Future X Communications

FXC3116
FXC3126
FXC3152

マネージメントガイド

改版履歴

版名	作成日	内容	備考
第1.0版	2006/09	作成	
第1.1版	2007/09	誤記訂正	
第1.2版	2009/06	制限事項を追記	

改版履歴

このページは構成の都合上、空白となっています。

目次

1 イントロダクション

2 本機の管理

3 Webインタフェース

付録

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 **SNMP** (FXC3116)または**SNMP v1/2c** (FXC3126/FXC3152) — コミュニティ名 **Port** — IEEE802.1X認証, MACアドレスフィルタリング
Access Control Lists	最大88IP/MAC ACLサポート
DHCP Client	サポート
DNS Server	サポート
Port Configuration	スピード、通信方式、フローコントロール
Rate Limiting	入力及び出力帯域制御
Port Mirroring	1つの分析ポートに対する単一ポートのミラーリング
Port Trunking	Static及びLACPによる最大4トランク
Broadcast Storm Control	サポート
Static Address	最大登録可能MACアドレス数 8K
IEEE 802.1D 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)
Virtual LANs	IEEE802.1Qタグ付VLAN/ポートベースVLAN/プライベートVLAN（最大256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、 IP Precedence/DSCP、TCP/UDPポート
Multicast Filtering	IGMP snooping, query

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/Configuration Backup and Restore

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ID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、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、TCPコントロールコードによる）IPフレーム又は（MACアドレス、イーサネットタイプによる）すべてのフレームへのパケット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送信及び受信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4グループのトランクをサポートしています。

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

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

静的アドレス/Static Addresses

特定のポートに対して静的なMACアドレスの設定を行うことができます。設定されたMACアドレスはポートに対して固定され、他のポートに移動することはできません。設定されたMACアドレスの機器が他のポートに接続された場合、MACアドレスは無視され、アドレステーブル上に学習されません。
静的MACアドレスの設定を行うことにより、指定のポートに接続される機器を制限し、ネットワークのセキュリティを提供します。

IEEE802.1Dブリッジ/IEEE 802.1D Bridge

本機ではIEEE802.1Dブリッジ機能をサポートします。
MACアドレステーブル上でMACアドレスの学習を行い、その情報に基づきパケットの転送を行います。本機では最大8K個のMACアドレスの登録を行うことが可能です。

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

本機ではスイッチング方式としてストア＆フォワードをサポートします。
本機では500KB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

本機は次のスパニングツリープロトコルをサポートしています。

- 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ループ検出や修復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（3～5 秒）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。

VLAN/Virtual LANs

本機は最大256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あるいはTCP/UDPポート番号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。

1-3 初期設定

本機の初期設定は設定ファイル"Factory_Default_Config.cfg"に保存されています。本機を初期設定にリセットするためには、"Factory_Default_Config.cfg"を起動設定ファイルとします。
詳細はP3-17「設定情報ファイルの保存・復元」を参照して下さい。

基本的な設定項目の初期設定は以下の表の通りです:

機能	パラメータ	初期設定
Console Port Connection	Baud Rate	9600
	Data bits	8
	Stop bits	1
	Parity	none
	Local Console Timeout	0 (disabled)
Authentication	Privileged Exec Level	Username “admin” Password “admin”
	Normal Exec Level	Username “guest” Password “guest”
	Enable Privileged Exec from Normal Exec Level	Password “super”
	RADIUS Authentication	Disabled
	TACACS Authentication	Disabled
	802.1X Port Authentication	Disabled
	HTTPS	Enabled
	SSH	Disabled
	Port Security	Disabled
	IP Filtering	Disabled
Web Management	HTTP Server	Enabled
	HTTP Port Number	80
	HTTP Secure Server	Enabled
	HTTP Secure Port Number	443

SNMP	Community Strings	“public” (read only) “private” (read/write)
	Traps	Authentication traps: enabled Link-up-down events: Enabled
Port Configuration	Admin Status	Enabled
	Auto-negotiation	Enabled
	Flow Control	Disabled
	Port Capability	100BASE-TX – 10 Mbps half duplex 10 Mbps full duplex 100 Mbps half duplex 100 Mbps full duplex Full-duplex flow control disabled Symmetric flow control disabled
	Module Port Capability	100BASE -FX – 100 Mbps full duplex Full duplex flow control disabled Symmetric flow control disabled 1000BASE-T/SX/LX/LH– 1000 Mbps full duplex Full-duplex flow control disabled Symmetric flow control disabled
Rate Limiting	Input and output limits	Disabled
Port Trunking	Static Trunks	None
	LACP (all ports)	Disabled
Broadcast Storm Protection	Status	Enabled (all ports, FXC3116) Disabled (all ports, FXC3126/52)
	Broadcast Limit Rate	32,000 packets per second

Spanning Tree Algorithm	Status	Enabled, RSTP (Defaults: All values based on IEEE 802.1s)
	Fast Forwarding (Edge Port)	Disabled
Address Table	Aging Time	300 seconds
Virtual LANs	Default VLAN	1
	PVID	1
	Acceptable Frame Type	All
	Ingress Filtering	Disabled
	Switchport Mode (Egress Mode)	Hybrid: tagged/untagged frames
	GVRP (global)	Disabled
	GVRP (port interface)	Disabled
Traffic Prioritization	Ingress Port Priority	0
	Weighted Round Robin	Queue: 0 1 2 3 Priority: 1 2 4 6
	IP Precedence Priority	Disabled
	IP DSCP Priority	Disabled
	IP Port Priority	Disabled
IP Settings	IP Address	0.0.0.0
	Subnet Mask	255.0.0.0
	Default Gateway	0.0.0.0
	DHCP	Client: Enabled
	BOOTP	Disabled
DNS Server	Lookup	Disabled
Multicast Filtering	IGMP Snooping	Snooping: Enabled Querier: Enabled
System Log	Status	Enabled
	Messages Logged Levels	0-7 (all, FXC3116) 0-6 (FXC3126/52)
	Messages Logged to Flash Levels	0-6 (FXC3116) 0-3 (FXC3126/52)
SMTP Email Alerts (FXC3126/52)	Event Handler	Enabled (but no server defined)
SNTP	Clock Synchronization	Disabled

2-1　本機への接続

設定方法

FXC3116/FXC3126/FXC3152は、ネットワーク管理エージェントを搭載しSNMP、RMON（グループ1、2、3、9）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えます。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　**初期設定では、本機のIPアドレスはDHCP経由で設定します。IPアドレスの設定を行うにはP2-5「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、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。

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(最大 16 ユーザ)
- 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
- IEEE802.1X に準拠した及び静的アドレスフィルタリングを使用したポートアクセスコントロール
- Access Control Lists (ACL)パケットフィルタリング
- IEEE802.1Q 準拠のタグ付 VLAN (最大 256 グループ)
- GVRP 有効
- IGMP マルチキャストフィルタリング設定

- TFTP 経由のファームウェアのアップロード及びダウンロード
- TFTP 経由の設定情報のアップロード及びダウンロード
- スパニングツリーの設定
- Class of Service (CoS)の設定
- 静的トランク及び LACP 設定（最大 4 グループ）
- 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
- 同一の IP アドレスを用いたスタック機器の設定（FXC3126/52）

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下さい:

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）
エミュレーション -- VT100
通信速度 ---------- 9600ボー(baud)
データビット -------- 8bit
パリティ ---------- なし
ストップビット ----- 1bit
フロー制御 ---------- なし

注意 ハイパーターミナルを使用する場合、**"ファンクションキー、方向キー、Ctrlキーの使い方"**で**"Windowsキー"**ではなく**"ターミナルキー"**を選択して下さい。
Windows2000ではWindows2000 Service Pack2以上でハイパーターミナルのVT100エミュレーションのバグが修正されています。

Windows2000でハイパーターミナルを使用する場合、Service Pack2以上がインストールされていることを確認して下さい。

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P4-11「Line Commands」を参照して下さい。

CLIの使い方はP4-1「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P4-9「コマンドグループ」を参照して下さい。

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DHCP経由でIPアドレスを設定します。手動でIPアドレスの設定を行う場合や、DHCP、BOOTPを用いて自動的にIPアドレスの設定を行う場合の設定方法はP2-5「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/SSH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

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。

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下さい。

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 FXC3126 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)#
```

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。

注意 1つのVLANインタフェースにのみIPアドレスを設定することができます（初期設定ではVLAN1）。IPアドレスを設定したVLANが管理機能にアクセスできる唯一の管理VLANとなります。他のVLANに対してIPアドレスを設定した場合、元のIPアドレスは無効となり、新たにIPアドレスを設定したVLANが管理機能にアクセス可能な管理VLANとなります。

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 初期設定では、本機のIPアドレスはDHCPl経由で設定します。

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**"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 global configuration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 client
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.
```

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)#
```

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。保存された設定ファイルは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 P3-17「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う他、CLI、Web インタフェースを提供します。
  詳細に関しては P3-15「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)。このコードは、さらにコンソールポートを通ってシステムへのファームウェア・ファイル直接アップロードする機能を提供します。
  詳細に関しては、付-B「シリアルポート経由のファームウェアアップグレード」を参照して下さい。

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。

このページは構成の都合上、空白となっています。

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第４章「コマンドラインインタフェース」を参照して下さい。

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

Webインタフェースを使用する場合は、事前に下記の設定を行って下さい。

① コンソール接続、BOOTP又はDHCPプロトコルを使用して本機にIPアドレス、サブネットマスク、デフォルトゲートウェイを設定します（詳細はP3-13「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すべての設定変更が行えます。

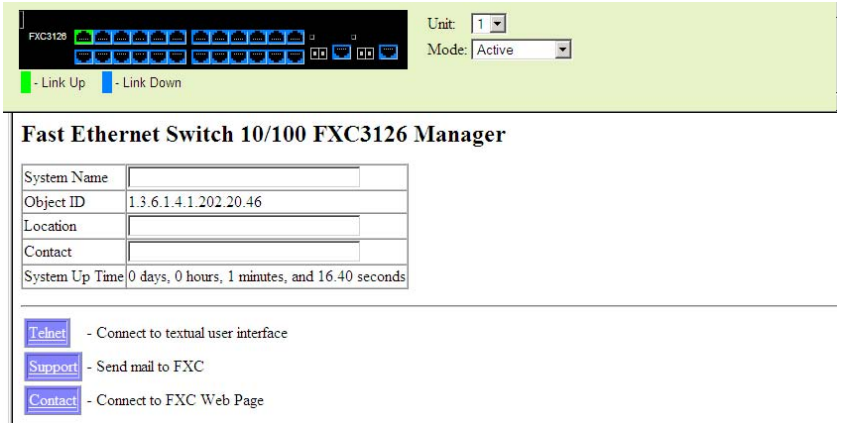
注意　管理用PCと本機の間でスパニングツリーアルゴリズム (STA)を使用しない場合、管理用PCに接続されたポートをファストフォワーディングにする（Admin Edge Portの有効化）ことにより、Webインタフェースからの設定に対する本機の応答速度を向上させることができます（詳細はP3-85「インタフェース設定」を参照して下さい）

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)ではすべ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。

ホームページ

Webインタフェースにアクセスした際、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。



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]又は[Apply Changes]ボタンをクリックして下さい。
次ページの表は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。

注意　本章内では、FXC3126を例に説明しています。ポート数以外に、FXC3116、FXC3126、FXC3152で大きな違いはありません。違いがある場合には、対応している機種を記載しています。

ボタン	動作
Revert	入力した値をキャンセルし、[Apply]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ヘルプを表示する

注意　ページ内容の更新を確実に行うためInternet Explorer 5.xでは、メニューから[ツール]→[インターネットオプション]→[全般]→[インターネット一時ファイル]を選択し、[設定で保存しているページの新しいバージョンの確認]の[ページを表示するごとに確認する]をチェックして下さい。

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

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P3-59「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。

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。次ページの表は、Webインタフェースで利用できる内容の一覧を示しています。

メニュー		解説	ページ
Port Security		セキュリティ侵害対応、登録MACアドレス数設定、ステータスなど各ポートのセキュリティ設定	3-42
802.1X		ポート認証	3-44
	Information	全体設定の表示	3-45
	Configuration	全体設定の設定	3-45
	Port Configuration	各ポートの認証モードの設定	3-46
	Statistics	指定ポートの統計情報の表示	3-47
ACL			*3-51*
	Configuration	IP及びMACアドレスベースのパケットフィルタリング設定	3-52
	Port Binding	ACLへのポートの登録	3-56
	IP Filter	Web、SNMP、Telnet経由での管理用クライアントのIPアドレスの設定	3-48
Port			*3-58*
Port Information		ポート接続状況の表示	3-58
Trunk Information		トランク接続状況の表示	3-58
Port Configuration		ポート接続設定	3-59
Trunk Configuration		トランク接続の設定	3-59
Trunk Membership		静的トランクに追加するポートの指定	3-61
LACP			3-62
	Configuration	ポートへの動的なトランクへの参加の許可	3-62
	Aggregation Port	リンクアグリゲーションメンバーのパラメータの設定	3-63
	Port Counters	LACPプロトコルメッセージ統計情報の表示	3-65
	Port Internal Information	ローカル側のオペレーション状態の設定及び表示	3-65
	Port Neighbors Information	リモート側のオペレーション状態の設定及び表示	3-67
Port Broadcast Control		各ポートのブロードキャストストームのしきい値の設定	3-68
Trunk Broadcast Control		各トランクのブロードキャストストームのしきい値の設定	3-68
Mirror Port Configuration		ミラーリングのソース及びターゲットポートの設定	3-69

メニュー		解説	ページ
VLAN			*3-88*
802.1Q VLAN			
	GVRP Status	GVRPの有効化	3-90
	Basic Information	本機でサポートしているVLANタイプの表示	3-91
	Current Table	各VLANの所属する現在のポートとタグのサポート状況の表示	3-91
	Static List	VLANグループの構成及び解除	3-92
	Static Table	既存VLANの設定変更	3-93
	Static Membership by port	インタフェースのメンバーシップタイプ設定	3-95
	Port Configuration	デフォルトPVIDとVLAN属性の設定	3-96
	Trunk Configuration	デフォルトトランクPVIDとVLAN属性の設定	3-96
Private VLAN			3-98
	Information	プライベートVLAN機能情報の表示	3-99
	Configuration	プライマリVLAN又はコミュニティVLANの作成/削除	3-100
	Association	各コミュニティVLANのプライマリVLANへの関連付け	3-100
	Port Information	VLANポートタイプ及び関連付けられたプライマリ/セカンダリVLANの表示	3-101
	Port Configuration	プライベートVLANインタフェースタイプの設定及びインタフェースのプライベートVLANとの関連付け	3-102
	Trunk Information	VLANポートタイプ及び関連付けられたプライマリ/セカンダリVLANの表示	3-101
	Trunk Configuration	プライベートVLANインタフェースタイプの設定及びインタフェースのプライベートVLANとの関連付け	3-102

メニュー	解説	ページ
Priority		*3-104*
Default Port Priority	各ポートのデフォルトプライオリティの設定	3-104
Default Trunk Priority	各トランクのデフォルトプライオリティの設定	3-104
Traffic Classes	出力キューのIEEE802.1pプライオリティタグのマッピング	3-105
Traffic Classes Status	トラフィッククラスプライオリティの有効/無効（本機には搭載されていません）	NA
Queue Mode	キューモードの設定（Strict/WRR）	3-106
Queue Scheduling	重み付けラウンドロビンキューの設定	3-107
IP Precedence/ DSCP Priority Status	IP Precedence又はDSCPプライオリティの選択、または両方の無効化	3-108
IP Precedence Priority	IP ToSのCoS値へのマッピング設定	3-109
IP DSCP Priority	IP DSCPのCoS値へのマッピング設定	3-110
IP Port Priority Status	IPポートプライオリティ全体の有効/無効	3-111
IP Port Priority	TCP/UDPポートプライオリティ、ソケット番号、CoS値の設定	3-111
ACL CoS Priority	ACLルールに一致するフレームのアウトプットキューとCoS値の変更	3-112
IGMP Snooping		*3-113*
IGMP Configuration	マルチキャストフィルタリングの有効化、マルチキャストクエリのパラメータの設定	3-114
Multicast Router Port Information	各VLAN IDの隣接したマルチキャストルータ又はスイッチに接続されたポートを表示	3-115
Static Multicast Router Port Configuration	隣接したマルチキャストルータ又はスイッチに接続したポートの割り当て	3-116
IP Multicast Registration Table	マルチキャストIPアドレスとVLAN IDを含む本機で使用中のすべてのマルチキャストグループの表示	3-117
IGMP Member Port Table	選択されたVLANに関連したマルチキャストアドレス	3-118

3-3　基本設定

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

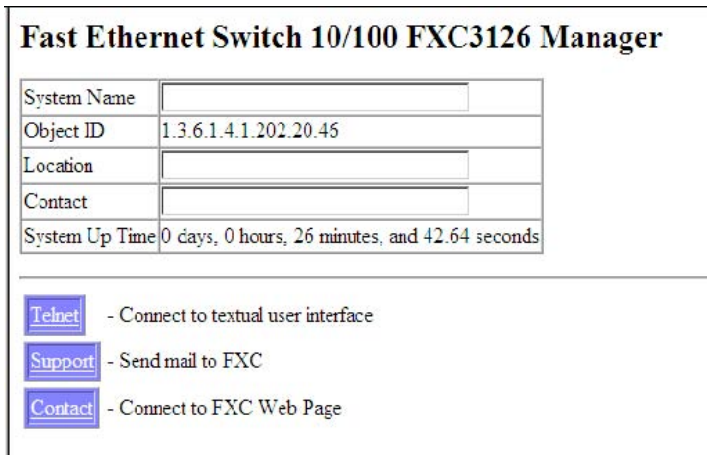
管理者のコンタクト情報

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）



ハードウェア及びソフトウェアバージョンの表示

Switch Information pageを利用し、ハードウェア及びソフトウェアのバージョンや電源ステータスを確認することができます。

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

Internal Power Status

内蔵電源のステータス

[Management Software](管理ソフトウェア)

Loader Version

Loader Codeのバージョン

Boot-ROM Version

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

Operation Code Version

runtime codeのバージョン

Role

Master/Slaveのどちらで動作しているかを表しています

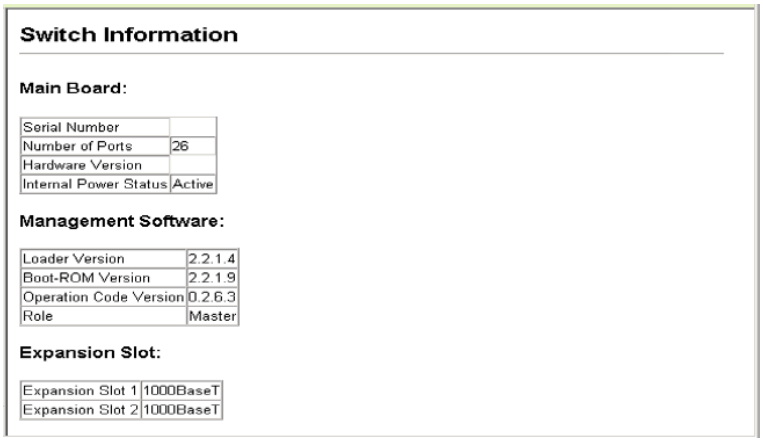
[Expansion Slot](拡張スロット)

Expansion Slot 1/2

拡張スロットの状態(RJ-45, SFP)

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	
Number of Ports	26
Hardware Version	
Internal Power Status	Active

Management Software:

Loader Version	2.2.1.4
Boot-ROM Version	2.2.1.9
Operation Code Version	0.2.6.3
Role	Master

Expansion Slot:

Expansion Slot 1	1000BaseT
Expansion Slot 2	1000BaseT

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、P3-104「Class of Service設定」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われていることを表します（詳細は、P3-76「静的アドレスの設定」を参照して下さい）

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（P3-88「VLAN設定」を参照して下さい）

Local VLAN Capable

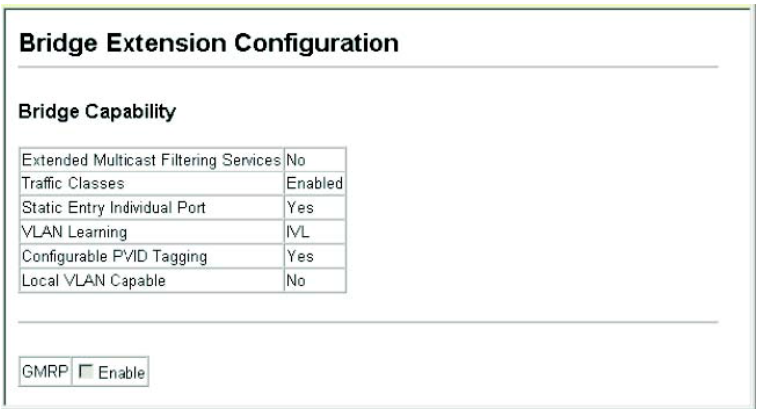
本機はIEEE 802.1Q規定外の複数のローカルブリッジ(複数のスパニングツリー)に対応していないことを表します。

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。



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DHCP経由で取得します。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:0.0.0.0、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(1-4096)。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。

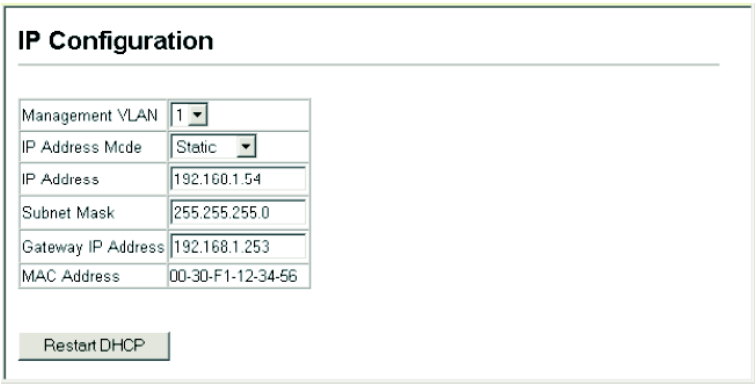
Restart DHCP

DHCPサーバからIPアドレスを再取得するようリクエストします。

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。



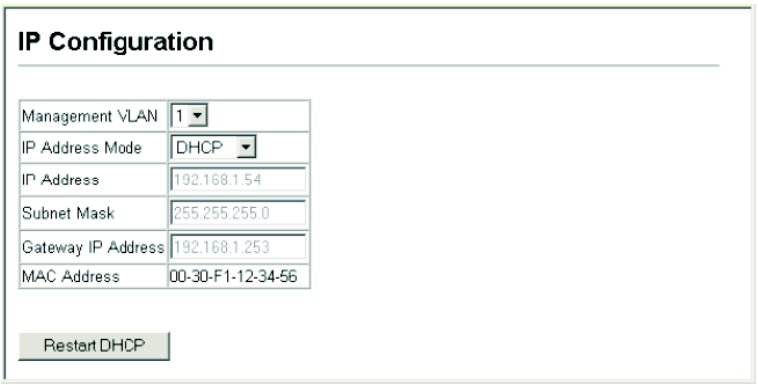
DHCP又はBOOTPによるIPアドレスの設定

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。

ファームウェアの管理

TFTPサーバを使用したファームウェアのダウンロード及びアップロードを行うことができます。TFTPサーバ上にruntime codeを保存することにより、後で本機の復元を行う際にダウンロードすることができます。また、以前のバージョンのファームウェアを上書きすることなく、新しいファームウェアを使用することができます。ファイルタイプ、ファイル名、ファイル転送方法を設定する必要があります。

設定・表示項目

File Transfer Method

ファームウェアコピーの操作方法。下記のオプションがあります。

－file to file ― 本機のディレクトリに新たなファイル名を付けて、ファームウェアをコピーします。

－file to tftp ― 本機からTFTPサーバへファイルをコピーします。

－tftp to file ― TFTPサーバから本機へファイルをコピーします。

TFTP Server IP Address

TFTPサーバのIPアドレス

File Type

ファームウェアコピーのためのopcode (オペレーションコード)

Destination 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, ".", "-", "_"）

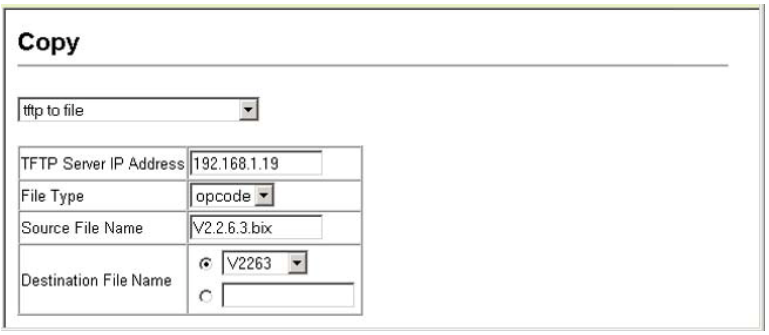
注意 runtimeファイルは最大2つまでしか保存できません。起動ファイルに指定されているファイルは削除することができません。

システムソフトウェアのダウンロード

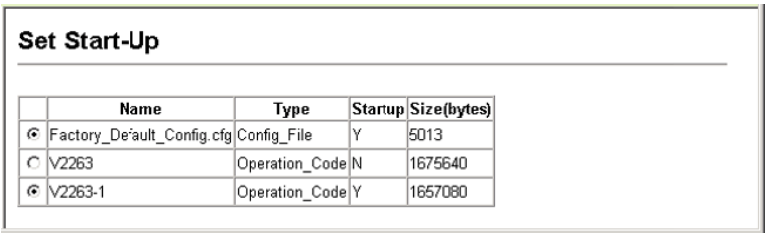
runtime codeをダウンロードする場合、現在のイメージと置き換えるために現在のファイルをDestination File Nameとして指定することができます。また、現在のruntime codeファイルと異なるファイル名を使用し本体にダウンロードし、その後ダウンロードしたファイルを起動ファイルに設定することもできます。

設定方法

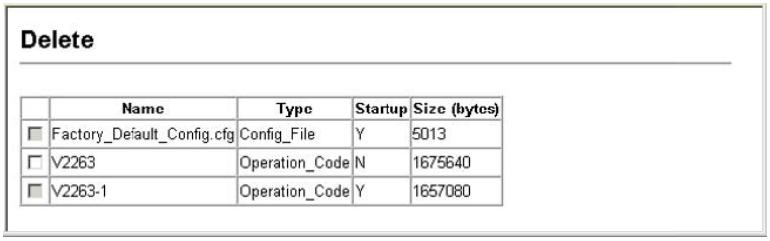
[System]→[File]→[Copy]をクリックします。tftp to file (転送方法)を選択し、TFTPサーバのIPアドレスを入力し、ファイルタイプをopcodeに設定します。Destination File Name（ダウンロード先のファイル名）で、本機内の既存のファイルを上書きする場合には既存ファイルを選択し、新しいファイルとして保存する場合にはファイル名を指定します。その後、[Apply]をクリックします。起動に使用しているファームウェアを変更し、新しいオペレーションコードを使用して起動するためには本機の再起動を行います。



現在のruntime code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オペレーションコードにする必要があります。[System]→[File]をクリックします。Set Start-Up画面で起動時に使用するオペレーションコードファイルを選択し、[Apply]をクリックします。新しいファームウェアを使用するためには本機の再起動を行います。



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



設定情報ファイルの保存・復元

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

設定・表示項目

File Transfer Method

設定情報ファイルコピーの操作方法。下記のオプションがあります。

－file to file ― 新たなファイル名を付けて本機のディレクトリへコピーします。

－file to running-config ― 本機のファイルを実行中の設定ファイルへコピーします。

－file to startup-config ― 本機のファイルを起動設定ファイルへコピーします。

－file to tftp ― 本機からTFTPサーバへファイルをコピーします。

－running-config to file ― 実行中の設定ファイルをコピーします。

－running-config to startup-config ― 実行中の設定ファイルを起動設定ファイルへコピーします。

－running-config to tftp ― 実行中の設定ファイルをTFTPサーバへコピーします。

－startup-config to file ― 起動設定ファイルを本機のファイルへコピーします。

－startup-config to running-config ― 起動設定ファイルを実行中の設定ファイルへコピーします。

－startup-config to tftp ― 起動設定ファイルをTFTPサーバへコピーします。

－tftp to file ― TFTPサーバから本機へファイルをコピーします。

－tftp to running-config ― TFTPサーバから実行中の設定ファイルへコピーします。

－tftp to startup-config ― TFTPサーバから起動設定ファイルへコピーします。

TFTP Server IP Address

TFTPサーバのIPアドレス

File Type

設定情報をコピーするためのconfig (設定ファイル)

Destination File Name

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

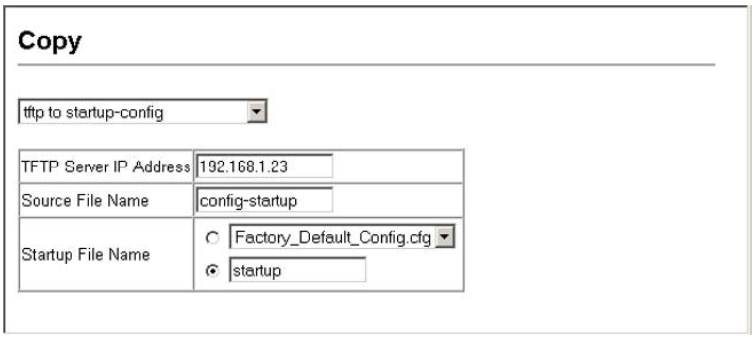
注意 **本機内に保存可能な設定ファイルの最大数はフラッシュメモリの容量に依存します。**

設定情報ファイルのダウンロード

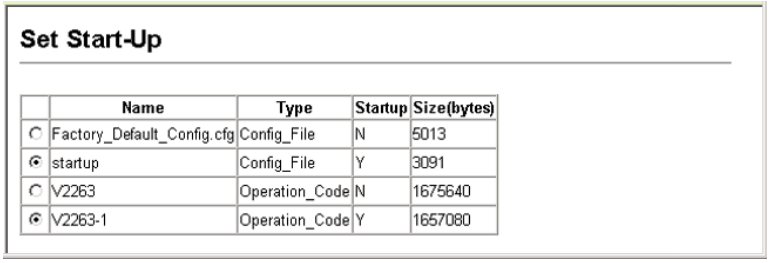
設定ファイルは新しいファイル名で保存し、起動ファイルとして設定できる他に、現在の起動設定ファイルを保存先に指定することで直接起動設定ファイルを置き換えることができます。
但し、"Factory_Default_Config.cfg"ファイルはTFTPサーバへコピーすることはできますが、設定ファイルをダウンロードする際に、ダウンロード先のファイル名として指定し、新しいファイルに置き換えることはできません。

設定方法

[System]→[File]→[Copy]をクリックします。"tftp to startup-config"又は"tftp to file"を選択し、TFTP Server IP Address（TFTPサーバのIPアドレス）とSource File Name（ダウンロードするファイル名）を入力します。Destination File Name（ダウンロード先のファイル名）で、本機内の既存のファイルを上書きする場合には既存ファイルを選択し、新しいファイルとして保存する場合にはファイル名を指定します。その後、[Apply]をクリックします。



"tftp to startup-config"又は"tftp to file"で新たなファイルのダウンロードを行った場合には、このファイルは自動的に起動設定ファイルに設定されます。新たな設定情報を反映する場合には、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。
[System]→[File]→[Set Start-Up]画面を使用し、設定ファイルを起動設定ファイルに選択できます。



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：0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

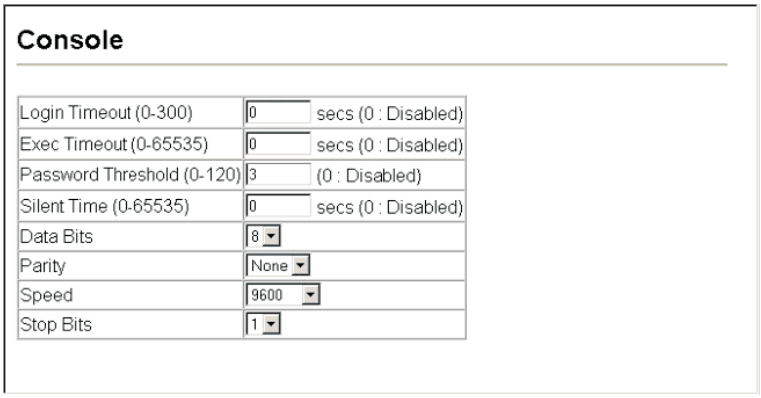
ターミナル接続の送信(ターミナルへの)/受信(ターミナルからの)ボーレート。シリアルポートに接続された機器でサポートされているボーレートを指定して下さい（範囲：9600、19200、38400、57600、115200 bps、初期設定：9600 bps）

Stop Bits

送信するストップビットの値（範囲：1-2、初期設定：1ストップビット）

設定方法

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



Telnetの設定

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

設定・表示項目

Telnet Status

本機へのTelnet接続の有効/無効（初期設定：有効）

Telnet Port Number

本機へTelnet接続する場合のTCPポート番号（初期設定：23）

Login Timeout

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

Exec Timeout

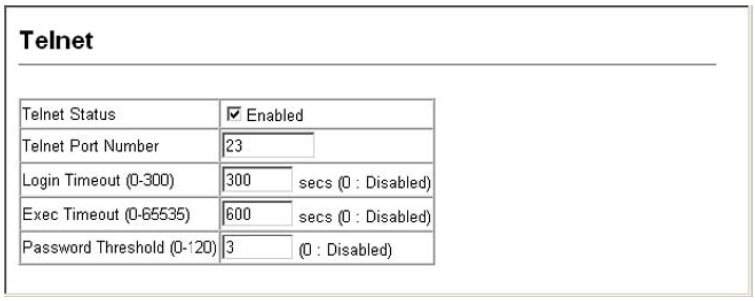
ユーザ入力のタイムアウト時間。設定時間内に入力が行われない場合、その接続は切断されます（範囲：0-65535秒、初期設定：600秒）

Password Threshold

ログイン時のパスワード入力のリトライ回数。
（範囲：0-120回、初期設定：3回）

設定方法

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



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
0	Emergency	システム不安定状態を示すメッセージ
1	Alert	迅速な対応が必要なメッセージ
2	Critical	重大な状態を示すエラーメッセージ
3	Error	エラー状態を示すメッセージ
4	Warning	警告メッセージ
5	Notice	重要なメッセージ

6	Informational	情報メッセージ
7	Debug	デバッグメッセージ

※ 現在のファームウェアではLevel 2, 5, 6のみサポートしています。

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RAM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"を指定し、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 Fasility

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：3（FXC3116）または6（FXC3126/52））

Host IP List

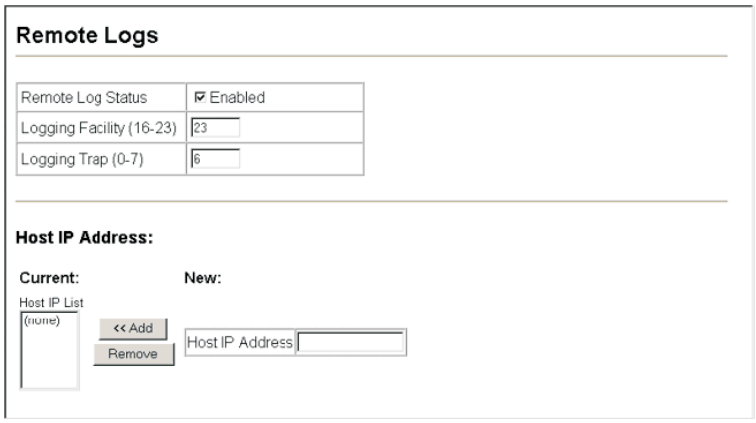
syslogメッセージを受け取るリモートsyslogサーバのIPアドレスのリストを表示します。Host IPアドレスの上限は5つです。

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。

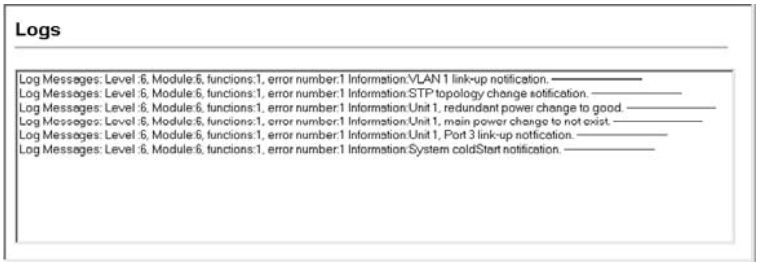


ログメッセージの表示

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アラートメッセージの送信（FXC3126/52）

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(P3-22の表を参照)。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（初期設定：7）

SMTP Server List

本機からのアラートメッセージを受信するSMTPサーバを3台まで指定できます。リストの最初のサーバが受信できない場合、リストされている他のサーバが接続を試みます。"New SMTP Server"に入力し、[Add]または[Remove]をクリックします。

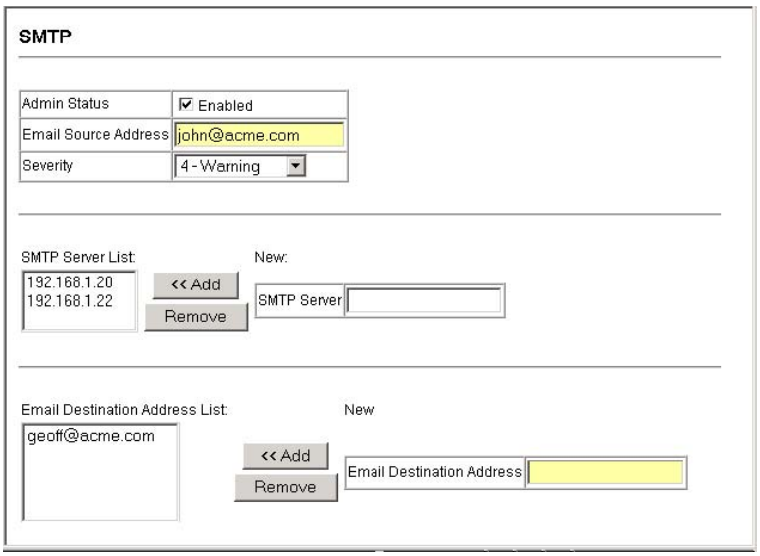
Email Destination Address Liet

アラートメッセージを受信する人。5人まで入力できます。"New Email Destination Address"に入力し、[Add]または[Remove]をクリックします。

設定方法

[System]→[Log]→[SMTP]をクリックします。送信元のメールアドレスを設定し、"Severity Level"を選択します。"SMTP Server List"に追加するサーバの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、"SMTP Server List"のエントリをクリックし、[Remove]

をクリックします。アラートメッセージの受信者は5人まで設定できます。その後、[Apply]をクリックします。



再起動

設定方法

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

注意　再起動時にはPower-On Self-Testが実行されます。

システムクロック設定

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

また、CLIから手動で時刻の設定を行うこともできます(詳細はP4-63「Calendar Set」を参照)

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

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

SNTP設定

本機では、特定のタイムサーバに対して時間の同期リクエストを送信します。

設定・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

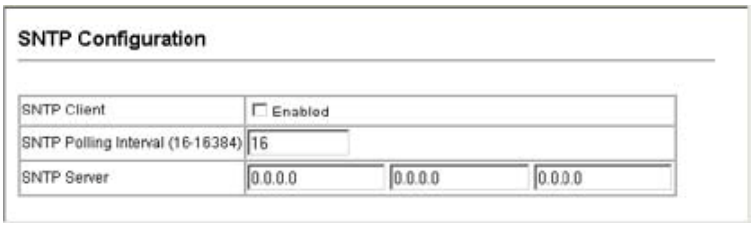
SNTPクライアントモード時のタイムサーバに対する時刻更新リクエストの送信間隔を設定します（範囲：16-16284秒、初期設定：16秒）

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。必要な項目を設定し[Apply]をクリックします。



タイムゾーンの設定

SNTPではUTC(Coordinated Universal Time:協定世界時間。別名：GMT/Greenwich Mean Time)を使用します。
本機を設置している現地時間に対応するためにUTCからの時差（タイムゾーン）の設定を行う必要があります。

設定・表示項目

Current Time

現在時刻の表示

Name

タイムゾーンに対する名称を設定します（範囲：1-29文字）

Hours (0-12)

UTCからの時間の差を設定します。

Minutes (0-59)

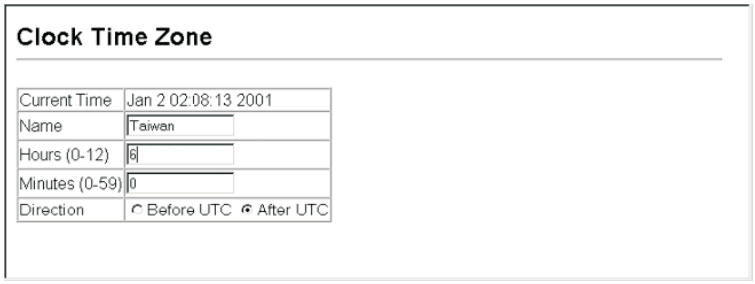
UTCからの時間（分数）の差を設定します。

Direction

UTCからのタイムゾーンの差がプラスかマイナスかを設定します。

設定方法

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



3-4 SNMP

Simple Network Management Protocol (SNMP)はネットワーク上の機器の管理用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できます。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。
コミュニティ名の設定及び、関連するトラップ機能、IPアドレスフィルタリングに関して、以下で解説しています。

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の設定:
－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。

トラップマネージャ・トラップタイプの指定

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

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

設定・表示項目

Trap Manager Capability

本機が最大5つのトラップマネージャをサポートしていることを表しています。

Current

登録されているトラップマネージャのリスト

Trap Manager IP Address

トラップを受信するホストのIPアドレス

Trap Manager Community String

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

Trap Version

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

Enable Authentication Traps

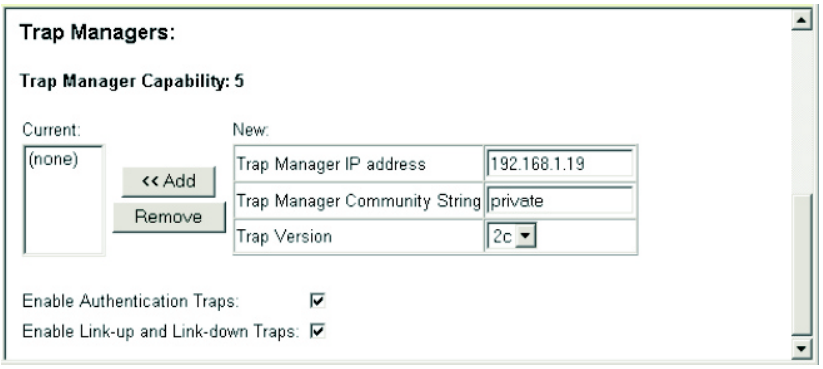
SNMP認証時に不正なコミュニティ名が送信された場合にトラップが発行されます（初期設定：enabled）

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：enabled）

設定方法

[SNMP]→[Configuration]をクリックします。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、[Add]をクリックします。トラップの種類(認証時、Link-up/down)に関し、必要な場合はチェックボックスで選択し、[Apply]をクリックします。



3-5 ユーザ認証

本機の管理アクセスへは以下の方法により制限を行えます。

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

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い、パスワードは安全な場所に保管して下さい。
初期設定では､ゲストモードのユーザ名･パスワードは共に｢guest｣、管理者モードのユーザ名・パスワードは「admin」です。
ユーザ名はCLIを使用した場合のみ利用、変更可能です。

設定・表示項目

Accout List

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

New Account

新たに追加するユーザアカウント情報

－**User Name** — ユーザ名(最大文字数：8文字、最大ユーザ数：16人)

－**Access Level** — ユーザのアクセスレベル(オプション:Normal, Privileged)

－**Password** ― ユーザのパスワード（範囲：0-8文字、大文字と小文字は区別されます）

Change Password

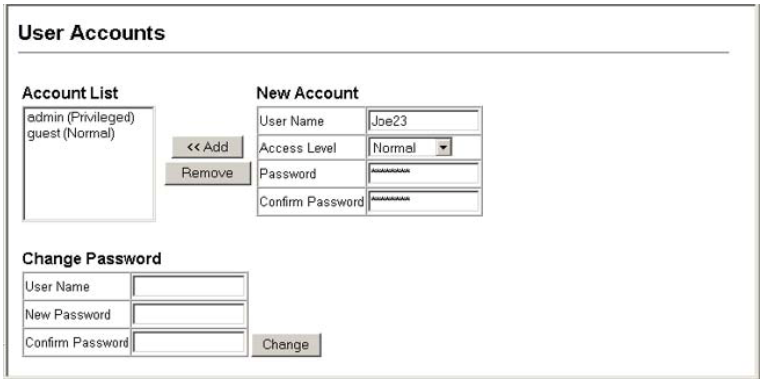
既存ユーザアカウントのパスワードを変更します。

Add/Remove

ユーザアカウントのリストへの追加、又はリストからの削除を行います。

設定方法

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



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+はすべ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。

－[authentication sequence] ― 表示された最大3つの認証方法を利用します。

RADIUS設定

Global

RADIUSサーバの設定をグローバルに適用します。

ServerIndex

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

Server IP Address

RADIUSサーバのIPアドレス（初期設定：10.1.0.1）

Server Port Number

RADIUSサーバで使用されるUDPポート番号（範囲：1-65535、初期設定：1812）

Secret Text String

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

Number of Server Transmits

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

Timeout for a reply

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

TACACS+設定

Server IP Address

TACACS+サーバのIPアドレス（初期設定：10.11.12.13）

Server Port Number

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

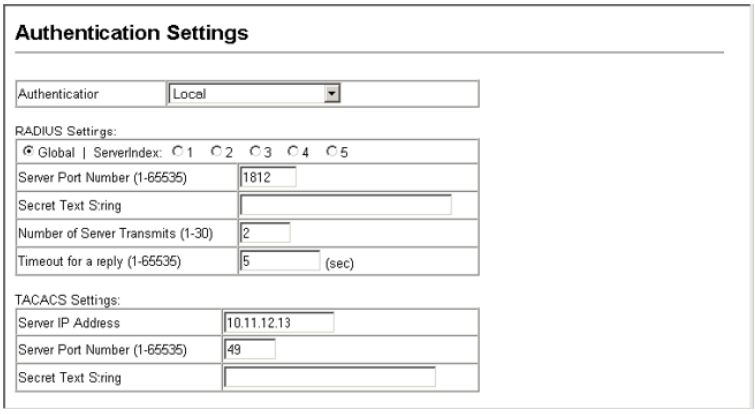
Secret Text String

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

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。



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。
  ー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。
  ー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。
  ー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以上又はNetscape Navigator 6.2 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

※ 安全なサイトの証明を指定するためには、P3-37「サイト証明書の設定変更」を参照して下さい。

設定・表示項目

HTTPS Status

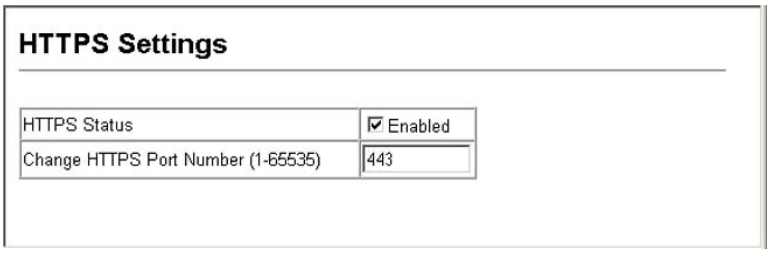
HTTPSサーバ機能を有効または無効に設定します（初期設定：有効(Enabled)）

Change HTTPS Port Number

HTTPS接続に使用されるUDPポートを指定します(初期設定:443)

設定方法

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



サイト証明書の設定変更

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

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

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

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

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

```
Console#reload
```

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います。

注意 **SSH経由での管理アクセスを行うためには、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クライアント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 156849954018676692593339467750546173253136748908365472541502024559319986854435836165199992332978176606583095610825913212890233 7654680172627257141342876294130119619556678259566410486957427888146206 5194174677298486546861571773939016477

93559423035774130980227370877945452408397175264635805817671670957480477611 7

③ **クライアント公開キーの本機への取り込み** — P4-71「copy tftp public-key」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(P3-32に記載したように、User Account画面でスイッチにクライアントを設定しておく必要があります)。クライアントはこれらのキーを使用し、認証が行われます。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(例はRSA Version1キー)。

1024 35 134108168560989392104094492015542534763164192187295892114317388 0 055536161631051775940838686311092912322268285192543746031009371877211996963178136627741416898513204911720483033925432410163799759237144901193800609025394840848271781943722884025331159521348610229029789827213532671316294325328189150453063939166 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って下さい。

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

⑥ **Challenge/Response認証** — SSHクライアントが本機と接続しようとした場合、SSHサーバはセッションキーと暗号化方式を調整するためにホストキーペアを使用します。本機上に保存された公開キーに対応するプライベートキーを持つクライアントのみアクセスすることができます。以下のような手順で認証プロセスが行われます。

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う必要はありません。

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

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 (Version 1): 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 (Version 2): 最初のフィールドはデジタル署名標準(DSS)に基づくSSHによって使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（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います。

Save Host-Key from Memory to Flash

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

Generate

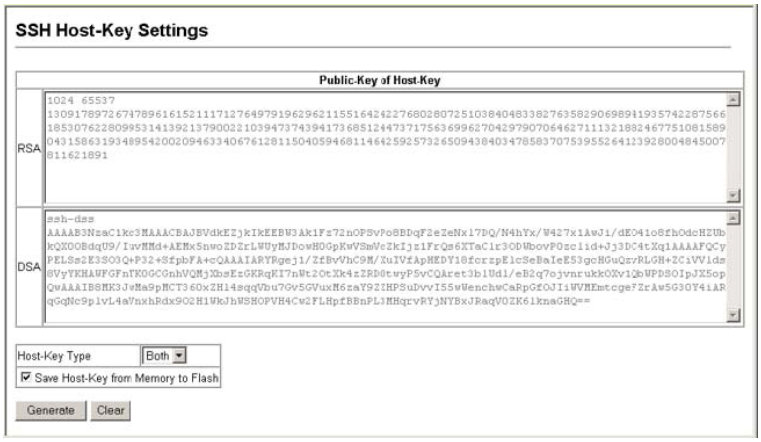
ホストキーペアを生成します。SSHサーバ設定ページでSSHサーバを有効にする前に、ホストキーペアを生成する必要があります。

Clear

RAM及びフラッシュメモリの両方に保存されているホストキーを削除します。

設定方法

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



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：有効）

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（範囲：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（範囲：1-5回、初期設定：3回）

SSH Server-Key Size

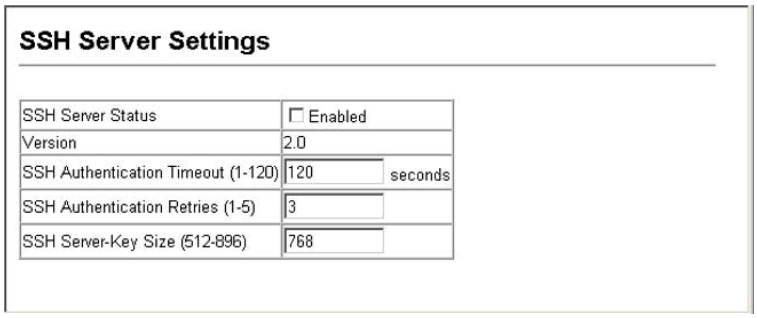
SSHサーバのキーサイズ（範囲：512-896ビット、初期設定：768ビット）

－ 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画面でhost key pairを生成する必要があります。



ポートセキュリティの設定

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

ポートセキュリティを有効にした場合、本機は有効にしたポートにおいて、設定した最大MACアドレス数に達すると、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。Static Address Table (P3-76)を使用し、入力によりMACアドレスを設定することもできます。ポートに設定された最大MACアドレス数に達すると、ポートは学習を終了します。アドレステーブルに保存されたMACアドレスは保持され、時間の経過により消去されることはありません。これ以外のデバイスがポートを利用しようとしても、スイッチにアクセスすることはできません。

機能解説

- セキュリティポートに設定できるポートは、以下の制限があります。
  －ポートモニタリングに使用できません。
  －マルチ VLAN ポートにはできません。
  －LACP 又は静的トランクポートに設定できません。
  －HUB などネットワーク接続デバイスは接続しないで下さい。
- 初期設定では、セキュリティポートへのアクセスを許可している最大 MAC アドレス数は"0"です。セキュリティポートへのアクセスを許可するためには、最大 MAC アドレス数を 1-1024 のいずれかに設定する必要があります。
- セキュリティ違反によりポートが Disabled となった(シャットダウンした)場合、Port/Port Configuration 画面(P3-59)からポートの再有効化を行って下さい。

設定・表示項目

Port

ポート番号

Name

ポートの説明(P4-118).

Action

ポートセキュリティ違反が検知された際の動作

－**None** ― 動作が行われません(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)

Max MAC Count

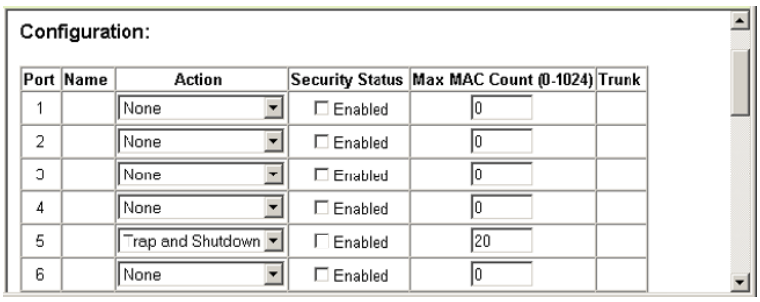
ポートが学習可能なMACアドレス数（範囲：1-1024、0は学習の無効)

Trunk

ポートがトランクされている場合のトランク番号 P3-61及び3-62)

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､最大MACアドレス数を設定し、[Apply]をクリックします。
さらに、Security Statusチェックボックスをオンにして、[Apply]をクリックします。



Configuration:

Port	Name	Action	Security Status	Max MAC Count (0-1024)	Trunk
1		None	Enabled	0	
2		None	Enabled	0	
3		None	Enabled	0	
4		None	Enabled	0	
5		Trap and Shutdown	Enabled	20	
6		None	Enabled	0	

802.1Xポート認証

スイッチは、クライアントPCをネットワーク上のスイッチに接続するだけで、容易にネットワークリソースにアクセスできるような環境を提供します。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。

ネットワーク上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。認証モードはMD5です。
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、許可または拒否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。
- スイッチ本体全体に対し、802.1X を有効に設定します。
- 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手いる必要があり、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同じ EAP 認証タイプ(MD5)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の設定

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。

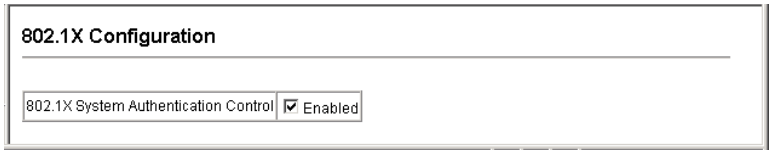
設定・表示項目

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認証ポート設定に関する設定

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（初期設定：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（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（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(初期設定はこの設定になっています)

－**Force-Unauthorized** ― dot1X対応クライアントを含めたすべてのクライアントのアクセスを禁止します。

Re-authen

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

Max-Req

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

Quiet Period

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

Re-authen Period

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

TX Period

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

Authorized

－Yes – 接続されたクライアントは認証されている

－No – 接続されたクライアントは認証されていない

－空欄 – dot1X認証がポートで無効に設定されている

Supplicant

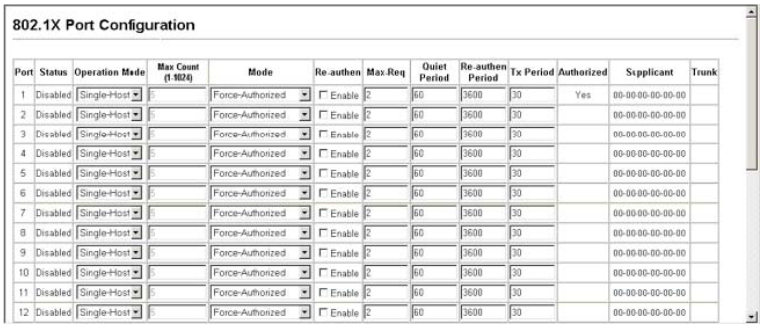
接続されたクライアントのMACアドレス

Trunk

トランク設定がされている場合に表示

設定方法

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



802.1X Port Configuration

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

IEEE802.1X統計情報の表示

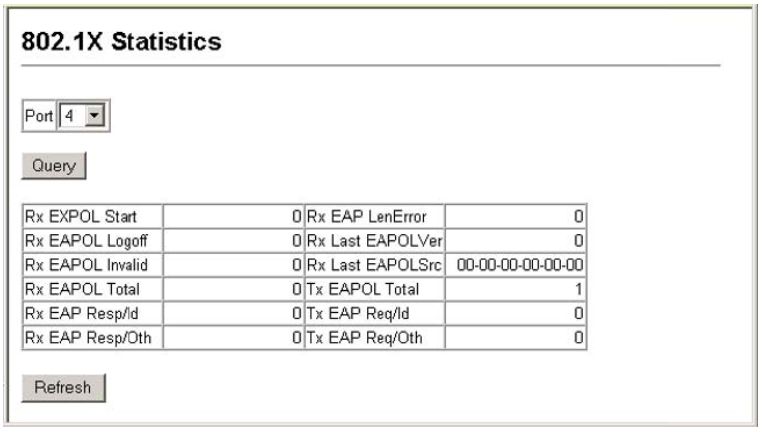
dot1Xプロトコルの各ポートの統計情報を表示します。

統計情報項目

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。ポートを選択し、[Query]をクリックします。[Refresh]をクリックすると最新の情報に更新されます。



管理アドレスのアドレスフィルタリング

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

機能解説

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

設定・表示項目

Web IP Filter

WebグループのIPアドレス

SNMP IP Filter

SNMPグループのIPアドレス

Telnet IP Filter

TelnetグループのIPアドレス

IP Filter List

そのインタフェースに接続が許可されているIPアドレス

Start IP Address

IPアドレス、又はIPアドレスを範囲で指定している場合の最初のIPアドレス

End IP Address

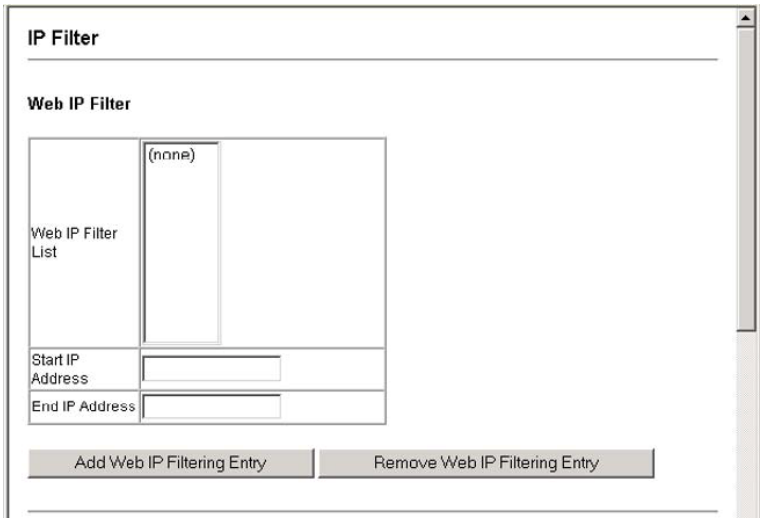
IPアドレスを範囲で指定している場合の最後のIPアドレス

Add/Remove Filtering Entry

IPアドレスをリストへ追加または削除

設定方法

[Security]→[IP Filter]をクリックします。そのインタフェースに管理アクセスを許可するIPアドレスを1つまたは範囲で指定し、[Add IP Filtering Entry]をクリックしてフィルタリストを更新します。


IP Filter
Web IP Filter
Web IP Filter List
(none)
Start IP Address
End IP Address
Add Web IP Filtering Entry
Remove Web IP Filtering Entry

3-6 ACL

Access Control Lists (ACL)は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によるIPフレームへのパケットフィルタリング及び、MACアドレス及びイーサネットタイプによるすべてのフレームに対するパケットフィルタリングを提供します。

入力されるパケットのフィルタリングを行うには、初めにアクセスリストを作成し、必要なルールを追加し、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、MACアドレス、又は他の条件と一致するパケットに対して許可(Permit)又は拒否(Deny)するためのリストです。本機では入力及び出力パケットに対してACLと一致するかどうか1個ずつ確認を行います。パケットが許可ルールと一致した場合には直ちに通信を許可し、拒否ルールと一致した場合にはパケットを落とします。リスト上の許可ルールに一致しない場合、パケットは落とされ、リスト上の拒否ルールに一致しない場合、パケットは通信を許可されます。

機能解説

ACLは以下の制限があります。

- 各 ACL は最大 32 ルールまで設定可能です。
- 最大 ACL 設定数は 88 個です。
- 但し、リソースの制限により、ポートに結び付けられた規則の数の平均は 20 を超えないようにして下さい。
- 本機は ingress (入力)フィルタリングの ACL のみをサポートしています。但し、1 個の IP ACL を任意のポートに、1 個の MAC ACL をイングレスフィルタリング全体にバインド可能です。つまり、1 つのインタフェースに対して、入力 IP ACL 及び入力 MAC ACL の 2 個の ACL のみバインドできます。

有効なACLは以下の順番で実行されます。

1. 入力ポートの入力MAC ACLのユーザに定義されたルール
2. 入力ポートの入力IP ACLのユーザに定義されたルール
3. 入力ポートの入力IP ACLのデフォルトルール(permit any any)
4. 入力ポートの入力MAC ACLのデフォルトルール(permit any any)

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

ACL名及びタイプの設定

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（最大文字数：16文字）

Type

以下の3つのタイプがあります。

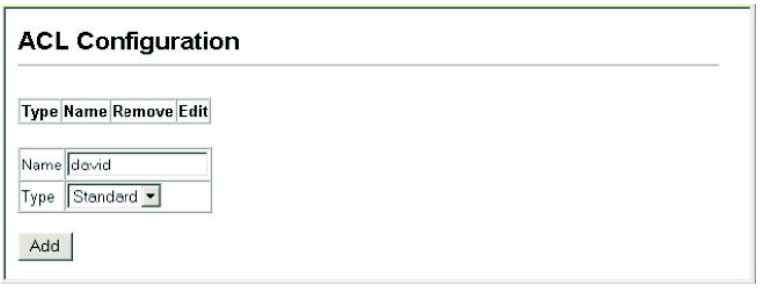
－**Standard** ― ソースIPアドレスに基づくフィルタリングを行うIP ACLモード

－**Extended** ― 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うIP ACLモード

－**MAC** ― ソース又はディスティネーションMACアドレス、イーサネットフレームタイプ(RFC 1060)に基づくフィルタリングを行うMAC ACLモード

設定方法

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



Standard IP ACLの設定

設定・表示項目

Action

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

Address Type

ソースIPアドレスの指定を行います。"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

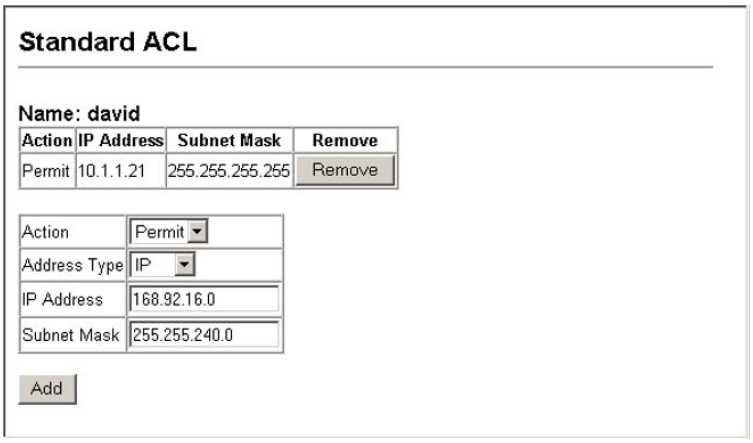
ソースIPアドレス

Subnet Mask

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ルール）

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 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

パケットプライオリティを以下の項目により設定

－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）

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 Bitmask

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

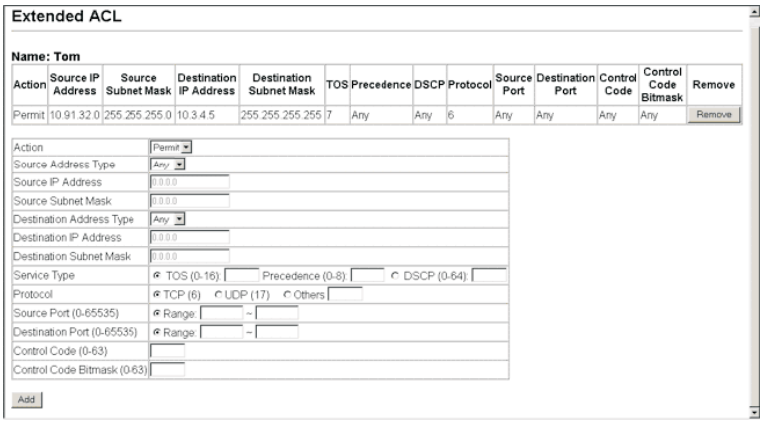
－有効なSYN及びACK — コントロールコード：18、コントロールビットマスク：18

－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。サービスタイプやプロトコルタイプ、TCPコントロールコード等のその他の必要項目を設定し、[Add]をクリックします。



MAC ACLの設定

設定・表示項目

Action

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

Source/Destination Address Type

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

Source/Destination MAC Address

ソース又はディスティネーションMACアドレス

Source/Destination Bitmask

ソース又はディスティネーションMACアドレスの16進数のマスク

VID

VLAN ID（範囲：1-4094）

Ethernet Type

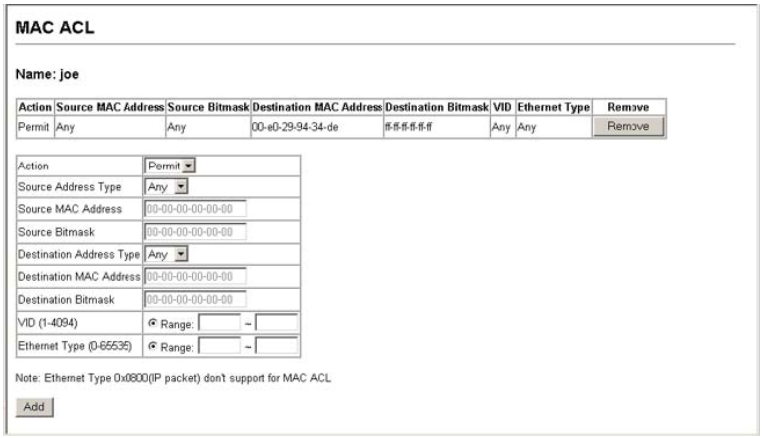
この項目はイーサネットIIフォーマットのパケットのフィルタリングに使用します（範囲：0-65535）

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。

設定方法

「許可」又は「拒否」の動作を設定し、その後ソース/ディスティネーションMACアドレスを特定し、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MACアドレスを指定します。"MAC"を選択した場合、ベースアドレス及び16進数のビットマスクを設定します。VIDやイーサネットタイプ等の他の項目を設定し、[Add]をクリックします。



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。IP ACLは1つを任意のポートに指定できますが、MAC ACLは1つのみ指定可能で、スイッチすべてのポートに設定されます。

機能解説

- ポートのバインドを行う前に、ACL ルールのマスクを設定する必要があります。
- 本機では ingress（入力）ACL をサポートします。1 個の IP ACL を任意のポートに、1 個の MAC ACL をイングレスフィルタリング全体にバインド可能です。

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：1-16/26/52）

IP

ポートにバインドするIP ACLルール

MAC

全体にバインドするMAC ACLルール

IN

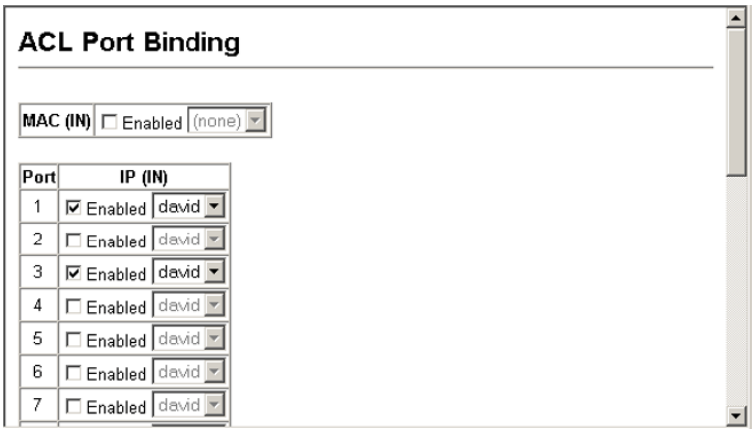
入力(ingress)パケットに対するACL

ACL Name

ACL名

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 ポート設定

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(1000Base-T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

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	Trunk Member
1		100Base-TX	Enabled	Up	100full	None	Enabled	
2		100Base-TX	Enabled	Down	100full	None	Enabled	
3		100Base-TX	Enabled	Up	100full	None	Enabled	
4		100Base-TX	Enabled	Down	100full	None	Enabled	
5		100Base-TX	Enabled	Down	100full	None	Enabled	
6		100Base-TX	Enabled	Down	100full	None	Enabled	
7		100Base-TX	Enabled	Down	100full	None	Enabled	
8		100Base-TX	Enabled	Down	100full	None	Enabled	
9		100Base-TX	Enabled	Down	100full	None	Enabled	
10		100Base-TX	Enabled	Down	100full	None	Enabled	
11		100Base-TX	Enabled	Down	100full	None	Enabled	
12		100Base-TX	Enabled	Down	100full	None	Enabled	
13		100Base-TX	Enabled	Down	100full	None	Enabled	

インタフェース接続の設定

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

設定・表示項目

Name

各インタフェースに管理識別用に名前をつけることができます(1-64文字)

Admin

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

Speed/Duplex

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

Flow Control

フローコントロールを自動設定又は手動設定で行うことができます。

Autonegotiation (Port Capabilities)

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

－**10half** ― 10 Mbps half-duplexで動作します。

－**10full** ― 10 Mbps full-duplexで動作します。

－**100half** ― 100 Mbps half-duplexで動作します。

－**100full** ― 100 Mbps full-duplexで動作します。

－**1000full** ― 1000 Mbps full-duplexで動作します。

－**Sym** (Gigabitのみ) ― ポーズフレームの送受信をする場合この項目をチェックします。また、非対称ポーズフレームにより送信者と受信者がオートネゴシエーションを行う場合はチェックを外します（現在のスイッチチップでは対称ポーズフレームのみサポートしています）

－**FC** ― フローコントロールをサポートします。フローコントロールはバッファがいっぱいの場合に本機へ直接接続される終端端末及びセグメントからの"blocking"トラフィックにより、フレームロスを解消します。フローコントロールの有効時には、half-duplexではバックプレッシャが、full-duplexではIEEE 802.3xが利用されます（障害回避などのために必要な場合以外は、ハブへの接続時にはフローコントロールを無効にして下さい。フローコントロ

ールを有効にした場合、バックプレッシャのジャミング信号により、ハブが接続されたセグメント全体のパフォーマンスを低下させる可能性があります)
(初期設定：オートネゴシエーション:有効
100BASE-TX - 10half, 10full, 100half, 100full、
1000BASE-T -10half, 10full, 100half, 100full, 1000full、
1000BASE-SX/LX/LH - 1000fullが対応機能として通知されます)

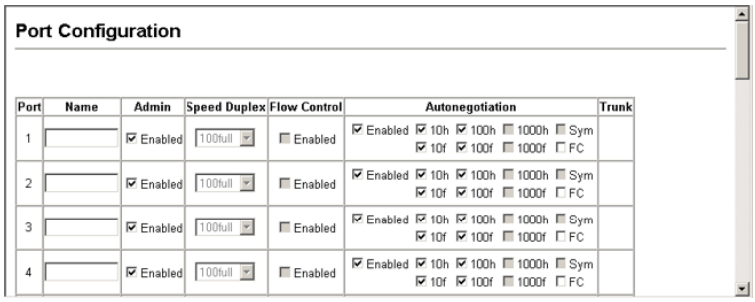
Trunk

ポートがトランクメンバーの場合に表示されます。トランクの設定及びポートメンバーの選択は、P3-60「トランクグループ設定」を参照して下さい。

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

設定方法

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



トランクグループ設定

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を束ねるトランク機能を利用することができます。最大4つのトランクを同時に設定できます。
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、すべてのポートをLACPポートに設定することができます。もし、9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、設定を行う場合には、デバイス間のケーブル接続を行う前に両端のデバイスにおいてトランクの設定を行って下さい。
トランクの設定を行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って下さい。
- 1 トランク最大 8 ポート、最大 4 つのトランクを作成できます。
- 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う必要があります。
- トランクのすべてのポートは VLAN の移動、追加及び削除を行う際に 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

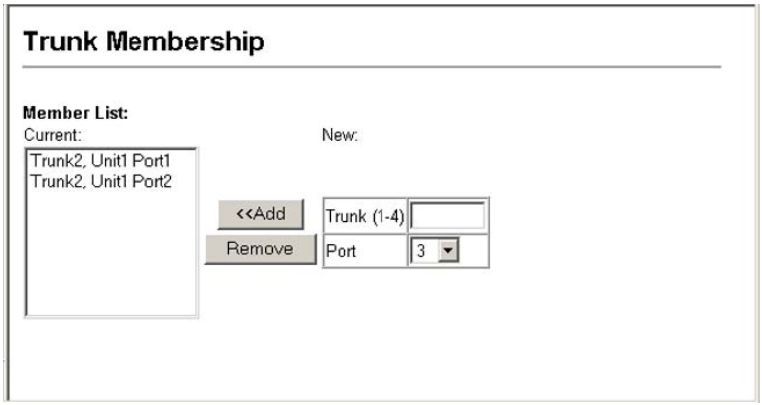
新規にトランクを作成するための入力欄

－**Trunk** ― トランク識別子（範囲：1-4）

－**Port** ― ポート識別子（範囲：1-16/26/52）

設定方法

[Port]→[Trunk Membership]をクリックします。1から4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。
- 9 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(P3-62)

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）

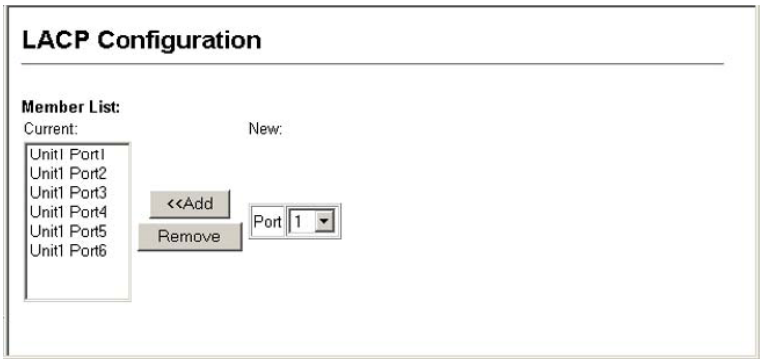
New

新規にトランクを作成するための入力欄

－**Port** ― ポート識別子（範囲：1-16/26/52）

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(P4-139)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）の設定を行います。

Port

ポート番号（範囲：1-16/26/52）

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。

ー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値に設定する必要があります（範囲：0-65535、初期設定：1）

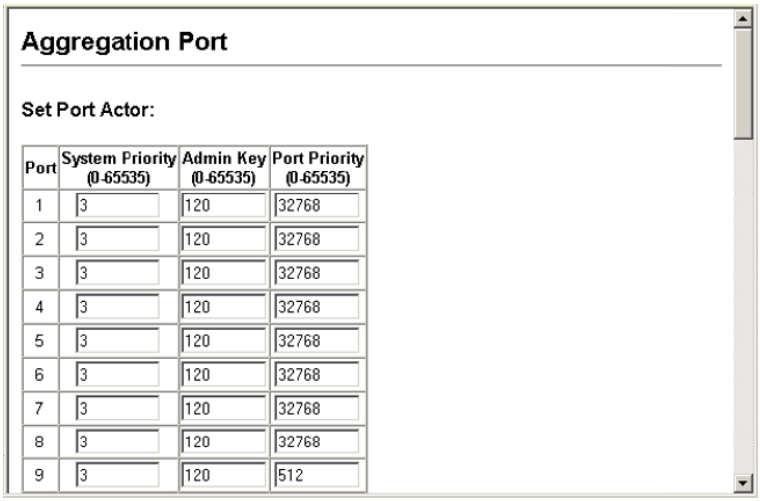
Port Priority

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の設定を行います。その他にPort Partnerの設定を行うこともできます(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。



Port	System Priority (0-65535)	Admin Key (0-65535)	Port Priority (0-65535)
1	3	120	32768
2	3	120	32768
3	3	120	32768
4	3	120	32768
5	3	120	32768
6	3	120	32768
7	3	120	32768
8	3	120	32768
9	3	120	512

LACPポートカウンターの表示

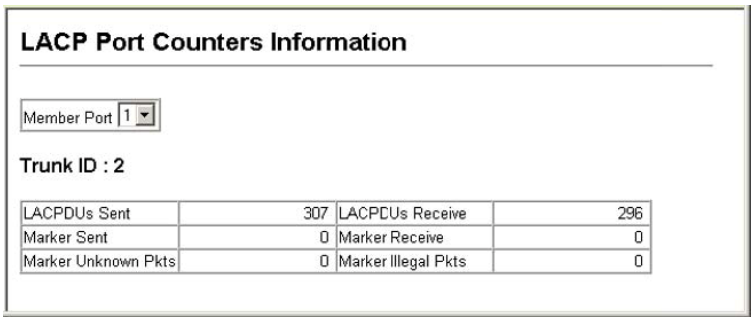
LACPプロトコルメッセージの統計情報の表示を行います。

カウンター情報

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

設定方法

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



ローカル側のLACP設定及びステータスの表示

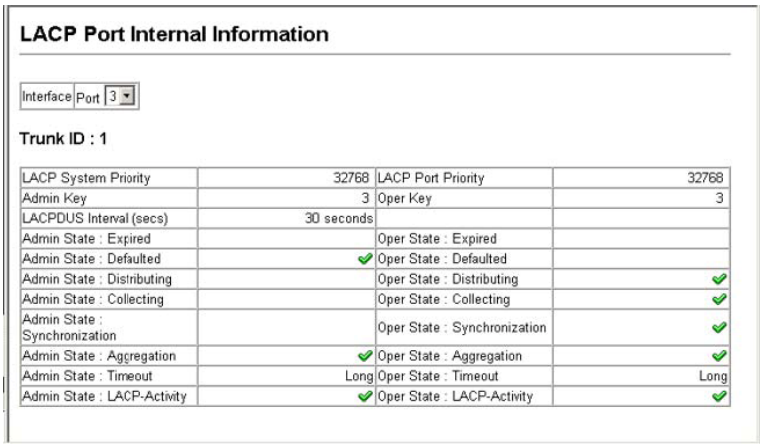
LACPのローカル側の設定及びステータスの表示を行うことができます。

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。



LACP Port Internal Information

Interface Port 3

Trunk ID : 1

LACP System Priority	32768	LACP Port Priority	32768
Admin Key	3	Oper Key	3
LACPDUS Interval (secs)	30 seconds		
Admin State : Expired		Oper State : Expired	
Admin State : Defaulted	✔	Oper State : Defaulted	
Admin State : Distributing		Oper State : Distributing	✔
Admin State : Collecting		Oper State : Collecting	✔
Admin State : Synchronization		Oper State : Synchronization	✔
Admin State : Aggregation	✔	Oper State : Aggregation	✔
Admin State : Timeout	Long	Oper State : Timeout	Long
Admin State : LACP-Activity	✔	Oper State : LACP-Activity	✔

リモート側のLACP設定及びステータスの表示

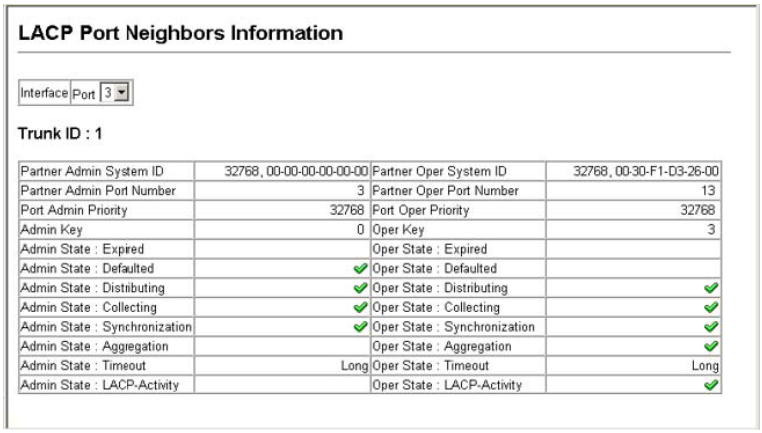
LACPのリモート側の設定及びステータスの表示を行うことができます。

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。



LACP Port Neighbors Information

Interface Port 3

Trunk ID : 1

Partner Admin System ID	32768, 00-00-00-00-00-00	Partner Oper System ID	32768, 00-30-F1-D3-26-00
Partner Admin Port Number	3	Partner Oper Port Number	13
Port Admin Priority	32768	Port Oper Priority	32768
Admin Key	0	Oper Key	3
Admin State : Expired		Oper State : Expired	
Admin State : Defaulted	✔	Oper State : Defaulted	
Admin State : Distributing	✔	Oper State : Distributing	✔
Admin State : Collecting	✔	Oper State : Collecting	✔
Admin State : Synchronization	✔	Oper State : Synchronization	✔
Admin State : Aggregation		Oper State : Aggregation	✔
Admin State : Timeout	Long	Oper State : Timeout	Long
Admin State : LACP-Activity		Oper State : LACP-Activity	✔

ブロードキャストストームのしきい値の設定

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場合、適切に構成されていない時に起こります。ネットワーク上で過度のブロードキャストトラフィックが発生した場合、ネットワークの性能は大幅に低下し、通信が完全に中断されることがあります。

各ポートのブロードキャストトラフィックのしきい値を設定することによりブロードキャスト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ブロードキャスト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を与えません。
- 指定されたしきい値はすべてのポートに適用されます。

設定・表示項目

Port

ポート番号（ポートのブロードキャストコントロール）

Trunk

トランク番号（トランクのブロードキャストコントロール）

Type

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

Threshold

ポートを通過するブロードキャストパケットの毎秒当たりのパケット数をしきい値で設定できます（範囲：64-95232000オクテット/秒、初期設定：32000オクテット/秒）

Protect Status

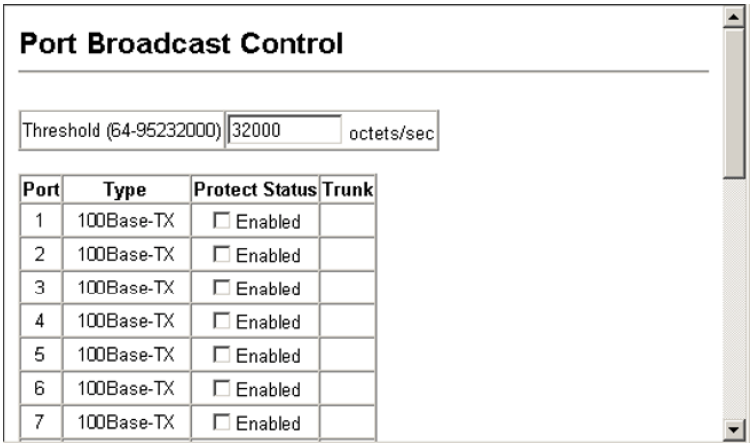
ブロードキャストストームコントロールの有効/無効（初期設定：有効）

Trunk

トランクメンバーのポートの場合表示（ポートのブロードキャストコントロール）

設定方法

[Port]→[Port/TrunkBroadcast Control]をクリックします。Threshold（しきい値）、Protect Status（有効にしたいポート）を設定し、[Apply]をクリックします。



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、任意のソースポートから1つの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。
- 当機器は、ソースポートとターゲットポートは一対一のミラーリングとなります。
- 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 Unit

通信がモニターされるソースポートのユニット

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）、（初期設定：Rx）

Target Unit

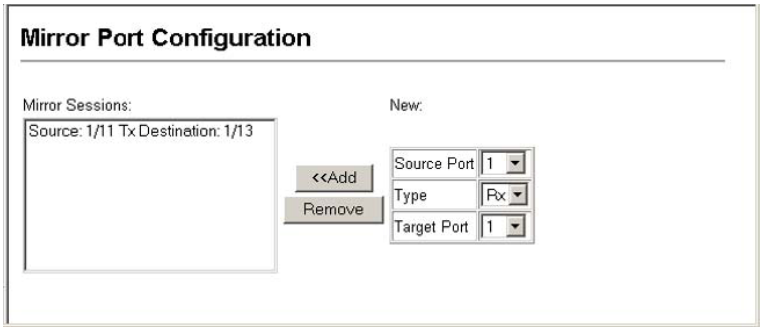
ソースポートの通信のミラーリングがされ、監視装置などを接続可能なターゲットポートのユニット

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/Unit(ソースポート/ユニット)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/Unit(ターゲットポート/ユニット)を指定し、[Add]をクリックします。



帯域制御

帯域制御機能では各ポート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。

帯域制御の粒度

帯域制御の粒度(Rate Limit Granularity)は、特定のネットワーク全体のトラフィック量をさらに制御できるようにする、ネットワーク管理の拡張機能です。"Rate Limit Granularity"は"Rate Limit

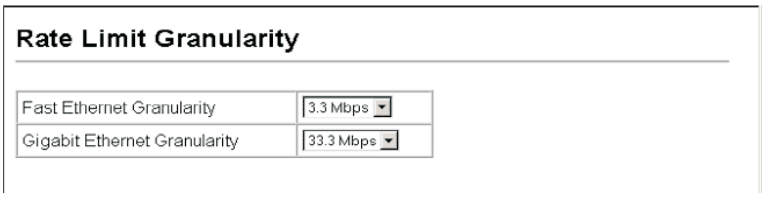
Level" (P3-71)で指定する値で乗算され、単一のインタフェースでの実際の帯域制御を設定するものです。粒度はファーストイーサネット又はギガビットイーサネットインタフェース全体に適用されます。

機能解説

- ファーストイーサネットインタフェースには、Rate Limit Granurality は 512Kbps 又は 1Mbps、3.3Mbps に設定します。
- ギガビットイーサネットインタフェースには、Rate Limit Granurality は 33.3Mbps に設定します。

設定方法

[Port]→[Rate Limit]→[Granularity]をクリックします。ファーストイーサネット/ギガビットイーサネットに設定する帯域制御粒度をそれぞれ選択し、[Apply]をクリックします。



帯域制御の設定

帯域制御の適用は、Rate Limit Configuration画面で行います。

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

Port又はTrunk

ポート番号

Rate Limit Status

帯域制御の有効/無効（初期設定：無効）

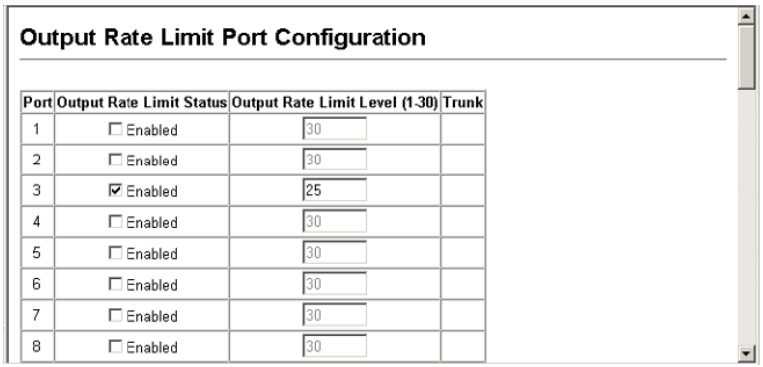
Rate Limit Level

帯域制御のレベル（範囲：1-30、初期設定：30）

注意　実際の帯域制御 = Rate Limit Level × Granularity

設定方法

[Port]→[Rate Limit]→[Input/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 Level]を設定し、[Apply]をクリックします。



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	上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

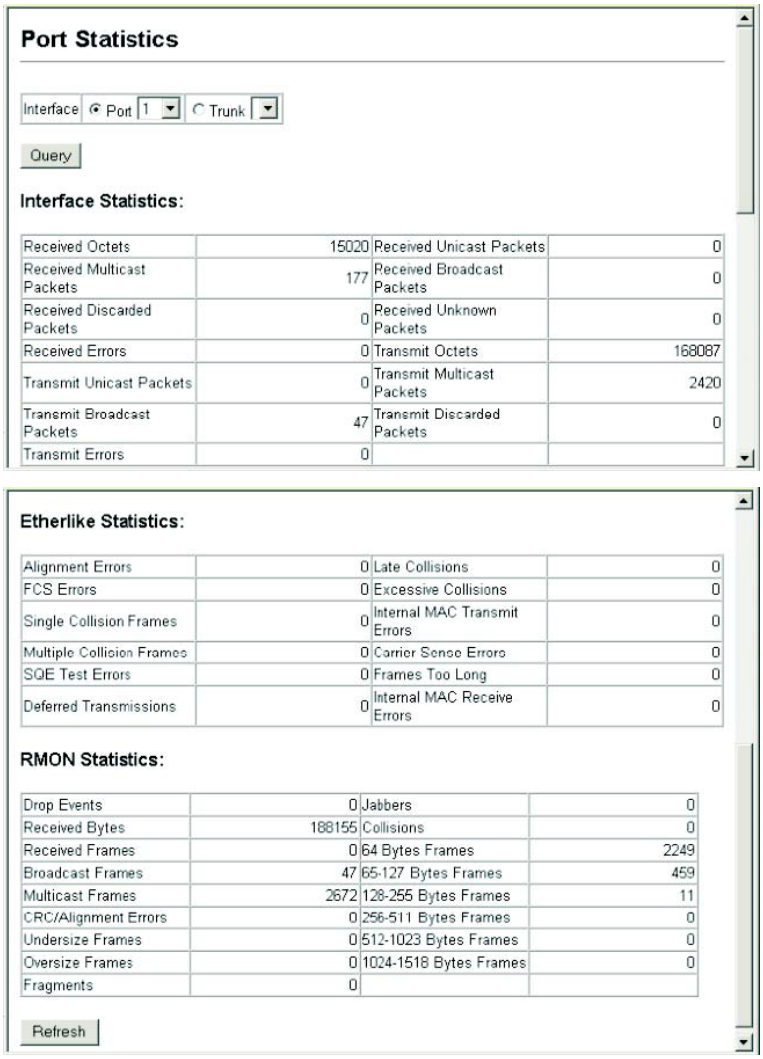
Received Broadcast Packets	このサブレイヤから送信され、高層のレイヤで受信されたパケットで、このサブレイヤのブロードキャストアドレス宛てのパケットの数
Received Discarded Packets	エラー以外の理由で削除された受信パケットの数。パケットが削除された理由は、バッファスペースを空けるためです
Received Unknown Packets	インタフェースから受信したパケットで、未知又は未対応プロトコルのために削除されたパケットの数
Received Errors	受信パケットで、上層位プロトコルへ届けることを妨げるエラーを含んでいたパケットの数
Transmit 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 Packets	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 Frames	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	フ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	リ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
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	受信した正常なフレームのうち、このマルチキャストアドレスに転送したフレーム数
CRC/Alignment Errors	CRC/配列エラー数(FCS又は配列エラー)
Undersize Frames	(フレーミングビットを除き、FCSオクテットは含む)64オクテットより短い長さの受信フレーム数で、その他の点では正常な受信フレーム数
Oversize Frames	(フレーミングビットを除き、FCSオクテットは含む)1518オクテットよりも長い受信フレームで、その他の点では正常な受信フレーム数

Fragments	(フレーミングビットを除き、FCSオクテットは含む)64オクテットよりも小さい長さでFCSもしくは配列エラーがあった受信フレーム数
64 Bytes Frames	不良パケットを含む送受信トータルフレーム数(フレーミングビットを除き、FCSオクテットは含みます。)
65-127 Byte Frames 128-255 Byte Frames 256-511 Byte Frames 512-1023 Byte Frames 1024-1518 Byte Frames 1519-1536 Byte Frames	不良パケットを含む送受信トータルフレーム数で、各オクテット数の範囲に含まれるもの(フレーミングビットを除き、FCSオクテットは含みます。)

設定方法

[Port]→[Port Statistics]をクリックします。表示するインタフェースを選択し[Query]をクリックします。
ページ下部の[Refresh]ボタンを使用することで、表示されている内容を最新の情報に更新することができます。



3-8 アドレステーブル設定

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すべての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。

静的アドレスの設定

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

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

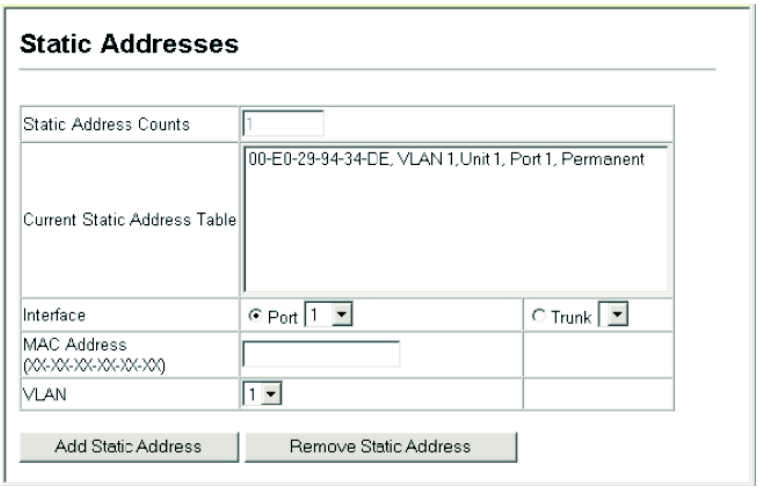
インタフェースのMACアドレス

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。



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すべ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

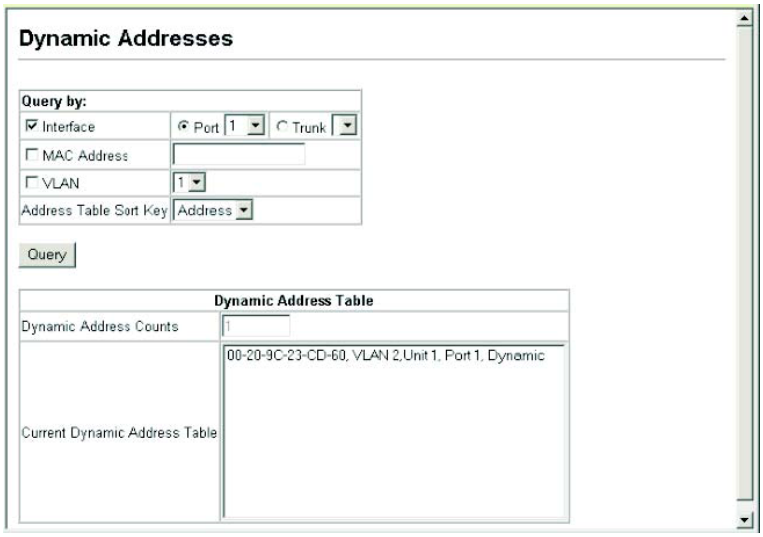
動的に学習するMACアドレス数

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。



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

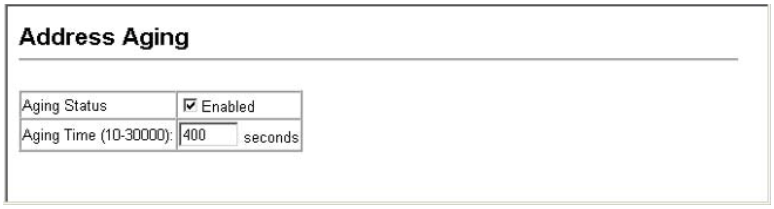
エージングタイムの機能の有効/無効

Aging Time

MACアドレスエージングタイム（範囲：10-30000秒、初期設定：300秒）

設定方法

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



3-9 スパニングツリーアルゴリズム設定

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)

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。指定されたデバイスに接続するすべてのポートは、指定ポートになります。
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に比べ速く(30秒以上かかったSTPに比べ、約1から3秒の速さで)ネットワークの再構築が行えます。

STP/RSTP使用時は、すべてのVLANメンバー間で安定的なパスを維持するのが難しくなります。ツリー構造の頻繁な変更により、グループメンバーのうちいくつかは簡単に孤立します。

グローバル設定の表示

STA Information画面から現在の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	32768.0000ABCD0000
Bridge ID	32768.0000ABCD0000	Root Port	0
Max Age	20	Root Path Cost	0
Hello Time	2	Configuration Changes	2
Forward Delay	15	Last Topology Change	0 d 0 h 0 min 35 s

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

STPに設定しIEEE802.1Dに準拠したBPDUのみを送信できます。（初期設定はRSTP）これによりネットワーク全体で1つのスパニングツリーインスタンスを作成します。1ネットワークに複数のVLANが存在する場合、ループ回避のためパス間の特定のVLANメンバーがVLANから外れ、孤立することがあります。（STP/RSTP BPDUはタグなしフレームとして転送され、VLAN境界を通過します）

- 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/RSTP BPDUはタグなしフレームとして転送され、VLAN境界を通過します）

－ **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。

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。

－**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)（初期設定）

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秒、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)]の小さい方の値）

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秒）

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（初期設定）

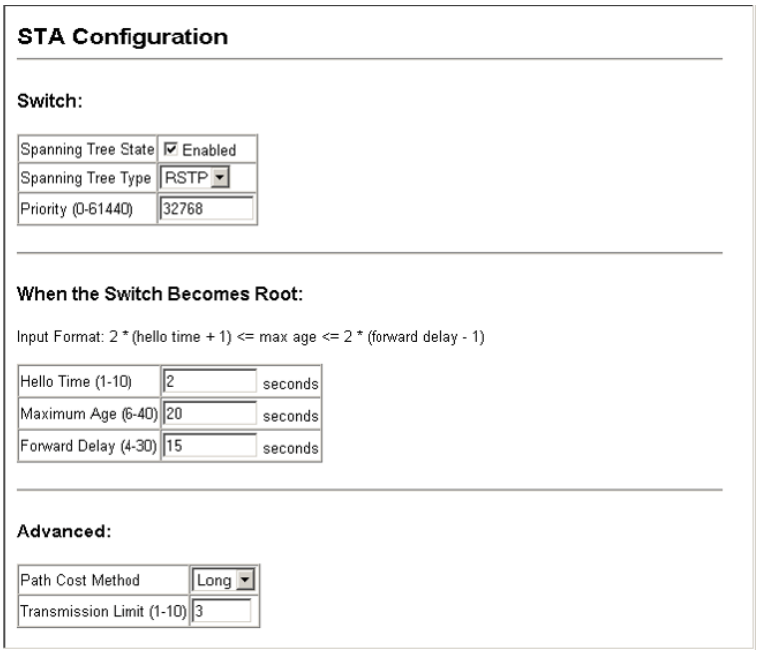
－**Short** ― 16ビットの1-65535の値

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秒）

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。



インタフェース設定の表示

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

設定・表示項目

Spanning Tree

STAの有効/無効が表示されます。

STA Status

スパニングツリー内での各ポートの現在の状態を表示します。

－**Discarding** ― STP設定メッセージを受信しますが、パケットの送信は行っていません。

－**Learning** ― 矛盾した情報を受信することなく、Forward Delayで設定した間隔で設定メッセージを送信しています。ポートアドレステーブルはクリアされ、アドレスの学習が開始されています。

－Forwarding — パケットの転送が行われ、アドレスの学習が継続されています。

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

Forward Transitions

ポートが転送状態(Forwarding)に遷移した回数が表示されます。

Designated Cost

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

Designated Bridge

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

Designated Port

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

Oper Link Type

インタフェースの属するLANセグメントの使用中の2点間の状況。この項目はSTP Port/Trunk Configuration画面の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画面の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画面のみ)

設定方法

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

STA Port Information

Port	Spanning Tree	STA Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port	Oper Link Type	Oper Edge Port	Port Role	Trunk Member
1	Enabled	Forwarding	7	200000	32768.0.0030F1552000	128.24	Point-to-Point	Disabled	Root	
2	Enabled	Discarding	0	200000	61440.0.0000E9313131	128.2	Point-to-Point	Enabled	Disabled	
3	Enabled	Discarding	0	200000	61440.0.0000E9313131	128.3	Point-to-Point	Enabled	Disabled	
4	Enabled	Discarding	0	200000	61440.0.0000E9313131	128.4	Point-to-Point	Enabled	Disabled	
5	Enabled	Discarding	0	200000	61440.0.0000E9313131	128.5	Point-to-Point	Enabled	Disabled	

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P3-83「インタフェース設定の表示」を参照して下さい)

－Discarding ― STP設定メッセージを受信しますが、パケットの送信は行っていません。

－Learning ― 矛盾した情報を受信することなく、Forward Delayで設定した間隔で設定メッセージを送信しています。ポートアドレステーブルはクリアされ、アドレスの学習が開始されています。

－Forwarding ― パケットの転送が行われ、アドレスの学習が継続されています。

Trunk Member

トランクメンバーに設定されているかどうかを表示します。
(STA Port Configuration画面のみ)

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

Path Cost

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

－設定範囲：
Ethernet: 200,000-20,000,000
Fast Ethernet: 20,000-2,000,000
Gigabit Ethernet: 2,000-200,000

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

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

Admin Link Type

インタフェースへ接続する接続方式（初期設定：Auto）
－Point-to-Point ― 他の1台のブリッジへの接続
－Shared ― 2台以上のブリッジへの接続
－Auto ― Point-to-PointかSharedのどちらかを自動的に判断します。

Admin Edge Port (Fast Forwarding)

ブリッジ型LANの終端、もしくはノードの終端にインタフェースが接続されている場合、本機能を有効にすることができます。
ノードの終端ではループが起きないため、直接、転送状態にすることができます。Edge Portを指定することにより、ワークステーションやサーバなどのデバイスへの迅速な転送を提供し、以前の

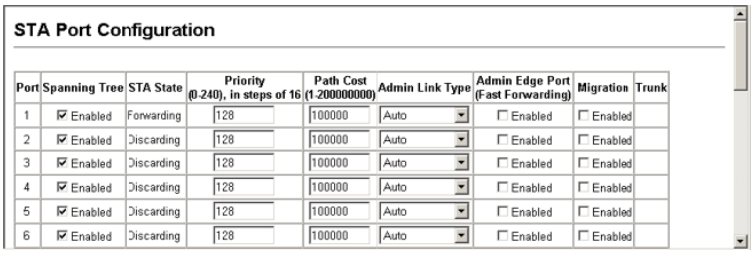
転送アドレステーブルを保持することにより、スパニングツリー再構築時のタイムアウト時間を削減します。
但し、必ずノードの終端デバイスに接続されているポートのみでEdge Portを有効にして下さい（初期設定：有効）

Migration

設定及びトポロジ変更通知BPDUを含むSTP BPDUを検知することにより、自動的にSTP互換モードに変更することができます。
また、本機能のチェックボックスをチェックし機能を有効にすることにより、手動で適切なBPDUフォーマット（RSTP又はSTP互換）の再確認を行うことができます。

設定方法

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



STA Port Configuration

Port	Spanning Tree	STA State	Priority (0-240), in steps of 16	Path Cost (1-200000000)	Admin Link Type	Admin Edge Port (Fast Forwarding)	Migration	Trunk
1	☑ Enabled	Forwarding	128	100000	Auto	☐ Enabled	☐ Enabled	
2	☑ Enabled	Discarding	128	100000	Auto	☐ Enabled	☐ Enabled	
3	☑ Enabled	Discarding	128	100000	Auto	☐ Enabled	☐ Enabled	
4	☑ Enabled	Discarding	128	100000	Auto	☐ Enabled	☐ Enabled	
5	☑ Enabled	Discarding	128	100000	Auto	☐ Enabled	☐ Enabled	
6	☑ Enabled	Discarding	128	100000	Auto	☐ Enabled	☐ Enabled	

3-10 VLAN設定

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。

- IEEE802.1Q 準拠の最大 256VLAN 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

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。初期設定ではすべてのポートが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、メッセージを他のすべ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、他のすべてのポートへメッセージ

が送られます。VLANの要求はネットワークを通じて送られます。GVRP対応デバイスは、終端装置の要求に基づき自動的にVLANグループの構成を行うことが可能となります。

ネットワークでGVRPを使用するために、最初に要求されたVLANへ（OS又はアプリケーションを使用して）ホストデバイスを追加します。その後、このVLAN情報がネットワーク上へ伝達されます。ホストに直接接続されたエッジスイッチおよびネットワークのコアスイッチにおいてGVRPを有効にします。また、ネットワークのセキュリティ境界線を決め、通知の伝送を防ぐためポートのGVRPを無効にするか、ポートのVLANへの参加を禁止する必要があります。

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

タグ付・タグなしフレームの送信

1台のスイッチでポートベースのVLANを構成する場合、同じタグなしVLANにポートを割り当てることで構成できます。しかし、複数のスイッチ間でのVLANグループに参加するためには、すべ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

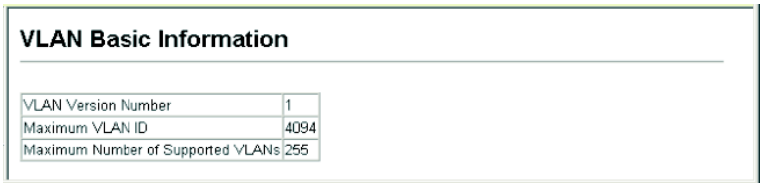
本機で認識可能なVLAN IDの最大値

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の表示

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

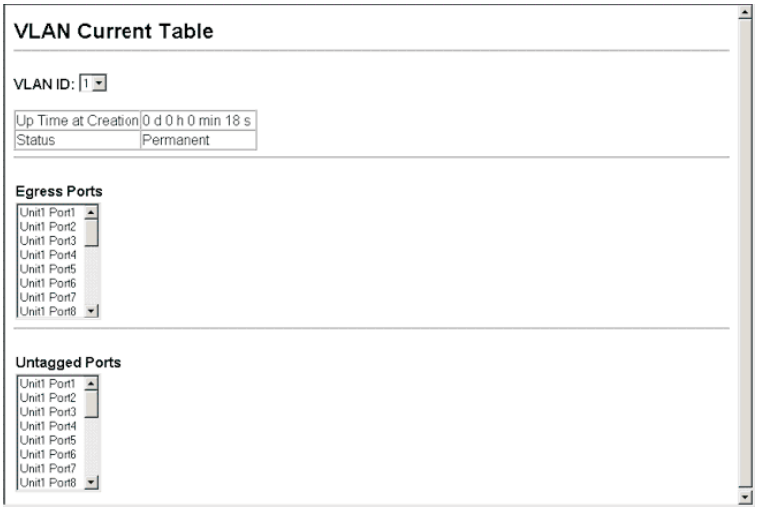
すべてのVLANポートメンバー

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すべての現在のVLANグループを表示します。最大255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（範囲：1-4094）

Name

VLAN名（範囲：1-32文字）

Status

このVLANを有効にします。

－**Enabled:** VLANは使用することができます。

－**Disabled:** VLANは停止されます。

Add

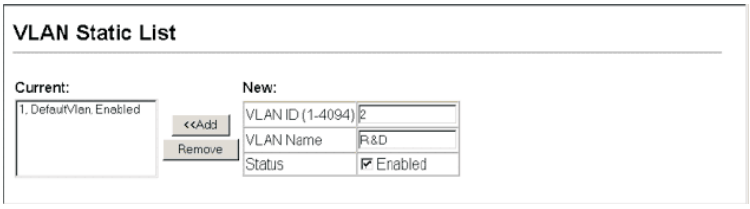
リストに新しいVLANグループを追加します。

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)

静的VLANテーブルを使用し、選択したVLANのポートメンバーの設定を行います。
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います。

注意　P3-93「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。P3-96「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を変更することにより修正することができます。

設定・表示項目

VLAN

設定されたVLAN ID（範囲：1-4094）

Name

VLAN名（範囲：1-32文字）

Status

このVLANが有効か無効かを表示します。

－Enable: VLAN は使用することができます。

－Disable: VLAN は停止されます。

Port

ポート番号

Membership Type

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

－Tagged —インタフェースはVLANのメンバーとなります。ポートから送信されるすべ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すべ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P3-89「自動VLAN登録」を参照して下さい。

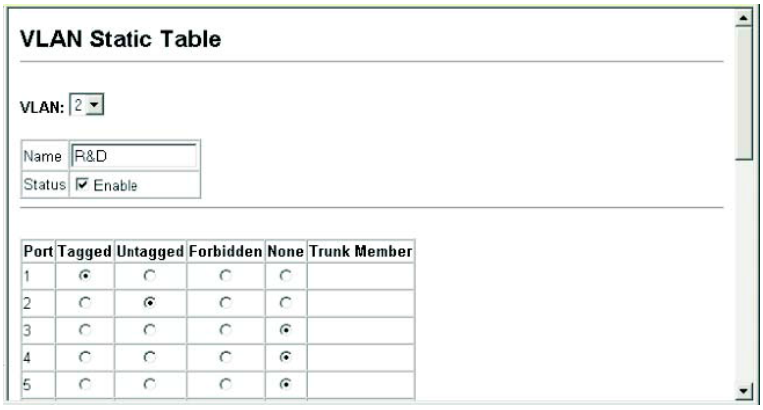
—None —インタフェースはVLANのメンバーではありません。このVLANに関連したパケットは、インタフェースから送信されません。

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]→[802.1Q VLAN]→[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

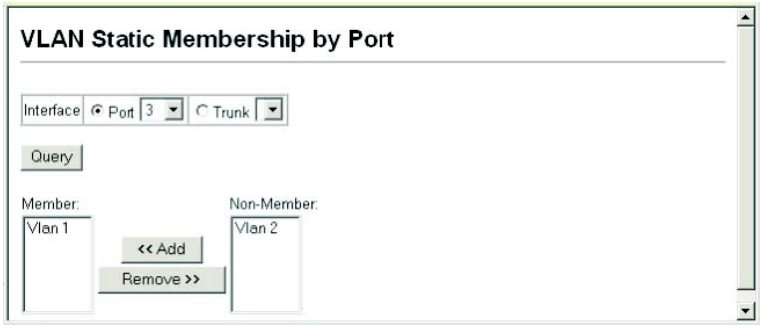
選択されたインタフェースがタグ付メンバーとして登録されているVLAN

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 by Port]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(Port/Trunk)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）
ーインタフェースが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。PVIDをグループに対し与えていない場合、他のすべてのVLANはタグなしメンバーとなります。

Acceptable Frame Type(受け入れ可能なフレームの種類)

すべ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。すべ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(オプション：All, Tagged、初期設定：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：無効）
ー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。
ーイングレスフィルタリングが無効で、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、（このポートで禁止されているVLANを除く）すべてのポートに対して受信フレームをフラッディングさせます。
ー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。
ー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。

GVRP Status

インタフェースGVRPを有効又は無効にします。GVRPはこの設定が実施される前にスイッチを全体的に有効にする必要があります（P3-12「ブリッジ拡張機能の表示」を参照して下さい）。無効な時、このポートで受信されたGVRPパケットは放棄されどのGVRP登録も他のポートから伝搬されなくなります（初期設定：無効）

GARP Join Timer*

VLANグループに参加するために送信される要求またはクエリの送信間隔（範囲：20-1000センチセカンド、初期設定：20）

GARP Leave Timer*

VLANグループを外れる前にポートが待機する間隔。この時間はJoin Timerの2倍以上の時間を設定する必要があります。これにより、Leave又はLeaveAllメッセージが発行された後、ポートが実際にグループを外れる前に再びVLANに参加できます（範囲：60-3000センチセカンド、初期設定：60）

GARP LeaveAll Timer*

VLANグループ参加者へのLeaveAllクエリメッセージの送信からポートがグループを外れるまでの間隔。この間隔はノードが再び参加することによるトラフィックの発生量を最小限にするためのLeave Timerよりも大幅に大きい値を設定する必要があります（範囲：500-18000センチセカンド、初期設定：1000）

* GARP タイマー設定は以下の規則に沿って設定して下さい:

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

Mode

ポートのVLANメンバーシップモードを表示します（初期設定：Hybrid）

－1Q Trunk — VLANトランクの終端となっているポートを指定します。トランクは2台のスイッチの直接接続となり、ポートは発信元VLANのタグ付フレームを送信します。但し、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ので注意して下さい。

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

Trunk Member

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

設定方法

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

VLAN Port Configuration

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

プライベートVLANの設定

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

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

プライマリグループ、セカンダリグループに設定するには、次の方法で行います。

1. Private VLAN Configuration画面(P3-100)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(P3-100)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(P3-102)でポートの種類をPromiscuous (プライマリVLANのすべてのポートへアクセス可能な無差別ポート)又はHost (コミュニティVLANから、又コミュニティVLAN以外の場合は無差別ポートへのアクセスのみ

可能)から指定します。その後、任意の無差別ポートをプライマリVLANとコミュニティVLANのホストポートに指定します。

独立VLANに設定するには、次の方法で行います。

1. Private VLAN Configuration画面(P3-100)ですべてのトラフィックが経由する無差別ポートを1つ設定します。
2. Private VLAN Port Configuration画面(P3-102)でポートの種類をPromiscuous（外部ネットワークとの単一の経路となる)又はIsolated (同一VLANの無差別ポートへのアクセスのみ可能)から指定します。その後、設定した無差別ポートと独立(ホスト)ポートを独立VLANに指定します。

現在のプライベートVLANの表示

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

設定・表示項目

VLAN ID

表示するVLAN ID（1-4094）とVLANの種類

Primary VLAN

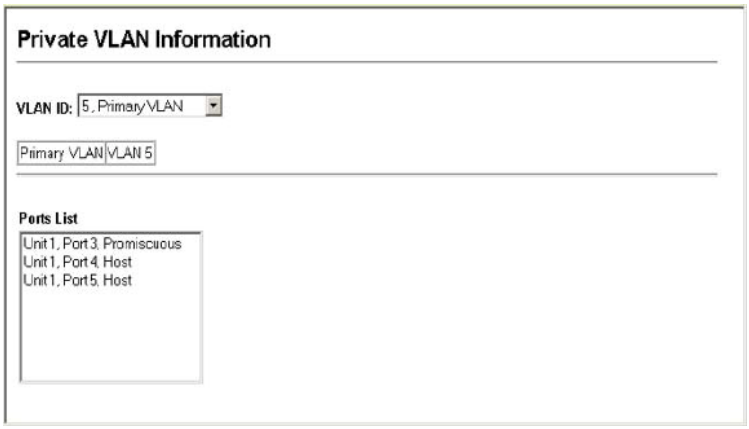
表示しているVLAN IDに関連付けされているVLAN。プライマリVLANの場合は自身のVLAN IDを、コミュニティVLANの場合は関連付けされているプライマリVLAN IDを、又独立VLANはスタンドアロンのVLANを表示します。

Ports List

表示しているプライベートVLANに所属するポート(ポートの種類)

設定方法

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



プライベートVLANの設定

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

設定・表示項目

VLAN ID

設定するVLAN ID（1-4094）

Type

プライベートVLANには次の3つの種類があります。

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

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

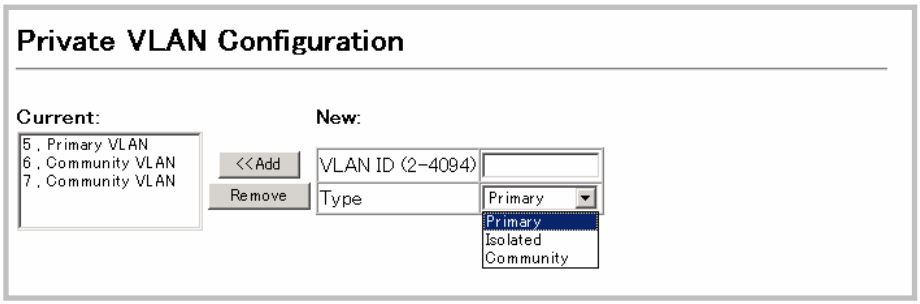
－Isolated ― そのVLAN内で、無差別ポートと独立ポート間のみでデータをやり取りします。同一VLAN内の独立ポート同士の通信は遮断されます。

Current

設定済みのVLANのリスト

設定方法

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



VLANの関連付け

コミュニティVLANとプライマリVLANは関連付けを行う必要があります。

設定・表示項目

Primary VLAN ID

プライマリVLAN ID（1-4094）

Association

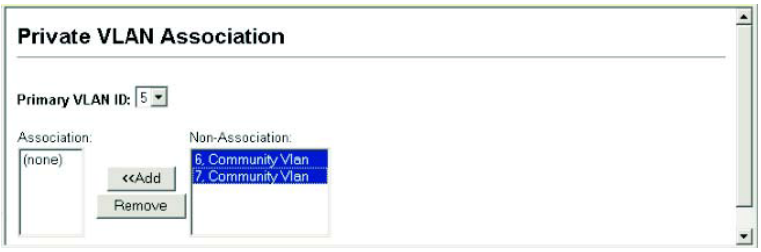
選択したプライマリVLANと既に関連付けられているコミュニティVLAN

Non-Association

選択したプライマリVLANと関連付けられていないコミュニティVLAN

設定方法

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



プライベートVLANインタフェース情報の表示

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

設定・表示項目

Port又はTrunk

本機のインタフェース

PVLAN Port Type

プライベートVLANのポートの種類を表示します。

－Normal ― このポートはプライベートVLANでの設定はありません。

－Host ― コミュニティポートに設定されており、同一コミュニティVLANに所属するポートと、又は指定された無差別ポートとのみ通信が可能です。あるいは、独立ポートに設定されており、同一の独立VLANに所属する無差別ポートとのみ通信が可能です。

－Promiscuous ― 無差別ポートに設定されており、プライベートVLAN内のすべてのポートと通信が可能です。

Primary VLAN

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

Community VLAN

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

Isolated VLAN

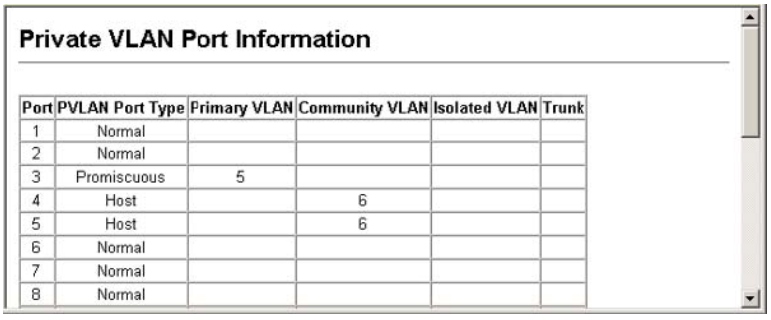
特定のVLANの独立ポートと無差別ポート間のみでデータをやり取りします。同一VLAN内の独立ポート同士の通信は遮断されます。

Trunk

トランク識別子（Port Information画面のみ）

設定方法

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



Private VLAN Port Information

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

本機のインタフェース

PVLAN Port Type

プライベートVLANのポートの種類を設定します。

－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。PVLAN Port TypeがPromiscuousの場合、関連付けたプライマリVLANを設定します。Hostの場合、表示されたプライマリVLANが選択中のセカンダリVLANに関連付けられています。

Community VLAN

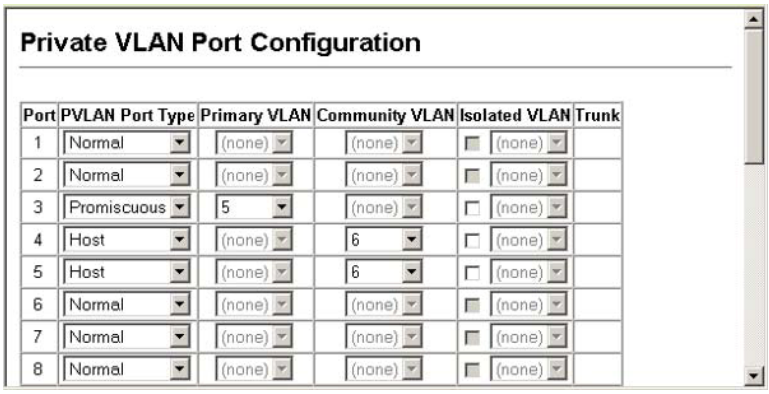
コミュニティVLAN。コミュニティポート間、又はコミュニティポートと指定した無差別ポート間でデータをやり取りします。PVLAN Port Typeを"Host"に設定し、関連付けたコミュニティVLANを設定します。

Isolated VLAN

特定のVLANの独立ポートと無差別ポート間のみでデータをやり取りします。同一VLAN内の独立ポート同士の通信は遮断されます。PVLAN Port Typeを"Host"に設定し、"Isolated VLAN"チェックボックスをクリックして独立VLANを設定し、ドロップダウンリストから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。



Private VLAN Port Configuration

Port	PVLAN Port Type	Primary VLAN	Community VLAN	Isolated VLAN	Trunk
1	Normal	(none)	(none)	(none)	
2	Normal	(none)	(none)	(none)	
3	Promiscuous	5	(none)	(none)	
4	Host	(none)	6	(none)	
5	Host	(none)	6	(none)	
6	Normal	(none)	(none)	(none)	
7	Normal	(none)	(none)	(none)	
8	Normal	(none)	(none)	(none)	

3-11 Class of Service設定

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8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。

レイヤ2キューの設定

インタフェース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。スイッチへ入るすべ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すべての VLAN タグを外します。

設定・表示項目

Default Priority

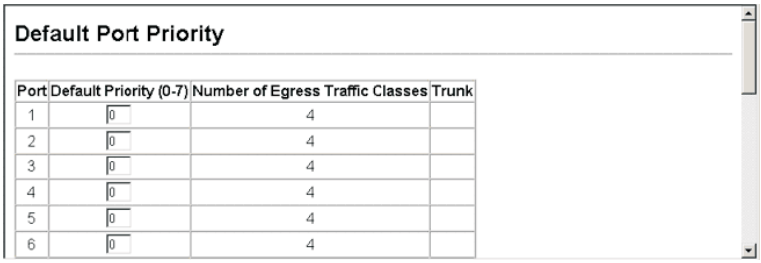
各インタフェースの受信されたタグなしフレームに割り当てられるプライオリティ（範囲：0-7、初期設定：0）

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4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：0-7、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：0-3、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。現在のCoS値のアウトプットキューへの割り当て状態が表示されます。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, 6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。

トラフィッククラスのサービスウェイトの設定

本機は各プライオリティキューの提供をする時に重み付けラウンドロビン(WRR)アルゴリズムを使用しています。P3-105「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4つのEgressキューのうちの一つにマッピングされます。これらのキューと対応しているトラフィックプライオリティのそれぞれへのウェイトを割り当てることができます。このウェイトは、各キューがサービスに登録され、それにより、特定のプライオリティ値に応じたソフトウェア・アプリケーション毎のレスポンス時間に影響する頻度が設定されます。

設定・表示項目

WRR Setting Table

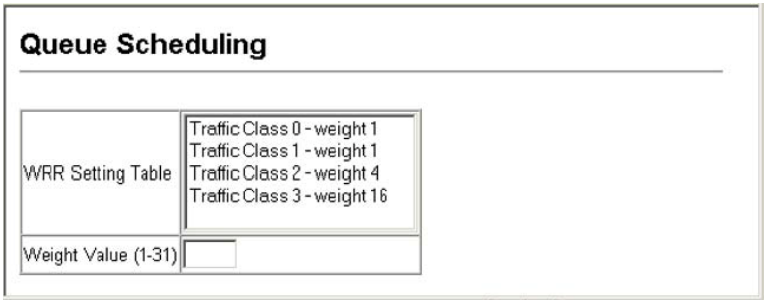
各トラフィッククラス（キュー）のウェイトの表を表します。

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。キュー0はウェイト0に固定され、変更できないことに注意して下さい（範囲：1-31）

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。



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、複数のレイヤ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3ビットのIP Precedence、又は６ビットのDifferentiated Services Code Point(DSCP)サービスの6ビットを含みます。これらのサービスが有効な時、プライオリティはCoS値へマッピングされ、該当する出力キューへ送られます。

異なったプライオリティ情報が通信に含まれている可能性があるため、本機は次の方法で出力キューへプライオリティ値をマッピングしています:

- プライオリティマッピングの優先順位はIPポートプライオリティ又は IP Precedence、DSCP プライオリティ、デフォルトポートプライオリティの順番となります。
- IP Precedence 及び DSCP プライオリティは両方有効にはできません。これらのプライオリティ形式の一つを有効にすると自動的にもう一方は無効になります。

IP Precedence/DSCPプライオリティの選択

本機は、使用しているIP Precedence又はDSCPプライオリティを選択することができます。どちらかの方式の一つを選択するか、この機能を無効にすることができます。

設定・表示項目

Disabled

IP Precedence及びDSCPの両方のサービスを無効にします（初期設定）

IP Precedence

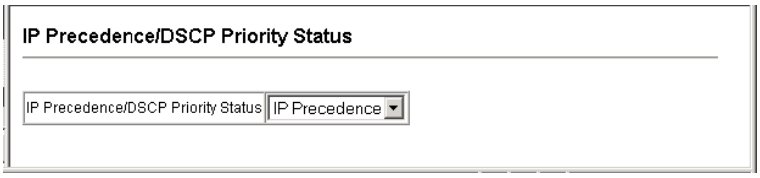
IP Precedenceを使用しL3/L4プライオリティをマッピングします。

IP DSCP

DSCPを使用しL3/L4プライオリティをマッピングします。

設定方法

[Priority]→[IP Precedence/ DSCP Priority Status]をクリックします。
IP Precedence/DSCP Priority Statusメニューから**IP Precedence**又は**IP DSCP**、**Disabled**を選択し、その後[Apply]をクリックします。



IP Precedenceのマッピング

IPv4ヘッダ中のToSオクテットは、先行3ビットにより、8段階のプライオリティレベルを定義します。初期設定のIP Precedence値はClass of Service値に1対1でマッピングされています（Precedence値0はCoS値0にマッピング）。プライオリティレベル6及び7は、ネットワーク制御に使用され、他のレベルは様々なアプリケーション形式に使用されます。ToSビットは以下の表で定められます：

プライオリティレベル	トラフィックタイプ	プライオリティレベル	トラフィックタイプ
7	Network Control	3	Flash
6	Internetwork Control	2	Immediate
5	Critical	1	Priority
4	Flash Override	0	Routine

設定・表示項目

IP Precedence Priority Table

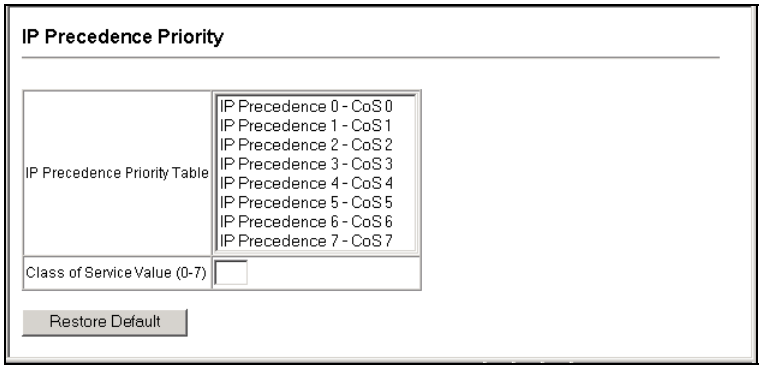
CoS値と各IP Precedence値の相関マップを表示します。

Class of Service Value

選択されたIP Precendence値へCoS値をマッピングします。“0”が低いプライオリティ、“7”が高いプライオリティを示します。

設定方法

[Priority]→[IP Precedence Priority]をクリックします。IP Precedence Priority Table からIP Precedence値を選択し、Class of Service Value欄を入力し[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。指定されていないすべての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。

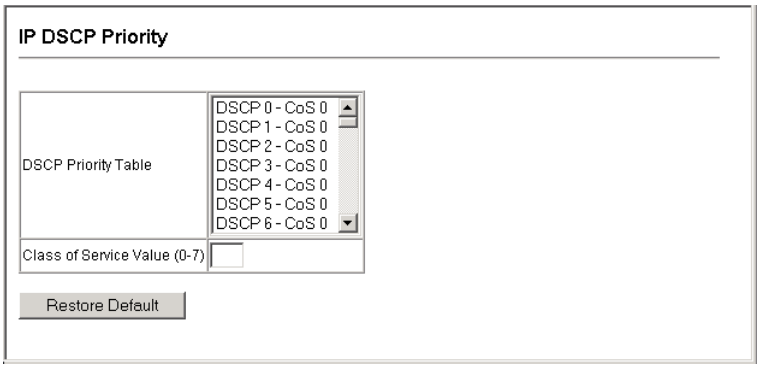
Class of Service Value

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、“7”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プライオリティ値を選択し、Class of Service Value欄で値を入力し、[Apply]をクリックします。



IPポートプライオリティのマッピング

フレームヘッダのIPポート番号(TCP/UDPポート番号)に基づき、ネットワークアプリケーションとCoSのマッピングが可能です。よく知られているTCP/UDPウェルノウンポート番号には、HTTP : 80、FTP : 21、Telnet : 23、POP3 : 110などがあります。

設定・表示項目

IP Port Priority Status

IPポートプライオリティの有効/無効

IP Port Priority Table

CoS値と各IPポート番号との相関マップを表示します。

IP Port Number (TCP/UDP)

IPポート番号を設定します。

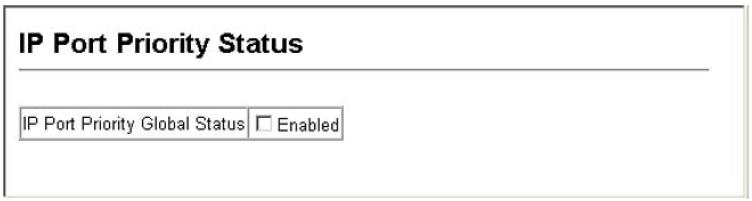
Class of Service Value

選択されたIPポートプライオリティへCoS値をマッピングします。
“0”が低いプライオリティ、“7”が高いプライオリティを示します。

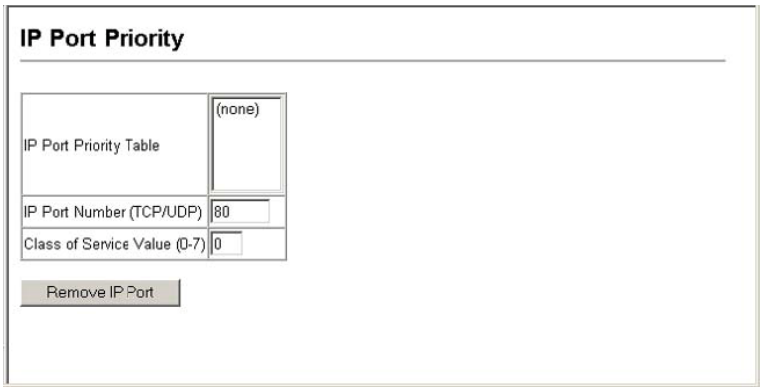
注意 IPポートプライオリティ設定はすべてのインタフェースに対して有効となります。

設定方法

[Priority]→[IP Port Priority Status]をクリックします。IP Port Priority StatusをEnabledに設定します。



[Priority]→[IP Port Priority]をクリックします。IP Port Number欄にネットワークアプリケーションに設定するポート番号を入力し、Class of Service Value欄にCoS値を設定します。その後[Apply]をクリックします。



ACLへのCoS値のマッピング

ACL CoSマッピングページでは、ACLルールに一致したパケットに対する出力キューの設定が以下の表に基づき設定を行うことができます。
指定したCoS値は一致したパケットの出力キューにのみ機能し、パケット自体にCoS値が記入されることはありません。詳細はP3-105「EgressキューへのCoS値のマッピング」を参照して下さい。

キュー	0	1	2	3
プライオリティ	1、2	0、3	4、5	6、7

設定・表示項目

Port

ポート番号

Name*

ACL名

Type

ACLタイプ(IP, MAC)

CoS Priority

ACLルールに一致するパケットのCoS値（範囲：0-7）

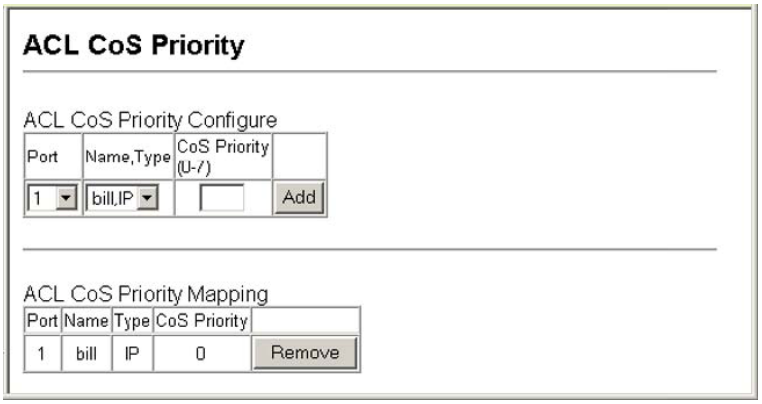
ACL CoS Priority Mapping

設定情報を表示します。

*詳細はP3-51「ACLの設定」を参照して下さい。

設定方法

[Priority]→[ACL CoS Priority]をクリックします。各ポートへのマッピングを有効にします。スクロールダウンリストからACLを選択し、[Apply]をクリックします。



3-12 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、サブネット内のすべてのポートにフラッディングするのを防ぎます。

レイヤ2 IGMP(Snooping and Query)

IGMP Snooping・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うことができます。

静的IGMPルータインタフェース－IGMP SnoopingがIGMPクエリアを検索できない場合、手動でIGMPクエリア（マルチキャストルータ/スイッチ）に接続された本機のインタフェースの指定を行うことができます。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(詳細はP3-118参照)

IGMP Snooping・Queryパラメータの設定

マルチキャストトラフィックの転送設定を行います。
IGMPクエリ及びリポートメッセージに基づき、マルチキャストトラフィックを必要とするポートにのみ通信します。すべてのポートに通信をブロードキャストし、ネットワークパフォーマンスの低下を招くことを防ぎます。

機能解説

- IGMP Snooping ― 本機は、IGMP クエリの snoop を受け、リポートパケットをIPマルチキャストルータ/スイッチ間で転送し、IPマルチキャストホストグループをIPマルチキャストグループメンバーに設定します。IGMP パケットの通過を監視し、グループ登録情報を検知し、それに従ってマルチキャストフィルタの設定を行います。
- IGMP Query ― ルータ又はマルチキャスト対応スイッチは、定期的にホストに対しマルチキャストトラフィックが必要かどうかを質問します。もしその LAN 上に 2 つ以上の IP マルチキャストルータ/スイッチが存在した場合、1 つのデバイスが”クエリア”となります。その後、マルチキャストサービスを受け続けるために接続されたマルチキャストスイッチ/ルータに対しサービスリクエストを広げます。

注意 **マルチキャストルータはこれらの情報を、DVMRPやPIMなどのマルチキャストルーティングプロトコルと共に、インターネットのIPマルチキャストをサポートするために使用します。**

設定・表示項目

IGMP Status

有効にした場合、本機はネットワークの通信を監視し、マルチキャストトラフィックを必要とするホストを特定します。これはIGMP Snoopingと呼ばれます（初期設定：有効）

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 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（範囲：2-10回、初期設定：2回）

IGMP Query Interval

IGMPクエリメッセージを送信する間隔を指定します（60-125秒、初期設定：125秒）

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が削除されるまでの時間を設定します（範囲：5-30秒、初期設定：10秒）

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を設定します（範囲：300-500秒、初期設定：300秒）

IGMP Version

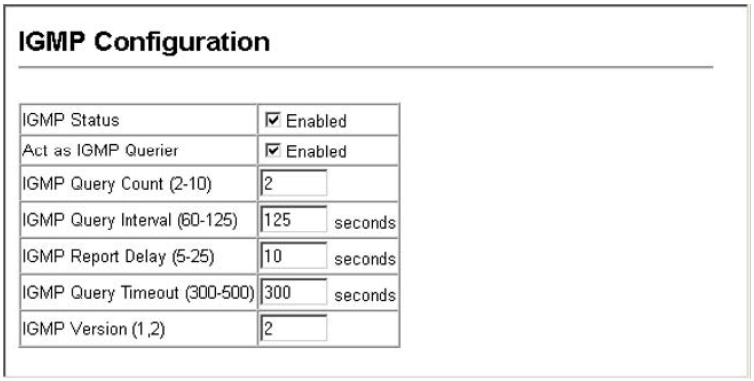
ネットワーク上の他のデバイスと互換性のあるIGMPバージョンの設定を行います（範囲：1-2、初期設定：2）

注意　サブネット上のすべてのデバイスが同じバージョンをサポートしている必要があります。

注意　IGMP Report Delay及びIGMP Query TimeoutはIGMP v2でのみサポートされます。

設定方法

[IGMP Snooping]→[IGMP Configuration]をクリックします。必要なIGMPの設定を行い、[Apply]をクリックします。
（以下の画面では初期設定を表示しています。）



マルチキャストルータに接続されたインタフェースの表示

マルチキャストルータは、IGMPからの情報に加え、インターネットでのIPマルチキャスティングを行うためDVMRP、PIM等のマルチキャスト・ルーティング・プロトコルを使用します。

ルータは、本機により動的に設定されるか、静的にインタフェースの追加を行うことができます。
Multicast Router Port Informationページでは、各VLAN IDで隣接するマルチキャストルータ/スイッチの接続されたポートを表示します。

設定・表示項目

VLAN ID

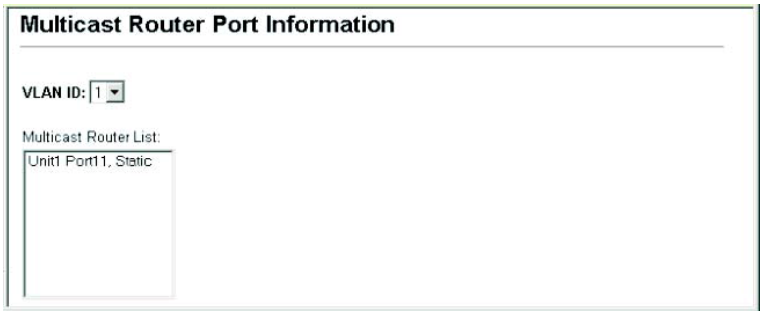
リストを表示させるVLAN ID（1-4094）

Multicast Router List

動的及び静的に設定されたマルチキャストルータの設定情報

設定方法

[IGMP Snooping]→[Multicast Router Port Information]をクリックします。スクロールダウンリストからVLAN IDを選択すると、関連するマルチキャストルータの情報を表示されます。



マルチキャストルータに接続するインタフェースの設定

ネットワーク接続状況により、IGMP snoopingによるIGMPクエリアが配置されない場合があります。IGMPクエリアとなるマルチキャストルータ/スイッチが接続されているインタフェース（ポート又はトランク）が判明している場合、ルータがサポートするマルチキャストグループへのインタフェース（及びVLAN）の参加設定を手動で行えます。これにより、本機のすべての適切なインタフェースへマルチキャストトラフィックが渡すことができます。

設定・表示項目

Interface

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

VLAN ID

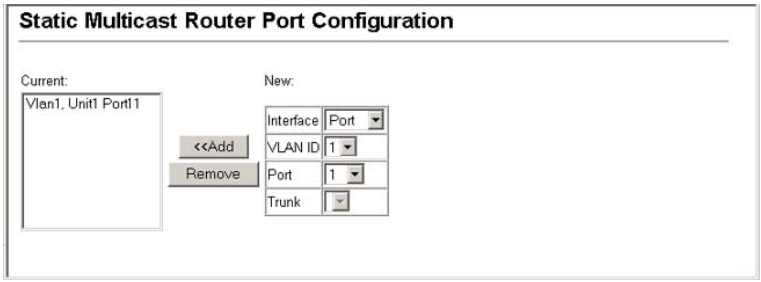
マルチキャストルータ/スイッチから送られるマルチキャストトラフィックを受信し、転送するVLANを選択します。

Port又はTrunk

マルチキャストルータに接続されたインタフェースを指定します。

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の表示

マルチキャストIPアドレス及びVLANを指定し、関連するポートメンバーを表示します。

設定・表示項目

VLAN ID

ポートメンバーを表示するVLANを選択します。

Multicast IP Address

マルチキャストサービスを行うIPアドレスを選択します。

Multicast Group Port List

VLANグループに所属し、マルチキャストサービスが送信されるポートが表示されます。

設定方法

[IGMP Snooping]→[IP Multicast Registration Table]をクリックします。VLAN IDとマルチキャストIPアドレスを選択すると、マルチキャストサービスが送信されるすべてのポートが表示されます。

マルチキャストサービスへのポートの指定

マルチキャストフィルタリングは、P3-114「IGMP Snooping・Queryパラメータの設定」の通り、IGMP snoopingとIGMPクエリメッセージを使用し、動的に設定することができます。一部のアプリケーションではさらに細かい設定が必要なため、静的にマルチキャストサービスの設定を行う必要があります。同じVLANに参加するホストの接続されたすべてのポートを加え、その後VLANグループにマルチキャストサービスの設定を行います。

機能解説

- 静的マルチキャストアドレスはタイムアウトを起こしません。
- マルチキャストアドレスが特定の VLAN に設定された場合、関連するトラフィックは VLAN 内のポートにのみ転送されます。

設定・表示項目

Interface

ポート(Port)又はトランク(Trunk)をスクロールダウンリストで選択します。

VLAN ID

マルチキャストルータ/スイッチからのマルチキャストトラフィックを受信し、転送するVLANを選択します。

Multicast IP Address

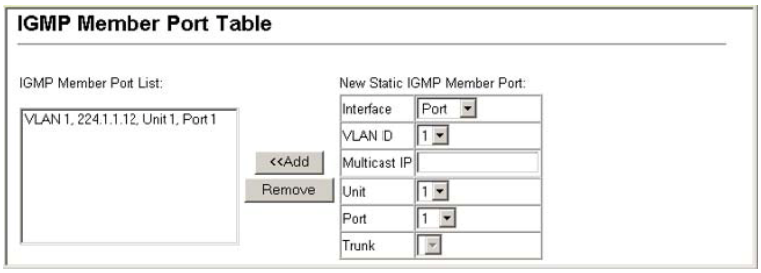
マルチキャストサービスを行うIPアドレスを入力します。

Port又はTrunk

マルチキャストルータに接続されたインタフェースの番号を指定します。

設定方法

[IGMP Snooping]→[IGMP Member Port Table]をクリックします。マルチキャストサービスに参加させるインタフェース、マルチキャストサービスを転送するVLAN、マルチキャストIPアドレスを指定し、[Add]をクリックします。すべての設定が終了後、[Apply]をクリックします。


IGMP Member Port Table
IGMP Member Port List:
VLAN 1, 224.1.1.12, Unit 1, Port 1
<<Add
Remove
New Static IGMP Member Port:
Interface
Port
VLAN ID
1
Multicast IP
Unit
1
Port
1
Trunk

このページは構成の都合上、空白となっています。

4-1　コマンドラインインタフェースの利用

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。

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 FXC3126 is opened.
To end the CLI session, enter [Exit].

Console#
```

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 **工場出荷時設定では本機のIPアドレスはDHCP経由で取得します。**

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-*n*#"と表示されます。Normal Execモードの場合には"Vty-*n*>"と表示されます。Nには各Telnetセッション番号が表示されます。**

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 FXC3126 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

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
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
```

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。

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。

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
  bridge-ext          Bridge extension information
  calendar            Date and time information
  dot1x               802.1X content
  garp                GARP properties
  gvrp                GVRP interface information
  history             History information
  interfaces          Interface information
  ip                  IP information
  lacp                LACP statistic
  line                TTY line information
  log                 Login records
  logging             Login setting
  mac                 MAC access list
  mac-address-table   Configuration of the address table
  management          Management IP filter
  map                 Maps priority
  port                Port Characteristics
  public-key          Public Key information
  queue               Priority queue information
  radius-server       RADIUS server information
  rate-limit          Configures rate-limits
  running-config      Information on the running configuration
  snmp Simple         Network Management Protocol statistics
  sntp Simple         Network Time Protocol configuration
  spanning-tree       Spanning-tree configuration
  ssh                 Secure shell server connections
  startup-config      Startup system configuration
  system              System Information
  tacacs-server       TACACS server settings
  users               Information about terminal lines
  version             System hardware and software versions
  vlan                Virtual LAN settings
Console#show
```

"**show interfaces ?**"と入力した場合には、以下のような情報が表示されます。

```
Console#show interfaces ?
  counters            Interface counters information
  status              Interface status information
  switchport          Interface switchport information
Console#
```

キーワードの検索

キーワードの一部と共に"?"を入力すると、入力した文字列から始まるすべてのキーワードが表示されます（入力する際に文字列と"?"の間にスペースを空けないで下さい）
例えば、"s?"と入力すると、以下のように"s"から始まるすべてのキーワードが表示されます:

```
Console#show s?
snmp sntp    spanning-tree   ssh   startup-config
Console#show s
```

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。

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。

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れ、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 Interface Line 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。

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。enableコマンドに続けてPrivilegedレベルのパスワード"super"を入力することによって、Normal Execモードからも Privileged Execモードにアクセスできます（page 4-31）

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 FXC3126 is opened.
To end the CLI session, enter [Exit].

Console#
```

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

CLI session with the FXC3126 is opened.
To end the CLI session, enter [Exit].

Console>enable
Password: [privileged level password]
Console#
```

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実行中の設定ファイルのみが変更され、再起動時には保存されません。
電源を切った場合にも実行中の設定ファイル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うためのモードです。
- **Interface Configuration** ― "**speed-duplex**"や"**negotiation**"コマンドなどポート設定を行うためのモードです。
- **Line Configuration** ― "**parity**"や"**databits**"などコンソールポート関連の設定を行うためのモードです。
- **VLAN Configuration** ― VLAN グループを設定するためのモードです。

Global Configurationモードにアクセスするためには、Privileged Execモードで"**configure**"コマンドを入力します。画面上のプロンプトが"**Console(config)#**"と変更になり、Global Configurationのすべてのコマンドを使用することができるようになります。

```
Console#configure
Console(config)#
```

他のモードへは、以下の表のコマンドを入力することにより入ることができます。又、それぞれのモードからは"**exit**"又は"**end**"コマンドを使用してPrivileged Execモードに戻ることもできます。

モード	コマンド	プロンプト
Line	Line {console | vty}	Console(config-line)#
Access Control List	access-list ip standard access-list ip extended access-list mac	Console(config-std-acl) Console(config-ext-acl) Console(config-mac-acl)
Interface	interface {ethernet *port* | port-channel *id* | vlan *id*}	Console(config-if)#
VLAN	vlan database	Console(config-vlan)#

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)#
```

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	1文字カーソルを進めます。
Delete又は backspace	コマンド入力を間違えた際に削除します。

4-3 コマンドグループ

システムコマンドは機能別に以下の表の通り分類されます:

コマンドグループ	内容	ページ
Line	ボーレートやタイムアウト時間などシリアルポート及びTelnetを使用した本機への接続に関する設定	4-11
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	4-22
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	4-28
Flash/File	ファームウェアコードやスイッチの設定ファイルに関連したコマンド	4-71
Authentication	IEEE802.1X及びポートセキュリティのリモート認証に関連したコマンド	4-77
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	4-96
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及びIPアドレスフィルタリングの設定	4-111
Interface	Trunk、LACPやVLANなどを各ポートの設定	4-117
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	4-129
Rate Limit	通信の最大送受信帯域のコントロール	4-131
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	4-134
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	4-145
Spanning Tree	STA設定	4-149
VLAN	各ポートのVLANグループの設定及びプライベートVLANの設定	4-162

GVRP and Bridge Extension	動的なVLANの設定を行うためのGVRPの設定、ブリッジ拡張MIBの設定	4-178
Priority	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/UDPトラフィックタイプのプライオリティの設定	4-183
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	4-197
IP Interface	管理アクセス用IPアドレスの設定	4-207

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。

NE (Normal Exec)
PE (Privileged Exec)
GC (Global Configuration)
ACL (Access Control List Configuration)
IC (Interface Configuration)
LC (Line Configuration)
VC (VLAN Database Configuration)

4-4 Line Commands

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	4-11
login	コンソール接続時のパスワードの有効化	LC	4-12
password	コンソール接続時のパスワードの設定	LC	4-13
timeout login response	CLIのログイン入力待ち時間の設定	LC	4-14
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	4-15
password-thresh	パスワード入力時のリトライ数の設定	LC	4-16
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	4-16
databits*	各文字あたりのデータビットの設定	LC	4-17
parity*	パリティビット生成の設定	LC	4-18
speed*	ボーレートの設定	LC	4-18
stopbits*	1byteあたりのストップビット値の設定	LC	4-19
disconnect	Line接続を終了	PE	4-20
show line	ターミナル接続の設定情報を表示	NE,PE	4-20

*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 (4-20)
show users (4-67)

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 (4-30)
password (4-13)

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を入力します。
- *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 (4-12)
password-thresh (4-16)

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 (4-16)
exec-timeout (4-15)

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）（範囲：0-65535 秒、0：タイムアウト設定なし）

初期設定

CLI：タイムアウト設定なし
Telnet：600秒（10分）

コマンドモード

Line Configuration

コマンド解説

- 設定時間内に入力が行われた場合、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。
- 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)#exec-timeout 120
Console(config-line)#
```

関連するコマンド

silent-time (4-16)
exec-timeout (4-15)

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します。"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(範囲:1-120、0:回数の制限をなくします)

初期設定

3

コマンドモード

Line Configuration

コマンド解説

- リトライ数が設定値を超えた場合、本機は一定時間、ログインのリクエストに応答しなくなります(応答をしなくなる時間に関しては"**silent-time**"コマンドでその長さを指定できます)。Telnet 時にリトライ数が制限値を超えた場合には Telnet インタフェースが終了となります。
- 本コマンドはコンソール接続と Telnet 接続の両方に有効です。

例

本例ではパスワードのリトライ回数を5回に設定しています。

```
Console(config-line)#password-thresh 5
Console(config-line)#
```

関連するコマンド

silent-time (4-16)

timeout login response (4-14)

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します。"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）（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

コマンド解説

"**password-thresh**"コマンドによりリトライ数が設定されていない場合は初期設定値の3回の入力ミスの後コンソールが無効となります。

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 (4-16)

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します。"no"を前に置くことで初期設定に戻します。

文法

databits {7 | 8}

no databits

- 7 — 7データビット
- 8 — 8データビット

初期設定

8データビット

コマンドモード

Line Configuration

コマンド解説

パリティが生成されている場合は7データビットを、パリティが生成されていない場合(no parity)は8データビットを指定して下さい。

例

本例では7データビットに設定しています。

```
Console(config-line)#databits 7
Console(config-line)#
```

関連するコマンド

parity (4-18)

parity

パリティビットの設定に使用します。"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** — No parity
- **even** — Even parity
- **odd** — Odd parity

初期設定

No parity

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します。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（9600, 57600, 38400, 19200, 115200 bps）

初期設定

9600

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下さい。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

本例では57600bpsに設定しています。

```
Console(config-line)#speed 57600
Console(config-line)#
```

stopbits

送信するストップビットの値を指定します。"no"を前に置くことで初期設定に戻します。

文法

stopbits {1 | 2}

- 1 — ストップビット"1"
- 2 — ストップビット"2"

初期設定

ストップビット1

コマンドモード

Line Configuration

例

本例ではストップビット"2"に設定しています。

```
Console(config-line)#stopbits 2
Console(config-line)#
```

disconnect

本コマンドを使用しSSH、Telnet、コンソール接続を終了することができます。

文法

disconnect *session-id*

- *session-id* — SSH、Telnet、コンソール接続のセッション ID

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 (4-46)
show users (4-67)

show line

ターミナル接続の設定を表示します。

文法

show line [console | vty]

- console — コンソール接続設定
- vty — リモート接続用の仮想ターミナル設定

初期設定

すべてを表示

コマンドモード

Normal Exec, Privileged Exec

例

本例ではすべての接続の設定を表示しています。

```
Console#show line
 Console configuration:
  Password threshold: 3 times
  Interactive timeout: Disabled
  Login timeout: Disabled
  Silent time: Disabled
  Baudrate: 9600
  Databits: 8
  Parity: none
  Stopbits: 1

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

4-5 General Commands

コマンド	機能	モード	ページ
enable	Privilegedモードの有効化	NE	4-22
disable	PrivilegedモードからNormalモードへの変更	PE	4-23
configure	Global Configurationモードの有効化	PE	4-24
show history	コマンド履歴バッファの表示	NE, PE	4-24
reload	本機の再起動	PE	4-25
end	Privileged Execモードへの変更	GC, IC, LC, VC	4-25
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	4-26
quit	CLIセッションを終了	NE, PE	4-26
help	ヘルプの使い方を表示	すべて	NA
?	状況に応じたコマンドオプションを表示	すべて	NA

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P4-5「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、P4-31「enable password」を参照して下さい）
- Level 15 のみ利用することが可能です。Level 0 に対する設定は無効となります。

例

```
Console>enable
Password: [privileged level password]
Console#
```

関連するコマンド

disable (4-23)
enable password (4-31)

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P4-5「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 (4-22)

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P4-5「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 (4-25)

show history

保存されているコマンドの履歴を表示する際に利用します。

初期設定
なし

コマンドモード
Normal Exec, Privileged Exec

コマンド解説
本機に保存できるコマンド履歴はExecutionコマンドとConfigurationコマンドがそれぞれ最大10コマンドです。

例

本例では、コマンド履歴として保存されているコマンドを表示しています。

```
Console#show history
Execution command history:
 2 config
 1 show history

Configuration command history:
 4 interface vlan 1
 3 exit
 2 interface vlan 1
 1 end

Console#
```

"!"コマンドを用いると、履歴のコマンドを実行することが可能です。Normal又はPrivileged Execモード時にはExecutionコマンドを、Configurationモード時にはConfigurationコマンドの実行が行えます。

本例では、"!2"コマンドを入力することで、Executionコマンド履歴内の2番目のコマンド（"config"コマンド）を実行しています。

```
Console#!2
Console#config
Console(config)#
```

reload

システムの再起動を行う際に利用します。

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

システム全体の再起動を行います。

例

本機の再起動方法を示しています:

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

end

Privilegedモードに戻る際に利用します。

初期設定

なし

コマンドモード

Global Configuration
Interface Configuration
Line Configuration
VLAN Database Configuration

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

コマンド解説

"quit"、"exit"コマンドはどちらもConfigurationモードを終了する際に利用できます。

例

本例は、CLIセッションの終了を示しています。

```
Console#quit

Press ENTER to start session

User Access Verification

Username:
```

4-6 System Management Commands

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。

コマンドグループ	機能	ページ
Device Designation	本機を特定する情報設定	4-28
User Access	管理アクセス用ユーザ名及びパスワード設定	4-29
IP Filter	管理アクセスを許可するIPアドレスの設定	4-32
Web Server	Webブラウザ経由での管理アクセスの有効化	4-34
Telnet Server	Telnet経由での管理アクセスの有効化	4-37
Secure Shell	セキュリティを確保したSSH接続	4-38
Event Logging	エラーメッセージログ設定	4-48
SMTP Alert	SMTPアラートメッセージの設定	4-55
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	4-59
System Status	管理者やシステムバージョン、システム情報の表示	4-64
Frame Size	ジャンボフレームサポートの有効化	4-69

Device Designation Commands

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	4-28
hostname	ホスト名の設定	GC	4-29
snmp-server contact	システムコンタクト者の設定	GC	4-112
snmp-server location	システムロケーションの設定	GC	4-112

prompt

CLIプロンプトのカスタマイズを行うことができます。"no"を前に置くことで初期設定に戻ります。

文法

prompt *string*

no prompt

- *string* — CLI プロンプトに表示される名称（最大 255 文字）

初期設定

Console

コマンドモード

Global Configuration

例

```
Console(config)#prompt RD2
RD2(config)#
```

hostname

本機のホスト名の設定及び変更を行うことができます。"no"を前に置くことで初期設定に戻ります。

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)#
```

User Access Commands

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、P4-13「password」やP4-77「Authentication Sequence」、P4-87「802.1X Port Authentication」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	4-30
enable password	各アクセスレベルのパスワードの設定	GC	4-31

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 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

- アクセスレベル：Normal Exec
- ユーザ名とパスワード：

ユーザ名	アクセスレベル	パスワード
guest	0	guest
admin	15	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下さい。変更したパスワードは忘れないようにして下さい。

文法

enable password [level *level*] {0 | 7} *password*
no enable password [level *level*]

- **level** *level* — Privileged Exec へは Level 15 を入力します。（Level0-14 は使用しません）
- **{0 | 7}** — "0"は平文パスワードを、"7"は暗号化されたパスワードとなります。
- *password* — Privileged Exec レベルへのパスワード（最大 8 文字、大文字小文字は区別されます）

初期設定

- Level：15
- 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。P4-22"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 (4-22)
authentication enable (4-78)

IP Filter Commands

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	4-32
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	4-33

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うことができます。"no"を前に置くことで設定を削除します。

文法

management {all-client | http-client | snmp-client | telnet-client} *start-address* [*end-address*]
no management {all-client | http-client | snmp-client | telnet-client} *start-address* [*end-address*]

- **all-client** — SNMP/Web ブラウザ/Telnet クライアントの IP アドレス
- **http-client** — Web ブラウザクライアントの IP アドレス
- **snmp-client** — SNMP クライアントの IP アドレス.
- **telnet-client** — Telnet クライアントの IP アドレス
- *start-address* — IP アドレス又は IP アドレスグループの最初の IP アドレス
- *end-address* — IP アドレスグループの最後の IP アドレス

初期設定

全アドレス

コマンドモード

Global Configuration

コマンド解説

- 設定以外の無効な IP アドレスから管理アクセスに接続された場合、本機は接続を拒否し、イベントメッセージをシステムログに保存し、トラップメッセージの送信を行います。
- 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

本例では、表示されているIPアドレス及びIPアドレスグループからの接続を許可する設定を行っています。

```
Console(config)#management all-client 192.168.1.19
Console(config)#management all-client 192.168.1.25 192.168.1.30
Console(config)#
```

show management

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#
```

Web Server Commands

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	4-34
ip http server	管理用Webインタフェースの使用	GC	4-34
ip http secure-server	セキュアHTTP(HTTPS)サーバの使用	GC	4-35
ip http secure-port	HTTPS接続に使用するポートの設定	GC	4-36

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 (範囲：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 (4-34)

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 (4-34)

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)を使用します。"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 6.2 以上の

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 6.2以上	Windows 98、Windows NT （サービスパック6a）、Windows 2000、Windows XP、Solaris 2.6

※ セキュアサイト証明の詳細はP3-37「サイト証明書の設定変更」及びP4-71「copy」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 (4-36)
copy tftp https-certificate (4-71)

ip http secure-port

Webインタフェースからの HTTPS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 に使用する UDP ポート番号 (範囲：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 (4-35)

Telnet Server Commands

コマンド	機能	モード	ページ
ip telnet port	Telnetインタフェースに使用するポートの設定	GC	4-37
ip telnet server	管理用Telnetインタフェースの使用	GC	4-37

ip telnet port

Telnetインタフェースでアクセスする場合のTCPポート番号を指定します。"no"を前に置くことで初期設定に戻ります。

文法

ip telnet port *port-number*

no ip telnet port

- *port-number* — Telnet インタフェースに使用する TCP ポート
  (範囲：1-65535)

初期設定

23

コマンドモード

Global Configuration

例

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

関連するコマンド

ip telnet server (4-37)

ip telnet server

Telnetから本機の設定、及び設定情報の閲覧を可能にします。
"no"を前に置くことで本機能は無効となります。

文法

ip http server
no ip http server

初期設定

有効

コマンドモード

Global Configuration

例

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

関連するコマンド

ip telnet port (4-37)

Secure Shell Commands

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	4-41
ip ssh timeout	SSHサーバの認証タイムアウト設定	GC	4-42
ip ssh authentication-retries	クライアントに許可するリトライ数の設定	GC	4-42

ip ssh server-key size	SSHサーバキーサイズの設定	GC	4-43
copy tftp public-key	ユーザ公開キーのTFTPサーバから本機へのコピー	PE	4-71
delete public-key	特定ユーザの公開キーの削除	PE	4-44
ip ssh crypto host-key generate	ホストキーの生成	PE	4-44
ip ssh crypto zeroize	RAMからのホストキーの削除	PE	4-45
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	4-45
disconnect	ライン接続の終了	PE	4-20
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	4-46
show ssh	SSHセッション状態の表示	PE	4-46
show public-key	特定のユーザ又はホストの公開キーの表示	PE	4-47
show users	SSHユーザ、アクセスレベル、公開キータイプの表示	PE	4-67

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 156849954018676692593339467750546173253136748908365472541502024559319986854435836165199992332978176606583095610825913212890233765468017262725714134287629413011961955667825956641048695742788814620651941746772984865468615717739390164779355942303577413098022737087794545240839717526463580581767167095748047761 17

③ **クライアント公開キーの本機への取り込み** — P4-71"copy tftp public-key"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（クライアントは、3-32ページに解説しているUser Accounts画面でスイッチへの設定が行われていなくてはなりません）。クライアントへはこれらのキーを使用し、認証が行われます。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（例はRSA Version1キー）

1024 35 134108168560989392104094492015542534763164192187295892114317388005553616163105177594083868631109291232226828519254374603100937187721199696317813662774141689851320491172048303392543241016379975923714490119380060902539484084827178194372288402533115952134861022902978982721353267131629432532818915045306393916643 steve@192.168.1.19

④ **オプションパラメータの設定** — SSH設定画面で、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って下さい。

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

有効

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)#
```

関連するコマンド

ip ssh crypto host-key generate (4-44)
show ssh (4-46)

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（範囲：1-20 秒）

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 (4-15)
show ip ssh (4-46)

ip ssh authentication-retries

SSHサーバがユーザの再認証を行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、認証を行うことができる回数（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 (4-46)

ip ssh server-key size

SSHサーバキーサイズを設定します。"no"を前に置くことで初期設定に戻ります。

文法

ip ssh server-key size *key-size*

no ip ssh server-key size

- *key-size* — サーバキーのサイズ（設定範囲：512-896bits）

初期設定

768 bits

コマンドモード

Global Configuration

コマンド解説

- サーバキーはプライベートキーとなり本機以外との共有はしません。
- SSH クライアントと共有するホストキーサイズは1024bit に固定されています。

例

```
Console(config)#ip ssh server-key size 512
```

```
Console(config)#
```

delete public-key

特定のユーザパブリックキーを削除します。

文法

delete public-key *username* [**dsa** | **rsa**]

- *username* — SSH サーバ名（範囲：1-8 文字）
- dsa — DSA 公開キータイプ
- rsa — RSA 公開キータイプ

初期設定

DSA及びRSAキーの両方の削除

コマンドモード

Privileged Exec

例

```
Console#delete public-key admin dsa
Console#
```

ip ssh crypto host-key generate

パブリック及びプライベートのホストキーペアの生成を行います。

文法

ip ssh crypto host-key generate [**dsa** | **rsa**]

- **dsa** — DSA（バージョン 2）キータイプ
- **rsa** — RSA（バージョン 1）キータイプ

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 (4-45)
ip ssh save host-key (4-45)

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#
```

関連するコマンド

ip ssh crypto host-key generate (4-44)
ip ssh save host-key (4-45)
no ip ssh server (4-41)

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 [dsa | rsa]

- **dsa** — DSA キータイプ
- **rsa** — RSA キータイプ

初期設定

DSA及びRSAキーの両方を保存

コマンドモード

Privileged Exec

例

```
Console#ip ssh save host-key dsa
Console#
```

関連するコマンド

ip ssh crypto host-key generate (4-44)

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
Connection	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い設定します。 SSH v1.5の選択肢：DES, 3DES SSH v2.0の選択肢：client-to-server（ctos），server-to-client (stoc)に個別に設定が可能 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 (DESを3重にしたもの、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

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
156849954018676692593339467750546173253136748908365472541502024559 3
199868544358361651999923329781766065830958610825913212890233765468 0
172627257141342876294130119619556678259566410486957427888146206519 4
174677298486546861571773939016477935594230357741309802273708779454 5
240839717526463580581767167095748047761 17
DSA:
ssh-dss AAAB3NzaC1kc3MAAACBAPWKZTPbsRIB8ydEXcxM3dyV/yrDbKStIlnzD/
Dg0h2HxcYV44sXZ2JXhamLK6P8bvuiyacWbUWa4PAtp1KMSdqsKeh3hKoA3vRRSy1N2
XFfAKxl5fwFfvJlPdOkFgzLGMinvSNYQwiQXbKTBH0Z4mUZpE85PWxDZMaCNBPjBrRA
AAAFQChb4vsdfQGNIjwbvwrNLaQ77isiwAAAIEAsy5YWDC99ebYHNRj5kh47wY4i8cZ
vH+p9cnrfwFTMU01VFDly3IR2G395NLy5Qd7ZDxfA9mCOfTyyEfbobMJZi8oGCstSNO
xrZZVnMqWrTYfdrKX7YKBw/Kjw6Bm iFq7O+jAhf1Dg45loAc27s6TLdtny1wRq/
ow2eTCD5nekAAACBAJ8rMccXTxHLFAczWS7EjOyDbsloBfPuSAb4oAsyjKXKVYNLQkT
LZfcFRu41bS2KV5LAwecsigF+DjKGWtPNIQqabKgYCw2odVzX4Gg+yqdTlYmGA7fHGm
8ARGeiG4ssFKy4Z6DmYPXFum1Yg0fhLwuHpOSKdxT3kk475S7 w0W
Console#
```

Event Logging Commands

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	4-49
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	4-49
logging host	syslogを送信するホストのIPアドレスの設定	GC	4-50
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設定	GC	4-51
logging trap	リモートサーバへの重要度に基づいたsyslogメッセージの保存	GC	4-51
clear logging	ログバッファのクリア	PE	4-52

show logging	ログ関連情報の表示	PE	4-53
show log	ログメッセージの表示	PE	4-54

logging on

エラーメッセージのログを取ります。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 (4-49)
clear logging (4-52)

logging history

本体のメモリに保存するメッセージの種類を指定することができます。"no"を前に置くことで初期設定に戻します。

文法

logging history {flash | ram} *level*
no logging history {flash | ram}

- **flash** — フラッシュメモリに保存されたイベント履歴
- **ram** — RAM に保存されたイベント履歴

  level — レベルは以下の表の通りです。選択したLevelからLevel0までのメッセージが保存されます（選択したLevelは含まれます）

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

※ 現在のファームウェアではLevel 2, 5, 6のみサポートしています。

初期設定

- Flash：errors (level 3-0)
- RAM：warnings (level 6-0)

コマンドモード

Global Configuration

コマンド解説

フラッシュメモリには、RAMに設定するLevelより高いLevelを設定して下さい。

例

```
Console(config)#logging history ram 0
Console(config)#
```

logging host

ログメッセージを受け取るsyslogサーバのIPアドレスを設定します。
"no"を前に置くことでsyslogサーバを削除します。

文法

logging host *host_ip_address*
no logging host *host_ip_address*

- *host_ip_address* — syslog サーバの IP アドレス

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

- 複数の syslog サーバを指定する場合、一度に 1 つの syslog サーバの IP アドレスを指定し、複数回コマンドを実行して下さい。
- 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*

- *type* ― syslog サーバで使用する facility タイプの値を指定します。(範囲：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サーバへのメッセージ送信を有効にし、又送信するメッセージの種類を指定することができます。コマンド実行時にレベルを指

定しない場合、syslogサーバへのメッセージ送信を有効に設定できます。"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*

level — レベルは以下の表の通りです。選択したLevelからLevel0までのメッセージが送信されます（選択したLevelは含まれます）

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

初期設定

- 有効
- Level 6 – 0

コマンドモード

Global Configuration

コマンド解説

- レベルを指定することによって、syslog サーバへの送信を有効に設定し、選択した Level から Level0 までのメッセージが保存されます（選択した Level は含まれます）
- レベルを指定しない場合、syslog サーバへの送信を有効に設定し、保存されるメッセージレベルを初期設定に戻します。

例

```
Console(config)#logging trap 4
Console(config)#
```

clear logging

ログをバッファから削除します。

文法

clear logging [flash | ram]

- **flash** — フラッシュメモリに保存されたイベント履歴
- **ram** — RAM に保存されたイベント履歴

初期設定

Flash及びRAM

コマンドモード

Privileged Exec

例

```
Console#clear logging
Console#
```

関連するコマンド

show logging (4-53)

show logging

スイッチ本体、SMTPイベントハンドラ、リモートのsyslogサーバに送信される、イベントメッセージの設定情報を表示します。

文法

show logging {flash | ram | sendmail | trap}

- **flash** — フラッシュメモリに保存されたイベント履歴の設定
- **ram** — RAM に保存されたイベント履歴の設定
- **sendmail** — SMTP イベントハンドラの設定を表示(P4-59)
  FXC3126/52 のみ使用可能
- **trap** — syslog サーバに送信されたメッセージ

初期設定

なし

コマンドモード

Privileged Exec

例

本例では、syslogが有効で、フラッシュメモリのメッセージレベルは "errors" （初期値 3-0）、RAM へのメッセージレベルは "informational"（初期値6-0）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:           Enabled
History logging in FLASH: level errors
Console#show logging ram
Syslog logging:              Enabled
History logging in RAM: level informational
Console#
```

項目	解説
Syslog logging	logging onコマンドによりシステムログが有効化されているかを表示
History logging in FLASH	logging historyコマンドによるリポートされるメッセージレベル
History logging in RAM	logging historyコマンドによるリポートされるメッセージレベル

本例では、トラップ機能の設定を表示しています。

```
Console#show logging trap
Syslog logging:          Enabled
REMOTELOG status:         Enabled
REMOTELOG facility type:  local use 7
REMOTELOG level type:     Informational messages only
REMOTELOG server IP address: 0.0.0.0
REMOTELOG server IP address: 0.0.0.0
REMOTELOG server IP address: 0.0.0.0
REMOTELOG server IP address: 0.0.0.0
REMOTELOG server IP address: 0.0.0.0
Console#
```

項目	解説
Syslog logging	logging onコマンドによりシステムログが有効化されているかを表示
REMOTELOG status	logging trapコマンドによりリモートロギングが有効化されているかを表示
REMOTELOG facility type	logging facilityコマンドによるリモートサーバに送信されるsyslogメッセージのファシリティタイプ
REMOTELOG level type	logging trapコマンドによるリモートサーバに送信されるsyslogメッセージのしきい値
REMOTELOG server IP address	logging hostコマンドによるsyslogサーバのIPアドレス

関連するコマンド

show logging sendmail (4-59)

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] [tail]

- **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
- **tail** —最新の履歴から表示

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 (P4-49)、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#
```

SMTP Alert Commands

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（FXC3126/52）	GC	4-56
logging sendmail level	アラートメッセージのしきい値設定（FXC3126/52）	GC	4-57

logging sendmail source-email	メールの"From"行に入力されるアドレスの設定（FXC3126/52）	GC	4-57
logging sendmail destination-email	メール受信者の設定（FXC3126/52）	GC	4-58
logging sendmail	SMTPイベントハンドリングの有効化（FXC3126/52）	GC	4-58
show logging sendmail	SMTPイベントハンドラ設定の表示（FXC3126/52）	NE, PE	4-59

logging sendmail host

FXC3126/52のみ使用可能なコマンドです。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

None

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

FXC3126/52のみ使用可能なコマンドです。アラートメッセージのしきい値の設定を行います。

文法

logging sendmail level *level*

- *level* — システムメッセージレベル(P4-49)。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（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

レベル4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 4
Console(config)#
```

logging sendmail source-email

FXC3126/52のみ使用可能なコマンドです。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（範囲：0-41 文字）

初期設定

None

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

本例では送信者名にjohn@acme.comを指定します。

```
Console(config)#logging sendmail source-email bill@hoge.com
Console(config)#
```

logging sendmail destination-email

FXC3126/52のみ使用可能なコマンドです。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（範囲：1-41 文字）

初期設定

None

コマンドモード

Global Configuration

コマンド解説

最大5つのアドレスを指定することができます。複数のアドレスを設定する際はアドレス毎にコマンドを入力して下さい。

例

```
Console(config)#logging sendmail destination-email
ted@this-company.com
Console(config)#
```

logging sendmail

FXC3126/52のみ使用可能なコマンドです。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

有効

コマンドモード

Global Configuration

例

```
Console(config)#logging sendmail
Console(config)#
```

show logging sendmail

FXC3126/52のみ使用可能なコマンドです。SMTPイベントハンドラの設定を表示します。

コマンドモード

Normal Exec, Privileged Exec

例

```
Console#show logging sendmail
SMTP servers
-----------------------------------------------
   1. 192.168.1.200
SMTP minimum severity level:  4
SMTP destination email addresses
-----------------------------------------------
   1. ted@this-company.com
SMTP source email address:   john@acme.com
SMTP status:                 Enabled
Console#
```

Time Commands

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うことができます。本機に正確な時刻を設定すると、システムログ機能によるイベントの保存時に、重要な項目である日時を保存できるようになります。システム時刻を設定しない場合、直前の起動時の時刻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。

コマンド	機能	モード	ページ
sntp client	特定のタイムサーバからの時刻の取得	GC	4-60
sntp server	タイムサーバの指定	GC	4-60
sntp poll	リクエスト送信間隔の設定	GC	4-61
show sntp	SNTP設定の表示	NE, PE	4-62
clock timezone	本機内部時刻のタイムゾーンの設定	GC	4-62
calendar set	システム日時の設定	PE	4-63
show calendar	現在の時刻及び設定の表示	NE, PE	4-63

sntp client

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 (4-60)
sntp poll (4-61)
show sntp (4-62)

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 *[ip1 [ip2 [ip3]]]*

- *ip* — NTP/SNTP タイムサーバの IP アドレス（範囲：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(config)#
```

関連するコマンド

sntp client (4-60)
sntp poll (4-61)
show sntp (4-62)

sntp poll

SNTPクライアントモード時に時刻同期要求の送信間隔を設定します。"no"を前に置くことで初期設定に戻します。

文法

sntp poll *seconds*

no sntp poll

- *seconds* — リクエスト間隔（範囲：16-16384 秒）

初期設定

16秒

コマンドモード

Global Configuration

例

```
Console(config)#sntp poll 60
Console(config)#
```

関連するコマンド

sntp client (4-60)

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SNMPモード（ユニキャスト等）を表示します。

例

```
Console#show sntp
Current time: Dec 23 05:13:28 2002
Poll interval: 16
Current mode: unicast
SNTP status : Enabled
SNTP server 137.92.140.80 0.0.0.0 0.0.0.0
Current server: 137.92.140.80
Console#
```

clock timezone

本機内部時刻のタイムゾーンの設定を行います。

文法

clock timezone *name* **hour** *hours* **minute** *minutes* {**before-utc** | **after-utc**}

- *name* — タイムゾーン名（範囲：1-29 文字）
- *hours* — UTC との時間差（時間）（範囲：0-12 時間）
- *minutes* — UTC との時間差（分）（範囲：0-59 分）
- *before-utc* — UTC からのタイムゾーンの時差がマイナスの（UTC より早い）場合
- *after-utc* — UTCからのタイムゾーンの時差がプラスの（UTC より遅い）場合

初期設定

なし

コマンドモード

Global Configuration

コマンド解説

SNTPではUTC(Coordinated Universal Time：協定世界時間。別名：GMT/Greenwich Mean Time)を使用します。
本機を設置している現地時間に対応させて表示するためにUTCからの時差（タイムゾーン）の設定を行う必要があります。

例

```
Console(config)#clock timezone Japan hours 8 minute 0 after-UTC
Console(config)#
```

関連するコマンド

show sntp (4-62)

calendar set

システム時刻の設定を行います。ネットワークでタイムサーバを使用していない場合、又はタイムサーバからの受信設定をしない場合に使用します。

文法

calendar set *hour min sec {day month year | month day year}*

- *hour* — 時間（範囲：0-23）
- *min* — 分（範囲：0-59）
- *sec* — 秒（範囲：0-59）
- *day* — 日付（範囲：1-31）
- *month* — 月：january | february | march | april | may | june | july | august | september | october | november | december
- *year* — 年（西暦 4 桁、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15:12:34, April 1st, 2004に設定しています。

```
Console#calendar set 15:12:34 1 April 2004
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 set
15:12:45 April 1 2004
Console#
```

System Status Commands

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	4-64
show running-config	実行中の設定ファイルの表示	PE	4-65
show system	システム情報の表示	NE, PE	4-67
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	4-67
show version	システムバージョン情報の表示	NE, PE	4-68

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します。

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

- 実行中の設定ファイルと、起動用ファイルの内容を比較する場合には"**show running-config**"コマンドを一緒に使用して下さい。
- キーコマンドモードの設定が表示されます。各モードのグループは"**!**"によって分けられて configuration モードと対応するモードが表示されます。このコマンドでは以下の情報が表示されます：

－SNMP コミュニティ名
－ユーザ（ユーザ名及びアクセスレベル）
－VLAN データベース（VLAN ID、VLAN 名及び状態）
－各インタフェースの VLAN 設定状態
－本機の IP アドレス設定
－スパニングツリー設定
－コンソール及び Telnet に関する設定

例

```
Console#show startup-config
building startup-config, please wait.....
!!
username admin access-level 15
username admin password 0 admin
!
username guest access-level 0
username guest password 0 guest
!
enable password level 15 0 super
!
snmp-server community public ro
snmp-server community private rw
!
logging history ram 6
logging history flash 3
!
vlan database
 vlan 1 name DefaultVlan media ethernet state active
!
interface ethernet 1/1
 switchport allowed vlan add 1 untagged
 switchport native vlan 1
...
interface vlan 1
ip address dhcp
!
line console
!
line VTY
!
end
Console#
```

関連するコマンド

show running-config (4-65)

show running-config

現在実行中の設定ファイルを表示します。

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

- 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）
  －イベントログの設定
  －VLAN データベース（VLAN ID、VLAN 名及び状態）
  －各インタフェースの VLAN 設定状態
  －本機の IP アドレス設定
  －IP precedence の設定
  －コンソール及び Telnet に関する設定

例

```
Console#show running-config
building running-config, please wait.....
!
phymap 00-30-f1-d3-26-00
!
SNTP server 0.0.0.0 0.0.0.0 0.0.0.0
!
clock timezone hours 0 minute 0 after-UTC
!
SNMP-server community private rw
SNMP-server community public ro
!!
username admin access-level 15
username admin password 7 21232f297a57a5a743894a0e4a801fc3
username guest access-level 0
username guest password 7 084e0343a0486ff05530df6c705c8bb4
enable password level 15 7 1b3231655cebb7a1f783eddf27d254ca
!!
logging history ram 6
logging history flash 3
!
vlan database
 vlan 1 name DefaultVlan media ethernet state active
!!
interface ethernet 1/1
 switchport allowed vlan add 1 untagged
 switchport native vlan 1
...!
interface vlan 1
 IP address DHCP
!!
no map IP precedence
no map IP DSCP
!!
line console
!
line VTY
!
end
!
Console#
```

関連するコマンド

show startup-config (4-64)

show system

システム情報を表示します。

初期設定

なし

コマンドモード

Normal Exec, Privileged Exec

コマンド解説

- コマンドを使用して表示された内容に関しての詳細はP3-10「システム情報の表示」を参照して下さい。
- "POST result"は正常時にはすべて"PASS"と表示されます。"POST result"に"FAIL"があった場合には販売店、又はサポートまで連絡して下さい。

例

```
Console#show system
System description: FastEthernetSwitch 10/100 FXC3126 Manager
System OID string: 1.3.6.1.4.1.202.20.46
System information
 System Up time:            3 hours, 0 minutes, and 7.18 seconds
 System Name:               [NONE]
 System Location:           [NONE]
 System Contact:            [NONE]
 MAC address:               00-30-F1-D3-26-00
 Web server:                enabled
 Web server port:           80
 Web secure server:         enabled
 Web secure server port:    443
 Telnet server           :  enable
 Telnet port             :  23
 Jumbo Frame  :             Disabled
 POST result
DUMMY Test 1.................PASS
UART LOOP BACK Test..........PASS
DRAM Test....................PASS
Timer Test...................PASS
Switch Int Loopback test.....PASS

Done All Pass.
Console#
```

show users

コンソール及びTelnetで接続されているユーザの情報を表示します。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

表示される情報に関する詳細はP3-10「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: A419048860
 Service tag:
 Hardware version: R0B
 Module A type: 1000BaseT
 Module B type: 1000BaseT
Number of ports: 26
 Main power status: up
 Redundant power status: not present

Agent(master)
 Unit ID: 1
 Loader version: 2.2.1.4
 Boot ROM version: 2.2.1.9
 Operation code version: 2.2.6.3
Console #
```

Frame Size Commands

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	4-69

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すべ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毎秒 64 パケットに制限されます（詳細は、P4-123 の"switchport broadcast"コマンドを参照して下さい）

例

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

4-7 Flash/File Commands

ここで解説するコマンドはシステムコードや設定ファイルの管理を行うためのコマンドです。

コマンド	機能	モード	ページ
copy	コードイメージや設定ファイルのフラッシュメモリへのコピーやTFTPサーバ間のコピー	PE	4-71
delete	ファイルやコードイメージの削除	PE	4-73
dir	フラッシュメモリ内のファイル一覧の表示	PE	4-74
whichboot	起動ファイルの表示	PE	4-75
boot system	システム起動ファイル､イメージの設定	GC	4-76

copy

コードイメージのアップロード、ダウンロードや設定ファイルの本機、TFTPサーバ間のアップロード、ダウンロードを行います。
コードイメージや設定ファイルをTFTPサーバに置いてある場合には、それらのファイルを本機にダウンロードしシステム設定等を置き換えることができます。ファイル転送はTFTPサーバの設定やネットワーク環境によっては失敗する場合があります。

文法

copy *file* **{file | running-config | startup-config | tftp}**
copy running-config {file | startup-config | tftp}
copy startup-config {file | running-config | tftp}
copy tftp {file | running-config | startup-config | https-certificate | public-key}

- *file* — ファイルのコピーを可能にするキーワード
- **running-config** — 実行中の設定をコピーするキーワード
- **startup-config** — システムの初期化に使用する設定
- **tftp** — TFTP サーバからのコピーを行うキーワード
- **https-certificate** — TFTP サーバ間の HTTPS 認証をコピー
- **public-key** — TFTPサーバから SSH キーをコピー（詳細は、P4-38 の"Secure Shell"コマンドを参照）

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

- データをコピーするために完全なコマンドの入力が必要です。
- ファイル名は大文字と小文字が区別されます。ファイル名にはスラッシュ及びバックスラッシュは使用できません。ファイル名の最初の文字にピリオド(.)は使用できません。ファイル名の長さは TFTP サーバ上では 137 文字以下、本機上は 31 文字以下となります（ファイル名に使用できる文字は A-Z, a-z, 0-9, "." , "-", "_"です）
- フラッシュメモリ容量の制限により、オペレーションコードは 2 つのみ保存可能です。
- ユーザ設定ファイル数はフラッシュメモリの容量に依存します。
- "Factory_Default_Config.cfg"を使用し、工場出荷時設定をコピー元にすることはできますが、" Factory_Default_Config.cfg" をコピー先に指定することはできません。
- 起動時の設定を変更するためには"startup-config"をコピー先にする必要があります。
- ブート ROM イメージは TFTP サーバからのアップロード及びダウンロードはできません。ブート ROM または診断用イメージのダウンロードを行うためには新規のファームウェアに関するリリースノートの解説か、又は代理店の指示に従う必要があります。
- "http-certificate"の設定については、P3-37 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、P4-35 の"ip http secure-server"コマンドの解説を参照して下さい。

例

本例では、TFTPサーバを利用した設定ファイルのアップロードを示しています。

```
Console#copy file tftp
Choose file type:
1. config: 2. opcode: <1-2>: 1
Source file name: startup
TFTP server ip address: 10.1.0.99
Destination file name: startup.01
TFTP completed.
Success.

Console#
```

本例では実行ファイルのスタートアップファイルへのコピーを示しています。

```
Console#copy running-config file
destination file name: startup
Write to FLASH Programming.
\Write to FLASH finish.
Success.

Console#
```

本例では、設定ファイルのダウンロード方法を示しています。

```
Console#copy tftp startup-config
TFTP server ip address: 10.1.0.99
Source configuration file name: startup.01
Startup configuration file name [startup]:
Write to FLASH Programming.

\Write to FLASH finish.
Success.

Console#
```

本例では、TFTPサーバのセキュアサイト承認を示しています。承認を完了するため、再起動を行っています。

```
Console#copy tftp https-certificate
TFTP server ip address: 10.1.0.19
Source certificate file name: SS-certificate
Source private file name: SS-private
Private password: ********

Success.
Console#reload
System will be restarted, continue <y/n>? y
```

本例では、TFTPサーバからSSHで使用するための公開キーをコピーしています。SSHによる公開キー認証は、本機に対して設定済みのユーザに対してのみ可能であることに注意して下さい。

```
Console#copy tftp public-key
TFTP server IP address: 192.168.1.19
Choose public key type:
 1. RSA: 2. DSA: <1-2>: 1
Source file name: steve.pub
Username: steve
TFTP Download
Success.
Write to FLASH Programming.
Success.
Console#
```

delete

ファイルやイメージを削除する際に利用します。

文法

delete *filename*

- *filename* — 設定ファイル又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 (4-74)

delete public-key (4-44)

dir

フラッシュメモリ内のファイルの一覧を表示させる際に利用します。

文法

dir [boot-rom | config | opcode [:*filename*]]

表示するファイル、イメージタイプは以下のとおりです:

- **boot-rom** — ブート ROM 又は、診断イメージファイル
- **config** — 設定ファイル
- **opcode** — Run-time operation code イメージファイル
- *filename* — ファイル又はイメージ名。ファイルが存在してもファイル内にエラーがある場合には表示できません。

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

- パラメータを入力せずに"dir"コマンドのみを入力した場合にはすべてのファイルが表示されます。

- 表示されるファイルの情報は以下の表の通りです：

項目	内容
file name	ファイル名
file type	ファイルタイプ：Boot-Rom、Operation Code、Config file
startup	起動時に使用されているかどうか
size	ファイルサイズ(byte)

例

本例は、すべてのファイル情報の表示を示しています。

```
Console#dir
           file name          file type      startup size (byte)
---------------------------- -------------- ------- -----------
 Unit1:
   Diag_V2.2.1.3.bix          Boot-Rom image  Y        196020
   V2.1.5.4.bix               Operation Code  N       1745120
   V2.2.2.2.bix               Operation Code  Y       1745500
   Factory_Default_Config.cfg Config File     N          5013
   startup                    Config File     Y          6023
-------------------------------------------------------------------
                                      Total free space:   340787
Console#
```

whichboot

本機の起動時に使用されるシステム起動ファイルを表示します。

文法

whichboot

初期設定

なし

コマンドモード

Privileged Exec

例

本例では"whichboot"コマンドを使用したシステム起動ファイルの一覧の表示を示しています。

このコマンドを使用して表示される各項目に関しては前ページの"dir"コマンドの説明を参照して下さい。

```
Console#whichboot
           file name          file type       startup  size (byte)
---------------------------- --------------  -------  -----------
  Unit1:
     Diag_V2.2.1.3.bix         Boot-Rom image Y          196020
     V2.2.2.2.bix              Operation Code Y         1745500
     startup                   Config File    Y            6023
-------------------------------------------------------------------
                                         Total free space: 340787
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** — Run-time operation code

コロン(:)は必ず必要です。

- *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

- ファイルタイプの後にはコロン(:)が必ず必要です。
- 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 (4-74)

whichboot (4-75)

4-8 Authentication Commands

システム管理のためのユーザログインはローカル及び認証サーバを用いたユーザ認証が利用可能です。
また、IEEE802.1Xを利用したポートベース認証によるユーザのネットワークへのアクセス管理も可能です。

コマンドグループ	機能	ページ
Authentication Sequence	ログイン認証方式と優先順位の設定	4-77
RADIUS Client	RADIUSサーバ認証の設定	4-79
TACACS+ Client	TACACS+サーバ認証の設定	4-83
Port Security	ポートへのセキュアアドレスの設定	4-85
Port Authentication	IEEE802.1Xによるポート認証の設定	4-87

Authentication Sequence

コマンド	機能	モード	ページ
authentication login	認証方式と優先順位の設定	GC	4-77
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	4-78

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+ログイン認証はコンソール接続、Web インタフェース、Telnet のすべてに対応しています。接続オプションは認証サーバ側で設定することができます。
- 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 (4-30) ― ローカルのユーザ名及びパスワードの設定

authentication enable

"enable"コマンド（P4-22）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+ログイン認証はコンソール接続、Web インタフェース、Telnet のすべてに対応しています。接続オプションは認証サーバ側で設定することができます。
- 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 (4-31) ― コマンドモード変更のためのパスワードの設定

RADIUS Client

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	4-80
radius-server port	RADIUSサーバのポートの設定	GC	4-81

radius-server key	RADIUS暗号キーの設定	GC	4-81
radius-server retransmit	リトライ回数の設定	GC	4-82
radius-server timeout	認証リクエストの間隔の設定	GC	4-82
show radius-server	RADIUS関連設定情報の表示	PE	4-83

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 host *index* **host** {*host_ip_address* | *host_alias*} [**auth-port** *auth_port*] [**timeout** *timeout*] [**retransmit** *retransmit*] [**key** *key*]
no radius-server host *index* **host** {*host_ip_address* | *host_alias*} [**auth-port** *auth_port*] [**timeout** *timeout*] [**retransmit** *retransmit*] [**key** *key*]

- *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
- *host_alias* — RADIUS サーバの名前（最大 20 文字）
- *port_number* — RADIUS サーバの認証用 UDP ポート番号（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
- timeout：5
- 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 port

RADIUS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

radius-server port *port_number*

no radius-server port

- *port_number* — RADIUSサーバの認証用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 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 20 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

```
Remote RADIUS server configuration:

Global settings
 Communication key with RADIUS server:
 Server port number: 1812
 Retransmit times: 2
 Request timeout: 5

Sever 1:
 Server IP address: 192.168.1.1
 Communication key with RADIUS server: *****
 Server port number: 181
 Retransmit times: 2
 Request timeout: 5

Console#
```

TACACS+ Client

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	4-84
tacacs-server port	TACACS+サーバのポートの設定	GC	4-84
tacacs-server key	TACACS+暗号キーの設定	GC	4-85
show tacacs-server	TACACS+関連設定情報の表示	GC	4-85

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 host *host_ip_address*

no tacacs-server host

- *host_ip_address* — TACACS+サーバの IP アドレス

初期設定

10.11.12.13

コマンドモード

Global Configuration

例

```
Console(config)#tacacs-server host 192.168.1.25
Console(config)#
```

tacacs-server port

TACACS+サーバの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 20 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)#
```

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:
 Server IP address: 10.11.12.13
 Communication key with TACACS server: *****
 Server port number: 49
Console#
```

Port Security Commands

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	4-86
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	4-145
show mac-address-table	フォーワディングデータベースのエントリの表示	PE	4-147

port security

ポートへのポートセキュリティを有効に設定します。キーワードを使用せず"no"を前に置くことでポートセキュリティを無効にします。キーワードと共に"no"を前に置くことで侵入動作及び最大MACアドレス登録数を初期設定に戻します。

文法

port security [action {shutdown | trap | trap-and-shutdown} | max-mac-count *address-count*]

no port security [action | *max-mac-count*]

- **action** — ポートセキュリティが破られた場合のアクション
  －shutdown — ポートを無効
  －trap — SNMP トラップメッセージの発行
  －trap-and-shutdown — SNMP トラップメッセージを発行しポートを無効
- max-mac-count
  －*address-count* — ポートにおいて学習するMACアドレスの最大値（範囲：0-1024）

初期設定

- Status：無効(Disabled)
- Action：なし
- Maximum Addresses：0

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- ポートセキュリティを有効にした場合、本機は設定した最大学習数に達すると、有効にしたポートで MAC アドレスの学習を行わなくなります。すでにアドレステーブルに登録済みの MAC アドレスのデータのみがアクセスすることができます。
- まず"**port security max-mac-count**"コマンドを使用して学習するアドレス数を設定し、"**port security**"コマンドでポートのセキュリティを有効に設定します。
- ポートセキュリティを無効に設定し、最大アドレス学習数を初期設定値に戻すには、"**no port security max-mac-count**"コマンドを使用します。
- 新しい VLAN メンバーを追加する場合には、MAC アドレスを"**mac-address-table static**"コマンドを使用します。
- セキュアポートには以下の制限があります：
  —ポートミラーリングは使用できません。
  —複数の VLAN に所属できません。
  —ネットワークを相互接続するデバイスには接続できません。
  —トランクグループに加えることはできません。
- ポートセキュリティが機能しポートを無効にした場合、"**no shutdown**"コマンドを使用し、手動で再度有効にする必要があります。

例

本例では、5番ポートにポートセキュリティとポートセキュリティ動作を設定しています。

```
Console(config)#interface ethernet 1/5
Console(config-if)#port security action trap
```

関連するコマンド

shutdown (4-123)
mac-address-table static (4-145)
show mac-address-table (4-147)

802.1X Port Authentication

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	4-88
dot1x default	dot1xの設定値をすべて初期設定に戻す	GC	4-89
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	IC	4-89
dot1x port-control	ポートへのdot1xモードの設定	IC	4-89
dot1x operation-mode	dot1xポートへの接続可能ホスト数の設定	IC	4-90
dot1x re-authenticate	特定ポートへの再認証の強制	PE	4-91
dot1x re-authentication	全ポートへの再認証の強制	IC	4-91
dot1x timeout quiet-period	max-reqを越えた後、クライアントの応答を待つ時間	IC	4-92
dot1x timeout re-authperiod	接続済みクライアントの再認証間隔の設定	IC	4-92
dot1x timeout tx-period	認証中のEAPパケットの再送信間隔の設定	IC	4-93
show dot1x	dot1x関連情報の表示	PE	4-93

dot1x system-auth-control

スイッチが、802.1Xポート認証を使用できるよう設定します。"no"を前に置くことで初期設定に戻します。

文法

dot1x system-auth-control
no dot1x system-auth-control

初期設定

無効（Disabled）

コマンドモード

Global Configuration

例

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

dot1x default

すべてのdot1xの設定を初期設定に戻します。

文法

dot1x default

コマンドモード

Global Configuration

例

```
Console(config)#dot1x default
Console(config)#
```

dot1x max-req

ユーザ認証のタイムアウトまでのクライアントへのEAPリクエストパケットの最大送信回数の設定を行います。"no"を前に置くことで初期設定に戻します。

文法

dot1x max-req *count*

no dot1x max-req

- *count* — 最大送信回数（範囲：1-10）

初期設定

2

コマンドモード

Interface Configuration

例

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x max-req 2
Console(config-if)#
```

dot1x port-control

ポートに対してdot1xモードの設定を行います。

文法

dot1x port-control {auto | force-authorized | force-unauthorized}
no dot1x port-control

- **auto** — dot1x対応クライアントに対してRADIUSサーバによる認証を要求します。dot1x非対応クライアントからのアクセスは許可しません。
- **force-authorized** — dot1x対応クライアントを含めたすべてのクライアントのアクセスを許可します。
- **force-unauthorized** — dot1x対応クライアントを含めたすべてのクライアントのアクセスを禁止します。

初期設定

force-authorized

コマンドモード

Interface Configuration

例

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x port-control auto
Console(config-if)#
```

dot1x operation-mode

IEEE802.1x認証ポートに対して1台もしくは複数のホスト（クライアント）の接続を許可する設定を行います。キーワードなしで"no"を前に置くことで初期設定に戻ります。" multi-host max-count"キーワードと共に"no"を前に置くことで複数ホスト時の初期値5となります。

文法

dot1x operation-mode {single-host | multi-host [max-count *count*]}
no dot1x operation-mode [multi-host max-count]

- single-host — ポートへの 1 台のホストの接続のみを許可
- multi-host — ポートへの複数のホストの接続を許可
- max-count — 最大ホスト数
  －count — ポートに接続可能な最大ホスト数（設定範囲：1-1024、初期設定：5）

初期設定

Single-host

コマンドモード

Interface Configuration

コマンド解説

- "max-count"パラメータは"dot1x port-control"コマンド(P4-89)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*]

- *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#dot1x re-authenticate
Console#
```

dot1x re-authentication

全ポートでの周期的な再認証を有効にします。"no"を前に置くことで再認証を無効にします。

文法

dot1x re-authentication

no dot1x re-authentication

コマンドモード

Interface Configuration

例

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x re-authentication
Console(config-if)#
```

dot1x timeout quiet-period

EAPリクエストパケットの最大送信回数を過ぎた後、新しいクライアントの接続待機状態に移行するまでの時間を設定します。"no"を前に置くことで初期設定に戻します。

文法

dot1x timeout quiet-period *seconds*

no dot1x timeout quiet-period *seconds*

- *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)#
```

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*]

- *statistics* — 各ポートの 802.1X の状態を表示
- *interface*
  - **ethernet** *unit/port*
    - *unit* — ユニット番号"1"
    - *port* — ポート番号（範囲：1-16/26/52）

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 — dot1x operation-mode (P4-90)の設定値
  －Mode — dot1x port-control で設定する dot1x モード(P4-89)
  －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(P4-91)
  －reauth-period – 接続されたクライアントに再認証を要求する間隔(P4-92)
  －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(P4-92)
  －tx-period – 認証時に EAP パケットの再送信を行う間隔(P4-93)
  －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(P4-89)
  －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(P4-90)
  －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(P4-89)
  －Supplicant – 認証されたクライアントの MAC アドレス
  －Current Identifier – 認証機能により、現行の認証接続を識別するために使用された整数値(0-255)
- *Authenticator State Machine* —
  －State — 現在の状態(initialize, disconnected, connecting, authenticating, authenticated, aborting, held, force_authorized, force_unauthorized)
  －Reauth Count — 再認証回数
- *Backend State Machine* —
  －State — 現在の状態(request, response, success, fail, timeout, idle, initialize)
  －Request Count — クライアントからの応答がない場合に送信される EAP リクエストパケットの送信回数
  －Identifier(Server) — 直近の EAP の成功/失敗又は認証サーバから受信したパケット

- *Reauthentication State Machine* —
  －State — 現在の状態(initialize, reauthenticate)

例

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

802.1X Port Summary

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

802.1X Port Details

802.1X is disabled on port 1/1

802.1X is enabled on port 1/2
 reauth-enabled: Enable
 reauth-period:  1800
 quiet-period:    30
 tx-period:      40
 supplicant-timeout:    30
 server-timeout: 10
 reauth-max:     2
 max-req:         5

Status              Authorized
Operation mode       Single-Host
Max count            5
Port-control         Auto
Supplicant           00-00-e8-49-5e-dc
Current Identifier   3
Authenticator State Machine
State               Authenticated
Reauth Count         0

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

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

4-9 Access Control List (ACL) Commands

Access Control Lists (ACL)は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によるIPパケットへのパケットフィルタリング及び、MACアドレス及びイーサネットタイプによるすべてのフレームに対するパケットフィルタリングを提供します。入力されるパケットのフィルタリングを行うには、初めにアクセスリストを作成し、必要なルールを追加し、ルールの優先順位を決めるためマスクの作成を行います。その後、リストに特定のポートをバインドします。

Access Control Lists

ACLはIPアドレス、MACアドレス、又は他の条件と一致するパケットに対して許可(Permit)又は拒否(Deny)するためのリストです。本機では入力パケットに対してACLと一致するかどうか1個ずつ確認を行います。パケットが許可ルールと一致した場合には直ちに通信を許可し、拒否ルールと一致した場合にはパケットを落とします。リスト上の許可ルールに一致しない場合、パケットは落とされ、リスト上の拒否ルールに一致しない場合、パケットは通信を許可されます。

本機には3つのフィルタリングモードがあります。

- Standard IP ACL mode (STD-ACL) — ソース IP アドレスに基づくフィルタリングを行う IP ACL モード
- Extended IP ACL mode (EXT-ACL) — ソース又はディスティネーション IP アドレス、プロトコルタイプ、TCP/UDP ポート番号、TCP コントロールコードに基づくフィルタリングを行う IP ACL モード
- MAC ACL mode (MAC-ACL) — 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う MAC ACL モード

ACLは以下の制限があります。

- 各 ACL は最大 32 ルールまで設定可能です。
- 最大 ACL 設定数は 88 個です。
- 但し、リソースの制限により、ポートに結び付けられた規則の数の平均は 20 を超えないようにして下さい。
- 本機は ingress（入力）ACL のみをサポートしています。1 個の IP ACL を任意のポートに、1 個の MAC ACL をイングレスフィルタリング全体にバインドできます。

有効なACLは以下の順番で実行されます。

1. 入力ポートの入力MAC ACLのユーザに定義されたルール

2. 入力ポートの入力IP ACLのユーザに定義されたルール
3. 入力ポートの入力IP ACLのデフォルトルール(permit any any)
4. 入力ポートの入力MAC ACLのデフォルトルール(permit any any)
5. 明確なルールに一致しない場合、暗黙のデフォルトルール(permit all)

コマンドグループ	機能	ページ
IP ACLs	IPアドレス、TCP/UDPポート番号、TCPコントロールコードに基づくACLの設定	4-97
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	4-105
ACL Information	ACL及び関連するルールの表示。各ポートのACLの表示	4-110

IP ACLs

コマンド	機能	モード	ページ
access-list ip	IP ACLの作成とconfiguration modeへの移行	GC	4-98
permit, deny	ソースIPアドレスが一致するパケットのフィルタリング	STD-ACL	4-98
permit, deny	ソース又はディスティネーションIPアドレス、プロトコルタイプ、TCP/UDPポート番号、TCPコントロールコードに基づくフィルタリング	EXT-ACL	4-99
show ip access-list	設定済みIP ACLのルールの表示	PE	4-101
ip access-group	IP ACLへのポートの追加	IC	4-102
show ip access-group	IP ACLに指定したポートの表示	PE	4-103
map access-list ip	ACLルールと一致するパケットへの出力キューのCoS値の設定	IC	4-103
show map access-list ip	インタフェースのアクセスリストにマッピングされたCoS値の表示	PE	4-104

access-list ip

IP ACLを追加し、スタンダード又は拡張IP ACLの設定モードに移行します。"no"を前に置くことで特定のACLを削除します。

文法

access-list ip {standard | extended} *acl_name*
no access-list ip {standard | extended} *acl_name*

- **standard** — ソース IP アドレスに基づくフィルタリングを行う ACL
- **extended** — ソース又はディスティネーション IP アドレス、プロトコルタイプ、TCP/UDP ポート番号、TCP コントロールコードに基づくフィルタリングを行う ACL
- *acl_name* — ACL 名（最大文字数：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 ip standard david
Console(config-std-acl)#
```

関連するコマンド

permit, deny (4-98)
ip access-group (4-102)
show ip access-list (4-101)

permit, deny (Standard ACL)

スタンダードIP ACLルールを追加します。本ルールでは特定のソースIPアドレスからのパケットへのフィルタリングが行えます。"no"を前に置くことでルールを削除します。

文法

{**permit** | **deny**} {**any** | *source bitmask* | **host** *source*}

no {**permit** | **deny**} {**any** | *source bitmask* | **host** *source*}

- **any** — すべての IP アドレス
- *source* — ソース IP アドレス
- *bitmask* — 一致するアドレスビットを表す 10 進数値
- **host** — 特定の IP アドレスを指定

初期設定

なし

コマンドモード

Standard ACL

コマンド解説

- 新しいルールはリストの最後に追加されます。
- アドレスビットマスクはサブネットマスクと似ており、4 つの 0-255 の値で表示され、それぞれがピリオド(.)により分割されています。2進数のビットが"1"の場合、一致するビットであり、"0"の場合、拒否するビットとなります。ビットマスクはビット毎に特定の IP アドレスと共に使用し、ACL が指定した入力 IP パケットのアドレスと比較されます。

例

本例では、10.1.1.21のソースアドレスへの許可(permit)ルールとビットマスクを使用した168.92.16.x-168.92.31.xまでのソースアドレスへの許可(permit)ルールを設定しています。

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

関連するコマンド

access-list ip (4-98)

permit, deny (Extended ACL)

拡張IP ACLへのルールの追加を行います。ソース又はディスティネーションIPアドレス、プロトコルタイプ、TCP/UDPポート番号、TCPコントロールコードに基づくフィルタリングを行います。"no"を前に置くことでルールの削除を行います。

文法

[no] {permit | deny} [*protocol-number* | udp]
{any | *source address-bitmask* | host *source*}
{any | *destination address-bitmask* | host *destination*}
[precedence *precedence*] [tos *tos*] [dscp *dscp*]
[source-port *sport* [*end*]] [destination-port *dport* [*end*]]
[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* [*end*]] [destination-port *dport* [*end*]]
[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(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）
- *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)
- *end* — プロトコルポート範囲の上限（範囲：0-65535）
- *control-flags* — TCP ヘッダのバイト 14 内のフラグ・ビットを指定（範囲：0-63）
- *flag-bitmask* — 一致するコードビットの値（範囲：0-63）

* Includes TCP, UDP or other protocol types.

初期設定

なし

コマンドモード

Extended ACL

コマンド解説

- 新しいルールはリストの最後に追加されます。
- アドレスビットマスクはサブネットマスクと似ており、4 つの 0-255 の値で表示され、それぞれがピリオド(.)により分割されています。2 進数のビットが"1"の場合、一致するビットであり、"0"の場合、拒否するビットとなります。ビットマスクはビット毎に特定の IP アドレスと共に使用し、ACL が指定した入力 IP パケットのアドレスと比較されます。

- 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、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 ― "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)##
```

クラスCアドレス192.168.1.0からのTCPコントロールコード"SYN"のすべてのTCPパケットを許可します。

```
Console(config-ext-acl)#permit tcp 192.168.1.0 255.255.255.0 any
  control-flag 2 2
Console(config-ext-acl)#
```

関連するコマンド

access-list ip (4-98)

show ip access-list

設定済みのIP ACLのルールを表示します。

文法

show ip access-list {**standard** | **extended**} [*acl_name*]

- **standard** — スタンダード IP ACL
- **extended** — 拡張 IP ACL
- *acl_name* — ACL 名（最大文字数：16 文字）

コマンドモード

Privileged Exec

例

```
Console#show ip access-list standard
IP standard access-list david:
  permit host 10.1.1.21
  permit 168.92.16.0 255.255.240.0
Console#
```

関連するコマンド

permit, deny (4-98)

ip access-group (4-102)

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**

- **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。
- ポートのバインドを行う前に ACL ルールのマスクの設定を行う必要があります。

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 (4-101)

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 (4-102)

map access-list ip

ACLルールに一致するパケットの出力キューを設定します。指定されたCoS値は一致したパケットの出力キューにのみ使用され、パケットには変更が加えられません。"no"を前に置くことでCoSマッピングを削除します。

文法

map access-list ip *acl_name* **cos** *cos-value*

no map access-list ip *acl_name* **cos** *cos-value*

- *acl_name*— ACL 名（最大文字数：16 文字）
- *cos-value* — CoS 値（範囲：0-7）

初期設定

なし

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

指定されたACLのルールと一致するパケットは、下の表に基づき出力キューがマッピングされます。CoS値の詳細はP4-186 "queue cos-map"を参照して下さい。

キュー	0	1	2	3
プライオリティ	1、2	0、3	4、5	6、7

例

```
Console(config)#interface ethernet 1/25
Console(config-if)#map access-list ip david cos 0
Console(config-if)#
```

関連するコマンド

queue cos-map (4-186)
show map access-list ip (4-104)

show map access-list ip

インタフェースのIP ACLにマッピングされたCoS値を表示します。CoS値はACLルールに一致するパケットの出力キューを決定します。

文法

show map access-list ip [*interface*]

- *interface*
  - **ethernet** *unit*/*port*
    - *unit* — ユニット番号"1"
    - *port* — ポート番号

コマンドモード

Privileged Exec

例

```
Console#show map access-list ip
Eth 1/25
 access-list ip david cos 0
Console#
```

関連するコマンド

map access-list ip (4-103)

MAC ACLs

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	4-105
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	4-106
show mac access-list	設定済みMAC ACLのルールの表示	PE	4-107
mac access-group	MAC ACLへのポートの追加	IC	4-107
show mac access-group	MAC ACLに指定したポートの表示	PE	4-108
map access-list mac	ACLルールと一致するパケットへの出力キューのCoS値の設定	IC	4-108
show map access-list mac	インタフェースのアクセスリストにマッピングされたCoS値の表示	PE	4-109

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

[no] **access-list mac** *acl_name*

- *acl_name* — ACL 名（最大文字数：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) (4-106)
mac access-group (4-107)
show mac access-list (4-107)

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-end*]] [**ethertype** *protocol* [*protocol-end*]]

注意 初期設定はEthernet IIパケットです。

- **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-end** — VLAN ID の上限値（範囲：1-4094）
- *protocol* — イーサネットプロトコルナンバー（範囲：0-65535）
- *protocol-end** — プロトコル範囲の上限値（範囲：0-65535）

* すべてのビットマスクはビットが"1"の場合、一致するビットであり、"0"の場合、拒否するビットです。

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

本例のルールでは、すべてのMACアドレスからのイーサネットタイプ0800のパケットに関して、ディスティネーションMACアドレス00-e0-29-94-34-deへの通信を許可しています。

```
Console(config-mac-acl)#permit any host 00-e0-29-94-34-de etherty
pe 0800
Console(config-mac-acl)#
```

関連するコマンド

access-list mac (4-105)

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（最大文字数：16 文字）

コマンドモード

Privileged Exec

例

```
Console#show mac access-list
MAC access-list jerry:
  permit any host 00-e0-29-94-34-de ethertype 800 800
Console#
```

関連するコマンド

permit, deny (4-106)
mac access-group (4-107)

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**

- *acl_name* ― ACL 名（最大文字数：16 文字）
- **in** ― 入力パケットのリストの表示

コマンドモード

Privileged Exec

例

```
Console(config)#interface ethernet 1/25
Console(config-if)#mac access-group jerry in
Console(config-if)#
```

関連するコマンド

show mac access-list (4-107)

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 jerry in
Console#
```

関連するコマンド

mac access-group (4-107)

map access-list mac

ACLルールに一致するパケットの出力キューを設定します。指定されたCoS値は一致したパケットの出力キューにのみ使用され、パケットには変更が加えられません。"no"を前に置くことでCoSマッピングを削除します。

文法

[no] map access-list mac *acl_name* **cos** *cos-value*

- *acl_name*― ACL 名（最大文字数：16 文字）
- *cos-value* ― CoS 値（範囲：0-7）

初期設定

なし

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- ルールへの CoS 値のマッピングを行う前に、ACL マスクの設定を行う必要があります。
- 指定された ACL のルールと一致するパケットは、下の表に基づき出力キューがマッピングされます。

キュー	0	1	2	3
プライオリティ	1、2	0、3	4、5	6、7

例

```
Console(config)#int eth 1/5
Console(config-if)#map access-list mac jerry cos 0
Console(config-if)#
```

関連するコマンド

queue cos-map (4-186)

show map access-list mac (4-109)

show map access-list mac

インタフェースのMAC ACLにマッピングされたCoS値を表示します。CoS値はACLルールに一致するパケットの出力キューを決定します。

文法

show map access-list mac [*interface*]

- *interface*
  - **ethernet** *unit*/*port*
    - *unit* — ユニット番号"1"
    - *port* — ポート番号（範囲：1-16/26/52）

コマンドモード

Privileged Exec

例

```
Console#show map access-list mac
Access-list to COS of Eth 1/5
  Access-list jerry cos 0
Console#
```

関連するコマンド

map access-list mac (4-108)

ACL Information

コマンド	機能	モード	ページ
show access-list	すべてのACLと関連するルールの表示	PE	4-110
show access-group	各ポートのACLの表示	PE	4-110

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 168.92.0.0 0.0.15.255
IP extended access-list bob:
  permit 10.7.1.1 255.255.255.0 any
  permit 192.168.1.0 255.255.255.0 any destination-port 80 80
  permit 192.168.1.0 255.255.255.0 any protocol tcp control-code 2
 2
MAC access-list jerry:
  permit any host 00-30-29-94-34-de ethertype 800 800
IP extended access-list A6:
  permit 10.7.1.0 255.255.255.0 any
  permit 192.168.1.0 255.255.255.0 any destination-port 80 80
  permit TCP 192.168.1.0 255.255.255.0 any control-flag 2 2
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 1/25
 IP standard access-list david
 MAC access-list jerry
Console#
```

4-10 SNMP Commands

トラップマネージャで送信するエラータイプなどのSNMP管理端末を使用した本機へのアクセスに関する設定を行います。

コマンド	機能	モード	ページ
snmp-server 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	4-111
snmp-server contact	システムコンタクト情報の設定	GC	4-112
snmp-server location	システム設置情報の設定	GC	4-112
snmp-server host	SNMPメッセージを受信するホストの設定	GC	4-113
snmp-server enable traps	SNMPメッセージを受信するホストの有効化	GC	4-114
show snmp	SNMP設定ステータスの表示	NE, PE	4-115

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(v1)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 *string*
no snmp-server contact

- *string* — 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)#
```

関連するコマンド

snmp-server location (4-112)

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)#
```

関連するコマンド

snmp-server contact (4-112)

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"を前に置くことで指定したホストを削除します。

文法

snmp-server host *{host-addr community-string}* [**version 1 | 2c**]
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）
- *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** — SNMP（v1 または v2c）トラップバージョンを指定します（範囲：1, 2c、初期設定：1）

初期設定

Host Address：なし
SNMP Version：1

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。
- 本機は管理端末がサポートするバージョンにあわせて SNMP バージョン 1 及び 2c に対応したトラップをホストに送信することが可能です。"**snmp-server host**"コマンドにおいて SNMP バージョンを指定しない場合には SNMP バージョン 1 に対応したトラップが送信されます。
- 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。

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 (4-114)

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

snmp-server enable traps [**authentication** | **link-up-down**]
no snmp-server enable traps [**authentication** | **link-up-down**]

- **authentication** — 認証エラー時トラップのキーワード
- **link-up-down** — リンクアップ及びリンクダウン時トラップのキーワード

初期設定

authentication及びlink-up-downトラップ

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 (4-113)

show snmp

SNMPのステータスを表示します。

初期設定

なし

コマンドモード

Normal Exec, Privileged Exec

コマンド解説

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てもいなくても表示されます。

例

```
Console#show snmp

 SNMP traps:
  Authentication: enabled
  Link-up-down: enabled
 SNMP communities:
    1. alpha, and the privilege is read-write
    2. private, and the privilege is read-write
    3. 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: enabled
    Logging to 10.1.19.23 batman version 1
Console#
```

4-11 Interface Commands

各ポートの設定及びポートトランク、VLANの設定及び設定の表示を行います。

コマンド	機能	モード	ページ
interface	インタフェースタイプの設定及びinterface configurationモードへの変更	GC	4-117
description	インタフェースの解説	IC	4-118
speed-duplex	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	4-119
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	4-120
capabilities	オートネゴシエーション時のインタフェースの設定	IC	4-120
flowcontrol	インタフェースへのフローコントロール設定	IC	4-122
shutdown	インタフェースの無効	IC	4-123
switchport broadcast packet-rate	ブロードキャストストームコントロールの設定	IC	4-123
clear counters	インタフェースの統計情報のクリア	PE	4-124
show interfaces status	インタフェースの設定状況を表示	NE, PE	4-125
show interfaces counters	インタフェースの統計情報の表示	NE, PE	4-126
show interfaces switchport	インタフェースの管理、運用状況の表示	NE, PE	4-127

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：1-16/26/52）
  - **port-channel** *channel-id* — Channel ID (1-4)
  - **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5番ポートの指定を行っています。

```
Console(config)#interface ethernet 1/5
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、5番ポートに解説を加えている設定です。

```
Console(config)#interface ethernet 1/5
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の際、各ポートの初期設定は100BASE-TX の場合は"**100half**"、ギガビットイーサネットの場合は"**1000full**"となります。

コマンドモード

Interface Configuration (Ethernet、Port Channel)

コマンド解説

- 通信速度と Duplex を固定設定にするためには"**speed-duplex**"コマンドを使用します。又、"**no negotiation**"コマンドを使用しオートネゴシエーションを無効にして下さい。
- "**negotiation**"コマンドを使用しオートネゴシエーションが有効になっている場合は"**capabilities**"コマンドを使用することで最適な接続を行うことができます。オートネゴシエーション時の通信速度、通信方式の設定を行うためには"**capabilities**"コマンドを使用する必要があります。

例

本例では5番ポートに100Mbps half-duplex固定の設定を行っています。

```
Console(config)#interface ethernet 1/5
Console(config-if)#speed-duplex 100half
Console(config-if)#no negotiation
Console(config-if)#
```

関連するコマンド

negotiation (4-120)
capabilities (4-120)

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 (4-120)
speed-duplex (4-119)

capabilities

オートネゴシエーション時のポートの通信方式を設定します。
"no"を前に置きパラメータを設定することで指定したパラメータの値を削除します。パラメータを設定せず"no"を前に置いた場合には初期設定に戻ります。

文法

capabilities {**1000full** | **100full** | **100half** | **10full** | **10half** | **flowcontrol** | **symmetric**}

no port-capabilities [**1000full** | **100full** | **100half** | **10full** | **10half** | **flowcontrol** | **symmetric**]

- **1000full** — 1000Mbps full-duplex 通信
- **100full** — 100Mbps full-duplex 通信
- **100half** — 100Mbps half-duplex 通信
- **10full** — 10Mbps full-duplex 通信
- **10half** — 10Mbps half-duplex 通信
- **flowcontrol** — 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

negotiation (4 -120)
speed-duplex (4 -119)
flowcontrol (4 -122)

flowcontrol

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 (4 -120)
capabilities (flowcontrol, symmetric) (4-120)

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 broadcast packet-rate

ブロードキャストストームコントロールの設定を行います。"no"を前に置くことで本機能を無効にします。

文法

switchport broadcast octet-rate *rate*

no switchport broadcast

- *rate* — ブロードキャストパケットのしきい値(オクテット/秒)（範囲：64-95232000）

初期設定

有効（全ポート）

パケットレートの上限：32000オクテット/秒

コマンドモード

Interface Configuration (Ethernet)

コマンド解説

- ブロードキャストトラフィックが指定したしきい値を超えた場合、超えたパケットに関しては破棄されます。
- 本機能の有効/無効の切り替えはポート毎に行えます。但し、しきい値に関してはすべてのポートで同じ設定となります。

例

本例では5番ポートに600ppsのしきい値を設定しています。

```
Console(config)#interface ethernet 1/5
Console(config-if)#switchport broadcast octet-rate 600
Console(config-if)#
```

clear counters

インタフェースの統計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：1-16/26/52）
  - **port-channel** *channel-id*（範囲：1-4）

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

統計情報は電源をリセットした場合のみ初期化されます。本機能を使用した場合、現在の管理セッションで表示されている統計情報はリセットされます。但し、一度ログアウトし再度管理画面にログインした場合には統計情報は最後に電源をリセットした時からの値となります。

例

本例では5番ポートの統計情報をクリアしています。

```
Console#clear counters ethernet 1/5
Console#
```

show interfaces status

インタフェースの状態を表示します。

文法

show interfaces status *interface*

- *interface*
  - －**ethernet** *unit/port*
    - －*unit* ― ユニット番号"1"
    - －*port* ― ポート番号（範囲：1-16/26/52）
  - －**port-channel** *channel-id*（範囲：1-4）
  - －**vlan** *vlan-id*（範囲：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 P3-58「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:            00-30-F1-D3-26-05
 Configuration:
  Name:
  Port admin:             Up
  Speed-duplex:           Auto
  Capabilities:           10half, 10full, 100half, 100full,
  Broadcast storm:        Enabled
  Broadcast storm limit:  32000 octets/second
  Flow control:           Disabled
  Lacp:                   Disabled
  Port security:          Disabled
  Max MAC count:          0
  Port security action:   None
Current status:
  Link status:            Up
  Port operation status:  Up
  Operation speed-duplex: 100full
  Flow control type:      None
Console#show interfaces status vlan 1
 Information of VLAN 1
 MAC address:             00-00-AB-CD-00-00
Console#
```

show interfaces counters

インタフェースの統計情報を表示します。

文法

show interfaces counters [*interface*]

- *interface*
  - **ethernet** *unit*/*port*
    - *unit* ― ユニット番号"1"
    - *port* ― ポート番号（範囲：1-16/26/52）
  - **port-channel** *channel-id*（範囲：1-4）

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 1023 octets: 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：1-16/26/52）
  - **port-channel** *channel-id*（範囲：1-4）

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

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。有効時にはしきい値を表示（4-123参照）
Lacp status	LACPの有効/無効（4-136参照）
Ingress/Egress rate limit	帯域制御の有効/無効。現在の設定（4-131参照）
VLAN membership mode	トランク又はHybridのメンバーモード（4-165参照）
Ingress rule	イングレスフィルタの有効/無効（4-166参照）
Acceptable frame type	VLANフレームは、すべ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（4-166参照）
Native VLAN	デフォルトポートVLAN ID（4-167参照）
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（4-183参照）
Gvrp status	GVRPの有効/無効（4-179参照）
Allowed Vlan	参加しているVLAN。"(u)"はタグなし、"(t)"はタグ（4-168参照）
Forbidden Vlan	GVRPによって動的に参加できないVLANの表示（4-169参照）
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（4-174参照）
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（4-175参照）
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（4-176参照）

例

本例は12番ポートの情報を表示しています。

```
Console#show interfaces switchport ethernet 1/12
 Broadcast threshold: Enabled, 600 octets/second
 LACP status: Enabled
 Ingress rate limit: disable, Level: 30
 Egress rate limit: disable, Level: 30
 VLAN membership mode: Hybrid
 Ingress rule: Disabled
 Acceptable frame type: All frames
 Native VLAN: 1
 Priority for untagged traffic: 0
 GVRP status: Disabled
 Allowed Vlan: 1(u),
 Forbidden Vlan:
 Private-VLAN mode: NONE
 Private-VLAN host-association: NONE
 Private-VLAN mapping: NONE
Console#
```

4-12 Mirror Port Commands

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	4-129
show port monitor	ミラーポートの設定の表示	PE	4-130

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**]
no port monitor *interface*

- *interface*
  - **ethernet** *unit/port* (source port)
    - *unit* — ユニット番号"1"
    - *port* — ポート番号（範囲：1-16/26/52）
- **rx** — 受信パケットのミラー
- **tx** — 送信パケットのミラー

初期設定

なし

コマンドモード

Interface Configuration (Ethernet, destination port)

コマンド解説

- ソースポートからディスティネーションポートに通信をミラーし、リアルタイムでの通信分析を行えます。ディスティネイションポートにネットワーク解析装置(Sniffer 等)又は RMON プローブを接続し、通信に影響を与えずにソースポートのトラフィックを解析することができます。
- ディスティネーションポートは Ethernet インタフェースに設定します。
- ソース及びディスティネーションポートの通信速度は同じ必要があります。同じ通信速度でない場合には通信がソースポートから落とされます。
- 単一のミラーセッションのみを作成することができます。

例

本例では6番から11番ポートへのミラーを行います。

```
Console(config)#interface ethernet 1/11
Console(config-if)#port monitor ethernet 1/6 rx
Console(config-if)#
```

show port monitor

ミラー情報の表示を行います。

文法

show port monitor [*interface*]

- *interface*
  - **ethernet** *unit*/*port*
    - *unit* — ユニット番号"1"
    - *port* — ポート番号（範囲：1-16/26/52）

初期設定

すべてのセッションを表示

コマンドモード

Privileged Exec

コマンド解説

本コマンドを使用することで現在設定されているソースポート、ディスティネーションポート、ミラーモード(RX, TX)の表示を行います。

例

本例では6番から11番ポートへのミラーの設定が表示されています。

```
Console(config)#interface ethernet 1/11
Console(config-if)#port monitor ethernet 1/6 rx
Console(config-if)#end
Console#show port monitor
Port Mirroring
-------------------------------------
 Destination port(listen port) :Eth1/11
 Source port(monitored port)   :Eth1/6
 Mode                          :RX
Console#
```

4-13 Rate Limiting

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。

注意 "rate limit granularity"は"rate limit" (P4-131)で乗算され、単一のインタフェースでの実際の帯域制御を設定するものです。粒度はファーストイーサネット又はギガビットイーサネットインタフェース全体に適用されます。

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	4-131
rate limit granularity	ファーストイーサネット、ギガビットイーサネットの粒度の設定	IC	4-132
show rate limit	帯域制御の粒度の表示	PE	4-132

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} level[*rate*]
no rate-limit {input | output}

- **input** — 入力帯域（レート）
- **output** — 出力帯域（レート）
- *rate* — 最大値（範囲：1-30）

初期設定

30

コマンドモード

Interface Configuration (Ethernet, Port Channel)

例

```
Console(config)#interface ethernet 1/1
Console(config-if)#rate-limit level 20
Console(config-if)#
```

rate-limit granularity

ファーストイーサネット、ギガビットイーサネットポートの帯域制御の粒度を設定します。"no"を前に置くことで初期設定に戻します。

文法

rate-limit {**fastethernet** | **gigabitethernet**}
granularity [*granularity*]
no rate-limit {**fastethernet** | **gigabitethernet**} **granularity**

- **fastethernet** – ファーストイーサネットの粒度
- **gigabitethernet** – ギガビットイーサネットの粒度
- *granularity* – システムに対する帯域制御粒度の制限。ファーストイーサネットの場合、512 Kbps、1 Mbps、3.3 Mbps から選択。ギガビットイーサネットの場合、33.3 Mbps

初期設定

- ファーストイーサネット：3.3Mbps
- ギガビットイーサネット：33.3Mbps

コマンドモード

Grobal Configuration (Ethernet, Port Channel)

コマンド解説

実際の帯域制御 = Rate Limit Level * Granularity

例

```
Console(config)#rate-limit fastethernet granularity 1000
Console(config)#rate-limit gigabitethernet granularity 33300
Console(config)#
```

show rate-limit

帯域制御の粒度を表示します。

文法

show rate-limit

初期設定

- ファーストイーサネット：3.3Mbps
- ギガビットイーサネット：33.3Mbps

コマンドモード

Privileged Exec

コマンド解説

- ファーストイーサネットの場合、512 Kbps、1 Mbps、3.3 Mbps
- ギガビットイーサネットの場合、33.3 Mbps

例

```
Console(config)#rate-limit fastethernet granularity 1000
Console(config)#rate-limit gigabitethernet granularity 33300
Console(config)#
```

4-14 Link Aggregation Commands

バンド幅拡張のため、又ネットワーク障害時の回避のため、ポートを束ねた静的グループを設定することができます。又、IEEE802.1ad準拠のLink Aggregation Control Protocol (LACP)を使用し、本機と他のデバイス間のトランクを自動的に行うこともできます。静的トランクでは、本機はCisco EtherChannel標準との互換性があります。動的トランクに関してはIEEE802.1ad準拠のLACPとなります。
本機では最大4トランクグループをサポートします。
2つの1000Mbpsポートをトランクした場合、full duplex時には最大4Gpbsのバンド幅となります。

コマンド	機能	モード	ページ
Manual Configuration Commands			
interface port-channel	interface configuration モードへの移行とトランク設定	GC	4-117
channel-group	トランクへのポートの追加	IC	4-135
Dynamic Configuration Command			
lacp	現在のインタフェースでのLACPの設定	IC	4-136
lacp system-priority	ポートLACPシステムプライオリティの設定	IC (Ethernet)	4-137
lacp admin-key	ポートアドミンキーの設定	IC (Ethernet)	4-138
lacp admin-key	ポートチャンネルアドミンキーの設定	IC (Port Channel)	4-139
lacp port-priority	ポートLACPポートプライオリティの設定	IC (Ethernet)	4-140
Trunk Status Display Command			
show interfaces status port-channel	トランク情報の表示	NE, PE	4-125
show lacp	LACP関連情報の表示	PE	4-140

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、グループのインター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：1-4）

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* — ポートチャンネルアドミンキーは本機のローカル LACP 設定中に特定の LAG を認識するために使用します（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
```

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：1-4）
- **counters** — LACP プロトコルメッセージの統計情報
- **internal** — ローカルサイドの運用状況と設定情報
- **neighbors** — リモートサイドの運用状況と設定情報
- **sysid** — すべてのチャンネルグループの MAC アドレスとシステムプライオリティのサマリ

初期設定

Port Channel：すべて

コマンドモード

Privileged Exec

例

```
Console#show lacp 1 counters
Port channel : 1
-------------------------------------------------------------------
Eth 1/ 1
-------------------------------------------------------------------
  LACPDUs Sent : 21
  LACPDUs Received : 21
  Marker Sent : 0
  Marker Received : 0
  LACPDUs Unknown Pkts : 0
  LACPDUs Illegal Pkts : 0
.
.
.
```

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

LACPDUs Illegal Pkts	不正なPDU又はプロトコルサブタイプが不正な値を含むスロープロトコルイーサネットパケットを運ぶフレーム数.

例

```
Console#show lacp 1 internal
Port channel : 1
-------------------------------------------------------------------
Oper Key : 4
Admin Key : 0
Eth 1/1
-------------------------------------------------------------------
  LACPDUs Internal : 30 sec
  LACP System Priority : 32768
  LACP Port Priority : 32768
  Admin Key : 4
  Oper Key : 4
  Admin State : defaulted,aggregation,long timeout, LACP-activity
  Oper State : distributing, collecting, synchronization,
               aggregation, long timeout, LACP-activity
.
.
.
```

項目	解説
Oper Key	現在のアグリゲーションポートのキーの運用値
Admin Key	現在のアグリゲーションポートのキーの管理値
LACPDUs Internal	受信したLACPDU情報を無効にするまでの秒数
LACP System Priority	本ポートチャンネルに割り当てられたLACP システムプライオリティ
LACP Port Priority	本ポートチャンネルグループに割り当てられたLACPポートプライオリティ
Admin State, Oper State	Actorの管理値又は運用値の状態のパラメータ。 ・ Expired — Actorの受信機器は失効状態です ・ Defaulted — Actorの受信機器は初期設定の運用partnerの情報を使用しています ・ Distributing — 誤りの場合、このリンク上の出力フレームの配信は無効になります。配信は現在無効状態で、受信プロトコル情報の管理上の変更、又は変更がない状態で有効にはなりません ・ Collecting — このリンク上の入力フレームの収集は可能な状態です。収集は現在可能な状態で、受信プロトコル情報の管理上の変化、又は変化がない状態で無効にはなりません ・ Synchronization — システムはリンクをIN_SYNCと認識します。それにより正しいリンクアグリゲーショングループに属すことができます。グループは互換性のある

	Aggregatorに関係します。リンクアグリゲーショングループのIDはシステムIDと送信されたオペレーショナルキー情報から形成されます ・ Aggregation — システムは、アグリゲーション可能なリンクと認識しています。アグリゲーションの存在的な候補です ・ Long timeout — LACPDUの周期的な送信にスロー転送レートを使用します ・ LACP-Activity — 本リンクに関するアクティブコントロール値（0：Passive、1：Active）

例

```
Console#show lacp 1 neighbors
Port channel : 1 neighbors
-------------------------------------------------------------------
Eth 1/1
-------------------------------------------------------------------
  Partner Admin System ID : 32768, 00-00-00-00-00-00
  Partner Oper System ID : 32768, 00-00-00-00-00-01
  Partner Admin Port Number : 1
  Partner Oper Port Number : 1
  Port Admin Priority : 32768
  Port Oper Priority : 32768
  Admin Key : 0
  Oper Key : 4
  Admin State : defaulted, distributing, collecting,
                synchronization, long timeout,
  Oper State : distributing, collecting, synchronization,
                aggregation, long timeout, LACP-activity
.
.
.
```

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

例

```
Console#show lacp sysid
Port Channel    System Priority    System MAC Address
-----------------------------------------------------------------
           1              32768     00-30-F1-D3-26-00
           2              32768     00-30-F1-D3-26-00
           3              32768     00-30-F1-D3-26-00
           4              32768     00-30-F1-D3-26-00
Console#
```

項目	解説
Channel group	本機のリンクアグリゲーショングループ設定.
System Priority*	本チャンネルグループのLACPシステムプライオリティ
System MAC Address*	システムMACアドレス

*LACP system priority及びsystem MAC addressはLAGシステムID形成します。

4-15 Address Table Commands

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のポートへのMACアドレスの静的なマッピング	GC	4-145
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	4-146
show mac-address-table	転送データベースに登録された情報の表示	PE	4-147
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	4-148
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	4-148

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：1-16/26/52）
- **port-channel** *channel-id*（範囲：1-4）
- **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* — アドレス内のビット数
- *interface*
  - **ethernet** *unit/port*
    - *unit* — ユニット番号"1"
    - *port* — ポート番号（範囲：1-16/26/52）
- **port-channel** *channel-id*（範囲：1-4）
- **vlan** *vlan-id* — VLAN ID (1-4094)
- **sort** — アドレス、VLAN、インタフェースによる並び替え

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

- MAC アドレステーブルはインタフェース毎に MAC アドレスが構成されます。Type の値として以下のタイプがあります：
  - Learned — 動的アドレス学習
  - Permanent — 静的アドレス学習
  - Delete-on-reset — システム再起動時に削除される静的アドレス学習
- mask は xx-xx-xx-xx-xx-xx で表される 16 進数の MAC アドレスとなります。16 進数の値を入力します。
- MAC アドレスの登録数は最大 16K 個です。

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 sec
Console(config)#
```

show mac-address-table aging-time

アドレステーブルのエージングタイムを表示します。

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#show mac-address-table aging-time
 Aging time: 100 sec.
Console#
```

4-16 Spanning Tree Commands

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	4-150
spanning-tree mode	STP/RSTPモードの選択	GC	4-150
spanning-tree forward-time	スパニングツリーブリッジ転送時間の設定	GC	4-151
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	4-152
spanning-tree max-age	スパニングツリーブリッジ最長時間の設定	GC	4-152
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	4-153
spanning-tree pathcost method	RSTPのパスコスト方法の設定	GC	4-154
spanning-tree transmission-limit	RSTPの送信リミットの設定	GC	4-154
spanning-tree spanning-disabled	インタフェースのスパニングツリーの無効化（FXC3126/52）	IC	4-155
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	4-155
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	4-156
spanning-tree edge-port	エッジポートへのポートファストの有効化	IC	4-157
spanning-tree portfast	インタフェースのポートファストの設定	IC	4-158
spanning-tree link-type	RSTPのリンクタイプを設定	IC	4-159
spanning-tree protocol-migration	適切なBPDUフォーマットの再確認	PE	4-160
show spanning-tree	スパニングツリーの設定を表示	PE	4-160

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}
no spanning-tree mode

- **stp** — Spanning Tree Protocol（IEEE 802.1D 準拠）
- **rstp** — Rapid Spanning Tree Protocol（IEEE 802.1w 準拠）

初期設定

rstp

コマンドモード

Global Configuration

コマンド解説

- Spanning Tree Protocol(STP)
  スイッチ内部では RSTP を用いますが、外部へは IEEE802.1D 準拠の BPDU の送信のみを行います。
- Rapid Spanning Tree Protocol(RSTP)
  RSTP は以下の入ってくるメッセージの種類を判断し STP 及び RSTP のいずれにも自動的に対応することができます。
  －STP Mode ― ポートの移行遅延タイマーが切れた後に IEEE802.1D BPDU を受け取ると、本機は IEEE802.1D ブリッジと接続していると判断し、IEEE802.1D BPDU のみを使用します。
  －RSTP Mode ― IEEE802.1D BPDU を使用し、ポートの移行遅延タイマーが切れた後に RSTP BPDU を受け取ると、RSTP は移行遅延タイマーを再スタートさせ、そのポートに対し RSTP BPDU を使用します。

例

本例ではRSTPを使用する設定をしています。

```
Console(config)#spanning-tree mode rstp
Console(config)#
```

spanning-tree forward-time

スパニングツリー転送遅延時間を本機すべてのインタフェースに設定します。"no"を前に置くことで初期設定に戻します。

文法

spanning-tree forward-time *seconds*
no spanning-tree forward-time

- *seconds* ― 秒数（範囲：4-30 秒）
  最小値は 4 又は[(max-age / 2) + 1]のどちらか小さい方となります。

初期設定

15（秒）

コマンドモード

Global Configuration

コマンド解説

ルートデバイスがステータスを変更するまでの最大時間を設定することができます。各デバイスがフレームの転送をはじめる前にトポロジー変更を受け取るために遅延時間が必要です。また、各ポートの競合する情報を受信し､廃棄するためにも時間が必要となります。そうしなければ一時的にでも、データのループが発生します。

例

```
Console(config)#spanning-tree forward-time 20
Console(config)#
```

spanning-tree hello-time

スパニングツリーHelloタイムを設定します。"no"を前に置くことで初期設定に戻します。

文法

spanning-tree hello-time *time*

no spanning-tree hello-time

- *time* ― 秒数（範囲：1-10 秒）
  最大値は 10 または[(max-age / 2) -1]の小さい方となります。

初期設定

2（秒）

コマンドモード

Global Configuration

コマンド解説

設定情報の送信を行う間隔を設定するためのコマンドです。

例

```
Console(config)#spanning-tree hello-time 5
Console(config)#
```

spanning-tree max-age

スパニングツリーの最大エージングタイムを設定します。"no"を前に置くことで初期設定に戻します。

文法

spanning-tree max-age *seconds*

no spanning-tree max-age

- *seconds* — 秒（範囲：6-40 秒）
  最小値は 6 又は[2 x (hello-time + 1)]のどちらか大きい値です。
  最大値は 40 又は[2 x (forward-time - 1)]のどちらか小さい値です。

初期設定

20（秒）

コマンドモード

Global Configuration

コマンド解説

設定変更を行う前に設定情報を受け取るまでの最大待ち時間(秒)。指定ポートを除くすべてのポートが設定情報を一定の間隔で受け取ります。タイムアウトしたSTPポートは付属するLANのための指定ポートになります。そのポートがルートポートの場合、ネットワークに接続された他のポートがルートポートとして選択されます。

例

```
Console(config)#spanning-tree max-age 40
Console(config)#
```

spanning-tree priority

本機全体に対してスパニングツリーのプライオリティの設定を行います。"no"を前に置くことで初期設定に戻します。

文法

spanning-tree priority *priority*

no spanning-tree priority

- *priority* — ブリッジの優先順位
  (0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440)

初期設定

32768

コマンドモード

Global Configuration

コマンド解説

プライオリティはルートデバイス、ルートポート、指定ポートを決定する際に使用されます。一番高いプライオリティを持ったデバイスがSTAルートデバイスとなります。すべてのデバイスが同じプライオリティの場合、MACアドレスが一番小さいデバイスがルートデバイスとなります。

例

```
Console(config)#spanning-tree priority 40960
Console(config)#
```

spanning-tree pathcost method

RSTPのパスコストを設定します。"no"を前に置くことで初期設定に戻します。

文法

spanning-tree pathcost method {long | short}

no spanning-tree pathcost method

- **long** — 0-200,000,000 までの 32 ビットの値
- **short** — 0-65535 までの 16 ビットの値

初期設定

long

コマンドモード

Global Configuration

コマンド解説

パスコストはデバイス間の最適なパスを決定するために使用されます。速度の速いポートに対し小さい値を設定し、速度の遅いポートに対し大きな値を設定します。pathcostはport priorityよりも優先されます。

例

```
Console(config)#spanning-tree pathcost method long
Console(config)#
```

spanning-tree transmission-limit

RSTP BPDUの最小送信間隔を設定します。"no"を前に置くことで初期設定に戻します。

文法

spanning-tree transmission-limit *count*

no spanning-tree transmission-limit

- *count* ― 転送リミットの秒数（範囲：1-10 秒）

初期設定

3

コマンドモード

Global Configuration

コマンド解説

本コマンドではBPDUの最大転送レートを制限します。

例

```
Console(config)#spanning-tree transmission-limit 4
Console(config)#
```

spanning-tree spanning-disabled

FXC3126/52のみ使用可能なコマンドです。特定のポートのSTAを無効にします。"no"を前に置くことで再びSTAを有効にします。

文法

spanning-tree spanning-disabled

no spanning-tree spanning-disabled

初期設定

有効

コマンドモード

Interface Configuration (Ethernet, Port Channel)

例

5番ポートのSTAを無効にしています。

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree spanning-disabled
Console(config-if)#
```

spanning-tree cost

各ポートのSTAパスコストを設定します。"no"を前に置くことで初期設定に戻します。

文法

spanning-tree cost *cost*

no spanning-tree cost

- *cost* ― インタフェースへのパスコストの値（範囲：1-200,000,000）
  推奨する値は以下の通りです。
  －Ethernet (10Mbps): 200,000-20,000,000
  －Fast Ethernet (100Mbps): 20,000-2,000,000
  －Gigabit Ethernet (1Gbps): 2,000-200,000

初期設定

- Ethernet ― half duplex: 2,000,000、full duplex: 1,000,000、トランク: 500,000
- Fast Ethernet ― half duplex: 200,000、full duplex: 100,000、トランク: 50,000
- Gigabit Ethernet ― full duplex: 10,000、トランク: 5,000

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- 本コマンドはデバイス間の STA のパスを最適に決定するためのコマンドです。従って、速度の速いポートに対し小さい値を設定し、速度の遅いポートに対し大きな値を設定します。
- パスコストはポートプライオリティより優先されます。
- STP パスコストが"**short**"に設定されている場合には最大値が 65,535 となります。

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree cost 5000
Console(config-if)#
```

spanning-tree port-priority

指定ポートのプライオリティを設定します。"no"を前に置くことで初期設定に戻します。

文法

spanning-tree port-priority *priority*

no spanning-tree port-priority

- *priority* ― ポートの優先順位（範囲：16 間隔で 0-240 の値）

初期設定

128

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- STPに使用するポートの優先順位を指定するためのコマンドです。もし、すべてのポートのパスコストが同じ場合には、高い優先順位（低い設定値）のポートがSTPのアクティブリンクとなります。
- 1つ以上のポートに最優先順位が割り当てられる場合、ポート番号の低いポートが有効となります。

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree port-priority 128
```

関連するコマンド

spanning-tree cost (4-155)

spanning-tree edge-port

エッジに対するポートを指定します。"no"を前に置くことで初期設定に戻します。

文法

spanning-tree edge-port
no spanning-tree edge-port

初期設定

無効(Disabled)

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 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#
```

関連するコマンド

spanning-tree portfast (4-158)

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

無効(Disabled)

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 (4-157)

spanning-tree link-type

RSTPのリンクタイプを設定します。"no"を前に置くことで初期設定に戻します。

文法

spanning-tree link-type {**auto** | **point-to-point** | **shared**}
no spanning-tree link-type

- **auto** — duplex モードの設定から自動的に設定
- **point-to-point** — point to point リンク
- **shared** — シェアードミディアム

初期設定

auto

コマンドモード

Interface Configuration (Ethernet, Port Channel)

コマンド解説

- ポートが対向のブリッジにのみ接続されている場合は point-to-point リンクを、複数のブリッジに接続されている場合には shared を選択します。
- 自動検知が選択されている場合、リンクタイプは duplex モードから選択されます。Full-duplex のポートでは point-to-point リンクが、half-duplex ポートでは、shared リンクが自動的に選択されます。
- RSTP は 2 つのブリッジ間の point-to-point リンクでのみ機能します。指定されたポートが shared リンクの場合には RSTP は許可されません。

例

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree link-type point-to-point
```

spanning-tree 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：1-16/26/52）
  - **port-channel** *channel-id*（1-4）

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。

例

show spanning-tree [*interface*]

- *interface*
  - **ethernet** *unit*/*port*
    - *unit* — ユニット番号"1"
    - *port* — ポート番号（範囲：1-16/26/52）
- **port-channel** *channel-id*（1-4）

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 P3-80「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 P3-83「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 information
----------------------------------------------------------------
 Spanning tree mode:                RSTP
Spanning tree enabled/disabled:    enabled
 Priority: 40960
 Bridge Hello Time (sec.):          2
 Bridge Max Age (sec.):             20
 Bridge Forward Delay (sec.):       15
 Root Hello Time (sec.):            2
 Root Max Age (sec.):               20
 Root Forward Delay (sec.):         15
 Designated Root:                   32768.0.0000ABCD0000
 Current root port:                 1
 Current root cost:                 50000
 Number of topology changes:        5
 Last topology changes time (sec.):  226
 Transmission limit:                3
 Path Cost Method:                  long
----------------------------------------------------------------
Eth 1/ 1 information
----------------------------------------------------------------
Admin status:           enabled
 Role:                  root
 State:                 forwarding
 Path cost:             100000
 Priority:              128
 Designated cost:       200000
 Designated port:       128.24
 Designated root:       32768.0.0000ABCD0000
 Designated bridge:     32768.0.0030F1552000
 Fast forwarding:       enabled
 Forward transitions:   1
 Admin edge port:       enabled
 Oper edge port:        disabled
 Admin Link type:       auto
 Oper Link type:        point-to-point
 Spanning Tree Status:  enabled
.
.
.
Console#
```

4-17 VLAN Commands

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
Editing VLAN Groups	VLAN名、VID、状態を含むVLANの設定	4-162
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	4-164
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	4-170
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	4-171

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	4-162
vlan	VID、VLAN名、ステートなどVLANの設定	VC	4-163

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 (4-170)

vlan

VLANを設定します。"no"を前に置くことでVLANの削除、もしくは初期設定に戻します。

文法

vlan *vlan-id* [**name** *vlan-name*] **media ethernet** [**state** {**active** | **suspend**}]

no vlan *vlan-id* [**name** | **state**]

- *vlan-id* — 設定する VLAN ID（範囲：1-4094）
- **name** — 識別するための VLAN 名
- *vlan-name* — 1-32 文字
- **media ethernet** — イーサネットメディアの種類
- **state** — VLAN のステートの識別
  －**active** — VLAN の実行
  －**suspend** — VLAN の中断。中断中の VLAN はパケットの転送を行いません。

初期設定

初期設定ではVLAN 1が存在し、active状態です。

コマンドモード

VLAN Database Configuration

コマンド解説

- "**no vlan** *vlan-id*"を使用した場合、VLAN が削除されます。

- "**no vlan** *vlan-id* **name**"を使用した場合、VLAN 名が削除されます。
- " **no vlan** *vlan-id* **state**"を使用した場合、VLAN は初期設定の状態(active)に戻ります。
- 最大 255VLAN の設定が可能です。

例

VLAN ID：105、VLAN name：RD5で新しいVLANを追加しています。VLANは初期設定でactiveになっています。

```
Console(config)#vlan database
Console(config-vlan)#vlan 105 name RD5 media ethernet
Console(config-vlan)#
```

関連するコマンド

show vlan (4-170)

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	4-164
switchport mode	インタフェースのVLANメンバーモードの設定	IC	4-165
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	4-166
switchport ingress-filtering	インタフェースへの入力フィルタの有効化	IC	4-166
switchport native vlan	インタフェースのPVID（native VLAN)の設定	IC	4-167
switchport allowed vlan	インタフェースに関連したVLANの設定	IC	4-168
switchport gvrp	インタフェースへのGVRPの有効化	IC	4-179
switchport forbidden vlan	インタフェースの登録を禁止するVLANの設定	IC	4-169
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(FXC3126/52)	IC	4-184

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 (4-170)

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 {**trunk** | **hybrid** | **private-vlan**}

no switchport mode

- **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。
- **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。
- **private-vlan** — 詳細については、P4-174 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)#
```

関連するコマンド

switchport acceptable-frame-types(4-166)

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 (4-165)

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

switchport ingress-filtering
no switchport ingress-filtering

初期設定

無効(Disabled)

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無効の場合、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、そのフレームはそのVLANを禁止しているポート以外のすべてのポートに転送されます。
- 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

- インタフェースがVLAN 1のメンバーではなく、PVIDをVLAN 1に設定している場合、インタフェースは自動的にVLAN 1のタグなしメンバーとなります。他のすべてのVLANで、PVIDをそのグループに設定するまでは、インタフェースはタグなしメンバーとして設定されます。
- 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VLAN2,5,6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	4-170
show interfaces status vlan	特定VLANインタフェースの状態の表示	NE, PE	4-125
show interfaces switchport	インタフェースの管理、運用状態の表示	NE, PE	4-127

show vlan

VLAN情報の表示を行います。

文法

show vlan [**id** *vlan-id* | **name** *vlan-name* | **private-lan** *private-vlan-type*]

- **id** — VLAN ID が続くキーワード
  －*vlan-id* — 表示する VLAN ID（範囲：1-4094）
- **name** — VLAN 名が続くキーワード
  －*vlan-name* — 1-32 文字の VLAN 名
- **private-vlan** — 本コマンドに関する詳細は、P4-177 の"show vlan private-vlan"コマンドを参照して下さい。
  －*private-van-type* — プライベート VLAN の種類（オプション：Community、Isolated、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
Vlan ID:            1
Type:               Static
Name:               DefaultVlan
Status:             Active
Ports/Port Channel:Eth1/ 1(S) Eth1/ 2(S) Eth1/ 3(S) Eth1/ 4(S) Eth1/ 5(S)
                    Eth1/ 6(S) Eth1/ 7(S) Eth1/ 8(S) Eth1/ 9(S) Eth1/10(S)
                    Eth1/11(S) Eth1/12(S) Eth1/13(S) Eth1/14(S) Eth1/15(S)
                    Eth1/16(S) Eth1/17(S) Eth1/18(S) Eth1/19(S) Eth1/20(S)
                    Eth1/21(S) Eth1/22(S) Eth1/23(S) Eth1/24(S) Eth1/25(S)
                    Eth1/26(S)
Console#
```

プライベートVLANの設定

プライベートVLANは、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
Edit Private VLANグループ			
private-vlan	プライマリ、コミュニティ、独立VLANの追加と削除	VC	4-173
private-vlan association	コミュニティVLANとプライマリVLANの関連付け	VC	4-174
Configure Private VLAN Interface			
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	4-174
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	4-175

switchport private-vlan isolated	インタフェースの独立VLANへの関連付け（FXC3126/52）	IC	4-176
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	4-176
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	4-177

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のすべてのポートへアクセス可能な無差別ポート）、又はホスト（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）に指定します。
④ "switchport private-vlan host-association"コマンドを使用し、ポートをセカンダリVLANに割り当てます。
⑤ "switchport private-vlan mapping"コマンドを使用し、ポートをプライマリVLANに割り当てます。
⑥ "show vlan private-vlan"コマンドを使用し、設定内容を確認します。

独立VLANを設定するには、以下の手順で行います。

① "private-vlan"コマンドを使用し、独立VLANを指定します。独立VLANには、1つの無差別ポートと1つ以上の独立ポートが所属しています。
② "switchport mode private-vlan"コマンドを使用し、ポートを無差別（プライマリVLANのすべてのポートと通信が可能）又はホスト（コミュニティポートなど）に指定します。
③ "switchport private-vlan isolated"コマンドを使用し、ポートを独立VLANに指定します。
④ "show vlan private-vlan"コマンドを使用し、設定内容を確認します。

private-vlan

プライベートVLAN（プライマリ、コミュニティ、独立）を作成します。"no"を前に置くことで、プライベートVLANを削除します。

文法

private-vlan *vlan-id* {**community** | **primary** | **isolated**}
no private-vlan *vlan-id*

- *vlan-id* — プライベート VLAN の ID（範囲：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
- **isolated** — 独立 VLAN。独立ポートに関連付けられたポートは、同じ VLAN に所属する無差別ポートとのみ通信が可能

初期設定

なし

初期設定

VLAN Configuration

コマンド解説

- プライベート VLAN は、同一のコミュニティ VLAN 又は同一の独立 VLAN に所属するポート宛に、或いは VLAN 外の場合は無差別ポート宛に、通信先を制限する場合に使用します。コミュニティ VLAN を使用する場合、無差別ポートを所有する"プライマリ"VLAN とマッピングされなくてはなりません。独立 VLAN を使用する場合、単一の無差別ポートを所有するように設定しなくてはなりません。
- プライベート VLAN におけるポートの所属方法は静的な設定で行います。一度ポートがプライベート VLAN に所属すると、GVRP で他の VLAN に動的に移動できなくなります。
- プライベート VLAN をトランクモードに設定することはできません（P4-165 の"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。
- 無差別ポート又はホストポートを独立VLANに割り当てるには、"switch port private-vlan isolated"コマンドを使用します。
- プライマリ VLAN に関連付けられた無差別ポートは、同一プライマリ VLAN に所属する他のすべての無差別ポートと、又はセカンダリ VLAN に所属するすべてのポートと通信できます。

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 isolated

FXC3126/52のみ使用可能なコマンドです。インタフェースを独立VLANに割り当てます。"no"を前に置くことで、割り当てを解除します。

文法

switchport private-vlan isolated *isolated-vlan-id*
no switchport private-vlan isolated

- *isolated-vlan-id* – 独立 VLAN の ID（範囲：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

独立VLANに割り当てたホストポートはグループメンバ間で通信できないため、グループ外との通信は無差別ポート経由で行わなくてはなりません。

例

```
Console(config)#interface ethernet 1/3
Console(config-if)#switchport private-vlan isolated 3
Console(config-if)#
```

switchport private-vlan mapping

インタフェースをプライマリVLANにマッピングします。"no"を前に置くことで、マッピングを削除します。

文法

switchport private-vlan mapping *primary-vlan-id*
no switchport private-vlan mapping

- *primary-vlan-id* – プライマリ VLAN の ID（範囲：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 | isolated | primary]

- **community** – コミュニティ VLAN をすべて表示します。関連付けられたプライベート VLAN、割り当てられたホストポート情報も一緒に表示します。
- **isolated** – 独立 VLAN を表示します。割り当てられた無差別ポートとホストポート情報も一緒に表示します。"Primary"又は"Secondary"フィールドに表示しているのは、独立 VLAN の ID 番号です。
- **primary** – プライマリ VLAN をすべて表示します。割り当てられた無差別ポート情報も一緒に表示します。

初期設定

なし

コマンドモード

Privileged Executive

例

```
Console#show vlan private-vlan
Primary   Secondary       Type       Interfaces
--------  -----------  ----------  ------------------------------
     5                 primary     Eth1/ 3
     5         6       community    Eth1/ 4  Eth1/ 5
     0         8       isolated
Console#
```

4-18 GVRP and Bridge Extension Commands

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	4-178
show bridge-ext	bridge extension情報の表示	PE	4-179
switchport gvrp	インタフェースへのGVRPの有効化	IC	4-179
switchport forbidden vlan	インタフェースへの登録禁止VLANの設定	IC	4-169
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	4-180
garp timer	選択した機能へのGARPタイマーの設定	IC	4-180
show garp timer	選択した機能へのGARPタイマーの表示	NE, PE	4-181

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P3-91「VLAN基本情報の表示」及びP3-12「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:              255
 Max support vlan ID:                   4094
 Extended multicast filtering services: No
 Static entry individual port:          Yes
 VLAN learning:                         IVL
 Configurable PVID tagging:             Yes
 Local VLAN capable:                    No
 Traffic classes:                       Enabled
 Global GVRP status:                    Enabled
 GMRP:                                  Disabled
Console#
```

switchport gvrp

ポートのGVRPを有効に設定します。"no"を前に置くことで機能を無効にします。

文法

switchport gvrp

no switchport gvrp

初期設定

無効(Disabled)

コマンドモード

Interface Configuration (Ethernet, Port Channel)

例

```
Console(config)#interface ethernet 1/6
Console(config-if)#switchport gvrp
Console(config-if)#
```

show gvrp configuration

GVRPが有効かどうかを表示します。

文法

show gvrp configuration [*interface*]

- *interface*
  - **ethernet** *unit*/*port*
    - *unit* — ユニット番号"1"
    - *port* — ポート番号（範囲：1-16/26/52）
  - **port-channel** *channel-id*（範囲：1-4）

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値に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 (4-181)

show garp timer

選択したポートのGARPタイマーを表示します。

文法

show garp timer [*interface*]

- *interface*
  －**ethernet** *unit*/*port*
    －*unit* ― ユニット番号"1"
    －*port* ― ポート番号（範囲：1-16/26/52）
  －**port-channel** *channel-id*（範囲：1-4）

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 (4-180)

4-19 Priority Commands

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	4-183
Priority (Layer 3 and 4)	TCPポート、IP precedenceタグ、IP DSCPタグのCoS値への設定	4-189

Priority Commands (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	4-184
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	4-184
queue bandwidth	プライオリティキューに重み付けラウンドロビンを指定	GC	4-186
queue cos-map	プライオリティキューにClass of Service(CoS)を指定	IC	4-186
show queue mode	現在のキューモードを表示	PE	4-187
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	4-188
show queue cos-map	CoSマップの表示	PE	4-188
show interfaces switchport	インタフェースの管理、運用ステータスの表示	PE	4-127

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

プライオリティの設定はしてありません。タグなしフレームへの初期設定値は0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

- プライオリティマッピングの優先順位は IP ポート、IP precedence 又は IP DSCP、デフォルトプライオリティの順番です。
- デフォルトプライオリティは、タグなしフレームを受信した際に設定されます。
  入力されたフレームが IEEE8021Q タグ付フレームの場合、IEEE802.1p のプライオリティ bit が使用されます。このプライオリティは IEEE802.1Q VLAN tagging フレームには適用されません。
- 本機では 8 段階のプライオリティキューを各ポートに提供します。それらは重み付けラウンドロビンを使用し、"**show queue bandwidth**"コマンドを使用し確認することが可能です。タグ VLAN ではない入力フレームは入力ポートでタグによりデフォルトプライオリティを付けられ、適切なプライオリティキューにより出力ポートに送られます。
  すべてのポートのデフォルトプライオリティは"0"に設定されています。したがって、初期設定ではプライオリティタグを持たないすべての入力フレームは出力ポートの"0"キューとなります（出力ポートがタグなしに設定されている場合、送信されるフレームは送信前にタグが取り外されます）

例

本例では3番ポートのデフォルトプライオリティを5に設定しています。

```
Console(config)#interface ethernet 1/3
Console(config-if)#switchport priority default 5
```

queue bandwidth

4つのCoSに対し重み付けラウンドロビン(Weighted Round-Robin / WRR)による重み付けを行います。"no"を前に置くことで初期設定に戻します。

文法

queue bandwidth *weight1...weight4*
no queue bandwidth

- *weight1...weight4* — キュー0～3のWRRスケジューラで使用される重みの比率（範囲：1-31）

初期設定

1、2、4、6がそれぞれキュー0-3に対応しています。キュー0は設定できません。

コマンドモード

Global Configuration

コマンド解説

WRRはスケジューリングされた重さでの出力ポートでのバンド幅の共用を許可します。

例

本例ではWRRの重み付けを行っています。

```
Console(config)#queue bandwidth 6 9 12
Console(config)#
```

関連するコマンド

show queue bandwidth (4-188)

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
  —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。

プライオリティ	0	1	2	3
キュー	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 1 2
Console(config-if)#queue cos-map 1 3
Console(config-if)#queue cos-map 2 4 5
Console(config-if)#queue cos-map 3 6 7
Console(config-if)#end
Console#show queue cos-map ethernet 1/1
Information of Eth 1/1
 CoS Value     : 0 1 2 3 4 5 6 7
 Priority Queue: 0 0 0 1 2 2 3 3
Console#
```

関連するコマンド

show queue cos-map (4-188)

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

4つのプライオリティキューにより設定された重み付けラウンドロビン(WRR)バンド幅を表示します。

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#show queue bandwidth
 Queue ID Weight
 -------- ------
    0       1
    1       2
    2       4
    3       6
Console#
```

show queue cos-map

CoSプライオリティマップを表示します。

文法

show queue cos-map [*interface*]

- *interface*
  - **ethernet** *unit*/*port*
    - *unit* — ユニット番号"1"
    - *port* — ポート番号（範囲：1-16/26/52）
  - **port-channel** *channel-id*（範囲：1-4）

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#
```

Priority Commands (Layer 3/4)

コマンド	機能	モード	ページ
map ip port	TCP CoSマッピングの有効化	GC	4-189
map ip port	TCPソケットのCoSへのマッピング	IC	4-190
map ip precedence	IP precedence CoSマップの有効化	GC	4-191
map ip precedence	IP precedence値のCoSへのマップ	IC	4-191
map ip dscp	IP DSCP CoSマップの有効化	GC	4-192
map ip dscp	IP DSCP CoSのマップ	IC	4-193
map access-list ip	パケットがACLルールに一致するよう、CoS値と各出力キューとを設定	IC	4-103
map access-list mac	パケットがACLルールに一致するよう、CoS値と各出力キューとを設定	IC	4-108
show map ip port	IPポートのマッピング情報を表示	PE	4-194
show map ip precedence	IP precedenceマップの表示	PE	4-194
show map ip dscp	IP DSCPマップの表示	PE	4-195
show map access-list ip	インタフェースのアクセスリストにマッピングされたCoS値の表示	PE	4-104
show map access-list mac	インタフェースのアクセスリストにマッピングされたCoS値の表示	PE	4-109

map ip port (Global Configuration)

IPポートのマッピング（CoSのTCP/UDPソケットへのマッピング）を有効に設定します。"no"を前に置くことでIPポートのマッピングを無効に設定します。

文法

map ip port

no map ip port

初期設定

無効(Disabled)

コマンドモード

Global Configuration

コマンド解説

プライオリティマッピングの優先順位はIPポート、IP precedence又はIP DSCP及び、スイッチポートプライオリティです。

例

本例では本機全体のTCP/UDPポートのマッピングを有効に設定しています。

```
Console(config)#map ip port
Console(config)#
```

map ip port (Interface Configuration)

IPポートプライオリティ（TCP/UDPポートプライオリティ）を設定します。"no"を前に置くことで設定内容を削除します。

文法

map ip port *port-number* **cos** *cos-value*

no map ip port *port-number*

- *port-number* ― TCP/UDP ポート番号（範囲：1-65535）
- *cos-value* ― CoS 値（範囲：0-7）

初期設定

なし

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 ポート、IP precedence 又は IP DSCP 及び、スイッチポートプライオリティです。
- このコマンドは、すべてのインタフェースの IP ポートプライオリティを設定します。

例

本例ではHTTPパケットをCoS値0にマッピングしています。

```
Console(config)#interface ethernet 1/5
Console(config-if)#map ip port 80 cos 0
Console(config-if)#
```

map ip precedence (Global Configuration)

IP precedenceマッピング(ToS)を有効にします。"no"を前に置くことで本機能を無効にします。

文法

map ip precedence

no map ip precedence

初期設定

無効(Disabled)

コマンドモード

Global Configuration

コマンド解説

- プライオリティマッピングの優先順位は IP ポート、IP precedence 又は IP DSCP 及び、スイッチポートプライオリティです。
- IP precedence 及び IP DSCP は両方を有効にすることはできません。一方を有効にした場合、他方は自動的に無効になります。

例

本例では本機にIP precedenceマッピングを設定しています。

```
Console(config)#map ip precedence
Console(config)#
```

map ip precedence (Interface Configuration)

IP precedenceプライオリティ(ToS)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

map ip precedence *ip-precedence-value* **cos** *cos-value*

no map ip precedence

- *ip-precedence-value* — 3-bit の優先値（範囲：0-7）
- *cos-value* — CoS 値（範囲：0-7）

初期設定

初期設定のプライオリティマッピングは以下の通りです。

IP Precedence値	0	1	2	3	4	5	6	7
CoS値	0	1	2	3	4	5	6	7

コマンドモード

Interface Configuration (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 ポート、IP precedence 又は IP DSCP 及び、スイッチポートプライオリティです。
- IP 優先値と CoS 値は IEEE802.1p 標準の推奨により初期設定において1対1でマッピングされ、キューの初期値が設定され、それにより8段階のハードウェアキューにマッピングされます。
- 本コマンドを使用すると IP 優先がすべてのインタフェースにセットされます。

例

本例ではIP precedence値1をCoS値0に設定しています。

```
Console(config)#interface ethernet 1/5
Console(config-if)#map ip precedence 1 cos 0
Console(config-if)#
```

map ip dscp (Global Configuration)

IP DSCP (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(Disabled)

コマンドモード

Global Configuration

コマンド解説

- プライオリティマッピングの優先順位は IP ポート、IP precedence 又は IP DSCP 及び、ポートプライオリティです。

- IP precedence 及び IP DSCP は両方を有効にすることはできません。一方を有効にした場合、他方は自動的に無効になります。

例

本例では本機にIP DSCPマッピングを有効にしています。

```
Console(config)#map ip dscp
Console(config)#
```

map ip dscp (Interface Configuration)

IP DSCP (Differentiated Services Code Point)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

map ip dscp *dscp-value* **cos** *cos-value*

no map ip dscp

- *dscp-value* ― 8-bit DSCP 値（範囲：0-63）
- *cos-value* ― CoS 値（範囲：0-7）

初期設定

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 ポート、IP precedence 又は IP DSCP 及び、ポートプライオリティです。
- DSCP プライオリティは IEEE802.1p 標準で推奨されている CoS 初期値にマッピングされ、その後、それに続けて 4 つのハードウェアプライオリティキューにマッピングされます。
- このコマンドは、すべてのインタフェースの IP DSCP プライオリティを設定します。

例

本例ではIP DSCP値1をCoS値0に設定しています。

```
Console(config)#interface ethernet 1/5
Console(config-if)#map ip dscp 1 cos 0
Console(config-if)#
```

show map ip port

IPポートプライオリティマップの表示を行います。

文法

show map ip port [*interface*]

- *interface*
  - **ethernet** *unit*/*port*
    - *unit* — ユニット番号"1"
    - *port* — ポート番号（範囲：1-16/26/52）
  - **port-channel** *channel-id*（範囲：1-4）

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#show map ip port
TCP port mapping status: enabled

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

関連するコマンド

map ip port (Global Configuration) (4-189)

map ip port (Interface Configuration) (4-190)

show map ip precedence

IP precedenceプライオリティマップの表示を行います。

文法

show map ip precedence [*interface*]

- *interface*
  - **ethernet** *unit*/*port*
    - *unit* — ユニット番号"1"
    - *port* — ポート番号（範囲：1-16/26/52）
  - **port-channel** *channel-id*（範囲：1-4）

初期設定

なし

コマンドモード

Privileged Exec

例

```
Console#show map ip precedence ethernet 1/5
Precedence mapping status: enabled

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

関連するコマンド

map ip port (Global Configuration) (4-189)
map ip precedence (Interface Configuration) (4-191)

show map ip dscp

IP DSCPプライオリティマップの表示を行います。

文法

show map ip dscp [*interface*]

- *interface*
  - **ethernet** *unit*/*port*
    - *unit* — ユニット番号"1"
    - *port* — ポート番号（範囲：1-16/26/52）
  - **port-channel** *channel-id*（範囲：1-4）

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: enabled

 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) (4-192)
map ip dscp (Interface Configuration) (4-193)

4-20 Multicast Filtering Commands

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	4-197
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	4-201
Static Multicast Routing	静的マルチキャストルータポートの設定	4-204

IGMP Snooping Commands

コマンド	機能	モード	ページ
ip igmp snooping	IGMP snoopingの有効化	GC	4-197
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	4-198
ip igmp snooping version	SnoopingのIGMPバージョンの設定	GC	4-199
show ip igmp snooping	IGMP snoopingの設定の表示	PE	4-199
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	4-200

ip igmp snooping

IGMP snoopingを有効にします。"no"を前に置くことで機能を無効にします。

文法

ip igmp snooping
no ip igmp snooping

初期設定

有効(Enabled)

コマンドモード

Global Configuration

例

本例ではIGMP snoopingを有効にしています。

```
Console(config)#ip igmp snooping
Console(config)#
```

ip igmp snooping vlan static

マルチキャストグループにポートを追加します。"no"を前に置くことでグループからポートを削除します。

文法

ip igmp snooping vlan *vlan-id* **static** *ip-address interface*
no ip igmp snooping vlan vlan-id static *ip-address interface*

- *vlan-id* — VLAN ID（範囲：1-4094）
- *ip-address* — マルチキャストグループの IP アドレス
- *interface*
  - **ethernet** *unit/port*
    - *unit* — ユニット番号"1"
    - *port* — ポート番号（範囲：1-16/26/52）
  - **port-channel** *channel-id*（範囲：1-4）

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}
no ip igmp snooping version

- 1 — IGMP Version 1
- 2 — IGMP Version 2

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)#
```

show ip igmp snooping

IGMP snoopingの設定情報を表示します。

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

表示される内容に関しては、P3-114「IGMP Snooping・Queryパラメータの設定」を参照して下さい。

例

本例では現在のIGMP snoopingの設定を表示しています。

```
Console#show ip igmp snooping
 Service status: Enabled
 Querier status: Enabled
 Query count: 2
 Query interval: 125 sec
 Query max response time: 10 sec
 Router port expire time: 300 sec
 IGMP snooping version: Version 2
Console#
```

show mac-address-table multicast

マルチキャストアドレスとして認識されているリストを表示します。

文法

show mac-address-table multicast [**vlan** *vlan-id*]
[**user** | **igmp-snooping**]

- *vlan-id* — VLAN ID（範囲：1-4094）
- **user** — ユーザ設定のマルチキャストエントリのみ表示
- **igmp-snooping** — IGMP snoopingによって学習されたアドレスのみ表示

初期設定

なし

コマンドモード

Privileged Exec

コマンド解説

メンバーの種類は選択したオプションによりIGMP又はUSERを含む表示がされます。

例

本例ではVLAN 1でIGMP snoopingにより登録されたマルチキャストエントリを表示しています。

```
Console#show mac-address-table multicast vlan 1 igmp-snooping
 VLAN M'cast IP addr. Member ports Type
 ---- --------------- ------------ -------
    1        224.1.2.3    Eth1/11   IGMP
Console#
```

IGMP Query Commands (Layer 2)

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	4-201
ip igmp snooping query-count	クエリーカウントの設定	GC	4-201
ip igmp snooping query-interval	クエリー間隔の設定	GC	4-202
ip igmp snooping query-max-response-time	レポート遅延の設定	GC	4-203
ip igmp snooping router-port-expire-time	クエリータイムアウトの設定	GC	4-204

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-count

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 (4 -203)

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

IGMP snoopingレポートの回答待ち時間を設定します。"no"を前に置くことで初期設定に戻します。

文法

ip igmp snooping query-max-response-time *seconds*

no ip igmp snooping query-max-response-time

- *seconds* — IGMP クエリの回答待ち時間（範囲：5-30(秒)）

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)#
```

関連するコマンド

ip igmp snooping version (4-199)

ip igmp snooping query-max-response-time (4 -203)

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 (4-199)

Static Multicast Routing Commands

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	4-204
show ip igmp snooping mrouter	マルチキャストルータポートの表示	PE	4-205

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：1-16/26/52）
  - **port-channel** *channel-id*（範囲：1-4）

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#
```

4-21 IP Interface Commands

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。

Basic IP Configuration

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	4-207
ip default-gateway	本機と管理端末を接続するためのゲートウェイの設定	GC	4-208
ip dhcp restart	BOOTP/DHCPクライアントリクエストの送信	PE	4-209
show ip interface	本機のIP設定の表示	PE	4-210
show ip redirects	本機のデフォルトゲートウェイ設定の表示	PE	4-210
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	4-211

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 (4-209)

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 (4-210)

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 (4-207)

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 (4-210)

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

show ip interface (4-210)

ping

ネットワーク上の他のノードに対しICMP echoリクエストパケットを送信します。

文法

ping *host* [**count** *count*][**size** *size*]

- *host* — ホストの IP アドレス/エイリアス
- *count* — 送信するパケット数（範囲：1-16、初期設定：5）
- *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。

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: 0 ms
Ping statistics for 10.1.0.9:
  5 packets transmitted, 5 packets received (100%), 0 packets lost
(0%)
Approximate round trip times:
  Minimum = 0 ms, Maximum = 10 ms, Average = 8 ms
Console#
```

関連するコマンド

interface (4-117)

付-A トラブルシューティング

Telnet又はWebブラウザ、SNMPソフトウェアから接続できない。

- スイッチに電源が投入されていることを確認して下さい。
- 管理端末とスイッチを接続するネットワークケーブルが、正しく接続されていることを確認して下さい。
- スイッチとの接続と接続先のポートが、無効になっていないか確認して下さい。
- 有効なIPアドレス、サブネットマスク、及びデフォルトゲートウェイが設定されたエージェントであることを確認して下さい。
- 管理端末が管理VLAN（初期設定ではVLAN 1）に接続していることを確認して下さい。
- 管理端末のIPアドレスが、スイッチが接続しているIPインタフェースと同じサブネットのIPアドレスであることを確認して下さい。
- タグ付VLANグループに所属するIPアドレスを使用してスイッチへの接続を行おうとしている場合は、管理端末、及びネットワークへの接続を中継するスイッチに接続しているポートの設定が正しいタグになっていることを確認して下さい。
- Telnetで接続できない場合は、同時に接続できるTelnetセッション数の最大値を超過している可能性があります。
  時間を置いて再度接続してみて下さい。

セキュアシェルを使用した接続ができない。

- SSHでの接続ができない場合は、同時に接続できるTelnet/SSHセッション数の最大値を超過している可能性があります。
  時間を置いて再度接続してみて下さい。
- SSHサーバの制御パラメータがスイッチに対して正しく設定されており、SSHクライアントソフトウェアが管理端末に対して正しく設定されていることを確認して下さい。
- スイッチの公開キーを生成し、このキーをSSHクライアントに提供していることを確認して下さい。
- 各SSHユーザアカウント（ユーザ名、認証レベル、パスワードを含む）を設定していることを確認して下さい。
- （公開キーによる認証機能を使用している場合）クライアントの公開キーをスイッチに取り込んでいることを確認して下さい。

シリアルポート接続から内蔵の設定プログラムに接続できない。

・ターミナルエミュレーションプログラムが、以下の通り設定されていることを確認して下さい。

ターミナル：	VT100互換
データビット：	8ビット
ストップビット：	1ビット
パリティ：	なし
通信速度：	9600 bps

・同梱のシリアルケーブルを使用していることを確認して下さい。

パスワードを無くしてしまった、又は忘れてしまった。

・お買い上げの販売店または、当社指定のサービス窓口にご連絡下さい。

付-B シリアルポート経由のファームウェアアップグレード

本機には、diagnostics（又はBoot-ROM）コード、runtime operationコード、及びloaderコードの3種類のアップグレード可能なファームウェアがあります。runtimeコードは、シリアル接続、TFTPサーバを利用したネットワーク接続及びSNMP管理ソフトウェアを利用してアップグレードが行えます。diagnosticsコード及びloaderコードは、シリアル接続でしかアップグレードを行うことができません。

注意 TFTPを使用しWebインタフェースからruntimeコードをダウンロードすることができます。サイズの大きいruntimeコードは、シリアル経由でのダウンロードよりもWebインタフェース経由の方が早くダウンロードすることができます。

ファームウェアのアップグレードは、XModemプロトコルをサポートするVT100互換のターミナルソフトウェアを利用しシリアル接続で行うことができます。詳細はP2-2「接続手順」を参照して下さい。

① 本機と管理端末をシリアルケーブルで接続します。

② ターミナルソフトウェアの設定をデータビット：8ビット、ストップビット：1ビット、パリティ：なし、通信速度：9600bps、フローコントロール：なし、に設定します。

③ 本機の電源を投入します。

④ 電源が入ってすぐに、<Ctrl>と<U>キーを押します。
システムファイルメニューに入ります。メニューに入ると以下のような画面が表示されます。

```
File Name                    S/Up Type Size            Create Time
---------------------------- ---- ---- -------------- -----------
$certificate                   0    7          20480  00:38:34
$logfile_1                     0    3            576
 runtime                       0    3        1674556  00:00:02
Factory_Default_Config.cfg     0    5           2574  00:00:12
diag_                          1    1         116228  00:00:00
---------------------------- ---- ---- -------------- -----------
[X]modem Download [D]elete File [S]et Startup File
[C]hange Baudrate [Q]uit
Select>
```

⑤ <C>キーを押し、本機のボーレートを変更します。

⑥ <B>キーを押し、115200ボーに設定します。
2つのボーレートのどちらも使用することができます。高いボーレートにすることによりファームウェアのダウンロード時間を短縮することができます。

⑦ ターミナルソフトウェアのボーレートも115200 bpsに設定します。<Enter>キーを押し、本機との接続をリセットします。

```
Select>
Change baudrate [A]9600 [B]115200
Baudrate set to 115200
```

⑧ ファームウェアのダウンロードを行う前に、新しいコードをダウンロードするメモリスペースがあるかどうかの確認を行います。
必要に応じて**[D]elete File**コマンドを使用し、runtime又はdiagnosticコードを削除して下さい。

⑨ <X>キーを押し、新しいコードファイルのダウンロードを行います。
ハイパーターミナルを使用している場合には、[送信]→[ファイルの送信...]を選択します。転送するファイルを指定した後、プロトコルでXmodemを選択し、[送信]をクリックします。以上の手順によりファームウェアの転送が行われます。

注意 ダウンロードするファイルは、弊社より提供する本機用のバイナリファイルを必ず使用して下さい。

⑩ ファイルのダウンロードが終了後、表示されている"Update Image File:"プロンプトに続けて、コードファイルのタイプを指定します。<R>キーでruntimeコードを、<L>キーでloaderコードを指定できます。

注意 <L>キーでloaderコードを指定する場合、指定するファイルが有効なloaderコードであることを事前に必ず確認して下さい。有効ではないファイルをダウンロードした場合、本機は起動しなくなります。安全のため、必要がない場合にはloaderコードファイルをダウンロードしないで下さい。

⑪ ダウンロードコードファイル名を指定します。ファイル名は大文字小文字の区別がされ、最大31文字です。ファイル名にはスラッシュが入れられません。また、ファイルの頭文字にはピリオド（.）は入れられません。
有効な文字はA-Z, a-z, 0-9, ".", "-", "_"です。

以下の例はruntimeコードファイルをダウンロードする手順を示しています。

```
Select>
Xmodem Receiving Start ::
Image downloaded to buffer.

          [R]untime
          [D]iagnostic
          [L]oader (Warning: you sure what you are doing?)
Update Image File:r
Diagnostic Image Filename : r_20019
Updating file system.
File system updated.
[Press any key to continue]
```

⑫ 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ためには**[S]et Startup File**メニューオプションを使用します。

⑬ コードファイルのダウンロードが終了した後、**[C]hange Baudrate**でボーレートを9600ボーに戻します。

⑭ PC側のターミナルソフトのボーレートも同じく9600ボーに戻します。<Enter>キーを押し、接続をリセットします。

⑮ <Q>キーを押し、システムファイルメニューを終了し、本機を起動します。

■制限事項

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

FXC3116/3126/3152 マネージメントガイド

２００９年５月 第３版

・ 改良のため製品の仕様を予告なく変更することがありますが、ご了承ください。

・ 予告なく本書の一部または全体を修正、変更することがありますが、ご了承ください。

・ ユーザマニュアルの内容に関しましては、万全を期しておりますが、万一ご不明な点がございましたら、弊社サポートセンターまでご相談ください。

(FXC06-DC-200017-R1.2)