過時間または周期的な時間経過後にシステムの再起動を行います。
"cancel" **オプションを使用することで設定を削除します。**

文法

reload { **at** *hour minute* { *month day* | *day month* } { *year* } |
in hour *hour* minute *minute*
regularity *hour* minute { period < daily | weekly *day-of-week* | *monthly day*} > }
cancel { at | in | regularity } }

- **reload at** ― **指定した日時にスイッチの再起動をおこないます。**
  - ー *hour* - **再起動する時間を指定（時）**(**範囲：**0-23)
  - ー *minute* - **再起動する時間を指定（分）**(**範囲：**0-59)
  - ー *month* - **再起動する時間を指定（月）**(**範囲：**january-december)
  - ー *day* - **再起動する時間を指定（日）**(**範囲：**1-31)
  - ー *year* - **再起動する時間を指定（年）**(**範囲：**2001-2050)
- **reload in** ― **指定した日時にスイッチの再起動をおこないます。**
  - ー *hour* - **経過時間を指定（時）**（0-576）
  - ー *minute* - **経過時間を指定（分）**（Range：0-59）
- **reload regularity** ― **周期的な間隔でスイッチの再起動をおこないます。**
  - ー *hour* - **再起動する時間（時）**(**範囲：**0-23)
  - ー *minute* - **再起動する時間（分）**(**範囲：**0-59)

ー *month* - 再起動する曜日 (範囲：Monday-saturday)

ー *day* - 再起動する日付（範囲：1-31）

- **reload cancel** ― 指定した再起動オプションをキャンセル。

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- 本コマンドは全システムの再起動を行います。
- 再起動オプションはどのような組み合わせでも指定できます。再指定時、前回の設定は上書きされます。
- システム再起動時、Power-On セルフテストが行われます。"copy running-config startup-config"（P324）コマンドで保存された全ての設定情報は保持されます。

例

30 分後にスイッチを再起動する設定です。

```
Console(config)#reload in minute 30
***
*** --- Rebooting at January  1 03:38:34 2001 ---
***

Are you sure to reboot the system at the specified time? <y/n>
```

show reload

現在の再起動設定と、次回予定されている再起動を表示します。

コマンドモード

Privileged Exec

例

```
Console#show reload
Reloading switch in time:             0 hours 29 minutes.

The switch will be rebooted at January 1 02:11:50 2001.
Remaining Time: 0 days, 0 hours, 29 minutes, 52 seconds.
Console#
```

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)#
```

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:
```

4.5 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**	P301
Banner Information	**管理上のコンタクト、デバイス識別、位置情報を設定**	P302
System Status	**管理者やシステムバージョン、システム情報の表示**	P315
Frame Size	**ジャンボフレームサポートの有効化**	P322
File Manargement	**コードイメージまたはスイッチ設定ファイルの管理**	P323
Line	**シリアルポートの接続パラメータを設定**	P334
Event Logging	**エラーメッセージログ設定**	P351
SMTP Alerts	SMTP E **メールアラートを設定**	P358
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**	P362
Switch Clustering	**複数デバイスを** 1 **つの** IP **アドレスで管理する設定**	P378
UPnP	Universal Plug-and-Play **パラメータを設定**	P385

4.5.1 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	P298
hostname	ホスト名の設定	GC	P301
snmp-server contact	システムコンタクト者の設定	GC	P392
snmp-server location	システムロケーションの設定	GC	P392

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)#
```

4.5.2 Banner Information

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	P303
banner configure company	**会社情報の設定**	GC	P304
banner configure dc-power-info	DC **電力情報の設定**	GC	P305
banner configure department	**部門情報の設定**	GC	P306
banner configure equipment-info	**装置情報の設定**	GC	P307
banner configure equipment-location	**装置設置場所情報の設定**	GC	P308
banner configure ip-lan	IP/LAN **情報の設定**	GC	P309
banner configure lp-number	LP **番号情報の設定**	GC	P310
banner configure manager-info	**マネージャコンタクト情報の設定**	GC	P311
banner configure mux	MUX **情報の設定**	GC	P312
banner configure note	**その他情報の設定**	GC	P313
show banner	**全てのバナー情報の表示**	NE, PE	P314

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#
```

4.5.3 システム情報の表示

システム情報を表示する為に使用するコマンドを解説します。

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	P315
show running-config	実行中の設定ファイルの表示	PE	P317
show system	システム情報の表示	NE,PE	P319
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	P320
show version	システムバージョン情報の表示	NE,PE	P321

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。

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：**
  - **本機の** MAC **アドレス**
  - SNMP **サーバ設定**
  - SNMP **コミュニティ名**
  - **ユーザ（ユーザ名及びアクセスレベル）**
  - 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**
  - MST **インスタンス（名前とインタフェース）**
  - **本機の** IP **アドレス設定**
  - **スパニングツリー設定**
  - **インタフェース設定**
  - **コンソール及び** Telnet **に関する設定**

例

```
Console#show startup-config
building startup-config, please wait...

!<stackingDB>00</stackingDB>
!<stackingMac>01_00-12-cf-bb-c0-c0_02</stackingMac>
!
phymap 00-12-cf-bb-c0-c0
SNTP server 0.0.0.0 0.0.0.0 0.0.0.0
NTP Poll 16
clock timezone-predefined GMT-Greenwich-Mean-
Time:Dublin,Edinburgh,Lisbon,London
!
snmp-server community public ro
snmp-server community private rw
!
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
!
VLAN database
 VLAN 1 name DefaultVlan media ethernet state active
 VLAN 4093 media ethernet state active
!
spanning-tree MST configuration
!
interface vlan 1
 IP address 192.168.1.154 255.255.255.0
 IP address DHCP
!
interface vlan 4093
!
interface ethernet 1/1
 switchport allowed vlan add 1 untagged
 switchport native vlan 1
 switchport allowed vlan add 4093 tagged
.
(省略)
.
interface ethernet 1/52
 switchport allowed vlan add 1 untagged
 switchport native vlan 1
 switchport allowed vlan add 4093 tagged
!
ip name-server auto
!
line console
 silent-time 0
!
line VTY
!
end
!
Console#
```

関連するコマンド

show running-config （P317）

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
  - 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
  - MST インスタンス（名前とインタフェース）
  - 本機の IP アドレス設定
  - スパニングツリー設定
  - インタフェース設定
  - コンソール及び Telnet に関する設定

例

```
Console#show running-config
building startup-config, please wait.....
!<stackingDB>00</stackingDB>
!<stackingMac>01_00-12-cf-bb-c0-c0_02</stackingMac>
!
phymap 00-12-cf-bb-c0-c0
SNTP server 0.0.0.0 0.0.0.0 0.0.0.0
NTP Poll 16
clock timezone-predefined GMT-Greenwich-Mean-
Time:Dublin,Edinburgh,Lisbon,London
!
snmp-server community public ro
snmp-server community private rw
!
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
!
VLAN database
 VLAN 1 name DefaultVlan media ethernet state active
 VLAN 4093 media ethernet state active
!
spanning-tree MST configuration
!
interface vlan 1
 IP address 192.168.1.154 255.255.255.0
 IP address DHCP
!
interface vlan 4093
!
interface ethernet 1/1
 switchport allowed vlan add 1 untagged
 switchport native vlan 1
 switchport allowed vlan add 4093 tagged
.
( 省略 )
.
interface ethernet 1/52
 switchport allowed vlan add 1 untagged
 switchport native vlan 1
 switchport allowed vlan add 4093 tagged
!
ip name-server auto
!
line console
 silent-time 0
!
line VTY
!
end
!
Console#
```

関連するコマンド

show startup-config （P315）

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、またはサポートまで連絡して下さい。**

例

```
Console#show system
System Description: 48p 10/100 L2 Switch
System OID String: 1.3.6.1.4.1.259.6.10.94
System Information
 System Up Time:          0 days, 0 hours, 51 minutes, and 18.21
seconds
 System Name:             [NONE]
 System Location:         [NONE]
 System Contact:          [NONE]
 MAC Address (Unit1):     00-12-CF-BB-C0-C0
 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:
DUMMY Test 1 ................. PASS
UART Loopback Test ........... PASS
DRAM Test .................... PASS
Timer 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
Unit 1
 Serial Number:            A945038589
 Hardware Version:         R01
 Chip Device ID:           Marvell 98DX106-B0, 88E6095[F]
 EPLD Version:             0.05
 Number of Ports:          52
 Main Power Status:        Up
 Redundant Power Status:   Not present

Agent (Master)
 Unit ID:                  1
 Loader Version:           1.0.2.0
 Boot ROM Version:         1.2.0.1
 Operation Code Version:   1.3.4.0

Console#
```

4.5.4 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	P322

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

jumbo frame

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、**P546 **「**switchport packet-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（**P319**）で確認ができます。**

例

```
Console(config)#jumbo frame
Console(config)#
```

4.5.5 ファイル管理（ Flash/File ）

ファームウェアの管理

FTP/TFTP サーバから、ファームウェアのアップロードおよびダウンロードが可能です。
FTP/TFTP サーバで、ファイルへランタイムコードをセーブすることによって、そのファイルを後にスイッチへダウンロードすることでオペレーションを復活することが可能です。
本機はまた、以前のバージョンを上書きせずに新しいファームウェアを使用するように設定することが可能です。
ランタイムコードをダウンロードする際、現在のイメージを置き換えるか最初のファイルとは別のファイル名を使用してダウンロードをすることが出来ますので、ダウンロード後に新しいファイルをスタートアップファイルとして設定してください。

設定のセーブまたはリストア

FTP/TFTP サーバから、設定ファイルのアップロードおよびダウンロードが可能です。
設定ファイルは後にスイッチの設定をリストアするために使用できます。
設定ファイルは新しいファイル名でダウンロードされ、スタートアップとして設定するか、現在のスタートアップファイルはディスティネーションファイルとして指定されたファイル名でダイレクトに置き換えることができます。

"Factory_Default_Config.cfg" は FTP/TFTP サーバにコピーすることは可能ですが、ディスティネーションとして使用することは出来ません。

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	P324
delete	ファイルやコードイメージの削除	PE	P327
dir	フラッシュメモリ内のファイルの一覧の表示	PE	P328
whichboot	ブートファイルの表示	PE	P329
boot system	システム起動ファイル、イメージの設定	GC	P330
自動コードアップグレードコマンド			
upgrade opcode auto	指定したサーバに新しいバージョンが見つかった時、現在のイメージを自動アップグレード。	GC	P331
upgrade opcode path	FTP/TFTP サーバの指定と新しいオペレーションコードが保存されるディレクトリを指定	GC	P333

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、FTP/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 FTP/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 | ftp | running-config | startup-config | tftp >

copy running-config < file | ftp | startup-config | tftp >

copy startup-config < file | ftp | 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**
- ftp ― FTP **サーバから (** **または** FTP **サーバーへ）のコピーを行うキーワード**
- 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 (** **または** TFTP **サーバーへ）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、**444 **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** FTP/TFTP **サーバ上では** 124 **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 **とローダは** FTP/TFTP **サーバからダウンロードができますが、スイッチからファイルサーバへのアップロードはできません。**
- "http-certificate" **の設定については、**92 **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、**441 **ページの「**ip http secure-server**」を参照して下さい。**

例

本例では、TFTP **サーバからの新しいファームウェアのダウンロードを示しています。**

```
Console#copy tftp file
TFTP server ip address: 10.1.0.19
Choose file type:
 1. config: 2. opcode: <1-2>: 2
Source file name: V3.1.16.20.BIX
Destination file name: V311620
\Write to FLASH Programming.
-Write to FLASH finish.
Success.
Console#
```

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#
```

以下はファイルを FTP サーバにコピーする方法を示しています。

```
Console#copy ftp file
FTP server IP address: 169.254.1.11
User[anonymous]: admin
Password[]: *****
Choose file type:
  1. config: 2. opcode: 4. diag: 5. loader: <1,2,4,5>: 2
Source file name: BLANC.BIX
Destination file name: BLANC.BIX
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 *filename*

- *filename* — **設定ファイルまたはイメージファイル名**

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 （P328）

delete public-key（P449）

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	解説
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:
         ES3528_52M_diag_V1.0.0.8.bix     Boot-Rom Image  Y          1383604
         ES3528_52M_opcode_V1.3.7.4.bix   Operation Code  N          4456432
         FXC3152A-OP-V1.1.3.4.bix         Operation Code  Y          3841972
         Factory_Default_Config.cfg      Config File     N             455
         basic                            Config File     N            6690
         mstp                             Config File     N            8512
         startup1.cfg                     Config File     Y            7913
 ------------------------------------------------------------------------------
                                                  Total free space:   5111808
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

```
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（P328）

upgrade opcode auto

"upgrade opcode path" コマンドで指定されたサーバに、新しいバージョンが検出された時、現在のオペレーションコードを自動でアップグレードします。"no" を使用することで設定を初期値に戻します。

文法

upgrade opcode auto

no upgrade opcode auto

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

- このコマンドは、オペレーションコードの自動アップグレードを有効または無効にします。本コマンドにより自動イメージアップグレードを有効にした場合、スイッチは起動時に以下のプロセスを行います。

  （1）"upgrade opcode path" コマンド（P333）で指定された場所でイメージの新しいバージョンを検索します。FTP/TFTP サーバに保存される新しいイメージの名前は "ES3528_52M.bix" にしてください。
  スイッチが現在使用しているよりも新しいコードバージョン検出した場合、新しいイメージをダウンロードします。もし既に 2 つのイメージがスイッチに保存されている場合、スタートアップに設定されていないイメージが新しいバージョンで上書きされます。

  （2）イメージのダウンロード後、スイッチはログへアップグレードオペレーションが成功したか否かのトラップメッセージを送信します。

  （3）新しいバージョンをスタートアップイメージとして設定します。

  （4）新しいイメージを使用するためにシステムの再起動を行います。

- 初期設定に対して行われた変更は "show running-config"（P317）または "show startup-config"（P315）コマンドで表示されます。

例

```
Console(config)#upgrade opcode auto
Console(config)#upgrade opcode path tftp://192.168.0.1/sm24/
Console(config)#
```

指定された場所に新しいイメージが見つかった場合、システム起動時に以下のタイプのメッセージが表示されます。

```
.
.
.
Automatic Upgrade is looking for a new image
New image detected: current version 1.1.1.0; new version 1.1.1.2
Image upgrade in progress
The switch will restart after upgrade succeeds
Downloading new image
Flash programming started
Flash programming completed
The switch will now restart
.
.
.
```

upgrade opcode path

新しいオペレーションコードが保存される FTP/TFTP サーバおよびディレクトリを指定します。"no" を前に置くことで現在の設定を削除します。

文法

upgrade opcode path *opcode-dir-url*

no upgrade opcode path

- *opcode-dir-url* — 新しいコードの場所

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- このコマンドで指定する場所に保存された新しいオペレーションコードの自動アップグレードを行います。
- FTP/TFTP サーバに保存された新しいイメージの名前は "ES3528_52M.bix" にしてください。ファイル名はこのコマンドに含まれません。
- TFTP サーバを指定した時、filedir が新しいイメージが含まれるディレクトリへのパスを示すには以下の文法が使われます。
  tftp://192.168.0.1[/filedir]
- FTP サーバを指定した時、filedir が新しいイメージが含まれるディレクトリへのパスを示すには以下の文法が使われます。
  ftp://[username[:password@]]192.168.0.1[/filedir]/
  ユーザ名が省略された場合、"Anonymous" が接続に使用されます。パスワードが省略された場合、空白 "" が接続に使用されます。

例

TFTP サーバで新しいコードが保存されている場所を指定しています。

```
Console(config)#upgrade opcode path tftp://192.168.0.1/sm24/
Console(config)##
```

例

FTP サーバで新しいコードが保存されている場所を指定しています。

```
Console(config)#upgrade opcode path ftp://
admin:billy@192.168.0.1/sm24/
Console(config)#
```

4.5.6 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	P335
login	コンソール接続時のパスワードの有効化	LC	P336
password	コンソール接続時のパスワードの設定	LC	P337
timeout login response	CLI のログイン入力待ち時間の設定	LC	P338
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	P339
password-thresh	パスワード入力時のリトライ数の設定	LC	P340
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	P341
databits*	各文字あたりのデータビットの設定	LC	P342
parity*	パリティビット生成の設定	LC	P342
speed*	ボーレートの設定	LC	P344
stopbits*	1byte あたりのストップビット値の設定	LC	P345
terminal length	ターミナルで表示するラインの数を設定	PE	P345
terminal width	ターミナル表示の幅を設定	PE	P346
terminal escape-character	ディスプレイ表示を中断するエスケープ文字を設定	PE	P346
terminal terminal-type	コンソールポートに接続するターミナルのタイプを指定	PE	P347
terminal history	以前に入力したコマンドを保存するパラメータの設定	PE	P348
disconnect	Line 接続を終了	PE	P345
show line	ターミナル接続の設定情報を表示	NE,PE	P350

* 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（P350）

show users（P320）

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（P412）

password（P337）

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（P336）

password-thresh（P340）

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：600 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（P341）

exec-timeout（P339）

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

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)#
```

関連するコマンド

silent-time（P341）
timeout login response（P338）

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：**1-120**、**0**：回数の制限をなくします）**

初期設定

3 **回**

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（P341）

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（P340）

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 ー 7 **データビット**
- 8 ー 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（P342）

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 ー **パリティ無し**
- even ー **偶数パリティ**
- odd ー **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（オプション：**9600、19200、38400**）**

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 38400
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 >

no stopbits

- 1 **ーストップビット** "1"
- 2 **ーストップビット** "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)#
```

terminal length

ターミナルで表示するライン数を設定します。"no" **を使用することで設定を初期値に戻します。**

文法

terminal length *screen-length*

no terminal length

- *screen-length* **ーターミナルで表示する文字数を設定**
  (範囲：0-512**、**0 **は 出力ディスプレイにポーズ無し**)

初期設定

24

コマンドモード

Privileged Exec

例

```
Console#terminal length 20
Console#
```

terminal width

ターミナル表示の一行の文字数を設定します。"no" **を前につけることで設定を初期値に戻します。**

文法

terminal width *characters*

no terminal width

- *characters* **ーターミナル表示の文字数を設定（範囲：**0-80**）**

初期設定

80

コマンドモード

Privileged Exec

例

```
Console#terminal width 70
Console#
```

terminal escape-character

ディスプレイ出力を中止するために使われるエスケープ文字を指定します。"no" **を使用することで設定を初期値に戻します。**

文法

terminal escape-character < *characters* | ACII-number *ACII-number* >

no terminal escape-character

- *characters* **ーエスケープ文字**
- *ACII-number* **ーエスケープ文字の** ASCII10 **進数同義語（範囲：**0-255**）**

初期設定

27 (**バックスペースキーの** ASCII **相当**)

コマンドモード

Privileged Exec

コマンド解説

本コマンドで指定されたエスケープキャラクタはスクリーン出力の中断に使用されます。Ctrl-C **もまた現在のコマンドラインインプットストリングを中断するのに使用できます。**

例

```
Console#terminal width 70
Console#
```

terminal terminal-type

コンソールポートへ接続するターミナルタイプを指定します。"no" **を使用することで設定を初期値に戻します。**

文法

terminal terminal-type < ansi-bbs | vt-100 | vt-102 >

no terminal terminal-type

- ansi-bbs ー ANSI-BBS
- vt-100 ー VT100
- vt-102 ー VT102

初期設定

VT100

コマンドモード

Privileged Exec

コマンド解説

本コマンドはコンソールポートへ接続するターミナルタイプまたはコンソールポートに接続された PC **で使用されるターミナルエミュレーションタイプを指定します。**

例

```
Console#terminal terminal-type vt-102
Console#
```

terminal history

過去に入力されたコマンドを保存するためのパラメータ設定を行います。

"no" **を使用することで設定を初期値に戻します。**

文法

terminal history { *size number-of-lines* }

no terminal history { *size* }

初期設定

有効、10 **行**

コマンドモード

Privileged Exec

コマンド解説

- size" **コマンド無しで本コマンドを実行すると、コマンドヒストリバッファを有効にします。**"size" **キーワードを使用することでコマンドヒストリバッファのサイズを設定します。**
- **ヒストリバッファの初期値は** 10 **実行コマンドに固定されています。**

例

```
Console#terminal history size 20
Console#
```

関連するコマンド

show history（P295）

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 :0-8）

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（P452）

show users（P320）

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
 Termianal Configuration for this session:
  Length: 24
  Width: 80
  History size: 10
  Escape character(ASCII-number): 27
  Terminal type: VT100

 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:  3 times
  Interactive Timeout: 600 sec
  Login Timeout: 300 sec
Console#
```

4.5.7 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	P351
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	P352
logging host	syslog を送信するホストの IP アドレスの設定	GC	P353
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	P353
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	P354
clear log	ログバッファのクリア	PE	P354
show logging	ログ関連情報の表示	PE	P356
show log	ログメッセージの表示	PE	P357

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（P352）

logging trap（P354）

clear logging（P354）

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（範囲：**0-7**）**

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

※現在のファームウェアではレベル 2、5、6 **のエラーメッセージのみサポート**

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* **ー** 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 **ー** 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 ー 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（P352 の表を参照）

初期設定

有効（level 7 - 0）

コマンドモード

Global Configuration

コマンド解説

- 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 ー **フラッシュメモリに保存されたイベント履歴**
- ram ー 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（P356）

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 >

- flash ー フラッシュメモリに保存されたイベント履歴
- ram ー RAM に保存されたイベント履歴
- sendmail ー SMTP イベントハンドラの設定を表示 (P360)

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

関連するコマンド

show logging sendmail（P361）

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#
```

4.5.8 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	P358
logging sendmail level	アラートメッセージのしきい値設定	GC	P359
logging sendmail source-email	メールの ”From” 行に入力されるアドレスの設定	GC	P359
logging sendmail destination-email	メール受信者の設定	GC	P360
logging sendmail	SMTP イベントハンドリングの有効化	GC	P360
show logging sendmail	SMTP イベントハンドラ設定の表示	NE,PE	P361

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 (P354)。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

なし

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: 4

SMTP destination email addresses
-------------------------------------------------
ted@this-company.com

SMTP source email address: bill@this-company.com

SMTP status: Enable

Console#
```

4.5.9 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 コマンド			
sntp client	特定のタイムサーバからの時刻の取得	GC	P363
sntp server	タイムサーバの指定	GC	P364
sntp poll	リクエスト送信間隔の設定	GC	P365
show sntp	SNTP 設定の表示	NE,PE	P366
NTP コマンド			
ntp client	NTP クライアント機能を有効化	GC	P367
ntp server	時刻更新に利用する NTP サーバを指定	GC	P368
ntp authenticate	NTP トラフィックの認証を有効化	GC	P369
ntp authentication-key	認証キーを設定	GC	P370
show ntp	現在の NTP 設定を表示	NE,PE	P371
手動設定コマンド			
clock timezone-predefined	既定義のタイムゾーンを設定	GC	P372
clock timezone	本機内部時刻のタイムゾーンの設定	GC	P373
clock summertime (date)	サマータイムを設定	GC	P374
clock summertime (predefined)	既定義のサマータイムを設定	GC	P375
clock summertime (recurring)	サマータイム（循環）を設定	GC	P376
calendar set	システム日時の設定	PE	P377
show calendar	現在の時刻及び設定の表示	NE,PE	P377

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（P364）

sntp poll（P365）

show sntp（P366）

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* ー 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* ーリクエスト間隔（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（**P363**）

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#
```

ntp client

指定された NTP **タイムサーバからの、時刻同期の** NTP **クライアントリクエストを有効にします。**"no" **を前に置くことで設定を無効にします。**

文法

ntp client

no ntp client

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

- SNTP、NTP **クライアントを同時に使用することはできません。**
  このコマンドを使用する前に、SNTP **クライアントを無効にしてください。**
- **タイムサーバから取得された時刻は、ログイベントの正確な日付と時刻を記録するために使用されます。**NTP **を使用しない場合、スイッチは工場出荷設定から前回のブートアップにセットされた時刻のみを記録します。（例：**00:00:00, Jan. 1, 2001）

例

```
Console(config)#ntp client
Console(config)#
```

関連するコマンド

sntp client（P363）

ntp server（P368）

ntp server

NTP サーバリクエストをおこなうサーバの IP アドレスを設定します。
"no" を前に置くことで、指定したタイムサーバまたは全てのタイムサーバをリストから削除します。

文法

ntp server *ip_address* { version *number* } {key *key-number*)

no ntp server {*ip_address*}

- *ip_address* ー NTP サーバの IP アドレス
- *number* ーサーバでサポートされる NTP バージョン（範囲：1-3）
- *key-number* ーサーバとのコミュニケーションに使用される認証キー（範囲：1-65535）

初期設定

バージョン：3

コマンドモード

Global Configuration

コマンド解説

- このコマンドは、NTP クライアントモードに設定時、スイッチが時刻更新をおこなうタイムサーバを指定します。ntp poll コマンドによって設定された、インターバ ル設定を基にした時刻同期リクエストを発行します。
  クライアントは設定された全てのタイムサーバをチェックし、全ての返答は一番信頼性が高い時刻更新のために、フィルタと比較を行い受信されます。
- 最大 50 の NTP サーバを設定することができます。設定をおこないたいサーバを全て入力するため、繰り返しコマンドを使用してください。
- NTP 認証は任意です。もし NTP 認証を有効にした場合、ntp authentication-key コマンドを使用するため、最低 1 つのキー番号を設定する必要があります。

例

```
Console(config)#ntp server 192.168.3.20
Console(config)#ntp server 192.168.3.21
Console(config)#ntp server 192.168.4.22 version 2
Console(config)#ntp server 192.168.5.23 version 3 key 19
Console(config)#
```

関連するコマンド

sntp client （P363）

show ntp （P371）

ntp authenticate

NTP クライアントとサーバ間の接続に使われる認証を有効にします。
"no" を前に置くことで無効にします。

文法

ntp authenticate

no ntp authenticate

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

- 認証された NTP サーバからのみ、信頼性の高い更新を受け取ることを可能にするため、NTP 認証を有効にできます。
  認証キーとそれらに関連付けられたキー番号は中央で管理され、手動で NTP サーバとクライアントに配布されます。
  キー番号とキー値は、サーバとクライアントで一致する必要があります。

例

```
Console(config)#ntp authenticate
Console(config)#
```

関連するコマンド

ntp authentication-key （P370）

ntp authentication-key

NTP 認証が有効時に使用される、認証キーとキー番号の設定をおこないます。

"no" を前に置くことで、指定した認証キーまたは全ての認証キーをリストから削除します。

文法

ntp authentication-key *number* { md5 *key* }

no ntp authentication-key {*number*}

- *number* ー NTP 認証キー ID 番号（範囲：1-65535）
- md5 ー認証が MD5（Message Digest algorithm 5）を使用して提供される場合に指定します。
- *key* ー MD5 認証キーストリング。
  （32 文字以内で大文字小文字を識別する ASCII。スペースは不可）

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- キー番号は NTP 認証キーリストのキー値を指定します。最大 255 キーがスイッチに設定できます。設定をおこないたいキー全て入力するため、繰り返しコマンドを使用してください。
- NTP 認証キー番号と値は、サーバとクライアントで一致する必要があります。
- NTP 認証は任意です。NTP 認証が有効な際は同時にこのコマンドを使用し、最低 1 つのキー番号を設定してください。

例

```
Console(config)#ntp authentication-key 45 md5 thisiskey45
Console(config)#
```

関連するコマンド

ntp authenticate（P369）

show ntp

現在の時刻と、NTP クライアント設定を表示します。また、ローカル時刻が適切に更新されたか否かも示します。

コマンドモード

Normal Exec, Privileged Exec

例

```
Console#show ntp
Current time: Jan 1 02:58:58 2001
Poll interval: 16
Current mode: unicast
NTP status : Enabled NTP Authenticate status : Enabled
Last Update NTP Server: 0.0.0.0      Port: 0
Last Update time: Dec 31 00:00:00 2000 UTC
NTP Server 192.168.3.20 version 3
NTP Server 192.168.3.21 version 3
NTP Server 192.168.3.22 version 2
NTP Server 192.168.4.50 version 3 key 30
NTP Server 192.168.5.35 version 3 key 19
NTP Authentication-Key 12 md5 156S46Q24142414222711K66N80 7
NTP Authentication-Key 19 md5 Q33O16Q6338241J022S29Q731K7 7
NTP Authentication-Key 30 md5 D2V8777I51K1132K3552L26R6141O4 7
NTP Authentication-Key 45 md5 3U865531O13K38F0R8 7
NTP Authentication-Key 125 md5 A48S2810327947M76 7
Console#
```

clock timezone-predefined

スイッチ内部時計のために、既定義タイムゾーンの設定をおこないます。

"no" **を前に置くことで、設定を初期値に戻します。**

文法

clock timezone-predefined *off-set city*

no clock taimezone-predefined

- *off-set* ー GMT **からのオフセットを選択します（範囲：**GMT-0100 ー GMT-1200**；**GMT-Greenwich-Mean-Time;GMT+0100 ー GMT+1300**）**
- *city* ー**選択された** GMT **と関連付けられる都市**

初期設定

GMT-Greenwich-Mean-Time-Dublin,Edinburgh,Lisbon,London

コマンドモード

Global Configuration

例

```
Console(config)#clock timezone-predefined GMT-0930-Taiohae
Console(config)#
```

関連するコマンド

show sntp（P366）

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* ー**タイムゾーン名（範囲：**1-29 **文字）**
- *hours* ー UTC **との時間差（時間）（範囲：**0-12 **時間）**
- *minutes* ー UTC **との時間差（分）（範囲：**0-59 **分）**
- *before-utc* ー 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* ー 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 （P366）

clock summer-time (date)

サマータイムの設定をおこないます。
"no" **を前に置くことで、サマータイムを無効にします。**

文法

clock summer-time *name* **date** *b-month b-day b-year b-hour b-minute e-month e-day e-year e-hour e-minute offset minute*

no clock summer-time

- *name* **－タイムゾーン名（範囲：**1-30 **文字）**
- *b-month* **－サマータイム開始の月（範囲：**january-december**）**
- *b-day* **－サマータイム開始の日（範囲：**sunday-saturday**）**
- *b-year* **－サマータイム開始の年**
- *b-hour* **－サマータイム開始の時間（時）**
- *b-minute* **－サマータイム開始の時間（分）**
- *e-month* **－サマータイム終了の月（範囲：**january-december**）**
- *e-day* **－サマータイム終了の日（範囲：**sunday-saturday**）**
- *e-year* **－サマータイム終了の年**
- *e-hour* **－サマータイム終了の時間（時）**
- *e-minute* **－サマータイム終了の時間（分）**
- *offset* **－レギュラータイムゾーンからのサマータイムオフセット（範囲：**0-99 **分）**

初期設定

無効

コマンドモード

Global Configuration

例

```
Console(config)#clock summer-time DEST date april 1 2007 23 23
april 23  2007 23 23 60
Console(config)#
```

関連するコマンド

show sntp（P366）

clock summer-time (predefined)

既定義サマータイム設定をおこないます。
"no" **を前に置くことで、サマータイムを無効にします。**

文法

clock summer-time *name* **predefined** <australia | europe | new-zealand | usa>
no clock summer-time

- *name* ― **タイムゾーン名（範囲：**1-30 **文字）**

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

既定義のサマータイムパラメータ

地域	開始時刻、日、週、月	終了時刻、日、週、月	Rel.Offset
Autsralia	00:00:00, Sunday, Week 5 of October	23:59:59, Sunday, Week 5 of March	60 **分**
Europe	00:00:00, Sunday, Week 5 of March	23:59:59, Sunday, Week 5 of October	60 **分**
New Zealand	00:00:00, Sunday, Week 1 of October	23:59:59, Sunday, Week 3 of March	60 **分**
USA	02:00:00, Sunday, Week 2 of March	02:00:00, Sunday, Week 1 of November	60 **分**

例

```
Console(config)#clock summer-time MESZ predefined europe
Console(config)#
```

関連するコマンド

show sntp（P366）

clock summer-time (recurring)

サマータイムの設定をおこないます。（循環）
"no" **を前に置くことで、サマータイムを無効にします。**

文法

clock summer-time *name* **recurring** *b-week b-day b-month b-hour b-minute*
e-week e-day e-month e-hour e-minute offset

no clock summer-time

- *name* **－タイムゾーン名（範囲：**1-30 **文字）**
- *b-week* **－サマータイム開始の週（範囲：**1-5**）**
- *b-day* **－サマータイム開始の日（範囲：**sunday-saturday**）**
- *b-month* **－サマータイム開始の月（範囲：**january-december**）**
- *b-hour* **－サマータイム開始の時間（時）**
- *b-minute* **－サマータイム開始の時間（分）**
- *e-week* **－サマータイム終了の週（範囲：**1-5**）**
- *e-day* **－サマータイム終了の日（範囲：**sunday-saturday**）**
- *e-month* **－サマータイム終了の月（範囲：**january-december**）**
- *e-hour* **－サマータイム終了の時間（時）**
- *e-minute* **－サマータイム終了の時間（分）**
- *offset* **－レギュラータイムゾーンからのサマータイムオフセット（範囲：**0-99 **分）**

初期設定

無効

コマンドモード

Global Configuration

例

```
Console(config)#clock summer-time MESZ recurring 1 friday june 23
59 3
saturday september 2 55 60
Console(config)#
```

関連するコマンド

show sntp（P366）

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* ー時間（範囲：0 - 23）
- *min* ー分（範囲 0 - 59）
- *sec* ー秒（範囲 0 - 59）
- *day* ー日付（範囲：1-31）
- *month* ー月：<**january | february | march | april | may | june | july | august | september | october | november | december**>
- *year* ー年（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#
```

4.5.10 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	P379
cluster commander	スイッチをクラスタコマンダに設定	GC	P380
cluster ip-pool	クラスタ IP アドレスプールを設定	GC	P381
cluster member	候補スイッチをクラスタメンバーに設定	GC	P382
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	P383
show cluster	スイッチクラスタリング設定を表示	PE	P384
show cluster members	現在のクラスタメンバーを表示	PE	P384
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	P384

スイッチクラスタリングの使用

- スイッチクラスタは " コマンダと呼ばれるプライマリユニットを持ちます。これは、クラスタ内のその他全ての "Member" スイッチを管理するために使用されます。管理ステーションは Tenet と Web インタフェースの両方を使用し、その IP アドレスを通るコマンドと直接通信します。
- 一旦スイッチがクラスタコマンダに設定されると、自動的にネットワーク内の他のクラスタ有効スイッチを検索します。管理ステーションからアドミニストレータに手動で選択された際、"Candidate" スイッチはクラスタメンバにのみなれます。

[注意] クラスタメンバスイッチはコマンダへの Telnet 接続またはコマンダへの Web 管理接続によって管理されることが可能です。コンソール接続使用時、メンバスイッチへの接続にはコマンダ CLI プロンプトから "rcommand" コマンド（P383）を使います。

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 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 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 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:    24/48 L2/L4 IPV4/IPV6 GE Switch
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  24/48 L2/L4 IPV4/IPV6 GE Switch
CANDIDATE       00-12-cf-0b-47-a0  24/48 L2/L4 IPV4/IPV6 GE Switch
Console#
```

4.5.11 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	P385
upnp device ttl	TTL 値を設定	GC	P386
upnp device advertise duration	アドバタイズメント継続時間を設定	GC	P386
show upnp	UPnP ステータスおよびパラメータの表示	PE	P387

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（P386）

upnp device advertise duration（P386）

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（P386）

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#
```

4.6 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
通常 SNMP コマンド			
snmp-server	SNMP **サーバーを有効化**	GC	P389
show snmp	SNMP **の設定情報を表示**	NE,PE	P390
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	P391
snmp-server contact	**システムコンタクト情報の設定**	GC	P392
snmp-server location	**システム設置情報の設定**	GC	P392
SNMP ターゲットホストコマンド			
snmp-server host	SNMP **メッセージを受信するホストの設定**	GC	P393
snmp-server enable traps	SNMP **メッセージを受信するホストの有効化**	GC	P395
SNMPv3 コマンド			
snmp-server engine-id	**エンジン** ID **の設定**	GC	P396
show snmp engine-id	**エンジン** ID **の表示**	PE	P397
snmp-server view	**ビューの設定**	GC	P398
show snmp view	**ビューの表示**	PE	P399
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	P400
show snmp group	**グループの表示**	PE	P401
snmp-server user	SNMP v3 **グループへユーザーの追加**	GC	P403
show snmp user	SNMP v3 **ユーザーの表示**	PE	P404
ATC トラップコマンド			
snmp-server enable port-traps atc broadcast-alarm-fired	**ブロードキャストトラフィックが自動ストームコントロールの上限値を超えた時にトラップを送信**	IC (Port)	P563
snmp-server enable port-traps atc multicast-alarm-fire	**マルチキャストトラフィックが自動ストームコントロールの上限値を超えた時にトラップを送信**	IC (Port)	P563
snmp-server enable port-traps atc broadcast-alarm-clear	**ストームコントロールレスポンスが発生した後、ブロードキャストトラフィックが下限値を下回った特にトラップを送信**	IC (Port)	P564
snmp-server enable port-traps atc multicast-alarm-clear	**ストームコントロールレスポンスが発生した後、マルチキャストトラフィックが下限値を下回った特にトラップを送信**	IC (Port)	P565
snmp-server enable port-traps atc broadcast-control-apply	**ブロードキャストトラフィックが自動ストームコントロールの上限値を越え、アプライタイマが失効した時にトラップを送信**	IC (Port)	P566
snmp-server enable port-traps atc multicast-control-apply	**マルチキャストトラフィックが自動ストームコントロールの上限値を越え、アプライタイマが失効した時にトラップを送信**	IC (Port)	P566
snmp-server enable port-traps atc broadcast-control-release	**ブロードキャストトラフィックが自動ストームコントロールの上限値を越え、アプライタイマが失効した時にトラップを送信**	IC (Port)	P567
snmp-server enable port-traps atc multicast-control-release	**マルチキャストトラフィックが自動ストームコントロールの上限値を越え、アプライタイマが失効した時にトラップを送信**	IC (Port)	P568

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。

文法

snmp-server

no snmp-server

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 < 1c | 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 P54 「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

SNMP Version：1

UDP ポート：162

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。**

  インフォームを SNMPv2 **ホストへ送信するには、以下のステップを行ってください。**

  （1）SNMP **エージェントを有効にする。**(P389)
  （2）スイッチに SNMP **トラップ（通知）送信を許可する。**(P395)
  （3）本項で解説する "snmp-server host" **コマンドを使用し、インフォームメッセージを受信するターゲットホストを指定。**
  （4）必要な通知メッセージでビューを作成。(P398)
  （5）必要な通知ビューを含むグループを作成。(P400)

  インフォームを SNMPv2 **ホストへ送信するには、以下のステップを行ってください。**
  （1）SNMP **エージェントを有効にする。**(P389)
  （2）スイッチに SNMP **トラップ（通知）送信を許可する。**(P395)
  （3）本項で解説する "snmp-server host" **コマンドを使用し、インフォームメッセージを受信するターゲットホストを指定。**
  （4）必要な通知メッセージでビューを作成。(P398)
  （5）必要な通知ビューを含むグループを作成 (P400)
  （6）ユーザが属するリモートエンジン ID **を指定** (P396)
  （7）リモートユーザの設定 (P403)

- **スイッチは** SNMPv1,2c,3 **通知を管理ステーションがサポートする** SNMP **バージョンに基づいて、ホスト** IP **アドレスに送信出来ます。**
  "snmp-server host" **コマンドが** SNMP **バージョンを指定しない場合、初期設定では** SNMP **バージョン** 1 **の通知を送信します。**

- 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** P403 **「**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（P395）

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（P393）

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** P393 **「**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)#
```

関連するコマンド

snmp-server host （P393）

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

項目	解説
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#
```

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*} <include | exclude>

no snmp-server view *view-name*

- *view-name* — **ビューの名前（**1-64 **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**
- include — include **ビューを指定**
- exclude —exclude **ビューを指定**

初期設定

デフォルトビュー（全ての MIB **ツリーへのアクセスを含む）**

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

項目	解説
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 P54 「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（1-64 文字）
- *writeview* — write アクセスのビューを設定します（1-64 文字）
- *notify view* — 通知ビューを設定します（1-64 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 P65 「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 P395 「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

項目	解説
groupname	**グループ名**
security model	**セキュリティモデル**
read view	read **ビュー**
write view	write **ビュー**
notify view	**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: fxc
Security Model: v3
Read View: defaultview
Write View: none
Notify View: none
Storage Type: nonvolatile
Row Status: active

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 {encrypted} {auth <md5 | sha > *auth-password* **}**

{priv des56 *priv-password* } >

no snmp-server user *username* { v1 | v2c | v3 | remote *IP Address* }

- *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
- encrypted ― 暗号化パスワード
- auth ― 認証を使用します
- md5 | sha ― MD5 または SHA 認証を選択します
- *auth-password* ― 認証パスワード（8 文字以上）
- priv des56 ― プライバシーと DES56 暗号化 SNMP V3 を使用
- *priv-password* ― プライバシーパスワード

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 P57 「トラップマネージャ・トラップタイプの指定」および P63 「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 r&d v3 auth md5 greenpeace priv des56
einstien
Console(config)#snmp-server user mark 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

項目	解説
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#
```

4.7 フローサンプリング

フローサンプリング（sFlow）機能は、リモート sFlow コレクタと共に本機に装備されており、ネットワーク管理者はトラフィックのタイプとレベルのオーバービューを正確・詳細かつリアルタイムで確認できます。
SFlow エージェントは、本機を通過する全てのパケットから n の内１のパケットを採取します。sFlow データグラムとしてサンプルを再度カプセル化し、これらを sFlow コレクタに転送します。
このサンプリングは内部ハードウェアレベルで起こるのに対し、従来の調査はモニタインタフェースでサンプルされたトラフィックの部分的なビューのみの物でした。
さらに、ローカル分析は行われない為、sFlow エージェントによって課せられるプロセッサとメモリロードは最小です。

コマンド	機能	モード	ページ
sflow	スイッチで sFlow を有効化	GC	P406
sflow source*	モニタを行われるソースポートで sFlow を有効化	IC	P406
sflow sample*	パケットサンプリングレートを設定	IC	P407
sflow polling-interval	カウンタがサンプルデータグラムへ追加される間隔を設定	IC	P407
sflow owner	レシーバの名前を設定	IC	P408
sflow timeout	全ての sFlow ポートパラメータがリセットされる前に、サンプルがコレクタに送られる時間を設定	IC	P408
sflow destination	コレクタで使用される IP アドレスおよび UDP ポートを設定	IC	P409
sflow max-header-size	sFlow データグラムヘッダの最大サイズを設定	IC	P409
sflow max-datagram-size	sFlow データグラムペイロードの最大サイズを設定	IC	P410
show sflow	グローバルおよびインタフェースの sFlow プロセス設定を表示	PE	P410

* スイッチのハードウェアデザインにより、これらのコマンドは特定のポートグループ（1-8、9-16、25-32、33-48）でのみ有効に出来ます。ただしギガビットコンビネーションポート（49-52）は個々にコントロールが出来ます。

sflow

sFlow をスイッチのグローバルで有効にします。"no" を前に置くことで機能を無効にします。

文法

sflow
no sflow

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

- フローサンプリングは、必要とされるポートと同様にスイッチでグローバルに有効にする必要があります。（"sflow source" コマンド（P406）を参照）

例

```
Console(config)#sflow
Console(config)#
```

sflow source

モニタをされるソースポートで sFlow を有効にします。"no" を前に置くことで、指定されたポートで sFlow を無効にします。

文法

sflow source

no sflow source

初期設定

無効

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- 100BASE-TX ポートは、スイッチの ASIC 制限の理由で 8 つのグループに組織化されます（1-8, 9-16, 17-24, 25-32, 33-48）。これらのグループの中の 1 ポートを選択することで、グループメンバー全てを sFlow ソースポートとして設定します。
  4 つのギガビットポート（49-52）は個々に設定を行うことが可能です。

例

ポート 9 から 16 までを sFlow 有効にしています。

```
Console(config)#interface ethernet 1/9
Console(config-if)#sflow source
Console(config-if)#
```

sflow sample

パケットサンプリングレートを設定します。"no" **を前に置くことで初期レートへ戻します。**

文法

sflow sample *rate*

no sflow sample

- *rate* — **パケットサンプリングレートまたは** 1 **つのサンプルで採取されるパケット数（範囲：**0-10000000　0 **はサンプリング無効）**

初期設定

無効

コマンドモード

Interface Configuration (Ethernet)

例

100 **パケット毎に** 1 **つのパケットレートを設定しています。**

```
Console(config)#interface ethernet 1/9
Console(config-if)#sflow sample 100
Console(config-if)#
```

sflow polling-interval

カウンタがサンプルデータグラムへ追加される間隔を設定します。
"no" **を前に置くことで設定を初期値へ戻します。**

文法

sflow polling-interval *seconds*

no sflow polling-interval

- *seconds* — sFlow **プロセスがカウンタ値をサンプルデータグラムへ追加する間隔（範囲：**0-10000000 **秒**　0 **は機能を無効）**

初期設定

無効

コマンドモード

Interface Configuration (Ethernet)

例

```
Console(config)#interface ethernet 1/9
Console(config-if)#sflow polling-interval 10
Console(config-if)#
```

sflow owner

レシーバの名前を設定します。"no" **を前に置くことで、設定した名前を削除します。**

文法

sflow owner *name*

no sflow owner

- *name* — **レシーバ名** (**範囲：**1-256 **文字**)

初期設定

なし

コマンドモード

Interface Configuration (Ethernet)

例

```
Console(config)#interface ethernet 1/9
Console(config-if)#sflow owner Lamer
Console(config-if)#
```

sflow timeout

全ての sFlow **パラメータがリセットされる前に、サンプルがコレクタへ送られる時間を設定します。**"no" **を前に置くことで設定を初期値に戻します。**

文法

sflow timeout *seconds*

no sflow timeout

- *seconds* — **s** Flow **プロセスが連続的に送信される時間**
  （範囲：0-10000000 **秒　**0 **はタイムアウト無し）**

初期設定

無効

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

このコマンドで影響を受ける sFlow **パラメータは** "sampling interval"、"receiver's name"、"address and UDP port"、"time out"、"maximum header size" **および** "maximum datagram size" **です。**

例

```
Console(config)#interface ethernet 1/9
Console(config-if)#sflow timeout 10000
Console(config-if)#
```

sflow destination

コレクタで使用される IP **アドレスと** UDP **ポートを設定します。**"no" **を前に置くことで設定を初期値に戻します。**

文法

sflow destination ipv4 *ip-address* { *destination-udp-port* }

no sflow destination

- *ip-address* — **s** Flow **コレクタの** IP **アドレス**
- destination-udp-port — UDP **ポート（範囲：**0-65534**）**

初期設定

IP **アドレス：なし**

UDP **ポート：**6343

コマンドモード

Interface Configuration (Ethernet)

例

```
Console(config)#interface ethernet 1/9
Console(config-if)#sflow destination ipv4 192.168.0.4
Console(config-if)#
```

sflow max-header-size

sFlow **データグラムヘッダの最大サイズを設定します。**"no" **を前に置くことで設定を初期値へ戻します。**

文法

sflow max-header-size *max-header-size*

no sflow max-header-size

- *max-header-size* — sFlow **データグラムヘッダの最大サイズ（範囲：**64-256 bytes**）**

初期設定

128bytes

コマンドモード

Interface Configuration (Ethernet)

例

```
Console(config)#interface ethernet 1/9
Console(config-if)#sflow max-header-size 256
Console(config-if)#
```

sflow max-datagram-size

sFlow データグラムペイロードの最大サイズを設定します。"no" を前に置くことで設定を初期値へ戻します。

文法

sflow max-datagram-size *max-datagram-size*
no sflow max-datagram-size

- *max-datagram-size* — sFlow データグラムペイロードの最大サイズ（範囲：200-1500 bytes）

初期設定

1400bytes

コマンドモード

Interface Configuration (Ethernet)

例

```
Console(config)#interface ethernet 1/9
Console(config-if)#sflow max-datagram-size 1500
Console(config-if)#
```

show sflow

sFlow プロセスのグローバルおよびインタフェース設定を表示します。

文法

sflow sflow *interface*

- *interface*
  - **ethernet** *unit/port*
    - *unit* — ユニット番号 ”1”
    - *port* — ポート番号 （範囲：1-52）

コマンドモード

Privileged Exec

例

```
Console#show sflow
 sFlow global status : Enabled
Console#show sflow interface ethernet 1/1
 Interface of Ethernet  1/1  :
   Interface status      : Enabled
   Owner name            : Lamar
   Owner destination     : 192.168.0.4
   Owner socket port     : 6343
   Time out              : 0
   Maximum header size   : 256
   Maximum datagram size : 1500
   Sample rate           : 1/100
   Polling interval      : 10
Console#
```

4.8 認証コマンド

コマンドグループ	機能	ページ
User Accounts	管理アクセスの基本ユーザ名、パスワードを設定	P411
Authentication Sequence	ログイン認証方式と優先順位の設定	P416
RADIUS Client	RADIUS サーバ認証の設定	P418
TACACS+ Client	TACACS+ サーバ認証の設定	P424
AAA	認証 , 認可 , アカウンティング (AAA) の設定	P428
Web Server	Web ブラウザからの管理アクセスを有効化	P439
Telnet Server	Telnet サーバからの管理アクセスを有効化	P443
Secure Shell	Telnet に安全なリプレイスを提供	P444
Port Authentication	EEE802.1X によるポート認証の設定	P454
Management IP Filter	管理アクセスを許可される IP アドレスを設定	P465

4.8.1 ユーザーアカウント

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、P337 **「**password**」や** P416 **「認証シーケンス」、**P454 **「**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	P412
enable password	各アクセスレベルのパスワードの設定	GC	P413
privilege	指定されたコマンドグループまたは個々のコマンドに privilege レベルを割り当て	GC	P414
privilege rerun	現在のセッション中に入力された privilege コマンドを実行設定ファイルにアップデート	PE	P415
show privilege	現在のユーザの privilege レベルまたは privilege コマンドによって修正されたコマンドの privilege レベルを表示	PE	P415

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 [l eve l *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。P292 「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（P292）

authentication enabled（P417）

privilege

指定したコマンドグループまたは個々のコマンドに privilege **レベルを割り当てます。**
"no" **を使用することで設定を初期値に戻します。**

文法

privilege *mode* { all } level *level command*

no privilege *mode* { all } *command*

- *mode* ― **指定したコマンド（**P286**、**P287 **を参照）を含む設定モード**
- all ― **指定されたコマンド下の全てのサブコマンドの** privilege **レベルを修正**
  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。**
- *level* ― **指定されたコマンドに** privilege **レベルを設定。**
  本機は 3 **つの既定義** privilege **レベル（**0**：**Normal Exec,8**：**Manager, 15**：**Privileged Exec**）を持ちます。（範囲：**0-15**）**
- *command* ― **指定されたモードを含むコマンドを指定。**

初期設定

Level 0**：スイッチの現在のステータスを表示するコマンドの限定された数と、いくつかのデータベースのクリアおよびリセット機能へアクセスを提供**

Level 8**：種々の認証を制御しているそれらとセキュリティ機能以外、全ての表示されるステータスと設定にアクセスを提供**

Level 15**：全てのコマンドにをフルアクセスを提供**

コマンドモード

Global Configuration

例

```
Console(config)#privilege exec level 15 ping
Console(config)#
```

privilege rerun

running configuration ファイルへ、現在のセッションの間に入力された全ての privilege コマンドを更新します。

コマンドモード

Privileged Exec

コマンド解説

現在のソフトウェアのシステム制限により現在のスイッチセッションの間に入力された privilege コマンドは running-config file （"show running-config" P317 参照）へ正しく保存されません。その為、running-config ファイルへこれらのコマンドを正確に更新するには、privilege rerun コマンドを使用します。

例

```
Console#privilege rerun
Console#
```

show privilege

現在のユーザの privilege レベルまたは "privilege" コマンド（P414）で修正されたコマンドの privilege レベルを表示します。

文法

show privilege { *command* }

- *command* — privilege コマンドで編集された全てのコマンドの privilege レベルを表示

コマンドモード

Privileged Exec

例

```
Console#show privilege command
privilege line all level 0 accounting
privilege exec level 15 ping
Console(config)#
```

4.8.2 認証シーケンス

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	P416
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	P416

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（P412）

authentication enable

"enable" コマンド（P292）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（P292）― コマンドモード変更のためのパスワードの設定

4.8.3 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	P419
radius-server acct-port	RADIUS **サーバネットワークポートの設定**	GC	P420
radius-server auth-port	RADIUS **サーバネットワークポートの設定**	GC	P420
radius-server key	RADIUS **暗号キーの設定**	GC	P421
radius-server retransmit	**リトライ回数の設定**	GC	P422
radius-server timeout	**認証リクエストの間隔の設定**	GC	P422
show radius-server	RADIUS **関連設定情報の表示**	PE	P423

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：**1-65535 **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：**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。間にスペースは入れられません（最大** 20 **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 acct-port

アカウンティングメッセージに使用する、RADIUS **サーバネットワーク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 port acct-port *port_number*

no radius-server acct-port

- *port_number* — **アカウンティングメッセージに使用される、**RADIUS **サーバ認証用** 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 181
Console(config)#
```

radius-server auth-port

アカウンティングメッセージに使用する、RADIUS **サーバネットワーク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 port auth-port *port_number*

no radius-server auth-port

- *port_number* —**認証メッセージに使用される、**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 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

Remote RADIUS Server Configuration:

Global Settings:
 Authentication Port : 1812
 Accounting Port : 1813
 Retransmit Times : 2
 Request Timeout : 5 seconds

Attributes:
 NAS-IP-Address (4) : 192.168.1.1

Server 1:
 Server IP Address : 10.1.2.3
 Authentication Port : 1812
 Accounting Port : 1813
 Retransmit Times : 2
 Request Timeout : 5 seconds

Radius server group:
 Group Name            Member Index
 --------------------- -------------
 radius                           1
Console#
```

4.8.4 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	P424
tacacs-server port	TACACS+ サーバのポートの設定	GC	P425
tacacs-server key	TACACS+ 暗号キーの設定	GC	P425
tacacs-server retransmit	リトライ回数の設定	GC	P426
tacacs-server timeout	認証リクエストの間隔の設定	GC	P425
show tacacs-server	TACACS+ 関連設定情報の表示	GC	P427

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：20 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#
```

4.8.5 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	P429
server	**グループリスト内サーバの IP アドレスを設定**	SG	P429
aaa accounting dot1x	802.1X **サービスのアカウンティングを有効**	GC	P430
aaa accounting exec	Exec **サービスのアカウンティングを有効**	GC	P431
aaa accounting commands	Exec **モードコマンドのアカウンティングを有効**	GC	P432
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	P433
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	P433
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	P434
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	P435
aaa authorization exec	Exec **セッションの許可を有効**	GC	P436
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	P437
show accounting	**アカウンティング情報の表示**	PE	P438

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（**P418 **参照）**
  - tacacs+ — TACACS+ **サーバに設定された全ての** TACACS+ **ホスト（**P424 **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（**P429 **参照）**

初期設定

アカウンティング：無効

サーバ：未指定

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（**P418 **参照）**
  - tacacs+ — TACACS+ **サーバに設定された全ての** TACACS+ **ホスト（**P424 **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（**P429 **参照）**

初期設定

アカウンティング：無効

サーバ：未指定

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
  - tacacs+ — TACACS+ サーバに設定された全ての TACACS+ ホスト（P424 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（P429 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* ー **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 ー "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（**P430 **参照）**
- *list-name* ー "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（**P430 **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* **ー実行コマンドの特権レベル（範囲：**0-15**）**
- default ー "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（**P430 **参照）**
- *list-name* ー "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 ー 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* ーメソッド名を指定します
- group ー使用するサーバグループを指定します
  - ー tacacs+ ー TACACS+ サーバに設定された全ての TACACS+ ホスト（P424 参照）
  - ー *server-group* ー 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（P429 参照）

初期設定

認証：有効
サーバ：未指定

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 ー "aaa authorization exec" **で作成されたデフォルトメソッドリスト（**P436 **参照）**
- *list-name* ー "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 *interface* } } | exec { statistics } } | statistics }

- commands **ー特権レベルコマンドアカウンティング情報の表示**
- *level* ー CLI **コマンドの特権レベル（範囲：**0-15**）**
- dot1x ー dod1x **アカウンティング情報の表示**
- exec ー exec **アカウンティング情報の表示**
- statistics **ーアカウンティング記録の表示**
- *user-name* **ー指定したユーザーのアカウンティング記録の表示**
- *interface*

ー ethernet *unit/port*

ー *unit* ― **ユニット番号** "1"

ー *port* ― **ポート番号（範囲：**1-52**）**

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:

 Method list: tps
 Group list: radius
 Interface: eth 1/2

Accounting type: Exec
 Method list: default
 Group list: radius
 Interface: vty

Console#
```

4.8.6 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	P439
ip http server	管理用 Web インタフェースの使用	GC	P440
ip http secure-server	セキュア HTTP（HTTPS）サーバの使用	GC	P441
ip http secure-port	HTTPS 接続に使用するポートの設定	GC	P442

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（P440）

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（P439）

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
Mozilla Firefox 2.0.0.0 以上	Windows 2000、Windows XP、Linux

※セキュアサイト証明の詳細は P92 「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（P442）

copy tftp https-certificate（P323）

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（P441）

4.8.7 Telnet サーバーコマンド

コマンド	機能	モード	ページ
ip telnet server	管理用 Telnet インタフェースの使用	GC	P443

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 telnet server { port *port-number* }

no ip telnet server { port }

- port － Telnet インタフェースが使用する TCP ポート
- *port-number* －ブラウザインタフェースが使用する TCP ポート番号 (1-65535)

初期設定

サーバ：有効

サーバポート：23

コマンドモード

Global Configuration

例

```
Console(config)#ip telnet server
Console(config)#ip telnet server port 123
Console(config)#
```

4.8.8 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	P446
ip ssh timeout	SSH サーバの認証タイムアウト設定	GC	P447
ip ssh authentication -retries	クライアントに許可するリトライ数の設定	GC	P448
ip ssh server-key size	SSH サーバキーサイズの設定	GC	P448
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	P323
delete public-key	特定ユーザの公開キーの削除	PE	P449
ip ssh crypto host-key generate	ホストキーの生成	PE	P450
ip ssh crypto zeroize	RAM からのホストキーの削除	PE	P451
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	P451
disconnect	ライン接続の終了	PE	P345
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	P452
show ssh	SSH セッション状態の表示	PE	P452
show public-key	特定のユーザ又はホストの公開キーの表示	PE	P453
show users	SSH ユーザ、アクセスレベル、公開キータイプの表示	PE	P320

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
15684995401867669259333946775054617325313674890836547254150202455931998685443583616519999233297817660658309561082591321289023376546801726272571413428762941301196195566782595664104869574278881462065194174677298486546861571773939016477935594230357741309802273708779454524083971752646358058176716709574804776117

(3) **クライアント公開キーの本機への取り込み** — P324 「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
13410816856098939210409449201554253476316419218729589211431738800555361616310517759408386863110929123222682851925437460310093718772119969631781366277414168985132049117204830339254324101637997592371449011938006090253948408482717819437228840253311595213486102290297898272135326713162943253281891504530639391664 3 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#configure
Console(config)#ip ssh server
Console(config)#
```

[注意] ホストキー生成には５分程度かかります。

関連するコマンド

ip ssh crypto host-key generate（P450）

show ssh（P452）

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

10 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（P339）

show ip ssh（P452）

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（P452）

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* ー SSH **サーバ名（設定範囲：**1-8 **文字）**
- dsa ー DSA **公開キータイプ**
- rsa ー 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 ー DSA（Version2）キータイプ
- rsa ー 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 （P451）

ip ssh save host-key （P451）

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 （P450）

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：1-8 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#
```

4.8.9 802.1x 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	P454
dot1x default	dot1x **の設定値をすべて初期設定に戻します。**	GC	P455
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	P455
dot1x port-control	**ポートへの** dot1x **モードの設定**	IC	P456
dot1x operation-mode	dot1x **ポートへの接続可能ホスト数の設定**	IC	P457
dot1x re-authenticate	**特定ポートへの再認証の強制**	PE	P458
dot1x re-authentication	**全ポートへの再認証の強制**	GC	P458
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	P459
dot1x timeout re-autheperiod	**接続済みクライアントの再認証間隔の設定**	GC	P459
dot1x timeout tx-period	**認証中の** EAP **パケットの再送信間隔の設定**	GC	P460
dot1x timeout supp-timeout	**スイッチが** EAP **パケットの再認証待機中の認証セッションの間の期間を設定**	IC	P461
dot1x intrusion-action	**認証失敗時の、侵入にたいするポート返答**	IC	P462
show dot1x	dot1x **関連情報の表示**	PE	P463

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

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

コマンド解説

- 802.1X **ポート認証およびポートセキュリティは同じポートで同時に設定することはできません。どちらかのセキュリティメカニズムのみ適用されます。**
- 802.1X **ポート認証はトランクポートに設定できません。静的トランクまたは動的トランクは自動または固定非認証モードに設定できません。**
- 802.1X **認証はポートで有効になった際、このポートの** MAC **アドレス学習機能は無効になり、ポートで動的に学習されたアドレスは取り除かれます。**
- **認証された** MAC **アドレスは動的エントリとしてスイッチのセキュア** MAC **アドレステーブルに保存されます。設定された静的** MAC **アドレスは、スイッチポートで見られた時、セキュア** MAC **アドレステーブルへ追加されます。静的** MAC **アドレスは、**RADIUS **サーバへのリクエスト送信無しで、認証されたものととして取り扱われます。**
- **ポートステータスがダウンへ変更された時、セキュア** MAC **アドレステーブルから全ての** MAC **アドレスがクリアされます。静的** VLAN **割り当ては復旧されません。**

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 P456 「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：1-52）

コマンドモード

Privileged Exec

コマンド解説

- 再認証プロセスは、接続されたクライアントのユーザ ID とパスワードを RADIUS サーバで照合します。再認証の間、クライアントはネットワークへの接続を維持し、プロセスは dot1x クライアントソフトウェアによって、透過的に処理されます。
  もし再認証が失敗した場合のみ、ポートはブロックされるか、ユーザはゲスト VLAN に割り当てられます。(462 ページの「dot1x intrusion-action」を参照)

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

コマンド解説

- 再認証プロセスは、接続されたクライアントのユーザ ID とパスワードを RADIUS サーバで照合します。再認証の間、クライアントはネットワークへの接続を維持し、プロセスは dot1x クライアントソフトウェアによって、透過的に処理されます。
  もし再認証が失敗した場合のみ、ポートはブロックされるか、ユーザはゲスト VLAN に割り当てられます。(462 ページの「dot1x intrusion-action」を参照)
- 接続されたクライアントは、" dot1x timeout re-authperiod" コマンド（P459）で設定したインターバルの後、再認証されます。初期設定は 3600 秒です。

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 timeout supp-timeout

スイッチのインタフェースが EAP **パケットを再送信する前に、クライアントから** EAP **リクエストへの返答待つ時間を設定します。**"no" **を前に置くことで設定を初期値に戻します。**

文法

dot1x timeout supp-timeout < *seconds* >

no dot1x timeout supp-timeout

- *seconds* — **秒数（範囲：**1-65535 **秒）**

初期設定

30 **秒**

コマンドモード

Interface Configuration

コマンド解説

- **このコマンドは、**EAP **リクエスト** /EAP identity **フレーム以外のリクエストフレームのタイムアウトを設定します。**dot1x **認証がポートで有効の場合、スイッチは、ポートリンクステーツが来た時に認証を開始します。それはクライアントへアイデンティティを要求するためと、その後に認証情報の** 1 **つ以上の要請を求めるため、**EAP **リクエスト** /EAP identity **フレームをクライアントへ送信します。また、要求された再認証のアクティブな接続の間、その他の** EAP **リクエストフレームをクライアントへ送ります**

例

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout supp-timeout 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。（P623 「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。（P478 「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*
  - ethernet *unit/port*

    unit — **ユニット番号** “1”
    port — **ポート番号（範囲：**1-52）

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 — P457 **「**dot1x operation-mode**」の設定値**
  - Mode — dot1x port-control **で設定する** dot1x **モード** (P456)
  - 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** (P458)
  - reauth-period - **接続されたクライアントに再認証を要求する間隔** (P459)
  - 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** (P459)
  - tx-period - **認証時に** EAP **パケットの再送信を行う間隔** (P460)
  - 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** (P455)
  - 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** (P457)
  - 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** (P456)
  - 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)
  - Intrusion action - **認証失敗時、スイッチが全ての非** EAP **トラフィックをブロックするか、ゲスト** VLAN **へのポートにトラフィックをアサインするかを表示**
- *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
Global 802.1X Parameters
system-auth-control: enable

802.1X Port Summary

Port Name Status Operation Mode Mode Authorized
1/1 disabled Single-Host ForceAuthorized n/a
1/2 enabled Single-Host auto yes ...
1/28 disabled Single-Host ForceAuthorized n/a

802.1X Port Details

802.1X is disabled on port 1/1

802.1X is enabled on port 1/2
 reauth-enabled: Enable
 reauth-period: 1800
 quiet-period: 30
 tx-period: 40
 supplicant-timeout: 30
 server-timeout: 10
 reauth-max: 2
 max-req: 5
Status Authorized
Operation mode Single-Host
Max count 5
Port-control Auto
Supplicant 00-12-cf-49-5e-dc
Current Identifier 3
Intrusion action Guest VLAN

Authenticator State Machine
State Authenticated
Reauth Count 0

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

Reauthentication State Machine
State Initialize
.
.
.
```

4.8.10 管理 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	P465
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	P466

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

全てのアドレス

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#
```

4.9 セキュリティ

本機はそれぞれのデータポートに接続されたクライアントのためにトラフィックを分離、また認証されたクライアントのみネットワークへのアクセスを可能にするため様々なメソッドをサポートしています。プライベート VLAN と IEEE 802.1X を使用したポートベース認証は通常これらの目的のために使用されます。
この節では、これらのメソッドに加え、クライアントセキュリティを提供するためのその他多数のオプションについて説明します。

コマンド	機能	ページ
Private VLANs	プライベート VLAN アップリンク、ダウンリンクポートの設定	P652
Port Security*	ポートのセキュアアドレスを設定	P467
Port Authentication*	802.1X を利用した、指定したポートでのホスト認証を設定	P454
Network Access*	MAC 認証及び動的 VLAN 割り当ての設定	P469
Web Authentication*	Web 認証の設定	P486
Access Control Lists*	IP フレーム（アドレス、プロトコル、レイヤ 4 プロトコルポート番号、TCP コントロールコードを基にする）、IP フレーム以外（MAC アドレスまたはイーサネットタイプを基にする）のフィルタリングを提供	P518
DHCP Snooping*	DHCP スヌーピングバインディングテーブルによる、アントラスト DHCP メッセージのフィルタ	P493
IP Source Guard*	DHCP スヌーピングテーブル上の動的エントリを基にし、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	P502
ARP Inspection	ARP パケットで MAC-to-IP アドレスバインディングの妥当性を検査	P507

* これらフィルタリングコマンド実行のプライオリティは、Port Security、Port Authentication、Network Access、Web Authentication、Access Control Lists、DHCP Snooping、IP Source Guard になります。

4.9.1 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	P468
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	P587
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	P588

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。**
- **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：**
  - ― **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
```

4.9.2 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ことがあります。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 aging	MAC アドレスエージングの有効化	GC	P470
network-access mac-filter	MAC アドレスをフィルタテーブルへ追加	GC	P471
network-access port-mac-filter	指定した MAC アドレスフィルタを有効化	IC	P472
network-access max-mac-count	インタフェースの認証 MAC アドレス最大数を設定	IC	P473
network-access mode	インタフェースで MAC 認証を有効	IC	P474
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	P476
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	P479
mac-authentication intrusion-action	ポートで認証可能な MAC アドレスの最大数を設定	IC	P476
network-access dynamic-vlan	認証ポートの、動的 VLAN 割り当てを有効	IC	P479
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	P478
network-access dynamic-qos	動的 QoS 機能を有効	IC	P479
network-access link-detection	リンク検出機能を有効化	IC	P479
network-access link-detection link-down	リンクダウンイベントを検出し作用するよう、リンク検出機能を有効化	IC	P480
network-access link-detection link-up	リンクアップイベントを検出し作用するよう、リンク検出機能を有効化	IC	P481
network-access link-detection link-up-down	リンクアップ / ダウンイベントを検出し作用するよう、リンク検出機能を有効化	IC	P481
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	P482
show network-access	ポートインタフェースの MAC 認証設定を表示	PE	P483
show network-access mac-filter	MAC フィルタテーブルのエントリ情報を表示	PE	P485

network-access aging

安全な MAC **アドレステーブルに保存されている認証** MAC **アドレスのエージングを有効にします。** "no" **を前に置くことで無効に設定します。**

文法

network-access aging

no network-access aging

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

- **認証された** MAC **アドレスは、スイッチのセキュア** MAC **アドレステーブルに動的エントリとして保存されており、エージングタイムが経過すると削除されます。**
  アドレスエージングタイムについては " mac-address-table aging-time "（P589）**を参照してください。**
- **本機でサポートされている、セキュア** MAC **アドレスの最大数は** 1024 **です。**

例

```
Console(config)#network-access aging
Console(config)#
```

network-access mac-filter

フィルタテーブルに MAC **アドレスを追加します。**"no" **を前に置くことで指定した** MAC **アドレスを取り除きます。**

文法

network-access mac-filter < *filter-id* > mac-address *mac-address* mask *mask*

no network-access mac-filter < *filter-id* > mac-address *mac-address* mask *mask*

- *filter-id* ― MAC **アドレスフィルタテーブルを指定** (**範囲：**1-64)
- *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で範囲を指定**

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

- **指定されたアドレスはネットワーク認証を免除されます。**
- **このコマンドは、マスクを使用しアドレスの範囲を設定する点と、**"network-access port-mac-filter" **を使用し、これらのアドレスを** 1 **つ以上のポートにアサインする点で** " mac-address-table static" **コマンド（**P587**）を使用する静的アドレスの設定とは異なります。**
- **最大** 64 **のフィルタテーブルを定義することができます。**
- **フィルタテーブルに入れるエントリ数に制限はありません。**

例

```
Console(config)#network-access mac-filter 1 mac-address 11-22-33-44-55-66
Console(config)#
```

network-access port-mac-filter

指定した MAC **アドレスフィルタを有効にします。**"no" **を前に置くことで無効にします。**

文法

network-access port-mac-filter < *filter-id* >

no network-access port-mac-filter

- *filter-id* ― MAC **アドレスフィルタテーブルを指定** (**範囲：**1-64)

初期設定

なし

コマンドモード

Interface Configuration

コマンド解説

- **ポートに割り当てられるフィルタテーブルは** 1 **つだけです。**

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access port-mac-filter 1
Console(config-if)#
```

network-access max-mac-count

全ての認証フォームによって、ポートインタフェースで認証できる MAC **アドレスの最大数を設定します。**"no" **を前に置くことで設定を初期状態に戻します。**

文法

network-access max-mac-count *count*

no network-access max-mac-count

- *count* ― **許可される認証** MAC **アドレスの最大数** (**範囲：**1-2048 0 **は制限無し**)

初期設定

2048

コマンドモード

Interface Configuration

コマンド解説

- **ポートごとの** MAC **アドレスの最大数は** 2048 **であり、本機でサポートされているセキュア** MAC **アドレスの最大数は** 1024 **です。制限に達すると、全ての新しい** MAC **アドレスは認証失敗として取り扱われます。**

例

```
Console(config-if)#network-access max-mac-count 5
Console(config-if)#
```

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

コマンド解説

- **ポートで有効の場合、認証プロセスは、設定された** RADIUS **サーバへパスワード認証プロトコル（**PAP**）リクエストを送信します。**
- RADIUS **サーバー上では、**PAP **ユーザ名とパスワードは** MAC **アドレスフォーマットで設定されます。**
- **認証された** MAC **アドレスは、スイッチのセキュアアドレステーブルに動的エントリとして保存され、エージングタイムの期限が切れると削除されます。**
  本機でサポートされているセキュア MAC **アドレスの最大数は** 1024 **です。**
- **スイッチポートで見られた静的** MAC **アドレスはセキュアアドレステーブルに追加されます。静的アドレスは** RADIUS **サーバーへリクエストを送らずに、認証されたアドレスとして取り扱われます。**
- MAC **認証、**802.1X**、ポートセキュリティは同時に同じポートに設定することはできません。**1 **つのセキュリティメカニズムのみが適用できます。**
- MAC **認証はトランクポートに設定できません。**
- **ポートステータスがダウンへ変わると、全ての** MAC **アドレスはセキュアアドレステーブルから削除されます。静的** VLAN **割り当てはリストアされません。**
- RADIUS **サーバはオプションとして、**VLAN **識別のリストを返します。**VLAN **識別リストは** "Tunnel-Private-Group-ID" **属性に載せられます。**VLAN **リストは、**"1u,2t," **フォーマットを使用して、複数の** VLAN **識別を含むことが出来ます。**"u" **はタグ無し** VLAN **を示し、**"t" **はタグ付き** VLAN **を示します。**"Tunnel-Type" **属性は** "VLAN," **と** "Tunnel-Medium-Type" **属性を** "802" **にセットします。**

例

```
Console(config-if)#network-access mode mac-authentication
Console(config-if)#
```

mac-authentication reauth-time

接続された MAC **アドレスが再認証された後の期間を設定します。**"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* ― **再認証間隔** (**範囲：**120-1000000 **秒**)

初期設定

1800

コマンドモード

Global Configuration

コマンド解説

- **再認証時間はグローバル設定と、全てのポートに適用されます。**
- **セキュア** MAC **アドレスの再認証時間の期限が切れると、**RADIUS **サーバーで再び認証がおこなわれます。再認証プロセスの間、ポートを通るトラフィックは影響を受けません。**

例

```
Console(config)#mac-authentication reauth-time 300
Console(config)#
```

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

認証ポートへの動的 VLAN の割り当てを有効にします。"no" を前に置くことで設定を無効にします。

文法

network-access dynamic-vlan

no network-access dynamic-vlan

初期設定

有効

コマンドモード

Interface Configuration

コマンド解説

- 有効時、スイッチに既に VLAN が作成されているならば、RADIUS サーバから返された VLAN 識別子がポートへ適用されます。VLAN を作成する為に GVRP は使用されません。
- 最初に認証された MAC アドレスによって指定された VLAN 設定がポートに導入されます。その他のポートで認証された MAC アドレスは同じ VLAN 設定を持つか、認証失敗として取り扱われます。
- もし動的 VLAN 割り当てがポートで使用可能であり、RADIUS サーバが VLAN 設定を返さないなら、認証は依然成功として取り扱われます。
- ポートで、動的 VLAN 割り当てステータスが変更された場合、全ての認証されたアドレスはセキュア MAC アドレステーブルからクリアされます。

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

コマンド解説

- **ゲスト** VLAN **として使用される** VLAN **は先に定義しアクティブに設定してください（**629 **ページの「**vlan database**」を参照）**
- 802.1X **認証で使用される際には、**"intrusion-action" **は** " guest-vlan" **に対し効果があるよう設定する必要があります。（**P462**）**

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access guest-vlan 25
Console(config-if)#
```

network-access dynamic-qos

認証ポートの、動的 QoS 機能を有効にします。"no" を前に置くことで無効に設定します。

文法

network-access dynamic-qos

no network-access dynamic-qos

初期設定

無効

コマンドモード

Interface Configuration

コマンド解説

- RADIUS サーバはオプションとして、認証されたユーザのスイッチポートへ適用される、ダイナミック QoS 割り当てを返します。"Filter-ID" 属性（属性 11）は以下の QoS 情報を渡す RADIUS サーバで設定されます。

ダイナミック QoS プロファイル

プロファイル	属性構文	例
DiffServ	service-policy-in=policy-map-name	service-policy-in=p1
Rate Limit	rate-limit-input=rate	rate-limit-input=100 (in units of Kbps)
802.1p	switchport-priority-default=value	switchport-priority-default=2

- 最後のユーザが QoS 割り当てを持つポートをログオフする時、スイッチはポートをオリジナル QoS 設定へリストアします。
- ユーザが、既に同じポートへログオンしたユーザと違う動的 QoS プロファイルと共にネットワークへのログインを試みた場合、アクセスは拒否されます。
- ポートが動的プロファイルされている間、全ての手動 QoS 設定変更は、全てのユーザがポートからログオフした後にのみ効果が適用されます。

[注意]　動的 QoS の設定変更はスイッチ設定ファイルに保存されません。

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#network-access dynamic-qos
Console(config-if)#
```

network-access link-detection

選択したポートでのリンク検出を有効にします。"no" **を前に置くことで設定を初期状態に戻します。**

文法

network-access link-detection

no network-access link-detection

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 link-detection
Console(config-if)#
```

network-access link-detection link-down

リンクダウンイベントの検出を行います。検出時、スイッチはポートをシャットダウンするか、SNMP **トラップを送信します。またはその両方を行います。**
"no" **を前に置くことで機能を無効します。**

文法

network-access link-detection link-down action [shutdown | trap | trap-and-shutdown]

no network-access link-detection

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 link-detection link-down action trap
Console(config-if)#
```

network-access link-detection link-up

リンクアップイベントの検出を行います。検出時、スイッチはポートをシャットダウンするか、SNMP トラップを送信します。またはその両方を行います。"no" **を前に置くことで機能を無効します。**

文法

network-access link-detection link-up action [shutdown | trap | trap-and-shutdown]

no network-access link-detection

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 link-detection link-up action trap
Console(config-if)#
```

network-access link-detection link-up-down

リンクアップとリンクダウンイベントの検出を行います。いずれかのイベントを検出時、スイッチはポートをシャットダウンするか、SNMP **トラップを送信します。またはその両方を行います。**"no" **を前に置くことで機能を無効します。**

文法

network-access link-detection link-up-down action [shutdown | trap | trap-and-shutdown]

no network-access link-detection

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 link-detection link-up-down action trap
Console(config-if)#
```

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：**1-52**）**

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* }

- *interface*

  ー ethernet *unit/port*

    ー *unit* ― **ユニット番号** "1"

    ー *port* ― **ポート番号（範囲：**1-52）

初期設定

全てのインタフェースを表示

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：**1-52**）**
- 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#
```

show network-access mac-filter

MAC フィルタテーブルの項目に関する情報を表示します。

文法

show network-access mac-filter { *filter-id* }

- *filter-id* — MAC アドレスフィルタテーブルを表示（範囲：1-64）

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-filter
Filter ID MAC Address MAC Mask
--------- ----------------- -----------------
1 00-00-01-02-03-08 FF-FF-FF-FF-FF-FF
Console#
```

4.9.3 Web 認証

Web 認証は、802.1x やネットワークアクセス認証が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 認証機能は 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] 適切に機能させるために RADIUS 認証をアクティベートし、Web 認証用に適切に構成してください。

[注意] Web 認証はトランクポートに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	P487
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	P487
web-auth session-timeout	セッションタイムアウト時間を設定	GC	P488
web-auth system-auth-control	Web 認証をグローバルで有効	GC	P488
web-auth	Web 認証をインタフェースで有効	IC	P489
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	P489
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	P490
show web-auth	グローバル Web 認証パラメータを表示	PE	P490
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	P491
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	P492

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値に戻します。**

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

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)#
```

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：**1-52）

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
Failed to reauth .
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* **ーユニット番号** "1"
    - *port* **ーポート番号（範囲：**1-52）
- *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

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#show web-auth

Global Web-Auth Parameters

  System Auth Control      : Disabled
  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：**1-52）

初期設定

なし

コマンドモード

Privileged Exec

例

```
Web Auth Status      : Disabled

Host Summary

IP address      Web-Auth-State Remaining-Session-Time
--------------- -------------- ----------------------
1.1.1.1         Authenticated   295
1.1.1.2         Authenticated   111
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#
```

4.9.4 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	P494
ip dhcp snooping vlan	DHCP スヌーピングを指定の VLAN で有効化	GC	P496
ip dhcp snooping trust	指定したインタフェースを trusted ポートに設定	IC	P497
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	P498
ip dhcp snooping information option	DHCP Option 82 情報リレーを有効 / 無効化	GC	P499
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	P500
ip dhcp snooping database flash	全ての動的学習スヌーピングエントリをフラッシュメモリに書き込み	GC	P500
clear ip dhcp snooping database flash	動的に学習されている全てのスヌーピングエントリをフラッシュメモリから削除	PE	P501
show ip dhcp snooping	DHCP スヌーピング設定を表示	PE	P501
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	P501

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（P496）
ip dhcp snooping trust（P497）

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* **ー設定を行う** 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 （P494）
ip dhcp snooping trust （P497）

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（P494）
ip dhcp snooping vlan（P496）

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（P494）

ip dhcp snooping vlan（P496）

ip dhcp snooping trust（P497）

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 **機能を有効にしてください。**

例

```
Console(config)#ip dhcp snooping information option
Console(config)#
```

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 ー 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 ー DHCP クライアント情報を残します。
- replace ー 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)#
```

ip dhcp snooping database flash

全ての動的学習スヌーピングエントリをフラッシュメモリから削除します。

コマンドモード

Privileged Exec

例

```
Console#ip dhcp snooping database flash
Console#
```

clear ip dhcp snooping database flash

全ての動的学習スヌーピングエントリをフラッシュメモリに書き込みます。

コマンドモード

Privileged Exec

例

```
Console#clear ip dhcp snooping database flash
Console#
```

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 is configured on the following VLANs:
1
Verify Source Mac-Address: enable
Interface        Trusted
----------      ----------
Eth 1/1           No
Eth 1/2           No
Eth 1/3           No
Eth 1/4           No
Eth 1/5           Yes
.
.
.
```

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#
```

4.9.5 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	P503
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	P505
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	P506
show ip source-guard binding	IP Source Guard のバインドテーブルを表示します。	PE	P505

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静的アドレスは、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（P506）
ip dhcp snooping（P494）
ip dhcp snooping vlan（P496）

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** 1-52）

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 00-11-22-33-44-55-66 vlan 1
192.168.0.99 interface ethernet 1/5
Console(config-if)#
```

関連するコマンド

ip source-guard（P503）
ip dhcp snooping（P494）
ip dhcp snooping vlan（P496）

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 }

- dhcp-snooping― DHCP **スヌーピングコマンド**（P493）**で設定された動的エントリを表示**
- static ― ip source-guard binding **コマンド**（P505）**で設定された静的エントリを表示（）**

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#
```

4.9.6 ARP インスペクション

ARP インスペクションは、Address Resolution packet（ARP）プロトコルのための、MAC アドレスバインディングの妥当性の検査を行うセキュリティ機能です。

この機能によりある種の man-in-the-middle 攻撃等からネットワークを保護できます。

この機能は、ローカル ARP キャッシュがアップデートされるか、またはパケットが適切な目的地に転送される前に全ての ARP リクエストを途中で捕らえ、これらのパケットのそれぞれを照合することによって達成されます。無効な ARP パケットは破棄されます。

ARP インスペクションは、信頼できるデータベース（DHCP スヌーピングバインディングデータベース）に保存された、正当な IP-to-MAC アドレスバインディングに基づいて、ARP パケットの正当性を決定します。このデータベースは機能がスイッチと VLAN で有効になっている時に、DHCP スヌーピングによって構築されます。
また、ARP インスペクションは、ユーザで設定された ARP アクセスコントロールリスト（ACL）に対して、ARP パケットの妥当性を確認することも可能です。

コマンド	機能	モード	ページ
ip arp inspection	ARP インスペクションをグローバルで有効化	GC	P508
ip arp inspection vlan	指定した VLAN または範囲で ARP インスペクションを有効化	GC	P509
ip arp inspection filter	1 つまたは 1 つ以上の VLAN へ適用する ARP ACL を指定	GC	P510
ip arp inspection validate	ARP パケットアドレスコンポーネントの追加妥当性検査を指定	GC	P511
ip arp inspection log-buffer logs	ログメッセージに保存されるエントリの最大数およびこれらのメッセージが送信されるレイトを設定	GC	P512
ip arp inspection trust	ポートを "trust" に設定し、ARP インスペクションから免除	IC	P513
ip arp inspection limit	ポートで受信される ARP パケットのレートリミットを設定	IC	P514
show ip arp inspection configuration	ARP インスペクションのグローバル設定を表示	PE	P515
show ip arp inspection interface	ポートの trust ステータスとインスペクションレートリミットを表示	PE	P515
show ip arp inspection vlan	ARP インスペクションステータス、ARP ACL 名および ACL 妥当性検査終了後に DHCP スヌーピングデータベースが使用されているかを含む、VLAN 設定を表示	PE	P516
show ip arp inspection log	関連付けられる VLAN、ポート、アドレスコンポーネントを含む、ログに保存されているエントリの情報を表示	PE	P516
show ip arp inspection statistics	処理された ARP パケット数に関する統計、または破棄された様々な理由の表示	PE	P517

ip arp inspection

ARP インスペクションを、スイッチでグローバルに有効にします。"no" を前に置くことでこの機能を無効にします。

文法

ip arp inspection

no ip arp inspection

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

- このコマンドを利用しグローバルで ARP インスペクションを有効にすると、"ip arp inspection vlan" コマンドで有効にされた VLAN でのみアクティブになります。（P509 を参照）
- ARP インスペクションがグローバルで有効であり、選択した VLAN でも有効である場合、こららの VLAN の全ての ARP リクエスト / リプライパケットは CPU へリダイレクトされ、スイッチングは ARP インスペクションエンジンによって処理されます。
- ARP インスペクションがグローバルで無効の際、ARP インスペクションが有効である物も含めて、全ての VLAN で非アクティブになります。
- ARP インスペクションが無効の際、全ての ARP リクエストとリプライパケットは ARP インスペクションエンジンを回避し、スイッチング方法はその他全てのパケットと同等になります。
- ARP インスペクションをグローバルで無効にすることと、その後に再度有効にすることは、VLAN の ARP インスペクション設定に影響を与えません。
- ARP インスペクションがグローバルで無効の際、それぞれの VLAN で、ARP インスペクションの設定は依然可能です。これらの設定変更は ARP インスペクションが再度グローバルで有効になった時のみアクティブになります。

例

```
Console(config)#ip arp inspection
Console(config)#
```

ip arp inspection vlan

指定した VLAN で ARP インスペクションを有効にします。"no" を前に置くことでこの機能を無効にします。

文法

ip arp inspection vlan *vlan-id*

no ip arp inspection vlan < *vlan-id* | *vlan-range* >

- *vlan-id* — VLAN ID. (Range: 1-4094)
- *vlan-range* — ハイフンを使用し VLAN の連続する範囲を指定、またはカンマでそれぞれのエントリを区切り、VLAN のランダムグループを指定

初期設定

全ての VLAN で無効

コマンドモード

Global Configuration

コマンド解説

- ARP インスペクションがグローバルで有効であり、選択した VLAN でも有効である場合、これらの VLAN の全ての ARP リクエスト / リプライパケットは CPU へリダイレクトされ、スイッチングは ARP インスペクションエンジンによって処理されます。
- ARP インスペクションがグローバルで無効の際、それは ARP インスペクションが有効である物も含めて、全ての VLAN で非アクティブになります。
- ARP インスペクションが無効の際、全ての ARP リクエストとリプライパケットは ARP インスペクションエンジンを回避し、スイッチング方法はその他全てのパケットと同等になります。
- ARP インスペクションをグローバルで無効にすることと、その後に再度有効にすることは、VLAN の ARP インスペクション設定に影響を与えません。
- ARP インスペクションがグローバルで無効の際、それぞれの VLAN で、ARP インスペクションの設定は依然可能です。これらの設定変更は ARP インスペクションが再度グローバルで有効になった時のみアクティブになります。

例

```
Console(config)#ip arp inspection vlan 10,20
Console(config)#
```

ip arp inspection filter

ARP ACL を VLAN に適用します。"no" を前に置くことで ACL バインディングを削除します。

文法

ip arp inspection filter *arp-acl-name* vlan < *vlan-id* | *vlan-range* > { static }

no ip arp inspection filter *arp-acl-name* vlan *vlan-id*

- *arp-acl-name* — ACL 名 (最大 16 文字)
- *vlan-id* — VLAN ID (範囲：1-4094)
- *vlan-range* — ハイフンを使用し VLAN の連続する範囲を指定、またはカンマでそれぞれのエントリを区切り、VLAN のランダムグループを指定
- static — ARP パケットは指定された ACL のみにたいして妥当性検査を実行し、DHCP スヌーピングデータベースのアドレスバインディングはチェックされません。

初期設定

ARP ACL は VLAN にバウンドされていません。

Static mode：無効

コマンドモード

Global Configuration

コマンド解説

- ARP ACL は "P527 「ARP ACL」" で設定をおこないます。
- Static モードが有効の場合、スイッチは ARP パケットと指定された ARP ACL を比較します。許可 / 拒否ルールで IP-to-MAC address へのバインディングと一致しているパケットがそれに応じて処理されます。ACL ルールのいずれとも一致しないパケットは破棄されます。DHCP スヌーピングのアドレスバインディングはチェックされません。
- Static モードが無効の場合、パケットは最初に指定した ARP ACL パケットにたいして妥当性検査を行われます。拒否ルールに一致したパケットは破棄されます。
  全ての残ったパケットは DHCP スヌーピングデータベースのアドレスバインディングにたいして妥当性検査が行われます。

例

```
Console(config)#ip arp inspection filter sales vlan 1
Console(config)#
```

ip arp inspection validate

ARP パケットのアドレスコンポーネントに対し、追加検証を指定します。"no" を前に置くことで ACL バインディングを初期状態に戻します。

文法

ip arp inspection validate < dst-mac { ip } {src-mac } | ip { src-mac } | src-mac >

no ip arp inspection validate

- dst-mac ― ARP ボディ内のターゲット MAC アドレスに対し、イーサネットヘッダのディスティネーション MAC アドレスの妥当性検査をおこないます。この検査は ARP レスポンスにたいして実行されます。有効時、異なる MAC アドレスのパケットは無効なパケットとして分類、破棄されます。
- ip ― 不正および予期せぬ IP アドレスの ARP ボディをチェックします。アドレスは 0.0.0.0, 255.255.255.255 と、全ての IP マルチキャストアドレスを含みます。センダー IP アドレスは全ての ARP リクエストとレスポンスをチェックされます。ターゲット IP アドレスは ARP レスポンスのみチェックされます。
- src-mac ― ハイフンを使用し VLAN の連続する範囲を指定、またはカンマでそれぞれのエントリを区切り、VLAN のランダムグループを指定

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- 初期設定では、ARP インスペクションは ARP ACL または DHCP スヌーピングデータベースで指定された IP-to-MAC アドレスバインディングのみチェックを行います。

例

```
Console(config)#ip arp inspection validate dst-mac
Console(config)#
```

ip arp inspection log-buffer logs

ログメッセージに保存されるエントリの最大数および、それらメッセージ送信のレートを設定します。"no" を前に置くことで設定を初期状態に戻します。

文法

ip arp inspection log-buffer logs *message-number* interval *seconds*

no ip arp inspection log-buffer logs

- *message-number* — ログメッセージに保存されるエントリの最大数 (範囲：0-256、0 はセーブ無効)
- *seconds* — ログメッセージが送信される間隔（範囲：0-86400）

初期設定

メッセージ数：5

間隔：1 秒

コマンドモード

Global Configuration

コマンド解説

- このコマンドをスイッチに適用する前に、ARP インスペクションを " ip arp inspection" で有効にしてください。（P508 参照）
- 初期設定ではロギングは ARP インスペクションで有効であり、無効には出来ません。
- スイッチはパケットをドロップした際、エントリをログバッファに起きます。それぞれのエントリは、受信した VLAN、ポート番号、ソースおよびディスティネーション IP アドレス、ソースおよびディスティネーション MAC アドレスの情報を含みます。
- もし複数の同一な無効 ARP パケットが同じ VLAN で連続して受信される場合、ロギングファシリティはバグバッファに 1 つのエントリと、対応する 1 つのシステムメッセージのみ生成します。
- ログバッファに保存可能なエントリの最大数はメッセージ番号パラメータで決定されます。もしログバッファがメッセージ送信前に一杯になった場合、一番古いエントリは最新のものに置き換えられます。
- スイッチは "seconds" 値によって決定されるレートコントロールを基にシステムメッセージを生成します。システムメッセージが生成された後、全てのエントリはログバッファからクリアされます。

例

```
Console(config)#ip arp inspection log-buffer logs 1 interval 10
Console(config)#
```

ip arp inspection trust

ポートを "trusted" **として設定し、**ARP **インスペクションから免除します。**"no" **を前に置くことで** ACL **バインディングを初期状態に戻します。**

文法

ip arp inspection trust

no ip arp inspection trust

初期設定

Untrusted

コマンドモード

Interface Configuration （Port）

コマンド解説

- Untrusted **ポートに到着したパケットは設定された** ARP **インスペクションと追加妥当性検査を受けます。**trusted **ポートに到着したパケットはそれら全てのテストを免除され、通常のスイッチルールに従って転送されます。**

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip arp inspection trust
Console(config-if)#
```

ip arp inspection limit

ポートを "trusted" **として設定し、**ARP **インスペクションから免除します。**"no" **を前に置くことで** ACL **バインディングを初期状態に戻します。**

文法

ip arp inspection limit < rate *pps* | none >

no ip arp inspection limit

- *pps* — CPU **で** 1 **秒ごとに処理可能な** ARP **パケットの最大数** (**範囲：**0-2048, 0 **は** ARP **パケット転送無効**)
- none — CPU **で処理可能な** ARP **パケット数に制限は無し**

初期設定

15

コマンドモード

Interface Configuration（Port）

コマンド解説

- **このコマンドは** Untrusted **ポートにのみ適用されます。**
- **入力** ARP **パケットのレートが設定した制限を越えた場合、スイッチは、制限を超えた全てのパケットを破棄します。**

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip arp inspection limit rate 150
Console(config-if)#
```

show ip arp inspection configuration

ARP インスペクションのグローバル設定を表示します。

コマンドモード

Privileged Exec

コマンド解説

- このコマンドは Untrusted ポートにのみ適用されます。
- 入力 ARP パケットのレートが設定した制限を越えた場合、スイッチは、制限を超えた全てのパケットを破棄します。

例

```
Console#show ip arp inspection configuration

ARP inspection global information:

Global IP ARP Inspection status : disabled
Log Message Interval            : 1 s
Log Message Number              : 5
Need Additional Validation(s)   : No
Additional Validation Type      :
Console#
```

show ip arp inspection interface

ポートの trust ステータスおよび ARP インスペクションレートリミットを表示します。

文法

show ip arp inspection interface { *interface* }

- *Interface*
  - **ethernet** *unit/port*
    - *unit* — ユニット番号 ”1”
    - *port* — ポート番号（範囲：1-52）

コマンドモード

Privileged Exec

例

```
Console#show ip arp inspection interface ethernet 1/5

Port Number        Trust Status             Limit Rate (pps)
-------------   --------------------    -------------------------
-----
Eth 1/5            trusted                  150
Console#
```

show ip arp inspection vlan

ARP インスペクションステータス、ARP ACL 名および ACL 妥当性検査終了後に DHCP スヌーピングデータベースが使用されているかを含む、VLAN 設定を表示します。

文法

show ip arp inspection vlan { *vlan-id* | *vlan-range* }

- *vlan-id* ー VLAN ID. (**範囲：**1-4094)
- *vlan-range* ーハイフンを使用し VLAN の連続する範囲を指定、またはカンマでそれぞれのエントリを区切り、VLAN のランダムグループを指定

コマンドモード

Privileged Exec

例

```
Console#show ip arp inspection vlan 1

VLAN ID     DAI Status              ACL Name             ACL Status
--------   ---------------    -------------------    --------------------
1           disable                 sales                 static
Console#
```

show ip arp inspection log

関連付けられた VLAN、ポート、アドレスコンポーネントを含む、ログに保存されているエントリの情報を表示します。

コマンドモード

Privileged Exec

例

```
Console#show ip arp inspection log
Total log entries number is 1

Num VLAN Port Src IP Address Dst IP Address Src MAC Address Dst MAC Address
--- ---- ---- -------------- -------------- --------------- ---------------
1    1   11  192.168.2.2   192.168.2.1 00-04-E2-A0-E2-7C FF-FF-FF-FF-FF-FF
Console#
```

show ip arp inspection statistics

処理された ARP パケット数に関する統計、または破棄された様々な理由の表示します。

コマンドモード

Privileged Exec

例

```
Console#show ip arp inspection statistics

ARP packets received before rate limit                                  : 0
ARP packets dropped due to rate limt                                    : 0
Total ARP packets processed by ARP Inspection                           : 0
ARP packets dropped by additional validation (source MAC address)       : 0
ARP packets dropped by additional validation (destination MAC address): 0
ARP packets dropped by additional validation (IP address)               : 0
ARP packets dropped by ARP ACLs                                         : 0
ARP packets dropped by DHCP snooping                                    : 0

Console#
```

4.10 ACL（Access Control Lists）

Access Control Lists (ACL) は IPv4 フレーム（アドレス、プロトコル、レイヤ 4 プロトコルポート番号または TCP コントロールコード）またはその他のフレーム（MAC アドレス、イーサネットタイプ）による 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。

コマンド	機能	ページ
IPv4 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	P518
ARP ACLs	ARP メッセージアドレスに基づく ACL の設定	P527
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	P530
ACL Information	ACL 及び関連するルールの表示。各ポートの ACL の表示	P535

4.10.1 IPv4 ACL

IP アドレス、TCP/UDP ポート番号、プロトコルタイプ、TCP コントロールコードに基づく ACL の設定をおこないます。

IP ACL の設定を行うには、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。

コマンド	機能	モード	ページ
access-list rule-mode	拡張ルールのみか、または標準、拡張ルールの両方を許可		P519
access-list IP	IPv4 ACL の作成と configuration mode への移行	GC	P520
permit,deny	ソース IPv4 アドレスが一致するパケットのフィルタリング	STD-ACL	P521
permit,deny	ソース又はディスティネーション IPv4 アドレス、TCP/UDP ポート番号、プロトコルタイプ、TCP コントロールコードに基づくフィルタリング	EXT-ACL	P522
show ip access-list	設定済み IPv4 ACL のルールの表示	PE	P524
ip access-group	IPv4 ACL へのポートの追加	IC	P525
show ip access-group	IPv4 ACL にアサインされたポートの表示	PE	P526

access-list rule-mode

アクセスリストを拡張ルールのみに制限、または標準・拡張ルールの両方をサポートします。"no" **を前に置くことで設定を初期状態に戻します。**

文法

access-list rule-mode [extended | mixed]

no access-list rule-mode

- extended ― **拡張ルールのみ許可**
- mixed ― **拡張・標準、両方のルールを許可**

初期設定

拡張モード（Extended mode）

コマンドモード

Global Configuration

コマンド解説

- **ルールモードが変更された際、変更はスタートアップコンフィグレーションファイルに保存され、スイッチは新しいモードを有効にするため再起動を行います。**
- **拡張ルールモードを使用時、**ACL **のそれぞれのルールは、**2 **つの標準ルールのスペースを占拠します。**
- "mixed" **ルールモードが使用されている時、標準または拡張いずれかのルールを使用することができます。しかしながら同じ** ACL **で使用されているルールは全て標準または全て拡張のいずれかにならなくてはなりません。**
- "mixed" **ルールモードが使用されている時、以下の機能はサポートされません。**DHCP **スヌーピング、**IP **ソースガード、**Web **認証、スイッチクラスタ、**PnP**m、**MAC **ベース** VLANs**、**MVR**。**
- **ルールモードが初期設定から変更された場合、現在のステータスは** "show running-config"（P317）**または** " show startup-config"（P315）**コマンドで表示することができます。**

例

```
Console(config)#access-list rule-mode extended
Warning: This will take effect only after rebooting the switch.
Console(config)#
```

access-list ip

IP ACL を追加し、スタンダード又は拡張 IPv4 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 ーソース IP アドレスに基づくフィルタリングを行う ACL
- extended ー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* ー ACL 名（最大 16 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（P521）
ip access-group（P525）
show ip access-list（P524）

permit,deny（Standard ACL）

スタンダード IPv4 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（P520）

permit,deny（Extended IPv4 ACL）

拡張 IPv4 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}
[precedence *precedence*] [tos *tos*] [dscp *dscp*]
[source-port sport [*bitmask*]] [destination-port *dport* [port-*bitmask*]]
[**no**] {**permit** | **deny**} tcp
{ any | *source address-bitmask* | host *source*}
{ any | *destination address-bitmask* | host *destination*}
[precedence *precedence*] [tos *tos*] [dscp *dscp*]
[source-port sport [*bitmask*]] [destination-port *dport* [*port-bitmask*]]
[control-flag *control-flags flag-bitmask*]

- *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**
- *precedence* ― IP precedence **レベル** (**範囲：**0-7)
- *tos* ― ToS **レベル** (**範囲：**0-15)
- *dscp* ― DSCP **プライオリティレベル** (**範囲：**0-63)
- *sport* ― **プロトコル** * **ソースポート番号（範囲：**0-65535**）**
- *dport* ― **プロトコル** * **ディスティネーションポート番号（範囲：**0-65535**）**
- *port-bitmask* ― **マッチするポートビットを表す** 10 **進数** (**範囲：**0-65535)
- *control-flags* ― TCP **ヘッダのバイト** 14 **でフラッグビットを指定する** 10 **進数（ビットストリングを表す）**(**範囲：**0-63)
- *flag-bitmask* ― **マッチするコードビットを表す** 10 **進数**

*TCP、UDP、**その他のプロトコルタイプを含む**

初期設定

なし

コマンドモード

Extended IPv4 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、無視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。
- 同じルール内で Precedence 及び ToS の両方を指定することができます。しかし、DSCP を使用した場合、Precedence 及び ToS は指定することができません。
- コントロールビットマスクは、コントロールコードに使用される 10 進数の値です。10 進数の値を入力し、等価な 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、無視するビットとなります。以下のビットが指定されます。
  - 1 (fin) — Finish
  - 2 (syn) — Synchronize
  - 4 (rst) — Reset
  - 8 (psh) — Push
  - 16 (ack) — Acknowledgement
  - 32 (urg) — Urgent pointer

  例えば、コード値及びコードマスクを利用し、パケットをつかむには以下のフラグをセットします。

  - 有効な SYN flag — "control-code 2 2"
  - 有効な SYN 及び ACK — "control-code 18 18"
  - 有効な SYN 及び無効な ACK — "control-code 2 18"

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（P520）

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 **ースタンダード** IP ACL
- extended **ー拡張** IP ACL
- *acl_name* ー 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#
```

関連するコマンド

permit, deny（P521）
ip access-group（P525）

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

no ip access-group *acl_name* in

- *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

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（P524）

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（P525）

4.10.2 ARP ACL

ARP リクエスト・リプライメッセージを含む、IP または MAC アドレスに基づく ACL の設定を行います。ARP ACL の設定を行うには、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、" ip arp inspection vlan" コマンド（P509）を使用し、アクセスリストを 1 つまたは 1 つ以上の VLAN へバインドします。

コマンド	機能	モード	ページ
access-list larp	ARP ACL を作成し、設定モードへ移行します	GC	P527
permit,deny	ARP メッセージのソースまたはディスティネーションアドレスが一致するパケットのフィルタリング	ARP-ACL	P528
show arp access-list	ARP ACL に設定されたルールを表示	PE	P529

access-list arp

ARP アクセスリストを追加し、ARP 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 arp *acl-name*

no access-list arp *acl-name*

- *acl-name* — ACL 名（最大 16 文字、スペースは不可）

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 を作成や、既存の ACL の設定モードに移行した時、"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 64 個のルールが設定可能です。

例

```
Console(config)#access-list arp factory
Console(config-arp-acl)#
```

関連するコマンド

permit, deny（P528）
show arp access-list（P529）

permit,deny（ARP ACL）

ARP ACL へルールを追加します。このルールは、ARP メッセージで指定されたソースまたはディスティネーションアドレスと一致しているパケットをフィルタします。"no" を前に置くことでルールを削除します。

文法

[no] { permit | deny }

ip { any | host *source-ip* | *source-ip ip-address-bitmask* }

mac { any | host *source-ip* | *source-ip ip-address-bitmask* } [log]

注意：この形式はリクエストまたはレスポンスパケットを示します。

[no] { permit | deny } request

ip { any | host *source-ip* | *source-ip ip-address-bitmask* }

mac {any | host *source-mac* | *source-mac mac-address-bitmask* } [log]

[no] { permit | deny } response

ip { any | host *source-ip* | *source-ip ip-address-bitmask* }

{ any | host *destination-ip* | *destination-ip ip-address-bitmask* }

mac { any | host *source-mac* | *source-mac mac-address-bitmask* }

[any | host *destination-mac* | *destination-mac mac-address-bitmask*] [log]

- *source-ip* — **ソース** IP **アドレス**
- *destination-ip* — **ディスティネーション** IP **アドレス**
- *ip-address-bitmask* — **マッチするアドレスビットを示す** IPv4 **番号**
- *source-mac* — **ソース** MAC **アドレス**
- *destination-mac* — **ディスティネーション** MAC **アドレス範囲**
- *mac-address-bitmask* — MAC **アドレスビットマスク**
- log — **アクセスコントロール縁撮るにマッチしたパケットのログ**

初期設定

なし

コマンドモード

ARP 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。**

例

```
Console(config-arp-acl)#$permit response ip any 192.168.0.0 255.255.0.0
mac any any
Console(config-mac-acl)#
```

関連するコマンド

access-list arp（P527）

show arp access-list

設定済みの ARP ACL **のルールを表示します。**

文法

show arp 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 arp access-list
ARP access-list factory:
  permit response ip any 192.168.0.0 255.255.0.0 mac any any
Console#
```

関連するコマンド

permit, deny（P528）

4.10.3 MAC ACL

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	P530
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	P531
show mac access-list	設定済み MAC ACL のルールの表示	PE	P533
mac access-group	MAC ACL へのポートの追加	IC	P533
show mac access-group	MAC ACL に指定したポートの表示	PE	P534

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* ー ACL 名（最大 16 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)（P521）
mac access-group（P525）
show mac access-list（P524）

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：1-4094）

- *vid bitmask* ― VLAN **ビットマスク（範囲：**1-4095**）**
- *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 (P530)

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（P531）
mac access-group（P533）

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 16 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（P533）

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 (P533)

4.10.4 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	P535
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	P535

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#
```

4.11 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	P537
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	P538
speed-duplex	インタフェースの解説	IC	P539
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	P540
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	P541
flowcontrol	インタフェースへのフローコントロール設定	IC	P542
media-type	コンボポートの固定ポートタイプを選択	IC	P543
giga-phy-mode	1000BASE-T Full duplex を有効にする為のマスタ / スレイブ設定	IC	P544
shutdown	インタフェースの無効	IC	P545
switchport packet-rate*	ストームコントロールの閾値を設定	IC	P546
clear counters	インタフェースの統計情報のクリア	PE	P547
show interfaces brief	操作上のステータス、VLAN ID、デフォルトプライオリティ、speed/duplex、ポートタイプを含む、キー情報のサマリを表示	PE	P548
show interfaces status	インタフェースの設定状況を表示	NE,PE	P549
show interfaces counters	インタフェースの統計情報の表示	NE,PE	P550
show interfaces switchport	インタフェースの管理、運用状況の表示	NE,PE	P551

* このコマンドでポートのハードウェアレベルストームコントロールを有効にした時、同じポートで "auto-traffic-control" コマンド（P558）によりソフトウェアレベル自動ストームコントロールが設定されている場合は無効になります。

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：**1-52）
  - port-channel *channel-id* — Channel ID (1-8)
  - 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：**1-64 **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。**
- **オートネゴシエーションが無効時、初期設定値は** 100BASE-TX**、ギガビットイーサネット共に** 100full **です。**

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（P540）

capabilities（P541）

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。
- オートネゴシエーションが無効の場合には RJ-45 ポートの MDI-MDI-X 自動認識機能も無効となります。

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（P541）

speed-duplex（P539）

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 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 ― flow 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)#
```

関連するコマンド

speed-duplex（P539）
negotiation（P540）
flow control（P542）

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（P540）
capabilities（flowcontrol, symmetric）（P541）

media-type

コンビネーションポート 49-52 **に、選択されたポートタイプを固定設定します。**
"no" **を前に置くことで設定を初期値に戻します。**

文法

media-type *mode*

no media-type

- *mode* — **モードを選択**
  - copper-forced —**常に組み込まれた** RJ-45 **ポートを使用**
  - sfp-forced —**常に** SFP **ポート** (**モジュールが未装着でも**) **を使用**
  - sfp-preferred-auto —**両方のコンビネーションタイプが作用し、**SFP **ポートが有効なリンクを保持している時、**SFP **ポートを使用**

初期設定

sfp-preferred-auto

コマンドモード

Interface Configuration (Ethernet- **ポート** 49-52)

例

```
Console(config)#interface ethernet 1/49
Console(config-if)#media-type copper-forced
Console(config-if)#
```

giga-phy-mode

２つの接続されたポートをギガビットポート 49-52 **で** 1000BASE-T Full **デュプレックス有効にする為に、マスタ / スレーブへ固定設定します。**
"no" **を前に置くことで設定を初期値に戻します。**

文法

giga-phy-mode *mode*

no giga-phy-mode

- *mode* ― **モードを選択**
  - master ―**選択したポートをマスタに設定**
  - slave ―**選択したポートをスレーブに設定**
  - auto-prefer-master ―**リンクの一方の終端に設定されたモードにかかわらず、イニシャル設定としてマスタモードを使用**
  - auto-prefer-slave ―**リンクの一方の終端に設定されたモードにかかわらず、イニシャル設定としてスレーブモードを使用**

初期設定

master

コマンドモード

Interface Configuration (Ethernet- **ポート** 49-52)

コマンド解説

- 1000BASE-T **標準はフォースモードをサポートしていません。全ての** 1000BASE-T **ポートまたはトランク接続では、常に接続確立の為に** Auto-negotiation **が使用されます。使用しない場合、他のタイプのスイッチとの接続時リンクプロセスの成功は保証されません。しかしながら、本機は** giga-phy-mode **コマンドを使用し、リンクを** 1000 Mbps Full Duplex **で稼動することを固定する手段を提供します。**

- 1000full **オペレーション固定はリンクの両端ポートが接続プロセスにおける、マスタまたはスレーブとしての役割が確立していることを要求します。**
  機能を使用する前に、最初に Auto-negotiation **を無効にしてから** Speed/Duplex **を** 1000Full **に設定します。その後、リンクの両端のモードで** compatible Giga PHY **モードを選択します。**

例

```
Console(config)#interface ethernet 1/49
Console(config-if)#no negotiation
Console(config-if)#speed-duplex 1000full
Console(config-if)#giga-phy-mode master
Console(config-if)#
```

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)#
```

switchport packet-rate

ブロードキャスト、マルチキャスト、未知のユニキャストストームコントロールの設定をします。"no" **を前に置くことでブロードキャストストームコントロールを無効にします。**

文法

switchport [broadcast octet-rate | multicast | unicast] *rate*

no switchport [broadcast octet-rate | multicast | unicast]

- *rate*―**レートの閾値（範囲：**64-100000（100Mbps）64-1000000（1Gbps)）

初期設定

ブロードキャストストームコントロール：有効、パケットレートリキット =64Kbps

マルチキャストストームコントロール：無効

未知のユニキャストストームコントロール：無効

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- **トラフィックが、ブロードキャスト、マルチキャスト、未知のユニキャストトラフィックが指定した閾値を超えた場合、超えたパケットは破棄されます。**
- ASIC **チップリミテーションのため、サポートされるストームコントロールモードは以下です。**
  - **―ブロードキャスト**
  - **―ブロードキャスト＋マルチキャスト**
  - **―ブロードキャスト＋マルチキャスト＋未知のユニキャスト**

  これはマルチキャストストームコントロールが有効である時、ブロードキャストストームコントロールもまた有効になるということを意味します。（マルチキャストストームコントロールコマンドで設定されたしきい値を使用）
  また、未知のユニキャストストームコントロールが有効である時、ブロードキャスト・マルチキャストストームコントロールの両方もまた有効になります。（未知のユニキャストストームコントロールコマンドで設定されたしきい値を使用）
- **トラフィックストームは、このコマンドを使用してハードウェアレベルで行うか、**"auto-traffic-control" **コマンド（**PXX**）を使用してのソフトウェアレベルでも行えます。これらのコントロールタイプのうち** 1 **つのみがはポートに適用できます。**
  ハードウェアレベルストームコントロールを有効にすることで、同じポートの自動ストームコントロールは無効になります。

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#switchport broadcast packet-rate 500
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：**1-52）
  - port-channel channel-id (**範囲：**1-8)

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 brief

オペレーショナルステータス、ネイティヴ VLAN ID、デフォルトプライオリティ、スピード / デュプレックスモード、全てのポートのポートタイプを含む、キー情報のサマリを表示します。

文法

show interfaces status brief

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#show interfaces brief
Interface Name              Status   PVID Pri Speed/Duplex  Type         Trunk
--------- ----------------- -------- ---- --- ------------- ------------ ----
Eth 1/ 1                     Down        1   0 Auto          100TX        None
Eth 1/ 2                     Down        1   0 Auto          100TX        None
Eth 1/ 3                     Down        1   0 Auto          100TX        None
Eth 1/ 4                     Down        1   0 Auto          100TX        None
Eth 1/ 5                     Down        1   0 Auto          100TX        None
Eth 1/ 6                     Down        1   0 Auto          100TX        None
Eth 1/ 7                     Down        1   0 Auto          100TX        None
Eth 1/ 8                     Down        1   0 Auto          100TX        None
Eth 1/ 9                     Down        1   0 Auto          100TX        None
.
.
.
```

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：**1-52**）**
  - port-channel *channel-id*（**範囲：**1-8）
  - vlan *vlan-id* — VLAN ID (1-4094)

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** P149 **「接続状況の表示」を参照して下さい。**

例

```
Console#show interfaces status ethernet 1/5
Information of Eth 1/5
 Basic Information:
  Port Type:              100TX
  Mac Address:            00-17-2E-11-94-25
 Configuration:
  Name:
  Port Admin:             Up
  Speed-duplex:           Auto
  Capabilities:           10half, 10full, 100half, 100full
  Broadcast Storm:        Enabled
  Broadcast Storm Limit:  64 Kbits/second
  Multicast Storm:        Disabled
  Multicast Storm Limit:  64 Kbits/second
  UnknownUnicast Storm:       Disabled
  UnknownUnicast Storm Limit:  64 Kbits/second
  Flow Control:           Disabled
  LACP:                   Disabled
  Port Security:          Disabled
  Max MAC Count:          0
  Port Security Action:   None
  Media Type:             None
  Giga PHY mode: Auto preferred master
 Current Status:
  Link Status:            Down
  Operation Speed-duplex: 10half
  Flow Control Type:      None
```

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：**1-52**）**
  - port-channel *channel-id***（範囲：**1-8**）**

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：**1-52）
  - port-channel *channel-id*（**範囲：**1-8）

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 24 **番ポートの情報を表示しています。**

```
Console#show interfaces switchport ethernet 1/1
Information of Eth 1/1
 Broadcast Threshold:           Enabled, 64 Kbits/second
 Multicast Threshold:           Disabled
 Unknown-unicast Threshold:     Disabled
 LACP Status:                   Disabled
 Ingress Rate Limit:            Disabled, 100000 Kbits per second
 Egress Rate Limit:             Disabled, 100000 Kbits per second
 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 host-association: 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（P546 参照）
Multicast Threshold	まるち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（P546 参照）
Unknown-unicast Threshold	未知の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（P546 参照）
Lacp status	LACP の有効 / 無効（P572 参照）
Ingress rate limit	入力帯域制御の有効 / 無効。現在の設定（P585 参照）
Egress rate limit	出力帯域制御の有効 / 無効。現在の設定（P585 参照）
VLAN membership mode	トランク又は Hybrid のメンバーモードを表示（P632 参照）
Ingress rule	イングレスフィルタの有効 / 無効の表示（P634 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（P633 参照）
Native VLAN	デフォルトポート VLAN ID の表示（P635 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（P699 参照）
Gvrp status	GVRP の有効 / 無効（P624 参照）
Allowed Vlan	参加している VLAN の表示。"(u)" はタグなし、"(t)" はタグ（P636 参照）
Forbidden Vlan	GVRP によって動的に参加できない VLAN の表示（P637 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（P653 参照）
Private VLAN host-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（P656 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（P657 参照）
802.1Q-tunnel Status	このインタフェースで 802.1Q トンネルが有効時に表示（P642 参照）
802.1Q-tunnel Mode	802.1Q トンネルまたは 802.1Q トンネルアップリンクのトンネルモードを表示（P643 参照）
802.1Q-tunnel TPID	学習とパケットのスイッチングに使用される、タグプロトコル識別を表示（P644 参照）

4.12 自動トラフィック制御

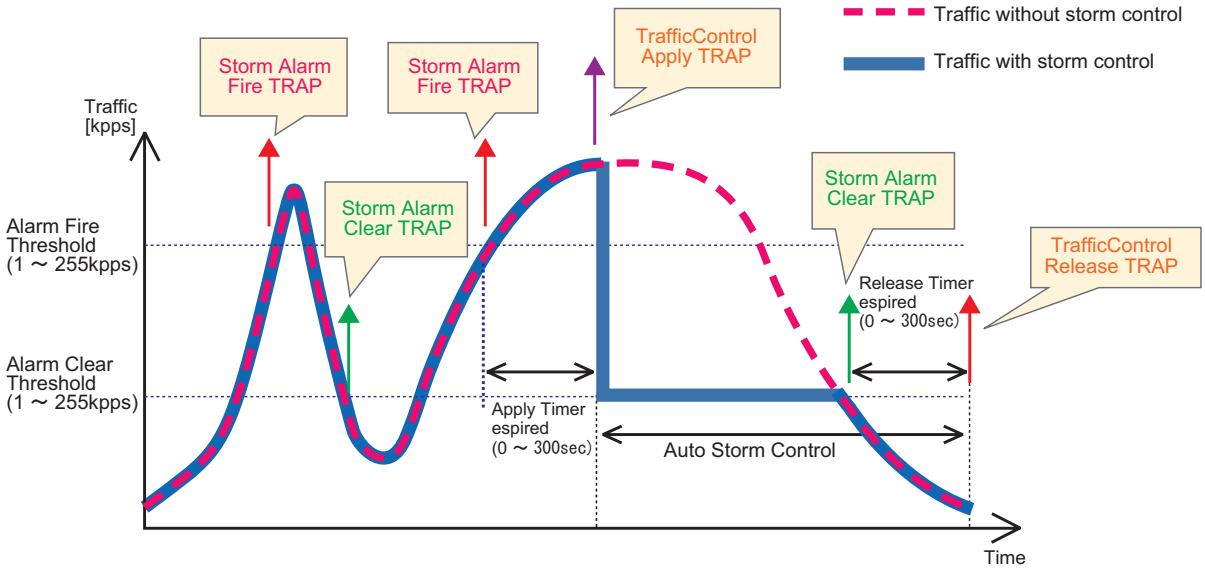
Automatic Traffic Control（ATC）**は、設定されたレートリミットまたはポートのシャットダウンのトリガに使用できる、ブロードキャスト、マルチキャストストームのしきい値の境界を設定します。**

コマンド	機能	モード	ページ
しきい値コマンド			
auto-traffic-control apply-timer	**入力トラフィックが上限値を超えた後、コントロールレスポンスを適用する時間を設定**	GC	P556
auto-traffic-control release-timer	**入力トラフィックが下限値を下まわった後、コントロールレスポンスをリリースする時間を設定**	GC	P557
auto-traffic-control*	**ブロードキャストまたはマルチキャストストームの自動トラフィックコントロールを有効化**	IC (Port)	P558
auto-traffic-control alarm-fire-threshold	**イングレストラフィックの上限値を越えて、ストームコントロールレスポンスがアプライタイマ失効の後に引き起こされる立入りトラフィックに設定**	IC (Port)	P559
auto-traffic-control alarm-clear-threshold	**クリアされたストームコントロールトラップが送られる入力フィルタの下限値を設定**	IC (Port)	P560
auto-traffic-control action	**入力トラフィックのリミットまたは攻撃的ポートのシャットダウンのコントロールアクションを設定**	IC (Port)	P561
auto-traffic-control control-release	**手動でコントロールレスポンスをリリース**	IC (Port)	P562
auto-traffic-control auto-control-release	**自動でコントロールレスポンスをリリース**	PE	P562
*SNMP **トラップコマンド***			
snmp-server enable port-traps atc broadcast-alarm-fire	**ブロードキャストトラフィックが自動ストームコントロールの上限値を超えた時にトラップを送信**	IC (Port)	P563
snmp-server enable port-traps atc multicast-alarm-fire	**マルチキャストトラフィックが自動ストームコントロールの上限値を超えた時にトラップを送信**	IC (Port)	P563
snmp-server enable port-traps atc broadcast-alarm-clear	**ストームコントロールレスポンスが発生した後、ブロードキャストトラフィックが下限値を下回った特にトラップを送信**	IC (Port)	P564
snmp-server enable port-traps atc multicast-alarm-clear	**ストームコントロールレスポンスが発生した後、マルチキャストトラフィックが下限値を下回った特にトラップを送信**	IC (Port)	P565
snmp-server enable port-traps atc broadcast-control-apply	**ブロードキャストトラフィックが自動ストームコントロールの上限値を越え、アプライタイマが失効した時にトラップを送信**	IC (Port)	P566
snmp-server enable port-traps atc multicast-control-apply	**マルチキャストトラフィックが自動ストームコントロールの上限値を越え、アプライタイマが失効した時にトラップを送信**	IC (Port)	P566
snmp-server enable port-traps atc broadcast-control-release	**ブロードキャストトラフィックが自動ストームコントロールの上限値を越え、アプライタイマが失効した時にトラップを送信**	IC (Port)	P567
snmp-server enable port-traps atc multicast-control-release	**マルチキャストトラフィックが自動ストームコントロールの上限値を越え、アプライタイマが失効した時にトラップを送信**	IC (Port)	P568
*ATC **表示コマンド***			
show auto-traffic-control	**自動ストームコントロールのグローバル設定を表示**	PE	P569
show auto-traffic-control interface	**指定したポートの、インタフェース設定およびストームコントロールステータスを表示**	PE	P569

* **ポートでの自動ストーム制御の有効は、もし** "switchport packet-rate" **コマンド（**P546**）で設定されている場合、同じポートのハードウェアレベルストームコントロールを無効にします。**

ユーザガイドライン

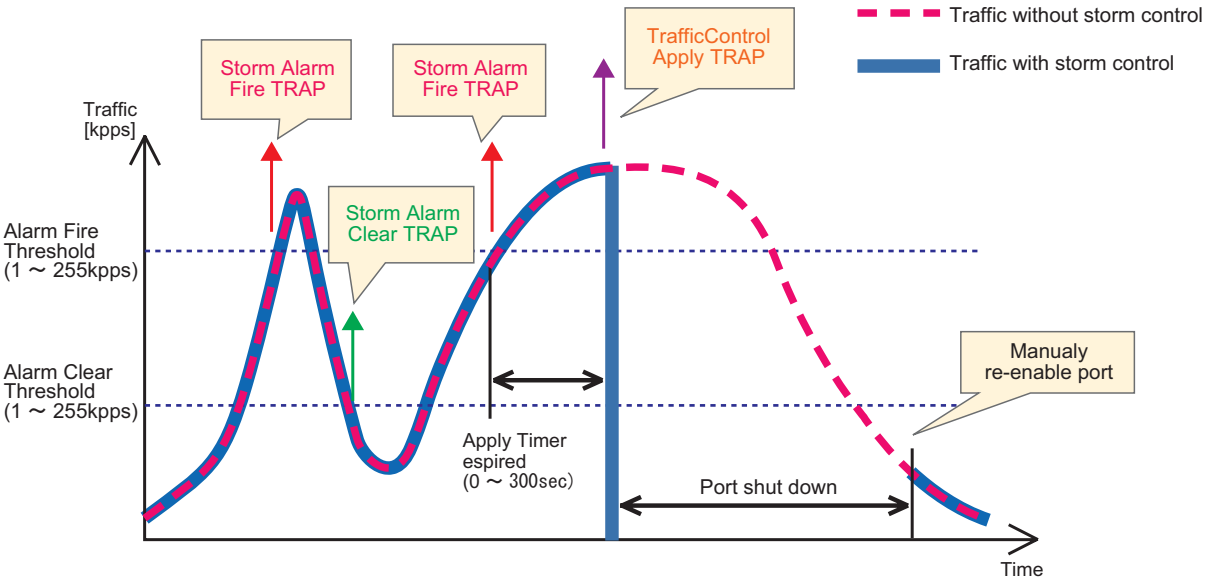
ATC はブロードキャストまたはマルチキャストトラフィックのストームコントロールを含みます。以下の図で示すように、これらトラフィックタイプとコントロールレスポンスは同様です。



この図のキーエレメントは以下です。

- Alarm Fire Threshold －受容可能な最大トラフィックレート。入力トラフィックがしきい値を越えた時、ATC は " Storm Alarm Fire Trap" の送信とログを行います。
- トラフィックが "alarm fire threshold" を越え、アプライタイマが失効した時、トラフィックコントロールレスポンスが適用され、"Traffic Control Apply" トラップ送信とログを行います。
- Alarm Clear Threshold －リリースタイマ期限が切れた後、下限値を下回るコントロールレスポンスは自動的に終了させられることができます。
  入力トラフィックがしきい値以下に下がる時、ATC は "Storm Alarm Clear Trap" トラップの送信とログを行います。
- リリースタイマ失効後、トラフィックがアラームクリアしきい値を下まわる時、トラフィックコントロールは停止し、"Traffic Control Release Trap" の送信とログをおこないます。
- レートリミットのトラフィックコントロールレスポンスは自動または手動でリリースが可能です。ポートのシャットダウンのコントロールレスポンスは手動でのみリリースが可能です。

ポートシャットダウンによるストームコントロール



この図のキーエレメントは、コントロールレスポンスの自動リリースが提供されないこと以外は、前の図で説明したのと同様です。
トラフィックコントロールが適用される時、ポートの再有効化は使用で行わなければなりません。

機能の制限

自動ストームコントロールはソフトウェアレベルコントロール機能です。

トラフィックストームは "switchport packet-rate" コマンド（P546）を使用して、ハードウェアレベルでもコントロールが可能です。これらのコントロールタイプの内 1 つだけがポートへ適用可能です。ポートで自動ストームコントロールが有効にされると、ハードウェアレベルストームコントロールは無効になります。

auto-traffic-control apply-timer

入力トラフィックが上限値を越えた後、コントロールレスポンスを適用する時間を設定します。"no" **を前に置くことで設定を初期状態に戻します。**

文法

auto-traffic-control [broadcast | multicast] apply-timer *seconds*

no auto-traffic-control [broadcast | multicast] apply-timer

- broadcast ― **ブロードキャストトラフィックの自動ストームコントロールを指定**
- multicast ― **マルチキャストトラフィックの自動ストームコントロールを指定**
- *seconds* ― **コントロールレスポンスを適用する上限値を超えた後のインターバル** (**範囲：**1-300 **秒**)

初期設定

300 **秒**

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- **アプライタイマが失効した後、**"auto-traffic-control action" **コマンド（**P561**）で指定されたコントロールアクションが発生し、**"snmp-server enable port-traps atc broadcast-control-apply"**（**P566**）または** "snmp-server enable port-traps atc multicast-control-apply" **コマンド（**P566**）で指定されたトラップメッセージが送信されます。**

例

```
Console(config)#auto-traffic-control broadcast apply-timer 200
Console(config)#
```

auto-traffic-control release-timer

入力トラフィックが下限値を下まわった後に、コントロールレスポンスのリリース時間を設定します。"no" **を前に置くことで設定を初期状態に戻します。**

文法

auto-traffic-control [broadcast | multicast] release-timer *seconds*

no auto-traffic-control [broadcast | multicast] release-timer

- broadcast ― **ブロードキャストトラフィックの自動ストームコントロールを指定**
- multicast ― **マルチキャストトラフィックの自動ストームコントロールを指定**
- *seconds* ― **入力トラフィックが下限値を下まわった後に、コントロールレスポンスをリリースする時間 (範囲：**1-900 **秒)**

初期設定

900 **秒**

コマンドモード

Global Configuration

コマンド解説

- **このコマンドは　コントロールレスポンスが終了された後の遅延を設定します。**"auto-traffic-control auto-control-release" **コマンド（**P562**）が自動リリースの有効 / 無効を設定するために使用されます。**

例

```
Console(config)#auto-traffic-control broadcast release-timer 800
Console(config)#
```

auto-traffic-control

ブロードキャストまたはマルチキャストストームの自動トラフィックコントロールを有効にします。"no" **を前に置くことで設定を無効にします。**

文法

auto-traffic-control [broadcast | multicast]

no auto-traffic-control [broadcast | multicast]

- broadcast ― **ブロードキャストトラフィックの自動ストームコントロールを指定**
- multicast ― **マルチキャストトラフィックの自動ストームコントロールを指定**

初期設定

無効

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- **自動ストームコントロールはブロードキャストあるいはマルチキャストトラフィックにたいし有効に出来ます。これら両方のトラフィックにたいし、同時に有効にすることは出来ません。**
- **自動ストームコントロールはソフトウェアレベルコントロール機能です。トラフィックストームは** "switchport packet-rate" **コマンド（**P546**）を使用して、ハードウェアレベルでもコントロールが可能です。これらのコントロールタイプの内** 1 **つだけがポートへ適用可能です。ポートで自動ストームコントロールが有効にされると、ハードウェアレベルストームコントロールは無効になります。**

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#auto-traffic-control broadcast
Console(config-if)#
```

auto-traffic-control alarm-fire-threshold

アプライタイマ失効後、ストームコントロールレスポンスが引き起こされる入力トラフィックの上限値を設定します。"no" **を前に置くことで設定を初期値に戻します。**

文法

auto-traffic-control [broadcast | multicast] **alarm-fire-threshold** *threshold*

no auto-traffic-control [broadcast | multicast] **alarm-fire-threshold**

- broadcast ― **ブロードキャストトラフィックの自動ストームコントロールを指定**
- multicast ― **マルチキャストトラフィックの自動ストームコントロールを指定**
- *threshold* ― **アプライタイマ失効後、ストームコントロールレスポンスが引き起こされる入力トラフィックの上限値（範囲：**1-255Kpacket/ **秒）**

初期設定

128Kpacket/ **秒**

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- " snmp-server enable port-traps atc broadcast-alarm-fire"（P563）**または** " snmp-server enable port-traps atc multicast-alarm-fire"（P563）**コマンドで設定がおこなわれている場合、一度上限値を越えると、トラップメッセージが送信されます。**
  上限値を越えた後、コントロールタイマは、"auto-traffic-control action"（P561）**によって設定される場合、コントロールレスポンスが引き起こされるより前に** "auto-traffic-control apply-timer"（P556）**コマンドの設定に準じ失効します。**

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#auto-traffic-control broadcast alarm-fire-threshold 255
Console(config-if)#
```

auto-traffic-control alarm-clear-threshold

ストームコントロールクリアトラップを送信する、入力トラフィックの下限値を設定します。"no" **を前に置くことで設定を初期値に戻します。**

文法

auto-traffic-control [broadcast | multicast] **alarm-clear-threshold** *threshold*

no auto-traffic-control [broadcast | multicast] **alarm-clear-threshold**

- broadcast — **ブロードキャストトラフィックの自動ストームコントロールを指定**
- multicast — **マルチキャストトラフィックの自動ストームコントロールを指定**
- *threshold* — **アプライタイマ失効後、ストームコントロールレスポンスが引き起こされる入力トラフィックの上限値（範囲：**1-255Kpacket/ **秒）**

初期設定

128Kpacket/ **秒**

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- **一度下限値を下回ると** " snmp-server enable port-traps atc broadcast-alarm-clear" **コマンド（**P564**）または** " snmp-server enable port-traps atc multicast-alarm-clear" **コマンド（**P565**）で設定されたトラップメッセージが送信されます。**

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#auto-traffic-control broadcast alarm-clear-threshold
  155
Console(config-if)#
```

auto-traffic-control action

入力トラフィックの制限または違反のあったポートのシャットダウンを行う為のコントロールアクションを設定します。"no" **を前に置くことで設定を初期値に戻します。**

文法

auto-traffic-control [broadcast | multicast] **action** [rate-control | shutdown]

no auto-traffic-control [broadcast | multicast] **action**

- broadcast — **ブロードキャストトラフィックの自動ストームコントロールを指定**
- multicast — **マルチキャストトラフィックの自動ストームコントロールを指定**
- rate-control — **コントロール反応が引き起こされた際、入力トラフィックのレートは** " auto-traffic-control alarm-clear-threshold" **コマンド（**P560**）で設定されたしきい値に基づいて制限されます。**
- shutdown — **コントロール反応が引き起こされた際、ポートは無効になります。自動トラフィックコントロールによって無効になったポートは手動でのみ再有効化が可能です。**

初期設定

rate-control

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- **上限のしきい値が超えられ、アプライタイマが期限切れになった時、このコマンドを基にコントロール反応が発生します。**
- **コントロール反応が、このコマンドによってレート制限に設定されている際、レートリミットは** " auto-traffic-control alarm-clear-threshold" **コマンド（**P560**）で決定されます。**
- **ポートがコントロール反応によってシャットダウンされた時、自動トラフィックコントロールでは再度有効にすることは出来ません。**" auto-traffic-control control-release" **コマンド（**P562**）により手動でのみ再有効化が可能です。**

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#auto-traffic-control broadcast action shutdown
Console(config-if)#
```

auto-traffic-control control-release

コントロールレスポンスを手動でリリースします。

文法

auto-traffic-control [broadcast | multicast] **control-release**

- broadcast ― **ブロードキャストトラフィックの自動ストームコントロールを指定**
- multicast ― **マルチキャストトラフィックの自動ストームコントロールを指定**

コマンドモード

Privileged Exec

コマンド解説

- **このコマンドは、指定されたアクションが引き起こされた後、コントロールレスポンスを手動で停止するために使用します。**

例

```
Console#auto-traffic-control broadcast control-release interface
  ethernet 1/1
Console#
```

auto-traffic-control auto-control-release

"auto-traffic-control release-timer" **コマンド（**P557**）で指定された期限が切れた後、コントロールレスポンスを自動でリリースします。**

文法

auto-traffic-control [broadcast | multicast] **auto-control-release**

- broadcast ― **ブロードキャストトラフィックの自動ストームコントロールを指定**
- multicast ― **マルチキャストトラフィックの自動ストームコントロールを指定**

コマンドモード

Privileged Exec

コマンド解説

- **このコマンドは、指定されたアクションが引き起こされ、リリースタイマの期限が切れた後に、コントロールレスポンスを自動で停止するために使用します。**

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#auto-traffic-control broadcast auto-control-release
Console(config-if)#
```

snmp-server enable port-traps atc broadcast-alarm-fire

ブロードキャストトラフィックが、自動ストームコントロールのしきい値の上限を超えた時にトラップを送ります。"no" **を前に置くことでトラップを無効にします。**

文法

snmp-server enable port-traps atc broadcast-alarm-fire

no snmp-server enable port-traps atc broadcast-alarm-fire

初期設定

無効

コマンドモード

Interface Configuration (Ethernet)

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc broadcast-alarm-fire
Console(config-if)#
```

関連するコマンド

auto-traffic-control alarm-fire-threshold （P559）

snmp-server enable port-traps atc multicast-alarm-fire

マルチキャストトラフィックが、自動ストームコントロールのしきい値の上限を超えた時にトラップを送ります。"no" **を前に置くことでトラップを無効にします。**

文法

snmp-server enable port-traps atc multicast-alarm-fire

no snmp-server enable port-traps atc multicast-alarm-fire

初期設定

無効

コマンドモード

Interface Configuration (Ethernet)

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc multicast-alarm-fire
Console(config-if)#
```

関連するコマンド

auto-traffic-control alarm-fire-threshold （P559）

snmp-server enable port-traps atc broadcast-alarm-clear

ストームコントロールレスポンスが引き起こされた後、ブロードキャストトラフィックが下限のしきい値を下回った時にトラップを送信します。"no" **を前に置くことでトラップを無効にします。**

文法

snmp-server enable port-traps atc broadcast-alarm-clear

no snmp-server enable port-traps atc broadcast-alarm-clear

初期設定

無効

コマンドモード

Interface Configuration (Ethernet)

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc broadcast-alarm-clear
Console(config-if)##
```

関連するコマンド

auto-traffic-control action（P561）

auto-traffic-control alarm-clear-threshold（P560）

snmp-server enable port-traps atc multicast-alarm-clear

ストームコントロールレスポンスが引き起こされた後、マルチキャストトラフィックが下限のしきい値を下回った時にトラップを送信します。"no" **を前に置くことでトラップを無効にします。**

文法

snmp-server enable port-traps atc multicast-alarm-clear

no snmp-server enable port-traps atc multicast-alarm-clear

初期設定

無効

コマンドモード

Interface Configuration (Ethernet)

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc multicast-alarm-clear
Console(config-if)#
```

関連するコマンド

auto-traffic-control action（P561）

auto-traffic-control alarm-clear-threshold（P560）

snmp-server enable port-traps atc broadcast-control-apply

ブロードキャストトラフィックが自動ストームコントロールの上限のしきい値を超え、アプライタイマが期限切れになった時にトラップを送信します。"no" **を前に置くことでトラップを無効にします。**

文法

snmp-server enable port-traps atc broadcast-control-apply
no snmp-server enable port-traps atc broadcast-control-apply

初期設定

無効

コマンドモード

Interface Configuration (Ethernet)

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc
 broadcast-control-apply
Console(config-if)#
```

関連するコマンド

auto-traffic-control alarm-fire-threshold（P559）
auto-traffic-control apply-timer（P556）

snmp-server enable port-traps atc multicast-control-apply

マルチキャストトラフィックが自動ストームコントロールの上限のしきい値を超え、アプライタイマが期限切れになった時にトラップを送信します。"no" **を前に置くことでトラップを無効にします。**

文法

snmp-server enable port-traps atc multicast-control-apply
no snmp-server enable port-traps atc multicast-control-apply

初期設定

無効

コマンドモード

Interface Configuration (Ethernet)

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc
 multicast-control-apply
Console(config-if)#
```

関連するコマンド

auto-traffic-control alarm-fire-threshold（P559）

snmp-server enable port-traps atc broadcast-control-release

ストームコントロールレスポンスが引き起こされ、リリースタイマの期限が切れた後に、ブロードキャストトラフィックが下限のしきい値を下回った時トラップを送信します。"no" **を前に置くことでトラップを無効にします。**

文法

snmp-server enable port-traps atc broadcast-control-release
no snmp-server enable port-traps atc broadcast-control-release

初期設定

無効

コマンドモード

Interface Configuration (Ethernet)

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc
 broadcast-control-release
Console(config-if)#
```

関連するコマンド

auto-traffic-control alarm-clear-threshold（P560）
auto-traffic-control action（P561）
auto-traffic-control release-timer（P557）

snmp-server enable port-traps atc multicast-control-release

ストームコントロールレスポンスが引き起こされ、リリースタイマの期限が切れた後に、マルチキャストトラフィックが下限のしきい値を下回った時トラップを送信します。"no" **を前に置くことでトラップを無効にします。**

文法

snmp-server enable port-traps atc multicast-control-release
no snmp-server enable port-traps atc multicast-control-release

初期設定

無効

コマンドモード

Interface Configuration (Ethernet)

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#snmp-server enable port-traps atc
 multicast-control-release
Console(config-if)#
```

関連するコマンド

auto-traffic-control alarm-clear-threshold（P560）

auto-traffic-control action（P561）

auto-traffic-control release-timer（P557）

show auto-traffic-control

自動ストームコントロールのグローバル設定を表示します。

コマンドモード

Privileged Exec

例

```
Console#show auto-traffic-control

Storm-control: Broadcast
 Apply-timer (sec)    : 300
 release-timer (sec) : 900

Storm-control: Multicast
 Apply-timer(sec)     : 300
 release-timer(sec)   : 900
Console#
```

show auto-traffic-control interface

指定されたポートのインタフェース設定とストームコントロールステータスを表示します。

文法

show auto-traffic-control interface *interface*

- *interface*

  − ethernet *unit/port*

    − *unit* — **ユニット番号** "1"

    − *port* — **ポート番号（範囲：**1-52）

コマンドモード

Privileged Exec

例

```
Console#show auto-traffic-control interface ethernet 1/1
Eth 1/1 Information
---------------------------------------------------------------
Storm Control:              Broadcast                Multicast
State:                      Disabled                 Disabled
Action:                       rate-control               rate-control
Auto Release Control:       Disabled                 Disabled
Alarm Fire Threshold(Kpps): 128                      128
Alarm Clear Threshold(Kpps):128                      128
Trap Storm Fire:            Disabled                 Disabled
Trap Storm Clear:           Disabled                 Disabled
Trap Traffic Apply:         Disabled                 Disabled
Trap Traffic Release:       Disabled                 Disabled
---------------------------------------------------------------

Console#
```

4.13 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。

2 つの 1000Mbps ポートをトランクした場合、full duplex 時には最大 4Gbps のバンド幅となります。

コマンド	機能	モード	ページ
手動設定コマンド			
interface port-channel	interface configuration モードへの移動とトランク設定	GC	P537
channel-group	トランクへのポートの追加	IC	P571
動的設定コマンド			
lacp	現在のインタフェースでの LACP の設定	IC	P572
lacp system-priority	ポート LACP システムプライオリティの設定	IC (Ethernet)	P574
lacp admin-key	ポートアドミンキーの設定	IC (Ethernet)	P575
lacp admin-key	ポートチャンネルアドミンキーの設定	IC(Port Channel)	P576
lacp port-priority	LACP ポートプライオリティの設定	IC (Ethernet)	P577
lacp active/passive	アクティブまたはパッシブ LACP イニシエーションモードを設定	IC (Ethernet)	P578
トランクステータス表示コマンド			
show interfaces status port-channel	トランク情報の表示	NE,PE	P549
show lacp	LACP 関連情報の表示	PE	P579

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：1-8）

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 {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 (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 actor 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
```

lacp active/passive

アクティブまたはパッシブ LACP **開始イニシエーションモードを設定します。**
"no" **を前に置くことで、設定を初期値に戻します。**

文法

lacp { actor | partner } { **active | passive** }

no lacp { actor | partner }

- actor — **アグリゲートリンクのローカルサイド**
- partner — **リンクアグリゲーションのリモート側**
- **active** — **ポートで** LACP **ネゴシエーションのアクティブイニシエーションを有効にします。自動的に** LACP **ネゴシエーションパケットを送信します**
- **passive** — **ポートで** LACP **ネゴシエーションのパッシブイニシエーションを有効にします。**LACP **デバイスがリンクのもう一方で検出された時のみネゴシエーションを開始します**

初期設定

active

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- LACP **イニシエーションモードに関わらず、ターゲットスイッチが同じく接続されたポートで有効になり、ネゴシエーションが成功裏に完了したならトランクは自動的に活動します。**

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor mode active
Console(config-if)#
```

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 から形成します。

4.14 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	P583
show port monitor	**ミラーポートの設定の表示**	PE	P584

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* { rx | tx | both} | vlan *vlan-id* | mac-address *mac-address*]

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：**1-52）
- rx ― **受信パケットのミラー**
- tx ― **送信パケットのミラー**
- both ― **送受信両パケットのミラー**
- *vlan-id* ― VLAN ID（**範囲：**1-4094）
- *mac-address* ― MAC **アドレス（フォーマット：**xx-xx-xx-xx-xx-xx **または** xxxxxxxxxxxx）

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。**
- VLAN **ミラーとポートミラーの両方が有効である時、ターゲットポートは** 2 **倍のミラーパケットを受信します。一度目はソースミラーポートから受信し、その後再びソースミラー** VLAN **からになります。**
- MAC **アドレスのミラー時、スイッチのターゲットポート以外の全てのポートに入る、指定されたソースアドレスの入力トラフィックはディスティネーションポートにミラーされます。**
- **スパニングツリー** BPDU **パケットはターゲットポートへミラーされません。**
- **複数のミラーセッションを作成することが可能ですが、全てのセッションは単一のディスティネーションポートを共有します。**

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* | vlan *vlan id* | mac-address *mac-address* }

- *interface*
  - ethernet *unit/port*
    - *unit* — **ユニット番号** "1"
    - *port* — **ポート番号（範囲：**1-52）
- *vlan-id* — VLAN ID（**範囲：**1-4094）
- *mac-address* — MAC **アドレス（フォーマット：**xx-xx-xx-xx-xx-xx **または** xxxxxxxxxxxx）

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

ソースがポートである時、コマンドはディスティネーションポート、ソースポートおよびミラーモード（RX、TX、RX/TX）**を表示します。ソースが** VLAN **である時、ディスティネーションポートとソースポートのみが表示されます。ソースが** MAC **アドレスである時、ディスティネーションポートと** MAC **アドレスのみが表示されます。**

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#
```

4.15 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	P585

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 > *rate*

no rate-limit <input | output>

- input ― **入力帯域（レート）**
- output ― **出力帯域（レート）**
- *rate*― **トラフィックレートリミットレベル**
  （範囲：64-100000Kbps（1000Mbps）64-1000000Kbps（1Gbps)）

初期設定

入力 / 出力レートリミットステータス：無効

コマンドモード

Interface Configuration （Ethernet, Port Channel）

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#rate-limit input 2000
Console(config-if)#
```

4.16 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	P587
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	P588
show mac-address-table	転送データベースに登録された情報の表示	PE	P588
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	P589
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	P589

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：1-52）
- port-channel *channel-id*（範囲：1-8）
- 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 {address *mac-address* { *mask* } } { interface *interface* } { vlan *vlan-id* } { sort <address | vlan | interface> }

- *mac-address* ― MAC **アドレス**
- *mask* ― **アドレス内の一致するビット**
- *interface*
  - ethernet *unit/port*
    - *unit* ― **ユニット番号** "1"
    - *port* ― **ポート番号（範囲：**1-52**）**
- port-channel *channel-id***（範囲：**1-8**）**
- *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

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 (10-30000 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#
```

4.17 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	P591
spanning-tree mode	STP/RSTP/MSTP **モードの選択**	GC	P592
spanning-tree forward-time	**スパニングツリーブリッジ転送時間の設定**	GC	P593
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	P594
spanning-tree max-age	**スパニングツリーブリッジ最長時間の設定**	GC	P595
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	P596
spanning-tree system-bpdu-flooding	**スパニングツリーがグローバルで無効時、他の全てのポートまたは同じ** VLAN **内の全てのポートのみに** BPDU **をフラッド**	GC	P597
spanning-tree path-cost method	RSTP/MSTP **のパスコスト方法の設定**	GC	P598
spanning-tree transmission-limit	RSTP/MSTP **の送信リミットの設定**	GC	P599
spanning-tree-mst-configuration	MSTP **設定モードの変更**	GC	P599
mst vlan	**スパニングツリーインスタンスへの** VLAN **の追加**	MST	P600
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	P601
name	MST **名の設定**	MST	P602
revision	MST **リビジョンナンバーの設定**	MST	P603
max-hops	BPDU **が破棄される前最大ホップ数の設定**	MST	P604
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	P604
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	P605
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	P606
spanning-tree edge-port	**エッジポートへのポートファストの有効化**	IC	P607
spanning-tree portfast	**インタフェースのポートファストの設定**	IC	P608
spanning-tree bpdu-filter	**エッジポートの** BPDU **フィルタ**	IC	P609
spanning-tree bpdu-guard	BPDU **受信時にエッジポートをシャットダウン**	IC	P610
spanning-tree port-bpdu-flooding	**グローバルでスパニングツリーが無効時、他のポートへ** BPDU **をフラッド**	IC	P611
spanning-tree root-guard	**指定されたポートが上位の** BPDU **通過を阻止**	IC	P612
spanning-tree link-type	RSTP/MSTP **のリンクタイプを設定**	IC	P613
spanning-tree loopback-detection	**ポートで** BPDU **ループバック検出を有効化**	IC	P614
spanning-tree loopback-detection release-mode	**ポートでループバックリリースモードを設定**	IC	P615
spanning-tree loopback-detection trap	**ポートの** BPDU **ループバック** SNMP **トラップ通知を有効化**	IC	P616

spanning-tree mst cost	MST インスタンスのパスコストの設定	IC	P617
spanning-tree mst port-priority	MST インスタンスプライオリティの設定	IC	P618
spanning-tree protocol-migration	適切な BPDU フォーマットの再確認	PE	P619
show spanning-tree	スパニングツリーの設定を表示	PE	P620
show spanning-tree mst configuration	MST 設定の表示	PE	P622

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。
  ー 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。
  ー 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)
  ーネットワーク上で 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。
  ー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。
  ー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)#
```

関連するコマンド

spanning-tree forward-time（P593）
spanning-tree max-age（P595）

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)#
```

関連するコマンド

spanning-tree forward-time（P593）
spanning-tree hello-time（P594）

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 system-bpdu-flooding

スイッチでスパニングツリーがグローバルまたは指定したポートで無効になった時、BPDU**をスイッチの他の全てのポートへフラッドあるいは同じ** VLAN **の他の全てのポートへのみへフラッドするかを設定します。**"no" **を前に置くことで設定を初期値に戻します。**

文法

spanning-tree system-bpdu-flooding < to-all | to-vlan >

no spanning-tree system-bpdu-flooding

- to-all ― BPDU **をスイッチ内の他の全てのポートへフラッド**
- to-all ― BPDU **を受信ポートのネイティブ** VLAN**（ポートの** PVID **を決定するように）の全てのポートへフラッド**

初期設定

同じ VLAN **内の他の全てのポートへフラッド**

コマンドモード

Global Configuration

コマンド解説

BPDU **フラッディングがポートで無効の場合、(**611 **ページの「**spanning-tree port-bpdu-flooding**」を参照)**spanning-tree system-bpdu-flooding **コマンドの効果はありません。**

例

```
Console(config)#spanning-tree system-bpdu-flooding
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（P600）
mst priority（P601）
name（P602）
revision（P603）
max-hops（P604）

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。**

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

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（**P603**）

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**）**

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（P602）

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)

表 4-1 STA **パスコスト推奨範囲**

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

表 4-2 STA **パスコスト推奨値**

ポートタイプ	**リンクタイプ**	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	Half Duplex Full Duplex Trunk	100 95 90	2,000,000 1,999,999 1,000,000
Fast Ethernet	Half Duplex Full Duplex Trunk	19 18 15	200,000 100,000 50,000
Gigabit Ethernet	Full Duplex Trunk	4 3	10,000 5,000

初期設定

表 4-3 **初期値**

ポートタイプ	**リンクタイプ**	IEEE 802.1w-2001
Ethernet	Half Duplex Full Duplex Trunk	2,000,000 1,000,000 500,000
Fast Ethernet	Half Duplex Full Duplex Trunk	200,000 100,000 50,000
Gigabit Ethernet	Full Duplex Trunk	10,000 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（P605）

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 { auto }

no spanning-tree edge-port

- auto ― **インタフェースがエッジポートの時に自動で決定**

初期設定

無効

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（P608）

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（P607）

spanning-tree bpdu-filter

エッジポートで受信された全ての BUDU **をフィルタします。**"no" **を使用することで機能を無効にします。**

文法

spanning-tree bpdu-filter

no spanning-tree bpdu-filter

初期設定

無効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

例

```
Console(config)#interface ethernet ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#spanning-tree bpdu-filter
Console(config-if)#
```

関連するコマンド

spanning-tree edge-port （P607）
spanning-tree portfast （P608）

spanning-tree bpdu-guard

BPDU が受信された際、エッジポートをシャットダウンします。"no" を前に置くことで設定を初期値へ戻します。

文法

spanning-tree bpdu-guard

no spanning-tree bpdu-guard

初期設定

無効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- エッジポートは BPDU を生成しないエンドノードへのみ接続されます。
  もし BPDU がエッジポートで受信された場合、不正なネットワーク設定またはスイッチがハッカーによるアタックを受けていることを示します。
  インタフェースが BPDU ガードによってシャットダウンされた場合、"no spanning-tree" コマンドを使用し、手動で再有効化する必要があります。

- BPDU ガードを有効にする前に、"spanning-tree edge-port" コマンドを使用し、インタフェースをエッジポートとして設定してください。

例

```
Console(config)#interface ethernet ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#spanning-tree bpdu-guard
Console(config-if)#
```

関連するコマンド

spanning-tree edge-port （P607）
spanning-tree portfast （P608）
spanning-tree spanning-disabled（P604）

spanning-tree port-bpdu-flooding

スパニングツリーがグローバルまたは特定のポートで無効時、BPDU **を他のポートへフラッドします。**"no" **を前に置くことで設定を初期値へ戻します。**

文法

spanning-tree port-bpdu-flooding

no spanning-tree port-bpdu-flooding

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- **有効時、**BPDU **はスイッチの他の全てのポートまたは、**"spanning-tree system-bpdu-flooding" **コマンド（**P597**）で指定された レシーバポートのネイティブ** VLAN **内の全てのポートへフラッドされます。**
- "spanning-tree port-bpdu-flooding" **コマンドにて、**BPDU **フラッディングがポートで無効になっている場合、**"spanning-tree system-bpdu-flooding" **コマンド（**P597**）の効果はありません。**

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree port-bpdu-flooding
Console(config-if)#
```

spanning-tree root-guard

このコマンドは、指定されたポートが上位の BPDU を考慮に入れ、新しい STP ルートポートを選択されることを阻止するよう設定します。
"no" を前に置くことで機能を無効にします。

文法

spanning-tree root-guard

no spanning-tree root-guard

初期設定

無効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- 低いブリッジ識別子（または同じ識別子と低い MAC アドレス）を持つブリッジはいつでもルートブリッジを引き継ぐことが可能です。
- スパニングツリーがスイッチまたはインタフェースででグローバルに初期化された時、スイッチはルートガードを有効にする前に、スパニングツリーが一点に集まったことが保証されるまで、20 秒間待ちます。

例

```
Console(config)#interface ethernet ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#spanning-tree root-guard
Console(config-if)#
```

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 ー duplex モードの設定から自動的に設定
- point-to-point ー point to point リンク
- shared ー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 loopback-detection

このコマンドは、ポートで検出とスパニングツリーループバックパケットへの返答を有効にします。"no" **を前に置くことでこの機能を無効にします。**

文法

spanning-tree loopback-detection

no spanning-tree loopback-detection

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- **ループバック検出が有効であり、ポートがそれ自身の** BPDU **を受信した場合、ポートは** IEEE Standard 802.1W-2001 9.3.4 **に従って、ループバック** BPDU **を破棄します。**.
- **スイッチでスパニングツリーが無効の場合、ポートループバック検出はアクティブになりません。**

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree loopback-detection
```

spanning-tree loopback-detection release-mode

BPDU ループバックが受信された為にディスカーディングステーツに置かれているポートのリリースモードを設定します。"no" を前に置くことで設定を初期状態に戻します。

文法

spanning-tree loopback-detection release-mode < auto | manual >

no spanning-tree loopback-detection

- auto ― ループバックステーツ終了時、ディスカーディングステーツから自動でリリースさせます。
- manual ― ポートは手動でのみリリースされます。

初期設定

auto

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- ポートが自動ループバックリリースに設定されている場合、以下の条件の内一つが満たされたとき、ポートはフォワーディングステーツへ戻ります。
  - ―ポートが自身以外の BPDU を受信
  - ―ポートリンクステータスがリンクダウンへ変更後再リンクアップ
  - ―フォワード遅延間隔の間にポートが自身の BPDU の受信を中止した場合
- ループバック検出が無効である、ポートが自身の BPDU を受信した場合、IEEE Standard 802.1W-2001 9.3.4 に従いループバック BPDU を破棄します。
- スイッチでスパニングツリーが無効の場合、ポートループバック検出はアクティブになりません。
- 手動リリースモードに設定されている時、リンクダウン / アップイベントはポートをディスカーディングステーツからリリースしません。

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree loopback-detection release-mode manual
```

spanning-tree loopback-detection trap

スパニングツリーループバック BPDU **検出の** SNMP **トラップ通知を有効にします。**
"no" **を前に置くことで設定を初期状態に戻します。**

文法

spanning-tree loopback-detection trap

no spanning-tree loopback-detection trap

初期設定

無効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

例

```
Console(config)#interface ethernet ethernet 1/5
Console(config-if)#spanning-tree loopback-detection trap
```

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)
  パスコスト推奨範囲は 605 ページの表 4-1、パスコスト推奨値は 605 ページの表 4-2 を参照してください。

初期設定

パスコスト初期値は 605 ページの表 4-3 の表を参照してください。

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（P618）

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 （P617）

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：**1-52）
  - port-channel *channel-id*（**範囲：**1-8）

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 { *interface* | mst *instance-id* }

- *interface*
  - ethernet *unit/port*
    - *unit* — ユニット番号 ”1”
    - *port* — ポート番号（範囲：1-52）
  - port-channel *channel-id*（範囲：1-8）
- *instance-id* — MST インスタンス 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 P179 「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 P182 「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:    Disabled
 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:                   32768.0012CFBBC0C0
 Current Root Port:                 0
 Current Root Cost:                 0
 Number of Topology Changes:        0
 Last Topology Change Time (sec.): 8822
 Transmission Limit:                3
 Path Cost Method:                  Long
 Flooding Behavior:                 To VLAN
--------------------------------------------------------------------
Eth  1/ 2 Information
--------------------------------------------------------------------
 Admin Status:              Enabled
 Role:                      Disabled
 State:                     Forwarding
 Admin Path Cost:           0
 Oper Path Cost:            1000000
 Priority:                  128
 Designated Cost:           0
 Designated Port:           128.2
 Designated Root:           32768.0012CFBBC0C0
 Designated Bridge:         32768.0012CFBBC0C0
 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

```
onsole#show spanning-tree mst configuration
MSTP Configuration Information
-------------------------------------------------------------
 Configuration Name: 00 12 cf bb c0 c0
 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	P624
Editing VLAN Groups	VLAN 名、VID、状態を含む VLAN の設定	P629
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	P631
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	P640
Configuring 802.1Q Tunneling	802.1Q トンネリング（QinQ トンネリング）の設定	P641
Configuring Port-based Traffic Segmentation	指定したダウンリンク / アップリンクポートに基づく、異なるクライアントセッションのトラフィックセグメンテーション設定	P646
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	P641
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	P659
Configuring IP Subnet VLANs	IP サブネット VLAN の設定	P663
Configuring MAC Based VLANs	MAC ベース VLAN の設定	P665
Configuring Voice VLANs	VoIP トラフィック検出とボイス VLAN の有効化	P667

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	P624
show bridge-ext	bridge extension 情報の表示	PE	P625
switchport gvrp	インタフェースへの GVRP の有効化	IC	P625
switchport forbidden vlan	インタフェースへの登録禁止 VLAN の設定	IC	P637
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	P626
garp timer	選択した機能への GARP タイマーの設定	IC	P627
show garp timer	選択した機能への GARP タイマーの表示	NE,PE	P628

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 P196 「VLAN 基本情報の表示」及び P22 「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:                    Disabled
 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*
  - ー *ethernet unit/port*
    unit ― **ユニット番号** ”1”
    port ― **ポート番号（範囲：**1-52）
  - ー port-channel *channel-id*（**範囲：**1-8）

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（P628）

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*

  ー ethernet *unit/port*

  unit ― **ユニット番号** ”1”

  port ― **ポート番号（範囲：**1-52）

  ー port-channel *channel-id*（**範囲：**1-8）

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（P627）

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	P629
VLAN	VID,VLAN 名、ステートなど VLAN の設定	VC	P630

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（P640）

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
  - ー active ― VLAN の実行
  - ー 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。

[注意] 本機は最大 255 個のユーザ管理可能な VLAN を作成することが出来ます。1 つのユーザ管理不可の VLAN（VLAN ID 4093）はスイッチクラスタに使用されます。

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 （P640）

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	P631
switchport mode	インタフェースの VLAN メンバーモードの設定	IC	P632
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	P633
switchport ingress-filtering	インタフェースへの入力フィルタの有効化	IC	P634
switchport native vlan	インタフェースの PVID(native VLAN) の設定	IC	P635
switchport allowed vlan	インタフェースに関連した VLAN の設定	IC	P636
switchport gvrp	インタフェースへの GVRP の有効化	IC	P625
switchport forbidden vlan	インタフェースの登録を禁止する VLAN の設定	IC	P637
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	P701
vlan-trunking	スイッチを通る未知の VLAN を許可	IC	P638

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 （P640）

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 < access | hybrid | trunk | private VLAN >

no switchport mode

- access — **アクセス** VLAN **インタフェースを指定。このポートはタグ無しフレームのみ受信 / 転送を行います。**
- 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。**
- private-vlan — **詳細については、**655 **ページの「**switchport mode private-vlan**」を参照して下さい。**

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（P632）

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。**

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。

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。

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)#
```

vlan-trunking

未知の VLAN グループが指定されたインタフェースを通過することを許可します。
"no" を前に置くことで、この機能を無効にします。

文法

vlan-trunking
no vlan-trunking

初期設定

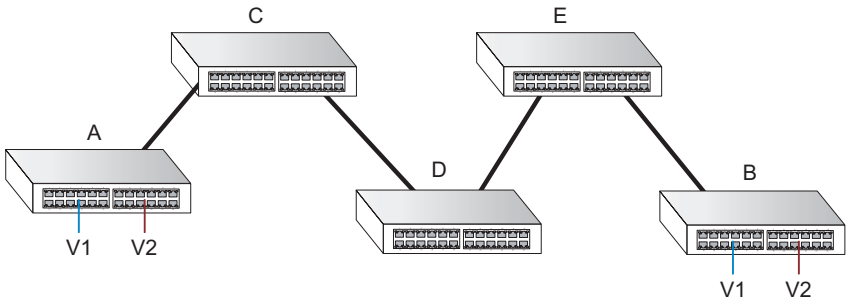
無効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- 本コマンドは、それらが属さない VLAN グループのトラフィックを渡す 1 つ以上の中間スイッチを横切るトンネルを設定します。
  以下の図は VLAN1 と 2 をスイッチ A と B へ VLAN トランキングと共に設定し、スイッチ C,D および E を横断するこれらの VLAN グループがトラフィックを渡すために使用されます。



  VLAN トランキングが無い場合、全ての中間スイッチへ VLAN1 と 2 を設定する必要があります。さもなければこれらのスイッチは未知の VLAN グループタグのついたフレームを破棄します。VLAN トランキングを有効にすれば、スイッチ A と B へのみ、これらの VLAN グループを作成するだけで中間スイッチポートは経路に沿って VLAN1 と VLAN2 の接続が行えます。
  D と E は、VLAN グループタグ 1 と 2 が付いたフレームを自動的に許可し、VLAN トランキングポートを通過することが可能になります。
- この機能には以下の制限が適用されます。
  - VLAN トランキングはギガビットスイッチポートまたはトランクでのみ有効に出来ます。
  - VLAN トランキングは "access" スイッチポートモード（632 ページの「switchport mode」を参照）と相互に排他的です。もし VLAN トランキングがインタフェースで有効の場合、このインタフェースはアクセスモードには設定することが出来ません。その逆もまた同様です。
- スパニングツリー構成からのループを防ぐ為、全ての未知の VLAN は一つのインスタンス（STP/RSTP または MSTP インスタンス、選択された STA モードに依存）へバインドされます。
- ポートで、VLAN トランキングとイングレスフィルタリングの両方が無効の場合、未知のタグが付いたパケットはこのインタフェースへ入ることを許可され、VLAN トランキングが有効であるその他全てのポートへフラッドされます。（VLAN トランキングの効果は未知の VLAN で依然有効です。）

例

```
Console(config)#interface ethernet 1/27
Console(config-if)#vlan-trunking
Console(config-if)#interface ethernet 1/28
Console(config-if)#vlan-trunking
```

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	P640
show interfaces status vlan	特定 VLAN インタフェースの状態の表示	NE,PE	P549
show interfaces switchport	インタフェースの管理、運用状態の表示	NE,PE	P551

show vlan

VLAN 情報の表示を行います。

文法

show vlan { id *vlan-id* | name *vlan-name* | Private-VLAN *private-vlan-type* }

- id － VLAN ID
- name － VLAN 名
- Private-VLAN －詳細については、658 ページの「show vlan private-vlan」を参照して下さい。
- *private-vlan-type* －プライベート VLAN タイプを指定
  （オプション：Community、Primary）

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

IEEE 802.1Q トンネリング（QinQ）機能を使用することにより、サービス プロバイダは複数の VLAN を設定しているカスタマを、1 つの VLAN を使用してサポートできます。カスタマの VID は保持されるため、さまざまなカスタマからのトラフィックは、同じ VLAN 上に存在するように見える場合でも、サービスプロバイダのインフラストラクチャ内では分離されています。QinQ トンネリングでは、VLAN 内 VLAN 階層を使用して、タグ付きパケットに再度タグ付けを行うこと（ダブルタギングとも呼ばれます）によって、VLAN スペースを拡張します。

この節では、QinQ トンネリングの設定に使用されるコマンドについて説明します。

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	P642
switchport dot1q-tunnel mode	インタフェースを QinQ トンネルポートに設定	IC	P643
switchport dot1q-tunnel tpid	トンネルポートの TPID（Tag Protocol Identifier）値を設定	IC	P644
show dot1q-tunnel	QinQ トンネルポートの設定を表示	PE	P645
show interfaces switchport	QinQ ポートステータスを表示	PE	P551

QinQ の一般的な設定ガイド

（1）スイッチを QinQ モードに設定（dot1q-tunnel system-tunnel-control P642）

（2）SPVLAN を作成（vlan P630）

（3）QinQ トンネルアクセスポートを dot1Q トンネルアクセスモードに設定
（switchport dot1q-tunnel mode P643）

（4）トンネルアクセスポートの Tag Protocol Identifier (TPID) 値を設定。このステップは、接続されているクライアントが、802.1Q タグ付きフレームの識別に非標準 2-byte イーサタイプを使用している場合に必要です。
（switchport dot1q-tunnel tpid　P644）

（5）QinQ トンネルアクセスポートをタグ無しメンバーとして SPVLAN に追加
（switchport allowed vlan　P636）

（6）QinQ トンネルアクセスポートの SPVLAN ID をネイティブ VID として設定
（switchport native vlan　P635）

（7）QinQ トンネルアップリンクポートを dot1Q トンネルアップリンクモードに設定
（switchport dot1q-tunnel mode　P643）

（8）QinQ トンネルアップリンクポートをタグ付きメンバーとして SPVLAN に追加
（switchport allowed vlan　P636）

QinQ の制限事項

- トンネルアップリンクポートのネイティブ VLAN とトンネルアクセスポートは同一には出来ませんが、同じサービス VLAN を両方のトンネルポートタイプに設定することは可能です。
- トンネルポートでは IGMP スヌーピングを有効に出来ません。
- スパニングツリープロトコルが有効時に、スパニングツリー構造がツリーの中断を克服するために自動で再配置された場合、トンネルアクセスまたはトンネルアップリンクポートは無効になります。これらのポートではスパニングツリーを無効にすることが賢明です。

dot1q-tunnel system-tunnel-control

スイッチが QinQ モードで動作するよう設定を行います。"no" を前に置くと QinQ オペレーティングモードを無効にします。

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

コマンド解説

QinQ インタフェース設定が機能するために、QinQ トンネルモードをスイッチで有効にしてください。

例

```
Console(config)#dot1q-tunnel system-tunnel-control
Console(config)#
```

関連するコマンド

show dot1q-tunnel （P645）
show interfaces switchport （P551）

switchport dot1q-tunnel mode

インタフェースを QinQ **トンネルポートとして設定します。**"no" **を前に置くことでインタフェースの** QinQ **を無効にします。**

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)

コマンド解説

- switchport dot1q-tunnel mode **インタフェースコマンドを使用する前に、**dot1q-tunnel system-tunnel-control **コマンドを使用して** QinQ **トンネリングを有効にする必要があります。**
- **トンネルアップリンクポートがカスタマからのパケットを受信した際、カスタマタグ（**1 **つ以上のタグレイヤがあるか否かにかかわらず）は内側に保持され、サービスプロバイダのタグが外側のタグに付加されます。**
- **トンネルアップリンクポートがサービスプロバイダからのパケットを受信した際、外側のサービスプロバイダタグは取り除かれ、パケットは内側のタグが示す** VLAN **へ渡されます。内側のタグが見つからない場合、パケットはアップリンクポートに定義されたネイティブ** VLAN **へ渡されます。**

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（P645）

show interfaces switchport（P551）

switchport dot1q-tunnel tpid

トンネルポートの Tag Protocol Identifier (TPID) **値を設定します。**"no" **を前に置くことで設定を初期値へ戻します。**

文法

switchport dot1q-tunnel tpid *tpid*

no switchport dot1q-tunnel tpid

- *tpid* ― 802.1Q **カプセル化のイーサタイプ値を設定。この識別子は** 802.1Q **タグ付きフレームの識別に非標準** 2-byte **を選択するために使用します。標準イーサタイプ値は** 0x8100 **（範囲：**0800-FFFF16 **進数）**

初期設定

0x8100

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- "switchport dot1q-tunnel tpid" **コマンドは選択されたインタフェースのカスタム** 802.1Q **イーサタイプ値を設定します。**
  この機能は本機へ、802.1Q **タグ付きフレームの識別に標準** 0x8100 **イーサタイプを使用しないサードパーティ製スイッチとインタオペレートすることを許可します。**
  例えば、0x1234 **はトランクポートのカスタム** 802.1Q **イーサタイプとして設定され、このイーサタイプを含む入力フレームは、イーサタイプフィールドに続くタグに含まれる** VLAN **へ、標準的** 802.1Q **トランクとして割り当てられます。**
  その他のイーサタイプを持つポートへ到着したフレームはタグ無しフレームとして見られ、このポートのネイティブ VLAN **へ割り当てられます。**

- **スイッチの全てのポートは同じイーサタイプに設定されます。**

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（P551）

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.
.
.
.
```

関連するコマンド

switchport dot1q-tunnel mode（P643）

4.18.6 ポートベーストラフィックセグメンテーション

ローカルネットワークおよびサービスプロバイダへのアップリンクポート上で、異なるクライアントからダウンリンクポートを通過するトラフィックに、より厳しいセキュリティが必要とされる際、個々のクライアントセッションのトラフィックを隔離するためにポートベーストラフィックセグメンテーションを使用できます。
それぞれのクライアントに属するトラフィックは、割り当てられたダウンリンクポートに隔離されます。
スイッチは、クライアントの割り当てられたアップリンクポート全体に渡る通過を、他のクライアントにアサインされたアップリンクポートから孤立させるようにする、または異なるクライアントへセキュリティの危険が低いアップリンクポートへのアクセスの共有を許可し他のクライアントを使用してトラフィックがアップリンクポートを通過・転送を可能にする、のいずれかに設定することができます。

コマンド	機能	モード	ページ
pvlan	トラフィックセグメンテーションの有効化	GC	P647
pvlan uplink/downlink	クライアントセッションのアップリンク / ダウンリンクポートを設定	GC	P648
pvlan session	クライアントセッションの作成	GC	P649
pvlan up-to-up	異なるクライアントセッションに割り当てられたアップリンクポート間で、トラフィック転送が可能か否かを指定	GC	P650
show pvlan	トラフィックセグメンテーション設定の表示	PE	P651

pvlan

ポートベーストラフィックセグメンテーションを有効にします。"no" **を前に置くことで機能を無効にします。**

文法

pvlan

no pvlan

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

- **トラフィックセグメンテーションが有効時、異なるクライアントセッションに割り当てられたアップリンクおよびダウンリンクポートのフォワーディングステーツは以下になります。**

Destination Source	Session #1 Downlinks	Session #1 Uplinks	Session #2 Downlinks	Session #2 Uplinks	Normal Ports
Session #1 Downlink Ports	Blocking	Forwarding	Blocking	Blocking	Blocking
Session #1 Uplink Ports	Forwarding	Forwarding	Blocking	Blocking/ Forwarding*	Forwarding
Session #2 Downlink Ports	Blocking	Blocking	Blocking	Forwarding	Blocking
Session #2 Uplink Ports	Blocking	Blocking/ Forwarding*	Forwarding	Forwarding	Forwarding
Normal Ports	Forwarding	Forwarding	Forwarding	Forwarding	Forwarding

* **アップリンクからアップリンクへのフォワーディングステーツは** "pvlan uplink/downlink" **コマンド**（P648）**によって設定をおこないます。**

- **トラフィックセグメンテーションが無効時、全てのポートは** VLAN **・スパニングツリー等他の機能に指定された設定を基にする通常フォワーディングモードで動作します。**

例

```
Console(config)#pvlan
Console(config)#
```

pvlan uplink/downlink

トラフィックセグメンテーションクライアントセッションのアップリンク / ダウンリンクポートを設定します。"no" **を前に置くことで、ポートを通常オペレーティングモードへ戻します。**

文法

[**no**] **pvlan** [session *session-id*] { **uplink** *interface-list* [**downlink** *interface-list*] | **downlink** *interface-list* }

- *session-id* — **トラフィックセグメンテーションセッション（範囲：**1-15**）**
- *interface-list* — 1 **つ以上のアップリンクまたはダウンリンクインタフェース**
  - ー ethernet *unit/port*
    unit — **ユニット番号** ”1”
    port — **ポート番号（範囲：**1-52**）**
  - ー port-channel *channel-id***（範囲：**1-8**）**

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- **ポートをアップリンク、ダウンリンク両リストに設定することは出来ません。**
- **ポートは** 1 **つのトラフィックセグメンテーションセッションへのみ割り当てることが可能です。**
- **ダウンリンクポートは同じセッション内でのみアップリンクポートと通信可能です。そのため、もしアップリンクポートがセッションで設定されていない場合、アサインされたダウンリンポートは他のどのポートとも通信は行えません。**
- **ダウンリンクポートがセッションで設定されていない場合、アサインされたアップリンクポートはノーマルポートとして機能します。**
- **スイッチの** ASIC **制限の理由で、いずれかのグループメンバーがアップリンクまたはダウンリンクインタフェースっとして設定されている際、ポート** 1-8、9-16、17-24 **はグループになります。**

例

```
Console(config)#pvlan session 1 uplink ethernet 1/5 downlink ethernet 1/6
Console(config)#
```

pvlan session

トラフィックセグメンテーションクライアントセッションを作成します。"no" **を前に置くことで、クライアントセッションを削除します。**

文法

pvlan session *session-id*

no pvlan session

- *session-id* ― **トラフィックセグメンテーションセッション（範囲：**1-15）

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- **本コマンドは新しいトラフィックセグメンテーションクライアントセッションを作成するために使用します。**
- "no" **を前に付けると、アサインされているアップリンクまたはダウンリンクポートを削除し、これらのインタフェースを通常オペレーティングモードへ戻します。**

例

```
Console(config)#pvlan session 1
Console(config)#
```

pvlan up-to-up

異なるクライアントセッションへアサインされたアップリンクポート間で、トラフィックの転送を可能にするか否かを設定します。"no" **を前に置くことで設定を初期値に戻します。**

文法

pvlan up-to-up < blocking | forwarding >

no pvlan up-to-up

- blocking ― **異なるセッションにアサインされたアップリンクポート間のトラフィックをブロックします。**
- forwarding ― **異なるセッションにアサインされたアップリンクポート間のトラフィックを転送します。**

初期設定

Blocking

コマンドモード

Global Configuration

コマンド解説

- **本コマンドは新しいトラフィックセグメンテーションクライアントセッションを作成するために使用します。**
- "no" **を前に付けると、アサインされているアップリンクまたはダウンリンクポートを削除し、これらのインタフェースを通常オペレーティングモードへ戻します。**

例

異なるセッションにアサインされたアップリンクポート間のトラフィック転送を有効にしています。

```
Console(config)#pvlan up-to-up blocking
Console(config)#
```

show pvlan

トラフィックセグメンテーション設定を表示します。

文法

show pvlan session *session-id*

- *session-id* — トラフィックセグメンテーションセッション（範囲：1-15）

コマンドモード

Privileged Exec

コマンド解説

- 本コマンドは新しいトラフィックセグメンテーションクライアントセッションを作成するために使用します。
- "no" を前に付けると、アサインされているアップリンクまたはダウンリンクポートを削除し、これらのインタフェースを通常オペレーティングモードへ戻します。

例

異なるセッションにアサインされたアップリンクポート間のトラフィック転送を有効にしています。

```
Console#show pvlan

 Private VLAN Status   :                  Enabled
 Uplink-to-Uplink Mode :                  Blocking

 Session   Uplink Ports                   Downlink Ports
--------- ------------------------------ ------------------------------
    1     Ethernet 1/28                  Ethernet 1/9
                                         Ethernet 1/10
                                         Ethernet 1/11
Console#
```

4.18.7 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	P653
private-vlan association	コミュニティ VLAN とプライマリ VLAN の関連付け	VC	P654
プライベート VLAN インタフェースの設定			
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	P655
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	P656
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	P657
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	P658

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。

Private vlan

プライベート VLAN**（プライマリ、コミュニティ）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 >

no private-vlan *vlan-id*

- *vlan-id* ― **プライベート** VLAN **の** ID**（範囲：**1-4094**）**
- 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

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。**
- **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** P632 **「**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** { *secondary-vlan-id* | add *secondary-vlan-id* | remove *secondary-vlan-id* }

no private vlan *primary-vlan-id* **association**

- *primary-vlan-id* ― **プライマリ** VLAN **の** ID**（範囲：**1-4094**）**
- *secondary-vlan-id* ― **セカンダリ（コミュニティ）**VLAN**（範囲：**1-4094**）**

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。**

例

```
Console(config)#interface ethernet 1/2
Console(config-if)#switchport mode private-vlan promiscuous
Console(config-if)#exit
Console(config)#interface ethernet 1/3
Console(config-if)#switchport mode private-vlan host
Console(config-if)#
```

switchport private-vlan host-association

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：**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

- **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 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：**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

- **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 | primary }

- community ーコミュニティ 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。
- primary ープライマリ 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
--------  -----------  ----------  ---------------------------------
----------
     0         10       Community
    20                  Primary
Console#
```

4.18.8 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	P660
protocol-vlan protocol-group	プロトコルグループの VLAN へのマッピング	IC	P661
show protocol-vlan protocol-group	プロトコルグループの設定の表示	PE	P662
show protocol-vlan protocol-group-vid	VLAN へのプロトコルグループマップングの表示	PE	P662

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 } frame-type *frame-type* protocol-type *protocol*]
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**）**
- frame-type ― **フレームタイプ（オプション：**ethernet**、**rfc_1042**、**llc_other**）**
- *protocol* ― **プロトコルタイプ。**iic_other **フレームタイプは** ipx_raw **のみ選択できます。その他全てのフレームタイプのオプションは** ip**、**arp**、**rarp **です。**

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 2 add frame-type ethernet
 protocol-type arp
Console(config)#
```

protocol-vlan protocol-group (Configuring VLANs)

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

- **本機には最大** 20 **のプロトコル** VLAN **グループを設定出来ます。**
- **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

```
Console#show protocol-vlan protocol-group

 ProtocolGroup ID Frame Type Protocol Type
------------------ ------------- ---------------
                2   RFC 1042      08 00
Console#
```

show protocol-vlan protocol-group-vid

プロトコルグループから VLAN **へのマッピングを表示します。**

文法

show protocol-vlan protocol-group-vid

初期設定

マッピングされた全てのプロトコルグループを表示

コマンドモード

Privileged Exec

例

```
Console#show protocol-vlan protocol-group-vid

ProtocolGroup ID     VLAN ID
------------------ -----------
              2      VLAN2
Console#
```

4.18.9 IP サブネット VLAN

ポートベースの分類を使用する時、ポートによって受け取られた全てのタグ無しフレームは、ポートと関連付けられた VID（PVID）**の** VLAN **に属しているとして分類されます。**
IP **サブネット** VLAN **分類が有効時、タグ無し入力フレームのソースアドレスは** IP subnet-to-VLAN **マッピングテーブルにたいしてチェックを行われます。**
エントリがサブネットに見つかった場合、これらのフレームはエントリが示し VLAN **へ割り当てられます。**
IP **サブネットが一致しない場合、タグ無しフレームは受信ポートの** VLAN ID（PVID）**に属しているとして分類されます。**

コマンド	機能	モード	ページ
subnet-vlan	IP **サブネット** VLAN **を定義**	GC	P663
show subnet-vlan	IP **サブネット** VLAN **設定を表示**	PE	P664

subnet-vlan

IP **サブネット** VLAN **割り当てを設定します。**"no" **を前に置くことで、**IP **サブネットから** VLAN **への割り当てを削除します。**

文法

subnet-vlan subnet *ip-address mask* vlan *vlan-id*

no subnet-vlan < *ip-address mask* | all >

- *ip-address* ― ip-address - **サブネットを定義する** IP **アドレス。有効な** IP **アドレスはピリオドで区切られた** 0-255 **の** 4 **つの** 10 **進数で成り立ちます。**
- *mask* ― IP **サブネットのホストアドレスビットを識別します。**
- *vlan-id* ― VLAN ID(**範囲：**1-4094)

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- **それぞれの** IP **サブネットは** 1 **つの** VLAN ID **へのみマップが可能です。**IP **サブネットは** IP **アドレスとマスクから構成されます。**
- **ポートでタグ無しフレームが受信された際、ソース** IP **アドレスは** IP subnet-to-VLAN **マッピングテーブルに対してチェックが行われ、もしエントリが見つかった場合、対応する** VLAN ID **がフレームに割り当てられます。**
  もしマッピングが見つからない場合、受信ポートの PVID **がフレームへ割り当てられます。**
- IP **サブネットはブロードキャストまたはマルチキャスト** IP **アドレスになることはできません。**

- MAC ベース、IP サブネットベース、プロトコルベース VLAN が同時にサポートされる時、プライオリティはこの順番で適用され、ポートベース VLAN は最後になります。

例

VLAN4 にサブネット 192.168.12.192、マスク 255.255.255.224 のトラフィックを割り当てます。

```
Console(config)#subnet-vlan subnet 192.168.12.192 255.255.255.224 vlan 4
Console(config)#
```

show subnet-vlan

IP サブネット VLAN 割り当てを表示します。

コマンドモード

Privileged Exec

コマンド解説

・本コマンドは subnet-to-VLAN マッピングを表示するために使用します。

例

全ての設定された IP サブネットベース VLAN を表示しています。

```
Console(config)#subnet-vlan subnet 192.168.12.192 255.255.255.224 vlan 4
Console(config)#
```

4.18.10 MAC ベース VLAN

802.1Q ポートベース VLAN 分類を使用する時、ポートで受信される全てのタグ無しフレームは、VID（PVID）がそのポートと関連付けられた VLAN に所属するように分類されます。MAC ベース VLAN 有効時、タグ無し入力フレームのソースアドレスは、MAC address-to-VLAN テーブルに対して照合が行われます。
このアドレスのエントリが見つかった場合、これらのフレームはエントリが示す VLAN へ割り当てられます。
MAC アドレスが一致しない場合、タグ無しフレームは受信ポートの VLAN ID（PVID）に属しているとして分類されます。

コマンド	機能	モード	ページ
mac-vlan	MAC address-to-VLAN マッピングを設定	GC	P665
show mac-vlan	MAC ベース VLAN 設定の表示	PE	P666

mac-vlan

MAC address-to-VLAN マッピングの設定を行います。"no" を前に置くことで割り当てを削除します。

文法

mac-vlan mac-address *mac-address* vlan *vlan-id*

no mac-vlan mac-address

- *mac-address* — マッチするソース MAC アドレス。設定された MAC アドレスはユニキャストアドレスにのみなれます。MAC アドレスは "xx-xx-xx-xx-xx-xx" または "xxxxxxxxxxxx" のフォーマットで指定してください。
- *vlan-id* — ソース MAC アドレスとマッチする VLAN（設定範囲：1-4094）

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- MAC-to-VLAN マッピングは本機の全てのポートへ適用されます。
- ソース MAC アドレスは 1 つの VLAN ID へのみマップされることが可能です。
- 設定された MAC アドレスはブロードキャストまたはマルチキャストアドレスにはなれません。
- MAC ベース、IP サブネットベース、プロトコル VLAN が同時にサポートされる時、このシーケンスではプライオリティが適用され、最後にポートベース VLAN になります。

例

```
Console(config)#mac-vlan mac-address 00-00-00-11-22-33 vlan 10
Console(config)#
```

show mac-vlan

MAC address-to-VLAN 割り当てを表示します。

コマンドモード

Privileged Exec

例

```
Console#show mac-vlan
     MAC address     VLAN ID
------------------- ---------
  00-00-00-11-22-33     10
Console#
```

4.18.11 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	P668
voice vlan aging	Voice VLAN ポートのエージングタイムを設定	GC	P668
voice vlan mac-address	VoIP デバイスの MAC アドレスを設定	GC	P669
switchport voice vlan	Voice VLAN ポートモードを設定	IC	P670
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	P671
switchport voice vlan security	ポートの Voice VLAN セキュリティを有効	IC	P672
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	P672
show voice vlan	Voice VLAN 設定を表示	PE	P673

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 の設定ー「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** 674 **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#
```

4.19 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	P675
lldp holdtime-multiplier	TTL(time-to-live) 値の設定	GC	P676
lldp med-fast-start-count	medFastStart の数を設定	GC	P677
lldp notification-interval	LLDP の変更に関する SNMP 通知送信の間隔を設定	GC	P677
lldp refresh-interval	LLDP 配信の転送間隔を設定	GC	P678
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	P678
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	P679
lldp admin-status	LLDP メッセージの送信・受信のモードを有効	IC	P679
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	P680
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	P680
lldp basic-tlv management-ip-address	TLV Type “management-ip-address“ を設定	IC	P681
lldp basic-tlv port-description	TLV Type “port-description“ を設定	IC	P681
lldp basic-tlv system-capabilities	TLV Type “system-capabilities“ を設定	IC	P682
lldp basic-tlv system-description	TLV Type “system-description“ を設定	IC	P683
lldp basic-tlv system-name	TLV Type “system-name“ を設定	IC	P684
lldp dot1-tlv proto-ident	lldp dot1-TLV“ proto-ident“ を設定	IC	P685
lldp dot1-tlv proto-vid	lldp dot1-TLV“ proto-vid“ を設定	IC	P685
lldp dot1-tlv pvid	lldp dot1-TLV“pvid“ を設定	IC	P686
lldp dot1-tlv vlan-name	lldp dot1-TLV“vlan-name“ を設定	IC	P687
lldp dot3-tlv link-agg	lldp dot3-TLV“link-agg“ を設定	IC	P688
lldp dot3-tlv mac-phy	lldp dot3-TLV“mac-phy“ を設定	IC	P689

lldp dot3-tlv max-frame	lldp dot3-TLV“max-frame“ を設定	IC	P689
lldp dot3-tlv poe	lldp dot3-TLV“poe“ を設定	IC	P690
lldp medtlv extPoe	MED TLV Type“extpoe“ を設定	IC	P691
lldp medtlv inventory	MED TLV Type“ inventory“ を設定	IC	P692
lldp medtlv location	MED TLV Type“location“ を設定	IC	P692
lldp medtlv med-cap	MED TLV Type“med-cap“ を設定	IC	P693
lldp medtlv network-policy	MED TLV Type“network-policy“ を設定	IC	P693
show lldp config	LLDP 設定の表示	PE	P694
show lldp info local-device	LLDP ローカルデバイス情報を表示	PE	P696
show lldp info remote-device	LLDP リモートデバイス情報を表示	PE	P697
show lldp info statistics	LLDP 統計情報を表示	PE	P698

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 P631 「VLAN インタフェースの設定」および P659 「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 P635 「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** P636 **「**switchport allowed vlan**」および** P660 **「**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 P322 「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 medtlv 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 medtlv extPoe

no lldp medtlv 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 medtlv extPoe
Console(config-if)#
```

lldp medtlv 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 medtlv inventory

no lldp medtlv 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 medtlv inventory
Console(config-if)#
```

lldp medtlv 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 medtlv location

no lldp medtlv 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 medtlv location
Console(config-if)#
```

lldp medtlv 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 medtlv med-cap

no lldp medtlv 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 medtlv med-cap
Console(config-if)#
```

lldp medtlv 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 medtlv network-policy

no lldp medtlv 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 medtlv 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：**1-52**）**
  - port-channel *channel-id*（**範囲：**1-8**）**

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
  .
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：**1-52**）**
  - port-channel *channel-id*（**範囲：**1-8）

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 : 52PORT 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：**1-52）
  - port-channel *channel-id*（**範囲：**1-8）

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：**1-52）
  - port-channel *channel-id*（**範囲：**1-8）

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#
```

4.20 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**	P699
Priority（Layer 3 and 4 ）	TCP **ポート、**IP DSCP **タグの** CoS **値への設定**	P705

4.20.1 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	P700
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	P701
queue cos map	**プライオリティキューに** Class of Service(CoS) **を指定**	IC	P702
show queue mode	**現在のキューモードを表示**	PE	P703
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	P703
show queue cos-map	CoS **マップの表示**	PE	P704
show interfaces switchport	**インタフェースの管理、運用ステータスの表示**	PE	P551

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 >

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。**

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
```

関連するコマンド

show queue bandwidth（P703）

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#
```

関連するコマンド

show queue cos-map （P704）

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         8
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：**1-52）

  ー port-channel *channel-id*（**範囲：**1-8）

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#
```

4.20.2 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 CoS マッピングを有効	GC	P705
map ip dscp	IP DSCP 値を CoS にマッピング	IC	P706
show map ip dscp	IP DSCP マップの表示	PE	P707

map ip dscp（Global Configuration）

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

no map ip dscp

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 DSCP、デフォルトポートプライオリティです。

例

本機に IP DSCP マッピングを有効にしています。

```
Console(config)#map ip dscp
Console(config)#
```

map ip dscp（Interface Configuration）

ポートで、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-value*

no map ip dscp

初期設定

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	0
8	1
10, 12, 14, 16	2
18, 20, 22, 24	3
26, 28, 30, 32, 34, 36,	4
38, 40, 42	5
48	6
46,56	7

コマンドモード

Interface Configuration （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

```
Console(config)#interface ethernet 1/5
Console(config-if)#map ip dscp 1 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 *interface*

- *interface*

  ー ethernet *unit/port*

  unit ― **ユニット番号** ”1”

  port ― **ポート番号（範囲：**1-52）

ー port-channel *channel-id*（**範囲：**1-8）

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#show map ip dscp ethernet 1/1
DSCP mapping status: disabled
Port      DSCP COS
--------- ---- ---
Eth 1/ 1     0  0
Eth 1/ 1     1  0
Eth 1/ 1     2  0
Eth 1/ 1     3  0
.
.
.
Eth 1/ 1    61  0
Eth 1/ 1    62  0
Eth 1/ 1    63  0
Console#
```

関連するコマンド

map ip dscp（Global Configuration）（P705）

map ip dscp（Interface Configuration）（P706）

4.21 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	P710
match	クラス分類のためトラフィックに使う条件を定義	CM	P711
rename	クラスマップの名前を再定義	CM	P712
description	クラスマップの説明を指定	CM	P712
policy-map	ポリシーマップを作成	GC	P713
class	ポリシー上で実行するクラスを設定	PM	P714
rename	クラスマップの名前を再定義	PM	P712
description	クラスマップの記述を指定	PM	P712
set	IP パケットに適用する CoS、DSCP、IP Precedence の値を設定	PM-C	P715
police	クラス分けされたトラフィックに制限を設定	PM-C	P716
service-policy	ポリシーマップをインターフェースに適用	IC	P717
show class-map	クラスマップの情報を表示	PE	P718
show policy-map	ポリシーマップの情報を表示	PE	P719
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	P720

指定された入力トラフィックのカテゴリのサービスポリシーを作成するには、以下の手順に従ってください。

（1）"Class-map" コマンドを使用して、指定したトラフィックのカテゴリにクラス名を指定し、クラスマップ設定モードへ移行します。

（2）"match" コマンドを使用し、アクセスリスト・DSCP・IP Precedence 値または VLAN をベースに、指定したトラフィックのタイプを選択します。

（3）ACL を "match" コマンドでで指定された基準のフィルタリングを有効にするように設定します。

（4）"Policy-map" コマンドを使用して、入力トラフィックが処理される指定したマナーのポリシー名を指名し、ポリシーマップ設定モードへ移行します。

（5）"class" コマンドを使用し、クラスマップを識別してポリシーマップクラス設定モードへ移行します。ポリシーマップは複数のクラスステートメントを含むことが出来ます。

（6）"set" コマンドを使用し、マッチングトラフィッククラスの QoS 値を編集し、"policer" コマンドを使用してフローおよびバーストレートの平均流をモニタします。
指定したレートを超えるトラフィックは破棄、もしくは指定したレートを超えたトラフィックの DSCP サービスレベルを下げます。

（7）"service-policy" コマンドを使用して、ポリシーマップを指定のインタフェースへ割り当てます。

[注意] クラスマップにたいし、最大 16 ルールの設定が可能です。また、一つのポリシーマップには複数のクラスを含むことが出来ます。

[注意] ポリシーマップ（P713）を作成する前に、クラスマップ （P710）を作成してください。ポリシーマップ設定モードに移行した後では、"class" コマンド（P714）を使用してクラスマップを指定することは出来ません。

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 ip dscp 3
Console(config-cmap)#
```

関連するコマンド

show class map（P718）

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。
no **を付けると基準を削除します。**

文法

match { access-list *acl-name* | ip dscp *dscp* | ip precedence *ip-precedence* | vlan *vlan* }

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**）
- *dscp* ― DSCP **値**（**範囲**：0-63）
- *ip-precedence* ― IP Precedence **値**（**範囲**：0-7）
- *vlan* ― VLAN（**範囲**：1-4094）

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 ip dscp 3
Console(config-cmap)#
```

rename

クラスマップまたはポリシーマップの名前を再定義します。

文法

rename *map-name*

map-name ― **クラスマップまたはポリシーマップの名前（範囲：**1-16 **文字）**

コマンドモード

Class Map Configuration

Policy Map Configuration

例

```
Console(config)#class-map rd-class#1
Console(config-cmap)#rename rd-class#9
Console(config-cmap)#
```

description

クラスマップまたはポリシーマップの説明を入力します。

文法

description *string*

string ― **クラスマップまたはポリシーマップの説明（範囲：**1-64 **文字）**

コマンドモード

Class Map Configuration

Policy Map Configuration

例

```
Console(config)#class-map rd-class#1
Console(config-cmap)#description matches packets marked for DSCP service
  value 3
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 ―コマンドは受信した IP パケットをクラス分けします。
  - police ―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 **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 | set } }

no police *rate-kbps burst-byte* { exceed-action { drop | set } }

- *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)
- 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。**
- set ― DSCP **サービスを指定した値に設定（**0-63）

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 { *policy-map-name* class *class-map-name*}

- *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*

  ー ethernet *unit/port*

  unit ― **ユニット番号** ”1”

  port ― **ポート番号（範囲：**1-52）

  ー port-channel *channel-id*（**範囲：**1-8）

コマンドモード

Privileged Exec

例

```
Console#show policy-map interface ethernet 1/5
Service-policy rd_policy input
Console#
```

4.22 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	P721
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	P728
Static Multicast Routing	静的マルチキャストルータポートの設定	P732
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	P734
Multicast VLAN Registration	MVR の設定	P744

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	P722
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	P723
ip igmp snooping version	Snooping の IGMP バージョンの設定	GC	P724
ip igmp snooping leave-proxy	leave-proxy の有効化	GC	P725
ip igmp snooping immediate-leave	immediate-leave の有効化	IC	P725
show ip igmp snooping	IGMP snooping の設定の表示	PE	P726
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	P727

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*

  ー ethernet *unit/port*

  unit ― **ユニット番号** ”1”

  port ― **ポート番号（範囲：**1-52）

  ー port-channel *channel-id*（**範囲：**1-8）

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

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、P249 「IGMP Snooping とクエリパラメータの設定」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：1-4092)
- 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	P728
ip igmp snooping query-count	クエリーカウントの設定	GC	P729
ip igmp snooping query-interval	クエリー間隔の設定	GC	P730
ip igmp snooping query-maxrsponse-time	レポート遅延の設定	GC	P730
ip igmp snooping rouoter-port-expire-time	クエリータイムアウトの設定	GC	P731

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（P730）

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-expire-time

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/v3 **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（P724）

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	P732
show ip igmp snooping mrouter	マルチキャストルータポートの表示	PE	P733

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：**1-52）
  - port-channel *channel-id*（**範囲：**1-8）

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	P734
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	P735
permit, deny	プロファイルアクセスモードを設定	IPC	P736
range	プロファイルのマルチキャストアドレスを設定	IPC	P737
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	P738
ip igmp max-groups	IGMP スロットリング番号を指定	IC	P739
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	P740
show ip igmp filter	IGMP フィルタリングステータスを表示	PE	P741
show ip igmp profile	IGMP プロファイルおよび設定の表示	PE	P742
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	P743

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：**0-64**）**

初期設定

64

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 ー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 ー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：**1-52）
  - port-channel *channel-id*（**範囲：**1-8）

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*

  ー ethernet *unit/port*

  unit ― ユニット番号 ”1”

  port ― ポート番号（範囲：1-52）

  ー port-channel *channel-id*（範囲：1-8）

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##
```

4.22.5 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	P745
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	P746
mvr immediate	即時離脱機能を有効化	IC	P748
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	P749

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* }
receiver-group *ip-address* | receiver-vlan *vlan-id*]

no mvr { group *ip-address* { count } | vlan receiver-group *ip-address* | receiver-vlan *vlan-id* }

- *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：1-4094）
- receiver-group― レシーバ VLAN を通して管理されるグループを指定
- receiver-vlan ― マルチキャストトラフィックが、タグ付きフレームで MVR VLAN のアイデンティティを明らかにしないで指定されたレシーバ VLAN からの転送を可能

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* | static-receiver-group *ip-address*]

no mvr [type | immediate | group *ip-address* | static-receiver-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。

- 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)#
```

mvr immediate

このコマンドは、グループの Leave メッセージ受信した後、直ちにインタフェースをマルチキャストストリームから取り除くように設定します。"no" を前につけることで設定を初期値に戻します。

文法

mvr immediate

no mvr immediate

初期設定

無効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- このオプションは MVR レシーバ (746 ページの「mvr (Interface Configuration)」を参照) として設定されたインタフェースにのみ適用できます。
- Immediate leave はレシーバポートにのみ適用可能です。
  有効時、レシーバポートは leave メッセージで確認されたマルチキャストグループから直ちに取り除かれます。
  無効時、スイッチはグループに指定されたクエリをレシーバポートに送信することによって標準ルールに従い、ポートをグループリストから取り除く前に、マルチキャストグループに残っている加入者の有無を決定するために返答を待ちます。
- Immediate leave は全ての MVR ドメインに適用されます。

例

レシーバポートで Immediate leave を有効にしています。

```
Console(config)#interface ethernet 1/5
Console(config-if)#mvr immediate
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：1-52）
  - port-channel *channel-id*（範囲：1-8）
- *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#
```

項目	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
MVR Receiver VLAN	MVR VLAN のアイデンティティを明らかにしないタグ付きフレームの、マルチキャストトラフィック転送に使用される VLAN
MVR Supported Receiver Multicast Groups	レシーバ VLAN を通して管理されるマルチキャストグループの数
MVR Used Receiver Multicast Groups	レシーバ VLAN で現在アクティブなマルチキャストグループの数

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#
```

項目	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#
```

項目	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。**
Receiver VLAN	MVR VLAN **のアイデンティティを明らかにしないタグ付きフレームの、マルチキャストトラフィック転送に使用される** VLAN
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。**

4.23 DNS（Domain Name Server)

本コマンドは DNS(Domain Naming System) **サービスの設定を行ないます。ドメイン名と** IP **アドレスのマッピングを行なう** DNS **テーブルの手動での設定を行なえる他、デフォルトドメイン名の設定又はアドレス変換を行なうための複数のネームサーバの指定を行なうことができます。**

DNS **は** "ip name-server" **コマンドを使用し最低** 1 **つのネームサーバを指定しなければ有効にすることはできません。また、ドメインルックアップは** " ip domain-lookup" **コマンドにより有効にします**

コマンド	機能	モード	ページ
ip host	**静的ホスト名－アドレスマッピング**	GC	P752
clear host	**ホスト名－アドレステーブルからのエントリの削除**	PE	P753
ip domain-name	**不完全なホスト用のデフォルトドメイン名の設定**	GC	P754
ip domain-list	**不完全なホスト用のデフォルトドメイン名リストの設定**	GC	P755
ip name-server	**ホスト名－アドレス変換のための** 1 **つ又は複数のネームサーバの指定**	GC	P756
ip domain-lookup	DNS **によるホスト名－アドレス変換の有効化**	GC	P757
show hosts	**静的ホスト名－アドレスマッピングテーブルの表示**	PE	P758
show dns	DNS **サービスの設定の表示**	PE	P758
show dns cache	DNS **キャッシュのエントリの表示**	PE	P759
clear dns cache	DNS **キャッシュのエントリのクリア**	PE	P759

ip host

DNS テーブルのホスト名と IP アドレスのマッピングの静的設定を行ないます。"no" を前に置くことでエントリを削除します。

文法

ip host *name address1* [*address2* … *address8*]

no ip host *name address1* [*address2* … *address8*]

- *name* — ホスト名（設定範囲：1-64 文字）
- *address1* — 関連する IP アドレス
- *address2* … *address8* — 関連する IP アドレス（追加分）

初期設定

静的エントリなし

コマンドモード

Global Configuration

コマンド解説

サーバや他のネットワーク機器は複数の IP アドレスによる複数接続をサポートしています。2 つ以上の IP アドレスを静的テーブルやネームサーバからの応答によりホスト名と関連付けする場合、DNS クライアントは接続が確立するまで各アドレスに接続を試みます。

例

2 つのアドレスをホスト名にマッピングしています。

```
Console(config)#ip host rd5 192.168.1.55 10.1.0.55
Console(config)#end
Console#show hosts

Hostname
  rd5
Inet address
  10.1.0.55 192.168.1.55
Alias
Console#
```

clear host

DNS テーブルのエントリを削除します。

文法

clear host {*name* | *}

- *name* ― ホスト名（設定範囲：1-64 文字）
- * ― すべてのエントリを削除

初期設定

なし

コマンドモード

Privileged Exec

例

本例ではすべての DNS テーブルのエントリを削除しています。

```
Console#clear host *
Console#
```

ip domain-name

不完全なホスト名に追加するデフォルトドメイン名を設定します。

"no" **を前に置くことでドメイン名を削除します。**

文法

ip domain-name *name*

no ip domain-name

- *name* ― **ホスト名。ドメイン名とホスト名の間のドット** (.) **は入力しないで下さい（設定範囲：**1-64 **文字）**

例

```
Console(config)#ip domain-name sample.com
Console(config)#end
Console#show dns
Domain Lookup Status:
    DNS disabled
Default Domain Name:
    .sample.com
Domain Name List:
Name Server List:
Console#
```

関連するコマンド

ip domain-list（P755）
ip name-server（P756）
ip domain-lookup（P757）

ip domain-list

このコマンドは、不完全なホスト名に追加するドメイン名のリストを設定します。"no" を前に置くことでリストからドメイン名を削除します。

文法

ip domain-list *name*

no ip domain-list *name*

- *name* ― ホスト名。ドメイン名とホスト名の間のドット (.) は入力しないで下さい（設定範囲：1-64 文字）

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- ドメイン名はリストの最後に追加されます。
- 本機の DNS サーバが不完全なホスト名を受信し、ドメイン名リストが指定された場合、本機は追加するリスト内の各ドメイン名をホスト名に加え、一致する特定のネームサーバを確認して、ドメインリストにより動作します。
- ドメインリストがない場合、デフォルトドメイン名が使用されます。ドメインリストがある場合には、デフォルトドメイン名は使用されません。

例

本例では、現在のリストに 2 つのドメイン名を追加し、その後リストを表示しています。

```
Console(config)#ip domain-list sample.com.jp
Console(config)#ip domain-list sample.com.uk
Console(config)#end
Console#show dns
Domain Lookup Status:
   DNS disabled
Default Domain Name:
   .sample.com
Domain Name List:
   .sample.com.jp
   .sample.com.uk
Name Server List:
Console#
```

関連するコマンド

ip domain-name（P754）

ip name-server

ドメイン名解決のために 1 **つ又は複数のドメインネームサーバのアドレスを指定します。**
"no" **を前に置くことでリストからネームサーバを削除します。**

文法

ip name-server *server-address1* [*server-address2* … *server-address6*]

no ip name-server *server-address1* [*server-address2* … *server-address6*]

- *server-address1* — **ドメインネームサーバの** IP **アドレス**
- *server-address2* … *server-address6* — **ドメインネームサーバの** IP **アドレス（追加分）**

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

応答を受信するまで、又はリストの最後に到達するまで、リスト内のネームサーバに対して順番にリクエストを送信します。

例

応答を受信するまで、又はリストの最後に到達するまで、リスト内のネームサーバに対して順番にリクエストを送信します。

```
Console(config)#ip domain-server 192.168.1.55 10.1.0.55
Console(config)#end
Console#show dns
Domain Lookup Status:
   DNS disabled
Default Domain Name:
   .sample.com
Domain Name List:
   .sample.com.jp
   .sample.com.uk
Name Server List:
192.168.1.55
10.1.0.55
Console#
```

関連するコマンド

ip domain-name（P754）

ip domain-lookup（P757）

ip domain-lookup

DNS ホスト名・アドレス変換を有効にします。"no" を前に置くことで DNS を無効にします。

文法

ip domain-lookup

no ip domain-lookup

初期設定

無効

コマンドモード

Global Configuration

コマンド解説

- DNS を有効にする前に最低 1 つのネームサーバを指定する必要があります。
- すべてのネームサーバが削除された場合には DNS は自動的に無効になります。

例

本例では、DNS を有効にし、設定を表示しています。

```
Console(config)#ip domain-lookup
Console(config)#end
Console#show dns
Domain Lookup Status:
    DNS enabled
Default Domain Name:
    .sample.com
Domain Name List:
    .sample.com.jp
    .sample.com.uk
Name Server List:
    192.168.1.55
    10.1.0.55
Console#
```

関連するコマンド

ip domain-name（P754）

ip name-server（P756）

show hosts

静的ホスト名ーアドレスマッピングテーブルを表示します。

コマンドモード

Privileged Exec

例

以前に設定されたエントリと同じアドレスがマッピングされた場合、ホスト名はエイリアスとして表示されます。

```
Console#show hosts

Hostname
  rd5
Inet address
  10.1.0.55 192.168.1.55
Alias
  1.rd6
Console#
```

show dns

DNS サーバの設定を表示します。

コマンドモード

Privileged Exec

例

```
Console#show dns
Domain Lookup Status:
    DNS enabled
Default Domain Name:
    sample.com
Domain Name List:
    sample.com.jp
    sample.com.uk
Name Server List:
    192.168.1.55
    10.1.0.55
Console#
```

show dns cache

DNS キャッシュの内容を表示します。

コマンドモード

Privileged Exec

例

```
Console#show dns cache
NO   FLAG TYPE    DOMAIN                              TTL  IP
0    4    Address www.times.com                       198  199.239.136.200
1    4    Address a1116.x.akamai.net                  19   61.213.189.120
2    4    Address a1116.x.akamai.net                  19   61.213.189.104
3    4    CNAME   graphics8.nytimes.com               19   POINTER TO:2
4    4    CNAME   graphics478.nytimes.com.edgesui 19   POINTER TO:2
Console#
```

項目	解説
NO	各リソースレコードのエントリ番号
FLAG	キャッシュエントリのフラグは常に "4"
TYPE	標準的又はプライマリ名が指定された「CNAME」、既存のエントリと同じ IP アドレスをマッピングされている多数のドメイン名が指定された「ALIAS」
IP	レコードに関連した IP アドレス
TTL	ネームサーバにより報告された生存可能時間
DOMAIN	レコードに関連するドメイン名

clear dns cache

DNS キャッシュのすべての値をクリアします。

コマンドモード

Privileged Exec

例

```
Console#clear dns cache
Console#show dns cache
NO      FLAG      TYPE     IP     TTL     DOMAIN
Console#
```

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	P760
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	P762
ip dhcp restart	BOOTP/DHCP クライアントリクエストの送信	PE	P763
show ip interface	本機の IP 設定の表示	PE	P764
show ip redirects	本機のデフォルトゲートウェイ設定の表示	PE	P764
show arp	ARP キャッシュを表示	PE	P764
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	P766

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（P763）

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（P764）

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 （P760）

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 （P764）

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 （P762）

show arp

ARP キャッシュを表示します。

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

- 本コマンドは対応する IP アドレス、MAC アドレス、タイプ（動的または other）、VLAN インタフェースを含む、ARP キャッシュについての情報を表示します。
  エントリタイプ "other" は本機のローカルアドレスを示します。

例

```
Console#show arp

IP Address       MAC Address             Type     Interface
---------------- -----------------   --------- -----------
192.168.0.1     00-01-ec-f8-d8-c6    dynamic             1
192.168.0.2     00-12-cf-12-34-56    other               1
192.168.0.3     00-10-b5-62-03-74    dynamic             1

Total entry : 3
Console#
```

関連するコマンド

ip default-gateway （P762）

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* {size *size* } { count *count* }

- *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（P537）

FXC3152A Management Guide
（FXC09-DC-200014-R1.0）

初版　　2010 **年** 1 **月**

Management Guide
FXC3152A
Management Guide
FXC3152A
Management Guide
FXC3152A
Management Guide
FXC3152A
Management Guide
FXC3152A
Management Guide
FXC3152A
Management Guide
FXC3152A
Management Guide
FXC3152A
Management Guide
FXC3152A
Management Guide
FXC3152A
Management Guide
FXC3152A
Management Guide
FXC3152A
Management Guide
FXC3152A
Management Guide
FXC3152A
Management Guide

FXC株式会社